Université Rennes 1
École Normale Supérieure de Rennes

Couplages et développements pour l'agrégation externe

Gabriel Lepetit

2016 – 2017

Table des matières

Chapitre 1

Couplages

SECTION 1.1

Liste de développements

Algèbre

1 $\mathfrak{A}_n$ est simple pour $n \geqslant 5$: *103, 104*, 105, *108*

2 Automorphismes de $\mathfrak{S}_n$: 105, 108

3 Borne de Bézout : 142, 144, 152

4 Chevalley-Warning et Erdös-Ginsburg-Ziv : 120, *121*, 123, 142, 144

5 Décomposition de Dunford par la méthode de Newton : 153, 155, 157

6 Endomorphismes semi-simples : 122, 153, 154, 155.

7 Étude de $O(p,q)$: 106, 150, 156, *158, 170*, 171

8 Formule de Poisson discrète : 110

9 Invariants de similitude : 150, 153, 154, 159

10 Irréductibilité des polynômes cyclotomiques : 102, *120, 125*, 141, *144*

11 Points extrémaux de la boule unité de $\mathscr{L}(E)$: 160, 161, 181

12 Polynômes irréductibles sur $\mathbb{F}_q$: 123, 125, 141, 190

13 Réciprocité quadratique : 101, 120, 121, *123, 126*, 170, 190

14 Sous-groupes distingués et table de caractères : 103, *104*, 107

15 Théorème d'Artin : 125, 151, 162

16 Théorème de Carathéodory et équations diophantiennes : 126, 181

17 Théorème de structure des groupes abéliens finis : 102, 104, 107, 110

18 Théorème des deux carrés : *120*, 121, 122, 126

19 Théorème de Sylow : 101, 103, 104

Analyse

1 Banach-Steinhaus et séries de Fourier : 205, 208, 209, *241*, 246

2 Diagonalisation des opérateurs symétriques compacts : 203, *205*, 213

3 Espace de Bergman : 201, 202, 205, *208*, 213, 234, *235*, 243, 245

4 Formule des compléments : *207*, 235, 236, *239*, *245*

5 Formule sommatoire de Poisson : *241*, 246, 250

6 Inégalité de Hoeffding : 253, 260, 262

7 Inversion de Fourier dans $\mathscr{S}(\mathbb{R})$: 236, 239, 250

8 La fonction caractéristique caractérise la loi : 261, 263

9 Méthode de Newton : *218*, 223, 226, 228

10 Nombre de zéros d'une équation différentielle : 220, 221, 224

11 Processus de Poisson : 263, 264

12 Prolongement de Γ : 207, 239, 241, 245

13 Quelques ordres moyens : *223*, 224, 230

14 Théorème central limite : 218, 261, 262, *263*

15 Théorème d'Abel angulaire et taubérien faible : 207, 223, 230, 235, 243

16 Théorème de Grothendieck : 201, 208, *213*, 234

17 Théorème de Helly : 203, 229, 241, *262*

18 Théorème de Liapounov : 220, 221

19 Théorème de Weierstrass par les polynômes de Bernstein : 202, 209, 228, 260, 264

Mixte

1 $SO_3(\mathbb{R})$ est simple : *103*, 106, 108, 160, 161, 204

2 Ellipsoïde de John-Loewner : 152, *158*, *171*, 203, *219*, 229, 253

3 Lemme de Morse : 158, 170, 171, 214, 215, 218

4 Méthode de gradient conjugué : 158, *162*, 219, *226*, 233

5 Méthodes itératives de résolution d'un système linéaire : 157, 162, 226, 233

6 Surjectivité de l'exponentielle : 153, 156, 204, *214*

7 Théorème des extréma liés : 151, 159, 214, 215, 219

SECTION 1.2

Leçons d'algèbre

101 Groupe opérant sur un ensemble. Exemples et applications.

- Théorème de Sylow
- Réciprocité quadratique

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

- Irréductibilité des polynômes cyclotomiques
- Théorème de structure des groupes abéliens finis

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

- Théorème de Sylow
- Sous-groupes distingués et table de caractères
- $SO_3(\mathbb{R})$ *est simple*
- $\mathfrak{A}_n$ *est simple*

104 Groupes finis. Exemples et applications.

- Théorème de Sylow
- Théorème de structure des groupes abéliens finis
- $\mathfrak{A}_n$ *est simple pour* $n \geqslant 5$
- *Sous-groupes distingués et table de caractères*

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

- $\mathfrak{A}_n$ est simple pour $n \geqslant 5$
- Automorphismes de $\mathfrak{S}_n$

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

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

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

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

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

- $SO_3(\mathbb{R})$ est simple
- Automorphismes de $\mathfrak{S}_n$
- $\mathfrak{A}_n$ *est simple*

110 Caractères d'un groupe abélien fini et transformée de Fourier discrète. Applications.

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

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

- Chevalley-Warning et EGZ
- Réciprocité quadratique
- *Théorème des deux carrés*

- *Irréductibilité des polynômes cyclotomiques*

121 Nombres premiers. Applications.

- Théorème des deux carrés
- Réciprocité quadratique
- *Chevalley-Warning et EGZ*

122 Anneaux principaux. Exemples et applications.

- Théorème des deux carrés
- Endomorphismes semi-simples

123 Corps finis. Applications.

- Polynômes irréductibles sur $\mathbb{F}_q$
- Chevalley-Warning et EGZ
- *Réciprocité quadratique*

125 Extensions de corps. Exemples et applications.

- Polynômes irréductibles sur $\mathbb{F}_q$
- Théorème d'Artin
- *Irréductibilité des polynômes cyclotomiques*

126 Exemples d'équations diophantiennes

- Théorème des deux carrés
- Théorème de Carathéodory et équations diophantiennes
- *Réciprocité quadratique*

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

- Polynômes irréductibles sur $\mathbb{F}_q$
- Irréductibilité des polynômes cyclotomiques

142 Algèbre des polynômes à plusieurs indéterminées. Applications.

- Chevalley-Warning et EGZ
- Borne de Bézout

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

- Borne de Bézout
- Chevalley-Warning et EGZ
- *Irréductibilité des polynômes cyclotomiques*

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

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

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

- Théorème des extréma liés
- Théorème d'Artin

152 Déterminant. Exemples et applications.

- Ellipsoïde de John-Loewner
- Borne de Bézout

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

- Invariants de similitude
- Décomposition de Dunford par la méthode de Newton
- *Endomorphismes semi-simples*
- *Surjectivité de l'exponentielle*

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

- Invariants de similitude
- Endomorphismes semi-simples

155 Endomorphismes diagonalisables en dimension finie.

- Dunford par la méthode de Newton
- Endomorphismes semi-simples

156 Exponentielle de matrices. Applications.

- Surjectivité de l'exponentielle
- Étude de $O(p,q)$.

157 Endomorphismes trigonalisables. Endomorphismes nilpotents.

- Dunford par la méthode de Newton
- Méthodes itératives de résolution d'un système linéaire.

158 Matrices symétriques réelles, matrices hermitiennes.

- Lemme de Morse
- Méthode de gradient conjugué
- *Étude de $O(p,q)$*
- *Ellipsoïde de John-Loewner*

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

- Invariants de similitude
- Théorème des extréma liés

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

- $SO_3(\mathbb{R})$ est simple
- Points extrémaux de la boule unité de $\mathscr{L}(E)$

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

- $SO_3(\mathbb{R})$ est simple
- Points extrémaux de la boule unité de $\mathscr{L}(E)$

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

- Théorème d'Artin
- Méthodes itératives de résolution d'un système linéaire
- *Méthode de gradient conjugué*

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

- Lemme de Morse
- Réciprocité quadratique
- *Étude de* $O(p,q)$

171 Formes quadratiques réelles. Exemples et applications. Coniques.

- Lemme de Morse
- Étude de $O(p,q)$
- *Ellipsoïde de John-Loewner*

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

- Théorème de Carathéodory
- Points extrémaux de la boule unité de $\mathscr{L}(E)$.

182 Applications des nombres complexes à la géométrie

183 Utilisation des groupes en géométrie

190 Méthodes combinatoires, problèmes de dénombrement.

- Polynômes irréductibles sur $\mathbb{F}_q$
- Réciprocité quadratique

SECTION 1.3

Leçons d'analyse

201 Espaces de fonctions ; exemples et applications.

- Théorème de Grothendieck
- Espace de Bergman

202 Exemples de parties denses et applications.

- Théorème de Weierstrass
- Espace de Bergman

203 Utilisation de la notion de compacité

- Théorème de Helly
- Diagonalisation des opérateurs symétriques compacts
- *Ellipsoïde de John-Loewner*

204 Connexité. Exemples et applications.

- Surjectivité de l'exponentielle
- $SO_3(\mathbb{R})$ est simple

205 Espaces complets. Exemples et applications.

- Banach-Steinhaus et séries de Fourier
- Espace de Bergman
- *Diagonalisation des opérateurs symétriques compacts*

207 Prolongement de fonctions. Exemples et applications.

- Prolongement de Γ
- Théorème d'Abel angulaire et taubérien faible
- *Formule des compléments*

208 Espaces vectoriels normés, applications linéaires continues. Exemples.

- Théorème de Grothendieck
- Banach-Steinhaus et séries de Fourier
- *Espace de Bergman*

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

- Théorème de Weierstrass
- Banach-Steinhaus et séries de Fourier

213 Espaces de Hilbert. Bases hilbertiennes. Exemples et applications

- Espace de Bergman
- Diagonalisation des opérateurs symétriques compacts
- *Théorème de Grothendieck*

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

- Lemme de Morse
- Théorème des extrémas liés
- *Surjectivité de l'exponentielle*

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

- Lemme de Morse
- Théorème des extrémas liés

218 Applications des formules de Taylor.

- Lemme de Morse
- Théorème central limite
- *Méthode de Newton*

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

- Théorème des extréma liés
- Méthode de gradient conjugué
- *Ellipsoïde de John-Loewner*

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

- Théorème de Lyapunov
- Nombre de zéros d'une équation différentielle

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

- Théorème de Lyapunov
- Nombre de zéros d'une équation différentielle

222 Exemples d'équations aux dérivées partielles linéaires

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

- Méthode de Newton
- Théorème d'Abel angulaire et taubérien faible
- *Quelques ordres moyens*

224 Exemples de développements asymptotiques de suites et de fonctions

- Nombre de zéros d'une équation différentielle
- Quelques ordres moyens

226 Suites vectorielles et réelles définies d'une variable réelle. Exemples et applications à la résolution approchée d'équations.

- Méthode de Newton
- Méthodes itératives de résolution d'un système linéaire
- *Méthode de gradient conjugué*

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

- Méthode de Newton
- Théorème de Weierstrass

229 Fonctions monotones. Fonctions convexes. Exemples et applications.

- Théorème de Helly
- Ellipsoïde de John-Loewner

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

- Théorème d'Abel angulaire et taubérien faible

- Quelques ordres moyens

233 Méthodes itératives en analyse numérique matricielle.

- Méthodes itératives de résolution d'un système linéaire
- Méthode de gradient conjugué

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

- Théorème de Grothendieck
- Espace de Bergman

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

- Formule des compléments
- Théorème d'Abel angulaire et taubérien faible
- *Espace de Bergman*

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

- Inversion de Fourier
- Formule des compléments

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

- Prolongement de Γ
- Inversion de Fourier
- *Formule des compléments*

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

- Théorème de Helly
- Prolongement de Γ
- *Banach-Steinhaus et séries de Fourier*
- *Formule sommatoire de Poisson*

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

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

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

- Espace de Bergman
- Prolongement de Γ
- *Formule des compléments*

246 Séries de Fourier. Exemples et applications.

- Formule sommatoire de Poisson
- Banach-Steinhaus et séries de Fourier

250 Transformation de Fourier. Applications.

- Formule sommatoire de Poisson
- Inversion de Fourier

253 Utilisation de la notion de convexité en analyse.

- Ellipsoïde de John-Loewner
- Inégalité de Hoeffding

260 Espérance, variance et moments de variables aléatoires.

- Inégalité de Hoeffding
- Théorème de Weierstrass

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

- Théorème central limite
- La fonction caractéristique caractérise la loi

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

- Théorème central limite
- Inégalité de Hoeffding
- *Théorème de Helly*

263 Variables aléatoires à densité. Exemples et applications.

- Processus de Poisson
- La fonction caractéristique caractérise la loi
- *Théorème central limite*

264 Variables aléatoires discrètes

- Théorème de Weierstrass
- Processus de Poisson

SECTION 1.4

Bibliographie commentée

1.4.1 Les indispensables

GOURDON 2009a et GOURDON 2009b : incontournables sur quasiment toutes les leçons qui portent sur l'adhérence du programme de prépa. Il faut souvent aller voir dans les exos ou les « problèmes » à la fin de chaque partie pour avoir des résultats classiques.

ROUVIÈRE 2003 : les exercices de ce livre sont vite devenus des classiques ou des développements qui dépassent le simple cadre du calcul différentiel.

BECK, MALICK et PEYRÉ 2005 : à l'apparence austère, ce livre est génial parce qu'il ne donne généralement pas de démonstrations et beaucoup de résultats illustrant les notions de manière brillante. Très utile en algèbre linéaire et en calcul différentiel notamment.

OUVRARD 2009 et BARBÉ et LEDOUX 2007 : les deux ouvrages qui font quasiment tout en probabilités, surtout le deuxième qui est assez synthétique. Pour les choses basiques, on a aussi OUVRARD 2007.

HIRSCH et LACOMBE 2009 : tout ce qu'il faut sur l'analyse fonctionnelle

QUEFFÉLEC et ZUILY 2013 : pas optimal sur le plan pédagogique, ce livre touffu contient surtout beaucoup de développements potentiels, il ne peut pas vraiment servir de livre de base pour une leçon.

BONY 2001 : très clair sur la transformée de Fourier et les distributions, thèmes un peu à la marge du programme depuis cette année.

BRIANE et PAGÈS 2006 : très pédagogique, incontournable sur l'intégration et en particulier les probabilités

QUEFFÉLEC 1998 : un peu dans la même veine que le précédent, mais pour les leçons de topologie : 203, 204, 205.

HAUCHECORNE 2007 : permet d'éviter de chercher des contre-exemples dans sa tête (quelle idée...) ou dans plein de livres différents.

Les Francinou-Gianella : corrections d'exos de concours, ils ne contiennent donc souvent rien de nouveau, mais rassemblent par thèmes des résultats d'applications utiles.

AMAR et MATHERON 2003 : à condition de combiner avec d'autres livres d'analyse complexe comme TAUVEL 2006 pour éviter la théorie trop compliquée menant à la formule de Cauchy, c'est un ouvrage remarquable, avec tout ce qu'il y a à dire sur les fonctions holomorphes, notamment une belle partie sur l'utilisation du théorème des résidus, et une autre sur les produits infinis.

DEMAILLY 2006 : pour les équations différentielles, l'interpolation, l'intégration numérique.

GRIFONE 2011 : indispensable pour la leçon 151 notamment, un livre qui donne proprement les bases de l'algèbre linéaire, éludées dans les ouvrages plus complexes.

CALDERO et GERMONI 2013 et CALDERO et GERMONI 2015 : drôles et bien écrits, conçus pour permettre au lecteur de briller à l'oral

PERRIN 1996 : le livre le plus synthétique sur les groupes, les anneaux, les extensions de corps. Moins convaincant sur la géométrie.

GOZARD 1997 : pour les extensions de corps, très bien fait avec de la théorie de Galois abordable.

RUDIN 1970 : je ne l'aime pas tellement, mais il y a plein de belles choses sur l'analyse complexe notamment.

1.4.2 Les originaux

DURRETT 2010 : un livre de probabilités en anglais pour le moins éclectique, mais il y a de belles choses à trouver dedans (notamment l'application du théorème de Helly et des calculs de fonctions caractéristiques qu'on ne trouve pas ailleurs).

DE SEGUINS PAZZIS 2011 : la somme théologique des formes quadratiques, dont une petite partie seulement peut être utilisée pour l'agrégation. Complet et fait proprement, mais pas assez synthétique.

RISLER et BOYER 2006 : une preuve originale de Dunford. Utile aussi pour la leçon 120.

1.4.3 Les subsidiaires

FOATA et FUCHS 2003 : pour compléter les probas, surtout sur la leçon 261

COLMEZ 2011 : pour les représentations

BRÉZIS 2005 : certains adorent ce livre, je le trouve vieillot. Il contient beaucoup de choses savantes, mais pas forcément essentielles, sur l'analyse fonctionnelle. La partie sur Hahn-Banach est la seule vraiment indispensable.

SAINT-RAYMOND 2008 : pour compléter un peu les autres livres de topologie.

RAMIS, DESCHAMPS et ODOUX 1990 et RAMIS, DESCHAMPS et ODOUX 1995 : des manuels bien faits pour certaines leçons comme 142 et 229

MÉRINDOL 2006 : pour le résultant.

SZPIRGLAS 2009 : idem.

Chapitre 2

Développements

$\mathfrak{A}_n$ est simple

Leçons : *103, 104*, 105, *108*

Théorème 1

Le groupe $\mathfrak{A}_n$ est simple.

Démonstration. Étape 1 : cas $n = 5$.

Dans $\mathfrak{A}_5$, les types d'éléments suivants forment des classes de conjugaison distinctes :

- l'identité ;
- les 3-cycles : il y en a $\dfrac{5\times 4\times 3}{3} = 20$. En effet, $\mathfrak{A}_5$ est 3-transitif : si (abc) et $(a'b'c')$ sont deux 3-cycles, il existe $\sigma \in \mathfrak{A}_5$ tel que $\sigma(a) = a', \sigma(b) = b'$ et $\sigma(c) = c'$ donc $\sigma(abc)\sigma^{-1} = (a'b'c')$;
- les doubles transpositions : une double transposition de $\mathfrak{A}_5$ est déterminée par le choix de l'élément x laissé fixe (5 possibilités) et par celui de la double transposition restreinte à $[\![1,5]\!] \setminus \{x\}$ (3 possibilités), donc il y en a 15. Elles sont deux à deux conjuguées car si $\tau = (ab)(cd)(e)$ et $\tau' = (a'b')(c'd')(e')$, il existe par 3-transitivité $\sigma \in \mathfrak{A}_5$ envoyant (c,d,e) sur (c',d',e'). Par conséquent, elle envoyant également l'ensemble $\{a,b\}$ sur $\{a',b'\}$ et $\sigma\tau\sigma^{-1} = \tau'$.

Pour des raisons d'ordre, les classes sont bien distinctes. Par ailleurs, il y a $\dfrac{5\times 4\times 3\times 2}{5} =$ 24 5-cycles dans $\mathfrak{A}_5$, et cela achève le catalogue de ses éléments.

Soit H un sous-groupe distingué non trivial de $\mathfrak{A}_5$. Par le théorème de Lagrange, $|H|$ divise 60. De plus, si H contient un 3-cycle (resp. une double transposition), il les contient tous. Il en va de même pour les 5-cycles car si H contient un élément d'ordre 5, il contient le 5-Sylow engendré par cet élément, donc comme les 5-Sylow sont deux à deux conjugués (théorème de Sylow), il contient tous les 5-Sylow donc tous les éléments d'ordre 5.

Étant donné que ni $24+15+1 = 40$, ni $24+20+1 = 45$, ni $15+20+1 = 36$ ne divisent 60, il est impossible que H ne contienne que deux catégories d'éléments (et pour les mêmes raisons, il est exclu qu'il en contienne une seule). Donc il les contient tous : $H = \mathfrak{A}_5$.

Étape 2 : cas général, en se ramenant à l'étape 1.

Soit $n > 5$, $E = [\![1,n]\!]$, H un sous-groupe distingué non trivial de $\mathfrak{A}_n$. Soit $\sigma \in H$ distinct de l'identité. On peut donc fixer $a \in E$ tel que $b = \sigma(a) \neq a$. Soit $c \notin \{a, b, \sigma(b)\}$ et $\tau = (acb)$. On a $\tau^{-1} = (abc)$.

Introduisons le commutateur $\rho = \tau\sigma\tau^{-1}\sigma^{-1} = (\tau\sigma\tau^{-1})\sigma^{-1} \in H$. On a

$$\rho = (acb)(\sigma(a)\sigma(b)\sigma(c)) = (acb)(b\sigma(b)\sigma(c))$$

donc ρ laisse fixes au moins $n-5$ éléments : quitte à ajouter des éléments à l'ensemble $F = \{a, b, c, \sigma(b), \sigma(c)\}$, on peut supposer que c'est exactement le cas.

Soit $\varphi : \begin{array}{ccc} \mathfrak{A}(F) & \longrightarrow & \mathfrak{A}(E) \\ u & \longmapsto & \overline{u} \end{array}$ où $\overline{u}_{|F} = u$ et $\overline{u}_{|E\setminus F} = \mathrm{id}_{E\setminus F}$. On note $H_0 = \varphi^{-1}(F)$, c'est un sous-groupe distingué non trivial de $\mathfrak{A}_5$ car $\rho_{|F} \in H_0$, donc selon l'étape 1, $H_0 = \mathfrak{A}_5$.

En particulier, si u est un cycle d'ordre 3 de $\mathfrak{A}(F)$, alors $u \in H_0$ donc $\overline{u} \in H$ donc comme les 3-cycles sont deux à deux conjugués dans $\mathfrak{A}_n$ (voir étape 1), H contient tous les 3-cycles donc $H = \mathfrak{A}_n$ car les 3-cycles engendrent $\mathfrak{A}_n$.

□

Remarque.
- S'il reste un peu de temps, on peut expliquer pourquoi les 3-cycles engendrent $\mathfrak{A}_n$ (décomposer en produit pair de transpositions de la forme $(1\,i)$ et regrouper deux à deux).
- $\mathfrak{A}_4$ n'est pas simple car $\langle (12), (34) \rangle$ est un sous-groupe distingué d'ordre 4.

Référence : PERRIN 1996, pp. 28-30.

$SO_3(\mathbb{R})$ est simple

Leçons : ***103*****, 106, 108, 160, 161, 204**

Théorème 2

Le groupe $SO_3(\mathbb{R})$ est simple.

Lemme 3

1 *Les retournements (i.e. les rotations d'angle π) sont tous conjugués dans $SO_3(\mathbb{R})$.*

2 *Le centre de $SO_3(R)$ est réduit à* $\{\mathrm{id}\}$.

Démonstration. **1** Soient r_D, r'_D des retournements de droites respectives D et D'. Une rotation $s \in SO_3(\mathbb{R})$ de plan $\mathrm{Vect}(D, D')$ bien choisie envoie D sur D'. Donc sr_Ds^{-1} est une rotation de droite $s(D) = D'$ et d'angle π, c'est à dire r'_D.

2 Si h est une rotation de droite Δ et $g \in Z(SO_3(\mathbb{R}))$, on a $ghg^{-1} = h$. Mais ghg^{-1} est une rotation de droite $g(\Delta)$ donc g fixe toutes les droites donc est une homothétie. En dimension impaire, on a nécessairement $g = \mathrm{id}$. En dimension paire, il y a aussi $-\mathrm{id}$ donc en particulier, les $SO_{2n}(\mathbb{R})$ ne sont pas simples.

□

Démonstration (du théorème)**.** Soit H un sous-groupe distingué de $SO_3(\mathbb{R})$ non réduit à $\{\mathrm{id}\}$. Comme $SO_3(\mathbb{R})$ est engendré par les retournements, on montrera que $H = SO_3(\mathbb{R})$ en montrant qu'il contient tous les retournements. Comme les retournements sont conjugués dans $SO_3(\mathbb{R})$, il suffit de montrer que H en contient un pour qu'il les contienne tous.

Soit $h \neq I_3 \in G$ et $\varphi : \begin{array}{ccc} SO_3(\mathbb{R}) & \longrightarrow & \mathbb{R} \\ g & \longmapsto & \mathrm{Tr}(ghg^{-1}h^{-1}) \end{array}$. Par continuité de la trace, φ est continue.

Comme $SO_3(\mathbb{R})$ est compact et connexe par arcs, l'image de φ est un compact connexe par arcs de $\mathbb{R}$, c'est-à-dire un segment.

De plus, dans une base adaptée, $g \in SO_3(\mathbb{R})$ peut s'écrire :

$$g = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

donc $\mathrm{Tr}(g) = 1 + 2\cos\theta \in [0, 3]$.

Donc comme $\varphi(h) = \mathrm{Tr}(I_3) = 3$, l'image de φ est de la forme $[a, 3]$ pour un certain $a \geqslant 0$

Supposons que $a = 3$. Alors pour tout $g \in SO_3(\mathbb{R})$, $ghg^{-1}h^{-1}$ est une rotation d'angle 0 c'est à dire I_3 donc h est dans le centre de $SO_3(\mathbb{R})$ dont on a vu qu'il était réduit à $\{I_3\}$, ce qui est contradictoire.

Donc $a < 3$ et on peut trouver $n \in \mathbb{N}^*$ tel que $a < 1+2\cos\left(\frac{\pi}{n}\right) < 3$ car $1+2\cos\left(\frac{\pi}{n}\right) \xrightarrow[n\to+\infty]{} 3$. Ainsi, il existe $g_n \in SO_3(\mathbb{R})$ tel que $h_n = g_n h g_n^{-1} h^{-1}$ soit une rotation d'angle $\pm\frac{\pi}{n}$. Or, comme H est distingué, $h_n \in H$ donc le retournement h_n^n est dans H, ce qui conclut. □

Remarque.
- On peut montrer que pour tout $n \geqslant 1, SO_{2n+1}(\mathbb{R})$ est simple (cf GONNORD et TOSEL 1998), la preuve repose sur la structure de sous-variété de cet ensemble.
- Comme le développement est un peu court, on peut expliquer, à partir du théorème de Cartan-Dieudonné, pourquoi $SO_3(\mathbb{R})$ est engendré par les retournements. Ou bien dans la leçon 204, donner les raisons de la connexité de $SO_3(\mathbb{R})$: tout élément de ce groupe est conjugué à une matrice de rotation $\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Référence : CALDERO et GERMONI 2013, p. 239. Merci à Antoine Diez pour ce développement.

Automorphismes de $\mathfrak{S}_n$

Leçons : 105, 108

Définition 4

Un automorphisme de $\mathfrak{S}_n$ de la forme $\varphi_\sigma : \tau \mapsto \sigma\tau\sigma^{-1}$ est appelé automorphisme intérieur. Le groupe des automorphismes intérieurs est noté $\mathrm{Int}(\mathfrak{S}_n)$.

Théorème 5

Si $n \neq 6$, $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$.

On va commencer par prouver la proposition suivante :

Proposition 6

Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. Si φ envoie les transpositions sur les transpositions, alors $\varphi \in \mathrm{Int}(\mathfrak{S}_n)$.

Démonstration. Soit φ un tel automorphisme. On sait que $\mathfrak{S}_n$ est engendré par les transpositions $\tau_i = (1\,i)$ pour $i \geqslant 2$. Comme les τ_i ne commutent pas deux à deux, il en va de même des $\varphi(\tau_i)$ donc les $\varphi(\tau_i)$ ne sont pas à supports deux à deux disjoints.

Posons $\varphi(\tau_2) = (\alpha_1\,\alpha_2)$, alors, par exemple, $\varphi(\tau_3) = (\alpha_1\,\alpha_3)$. Comme pour $i > 3$, $\varphi(\tau_i)$ ne commute ni avec $\varphi(\tau_2)$, ni avec $\varphi(\tau_3)$, $\varphi(\tau_i)$ est de la forme $(\alpha_1\alpha_i)$. De plus, les α_i sont deux à deux distincts donc $\{\alpha_1, \ldots, \alpha_n\} = \{1, \ldots, n\}$. On a ainsi défini une permutation $\alpha \in \mathfrak{S}_n$. De plus, $\forall i \geqslant 2, \alpha\tau_i\alpha^{-1} = (\alpha_1\,\alpha_i) = \varphi(\tau_i)$, donc φ est intérieur. □

Démonstration (du théorème)**.** L'idée générale est de considérer l'action par conjugaison de $\mathfrak{S}_n$ sur lui-même. On note $c(s)$ le centralisateur d'un élément s.

Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. Pour $n \geqslant 2, D(\mathfrak{S}_n) = \mathfrak{A}_n$ [1] donc comme φ préserve les commutateurs, il envoie $\mathfrak{A}_n$ sur lui-même. Ainsi, l'image d'une transposition par φ est un élément d'ordre 2 donc un produit d'un nombre d'un impair k de transpositions disjointes. Si $n < 6$, $\mathfrak{A}_n$ ne contient pas de triples transpositions donc $k = 1$ ce qui conclut. Supposons à présent $n > 6$.

Soit $\tau = (a\,b)$. Alors

$$s \in c(\tau) \Leftrightarrow s\tau s^{-1} = \tau \Leftrightarrow (s(a)s(b)) = (a\,b) \Leftrightarrow s(F) = F$$

où $F = E \setminus \{a, b\}$ et $E = [\![1, n]\!]$. Cela fournit un morphisme surjectif $\begin{array}{rccc} r : & c(\tau) & \longrightarrow & \mathfrak{S}_{n-2} \\ & s & \longmapsto & s_{|F} \end{array}$ de noyau $\{1, \tau\}$ donc $\mathfrak{S}_{n-2} \simeq c(\tau)/(\mathbb{Z}/2\mathbb{Z})$.

Supposons que $\varphi(\tau) = \tau'$ soit un produit d'un nombre impair $k \geqslant 3$ de transpositions disjointes $\tau' = (a_1\,a_2)\ldots(a_{2k-1}\,a_{2k})$. On note $\tau_i = (a_{2i-1}\,a_2 i)$. Les τ_i commutent entre eux deux à deux donc pour tout i, $\tau_i \in c(\tau)$. De plus, si $N =< \tau_1, \ldots, \tau_k >$, N est un sous-groupe distingué de $c(\tau')$: si $s \in c(\tau')$, $s\tau' s^{-1} = (s\tau_1 s^{-1})\ldots(s\tau_k s^{-1})$ donc par unicité de la décomposition en cycles à supports disjoints, $\forall i, \exists 1 \leqslant j \leqslant k : s\tau_i s^{-1} = \tau_j$. Donc $c(\tau')$ a un sous-groupe distingué N isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$.

Par ailleurs $c(\tau)$ est isomorphe via φ à $c(\tau')$ donc à $c(\tau)$ de sorte qu'en composant avec r, on obtient un morphisme surjectif $f : c(\tau') \twoheadrightarrow \mathfrak{S}_{n-2}$ de noyau $\{1, \tau'\}$.

1. En effet, pour $n \geqslant 3$, $\mathfrak{A}_n$ est engendré par les 3-cycles et ceux-ci sont deux à deux conjugués, donc si $\sigma = (abc)$ est un 3-cycle, $\sigma^2 = (acb)$ en est aussi un donc il existe $\tau \in \mathfrak{A}_n$ tel que $\sigma^2 = \tau\sigma\tau^{-1}$ donc σ est un commutateur

Par théorème d'isomorphisme, $f(N) \simeq N/(\ker(f) \cap N)$. Comme $\tau' \in N$, $\ker f \subset N$ et $f(N) \simeq (\mathbb{Z}/2\mathbb{Z})^k/(\mathbb{Z}/2\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z})^{k-1}$ [2]. Or, comme $n-2 \geqslant 5$, les seuls sous-groupes distingués de $\mathfrak{S}_{n-2}$ sont $\mathfrak{A}_{n-2}$, {id} et lui-même : par un argument de cardinalité, on conclut à une absurdité. Donc $k = 1$ et φ est intérieur.

□

Remarque.
- La preuve peut également se faire par dénombrement en calculant le cardinal du centralisateur de s produit de $k_1 + \cdots + k_n$ cycles disjoints parmi lesquels k_1 cycles d'ordre 1, ..., k_n d'ordre n, en supposant que $n = k_1 + 2k_2 + \cdots + nk_n$.
- Comme on utilise le fait que $\mathfrak{A}_n$ est le seul sous-groupe distingué non trivial de $\mathfrak{S}_n$ pour $n \geqslant 5$, il faut aussi savoir le prouver !

Référence : PERRIN 1996, pp. 31-32.

2. Ici, il me semble qu'il y a une imprécision dans le Perrin qui affirme que le cas $f(N) \simeq (\mathbb{Z}/2\mathbb{Z})^k$ n'est pas exclu.

Banach-Steinhaus et séries de Fourier

Leçons : 205, 208, 209, *241*, 246

Théorème 7

Soit E espace de Banach, F espace vectoriel normé, $H \subset \mathscr{L}_c(E,F)$. Alors soit il existe M tel que $\forall f \in H, \|f\| \leqslant M$, soit l'ensemble des $x \in E$ tels que $\sup_{f\in H} \|f(x)\| = +\infty$ est dense dans E.

Démonstration. Introduisons pour $k \in \mathbb{N}$, $\Omega_k = \{x \in E : \exists f \in H, \|f_i(x)\| > k\}$. Le complémentaire de cette ensemble étant fermé comme intersection de fermés, Ω_k est ouvert. Si $\Omega = \bigcap_{k\in\mathbb{N}} \Omega_k$, on remarque que $\forall x \in \Omega, \sup_{f\in H} \|f(x)\| = +\infty$.

Supposons qu'il existe $k \in \mathbb{N}$ tel que Ω_k ne soit pas dense. Il existe $x_0 \in E, r > 0$ tel que $B(x_0, r) \cap \Omega_k = \emptyset$. Si $\|x\| < r$ et $f \in H$, alors $\|f(x + x_0)\| \leqslant k$ donc $\|f(x)\| \leqslant k + \|f(x_0)\|$.

Donc si $\|x\| \leqslant 1$,

$$\|f(x)\| = \left\|\frac{2}{r} f\left(\frac{rx}{2}\right)\right\| \leqslant \frac{2k}{r} + \frac{2}{r}\|f(x_0)\|.$$

Ainsi, $\|f\| \leqslant \dfrac{2k}{r} + \dfrac{2}{r}\|f(x_0)\|$.

Sinon, tous les Ω_k sont denses donc selon le théorème de Baire, Ω est dense dans l'espace complet E donc l'ensemble des $x \in E$ tels que $\sup_{f\in H} \|f(x)\| = +\infty$, qui le contient, également.

□

Proposition 8

L'ensemble des fonctions continues 2π-périodiques dont la série de Fourier diverge en 0 est dense dans $\mathscr{C}^0_{2\pi}$.

Démonstration. Rappelons que $\mathscr{C}^0_{2\pi}$ muni de $\|\cdot\|_\infty$ est un espace de Banach. Soit, pour $n \in \mathbb{N}^*$,

$$\begin{array}{rccc} l_n : & \mathscr{C}^0_{2\pi} & \longrightarrow & \mathbb{C} \\ & f & \longmapsto & S_n(f)(0) = \sum_{k=-n}^{n} c_k(f) \end{array}.$$

Pour tout $f \in \mathscr{C}^0_{2\pi}$, $l_n(f) = (f \star D_n)(0) = \displaystyle\int_{-\pi}^{\pi} \frac{\sin\left(\left(n+\frac{1}{2}\right)t\right)}{\sin\left(\frac{t}{2}\right)} f(t)\mathrm{d}t$ donc $|l_n(f)| \leqslant \|D_n\|_1 \|f\|_\infty$ de sorte que $\|l_n\| \leqslant \|D_n\|_1$.

Pour $\varepsilon > 0$, soit $f_\varepsilon : t \to \dfrac{|D_n(t)|}{|D_n(t)| + \varepsilon} \in \mathscr{C}^0_{2\pi}$. Alors par convergence dominée, comme $\forall \varepsilon, \forall t, |f_\varepsilon(t)| \leqslant 1$,

$$l_n(f_\varepsilon) = \int_{-\pi}^{\pi} \frac{|D_n(t)|^2}{|D_n(t)| + \varepsilon}\mathrm{d}t \xrightarrow[\varepsilon\to 0]{} \int_{-\pi}^{\pi} |D_n(t)|\mathrm{d}t.$$

Donc pour tout $n \in \mathbb{N}$, $\|l_n\| = \|D_n\|_1$.

Or, il découle de l'inégalité $\sin t \leqslant t$, valable pour $t \in \left[0, \dfrac{\pi}{2}\right]$, que

$$\|D_n\|_1 = \int_{-\pi}^{\pi} \frac{2}{|t|}\left|\sin\left(\left(n+\frac{1}{2}\right)t\right)\right|\mathrm{d}t \geqslant 2\int_0^{\pi} \frac{\left|\sin\left(\left(n+\frac{1}{2}\right)t\right)\right|}{|t|}\mathrm{d}t \geqslant \int_0^{\left(n+\frac{1}{2}\right)\pi} \frac{|\sin u|}{u}\mathrm{d}u.$$

Donc $(\|D_n\|_1)_{n\in\mathbb{N}^*}$ tend en croissant vers $\displaystyle\int_{\mathbb{R}_+} \frac{|\sin u|}{u}\mathrm{d}u$, par convergence monotone. Mais $\varphi : u \mapsto \dfrac{|\sin u|}{u}\mathrm{d}u$ n'est pas intégrable. En effet, elle est périodique de moyenne $M = \displaystyle\int_0^{2\pi} \varphi(u)\mathrm{d}u > 0$ donc $\int_0^{2\pi n} \varphi(u)\mathrm{d}u = nM \xrightarrow[n\to+\infty]{} +\infty$ alors que dans le même temps, toujours par convergence monotone, cette suite tend vers $\int_{\mathbb{R}_+} \varphi(u)\mathrm{d}u$.

En conclusion, le premier cas de l'alternative du théorème de Banach-Steinhaus ne pouvant être réalisée, il s'ensuit que l'ensemble des $f \in \mathscr{C}^0_{2\pi}$ tels que $(l_n(f))_n$ n'est pas bornée est dense dans $\mathscr{C}^0_{2\pi}$. □

Remarque. Dans l'alternative du théorème de Banach-Steinhaus, le premier cas est en particulier réalisé quand il existe $x \in E$ tel que $\sup_{f\in H} \|f(x)\| < +\infty$.

Référence : RUDIN 1970, p. 130.

Borne de Bézout

Leçons : 142, 144, 152

Théorème 9

Soit k un corps infini et $A, B \in k[X,Y]$ de degrés totaux respectifs m et n. Alors si $Z(A)$ désigne l'ensemble des zéros de A, on a $\mathrm{Card}(Z(A) \cap Z(B)) \leqslant mn$.

Démonstration. Étape 1 : majoration du degré d'un résultant

On sait que si $(x,y) \in Z(A) \cap Z(B)$, on a $\mathrm{Res}_X(A,B)(y) = \mathrm{Res}_Y(A,B)(x) = 0$, donc

$$\mathrm{Card}(Z(A) \cap Z(B)) \leqslant \deg \mathrm{Res}_X(A,B) \times \deg \mathrm{Res}_Y(A,B)).$$

Écrivons $A = \sum_{i=0}^{p} a_i(X)Y^i$, $B = \sum_{j=0}^{q} b_j(X)Y^j$ où pour tout i, $\deg a_i \leqslant m-i$, pour tout j, $\deg b_j \leqslant n-j$.

