Mes Développements d'Agrégation

Adrien Laurent
École Normale Supérieure de Rennes

2015 - 2016

Table des matières

Introduction

Voici les développements que j'ai préparé pendant mon année d'agrégation.
Je remercie tous mes camarades de classe qui m'ont aidé à les écrire, à les corriger et à les apprendre.
J'ai utilisé certains développements et beaucoup d'idées de ceux-ci, je le préciserai à chaque fois que cela arrive (même si j'ai souvent ajouté ma touche personnelle à leur travail !).
Je trouve important de préciser que ce fichier est le fruit d'un grand travail de groupe dont je ne suis que l'humble transcripteur.

Il est assez difficile de savoir ce qui est attendu des candidats en matière de développements : faut-il faire un développement didactique et compréhensible ou montrer qu'on sait faire des choses complexes ?
La question se pose car l'agrégation est un concours d'enseignement et l'état actuel de l'épreuve rend plutôt compte d'une course vers des développements complexes que l'on présente sans rien expliquer mais plutôt en faisant des ellipses pour tenir en 15 minutes.
Je pense qu'il sera apprécié du candidat qu'il fasse des développements complexes et rares mais il est aussi important que celui-ci montre ses compétences pédagogiques au jury via des exemples simples, des applications, des dessins... C'est pourquoi je me suis efforcé de présenter pour chaque développement des petites remarques permettant de comprendre un peu mieux les résultats prouvés. Je suis persuadé que celles-ci peuvent faire la différence le jour de l'oral entre un bête rabâchage et un exposé réussi.

Aux agrégatifs qui lisent ces lignes, je dis BON COURAGE !
Aux autres lecteurs, je souhaite une bonne lecture et j'espère que vous trouverez ici ce que vous cherchez.

PS : Je tiens à préciser que ce fichier contient beaucoup de développements complexes. Je conseille donc au lecteur de bien s'approprier les notions associées à ceux-ci avant de les adopter. Certains développements me paraissent toujours dangereux même après avoir passé des heures dessus (le théorème de Pascal ou les polygones réguliers constructibles par exemple).

Première partie

Couplages

Chapitre 1

Couplages d'algèbre

101 - Groupe opérant sur un ensemble. Exemples et applications.
Groupes paveurs
Cône nilpotent
Théorème de Molien
Sous-groupes finis de $SO_3(\mathbb{R})$

102 - Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.
Polygones réguliers constructibles
Théorème de structure des groupes abéliens finis
Transformée de Fourier rapide
Irréductibilité de Φ_n sur $\mathbb{Z}$

103 - Exemples et applications des notions de sous-groupes distingués et de groupes quotients.
Frobenius-Zolotarev
Simplicité de SO_3

104 - Groupes finis. Exemples et applications.
Sous-groupes finis de $SO_3(\mathbb{R})$
Théorème de structure des groupes abéliens finis
Théorème de Molien

105 - Groupe des permutations d'un ensemble fini. Applications.
Sous-groupes finis de $SO_3(\mathbb{R})$
Table de $\mathcal{S}_4$
Frobenius-Zolotarev

106 - Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.
Théorème de Cartan Von Neumann
Sous-groupes finis de $SO_3(\mathbb{R})$
Étude de $O(p,q)$
Théorème de Frobenius-Zolotarev

107 - Représentations et caractères d'un groupe fini sur un $\mathbb{C}$-espace vectoriel.
Théorème de structure des groupes abéliens finis
Table de $\mathcal{S}_4$
Théorème de Molien

108 - Exemples de parties génératrices d'un groupe.
Groupe circulaire
$SO_3(\mathbb{R})$ est simple

109 - Représentations de groupes finis de petit cardinal.
Théorème de structure des groupes abéliens finis
Table de $\mathcal{S}_4$

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

Théorème de structure des groupes abéliens finis
Transformée de Fourier rapide
Étude du θ-schéma pour l'équation de la chaleur

120 - Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
Chevalley-Warning+EGZ
Théorème de Frobenius-Zolotarev
Polynômes irréductibles de $\mathbb{F}_q$
Théorème de structure des groupes abéliens finis

121 - Nombres premiers. Applications.
Polygones réguliers constructibles
Chevalley-Warning+EGZ
Polynômes irréductibles de $\mathbb{F}_q$
Théorème de Frobenius-Zolotarev

122 - Anneaux principaux. Exemples et applications.
$\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais non euclidien
Irréductibilité des polynômes cyclotomiques
Équation de Nagell-Ramanujan

123 - Corps finis. Applications.
Chevalley-Warning+EGZ
Polynômes irréductibles de $\mathbb{F}_q$
Théorème de Frobenius-Zolotarev

124 - Anneau des séries formelles. Applications.
Théorème de Molien
Partitions d'un entier en parts fixées

125 - Extensions de corps. Exemples et applications.
Polygones réguliers constructibles
Polynômes irréductibles de $\mathbb{F}_q$
Automorphismes de $\mathbb{K}(X)$

126 - Exemples d'équations diophantiennes.
Équation de Nagell-Ramanujan
Équation de Pell-Fermat
Partitions d'un entier en parts fixées

127 - Droite projective et birapport.
Théorème de Pascal
Groupe circulaire

140 - Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.
Automorphismes de $\mathbb{K}(X)$
Partitions d'un entier en parts fixées

141 - Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
Polygones réguliers constructibles
Polynômes irréductibles de $\mathbb{F}_q$
Irréductibilité des polynômes cyclotomiques

142 - Algèbre des polynômes à plusieurs indéterminées. Applications.
Borne de Bézout
Chevalley-Warning+EGZ
Théorème de Molien

143 - Résultant. Applications.
Borne de Bézout

Théorème d'extension

144 - Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.
Chevalley-Warning+EGZ
Borne de Bézout

150 - Exemples d'actions de groupes sur les espaces de matrices.
Cône nilpotent
Étude de $\mathrm{O}(p,q)$
Théorème de réduction des endomorphismes normaux

151 - Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.
Théorème de Molien
Polygones réguliers constructibles

152 - Déterminant. Exemples et applications.
Borne de Bézout
Ellipsoïde de John-Loewner
Théorème de Frobenius-Zolotarev

153 - Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.
Image de l'exponentielle
Décomposition de Dunford
Théorème de réduction des endomorphismes normaux
Théorème de Liapounov

154 - Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.
Théorème de réduction des endomorphismes normaux
Cône nilpotent
Décomposition de Dunford

155 - Endomorphismes diagonalisables en dimension finie.
Théorème de réduction des endomorphismes normaux
Décomposition de Dunford

156 - Exponentielle de matrices. Applications.
Étude de $\mathrm{O}(p,q)$
Théorème de Cartan-Von Neumann
Image de l'exponentielle

157 - Endomorphismes trigonalisables. Endomorphismes nilpotents.
Décomposition de Dunford
Cône nilpotent

158 - Matrices symétriques réelles, matrices hermitiennes.
Étude de $\mathrm{O}(p,q)$
Lemme de Morse
Ellipsoïde de John Loewner

159 - Formes linéaires et dualité en dimension finie. Exemples et applications.
Transformée de Fourier rapide
Théorème des extrema liés

160 - Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).
Points extrémaux de la boule unité de $\mathcal{L}(E)$
Théorème de réduction des endomorphismes normaux
Simplicité de SO_3

Ellipsoïde de John-Loewner

161 - Isométries d'un espace affine euclidien de dimension finie. Applications en dimensions 2 et 3.
Groupes paveurs
Points extrémaux de la boule unité de $\mathcal{L}(E)$
Sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$
$\mathrm{SO}_3(\mathbb{R})$ est simple

162 - Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques.
Méthode de gradient à pas optimal
Méthode de Kacmarz

170 - Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.
Lemme de Morse
Étude de $\mathrm{O}(p,q)$
Ellipsoïde de John-Loewner

171 - Formes quadratiques réelles. Exemples et applications.
Lemme de Morse
Étude de $\mathrm{O}(p,q)$
Ellipsoïde de John-Loewner

180 - Coniques. Applications.
Théorème de Pascal
Équation de Pell-Fermat

181 - Barycentres dans un espace affine réel de dimension finie, convexité. Applications.
Points extrémaux de la boule unité de $\mathcal{L}(E)$
Méthode de gradient à pas optimal

182 - Applications des nombres complexes à la géométrie.
Polygones réguliers constructibles
Groupe circulaire

183 - Utilisation des groupes en géométrie.
Groupes paveurs
Groupe circulaire
Polygones réguliers constructibles

190 - Méthodes combinatoires. Problèmes de dénombrement.
Sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$ Irréductibles de $\mathbb{F}_q$
Cône nilpotent
Partitions d'un entier en parts fixées
Groupes paveurs

Chapitre 2

Couplages d'analyse

201 - Espaces de fonctions : exemples et applications.
Espace de Bergman
Théorème de Grothendieck

202 - Exemples de parties denses et applications.
Espace de Bergman
Théorème de Weierstrass
Résolution de l'équation de la chaleur

203 - Utilisation de la notion de compacité.
Ellipsoïde de John Loewner
Théorèmes de Schauder et de Cauchy-Arzela-Peano
Théorème d'Ascoli

204 - Connexité. Exemples et applications.
Surjectivité de l'exponentielle
Théorème de Cauchy-Lipschitz
$SO_3(\mathbb{R})$ est simple.

205 - Espaces complets. Exemples et applications.
Espace de Bergman
Théorème de Cauchy-Lipschitz

206 - Théorèmes de point fixe. Exemples et applications.
Théorèmes de Schauder et de Cauchy-Arzela-Peano
Théorème de Cauchy-Lipschitz
Méthode de la sécante
Méthode de gradient à pas optimal

207 - Prolongement de fonctions. Exemples et applications.
Théorèmes d'Abel angulaire et taubérien faible
Théorème de Cauchy-Lipschitz

208 - Espaces vectoriels normés, applications linéaires continues. Exemples.
Espace de Bergman
Théorème de Grothendieck

209 - Approximation d'une fonction par des polynômes et des polynômes trigonométriques. Exemples et applications.
Théorème de Weierstrass
Équation de la chaleur

213 - Espaces de Hilbert. Bases hilbertiennes. Exemples et applications.
Espace de Bergman
Théorème de Grothendieck

214 - Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications.
Théorème de Cartan Van Neumann
Lemme de Morse
Théorème des extrema liés

215 - Applications différentiables définies sur un ouvert de $\mathbb{R}^n$. Exemples et applications.
Théorème de Cartan Van Neumann
Méthode de gradient à pas optimal
Lemme de Morse
Théorème des extrema liés

217 - Sous variétés de $\mathbb{R}^n$. Exemples.
Théorème de Cartan Van Neumann
Lemme de Morse

218 - Applications des formules de Taylor.
Étude du θ-schéma pour l'équation de la chaleur
Lemme de Morse
Méthode de Laplace
Méthode de la sécante
TCL

219 - Extremums : existence, caractérisation, recherche. Exemples et applications.
Méthode de gradient à pas optimal
Ellipsoïde de John-Loewner
Méthode de la sécante

220 - Équations différentielles $X' = f(t, X)$. Exemples d'étude des solutions en dimension 1 et 2.
Théorèmes de Schauder et de Cauchy-Arzela-Peano
Théorème de Cauchy-Lipschitz
Équation de Hill-Mathieu
Théorème de Lyapounov

221 - Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.
Théorème de Lyapounov
Équation de Hill-Mathieu

222 - Exemples d'équations aux dérivées partielles linéaires.
Étude du θ-schéma pour l'équation de la chaleur
Solution élémentaire de l'équation de Schrödinger
Équation de la chaleur

223 - Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.
Méthode de la sécante
Méthode des petits pas

224 - Exemples de développements asymptotiques de suites et de fonctions.
Méthode de Laplace
Quelques ordres moyens
Méthode des petits pas

226 - Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples et applications.
Méthode de la sécante
Méthode des petits pas
Étude du θ-schéma pour l'équation de la chaleur
Méthode de gradient à pas optimal

228 - Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et contre-exemples.
Théorème de Weierstrass

Méthode de la sécante
Théorème d'Ascoli

229 - Fonctions monotones. Fonctions convexes. Exemples et applications.
Méthode de gradient à pas optimal
Ellipsoïde de John Loewner
Inégalité de Hoeffding

230 - Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.
Théorèmes d'Abel et taubérien faible
Quelques ordres moyens

232 - Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Exemples.
Méthode de la sécante
Méthode de gradient à pas optimal

233 - Analyse numérique matricielle : résolution approchée de systèmes linéaires, recherche de vecteurs propres, exemples.
Étude du θ-schéma pour l'équation de la chaleur
Méthode de gradient à pas optimal
Méthode de la sécante

234 - Espaces L^p, $1 \leqslant p \leqslant +\infty$.
Espace de Bergman
Théorème de Grothendieck

235 - Problèmes d'interversion de limites et d'intégrales.
Méthode de Laplace
Solution élémentaire de l'équation de Schrödinger
Espace de Bergman
Théorèmes d'Abel angulaire et taubérien faible

236 - Illustrer par des exemples quelques méthodes d'intégration des fonctions d'une ou plusieurs variables réelles.
Solution élémentaire de l'équation de Schrödinger
Formule des compléments

239 - Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.
Solution élémentaire à l'équation de Schrödinger
Méthode de Laplace

240 - Produit de convolution, transformation de Fourier. Applications.
Solution élémentaire à l'équation de Schrödinger
Formule sommatoire de Poisson

241 - Suites et séries de fonctions. Exemples et contre-exemples.
Équation de la chaleur
Théorème de Weierstrass
Théorème d'Abel angulaire et taubérien faible

243 - Convergence des séries entières, propriétés de la somme. Exemples et applications.
Espace de Bergman
Théorèmes d'Abel angulaire et taubérien faible
Partitions d'un entier en parts fixées

244 - Fonctions développables en série entière, fonctions analytiques. Exemples.
Espace de Bergman
Théorèmes d'Abel angulaire et taubérien faible
Partitions d'un entier en parts fixées

245 - Fonctions holomorphes sur un ouvert de C. Exemples et applications.
Espace de Bergman
Formule des compléments

246 - Séries de Fourier. Exemples et applications.
Équation de la chaleur
Formule sommatoire de Poisson

247 - Exemples de problèmes d'interversion de limites.
Méthode de Laplace
Théorèmes d'Abel angulaire et taubérien faible
Espace de Bergman

249 - Suites de variables de Bernoulli indépendantes.
Théorème de Weierstrass
Modélisation de suites de variables aléatoires indépendantes

253 - Utilisation de la notion de convexité en analyse.
Méthode du gradient à pas optimal
Théorèmes de Schauder et de Cauchy-Arzela-Peano
Inégalité de Hoeffding
Point fixe de Schauder

254 - Espaces de Schwartz $\mathcal{S}(\mathbb{R}^d)$ et distributions tempérées. Dérivation et transformation de Fourier dans $\mathcal{S}(\mathbb{R}^d)$ et $\mathcal{S}'(\mathbb{R}^d)$.
Solution élémentaire à l'équation de Schrödinger
Formule sommatoire de Poisson

260 - Espérance, variance et moments de variables aléatoires.
TCL
Théorème de Stone Weierstrass
Inégalité de Hoeffding

261 - Fonction caractéristique et transformée de Laplace d'une variable aléatoire. Exemples et applications.
TCL
Inégalité de Hoeffding

262 - Modes de convergence d'une suite de variables aléatoires. Exemples et applications.
TCL
Inégalité de Hoeffding

263 - Variables aléatoires à densité. Exemples et applications.
TCL
Modélisation de suites de variables aléatoires indépendantes

264 - Variables aléatoires discrètes. Exemples et applications.
Théorème de Weierstrass
Modélisation de suites de variables aléatoires indépendantes

Deuxième partie

Développements

Chapitre 1

Automorphismes de $\mathbb{K}(X)$

Références : Francinou, Gianella, Nicolas, *Oraux X-ENS - Algèbre 1*, 5.54
Francinou, Gianella, *Exercices de mathématiques pour l'agrégation - Algèbre 1*, 5.15

Théorème.

Les automorphismes de la $\mathbb{K}$-algèbre $\mathbb{K}(X)$ sont les homographies (ie les éléments de $\mathrm{PGL}_2(\mathbb{K})$).

Démonstration. • On pose Φ un tel automorphisme, et $F = \Phi(X)$, alors on remarque que si $P = \sum a_k X^k$, on a $\Phi(P) = \sum a_k \Phi(X)^k = P \circ F$.
Soit maintenant $G = \dfrac{P}{Q} \in \mathbb{K}(X)$, on a $\Phi(P) = \Phi\left(\dfrac{P}{Q} \times Q\right) = \Phi\left(\dfrac{P}{Q}\right)\Phi(Q)$.
On en déduit $\Phi(G) = \dfrac{\Phi(P)}{\Phi(Q)} = \dfrac{P \circ F}{Q \circ F} = G \circ F$.
Dans la suite, on note $\Phi_F : G \mapsto G \circ F$ le morphisme de $\mathbb{K}$-algèbre précédent. On va chercher sous quelles conditions sur F, Φ_F est un automorphisme.

• Si Φ_F est un automorphisme, en particulier, il existe $G = \dfrac{P}{Q}$ (avec $P \wedge Q = 1$) tel que $\Phi_F(G) = X$. On note $F = \dfrac{A}{B}$ avec $A \wedge B = 1$. [1]
Si on note $P = \sum_{j=0}^{p} a_j X^j$ et $Q = \sum_{k=0}^{q} b_k X^k$ (avec p et q les degrés de P et Q), on peut transformer $G \circ F = X$ en $P \circ F = X(Q \circ F)$, puis en $\sum_{j=0}^{p} a_j F^j = X \sum_{k=0}^{q} b_k F^k$.
On a donc $\sum_{j=0}^{p} a_j \dfrac{A^j}{B^j} = X \sum_{k=0}^{q} b_k \dfrac{A^k}{B^k}$, puis en notant $m = \max(p, q)$, on obtient $\sum_{j=0}^{p} a_j A^j B^{m-j} = X \sum_{k=0}^{q} b_k A^k B^{m-k}$.

• Avec l'égalité précédente, on obtient en particulier que $A | (a_0 - b_0 X) B^m$, donc par Gauss, $A | a_0 - b_0 X$. Le couple (a_0, b_0) n'est pas nul, sinon $X | P$ et $X | Q$, donc $P \wedge Q \neq 1$.
On a donc $\deg(A) \leqslant 1$.

• On opère maintenant le même travail pour les puissances maximales de notre égalité.

— Si $m = q = p$, alors $B | a_p - b_p X$ et le couple (a_p, b_p) est non nul car p est le degré exact de A et B.
— Si $m = q > p$, $B | b_q X$ et $b_q \neq 0$.
— Si $m = p > q$, $B | a_p$ et $a_p \neq 0$.
Dans tous les cas, $\deg(B) \leqslant 1$.
On en déduit que F est de la forme $F = \dfrac{aX + b}{cX + d}$. Puis comme F ne peut être constant (sinon Φ_F n'est pas surjectif), on a $\dfrac{a}{c} \neq \dfrac{b}{d}$, c'est à dire $ad - bc \neq 0$.

1. Choisir des représentants irréductibles est possible car F et G ne peuvent être nuls, sinon Φ n'est pas un automorphisme.

• Réciproquement, montrons que Φ_F est un automorphisme si F est une homographie. On note dorénavant $\Phi\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ pour $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{K})$ (équivalent à dire $ad - bc \neq 0$), le morphisme qui à X associe $\dfrac{aX+b}{cX+d}$.
On remarque alors que pour deux matrices M et N inversibles, on a $\Phi_M \circ \Phi_N = \Phi_{NM}$. Donc comme les matrices sont inversibles, on connaît l'inverse de Φ_M : c'est $\Phi_{M^{-1}}$.
On vient donc de montrer que $\Phi\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ était bien un automorphisme.

→ L'ensemble des automorphismes d'algèbre de $\mathbb{K}(X)$ est donc l'ensemble des Φ_M avec $M \in \mathrm{GL}_2(\mathbb{K})$.

• Francinou-Gianella : on a même montré mieux !
Introduisons l'application $\varphi : \begin{array}{ccc} \mathrm{GL}_2(\mathbb{K}) & \longrightarrow & \mathrm{Gal}(\mathbb{K}(X):\mathbb{K}) \\ M & \longmapsto & \Phi_{M^{-1}} \end{array}$ avec la notation $\mathrm{Gal}(\mathbb{K}(X):\mathbb{K})$ pour désigner l'ensemble des $\mathbb{K}$-automorphismes de la $\mathbb{K}$-algèbre $\mathbb{K}(X)$.
On remarque que $\varphi(I_2) = Id_{\mathbb{K}(X)}$, donc par le travail précédent, φ est un morphisme de groupes surjectif. [2]
De plus, son noyau est $\mathbb{K}^* I_2$. Le premier théorème d'isomorphisme donne alors

$$\mathrm{Gal}(\mathbb{K}(X):\mathbb{K}) \simeq \mathrm{GL}_2(\mathbb{K})/\mathbb{K}^* I_2 = \mathrm{PGL}_2(\mathbb{K}) \quad .$$

Les automorphismes sont donc bien les homographies ! □

Remarques : • Comment tracer le graphe d'une fonction homographique ?
Soit $c = 0$ et c'est une droite.
Soit $c \neq 0$, on met notre fonction sous la forme canonique $f(x) = \dfrac{\alpha}{x-\beta} + \gamma$, alors le graphe est l'hyperbole $\dfrac{\alpha}{x}$ centré au point (β, γ).

2. Attention, il y a une erreur dans le FGN, ils disent que $\Phi_M \circ \Phi_N = \Phi_{MN}$, ce qui est faux ! Le morphisme φ qu'ils construisent est un antimorphisme ! En associant $\Phi_{M^{-1}}$ à M, on règle ce problème. (voir Szpirglas)

Chapitre 2

Borne de Bézout

Références : Szpirglas, *Mathématiques L3 - Algèbre*, p 592
Mérindol, *Nombres et algèbre*, p 386
Saux Picart, *Cours de calcul formel - Algorithmes fondamentaux*, p 157

Soit k un corps commutatif de cardinal infini. On se propose dans ce développement de majorer le nombre de points d'intersection de deux courbes planes à valeurs dans k.

Théorème.

Soient A et B deux polynômes de $k[X,Y]$ de degrés totaux respectifs m et n. Si A et B sont premiers entre eux et que k est de cardinal infini, alors $\#Z(A) \cap Z(B) \leqslant mn$.

Démonstration. Si A et B n'ont pas de racine commune, le résultat est évident et dans toute la suite, on suppose que $Z(A) \cap Z(B)$ est non vide.

On note $R_Y = \mathrm{Res}_Y(A,B)$ et $R_X = \mathrm{Res}_X(A,B)$. Pour tout $(x,y) \in Z(A) \cap Z(B)$, il vient $R_Y(x) = R_X(y) = 0$. Comme A et B sont premiers entre eux, R_Y est un polynôme non nul de $k[X]$ et il a au plus $\deg R_Y$ racines. Ainsi, il y a au plus $\deg R_Y$ possibilités pour l'abscisse d'un point de $Z(A) \cap Z(B)$. De la même façon, il y au plus $\deg R_X$ possibilités pour l'ordonnée de ces points. On en déduit que

$$\#Z(A) \cap Z(B) \leqslant \deg R_X \deg R_Y.$$

Notons à présent

$$A(X,Y) = \sum_{k=0}^{p} a_k(X) Y^k \quad B(X,Y) = \sum_{k=0}^{q} b_k(X) Y^k,$$

où $\deg a_k \leqslant m-k$, $\deg b_k \leqslant n-k$ et a_p, b_q sont deux éléments non nuls de k. Alors

$$R_Y = \det(\mathrm{Syl}_Y(A,B)) = \begin{vmatrix} a_p & & & b_q & & & \\ \vdots & \ddots & & \vdots & \ddots & & \\ \vdots & & a_p & b_0 & & \ddots & \\ a_0 & & \vdots & & \ddots & & b_q \\ & \ddots & \vdots & & & \ddots & \vdots \\ & & a_0 & & & & b_0 \end{vmatrix}.$$

On note $\mathrm{Syl}_Y(A,B) = (c_{i,j})$. Alors

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

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

On en déduit :

$$\forall \sigma \in \mathcal{S}_{p+q} : \deg\left(\varepsilon(\sigma)\prod_{j=1}^{p+q} c_{\sigma(j),j}\right) = \sum_{j=1}^{p+q} \deg c_{\sigma(j),j} \leqslant \sum_{j=1}^{q}(m-p+\sigma(j)-j) + \sum_{j=q+1}^{q+p}(n-j+\sigma(j))$$
$$= mq - pq + np = mn + (m-p)(q-n) \leqslant mn,$$

et avec la formule du déterminant, $\deg R_Y \leqslant mn$. On obtient de même $\deg R_X \leqslant mn$ puis

$$\#Z(A) \cap Z(B) \leqslant (mn)^2.$$

Pour achever la démonstration, il ne reste plus qu'à affiner la majoration précédente. Dans ce but, on numérote les éléments de $Z(A) \cap Z(B) = \{(x_i, y_i) : i \in [\![1, r]\!]\}$ et on pose

$$\mathcal{E} = \left\{ \frac{x_i - x_j}{y_j - y_i} : y_j \neq y_i, i, j \in [\![1, r]\!] \right\}.$$

Alors $\#\mathcal{E} < \#k^*$ car k est de cardinal infini et on peut considérer $u \in k^* \backslash \mathcal{E}$. Remarquons le fait suivant :

$$\forall i, j \in [\![1, r]\!] : x_i - x_j \neq u(y_j - y_i) \Leftrightarrow x_i + uy_i \neq x_j + uy_j.$$

On effectue alors le changement de variables suivant :

$$\begin{cases} X' = X + uY \\ Y' = Y \end{cases} \quad \begin{cases} \tilde{A}(X', Y') = A(X, Y) \\ \tilde{B}(X', Y') = B(X, Y) \end{cases}.$$

Soit alors la fonction φ : $\begin{array}{ccc} Z(A) \cap Z(B) & \to & Z(\mathrm{Res}_{Y'}(\tilde{A}, \tilde{B})) \\ (x, y) & \mapsto & x + uy \end{array}$.

La fonction φ est bien définie car si $(x, y) \in Z(A) \cap Z(B)$, alors $A(x, y) = B(x, y) = 0$ ce qui entraîne $\tilde{A}(x + uy, y) = \tilde{B}(x + uy, y) = 0$ puis $\mathrm{Res}_{Y'}(\tilde{A}, \tilde{B})(x + uy) = 0$. De plus, φ est injective puisque u n'est pas un élément de $\mathcal{E}$. Ainsi :

$$\#Z(A) \cap Z(B) \leqslant \#Z(\mathrm{Res}_{Y'}(\tilde{A}, \tilde{B}) \leqslant \deg \mathrm{Res}_{Y'}(\tilde{A}, \tilde{B}) \leqslant mn$$

d'après le point précédent, ce qui achève la démonstration.

□

Remarques : • Ce développement est une simplification du vrai théorème de Bézout. Si on homogénéise A et B en polynômes homogènes de $\overline{k}[X, Y, T]$, alors si on compte la multiplicité des intersections et les points à l'infini, on a $\#Z(A) \cap Z(B) = mn$.