Le résultant $\mathrm{Res}_Y(A,B)$ est le déterminant de la matrice de Sylvester

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

où si $1 \leqslant j \leqslant q$,

$$c_{i,j} = \begin{cases} a_{i-j} & \text{si} \quad 0 \leqslant i-j \leqslant p \\ 0 & \text{sinon} \end{cases},$$

et si $q+1 \leqslant j \leqslant p+q$,

$$c_{i,j} = \begin{cases} a_{i-j+q)} & \text{si} \quad 0 \leqslant i-j+q \leqslant p \\ 0 & \text{sinon} \end{cases}.$$ [3]

Donc $\mathrm{Res}_Y(A,B) = \sum_{\sigma \in \mathfrak{S}_{p+q}} \varepsilon(\sigma) \prod_{j=1}^{p+q} c_{\sigma(j),j}$. Or, si $\sigma \in \mathfrak{S}_{p+q}$,

$$\begin{aligned} \deg\left(\prod_{j=1}^{p+q} c_{\sigma(j),j}\right) = \sum_{j=1}^{p+q} \deg(c_{\sigma(j),j}) &\leqslant \sum_{j=1}^{q} m-(\sigma(j)-j) + \sum_{j=q+1}^{p+q} n-(\sigma(j)-j+q) \\ &\leqslant (m-p)(q-n)+mn \leqslant mn, \end{aligned}$$

puisque $q \leqslant n$ et $p \leqslant m$. Ainsi, $\deg \mathrm{Res}_Y(A,B) \leqslant mn$, et symétriquement, il en va de même de $\mathrm{Res}_X(A,B)$. D'où $\mathrm{Card}(Z(A) \cap Z(B)) \leqslant (mn)^2$.

Étape 2 : changement de variable astucieux

Notons $Z(A) \cap Z(B) = \{(x_i, y_i), i \in I\}$, I fini. Soit $\mathscr{E} = \left\{ \dfrac{x_i - x_j}{y_j - y_i}, i \neq j, y_j \neq y_i \right\}$ qui est également fini.

3. pour s'en souvenir, examiner les éléments en bas à droite des deux moitiés de la matrice correspondant à A et B.

Soit $u \in k^* \setminus \mathscr{E}$ (k est infini). Si $i \neq j \in I$,

$$x_i + uy_i = x_j + uy_j \Leftrightarrow x_i - x_j = u(y_j - y_i) \Leftrightarrow u = \frac{x_i - x_j}{y_j - y_i} \quad \text{ou} \quad (x_i, y_i) = (x_j, y_j)$$

ce qui est faux car $u \notin \mathscr{E}$. Donc $\varphi : (x, y) \in Z(A) \cap Z(B) \mapsto x + uy$ est injective.

Posons $\tilde{A}(X, Y) = A(X - uY, Y)$ et $\tilde{B}(X, Y) = B(X - uY, Y)$. Si $(x, y) \in Z(A) \cap Z(B)$, $\tilde{A}(x + uy, y) = A(x, y) = 0$ et $\tilde{B}(x, y) = 0$, d'où $\mathrm{Res}_Y(\tilde{A}, \tilde{B})(x + uy) = 0$.

Ainsi, φ est à valeurs dans l'ensemble des racines de $\mathrm{Res}_Y(\tilde{A}, \tilde{B})$. Selon l'étape 1, comme $\tilde{A}$ et $\tilde{B}$ sont de degrés totaux inférieurs à ceux de A et B, on a $\mathrm{Card}(Z(A) \cap Z(B)) \leqslant mn$.

□

Remarque. Le « vrai » théorème de Bézout affirme que le nombre de points d'intersections des courbes algébriques définies par A et B est égal à mn, à condition de les compter avec une notion de « multiplicité » à définir.

Références : bricolé (merci à Adrien Laurent) à partir de MÉRINDOL 2006 et de SZPIRGLAS 2009.

Chevalley-Warning et Erdös-Ginsburg-Ziv

Leçons : 120, *121*, 123, 142, 144

Théorème 10

Soit $q = p^s$ où p est premier et $(f_a)_{a\in A}$ une famille finie de polynômes de $\mathbb{F}_q[X_1,\dots,X_m]$ tels que $\sum_{a\in A} \deg f_a < m$. Alors si $V = \{x = (x_1,\dots,x_m) \in K^m : \forall a \in A, f_a(x_1,\dots,x_m) = 0\}$, on a $\mathrm{Card}(V) \equiv 0[p]$.

Démonstration. On note $K = \mathbb{F}_q$.

Étape 1 : Soit $u \in \mathbb{N}$ et $S(u) = \sum_{x\in K} x^u$. Montrons que $S(u) = 0$ si $u = 0$ ou $q-1 \nmid u$ et -1 sinon.

D'abord, si $u = 0$, avec la convention $0^0 = 1$, on a $S(0) = 1 + \sum_{x\in K^\times} 1 = q = 0$ dans $\mathbb{F}_q$. Si $u \neq 0$, rappelons que $K^\times$ est cyclique. Prenons en un générateur z, qui est donc d'ordre q, de sorte que $z^u = 1 \Leftrightarrow q-1 \mid u$.

Ainsi, si $q-1$ ne divise pas u, $S(u) = \sum_{j=0}^{q-1} z^{ju} = \dfrac{z^{qu}-1}{z^u-1} = 0$ car $z^q = z$.

Et sinon, $S(u) = \sum_{j=1}^{q-1} 1 = q-1 = -1$ dans $\mathbb{F}_q$.

Étape 2 : soit $P = \prod_{a\in A}\left(1 - f_a^{q-1}\right)$. Si $x \in V, P(x) = 1$ et si $x \notin V$, il existe $a \in A$ tel que $f_a(x) \neq 0$ donc $f_a(x)^{q-1} = 1$, si bien que $P(x) = 0$. Donc la fonction $x \mapsto P(x)$ est l'indicatrice $\mathbb{1}_V$.

Par ailleurs, le degré de V est inférieur à $\sum_{a\in A}(\deg f_a)(q-1) < m(q-1)$ par hypothèse. Donc P est une combinaison linéaire de monômes $X^u = X_1^{u_1}\dots X_m^{u_m}$ où $u_1+\dots+u_m < m(q-1)$. Pour un tel monôme :

$$\sum_{x\in K^m} x^u = \sum_{x\in K^m} x_1^{u_1}\dots x_m^{u_m} = \prod_{j=1}^{m}\sum_{x_i\in K} x_i^{u_i} = \prod_{j=1}^{m} S(u_i).$$

Or, il existe i_0 tel que $u_{i_0} < q-1$ donc $\sum_{x\in K^m} x^u = 0$. Par linéarité, $\forall x \in \mathbb{F}_q, 0 = \sum_{x\in K^m} P(x) = \sum_{x\in K^m} \mathbb{1}_V(x) = \mathrm{Card}V$. Comme $\mathbb{F}_q$ est de caractéristique p, le résultat désiré s'ensuit. □

Proposition 11 (*Erdös-Ginsburg-Ziv*)

Soit $n \in \mathbb{N}^*$. Parmi $2n-1$ entiers $a_1,\dots,a_{2n-1}$, on peut en trouver n dont la somme est divisible par n.

Démonstration. Étape 1 : pour $n = p$ premier. Introduisons les polynômes de $\mathbb{F}_p[X_1,\dots,X_{2p-1}]$, $P_1(X_1,\dots,X_{2p-1}) = \sum_{k=1}^{2p-1} X_k^{2p-1}$ et $P_2(X_1,\dots,X_{2p-1}) = \sum_{k=1}^{2p-1} \overline{a_k} X_k^{2p-1}$. On a $\deg P_1 + \deg P_2 = 2(p-1) < 2p-1$

De plus, $P_1(0) = 0 = P_2(0)$ donc en reprenant les notations du théorème précédent, V est non vide donc par Chevalley-Warning, V est de cardinal au moins p. Il existe donc $x \neq 0$ tel que $P_1(x) = P_2(x) = 0$. Or, si $x = (x_1,\dots,x_{2p-1})$, $P_1(x) = \mathrm{Card}\left\{i \in [\![1, 2p-1]\!], x_i \neq 0\right\}$ donc il y a exactement p composantes de x non nulles.

Donc comme $P_2(x) = \sum_{k\in[\![1,2p-1]\!],x_k\neq 0} \overline{a_k} = 0$, il existe $a_{i_1},\dots,a_{i_p}$ tels que $\sum_{k=1}^{p} \overline{a_{i_k}}$ soit divisible par p.

Étape 2 : pour le cas général, on procède par récurrence forte sur n.

Si n est premier, il n'y a rien à démontrer ; sinon, on écrit $n = pn'$ avec p premier et $n' > 1$. Soit $E = \{a_1,\dots,a_{2n-1}\}$ un ensemble de $2n-1$ entiers.

On a $2n-1 = 2pn'-1 = (2n'-1)p+p-1$. Selon l'étape 1, on peut trouver un ensemble E_1 de p entiers pris parmi $a_1,\dots,a_{2p-1}$ dont la somme est divisible par p ; puis E_2 ensemble de p entiers pris dans $\{a_1,\dots,a_{3p-1}\} \setminus E_1$ de somme divisible par p, etc...

On construit ainsi des ensembles deux à deux disjoints $E_1,\dots,E_{2n'-1}$. On note $S_i = \sum_{x\in E_i} x$, et on peut donc écrire $S_i = pS_i'$.

Par hypothèse de récurrence, il existe $\{i_1,\dots,i_{n'}\} \subset [\![1,2n'-1]\!]$ tel que $\sum_{k=1}^{n'} S'_{i_k}$ est divisible par n' de sorte que $\sum_{k=1}^{n'} S_{i_k}$ est divisible par n. Or, par construction, cette dernière somme est une somme de $n' \times p = n$ éléments de E ce qui termine la démonstration. □

Références : SERRE 1994 et ZAVIDOVIQUE 2013.

Décomposition de Dunford par la méthode de Newton

Leçons : 153, 155, 157

Théorème 12

Soit $\mathbb{K}$ sous-corps de $\mathbb{C}$ et $A \in \mathcal{M}_n(\mathbb{K})$. Il existe un unique couple $(D,N) \in \mathcal{M}_n(\mathbb{K})^2$ tel que $A = D+N$, $DN = ND$, avec D diagonalisable sur $\mathbb{C}$ et N nilpotent. De plus, D et N sont des éléments de $\mathbb{K}[A]$.

Lemme 13

Si U est une matrice inversible et N une matrice nilpotente commutant avec U alors $U-N$ est inversible.

Démonstration. Soit m tel que $N^m = 0$. Comme U et N commutent, $(U^{-1}N)^m = 0$, on peut donc supposer, quitte à multiplier par U^{-1} que $U = I_n$. Alors

$$\left(\sum_{k=0}^{m-1} N^k\right)(I_n - N) = (I_n - N)\left(\sum_{k=0}^{m-1} N^k\right) = I_n - N^m = I_n.$$

□

Démonstration (du théorème)**.** Notons χ_A le polynôme caractéristique de A. Il est scindé sur $\mathbb{C}$ algébriquement clos donc peut s'écrire $\chi_A = \prod_i (X-\lambda_i)^{n_i}$. Introduisons $P = \prod_i (X-\lambda_i)$. On remarque que $P = \dfrac{\chi_A}{\chi_A \wedge \chi_A'}$ donc $P \in \mathbb{K}[X]$. De plus, il existe $r = \max_i(n_i)$ tel que $\chi_A | P^r$ de sorte que $P^r(A) = 0$ (Cayley-Hamilton).

Introduisons la suite suivante :

$$\begin{cases} A_0 = A \\ A_{n+1} = A_n - P(A_n)P'(A_n)^{-1} \end{cases}.$$

Soit H le prédicat défini sur $\mathbb{N}$ par H_n : « A_n est bien définie et dans $K[A]$, $P(A_n) = P(A)^{2^n}B_n$ où $B_n \in K[A]$ et $P'(A_n)$ est inversible. »

- Pour montrer H_0, il suffit de vérifier que $P'(A)$ est inversible. Comme P et P' sont premiers entre eux, on peut fixer U, V tels que $UP + VP' = 1$. En évaluant en A, on a $V(A)P'(A) = I_n - U(A)P(A)$. Comme $P(A)$ est nilpotent, selon le lemme, $P'(A)$ est inversible.
- Soit $n \in \mathbb{N}$, supposons H_n. Il est immédiat que A_{n+1} est bien définie et est un polynôme en A.
  Remarquons que si $Q \in \mathbb{K}[X]$, il existe $\tilde{Q} \in \mathbb{K}[X,Y]$ tel que $Q(X+Y) = Q(X) + YQ'(X) + Y^2\tilde{Q}(X,Y)$. Il suffit, par linéarité, de le vérifier sur $Q(X) = X^m$. On a alors :

  $$(X+Y)^m = \sum_{k=0}^{m} \binom{m}{k} X^k Y^{m-k} = X^m + mYX^{m-1} + Y^2\left(\sum_{k=0}^{m-2} \binom{m}{k} X^k Y^{m-k-2}\right),$$

  ce qui donne le résultat voulu.
  Appliquons cela à P : $P(X+Y) = P(X) + YP'(X) + Y^2\tilde{P}(X,Y)$, et évaluons dans la $\mathbb{K}$-algèbre commutative $\mathbb{K}[A]$. On peut trouver $\tilde{B}_n \in \mathbb{K}[A]$ tel que $P(A_{n+1}) = P(A_n) - P(A_n)(P'(A_n))^{-1}P'(A_n) + P(A_n)^2\tilde{B}_n = P(A)^{2^{n+1}}B_n^2\tilde{B}_n = P(A)^{2^{n+1}}B_{n+1}$ où $B_{n+1} \in \mathbb{K}[A]$ par hypothèse de récurrence.

Enfin, pour montrer que $P'(A_{n+1})$ est inversible, on peut utiliser le même argument que dans l'initialisation ; ou bien écrire un développement $P'(X+Y) = P'(X) + YQ(X,Y)$ de P' et l'évaluer pour obtenir $P'(A_{n+1}) = P'(A_n) + P(A_n)C_n$ avec $C_n \in \mathbb{K}[A]$ donc comme $P(A_n)$ est nilpotent, le lemme fournit l'inversibilité de $P'(A_{n+1})$. Cela conclut la récurrence

- **Conclusion** : Soit $r \in \mathbb{N}$ tel que $P(A)^r = 0$. Alors si $n \geqslant n_0 = E(\log_2(r))+1$, $P(A_n) = 0$ donc $A_{n+1} = A_n$: la suite est stationnaire. Comme P est scindé à racines simples dans $\mathbb{C}$ et annule A_{n_0}, cette dernière matrice est diagonalisable sur $\mathbb{C}$.
  De plus, $A_{n_0} - A = \sum_{k=0}^{n_0-1} A_{k+1} - A_k$ et $A_{k+1} - A_k = P(A_k)(P'(A_k))^{-1} \in \mathbb{K}[A]$ est nilpotent donc $A_{n_0} - A$ est nilpotent comme somme de nilpotents commutant deux à deux. Ainsi $D = A_{n_0}$ et $N = A - A_{n_0}$ conviennent (ils commutent entre eux comme polynômes en A).

Prouvons pour finir l'unicité : soit (D', N') tel que $A = D' + N'$, $D'N' = N'D'$ et N' est nilpotent, D' est diagonalisable.

Alors N' commute avec A donc avec N élément de $\mathbb{K}[A]$. De plus, $N - N' = D' - D$ est diagonalisable, et nilpotent comme somme de deux nilpotents commutant entre eux. Donc $N - N' = 0$ et $D = D'$ ce qui prouve l'unicité.

□

Remarque.

- L'algorithme reprend le principe de la méthode de Newton. Comme dans le cas « ordinaire » , la convergence est quadratique : si $P^r(A) = 0$, il faut $\log_2(r)$ étapes pour obtenir (D, N).
- Voici la démonstration du petit résultat cité dans la preuve du théorème : si x, y sont deux nilpotents d'un anneau A tels que $xy = yx$, prenons n tel que $x^n = y^n = 0$. Alors par le binôme de Newton, $(x+y)^n = \sum_{k=0}^{2n} \binom{2n}{k} x^k y^{2n-k}$ et si $k \in [\![0, 2n]\!]$, alors $k \in [\![n+1, 2n]\!]$ ou $2n-k \in [\![n+1, 2n]\!]$ donc $x^k = 0$ ou $y^{2n-k} = 0$. *In fine*, $(x+y)^n = 0$.

Références : RISLER et BOYER 2006, p. 62. L'unicité est dans GOURDON 2009a, p. 193 avec un raccourci.

Diagonalisation des opérateurs symétriques compacts

Leçons : 203, *205*, 213

Théorème 14

Soit H un Hilbert séparable et $T \in \mathscr{L}(H)$ un opérateur symétrique ($T = T^*$) compact non nul. Il existe $(e_n)_{n\in\mathbb{N}}$ base hilbertienne de H constituée de vecteurs propres de T. La suite des valeurs propres de T, notée $(\lambda_n)_{n\in\mathbb{N}}$ tend vers 0 et pour tout $x \in H$, $T(x) = \sum_{n=0}^{+\infty} \lambda_n \langle x, e_n\rangle e_n$.

Lemme 15

L'opérateur symétrique compact T admet $\|T\|$ ou $-\|T\|$ pour valeur propre.

Démonstration. Montrons d'abord que $\|T\|^2$ est valeur propre de T^2. On a pour tout élément x de H :

$$\begin{aligned}\|T^2(x) - \|T\|^2 x\|^2 &= \|T^2x\|^2 + \|T\|^4\|x\|^2 - 2\mathrm{Re}\langle T^2x, x\rangle\|T\|^2 \\ &\overset{T=T^*}{=} \|T^2x\|^2 + \|T\|^4\|x\|^2 - 2\|T\|^2\|Tx\|^2 \\ &\leqslant \|T\|^2(\|T\|^2\|x\|^2 - \|Tx\|^2.\end{aligned}$$

Prenons une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments unitaires tels que $\|T(x_n)\| \xrightarrow[n\to+\infty]{} \|T\|$. Comme T est compact et (x_n) est bornée, quitte à extraire une sous-suite, on peut supposer que $T(x_n)$ admet une limite y. Donc $T^2(x_n)$ tend vers $T(y)$.

Par ailleurs, l'inégalité ci-dessus nous assure que $\left(\|T^2x_n - \|T\|^2x_n\|^2\right)_n$ tend vers 0 car $\|T\|^2(\|T\|^2 - \|T(x_n)\|^2) \xrightarrow[n\to+\infty]{} 0$. Ainsi, $\|T\|^2x_n \xrightarrow[n\to+\infty]{} T(y)$, de sorte que x_n tend vers $x = \dfrac{T}{\|T\|^2}y \neq 0$. Comme $T^2x_n \xrightarrow[n\to+\infty]{} T(y) = \|T\|^2x$, on a $T^2(x) = \|T\|^2x$: x est un vecteur propre de T^2 associé à $\|T\|^2$.

Mais $T^2 - \|T\|^2 = (T - \|T\|)(T + \|T\|)$ donc ou bien $(T + \|T\|)(x) = 0$ et $-\|T\|$ est valeur propre de T, ou bien $x' = (T + \|T\|)(x) \neq 0$ et x' est vecteur propre de T associé à la valeur propre $\|T\|$.

□

Démonstration (du théorème)**.** Construisons par récurrence une suite $(\lambda_n)_{n\in\mathbb{N}}$ décroissante en module de valeurs propres de T.

On pose $T_1 = T \neq 0$. Selon la première étape, on peut trouver une valeur propre λ_1 de module $\|T\|$ de T. Comme T est compact, l'espace propre $E_1 = \ker(T - \lambda_1\mathrm{id})$ est de dimension finie donc fermé ; d'où, selon le théorème du supplémentaire orthogonal $H = E_1 \oplus E_1^\perp$.

Supposons construits $\lambda_1, \ldots, \lambda_n$ valeurs propres de T telles que λ_k est de module $\|T_k\|$ où $\|T_k\|$ est la restriction de T à $\left(\bigoplus_{i=1}^{k-1} E_i\right)^\perp$ où $E_i = \ker(T - \lambda_i)$ (sous-espace stable par T symétrique comme orthogonal d'un sous-espace stable). En particulier, $|\lambda_n| \geqslant \cdots \geqslant |\lambda_1|$.

Si T_{n+1} est nul, la construction s'arrête.

Sinon, T_{n+1} est symétrique compact non nul donc selon le lemme, il admet une valeur propre λ_{n+1} de module $\|T_{n+1}\|$. C'est également une valeur propre de T et $H = \bigoplus_{i=1}^{n+1} E_i \oplus \left(\bigoplus_{i=1}^{n+1} E_i\right)^{\perp}$, les sommes directes étant orthogonales puisque $\ker(T-\lambda_{n+1}) = \ker(T_{n+1} - \lambda_{n+1}) \subset \left(\bigoplus_{i=1}^{n} E_i\right)^{\perp}$.

Montrons que les λ_n forment une suite tendant vers 0 et qu'elles sont les seules valeurs propres non nulles de T. Ceci est clair si la récurrence précédente s'arrête puisqu'il existe un $N \in \mathbb{N}$ tel que $\left(\bigoplus_{i=1}^{N} \ker(T-\lambda_i)\right)^{\perp} \subset \ker T$ donc

$$H = \bigoplus_{i=1}^{N} \ker(T-\lambda_i) \oplus \ker T.$$

Supposons donc $\{\lambda_n, n \in \mathbb{N}\}$ infini. La suite $(|\lambda_n|)$ est décroissante et minorée donc tend vers sa borne inférieure $m \geqslant 0$. Si $m \neq 0$, prenons pour tout n, un élément (e_n) unitaire tel que $T(e_n) = \lambda_n e_n$. Comme T est compact et $\left(\frac{e_n}{\lambda_n}\right)$ est bornée, quitte à extraire une sous-suite, on a $e_n = T\left(\frac{e_n}{\lambda_n}\right) \xrightarrow[n\to+\infty]{} z \in H$. Mais comme les espaces propres associés aux λ_n sont deux à deux orthogonaux, on a pour tout $n \neq m$, $\|e_n - e_m\|^2 = 2$: (e_n) n'étant pas de Cauchy, elle ne peut donc converger.

Ainsi, $m = 0$ et $|\lambda_n|$ tend vers 0.

Maintenant, si $F = \bigoplus_{n\in\mathbb{N}^*} E_n$, on a $F^{\perp} \subset \ker T$. En effet, si $T_{|F^{\perp}}$ était non nul, cet opérateur symétrique compact admettrait une valeur propre λ de module $\|T_{|F^{\perp}}\|$. Or, pour tout n, λ_n est de module $\left\| T_{|\bigoplus_{i=1}^{n-1} E_i} \right\| \geqslant \|T_{|F^{\perp}}\|$ donc en faisant tendre n vers l'infini, $\lambda = 0$ ce qui est absurde. D'où $F^{\perp} \subset \ker T$, l'autre inclusion étant également facilement vérifiable.

Conclusion : par le théorème du supplémentaire orthogonal, $H = \overline{\bigoplus_{n\in\mathbb{N}^*} E_n} \oplus \ker T$, les sommes étant orthogonales. Pour tout n, $E_n = \ker(T-\lambda_n)$ est de dimension finie[4], on en prend une base orthonormée $(e_n^m)_{1\leqslant m\leqslant N_m}$. En concaténant ces bases, on obtient $(e_n^m)_{n,m}$ base hilbertienne de $\overline{\bigoplus_{n\in\mathbb{N}^*} E_n}$ formée de vecteurs propres de T. Par ailleurs, on peut fixer une base hilbertienne $(e_0^m)_{m\in\mathbb{N}}$ de $\ker T$ (qui est séparable car H l'est). La réunion de ces deux bases fournit la base hilbertienne de H annoncée.

□

Référence : Inspiré de WILLEM 2003, pp. 38-40, mais largement remanié par Salim Rostam (`http://perso.eleves.ens-rennes.fr/~srostam/html/Agreg/index.html`).

4. $T_{|E_n} = \lambda_n \mathrm{id}$ est compact donc $\lambda_n \overline{B_{E_n}(0,1)}$ est compact, ce qui selon le théorème de Riesz ne peut se produire que si E_n est de dimension finie.

Deux méthodes de gradient

Leçons : 158, *162*, 219, *226*, 233 (gradient conjugué)

On considère $A \in \mathcal{S}_n^{++}(\mathbb{R})$.

Proposition 16

La résolution de $Ax = b$ équivaut à trouver le point qui minimise la fonctionnelle :

$$\Phi(y) = \frac{1}{2} y^T A y - y^T b.$$

Démonstration. Il est facile de voir que

$$\nabla\Phi(y) = \frac{1}{2}(A^T + A)y - b = Ay - b. \tag{2.1}$$

Et si x est solution du système linéaire, alors $\Phi(y) = \Phi(x + (y-x)) = \Phi(x) + \frac{1}{2}(y-x)^T A(y-x)$ *i.e* $\frac{1}{2}\|y-x\|_A^2 = \Phi(y) - \Phi(x)$, où $\|z\|_A^2 = z^T A z$ est la norme associée à A que l'on utilisera toujours par la suite.

□

Définition 17

Une méthode de gradient consiste à partir d'un point $x_0 \in \mathbb{R}^n$ et à construire la suite

$$x_{k+1} = x_k + \alpha_k d_k \tag{2.2}$$

où $d_k \in \mathbb{R}^n$ est une direction à choisir et $\alpha_k \in \mathbb{R}$.

Une idée naturelle est de choisir α_k de sorte à optimiser $\Phi(x_{k+1})$ dans la direction d_k, c'est à dire tel que $\frac{d}{d\alpha_k}\Phi(x_k + \alpha_k d_k) = -d_k^T r_k + \alpha_k d_k^T A d_k = 0$, où $-r_k := \nabla\Phi(x_k) = Ax_k - b$. On trouve :

$$\alpha_k = \frac{\langle d_k, r_k \rangle}{\|d_k\|_A^2} \tag{2.3}$$

(c'est bien défini lorsque $d_k \neq 0$ car $A \in \mathcal{S}_n^{++}(\mathbb{R})$).

Méthode de gradient conjugué

Remarquons que pour tout $k \in \mathbb{N}$:

$$r_{k+1} = r_k - \alpha_k A d_k \tag{2.4}$$

et α_k est choisi de sorte à ce que

$$\langle r_{k+1}, d_k \rangle = 0. \tag{2.5}$$

Idée. Construire des directions (d_k) deux à deux A-orthogonales ; ainsi, r_{k+1} sera orthogonal à $\mathrm{Vect}(d_0, \ldots, d_k)$.

Notations. Pour $x, y \in \mathbb{R}^n$, on note $x \perp y$ lorsque x et y sont orthogonaux pour le produit scalaire euclidien et $x \perp_A y$ lorsque x et y sont orthogonaux pour le produit scalaire donné par A. On étend naturellement cette notation à des sous-espaces de $\mathbb{R}^n$.

On pose $d_0 = r_0$ et pour $k \in \mathbb{N}$, on construit d_{k+1} comme l'orthogonalisé de Gram-Schmidt pour le produit scalaire donné par A de r_{k+1} relativement à $\text{Vect}(d_k)$:

$$d_{k+1} = r_{k+1} - \beta_k d_k \tag{2.6}$$

où

$$\beta_k = \frac{\langle r_{k+1}, Ad_k \rangle}{\|d_k\|_A^2} \quad \text{si } d_k \neq 0, \quad \beta_k = 0 \text{ sinon.} \tag{2.7}$$

Remarquons que si $d_k = 0$ alors r_k et d_{k-1} sont colinéaires et comme ils sont aussi orthogonaux par (2.5), $r_k = 0$.

Lemme 18

Avec le choix (2.7)*, les directions* (2.6) *vérifient pour tout $k \in \mathbb{N}$ la propriété suivante : si $r_0, \ldots, r_k$ ne sont pas nuls alors,*

1 $\text{Vect}(r_0, \ldots, r_k) = \text{Vect}(d_0, \ldots, d_k)$

2 $r_{k+1} \perp \text{Vect}(d_0, \ldots, d_k)$

3 $d_{k+1} \perp_A \text{Vect}(d_0, \ldots, d_k)$

Démonstration. On procède par récurrence sur $k \in \mathbb{N}$. Lorsque $k = 0$, 1, 2 et 3 sont vrais grâce aux relations $r_0 = d_0$, (2.5) et (2.6) et bien sûr $r_0 \neq 0$ sinon il n'y a rien à faire. Supposons donc le résultat vrai au rang $k-1$, $k \in \mathbb{N}^*$.

1 Par (2.6), on a : $d_k = r_k - \beta_{k-1} d_{k-1}$.

2 Par (2.5), on a déjà $r_{k+1} \perp d_k$ et si $j \in \{0, \ldots, k-1\}$, la relation (2.4) couplée à l'hypothèse de récurrence 2 et 3 donne $r_{k+1} \perp d_j$.

3 Par (2.6), on a déjà $d_{k+1} \perp_A d_k$ (c'est la définition) et si $j \in \{0, \ldots, k-1\}$, la relation (2.6) couplée à l'hypothèse de récurrence 3 donne $\langle d_{k+1}, Ad_j \rangle = \langle r_{k+1}, Ad_j \rangle$.

Montrons que $Ad_j \in \text{Vect}(r_0, \ldots, r_k)$, ce qui conclura grâce aux relations 1 et 2 que l'on vient de prouver. Grâce à la relation (2.4) avec $k = j$, il suffit de montrer que $\alpha_j \neq 0$.

Or, $\alpha_j = 0 \overset{(2.3)}{\iff} \langle r_j, d_j \rangle = 0 \overset{(2.6)}{\iff} r_j = 0$ puisque $\langle r_j, r_j \rangle = \langle d_j, r_j \rangle + \beta_{j-1} \langle d_{j-1}, r_j \rangle = \langle d_j, r_j \rangle$ selon 2. Donc comme on a supposé $r_j \neq 0$, on a $\alpha_j \neq 0$.

□

Théorème 19

La méthode de gradient associée aux directions (2.6) *avec le choix* (2.7) *converge vers la solution x du problème $Ax = b$ en au plus n itérations.*

Démonstration. Les conditions 1 et 2 du lemme précédent assurent que tant que $r_l \neq 0$, la famille $(r_0, \ldots, r_l)$ est une famille orthogonale donc libre. On est en dimension n donc nécessairement $l + 1 \leqslant n$ et si $r_l = 0$, x_l est solution du système. □

Méthode de gradient à pas optimal

On choisit pour direction la « plus grande pente » , c'est à dire $d_k = -\nabla\Phi(x_k) = -Ax_k + b = r_k$.

Dans ce cas, $d_k \neq 0$ tant que la solution n'est pas atteinte. La convergence découle essentiellement de l'inégalité de Kantorovich :

Lemme 20 (*Inégalité de Kantorovich*)

En notant $0 < \lambda_1 \leq \ldots \leq \lambda_n$ les valeurs propres de A, on a pour tout $y \in \mathbb{R}^n$,

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

Démonstration. On va montrer l'inégalité équivalente :

$$\forall y \in \mathbb{R}^n,\ \|y\|^4 \leq \frac{1}{4}\left(\sqrt{\frac{\lambda_n}{\lambda_1}} + \sqrt{\frac{\lambda_1}{\lambda_n}}\right)^2.$$

On peut même supposer que $\|y\| = 1$ et commencer par remarquer :

$$1 = \|y\|^2 = \langle y, AA^{-1}y\rangle \leq \|y\|_A \|A^{-1}y\|_A = \|y\|_A \|y\|_{A^{-1}}$$

Et dans une base orthonormale de vecteurs propres :

$$\begin{aligned}
\|y\|_A \|y\|_{A^{-1}} &= \sqrt{\left(\sum_{i=1}^n \lambda_i y_i^2\right)\left(\sum_{i=1}^n \frac{1}{\lambda_i} y_i^2\right)} = \sqrt{\frac{\lambda_1}{\lambda_n}\left(\sum_{i=1}^n \frac{\lambda_i}{\lambda_1} y_i^2\right)\left(\sum_{i=1}^n \frac{\lambda_n}{\lambda_i} y_i^2\right)} \\
&\leq \frac{1}{2}\sqrt{\frac{\lambda_1}{\lambda_n}}\left(\left(\sum_{i=1}^n \frac{\lambda_i}{\lambda_1} y_i^2\right) + \left(\sum_{i=1}^n \frac{\lambda_n}{\lambda_i} y_i^2\right)\right) \\
&\leq \frac{1}{2}\sqrt{\frac{\lambda_1}{\lambda_n}}\left(\sum_{i=1}^n \left(\frac{\lambda_i}{\lambda_1} + \frac{\lambda_n}{\lambda_i}\right) y_i^2\right)
\end{aligned}$$

La fonction $x \mapsto \dfrac{x}{\lambda_1} + \dfrac{\lambda_n}{x}$ admet un maximum en λ_1 ou en λ_n et il vaut dans les deux cas : $1 + \dfrac{\lambda_n}{\lambda_1}$. Ainsi,

$$\|y\|_A \|y\|_{A^{-1}} \leq \frac{1}{2}\sqrt{\frac{\lambda_1}{\lambda_n}}\left(\sum_{i=1}^n \left(1 + \frac{\lambda_n}{\lambda_1}\right) y_i^2\right) \leq \frac{1}{2}\left(\sqrt{\frac{\lambda_n}{\lambda_1}} + \sqrt{\frac{\lambda_1}{\lambda_n}}\right),$$

et le résultat suit en élevant au carré. □

Et sachant que $\mathrm{cond}(A) = \lambda_n/\lambda_1$, on obtient le résultat suivant :

Théorème 21

Avec les choix précédents et $d_k = r_k$, la suite (2.2) *converge vers x avec :*

$$\|x_{k+1} - x\|_A \leq \frac{\lambda_n - \lambda_1}{\lambda_n + \lambda_1}\|x_k - x\|_A.$$

Plus précisément,

$$\|x_k - x\| \leq \sqrt{\mathrm{cond}(A)}\left(\frac{\mathrm{cond}(A) - 1}{\mathrm{cond}(A) + 1}\right)^k \|x_0 - x\|.$$

Démonstration. La première inégalité découle directement de l'inégalité de Kantorovich. Pour la seconde, on remarque que pour tout $y \in \mathbb{R}^n$, $\lambda_1 \|y\|^2 \leq \|y\|_A^2 \leq \lambda_n \|y\|^2$. □

Avec la dernière inégalité, on voit que la convergence peut être lente lorsque la matrice est mal conditionnée.

Référence : QUARTERONI, SACCO et SALERI 2007, pp. 138-145. Merci à Antoine Diez pour ce développement.

Ellipsoïde de John-Loewner

Leçons : 152, *158*, *171*, *203*, *219*, 229, 253

Définition 22

Un ellipsoïde centré en 0 *est une surface de* $\mathbb{R}^n$ *d'équation* $q(x) = 1$ *où* q *est une forme quadratique définie positive. On le note* $\mathscr{E}_q$.

Lemme 23

Si A *et* B *sont deux matrices définies positives et* $\alpha \in]0,1[$, *alors* $\det(\alpha A + (1-\alpha)B) \geqslant (\det A)^\alpha (\det B)^{1-\alpha}$ *avec inégalité stricte si* $A \neq B$.

Démonstration. On utilise le théorème de réduction simultanée : il existe $P \in \mathrm{GL}_n(\mathbb{R})$ tel que $A = {}^tPP$ et $B = {}^tPDP$ où $D = \mathrm{Diag}(\lambda_1, \dots, \lambda_n)$, $\lambda_i > 0$. Ainsi, si $\alpha \in]0,1[$:

$$\det(\alpha A + (1-\alpha)B) = (\det P)^2 \prod_{i=1}^{n} (\alpha + (1-\alpha)\lambda_i).$$

Or, ln étant strictement concave, pour $i \in [\![1, n]\!]$,

$$\ln(\alpha + (1-\alpha)\lambda_i) \geqslant \alpha \ln(1) + (1-\alpha)\ln(\lambda_i) = (1-\alpha)\ln(\lambda_i),$$

d'où en sommant et en composant par exp, $\displaystyle\prod_{i=1}^{n} (\alpha + (1-\alpha)\lambda_i) \geqslant \left(\prod_{i=1}^{n} \lambda_i\right)^{1-\alpha}$.

Mais $\det(A)^\alpha \det(B)^{1-\alpha} = \det P^{2\alpha+2(1-\alpha)} \det(D)^{1-\alpha} = \det P^2 \left(\displaystyle\prod_{i=1}^{n} \lambda_i\right)^{1-\alpha}$ donc on a l'inégalité voulue. □

Théorème 24

Soit K *compact de* $\mathbb{R}^n$ *d'intérieur non vide. Il existe un unique ellipsoïde centré en* 0 *de volume minimal contenant* K

Démonstration. On munit $\mathbb{R}^n$ de son produit scalaire canonique, de norme associée $\|\cdot\|$. On note $\mathscr{Q}$ (resp. $\mathscr{Q}^+$, $\mathscr{Q}^{++}$) l'ensemble des formes quadratiques (resp. positives, définies positives) sur $\mathbb{R}^n$.

Étape 1 : calcul du volume d'un ellipsoïde centré en 0**.**

Soit q forme quadratique positive. Selon le théorème de réduction simultanée, il existe une base orthonormée $\mathscr{B}$ de $\mathbb{R}^n$ (pour le produit scalaire canonique) et $a_1, \dots, a_n \geqslant 0$ tels que $M_{\mathscr{B}}(q) = \mathrm{Diag}(a_1, \dots, a_n)$.

Par un premier de changement de variable envoyant $(x_1, \dots, x_n)$ sur ses coordonnées dans la base $\mathscr{B}$, on voit que le volume V_q de $\mathscr{E}_q$ est

$$V_q = \int_{\{a_1 u_1^2 + \cdots + a_n u_n^2\}} \mathrm{d}x.$$

Donc, en posant $u_i' = \sqrt{a_i} u_i$, on obtient par un nouveau changement de variable $V_q = \dfrac{1}{\sqrt{a_1 \dots a_n}} V_0$ où V_0 est le volume de la boule unité de $\mathbb{R}^n$. Or le déterminant de $M_{\mathscr{B}}(q)$ est

$D(q) = a_1 \dots a_n$, et c'est une quantité invariante par changement de base orthonormée, appelée discriminant. Donc $q \mapsto D(q)$ est une application continue sur $\mathcal{Q}^+$, qu'on va chercher à maximiser.

Étape 2 : minimisation du discriminant.
Soit $\mathcal{A} = \{q \in \mathcal{Q}^+ : \forall x \in K, q(x) \leqslant 1\}$. On munit l'espace vectoriel $\mathcal{Q}$ de la norme

$$N : q \mapsto \sup_{\|x\| \leqslant 1} |q(x)|.$$

$\mathcal{A}$ est fermé : supposons que la suite $(q_n) \in (\mathcal{Q}^+)^{\mathbb{N}}$ converge vers $q \in \mathcal{Q}$. Alors pour tout $x \in \mathbb{R}^n$, $|q_n(x) - q(x)| \leqslant N(q_n - q)\|x\|^2$ donc $q_n(x) \xrightarrow[n \to +\infty]{} q(x)$. En particulier, $q(x) \geqslant 0$ et $q(x) \leqslant 1$ pour $x \in K$.

$\mathcal{A}$ est borné : Comme K est d'intérieur non vide, on peut fixer une boule $B(a, r) \subset K$. Donc si $q \in \mathcal{A}$ et $\|x\| \leqslant r$, $q(a + x) \leqslant 1$, de sorte que par l'inégalité de Minkowski,

$$\sqrt{q(x)} = \sqrt{q(a + x - a)} \leqslant \sqrt{q(a + x)} + \sqrt{q(a)} \leqslant 2.$$

Ainsi, pour $\|x\| \leqslant 1$, $q(x) = \dfrac{1}{r^2} q(rx) \leqslant \dfrac{2}{r^2}$, soit $N(q) \leqslant \dfrac{2}{r^2}$.

$\mathcal{A}$ est non vide : en effet, on peut trouver $M > 0$ tel que $K \subset B(0, M)$ et $q : x \mapsto \dfrac{\|x\|^2}{M^2}$ est un élément de $\mathcal{A}$.

Finalement, $q \mapsto D(q)$ est une application continue sur le compact non vide $\mathcal{A}$ donc elle est bornée et atteint ses bornes en $q_0 \in \mathcal{Q}^{++} \cap \mathcal{A}$ car le discriminant est nul pour un élément de $\mathbb{Q}^+ \setminus \mathcal{Q}^{++}$. En d'autres termes, selon l'étape 1, $\mathcal{E}_{q_0}$ est un ellipsoïde centré en 0 de volume minimal contenant K.

Étape 3 : Unicité.
Supposons que q_1 soit un autre point de $\mathcal{A}$ où le minimum est atteint. Remarquons que $\mathcal{A}$ est convexe, et notons $q_2 = \dfrac{q_0 + q_1}{2} \in \mathcal{A}$. Alors par log-concavité stricte du déterminant, $D(q_2) > \sqrt{D(q_0)}\sqrt{D(q_1)} = D(q_0)$ qui est pourtant supposé maximal : c'est absurde.

□

Proposition 25

Si G est un sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$, il existe $q \in \mathcal{Q}^{++}$ tel que $G \subset O(q)$.

Démonstration. Soit G un sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$, B la boule unité fermée de $\mathbb{R}^n$ muni d'une norme euclidienne. Introduisons $K = \{g(x)/g \in G, x \in B\}$. C'est un compact comme image de $G \times B$ par $(g, x) \mapsto g(x)$ continue. De plus, $B \subset K$ donc K est d'intérieur non vide. Soit donc $\mathcal{E}_q$ l'ellipsoïde de John-Loewner associée à K où $q \in \mathcal{Q}^{++}$.

Si $g \in G$, $q' : x \mapsto q(g(x))$ est définie positive et puisque $g(K) = K$, $\mathcal{E}_{q'}$ contient K. Classiquement, comme det est bornée sur G compact, on a $|\det g| = 1$, donc q' et q ont même discriminant. Donc selon l'étape 3 de la preuve précédente, $q = q'$, *i.e.* $g \in O(q)$. Ainsi, $G \subset O(q)$.

□

Remarque. On peut même montrer que les sous-groupes compacts maximaux de $\mathrm{GL}_n(\mathbb{R})$ sont les $O(q)$ avec $q \in \mathcal{Q}^{++}$.

Remarquons d'abord qu'il suffit de montrer que $O_n(\mathbb{R})$ est un sous-groupe compact maximal. En effet, si $q \in \mathcal{Q}^{++}$, il existe une base de E dans laquelle la matrice de q est I_n, donc $O(q)$ et $O_n(\mathbb{R})$ sont conjugués.

Soit donc G compact tel que $O_n(\mathbb{R}) \subset G$. Soit $g \in G$. Par décomposition polaire, on peut écrire $G = OS$ où $O \in O_n(\mathbb{R})$ et $S \in \mathcal{S}_n^{++}(\mathbb{R})$. Donc $S = O^{-1}g \in G$. Mais S est diagonalisable dans une base orthonormée donc on montre sans mal que $\|S\|_2 = \rho(S)$, plus grande valeur propre de S (car les valeurs propres de S sont positives). Ainsi, les valeurs propres de S sont toutes égales à 1 puisque sinon $(S^k)_{k\in\mathbb{N}}$ ou $(S^{-k})_{k\in\mathbb{N}}$ ne seraient pas bornés. En d'autres termes, $S = I_n$ et $g \in O_n(\mathbb{R})$, ce qu'il fallait démontrer.

Références : Francinou, Gianella et Nicolas 2008, p. 229-232 et Caldero et Germoni 2013, p. 205.

Endomorphismes semi-simples

Leçons : 122, *153*, 154, 155

On se place dans E, un $\mathbb{K}$-espace vectoriel de dimension finie n.

Définition 26

On dit que $f \in \mathscr{L}(E)$ est semi-simple lorsque tout sous-espace vectoriel de E stable par f admet un supplémentaire stable par f.

Lemme 27

Soit $\mathbb{L}/\mathbb{K}$ une extension de corps. Alors $\Pi_{f,\mathbb{K}} = \Pi_{f,\mathbb{L}}$.

Démonstration. C'est une conséquence de l'indépendance du rang vis à vis du corps de base (qui provient de l'indépendance du résultat du calcul des mineurs). Maintenant, on a déjà $\Pi_{f,\mathbb{L}} | \Pi_{f,\mathbb{K}}$ et comme ces polynômes sont unitaires, il suffit de montrer qu'ils sont de même degré pour conclure. Or, le degré du polynôme minimal de f sur $\mathbb{L}$ est égal au rang de la famille $(\mathrm{id}, f, \dots, f^{n-1})$ dans $\mathscr{L}(E)$ qui est un espace vectoriel de dimension finie n^2. Comme le rang ne dépend pas du corps de base, on en déduit l'égalité annoncée. □

Lemme 28

Soit F un sous-espace stable par f. On note $\Pi_f = P_1^{\alpha_1} \dots P_r^{\alpha_r}$. On a :

$$F = \bigoplus_{i=1}^{r} \Big[\ker P_i^{\alpha_i}(f) \cap F \Big].$$

Démonstration. Par le lemme des noyaux, on sait que :

$$F = \bigoplus_{i=1}^{r} \ker P_i^{\alpha_i}(f|_F) = \bigoplus_{i=1}^{r} \Big[\ker P_i^{\alpha_i}(f) \cap F \Big].$$

□

Théorème 29

Un endomorphisme f est semi-simple si et seulement si son polynôme minimal Π_f est un produit de polynômes irréductibles unitaires distincts deux à deux.

Démonstration. Étape 1. Lorsque Π_f est irréductible.

On va montrer que f est semi-simple, considérons donc F un sous-espace stable par f. Si $F = E$, il n'y a rien à faire. Sinon, soit $x \in E \setminus F$ et

$$E_x = \{P(f)(x),\ P \in \mathbb{K}[X]\}.$$

Clairement E_x est stable par f. Pour conclure et quitte à itérer le processus, il suffit de montrer que F et E_x sont en somme directe. L'idéal $I_x = \{P \in \mathbb{K}[X],\ P(f)(x) = 0\}$ est non réduit à 0 (il y a Π_f) et principal donc il est engendré par un unique polynôme unitaire Π_x. Comme $\Pi_x | \Pi_f$, ce polynôme est irréductible.

Soit $y = P(f)(x) \in E_x \cap F$ que l'on suppose non nul. Alors $P \notin I_x$, c'est à dire que Π_x ne divise pas P et comme il est irréductible, P et Π_x sont premiers entre eux. Par le théorème

de Bézout, on peut écrire $UP + V\Pi_x = 1$. On a donc$x = U(f) \circ P(f)(x) = U(f)(y) \in F$ car $y \in F$, ce qui est absurde.

Étape 2. Cas général, condition nécessaire.

Soit $f \in \mathscr{L}(E)$ un endomorphisme semi-simple de polynôme minimal $\Pi_f = P_1^{\alpha_1} \dots P_r^{\alpha_r}$. Supposons qu'il existe $\alpha_i \geq 2$. On écrit alors $\Pi_f = P^2 Q$.

$F = \ker P(f)$ est un sous-espace stable par f qui admet un supplémentaire stable noté S. Si $x \in S$, alors $\Pi_f(f)(x) = P(f)P(f)Q(f)(x) = 0$ donc $P(f)Q(f)(x) \in F$. Par ailleurs, S est stable par f donc $P(f)Q(f)(x) \in S$.

Finalement, $P(f)Q(f)(x) \in F \cap S = \{0\}$ et $P(f)Q(f)$ s'annule sur S.

Mais $P(f)Q(f) = Q(f)P(f)$ donc par définition de F, $P(f)Q(f)$ s'annule aussi sur F. Puisque F et S sont supplémentaires, le polynôme PQ annule f ce qui contredit la minimalité de Π_f.

Étape 3. Cas général, condition suffisante.

Soit $f \in \mathscr{L}(E)$ dont le polynôme minimal est de la forme $\Pi_f = P_1 \dots P_r$ où les P_i sont des polynômes irréductibles distincts. Soit F un sous-espace stable par f. Pour tout $i \in \{1, \dots r\}$, $F \cap \ker P_i(f)$ est stable par $f|_{\ker P_i(f)}$. Puisque P_i est un polynôme irréductible qui annule $f|_{\ker P_i(f)}$, c'est le polynôme minimal de $f|_{\ker P_i(f)}$. La première étape fournit l'existence d'un sous-espace S_i stable par $f|_{\ker P_i(f)}$ (donc par f) tel que $\ker P_i(f) = (F \cap \ker P_i(f)) \cap S_i$.

Il suffit d'écrire :

$$E = \bigoplus_{i=1}^{r} \Big[F \cap \ker P_i(f) \oplus S_i \Big] = \Big[\bigoplus_{i=1}^{r} \Big(F \cap \ker P_i(f) \Big) \Big] \oplus \bigoplus_{i=1}^{r} S_i = F \oplus S$$

et S est stable par f qui est donc semi-simple. □

Lorsque $\mathbb{K}$ est algébriquement clos, les polynômes irréductibles sont de degré 1 donc f est semi-simple si et seulement si f est diagonalisable. On note maintenant M la matrice de f dans une base et on dit qu'elle est semi-simple lorsque f l'est.

Théorème 30

Si le corps $\mathbb{K}$ est de caractéristique nulle, alors M est semi-simple si et seulement s'il existe une extension $\mathbb{L}/\mathbb{K}$ dans laquelle M est diagonalisable.

Démonstration. Soit $\mathbb{K}$ de caractéristique nulle et $\mathbb{L}/\mathbb{K}$ une extension de corps. On commence par montrer que M est semi-simple sur $\mathbb{K}$ si et seulement si M l'est sur $\mathbb{L}$ (ici, M est à coefficients dans $\mathbb{K}$). Le polynôme minimal de M sur $\mathbb{K}$ est le même que celui de M sur $\mathbb{L}$. Il suffit donc de montrer que Π_M est sans facteur carré dans $\mathbb{K}[X]$ si et seulement s'il est sans facteur carré dans $\mathbb{L}[X]$.

Dans un corps de caractéristique nulle, P est sans facteur carré équivaut à $P \wedge P' = 1$. Mais comme le calcul du pgcd s'effectue dans $\mathbb{K}$, le fait que P et P' soient premiers entre eux ne dépend pas du corps considéré.

Prouvons le théorème : supposons que M est semi-simple dans $\mathbb{K}$. Alors soit $\mathbb{L}$ est un corps de décomposition de $\Pi_M \in \mathbb{K}[X]$. Dans $\mathbb{L}[X]$, le polynôme Π_M est scindé à racines simples donc M est diagonalisable. Réciproquement, si M est diagonalisable dans $\mathbb{L}$ alors M est semi-simple dans $\mathbb{L}$ et on vient de montrer que ce fait était équivalent à la semi-simplicité de M sur $\mathbb{K}$. □

Références : GOURDON 2009a, p. 224 et BECK, MALICK et PEYRÉ 2005, pp. 103-104. Merci à Antoine Diez pour ce développement.

Espace de Bergman

Leçons : 201, 202, 205, 208, 213, 234, *235*, 243, 245

Théorème 31

Soit Ω un ouvert connexe et $\mathscr{H}^2(\Omega)$ l'ensemble des fonctions f holomorphes sur Ω et de carré intégrable pour la mesure de Lebesgue sur $\mathbb{C}$ identifié à $\mathbb{R}^2$. On munit cet espace du produit scalaire hermitien $\langle f,g\rangle = \iint_\Omega f(x+iy)\overline{g(x+iy)}\mathrm{d}x\mathrm{d}y$ et de la norme $\|\cdot\|$ associée. Alors :

1 *$\mathscr{H}^2(\Omega)$ est un espace de Hilbert.*

2 *Si $\Omega = \mathbb{D}$ est le disque unité, et $e_n : z \mapsto \sqrt{\dfrac{n+1}{\pi}} z^n$, alors $(e_n)_{n\in\mathbb{N}}$ est une base hilbertienne de $\mathscr{H}^2(\Omega)$.*

Démonstration. **1** Soit $f \in \mathscr{H}^2(\Omega)$, $a \in \Omega$ et ρ tel que $D(a,\rho) \subset \Omega$. Alors selon la formule de la moyenne, $f(a) = \dfrac{1}{2\pi}\int_0^{2\pi} f(a+re^{i\theta})\mathrm{d}\theta$ pour tout $r < \rho$. Donc en multipliant par r et en intégrant, on obtient par un changement de coordonnées polaires :

$$\frac{\rho^2}{2} f(a) = \frac{1}{2\pi}\int_{r=0}^{\rho}\int_{\theta=0}^{2\pi} f(a+re^{i\theta}) r\mathrm{d}\theta\mathrm{d}r = \frac{1}{2\pi}\iint_{D(a,\rho)} f(x+iy)\mathrm{d}x\mathrm{d}y$$

Ainsi, $f(a) = \dfrac{1}{\pi\rho^2}\iint_{D(a,\rho)} f(x+iy)\mathrm{d}x\mathrm{d}y$.

Donc en utilisant l'inégalité de Hölder, on a $|f(a)| \leqslant \dfrac{1}{\pi\rho^2}\,\|f\|\,\|1\| \leqslant \dfrac{1}{\sqrt{\pi}\rho}\,\|f\|$.

Montrons ensuite, grâce à cette inégalité, que $\mathscr{H}^2(\Omega)$ est complet. Soit $(f_n)_{n\in\mathbb{N}}$ une suite de Cauchy dans $\mathscr{H}^2(\Omega)$.

Soit K compact de Ω. La distance d de K au fermé $\mathbb{C}\setminus\Omega$, en le supposant non vide, est donc atteinte et strictement positive.

Si $z \in K$, alors $D(z,d) \subset \Omega$ car $d = \inf_{x\in K, y\notin\Omega}|x-y|$. Donc pour tout z dans K, pour tout $n,m \in \mathbb{N}$, $|f_n(z) - f_m(z)| \leqslant \dfrac{1}{\sqrt{\pi}d}\,\|f_n - f_m\|$ donc (f_n) vérifie le critère de Cauchy uniforme sur tout compact, donc converge uniformément sur tout compact de Ω vers une fonction holomorphe f [5].

Par ailleurs, $\mathrm{L}^2(\Omega)$ est complet selon le théorème de Riesz-Fischer, donc il existe $g \in \mathrm{L}^2(\Omega)$ tel que (f_n) converge vers g pour la norme $\|\cdot\|$. De plus, ce même théorème nous assure qu'il existe une sous suite $(f_{\phi(n)})_{n\in\mathbb{N}}$ convergeant vers g presque partout. Par suite, $f = g$ presque partout et $f \in \mathscr{H}^2(\Omega)$, ce qui conclut.

2 D'abord, $(e_n)_{n\in\mathbb{N}}$ est orthonormée.

En effet, si $n,m \in \mathbb{N}$, alors

5. Ce point est moins élémentaire qu'il n'y paraît. On trouve pour tout compact d'intérieur non vide K de Ω un certain f_K holomorphe sur $\overset{\circ}{K}$ qui est la limite de $(f_{n|K})_{n\in\mathbb{N}}$ pour la norme uniforme. Pour aboutir à la limite f voulue, considérons une suite exhaustive de compacts de Ω, c'est à dire une suite $(K_p)_{p\in\mathbb{N}}$ de compacts tels que $\Omega = \bigcup_{p\in\mathbb{N}} K_p$, et pour tout p, $K_p \overset{circ}{\subset} K_{p+1}$; et posons $f(x) = f_{K_p}(x)$ si $x \in K_p$.

$$\begin{aligned}\langle e_n, e_m\rangle &= \iint_{\mathbb{D}} \sqrt{\frac{(n+1)(m+1)}{\pi^2}}\overline{x+iy}^m (x+iy)^m \,\mathrm{d}x\,\mathrm{d}y \\ &= \frac{\sqrt{(n+1)(m+1)}}{\pi}\int_{r=0}^{1}\int_{\theta=0}^{2\pi} r^{m+n}e^{i\theta(n-m)} r\,\mathrm{d}\theta\,\mathrm{d}r \\ &= \begin{cases} 0 \quad \text{si} \quad n\neq m \\ \dfrac{n+1}{\pi}\times\dfrac{1}{2n+2}\times 2\pi = 1 \quad \text{si} \quad n=m \end{cases}\end{aligned}$$

Pour montrer que $(e_n)_n$ est une suite totale, il suffit de montrer que $\mathrm{Vect}((e_n)_n)^\perp = \{0\}$. Soit $f \in \mathscr{H}^2(\Omega)$. Écrivons le développement en série entière de f autour de 0 : $\forall z \in \mathbb{D}, f(z) = \sum_{m=0}^{+\infty} \alpha_m z^m$, le membre de droite étant uniformément convergent sur tout disque fermé $\overline{D}(0,r)$.

Par ailleurs, pour tout $n \in \mathbb{N}^*$,

$$c_n = \langle e_n, f\rangle = \sqrt{\frac{n+1}{\pi}}\iint_{\mathbb{D}} \overline{z}^n f(z)\mathrm{d}x\mathrm{d}y = \sqrt{\frac{n+1}{\pi}}\iint_{\mathbb{D}} \sum_{m=0}^{+\infty}\alpha_m \overline{z}^n z^m \mathrm{d}x\mathrm{d}y.$$

Par convergence uniforme, on a pour tout $0<r<1$:

$$\begin{aligned}\iint_{\overline{D}(0,r)} \overline{z}^n f(z)\mathrm{d}x\mathrm{d}y &= \sum_{m=0}^{+\infty}\alpha_m \iint_{\overline{D}(0,r)} \overline{z}^n z^m \mathrm{d}x\mathrm{d}y \\ &\overset{x=rx',y=ry'}{=} \sum_{m=0}^{+\infty}\alpha_m r^2 r^n r^m \langle e_n, e_m\rangle \times \frac{\pi}{\sqrt{(n+1)(m+1)}} = \pi\alpha_n \frac{r^{2n+2}}{n+1}\end{aligned}$$

.

Donc $c_n = \lim_{r\to 1^-} \dfrac{\pi\alpha_n r^{2n+2}}{n+1}\sqrt{\dfrac{n+1}{\pi}} = \dfrac{\sqrt{\pi}\alpha_n}{\sqrt{n+1}}$, de sorte que si $\forall n \in \mathbb{N}, \langle e_n, f\rangle = 0$, alors $f = 0$.

□

Référence : BAYEN et MARGARIA 1986, mais surtout tiré du fichier de développements d'Adrien Laurent.

Étude de $O(p,q)$

Leçons : 106, 150, 156, *158*, *170*, 171

Prérequis : exp : $\mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ est un homéomorphisme, et décomposition polaire.

Définition 32

Le groupe orthogonal de la forme quadratique sur $\mathbb{R}^n$ représentée dans la base canonique par la matrice $I_{p,q} = \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix}$, où $p+q=n$ est noté $O(p,q)$.

Théorème 33

On a un homéomorphisme $O(p,q) \simeq O_p(\mathbb{R}) \times O_q(\mathbb{R}) \times \mathbb{R}^{pq}$.

Démonstration. Étape 1 : obtention d'un homéomorphisme $O(p,q) \simeq (O_n(\mathbb{R}) \cap O(p,q)) \times (S_n^{++}(R) \cap O(p,q))$.

D'abord, $O(p,q)$ est stable par transposition :

$$\begin{aligned} M \in O(p,q) &\Leftrightarrow M I_{p,q}\, {}^tM = I_{p,q} \Leftrightarrow M^{-1} = I_{p,q}\, {}^tM I_{p,q}^{-1} = I_{p,q}\, {}^tM I_{p,q} \\ &\Leftrightarrow {}^t M^{-1} = I_{p,q} M I_{p,q} \Leftrightarrow {}^tM \in O(p,q). \end{aligned}$$

Soit $M \in O(p,q)$, de décomposition polaire $M = OS, O \in O_n(R), S \in \mathcal{S}_n^{++}(\mathbb{R})$. On a $S^2 = {}^tMM = T \in \mathcal{S}_n^{++}(\mathbb{R})$. Soit donc $U \in \mathcal{S}_n(\mathbb{R})$ tel que $T = \exp(U)$. Selon ce qui précède, on a de plus $T \in O(p,q)$. Or,

$$\begin{aligned} T \in O(p,q) &\Leftrightarrow \exp(U) I_{p,q} \exp({}^tU) = I_{p,q} \\ &\Leftrightarrow \exp({}^tU) = I_{p,q} \exp(-U) I_{p,q} = \exp(-I_{p,q} U I_{p,q}) \\ &\Leftrightarrow {}^tU = U = -I_{p,q} U I_{p,q} \Leftrightarrow \frac{U}{2} I_{p,q} + I_{p,q} \frac{U}{2} = 0 \\ &\Leftrightarrow {}^t \exp\left(\frac{U}{2}\right) = I_{p,q} \exp\left(\frac{U}{2}\right)^{-1} I_{p,q} \Leftrightarrow \exp\left(\frac{U}{2}\right) \in O(p,q). \end{aligned}$$

Mais $\exp\left(\frac{U}{2}\right)^2 = T$ donc par unicité de la décomposition polaire, $S = \exp\left(\frac{U}{2}\right)$, de sorte que $S \in O(p,q)$. Ainsi, cette décomposition fournit un homéomorphisme

$$O(p,q) \simeq (O_n(\mathbb{R}) \cap O(p,q)) \times (S_n^{++}(R) \cap O(p,q)).$$

Étape 2 : description de $O_n(\mathbb{R}) \cap O(p,q)$.

Soit $O = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in O_n(\mathbb{R}) \cap O(p,q)$, où $A \in \mathcal{M}_p(\mathbb{R}), D \in \mathcal{M}_q(\mathbb{R})$. On a

$${}^tO I_{p,q} O = \begin{pmatrix} {}^tA & {}^tC \\ {}^tB & {}^tD \end{pmatrix} \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} {}^tAA - {}^tCC & {}^tAB - {}^tCD \\ {}^tBA - {}^tDC & {}^tBB - {}^tDD \end{pmatrix} = I_{p,q}$$

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

De plus, $I_n = {}^tOO = \begin{pmatrix} {}^tAA + {}^tCC & {}^tAB + {}^tCD \\ {}^tBA + {}^tDC & {}^tBB + {}^tDD \end{pmatrix}$ donc en combinant les deux résultats, on a ${}^tAA = I_p, {}^tCC = 0, {}^tBB = 0$ et ${}^tDD = I_q$ donc $A \in O_p(\mathbb{R})$, $D \in O_q(\mathbb{R})$ et comme $X \mapsto$

$\mathrm{Tr}({}^tXX)$ est un produit scalaire sur $\mathscr{M}_n(\mathbb{R})$, $C=0$ et $B=0$. Ainsi, on a un homéomorphisme $O_n(\mathbb{R})\cap O(p,q)\simeq O_p(\mathbb{R})\times O_q(\mathbb{R})$.

Étape 3 : description de $S_n^{++}(R)\cap O(p,q)$.

En réutilisant les calculs de la première partie, exp est un homéomorphisme entre $L\cap\mathscr{S}_n(\mathbb{R})$ et $S_n^{++}(R)\cap O(p,q)$ où $L=\left\{U\in\mathscr{S}_n(\mathbb{R}) : UI_{p,q}+I_{p,q}U=0\right\}$.

Soit $U=\begin{pmatrix}A & B\\ {}^tB & C\end{pmatrix}\in L\cap\mathscr{S}_n(\mathbb{R})$, où $A\in S_p(\mathbb{R}), C\in S_q(\mathbb{R})$. On a

$$0=\begin{pmatrix}A & -B\\ {}^tB & -C\end{pmatrix}+\begin{pmatrix}A & B\\ -{}^tB & -C\end{pmatrix}=\begin{pmatrix}2A & 0\\ 0 & -2C\end{pmatrix},$$

donc $A=C=0$ et $U=\begin{pmatrix}0 & B\\ {}^tB & 0\end{pmatrix}$, ce qui fournit l'homéomorphisme $L\cap\mathscr{S}_n(\mathbb{R})\simeq\mathbb{R}^{pq}$ voulu.

□

En se rappelant que $O_p(\mathbb{R})$ et $O_q(\mathbb{R})$ ont deux composantes connexes, on obtient le résultat suivant :

Corollaire 34

L'ensemble $O(p,q)$ a quatre composantes connexes.

En guise de complément, voici la démonstration du prérequis :

Lemme 35

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

Démonstration.

- Si $A\in\mathscr{S}_n(\mathbb{R})$, par le théorème spectral, on peut écrire $A=PDP^{-1}$ où $D=\mathrm{Diag}(\lambda_1,\dots,\lambda_n)$ et $P\in O_n(\mathbb{R})$ donc $\exp(A)=P\exp(D)P^{-1}$ est à valeurs propres strictement positives, donc appartient à $\mathscr{S}_n^{++}(\mathbb{R})$.
- *Injectivité* : soient $A,A'\in\mathscr{S}_n(\mathbb{R})$ telles que $\exp(A)=\exp(A')$. Écrivons $A=PDP^{-1}$ où $D=\mathrm{Diag}(\lambda_1,\dots,\lambda_n)$ et $P\in O_n(\mathbb{R})$. Soit $Q\in\mathbb{R}[X]$ tel que $Q(e^{\lambda_i})=\lambda_i$: il vérifie donc $Q(\exp(A))=A=Q(\exp(A'))$. Comme A' commute avec $\exp(A')$, il commute avec A donc A et A' sont simultanément diagonalisables ce qui donne immédiatement par injectivité de l'exponentielle réelle $A=A'$.
- *Surjectivité* : Soit $B=PDP^{-1}\in\mathscr{S}_n^{++}(\mathbb{R})$ où $D=\mathrm{Diag}(\lambda_1,\dots,\lambda_n)$, $\lambda_i>0$ et $P\in O_n(\mathbb{R})$. Si $A=PD'P^{-1}$ où $D'=\mathrm{Diag}(\ln\lambda_1,\dots,\ln\lambda_n)$, alors $\exp(A)=B$.
- *Bicontinuité* : La continuité de exp étant connue, il reste à montrer que c'est une application ouverte. Soit $(B_p)_p=(\exp(A_p))_p$ suite de $\mathscr{S}_n^{++}(\mathbb{R})$ convergeant vers $B=\exp A\in\mathscr{S}_n^{++}(\mathbb{R})$. Alors comme B est inversible, $(B_p^{-1})_p$ converge vers B^{-1}. Ainsi, pour la norme $\|\cdot\|_2$, $(B_p)_p$ et $(B_p^{-1})_p$ sont bornées.
  Or, si $M\in\mathscr{S}_n^{++}(\mathbb{R})$, $\|M\|_2=\rho(M)$ (car M est diagonalisable en base orthonormée à valeurs propres positives). Donc il existe $C,C''>0$ tel que $\forall p,\mathrm{sp}(B_p)\subset[0,C]$ et $\mathrm{sp}(B_p^{-1})\subset[0,C'']$ de sorte que $\forall p,\mathrm{sp}(B_p)\subset[C',C]$ (où $C'=C''^{-1}$). Mais $\mathrm{sp}(A_p)=\ln\mathrm{sp}(B_p)\subset[\ln C',\ln C]$ donc $(A_p)_p$ est bornée.
  Il reste à montrer que cette suite n'a qu'une seule valeur d'adhérence pour conclure à sa convergence. Si $A_{\varphi(p)}\xrightarrow[p\to+\infty]{}A'\in\mathscr{S}_n(\mathbb{R})$, alors $\exp\left(A_{\varphi(p)}\right)\xrightarrow[p\to+\infty]{}\exp(A')$ donc $\exp(A')=B=\exp(A)$, d'où par injectivité $A=A'$.

□

Référence : Caldero et Germoni 2013, p. 210

Formule des compléments

Leçons : ***207*****, 235, 236,** ***239*****,** ***245***

Référence : AMAR et MATHERON 2003, pp. 249 - 251.

Formule sommatoire de Poisson

Leçons : *241*, 246, 250

Théorème 36

Si $f \in \mathscr{S}(\mathbb{R})$, *et* $\hat{f} : x \mapsto \displaystyle\int_{\mathbb{R}} f(t)e^{-2i\pi tx}\mathrm{d}t$, *alors*

$$\forall x \in \mathbb{R},\ \sum_{n=-\infty}^{+\infty} \hat{f}(n)e^{2i\pi nx} = \sum_{n=-\infty}^{+\infty} f(x+n).$$

Démonstration. Soit $G : x \mapsto \displaystyle\sum_{n=-\infty}^{+\infty} f(x+n)$.

- G **est continue** : en effet, soit $M > 0$ tel que $|f(x)| \leqslant \dfrac{M}{x^2}$ pour $|x| \geqslant 1$. Alors si $K > 0$, et $x \in [-K, K]$, on a pour tout $|n| \geqslant K$,

$$|f(x+n)| \leqslant \frac{M}{(x+n)^2} \leqslant \frac{M}{(|n|-|x|)^2} \leqslant \frac{M}{(|n|-K)^2},$$

  qui est le terme général positif d'une série convergente. Donc G est la somme d'une série de fonctions continues convergeant normalement sur tout segment, donc est continue.
- G **est** $\mathscr{C}^1$: en répétant ce raisonnement, on voit que $\displaystyle\sum_{n\in\mathbb{Z}} f'(x+n)$ converge normalement sur tout segment de $\mathbb{R}$ donc le théorème de dérivation terme à terme nous assure que G est $\mathscr{C}^1$ et $\forall x \in \mathbb{R}, G'(x) = \displaystyle\sum_{n=-\infty}^{+\infty} f'(x+n)$
- G **est 1-périodique** : si $x \in \mathbb{R}$, $G(x+1) = \displaystyle\sum_{n=-\infty}^{+\infty} f(x+n+1) = \sum_{p=-\infty}^{+\infty} f(x+p)$ par un changement d'indice $p = n+1$, soit $G(x+1) = G(x)$.

La fonction G vérifiant les conditions du théorème de convergence normale des séries de Fourier (continue périodique et $\mathscr{C}^1$ par morceaux), elle est somme de sa série de Fourier sur $\mathbb{R}$.

Mais si $n \in \mathbb{Z}$, le n-ième coefficient de Fourier de G est

$$\begin{aligned} c_n(G) &= \int_0^1 G(x)e^{-2i\pi nx}\mathrm{d}x = \int_0^1 \sum_{n=-\infty}^{+\infty} f(x+n)e^{-2i\pi nx}\mathrm{d}x \\ &\overset{\text{CV normale}}{=} \sum_{n=-\infty}^{+\infty} \left(\int_0^1 f(x+n)e^{-2i\pi nx}\mathrm{d}x \right) \\ &\overset{u=x+n}{=} \sum_{n=-\infty}^{+\infty} \left(\int_n^{n+1} f(u)e^{-2i\pi nu}\mathrm{d}u \right) = \int_{-\infty}^{+\infty} f(u)e^{-2i\pi nu}\mathrm{d}u = \hat{f}(n). \end{aligned}$$

En d'autres termes, $\forall x \in \mathbb{R}$, $\displaystyle\sum_{n=-\infty}^{+\infty} f(x+n) = \sum_{n=-\infty}^{+\infty} \hat{f}(n)e^{2i\pi nx}$. □

Proposition 37

Si $s > 0$,

$$\sum_{n=-\infty}^{+\infty} e^{-\pi n^2 s} = \frac{1}{\sqrt{s}} \sum_{n=-\infty}^{+\infty} e^{-\pi n^2/s}.$$

Démonstration. Soit $\alpha > 0$ et $f : x \mapsto e^{-\alpha x^2}$. Si $n \in \mathbb{Z}$,

$$\hat{f}(n) = \int_{\mathbb{R}} e^{-\alpha t^2} e^{-2i\pi nt} \mathrm{d}t \overset{u=\sqrt{\alpha}t}{=} \frac{1}{\sqrt{\alpha}} \int_{\mathbb{R}} e^{-u^2} e^{-2i\pi nu/\sqrt{\alpha}} \mathrm{d}t = \sqrt{\frac{\pi}{\alpha}} e^{-\frac{1}{4}\left(\frac{2\pi n}{\sqrt{\alpha}}\right)^2} = \sqrt{\frac{\pi}{\alpha}} e^{-\pi^2 n^2/\alpha}$$

(transformée de Fourier d'une gaussienne). Donc par la formule de Poisson,

$$\sum_{n=-\infty}^{+\infty} \sqrt{\pi}\alpha e^{-\pi^2 n^2/\alpha} = \sum_{n=-\infty}^{+\infty} e^{-\alpha n^2}.$$

En posant $s = \dfrac{\pi}{\alpha}$, on obtient le résultat désiré. □

Proposition 38

La distribution tempérée $\delta_{\mathbb{Z}} = \sum_{n=-\infty}^{+\infty} \delta_n$ est invariante par transformation de Fourier.

Démonstration. Cette distribution est bien définie car si $f \in \mathscr{S}(\mathbb{R})$, $\langle \delta_{\mathbb{Z}}, f \rangle = \sum_{k=-\infty}^{+\infty} f(k)$ qui est une série convergente selon la formule de Poisson.

Elle est tempérée car si $f \in \mathscr{S}(\mathbb{R})$,

$$\sum_{k=-\infty}^{+\infty} |f(k)| \leqslant \sum_{k=-\infty}^{+\infty} \frac{1}{1+k^2} \|(1+x^2)f\|_\infty = C(\|f\|_\infty + \|x^2 f\|_\infty,$$

avec C constante. Enfin,

$$\langle \hat{\delta_{\mathbb{Z}}}, f \rangle = \langle \delta_{\mathbb{Z}}, \hat{f} \rangle = \sum_{k=-\infty}^{+\infty} \hat{f}(k) \overset{\text{Poisson}}{=} \sum_{k=-\infty}^{+\infty} f(k) = \langle \delta_{\mathbb{Z}}, f \rangle,$$

donc $\hat{\delta_{\mathbb{Z}}} = \delta_{\mathbb{Z}}$. □

Remarque.
- Il faut se souvenir de la transformée de Fourier d'une gaussienne (cf « Inversion de Fourier ») :
- La deuxième application est plutôt pour la leçon 250 qui inclut la transformation de Fourier des distributions.
- La distribution $\sum_{k=-\infty}^{+\infty} a_k \delta_k$ est tempérée si et seulement si il existe $C > 0$ et $N \in \mathbb{N}$ tel que $\forall k \in \mathbb{Z}, |a_k| \leqslant C(1+|k|)^N$ (BONY 2001, p. 171).
- On peut déduire de la deuxième application la formule d'inversion de Fourier, c'est dans LESFARI 2012.

Références : GOURDON 2009b, p. 277 pour le théorème et la première application, WILLEM 1995 p. 149 pour la deuxième application

Inégalité de Hoeffding

Leçons : 253, 260, 262

On se place dans $(\Omega, \mathscr{F}, \mathbb{P})$ un espace probabilisé.

Théorème 39

Soit $(X_n)_n$ suite de variables aléatoires centrées telles que $|X_n| \leqslant c_n$ presque sûrement. Soit $a_n = \sum_{j=1}^{n} c_j^2$ et $S_n = \sum_{j=1}^{n} X_j$. Alors si $\varepsilon > 0$,

$$\mathbb{P}(|S_n| > \varepsilon) \leqslant 2\exp\left(\frac{-\varepsilon^2}{2a_n}\right).$$

Lemme 40

Soit X variable aléatoire centrée telle que $|X| \leqslant 1$ presque sûrement. Alors $L_X(t) = \mathbb{E}[e^{tX}] \leqslant e^{\frac{t^2}{2}}$.

Démonstration. Si $t \in \mathbb{R}$ et $x \in [-1,1]$ alors $tx = \dfrac{1-x}{2} \times (-t) + \dfrac{1+x}{2} \times t$ donc par convexité de la fonction exp, $e^{tx} \leqslant \dfrac{1-x}{2}e^{-t} + \dfrac{1+x}{2}e^{t}$.

Appliquant ce résultat à e^{tX}, on obtient, comme $|X| \leqslant 1$ presque sûrement, $L_X(t) \leqslant \mathbb{E}\left[\dfrac{1-X}{2}\right]e^{-t} + \mathbb{E}\left[\dfrac{1+X}{2}\right]e^{t} = \mathrm{ch}(t)$ car X est centrée.

Enfin, $\mathrm{ch}(t) = \sum_{n=0}^{+\infty} \dfrac{t^{2n}}{(2n)!} \leqslant \sum_{n=0}^{+\infty} \dfrac{t^{2n}}{2^n n!} = e^{\frac{t^2}{2}}$ car $(2n)! = n! \times (n+1) \times \cdots \times (2n) \geqslant 2^n n!$ □

Démonstration (du théorème)**.** Soit $n \in \mathbb{N}^*$. Par indépendance des X_j, on a en remarquant que pour tout $1 \leqslant j \leqslant n$, $\dfrac{X_j}{c_j}$ vérifie les conditions du lemme,

$$\forall t \in \mathbb{R}, L_{S_n}(t) = \prod_{j=1}^{n} L_{X_j}(t) = \prod_{j=1}^{n} L_{\frac{X_j}{c_j}}(tc_j) \leqslant \prod_{i=1}^{n} \exp\left(\frac{t^2 c_j^2}{2}\right) = \exp\left(\frac{t^2 a_n}{2}\right).$$

Soit $\varepsilon > 0$. Selon l'inégalité de Markov,

$$\mathbb{P}(S_n > \varepsilon) = \mathbb{P}(e^{tS_n} > e^{t\varepsilon}) \leqslant \frac{\mathbb{E}\left[e^{tS_n}\right]}{e^{t\varepsilon}} \leqslant \exp\left(\frac{t^2 a_n}{2} - t\varepsilon\right).$$

Or $\varphi : t \mapsto \dfrac{t^2 a_n}{2} - t\varepsilon$ est une fonction polynômiale de degré 2 de coefficient dominant positif et $\varphi'(t) = ta_n - \varepsilon$ donc φ atteint son minimum en $\dfrac{\varepsilon}{a_n}$. Ainsi,

$$\mathbb{P}(S_n > \varepsilon) \leqslant \exp\left(\frac{\varepsilon^2}{a_n^2}\frac{a_n}{2} - \frac{\varepsilon^2}{a_n}\right) = \exp\left(\frac{-\varepsilon^2}{2a_n}\right).$$

En appliquant ce résultat à $-S_n$, on obtient

$$\mathbb{P}(|S_n| > \varepsilon) \leqslant \mathbb{P}(S_n > \varepsilon) + \mathbb{P}(S_n < -\varepsilon) \leqslant 2\exp\left(\frac{-\varepsilon^2}{2a_n}\right),$$

ce qu'il fallait démontrer. □

Proposition 41

On suppose de plus qu'il existe $\alpha, \beta > 0$ tels que $2\alpha - \beta > 0$ et $a_n \leqslant n^{2\alpha-\beta}$ pour tout $n \in \mathbb{N}$. Alors presque sûrement $\frac{S_n}{n^\alpha}$ tend vers 0.

Démonstration. Selon le théorème précédent, $\mathbb{P}(|S_n| \geqslant \varepsilon n^\alpha) \leqslant \exp\left(\frac{-\varepsilon^2 n^{2\alpha}}{2a_n}\right) \leqslant \exp\left(\frac{-\varepsilon^2 n^\beta}{2}\right)$, ce dernier terme étant le terme général positif d'une série convergente (par exemple parce que il est négligeable devant $\frac{1}{n^2}$).

Donc, selon le lemme de Borel-Cantelli, $\frac{S_n}{n^\alpha}$ converge presque sûrement. □

Référence : OUVRARD 2009, p. 210

Invariants de similitude

Leçons : 150, 153, 154, 159

Soit K corps quelconque et E, un $\mathbb{K}$-espace vectoriel de dimension n. Génériquement, u désignera un endomorphisme dans $\mathscr{L}(E)$ dont le polynôme minimal est noté Π_u et le polynôme caractéristique χ_u.