• Pour trouver les points d'intersections en pratique, on fait comme dans la preuve : on calcule les deux résultants (en X et en Y) et on cherche leurs zéros communs. En faisant cela, on obtient des équations seulement en X ou seulement en Y, d'où le nom de théorie de l'élimination.
Si on veut les points d'intersection à l'infini, il suffit d'homogénéiser les résultants, d'évaluer en "$T = 0$", puis de résoudre.

• La condition k infini n'est pas nécessaire. Il suffit de faire la preuve dans $\overline{k}$ qui est infini, puis comme $k \subset \overline{k}$, on a le résultat.

Adapté du travail de Paul Alphonse, Florian Lemonnier et Arnaud Stocker.

Chapitre 3

Cône nilpotent

Références : Caldero, Germoni, *Histoires hédonistes de groupes et de géométrie - Tome second*, p 213-215

On s'intéresse au nombre d'endomorphisme nilpotents sur un $\mathbb{F}_q$-espace vectoriel de dimension finie d. On notera $\mathcal{N}(E)$ l'ensemble des endomorphisme nilpotent. Un choix de base le met en bijection avec l'ensemble $\mathcal{N}_d(\mathbb{F}_q)$ des matrices nilpotentes de taille d à coefficients dans $\mathbb{F}_q$.

Théorème.

Soit E un $\mathbb{F}_q$-espace vectoriel de dimension d. On a :

$$n_d = |\mathcal{N}(E)| = q^{d(d-1)} \quad .$$

Pour $1 \leqslant r \leqslant d$, on pose $L_{r,d}$ l'ensemble des familles des vecteurs de E, libres à r éléments. On dit qu'un endomorphisme nilpotent N *respecte* une famille $\varepsilon \in L_{r,d}$ si pour tout $1 \leqslant i \leqslant r-1$, on a $\varepsilon_{i+1} = N\varepsilon_i$ et $N\varepsilon_r = 0$.

On pose X l'ensemble suivant :

$$X = \{(N, \varepsilon)/N \in \mathcal{N}(E), \exists r, \varepsilon \in L_{r,d} \text{ et } N \text{ respecte } \varepsilon\} \quad .$$

On va dénombrer X de deux manières.

Lemme.

Soit $e \in E\backslash\{0\}$ et $N \in \mathcal{N}(E)$, alors il existe un unique r maximal tel que la famille

$$\varepsilon = (e, Ne, \dots, N^{r-1}e)$$

soit libre. On a de plus : $N^r e = 0$.

Démonstration. L'existence de r est triviale car N est nilpotente. Soit F le sous-espace vectoriel engendré par $\{N^s e/s \in \mathbb{N}\}$. La famille ε est libre dans F. Montrons qu'elle est génératrice. La famille $(e, Ne, \dots, N^r e)$ est liée, il existe donc une famille de scalaire $(a_i)_{0 \leqslant i \leqslant r}$ non tous nuls telle que : $\sum_{i=0}^{r} a_i N^i e = 0$. Par liberté de ε, a_r ne peut-être nul. On le supposera donc égal à 1. On a donc : $N^r e = -\sum_{i=0}^{r-1} a_i N^i e$.

Pour $s = r + k$, on montre par récurrence sur k que $N^s e \in \text{Vect}(\varepsilon)$. En effet, on a : $N^s e = -\sum_{i=0}^{r-1} a_i N^{i+k} e$. La famille ε est donc une base de F.
On considère la restriction de N à F, notée $\tilde{N}$. C'est un endomorphisme nilpotent. Dans la base ε, sa matrice est la matrice compagnon suivante :

$$\begin{pmatrix} 0 & 0 & \dots & -a_0 \\ 1 & 0 & & -a_1 \\ & \ddots & \ddots & \vdots \\ & & 1 & -a_{r-1} \end{pmatrix}$$

Son polynôme caractéristique est donc : $\chi_{\tilde{N}} = X^r + \sum_{i=0}^{r-1} a_i X^i$. Comme $\tilde{N}$ est nilpotent, on a donc $a_i = 0$ pour tout $0 \leqslant i \leqslant r-1$. Donc $N^r e = 0$ □

Étape 1 : dénombrement sur la première coordonnée.
On a :

$$|X| = \sum_{N \in \mathcal{N}(E)} \pi_1^{-1}(N) \quad ,$$

où π_1 désigne la projection sur la première coordonnée. Or d'après le lemme, pour tout $N \in \mathcal{N}(E)$, on a une bijection entre les éléments de $E\backslash\{0\}$ et l'ensemble des familles libres respectées par N. Ainsi, on a : $|X| = n_d(q^d - 1)$.

Étape 2 : dénombrement sur la seconde coordonnée.
On a :

$$|X| = \sum_{r=1}^{d} \sum_{\varepsilon \in L_{r,d}} \pi_2^{-1}(\varepsilon) \quad ,$$

où π_2 désigne la projection sur la seconde coordonnée.
Soit $1 \leqslant r \leqslant d$. Le groupe $\mathrm{GL}(E)$ agit transitivement sur $L_{r,d}$ (d'après le théorème de la base incomplète). Pour $\varepsilon \in L_{r,d}$ on a donc $|L_{r,d}| = |Orb(\varepsilon)|$. D'après les relations orbite-stabilisateur, on a donc :

$$|L_{r,d}| = \frac{|GL(E)|}{|Stab(\varepsilon)|} \quad .$$

On complète ε en une base de E. Tous les raisonnements à suivre se feront dans cette base.
Or les matrices dans le stabilisateur de ε ont pour forme :

$$\left(\begin{array}{c|c} I_r & \mathcal{M}_{r,d-r}(\mathbb{F}_q) \\ \hline 0 & \mathrm{GL}_{d-r}(\mathbb{F}_q) \end{array}\right) \quad ,$$

ainsi, on a : $|Stab(\varepsilon)| = |\mathcal{M}_{r,d-r}(\mathbb{F}_q)||\,\mathrm{GL}_{d-r}(\mathbb{F}_q)| = q^{r(d-r)} g_{d-r}$, (où $g_i = |\,\mathrm{GL}_i(\mathbb{F}_q)|$). Le nombre de familles libres à r éléments est donc :

$$|L_{r,d}| = \frac{g_d}{q^{r(d-r)} g_{d-r}} \quad .$$

De plus, les matrices nilpotentes respectant ε sont de la forme :

$$\left(\begin{array}{c|c} J_r & \mathcal{M}_{r,d-r}(\mathbb{F}_q) \\ \hline 0 & \mathcal{N}_{d-r}(\mathbb{F}_q) \end{array}\right) \quad ,$$

ainsi, pour tout $\varepsilon \in L_{r,d}$, on a : $|\pi_2^{-1}(\varepsilon)| = q^{r(d-r)} n_{d-r}$. On a donc :

$$|X| = \sum_{r=1}^{d} \frac{g_d n_{d-r}}{g_{d-r}} \quad .$$

Étape 3 : Conclusion.
En comparant les deux formules obtenues pour le cardinal de X, on a pour $d \geqslant 2$:

$$\begin{aligned} \frac{n_d}{g_d}(q^d - 1) &= \sum_{r=1}^{d} \frac{n_{d-r}}{g_{d-r}} \\ &= \sum_{r=0}^{d-1} \frac{n_r}{g_r} \\ &= \frac{n_{d-1}}{g_{d-1}} + \sum_{r=0}^{d-2} \frac{n_r}{g_r} \\ &= \frac{n_{d-1}}{g_{d-1}} + \frac{n_{d-1}}{g_{d-1}}(q^{d-1} - 1) \\ &= \frac{n_{d-1}}{g_{d-1}} q^{d-1} \end{aligned} \quad .$$

Par récurrence, comme $n_1 = 1$ et $g_1 = q - 1$, on a :

$$\forall d \in \mathbb{N}^*,\ n_d = g_d \frac{\prod_{r=2}^{d} q^{r-1}}{\prod_{r=2}^{d} (q^r - 1)} \frac{n_1}{g_1} = g_d \frac{q^{d(d-1)/2}}{\prod_{r=1}^{d} (q^r - 1)}$$

et en utilisant la formule du cardinal de $\mathrm{GL}_d(\mathbb{F}_q)$, on obtient le résultat voulu.

Remarques : • On rappelle que pour calculer g_r, il faut compter le nombre de bases possibles. On a donc

$$g_r = \prod_{r=0}^{d-1} (q^d - q^r) = \prod_{r=0}^{d-1} q^r \times \prod_{r=1}^{d} (q^r - 1) = q^{d(d-1)/2} \prod_{r=1}^{d} (q^r - 1).$$

Adapté du travail de Baptiste Huguet.

Chapitre 4

Décomposition de Dunford

Références : : Gourdon, *Les maths en tête - Algèbre*, 4.4.2
Francinou, Gianella, Nicolas, *Oraux X-ENS - Algèbre 2*, 4.25

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

Théorème.

Soit $f \in \mathcal{L}(E)$ tel que χ_f soit scindé sur $\mathbb{K}$. Alors il existe un unique couple (d, n) avec d diagonalisable et n nilpotent, $f = d + n$ et d et n commutent. De plus d et n sont des polynômes en f.

Lemme.

Soit F un polynôme annulateur de f, on note $F = \beta \prod_{i=1}^{s} M_i^{\alpha_i}$ sa décomposition en facteurs irréductibles et $N_i = \mathrm{Ker}(M_i^{\alpha_i}(f))$. Alors $E = \bigoplus N_i$ et pour tout i, la projection sur N_i parallèlement à $\bigoplus_{j \neq i} N_j$ est un polynôme en f.

Démonstration. Le lemme des noyaux donne $E = \bigoplus N_i$. Puis on pose $Q_i = \prod_{j \neq i} M_j^{\alpha_j}$.

Les Q_i n'ont aucun facteur commun ensemble donc par Bézout, il existe U_1, ..., U_s tel que $\sum U_i Q_i = 1$ [1].
On a donc $\sum U_i(f) \circ Q_i(f) = Id$; il est logique de poser $P_i = U_i Q_i$ et $p_i = P_i(f)$. On va montrer que p_i est le projecteur recherché.

- Les p_i sont des projecteurs :

Pour $i \neq j$, $p_i \circ p_j = Q_i Q_j(f) \circ U_i U_j(f)$. Or $F | Q_i Q_j$, donc $p_i \circ p_j = 0$.
On a $\sum p_j = Id$, donc en composant par p_i, on a $p_i = p_i \circ p_i$. Les p_i sont donc bien des projecteurs.

- $\mathrm{Im}(p_i) = N_i$:

Soit $y = p_i(x) \in \mathrm{Im}(p_i)$, alors $M_i^{\alpha_i}(f)(y) = M_i^{\alpha_i}(f) \circ P_i(f)(y) = F(f) \circ U_i(f)(y) = 0$. Donc $\mathrm{Im}(p_i) \subset N_i$.
Puis soit $x \in N_i = \mathrm{Ker}(M_i^{\alpha_i}(f))$, alors on sait que $x = \sum p_j(x)$. Or si $j \neq i$, $p_j(x) = U_j(f) \circ Q_j(f)(x) = 0$ car $M_i^{\alpha_i} | Q_j$. D'où $x = p_i(x) \in \mathrm{Im}(p_i)$.

- $\mathrm{Ker}(p_i) = \bigoplus_{j \neq i} N_j$:

Soit $j \neq i$, $x \in N_j$, alors $p_i(x) = U_i(f) \circ Q_i(f)(x) = 0$ car $M_j^{\alpha_j} | Q_i$. Donc $\bigoplus_{j \neq i} N_j \subset \mathrm{Ker}(p_i)$.

Puis soit $x \in \mathrm{Ker}(p_i)$, alors $x = \sum_{j \neq i} p_j(x) \in \bigoplus_{j \neq i} N_j$ car $\mathrm{Im}(p_j) = N_j$.

1. En effet, $\{\sum U_i Q_i, U_i\}$ est un idéal de $\mathbb{K}[X]$, anneau principal, donc il est engendré par un polynôme unitaire m. m divise alors Q_i pour tout i, donc $m = 1$ car ils sont premiers entre eux.

- Les p_i sont des polynômes en f par construction. □

Démonstration. Existence : on applique le lemme précédent au polynôme $\chi_f = (-1)^n \prod (X-\lambda_i)^{\alpha_i}$. Les N_i sont les sous-espaces caractéristiques.
On pose $d = \sum \lambda_i p_i$ (d est donc diagonalisable) et $n = f - d = \sum (f - \lambda Id) p_i$.
Comme pour tout i et $j \neq i$, $p_i \circ p_j = 0$ et $p_i^2 = p_i$, et comme les p_i commutent avec f (car ce sont des polynômes en f), on a $n^q = \sum (f - \lambda Id)^q p_i$. En particulier, si on pose $\alpha = \max(\alpha_i)$, on a $n^\alpha = 0$. Donc n est nilpotente.
Enfin, d et n sont des polynômes en f donc commutent.

Unicité : on se donne un nouveau couple (d', n') solution du problème (pas forcément un polynôme en f).
n' commute avec d', donc commute avec $f = d' + n'$. Comme n est un polynôme en f, n' commute avec n. On peut prouver de même que d' commute avec d.
Les endomorphismes d et d' sont donc codiagonalisables. D'où $d - d'$ est diagonalisable. Or $d - d' = n' - n$ est nilpotente ($n' - n$ nilpotente car n et n' commutent) donc $d - d'$ n'a que la valeur propre 0, donc $d = d'$, puis $n = n'$.
(Merci à Anne-Elisabeth Falq pour la correction) □

Remarques : → Pour trouver les projecteurs explicitement, on utilise la décomposition en éléments simples des fractions rationnelles (voir Gourdon).
→ Ce théorème peut être généralisé sur $\mathbb{R}$ si χ_f n'est pas scindé. On obtient alors s semi simple au lieu de diagonalisable.
→ Si il n'y a qu'un seul espace caractéristique N_1, on a $p_1 = id$. D est alors la matrice diagonale constitué de l'unique valeur propre, et N est la différence de A et D.

Corollaire.

Les seules matrices A de $\mathcal{M}_n(\mathbb{C})$ telles que $\exp(A) = I_n$ sont les matrices diagonalisables dont le spectre est contenu dans $2i\pi\mathbb{Z}$.

Démonstration. Soit A telle que $\exp(A) = I_n$. On écrit $A = D + N$.
On rappelle que la décomposition de Dunford de $\exp(A)$ est $\exp(A) = \exp(D) + \exp(D)N'$ où $N' = \sum_{k=1}^{n-1} \frac{N^k}{k!}$.
Par unicité de la décomposition de Dunford, il faut $\exp(D) = I_n$ et $\exp(D)N' = 0$. Donc $N' = 0$.
Or $N' = NP(N)$ où $P(X) = \sum_{k=1}^{n-1} \frac{X^{k-1}}{k!}$. Dans une base trigonalisant N, on a donc $P(N)$ triangulaire supérieure avec une diagonale de 1, donc $P(N)$ est inversible, donc $N = 0$.
On en déduit ainsi que $A = D$ est diagonalisable.
Puis, comme $\exp(\mathrm{Sp}(A)) = \mathrm{Sp}(\exp(A)) = \{1\}$, on a $\mathrm{Sp}(A) \subset 2i\pi\mathbb{Z}$, ce qui conclut la preuve. □

Remarque : Ce corollaire ne donne pas énormément d'informations en plus sur les matrices réelles dont l'exponentielle est l'identité.
Un bon exemple à retenir d'une telle matrice est $\begin{pmatrix} 0 & 2\pi \\ -2\pi & 0 \end{pmatrix}$.

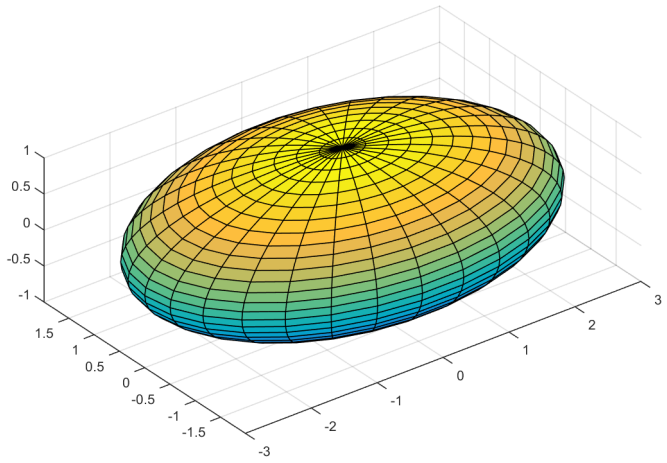
Chapitre 5

Ellipsoïde de John-Loewner

Références : : Francinou, Gianella, Nicolas, *Oraux X-ENS - Algèbre 3*, 3.37

On se place sur $\mathbb{R}^n$ muni de sa structure euclidienne usuelle.

Un ellipsoïde centré en l'origine est une quadrique définie par une équation du type $\sum_{i=1}^{n} \frac{x_i^2}{\alpha_i^2} = 1$, quitte à appliquer la méthode de Gauss. Un ellipsoïde plein centré en l'origine est donc défini intuitivement par l'équation $q(x) \leqslant 1$ où q est une forme quadratique définie positive (id est de signature $(n, 0)$). On notera ε_q l'ellipsoïde plein associé à q et Q (resp. Q^+, Q^{++}) l'ensemble des formes quadratiques (resp. positives, définies positives).



L'ellipsoïde d'équation $\frac{x^2}{3^2} + \frac{y^2}{2^2} + \frac{z^2}{1^2} = 1$

Théorème.

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

Démonstration. • Commençons par nous donner une forme quadratique q définie positive et calculons le volume V_q de ε_q.
On utilise le théorème spectral pour dire qu'il existe une base orthonormale pour le produit scalaire euclidien et orthogonale pour q. On la note $\mathcal{B} = (e_1, ..., e_n)$.

q s'écrit dans cette base $q(x) = \sum_{i=1}^{n} a_i x_i^2$ avec $a_i > 0$, donc $\det(q) = a_1 ... a_n$.

Le volume de l'ellipsoïde associé est $V_q = \int_{q(y)\leqslant 1} \mathrm{d}\lambda(y)$ avec λ la mesure de Lebesgue (sur la base canonique

donc). On fait alors le changement de base orthonormée $x = Py$ avec P la matrice de passage de la base canonique à la base $\mathcal{B}$. Le jacobien vaut donc 1 car P est orthogonale.
On a donc $V_q = \int_{a_1x_1^2+...+a_nx_n^2 \leqslant 1} \mathrm{d}x_1...\mathrm{d}x_n$.
On fait le changement de variable avec $\phi : \begin{array}{ccc} \mathbb{R}^n & \to & \mathbb{R}^n \\ (x_1,...,x_n) & \mapsto & (\frac{x_1}{\sqrt{a_1}},...,\frac{x_n}{\sqrt{a_n}}) \end{array}$. On a bien un $\mathcal{C}^1$ difféomorphisme et le jacobien est $\frac{1}{\sqrt{\prod a_i}}$.
On note $D(q)$ le déterminant de q dans n'importe quelle base orthonormée, alors on a $V_q = \frac{1}{\sqrt{D(q)}} \int_{x_1^2+...+x_n^2 \leqslant 1} \mathrm{d}x_1...\mathrm{d}x_n = \frac{V_0}{\sqrt{D(q)}}$ où V_0 est le volume de la boule unité pour la norme euclidienne. [1]

→ Le problème se ramène donc à celui-ci : il existe une unique forme quadratique $q \in Q^{++}$ telle que $D(q)$ soit maximal et pour tout $x \in K$, $q(x) \leqslant 1$.
On introduit maintenant la norme $N(q) = \sup_{\|x\| \leqslant 1} |q(x)|$ sur l'espace Q [2] et on définit l'ensemble $\mathcal{A} = \{q \in Q^+, \forall x \in K, q(x) \leqslant 1\} \subset Q$. On va chercher à maximiser D sur ce domaine.

- $\mathcal{A}$ est convexe :

$\lambda q + (1-\lambda)q'$ est une forme quadratique positive.
De plus, $\lambda q(x) + (1-\lambda)q'(x) \leqslant \lambda + 1 - \lambda = 1$ pour $x \in K$. Donc $\lambda q + (1-\lambda)q' \in \mathcal{A}$.

- $\mathcal{A}$ est fermé :

Soit q_n une suite de $\mathcal{A}$ convergeant vers q dans Q. On remarque que $\forall x \in \mathbb{R}^n$, $|q(x) - q_n(x)| \leqslant N(q-q_n)\|x\|^2$, donc $q_n(x) \to q(x)$.
Comme pour tout n, pour tout x, $q_n(x) \geqslant 0$, on a $1 \geqslant q(x) \geqslant 0$, et pour $x \in K$, $q_n(x) \leqslant 1$, donc $q(x) \leqslant 1$. Il vient $q \in \mathcal{A}$.

- $\mathcal{A}$ est borné :

K est d'intérieur non vide [3] donc il existe $a \in K$, $r > 0$ tels que $B(a,r) \subset K$.
Soit $q \in \mathcal{A}$ et $x \in B(0,r)$, alors $q(a+x) \leqslant 1$.
On applique l'inégalité de Minkowski [4] et on a $\sqrt{q(x)} \leqslant \sqrt{q(x+a)} + \sqrt{q(-a)} = \sqrt{q(x+a)} + \sqrt{q(a)} \leqslant 2$ d'où $q(B(0,r)) \leqslant 4$.
On en déduit $\forall x \in B(0,1)$, $q(x) = q(rx)\frac{1}{r^2} \leqslant \frac{4}{r^2}$ et donc $N(q) \leqslant \frac{4}{r^2}$.

- $\mathcal{A}$ est non vide :

K est borné donc inclus dans une boule $B(0,M)$. On pose $q(x) = \frac{\|x\|^2}{M^2}$. On a bien $q \in \mathcal{A}$ car $\forall x \in K$, $q(x) \leqslant 1$.

- Conclusion sur l'existence :

L'application D est continue (car le déterminant est continu) sur $\mathcal{A}$ compact, donc D atteint son maximum en q_0.
On a $D(x \mapsto \frac{\|x\|^2}{M^2}) > 0$ et c'est une forme quadratique dans $\mathcal{A}$, donc $D(q_0) > 0$, d'où $q_0 \in Q^{++}$.
On a donc existence d'un ellipsoïde de volume minimal contenant K.

- Unicité :

Soit $q \in \mathcal{A}$ tel que $D(q) = D(q_0)$ et $q \neq q_0$. Comme $\mathcal{A}$ est convexe, $\frac{q+q_0}{2} \in \mathcal{A}$, or comme det est strictement log-concave sur les matrices symétriques définies positives, on a $D(\frac{q+q_0}{2}) > \sqrt{D(q)}\sqrt{D(q_0)} \geqslant D(q_0)$, ce qui contredit la maximalité de $D(q_0)$. □

1. On a l'impression que le calcul du volume V_q fait ici dépend du choix de la base $\mathcal{B}$, mais ce n'est pas le cas. Si on prend une autre base orthonormée, la matrice de passage de l'une à l'autre est orthogonale, donc le jacobien du changement de variable correspondant est 1.
2. Les sup ou max de normes sont toujours de bons candidats de normes...
3. C'est ici qu'on l'utilise !!!
4. On a le droit de l'appliquer car on est sur Q^+.

Lemme (Log-concavité du déterminant sur $\mathcal{S}_n^{++}$)**.**

Soient A, $B \in \mathcal{S}_n^{++}(\mathbb{R})$, α, $\beta \in [0,1]$ tels que $\alpha+\beta=1$, alors $\det(\alpha A+\beta B) \geqslant (\det A)^\alpha (\det B)^\beta$.
Si $A \neq B$ et α, $\beta \neq 0$, l'inégalité est stricte.

Démonstration. On utilise le théorème de pseudo-réduction simultanée [5] pour écrire $A = {}^tPP$ et $B = {}^tPDP$ avec $P \in \mathrm{GL}_n(\mathbb{R})$ et $D = \mathrm{Diag}(\lambda_1, ..., \lambda_n)$ avec $\lambda_i > 0$. [6]
On a donc $(\det A)^\alpha (\det B)^\beta = \det P^2 (\det D)^\beta$ et $\det(\alpha A+\beta B) = \det P^2 (\det(\alpha I_n + \beta D)$.
On veut donc montrer $\det(\alpha I_n+\beta D) \geqslant (\det D)^\beta$, soit $\prod(\alpha+\beta\lambda_i) \geqslant \left(\prod \lambda_i\right)^\beta$, soit $\sum \ln(\alpha+\beta\lambda_i) \geqslant \beta \sum \ln(\lambda_i)$.
Or $\ln(\alpha+\beta\lambda_i) \geqslant \alpha\ln(1) + \beta\ln(\lambda_i) = \beta\ln(\lambda_i)$ par concavité du logarithme. On a ainsi le résultat en sommant ces inégalités et en remontant le raisonnement.
Si $A \neq B$, un des λ_i est différent de 1 et on utilise la stricte concavité du log pour conclure. □

Remarques : → On peut déplacer le problème en n'importe quel point de l'espace. En effet, si on prend $a \in \mathbb{R}^n$ comme nouveau centre du repère de l'espace, on opère une translation de notre compact et il reste d'intérieur non vide. On applique notre théorème et on obtient un unique ellipsoïde centré en 0 de volume minimal contenant K. On opère la translation inverse pour résoudre le problème. En effet, un ellipsoïde translaté reste un ellipsoïde.
→ On peut appliquer ce théorème sur n'importe quel espace vectoriel réel euclidien.
→ Application : FGN 3.38 : les sous-groupes compacts de $\mathrm{GL}(E)$ maximaux pour l'inclusion sont les $\mathrm{O}(q)$ où E est un espace vectoriel réel de dimension finie et $q \in Q^{++}$.
→ Si K est un triangle équilatéral dont un des sommets est l'origine, il faut savoir déterminer l'ellipsoïde correspondant. Celui-ci passe par deux points du triangle et cela le détermine entièrement. Si on appelle a le côté du triangle, on a l'équation $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$ avec b tel que $\cos^2(\frac{\pi}{3})+\frac{a^2}{b^2}\sin^2(\frac{\pi}{3})=1$. C'est donc un cercle.
Pour montrer qu'il passe par les deux sommets. Il suffit de dire que via une affinité orthogonale, on peut faire passer l'ellipse par un sommet. Puis si il était minimal alors il serait unique or si on tourne notre ellipsoïde, il passe par l'autre côté et contient toujours le triangle. On en déduit qu'on passe nécessairement par les deux sommets.
→ **Un prolongement du théorème :** on peut poser l'application φ qui à $x \in \mathbb{R}^n$ associe le volume de $\mathcal{E}_{q_x}$ avec q_x l'unique forme quadratique définissant l'ellipsoïde $\mathcal{E}_{q_x}$ centré en x de volume minimal contenant K.
Si on prouve que φ est continue, et que hors d'un certain compact le volume devient grand (l'enveloppe convexe ?), alors on aura montré qu'il existe un ellipsoïde de volume minimal contenant K (et ceci sans fixer son centre).
Une preuve complète peut être trouvée dans le super livre *Analyse pour l'agrégation de mathématiques, 40 développements* de notre cher camarade Julien Bernis.
→ On peut se poser la question de savoir s'il existe un unique ellipsoïde de volume maximal à l'intérieur d'un compact. (Baptiste)
C'est faux ! On prend deux compacts connexes identiques disjoints. Leur union forme un compact. Mais si il existe un unique ellipsoïde dans ce compact, il est dans l'un deux sous compacts connexe. Comme ils sont identiques, on perd l'unicité.
→ Dans le Alessandri, il y a une application de l'ellipsoïde de John Loewner à la recherche des sous-groupes compacts de $\mathrm{GL}_n(\mathbb{R})$.