Définition 42

Soit $u \in \mathscr{L}(E)$ et soit $x \in E$. On appelle polynôme minimal de u en x l'unique générateur unitaire de l'idéal

$$\{P \in \mathbb{K}[X],\ P(u)(x) = 0\}.$$

On le note $\Pi_{u,x}$. On a $\Pi_{u,x} | \Pi_u$.

Proposition 43

Il existe $x \in E$ tel que $\Pi_u = \Pi_{u,x}$.

Démonstration. On écrit $\Pi_u = \prod_{i=1}^{r} P_i^{m_i}$ où P_i sont des irréductibles distincts. On note $K_i = \ker P_i^{m_i}(u)$ et $u_i = u|_{K_i}$. Par le lemme des noyaux, $E = \oplus_i K_i$.

Montrons le résultat sur chaque sous-espace K_i. Par l'absurde, si le résultat ne tenait pas, alors pour tout $x_i \in K_i$, Π_{u_i,x_i} diviserait strictement $\Pi_{u_i} = P_i^{m_i}$ donc diviserait $P_i^{m_i-1}$ par irréductibilité. Mais alors $P_i^{m_i-1}(u_i)$ serait nul sur tout K_i, ce qui est impossible par minimalité de Π_{u_i}. On dispose donc d'éléments x_i comme dans l'énoncé sur chaque sous-espace K_i. Montrons que $x = x_1 + \ldots + x_r$ convient. On a :

$$0 = \Pi_{u,x}(u)(x) = \sum_i \Pi_{u,x}(x_i)$$

donc $\Pi_{u,x}(u)(x_i) = 0$ puisque les K_i sont en somme directe. Ainsi, $P_i^{m_i} = \Pi_{u_i,x_i} | \Pi_{u,x}$ pour tout i. Puisque les $P_i^{m_i}$ sont premiers entre eux, leur produit qui est égal à Π_u divise aussi $\Pi_{u,x}$, ce qui conclut. □

Théorème 44

Soit $u \in \mathscr{L}(E)$. Il existe une unique famille $P_1, \ldots, P_r$ de polynômes unitaires et une famille $E_1, \ldots, E_r$ de sous-espaces de E vérifiant :

1. *$P_r | \ldots | P_1$*
2. *$E = E_1 \oplus \ldots \oplus E_r$*
3. *Pour tout $i \in \{1, \ldots, r\}$, E_i est stable par u et $u_{|E_i}$ est cyclique de polynôme P_i.*

Les polynômes $P_1, \ldots . P_r$ sont appelés les invariants de similitudes de u.

Démonstration. Existence. Montrons le résultat par récurrence sur $\dim E$. Il est trivial pour $\dim E = 1$, supposons donc $\dim E > 2$.

Soit $d = \deg(\Pi_u)$ et soit $x \in E$ tel que $\Pi_{u,x} = \Pi_u$. On note $F = \mathrm{Vect}(x, u(x), \ldots, u^{d-1}(x))$. Clairement, F est stable par u et $u|_F$ est cyclique. On va montrer par dualité que F admet un supplémentaire stable par u. Soit $\varphi \in E^*$ tel que :

$$\varphi(x) = \varphi(u(x)) = \ldots = \varphi\left(u^{d-2}(x)\right) = 0 \ \text{ et } \ \varphi\left(u^{d-1}(x)\right) = 1.$$

La famille $(\varphi, \varphi\circ u, \dots, \varphi\circ u^{d-1})$ est une famille libre de E^* et on note Φ le sous-espace vectoriel de E^* engendré par cette famille. On pose alors $G := \Phi^\circ = \{y \in E,\ \forall \psi \in \Phi,\ \psi(y) = 0\}$ et on montre que c'est un supplémentaire de F stable par u.

- *G est stable par u* : soit $y \in G$. Par construction, on a déjà $\forall k \in [\![0, d-2]\!], \varphi \circ u^k\big(u(y)\big) = 0$.. Comme le polynôme minimal de u est de degré d, on a $u^d(y) \in \mathrm{Vect}\big(y, u(y), \dots, u^{d-1}(y)\big)$ et donc $\varphi \circ u^{d-1}\big(u(y)\big) = \varphi\big(u^d(y)\big) = 0$ par ce qui précède.
- $F \cap G = \{0\}$. Soit $y \in F \cap G$, alors on peut écrire $y = a_0 x + \dots a_{d-1} u^{d-1}(x)$ et en appliquant $\varphi \circ u^i$ pour i allant de 0 à $d-1$, on trouve que tous les a_k sont nuls.
- $\dim F + \dim G = n$. C'est une propriété générale de l'orthogonal au sens de la dualité : $\dim \Phi + \dim \Phi^\circ = n$.

De plus, $\Pi_{u_{|G}} | \Pi_u$ puisque Π_u annule $u_{|G}$. En appliquant l'hypothèse de récurrence à $u_{|G}$, on obtient le résultat voulu.

Unicité. On suppose l'existence d'une autre famille de polynôme $Q_1, \dots, Q_s$ donnant lieu à une autre décomposition $F_1 \oplus \dots \oplus F_s$ comme dans l'énoncé. On a déjà $P_1 = Q_i = \Pi_u$. Soit $j > 1$ l'indice minimal tel que $P_j \neq Q_j$. Alors, on a d'une part :

$$P_j(u)(E) = P_j(u)(E_1) \oplus \dots \oplus P_j(u)(E_{j-1}),$$

et d'autre part :

$$P_j(u)(E) = P_j(u)(F_1) \oplus \dots \oplus P_j(u)(F_{j-1}) \oplus P_j(u)(F_j) \oplus \dots \oplus P_j(u)(F_s).$$

Mais pour $i < j$, on a $\dim P_j(u)(E_i) = \dim P_j(u)(F_i)$ donc $0 = \dim P_j(u)(F_j) = \dots = \dim P_j(u)(G_s)$, ce qui prouve que $Q_j | P_j$ et par symétrie $P_j | Q_j$. C'est absurde car $P_j \neq Q_j$. Finalement $r = s$ et $P_i = Q_i$ pour tout i. □

Corollaire 45 (*Décomposition de Frobenius*)

Soit $u \in \mathscr{L}(E)$. Il existe une base dans laquelle la matrice de u est de la forme

$$\begin{pmatrix} C_{P_1} & & \\ & \ddots & \\ & & C_{P_r} \end{pmatrix}$$

où C_{P_i} est la matrice compagnon associée au polynôme P_i avec $P_r | \dots | P_1$. De plus, on a

$$\chi_u = P_1 \dots P_r.$$

Corollaire 46

Deux endomorphismes u et v sont semblables si et seulement s'ils ont les mêmes invariants de similitude.

Démonstration (idée)**.** Supposons u et v semblables. On considère E_i les sous-espaces cycliques associés à u et φ tel que $\varphi \circ u = v \circ \varphi$. Alors si $F_i = \varphi(E_i)$, les F_i sont les sous-espaces cycliques associés à F. □

Corollaire 47

Soit $A \in \mathscr{M}_n(\mathbb{K})$. Alors A est semblable à sa transposée.

Démonstration. Il suffit de le montrer pour A matrice compagnon de la forme $C_P = M_{(e_1,\dots,e_n)}(u)$ où $P = X^n + \sum_{i=0}^{n-1} a_i X^i$. Le changement de base $e'_i = a_1 e_1 + \cdots + a_{n-i} e_{n-i} + e_{n-i+1}$ conduit au résultat. □

Remarque.
- On retrouve en particulier la décomposition de Jordan des endomorphismes nilpotents puisque dans ce cas $\chi_u = X^n$: les invariants de similitudes sont donc de la forme X^{n_i} pour $n_i \leqslant n$.
- Les invariants de similitude ne dépendent pas du corps de base.
- La théorie des $\mathbb{K}[X]$-modules donne une façon simple pour calculer les invariants de similitude : Si U est la matrice de $u \in \mathscr{L}(E)$ dans une certaine base, alors les invariants de similitude de u sont les facteurs invariants non inversibles de la matrice $U - XI_n \in \mathscr{M}_n(\mathbb{K}[X])$.
  En effet, on montre par des opérations élémentaires sur les lignes et les colonnes qu'une matrice de la forme $C_P - XI$ est équivalente à

$$\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ & 1 & \\ 0 & & P \end{pmatrix}$$

  et on utilise la décomposition de Frobenius pour conclure.

Référence : GOURDON 2009a, pp. 289-291. Merci à Antoine Diez pour ce développement.

Inversion de Fourier dans $\mathscr{S}(\mathbb{R})$

Leçons : 236, 239, 250

Théorème 48

Si $f \in \mathscr{S}(\mathbb{R})$ alors $\hat{f} \in \mathscr{S}(\mathbb{R})$ et $\forall x \in \mathbb{R}, \hat{\hat{f}}(x) = 2\pi f(-x)$.

Démonstration. L'idée phare de la preuve est d'approcher pour x donné $\hat{\hat{f}}(x)$ en multipliant par une fonction gaussienne $t \mapsto e^{-\varepsilon t^2}$. Soit donc $f_\varepsilon : t \mapsto e^{-\varepsilon t^2}\hat{f}(t)e^{itx}$.

Étape 1 : par convergence dominée, on remarque que $\displaystyle\int_{\mathbb{R}} f_\varepsilon(t)\mathrm{d}t \xrightarrow[\varepsilon\to 0]{} \int_{\mathbb{R}} \hat{f}(t)e^{itx}\mathrm{d}t$

En effet, pour tout $t \in \mathbb{R}$, $e^{-\varepsilon t^2}\hat{f}(t)e^{itx} \xrightarrow[\varepsilon\to 0]{} \hat{f}(t)e^{itx}$; de plus, pour tout $\varepsilon > 0$, pour tout $t \in \mathbb{R}$, $|f_\varepsilon(t)| \leqslant \left|\hat{f}(t)\right|$, et $\hat{f}$ est intégrable car dans l'espace de Schwartz.

Étape 2 : montrons que $\displaystyle\int_{\mathbb{R}} f_\varepsilon(t)\mathrm{d}t \xrightarrow[\varepsilon\to 0]{} 2\pi f(x)$.

$$\int_{\mathbb{R}} f_\varepsilon(t)\mathrm{d}t = \int_{\mathbb{R}} e^{-\varepsilon t^2}\hat{f}(t)e^{itx}\mathrm{d}t = \int_{\mathbb{R}}\left(\int_{\mathbb{R}} f(u)e^{-itu}e^{itx}e^{-\varepsilon t^2}\mathrm{d}u\right)\mathrm{d}t$$
$$\overset{\text{Fubini}}{=} \int_{\mathbb{R}} f(u)\left(\int_{\mathbb{R}} e^{it(x-u)}e^{-\varepsilon t^2}\mathrm{d}t\right)\mathrm{d}u = \int_{\mathbb{R}} f(u)\hat{g}_\varepsilon(x-u)\mathrm{d}u$$

où $g_\varepsilon : t \mapsto e^{-\varepsilon t^2}$. L'interversion par le théorème de Fubini est justifiée par le fait que f et g_ε sont intégrables.

Par le théorème de dérivation sous le signe intégrale, on a

$$\forall v \in \mathbb{R}, \hat{g}_\varepsilon'(v) = \int_{\mathbb{R}} (-it)e^{-\varepsilon t^2}e^{-itv}\mathrm{d}t \overset{\text{IPP}}{=} \left[\frac{i}{2\varepsilon}e^{-\varepsilon t^2}e^{-itv}\right]_{-\infty}^{+\infty} - \int_{\mathbb{R}} \frac{i}{2\varepsilon}e^{-\varepsilon t^2}\times(-iv)e^{-itv}\mathrm{d}t = \frac{-v}{2\varepsilon}\hat{g}_\varepsilon(v).$$

De plus,

$$\hat{g}_\varepsilon(0) = \int_{\mathbb{R}} e^{-\varepsilon t^2}\mathrm{d}t \overset{\tau=\sqrt{\varepsilon}t}{=} \frac{1}{\sqrt{\varepsilon}}\int_{\mathbb{R}} e^{-t^2}\mathrm{d}t = \sqrt{\frac{\pi}{\varepsilon}}.$$

Donc

$$\int_{\mathbb{R}} f_\varepsilon(t)\mathrm{d}t = \int_{\mathbb{R}} f(u)\sqrt{\frac{\pi}{\varepsilon}}e^{-(x-u)^2}4\varepsilon\mathrm{d}u$$
$$\overset{v=(u-x)/(2\sqrt{\varepsilon})}{=} \int_{\mathbb{R}} f(x+2\sqrt{\varepsilon}v)\sqrt{\frac{\pi}{\varepsilon}}e^{-v^2}2\sqrt{\varepsilon}\mathrm{d}v = \int_{\mathbb{R}} f(x+2\sqrt{\varepsilon}v)2\sqrt{\pi}e^{-v^2}\mathrm{d}v.$$

Par convergence dominée, on obtient

$$\int_{\mathbb{R}} f_\varepsilon(t)\mathrm{d}t \xrightarrow[\varepsilon\to 0]{} \int_{\mathbb{R}} f(x)2\sqrt{\pi}e^{-v^2}\mathrm{d}v = 2\pi f(x).$$

L'hypothèse de domination est bien vérifiée car f est bornée comme tout élément de l'espace de Schwartz donc

$$\forall \varepsilon > 0, \forall v \in \mathbb{R}, |f(x+2\sqrt{\varepsilon}v)|2\sqrt{\pi}e^{-v^2} \leqslant \|f\|_\infty 2\sqrt{\pi}e^{-v^2},$$

de sorte que l'intégrande est dominée par une gaussienne intégrable.

□

Remarque. Le développement est probablement un peu court, on a le temps de détailler les convergences dominées / Fubini effectuées. On peut justifier que $\hat{f} \in \mathscr{S}(\mathbb{R})$ pour terminer, ou bien, spécialement dans la leçon 236, donner un exemple d'utilisation de cette formule pour un calcul d'intégrales.

Référence : QUEFFÉLEC et ZUILY 2013, pp. 330-331.

Inversion de la fonction caractéristique

Leçons : 261, 263

Théorème 49

Soit μ mesure de probabilité sur $(\mathbb{R}, \mathscr{B}(\mathbb{R}))$ et $\varphi : t \mapsto \int_{\mathbb{R}} e^{itx} \mathrm{d}\mu(x)$ sa fonction caractéristique. Alors si $a < b$,

$$\mu(]a,b[) + \frac{1}{2}\mu(\{a,b\}) = \lim_{T\to+\infty} \int_{-T}^{T} \frac{e^{-ita} - e^{-itb}}{it} \varphi(t)\mathrm{d}t.$$

Démonstration. Soit, pour $T > 0$,

$$I_T = \int_{-T}^{T} \frac{e^{-ita} - e^{-itb}}{it} \varphi(t)\mathrm{d}t = \int_{-T}^{T} \left(\int_{\mathbb{R}} \frac{e^{-ita} - e^{-itb}}{it} e^{itx} \mathrm{d}\mu(x) \right) \mathrm{d}t.$$

En remarquant que $\forall t, \left| \frac{e^{-ita} - e^{-itb}}{it} e^{itx} \right| = \left| \int_a^b e^{-ity} \mathrm{d}y \right| \leqslant b - a$, on voit que le théorème de Fubini est applicable. De plus,

$$\overline{I_T} = \int_{-T}^{T} \frac{e^{ita} - e^{itb}}{-it} \varphi(-t)\mathrm{d}t = \int_{-T}^{T} \frac{e^{-iua} - e^{-iub}}{iu} \varphi(u)\mathrm{d}t = I_T$$

par un changement de variable $u = -t$, donc $I_T \in \mathbb{R}$. Ainsi,

$$I_T = \int_{\mathbb{R}} \left(\int_{-T}^{T} \frac{\sin(t(x-a))}{t} \mathrm{d}t - \int_{-T}^{T} \frac{\sin(t(x-b))}{t} \mathrm{d}t \right) \mathrm{d}\mu(x) = \int_{\mathbb{R}} R(x-a,T) - R(x-b,T) \mathrm{d}\mu(x).$$

où $R(\theta, T) = \int_{-T}^{T} \frac{\sin(\theta t)}{t} \mathrm{d}t$. Mais si $\theta > 0$,

$$R(\theta,T) = 2\int_0^T \frac{\sin(\theta t)}{t} \mathrm{d}t = 2\int_0^{\theta T} \frac{\sin(x)}{x} \mathrm{d}x = 2S(\theta T),$$

où $S(x) = \int_0^x \frac{\sin x}{x}$. Si $\theta < 0$, $R(\theta,T) = -R(|\theta|,T)$ donc dans tous les cas, $R(\theta,T) = 2(\mathrm{sgn}\theta)S(|\theta|T)$.

Or, $S(x) \xrightarrow[x\to+\infty]{} \frac{\pi}{2}$ donc $R(\theta,T) \xrightarrow[T\to+\infty]{} \pi(\mathrm{sgn}\theta)$ donc à x fixé,

$$R(x-a,T) - R(x-b,T) \xrightarrow[T\to+\infty]{} \begin{cases} 0 \text{ si } x < a \text{ ou } x > b \\ 2\pi \text{ si } a < x < b \\ \pi \text{ si } x = a \text{ ou } x = b \end{cases}.$$

De plus, $\forall \theta, T, R(\theta,T) \leqslant 2\sup_{y\in R_+} S(y) < +\infty$ car S admet une limite à l'infini et est continue sur $\mathbb{R}_+$. Donc par convergence dominée, $\frac{1}{2\pi} I_T \xrightarrow[T\to+\infty]{} \mu(]a,b[) + \frac{1}{2}\mu(\{a,b\})$. □

Corollaire 50

Si de plus $\int_{\mathbb{R}} |\varphi(t)|\mathrm{d}t < +\infty$*, alors* μ *est une mesure à densité par rapport à la mesure de Lebesgue, de densité* $f : y \mapsto \frac{1}{2\pi}\int_{\mathbb{R}} e^{-ity}\varphi(t)\mathrm{d}t$.

Démonstration. Sous cette hypothèse, si $a < b$, $t \mapsto \varphi(t)\frac{e^{-ita}-e^{-itb}}{it} \in L^1(\mathbb{R})$. Donc

$$\frac{1}{2\pi}\int_{-\infty}^{\infty}\frac{e^{-ita}-e^{-itb}}{it}\varphi(t)\mathrm{d}t = \mu(]a,b[) + \frac{1}{2}\mu(\{a,b\}) \leqslant \frac{b-a}{2\pi}\int_{\mathbb{R}}|\varphi(t)|\mathrm{d}t.$$

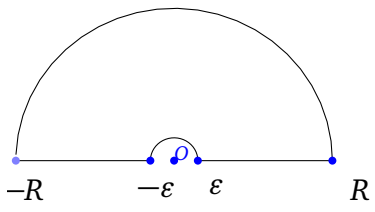
En particulier, $\mu(]a,b[)+\frac{1}{2}\mu(\{a,b\}) \xrightarrow[b\to a]{} 0$. Or, si $\mu(\{a\}) > 0$, on aurait $\forall b > a, \mu(]a,b[) + \frac{1}{2}\mu(\{a,b\}) \geqslant \frac{1}{2}\mu(\{a\}) > 0$ ce qui est absurde. Donc $\mu(\{a\}) = 0$ pour tout $a \in \mathbb{R}$.

Par suite, si $x \in \mathbb{R}, h > 0$,

$$\begin{aligned}\mu(]x,x+h[) &= \frac{1}{2\pi}\int_{\mathbb{R}}\frac{e^{-itx}-e^{-it(x+h)}}{it}\varphi(t)\mathrm{d}t = \frac{1}{2\pi}\int_{\mathbb{R}}\left(\int_x^{x+h} e^{-ity}\mathrm{d}y\right)\varphi(t)\mathrm{d}t \\ &= \int_x^{x+h}\left(\frac{1}{2\pi}\int_{\mathbb{R}} e^{-ity}\varphi(t)\mathrm{d}t\right)\mathrm{d}y\end{aligned}$$

en utilisant le théorème de Fubini. Donc comme $\mathscr{B}(\mathbb{R})$ est engendré par la classe stable par intersection finie $\{]x,x+h[, (x,h) \in \mathbb{R}^2\}$, par le théorème de classe monotone, on en déduit que μ a la densité annoncée par rapport à la mesure de Lebesgue. □

Remarque. • La démonstration repose sur le fait que $\int_0^{+\infty}\frac{\sin x}{x}\mathrm{d}x = \frac{\pi}{2}$ (intégrale de Dirichlet), ce qui est loin d'être évident. Le fait que cette intégrale impropre converge est élémentaire : il suffit de faire une intégration par parties. Pour sa valeur, il y a un bon nombre de preuves différentes, dont un calcul par la transformée de Laplace (dans GOURDON 2009b), une astuce pour se ramener au calcul de $\int_0^{\pi/2}\frac{\sin((2n+1)x)}{\sin x}\mathrm{d}x$, ou bien une preuve par la formule de Cauchy qui est particulièrement élégante.



Soit $f : z \mapsto \frac{e^{iz}}{z}$ holomorphe. Sur le contour dessiné, on a

$$0 = \int_{-R}^{-\varepsilon} f(t)\mathrm{d}t + \int_{\varepsilon}^{R} f(t)\mathrm{d}t - \int_0^{\pi} f(\varepsilon e^{i\theta}) \times (i\varepsilon e^{i\theta})\mathrm{d}\theta + \int_0^{\pi} f(Re^{i\theta} \times (iRe^{i\theta})\mathrm{d}\theta.$$

Comme cos est paire, on voit que la somme des deux premiers termes vaut $i\displaystyle\int_{\varepsilon\leqslant|t|\leqslant R}\frac{\sin t}{t}\mathrm{d}t$.
Par ailleurs, l'intégrande du troisième terme est $i\exp(i\varepsilon e^{i\theta})$ qui converge simplement vers 1 et est de module $\exp(-\varepsilon\sin\theta)\leqslant 1$ donc par convergence dominée, l'intégrale tend vers $i\pi$ quand ε tend vers 0.
De la même manière, le quatrième terme tend vers 0 quand R tend vers $+\infty$.
Ainsi, $\displaystyle\int_{-\infty}^{+\infty}\frac{\sin t}{t}\mathrm{d}t$ est bien définie et vaut π.

- On peut montrer avec des arguments analogues à ceux du théorème que si $a\in\mathbb{R}$, $\mu(\{a\})=\lim\limits_{T\to+\infty}\dfrac{1}{2T}\displaystyle\int_{-T}^{T}e^{-ita}\varphi(t)\mathrm{d}t$. Ainsi, comme les intervalles de la forme $]a,b[$ constituent une classe stable par intersection finie, une mesure de probabilité sur $(\mathbb{R},\mathscr{B}(\mathbb{R}))$ est entièrement déterminée par sa fonction caractéristique.
- Si X est une variable aléatoire telle que $\forall t\in\mathbb{R},\varphi_X(t)\in\mathbb{R}$, alors X et $-X$ ont la même loi.
- Si $X_1\sim\mathcal{N}(0,\sigma_1^2)$, $X_2\sim\mathcal{N}(0,\sigma_2^2)$ et X_1 et X_2 sont indépendants, alors $X_1+X_2\sim\mathcal{N}(0,\sigma_1^2+\sigma_2^2)$.

Référence : DURRETT 2010, p. 105.

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

Leçons : 102, *120, 125*, 141, *144*

Définition 51

Soit k un corps, K_n le corps de décomposition de $P_n = X^n - 1$. On note $\mu_n(K_n)$ le groupe des racines de P_n dans k_n et $\mu_n(K_n)^*$ l'ensemble de ses générateurs. Le n-ième polynôme cyclotomique est

$$\phi_{n,k} = \prod_{\zeta \in \mu_n(K_n)^*} (X - \zeta) \in K_n[X].$$

On note $\phi_n = \phi_{n,\mathbb{Q}}$

On rappelle que $\phi_{n,k} \in k[X]$, que $X^n - 1 = \prod_{d|n} \phi_{d,k}(X)$ et que $\phi_{n,k}$ est de degré $\phi(n)$.

Proposition 52

On a $\phi_n \in \mathbb{Z}[X]$ et si k est un corps, $\sigma : \mathbb{Z} \to k$ le morphisme canonique, $\phi_{n,k} = \sigma(\phi_n)$.

Théorème 53

Le polynôme ϕ_n est irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$.

Démonstration. Soit K corps de décomposition de ϕ_n sur $\mathbb{Q}$, $\zeta \in K$ une racine primitive n-ième de l'unité. Soit p premier ne divisant pas n.

Étape 1 : ζ^p est aussi une racine primitive n-ième de l'unité. En effet, si $up + vn = 1$ est une relation de Bézout entre p et n, on a $\zeta = (\zeta^p)^u(\zeta^n)^v = (\zeta^p)^u$.

Étape 2 : Soient f et g les polynômes minimaux respectifs de ζ et ζ^p sur $\mathbb{Q}$. Ecrivons la décomposition en facteurs irréductibles de ϕ_n sur $\mathbb{Z}$: $\phi_n = \prod_{i=1}^{r} f_i^{\alpha_i}$. Comme ϕ_n est unitaire, il en va de même des f_i quitte à multiplier par -1. De plus, ζ étant racine de ϕ_n, ζ est racine d'un des f_i de sorte que $f_i = f$ par minimalité de f. En particulier $f \in \mathbb{Z}[X]$ et est unitaire et il en va de même pour g.

Étape 3 : Montrons par l'absurde que $f = g$. Si ce n'est pas le cas, f et g sont premiers entre eux donc par le lemme de Gauss, fg divise ϕ_n dans $\mathbb{Z}[X]$. De plus, $g(\zeta^p) = 0$ donc $f(X)$ divise $g(X^p)$ dans $\mathbb{Q}[X]$: $g(X^p) = f(X)h(X), h \in \mathbb{Q}[X]$. En écrivant $h = \frac{a}{b}h_1$ où h_1 polynôme entier primitif, on voit en comparant le contenu de part et d'autre de l'égalité que $h \in \mathbb{Z}[X]$.

Réduisons maintenant modulo p : si $g(X) = a_s X^s + \cdots + a_0$, alors si $\overline{g}$ est la réduction modulo p de g, on a

$$\overline{g}(X^p) = \overline{a_s}X^{ps} + \cdots + \overline{a_0} = \overline{a_s}^p X^{ps} + \cdots + \overline{a_0}^p = (\overline{g}(X))^p$$

par linéarité de l'extension du morphisme de Frobenius à $\mathbb{F}_p[X]$.

Soit φ un facteur irréductible de $\overline{f}$ dans $\mathbb{F}_p[X]$. Alors comme $\overline{g}(X)^p = \overline{f}(X)\overline{h}(X)$, on a par le lemme de Gauss, $\varphi | \overline{g}(X)$. Comme $\overline{f}(X)\overline{g}(X)$ divise $\overline{\phi_n}$, $\overline{\phi_n}$ a un facteur double dans $\mathbb{F}_p[X]$. Mais selon la proposition préliminaire, $\overline{\phi_n} = \phi_{n,\mathbb{F}_q}$ qui n'a pas de racine multiple dans son corps de décomposition donc pas de facteur double. Ayant abouti à une contradiction, on conclut que $f = g$.

Étape 4 : conclusion. Soit ζ' une racine primitive n-ième de l'unité. De même que dans l'étape 1, on a $\zeta' = \zeta^m$ où m est premier avec n. Ainsi, si $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ est la décomposition de m

en facteurs premiers, aucun des p_i ne divise n. Par une récurrence immédiate s'appuyant sur le résultat de l'étape 3, on obtient que le polynôme minimal de ζ' sur $\mathbb{Q}$ est f. En particulier, f annule toutes les racines primitives n-ièmes de l'unité donc, puisque f est unitaire entier et divise ϕ_n, $f = \phi_n$. □

Il est intéressant de prolonger l'étude dans les corps finis, bien que cela dépasse le cadre du développement proprement dit.

Proposition 54

Soit $k = \mathbb{F}_q[X]$, n un entier premier avec q et r l'ordre de $[q]$ dans $(\mathbb{Z}/n\mathbb{Z})^*$. Alors $\phi_{n,k}$ est un produit de facteurs irréductibles simples, tous de degré r.

Démonstration. Le fait que $\phi_{n,k}$ est à facteurs simples a déjà été établi dans la démonstration du théorème.

Soit P un facteur irréductible de ϕ_n, s son degré. Notons $K = k[X]/(P)$ un corps de rupture de P. Celui-ci est de cardinal q^s donc $\forall x \in K, x^{q^s-1} = 1$. De plus, il contient une racine ζ de P, donc de $\phi_{n,k} = \phi_{n,K}$. Donc ζ est une racine primitive n-ième de l'unité de K, de sorte que $n \mid q^s - 1$ puisque n est l'ordre de ζ dans K^*. D'où $q^s \equiv 1[n]$ et comme r est l'ordre multiplicatif de $[q]$, r divise s.

Par ailleurs, $n \mid q^r - 1$ par définition de r donc $\zeta^{q^r} = \zeta : \zeta$ appartient au sous-corps L de K constitué des racines de $X^{q^r} - X$ dans K (cf construction des corps finis). Comme ζ est un générateur du groupe des racines n-ièmes de l'unité dans un corps de décomposition K_n de $X^n - 1$ et $K \subset K_n$, ζ engendre K^*, d'où $K = k[\zeta]$. De même, $L = k[\zeta]$ donc $K = L$. En particulier, $\mathrm{Card}(K) = q^s \leqslant q^r$ donc $s \leqslant r$, et finalement $s = r$. □

Corollaire 55

Le polynôme $\phi_{n,\mathbb{F}_q}$ est irréductible si et seulement si q engendre $(\mathbb{Z}/n\mathbb{Z})^*$.

Remarque.
- L'exemple de $\phi_7 = 1 + X + \cdots + X^6$ montre la complexité de la situation sur les corps finis. Modulo 2, $\phi_7 = (1 + X + X^3)(1 + X^2 + X^3)$ n'est pas irréductible.
- Une première application est la description du groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ pour ζ racine primitive n-ième de l'unité. Une conséquence immédiate du théorème est que ϕ_n est le polynôme minimal de ζ et $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.
  Soit le morphisme de groupes $j : \begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^* & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \\ [m]_n & \longmapsto & \sigma_m : \zeta \mapsto \zeta^m \end{array}$. Il est injectif car si $j([m]) = \mathrm{id}$, on a $\zeta^m = \zeta$ donc $\zeta^{m-1} = 1$ et comme ζ est primitive, $m \equiv 1[n]$. De plus, les racines de ϕ_n dans $\mathbb{Q}(\zeta) = \mathbb{Q}(\mathbb{U}_n)$ sont les ζ^k pour k premier avec n et tout $\mathbb{Q}$-automorphisme envoie une racine du polynôme minimal ϕ_n de ζ sur une autre, ce qui prouve la surjectivité. Ainsi $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.
- Pour la culture, une (lointaine) application de l'irréductibilité de ϕ_n est le théorème de la progression arithmétique de Dirichlet, et plus généralement le théorème de densité de Chebotarev qui s'appuie sur la structure du groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

Références : PERRIN 1996, p. 79, et DEMAZURE 2008, p. 206

Lemme de Morse

Leçons : 158, 170, 171, 214, 215, 218

Théorème 56

Soit U ouvert de R^n, $f \in \mathscr{C}^3(U,\mathbb{R})$ telle que $f(0)=0$, $Df(0)=0$ et $D^2f(0)$ est une forme bilinéaire non dégénérée de signature $(p,n-p)$. Alors il existe V, W voisinages ouverts de 0 et un $\mathscr{C}^1$-difféomorphisme $\varphi : V \to W$ tels que $\forall x \in V, f(x) = Q_0(\varphi(x))$ où $Q_0(y_1,\dots,y_n) = y_1^2+\cdots+y_p^2-y_{p+1}^2-\cdots-y_n^2$.

Lemme 57

Si $A_0 \in \mathrm{GL}_n(\mathbb{R}) \cap \mathscr{S}_n(\mathbb{R})$, alors il existe un voisinage V de A_0 dans $\mathscr{S}_n(\mathbb{R})$ et $\rho \in \mathscr{C}^1(V, \mathrm{GL}_n(\mathbb{R})$ tel que $\forall A \in V, A = {}^t\rho(A)A_0\rho(A)$.

Démonstration. Soit $\psi : \begin{array}{ccc} \mathscr{M}_n(\mathbb{R}) & \longrightarrow & \mathscr{S}_n(\mathbb{R}) \\ M & \longmapsto & {}^tMA_0M \end{array}$. Cette fonction est de classe $\mathscr{C}^1$ et sa différentielle en l'identité est $D\psi(I_n) : H \mapsto {}^tHA_0 + A_0H$ (différentielle d'une application bilinéaire).

Donc $\ker D\psi(I_n) = A_0^{-1}\mathscr{A}_n(\mathbb{R})$. De plus, $\mathscr{M}_n(\mathbb{R})$ se décompose en $\mathscr{M}_n(\mathbb{R}) = A_0^{-1}S_n(R) + A_0^{-1}\mathscr{A}_n(\mathbb{R})$. Donc selon le théorème d'inversion local appliqué à $\tilde{\psi} = \psi_{|A_0^{-1}\mathscr{S}_n(\mathbb{R})}$, il existe U voisinage de $I_n = A_0A_0^{-1}$ dans $A_0^{-1}\mathscr{S}_n(\mathbb{R})$, V voisinage de A_0 dans $\mathscr{S}_n(\mathbb{R})$ tels que $\tilde{\psi} : U \to V$ soit un $\mathscr{C}^1$-difféomorphisme.

Or, $\mathrm{GL}_n(\mathbb{R})$ est un ouvert de $\mathscr{M}_n(\mathbb{R})$ donc $\tilde{U} = U \cap \mathrm{GL}_n(\mathbb{R})$ est un ouvert (non vide car contenant I_n). L'inverse de la restriction de $\tilde{\psi}$ à cet ouvert fournit une application ρ de classe $\mathscr{C}^1$ de $\tilde{V}$ voisinage de A_0 dans $\tilde{U} \subset \mathrm{GL}_n(\mathbb{R})$ vérifiant $\forall A \in \tilde{V}, A = \tilde{\psi}(\rho(A)) = {}^t\rho(A)A_0\rho(A)$.

□

Démonstration (du théorème)**.** Notons, pour $x \in U$, $H(x)$ la matrice hessienne de f en x. Selon la formule de Taylor avec reste intégral à l'ordre 1, applicable car f est de classe $\mathscr{C}^2$, on a

$$\forall x \in U, f(x) = \int_0^1 (1-t)\,{}^txH(tx)x\,\mathrm{d}t = {}^tx\left(\int_0^1 (1-t)H(tx)\right)x = {}^txQ(x)x$$

où Q est une matrice réelle symétrique et $Q(0) = \dfrac{H(0)}{2}$ est une matrice symétrique inversible de signature $(p,n-p)$.

Selon le lemme précédent, il existe un voisinage V de $Q(0)$ dans $\mathscr{S}_n(\mathbb{R})$ et $\rho \in \mathscr{C}^1(V, \mathrm{GL}_n(\mathbb{R}))$ tels que $\forall A \in V, {}^t\rho(A)Q(0)\rho(A)$.

Or, $x \mapsto Q(x)$ est continue sur U puisque f est de classe $\mathscr{C}^3$ donc il existe un voisinage V_0 de 0 dans U tel que $\forall x \in V_0, Q(x) \in V$.

Donc $\psi : x \in V_0 \mapsto \rho(Q(x))$ est telle que $\forall x \in V_0, Q(x) = {}^t\psi(x)Q(0)\psi(x)$, d'où

$$f(x) = {}^t\varphi(x)I_{p,n-p}\varphi(x)$$

où $I_{p,n-p} = \begin{pmatrix} I_p & 0 \\ 0 & -I_{n-p} \end{pmatrix}$, $Q(0) = {}^tPI_{p,n-p}P$ (théorème de Sylvester) et $\varphi : x \mapsto P\rho(Q(x))x$.

Montrons finalement que $\varphi : V_0 \to W_0 = \varphi(V_0)$ est un $\mathscr{C}^1$-difféomorphisme à l'aide du théorème d'inversion locale.

$$\forall h \in V_0, \varphi(h) - \varphi(0) = P(\psi(0) + D\psi(0).h + o(\|h\|))h = P\psi(0)h + o(\|h\|)$$

car $D\psi(0)$ est une application linéaire continue. Donc la matrice jacobienne de φ en 0 est $P\psi(0) \in \mathrm{GL}_n(\mathbb{R})$, de sorte que φ est le $\mathscr{C}^1$-difféomorphisme local attendu. □

Remarque.
- Le résultat est en fait vrai pour une fonction de classe $\mathscr{C}^2$, mais la démonstration est plus subtile.
- La preuve peut être faite de manière plus concise avec le théorème des submersions.

Référence : ROUVIÈRE 2003, p. 344.

Loi de réciprocité quadratique

Leçons : 101, 120, 121, *123, 126*, 170, 190

Définition 58

Soit p premier impair. Le symbole de Legendre associé à p est $\left(\frac{\cdot}{p}\right) : a \in \mathbb{F}_p^* \mapsto a^{\frac{p-1}{2}}$. Il vaut 1 si a est un carré modulo p et -1 sinon.

Théorème 59

Si p et q sont deux premiers impairs distincts, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Lemme 60

Si $a \in \mathbb{F}_q^*$, l'équation $ax^2 = 1$ a $1 + \left(\frac{a}{q}\right)$ solutions.

Démonstration. Soit $X = \left\{(x_1, \dots, x_p) \in \mathbb{F}_q^p : \sum_{i=1}^{p} x_i^2 = 1\right\}$. On va compter le nombre d'éléments de X de deux manières différentes.

Étape 1 : dénombrement par la formule des classes.

$\mathbb{Z}/p\mathbb{Z}$ agit sur X par permutation circulaire via $\overline{a} \cdot (x_1, \dots, x_p) = (x_{1+a}, \dots, x_{p+a})$, les indices étant considérés modulo p.

Le stabilisateur d'un élément x étant un sous groupe de $\mathbb{Z}/p\mathbb{Z}$, il est soit trivial soit le groupe tout entier. Dans le second cas, cela signifie que toutes les composantes de x sont égales et que $px_1^2 = 1$ dans $\mathbb{Z}/q\mathbb{Z}$. Selon le lemme, il y a donc $1 + \left(\frac{p}{q}\right)$ orbites réduites à un singleton.

Ainsi, selon la formule des classes, si $x^1, \dots, x^r$ sont les représentants des orbites non triviales,

$$|X| = 1 + \left(\frac{p}{q}\right) + \sum_{i=1}^{r} \frac{p}{|\mathrm{Stab}(x^i)|} \equiv 1 + \left(\frac{p}{q}\right) [p]$$

Étape 2 : dénombrement « géométrique » .

On remarque que $X = \left\{x \in \mathbb{F}_q^p : q(x) = 1\right\}$ où $q(x) = \sum_{i=1}^{p} x_i^2$. Cette forme quadratique est représentée dans la base canonique $\mathscr{B}$ par I_p.

Introduisons la forme quadratique $r : (y_1, \dots, y_d, z_1, \dots, z_d, t) \mapsto 2\sum_{i=1}^{d} y_i z_i + at^2$ où $d = \frac{p-1}{2}$ et $a = (-1)^{\frac{p-1}{2}}$. Quitte à écrire $(y_1, \dots, y_d, z_1, \dots, z_d, t)$ sous la forme $(y_1, z_1, \dots, y_d, z_d, t)$, on peut supposer que la matrice

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

représente r dans $\mathscr{B}$. Or, $\det A = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}} = 1$ donc selon la classification des formes quadratiques dans un corps fini, r et q sont équivalentes. Si on fixe $u \in \mathrm{GL}_p(\mathbb{F}_q)$ tel que $r = q \circ u$, on constate que u induit une bijection de X sur

$$X' = \left\{ (y_1, \dots, y_d, z_1, \dots, z_d, t) : 2\sum_{i=1}^{d} y_i z_i + at^2 = 1 \right\}.$$

Il s'agit donc de dénombrer $|X'|$. Il y a deux types de points dans X' :

- Ceux qui vérifient $y_1 = \cdots = y_d = 0$: il y en a q^d (choix de z) multiplié par $1 + \left(\frac{a}{p}\right) = 1 + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ (nombre de solutions de $at^2 = 1$).
- Les autres : une fois choisi $(y_1, \dots, y_d)$ non nul ($q^d - 1$ choix) et t (q choix), z est déterminé par l'équation $2\sum_{i=1}^{d} y_i z_i + at^2 = 1$ est celle d'un hyperplan affine de $\mathbb{F}_q^d$; il y a donc q^{d-1} possibilités pour z.

Ainsi, X' a pour cardinal

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

Étape 3 : Conclusion

En comparant les deux calculs précédents modulo p, on a $1 + \left(\frac{p}{q}\right) \equiv q^{p-1} + q^d (-1)^{\frac{p-1}{2}\frac{q-1}{2}} [p]$

Or, dans $\mathbb{F}_p$, $q^d = q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right)$, et $q^{p-1} = 1$ (Fermat) donc $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, ce qui n'est autre que la loi de réciprocité quadratique.

□

Théorème 61

Il y a deux classes d'équivalences de formes quadratiques non dégénérées sur $\mathbb{F}_q^n$, représentées par I_n et $\begin{pmatrix} 1 & & (0) \\ & \ddots & \\ & & 1 \\ (0) & & a \end{pmatrix}$ *où $a \in \mathbb{F}_q^*$ n'est pas un carré.*

Référence : CALDERO et GERMONI 2013, pp. 185-186.

Méthode de Newton

Leçons : *218*, 223, 226, 228, 229

Théorème 62

Soit I intervalle de $\mathbb{R}$, $a \in I$ et $f : I \to \mathbb{R}$ de classe $\mathscr{C}^2$. Si $f(a) = 0$ et $f'(a) > 0$, il existe $J = [a-h, a+h]$ tel qu'on ait $\forall x \in J, f'(x) > 0$ et que J soit stable par $\varphi : x \mapsto x - \dfrac{f(x)}{f'(x)}$.

Alors si $x_0 \in J$, la suite définie par la relation de récurrence $x_{n+1} = \varphi(x_n)$ converge vers a, et il existe $C > 0$ tel que $\forall n \in \mathbb{N}, |x_n - a|^2 \leqslant C^{2^n-1}|x_0 - a|^{2^n}$

De plus, si $f''(a) > 0$ et $x_0 > a$, la suite (x_n) est décroissante et

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

Démonstration. Comme f' est continue sur I et $f'(a) > 0$, on peut trouver $J = [a-h, a+h]$ tel que $\forall x \in J, f'(x) > 0$. De plus, si $x \in J$,

$$\varphi(x) - a = x - a - \frac{f(x) - f(a)}{f'(x)} = \frac{f(a) - f(x) - (a-x)f'(x)}{f'(x)}.$$

Selon l'égalité de Taylor appliquée à la fonction f de classe $\mathscr{C}^2$ entre a et x, il existe $z_x \in [a, x]$ tel que

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

Ainsi, si $m = \min_J |f'| > 0$ (car f' est continue et strictement positive sur J compact) et $M = \max_J |f''|$, on a

$$|\varphi(x) - a| \leqslant \frac{1}{2}\frac{M}{m}|x-a|^2 = C|x-a|^2.$$

En particulier, si $Ch^2 \leqslant h$ soit $h \leqslant \dfrac{1}{C}$, J est un intervalle stable par φ. Quitte à prendre h plus petit, on suppose donc que cette hypothèse est vérifiée.

Ainsi, si $x_0 \in J$, la suite $(x_n)_n$ est bien définie et vérifie $\forall n \in \mathbb{N}, |x_{n+1} - a| \leqslant C|x_n - a|^2$. Par conséquent, $C|x_{n+1} - a| \leqslant (C|x_n - a|^2)^2$ donc une récurrence immédiate nous assure que

$$\forall n \in \mathbb{N}, |x_n - a|^2 \leqslant C^{2^n-1}|x_0 - a|^{2^n}.$$

En particulier, (x_n) converge vers a.

Supposons à présent que $f''(a) > 0$. Par le même argument que pour f', on peut supposer, quitte à remplacer J par un sous-intervalle, que $\forall x \in J, f''(x) > 0$. Par suite, f' est croissante sur J et en particulier, si $x \geqslant a$, $f'(x) \geqslant f'(a) > 0$ donc f elle-même est croissante. Ainsi, $\forall x > a, f(x) > f(a) = 0$.

On obtient donc $\forall x > a, \varphi(x) = x - \dfrac{f(x)}{f'(x)} < x$. De plus si $x \geqslant a$,

$$\varphi(x) - a = \frac{1}{2}\frac{f''(z_x)}{f'(x)}(x-a)^2 \geqslant 0.$$

car $a \leqslant z_x \leqslant x$ [6]. Par conséquent, si $x_0 > a$, la suite (x_n) est décroissante et $\forall n \in \mathbb{N}, x_n \geqslant a$.

6. Cette inégalité exprime simplement le fait que, par convexité de f, le graphe de f est au-dessus de ses tangentes.

De plus,

$$\forall n \in \mathbb{N}, x_{n+1} - a = \frac{1}{2}\frac{f''(z_n)}{f'(x_n)}(x_n - a)^2 \quad \text{avec} \quad a \leqslant z_n \leqslant x_n,$$

donc comme $x_n \xrightarrow[n\to+\infty]{} a$, il en va de même pour (z_n) et par continuité de f' et f'', on a

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

□

Exemple. Application à l'approximation d'une racine carrée : si $y > 0$ et $f : x \mapsto x^2 - y$, $a = \sqrt{y}$ alors si $c > a$ et $c^2 > c$, l'intervalle $J = [a, +\infty[$ est stable et si $x_0 \in J$, on a la majoration de l'erreur

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

En effet, soit $F : x \mapsto x - \dfrac{f(x)}{f'(x)} = \dfrac{x^2 + a^2}{2x}$. On a

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

de sorte que

$$\frac{F(x) - a}{F(x) + a} = \left(\frac{x-a}{x+a}\right)^2.$$

Donc en considérant $\varphi : x \mapsto \dfrac{x-a}{x+a}$ qui est une bijection de $]-a, +\infty[$ sur $]-\infty, 1[$, et $G : x \mapsto x^2$, on a $F = \varphi^{-1} \circ G \circ \varphi$.

Ainsi, si $x_0 \in J$ et $x_{n+1} = F(x_n)$, on a pour tout $n \in \mathbb{N}$, $x_n = (\varphi^{-1} \circ G^n \circ \varphi)(x_0)$, soit

$$\frac{x_n - a}{x_n + a} = \left(\frac{x_0 - a}{x_0 + a}\right)^{2^n}.$$

D'où

$$1 + \frac{2a}{x_n - a} = \left(1 + \frac{2a}{x_0 - a}\right)^{2^n} \overset{x_0 > a}{\geqslant} 1 + \left(\frac{2a}{x_0 - a}\right)^{2^n}.$$

Une simplification immédiate nous fournit la majoration voulue.

Remarque.
- Attention à bien adapter l'énoncé du théorème pour le rendre tout à fait général, les jurys y seront attentifs puisque c'est un développement très classique.
- L'énoncé du théorème peut être résumé en disant simplement que a est un point fixe superattractif de φ.
- Une généralisation existe en dimension n (et a une preuve identique) : Newton-Raphson. Si $f : U \subset \mathbb{R}^n \to \mathbb{R}^n$ est tel que $Df(a)$ est inversible et $f(a) = 0$, alors a est un point fixe superattractif de $\varphi : x \to x - (Df(x))^{-1}.f(x)$. (voir DEMAILLY 2006, p. 110).

Référence : ROUVIÈRE 2003 p. 142.

Méthodes itératives de résolution d'un système linéaire

Leçons : 157, 162, 226, 233

Soit $A \in \mathrm{GL}_n(\mathbb{R})$, $b \in \mathbb{R}^n$. On étudie le système $Ax = b$.

Définition 63

Si $(M,N) \in \mathrm{GL}_n(\mathbb{R}) \times \mathscr{M}_n(\mathbb{R})$ est tel que $A = M - N$, on dit que la méthode itérative associée à (M,N) converge si pour tout $u_0 \in \mathbb{R}^n$, la suite de premier terme u_0 et définie par $\forall k \in \mathbb{N}, u_{k+1} = M^{-1}(Nu_k + b)$ converge.

Théorème 64

La méthode itérative associée à (M,N) converge si et seulement si $\rho(M^{-1}N) < 1$.

Commençons par montrer un lemme :

Lemme 65

Soit $A \in \mathscr{M}_n(\mathbb{C})$, $\varepsilon > 0$. Alors il existe une norme subordonnée $|||\cdot|||$ telle que $|||A||| \leqslant \rho(A) + \varepsilon$.

Démonstration. Comme A est à coefficients dans $\mathbb{C}$, elle est trigonalisable : on se donne donc P inversible et $T = (t_{ij})_{1 \leqslant i,j \leqslant n}$ triangulaire supérieure tels que $A = PTP^{-1}$.

Notons $(e_1, \dots, e_n)$ la base canonique de $\mathbb{C}^n$. Pour $\delta > 0$, on pose $e'_1 = \delta^{i-1} e_i$ et $D_\delta = \mathrm{Diag}(1, \delta, \cdots, \delta^{n-1})$.

On a donc

$$\forall j \in [\![1,n]\!], Te'_j = \delta^{j-1} Te_j = \delta^{j-1} \sum_{i=1}^{j} t_{ij} e_i = \sum_{i=1} \delta^{j-i} t_{ij} e'_i,$$

de sorte que

$$T_\delta := D_\delta^{-1} T D_\delta = \begin{pmatrix} t_{11} & \delta t_{12} & \dots & \delta^{n-1} t_{1n} \\ & \ddots & \ddots & \dots \\ (0) & & \ddots & \delta t_{n-1n} \\ & & & t_{nn} \end{pmatrix}.$$

On définit pour $x \in \mathbb{R}^n$, $\| x \| = \| (PD_\delta)^{-1} x \|_\infty$, et on note $|||\cdot|||$ la norme subordonnée associée. On vérifie aisément que $\forall B \in \mathscr{M}_n(\mathbb{R}), |||B||| = |||(PD_\delta)^{-1} B P D_\delta|||_\infty$.

Or (admis ici), pour tout $B = (b_{ij})_{i,j} \in \mathscr{M}_n(\mathbb{R})$, on a $|||B|||_\infty = \sup\limits_{1 \leqslant i \leqslant n} \sum\limits_{j=1}^{n} |b_{ij}|$. En choisissant $\delta > 0$ tel que pour tout $1 \leqslant i \leqslant n-1$, $\sum\limits_{j=i+1}^{n} \delta^{j-i} |t_{ij}| \leqslant \varepsilon$, on obtient donc, puisque $\rho(A) = \sup_{1 \leqslant i \leqslant n} |t_{ii}|$, $|||A||| = |||T_\delta|||_\infty \leqslant \rho(A) + \varepsilon$. □

Démonstration (du théorème)**.** Soit $u \in \mathbb{R}^n$ tel que $Au = b$, c'est à dire $Mu = Nu + b$. Posons $e_k = u_k - u$ en reprenant les notations du théorème. Alors

$$e_{k+1} = M^{-1}(Nu_k + b) - M^{-1}Nu - M^{-1}b = M^{-1}N(u_k - u) = M^{-1}Ne_k.$$

Ainsi, par une récurrence immédiate, $\forall k \in \mathbb{N}, e_k = (M^{-1}N)^k e_0$. Dès lors, deux cas se présentent :

- Si $\rho(M^{-1}N) < 1$, on fixe $\varepsilon = \dfrac{1-\rho(M^{-1}N)}{2}$ et le lemme nous fournit une norme subordonnée $|||\cdot|||$ telle que $|||M^{-1}N||| \leqslant \rho(M^{-1}N)+\varepsilon < 1$. Donc pour la norme $\|\cdot\|$ associée, on a pour tout k, $\| e_k \| \leqslant |||M^{-1}N|||^k \| e_0 \|$ donc $\lim\limits_{k\to+\infty} e_k = 0$ si bien que $(u_k)_k$ converge vers u.
- Si $\rho(M^{-1}N) \geqslant 1$, soit λ valeur propre complexe de module supérieur ou égal à 1, et $\tilde{u} = \tilde{u}_1 + i\tilde{u}_2$ un vecteur propre associé. Comme pour tout k, $(M^{-1}N)^k\tilde{u} = \lambda^k\tilde{u}$, la méthode itérative ne converge pas pour $u_0 = u + \tilde{u}_1$.

□

Décrivons maintenant quelques cas particuliers de méthodes itératives :

- Méthode de Jacobi : $M = \mathrm{Diag}(a_{11},\dots,a_{nn}) = D$ et $N = D-A$. On note $J = D^{-1}(D-A)$
- Méthode de Gauss-Seidel : $M = D-E$ où $D = \mathrm{Diag}(a_{11},\dots,a_{nn})$ et $E = -A_{\mathrm{inf}}$, partie triangulaire inférieure stricte de A. $N = -A_{\mathrm{sup}} = F$. On note $\mathscr{L}_1 = (D-E)^{-1}F$.
- Méthode de relaxation : $M = \dfrac{D}{\omega} - E$ et $N = \dfrac{1-\omega}{\omega}D + F$,

$$\mathscr{L}_\omega = \left(\frac{D}{\omega} - E\right)^{-1}\left(\frac{1-\omega}{\omega}D + F\right).$$

Proposition 66

Si A est une matrice tridiagonale, $\rho(\mathscr{L}_1) = (\rho(J))^2$. La méthode de Gauss-Seidel a donc une vitesse de convergence double de celle de la méthode de Jacobi.

Démonstration. Remarque préliminaire : introduisons pour $\mu \neq 0$:

$$A(\mu) = \begin{pmatrix} b_1 & \mu^{-1}c_2 & & (0) \\ \mu a_2 & b_2 & \ddots & \\ & \ddots & \ddots & \mu^{-1}c_n \\ (0) & & \mu a_n & b_n \end{pmatrix}$$

où $A = A(1)$. Alors $A(\mu) = Q(\mu)A(1)Q(\mu)^{-1}$ où $Q(\mu) = \mathrm{Diag}(\mu,\mu^2,\dots,\mu^n)$, donc $\det A(\mu) = \det A(1)$.

Les valeurs propres de J sont les racines du polynôme caractéristique

$$p_J(\lambda) = \det(D^{-1}(E+F) - \lambda I),$$

ce sont aussi celles de $q_J(\lambda) = \det(\lambda D - E - F)$. De même, les valeurs propres de $\mathscr{L}_1$ sont les racines de $p_{\mathscr{L}_1}(\lambda) = \det((D-E)^{-1}F - \lambda I)$, et celles de $q_{\mathscr{L}_1}(\lambda) = \det(\lambda D - \lambda E - F)$.

Mais selon la remarque préliminaire,

$$\forall \lambda \in \mathbb{C}^*, q_{\mathscr{L}_1}(\lambda^2) = \det(\lambda^2 D - \lambda^2 E - F) = \lambda^n \det(\lambda D - \lambda E - \lambda^{-1}F) = \lambda^n \det(\lambda D - E - F) = \lambda^n q_J(\lambda).$$

Donc les valeurs propres non nulles de $\mathscr{L}_1$ sont les carrés de valeurs propres non nulles de J, ce qui permet de conclure. □

Proposition 67

Le rayon spectral de $\mathscr{L}_\omega$ est strictement supérieur à $|\omega - 1|$. La méthode de relaxation ne peut donc converger que si $\omega \in]0,2[$.

Démonstration. La matrice $\mathscr{L}_\omega = \left(\frac{D}{\omega} - E\right)^{-1}\left(\frac{1-\omega}{\omega}D + F\right)$ est trigonalisable comme produit de matrices trigonalisables et en notant $\lambda_1, \ldots, \lambda_n$ ses valeurs propres avec multiplicité, on a

$$\prod_{i=1}^{n} \lambda_i = \det(\mathscr{L}_\omega) = \frac{\det\left(\frac{1-\omega}{\omega}D + F\right)}{\det\left(\frac{D}{\omega} - E\right)} = \frac{\prod_{i=1}^{n} \frac{1-\omega}{\omega} a_{ii}}{\prod_{i=1}^{n} \frac{a_i i}{\omega}} = (1-\omega)^n.$$

Donc $\rho(\mathscr{L}_\omega)^n \geqslant |\det(\mathscr{L}_\omega)| = |1-\omega|^n$ de sorte que $\rho(\mathscr{L}_\omega) \geqslant |\omega - 1|$. □

Remarque.
- Par des techniques similaires, on montre que si A est tridiagonale et J a un spectre réel, la méthode de Jacobi et la méthode de relaxation pour $0 < \omega < 2$ convergent ou divergent simultanément. De plus, $\omega_0 = \dfrac{1}{1 + \sqrt{1 - \rho(J)^2}}$ est un paramètre de relaxation tel que $\rho(\mathscr{L}_{\omega_0})$ est minimal.
- En 15 minutes, on peut difficilement faire tout le développement, la dernière proposition est là à titre culturel.

Référence : CIARLET 1988, p. 102

Nombre de zéros d'une équation différentielle

Leçons : 220, 221, 224

On considère l'équation différentielle linéaire du second ordre $(E) : y'' + qy = 0$. On suppose que $q \in \mathscr{C}^1([a,+\infty[,\mathbb{R}_+^*)$, que $\displaystyle\int_a^{+\infty} \sqrt{q(u)}\mathrm{d}u = +\infty$ et que $q'(x) = o_{+\infty}(q^{3/2}(x))$. On se donne une solution y non nulle de (E) et on cherche à obtenir un équivalent à l'infini de la fonction $N : x \mapsto \mathrm{Card}\,\{u \in [a,x] : y(u) = 0\}$.

Théorème 68

Sous ces hypothèses, on a

$$N(x) \backsim_{x\to+\infty} \frac{1}{\pi}\int_a^x \sqrt{q(u)}\mathrm{d}u.$$

Lemme 69

Soient y_1 et y_2 deux fonctions de $\mathscr{C}^1([a,+\infty[,\mathbb{R}_+^*)$ sans zéro commun. Alors si $w = y_1y_2' - y_2y_1'$ (Wronskien), et $y_1(a) + iy_2(a) = r_0e^{i\theta_0}$, il existe $r, \theta \in \mathscr{C}^1([a,+\infty[,\mathbb{R})$ tels que $y_1 = r\cos\theta, y_2 = r\sin\theta$ où $r = \sqrt{y_1^2+y_2^2}$ et $\forall x, \theta(x) = \theta_0 + \displaystyle\int_a^x \frac{w(t)}{r(t)^2}\mathrm{d}t$.

Démonstration. Posons $\varphi = y_1 + iy_2$. Par hypothèse, cette fonction ne s'annule pas donc $\psi : x \mapsto \displaystyle\int_a^x \frac{\varphi'(t)}{\varphi(t)}\mathrm{d}t + \ln r_0 + i\theta_0$ est bien définie et $\mathscr{C}^1$ sur $[a,+\infty[$.

De plus, un calcul rapide montre que $\left(\varphi e^{-\psi}\right)' = 0$ donc

$$\forall x, \varphi(x) = e^{\psi(x)}(\varphi(a)e^{-\psi(a)}) = e^{\psi(x)}(r_0e^{i\theta_0} \times r_0^{-1}e^{-i\theta_0} = e^{\psi(x)}.$$

Donc

$$\begin{aligned}\varphi(x) &= r_0e^{i\theta_0}\exp\left(\int_a^x \frac{\varphi'(t)}{\varphi(t)}\mathrm{d}t\right) = r_0e^{i\theta_0}\exp\left(\int_a^x \frac{(y_1'+iy_2')(y_1-iy_2)(t)}{r^2(t)}\mathrm{d}t\right)\\ &= r_0e^{i\theta_0}\exp\left(i\int_a^x \frac{w(t)}{r^2(t)}\mathrm{d}t + \int_a^x \frac{(y_1'y_1+y_2'y_2)(t)}{r^2(t)}\mathrm{d}t\right)\\ &= r_0e^{i\theta_0}\exp\left(i\int_a^x \frac{w(t)}{r^2(t)}\mathrm{d}t + \ln r(x) - \ln r(a)\right) = r(x)e^{i\theta_0}\exp\left(i\int_a^x \frac{w(t)}{r^2(t)}\mathrm{d}t\right)\end{aligned}$$

car $(r^2)' = y_1'y_1 + y_2'y_2$. Donc $\varphi(x) = r(x)e^{i\theta(x)}$ où $\theta(x) = \theta_0 + \displaystyle\int_a^x \frac{w(t)}{r^2(t)}\mathrm{d}t$. □

Démonstration (du théorème)**. Étape 1 : changement de variable** : Posons $\tau(x) = \displaystyle\int_a^x \sqrt{q(u)}\mathrm{d}u$. La fonction τ est de classe $\mathscr{C}^1$ sur $[a,+\infty[$, $\forall x \geqslant a, \tau'(x) = \sqrt{q(x)} > 0$ et $\tau(x) \xrightarrow[x\to+\infty]{} +\infty$, de sorte que τ est une bijection de classe $\mathscr{C}^1$ de $[a,+\infty[$ sur $[0,+\infty[$.

Posons $Y = y \circ \tau^{-1}$. On a $\forall x > 0, y'(x) = Y'(\tau(x))\sqrt{q(x)}$ et

$$y''(x) = Y''(\tau(x))q(x) + Y'(\tau(x)) \times \frac{q'(x)}{2\sqrt{q(x)}}.$$

Ainsi :

$$0 = y''(x) + q(x)y(x) = q(x)Y''(\tau(x)) + \frac{q'(x)}{2\sqrt{q(x)}}Y'(\tau(x)) + q(x)Y(\tau(x))$$

Posons pour $t \geqslant 0$, $\varphi(t) = \dfrac{q'(\tau^{-1}(t))}{2q^{3/2}(\tau^{-1}(t))}$. La fonction Y est donc solution de (E') : $Y'' + \varphi Y' + Y = 0$

Étape 2 : utilisons le lemme pour écrire $Y = r\sin\theta, Y' = r\cos\theta$. En effet, Y et Y' n'ont pas de zéro commun, car sinon, selon le théorème de Cauchy-Lipschitz , Y serait nulle. Donc

$$Y' = r'\sin\theta + r\theta'\cos\theta = r\cos\theta \tag{2.8}$$

et d'autre part

$$Y'' = r'\cos\theta - r\theta'\sin\theta = -\varphi r\cos\theta - r\sin\theta. \tag{2.9}$$

L'opération (2.8) $\times \cos\theta$ + (2.9) $\times (-\sin\theta)$ donne $r\theta' = r + \varphi r\cos\theta\sin\theta$, d'où $\theta' = 1 + \varphi\cos\theta\sin\theta$. En particulier, comme $\cos\theta\sin\theta = \dfrac{1}{2}\sin(2\theta)$, $|\theta'(t) - 1| \leqslant \dfrac{1}{2}|\varphi(t)|$.

Étape 3 : étude asymptotique. Puisque $\varphi(t) \xrightarrow[t\to+\infty]{} 0$ par hypothèse, θ' tend vers 1 à l'infini. Par intégration des équivalents, on a $\theta(t) \backsim t$.

Notons $M(t)$ le nombre de zéros de Y sur $[0,t]$, montrons que $M(t) \backsim \dfrac{t}{\pi}$ quand t tend vers $+\infty$.

Montrons d'abord par l'absurde que $M(t) < \infty$ pour tout t. Si il existait t_0 tel que $M(t_0) = \infty$, alors l'ensemble des zéros de Y dans $[0,t_0]$ aurait un point d'accumulation u. Soit $(u_n)_n$ suite de zéros de Y tendant vers u. Alors

$$0 = \frac{Y(u_n) - Y(u)}{u_n - u} \xrightarrow[n\to+\infty]{} Y'(u),$$

ce qui contredit l'absence de zéro commun de Y et Y'. Donc pour tout t, $M(t) < \infty$.

Fixons $t_0 \geqslant 0$ tel que $\theta'(t) > 0$ sur $[t_0, +\infty[$. Alors

$$M(t) \backsim_{t\to+\infty} \text{Card}\,\{u \in [t_0,t] : \sin\theta(u) = 0\} = \text{Card}\,\{v \in [\theta(t_0),\theta(t)] : \sin v = 0\}$$

puisque θ est un $\mathscr{C}^1$-difféomorphisme de $[t_0,t]$ sur $[\theta(t_0),\theta(t)]$. Donc

$$M(t) \backsim_{t\to+\infty} \text{Card}\,\{k \in \mathbb{Z} : \theta(t_0) \leqslant k\pi \leqslant \theta(t)\} = \mathrm{E}\left(\frac{\theta(t)}{\pi}\right) - \mathrm{E}\left(\frac{\theta(t_0)}{\pi}\right),$$

de sorte que $M(t) \backsim_{t\to+\infty} \dfrac{\theta(t)}{\pi} \backsim \dfrac{t}{\pi}$.

Or, on se convainc sans mal que $N(x) = M(\tau(x))$ donc

$$N(x) \backsim_{x\to+\infty} \frac{\tau(x)}{\pi} = \frac{1}{\pi}\int_a^x \sqrt{q(u)}\mathrm{d}u.$$

□

Remarque.
- Le jour de l'oral, faire le lemme technique rapidement ou l'admettre pour avoir assez de temps pour la suite.
- Si la condition $q' = o(q^3/2)$ n'est pas vérifiée, le résultat n'est plus vrai. Par exemple, si $q(x) = \frac{1}{4x^2}$, $q'(x) = -\frac{1}{2x^3}$, et $y'' + \frac{1}{4x^2}y = 0$ admet pour solution générale $\sqrt{x}(a + b\ln(x)), a, b \in \mathbb{R}$ – puisque $\sqrt{x}$ et $\sqrt{x}\ln(x)$ sont solutions – qui s'annule au plus une fois sur $\mathbb{R}_+$.

Référence : QUEFFÉLEC et ZUILY 2013 p. 405.

Points extrémaux de la boule unité de $\mathscr{L}(E)$

Leçons : 160, 161, 181

Définition 70

Un point extrémal de X est un point qui n'appartient à aucun segment $[AB]$, où A et B sont des points de X.

Théorème 71

Soit E espace euclidien. Les points extrémaux de la boule unité de $\mathscr{L}(E)$ sont les éléments de $O(E)$

Lemme 72

Si X est convexe, un point extrémal de X est un point qui ne peut s'écrire comme milieu de deux points distincts de X.

Démonstration. Supposons que z vérifie une telle propriété et que $tx_1 + (1-t)x_2 = z$ où $x_i \in X \setminus \{z\}$. Quitte à échanger x_1 et x_2, on peut supposer $t \leqslant \frac{1}{2}$ et alors $z = \frac{x_2}{2} + \frac{2tx_1 + (1-2t)x_2}{2}$ ce qui est absurde. □

Démonstration (du théorème)**. Étape 1 : tout $u \in O(E)$ est extrémal** : Comme u est une isométrie, $\|u\| = 1$. Supposons que $u = \frac{v+w}{2}$ où $v, w \in B$. Soit $x \in E$ de norme 1. Alors

$$1 = \|u(x)\| = \|x\| \leqslant \frac{1}{2}(\|v(x)\| + \|w(x)\|) \leqslant \frac{1}{2}(\|v\| + \|w\|) \leqslant 1,$$

donc toutes les inégalités sont des égalités. En particulier, on a un cas d'égalité dans l'inégalité triangulaire pour une norme euclidienne donc il existe $\lambda \geqslant 0$ tel que $v(x) = \lambda w(x)$. Or, comme $v, w \in B$, on a $\|v(x)\| \leqslant \|x\| = 1$ et $\|w(x)\| \leqslant 1$. De plus, $\frac{1}{2}(\|v(x)\| + \|w(x)\|) = 1$ donc $\|v(x)\| = \|w(x)\| = 1$. Ainsi, $\lambda = 1$ et $v(x) = w(x)$.

Étape 2 : les éléments de $B \setminus O(E)$ ne sont pas extrémaux : soit u un tel élément, soit $\mathscr{B}$ une base orthonormée de E et A la matrice de u dans cette base. Par décomposition polaire, on peut trouver $O \in O_n(\mathbb{R})$, $S \in \mathscr{S}_n^{++}(\mathbb{R})$ tels que $A = OS$.

En outre, par le théorème spectral, il existe $P \in O_n(\mathbb{R})$ tel que $S = {}^tPDP$ où $D = \mathrm{Diag}(d_1, \dots, d_n)$ avec $0 < d_1 \leqslant \cdots \leqslant d_n$. Comme A et O^{-1} sont éléments de B, S l'est aussi, donc $\forall k \in [\![1, n]\!], d_k \leqslant 1$. En effet, si $\mathscr{B}' = (e'_1, \dots, e'_n)$ est une base de diagonalisation de de S et $x = \sum a_i e'_i$, alors

$$\|S(x)\|^2 = \sum d_i^2 |a_i|^2 \leqslant (\max_i(d_i))^2 \|x\|.$$

A n'est pas orthogonale donc il existe $k \in [\![1, n]\!]$ tel que $d_k < 1$. Pour simplifier, on prend $k = 1$. Il existe alors $\alpha, \beta \in [-1, 1]$ tels que $d_1 = \frac{\alpha + \beta}{2}$. Introduisons $D' = \mathrm{Diag}(\alpha, d_2, \dots, d_n)$ et $D'' = \mathrm{Diag}(\beta, d_2, \dots, d_n)$. On a alors $A = \frac{O\,{}^tPD'P + O\,{}^tPD''P}{2}$.

Enfin, si $\|X\| = 1$,

$$\|O\,{}^tPD'PX\|^2 \overset{P, O \in O_n}{=} {}^tX\,{}^tPD'P\,{}^tOO\,{}^tPD'PX = {}^tX\,{}^tP(D')^2PX = {}^t(PX)(D')^2PX \leqslant 1$$

car $\|PX\| = \|X\| = 1$ et $(D')^2$ a des coefficients diagonaux entre 0 et 1. Donc $O^tPD'P$ et $O^tPD''P$ sont deux éléments distincts de B, de sorte que u n'est pas extrémal.

□

Remarque. Selon le théorème de Krein-Milman (ou Minkowski), la boule unité de $\mathscr{L}(E)$ est donc l'enveloppe convexe de $O(E)$.

Référence : FRANCINOU, GIANELLA et NICOLAS 2008, p. 130.

Polynômes irréductibles sur $\mathbb{F}_q[X]$

Leçons : 123, 125, 141, 190

Théorème 73

On note $\mathscr{P}_q(d)$ l'ensemble des polynômes irréductibles de degré d sur $\mathbb{F}_q$. Alors si $n \in \mathbb{N}^*$,

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

Démonstration. Soit $P \in \mathscr{P}_q(d)$. Alors $K = \mathbb{F}_q[X]/(P)$ est un corps de cardinal q^d donc pour tout $x \in K$, on a $x^{q^d} = x$. Mais si $n = dk, k \in \mathbb{N}$, alors

$$x^{q^n} = x^{q^{dk}} = \underbrace{\left(\dots(x^{q^d})\dots\right)^{q^d}}_{k \text{ fois}} = x.$$

par une récurrence immédiate. Donc en particulier avec $x = \overline{X}$, on obtient $P \mid X^{q^n} - X$. Ainsi, par le lemme de Gauss, $\prod_{d|n} \prod_{P \in \mathscr{P}_q(d)} P(X) \mid X^{q^n} - X$.

Soit P un facteur irréductible de $X^{q^n} - X$ dans $\mathbb{F}_q[X]$. Comme $\mathbb{F}_{q^n}$ est le corps de décomposition de $X^{q^n} - X$, P est scindé sur $\mathbb{F}_{q^n}$. Donc si x est une racine de P dans $\mathbb{F}_{q^n}$, selon le théorème de la base télescopique, $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q]$. Mais comme P est irréductible, P est le polynôme minimal de x sur $\mathbb{F}_q$ donc $[\mathbb{F}_q(x) : \mathbb{F}_q] = d$, de sorte que $d \mid n$.

Enfin, $X^{q^n} - X$ est à facteurs simples : si $X^{q^n} - X$ avait un facteur double, il aurait une racine double dans son corps de décomposition. Mais $(X^{q^n} - X)' = -1$ dans toute extension de $\mathbb{F}_q$ (à cause de la caractéristique de $\mathbb{F}_q$) donc $X^{q^n} - X$ est à racines simples dans son corps de décomposition [7]. □

Proposition 74

Soit $g : \mathbb{N}^* \to \mathbb{C}$, alors si $G(n) = \sum_{d|n} g(d)$, on a pour tout $n \in \mathbb{N}^*$, $g(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$, où μ est la fonction de Möbius.

Démonstration. On remarque que $d \mid n$ et $d' \mid \frac{n}{d}$ si et seulement si $dd' \mid n$.

$$\sum_{d|n} \mu(d) G\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{d' \mid \frac{n}{d}} g(d') = \sum_{dd' \mid n} \mu(d) g(d') = \sum_{d'|n} g(d') \sum_{d \mid \frac{n}{d'}} \mu(d).$$

Or, si $m \neq 1$, $\sum_{d|m} \mu(d) = 0$ [8] donc $\sum_{d|n} \mu(d) G\left(\frac{n}{d}\right) = g(n)$. □

7. Une racine double de P est une racine de P' dans un corps de caractéristique quelconque, mais la réciproque n'est vraie qu'en caractéristique nulle

8. en effet, si $m = \prod_{i=1}^{r} p_i^{\alpha_i}$, $\sum_{d|m} \mu(d) = \sum_{d|m} \mu(d) = \sum_{\beta \leqslant \alpha} \mu(p_1^{\beta_1} \dots p_r^{\beta_r}) = \sum_{\beta \in \{0,1\}^r} (-1)^{|\beta|} = \sum_{k=0}^{r} \binom{r}{k} (-1)^k$ (choix de k 1 parmi r termes) donc $\sum_{d|m} \mu(d) = 0$

Corollaire 75

Si $I(q,d) = \text{Card}\mathscr{P}_q(d)$*, alors* $\forall n \in \mathbb{N}^*, I(q,n) = \dfrac{1}{n}\sum_{d|n}\mu\left(\dfrac{n}{d}\right)q^d$ *et* $I(q,n) \sim_{n\to+\infty} \dfrac{q^n}{n}$.

Démonstration. La première formule est une conséquence immédiate de l'inversion de Möbius. Pour la deuxième, posons $r_n = \sum_{d|n, d<n} \mu\left(\dfrac{n}{d}\right)q^d$. Alors

$$|r_n| \leqslant \sum_{\substack{d|n \\ d\neq n}} q^d \leqslant \sum_{d=0}^{E\left(\frac{n}{2}\right)} q^d = \frac{q^{E\left(\frac{n}{2}\right)+1}-1}{q-1} \xrightarrow[n\to+\infty]{} \frac{1}{1-q}$$

donc en particulier, $r_n = o(q^n)$.

Ainsi, comme $I(n,q) = \dfrac{q^n + r_n}{n}$, on a $I(n,q) \sim_{n\to+\infty} \dfrac{q^n}{n}$. □

Référence : TAUVEL 2008, p. 121.

Processus de Poisson

Leçons : 263, 264

Soit $(\Omega, \mathscr{F}, \mathbb{P})$ un espace probabilisé.

Définition 76

Un processus de comptage est une suite de variables aléatoires réelles $(N(t))_{t\geqslant 0}$ telles que

1. $N(0) = 0$.
2. $\forall t \geqslant 0, N(t) \in \mathbb{N}^*$.
3. $t \mapsto N(t)$ *est croissante.*

Du point de vue de la modélisation, $\forall 0 \leqslant a \leqslant b$, $N(b) - N(a)$ représente le nombre de « tops » se produisant dans l'intervalle de temps $[a, b[$.

Définition 77

Un processus de Poisson de densité $\lambda > 0$ est un processus de comptage $(N(t))_{t\geqslant 0}$ tel que :

1. *Le processus est à accroissement indépendants : $\forall t_0 \leqslant t_1 < \cdots < t_k$, les variables aléatoires $N_{t_k} - N_{t_{k-1}}, \ldots, N_{t_1} - N_{t_0}$ sont indépendantes.*
2. *Pour tout $(s,t) \in \mathbb{R}_+^2$, $N(s+t) - N(s)$ suit la loi de Poisson de paramètre λt.*

Les processus de Poisson sont souvent utilisés pour modéliser des files d'attente, chaque top représentant l'appel d'un client au guichet.

Proposition 78

Un processus de Poisson est à accroissements stationnaires : soit $N_1, \ldots, N_k$ le nombre de tops se produisant dans les intervalles $I_1, \ldots, I_k$; alors si $\tau \geqslant 0$, et $N'_1, \ldots, N'_k$ est le nombre de tops se produisant dans les intervalles translatés de τ $I'_1 + \tau, \ldots, I'_k$, $(N'_1, \ldots, N'_k)$ et $(N_1, \ldots, N_k)$ ont la même loi.

Proposition 79

Un processus de Poisson est localement continu : $\lim\limits_{h\to 0^+} \mathbb{P}(N(t+h) - N(t) \geqslant 1) = 0$.

Le but du développement est d'étudier le temps d'attente entre deux tops :

Théorème 80

Soit $S_n = \inf\{t \geqslant 0, N(t) \geqslant n\}$ et $T_k = S_k - S_{k-1}$ pour $k \geqslant 1$. Alors

1. *$(T_n)_n$ est une suite de variables aléatoires i.i.d. de loi $\mathscr{E}(\lambda)$.*
2. *$S_n = T_1 + \cdots + T_n$ suit la loi $\Gamma(n, \lambda)$ de densité*

$$f_{S_n}(s) = \begin{cases} \dfrac{\lambda}{(n-1)!} e^{-\lambda s} (\lambda s)^{n-1} & \text{si} \quad s \geqslant 0 \\ 0 \quad \text{sinon} \end{cases}.$$

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

Étape 1 : Changement de variable : supposons que le vecteur aléatoire $(S_1,\dots,S_n)$ soit à densité, de densité φ. Soit $f:\mathbb{R}^n\to\mathbb{R}$ continue bornée. Alors comme $S_n\geqslant\dots,\geqslant S_1$, par un changement de variable $s_k=t_1+\cdots+t_k$ de jacobien 1 (la matrice jacobienne est triangulaire), on a

$$\begin{aligned}\mathbb{E}[f(T_1,\dots,T_n)] &= \mathbb{E}[\mathbb{1}_{S_n\geqslant\dots\geqslant S_1} f(S_1,\dots,S_n-S_{n-1})]\\ &= \int_{0\leqslant s_1\leqslant\dots\leqslant s_n} f(s_1,\dots,s_n-s_{n-1})\varphi(s_1,\dots,s_n)\mathrm{d}s_1\dots\mathrm{d}s_n\\ &= \int_{t_1,\dots,t_n\geqslant 0} f(t_1,\dots,t_n)\varphi(t_1,\dots,t_1+\cdots+t_n)\mathrm{d}t_1\dots\mathrm{d}t_n.\end{aligned}$$

Donc $\psi:(t_1,\dots,t_n)\mapsto\varphi(t_1,t_1+t_2,\dots,t_1+\cdots+t_n)$ est la densité de $(T_1,\dots,T_n)$.