5.

Théorème.

Si A et B sont dans $\mathcal{S}_n(\mathbb{R})$ et si A est définie positive, alors il existe $P \in \mathrm{GL}_n(\mathbb{R})$ telle que ${}^tPAP = I_n$ et ${}^tPBP$ soit diagonale.

6. On rappelle qu'on n'a pas diagonalisé A et B ! Les λ_i ne sont pas les valeurs propres de B. On a juste trouvé une base orthogonale commune pour deux produits scalaires.

Chapitre 6

Espace de Bergman

Références : Bayen, Margaria, *Espaces de Hilbert et opérateurs*, p 104

L'objectif de ce développement est d'étudier l'espace de Bergman

$$A^2(\mathbb{D}) = \left\{ f \in \mathcal{H}(\mathbb{D}) : \int_{\mathbb{D}} |f(z)|^2 \, dxdy < \infty \right\}.$$

On munit cet espace du produit scalaire de $L^2(\mathbb{D})$.

Lemme.

Pour tout K compact de $\mathbb{D}$, on a

$$\forall f \in A^2(\mathbb{D}),\ \|f\|_{\infty,K} \leqslant \frac{1}{\sqrt{\pi}\ d(K,\mathbb{S}^1)} \times \|f\|_{L^2}.$$

Démonstration. Soit a un élément de $\mathbb{D}$. Comme $\mathbb{D}$ est ouvert, il existe r un réel strictement positif tel que $\mathbb{D}(a,r)$ soit inclus dans $\mathbb{D}$. D'après la formule de la moyenne :

$$f(a) = \frac{1}{\pi r^2} \int_{\mathbb{D}(a,r)} f(z) \, dxdy.$$

Alors d'après l'inégalité de Cauchy-Schwarz :

$$\begin{aligned} |f(a)| &\leqslant \frac{1}{\pi r^2} \left(\int_{\mathbb{D}(a,r)} |f(z)|^2 \, dxdy \right)^{1/2} \left(\int_{\mathbb{D}(a,r)} dxdy \right)^{1/2} \\ &\leqslant \frac{\left(\pi r^2\right)^{1/2}}{\pi r^2} \|f\|_{L^2} \\ &= \frac{\|f\|_{L^2}}{\sqrt{\pi}\ r}. \end{aligned}$$

On fait alors tendre r vers $d(a,\mathbb{S}^1)$ pour obtenir

$$|f(a)| \leqslant \frac{\|f\|_{L^2}}{\sqrt{\pi}\ d(a,\mathbb{S}^1)}.$$

Étant donné que $d(K,\mathbb{S}^1) \leqslant d(a,\mathbb{S}^1)$, le résultat s'ensuit alors. □

Proposition.

$A^2(\mathbb{D})$ munit du produit scalaire de $L^2(\mathbb{D})$ est un espace de Hilbert.

Démonstration. Soit (f_n) une suite de Cauchy de $A^2(\mathbb{D})$. Alors d'après le lemme précédent, on a pour tout compact K de $\mathbb{D}$:

$$\forall m,n\in\mathbb{N} : \|f_n-f_m\|_{\infty,K} \leqslant \frac{\|f_n-f_m\|_{L^2}}{\sqrt{\pi}\ d(K,\mathbb{S}^1)}.$$

Ainsi, sur tout compact, (f_n) est de Cauchy dans $\mathcal{C}(K,\mathbb{C})$ qui est complet pour la norme uniforme, donc quitte à prendre des compacts emboîtés, on a l'existence de f continue sur $\mathbb{D}$ et limite uniforme sur tout compact de (f_n). D'après le théorème de Weierstrass, f est holomorphe.
De plus, $L^2(\mathbb{D})$ est un espace complet donc (f_n) admet une limite g dans $L^2(\mathbb{D})$. Or, d'après le théorème de Riesz-Fischer, il existe une extractrice φ telle que $(f_{\varphi(n)})$ converge presque partout sur $\mathbb{D}$ vers g. Ainsi, $f=g$ presque partout sur $\mathbb{D}$ et f est un élément de $L^2(\mathbb{D})$. □

Pour toute la suite, on pose pour tout entier naturel n

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

Proposition.

La famille (e_n) forme une base hilbertienne de $A^2(\mathbb{D})$.

Démonstration. Le caractère orthonormée de (e_n) est immédiat, il suffit de calculer :

$$\begin{aligned}
\langle e_n,e_m\rangle &= \frac{\sqrt{(n+1)(m+1)}}{\pi}\int_{\mathbb{D}}\overline{z}^n z^m \mathrm{d}x\mathrm{d}y \\
&= \frac{\sqrt{(n+1)(m+1)}}{\pi}\left(\int_{r=0}^1 r^{n+m+1}\mathrm{d}r\right)\left(\int_{\theta=0}^{2\pi} e^{i(n-m)\theta}\mathrm{d}\theta\right) \\
&= \frac{2\pi\sqrt{(n+1)(m+1)}}{(n+m+2)\pi}\delta_{n,m} \\
&= \frac{2\pi(n+1)}{(2n+2)\pi}\delta_{n,m} \\
&= \delta_{n,m}
\end{aligned}$$

À présent, considérons f une fonction de $A^2(\mathbb{D})$ orthogonale à $\mathrm{Vect}(e_n)$. On note $c_n(f)=\langle f,e_n\rangle$ et on a donc par supposition $c_n(f)=0$.
Comme f est holomorphe sur $\mathbb{D}$, elle est analytique sur $\mathbb{D}$ et il existe (a_n) une suite de nombres complexes telle que

$$\forall z\in\mathbb{D} : f(z)=\sum_{n=0}^{\infty} a_n z^n.$$

Alors :

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

la première égalité provenant du théorème de convergence dominé et la deuxième du fait de la convergence normale sur tout compact de $\mathbb{D}$ de la série entière $\sum a_n z^n$. Or avec un changement de variables polaires, il vient :

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

donc

$$c_n(f)=\sqrt{\frac{n+1}{\pi}}\lim_{r\to 1}\left(\sum_{k=0}^{\infty} a_k\frac{\pi\ r^{2n+2}}{n+1}\delta_{k,n}\right)=\sqrt{\frac{\pi}{n+1}}\ a_n\ \lim_{r\to 1} r^{2n+2}=\sqrt{\frac{\pi}{n+1}}\ a_n.$$

Donc pour tout $n\in\mathbb{N}$, $a_n=0$. On en déduit $f=0$ et la famille $(e_n)_n$ est bien une base hilbertienne. □

Remarques : • Il existe un noyau pour les fonctions de $A^2(\mathbb{D})$.

Proposition.

Soit F une fonction de $A^2(\mathbb{D})$. Alors :

$$\forall \zeta \in \mathbb{D} : F(\zeta) = \int_{\mathbb{D}} \frac{F(z)}{\pi(1-\zeta\ \overline{z})^2}\ dxdy.$$

Démonstration. Posons

$$k : \begin{array}{ccc} \mathbb{D}^2 & \to & \mathbb{C} \\ (\zeta, z) & \mapsto & \dfrac{1}{\pi(1-\zeta\ \overline{z})^2} \end{array}.$$

Il est immédiat que pour tout ζ de $\mathbb{D}$, $k(\zeta,.)$ est un élément de $A^2(\mathbb{D})$. Soit $F \in A^2(\mathbb{D})$ et (a_n) la suite de nombres complexes associée telle que

$$\forall z \in \mathbb{D} : F(z) = \sum_{n=0}^{\infty} a_n z^n.$$

On fixe $\zeta \in \mathbb{D}$. Comme (e_n) est une base hilbertienne de $A^2(\mathbb{D})$, il vient

$$\langle k(\zeta,.), F\rangle = \sum_{n=0}^{\infty} \sqrt{\frac{\pi}{n+1}} a_n \langle k(\zeta,.), e_n\rangle.$$

Or, pour tout entier naturel n :

$$\begin{aligned} \langle k(\zeta,.), e_n\rangle &= \frac{\sqrt{n+1}}{\pi^{3/2}} \int_{\mathbb{D}} \frac{z^n}{(1-\zeta\ \overline{z})^2}\ dxdy &&= \frac{\sqrt{n+1}}{\pi^{3/2}} \int_{\mathbb{D}} \left(\sum_{k=0}^{\infty} (\zeta\ \overline{z})^k\right)' z^n\ dxdy \\ &= \frac{\sqrt{n+1}}{\pi^{3/2}} \int_{\mathbb{D}} \left(\sum_{k=0}^{\infty} (k+1)(\zeta\ \overline{z})^k z^n\right) dxdy &&= \frac{\sqrt{n+1}}{\pi^{3/2}} \sum_{k=0}^{\infty} (k+1)\zeta^k \int_{\mathbb{D}} \overline{z}^k z^n dxdy\ . \\ &= \frac{\sqrt{n+1}}{\pi^{3/2}} \sum_{k=0}^{\infty} (k+1)\zeta^k \frac{2\pi}{2k+2}\delta_{n,k} &&= \sqrt{\frac{n+1}{\pi}}\zeta^n \end{aligned}$$

Il suffit alors de reporter cette expression pour conclure. □

• Apparemment, on peut faire des opérateurs de Toeplitz sur les espaces de Bergman et il y aurait des applications obscures en physique quantique...

Adapté du travail de Paul Alphonse.

Chapitre 7

Équation de Hill-Mathieu

Références : Zuily, Queffelec, *Analyse pour l'agrégation*, p 410-412

On considère l'équation différentielle suivante :

$$(E) : y'' + qy = 0 \quad ;$$

avec $q : \mathbb{R} \to \mathbb{R}$ une fonction continue, paire, π-périodique. On cherche une quantité que caractérise l'existence de solution bornée. En vertu du théorème de *Cauchy - Lipschitz*, l'espace des solutions de (E) est un sous-espace vectoriel de $\mathcal{C}^2(\mathbb{R})$, de dimension 2, que l'on notera W. On peut, de plus, le munir d'une base "canonique" (y_1, y_2) définie par :

$$\left\{ \begin{array}{l} y_1(0) = 1 \\ y_1'(0) = 0 \end{array} \right. \text{ et } \left\{ \begin{array}{l} y_2(0) = 0 \\ y_2'(0) = 1 \end{array} \right.$$

On considère l'endomorphisme de translation suivant :

$$\begin{array}{rccc} u : & \mathcal{C}^2(\mathbb{R}) & \to & \mathcal{C}^2(\mathbb{R}) \\ & f & \mapsto & f(. + \pi) \end{array} .$$

Étape 1 : W est u-stable.
Soit $y \in W$, pour tout $x \in \mathbb{R}$ on a, comme q est π-périodique,

$$u(y)''(x) + q(x)u(y)(x) = y''(x + \pi) + q(x)u(x + \pi) = y''(x + \pi) + q(x + \pi)u(x + \pi) = 0.$$

Donc $u(y)$ est solution de (E).

Par abus on identifiera u à la matrice de $u_{|W}$ dans la base (y_1, y_2). On a :

$$u = \left(\begin{array}{cc} a & c \\ b & d \end{array} \right) .$$

Étape 2 : a,b,c,d ?
Pour tout $x \in \mathbb{R}$, on a : $u(y_1)(x) = ay_1(x) + by_2(x)$. En évaluant en 0, on obtient : $a = y_1(\pi)$. De plus en dérivant l'expression précédente et en évaluant en 0, on obtient : $b = y_1'(\pi)$. En procédant de même avec y_2, on montre que l'on a : $c = y_2(\pi)$ et $d = y_2'(\pi)$.

On pose : $T = tr(u) = a + d$.

Étape 3 : $\det(u)$?
Soit w la wronskien de la base (y_1, y_2). On a : $w = y_1y_2' - y_2y_1'$. On vérifie que la dérivée de w est constante égale à 0. Par continuité du wronskien, il est donc constant. On a donc : $\det(u) = w(\pi) = w(0) = 1$.

Étape 4 : $a = d$
On pose $z = y_1(-.)$. Pour tout $x \in \mathbb{R}$, on a :

$$z''(x) + q(x)z(x) = y_1''(-x) + q(x)y_1(-x) = y_1''(-x) + q(-x)y_1(-x) = 0,$$

car q est paire. On en conclut que z est solution de (E). Or elle vérifie les mêmes conditions initiales que y_1, elle lui est donc égale. On en déduit que y_1 est paire. De la même manière, il apparaît que y_2 est impaire.

L'inverse de u est l'endomorphisme $u^{-1} : f \mapsto f(. - \pi)$. Sa matrice dans la base (y_1, y_2) est donc :

$$u^{-1} = \begin{pmatrix} y_1(-\pi) & y_2(-\pi) \\ y_1'(-\pi) & y_2'(-\pi) \end{pmatrix} = \begin{pmatrix} a & -c \\ -b & d \end{pmatrix} \quad .$$

Or d'après la formule de l'inverse (avec la comatrice) on a aussi :

$$u^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \quad .$$

On en déduit que $a = d$.

Nous avons donc à présent toutes les cartes en main pour démontrer le théorème suivant :

Théorème.

- Si $|T| < 2$, alors toutes les solutions de (E) sont bornées.
- Si $|T| = 2$, alors il existe des solutions bornées non nulles.
- Si $|T| > 2$, alors toutes les solutions non nulles sont non-bornées.

Démonstration. Le polynôme caractéristique de u est : $\chi_u(X) = X^2 - TX + 1$. Son discriminant est donc $\Delta = T^2 - 4$.

Cas 1 : Si $|T| < 2$.
Dans ce cas, on a $\Delta < 0$. u admet donc deux valeurs propres complexes conjuguées, ρ et $\bar{\rho}$. On a : $\rho\bar{\rho} = 1$ donc $|\rho| = 1$. Soient z_1 et z_2 les valeurs propres associées. C'est une base propre de W. Pour tout $x \in \mathbb{R}$, on a : $z_1(x + \pi) = \rho z_1(x)$. La fonction $|z_1|$ est donc π-périodique et donc bornée. On en déduit que z_1 est bornée. De la même manière, z_2 est bornée. Par linéarité, toutes les solutions sont bornées.

Cas 2 : $|T| = 2$.
Si $|T| = 2$, le discriminant est nul et ± 1 est l'unique valeur propre. En considérant un vecteur propre z associé, on montre de la même manière que $|z|$ est π-périodique et que z est une solution bornée.

Cas 3 : Si $|T| > 2$.
Dans ce cas, u admet deux valeurs propres réelles α et α^{-1} (avec $\alpha > 1$). On note z_1 et z_2 les vecteurs propres associés. Ils forment une base. Soit y une solution non nulle, on dispose de β et γ non tous nuls, tels que : $y = \beta z_1 + \gamma z_2$. Si $\beta \neq 0$, on dispose de x_0 tel que $z_1(x_0) \neq 0$. Pour tout $n \in \mathbb{Z}$ on a :

$$y(x_0 + n\pi) = \alpha^n \beta z_1(x_0) + \alpha^{-n} \gamma z_2(x_0) \text{ , qui explose quand } n \text{ croît.}$$

De la même manière, si γ est non nul, il faut faire tendre n vers $-\infty$ pour montrer l'explosion. Ainsi toute solution non nulle est non bornée. □

Remarques : • Si $q = 1$, on trouve $y_1 = \cos$ et $y_2 = \sin$. La trace est alors

$$T = y_1(\pi) + y_2'(\pi) = 2\cos(\pi) = -2.$$

Donc il existe des solutions bornées et en fait elles le sont toutes dans ce cas là.
• Si $q = -1$, on trouve $y_1 = \cosh$ et $y_2 = \sinh$. La trace est alors

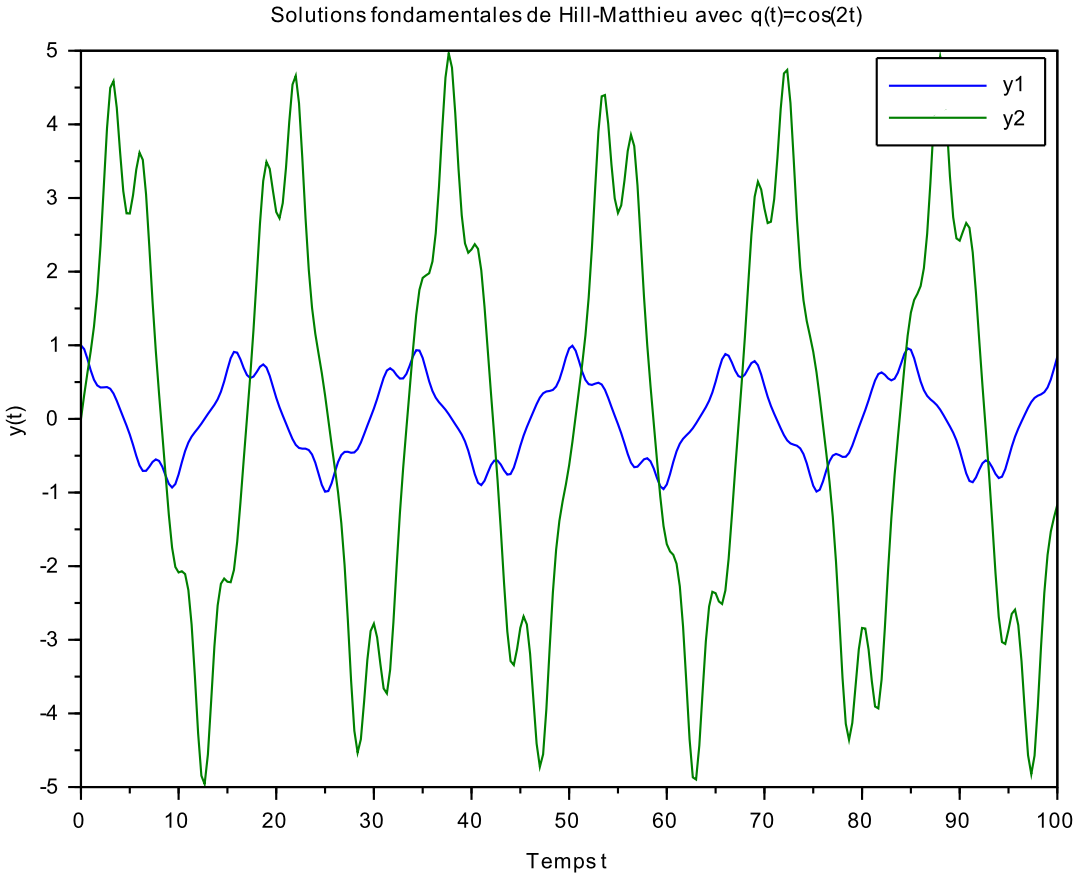
$$T = y_1(\pi) + y_2'(\pi) = 2\cosh(\pi) > 2.$$

Il n'y a donc pas de solution bornée non nulle.
• On pourrait essayer de résoudre explicitement l'équation pour des q plus complexes mais c'est difficile. Par exemple, pour $q(x) = \cos(2x)$, la résolvante est déjà incalculable.
Le théorème n'en est pas pour autant inutilisable. En effet, T est donné par

$$T = y_1(\pi) + y_2'(\pi).$$

Il suffit donc de savoir approximer assez précisément y_1 et y_2 (avec un RK4 par exemple) pour pouvoir déterminer si on a une chance de trouver des solutions bornées non triviales.

Voici un exemple où T vaut environ 0.77. On observe que y_1 et y_2 sont bornées.



D'ailleurs je n'ai pas choisi cet exemple au hasard. Mathieu a étudié cette équation pour $q(x) = \lambda - 2\varepsilon\cos(2x)$. Il s'intéressait à l'équation d'onde pour une membrane elliptique. Hill a retrouvé une équation similaire en étudiant le périgée de la lune.

Adapté du travail de Baptiste Huguet.

Chapitre 8

Équation de la chaleur

Références : Zuily, Queffelec, *Analyse pour l'agrégation*, p 105
Evans, *Partial differential equations*, p 63

Dans ce développement, on se propose de résoudre l'équation de la chaleur à l'aide des séries de Fourier.

Soient L un réel non nul et $Q =]0, L[\times]0, \infty[$. Considérons le problème

$$(EC) : \begin{cases} u \in \mathcal{C}(\overline{Q}) & u \in \mathcal{C}_1^2(Q) \quad (1) \\ \dfrac{\partial u}{\partial t}(t,x) - \dfrac{\partial^2 u}{\partial x^2}(t,x) = 0 & (t,x) \in Q \quad (2) \\ u(0,t) = u(L,t) = 0 & t \in [0, \infty[\quad (3) \\ u(x,0) = h(x) & x \in [0, L] \quad (4) \end{cases}$$

où h est une fonction de classe $\mathcal{C}^1$ sur $[0, L]$ vérifiant $h(0) = h(L) = 0$ et où $\mathcal{C}_1^2$ est l'espace des fonctions dérivables deux fois en espace et une fois en temps.

Théorème.

Le problème (EC) admet une solution de classe $\mathcal{C}^\infty$ sur Q.

Démonstration. • Analyse par séparation des variables :
L'idée est de chercher des solutions de la forme $u(x,t) = f(x)g(t)$ (séparation des variables). Alors (2) est équivalent à $f(x)g'(t) = f''(x)g'(t)$ sur Q. Supposons que f et g ne s'annulent pas sur Q alors

$$\frac{f''(x)}{f(x)} = \frac{g'(t)}{g(t)}, \forall (x,t) \in Q.$$

Les deux membres de cette équation sont donc égaux à une certaine constante $\lambda \in \mathbb{R}$. On a

$$\begin{cases} f''(x) = \lambda f(x), & x \in]0, L[\\ g'(t) = \lambda g(t), & t \in]0, +\infty[\end{cases}.$$

Trois cas se présentent à nous :

1. Si $\lambda > 0$, alors $f(x) = Ae^{\sqrt{\lambda}x} + Be^{-\sqrt{\lambda}x}$. Puis on a $f(0) = f(L) = 0$ donc $A = -B$ et $A \sinh(\sqrt{\lambda}L) = 0$. On en déduit $f = 0$ et $u = 0$, ce qui ne convient pas à la condition (4) en général.
2. Si $\lambda = 0$, $f(x) = Ax + B$ et les conditions aux bords donnent à nouveau $u = 0$.
3. Si $\lambda < 0$, on pose ξ une racine de $(-\lambda)$, alors $f(x) = A\cos(\xi x) + B\sin(\xi x)$ et $g(t) = e^{-\xi^2 t}$. Les conditions de bord donnent $A = 0$ et $B\sin(\xi L) = 0$, d'où $\xi = \dfrac{n\pi}{L}$ pour $n \in \mathbb{Z}$.

On a donc trouvé une famille de solutions possibles donnée par

$$u_n(x,t) = b_n \sin\left(\frac{n\pi}{L}\right) e^{-\frac{n^2\pi^2}{L^2}t}, n \in \mathbb{Z}.$$

Néanmoins, il n'est pas dit qu'une de ces solutions puisse vérifier (4). On va donc chercher une solution sous la forme

$$u(x,t) = \sum_{n=1}^{\infty} b_n \sin\left(\frac{n\pi}{L}\right) e^{-\frac{n^2\pi^2}{L^2}t}.$$

- Synthèse :

Soit h_1 la fonction définie sur $[-L, L]$ par

$$h_1(x) = \begin{cases} h(x) & \text{si } x \in [0, L] \\ -h(-x) & \text{si } x \in [-L, 0] \end{cases}.$$

Comme $h(0) = 0$, il s'ensuit que la fonction h_1 est de classe $\mathcal{C}^1$ sur $[-L, L]$. Considérons à présent H la fonction $2L$-périodique sur $\mathbb{R}$ qui coïncide avec h_1 sur $[-L, L]$. Étant donné que $h(L) = 0$, H est continue sur $\mathbb{R}$ et $\mathcal{C}^1$ par morceaux. Alors la série de Fourier de H converge uniformément et normalement sur $\mathbb{R}$ vers H. H est une fonction impaire donc

$$\forall x \in \mathbb{R} : H(x) = \sum_{n=1}^{\infty} b_n \sin\left(\frac{n\pi}{L}x\right)$$

avec

$$b_n = \frac{2}{L}\int_0^L h(x) \sin\left(\frac{n\pi}{L}x\right)\, dx$$

et la série $\sum b_n$ converge absolument. Ainsi, la fonction

$$u : \begin{array}{ccc} \overline{Q} & \to & \mathbb{R} \\ (x,t) & \mapsto & \displaystyle\sum_{n=1}^{\infty} b_n \sin\left(\frac{n\pi}{L}x\right) \exp\left(-\left(\frac{n\pi}{L}\right)^2 t\right) \end{array}$$

est continue d'après le théorème de continuité sous le signe somme. Montrons qu'elle est de classe $\mathcal{C}^\infty$ sur Q. On pose pour cela pour tout entier naturel non nul n

$$u_n : \begin{array}{ccc} \overline{Q} & \to & \mathbb{R} \\ (x,t) & \mapsto & b_n \sin\left(\frac{n\pi}{L}x\right) \exp\left(-\left(\frac{n\pi}{L}\right)^2 t\right) \end{array}.$$

Alors :

1. Les fonctions u_n sont toutes de classe $\mathcal{C}^\infty$ sur Q.
2. Soit $[\varepsilon, \infty[\subset]0, \infty[$. Alors les différentielles partielles d'ordre k des u_n sont majorées (uniformément) sur $]0, L[\times[\varepsilon, \infty[$ par un terme de la forme

   $$C_k\, |b_n|\, n^{2k} \exp\left(-\left(\frac{n\pi}{L}\right)^2 \varepsilon\right)$$

   qui est le terme général d'une série convergente étant donné que la suite de terme général $n^{2k} \exp\left(-\left(\frac{n\pi}{L}\right)^2 \varepsilon\right)$ est bornée et la série $\sum b_n$ converge absolument.

D'après le théorème de dérivation des intégrales à paramètre, u admet des dérivées partielles dans les directions x et t et elles sont continues. Comme les dérivées partielles de u sont continues, u est $\mathcal{C}^1$.
On peut itérer ce raisonnement autant de fois que l'on veut et cela montre que u est bien de classe $\mathcal{C}^\infty$ sur Q.

Pour terminer, il ne reste plus qu'à montrer que u est solution de notre problème. Dans le point précédent, on a montré que u satisfait (1). De manière immédiate, il vient que

$$\forall n \in \mathbb{N}^*, \forall (t,x) \in Q : \frac{\partial u_n}{\partial t}(t,x) - \frac{\partial^2 u_n}{\partial x^2}(t,x) = 0$$

et donc d'après le théorème de dérivation des intégrales à paramètre, u vérifie (2). Enfin, pour tous t réel strictement positif et x élément de $[0, L]$:

$$u(0,t) = \sum_{n=1}^{\infty} b_n \sin(0) \exp\left(-\left(\frac{n\pi}{L}\right)^2 t\right) = \sum_{n=1}^{\infty} b_n \sin(n\pi) \exp\left(-\left(\frac{n\pi}{L}\right)^2 t\right) = u(L,t) = 0,$$

$$u(x,0) = \sum_{n=1}^{\infty} b_n \sin\left(\frac{n\pi}{L}x\right) = h(x),$$

donc u satisfait les points (3) et (4), ce qui achève la démonstration. □

Théorème.