Étape 2 : Calcul de la densité de $(S_1,\dots,S_n)$:

Soit A_n l'évènement : $S_1\in[s_1,s_1+h_1[,\dots,S_n\in[s_n,s_n+h_n[$ où $0<s_1<s_1+h_1<s_2<\cdots<s_n+h_n$. Alors A_n est la réunion des évènements :

- zéro top dans $[0,s_1[$ et *exactement* un top dans $[s_1,s_1+h_1[$
- zéro top dans $[s_1+h_1,s_2[$ et exactement un top dans $[s_2,s_2+h_2[$
- $\vdots$
- zéro top dans $[s_{n-1}+h_{n-1},s_n[$ et *au moins* un top dans $[s_n,s_n+h_n[$.

Or, le processus étant à accroissements indépendants, les variables aléatoires « nombre de tops » dans des intervalles disjoints sont indépendantes de sorte que

$$\begin{aligned}&\mathbb{P}(A_n)=\mathbb{P}(N(s_1)=0)\times\mathbb{P}(N(s_1+h_1)-N(s_1)=1)\times\mathbb{P}(N(s_2)-N(s_1+h_1)=0)\times\\ &\mathbb{P}(N(s_2+h_2)-N(s_2)=1)\times\cdots\times\mathbb{P}(N(s_n)-N(s_{n-1}+h_{n-1})=0)\times\mathbb{P}(N(s_n+h_n)-N(s_n)\geqslant 1)\end{aligned}$$

donc

$$\begin{aligned}\mathbb{P}(A_n) &= e^{-\lambda s_1}e^{-\lambda h_1}(\lambda h_1)e^{-\lambda(s_2-s_1-h_1)}e^{-\lambda h_2}(\lambda h_2)\dots e^{-\lambda(s_n-s_{n-1}-h_{n-1})}(1-e^{-\lambda h_n})\\ &= e^{-\lambda s_n}\lambda^{n-1}h_1\dots h_{n-1}(1-e^{-\lambda h_n}).\end{aligned}$$

Pour conclure, il suffit de remarquer que

$$\mathbb{P}(A_n)=\int_{\xi_1=s_1}^{s_1+h_1}\dots\int_{\xi_n=s_n}^{s_n+h_n}\mathbb{1}_{0\leqslant\xi_1\leqslant\dots\leqslant\xi_n}\lambda^n e^{-\lambda\xi_n}\mathrm{d}\xi_1\dots\mathrm{d}\xi_n,$$

ceci valant pour tous les pavés $[s_1,s_1+h_1[\times\cdots\times[s_n+h_n[$, qui constituent une classe stable par intersection engendrant $\mathscr{B}(\mathbb{R}^n)$ donc $(S_1,\dots,S_n)$ a pour densité $\mathbb{1}_{\xi_1\leqslant\dots\leqslant x_n}\lambda^n e^{-\lambda\xi_n}$.

Conclusion : selon la première étape, la densité de $(T_1,\dots,T_n)$ est

$$(t_1,\dots,t_n)\mapsto\lambda^n e^{-\lambda t_1}\dots e^{-\lambda t_n}\mathbb{1}_{\mathbb{R}_+^n}(t_1,\dots,t_n).$$

En calculant les densités marginales, on constate immédiatement que $f_{(T_1,\dots,T_n)}(t_1,\dots,t_n)=f_{T_1}(t_1)\dots f_{T_n}(t_n)$; en d'autres termes, $T_1,\dots,T_n$ sont indépendantes. La loi de S_n est donc $\Gamma(n,\lambda)$ en vertu du lemme ci-dessous. □

Lemme 81

Si $T_1,\dots,T_n$ sont n variables aléatoires i.i.d de loi $\mathscr{E}(\lambda)$, alors $S=T_1+\cdots+T_n$ suit la loi $\Gamma(n,\lambda)$

Démonstration. Calculons la transformée de Laplace d'une variable aléatoire V suivant la loi $\Gamma(n,\lambda)$, en rappelant que la transformée de Laplace caractérise la loi :

$$L_V(u) = \mathbb{E}[e^{uS}] = \frac{\lambda}{\Gamma(n)} \int_0^\infty e^{ux} e^{-\lambda x} (\lambda x)^{n-1} \mathrm{d}x = \frac{\lambda}{\Gamma(n)} \int_0^\infty e^{-x(\lambda-u)} (\lambda x)^{n-1} \mathrm{d}x$$

bien définie pour $\lambda - u > 0$ donc en posant $y = x(\lambda - u)$, on a

$$L_V(u) = \frac{\lambda}{\Gamma(n)} \int_0^\infty e^{-y} \left(\frac{\lambda y}{\lambda - u}\right)^{n-1} \frac{\mathrm{d}y}{\lambda - u} = \frac{1}{\Gamma(n)} \left(\frac{\lambda}{\lambda - u}\right)^n \int_0^\infty e^{-y} y^{n-1} \mathrm{d}y = \left(\frac{\lambda}{\lambda - u}\right)^n.$$

Or, par le même changement de variable, si $T \sim \mathscr{E}(\lambda)$,

$$L_T(u) = \int_0^{+\infty} e^{ux} \lambda e^{-\lambda x} \mathrm{d}x = \frac{\lambda}{\lambda - u} \int_0^\infty e^{-y} \mathrm{d}y = \frac{\lambda}{\lambda - u}$$

donc comme la transformée de Laplace d'une somme de variable aléatoires indépendantes est le produit de leurs transformées de Laplace, on a le résultat. □

Remarque.
- On peut aussi parler du paradoxe de l'inspection, ou paradoxe de l'autobus, c'est dans le Foata–Fuchs juste après.
- Les deux premières propositions sont indépendantes du développement proprement dit.

Références : FOATA et FUCHS 2004, pp. 28-31 et FOATA et FUCHS 2003, p. 148

Prolongement de Γ

Leçons : 207, 239, 241, 245

Références : QUEFFÉLEC et ZUILY 2013 et BECK, MALICK et PEYRÉ 2005, p. 82

Quelques ordres moyens

Leçons : *223*, 224, 230

Définition 82

Un ordre moyen de $f : \mathbb{N} \to \mathbb{R}$ est une fonction $g : \mathbb{R} \to \mathbb{R}$ telle que

$$\sum_{1 \leqslant n \leqslant x} f(n) \sim_{x \to +\infty} \sum_{1 \leqslant n \leqslant x} g(n).$$

Proposition 83

Un ordre moyen de $\sigma : n \mapsto \sum_{d|n} d$ est $x \mapsto \frac{\pi^2}{12}x$ et $\sum_{n \leqslant x} \sigma(n) = \frac{\pi^2}{12}x^2 + O(x \ln x)$.

Démonstration. Si $x \geqslant 1$, on a

$$\sum_{n \leqslant x} \sigma(n) = \sum_{n=1}^{E(x)} \sum_{d|n} d = \sum_{\substack{(d,m) \in [\![1, E(x)]\!] \\ dm \leqslant x}} d = \sum_{m=1}^{E(x)} \sum_{d=1}^{E\left(\frac{x}{m}\right)} d = \sum_{m=1}^{E(x)} \frac{1}{2} E\left(\frac{x}{m}\right)\left(E\left(\frac{x}{m}\right)+1\right).$$

Or, $E\left(\frac{x}{m}\right)\left(E\left(\frac{x}{m}\right)+1\right) = \left(\frac{x}{m} - \left\{\frac{x}{m}\right\}\right)\left(\frac{x}{m} - \left\{\frac{x}{m}\right\} + 1\right) = \left(\frac{x}{m}\right)^2 + \frac{x}{m} O_u(1) + O_u(1)$.[9]
Donc en sommant, on a

$$\sum_{n \leqslant x} \sigma(n) = \sum_{m=1}^{E(x)} \left(\frac{x}{m}\right)^2 + O(1) \sum_{m=1}^{E(x)} \frac{x}{m} + O(x).$$

Or, $\sum_{m=1}^{+\infty} \frac{1}{m^2} = \frac{\pi^2}{6}$ et si $m \geqslant 2$, par comparaison série-intégrale,

$$\int_m^{m+1} \frac{\mathrm{d}t}{t^2} \leqslant \frac{1}{m^2} \leqslant \int_{m-1}^{m} \frac{\mathrm{d}t}{t^2}$$

soit, en sommant pour $m \in [\![E(x)+1, +\infty[\![$,

$$\frac{1}{E(x)+1} = \int_{E(x)+1}^{+\infty} \frac{\mathrm{d}t}{t^2} \leqslant \frac{1}{m^2} \leqslant \int_{E(x)}^{+\infty} \frac{\mathrm{d}t}{t^2} = \frac{1}{E(x)}.$$

Donc $\sum_{m>x} \frac{1}{m^2} \sim_{m \to +\infty} \frac{1}{x}$, en particulier, $\sum_{m \leqslant x} \frac{1}{m^2} = \frac{\pi^2}{6} + O\left(\frac{1}{x}\right)$.

Par ailleurs, le même procédé de comparaison série-intégrale donne $\sum_{m \leqslant x} \frac{1}{m} = \ln(x) + O(1)$ de sorte que

$$\sum_{n \leqslant x} \sigma(n) = \frac{\pi^2}{6}x^2 + O(x) + O(x \ln(x)) = \frac{\pi^2}{6}x^2 + O(x \ln(x)),$$

ce qui est le résultat voulu. □

9. O_u désignant une notation O uniforme par rapport à x

Proposition 84

Un ordre moyen de l'indicatrice d'Euler φ est $x \mapsto \frac{3}{\pi^2}x$ et $\sum_{1\leqslant n\leqslant} \varphi(n) = \frac{3}{\pi^2}x^2 + O(x\ln x)$.

Démonstration. Selon la formule d'inversion de Möbius, $\varphi(n) = \sum_{d|n}\mu(d)\frac{n}{d} = \sum_{md=n}\mu(d)m$. Donc

$$\begin{aligned}\sum_{n\leqslant x}\varphi(n) &= \sum_{n\leqslant x}\sum_{md=n}\mu(d)m = \sum_{d\leqslant x}\mu(d)\sum_{m=1}^{E\left(\frac{x}{d}\right)} m \\ &= \sum_{d\leqslant x}\mu(d)\frac{1}{2}E\left(\frac{x}{d}\right)\left(E\left(\frac{x}{d}\right)+1\right) = \frac{x^2}{2}\sum_{d\leqslant x}\frac{\mu(d)}{d^2} + O(x\ln x),\end{aligned}$$

la dernière égalité découlant de la démonstration précédente et du fait que $\mu(d) = O_u(1)$.

Or, si $N \in \mathbb{N}^*$,

$$\left(\sum_{d=1}^{N}\frac{\mu(d)}{d^2}\right)\left(\sum_{k=1}^{N}\frac{1}{k^2}\right) = \sum_{d=1}^{N}\sum_{k=1}^{N}\frac{\mu(d)}{(dk)^2} \overset{m=dk}{=} \sum_{m=1}^{N^2}\frac{1}{m^2}\sum_{d|m}\mu(d) = 1$$

puisque $\sum_{d|m}\mu(d) = 1$ sauf si $m = 1$.

Donc en faisant tendre N vers $+\infty$, on a $\sum_{d=1}^{+\infty}\frac{\mu(d)}{d^2} = \frac{6}{\pi^2}$. Ainsi,

$$\sum_{n\leqslant x}\varphi(n) = \frac{3x^2}{\pi^2} + O(x\ln x).$$

□

Référence : TENENBAUM 2015, pp. 46-47, largement complété par Adrien Laurent.

Sous-groupes distingués et table de caractères

Leçons : 103, *104*, 107

Théorème 85

Soit G un groupe fini et $\chi_1, \dots, \chi_m$ ses caractères irréductibles. Alors les sous-groupes distingués de G sont les $\bigcap_{j\in J} \ker \chi_j$ quand $J \subset [\![1, m]\!]$.

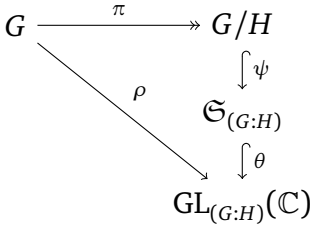
Démonstration. Étape 1 : le noyau d'un caractère est le noyau de la représentation associée.

En effet, soit (V, ρ) représentation de G de caractère χ. Comme G est fini, on sait que $\rho(g)$ est diagonalisable de valeurs propres $\lambda_1, \dots, \lambda_r$ où $r = \dim V$ de module 1 (ce sont des racines du polynôme annulateur $X^{|G|} - 1$ donc des racines de l'unité).

Par suite, $|\chi(g)| = \left|\sum_{i=1}^{r} \lambda_i\right| \overset{INT}{\leqslant} \sum_{i=1}^{r} |\lambda_i| = \dim V = \chi(e)$ avec égalité si et seulement si il y a égalité dans l'égalité triangulaire, c'est-à-dire si les λ_i sont deux à deux colinéaires de même sens, donc si elles sont égales puisqu'elles sont toutes de même module. Donc $\chi(g) = \chi(e) \Leftrightarrow \rho(g) = \mathrm{id} \Leftrightarrow g \in \ker \rho$.

Étape 2 : construction d'une représentation associée à H.

Soit H un sous-groupe distingué de G et $\pi : G \mapsto G/H$ le morphisme (surjectif) quotient. On sait selon le théorème de Cayley qu'il existe un morphisme injectif $\psi : G/H \to \mathfrak{S}_{(G:H)}$ et de plus la représentation régulière de $\mathfrak{S}_{(G:H)}$ fournit un morphisme injectif θ de $\mathfrak{S}_{(G:H)}$ dans $\mathrm{GL}_{(G:H)}(\mathbb{C})$. Ainsi par composition, on obtient un morphisme $\rho : G \to \mathrm{GL}_{(G:H)}(\mathbb{C})$ de noyau H.



Selon l'étape 1, on a donc $H = \ker \rho = \ker \chi$ où χ est le caractère de ρ.

Étape 3 : décomposons la représentation (V, ρ) précédemment obtenue en une somme directe de représentations irréductibles $V = \bigoplus_{i=1}^{r} V_i$, où χ_i est le caractère de V_i.

Selon l'étape 1, si $g \in G$, $g \in \ker \rho \Leftrightarrow \chi(g) = \chi(e) = \dim V = \sum_{i=1}^{r} \chi_i(g)$.

Or,

$$\left|\sum_{i=1}^{r} \chi_i(g)\right| \leqslant \sum_{i=1}^{r} |\chi_i(g)| \leqslant \sum_{i=1}^{r} |\chi_i(e)| = \sum_{i=1}^{r} |\chi_i(e)| = \dim V$$

donc $\sum_{i=1}^{r} |\chi_i(g)| = \sum_{i=1}^{r} |\chi_i(e)|$ avec pour tout i, l'inégalité $|\chi_i(g)| \leqslant |\chi_i(e)|$ de sorte que $\forall i \in [\![1, r]\!]$, $g \in \ker \chi_i$. Ainsi, $\ker \rho = H = \bigcap_{i=1}^{r} \ker \chi_i$.

□

Proposition 86

Les sous-groupes distingués du groupe diédral $D_6 = \left\langle r,s \mid r^5 = e, s^2 = e, srs = r^{-1} \right\rangle$ *sont* $\{e\}, \langle s\rangle, \langle r^2, s\rangle, \langle r^2, sr\rangle, \langle r^2\rangle, \langle r^3\rangle$ *et* D_6

Démonstration. Tout d'abord, on sait que D_6 a 6 classes de conjugaison donc il y a 6 caractères irréductibles.

- Un caractère χ de degré 1 est déterminé par $\chi(r)$ et $\chi(s)$. Comme $1 = \chi(s^2) = \chi(s)^2$, on a $\chi(s) \in \{\pm 1\}$. De plus, rs est une symétrie donc $\chi(rs) = \chi(r)\chi(s) \in \{\pm 1\}$ d'où $\chi(r) \in \{\pm 1\}$. Ceci fournit 4 caractères linéaires de D_6 (il n'est pas difficile de se convaincre que ce sont effectivement des morphismes de groupes de D_6 dans $\mathbb{C}^*$).
- Selon la formule de Burnside, si χ_1 et χ_2 sont les deux caractères restants de degrés d_1 et d_2, alors $4 \times 1^2 + d_1^2 + d_2^2 = |D_6| = 12$ donc $d_1 = d_2 = 1$.
  Introduisons $\omega = e^{i\frac{\pi}{3}}$ et pour $h \in \{1,2\}$, $\rho_h : D_6 \to \mathrm{GL}_2(C)$ tel que $\rho_h(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $\rho_h(r) = \begin{pmatrix} \omega^h & 0 \\ 0 & \omega^{-h} \end{pmatrix}$. On a donc pour $k \in [\![0,5]\!]$, $\rho_h(sr^k) = \begin{pmatrix} 0 & \omega^{-hk} \\ \omega^{hk} & 0 \end{pmatrix}$ qui est de trace nulle.
  Ainsi, pour le produit scalaire $\langle \cdot, \cdot \rangle$ classique sur l'espace des fonctions centrales, on a

$$\begin{aligned} \langle \chi_h, \chi_h \rangle &= \frac{1}{12}\left(\sum_{k=0}^{5} (\omega^{hk} + \omega^{-hk})^2\right) = \frac{1}{12}\left(12 + \sum_{k=0}^{5} \omega^{2hk} + \omega^{-2hk}\right) \\ &= 1 + \frac{1}{12}\left(\frac{\omega^{12h}-1}{\omega^{2h}-1} + \frac{\omega^{-12h}-1}{\omega^{-2h}-1}\right) = 1, \end{aligned}$$

  ce qui prouve que χ_h est un caractère irréductible [10].
- Ceci nous fournit la « table de caractères » suivante (qui n'en est pas une puisqu'on ne donne pas les valeurs sur les classes de conjugaison), à laquelle on adjoint la liste des noyaux des caractères.

	ψ_1	ψ_2	ψ_3	ψ_4	χ_1	χ_2
r^k	1	$(-1)^k$	$(-1)^k$	1	$2\cos\left(\frac{k\pi}{3}\right)$	$2\cos\left(\frac{2k\pi}{3}\right)$
sr^k	1	$(-1)^k$	$(-1)^{k+1}$	-1	0	0
Noyau	D_6	$\langle r^2, s\rangle$	$\langle r^2, sr\rangle$	$\langle s\rangle$	$\{e\}$	$\langle r^3\rangle$

  On constate à l'œil nu que les intersections des 6 noyaux de caractères irréductibles ne fournissent pas d'autres sous-groupes de D_6 qu'eux-mêmes et $\langle r^2\rangle = \ker\psi_2 \cap \ker\psi_3$, donc on a bien établi la liste voulue.

□

Références : ULMER 2012, p. 158 pour le théorème et PEYRÉ 2004, p. 227 pour la table de caractères.

10. Variante : une sous-représentation de degré 1 de ρ_h serait une droite stable ; or une droite stable par $\rho_h(r)$ est soit l'axe (Ox) soit l'axe (Oy), lesquels ne sont pas stables par la symétrie $\rho_h(r)$.

Surjectivité de l'exponentielle

Leçons : 153, 156, 204, *214*

Théorème 87

Soit $A \in \mathcal{M}_n(\mathbb{C})$. Alors, $\exp(\mathbb{C}[A]) = \mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C})$. *En particulier,* $\exp : \mathcal{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ *est surjective et un antécédent de $A \in \mathrm{GL}_n(\mathbb{C})$ est un polynôme (complexe) en A.*

Démonstration. Étape 1 : quelques résultats préliminaires

- On commence par observer l'égalité $\mathbb{C}[A]^\times = \mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C})$ où $\mathbb{C}[A]^\times$ est le groupe des inversibles de $\mathbb{C}[A]$. Seule l'inclusion $\supset$ pose question : il s'agit de voir que l'inverse d'une matrice M est un polynôme en M (en effet le coefficient constant de son polynôme minimal est non nul : $\mu_M = \alpha + XP$ et $M^{-1} = -P(M)/\alpha$). Ainsi, l'inverse d'un élément de $\mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C})$ reste dans $\mathbb{C}[A]$ (c'est un polynôme de polynôme en A)
- Pour tout $M \in \mathcal{M}_n(\mathbb{C})$, $\exp(M) \in \mathbb{C}[M]$: en effet, c'est une limite dans $\mathcal{M}_n(\mathbb{C})$ (pour la norme d'algèbre) d'éléments de $\mathbb{C}[M]$ qui est un sous-espace vectoriel de dimension finie donc fermé. En conséquence, $\exp : \mathbb{C}[A] \to \mathbb{C}[A]^\times$ est un morphisme de groupes.
- $\mathbb{C}[A]^\times = \mathbb{C}[A] \cap \det^{-1}(\mathbb{R}^*)$ est un ouvert de $\mathbb{C}[A]$. Il est aussi connexe par arcs (donc connexe) car si $M, N \in \mathbb{C}[A]^\times$, la fonction $z \in \mathbb{C} \mapsto \det(zM + (1-z)N)$ est polynomiale en z et non nulle donc admet un nombre fini de zéros. 0 et 1 ne sont pas des zéros de ce polynôme donc on peut construire une courbe $z(t) \in \mathbb{C}$ reliant 0 et 1 en évitant ces zéros [11]. Ainsi $t \in [0,1] \mapsto z(t)M + (1-z(t))N$ est une courbe tracée dans $\mathbb{C}[A]^\times$ reliant continûment N et M.

Étape 2 : exp **est localement un difféomorphisme**

Comme la différentielle de $\exp : \mathcal{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ en 0 est l'identité de $\mathcal{M}_n(\mathbb{C})$, on a aussi en restreignant $\exp : \mathbb{C}[A] \to \mathbb{C}[A]^\times$, que $d\exp(0) = id_{\mathbb{C}[A]}$.

En particulier cette différentielle est bijective et le théorème d'inversion locale assure l'existence de deux ouverts $\mathcal{U} \subset \mathbb{C}[A]$ et $\mathcal{V} \subset \mathbb{C}[A]^\times$ contenant respectivement 0 et Id tel que $\exp : \mathcal{U} \to \mathcal{V}$ soit un difféomorphisme. Comme exp est un morphisme de groupes, le résultat demeure au voisinage de chaque point $M \in \mathbb{C}[A]$: $\exp : M + \mathcal{U} \to \exp(M)\mathcal{V}$ est un difféomorphisme.

Étape 3 : un argument de connexité pour conclure.

L'étape 2 implique en fait que $\exp(\mathbb{C}[A])$ est un ouvert de $\mathbb{C}[A]^\times$. Mais c'est aussi un fermé en remarquant que $\mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A]) = \bigcup_{M \in \mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A])} M\exp(\mathbb{C}[A])$ (l'inclusion $\supset$ se prouve par contraposée). En vertu de la connexité de $\mathbb{C}[A]^\times$, on conclut que

$$\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times = \mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C}).$$

□

Corollaire 88

L'image par l'application exponentielle de $\mathcal{M}_n(\mathbb{R})$ est l'ensemble

$$\exp(\mathcal{M}_n(\mathbb{R})) = \{A^2,\ A \in \mathrm{GL}_n(\mathbb{R})\}.$$

11. On montre même que $\mathbb{R}^2 \setminus D$ où D est dénombrable est connexe par arcs

Démonstration. $\subset$: Il suffit de remarquer que $\exp(M) = \exp(\frac{1}{2}M)^2$ $\supset$: Soit $M = A^2$ où $A \in \mathrm{GL}_n(\mathbb{R})$. Il existe un polynôme $P \in \mathbb{C}[X]$ tel que $A = \exp(P(A))$. Comme A est réelle, on a aussi $\exp(\overline{P}(A)) = \overline{A} = A$ et donc

$$\exp((P + \overline{P})(A)) = A^2 = M.$$

□

Référence : ZAVIDOVIQUE 2013. Merci à Antoine Diez pour ce développement.

Théorème central limite

Leçons : 218, 261, 262, *263*

Théorème 89

Si $(X_i)_i$ est une suite de variables aléatoires iid et $E(X_0^2) < \infty$ alors $\dfrac{S_n - nE(X_0)}{\sqrt{n}\sigma}$ converge en loi vers $\mathcal{N}(0,1)$ où $\sigma^2 = \mathrm{Var}(X_0)$ et $S_n = \sum_{i=0}^{n-1} X_i$.

Lemme 90

Si $(z_n)_n$ est une suite de nombres complexes tendant vers 0, alors $\lim_{n\to+\infty} \left(1 + \dfrac{z_n}{n}\right)^n = 1$.

Démonstration. On a

$$\left|\left(1+\frac{z_n}{n}\right)^n - 1\right| = \left|\sum_{k=1}^{n} \binom{n}{k} \frac{z_n^k}{n^k}\right| \leqslant \sum_{k=1}^{n} \binom{n}{k} \frac{|z_n|^k}{n^k} = \left(1+\frac{|z_n|}{n}\right)^n - 1.$$

On est donc ramené au cas où $\forall n \in \mathbb{N}, z_n \in \mathbb{R}$. A partir d'un certain rang, $z_n > -1$ et $\ln\left(\left(1+\dfrac{z_n}{n}\right)^n\right) = n\ln\left(1+\dfrac{z_n}{n}\right) = n\left(\dfrac{z_n}{n} + o\left(\dfrac{z_n}{n}\right)\right) = z_n + o(z_n)$

Donc en passant à l'exponentielle, la limite de $\left(1+\dfrac{z_n}{n}\right)^n$ est bien 1. □

Démonstration (du théorème)**.** Quitte à remplacer X_i par $\dfrac{X_i - E(X_0)}{\sigma}$, on peut supposer que $E(X_0) = 0$ et $\sigma = 1$. On note $X = X_0$. La fonction caractéristique de $\dfrac{S_n}{\sqrt{n}}$ est

$$\varphi_{S_n/\sqrt{n}}(t) = \left(\varphi_{X/\sqrt{n}}(t)\right)^n = \left(\varphi_X\left(\frac{t}{\sqrt{n}}\right)\right)^n$$

par indépendance des X_i.

De plus on sait que $\varphi_X'(0) = iE(X) = 0$, $\varphi_X''(0) = -E(X^2) = -1$. Donc selon la formule de Taylor-Young à l'ordre 2 au voisinage de 0, on a $\varphi_X(t) = 1 - \dfrac{t^2}{2} + t^2\varepsilon(t)$ où $\lim_{t\to 0} \varepsilon(t) = 0$. Donc

$$\varphi_{S_n/\sqrt{n}}(t) = \left(1 - \frac{t^2}{2n} + \frac{t^2}{n}\varepsilon\left(\frac{t}{\sqrt{n}}\right)\right)^n = \left(1-\frac{t^2}{2n}\right)^n \left(1 + \frac{t^2}{n\left(1-\frac{t^2}{2n}\right)}\varepsilon\left(\frac{t}{\sqrt{n}}\right)\right)^n$$

Le premier terme tend vers $e^{-t^2/2}$, et selon le lemme, comme

$$\lim_{n\to+\infty} \frac{t^2}{1-\frac{t^2}{2n}} = 1,$$

le second terme tend vers 1 quand n tend vers l'infini. Donc pour tout $t \in \mathbb{R}$, $\varphi_{S_n/\sqrt{n}}(t) \to e^{-t^2/2}$, qui est la fonction caractéristique de $\mathcal{N}(0,1)$. Selon le théorème de Paul-Lévy, on a le résultat voulu. □

Exemple. Dans le cadre d'un sondage pour le deuxième tour de l'élection présidentielle, on interroge n personnes pour savoir s'ils comptent voter pour le candidat A (n_A personnes) ou le candidat B (n_B personnes).Chaque personne est modélisée par une variable aléatoire $X_i : \Omega \to \{A, B\}$ suivant la loi de Bernoulli de paramètre p. On suppose que les X_i sont indépendantes. C'est ce paramètre p qui nous est inconnu et qu'on cherche à déterminer *a posteriori* à partir des données observables (les valeurs des X_i). Cela est rendu possible par le théorème central limite.

Un *intervalle de confiance* à α près pour p est un intervalle **aléatoire** I de $\mathbb{R}$ tel que $\mathbb{P}(p \in I) = 1-\alpha$.

Soit G une variable gaussienne de loi $\mathcal{N}(0,1)$ de fonction de répartition ϕ. On note $\overline{X_n} = \dfrac{X_1 + \cdots + X_n}{n}$ (dans la modélisation ci-dessus, $\overline{X_n}$ correspond à $\dfrac{n_A}{n}$). On sait que la loi de cette variable aléatoire est $\mathcal{B}(n,p)$ donc selon le TCL, $Y_n = \sqrt{n}\dfrac{\overline{X_n} - p}{\sqrt{p(1-p)}}$ converge en loi vers G.

De plus, selon la loi faible des grands nombres, $\overline{X_n} \xrightarrow[n\to+\infty]{\mathbb{P}} p$ donc selon le lemme de Slutsky, $(Y_n, \overline{X_n}) \xrightarrow[n\to+\infty]{\mathcal{L}} (G, p)$ de sorte qu'en composant par des fonctions continues, on obtient

$$Y_n \frac{\sqrt{p(1-p)}}{\sqrt{\overline{X_n}(1-\overline{X_n})}} = \frac{\sqrt{n}(\overline{X_n} - p)}{\sqrt{\overline{X_n}(1-\overline{X_n})}} \xrightarrow[n\to+\infty]{\mathcal{L}} G \times \frac{\sqrt{p(1-p)}}{\sqrt{p(1-p)}} = G.$$

Donc en vertu de la caractérisation de la convergence en loi avec les fonctions de répartitions, pour tout $a \geqslant 0$,

$$\mathbb{P}\left(-a \leqslant \frac{\sqrt{n}(\overline{X_n} - p)}{\sqrt{\overline{X_n}(1-\overline{X_n})}} \leqslant a\right) \xrightarrow[n\to+\infty]{} C_a = \phi(a) - \phi(-a),$$

c'est-à-dire, avec $I_{a,n} = \left[-a\dfrac{\sqrt{\overline{X_n}(1-\overline{X_n})}}{\sqrt{n}} + \overline{X_n}, a\dfrac{\sqrt{\overline{X_n}(1-\overline{X_n})}}{\sqrt{n}} + \overline{X_n}\right]$, $\mathbb{P}(p \in I_{a,n}) \xrightarrow[n\to+\infty]{} C_a$.

En prenant C_a suffisamment petit, à partir d'un certain rang, $\mathbb{P}(p \in I_{a,n}) \leqslant 1-\alpha$: $I_{a,n}$ est un intervalle de confiance à α près.

Complétons ce théorème par un autre théorème limite, le théorème des évènements rares de Poisson. Il faut faire attention car la preuve du Ouvrard présente une imprécision sur le logarithme complexe.

Théorème 91 (*Théorème des événements rares*)

Soit pour tout $n \in \mathbb{N}^*$ une famille finie $\{A_{n,j} | 1 \leq j \leq M_n\}$ d'évènements indépendants. On pose $p_{n,j} = \mathbb{P}(A_{n,j})$ et on note $S_n = \sum_{j=1}^{M_n} \mathbb{1}_{A_{n,j}}$ On suppose que la suite de terme général M_n tend en croissant vers $+\infty$ et que

$$\sup_{1\leq j\leq M_n} p_{n,j} \xrightarrow[n\to+\infty]{} 0, \quad \sum_{j=1}^{M_n} p_{n,j} \xrightarrow[n\to+\infty]{} \lambda$$

où $\lambda > 0$. Alors la suite $(S_n)_{n\in\mathbb{N}^*}$ converge en loi vers la loi de Poisson $\mathcal{P}(\lambda)$ de paramètre λ.

Démonstration. Soit $t \in \mathbb{R}$. Par indépendance des $A_{n,j}$, la fonction caractéristique de S_n est

$$\varphi_{S_n}(t) = \prod_{j=1}^{M_n} (p_{n,j}e^{it} + (1-p_{n,j})) = \prod_{j=1}^{M_n} \left[1 + p_{n,j}(e^{it}-1)\right].$$

On pose $z = e^{it} - 1$. Comme $\sup_{1\leq j\leq M_n} p_{n,j} \xrightarrow[n\to+\infty]{} 0$, il existe $N \geqslant 1$ tel que pour $n \geqslant N$, et $j \in \{1,\dots,M_n\}$, $|p_{n,j}z| < \dfrac{1}{2}$ de sorte que $1 + p_{n,j}z = \exp\left\{\log\left[1+p_{n,j}z\right]\right\}$ où log désigne une détermination principale du logarithme complexe sur le plan fendu de Cauchy $\mathbb{C}\setminus\mathbb{R}_-$.

Or, par la formule de Taylor avec reste intégral, si $|w| < 1$,

$$\log(1+w) = w - w^2 \int_0^1 (1-u)\frac{1}{(1+uw)^2}\mathrm{d}u$$

Si $n \geqslant N$, et $u \in [0,1]$, $j \in [\![1, M_n]\!]$, $|1 + up_{n,j}z| \geqslant 1 - up_{n,j}|z| \geqslant 1 - \dfrac{u}{2} \geqslant \dfrac{1}{2}$, d'où

$$\left|\sum_{j=1}^{M_n} p_{n,j}^2 \int_0^1 \frac{1-u}{(1+up_{n,j}z)^2}\mathrm{d}u\right| \leqslant 2\left|\sum_{j=1}^{M_n} p_{n,j}^2\right| \leqslant 2\left[\sup_{1\leq j\leq M_n} p_{n,j}\right]\left[\sum_{j=1}^{M_n} p_{n,j}\right] \xrightarrow[n\to+\infty]{} 0.$$

Donc par la formule de Taylor précédente et par hypothèse,

$$\sum_{j=1}^{M_n} \log(1+p_{n,j}z) = z\sum_{j=1}^{M_n} p_{n,j} - z^2 \sum_{j=1}^{M_n} p_{n,j}^2 \int_0^1 \frac{1-u}{(1+up_{n,j}z)^2}\mathrm{d}u \xrightarrow[n\to+\infty]{} \lambda z.$$

Donc

$$\exp\left(\sum_{j=1}^{M_n} \log(1+p_{n,j}z)\right) \xrightarrow[n\to+\infty]{} \exp(\lambda z) = \exp(\lambda(e^{it}-1),$$

fonction caractéristique d'une loi de Poisson $\mathscr{P}(\lambda)$.

Mais $\exp\left(\sum_{j=1}^{M_n} \log(1+p_{n,j}z)\right) = \prod_{j=1}^{M_n} \exp(\log(1+p_{n,j}z)) = \prod_{j=1}^{M_n} 1 + p_{n,j}z = \varphi_{S_n}(t)$, donc selon le théorème de Lévy, $(S_n)_{n\in\mathbb{N}^*}$ converge en loi vers $\mathscr{P}(\lambda)$. □

Remarque. Pour compléter ce développement un peu court, on peut calculer la fonction caractéristique d'une loi normale (cf « Inversion de Fourier »). Dans la leçon 218, il est bienvenu de mentionner le théorème des évènements rares de Poisson plutôt que la recherche d'un intervalle de confiance.

Références : BARBÉ et LEDOUX 2007, pp. 136-138 et OUVRARD 2009, p. 311 (évènements rares).

Théorème d'Abel angulaire et théorème taubérien faible

Leçons : 207, 223, 230, 235, 243

Soit $\sum a_n z^n$ une série entière de rayon de convergence 1 dont la somme sur le disque unité est notée f.

Théorème 92

On suppose que $\sum_n a_n$ converge et a pour somme S. Alors si $0 < \theta_0 < \frac{\pi}{2}$ et $\Delta_{\theta_0} = \left\{z \in D(0,1) : \exists(\rho,\theta) \in [0,1[\times[-\theta_0,\theta_0], z = 1-\rho e^{i\theta}\right\}$, on a $f(z) \xrightarrow[\substack{z\in\Delta_{\theta_0}\\ z\to 1}]{} S$.

Démonstration. L'idée clef de la preuve est de procéder à une transformation d'Abel sur les sommes partielles $\sum a_n z^n$. Pour tout $n \in \mathbb{N}$, on a $a_n = R_{n-1} - R_n$ où $R_{-1} = 0$ et $R_p = \sum_{k=p+1}^{+\infty} a_k$ pour $p \geqslant 0$. Donc si $N \in \mathbb{N}$ et $z \in D(0,1)$,

$$\sum_{n=0}^{+\infty} a_n z^n - \sum_{n=0}^{N} = \sum_{n=0}^{N} (R_{n-1} - R_n)(z^n - 1) = \sum_{n=0}^{N-1} R_n(z^{n+1} - 1) - \sum_{n=0}^{N} R_n(z^n - 1) = \sum_{n=0}^{N-1} R_n z^n (z-1).$$

D'où, en faisant tendre N vers $+\infty$, $f(z) - S = (z-1)\sum_{n=0}^{+\infty} R_n z^n$.

Soit $\varepsilon > 0$. Comme la suite des restes tend vers 0 par convergence de $\sum_n a_n$, on peut fixer $N \in \mathbb{N}$ tel que $\forall n \geqslant N, |R_n| \leqslant \varepsilon$. Ainsi,

$$|f(z) - S| \leqslant \left|\sum_{n=0}^{N} R_n z^n\right| |z-1| + \varepsilon \left(\sum_{n=N+1}^{+\infty} |z|^n\right) |z-1| \leqslant \left(\sum_{n=0}^{N} |R_n|\right) |z-1| + \varepsilon \frac{1}{1-|z|} |z-1|. \tag{2.10}$$

Étudions le second terme : si $z = 1 - \rho e^{i\theta} \in \Delta_{\theta_0}$, alors

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

et

$$1 - |z|^2 = 1 - (1 - \rho\cos\theta)^2 - \rho^2 \sin^2\theta = 2\rho\cos\theta - \rho^2 \geqslant 2\rho\cos\theta_0 - \rho^2$$

car $|\theta| \leqslant \theta_0$. Donc si $\rho \leqslant \cos\theta_0$, on a

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

Si de plus, on suppose que $\rho\left(\sum_{n=0}^{N} |R_n|\right) \leqslant \varepsilon$ et $\rho \leqslant \varepsilon$, selon (2.10), $|f(z) - S| \leqslant \varepsilon + \frac{2}{\cos\theta_0}\varepsilon$. En d'autres termes, $f(z) \xrightarrow[\substack{z\in\Delta_{\theta_0}\\ z\to 1}]{} S$.

□

Une réciproque (partielle) de ce théorème est donnée par le théorème « taubérien faible » :

Proposition 93

Si $a_n = o\left(\frac{1}{n}\right)$ et $f(x) \xrightarrow[x\to 1^-]{} S$, alors $\sum_n a_n$ converge et $\sum_{n=0}^{+\infty} a_n = S$.