Le problème (EC) admet une unique solution. De plus, elle est de classe $\mathcal{C}^\infty$ sur Q.

Démonstration. On va utiliser une méthode d'énergie.
Soient u_1 et u_2 deux solutions du problème de la chaleur. On pose $w = u_1 - u_2$ alors w vérifie

$$\begin{cases} w \in \mathcal{C}(\overline{Q}) & w \in \mathcal{C}_1^2(Q) \\ \dfrac{\partial w}{\partial t}(t,x) - \dfrac{\partial^2 w}{\partial x^2}(t,x) = 0 & (t,x) \in Q \\ w(x,t) = 0 & (x,t) \in \partial Q \end{cases}.$$

On pose l'énergie

$$e(t) := \int_{[0,L]} w^2(x,t)\mathrm{d}x, \quad t \in [0,\infty[.$$

Alors en utilisant le théorème de dérivation sous l'intégrale sur tout compact de $[0,\infty[$, on a

$$\begin{aligned} \frac{\mathrm{d}e}{\mathrm{d}t}(t) &= 2\int_{[0,L]} w\frac{\partial w}{\partial t}\mathrm{d}x \\ &= 2\int_{[0,L]} w\Delta w\mathrm{d}x \\ &= 2\left[w\nabla w\right]_0^L - 2\int_{[0,L]} \nabla w.\nabla w\mathrm{d}x \\ &= -2\int_{[0,L]} |\nabla w|^2\,\mathrm{d}x \\ &\leqslant 0 \end{aligned}$$

D'où on en déduit

$$\forall t \in [0,\infty[, e(t) \leqslant e(0) = 0.$$

Or comme e est positif, $e = 0$ et $w = 0$.
On a bien l'unicité. □

Remarques : • On retrouve la propriété de régularisation de l'équation de la chaleur, ainsi que sa propagation à vitesse infinie, et sa non-réversibilité.
• Originellement, Fourier a résolu l'équation de la chaleur de cette manière. Néanmoins il n'a rien justifié des convergences et existence de ses sommes...
• On peut aussi prouver l'unicité par le principe du maximum (difficile).

Lemme (Principe du maximum pour l'équation de la chaleur)**.**

Soit $u \in \mathcal{C}(\overline{Q}) \cap \mathcal{C}^2(Q)$ telle que

$$\forall (x,t) \in Q : \frac{\partial^2 u}{\partial x^2}(t,x) - \frac{\partial u}{\partial t}(t,x) \geqslant 0.$$

Soient $T > 0$ et $K = [0,L] \cap [0,T]$. Alors :

$$\sup_{(x,t)\in K} u(x,t) = \sup_{(x,t)\in K\cap\partial Q} u(x,t).$$

Démonstration. Considérons l'opérateur différentiel

$$P = \frac{\partial^2}{\partial x^2} - \frac{\partial}{\partial t}.$$

Soient $\varepsilon > 0$ et $u_\varepsilon : (x,t) \mapsto u(x,t) + \varepsilon x^2$ qui vérifie $Pu_\varepsilon \geqslant 2\varepsilon$ sur Q. Soit $m_\varepsilon = (x_\varepsilon, t_\varepsilon)$ un point de K où u_ε atteint son maximum sur K. Supposons par l'absurde de m_ε n'appartienne pas à $K \cap \partial Q$. Alors :

$$\begin{cases} 0 < x_\varepsilon < L \quad \text{donc} \quad \dfrac{\partial u_\varepsilon}{\partial x}(m_\varepsilon) = 0 \quad \text{et} \quad \dfrac{\partial^2 u_\varepsilon}{\partial x^2}(m_\varepsilon) \leqslant 0, \\ 0 < t_\varepsilon \leqslant T \quad \text{donc} \quad \dfrac{\partial u_\varepsilon}{\partial t}(m_\varepsilon) = \lim\limits_{h \to 0 \,:\, h<0} \left(\dfrac{u_\varepsilon(x_\varepsilon, t_\varepsilon - h) - u(x_\varepsilon, t_\varepsilon)}{-h} \right) \geqslant 0. \end{cases}$$

Il en résulte que $Pu_\varepsilon(m_\varepsilon) \leqslant 0$ ce qui contredit $Pu_\varepsilon(m_\varepsilon) \geqslant 2\varepsilon$. Ainsi, $m_\varepsilon \in K \cap \partial Q$ puis :

$$\sup_{(x,t)\in K} u(x,t) \leqslant \sup_{(x,t)\in K} u_\varepsilon(x,t) = \sup_{(x,t)\in K\cap\partial Q} u_\varepsilon(x,t) \leqslant \sup_{(x,t)\in K\cap\partial Q} u(x,t) + \varepsilon L^2.$$

Il suffit alors de faire tendre ε vers 0 pour conclure. □

Pour prouver l'unicité, on se donne u_1 et u_2 deux solutions du problème, puis on pose $v = u_1 - u_2$. Alors, le principe du maximum prouve que $v = 0$, car v est nulle sur ∂Q.

Adapté du travail de Paul Alphonse.

Chapitre 9

Équation de Nagell-Ramanujan

Références : Francinou, Gianella, *Exercices de mathématiques pour l'agrégation - Algèbre 1*, p 166-171
Un corrigé de partiel sur la page de Lionel Fourquaux : `https://www.normalesup.org/~fourquau/pro/teaching/2011-2012/thno/exam1-corrige.pdf`

Théorème.

L'équation diophantienne $x^2+3=2^n$ n'admet que deux solutions (x,n) : $(1,2)$ et $(-1,2)$.

Démonstration. • On commence par remarque que x doit être impair et que $n \geqslant 2$.
Supposons que $n=2p$ soit pair. Alors on peut factoriser l'équation en $3=(2^p-x)(2^p+x)$.
Les seuls diviseurs de 3 étant 1 et 3, on a seulement deux solutions : $(1,2)$ et $(-1,2)$.

- On prend n impair plus grand que 3, d'où $x^2+3 \equiv 0[4]$.

L'équation est équivalente à $\dfrac{x^2+3}{4} = \dfrac{x+i\sqrt{3}}{2}\dfrac{x-i\sqrt{3}}{2} = 2^m$ avec $m=n-2$.
Comme x est impair, on peut l'écrire $x=2k+1$ et on a $(k+j)(k+j^2)=2^m$.
On a besoin d'un lemme pour continuer.

Lemme.

L'anneau $\mathbb{Z}[j]$ est euclidien et $\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\}$.

Démonstration. • La norme N est celle du corps quadratique $\mathbb{Q}(i\sqrt{3})$ associé à $\mathbb{Z}[j]$, elle est définie par

$$N(x+i\sqrt{3}y) = x^2+3y^2.$$

Soient $x,y \in \mathbb{Q}$, montrons que l'on peut trouver $z_0 = x_0+jy_0 \in \mathbb{Z}[j]$ tel que $N(z-z_0)<1$, avec $z=x+i\sqrt{3}y$.
On a

$$N(z-z_0) = \left(x-x_0+\frac{y_0}{2}\right)^2 + 3\left(y-\frac{y_0}{2}\right)^2.$$

On choisit donc y_0 l'entier le plus proche de $2y$, puis x_0 l'entier le plus proche de $x-\dfrac{y_0}{2}$, ainsi on a

$$\begin{aligned} N(z-z_0) &\leqslant \left(\frac{1}{2}\right)^2 + 3\left(\frac{1}{4}\right)^2 \\ &\leqslant \frac{1}{4}+\frac{3}{16} = \frac{7}{16} < 1. \end{aligned}$$

Maintenant prenons z_1 et z_2 dans $\mathbb{Z}[j]$, et prenons $z_0 \in \mathbb{Z}[j]$ tel que $N\left(\dfrac{z_1}{z_2}-z_0\right)<1$.
Alors il vient $z_1 = z_0z_2 + z_2\left(\dfrac{z_1}{z_2}-z_0\right)$ et $N\left(z_2\left(\dfrac{z_1}{z_2}-z_0\right)\right) = N(z_2)N\left(\dfrac{z_1}{z_2}-z_0\right) < N(z_2)$.

L'anneau $\mathbb{Z}[j]$ est bien euclidien.

- Pour trouver les unités, il suffit de résoudre $N(x+yj)=1$.

Cela donne $\left(x-\frac{y}{2}\right)^2+\frac{3y^2}{4}=1$.
D'où $x^2+y^2-xy=1$.
Puis

$$1=|x^2+y^2-xy|\geqslant x^2+y^2-|xy|\geqslant\frac{x^2+y^2}{2}.$$

Donc $x^2+y^2\leqslant 2$ et les seuls cas possibles sont $x,\,y\in\{-1,0,1\}$.
On retrouve bien l'ensemble $\{\pm 1,\pm j,\pm j^2\}$. □

- Montrons que 2 est irréductible dans $\mathbb{Z}[j]$.

Si $2=ab$, avec $N(a)$, $N(b)\neq 1$, alors $4=N(2)=N(a)N(b)$, donc $N(a)=N(b)=2$. Mais il n'existe pas d'élément de $\mathbb{Z}[j]$ de norme 2.
En effet, si $N(x+jy)=2$, on a $x^2+y^2-xy=2$, donc $x^2+y^2\leqslant 4$. Donc x et y sont entre -2 et 2. On vérifie qu'aucun des nombres possibles n'est de norme 2.

- Comme $\mathbb{Z}[j]$ est euclidien, il est factoriel, donc par unicité de la décomposition en irréductibles, l'équation $(k+j)(k+j^2)=2^m$ donne $k+j=\alpha 2^l$ et $k+j^2=\alpha^{-1}2^{m-l}$ avec $0\leqslant l\leqslant m$.
α ne peut être réel, donc c'est soit $\pm j$, soit $\pm j^2$.

Or dans ce cas, en prenant la partie imaginaire, on a $\pm\frac{\sqrt{3}}{2}=\frac{\sqrt{3}}{2}2^l$ et $\pm\frac{\sqrt{3}}{2}=\frac{\sqrt{3}}{2}2^{m-l}$.
Comme on ne peut avoir $l=m-l=0$, on a une absurdité, ce qui conclut la preuve. □

Remarques : • Tristement, il y a une manière triviale de résoudre cette équation. En effet, dans $\mathbb{F}_3$, l'équation diophantienne est $x^2=(-1)^n$. Donc si n est impair, -1 est un carré modulo 3, ce qui est faux.
On peut tout de même garder ce développement car la vraie équation de Nagell-Ramanujan est $x^2+7=2^n$. Pour celle-ci, il n'y a plus d'absurdité mais le raisonnement est trop complexe pour tenir en 15 minutes.
• Ce développement ressemble au théorème des deux carrés dans les outils utilisés. Je ne pense pas que faire les deux en développement soit une bonne idée.
• Rappelons l'idée de pourquoi l'anneau des entiers algébriques de $\mathbb{Q}(\sqrt{d})$ est $\mathbb{Z}[\sqrt{d}]$ si $d\equiv 2,3[4]$ et $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ si $d\equiv 1[4]$.
Si on prend un élément non rationnel, son polynôme minimal est $X^2-\mathrm{Tr}(\alpha)X+N(\alpha)$. Les entiers algébriques sont donc les éléments de trace et de norme entière.
Il s'agit ensuite de détailler ce que cela veut dire sur α et on trouve le résultat.

Adapté du travail de Alexandre Bailleul.

Chapitre 10

Équation de Pell-Fermat

Références : Caldero, Germoni, *Histoires hédonistes de groupes et de géométrie - Tome 2*, p 388

L'objectif est de résoudre l'équation de Pell-Fermat, i.e chercher les couples d'entiers (x, y) vérifiant $x^2 - dy^2 = 1$ avec d un entier supérieur ou égal à 2 sans facteur carré.

Théorème.

Soit d un entier naturel sans facteur carré et soit $\mathcal{H}$ l'hyperbole d'équation $X^2 - dY^2 = 1$ dans le plan $\mathbb{R}^2$. Soit $E = M_0 = (1, 0)$. **On admet l'existence de** $M_1 = (X_1, Y_1)$, un point de $\mathcal{H}$ où X_1 et Y_1 sont des entiers naturels avec $X_1^2 + Y_1^2$ aussi petit que possible. Alors l'ensemble des points entiers de la branche de $\mathcal{H}$ qui contient M_0 est le groupe engendré par M_1. L'ensemble des points entiers de $\mathcal{H}$ forme un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Démonstration. • On calcule, en coordonnées, l'application $\varphi : M \in \mathcal{H} \mapsto M_1 \star M \in \mathcal{H}$. On pourrait le faire directement mais c'est compliqué. On va faire un changement de repère. On passe au repère OXY où M_0 a pour coordonnées $(1, 1)$, en posant

$$\begin{cases} x = X + \sqrt{d}Y \\ y = X - \sqrt{d}Y \end{cases}$$

Notons (x_1, y_1) les coordonnées de M_1 dans ce repère. Si un point M a pour coordonnées (X, Y) dans le premier repère et (x, y) dans le deuxième, alors $M_1 \star M$ a pour coordonnées $(x_1 x, y_1 y)$ dans le deuxième repère et

$$(X', Y') = (X_1 X + dY_1 Y, Y_1 X + X Y_1)$$

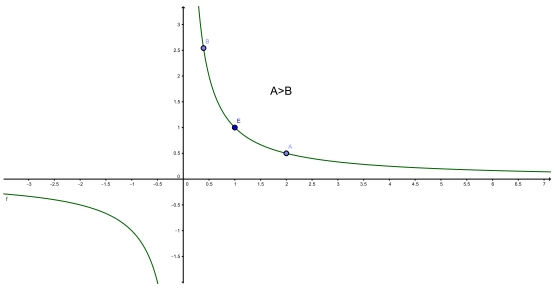
dans le premier.
En effet, la droite parallèle à $(M_1 M)$ passant par E a pour équation

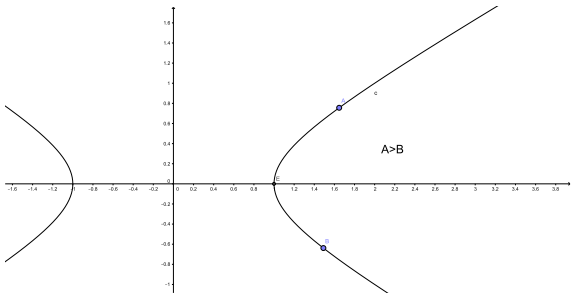
$$\tilde{y} - 1 = \frac{y - y_1}{x - x_1}(\tilde{x} - 1).$$

$\varphi(M)$ est donc l'intersection de cette droite avec l'hyperbole $\tilde{y} = \dfrac{1}{\tilde{x}}$. On trouve facilement le résultat attendu après quelques calculs.

• L'hyperbole $\mathcal{H}$ est la réunion de deux branches. On appelle $\mathcal{H}_0$ celle qui contient E.
On remarque que $(x, y) \in \mathcal{H}_0$ si et seulement si $(x, y) \in \mathcal{H}$ et $x > 0$. Comme $x_1 > 0$, il s'ensuit que $\mathcal{H}_0$ est stable par φ et forme même un sous-groupe de $\mathcal{H}$ pour $*$.

• On remarque que $p : (x, y) \in \mathcal{H}_0 \mapsto x \in \mathbb{R}^{+*}$ est bijective. On peut donc mettre l'ordre de $\mathbb{R}^{+*}$ sur $\mathcal{H}_0$.
De plus, $x = \sqrt{1 - dY^2} + \sqrt{d}Y$ (car $X^2 - dY^2 = 1$). Cette fonction de Y est strictement croissante donc l'ordre se lit indifféremment sur la coordonnée x ou sur la coordonnée Y.
Pour cet ordre, la fonction φ est strictement croissante sur $\mathcal{H}_0$ car $x_1 > 1$ (car $X_1 \geqslant 1$ et $Y_1 \geqslant 0$).





• Pour tout n entier, posons $M_n = M_1^n = (X_n, Y_n)$. Il est immédiat que $M_{-1} = (X_1, -Y_1)$ d'où on tire par récurrence que $Y_{-n} = -Y_n$ pour tout n entier. Comme φ est strictement croissante et que $M_{n+1} = \varphi(M_n)$, la suite (M_n) est strictement croissante. De plus, comme $X_1 \geqslant 1$, $Y_1 > 0$ et $X_n \geqslant 1$ pour tout n, $Y_{n+1} > Y_n$ pour tout $n \in \mathbb{Z}$. Comme les Y_n sont entiers, (Y_n) diverge vers $+\infty$.

• Soit $M = (X, Y)$ un point entier de $\mathcal{H}_0$. D'après ce qui précède, il existe un entier n tel que $Y_n \leqslant Y < Y_{n+1}$, donc $M_n \leqslant M < M_{n+1}$. Notons $M' = (X', Y') = M_{-n} \star M$. Grâce à la croissance stricte de φ, donc de φ^{-n}, on a $M_0 \leqslant M' < M_1$. Mais, par hypothèse, M_1 est la solution entière minimale de l'équation de Pell-Fermat, donc $M' = M_0$ puis $M = M_n$.

• On remarque pour terminer que la réflexion $\sigma : (X, Y) \mapsto (-X, Y)$ échange les deux branches de $\mathcal{H}$ et préserve $\mathbb{Z}^2$, et on peut affirmer que les points entiers de $\mathcal{H}$ sont les $(\pm X_n, Y_n)$ pour $n \in \mathbb{Z}$.
Comme les Y_n sont symétriques, on peut même dire que les points entiers sont les $\pm M_n$ pour $n \in \mathbb{Z}$.
On pose l'application

$$\begin{array}{rcl} \Gamma & \to & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \\ \varepsilon M_n & \mapsto & (\varepsilon, n) \end{array}$$

et on vérifie qu'elle forme bien un morphisme de groupes.
L'ensemble des points entiers de $\mathcal{H}$ forme donc bien un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. □

Corollaire.

Soit d un entier naturel supérieur ou égal à 2 et sans facteur carré, alors il existe une solution fondamentale $x_1 = X_1 + \sqrt{d}Y_1$ solution de l'équation de Pell-Fermat $X^2 - dY^2 = 1$ telle que l'ensemble des solutions soit $\{\pm x_1^n, n \in \mathbb{Z}\}$.

Démonstration. Les solutions de l'équation de Pell-Fermat sont exactement les points entiers de l'hyperbole précédente. □

Corollaire.

Soit d un entier naturel supérieur ou égal à 2 et sans facteur carré et tel que (-1) ne soit pas un carré modulo d, soit $A = \mathbb{Z}[\sqrt{d}]$, alors $A^\times \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Démonstration. Les inversibles de A sont les éléments de norme ± 1, en prenant la norme de $\mathbb{Q}(\sqrt{d})$ [1].
Les inversibles sont donc les points entiers des hyperboles $X^2 - dY^2 = \pm 1$. On connaît les points entiers de $X^2 - dY^2 = 1$. L'idée est donc de montrer qu'il n'y a pas de points entiers non triviaux sur $X^2 - dY^2 = -1$.
Si c'était le cas, on aurait $X^2 \equiv -1[d]$, ce qui est absurde car (-1) n'est pas un carré modulo d. □

Remarques : • Le problème des bœufs d'Hélios se résout à l'aide d'une équation de Pell-Fermat. L'entier d correspondant est de l'ordre de 10^{14}...
• La solution fondamentale de $X^2 - 15Y^2 = 1$ est $(4, 1)$. On peut ainsi trouver toutes les solutions. Pour cela, on écrit $x_n = x_1^n$ et soit on développe, soit on trouve une relation de récurrence suivie par X_n et Y_n.
Ici on a

$$x_{n+1} = (4 + \sqrt{15})x_n = (4 + \sqrt{15})(X_n + \sqrt{15}Y_n) = (4X_n + 15Y_n) + \sqrt{15}(X_n + 4Y_n),$$

1. A n'est pas toujours l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$, mais ça ne change rien à la caractérisation de ses inversibles. On a toujours $A^\times \subset \mathcal{O}(\mathbb{Q}(\sqrt{d}))^\times$. L'inverse reste le conjugué.

d'où

$$\begin{matrix} X_{n+1} = 4X_n + 15Y_n \\ Y_{n+1} = X_n + 4Y_n \end{matrix} .$$

• La solution fondamentale de $X^2 - 19Y^2 = 1$ est $(170, 39)$. C'est plus difficile à trouver. Il y a donc encore du travail à faire.
Pour prouver l'existence de la solution fondamentale, on utilise des développements en fraction continue. Cela donne explicitement (X_1, Y_1), mais c'est compliqué...
• Si d est premier et $d \equiv 3[4]$, on sait que (-1) n'est pas un carré modulo d. On a donc les exemples $d = 3, 7, 11, 19, ...$
Si $d = 15$, on a $\left(\frac{-1}{15}\right) = -1$ donc (-1) n'est pas un carré modulo 15. On peut donc aussi appliquer le corollaire dans ce cas là.
• En fait, le corollaire reste vrai même quand (-1) est un carré modulo d, c'est le théorème des unités de Dirichlet, mais c'est plus difficile à prouver.

Adapté du travail de Paul Alphonse.

Chapitre 11

Étude de $\mathrm{O}(p,q)$

Références : Caldero, Germoni, *Histoires hédonistes de groupes et de géométries*, p 211

Cadre : on note $\mathrm{O}(p,q)$ le sous groupe de $\mathrm{GL}_{p+q}(\mathbb{R})$ des isométries pour la forme quadratique $q(x) = x_1^2 + ... + x_p^2 - x_{p+1}^2 - x_{p+q}^2$. On note $I_{(p,q)} = \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix}$ et on rappelle que $M \in \mathrm{O}(p,q) \Leftrightarrow MI_{(p,q)}{}^{\mathrm{t}}M = I_{(p,q)}$.

Théorème.

Soient $p, q \geqslant 1$, alors il existe un homéomorphisme

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

Démonstration. • Prenons $M \in \mathrm{O}(p,q)$, alors par décomposition polaire, $M = OS$ avec $O \in \mathrm{O}(n)$ et $S \in \mathcal{S}_n^{++}$ pour $n = p+q$. Montrons que $O, S \in \mathrm{O}(p,q)$.
On pose $T = {}^{\mathrm{t}}MM$, alors $S^2 = T$.
On a $M \in \mathrm{O}(p,q)$ donc $MI_{(p,q)}{}^{\mathrm{t}}M = I_{(p,q)}$, donc ${}^{\mathrm{t}}M^{-1}I_{(p,q)}M^{-1} = I_{(p,q)}$, d'où ${}^{\mathrm{t}}M^{-1} \in \mathrm{O}(p,q)$ et ainsi ${}^{\mathrm{t}}M \in \mathrm{O}(p,q)$.
Donc $S^2 = T = {}^{\mathrm{t}}MM \in \mathrm{O}(p,q)$.

A présent, on sait que $T \in \mathcal{S}_n^{++}$, donc comme exp réalise un homéomorphisme de $\mathcal{S}_n$ sur $\mathcal{S}_n^{++}$, on a l'existence de $U \in \mathcal{S}_n$ tel que $T = \exp(U)$. Alors

$$\begin{aligned}
T \in \mathrm{O}(p,q) &\Leftrightarrow TI_{(p,q)}{}^{\mathrm{t}}T = I_{(p,q)} \\
&\Leftrightarrow {}^{\mathrm{t}}T = I_{(p,q)}T^{-1}I_{(p,q)} \\
&\Leftrightarrow {}^{\mathrm{t}}\exp(U) = I_{(p,q)}\exp(U)^{-1}I_{(p,q)}^{-1} \\
&\Leftrightarrow \exp({}^{\mathrm{t}}U) = \exp(-I_{(p,q)}UI_{(p,q)}^{-1}) \\
&\Leftrightarrow {}^{\mathrm{t}}U = U = -I_{(p,q)}UI_{(p,q)}^{-1} \text{ (par bijectivité de exp)} \\
&\Leftrightarrow UI_{(p,q)} + I_{(p,q)}U = 0 \\
&\Leftrightarrow \frac{U}{2}I_{(p,q)} + I_{(p,q)}\frac{U}{2} = 0 \\
&\Leftrightarrow {}^{\mathrm{t}}\exp(\frac{U}{2}) = I_{(p,q)}\exp(\frac{U}{2})^{-1}I_{(p,q)}^{-1} \text{ (en remontant les calculs comme précédemment).}
\end{aligned}$$

Comme $\exp(\frac{U}{2}) \in \mathcal{S}_n$ et $\exp(\frac{U}{2})^2 = T$, par unicité de la racine carrée, $S = \exp(\frac{U}{2})$ et donc $SI_{(p,q)}{}^{\mathrm{t}}S = I_{(p,q)}$.
Il vient $S \in \mathrm{O}(p,q)$, et donc $O \in \mathrm{O}(p,q)$.

On sait que la décomposition polaire induit l'homéomorphisme $\mathrm{GL}_n \cong \mathrm{O}(n) \times \mathcal{S}_n^{++}$, donc par le travail précédent, on a l'homéomorphisme

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

• Étudions $\mathrm{O}(p,q) \cap \mathrm{O}(n)$.

Soit O dans ce groupe, alors $OI_{(p,q)}{}^{\mathrm{t}}O = I_{(p,q)}$ et $O^{\mathrm{t}}O = I_n$. Si on écrit $O = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, alors

$$\begin{cases} A^{\mathrm{t}}A - B^{\mathrm{t}}B = I_p \\ A^{\mathrm{t}}C - B^{\mathrm{t}}D = 0 \\ C^{\mathrm{t}}A - D^{\mathrm{t}}B = 0 \\ C^{\mathrm{t}}C - D^{\mathrm{t}}D = -I_q \end{cases} \quad \text{et} \quad \begin{cases} A^{\mathrm{t}}A + B^{\mathrm{t}}B = I_p \\ A^{\mathrm{t}}C + B^{\mathrm{t}}D = 0 \\ C^{\mathrm{t}}A + D^{\mathrm{t}}B = 0 \\ C^{\mathrm{t}}C + D^{\mathrm{t}}D = I_q \end{cases}$$

On en déduit $B^{\mathrm{t}}B = 0$, donc comme $(M,N) \mapsto \mathrm{Tr}(M^{\mathrm{t}}N)$ est un produit scalaire, on a $B = 0$.
De même, on a $C = 0$. Ainsi $A \in \mathrm{O}(p)$ et $D \in \mathrm{O}(q)$.
On en déduit $\mathrm{O}(p,q) \cap \mathrm{O}(n) = \left\{ \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}, A \in \mathrm{O}(p), D \in \mathrm{O}(q) \right\} \cong \mathrm{O}(p) \times \mathrm{O}(q)$.

• Étudions $\mathrm{O}(p,q) \cap \mathcal{S}_n^{++}$.

On pose $L = \{U \in \mathcal{M}_n(\mathbb{R}), UI_{(p,q)} + I_{(p,q)}U = 0\}$, alors on a vu plus haut que exp réalise une bijection entre $L \cap \mathcal{S}_n$ et $\mathrm{O}(p,q) \cap \mathcal{S}_n^{++}$. Or l'exponentielle réalise un homéomorphisme de $\mathcal{S}_n$ sur $\mathcal{S}_n^{++}$ donc elle induit l'homéomorphisme $\mathrm{O}(p,q) \cap \mathcal{S}_n^{++} \cong L \cap \mathcal{S}_n$.

Soit $U = \begin{pmatrix} A & B \\ {}^{\mathrm{t}}B & D \end{pmatrix} \in \mathcal{S}_n$, avec A, D symétriques, alors comme $UI_{(p,q)} + I_{(p,q)}U = 2\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}$, on a $U \in L \Leftrightarrow A = 0$ et $D = 0$.
Il en découle que $L \cap \mathcal{S}_n = \left\{ \begin{pmatrix} 0 & B \\ {}^{\mathrm{t}}B & 0 \end{pmatrix}, B \in \mathcal{M}_{p,q} \right\}$ et on déduit l'homéomorphisme $L \cap \mathcal{S}_n \cong \mathbb{R}^{pq}$.

→ On a donc comme annoncé :

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

□

Corollaire.

1. $\mathrm{O}(p,q)$ est compact si et seulement si p ou q est nul.
2. $\mathrm{O}(p,q)$ a quatre composantes connexes si $p, q \neq 0$.
3. La composante connexe de l'identité est $\mathrm{SO}_0(p,q) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{SO}(p,q), A \in \mathrm{GL}_p^+ \right\}$.

La troisième propriété est la seule non évidente. On pourra trouver la preuve dans le H2G2.

Remarques : • Au fait, $\mathrm{O}(p,q)$ est un groupe. Pour le voir, on multiplie par l'inverse à gauche et sa transposée à droite dans $MI_{(p,q)}{}^{\mathrm{t}}M = I_{(p,q)}$ pour obtenir l'égalité voulue.
• On utilise beaucoup le fait que l'exponentielle réalise un homéomorphisme de $\mathcal{S}_n(\mathbb{R})$ sur $\mathcal{S}_n^{++}(\mathbb{R})$. On peut voir ça au chapitre 4.
• Le groupe $\mathrm{SO}_0(3,1)$ est appelé groupe de Lorentz restreint et sert en physique quantique et en électromagnétisme.
• En fait $\mathrm{O}(p,q)$ est un groupe de Lie car c'est un sous groupe fermé de $\mathrm{GL}(n)$ (voir le théorème de Cartan - Von Neumann au chapitre 39). En effet, pour M dans $\mathrm{O}(p,q)$, $M(I_{(p,q)}{}^{\mathrm{t}}MI_{(p,q)}) = I_n$ et si on pose l'application continue $\varphi : M \mapsto MI_{(p,q)}{}^{\mathrm{t}}M$ alors $\mathrm{O}(p,q) = \varphi^{-1}(I_{(p,q)})$.
L'algèbre de Lie associée est $\mathrm{Ker}(D\varphi(I_n)) = \{H \in \mathcal{M}_n(\mathbb{R}), HI_{(p,q)} + I_{(p,q)}{}^{\mathrm{t}}H = 0\}$ (l'espace tangent en l'identité). On reconnaît bien sûr l'ensemble L défini précédemment !

Chapitre 12

Étude du θ-schéma pour l'équation de la chaleur

Références : Quarteroni, Sacco, Saleri, *Méthodes numériques*, p 458-459
Di Menza, *Analyse numérique des équations aux dérivées partielles*, p 98

On étudie l'équation de la chaleur unidimensionnelle sur le pavé $[0,T]\times[0,L]$. Elle s'écrit comme suit, pour un paramètre $\nu>0$:

$$\frac{\partial u}{\partial t}-\nu\frac{\partial^2 u}{\partial x^2}=0.$$

On suppose connue l'existence de la solution classique. De plus, on peut montrer qu'elle est $\mathcal{C}^\infty$.

Notre but est d'approcher numériquement la solution de cette équation avec un schéma numérique aux différences finies particulier nommé le θ-schéma.

On se donne une discrétisation en temps $t_n=n\tau$ et en espace $x_j=jh$ avec $n\in[0,N]$, $j\in[0,J]$ et $N\tau=T$, $Jh=L$. On note u_j^n une approximation de $u(t_n,x_j)$ (que l'on va construire).
Pour $\theta\in[0,1]$, on définit le θ-schéma par

$$\frac{u_j^{n+1}-u_j^n}{\tau}=\nu\theta\frac{u_{j+1}^{n+1}-2u_j^{n+1}+u_{j-1}^{n+1}}{h^2}+\nu(1-\theta)\frac{u_{j+1}^n-2u_j^n+u_{j-1}^n}{h^2}.$$

Si les indices sortent du domaine défini, on leur donne la valeur 0 pour simplifier.

Théorème.

Le θ-schéma est convergent pour la norme l^2 si $\theta\geqslant\dfrac{1}{2}$, ou sous la condition CFL $(1-2\theta)\dfrac{2\nu\tau}{h^2}\leqslant 1$ si $\theta<\dfrac{1}{2}$.
Il est d'ordre un en temps et deux en espace si $\theta\neq\dfrac{1}{2}$ et d'ordre deux en temps et en espace sinon (schéma de Crank-Nicholson).

Démonstration. • Le schéma est-il bien défini ?
On note $u^n=(u_j^n)_j$ et

$$A_\Delta=\begin{pmatrix}2&-1&&&\\-1&2&-1&&\\&\ddots&\ddots&\ddots&\\&&-1&2&-1\\&&&-1&2\end{pmatrix}.$$

Alors le schéma se réécrit

$$\left(I+\theta\frac{\nu\tau}{h^2}A_\Delta\right)u^{n+1}=\left(I-(1-\theta)\frac{\nu\tau}{h^2}A_\Delta\right)u^n.$$

Le schéma est donc bien défini si $I+\theta\dfrac{\nu\tau}{h^2}A_\Delta$ est inversible.
Observons les valeurs propres de A_Δ :

On remarque que le vecteur $V_p = \left(\sin\left(\frac{jp\pi}{J+1}\right)\right)_j$ est vecteur propre de A_Δ pour la valeur propre $\lambda_p = 2\left(1-\cos\left(\frac{p\pi}{J+1}\right)\right)$ pour $p \in [1, J]$. Donc $\mathrm{Sp}(A_\Delta) = \left\{4\sin^2\left(\frac{p\pi}{2(J+1)}\right)\right\}$.
Il vient donc

$$\min \mathrm{Sp}(I + \theta\frac{\nu\tau}{h^2}A_\Delta) = 1 + \theta\frac{4\nu\tau}{h^2}\sin^2\left(\frac{\pi}{2(J+1)}\right) > 0.$$

Donc $I + \theta\frac{\nu\tau}{h^2}A_\Delta$ est inversible et le schéma est bien défini.

- Consistance du schéma. [1]

Il s'agit d'utiliser les formules de Taylor pour montrer que la vraie solution vérifie avec un bon ordre le schéma. On remarque d'abord que

$$\frac{u(t_{n+1}, x_j) - u(t_n, x_j)}{\tau} = \frac{\partial u}{\partial t}(t_n, x_j) + \frac{\tau}{2}\frac{\partial^2 u}{\partial t^2}(t_n, x_j) + O(\tau^2).$$

Puis

$$\begin{aligned}\frac{u(t_n, x_{j+1}) - 2u(t_n, x_j) + u(t_n, x_{j-1})}{h^2} &= \frac{1}{h}\left(\frac{\partial u}{\partial x}(t_n, x_j) + \frac{h}{2}\frac{\partial^2 u}{\partial x^2}(t_n, x_j) + \frac{h^2}{3!}\frac{\partial^3 u}{\partial x^3}(t_n, x_j) + O(h^3)\right.\\ &\quad \left. - \frac{\partial u}{\partial x}(t_n, x_j) + \frac{h}{2}\frac{\partial^2 u}{\partial x^2}(t_n, x_j) - \frac{h^2}{3!}\frac{\partial^3 u}{\partial x^3}(t_n, x_j) + O(h^3)\right)\\ &= \frac{\partial^2 u}{\partial x^2}(t_n, x_j) + O(h^2).\end{aligned}$$

De même,

$$\begin{aligned}\frac{u(t_{n+1}, x_{j+1}) - 2u(t_{n+1}, x_j) + u(t_{n+1}, x_{j-1})}{h^2} &= \frac{\partial^2 u}{\partial x^2}(t_{n+1}, x_j) + O(h^2)\\ &= \frac{1}{\nu}\frac{\partial u}{\partial t}(t_{n+1}, x_j) + O(h^2)\\ &= \frac{1}{\nu}\frac{\partial u}{\partial t}(t_n, x_j) + \frac{\tau}{\nu}\frac{\partial^2 u}{\partial t^2}(t_n, x_j) + O(h^2 + \tau^2)\end{aligned}$$

En remplaçant tous ces termes dans le schéma, on obtient l'erreur de consistance en (t_n, x_j) ε_j^n :

$$\begin{aligned}\varepsilon_j^n &= \frac{\partial u}{\partial t}(t_n, x_j) + \frac{\tau}{2}\frac{\partial^2 u}{\partial t^2}(t_n, x_j) - \theta\frac{\partial u}{\partial t}(t_n, x_j) - \tau\theta\frac{\partial^2 u}{\partial t^2}(t_n, x_j) - \nu(1-\theta)\frac{\partial^2 u}{\partial x^2}(t_n, x_j) + O(h^2 + \tau^2)\\ &= (1-\theta)\left(\frac{\partial u}{\partial t} - \nu\frac{\partial^2 u}{\partial x^2}\right)(t_n, x_j) + \tau\left(\frac{1}{2} - \theta\right)\frac{\partial^2 u}{\partial t^2}(t_n, x_j) + O(h^2 + \tau^2)\\ &= \tau\left(\frac{1}{2} - \theta\right)\frac{\partial^2 u}{\partial t^2}(t_n, x_j) + O(h^2 + \tau^2)\end{aligned}$$

On a $\max_n \|\varepsilon^n\| = O(h^2 + \tau)$, donc le schéma est consistant.
De plus, si $\theta = \frac{1}{2}$, on gagne un ordre en temps !

- Stabilité du schéma.

On a

$$u^{n+1} = \left(I + \theta\frac{\nu\tau}{h^2}A_\Delta\right)^{-1}\left(I - (1-\theta)\frac{\nu\tau}{h^2}A_\Delta\right)u^n.$$

Si on écrit $B = \left(I + \theta\frac{\nu\tau}{h^2}A_\Delta\right)^{-1}\left(I - (1-\theta)\frac{\nu\tau}{h^2}A_\Delta\right)$, alors son spectre est

$$\mathrm{Sp}(B) = \left\{\left(1 + \theta\frac{4\nu\tau}{h^2}\sin^2\left(\frac{p\pi}{2(J+1)}\right)\right)^{-1}\left(1 - (1-\theta)\frac{4\nu\tau}{h^2}\sin^2\left(\frac{p\pi}{2(J+1)}\right)\right)\right\}$$

En simplifiant,

$$\mathrm{Sp}(B) = \left\{1 - \left(1 + \theta\frac{4\nu\tau}{h^2}\sin^2\left(\frac{p\pi}{2(J+1)}\right)\right)^{-1}\frac{4\nu\tau}{h^2}\sin^2\left(\frac{p\pi}{2(J+1)}\right)\right\} \subset]-\infty, 1[$$

1. Selon la leçon, on va plus ou moins vite sur cette partie.

La méthode est donc stable si et seulement si $\rho(B) \leqslant 1$ (car B est symétrique), c'est à dire si et seulement si pour tout $p \in [1, J]$, on a

$$\frac{4\nu\tau}{h^2}\sin^2\left(\frac{p\pi}{2(J+1)}\right) \leqslant 2\left(1+\theta\frac{4\nu\tau}{h^2}\sin^2\left(\frac{p\pi}{2(J+1)}\right)\right).$$

Donc si et seulement si

$$(2\theta-1)\frac{2\nu\tau}{h^2}\sin^2\left(\frac{J\pi}{2(J+1)}\right) \geqslant -1.$$

On voit d'abord que si $\theta \geqslant \dfrac{1}{2}$, alors le schéma est inconditionnellement stable.

Si ce n'est pas le cas, comme on peut faire tendre $\sin^2\left(\dfrac{J\pi}{2(J+1)}\right)$ vers 1 en augmentant J, il faut que la condition $(1-2\theta)\dfrac{2\nu\tau}{h^2} \leqslant 1$ soit vérifiée.

On retrouve ainsi les conditions du théorème.

• Autre version de la stabilité pour la leçon 110 (transformée de Fourier discrète).
On applique la transformée de Fourier discrète à notre schéma : pour tout $\xi \in \left[-\dfrac{\pi}{h}, \dfrac{\pi}{h}\right]$, on a

$$\widehat{u^{n+1}} = \widehat{u^n} + \frac{\nu\theta\tau}{h^2}(e^{ih\xi} - 2 + e^{-ih\xi})\widehat{u^{n+1}} + \frac{\nu(1-\theta)\tau}{h^2}(e^{ih\xi} - 2 + e^{-ih\xi})\widehat{u^n}.$$

Or $e^{ih\xi} - 2 + e^{-ih\xi} = 2(\cos(h\xi) - 1) = -4\sin^2\left(\dfrac{h\xi}{2}\right)$, d'où il vient

$$\widehat{u^{n+1}} = \left(1 + \frac{4\nu\theta\tau}{h^2}\sin^2\left(\frac{h\xi}{2}\right)\right)^{-1}\left(1 - \frac{4\nu(1-\theta)\tau}{h^2}\sin^2\left(\frac{h\xi}{2}\right)\right)\widehat{u^n}.$$

Le schéma est stable si et seulement si le coefficient d'amplification est de module inférieur ou égal à 1. On retrouve ainsi les calculs présentés précédemment et on obtient la même condition CFL en évaluant en $\xi = \dfrac{\pi}{h}$.

• Convergence du schéma.
On va reprouver le théorème de Lax qui dit qu'un schéma stable et consistant est convergeant, c'est à dire $\max\limits_n \|u^n - v^n\| \underset{h,\tau\to 0}{\to} 0$, où on note v^n le vecteur donné par la solution exacte évalué au temps t_n et en les points x_j.

On a $v^{n+1} = Bv^n + \tau\varepsilon^n$, donc si l'on pose $w_n = v_n - u_n$, on a

$$w^{n+1} = Bw^n + \tau\varepsilon^n.$$

Donc $w^n = B^n w^0 + \tau\sum\limits_{k=0}^{n-1} B^k\varepsilon^k$.
Puis on sait que $w^0 = 0$, $\|B\| \leqslant 1$ (par stabilité) et $\max\limits_n \|\varepsilon^n\| \underset{h,\tau\to 0}{\to} 0$ (par consistance), donc

$$\max_n \|w^n\| \leqslant \underbrace{N\tau}_{=T} \max_n \|\varepsilon^n\| \underset{h,\tau\to 0}{\to} 0.$$

Le schéma est donc convergent.

□

Remarques : • On peut aussi étudier la stabilité l^∞, mais la l^2 est plus simple : il suffit d'étudier le rayon spectral.
En effet, si $\rho(B) \leqslant 1$, alors

$$\left\|u^{n+1}\right\|_2 = \|Bu^n\|_2 \leqslant \|B\|_2 \|u^n\|_2 = \rho(B)\|u^n\|_2 \leqslant \|u^n\|_2.$$

Donc $\|u^n\|_2 \leqslant \left\|u^0\right\|_2$ et on a la stabilité.

Si au contraire $\rho(B) > 1$, alors on a une valeur propre de module strictement plus grand que 1, donc en prenant pour condition initiale le vecteur propre associé, on explose.
• Si c'est trop long, on peut juste étudier le cas $\theta = 0$.

Chapitre 13

Formule des compléments

Références : Amar, Matheron, *Analyse complexe*, p 249-251

Théorème.

On rappelle qu'on définit la fonction Gamma d'Euler par :

$$\forall z \in \{s \in \mathbb{C} | \Re(s) > 0\}, \Gamma(z) = \int_0^{+\infty} t^{z-1} e^{-t} \, \mathrm{d}t$$

On a l'égalité suivante :

$$\forall z \in \{s \in \mathbb{C} | 0 < \Re(s) < 1\}, \Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z}$$

Démonstration. D'après le théorème des zéros isolés, il suffit de prouver l'égalité pour $z = \alpha \in]0,1[$. Soit donc $\alpha \in]0,1[$.
En utilisant le théorème de Fubini, on obtient :

$$\begin{aligned}\Gamma(\alpha)\Gamma(1-\alpha) &= \left(\int_0^{+\infty} t^{\alpha-1} e^{-t} \, \mathrm{d}t\right)\left(\int_0^{+\infty} s^{-\alpha} e^{-s} \, \mathrm{d}s\right) = \int_0^{+\infty}\int_0^{+\infty} s^{-\alpha} t^{\alpha-1} e^{-t-s} \, \mathrm{d}t \, \mathrm{d}s \\ &= \int_0^{+\infty}\int_0^{+\infty} \left(\frac{t}{s}\right)^{\alpha} e^{-(s+t)} \, \mathrm{d}s \, \frac{\mathrm{d}t}{t}\end{aligned}$$

On réalise le changement de variables donné par le système $\begin{cases} u &= s+t \\ v &= \dfrac{s}{t} \end{cases}$ et dont le jacobien vaut

$$\left|\det \begin{pmatrix} 1 & 1 \\ \frac{1}{t} & \frac{-s}{t^2} \end{pmatrix}\right| = \frac{1}{t} + \frac{s}{t^2} = \frac{1}{t} + \frac{v}{t} = \frac{v+1}{t}$$

On en déduit donc :

$$\Gamma(\alpha)\Gamma(1-\alpha) = \int_0^{+\infty}\int_0^{+\infty} v^{-\alpha} e^{-u} \frac{\mathrm{d}u \, \mathrm{d}v}{v+1} = \int_0^{+\infty} \frac{1}{v^{\alpha}(v+1)} \int_0^{+\infty} e^{-u} \, \mathrm{d}u \, \mathrm{d}v = \int_0^{+\infty} \frac{\mathrm{d}v}{v^{\alpha}(v+1)}.$$

Le lemme suivant termine la preuve. □

Lemme.

On a l'égalité suivante :

$$\forall \alpha \in]0,1[, \int_0^{+\infty} \frac{\mathrm{d}t}{t^{\alpha}(1+t)} = \frac{\pi}{\sin \pi\alpha}$$

Démonstration. $\forall \alpha \in]0,1[$, on définit $I_\alpha := \displaystyle\int_0^{+\infty} \frac{\mathrm{d}t}{t^\alpha(1+t)}$.
I_α est bien définie car c'est l'intégrale d'une fonction mesurable positive ; on a même $I_\alpha < +\infty$. En effet :

— $t \mapsto \dfrac{1}{t^\alpha(1+t)}$ est continue sur $]0,+\infty[$ (donc localement intégrable) ;

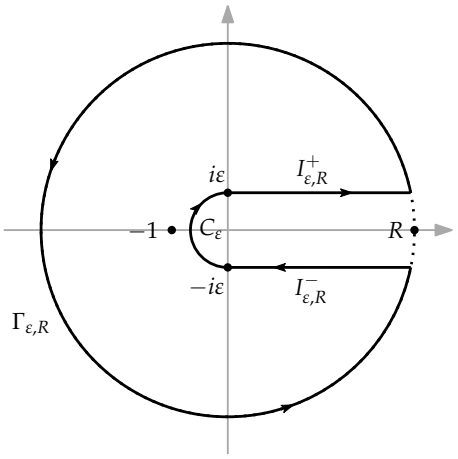
— En 0 : $\dfrac{1}{t^\alpha(1+t)} \underset{t\to 0}{\sim} \dfrac{1}{t^\alpha}$, qui est intégrable car $0<\alpha<1$;

— En $+\infty$: $\dfrac{1}{t^\alpha(1+t)} \underset{t\to+\infty}{\sim} \dfrac{1}{t^{\alpha+1}}$, qui est intégrable car $\alpha+1>1$.

On note $\Omega = \mathbb{C}\backslash\mathbb{R}^+$, on prend la définition de l'argument associée à Ω [1] et on note $f : \left|\begin{array}{ccc} \Omega\backslash\{-1\} & \to & \mathbb{C} \\ z & \mapsto & \dfrac{1}{z^\alpha(1+z)} \end{array}\right.$,

où l'on convient $z^\alpha = r^\alpha e^{i\alpha\theta}$ quand $z = re^{i\theta}$, où $\theta \in]0,2\pi[$.
La fonction f est holomorphe sur $\Omega\backslash\{-1\}$ et possède un pôle simple en -1 avec :

$$\mathrm{Res}(f,-1) = \lim_{z\to -1}(1+z)f(z) = \frac{1}{(-1)^\alpha} = e^{-i\pi\alpha}$$



Pour $R>1$ et $\varepsilon<1$, on définit le chemin orienté (voir dessin) $\gamma_{\varepsilon,R} = C_\varepsilon \cup I^+_{\varepsilon,R} \cup \Gamma_{\varepsilon,R} \cup I^-_{\varepsilon,R}$, où :

— $C_\varepsilon = \left\{ \varepsilon e^{i\theta} \middle| \theta \in \left[\frac{\pi}{2}, \frac{3\pi}{2}\right] \right\}$;

— $I^\pm_{\varepsilon,R} = \left[\pm\varepsilon i, \pm\varepsilon i + \sqrt{R^2-\varepsilon^2}\right]$;

— $\Gamma_{\varepsilon,R} = \left\{ Re^{i\theta} \middle| \theta \in [\theta_{\varepsilon,R}, 2\pi - \theta_{\varepsilon,R}] \right\}$,
avec $\theta_{\varepsilon,R} = \arctan\left(\dfrac{\varepsilon}{\sqrt{R^2-\varepsilon^2}}\right)$.

Le théorème des résidus donne donc :

$$\int_{\gamma_{\varepsilon,R}} f(z)\,\mathrm{d}z = 2i\pi e^{-i\pi\alpha}$$

On va passer à la limite quand $R\to+\infty$ et $\varepsilon\to 0$.

- Sur C_ε, on a
$$\left|\int_{C_\varepsilon} f(z)\mathrm{d}z\right| \leqslant \frac{1}{\varepsilon^\alpha(1-\varepsilon)} \times \pi\varepsilon = \frac{\pi\varepsilon^{(1-\alpha)}}{1-\varepsilon} \underset{\varepsilon\to 0}{\longrightarrow} 0.$$
- Sur $\Gamma_{\varepsilon,R}$, on a
$$\left|\int_{\Gamma_{\varepsilon,R}} f(z)\,\mathrm{d}z\right| \leqslant \left|\int_0^{2\pi} f(z)\,\mathrm{d}z\right| \leqslant 2\pi\frac{R^{1-\alpha}}{R-1} \underset{R\to+\infty}{\longrightarrow} 0.$$
- Sur $I^+_{\varepsilon,R}$, on a
$$\int_{I^+_{\varepsilon,R}} f(z)\,\mathrm{d}z = \int_0^{\sqrt{R^2-\varepsilon^2}} f(\varepsilon i + t)\,\mathrm{d}t = \int_0^{\sqrt{R^2-\varepsilon^2}} \frac{1}{(t+\varepsilon i)^\alpha(1+t+\varepsilon i)}\,\mathrm{d}t.$$

Or $(t+\varepsilon i)^\alpha \underset{\varepsilon\to 0}{\longrightarrow} t^\alpha$, donc comme

— $\mathbb{1}_{]0,\sqrt{R^2-\varepsilon^2}]}(t) f(\varepsilon i + t) \longrightarrow \mathbb{1}_{\mathbb{R}^{+*}}(t)\dfrac{1}{t^\alpha(1+t)}$;

— $\left|\mathbb{1}_{]0,\sqrt{R^2-\varepsilon^2}]}(t) f(\varepsilon i + t)\right| \leqslant \mathbb{1}_{\mathbb{R}^{+*}}(t)\dfrac{1}{|t-\varepsilon|^\alpha(1+t)}$ qui est intégrable,

par théorème de convergence dominée, on déduit :

$$\lim \int_{I^+_{\varepsilon,R}} f(z)\,\mathrm{d}z = I_\alpha$$

- Enfin, de la même façon, en utilisant le fait que $(t-\varepsilon i)^\alpha \underset{\varepsilon\to 0}{\longrightarrow} t^\alpha e^{2i\pi\alpha}$ ([2]), on a :
$$\lim \int_{I^-_{\varepsilon,R}} f(z)\,\mathrm{d}z = -e^{-2i\pi\alpha} I_\alpha$$

1. Il est important d'insister sur ce point ! Si l'on prenait la détermination sur $]-\pi,\pi[$, nos intégrales ne seraient pas définies.
2. C'est ici que notre définition de l'argument sur $]0,2\pi[$ prend du sens : dans le premier cas, on est à partie imaginaire positive, alors qu'ici on tend vers t à partie imaginaire négative.

Conclusion : en tenant compte de l'orientation des intégrales, notre théorème des résidus donne

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

On a donc bien

$$I_\alpha = \frac{\pi}{\sin \pi\alpha}.$$

□

Remarques : • J'admets qu'appeler un contour $\Gamma_{\varepsilon,R}$ quand on étudie la fonction Γ n'est pas très malin.
• Une application importante de la formule des compléments est le prolongement méromorphe sur $\mathbb{C}$ de ζ (voir Amar, Matheron, p252-254).
La fonction ζ sert partout et son prolongement permet notamment de donner du sens à des sommes non définies du type $1 + 2 + 3 + 4 + 5 + ...$ Elle permet aussi d'étudier les nombres premiers et leur répartition.
Cela devrait suffire comme application. ♡
• Il y a une autre application au calcul de $\displaystyle\int_x^{x+1} \log(\Gamma(s))\mathrm{d}s$ à la page 54 du Chambert-Loir (analyse 2). (Merci Cléééééééééééééééééééééément Vince !)

Adapté du travail de Florian Lemonnier.

Chapitre 14

Formule sommatoire de Poisson

Références : Gourdon, *Les maths en tête - Analyse*, problème 4.6.4 et exercice 3.4.4
Willem, *Analyse harmonique réelle*, exemple 7.29.f
Lesfari, *Distributions, analyse de Fourier et transformation de Laplace*, p 254

Théorème.

Soit $f \in \mathcal{S}(\mathbb{R})$.
Alors la série $\sum_{n\in\mathbb{Z}} f(.+n)$ converge normalement sur tout compact de $\mathbb{R}$ et :

$$\forall x \in \mathbb{R}, \sum_{n\in\mathbb{Z}} f(x+n) = \sum_{n\in\mathbb{Z}} \widehat{f}(n) e^{2i\pi nx},$$

où on a noté $\widehat{f}(x) = \int_{-\infty}^{+\infty} f(t)e^{-2i\pi xt}\,\mathrm{d}t$, pour $x \in \mathbb{R}$.