Démonstration. Soit $0 < x < 1$. Si $n \in \mathbb{N}$ et $S_n = \sum_{k=0}^{n} a_k$, alors

$$S_n - S = (S_n - f(x)) + (f(x) - S).$$

C'est le premier terme de la somme qu'il est intéressant d'étudier pour obtenir la convergence voulue. On a

$$|S_n - f(x)| \leqslant \left|\sum_{k=0}^{n} a_k - \sum_{k=0}^{n} a_k x^k\right| + \left|\sum_{k=n+1}^{+\infty} a_k x^k\right| \leqslant \sum_{k=0}^{n} k|a_k|(1-x) + \left|\sum_{k=n+1}^{+\infty} \frac{ka_k}{n} x^k\right|$$

puisque d'une part, $0 \leqslant 1 - x^k = (1-x)(1 + x + \cdots + x^{k-1}) \leqslant k(1-x)$ et d'autre part $\frac{k}{n} \geqslant 1$ si $k \geqslant n+1$. Ainsi, si $M = \sup_{k\in\mathbb{N}} k|a_k|$ et $L_n = \sup_{k\geqslant n} k|a_k|$, on a

$$|S_n - f(x)| \leqslant Mn(1-x) + \frac{L_n}{n}\frac{1-x^{n+1}}{1-x} \leqslant\leqslant Mn(1-x) + \frac{L_n}{n}\frac{1}{1-x}.$$

Soit $\varepsilon > 0$. Pour tout $n \in \mathbb{N}^*$, $\left|S_n - f\left(1 - \frac{\varepsilon}{n}\right)\right| \leqslant M\varepsilon + \frac{L_n}{n} \times \frac{n}{\varepsilon} \leqslant M\varepsilon + \frac{L_n}{\varepsilon}$. Par hypothèse, $L_n \xrightarrow[n\to+\infty]{} 0$ donc il existe $N \in \mathbb{N}$ tel que $\forall n \geqslant N$, $L_n \leqslant \varepsilon^2$, d'où

$$\left|S_n - f\left(1 - \frac{\varepsilon}{n}\right)\right| \leqslant (M+1)\varepsilon.$$

Or, $f\left(1 - \frac{\varepsilon}{n}\right) \xrightarrow[n\to+\infty]{} S$ donc il existe $n_0 \in \mathbb{N}$ tel que $\left|f\left(1 - \frac{\varepsilon}{n}\right) - S\right| \leqslant \varepsilon$. Par suite, $\forall n \geqslant \max(n_0, N), |S_n - S| \leqslant (M+2)\varepsilon$. Donc $S = \sum_{n=0}^{+\infty} a_n$. □

Remarque.

- La réciproque du théorème d'Abel angulaire est fausse en général, car $\sum_{n=0}^{+\infty} (-1)^n z^n = \frac{1}{1+z} \xrightarrow{z\to 1} \frac{1}{2}$ tandis que $\sum_{n=0}^{+\infty} (-1)^n$ diverge.
- Un exemple d'application du théorème : $\sum_{n=1}^{+\infty} \frac{(-1)^n}{2n+1} = \sum_{n=1}^{+\infty} \frac{(-1)^n}{2n+1} x^n = \lim_{x\to 1} \arctan x = \arctan 1 = \frac{\pi}{4}$.
- Le théorème taubérien faible est encore vrai si $a_n = O\left(\frac{1}{n}\right)$, c'est le théorème taubérien de Hardy-Littlewood.

Référence : GOURDON 2009b, pp. 253-254

Théorème d'Artin

Leçons : 125, 151, 162

Théorème 94 (*Artin*)

Si L est un corps et H est un sous-groupe fini du groupe des automorphismes de L, alors si $L^H = \{x \in L : \forall \sigma \in H, \sigma(x) = x\}$, L/L^H est une extension finie, $|H| = [L : L^H]$ et H est le groupe des L^H-automorphismes de L.

Lemme 95 (*Dedekind*)

Soient $\sigma_1, \dots, \sigma_n$ des automorphismes distincts de L, alors $(\sigma_1, \dots, \sigma_n)$ est libre sur L, c'est-à-dire que si $\forall x, \sum_{i=1}^{n} \lambda_i \sigma_i(x) = 0$, alors $\lambda_1 = \dots = \lambda_n = 0$.

Démonstration (du lemme)**.** Supposons la famille $(\sigma_1, \dots, \sigma_n)$ non libre et prenons $(\lambda_1, \dots, \lambda_n) \in L^n \setminus \{0\}$ avec un nombre minimal r de composantes non nulles tel que $\sum_{i=1}^{n} \lambda_i \sigma_i = 0$. On peut supposer sans perte de généralité que $\lambda_1, \dots, \lambda_r$ sont non nuls et $\lambda_{r+1} = \dots = \lambda_n = 0$.

Soit $y \in L$ tel que $\sigma_1(y) \neq \sigma_2(y)$. Pour tout $x \in L$, on a

$$\sum_{i=1}^{r} \lambda_i \sigma_i(x) = 0 \tag{2.11}$$

et par ailleurs,

$$\sum_{i=1}^{n} \lambda_i \sigma_i(xy) = \sigma_i(y) \sum_{i=1}^{r} \sigma_i(x) = 0. \tag{2.12}$$

Donc en effectuant (2.12)$-\sigma_1(y)\times$ (2.11), on obtient $\sum_{i=2}^{r} \lambda_i(\sigma_i(y) - \sigma_1(y))\sigma_i(x) = 0$, ce qui contredit l'hypothèse de minimalité sur r.

□

Démonstration. On note $m = [L : L^H]$ (éventuellement égal à ∞) et $n = |H|$. On va vérifier dans un premier temps que $m = n$.

1 Supposons que $m < n < +\infty$. Fixons $x_1, \dots, x_m$ une base de L sur L^H et notons $H = \{\sigma_1, \dots, \sigma_n\}$. Considérons le système de m équations à n inconnues dans L, $Y_1, \dots, Y_n$ défini par

$$\forall j \in [\![1, m]\!], \sigma_1(x_j)Y_1 + \dots \sigma_n(x_j)Y_n = 0.$$

C'est un système surdéterminé donc il admet une solution non nulle $(y_1, \dots, y_n)$. Par suite, pour tout $x = \sum_{j=1}^{m} \alpha_j x_j \in L$, où $\alpha_j \in L^H$, on a

$$\sum_{i=1}^{n} \sigma_i(x) y_i = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_j \sigma_i(x_j) y_i = \sum_{j=1}^{m} \alpha_j \left(\sum_{i=1}^{m} \sigma_i(x_j) y_i \right) = 0.$$

On a donc $\sum_{i=1}^{n} y_i \sigma_i = 0$ avec les y_i non tous nuls ce qui contredit le lemme d'indépendance de Dedekind ci-dessus. Donc $m \geqslant n$.

2 Supposons que $m > n$. Il existe donc une famille $(x_1, \dots, x_{n+1})$ d'éléments de L libre sur L^H. Selon le même argument que pour le premier point, on peut trouver une famille non nulle $(y_1, \dots, y_{n+1}) \in L^{n+1}$) vérifiant

$$\forall i \in [\![1, n]\!], \sigma_i(x_1)y_1 + \cdots + \sigma_i(x_{n+1})y_{n+1} = 0. \tag{2.13}$$

Sans perte de généralité, on peut supposer que parmi toutes les solutions non nulles, $(y_1, \dots, y_{n+1})$ a un nombre minimal r de termes non nuls. Alors quitte à renuméroter, on peut supposer que $\forall i \leqslant r, y_i \neq 0$ et $\forall i > r, y_i = 0$. Ainsi, (2) se réécrit

$$\forall i \in [\![1, n]\!], \sigma_i(x_1)y_1 + \cdots + \sigma_i(x_r)y_r = 0.$$

Soit $\sigma \in H$, appliquons σ au système :

$$\forall i \in [\![1, n]\!], (\sigma \circ \sigma_i)(x_1)\sigma(y_1) + \cdots + (\sigma \circ \sigma_i)\sigma(y_r) = 0.$$

Comme $\tau \mapsto \sigma \circ \tau$ est une permutation de l'ensemble fini H, on a donc

$$\forall i \in [\![1, n]\!], \sigma_i(x_1)y_1 + \cdots + \sigma_i(x_r)y_r = 0. \tag{2.14}$$

En multipliant (2) par $\sigma(y_1)$, (2.14) par y_1 et en additionnant les deux systèmes, on obtient

$$\forall i \in [\![1, n]\!], \sigma_i(x_2)(\sigma(y_1)y_2 - \sigma(y_2)y_1) + \cdots + \sigma_i(x_r)(\sigma(y_1)y_r - \sigma(y_r)y_1) = 0.$$

L'entier r étant le nombre minimal de termes non nuls d'une solution non triviale de (2), on a $\forall j \in [\![2, r]\!], \sigma(y_1)y_j - y_1\sigma(y_j) = 0$, soit $\sigma(y_1y_j^{-1}) = y_1y_j^{-1}$ donc $\forall j \in [\![2, r]\!], y_1y_j^{-1} \in L^H$.

Ainsi pour tout $2 \leqslant j \leqslant r$, il existe $z_j \in (L^H)^*$ tel que $y_j = z_jy_1$.

La ligne de (2) correspondant à $\sigma_i = \mathrm{id}_L$ devient alors

$$x_1y_1 + x_2z_2y_1 + \cdots + x_rz_ry_1 = 0$$

donc comme $y_1 \neq 0$, on a $x_1 + x_2z_2 + \cdots + x_rz_r = 0$, de sorte que $(x_1, \dots, x_r)$ est une famille liée, ce qui contredit l'hypothèse initiale. Donc $m \leqslant n < +\infty$ et finalement $m = n$.

3 Notons G le groupe des L^H-automorphismes de L. Il contient H de manière évidente. Montrons que G est fini. Soit $(a_1, \dots, a_n)$ une base de L sur L^H, $\Pi_1, \dots, \Pi_r$ les polynômes minimaux respectifs des a_i sur L^H et $f = \Pi_1 \dots \Pi_r \in L^H[X]$. Soit R l'ensemble (fini) des racines de f dans L. Comme $\Pi_j(a_j) = 0$ pour tout j, R contient $\{a_1, \dots a_n\}$.

De plus, si $x = \sum_{i=1}^{n} \alpha_i a_i \in L$, où $\alpha_i \in L^H$, alors, pour tout élément σ de G, on a $\sigma(x) = \sum_{i=1}^{n} \alpha_i \sigma(a_i)$. Cela nous assure que $\psi : \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}(R) \\ \sigma & \longmapsto & \sigma_{|R} \end{array}$ est injective et donc que G est fini.

On a $L^H \subset L^G \subset L$ par définition de G, et $L^G \subset L^H \subset L$ car $H \subset G$ donc $L^H = L^G$. Selon la conclusion du deuxième point, on a $|G| = [L : L^H] = [L : L^G] = |H|$ donc $G = H$.

□

Quelques précisions supplémentaires : ce développement s'inscrit dans une théorie plus générale, la théorie de Galois. Étant donné une extension de corps L/K, on s'intéresse à son *groupe de Galois* $\mathrm{Gal}(L/K)$ qui est le groupe des K-automorphismes de corps de L. Le résultat majeur de cette théorie est la correspondance de Galois entre les corps intermédiaires $K \subset M \subset L$ et les sous-groupes H de $\mathrm{Gal}(L/K)$:

Théorème 96

Si L/K est une extension galoisienne, les applications $\mathrm{Fix} : H \mapsto L^H$ *et* $\mathrm{Gal} : M \mapsto \mathrm{Gal}(L/M)$ *sont réciproques l'une de l'autre, où L^H, comme défini dans l'énoncé du théorème d'Artin est appelé sous-corps fixe de L associé à H.*

Il est remarquable qu'en vertu du théorème d'Artin, toute extension finie vérifie $\mathrm{Gal} \circ \mathrm{Fix} = \mathrm{id}$.

Définition 97

Soit L/K une extension algébrique. On dit que c'est une extension galoisienne si $L^{\mathrm{Gal}(L/K)} = K$.

On suppose à présent que K est un corps parfait, c'est-à-dire que si L/K est une extension algébrique, alors tout polynôme de $L[X]$ n'admet que des racines simples dans son corps de décomposition – L est dit *séparable*. La plupart des corps usuels sont parfaits : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, les corps finis. En revanche pour p premier, $\mathbb{F}_p(T)$ n'est pas parfait.

Définition 98

L'extension algébrique L/K est dite normale si tout polynôme ***irréductible*** *$f \in K[X]$ admettant une racine dans L se décompose en produit de facteurs de degré 1 dans L.*

Par exemple $\mathbb{C}/\mathbb{R}$ est une extension normale.

Proposition 99

Soit L/K une extension finie, alors on a l'équivalence entre :

1. *L/K est galoisienne ;*
2. *L/K est normale ;*
3. *L est le corps de décomposition d'un polynôme $f \in K[X]$;*
4. *$\mathrm{Gal}(L/K)$ est d'ordre $[L : K]$.*

En particulier si L/K est galoisienne finie et $K \subset M \subset L$ est un corps intermédiaire, alors L/M est galoisienne puisque L est le corps de décomposition de $f \in K[X] \subset M[X]$, ce qui prouve la correspondance de Galois.

Remarque.
- C'est un peu long pour 15 minutes, il vaut mieux démontrer le lemme de Dedekind que le dernier point de la démonstration du théorème.
- Pour bien se souvenir du système à poser à chaque étape, retenir qu'un système surdéterminé, c'est **plus d'inconnues que d'équations**.

Références : JEANNERET et LINES 2008, p. 297. Voir également SAMUEL 1967 pour la théorie de Galois.

Théorème de Carathéodory et application aux équations diophantiennes

Leçons : 126, 181

Théorème 100 (*Carathéodory*)

Soit E un $\mathbb{R}$-espace vectoriel de dimension n. Soit A une partie de E. Alors l'enveloppe convexe $\mathrm{Conv}(A)$ *est l'ensemble des combinaisons convexes de $n+1$ points de A.*

Démonstration. Soit $x = \sum_{i=1}^{p} \alpha_i x_i$ un élément de $\mathrm{Conv}(A)$. Sans perte de généralité, on peut supposer que p est le nombre minimal de termes intervenant dans une écriture comme combinaison convexe de x. Raisonnons par l'absurde, et supposons que $p \geqslant n+2$.

Soit

$$\begin{array}{rccc} \phi : & \mathbb{R}^p & \longrightarrow & E \times R \\ & (\lambda_1, \ldots, \lambda_p) & \longmapsto & \left(\sum_{i=1}^p \lambda_i x_i, \sum_{i=1}^p \lambda_i\right) \end{array}.$$

Selon le théorème du rang, le noyau de ϕ a pour dimension $\dim(E \times \mathbb{R}) - \dim \mathrm{Im}\, \phi \geqslant 1$ par hypothèse sur p. Donc on peut trouver $(\lambda_1, \ldots, \lambda_p) \neq 0$ tel que $\sum_{i=1}^{p} \lambda_i = 0$ et $\sum_{i=1}^{p} \lambda_i x_i = 0$, de sorte que $\forall \tau \in \mathbb{R}, x = \sum_{i=1}^{p} (\alpha_i + \tau\lambda_i) x_i$ et $\sum_{i=1}^{p} \alpha_i + \tau\lambda_i = 1$.

Introduisons donc

$$F = \left\{\tau \in \mathbb{R} | \forall i \in [\![1, p]\!], \alpha_i + \tau\lambda_i \geqslant 0\right\} = \bigcap_{\lambda_i < 0} \left]-\infty, \frac{-\alpha_i}{\lambda_i}\right] \cap \bigcap_{\lambda_i < 0} \left[\frac{-\alpha_i}{\lambda_i}, +\infty\right[.$$

Il existe donc $\lambda_j < 0$ et $\lambda_k > 0$ tels que $F = \left[-\frac{\alpha_j}{\lambda_j}, -\frac{\alpha_k}{\lambda_k}\right]$. Ainsi, $\tau = -\frac{\alpha_j}{\lambda_j} \in F$ et $x = \sum_{i \neq j} (\alpha_i + \tau\lambda_i) x_i$ est une écriture de x comme combinaison convexe de $p-1$ éléments de $\left\{x_1, \ldots, x_p\right\}$, ce qui contredit la minimalité de p. □

Corollaire 101

Soit $A \in \mathscr{M}_n(\mathbb{Z})$. Le système diophantien $Ax = 0$ admet une solution non nulle dans $\mathbb{N}^n$ si et seulement $0_{\mathbb{R}^n}$ est dans l'enveloppe convexe des colonnes de A.

Démonstration. On note A_i la i-ème colonne de A.

$\Leftarrow$: soit x solution non nulle dans $\mathbb{N}^n$, alors $0 = (A_1 \ldots A_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i=1}^{n} x_i A_i$ donc en divisant par n, on obtient le résultat.

$\Rightarrow$: soit l minimal tel que 0 s'écrive comme combinaison convexe à l termes $\sum_{j=1}^{l} x_j A_{i_j}$ des colonnes de A. Selon le théorème de Carathéodory, en notant r le rang sur $\mathbb{Q}$ de la matrice $(A_{i_1}, \ldots, A_{i_l})$, on a $l \leqslant r+1$. Mais puisqu'on a exhibé une relation de dépendance linéaire entre ces colonnes, $r < l$. Ainsi $r = l-1$ et par l'algorithme du pivot de Gauss sur $\mathbb{Q}$, on peut trouver $P \in \mathrm{GL}_m(\mathbb{Q})$ tel que $P(A_{i_1} \ldots A_{i_r}) = \begin{pmatrix} M \\ 0 \end{pmatrix}$ où $M \in \mathscr{M}_{r,r+1}(\mathbb{Z})$ est de rang r.

Donc $\ker_{\mathbb{Q}} M$ est de dimension 1 sur $\mathbb{Q}$ et de plus $M \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = 0$ donc $x' = (x_1, \ldots, x_r)$ est un vecteur directeur à coefficients positifs de $\ker_{\mathbb{Q}} M$.

Or $\ker_{\mathbb{Q}} M \subset \ker_{\mathbb{R}} M$ donc x' est également un vecteur directeur de $\ker_{\mathbb{R}} M$, de sorte que tous ses éléments ont leurs coefficients tous positifs ou tous négatifs. En multipliant x' par un coefficient bien choisi, on peut donc trouver $y' \in \mathbb{N}^r$ tel que $(A_{i_1} \ldots A_{i_r})y' = 0$. On obtient $y \in \mathbb{N}^n$ tel que $Ay = 0$ en complétant y' avec des 0. □

Corollaire 102

Si K est une partie compacte de $\mathbb{R}^n$, alors l'enveloppe convexe de K est compacte.

Référence : GOURDON 2009b, p. 54 pour le théorème et la deuxième application. L'optimisation de la preuve et la première application sont dues à Benjamin Havret.

Théorème de Grothendieck

Leçons : 201, 208, *213*, 234

Théorème 103

Soit (X,μ) un espace de probabilités, et S un sous-espace vectoriel fermé de $L^p(\mu)$ tel que $S \subset L^\infty(\mu)$. Alors S est de dimension finie.

Démonstration. Étape 1 : il existe $K>0$ tel que $\forall f \in S, \|f\|_\infty \leqslant K\|f\|_p$.

Soit i l'injection canonique de $(S, \|\cdot\|_\infty)$ dans $(S, \|\cdot\|_p)$. C'est une application linéaire bijective, qui est continue car $\|\cdot\|_p \leqslant \|\cdot\|_\infty$ puisque $\mu(X)=1$. De plus ses espaces de départ et d'arrivée sont des Banach :

- D'une part car S est fermé dans $L^p(\mu)$ qui est complet selon le théorème de Riesz-Fischer ;
- D'autre part, si $(f_n)_n \in S^{\mathbb{N}}$ tend vers f dans $L^\infty(\mu)$, alors $(i(f_n))_n$ tend vers $i(f)$ dans $L^p(\mu)$ donc comme S est fermé dans L^p, $i(f)=f\in S$, de sorte que S est aussi un sous-espace fermé de $L^\infty(\mu)$, donc est complet.

Par conséquent, selon le théorème d'isomorphisme de Banach, i est un isomorphisme bicontinu ; en particulier, il existe $K>0$ tel que $\forall f \in S, \|f\|_\infty \leqslant K\|f\|_p$.

Étape 2 : il existe $M>0$ tel que $\forall f \in S, \|f\|_p \leqslant K\|f\|_\infty$.

Soit $f\in S$, on distingue deux cas :

- *Premier cas* : $p<2$. Selon l'inégalité de Hölder,

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

  si bien que $\|f\|_p \leqslant \|f\|_2$.
- *Deuxième cas* : $p \geqslant 2$.

$$\|f\|_p^p = \int_X |f(x)|^{p-2}|f(x)|^2 \mathrm{d}\mu(x) \leqslant \|f\|_\infty^{p-2}\|f\|_2^2 \overset{\text{etape 1}}{=} K^{p-2}\|f\|_p^{p-2}\|f\|_2^2$$

  donc en simplifiant de part et d'autre de l'inégalité, $\|f\|_p^2 \leqslant K^{p-2}\|f\|_2^2$ et le résultat s'ensuit.

Étape 3 : utilisation de ces relations de domination.

Soit $(f_1,\dots,f_n)$ une famille orthonormée de S. Si $c=(c_1,\dots,c_n)\in\mathbb{Q}^n$, il existe $X_c \subset X$ de mesure pleine tel que

$$\forall x \in X_c, \left|\sum_{i=1}^n c_i f_i(x)\right| \leqslant \left\|\sum_{i=1}^n c_i f_i\right\|_\infty \leqslant M_1\left\|\sum_{i=1}^n c_i f_i\right\|_2 = M_1\sqrt{\sum_{i=1}^n c_i^2}$$

avec $M_1>0$ une constante (cf étapes 1 et 2).

Donc si $X' = \bigcup_{c\in\mathbb{Q}^n} X_c$, X' est de mesure pleine et on a

$$\forall c\in\mathbb{Q}^n, \forall x\in X', \left|\sum_{i=1}^n c_i f_i(x)\right| \leqslant M_1\sqrt{\sum_{i=1}^n c_i^2}.$$

Comme $\mathbb{Q}^n$ est dense dans $\mathbb{R}^n$, le résultat vaut également pour $c\in\mathbb{R}^n$.

En particulier, si $x \in X'$, $c_i = f_i(x)$, on obtient $\left|\sum_{i=1}^{n} f_i(x)^2\right| \leqslant M_1 \sqrt{\sum_{i=1}^{n} f_i(x)^2}$ soit

$$\left(\sum_{i=1}^{n} f_i(x)^2\right) \leqslant M_1^2.$$

Donc en intégrant, $\sum_{i=1}^{n} \|f_i\|_2^2 \leqslant M_1^2$ soit, comme $(f_1, \ldots, f_n)$ est orthonormée, $n \leqslant M_1^2$.

Supposons que S soit de dimension infinie. On pourrait alors trouver une famille libre de taille $E(M_1^2)+1$, ce qui fournirait par le procédé d'orthonormalisation de Gram-Schmidt, une famille orthonormée de S de cette taille : cela contredit le résultat ci-dessus. Donc S est de dimension finie.

□

Remarque. Le théorème de l'isomorphisme de Banach est une conséquence du théorème de Baire, qu'il faut donc connaître.

Références : ZAVIDOVIQUE 2013 (attention il y a une erreur).

Théorème de Liapounov

Leçons : 220, 221

Définition 104

Soit $f : \mathbb{R}^n \to \mathbb{R}^n$ une application de classe $\mathscr{C}^1$.

- *Un point d'équilibre stable attractif du système $y' = f(y)$ est $y_0 \in \mathbb{R}^n$ tel que $f(y_0) = 0$ et pour tout $\varepsilon > 0$, il existe $\delta > 0$ tel que pour toute solution y du système, $\|y(0) - y_0\| \leqslant \delta \Rightarrow \forall t \geqslant 0, \|y(t) - y_0\| \leqslant \varepsilon$.*
- *Le point d'équilibre attractif stable y_0 est dit asymptotiquement stable s'il existe $\delta_0 > 0$ tel que pour toute solution y du système vérifiant $\|y(0) - y_0\| \leqslant \delta_0$, $\lim\limits_{t \to +\infty} y(t) = y(0)$.*

Théorème 105

Soit $f : \mathbb{R}^n \to \mathbb{R}^n$ une application de classe $\mathscr{C}^1$ telle que $f(0) = 0$. Si $A = Df(0)$ a des valeurs propres de parties réelles dans $\mathbb{R}_-^*$, alors l'origine est un point d'équilibre attractif asymptotiquement stable du système $y' = f(y)$. Précisément, il existe $\beta > 0, \eta > 0, C > 0$ tels que pour tout $\|x\| < \eta$, la solution y_x de $\begin{cases} y' = f(y) \\ y(0) = x \end{cases}$ vérifie

$$\forall t \geqslant 0, \|y_x(t)\| \leqslant Ce^{-\beta t}\|x\|.$$

Démonstration. Soit $\langle \cdot, \cdot \rangle$ un produit scalaire sur $\mathbb{R}^n$ définissant la norme $\| \cdot \|$.

On procède en trois temps :

Étape 1 : Étude du système linéarisé $\begin{cases} z' = Az \\ z(0) = x \end{cases}$

On sait que la solution z de ce système est $z : t \mapsto e^{tA}x$. Par le lemme des noyaux, on a $\mathbb{R}^n = \bigoplus\limits_{i=1}^{l} \ker(A - \lambda_i I)^{\alpha_i}$ où les λ_i sont les valeurs propres de A de multiplicité α_i. Écrivons $x = x_i + \cdots + x_l$ selon cette décomposition en somme directe. On a

$$e^{tA}x_i = e^{t\lambda_i}e^{t(A-\lambda_i I)}x_i = e^{t\lambda_i}\sum_{j=0}^{\alpha_i - 1}\frac{(A-\lambda_i I)^j}{j!}x_i = e^{t\lambda_i}P_i(A)x_i$$

où $P_i \in \mathbb{C}[X]$. Ainsi, comme $\|x_i\| \leqslant \|x\|$, on a $\|e^{tA}x_i\| \leqslant e^{t\mathrm{Re}\lambda_i}\|P_i(A)\|\|x\|$, d'où par inégalité triangulaire,

$$\forall t \geqslant 0, \|z(t)\| \leqslant \tilde{C}\left(\sum_{i=0}^{k} e^{t\mathrm{Re}\lambda_i}\right)\|x\|$$

où $\tilde{C}$ est une constante.

Donc comme les $\mathrm{Re}(\lambda_i)$ sont strictement négatifs, on peut fixer $a > 0$ et une constante $C > 0$ tels que $\forall t \geqslant 0, \|z(t)\| \leqslant Ce^{-at}\|x\|$: l'origine est un point d'équilibre attractif du système linéarisé.

Étape 2 : Introduction d'une norme auxiliaire

Soit $b : (x, y) \mapsto \displaystyle\int_0^{+\infty} \langle e^{tA}x, e^{tA}y \rangle \mathrm{d}t$. La forme bilinéaire symétrique b est bien définie

car, en vertu du premier point,

$$\forall (x,y), |b(x,y)| \leqslant C\left(\int_0^{+\infty} e^{-2at}\mathrm{d}t\right)\|x\|\|y\|.$$

Elle est de plus définie positive car $\langle\cdot,\cdot\rangle$ l'est et e^{tA} est inversible pour $t \geqslant 0$.

Soit y la solution de $\begin{cases} y' = f(y) \\ y(0) = x \end{cases}$ On note $r(y) = f(y) - Ay$. On cherche à obtenir une inégalité du type $q(y)'(t) \leqslant -\beta q(y)$. On a

$$\forall t \geqslant 0, (q\circ y)'(t) = (\nabla q)(y(t)).y'(t) = 2b(y(t), f(y(t))) = 2b(y(t), r(y(t))) + 2b(y(t), Ay(t))$$

où $r(y) = f(y) - Ay$. Or, si $x \in \mathbb{R}^n$,

$$2b(x,Ax) = 2\int_0^{+\infty} \langle e^{tA}x, e^{tA}Ax\rangle \mathrm{d}t = \int_0^{+\infty} \frac{\mathrm{d}}{\mathrm{d}t}\left(\|e^{tA}x\|^2\right)\mathrm{d}t = -\|x\|^2.$$

La norme $\sqrt{q}$ est équivalente à $\|\cdot\|$ donc on peut fixer $\beta_1 > 0$ tel que $\sqrt{q} \geqslant \beta_1\|\cdot\|$. En outre, par Cauchy-Schwarz, $|b(y, r(y))| \leqslant \sqrt{q(y)}\sqrt{q(r(y))}$. La fonction f étant $\mathscr{C}^1$, on a $r(u) = o(u)$, ce qui implique qu'il existe $\eta > 0$ tel que

$$\sqrt{q(y)} \leqslant \sqrt{\eta} \Rightarrow \sqrt{q(r(y))} \leqslant \sqrt{\beta_1^2}2\sqrt{q(y)}.$$

Donc en combinant ces deux résultats, si $q(y) \leqslant \eta$,

$$(q\circ y)' \leqslant -\|y\|^2 + \frac{\beta_1^2}{2}q(y) \leqslant -\frac{\beta_1^2}{2}q(y) = -\beta q(y).$$

Étape 3 : Résolution d'une inéquation différentielle.

Supposons que $q(x) \leqslant \eta$, alors $\forall t \geqslant 0, q(y(t)) \leqslant \eta$. En effet, dans le cas contraire, on peut fixer, par continuité de $q(y)$, $t_0 > 0$ tel que $q(y(t_0)) = \eta$ et $\forall t < t_0, q(y(t)) < \eta$. Alors

$$(q\circ y)'(t_0) \leqslant -\beta q(y)(t_0) < 0,$$

donc pour $t < t_0$ proche de t_0, on $q(y)(t) > q(y)(t_0) = \eta$ ce qui est contradictoire.

Soit $\psi : t \mapsto e^{\beta t}q(y(t))$. Alors

$$\forall t \geqslant 0, \psi'(t) = e^{\beta t}(\beta q(y)(t) - (q\circ y)'(t)) \leqslant 0$$

donc $\psi(t) \leqslant \psi(0) = q(x)$.

On en conclut que si $q(x) \leqslant \eta$, on a $\forall t \geqslant 0, q(y) \leqslant q(x)e^{-\beta t}$, ce qui prouve que l'origine est un point d'équilibre attractif asymptotiquement stable du système. □

Remarque.
- L'étude du système linéarisé intervient de manière cruciale pour pouvoir définir b.
- Si $Df(0)$ a une valeur propre de partie réelle strictement positive, alors 0 est un point d'équilibre instable.

Référence : ROUVIÈRE 2003, pp. 129–135.

Théorème des deux carrés

Leçons : ***120*****, 121, 122, 126**

Théorème 106

Soit $n = \prod_{p\in\mathscr{P}} p^{v_p(n)} \in \mathbb{N}^*$*. Alors* p *s'écrit comme somme de deux carrés dans* $\mathbb{Z}$ *si et seulement si* $v_p(n)$ *est pair pour* $p \equiv 3[4]$*.*

Démonstration. Considérons l'anneau des entiers de Gauss

$$\mathbb{Z}[i] = \left\{a + ib, (a,b) \in \mathbb{Z}^2\right\}$$

muni de $N : z = a + ib \mapsto a^2 + b^2$. Soit $\Sigma = \left\{a^2 + b^2, (a,b) \in \mathbb{Z}^2\right\} = N(\mathbb{Z}[i])$.

- $(\mathbb{Z}[i], N)$ est un anneau euclidien. En effet, si $z, z' \in \mathbb{Z}[i]$, alors $\dfrac{z}{z'} = x + iy \in \mathbb{Q}[i]$ donc en prenant $a, b \in \mathbb{Z}$ tels que $|a-x| \leqslant \dfrac{1}{2}$ et $|b-y| \leqslant \dfrac{1}{2}$, on a en posant $q = a+ib$,

  $$\left|\frac{z}{z'} - q\right| \leqslant \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

  donc $z = qz' + r$, où $N(z) < N(z')$.

- Si $z = a + ib \in \mathbb{Z}[i]^\times$, alors il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$ donc $N(zz') = 1 = N(z)N(z')$ de sorte que $N(z) = 1 = a^2 + b^2$. Ainsi, $z = \pm 1$ ou $\pm i$ et

  $$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}.$$

- Soit p premier dans $\mathbb{Z}$. Montrons que $p \in \Sigma \Leftrightarrow p$ n'est pas irréductible dans $\mathbb{Z}[i]$.
  En effet, d'une part, si $p = a^2 + b^2 = (a - ib)(a + ib)$, p n'est pas irréductible : on ne peut avoir $a = 0$ ou $b = 0$ puisque p est premier dans $\mathbb{Z}$, donc selon la description de $\mathbb{Z}[i]^\times$, ni $a + ib$, ni $a - ib$ ne sont des unités de $\mathbb{Z}[i]$.
  Réciproquement, si p n'est pas irréductible, on écrit $p = zz'$ avec $z, z' \notin \{\pm 1, \pm i\}$ donc $p^2 = N(p) = N(z)N(z')$ avec $N(z), N(z') \neq p$. Par conséquent, $N(z) = N(z') = p$ et $p \in \Sigma$.

- Comme $\mathbb{Z}[i]$ est principal, p est irréductible dans $\mathbb{Z}[i]$ si et seulement si $\mathbb{Z}[i]/(p)$ est intègre. Or, $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2 + 1)$ et le morphisme canonique

  $$\mathbb{Z}[X] \xrightarrow[\text{reduction} \mod p]{} (\mathbb{Z}/p\mathbb{Z})[X] \to (\mathbb{Z}/p\mathbb{Z})[X]/(X^2 + 1)$$

  se factorise en $\mathbb{Z}[X]/(X^2 + 1) \to \mathbb{F}_p[X]/(X^2 + 1)$ dont on vérifie immédiatement qu'il est de noyau (p). Donc

  $$\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2 + 1).$$

  Ainsi, p est irréductible dans $\mathbb{Z}[i] \Leftrightarrow X^2 + 1$ est irréductible dans $\mathbb{F}_p[X]$, c'est-à-dire s'il n'a aucune racine dans $\mathbb{F}_p[X]$, soit encore si -1 n'est pas un carré modulo p. Or, dans $\mathbb{F}_p$,

  $$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow \frac{p-1}{2} \equiv -1[2] \Leftrightarrow p \equiv 3[4].$$

  Finalement, $p \in \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1[4]$.

- Pour terminer, traitons le cas général. Soit $n = \prod_{p \in \mathscr{P}} p^{v_p(n)}$. Remarquons que $\Sigma = N(\mathbb{Z}[i])$ est stable par multiplication car $\mathbb{Z}[i]$ est un anneau.
  Alors si pour tout $p \equiv 3[4]$, $v_p(n)$ est pair, on a

$$n = \left(\prod_{p \equiv 3} p^{\frac{v_p(n)}{2}} \right)^2 \times \left(\prod_{p \equiv 1 \text{ ou } p=2} p^{v_p(n)} \right)$$

  si bien que $n \in \Sigma$ en tant que produit d'éléments de Σ.
  Montrons la réciproque par récurrence sur n. Soit $n = a^2 + b^2 \in \Sigma$, et $p \equiv 3[4]$ tel que $v_p(n) > 0$. Alors $p | a^2 + b^2 = (a+ib)(a-ib)$ donc comme p est irréductible dans $\mathbb{Z}[i]$, $p|a+ib$ ou $p|a-ib$ dans $\mathbb{Z}[i]$. Dans les deux cas, comme p est entier, on a $p|a$ et $p|b$, si bien que $p^2|n$. Appliquant l'hypothèse de récurrence à $\frac{n}{p^2} = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2 \in \Sigma$, on obtient que $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2$ est pair, ce qui conclut.

□

Corollaire 107

Les irréductibles de $\mathbb{Z}[i]$ sont, à association près, les premiers $p \in \mathbb{Z}$ tels que $p \equiv 3[4]$ et les entiers de Gauss $z = a + ib$ tels que $N(z)$ est un premier de $\mathbb{Z}$.

Démonstration.
- On a déjà vu que les premiers $p \in \mathbb{Z}$ tels que $p \equiv 3[4]$ sont irréductibles. Soit $z = a + ib$ tels que $p = N(z)$ est premier dans $\mathbb{Z}$. Si $z = z'z''$, alors $N(z) = N(z')N(z")$ donc $N(z') = 1$ ou $N(z") = 1$ c'est-à-dire z' ou $z'' \in \mathbb{Z}[i]^\times$.
- Réciproquement, soit $z = a + ib \in \mathbb{Z}[i]$ irréductible. Alors $N(z) = z\overline{z}$. Soit p premier dans $\mathbb{Z}$ tel que $p \mid N(z)$. Alors si $p \equiv 3[4]$, p divise z ou $\overline{z}$ dans $\mathbb{Z}[i]$ donc comme z est irréductible, $z = p$ à $\pm 1, \pm i$ près. Sinon, $p \in \Sigma$, $p = a^2 + b^2$ donc selon le premier point, $t = a + ib$ est irréductible. Selon le lemme de Gauss, t divise z ou $\overline{z}$ donc est égal à z à association près.

□

Référence : PERRIN 1996, pp. 56-58.

Théorème des extréma liés

Leçons : 151, 159, 214, 215, 219

Théorème 108

Soit U ouvert de $\mathbb{R}^n$, $a \in U$ et $g_1, \dots, g_r, f \in \mathscr{C}^1(U, \mathbb{R})$ tels que $(\mathrm{d}g_1(a), \dots, \mathrm{d}g_r(a))$ est une famille libre de $(\mathbb{R}^n)^*$.

$\Gamma = \{x \in U : g_1(x) = \cdots = g_r(x) = 0\}$, $f_{|\Gamma}$ admet un extremum local en $a \in \Gamma$. Alors il existe des uniques réels, $\lambda_1, \dots, \lambda_r$, appelés multiplicateurs de Lagrange, tels que

$$\mathrm{d}f(a) = \sum_{i=1}^{r} \lambda_i \mathrm{d}g_i(a).$$

Démonstration. Remarquons en premier lieu que le cas $n = r$ est évident donc on suppose $r \leqslant n-1$. Notons $s = n-r$ et procédons à l'identification $\mathbb{R}^n \simeq \mathbb{R}^s \times \mathbb{R}^r$ en notant les éléments de $\mathbb{R}^n$ sous la forme (x, y). En particulier, on pose $a = (\alpha, \beta)$. On note $g = (g_1, \dots, g_r)$

La matrice jacobienne $Jg(a) \in \mathscr{M}_{r,n}$ est de rang r donc elle admet une matrice extraite de rang r et quitte à renuméroter les variables, on peut supposer que $\begin{pmatrix} \frac{\partial g_1}{\partial y_1} & \dots & \frac{\partial g_1}{\partial y_r} \\ \vdots & & \vdots \\ \frac{\partial g_r}{\partial y_1} & \dots & \frac{\partial g_r}{\partial y_r} \end{pmatrix}$ est inversible.

Ainsi, $D_y g(a)$ est inversible donc selon le théorème des fonctions implicites, il existe un voisinage ouvert U de α, V un voisinage ouvert de β et $\varphi : U \to V$ de classe $\mathscr{C}^1$ tels que

$$((x, y) \in U \times V \quad \text{et} \quad g(x, y) = 0) \iff (x \in U \quad \text{et} \quad y = \varphi(x)).$$

En particulier, $\forall x \in U, (x, \varphi(x)) \in \Gamma$.