Démonstration. 1. Comme $f \in \mathcal{S}(\mathbb{R})$, en particulier, $\forall k \in \mathbb{N}, f^{(k)}(x) = \mathcal{O}_{+\infty}\left(\frac{1}{x^2}\right)$.
Ainsi, $\exists M > 0, \forall x \in \mathbb{R}, |f(x)| \leqslant \frac{M}{(1+x)^2}$.
D'où $\forall K > 0, \forall x \in [-K, K], \forall n \in \mathbb{Z}, |n| \geqslant K \Rightarrow |f(x+n)| \leqslant \frac{M}{(x+n+1)^2} \leqslant \frac{M}{(|n+1|-K)^2}$.
Donc la série $\sum_{n\in\mathbb{Z}} f(.+n)$ converge normalement sur tout compact.
On note F sa limite simple.
De façon similaire, on montre que $\sum_{n\in\mathbb{Z}} f'(.+n)$ converge normalement sur tout compact, donc uniformément sur tout segment de $\mathbb{R}$.
On peut donc appliquer le théorème de dérivation des séries de fonctions (on rappelle que f est $\mathcal{C}^1$) : la fonction F est de classe $\mathcal{C}^1$ sur $\mathbb{R}$ (en fait le théorème dit d'abord "sur tout segment de $\mathbb{R}$") et $\forall x \in \mathbb{R}, F'(x) = \sum_{n\in\mathbb{Z}} f'(x+n)$.

2. Par ailleurs, soit $x \in \mathbb{R}$: $\forall N \in \mathbb{N}, \sum_{n=-N}^{N} f(x+1+n) = \sum_{n=-N+1}^{N+1} f(x+n)$.
Donc en faisant tendre N vers l'infini, on obtient $F(x+1) = F(x)$; F est donc 1-périodique.
On va calculer ses coefficients de Fourier, pour $N \in \mathbb{Z}$:

$$\begin{aligned} c_N(F) &= \int_0^1 F(t)e^{-2i\pi Nt}\,\mathrm{d}t \underset{\text{(cvu)}}{=} \sum_{n\in\mathbb{Z}} \int_0^1 f(t+n)e^{-2i\pi Nt}\,\mathrm{d}t = \sum_{n\in\mathbb{Z}} \int_n^{n+1} f(t)e^{-2i\pi Nt}e^{2i\pi Nn}\,\mathrm{d}t \\ &\underset{1}{=} \int_{-\infty}^{+\infty} f(t)e^{-2i\pi Nt}\,\mathrm{d}t = \widehat{f}(N) \end{aligned}$$

Comme F est $\mathcal{C}^1$ sur $\mathbb{R}$, sa série de Fourier converge normalement vers F sur $\mathbb{R}$ et :

$$\forall x \in \mathbb{R}, F(x) = \sum_{n\in\mathbb{Z}} \hat{f}(n) e^{2i\pi nx}.$$ [2]

□

Corollaire (Une distribution invariante par transformation de Fourier)**.**

On note $\delta_{\mathbb{Z}} = \sum_{k\in\mathbb{Z}} \delta_k$.
Alors $\delta_{\mathbb{Z}} \in \mathcal{S}'(\mathbb{R})$ et on a $\delta_{\mathbb{Z}} = \widehat{\delta_{\mathbb{Z}}}$.

Démonstration. 1. Montrons que $\delta_{\mathbb{Z}}$ définit bien un élément de $\mathcal{S}'(\mathbb{R})$.
D'après ce qu'on vient de faire : $\forall \varphi \in \mathcal{S}(\mathbb{R}), \langle \delta_{\mathbb{Z}}, \varphi\rangle = \sum_{k\in\mathbb{Z}} \varphi(k)$ est bien défini.
Reste à montrer que $\delta_{\mathbb{Z}}$ est une distribution tempérée.
On rappelle que $\|.\|_{n,p} : \varphi \mapsto \sup_{x\in\mathbb{R}} \left|x^n \varphi^{(p)}(x)\right|$, où $n, p \in \mathbb{N}$, sont les semi-normes qui définissent la topologie de $\mathcal{S}(\mathbb{R})$.

$$\begin{aligned}\forall \varphi \in \mathcal{S}(\mathbb{R}), |\langle \delta_{\mathbb{Z}}, \varphi\rangle| &\leqslant \sum_{k\in\mathbb{Z}} |\varphi(k)| = |\varphi(0)| + \sum_{k\in\mathbb{Z}^*} \frac{1}{k^2} \left|k^2 \varphi(k)\right| \\ &\leqslant \|\varphi\|_{0,0} + \sum_{k\in\mathbb{Z}^*} \frac{1}{k^2} \|\varphi\|_{2,0} \leqslant \frac{\pi^2}{3} \left(\|\varphi\|_{0,0} + \|\varphi\|_{2,0}\right)\end{aligned}$$

Ainsi, $\delta_{\mathbb{Z}} \in \mathcal{S}'(\mathbb{R})$.

2. On peut donc calculer sa transformée de Fourier, en utilisant la formule de Poisson en 0 :

$$\forall \varphi \in \mathcal{S}(\mathbb{R}), \langle \widehat{\delta_{\mathbb{Z}}}, \varphi\rangle = \langle \delta_{\mathbb{Z}}, \widehat{\varphi}\rangle = \sum_{n\in\mathbb{Z}} \widehat{\varphi}(n) = \sum_{n\in\mathbb{Z}} \varphi(n) = \langle \delta_{\mathbb{Z}}, \varphi\rangle.$$

Donc $\widehat{\delta_{\mathbb{Z}}} = \delta_{\mathbb{Z}}$.

□

Corollaire (Formule d'inversion de Fourier dans $\mathcal{S}(\mathbb{R})$)**.**

Si $\varphi \in \mathcal{S}(\mathbb{R})$, alors

$$\varphi(x) = \int_{-\infty}^{+\infty} \widehat{\varphi}(\xi) e^{2i\pi x\xi} \mathrm{d}\xi.$$

Démonstration. Soit $t \in [0,1]$, on pose $\psi(x) = e^{2i\pi tx}\varphi(x)$, alors le corollaire précédent donne (en appliquant $\delta_{\mathbb{Z}}$ à ψ)

$$\sum_{k=-\infty}^{+\infty} \psi(k) = \sum_{k=-\infty}^{+\infty} \widehat{\psi}(k) = \sum_{k=-\infty}^{+\infty} \widehat{\widehat{\psi}}(k).$$

Cela se réécrit après quelques petits calculs :

$$\sum_{k=-\infty}^{+\infty} e^{2i\pi tk}\varphi(k) = \sum_{k=-\infty}^{+\infty} \widehat{\varphi}(k-t) = \sum_{k=-\infty}^{+\infty} \widehat{\widehat{\varphi}}(k) e^{-2i\pi tk}.$$

Comme ces séries convergent normalement sur $[0,1]$, on peut légitimement intégrer en t (et permuter les signes somme et intégrale).

1. L'intégrale converge car $f(t) = \mathcal{O}_{+\infty}\left(\frac{1}{t^2}\right)$.
2. Rappelons que la période de F vaut 1.

On a donc, comme $\int_0^1 e^{2i\pi kt}\mathrm{d}t = \delta_{k,0}$, l'égalité $\varphi(0) = \widehat{\widehat{\varphi}}(0)$.

On applique cette formule à $\zeta(x) = \varphi(x+t)$ (avec $t \in \mathbb{R}$ cette fois), ainsi, comme $\widehat{\zeta}(\xi) = \widehat{\varphi}(\xi)e^{2i\pi\xi t}$ et $\widehat{\widehat{\zeta}}(x) = \widehat{\widehat{\varphi}}(x-t)$, on a

$$\varphi(t) = \zeta(0) = \widehat{\widehat{\zeta}}(0) = \widehat{\widehat{\varphi}}(-t).$$

C'est bien la formule d'inversion de Fourier ! □

Remarques : • Pour tout faire dans les temps, il vaut mieux connaître par coeur toutes les propriétés liées à la compatibilité entre l'opérateur translation et la transformée de Fourier.
• On a aussi un autre résultat (Gourdon).

Corollaire (Une égalité entre deux sommes)**.**

On a

$$\forall s > 0, \sum_{n\in\mathbb{Z}} e^{-\pi n^2 s} = \frac{1}{\sqrt{s}} \sum_{n\in\mathbb{Z}} e^{-\frac{\pi n^2}{s}}.$$

Démonstration. Soit $\alpha > 0$, on va appliquer la formule sommatoire de Poisson à $f : x \mapsto e^{-\alpha x^2}$.
Soit $n \in \mathbb{Z}$, $\widehat{f}(n) = \displaystyle\int_{-\infty}^{+\infty} e^{-\alpha t^2} e^{-2i\pi nt}\,\mathrm{d}t = \frac{1}{\sqrt{\alpha}} \int_{-\infty}^{+\infty} e^{-u^2} e^{-2i\pi n \frac{u}{\sqrt{\alpha}}}\,\mathrm{d}u = \frac{1}{\sqrt{\alpha}} I(n)$, où on a posé $u = \sqrt{\alpha}t$ et $\forall x \in \mathbb{R}, I(x) := \displaystyle\int_{-\infty}^{+\infty} e^{-u^2} e^{-2i\pi x \frac{u}{\sqrt{\alpha}}}\,\mathrm{d}u$.
On va chercher une équation différentielle vérifiée par I ;

→ I est dérivable, en effet : posons $h : (x,u) \mapsto e^{-u^2} e^{-2i\pi x \frac{u}{\sqrt{\alpha}}}$.
— $\forall x \in \mathbb{R}, h(x,.)$ est $\mathcal{C}^1$ et intégrable (par comparaison avec l'intégrale de Gauss) ;
— $\forall x, u \in \mathbb{R}, \dfrac{\partial h}{\partial x}(x,u) = -2i\pi \dfrac{u}{\sqrt{\alpha}} e^{-u^2} e^{-2i\pi x \frac{u}{\sqrt{\alpha}}}$;
— $\dfrac{\partial h}{\partial x}$ est continue sur $\mathbb{R}^2$ et $\forall x, u \in \mathbb{R}, \left|\dfrac{\partial h}{\partial x}(x,u)\right| \leqslant \dfrac{2\pi u}{\sqrt{\alpha}} e^{-u^2}$, fonction majorante à la fois intégrable et indépendante de x.
On en déduit en plus que $I'(x) = \dfrac{-2i\pi}{\sqrt{\alpha}} \displaystyle\int_{-\infty}^{+\infty} u e^{-u^2} e^{-2i\pi x \frac{u}{\sqrt{\alpha}}}\,\mathrm{d}u$.

→ Par une intégration par parties :

$$\begin{aligned} I(x) &= \left[e^{-u^2} \frac{-\sqrt{\alpha}}{2i\pi x} e^{-2i\pi x \frac{u}{\sqrt{\alpha}}}\right]_{-\infty}^{+\infty} - \int_{-\infty}^{+\infty} -2u e^{-u^2} \frac{-\sqrt{\alpha}}{2i\pi x} e^{-2i\pi x \frac{u}{\sqrt{\alpha}}}\,\mathrm{d}u \\ &= 0 - \frac{\sqrt{\alpha}}{i\pi x} \int_{-\infty}^{+\infty} u e^{-u^2} e^{-2i\pi x \frac{u}{\sqrt{\alpha}}}\,\mathrm{d}u \\ &= -\frac{\sqrt{\alpha}}{i\pi x} \frac{\sqrt{\alpha}}{-2i\pi} I'(x) = -\frac{\alpha}{2\pi^2 x} I'(x) \end{aligned}$$

Donc $I(x) = I(0)\exp\left(-\dfrac{\pi^2 x^2}{\alpha}\right) = \sqrt{\pi}\exp\left(-\dfrac{\pi^2 x^2}{\alpha}\right)$.

Ainsi, $\widehat{f}(n) = \sqrt{\dfrac{\pi}{\alpha}}\exp\left(-\dfrac{\pi^2 n^2}{\alpha}\right)$.

On applique la formule de Poisson en 0 : $\displaystyle\sum_{n\in\mathbb{Z}} e^{-\alpha n^2} = \sum_{n\in\mathbb{Z}} \sqrt{\frac{\pi}{\alpha}} e^{-\frac{\pi^2 n^2}{\alpha}}$.

On pose enfin $s = \dfrac{\pi}{\alpha}$, et alors : $\displaystyle\sum_{n\in\mathbb{Z}} e^{-\frac{n^2\pi}{s}} = \sqrt{s} \sum_{n\in\mathbb{Z}} e^{-\pi n^2 s}$. □

Adapté du travail de Florian Lemonnier et sur une idée de Clément Vince.

Chapitre 15

Groupe circulaire

Références : Audin, *Géométrie*, p 203

On définit G le groupe de transformations de $\mathbb{P}_1(\mathbb{C})$ engendré par les homographies et la symétrie $z \mapsto \overline{z}$. Le groupe G contient donc $\mathrm{PGL}_2(\mathbb{C})$ et les inversions.

Théorème.

Le groupe G est exactement l'ensemble des transformations **bijectives** préservant les droites-cercles de $\mathbb{P}_1(\mathbb{C})$.

Démonstration. $\subset$ La conjugaison complexe préserve les droites cercles.
Passons aux homographies :
On rappelle que pour que quatre points de $\mathbb{P}_1(\mathbb{C})$ soient sur une droite-cercle, il faut et il suffit que leur birapport soit réel.
Donnons-nous un droite-cercle D, ainsi que trois points distincts a, b et c le définissant, et une homographie h. Alors pour tout z sur D, on sait que $h(a)$, $h(b)$, $h(c)$ et $h(z)$ sont alignés ou cocycliques car les homographies conservent le birapport [1]. Comme $h(a)$, $h(b)$ et $h(c)$ déterminent entièrement le cercle-droite image D', pour tout z sur D, $h(z)$ est sur D'. Par bijectivité de h, on a $h(D) = D'$.

$\supset$ Réciproquement, soit φ une bijection de $\mathbb{P}_1(\mathbb{C})$ préservant les droite-cercles. Pour simplifier, on peut composer à gauche φ par une homographie (ce qui ne change pas son appartenance à G) pour que $\varphi(0) = 0$, $\varphi(1) = 1$ et $\varphi(\infty) = \infty$, ainsi elle envoie les cercles sur les cercles et les droites sur les droites.
Commençons par montrer que φ préserve les divisions harmoniques. [2]

Lemme.

Toute application bijective f préservant les droite-cercles préserve aussi les divisions harmoniques.

Démonstration. • Soient a, b, c et d en division harmonique. Soient h_1 et h_2 deux homographies tels que

$$\begin{cases} h_1(f(d)) = \infty \\ h_2(0) = a \\ h_2(1) = b \\ h_2\left(\dfrac{1}{2}\right) = c \\ h_2(\infty) = d \end{cases},$$

1. Soit h une homographie, f l'unique homographie tel que $[a,b,c,d] = f(d)$ et g l'unique homographie tel que $[h(a),h(b),h(c),h(d)] = g(h(d))$, alors $g \circ h$ est une homographie qui envoie a sur ∞, b sur 0 et c sur 1, donc par unicité $g \circ h = f$, ce qui montre que les homographies conservent le birapport.

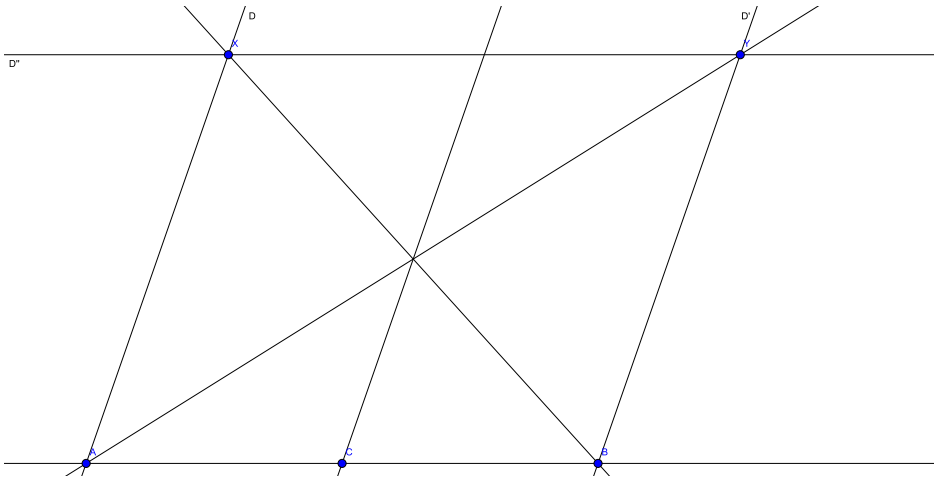
2. On rappelle qu'une division harmonique est un quadruplet de points tels que $[a,b,c,d] = -1$. En particulier, si $d = \infty$, $[a,b,c,d] = -1$ donne $\dfrac{c-b}{c-a} = -1$ donc $c = \dfrac{a+b}{2}$, c est le milieu de $[ab]$.

Alors $h_1 \circ f \circ h_2$ préserve aussi les droite-cercles et envoie l'infini sur l'infini. De plus, f préserve la division harmonique de a, b, c et d si set seulement si $h_1 \circ f \circ h_2$ préserve celle de 0, 1, $\frac{1}{2}$ et ∞.
On renomme par abus f l'application $h_1 \circ f \circ h_2$. Alors il suffit de montrer que

$$f\left(\frac{1}{2}\right) = \frac{f(0)+f(1)}{2}.$$

- On trace la figure suivante :

On prend une droite D passant par $A(0)$ et non colinéaire à (AB) (avec $B(1)$). On trace la parallèle passant par B, D'. Puis on trace une parallèle à (AB) et enfin on retrouve le point $C(1/2)$ en traçant la parallèle à D passant par l'intersections des diagonales du parallélogramme obtenu.



- On a ainsi construit C grâce à des parallèles et des intersections.

Or f envoie l'infini sur l'infini donc envoie les droites sur les droites. Puis f préserve le parallélisme, car deux droites parallèles s'intersectent à l'infini et f préserve l'infini. De même, f préserve les intersections.
On en déduit que l'on peut appliquer f à cette construction. Le point $f(C)$ est alors bien le milieu de $f(A)$ et $f(B)$.
Donc f préserve les divisions harmoniques. □

Fort de ce résultat, nous pouvons maintenant montrer que φ est un morphisme de corps de $\mathbb{C}$.
On a déjà astucieusement modifié φ au départ pour que 0 et 1 soient fixés. On doit juste montrer que φ est additive et multiplicative.
Soient $a \neq b \in \mathbb{C}$, alors $[a, b, \frac{a+b}{2}, \infty] = -1$, donc $[\varphi(a), \varphi(b), \varphi\left(\frac{a+b}{2}\right), \infty] = -1 = [\varphi(a), \varphi(b), \frac{\varphi(a)+\varphi(b)}{2}, \infty]$, d'où il vient que $\varphi\left(\frac{a+b}{2}\right) = \frac{\varphi(a)+\varphi(b)}{2}$.
En prenant $b = 0$, comme $\varphi(0) = 0$, il vient $\varphi(a) = 2\varphi\left(\frac{a}{2}\right)$. On a donc

$$\varphi(a+b) = \varphi\left(\frac{2a+2b}{2}\right) = \frac{\varphi(2a)+\varphi(2b)}{2} = \frac{2\varphi(a)+2\varphi(b)}{2} = \varphi(a)+\varphi(b)$$

Étudions maintenant la multiplicativité.
Pour cela, on remarque que $[a, -a, a^2, 1] = \frac{a^2-a}{a^2+a} \times \frac{1+a}{1-a} = -1$ pour tout $a \in \mathbb{C}$, $a \neq 0$. On a en particulier $[\varphi(a), -\varphi(a), \varphi(a)^2, 1] = -1$ et comme φ conserve les divisions harmoniques, $[\varphi(a), \varphi(-a), \varphi(a^2), \varphi(1)] = -1$.
On a $[\varphi(a), -\varphi(a), \varphi(a)^2, 1] = [\varphi(a), -\varphi - a), \varphi(a^2), 1]$. Donc $\varphi(a^2) = \varphi(a)^2$.
On se rappelle alors astucieusement que $ab = \frac{(a+b)^2-(a-b)^2}{4}$, alors on a

$$4\varphi(ab) = \varphi(4ab) = \varphi((a+b)^2) - \varphi((a-b)^2) = \varphi(a+b)^2 - \varphi(a-b)^2 = (\varphi(a)+\varphi(b))^2 - (\varphi(a)-\varphi(b))^2 = 4\varphi(a)\varphi(b)$$

Il vient $\varphi(ab) = \varphi(a)\varphi(b)$, donc φ est un automorphisme de corps de $\mathbb{C}$.

Pour finir, φ envoie 0 sur 0, 1 sur 1 et ∞ sur ∞, donc il envoie la droite réelle sur elle-même.
Par le raisonnement classique, φ est l'identité sur $\mathbb{Q}$.
Puis soient $x < y$ dans $\mathbb{R}$, alors il existe $z \in \mathbb{R}$ tel que $y - x = z^2$. On a ainsi

$$\varphi(y) - \varphi(x) = \varphi(y - x) = \varphi(z^2) = \varphi(z)^2 > 0.$$

En effet, $\varphi(z) \in \mathbb{R}^{+*}$ car φ préserve la droite réelle et n'envoie que 0 sur 0.
Donc φ est croissante.

Soit $x \in \mathbb{R}$, et $a_n < x < b_n$ deux suites de rationnels tendant vers x, alors $a_n < \varphi(x) < b_n$ et en passant à la limite $\varphi(x) = x$. φ est l'identité sur $\mathbb{R}$.

φ est alors uniquement déterminée par $\varphi(i)$ car $\varphi(a + ib) = a + \varphi(i)b$, mais $-1 = \varphi(i^2) = \varphi(i)^2$, donc $\varphi(i) \in \{1, -1\}$. On en déduit que φ est soit l'identité, soit la conjugaison complexe. Donc $\varphi \in G$. □

Remarques : • Le Audin semble trouver évident le fait que toutes les applications préservant les droites/cercles sont bijectives... Je ne vois pas pourquoi ! Il vaut donc mieux le rajouter.
• Il ne suffit pas de dire que φ est un automorphisme de corps de $\mathbb{C}$ pour conclure. Il y a BEAUCOUP d'automorphismes de corps de $\mathbb{C}$.
• En fait, on peut montrer un autre résultat avec tout ce que l'on a fait :

$$G \simeq \mathrm{PGL}_2(\mathbb{C}) \rtimes \langle \sigma \rangle.$$

Le produit semi direct est donné par $\psi(\sigma)(g) = \bar{g}$ avec $\bar{g}$ l'homographie où tous les coefficients sont remplacés par leur conjugué.

Adapté du travail de Alexandre Bailleul, Corentin Caillaud, Benoît Gaudeul, Baptiste Huguet et Anne-Elisabeth Falq.

Chapitre 16

Groupes paveurs

Références : Berger, *Géométrie 1*, p 33
Cours de Madame Dal'Bo sur les pavages
Boyer, *Algèbre et géométries*, p 314-316

Définition.

On se donne P un compact connexe de $\mathbb{R}^2$ d'intérieur non vide, et G un sous-groupe de $Is^+(\mathbb{R}^2)$, alors G est un groupe paveur si il vérifie les conditions suivantes :
- $\bigcup_{g\in G} g(P) = \mathbb{R}^2$
- si $g(\mathring{P}) \cap h(\mathring{P}) \neq \varnothing \Rightarrow g = h$

Le but ici est d'étudier les groupes paveurs du plan et de montrer qu'il n'y en a que 5 à conjugaison dans $Is^+(\mathbb{R}^2)$ près. [1]

On rappelle que $Is^+(\mathbb{R}^2) \simeq \mathbb{R}^2 \rtimes \mathrm{SO}_2(\mathbb{R})$ (isomorphisme de groupe) via l'application $A\begin{pmatrix} x \\ y \end{pmatrix} + b \mapsto (b, A)$.
On note T l'ensemble des translations (les isométries de partie linéaire nulle) de $Is^+(\mathbb{R}^2)$.

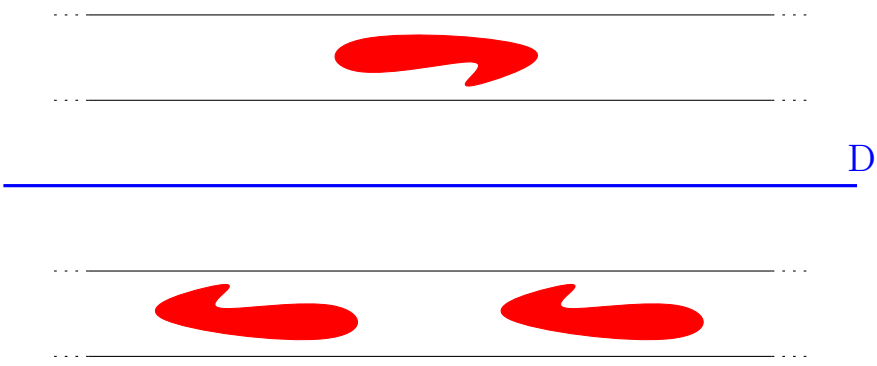
Proposition.

Soit $\Gamma = T \cap G$, alors Γ est un réseau de $\mathbb{R}^2$, c'est à dire qu'il existe une base $(\vec{u_0}, \vec{v_0})$ de $\mathbb{R}^2$ telle que $\Gamma = t_{\mathbb{Z}\vec{u_0}+\mathbb{Z}\vec{v_0}}$.

Démonstration. • Si $\Gamma = \{id\}$, alors G ne contient que des rotations. De plus, si deux rotations r, s avaient des centres distincts, alors le commutateur $rsr^{-1}s^{-1}$ serait une translation non triviale (Il suffit de calculer en se rappelant que SO_2 est abélien.). Elles ont donc un même centre ω.
Donc si $P \subset B(\omega, M)$, alors $\forall g \in G$, $gP \subset B(\omega, M)$. Donc l'axiome premier des groupes paveurs n'est pas respecté.

• Soit $t_{\vec{u}} \in \Gamma$, supposons maintenant que $\forall t_{\vec{w}} \in \Gamma$, $\exists \lambda, \vec{w} = \lambda\vec{u}$.
Soit $r \in G \setminus \Gamma$, alors $rt_{\vec{u}}r^{-1} = t_{\vec{r}(\vec{u})} \in \Gamma$. Donc $\vec{r}(\vec{u}) = \lambda\vec{u}$, donc r est une symétrie autour d'un point.
Si r et s sont deux symétries autour des points A et B, alors rs est la translation de vecteur $2\overrightarrow{AB}$, et donc $\overrightarrow{AB}$ est colinéaire à $\vec{u}$.
Les centres des symétries sont donc sur une même droite D dirigée par $\vec{u}$. Ainsi $\forall g \in \Gamma$, gP est soit dans une bande dirigée par $\vec{u}$ et contenant P, soit dans la bande symétrique à la précédente par rapport à D.
Cela contredit l'axiome 1.

1. Attention, il peut y avoir une infinité de pavés différents, c'est juste la manière de recouvrir le plan avec qui va changer !



→ À partir d'ici, tout est à apprendre par cœur.

• Soit $\alpha = \inf\{\|\vec{w}\|, t_{\vec{w}} \in \Gamma \setminus \{t_{\vec{0}}\}\}$, soit $(\vec{w_n})_n$ une suite de vecteurs telle que $t_{\vec{w_n}} \in \Gamma \setminus \{t_{\vec{0}}\}$ et qui converge vers cet infimum. A partir d'un certain rang, elle est comprise dans une boule $B(0, \alpha+\varepsilon)$, donc quitte à extraire une sous-suite, on peut supposer que $(\vec{w_n})_n$ converge (vers $\vec{v}$).
On pose $g_n = t_{\vec{w_{n+1}} - \vec{w_n}}$, on a $\forall x, g_n(x) = \vec{w_{n+1}} - \vec{w_n} + x \to x$ donc $g_n \to id$ simplement. En particulier, pour n grand, $g_n(\mathring{P}) \cap \mathring{P} \neq \varnothing$, donc g_n est stationnaire à l'identité. Donc $\vec{w_n}$ est stationnaire à $\vec{v}$. Donc $\vec{v} \in \Gamma$ et $\|v\| = \alpha$.
Il reste cependant le cas où $\alpha = 0$. On voit que si c'est le cas, le deuxième axiome n'est pas vérifié pour une translation trop faible.

• On pose $\vec{u_0}$ le vecteur réalisant l'infimum. Puis on pose $\vec{v_0}$ tel que $\|\vec{v_0}\| = \inf\{\|\vec{w}\|, \vec{w}$ non colinéaire à $\vec{u_0}, t_{\vec{w}} \in \Gamma\}$. Ce vecteur existe par les mêmes arguments qu'au dessus.
Soit $t_{\vec{w}} \in G$, montrons que $\vec{w} \in \mathbb{Z}\vec{u_0} + \mathbb{Z}\vec{v_0}$. On a déjà $\vec{w} = a\vec{u_0} + b\vec{v_0}$ avec $a, b \in \mathbb{R}$. Par translation, on peut supposer $a, b \in [0, 1[$.
→ Si $a = b = 0$, c'est bon.
→ Si $a = 0$ et $b \neq 0$, $\|\vec{w}\| < \|\vec{v_0}\|$, ce qui contredit la minimalité de $\|\vec{v_0}\|$. C'est donc absurde.
→ Il en va de même pour le cas $a \neq 0$ et $b = 0$.
→ Si a et b sont non-nuls, alors

$$\begin{aligned}\|w\|^2 &\leqslant a^2\|\vec{u_0}\| + b^2\|\vec{v_0}\| + 2ab|(\vec{u_0}, \vec{v_0})| \\ &< a^2\|\vec{u_0}\| + b^2\|\vec{v_0}\| + 2ab\|\vec{u_0}\|\|\vec{v_0}\| \text{ (car } \vec{u_0} \text{ et } \vec{v_0} \text{ ne sont pas colinéaires)} \\ &< (a^2 + b^2 + 2ab)\|\vec{v_0}\|^2 = (a+b)^2\|\vec{v_0}\|^2\end{aligned}$$

On en déduit $\|w\| < (a+b)\|\vec{v_0}\|$, donc $a + b > 1$.
En refaisant le même travail avec $\vec{w'} = (1-a)\vec{u_0} + (1-b)\vec{v_0}$, on trouve $a + b < 1$, ce qui donne une contradiction et implique donc que $w = 0$.

Γ est donc bien un réseau. □

Théorème.

Pour $G \subset Is^+(\mathbb{R}^2)$, il n'y a que 5 pavages du plan.

On rappelle que deux groupes paveurs G_1 et G_2 sont équivalents si ils sont conjugués dans $Is^+(\mathbb{R}^2)$. [2]

Démonstration. On appelle L l'application qui à un déplacement de G associe sa partie linéaire dans $\mathrm{SO}_2(\mathbb{R})$.
Soit $g \in G$, et $\mathcal{B} = (\vec{u_0}, \vec{v_0})$ la base (pas forcément orthonormée) de $\mathbb{R}^2$ associée au réseau Γ.
On a $gt_{\vec{u_0}}g^{-1} = t_{L(g)(\vec{u_0})} \in \Gamma$. Il en va de même pour v_0.
On en déduit $\begin{cases} L(g)(\vec{u_0}) &= n_1\vec{u_0} + m_1\vec{v_0} \\ L(g)(\vec{v_0}) &= n_2\vec{u_0} + m_2\vec{v_0} \end{cases}$ avec $n_1, n_2, m_1, m_2 \in \mathbb{Z}$.
D'où, $L(g) = \begin{pmatrix} n_1 & n_2 \\ m_1 & m_2 \end{pmatrix}$ dans la base $\mathcal{B}$. Il vient $\mathrm{Tr}(L(g)) = 2\cos(\theta) \in \mathbb{Z}$.

2. Dans le Audin, il est dit à ce sujet : si τ est un élément d'un groupe de transformations G, son conjugué par un élément de G est un élément de même nature géométrique que τ, et les éléments définissants cette nature sont, pour le conjugué de τ par ϕ les images de ceux de τ par ϕ.
Par exemple, $\phi \circ t_{\vec{u}} \circ \phi^{-1} = t_{\vec{\phi}(\vec{u})}$.

On en déduit la disjonction des cas suivante :
→ soit $\cos(\theta) = -1$ et $L(g) = -id$,
→ soit $\cos(\theta) = -\frac{1}{2}$ et $L(g) = R_{\frac{2\pi}{3}}$,
→ soit $\cos(\theta) = 0$ et $L(g) = R_{\frac{\pi}{2}}$,
→ soit $\cos(\theta) = \frac{1}{2}$ et $L(g) = R_{\frac{\pi}{3}}$,
→ soit $\cos(\theta) = 1$ et $L(g) = id$.

On a alors $L(G) =< R >$ cyclique avec R rotation parmi celles citées ci-dessus.
En effet, on a $L(G) \subset \mathrm{SO}_2(\mathbb{R})$ abélien, et si on compose bien deux des rotations du dessus, on obtient des rotations interdites. Par exemple, $R_{\frac{\pi}{3}} R_{\frac{\pi}{2}} = R_{\frac{5\pi}{6}}$ est banni.
On a ainsi 5 types de groupes différents. □

Pour finir, on dessine les 5 types de pavages que voici (image prise dans Berger, *Géométrie*).

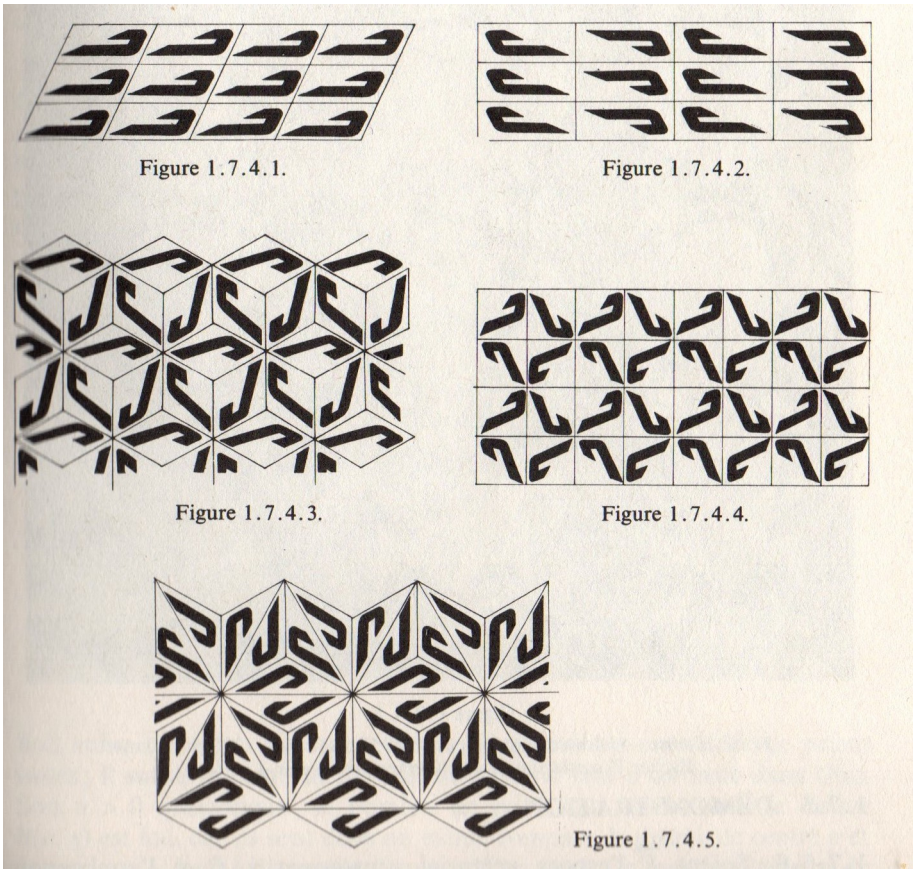


Figure 1.7.4.1.

Figure 1.7.4.2.

Figure 1.7.4.3.

Figure 1.7.4.4.

Figure 1.7.4.5.

Remarques : • Si on définit le groupe paveur comme un sous groupe de $Is(\mathbb{R}^2)$, on a alors 17 groupes paveurs possibles. La première démonstration de ce fait a été trouvée à Saint-Petersbourg en 1891 par Evgraf Stepanovitch Fedorov (à ne pas confondre avec Stépane Arkadiévitch Oblonskï). On peut trouver des précisions très claires et passionnantes sur le site de Thérèse Eveilleau : `http://therese.eveilleau.pagesperso-orange.fr/pages/jeux_mat/textes/pavage_17_types.htm`
• Le palais de l'Alhambra à Grenade est rempli de pavages différents. Il contient 13 des pavages périodiques du plan.
• Il n'y a pas que des pavages périodiques ! Même si il est assez difficile de s'imaginer un pavage apériodique, ils existent ! On peut citer les pavages de Penrose notamment.
• En cristallographie, on étudie les symétries dans les cristaux avec la déviation de faisceaux lumineux par diffraction. On trouve ainsi des "mailles élémentaires" (notre pavé) et des "groupes d'espace" qui sont exactement nos groupes paveurs (mais en dimension 3). On peut montrer qu'il y a 230 types de groupes d'espace.
• Si on a un groupe paveur G opérant sans point fixe, on peut montrer que $X = \mathbb{R}^2/G$ est une variété différentielle. Pour $L(G) =< id >$, on a $G = \mathbb{Z}^2$ et on trouve $X = \mathbb{R}^2/\mathbb{Z}^2$ le tore. On peut aussi trouver la bouteille de Klein pour un pavage que nous n'avons pas étudié ici.

Chapitre 17

Image de l'exponentielle

Références : Zavidovique, *Un max de maths*, p 48-55

Théorème.

Soit $A \in \mathcal{M}_n(\mathbb{C})$, alors $\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$.

Démonstration. • Commençons par montrer que $\mathbb{C}[A]^\times = \mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C})$. [1]
L'inclusion $\mathbb{C}[A]^\times \subset \mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C})$ est évidente. Pour l'autre inclusion, il faut se rappeler que si $A \in \mathrm{GL}_n(\mathbb{C})$, alors A^{-1} est un polynôme en A. En effet, il suffit d'utiliser Cayley-Hamilton et de multiplier par A^{-1} l'égalité obtenue.
Si $M \in \mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C})$, alors M^{-1} est un polynôme en M, donc un polynôme en A. On en déduit que $M \in \mathbb{C}[A]^\times$.

• $\mathbb{C}[A]^\times$ est un ouvert connexe (par arcs) de $\mathbb{C}[A]$.
$\mathbb{C}[A]^\times = \mathbb{C}[A] \cap \det{}^{-1}(\mathbb{C}^\times)$ donc $\mathbb{C}[A]^\times$ est un ouvert de $\mathbb{C}[A]$. Pour démontrer la connexité, on se donne M, $N \in \mathbb{C}[A]^\times$ et on va créer un chemin reliant M et N.
On remarque que pour tout $z \in \mathbb{C}$, $M(z) := zM + (1-z)N$ est dans $\mathbb{C}[A]$. On remarque que $z \mapsto \det(M(z))$ est polynomiale en z, donc ne s'annule qu'un nombre fini de fois. Il s'agit donc de trouver un chemin $z(t)$ qui évite ces points.
On peut prendre un chemin de la forme $z_a(t) = t + iat(1-t)$. En effet, on voit vite que $(a,t) \mapsto z_a(t)$ est injectif. Donc le nombre de $z_a(t)$ passant par des zéros de $\det(M(z))$ est inférieur ou égal au nombre de zéros de $\det(M(z))$. Comme il est fini, on a une infinité de chemins à disposition.

→ Pour montrer que $\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$, comme $\mathbb{C}[A]^\times$ est connexe, il suffit de montrer que $\exp(\mathbb{C}[A])$ est ouvert, fermé et non vide.
On voit déjà que $\exp(\mathbb{C}[A]) \subset \mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C}) = \mathbb{C}[A]^\times$. Puis $I_n = \exp(0) \in \mathbb{C}[A]^\times$.

• Montrons que $\exp(\mathbb{C}[A])$ est ouvert.
On se rappelle que $D\exp(0) = I_n$. Par le théorème d'inversion locale, on a donc existence d'un voisinage ouvert U de 0 dans $\mathbb{C}[A]$ et d'un voisinage ouvert V de I_n dans $\exp(\mathbb{C}[A])$ tel que exp réalise un $\mathcal{C}^1$-difféomorphisme de U sur V.
Soit $M = \exp(N) \in \exp(\mathbb{C}[A])$, alors $M.V$ est un voisinage ouvert de M dans $\exp(\mathbb{C}[A])$. En effet, l'exponentielle commute sur les polynômes en A, donc $\exp(N+U) = \exp(N).\exp(U) = M.V$. On a donc prouvé que $\exp(\mathbb{C}[A])$ est ouvert.

• Montrons que $\exp(\mathbb{C}[A])$ est fermé.
On utilise ici une astuce usuelle dans le cadre des groupes topologiques. On remarque que

$$\mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A]) = \bigcup_{M \in \mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A])} M.\exp(\mathbb{C}[A]).$$

La première inclusion est évidente :

$$\mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A]) = \bigcup_{M \in \mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A])} M\exp(0) \subset \bigcup_{M \in \mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A])} M.\exp(\mathbb{C}[A]).$$

1. C'est aussi vrai sur $\mathbb{R}$. On a $\mathbb{R}[A]^\times = \mathbb{R}[A] \cap \mathrm{GL}_n(\mathbb{R})$ par le même raisonnement.

Puis soit $M \in \mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A])$ et $N = M\exp(B)$ avec $B \in \mathbb{C}[A]$, alors $M = N\exp(-B)$. Donc si on suppose par l'absurde que $N \in \exp(\mathbb{C}[A])$, alors $M \in \exp(\mathbb{C}[A])$, ce qui est exclu.
La formule est prouvée et cela conclut la preuve par connexité. □

Corollaire.

L'image de $\mathbb{M}_n(\mathbb{C})$ par l'exponentielle est $\mathrm{GL}_n(\mathbb{C})$.

Démonstration. Soit $A \in \mathrm{GL}_n(\mathbb{C})$, alors comme $A \in \mathbb{C}[A]^\times$ et $\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$, on a l'existence de B dans $\mathbb{C}[A]$ (donc dans $\mathcal{M}_n(\mathbb{C})$) tel que $A = \exp(B)$. □

Corollaire.

On a $\exp(\mathcal{M}_n(\mathbb{R})) = \mathrm{GL}_n(\mathbb{R})^2 := \{A^2, A \in \mathrm{GL}_n(\mathbb{R})\}$.

Démonstration. Soit $M \in \mathcal{M}_n(\mathbb{R})$, alors $\exp(M) = \exp(M/2)^2$, ce qui donne la première inclusion.
Soit $B = A^2$, avec $A \in \mathrm{GL}_n(\mathbb{R})$, alors par le théorème, il existe $P \in \mathbb{C}[X]$ tel que $A = \exp(P(A))$. En passant au conjugué, on a $A = \exp(\overline{P}(A))$. Alors $B = A^2 = \exp((P + \overline{P})(A))$. □

Remarques : • Attention l'égalité $\exp(\mathbb{R}[A]) = \mathbb{R}[A]^\times$ est fausse en général ! Si A est diagonale, alors $-I_n \in \mathbb{R}[A]^\times$ et n'est pas dans l'image de l'exponentielle.
• Un bon moyen de voir que $\exp(\mathcal{M}_n(\mathbb{R})) \neq \mathrm{GL}_n(\mathbb{R})$ est de se rappeler que $\exp(\mathcal{M}_n(\mathbb{R})) \subset \mathrm{GL}_n^+(\mathbb{R})$.
• Attention $\exp(\mathcal{M}_n(\mathbb{R})) \neq \mathrm{GL}_n^+(\mathbb{R})$. En effet, la matrice

$$\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \in \mathrm{GL}_n^+(\mathbb{R}) \setminus \exp(\mathcal{M}_n(\mathbb{R})).$$

Chapitre 18

Inégalité de Hoeffding

Références : Ouvrard, *Probabilités 2*, 10.11

Théorème.

Soit $(X_n)_n$ une suite de variables aléatoires réelles indépendantes et centrées. On suppose de plus $|X_n| \leqslant c_n$ presque partout, où $c_n > 0$. Alors, en notant $S_n = \sum_{j=1}^{n} X_j$, on a $\forall \varepsilon > 0$,

$$\mathbb{P}(|S_n| > \varepsilon) \leqslant 2 \exp\left(-\frac{\varepsilon^2}{2\sum_{j=1}^{n} c_j^2} \right).$$

Lemme.

Soit X une variable aléatoire réelle centrée et bornée par 1 ps, alors $\forall t \in \mathbb{R}$, $\mathbb{E}[e^{tX}] \leqslant e^{\frac{t^2}{2}}$.

Démonstration. Soit $x \in [-1, 1]$, alors par convexité de l'exponentielle, on a

$$e^{tx} = \exp\left(\frac{1-x}{2} \times (-t) + \frac{1+x}{2} \times t \right) \leqslant \frac{1-x}{2} e^{-t} + \frac{1+x}{2} e^{t}.$$

On rappelle que l'exponentielle est convexe car de dérivée seconde positive, et on peut utiliser l'inégalité car $\frac{1-x}{2} + \frac{1+x}{2} = 1$ et $\frac{1-x}{2}$, $\frac{1+x}{2}$ sont dans $[0, 1]$.

X étant bornée presque surement par 1, on peut utiliser l'inégalité précédente : $e^{tX} \leqslant \frac{1-X}{2} e^{-t} + \frac{1+X}{2} e^{t}$. En intégrant, on obtient $\mathbb{E}[e^{tX}] \leqslant \frac{1}{2}(e^{-t} + e^{t}) = \cosh(t)$ car X est centrée.

Puis $\cosh(t) = \sum \frac{t^{2n}}{(2n)!} \leqslant \sum \frac{t^{2n}}{2^n n!} = e^{\frac{t^2}{2}}$. En effet, $\frac{(2n)!}{n!} = (2n)(2n-1)...(n+1) \geqslant 2 \times 2 \times ... \times 2 = 2^n$.

D'où il vient $\mathbb{E}[e^{tX}] \leqslant e^{\frac{t^2}{2}}$. □

On va maintenant prouver l'inégalité de Hoeffding.

Démonstration. Commençons par étudier $\mathbb{P}(S_n > \varepsilon)$.
On a $\forall t > 0$, $\mathbb{P}(S_n > \varepsilon) = \mathbb{P}(e^{tS_n} > e^{t\varepsilon})$.

L'inégalité de Markov donne alors $\mathbb{P}(e^{tS_n} > e^{t\varepsilon}) \leqslant \frac{\mathbb{E}[e^{tS_n}]}{e^{t\varepsilon}}$ car e^{tS_n} est positive.

De plus, $\mathbb{E}[e^{tS_n}] = \prod_{j=1}^{n} \mathbb{E}[e^{tX_j}]$ par indépendance et $\mathbb{E}[e^{tX_j}] = \mathbb{E}[e^{(c_j t)\frac{X_j}{c_j}}] \leqslant e^{\frac{c_j^2 t^2}{2}}$ par le lemme.

On en déduit $\mathbb{E}[e^{tS_n}] \leqslant \prod_{j=1}^{n} e^{\frac{c_j^2 t^2}{2}} = \exp\left(\frac{t^2 \sum_{j=1}^{n} c_j^2}{2} \right)$.

Finalement $\mathbb{P}(S_n > \varepsilon) \leqslant \exp\left(\frac{t^2 \sum_{j=1}^n c_j^2}{2} - t\varepsilon\right)$.

On définit $a := \sum_{j=1}^n c_j^2$, alors on va tenter de minimiser sur $\mathbb{R}^{+*}$ la fonction de t, $\frac{at^2}{2} - t\varepsilon$. Elle atteint son minimum en $t_0 = \frac{\varepsilon}{a}$ et elle vaut alors $-\frac{\varepsilon^2}{2a}$. On a donc $\mathbb{P}(S_n > \varepsilon) \leqslant \exp\left(-\frac{\varepsilon^2}{2a}\right)$.

Pour finir, si on refait le même raisonnement avec la suite $(-X_i)_i$, on trouve $\mathbb{P}(S_n < -\varepsilon) = \mathbb{P}(-S_n > \varepsilon) \leqslant \exp\left(-\frac{\varepsilon^2}{2a}\right)$.

D'où $\mathbb{P}(|S_n| > \varepsilon) = \mathbb{P}(S_n > \varepsilon) + \mathbb{P}(S_n < -\varepsilon) \leqslant 2\exp\left(-\frac{\varepsilon^2}{2a}\right) = 2\exp\left(-\frac{\varepsilon^2}{2\sum_{j=1}^n c_j^2}\right)$. □

Corollaire.

Si il existe $\alpha, \beta > 0$ tels que $\sum_{j=1}^n c_j^2 \leqslant n^{2\alpha-\beta}$, alors $\frac{S_n}{n^\alpha}$ converge presque surement vers 0.

Démonstration. Soit $\varepsilon > 0$, on utilise l'inégalité de Hoeffding : $\mathbb{P}(|S_n| > n^\alpha\varepsilon) \leqslant 2\exp\left(-\frac{n^{2\alpha}\varepsilon^2}{2\sum_{j=1}^n c_j^2}\right)$.

On a alors sous nos hypothèses : $\mathbb{P}\left(\frac{|S_n|}{n^\alpha} > \varepsilon\right) \leqslant 2\exp\left(-\frac{n^\beta\varepsilon^2}{2}\right)$.

La série de terme général $\exp\left(-\frac{n^\beta\varepsilon^2}{2}\right)$ converge car à termes positifs et $\exp\left(-\frac{n^\beta\varepsilon^2}{2}\right) = o\left(\frac{1}{n^2}\right)$.

On en déduit par Borel-Cantelli que $\mathbb{P}\left(\liminf_n \left\{\frac{|S_n|}{n^\alpha} < \varepsilon\right\}\right) = 1$, ce qui est une manière de dire que $\frac{|S_n|}{n^\alpha} \to 0$ presque surement. [1] □

Remarques : • Si on compare les inégalités de Bienaymé-Tchebychev et Hoeffding sur des lois de Bernoulli ($c_n = 1$), on a

$\mathbb{P}(|Sn - np| > \sqrt{n}\varepsilon) \leqslant \frac{p(1-p)}{\varepsilon^2}$ pour Bienaymé-Tchebychev,

et $\mathbb{P}(|Sn - np| > \sqrt{n}\varepsilon) \leqslant 2\exp\left(-\frac{\epsilon^2}{2}\right)$ pour Hoeffding.

C'est quand même carrément mieux avec Hoeffding !

• Cette inégalité permet d'obtenir des intervalles de confiance... mais on préfère souvent utiliser le TCL.

• Une généralisation de cette inégalité est l'inégalité d'Azuma :

Théorème.

Soit $(X_n)_n$ une martingale issue de 0 dont les accroissements sont contrôlés par une suite déterministe (c_n), c'est à dire $|X_n - X_{n-1}| \leqslant c_n$ presque surement pour tout $n \geqslant 1$. Alors pour tout $\varepsilon > 0$, on a

$$\mathbb{P}(|X_n| \geqslant \varepsilon) \leqslant 2e^{-\frac{\lambda^2}{2\sigma_n^2}}, \text{ où } \sigma_n^2 = \sum_{i=1}^n c_i^2 .$$

1.

$$X_n \to Xps \Leftrightarrow \mathbb{P}\left(\bigcap_{\varepsilon>0}\bigcup_{n\in\mathbb{N}}\bigcap_{m\geqslant n}\{|X_m - X| < \varepsilon\}\right) = 1$$
$$\Leftrightarrow \mathbb{P}\left(\bigcap_{k>0}\bigcup_{n\in\mathbb{N}}\bigcap_{m\geqslant n}\left\{|X_m - X| < \frac{1}{k}\right\}\right) = 1$$
$$\Leftrightarrow \lim_{k\to\infty} \mathbb{P}\left(\liminf_n \left\{|X_n - X| < \frac{1}{k}\right\}\right) = 1$$

On peut appliquer ce résultat au calcul du nombre de couleurs nécessaires pour colorier un graphe à n sommets avec la condition que deux sommets reliés par une arête ne peuvent être de la même couleur.

Il y a au maximum $\binom{n}{k}$ arêtes possibles. On note Y_k la variable aléatoire de loi de Bernoulli $b(p)$ décidant de si on rajoute l'arête k ou non. On note enfin χ le nombre minimal de couleurs nécessaires selon les arêtes présentes.

On montre alors $\mathbb{P}(|\chi - \mathbb{E}[\chi]| \geqslant \varepsilon\sqrt{n-1}) \leqslant 2e^{-\frac{\lambda^2}{2}}$.

Chapitre 19

Irréductibilité des polynômes cyclotomiques

Références : Perrin, *Cours d'algèbre*, p 82

On rappelle que $\Phi_{n,k}(X) = \prod_{\zeta \in \mu_n^*(K_n)} (X - \zeta)$ où K_n est le corps de décomposition de $X^n - 1$ sur k, $\mu_n(K_n)$ est l'ensemble des racines de l'unité dans K_n (qui est cyclique car sous-groupe de k^* qui est cyclique) et $\mu_n^*(K_n)$ est l'ensemble des racines primitives de l'unité, c'est à dire celles qui engendrent $\mu_n(K_n)$.
On note $\Phi_n = \Phi_{n,\mathbb{Q}}$ pour simplifier.

Proposition.

Les Φ_n sont dans $\mathbb{Z}[X]$.

Démonstration. On fait la démonstration par récurrence forte.
On a $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$.
Au rang n, on pose $F(X) = \prod_{d|n, d \neq n} \Phi_d(X)$. On a $F \in \mathbb{Z}[X]$ par hypothèse.
On rappelle que $X^n - 1 = \prod_{d|n} \Phi_d(X) = \Phi_n(X)F(X)$.
Puis on fait la division euclidienne de $X^n - 1$ par F dans $\mathbb{Z}[X]$ (possible car F unitaire) : $X^n - 1 = F(X)P(X) + R(X)$. Donc $F(X)(\Phi_n(X) - P(X)) = R(X)$ et comme $\deg(R) < \deg(F)$, on a $\Phi_n = P \in \mathbb{Z}[X]$. □

Théorème.

Les polynômes cyclotomiques sont irréductibles dans $\mathbb{Z}[X]$ (et donc dans $\mathbb{Q}[X]$).