Introduisons $h : x \in U \mapsto f(x, \varphi(x))$. Par hypothèse, h est une fonction $\mathscr{C}^1$ admettant un extremum local en α. Donc

$$0 = Jh(\alpha) = Jf(a) \times \begin{pmatrix} I_s \\ J\varphi(\alpha) \end{pmatrix} = \begin{pmatrix} \frac{\partial f}{\partial x_1} \cdots \frac{\partial f}{\partial x_s} \cdots \frac{\partial f}{\partial y_1} \cdots \frac{\partial f}{\partial y_s} \end{pmatrix} \times \begin{pmatrix} I_s \\ J\varphi(\alpha) \end{pmatrix},$$

de sorte que

$$\forall i \in [\![1, r]\!], \frac{\partial f}{\partial x_i}(a) + \sum_{j=1}^{s} \frac{\partial f}{\partial y_j}(a) \times \frac{\partial \varphi_j}{\partial x_i}(\alpha) = 0. \tag{2.15}$$

Or, $\forall k \in [\![1, r]\!]$, $\forall x \in U, g_k(x, \varphi(x)) = 0$ donc on a une relation identique à (2.15) pour les g_k. Ainsi, si

$$M = \begin{pmatrix} \frac{\partial f}{\partial x_1} & \dots & \frac{\partial f}{\partial x_s} & \frac{\partial f}{\partial y_1} & \dots & \frac{\partial f}{\partial y_r} \\ \frac{\partial g_1}{\partial x_1} & \dots & \frac{\partial g_1}{\partial x_s} & \frac{\partial g_1}{\partial y_1} & \dots & \frac{\partial g_1}{\partial y_r} \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial g_r}{\partial x_1} & \dots & \frac{\partial g_r}{\partial x_s} & \frac{\partial g_r}{\partial y_1} & \dots & \frac{\partial g_r}{\partial y_r} \end{pmatrix},$$

les s premières lignes de M sont combinaisons linéaires des r dernières, donc le rang de M est inférieur à $n - s = r$. Par conséquent, les r premières lignes de M formant une famille libre par hypothèse, la première ligne est combinaison linéaire des r dernières, ce qui est le résultat voulu. □

Remarque.
- Il faut absolument (surtout dans la leçon 214) avoir une idée précise de l'interprétation géométrique du résultat. On remarque que Γ est une sous-variété de $\mathbb{R}^n$ de dimension r définie par la submersion g. Si $c :]-\varepsilon, \varepsilon[\to \Gamma$ est un chemin dérivable tel que $c(0) = a$, alors $f \circ c$ admet un extremum local en a donc $0 = (f \circ c)'(0) = df(a).c'(0)$ donc $T_a\Gamma \subset \ker df(a)$. Or, $T_a\Gamma = \ker \mathrm{d}g(a) = \bigcap_{i=1}^{r} \ker \mathrm{d}g_i(a)$ donc un raisonnement élémentaire d'algèbre linéaire nous indique que $df(a) \in \mathrm{Vect}(\mathrm{d}g_1(a), \dots, \mathrm{d}g_r(a))$. (compléter $(dg_1(a), \dots, dg_r(a))$ en une base de $(\mathbb{R}^n)^*$ et évaluer l'expression $\mathrm{d}f(a) = \sum_{i=1}^{n} \lambda_i \mathrm{d}g_i(a)$ sur la base antéduale).
- Le jury dit qu'il aime moins cette preuve matricielle, mais elle reste acceptable.
- Une application du théorème est donnée par la preuve de l'inégalité d'Hadamard ou l'inégalité arithmético-géométrique (ROUVIÈRE 2003), ou encore le théorème spectral (BECK, MALICK et PEYRÉ 2005).
  Développons cette dernière. Soit $(E, \langle \cdot, \cdot \rangle)$ un espace euclidien, $u \in \mathscr{L}(E)$ symétrique et $f : \begin{array}{ccc} E & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \langle u(x), x \rangle \end{array}$, $g : \begin{array}{ccc} E & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \langle x, x \rangle - 1 \end{array}$. Alors si S est la sphère unité de E, S est le lieu d'annulation de g. De plus, elle est compacte donc f continue admet un maximum sur S atteint en $e_1 \in S$.
  Selon le théorème des extréma liés, il existe $\lambda_1 \in \mathbb{R}$ tel que $\mathrm{d}f(e_1) = \lambda_1 \mathrm{d}g(e_1)$.
  Or, pour tous $x, h \in \mathbb{R}^n$, $\mathrm{d}g(x).h = 2\langle x, h \rangle$ et $\mathrm{d}f(x).h = 2\langle u(x), h \rangle$ car u est symétrique.
  Donc pour tout $h \in \mathbb{R}^n$, $\langle e_1, h \rangle = \lambda_1 \langle u(e_1), h \rangle$ donc $u(e_1) = \lambda_1 e_1$: u admet une valeur propre.

Références : GOURDON 2009b, p. 317 et ROUVIÈRE 2003, chapitre 7.

Théorème de sélection de Helly

Leçons : 203, 229, 241, *262*

Théorème 109

Si $(f_n)_{n\in\mathbb{N}}$ est une suite de fonctions croissantes de $\mathbb{R}$ dans $[0,1]$, il existe une sous-suite de (f_n) convergeant simplement vers $f : \mathbb{R} \to [0,1]$.

Démonstration.

- Par un procédé d'extraction diagonal on obtient le résultat préliminaire suivant : si $E \subset \mathbb{R}$ est un ensemble dénombrable et $(f_n)_n$ une suite de fonctions de E dans $[0,1]$, alors il existe une sous-suite de (f_n) convergeant simplement vers $f : E \to [0,1]$. En particulier avec $E = \mathbb{Q}$, quitte à extraire une sous-suite, on peut supposer que (f_n) converge simplement vers $f : \mathbb{Q} \to [0,1]$ sur $\mathbb{Q}$. Comme les f_n sont croissantes, f l'est également.
- Soit $x \in \mathbb{R}$. La fonction croissante f admet une limite à gauche l^- et à droite l^+ en x. Supposons que $l^- = l^+ = l$, montrons que $f_n(x) \to l$.
  Soit $\varepsilon > 0$, fixons $\eta > 0$ tel que
  $$\forall t \in \mathbb{Q} \cap [x-\eta, x+\eta], |f(t) - l| \leqslant \varepsilon.$$
  Soit $\alpha \in [x-\eta, x] \cap \mathbb{Q}$ et $\beta \in [x, x+\eta]$. On a $f_n(\alpha) \leqslant f_n(x) \leqslant f_n(\beta)$ et à partir d'un certain rang,
  $$l - 2\varepsilon \leqslant f(\alpha) - \varepsilon \leqslant f_n(\alpha) \leqslant f_n(x) \leqslant f_n(\beta) \leqslant f(\beta) + \varepsilon \leqslant l + 2\varepsilon.$$
  Donc $l - 2\varepsilon \leqslant f_n(x) \leqslant l + 2\varepsilon$ à partir d'un certain rang, de sorte que $(f_n(x))_n$ converge vers l.
- Montrons que l'ensemble D des points où la limite à gauche et à droite de f diffèrent est dénombrable. En effet, si $x \in D$, on peut fixer $q_x \in \mathbb{Q}$ tel que $l^-(x) < q_x < l^+(x)$. De plus, $x \mapsto q_x$ est injective car f est croissante, donc l^+ et l^- aussi. Ainsi, en utilisant à nouveau le résultat préliminaire avec $E = D$, on peut extraire une sous-suite de (f_n) convergeant simplement sur D. Comme (f_n) converge sur $\mathbb{R} \setminus D$, on a bien trouvé une sous-suite convergente sur $\mathbb{R}$.

□

Corollaire 110

Soit $(\mu_n)_{n\in\mathbb{N}}$ une suite de mesures de probabilités sur $(\mathbb{R}, \mathscr{B}(\mathbb{R}))$. Si $(\mu_n)_n$ est tendue, c'est-à-dire
$$\forall \varepsilon > 0, \exists M_\varepsilon > 0, \limsup(1 - \mu_n([-M_\varepsilon, M_\varepsilon])) \leqslant \varepsilon,$$
alors il existe une sous-suite de (μ_n) convergeant étroitement vers une mesure de probabilité μ.

Démonstration. Notons $(F_n)_{n\in\mathbb{N}}$ la suite de leurs fonctions de répartitions. Alors selon le théorème de Helly, il existe une fonction croissante $F : \mathbb{R} \to [-1,1]$ telle qu'une sous-suite $(F_{n_k})_{k\in\mathbb{N}}$ de (F_n) converge simplement vers G sur $\mathbb{R}$. Introduisons $F = \inf\{G(q), q > x\}$.

1 F est croissante.

2 F est continue à droite en tout point :

Soit $(x_n)_n$ suite décroissante convergeant vers x. Alors comme F est croissante,

$$\lim_{x_n \to x} F(x_n) = \inf_{n\in\mathbb{N}} F(x_n) = \inf\{G(q) \mid \exists n \in \mathbb{N} : q > x_n\} \overset{G \text{ croissante}}{=} \inf\{G(q) \mid q > x\} = F(x).$$

3 $(F_{n_k})_k$ converge vers F en tout point de continuité x de F :

Soit $\varepsilon > 0$, soient $r_1 < r_2 < x < s$ tels que

$$F(x) - \varepsilon < F(r_1) \leqslant F(r_2) \leqslant F(x) \leqslant F(s) \leqslant F(x) + \varepsilon.$$

On a $F_{n_k}(r_2) \xrightarrow[k\to+\infty]{} G(r_2) \geqslant F(r_1)$ et $F_{n_k}(s) \xrightarrow[k\to+\infty]{} G(s) \leqslant F(s)$ car G est croissante.

Donc si k est assez grand, $F_{n_k}(r_2) \geqslant F(r_1) - \varepsilon$ et $F_{n_k}(s) \leqslant F(s) + \varepsilon$. Ainsi, par les inégalités précédentes et la croissance de F_{n_k}, $F(x) - 2\varepsilon \leqslant F_{n_k}(x) \leqslant F(x) + 2\varepsilon$ à partir d'un certain rang.

4 $\lim_{x\to-\infty} F(x) = 0$ et $\lim_{x\to+\infty} F(x) = 1$:

Soit $\varepsilon > 0$ et $r < -M_\varepsilon, s > M_\varepsilon$ des points de continuité de F. Alors

$$1 - F(s) + F(r) = \lim_{k\to+\infty} 1 - F_{n_k}(s) + F_{n_k}(r) \leqslant \limsup_{n\to+\infty} 1 - F_n(M_\varepsilon) + F_n(-M_\varepsilon) \leqslant \varepsilon$$

car (μ_n) est tendue. En particulier, $0 \leqslant \limsup_{x\to+\infty} 1 - F(x) + F(-x) \leqslant \varepsilon$ donc, ceci valant pour tout $\varepsilon > 0$, $\lim_{x\to+\infty} 1 - F(x) + F(-x) = 0$, ce qui prouve le résultat.

Par le théorème des caractérisation des fonctions de répartition (points **1,2** et **4**), la fonction F est bien la fonction de répartition d'une mesure de probabilité μ. Selon le point **3**, il y a bien convergence étroite de (μ_n) vers μ.

□

Remarque.
- Le théorème de caractérisation des fonctions de répartition se trouve dans DURRETT 2010, p. 104. La clef de la preuve est de poser, F étant une fonction croissante continue à droite de limites 0 en $-\infty$, 1 en $+\infty$, $X(\omega) = \sup\{y : F(y) < \omega\}$ et de montrer que X est une variable aléatoire sur $\Omega = [0,1]$ de fonction de répartition F.
- La réciproque du corollaire est également vraie et se prouve de la même manière, par contraposée.
- S'il existe $\varphi \geqslant 0$ telle que $\varphi(x) \to +\infty$ et $\sup_n \int |\varphi(x)| \mathrm{d}\mu_n(x) < +\infty$, alors la suite (μ_n) est tendue.

Références : FRANCINOU, GIANELLA et NICOLAS 2009b, p. 166 et DURRETT 2010, pp. 103-104.

Théorème de structure des groupes abéliens finis

Leçons : 102, 104, 107, 110

Définition 111

Si G est un groupe abélien fini, son groupe dual est $\hat{G}$, ensemble des morphismes de groupes de G dans $\mathbb{C}^*$, muni de la multiplication. Les éléments de $\hat{G}$ sont appelés caractères linéaires.

On sait que les caractères linéaires sont associés à des représentations de degré 1 de G donc sont des caractères irréductibles. De plus, il y a autant de caractères irréductibles de G que de classes de conjugaison de G, en l'occurrence $|G|$. D'où $\mathrm{Irr}(G) = \hat{G}$.

Définition 112

L'exposant d'un groupe fini G est le plus petit N tel que $\forall g \in G, g^N = e$.

Théorème 113

Si G est un groupe abélien fini, et N_1 est l'exposant de G, il existe $N_2 | \dots | N_r$ tels que

$$G \simeq \mathbb{Z}/N_1\mathbb{Z} \times \dots \mathbb{Z}/N_r\mathbb{Z}.$$

Lemme 114

L'exposant N de g est égal à $\mathrm{ppcm}_{g\in G} o(g)$*. De plus, il existe un élément d'ordre N dans g.*

Démonstration. Il suffit de montrer que si x et y ont pour ordres respectifs n et m, il existe $z \in G$ d'ordre $\mathrm{ppcm}(n,m)$. Une récurrence immédiate fournira le résultat de l'énoncé.

La preuve ne pose pas de difficultés si n et m sont premiers entre eux. Dans le cas général, soit $k = \prod_{p|n, v_p(n)\geqslant v_p(m)} p^{v_p(n)}$ et $l = \prod_{v_p(m)>v_p(n)} p^{v_p(m)}$. Alors k et l n'ont aucun facteur premier commun, donc sont premiers entre eux. De plus, pour tout p premier,

$$v_p(kl) = \begin{cases} v_p(n) & \text{si} \quad v_p(n) \geqslant v_p(m) \\ v_p(m) & \text{si} \quad v_p(m) > v_p(n) \end{cases},$$

donc $kl = \mathrm{ppcm}(n,m)$. Donc comme $k|a$, $x' = x^{n/k}$ est d'ordre k et $y' = y^{m/l}$ est d'ordre l. Ainsi, comme k et l sont premiers entre eux, $x'y'$ est d'ordre $kl = \mathrm{ppcm}(n,m)$.

□

Lemme 115

Si G est un groupe abélien fini, $i : \begin{array}{ccc} G & \longrightarrow & \hat{\hat{G}} \\ g & \longmapsto & \mathrm{ev}_g : \chi \mapsto \chi(g) \end{array}$ est un isomorphisme de groupes.

Démonstration. Comme G et $\hat{\hat{G}}$ ont meme cardinal, il suffit de montrer que i est injectif. Soit $g \in G$ tel que $i(g) = 1$. Alors $\forall \chi \in \hat{G}, \chi(g) = 1$.

On sait que les caractères irréductibles, c'est-à-dire ici les éléments de $\hat{G}$, forment une base orthonormée de l'espace des fonctions centrales de G dans $\mathbb{C}$.

En particulier, $\mathbb{1}_g = \sum_{\chi\in\hat{G}} \langle \mathbb{1}_g, \chi\rangle \chi$ et pour χ caractère,

$$\langle \mathbb{1}_g, \chi\rangle = \frac{1}{|G|}\sum_{h\in G} \overline{\mathbb{1}_g(h)}\chi(h) = \frac{\chi(g)}{|G|} = \frac{1}{|G|}$$

puisque $\chi(g) = 1$.

D'où, en évaluant en l'élément neutre, $\mathbb{1}_g(e) = \sum_{\chi\in\hat{G}} \frac{\chi(e)}{|G|} = 1$ donc $g = e$. □

Démonstration (du théorème)**.** Remarquons tout d'abord qu'en vertu du lemme précédent, G et $\hat{G}$ ont même exposant. En effet si $\forall \chi \in \hat{G}, \chi^M = 1$, alors $\forall g \in G, \forall \chi \in \hat{G}, \chi(g^M) = 1$ d'où $g^M = 1$ donc l'exposant de G divise M. Symétriquement, on obtient que M divise l'exposant de G ce qui donne l'égalité voulue.

Montrons le théorème de structure par récurrence sur $|G|$. Il est évident pour $|G| = 1$, on suppose donc $|G| \geqslant 2$

Notons N_1 l'exposant de G et prenons $\chi_1 \in N_1$ d'ordre N_1. Son image $\chi_1(G)$ est donc un sous-groupe du groupe $\mathbb{U}_{N_1}$ des racines N_1-èmes de l'unité, donc de la forme $\mathbb{U}_l$ où $l|N_1$. Comme χ_1 est d'ordre N_1, on a $l = N_1$. En particulier, on peut se donner $x_1 \in G$ tel que

$$\chi_1(x_1) = \exp\left(\frac{2i\pi}{N_1}\right).$$

L'ordre de x_1 est N_1 et donc $H = \langle x_1\rangle$ est un sous-groupe cyclique d'ordre N_1 de G.

Montrons que $G \simeq H \times \ker\chi_1$.

- On a $\chi_1(H) = \chi_1(G)$ donc $\chi_{1|H}$ est injectif pour des raisons de cardinal. En d'autres termes, $H \cap \ker\chi_1 = \{e\}$.
- De plus, si $g \in G$, il existe $h \in H$ tel que $\chi_1(g) = \chi_1(h)$ donc $gh^{-1} \in \ker\chi_1$ ce qui assure que $G = H\ker\chi_1$.

Selon le théorème de factorisation en produit direct, on a $G \simeq H \times \ker\chi_1$.

Enfin, il est clair que l'exposant N_2 de $\ker\chi_1$ divise celui de G et par hypothèse de récurrence $\ker\chi_1 \simeq \mathbb{Z}/N_2\mathbb{Z} \times \ldots \mathbb{Z}/N_r\mathbb{Z}$ donc comme $H \simeq \mathbb{Z}/N_1\mathbb{Z}$, on a le résultat par récurrence. □

Référence : COLMEZ 2011, p. 252.

Théorème de Sylow

Leçons : 101, 103, 104

Soit p premier et G un groupe d'ordre $n = p^\alpha m$ où p ne divise pas m.

Définition 116

Un p-Sylow de G est un sous-groupe de G d'ordre p^α, ou bien de manière équivalente un p-sous-groupe maximal de G.

Théorème 117

Soit p premier et G un groupe d'ordre $p^\alpha m$ où $p \not| m$. Alors

1. *G admet au moins un p-Sylow.*
2. *Si H est un sous-groupe de G qui est un p-groupe, il existe un p-Sylow S de G contenant H.*
3. *Les p-Sylow sont tous conjugués et leur nombre k divise n.*
4. *$k \equiv 1[p]$ donc k divise m.*

Lemme 118

Si G admet un p-Sylow S et H est un sous-groupe de G d'ordre divisible par p, alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de G.

Démonstration. Le groupe G agit sur l'ensemble des classes à gauche modulo S, G/S, via $g \cdot (aS) = (ga)S$ (action par translation) et on vérifie sans mal que le stabilisateur de aS est aSa^{-1}. Donc H agit par restriction sur G/S et le stabilisateur de aS est $aSa^{-1} \cap H$. Fixons $a_1, \dots, a_r$ des représentants des orbites de cette action. Selon la formule des classes,

$$m = \frac{|G|}{|S|} = \sum_{i=1}^{r} \frac{|H|}{|a_i S a_i^{-1} \cap H|}$$

donc comme p ne divise pas m, il existe $i \in [\![1, r]\!]$ tel que p ne divise pas $\dfrac{|H|}{|a_i S a_i^{-1} \cap H|}$. Par conséquent, $a_i S a_i^{-1} \cap H$ est un p-Sylow de H. □

Démonstration. **1** Tout d'abord, remarquons qu'on peut supposer que G est un sous-groupe de $G' = \mathrm{GL}_n(\mathbb{F}_p)$. En effet,

$$\varphi : \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}_n \\ g & \longmapsto & (x \mapsto gx) \end{array} \qquad \text{et} \qquad \psi : \begin{array}{ccc} \mathfrak{S}_n & \longrightarrow & \mathrm{GL}(\mathbb{F}_p^n) \\ \sigma & \longmapsto & (e_i \mapsto e_{\sigma(i)}) \end{array}$$

(avec $(e_1, \dots, e_n)$ la base canonique de $\mathbb{F}_p^n$) sont des morphismes injectifs.

Or, l'ensemble T des matrices triangulaires supérieures de la forme $\begin{pmatrix} 1 & & \star \\ & \ddots & \\ (0) & & 1 \end{pmatrix}$ est de cardinal $p \times p^2 \times \cdots \times p^{n-1} = p^{n(n-1)/2}$, alors que $\mathrm{GL}_n(\mathbb{F}_p)$ est d'ordre

$$(p^n - 1) \times (p^n - p) \times \cdots \times (p^n - p^{n-1}) = p^{n(n-1)/2} \prod_{i=0}^{n-1} (p^{n-i} - 1)$$

donc T est un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$. Selon le lemme, G admet un p-Sylow.

2 Soit H sous-groupe de G d'ordre p^i, soit S p-Sylow de G. Selon le lemme, il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H. Mais H étant un p-groupe, on a $aSa^{-1} \cap H = H$. Par ailleurs, $aSa^{-1} \cap H \subset aSa^{-1}$, ce dernier groupe étant un p-Sylow de G puisqu'il est de même ordre que S. Donc H est bien contenu dans un p-Sylow de G.

3 Soit S' p-Sylow de G. Appliquons le raisonnement du **2** avec $H = S'$: on trouve que $S' = aSa^{-1} \cap S' \subset aSa^{-1}$; ainsi, grâce à l'égalité des cardinaux de part et d'autre, $S' = aSa^{-1}$: les p-Sylow sont tous conjugués. Par conséquent, si X est l'ensemble des p-Sylow de G, G agit transitivement par conjugaison sur X, de sorte que selon la relation orbite-stabilisateur, k divise n.

4 Si S est un p-Sylow de G, il agit sur X par restriction de l'action précédente. S étant un p-groupe, selon un résultat bien connu, si $X^S = \left\{S' \in X : \forall s \in S, sSs^{-1} = S'\right\}$, $|X| \equiv \left|X^S\right| [p]$.

Or, soit $T \in X^S$. Introduisons (c'est l'« argument de Frattini ») le sous-groupe N de G engendré par T et S. Le groupe T est distingué dans N par hypothèse, et de plus c'est un p-Sylow de N (puisque $N \subset G$). Donc T est l'unique p-Sylow de N selon le point **3**. Comme S est un p-Sylow de N, l'égalité $T = S$ s'ensuit, si bien que X^S est de cardinal 1. Donc $k = |X| \equiv 1[p]$.

Enfin, k divise m car $pk + 1$ et p sont premiers entre eux pour $k \in \mathbb{Z}$.

□

Corollaire 119

Il n'y a pas de groupe simple d'ordre 255.

Démonstration. Soit G d'ordre $255 = 3 \times 5 \times 17$. G admet $k_5 \equiv 1[5]$ p-Sylow d'ordre 5 et k_5 divise $3 \times 17 = 51$. Cela est impossible si $k_5 \neq 1$ (il suffit d'énumérer les premières valeurs possibles de k_5 pour s'en convaincre). Donc G admet un unique p-Sylow d'ordre 5 qui est donc un sous-groupe distingué.

□

Référence : PERRIN 1996, pp. 18-20.

Théorème de Weierstrass par les polynômes de Bernstein

Leçons : 202, 209, 228, 260, 264

Théorème 120

Soit $f : [0,1] \to \mathbb{C}$ continue et $B_n : x \mapsto \sum_{k=0}^{n} \binom{k}{n} x^k (1-x)^{n-k} f\left(\frac{k}{n}\right)$ le n-ième polynôme de Bernstein associé à f.

Soit $\omega : h \mapsto \sup\{|f(u)-f(v)|, |u-v| \leqslant h\}$ le module d'uniforme continuité de f. Alors

$$\|f - B_n\|_\infty \leqslant \frac{3}{2}\omega\left(\frac{1}{\sqrt{n}}\right)$$

donc $(B_n)_n$ converge uniformément vers f sur $[0,1]$.

L'inégalité est optimale dans le sens où il existe $f \in \mathscr{C}([0,1]$ et $\delta > 0$ telle que

$$\forall n \in \mathbb{N}^*, \|f - B_n\|_\infty \geqslant \delta\,\omega\left(\frac{1}{\sqrt{n}}\right).$$

Remarquons d'abord que ω est bien définie puisque, selon le théorème de Heine, f est uniformément continue sur $[0,1]$, ce qui assure de plus que $\omega(h) \xrightarrow[h\to 0]{} 0$.

Lemme 121

La fonction ω est croissante, sous-additive et pour tout $h \in [0,1]$, pour tout $\lambda \in \mathbb{R}_+$ tel que $\lambda h \in [0,1]$, on a $\omega(\lambda h) \leqslant (\lambda+1)\omega(h)$.

Démonstration. La croissance de ω est évidente.

Soient $h_1, h_2 \in [0,1]$ tels que $h_1 + h_2 \in [0,1]$. Soient $v > u$ tels que $v - u \leqslant h_1 + h_2$. S'il existe i tel que $v - u \leqslant h_i$, alors $|f(v) - f(u)| \leqslant \omega(h_i)$.

Sinon, on peut écrire

$$v - u = v - (u + h_1) + u + h_1 - u \quad \text{et} \quad 0 \leqslant v - (u + h_1) \leqslant h_1 + h_2 - h_1 \leqslant h_2$$

donc $|f(v) - f(u)| \leqslant \omega(h_2) + \omega(h_2)$.

On en déduit que $\omega(h_1 + h_2) \leqslant \omega(h_1) + \omega(h_2)$: ω est sous-additive.

Par une récurrence immédiate, on a pour tous $h \in [0,1]$ et $r \in \mathbb{N}$ tels que $rh \in [0,1]$, on a $\omega(rh) \leqslant r\omega(h)$.

Soit $\lambda \in \mathbb{R}_+$ tel que $\lambda h \in [0,1]$. Alors par croissance de ω, on a

$$\omega(\lambda h) \leqslant \omega\left((E(\lambda)+1)h\right) \leqslant (E(\lambda)+1)\omega(h) \leqslant (\lambda+1)\omega(h).$$

□

Démonstration (du théorème)**.** Soit $x \in [0,1]$ et $(X_i)_i$ une suite de variables aléatoires i.i.d. de loi $\mathscr{B}(x)$. Alors si $S_n = X_1 + \cdots + X_n$, on sait que S_n suit la loi binômiale $\mathscr{B}(x,n)$ et par théorème de transfert, $\mathbb{E}\left[f\left(\frac{S_n}{n}\right)\right] = B_n(x)$. Ainsi,

$$|f(x) - B_n(x)| \leqslant \mathbb{E}\left[\left|f(x) - f\left(\frac{S_n}{n}\right)\right|\right] \leqslant \mathbb{E}\left[\omega\left(\left|x - \frac{S_n}{n}\right|\right)\right].$$

Or, selon le lemme,

$$\omega\left(\left|x-\frac{S_n}{n}\right|\right)=\omega\left(\frac{1}{\sqrt{n}}\right)\times\left(\sqrt{n}\left|x-\frac{S_n}{n}\right|\right)\leqslant\left(\left|x-\frac{S_n}{n}\right|+1\right)\omega\left(\frac{1}{\sqrt{n}}\right).$$

Donc

$$|f(x)-B_n(x)|\leqslant\omega\left(\frac{1}{\sqrt{n}}\right)\left(\sqrt{n}\left\|x-\frac{S_n}{n}\right\|_1+1\right)\leqslant\omega\left(\frac{1}{\sqrt{n}}\right)\left(\sqrt{n}\left\|x-\frac{S_n}{n}\right\|_2+1\right).$$

Or, puisque $\mathbb{E}\left[\frac{S_n}{n}\right]=x$, on a, par indépendance des X_i,

$$\left\|x-\frac{S_n}{n}\right\|_2^2=\mathrm{Var}\left(\frac{S_n}{n}\right)=\frac{1}{n^2}\sum_{i=1}^{n}\mathrm{Var}(X_i)=\frac{1}{n^2}\sum_{i=1}^{n}x(1-x)=\frac{x(1-x)}{n}.$$

Donc finalement,

$$|f(x)-B_n(x)|\leqslant\omega\left(\frac{1}{\sqrt{n}}\right)(\sqrt{x(1-x)}+1)\leqslant\frac{3}{2}\omega\left(\frac{1}{\sqrt{n}}\right),$$

car si $x\in[0,1]$, $x\leqslant\frac{1}{2}$ ou $1-x\leqslant\frac{1}{2}$.

Prouvons maintenant l'optimalité de cette majoration. Soit $f(x)=\left|x-\frac{1}{2}\right|$. Par inégalité triangulaire renversée, on a $\omega(h)\leqslant h$ pour tout h.

Soient $X_1,\dots,X_n$ une suite de variables de Bernoulli de paramètre $\frac{1}{2}$ indépendantes, $\varepsilon_j=2X_j-1$ pour tout $j\in\mathbb{N}^*$ et $T_n=\sum_{j=1}^{n}\varepsilon_j=2S_n-n$. Les ε_j constituent une suite de variables de Rademacher indépendantes. De plus,

$$\|f-B_n\|_\infty\geqslant\left|f\left(\frac{1}{2}\right)-B_n\left(\frac{1}{2}\right)\right|=\left|B_n\left(\frac{1}{2}\right)\right|=\mathbb{E}\left|\frac{S_n}{n}-\frac{1}{2}\right|=\frac{1}{2n}\mathbb{E}[|T_n|].$$

Soit $Y=\prod_{j=1}^{n}\left(1+\frac{i}{\sqrt{n}}\varepsilon_j\right)$. En utilisant l'inégalité $e^x\geqslant 1+x$, on obtient

$$|Y|=\prod_{j=1}^{n}\sqrt{1+\frac{\varepsilon_j^2}{n}}\leqslant\prod_{j=1}^{n}\sqrt{1+\frac{1}{n}}\leqslant\prod_{j=1}^{n}\sqrt{e^{1/n}}=\exp\left(\frac{1}{2}\sum_{j=1}^{n}\frac{1}{n}\right)=\sqrt{e}.$$

Donc $|\mathbb{E}[T_nY]|\leqslant\sqrt{e}\mathbb{E}[|T_n|]$

Mais par ailleurs, les ε_j étant indépendantes et centrées,

$$\begin{aligned}\mathbb{E}[T_nY]&=\sum_{j=1}^{n}\mathbb{E}[\varepsilon_j\left(1+\frac{i}{\sqrt{n}}\varepsilon_j\right)\prod_{k\neq j}\left(1+\frac{i}{\sqrt{n}}\varepsilon_k\right)\\&=\sum_{j=1}^{n}\mathbb{E}[\varepsilon_j]\prod_{k\neq j}\left(1+\frac{i}{\sqrt{n}}\mathbb{E}[\varepsilon_k]\right)+\frac{i}{\sqrt{n}}\mathbb{E}[\varepsilon_j^2]\prod_{k\neq j}\left(1+\frac{i}{\sqrt{n}}\mathbb{E}[\varepsilon_k]\right)\\&=\sum_{j=1}^{n}\frac{i}{\sqrt{n}}=i\sqrt{n}\end{aligned}$$

Donc $\sqrt{n}\leqslant\sqrt{e}\mathbb{E}[|T_n|]$ de sorte que $\|f-B_n\|_\infty\geqslant\sqrt{\frac{n}{e}}\times\frac{1}{2n}\geqslant\frac{1}{2\sqrt{e}}\omega\left(\frac{1}{\sqrt{n}}\right)$.

□

Remarque. On se ramène au théorème de Weierstrass sur un intervalle quelconque $[a, b]$ en posant pour $f : [a, b] \to \mathbb{C}$ continue, $\tilde{f} : x \mapsto f(a + (b - a)x)$.

Référence : QUEFFÉLEC et ZUILY 2013, p. 518.

Bibliographie

AIGNER, Martin et Günter M. ZIEGLER (2013). *Raisonnements divins : Quelques démonstrations mathématiques particulièrement élégantes*. Springer Paris.

ALLAIRE, Grégoire (2005). *Analyse numérique et optimisation*. Editions de l'Ecole Polytechnique.

AMAR, Eric et Etienne MATHERON (2003). *Analyse complexe*. Cassini.

AUDIN, Michèle (2006). *Géométrie*. EDP Sciences.

BARBÉ, Philippe et Michel LEDOUX (2007). *Probabilité*. EDP Sciences.

BAYEN, François et Christian MARGARIA (1986). *Problèmes de mathématiques appliquées, tome 2 : espaces de Hilbert et opérateurs*. Ellipses.

BECK, Vincent, Jérome MALICK et Gabriel PEYRÉ (2005). *Objectif agrégation*. 2e éd. H et K.

BERHUY, Grégory (2012). *Modules : théorie, pratique...Et un peu d'arithmétique !* Calvage et Mounet.

BONY, Jean-Michel (2001). *Cours d'analyse - Théorie des distributions et analyse de Fourier*. Ellipses.

BRÉZIS, Haim (2005). *Analyse fonctionnelle*. Dunod.

BRIANE, Marc et Gilles PAGÈS (2006). *Théorie de l'intégration : cours et exercices*. 4e éd. Vuibert.

CALAIS, Josette (1998). *Eléments de théorie des groupes*. 2e éd. Presses universitaires de France.

CALDERO, Philippe et Jérome GERMONI (2013). *Histoires hédonistes de groupes et de géométrie*. T. 1. Calvage et Mounet.

— (2015). *Histoires hédonistes de groupes et de géométrie*. T. 2. Calvage et Mounet.

CARTAN, Henri (1967). *Calcul différentiel*. Hermann.

CIARLET, Philippe (1988). *Introduction à l'analyse numérique et à l'optimisation*. Masson.

COLMEZ, Pierre (2011). *Eléments d'analyse et d'algèbre (et de théorie des nombres)*. Ecole Polytechnique.

COMBES, François (1998). *Algèbre et géométrie*. Bréal.

CORMEN, Thomas et al. (2010). *Algorithmique*. 3e éd. Dunod.

DE BIASI, Jean (1998). *Mathématiques pour le CAPES et l'agrégation interne*. Ellipses.

DE SEGUINS PAZZIS, Clément (2011). *Invitation aux formes quadratiques*. Calvage et Mounet.

DEMAILLY, Jean-Pierre (2006). *Analyse numérique et équations différentielles*. EDP Sciences.

DEMAZURE, Michel (2008). *Cours d'algèbre*. Cassini.

DOLECKI, Szymon (2011). *Analyse fondamentale*. Hermann.

DURRETT, Rick (2010). *Probability : Theory and Examples*. 4e éd. Cambridge Series in Statistical and Probabilistic Mathematics. Cambridge University Press.

DUVERNEY, Daniel (2007). *Théorie des nombres*. 2e éd. Dunod.

EL AMRANI, Mohammed (2011). *Suites et séries numériques, suites et séries de fonctions*. Ellipses.

FOATA, Dominique et Aimé FUCHS (2003). *Calcul des probabilités*. Dunod.

— (2004). *Processus stochastiques : processus de Poisson, chaînes de Markov et martingales*. Dunod.

FRANCINOU, Serge, Hervé GIANELLA et Serge NICOLAS (2007a). *Exercices de mathématiques – Oraux X-ENS : Algèbre 1*. Cassini.
— (2007b). *Exercices de mathématiques – Oraux X-ENS : Analyse 1*. Cassini.
— (2008). *Exercices de mathématiques – Oraux X-ENS : Algèbre 3*. Cassini.
— (2009a). *Exercices de mathématiques – Oraux X-ENS : Algèbre 2*. Cassini.
— (2009b). *Exercices de mathématiques – Oraux X-ENS : Analyse 2*. Cassini.
— (2009c). *Exercices de mathématiques – Oraux X-ENS : Analyse 4*. Cassini.
GOBLOT, Rémi (2001). *Algèbre commutative*. 2e éd. Dunod.
GONNORD, Rémi et Nicolas TOSEL (1998). *Thèmes d'analyse pour l'agrégation : calcul différentiel*. Ellipses.
GOURDON, Xavier (2009a). *Les maths en tête : algèbre*. 2e éd. Ellipses.
— (2009b). *Les maths en tête : analyse*. 2e éd. Ellipses.
GOZARD, Yvan (1997). *Théorie de Galois*. Ellipses.
GRIFONE, Joseph (2011). *Algèbre linéaire*. 4e éd. Editions Cépaduès.
HAUCHECORNE, Bertrand (2007). *Les contre-exemples en mathématique*. Ellipses.
HIRIART-URRUTY, Jean-Baptiste et Claude LEMARÉCHAL (1993). *Convex Analysis and Minimization Algorithms I : Fundamentals*. Grundlehren der mathematischen Wissenschaften 305. Springer-Verlag Berlin Heidelberg.
HIRSCH, Francis et Gilles LACOMBE (2009). *Analyse fonctionnelle*. Dunod.
JEANNERET, Alain et Daniel LINES (2008). *Invitation à l'algèbre*. Editions Cépaduès.
LAFONTAINE, Jacques (1997). *Introduction aux variétés différentielles*. Presses Universitaires de Grenoble.
LAX, Peter (2007). *Linear algebra and its applications*. 2e éd. Wiley Intersciences.
LESFARI, Ahmed (2012). *Distributions, analyse de Fourier et transformation de Laplace*. Ellipses.
MANSUY, Roger et Rached MNEIMNÉ (2012). *Réduction des endomorphismes*. Vuibert.
MERCIER, Dany-Jack (2008). *Cours de géométrie, préparation au CAPES et à l'agrégation*.
MÉRINDOL, Jean-Yves (2006). *Nombres et algèbre*. EDP Sciences.
MNEIMNÉ, Rached et Frédéric TESTARD (1986). *Introduction à la théorie des groupes de Lie classiques*. Hermann.
NOURDIN, Ivan (2006). *Agrégation de mathématiques, épreuve orale. 68 thèmes pour se préparer efficacement*. Dunod.
OUVRARD, Jean-Yves (2007). *Probabilités (Licence CAPES)*. T. 1. Cassini.
— (2009). *Probabilités (Master Agrégation)*. T. 2. Cassini.
PERRIN, Daniel (1996). *Cours d'algèbre*. Ellipses.
PEYRÉ, Gabriel (2004). *L'algèbre discrète de la transformée de Fourier*. Ellipses.
POMMELLET, Alain (1997). *Cours d'Analyse*. Ellipses.
QUARTERONI, Alfio, Ricardo SACCO et Fausto SALERI (2007). *Méthodes numériques : Algorithmes, analyse et applications*. Springer.
QUEFFÉLEC, Hervé (1998). *Topologie*. Dunod.
QUEFFÉLEC, Hervé et Claude ZUILY (2013). *Analyse pour l'agrégation*. 4e éd. Dunod.
RAMIS, Edouard, Claude DESCHAMPS et Jacques ODOUX (1990). *Cours de mathématiques spéciales*. T. 1. Dunod.
— (1995). *Cours de mathématiques spéciales*. T. 3. Dunod.
RISLER, Jean-Jacques et Pascal BOYER (2006). *Algèbre pour la licence 3. Groupes, anneaux, corps.* Dunod.
ROMBALDI, Jean-Etienne (2004). *Eléments d'analyse pour le Capes et l'Agrégation de Mathématiques*. EDP Sciences.
ROUVIÈRE, François (2003). *Petit guide de calcul différentiel*. 2e éd. Cassini.
RUDIN, Walter (1970). *Real and complex analysis*. 3e éd. McGraw-Hill series in higher mathematics. ; International student edition. McGraw-Hill.

SAINT-RAYMOND, Jean (2008). *Topologie, calcul différentiel et variable complexe*. Calvage et Mounet.
SAMUEL, Pierre (1967). *Théorie algébrique des nombres*. Hermann.
SERRE, Jean-Pierre (1994). *Cours d'arithmétique*. Presses universitaires de France.
— (1998). *Représentations linéaires des groupes finis*. 5e éd. Hermann.
SZPIRGLAS, Aviva (2009). *Mathématiques L3*. Pearson Education.
TAUVEL, Patrice (2005a). *Algèbre*. 2e éd. Dunod.
— (2005b). *Géométrie*. 2e éd. Dunod.
— (2006). *Analyse complexe pour la Licence 3*. Dunod.
— (2008). *Corps commutatifs et théorie de Galois*. Calvage et Mounet.
TENENBAUM, Gerald (2015). *Introduction à la théorie probabiliste et analytique des nombres*. 4e éd. Belin.
ULMER, Felix (2012). *Théorie des groupes*. Ellipses.
WILLEM, Michel (1995). *Analyse harmonique réelle*. Hermann.
— (2003). *Analyse fonctionnelle élémentaire*. Cassini.
ZAVIDOVIQUE, Maxime (2013). *Un max de maths*. Calvage et Mounet.
ZUILY, Claude (1986). *Distributions et équations aux dérivées partielles*. Hermann.