Démonstration. • On se donne un nombre premier p ne divisant pas n et ζ une racine primitive de l'unité. On sait que ζ^p est aussi une racine primitive (car ζ^m est primitive ssi $m \wedge n = 1$). On note f et g les polynômes minimaux respectifs de ζ et ζ^p. Ce sont des polynômes de $\mathbb{Q}[X]$. Montrons que f, $g \in \mathbb{Z}[X]$.
On décompose Φ_n en produit d'irréductibles $\Phi_n = f_1 ... f_r$ avec $f_i \in \mathbb{Z}[X]$ (car $\mathbb{Z}[X]$ est factoriel). Comme Φ_n est unitaire, quitte à multiplier les f_i par -1, on peut supposer que les f_i sont unitaires.
$\Phi_n(\zeta) = 0$ donc il existe i_0 tel que $f_{i_0}(\zeta) = 0$. Or f_{i_0} est irréductible et unitaire sur $\mathbb{Z}[X]$, donc sur $\mathbb{Q}[X]$, donc $f = f_{i_0} \in \mathbb{Z}[X]$ et $f | \Phi_n$.
On peut faire le même travail pour montrer que $g \in \mathbb{Z}[X]$ et $g | \Phi_n$.

• Montrons à présent que $f = g$.
Supposons f et g distincts, alors comme ils sont irréductibles, $fg | \Phi_n$ dans $\mathbb{Z}[X]$. D'autre part comme ζ est racine de $g(X^p)$, on a que $f(X) | g(X^p)$ dans $\mathbb{Q}[X]$. Il existe $h \in \mathbb{Q}[X]$ tel que $g(X^p) = f(X)h(X)$. On écrit $h = \frac{a}{b} h'$ avec $h' \in \mathbb{Z}[X]$ de contenu 1, alors comme $g(X^p)$ et $f(X)$ sont unitaires, on a $1 = \frac{a}{b}$ en passant au contenu, ce qui donne $h \in \mathbb{Z}[X]$.

On écrit $g(X) = \sum a_i X^i$, alors en réduisant dans $\mathbb{F}_p$, on a $\overline{g}(X^p) = \sum \overline{a_i} X^{pi} = \overline{g}(X)^p$ par Frobenius.
Soit φ un facteur irréductible de $\overline{f}$, alors comme $\overline{g}^p = \overline{fh}$, φ divise $\overline{g}^p$ et par le lemme d'Euclide [1], φ divise $\overline{g}$.
Comme $fg|\Phi_n$, on a $\overline{f}\overline{g}|\overline{\Phi_n}$ sur $\mathbb{F}_p$, donc φ^2 divise $\overline{\Phi_n} = \Phi_{n,\mathbb{F}_p}$. [2] Mais cela est absurde car alors $\Phi_{n,\mathbb{F}_p}$ aurait une racine double dans un corps de décomposition, ce qui est faux par construction des polynômes cyclotomiques.
Donc $f = g$.

• À présent, prenons ζ^m une racine primitive n-ième de l'unité, avec $m = p_1^{\alpha_1}...p_s^{\alpha_s}$. Par le travail précédent, on a $0 = f(\zeta^{p_1}) = f((\zeta^{p_1})^{p_1}) = ... = f(\zeta^{p_1^{\alpha_1}}) = f((\zeta^{p_1^{\alpha_1}})^{p_2}) = ... = f(\zeta^m)$.
Finalement, f divise Φ_n, il admet toutes les racines primitives n-ièmes de l'unité comme racines et il est unitaire, donc $\Phi_n = f$ et Φ_n est irréductible sur $\mathbb{Q}$. Comme Φ_n est unitaire, son contenu est 1 et il est irréductible sur $\mathbb{Z}$. □

Remarque : • La difficulté de ce développement est de voir dans quoi on fait les divisions euclidiennes ou dans quel ensemble sont les éléments. Je rappelle donc ici (et il faut le dire à l'oral) qu'un polynôme minimal n'a de sens que sur un anneau *principal* (donc pas $\mathbb{Z}[X]$) car il est l'élément engendrant l'idéal annulateur. De même on doit faire nos divisions euclidiennes sur un anneau *euclidien* (et $A[X]$ est euclidien ssi A est un corps). Les divisions euclidiennes sont aussi possibles dans $A[X]$ si on veut diviser par un polynôme **unitaire**. On peut le montrer par récurrence en divisant tout monôme X^n par $P = \alpha X^p + P_0$. On a $X^n = \alpha^{-1} X^{n-p} P - \alpha^{-1} X^{n-p} P_0$ et on s'est ramené à un degré plus faible.
• L'application majeure de ce développement est de montrer que Φ_n est le polynôme minimal de toute racine primitive n-ième de l'unité. On déduit de cela le degré des extensions cyclotomiques et on peut faire de la théorie de Galois avec. On se sert notamment de ce résultat dans la constructibilité des polygones réguliers.

1. Si φ divise $\overline{g}^p$, alors soit φ divise $\overline{g}$, soit il divise $\overline{g}^{p-1}$...

2. On montre ça par récurrence à nouveau. On a $X^n - 1 = \overline{X^n - 1} = \overline{\Phi_n F} = \overline{\Phi_n} F$ (par hypothèse de récurrence). Donc $(\overline{\Phi_n} - \Phi_{n,\mathbb{F}_p})F = 0$ et on a le résultat par intégrité de $\mathbb{F}_p[X]$.

Chapitre 20

Lemme de Morse

Références : Rouvière, *Petit guide de calcul différentiel*, ex114 p354 + ex66 p209 (lemme)

Lemme (Réduction des formes quadratiques, version différentiable)**.**

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

En d'autres termes, toute forme quadratique suffisamment voisine d'une forme quadratique non dégénérée, lui est équivalente et le changement de base "dépend de manière $\mathcal{C}^1$" en la matrice. En particulier, ce lemme prouve que l'ensemble des formes quadratiques non dégénérées de signature donnée forme un ouvert de $\mathcal{S}(\mathbb{R})$ [1].

Démonstration. • Soit $\varphi : \begin{array}{ccc} \mathcal{M}_n(\mathbb{R}) & \longrightarrow & \mathcal{S}_n(\mathbb{R}) \\ M & \longmapsto & {}^tMA_0M \end{array}$, elle est polynomiale donc $\mathcal{C}^1$.
On munit $\mathcal{M}_n(\mathbb{R})$ d'une norme sous multiplicative $\|.\|$.
Soit $H \in \mathcal{M}_n(\mathbb{R})$, $\varphi(I_n + H) - \varphi(I_n) = {}^tHA_0 + A_0H + o(\|H\|) = {}^t(A_0H) + A_0H + o(\|H\|)$.
D'où $D\varphi(I_n)(H) = {}^t(A_0H) + A_0H$.

On a de plus $H \in \mathrm{Ker}(D\varphi(I_n)) \Leftrightarrow A_0H \in \mathcal{A}_n(\mathbb{R})$ donc $\mathrm{Ker}(D\varphi(I_n)) = A_0^{-1}\mathcal{A}_n(\mathbb{R})$. [2]. On ne peut donc pas appliquer le théorème d'inversion locale.

• On va restreindre φ sur un supplémentaire de son noyau et appliquer le théorème d'inversion.
On a $\mathcal{M}_n(\mathbb{R}) = A_0^{-1}\mathcal{S}_n(\mathbb{R}) \oplus A_0^{-1}\mathcal{A}_n(\mathbb{R})$. On pose donc $F = A_0^{-1}\mathcal{S}_n(\mathbb{R})$ et on remarque $I_n \in F$.
Soit $\psi : F \to \mathcal{S}_n(\mathbb{R})$ la restriction de φ à F. $D\psi(I_n)$ est injective par construction. Elle est même bijective car $\dim(F) = \dim(\mathcal{S}_n(\mathbb{R}))$.
Par le théorème d'inversion locale, il existe un voisinage ouvert U de I_n dans F tel que ψ soit un difféomorphisme de classe $\mathcal{C}^1$ de U sur $V = \psi(U)$.
On peut de plus supposer $U \subset \mathrm{GL}_n(\mathbb{R})$. En effet, par continuité de det, il existe un voisinage ouvert U' de I_n dans $\mathrm{GL}_n(\mathbb{R})$ contenu dans U. On peut alors restreindre notre $\mathcal{C}^1$-difféomorphisme à U' et son image sera $\psi(U')$, il reste alors un $\mathcal{C}^1$-difféomorphisme.
Ainsi, V est un voisinage ouvert de $A_0 = \psi(I_n)$ dans $\mathcal{S}_n(\mathbb{R})$ et $\forall A \in V$, $A = {}^t\psi^{-1}(A)A_0\psi^{-1}(A)$ d'où le résultat avec $\rho = \psi^{-1}$. □

Théorème (Lemme de Morse)**.**

Soit $f : U \to \mathbb{R}$, de classe $\mathcal{C}^3$ sur U ouvert de $\mathbb{R}^n$ tel que $0 \in U$.
On suppose que $Df(0) = 0$ (0 est un point critique), que $D^2f(0)$ est non dégénérée et que $\varepsilon(D^2f(0)) = (p, n-p)$.
Alors il existe φ un $\mathcal{C}^1$-difféomorphisme entre deux voisinages ouverts de 0 dans $\mathbb{R}^n$ tel que $\varphi(0) = 0$ et $f(x) - f(0) = u_1^2 + \cdots + u_p^2 - u_{p+1}^2 \cdots - u_n^2$ où $u = \varphi(x)$.

1. pour $A_0 = I_n$, on en déduit l'existence d'une racine carrée symétrique pour A symétrique proche de I_n.
2. On peut montrer que cette application est aussi surjective.

Démonstration. On écrit la formule de Taylor à l'ordre 1 avec reste intégral au voisinage de 0.
$f(x) - f(0) = Df(0)(x) + \int_0^1 (1-t)D^2f(tx)(x,x)\mathrm{d}t = {}^{\mathrm{t}}xQ(x)x$ avec $Q(x) = \int_0^1 (1-t)D^2f(tx)\mathrm{d}t$.
Q est de classe $\mathcal{C}^1$. De plus, $Q(0) = \frac{1}{2}D^2f(0) \in \mathcal{S}_n(\mathbb{R}) \cap \mathrm{GL}_n(\mathbb{R})$ car non dégénérée.
On peut donc appliquer le lemme : il existe V un voisinage de $Q(0)$ dans $\mathcal{S}_n(\mathbb{R})$ et $\rho \in \mathcal{C}^1(V, \mathrm{GL}_n(\mathbb{R}))$ tel que $\forall A \in V$, $A = {}^{\mathrm{t}}\rho(A)Q(0)\rho(A)$.
Or Q est continue, donc il existe un voisinage V_0 de 0 dans $\mathbb{R}^n$ tel que $V_0 \subset Q^{-1}(V)$. Ainsi, $\forall x \in V_0$, $Q(x) \in V$, donc $Q(x) = {}^{\mathrm{t}}\rho(Q(x))Q(0)\rho(Q(x))$. On pose $M(x) = \rho(Q(x))$.

D'autre part, d'après le théorème d'inertie de Sylvester appliquée à $Q(0)$ qui est aussi de signature $(p, n-p)$, $\exists A \in \mathrm{GL}_n(\mathbb{R})$ telle que $Q(0) = {}^t A \begin{pmatrix} I_p & 0 \\ 0 & -I_{n-p} \end{pmatrix} A$. Finalement $f(x) - f(0) = {}^t x {}^t M(x) {}^t A \begin{pmatrix} I_p & 0 \\ 0 & -I_{n-p} \end{pmatrix} AM(x)x$.
En posant $\varphi(x) = AM(x)x$, on a $f(x) - f(0) = {}^t \varphi(x) \begin{pmatrix} I_p & 0 \\ 0 & -I_{n-p} \end{pmatrix} \varphi(x)$. Et donc avec $u = \varphi(x)$, on a bien $\varphi(0) = 0$ et $f(x) - f(0) = u_1^2 + \cdots + u_p^2 - u_{p+1}^2 \cdots - u_n^2$.

Il reste à montrer que φ définit un $\mathcal{C}^1$-difféomorphisme entre deux voisinages de 0.
φ est $\mathcal{C}^1$ car M l'est (en effet, ρ est $\mathcal{C}^1$ et Q est supposé $\mathcal{C}^1$ car f est $\mathcal{C}^3$).
Calculons la différentielle à l'origine de φ : $\varphi(h) - \varphi(0) = AM(h)h = AM(0)h + o(\|h\|)$.
Comme $AM(0) \in \mathrm{GL}_n(\mathbb{R})$, $D\varphi(0)$ est inversible.
D'après le théorème d'inversion locale appliqué à φ, il existe deux voisinages de 0 (en fait de 0 et de $\varphi(0) = 0$) tels que φ soit un $\mathcal{C}^1$-difféomorphisme entre ces deux voisinages. □

Remarque : • En fait ce théorème est vrai pour f de classe $\mathcal{C}^1$ et possédant une différentielle seconde non dégénérée en 0. On peut trouver une preuve dans le cours d'analyse de Doukhan et Sifre.
• (Rouvière, ex 111) On se donne f de classe $\mathcal{C}^3$ et a un tel que $D^2f(a)$ **soit non dégénérée**. On pose $\delta(h) = f(a+h) - f(a) - Df(a)h$, alors par le lemme de Morse, $\delta(h) = \varepsilon_1 u_1^2(h) + \varepsilon_2 u_2^2(h)$ dans un voisinage de a, avec $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$.
$h \in \mathbb{R}^2 \mapsto f(a) + Df(a)h$ est l'équation paramétrique du plan tangent, donc $\delta(h)$ représente la différence entre $f(h)$ et sa projection verticale sur le plan tangent.
On en déduit que si la signature est $(2,0)$, alors $\varepsilon_1 = \varepsilon_2 = 1$ et f est au dessus de son plan tangent localement en a. Au contraire, si la hessienne est définie négative, f est localement au dessous de son plan tangent.
Si la signature est $(1,1)$, $\delta(h) = u_1^2(h) - u_2^2(h)$ et donc f coupe son plan tangent en une courbe (qui n'est pas une variété) avec un point double définie par $u = \pm v$. [3]
• Si $D^2f(a)$ est dégénérée, on ne peut rien dire sans étudier les termes suivants dans le développement de Taylor.
• Pour aller plus vite, on note $V \in \mathcal{V}(A)$ pour dire V voisinage de A.

Adapté du travail de Laura Gay

3. C'est là un lien important entre cône isotrope et géométrie différentielle.

Chapitre 21

Méthode de gradient à pas optimal

Références : Hirriart-Urruty, *Optimisation et analyse convexe*, p 17-19 et p 53-56

Lemme (Inégalité de Kantorovitch)**.**

Soit $A \in \mathcal{S}_n^{++}$ et $\lambda_1 \geqslant ... \geqslant \lambda_n$ ses valeurs propres, alors pour tout $x \in \mathbb{R}^n$,

$$\|x\|^4 \leqslant (Ax,x)(A^{-1}x,x) \leqslant \frac{1}{4}\left(\sqrt{\frac{\lambda_1}{\lambda_n}} + \sqrt{\frac{\lambda_n}{\lambda_1}}\right)^2 \|x\|^4.$$

Démonstration. Il suffit de démontrer l'inégalité pour $\|x\| = 1$. Puis comme $A \in \mathcal{S}_n^{++}$, il existe $P \in \mathrm{O}_n(\mathbb{R})$ telle que $A = {}^tP\Delta P$ avec $\Delta = \mathrm{Diag}(\lambda_1, ..., \lambda_n)$. Par le changement de variable $y = Px$, il suffit de démontrer

$$1 \leqslant (\Delta y, y)(\Delta^{-1}y, y) \leqslant \frac{1}{4}\left(\sqrt{\frac{\lambda_1}{\lambda_n}} + \sqrt{\frac{\lambda_n}{\lambda_1}}\right)^2.$$

On fixe y. On note ensuite M_i le point de coordonnées $\left(\lambda_i, \frac{1}{\lambda_i}\right)$, et M le barycentre des M_i avec les coefficients y_i^2. Alors M a pour coordonnées $\big((\Delta y, y), (\Delta^{-1}y, y)\big)$.
Tous les M_i sont dans l'intersection de l'épigraphe de $x \mapsto \frac{1}{x}$ et du demi-plan inférieur donné par la droite liant M_1 et M_n, donc M est dans ce domaine.
On peut alors majorer et minorer l'ordonnée de M :

$$\frac{1}{(\Delta y, y)} \leqslant (\Delta^{-1}y, y) \leqslant -\frac{(\Delta y, y)}{\lambda_1\lambda_n} + \frac{1}{\lambda_1} + \frac{1}{\lambda_n}.$$

D'où il vient

$$1 \leqslant (\Delta y, y)(\Delta^{-1}y, y) \leqslant \frac{(\Delta y, y)(\lambda_1 + \lambda_n - (\Delta y, y))}{\lambda_1\lambda_n}.$$

En trouvant le maximum de $u \mapsto \frac{u(\lambda_1 + \lambda_n - u)}{\lambda_1\lambda_n}$, on a exactement l'inégalité voulue. □

Le but de ce développement est d'appliquer l'algorithme de gradient optimal à la fonction $f : x \in \mathbb{R}^n \mapsto \frac{1}{2}(Ax,x) + (b,x) + c$ où $A \in \mathcal{S}_n^{++}$, $b \in \mathbb{R}^n$ et $c \in \mathbb{R}$. Celle-ci est sympathique car l'algorithme pourra être calculé explicitement avec elle, ce qui n'est quasiment jamais le cas.
On gardera la notation $\lambda_1 \geqslant ... \geqslant \lambda_n$ pour les valeurs propres de A.

L'algorithme de gradient à pas optimal donne une méthode numérique permettant de minimiser des fonctions de $\mathbb{R}^n$. Il est défini comme suit :
On se donne $x_0 \in \mathbb{R}^n$, puis pour passer de l'étape k à l'étape $k+1$, on calcule $x_{k+1} = x_k + t_k d_k$, où $d_k = -\nabla f(x_k)$ et t_k est l'unique réel positif minimisant $t \mapsto f(x_k + td_k)$ (si $\nabla f(x_k) \neq 0$). On s'arrête lorsqu'on est assez proche du minimum, c'est à dire lorsque $\|\nabla f(x_k)\| < \epsilon$ pour une tolérance ϵ que l'on s'est fixé.

Théorème.

La fonction f définie auparavant a un unique minimum, noté $\overline{x}$. On appelle $\overline{f} = f(\overline{x})$ et $c(A) = \|A\| \left\|A^{-1}\right\| = \dfrac{\lambda_1}{\lambda_n}$ le conditionnement de A, alors la suite $(x_k)_k$ donnée par la méthode de gradient à pas optimal vérifie

$$f(x_k) - \overline{f} \leqslant (f(x_0) - \overline{f}) \left(\frac{c(A)-1}{c(A)+1}\right)^{2k}$$

et

$$\|x_k - \overline{x}\| \leqslant \left(\frac{2(f(x_0)-\overline{f})}{\lambda_n}\right)^{\frac{1}{2}} \left(\frac{c(A)-1}{c(A)+1}\right)^{k}$$

Démonstration. • Existence et unicité du minimum :
f est coercive ($\lim\limits_{x\to\infty} f(x) = \infty$), donc le minimum de f n'est pas à l'infini. En se restreignant à un compact assez grand, comme f est continue sur ce compact, elle atteint son minimum sur celui-ci. On a donc existence du minimum.
Puis comme $D^2 f(x) = A$ est définie positive, f est fortement convexe, donc le minimum est unique.
Le minimum est caractérisé par $\nabla f(\overline{x}) = 0$, soit $\overline{x} = -A^{-1}b$. D'où $\overline{f} = -\dfrac{1}{2}(A^{-1}b, b) + c$.

• Précisions sur d_k et t_k :
On suppose que pour les k étudiés $\nabla f(x_k)$ ne s'annule pas, sinon l'algorithme est terminé.
On a, pour $t \in \mathbb{R}$,

$$\begin{aligned} f(x_k + td_k) &= \frac{1}{2}(Ax_k, x_k) + \frac{t}{2}(Ax_k, d_k) + \frac{t}{2}(Ad_k, x_k) + \frac{t^2}{2}(Ad_k, d_k) + (b, x_k) + t(b, d_k) + c \\ &= f(x_k) + t(Ax_k + b, d_k) + \frac{t^2}{2}(Ad_k, d_k) \end{aligned}$$

Ce polynôme est minimisé lorsque $t = t_k := -\dfrac{(Ax_k + b, d_k)}{(Ad_k, d_k)} = \dfrac{\|d_k\|^2}{(Ad_k, d_k)}$ (car $d_k = -\nabla f(x_k) = -(Ax_k + b)$).[1]

• On peut maintenant calculer $f(x_{k+1})$:

$$\begin{aligned} f(x_{k+1}) = f(x_k + t_k d_k) &= f(x_k) + \frac{\|d_k\|^2}{(Ad_k, d_k)}(Ax_k + b, d_k) + \frac{1}{2}\frac{\|d_k\|^4}{(Ad_k, d_k)^2}(Ad_k, d_k) \\ &= f(x_k) - \frac{\|d_k\|^2}{(Ad_k, d_k)}\|d_k\|^2 + \frac{\|d_k\|^4}{2(Ad_k, d_k)} \\ &= f(x_k) - \frac{\|d_k\|^4}{2(Ad_k, d_k)}. \end{aligned}$$

Pour se ramener au lemme de Kantorovitch, on calcule $(A^{-1}d_k, d_k)$:

$$\begin{aligned} (A^{-1}d_k, d_k) &= (A^{-1}(Ax_k + b), Ax_k + b) \\ &= (Ax_k, x_k) + (b, x_k) + (Ax_k, A^{-1}b) + (A^{-1}b, b) \\ &= 2\left(\frac{1}{2}(Ax_k, x_k) + (b, x_k) + c + \frac{1}{2}(A^{-1}b, b) - c\right) \\ &= 2(f(x_k) - \overline{f}). \end{aligned}$$

On a donc

$$\begin{aligned} f(x_{k+1}) - \overline{f} &= (f(x_k) - \overline{f}) - \frac{\|d_k\|^4}{2(Ad_k, d_k)} \\ &= (f(x_k) - \overline{f})\left(1 - \frac{\|d_k\|^4}{2(f(x_k) - \overline{f})(Ad_k, d_k)}\right) \\ &= (f(x_k) - \overline{f})\left(1 - \frac{\|d_k\|^4}{(Ad_k, d_k)(A^{-1}d_k, d_k)}\right). \end{aligned}$$

1. On rappelle que (Ad_k, d_k) est non nul par définition de la définie positivité de A.

• On applique Kantorovitch :
On a

$$(Ad_k, d_k)(A^{-1}d_k, d_k) \leqslant \frac{1}{4}\left(\sqrt{\frac{\lambda_1}{\lambda_n}} + \sqrt{\frac{\lambda_n}{\lambda_1}}\right)^2 \|d\|_k^4 .$$

Donc, comme $f(x_k) - \overline{f} \geqslant 0$, on a

$$\begin{aligned} f(x_{k+1}) - \overline{f} &= (f(x_k) - \overline{f})\left(1 - \frac{\|d_k\|^4}{(Ad_k, d_k)(A^{-1}d_k, d_k)}\right) \\ &\leqslant (f(x_k) - \overline{f})\left(1 - 4\left(\sqrt{\frac{\lambda_1}{\lambda_n}} + \sqrt{\frac{\lambda_n}{\lambda_1}}\right)^{-2}\right) \\ &\leqslant (f(x_k) - \overline{f})\left(1 - 4\frac{1}{c(A) + c(A)^{-1} + 2}\right) \\ &\leqslant (f(x_k) - \overline{f})\left(1 - 4\frac{c(A)}{(c(A)+1)^2}\right) \\ &\leqslant (f(x_k) - \overline{f})\left(\frac{c(A)-1}{c(A)+1}\right)^2 . \end{aligned}$$

On a ainsi la première inégalité voulue par récurrence.
Pour la deuxième, on la déduit de la précédente en remarquant que

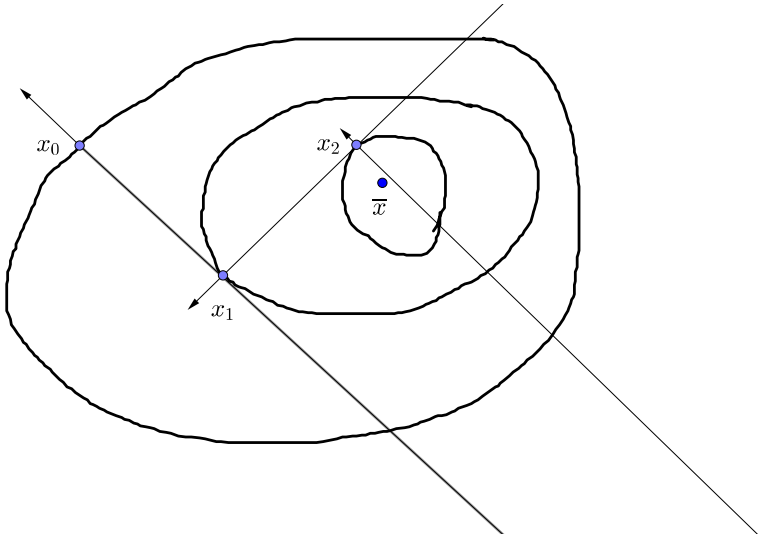
$$\begin{aligned} f(x_k) - \overline{f} &= \frac{1}{2}(Ax_k, x_k) + (b, x_k) + c + \frac{1}{2}(A^{-1}b, b) - c \\ &= \frac{1}{2}(Ax_k, x_k) - (A\overline{x}, x_k) + \frac{1}{2}(A\overline{x}, \overline{x}) \\ &= \frac{1}{2}(A(x_k - \overline{x}), (x_k - \overline{x})) \\ &\geqslant \frac{\lambda_n}{2}\|x_k - \overline{x}\|^2 . \end{aligned}$$

□

On voit sur le dessin ci-dessous l'algorithme appliqué. On part de x_0, on cherche le gradient de f en ce point et on part chercher le prochain point sur la droite donné par $\nabla f(x_0)$. Les courbes tracées représentent certaines lignes de niveau de f.

On a $d_{k+1} = -Ax_{k+1} - b = -Ax_k - b - t_k Ad_k = d_k - t_k Ad_k$, donc $(d_{k+1}, d_k) = \|d_k\|^2 - t_k(Ad_k, d_k) = 0$. Les directions de descente sont donc consécutivement orthogonales entre elles.

D'autre part, x_{k+1} est le point d'une courbe de niveau tangente à $\nabla f(x_k)$ en x_{k+1}. En effet, si ce n'était pas le cas, la droite donnée par $t \mapsto x_k + td_k$ couperait la ligne de niveau contenant x_{k+1} en deux points distincts. Le segment reliant ceux-ci contiendrait des valeurs de f plus faibles que $f(x_{k+1})$ car f est fortement convexe ; cela est absurde. Par régularité de f, donc des courbes de niveau, la droite est tangente à la ligne de niveau en l'unique point d'intersection.



On voit que si $c(A)$ est proche de 1 - c'est à dire que l'on a un faible conditionnement/que les valeurs propres de A sont proches les unes des autres - alors l'algorithme converge rapidement. Sur le dessin, cela correspond au cas où les lignes de niveaux sont quasiment des cercles.
Au contraire, si le conditionnement est fort, la convergence est beaucoup plus lente. Cela correspond à des sortes d'ellipses très aplaties.
Trouver le minimum revient à inverser la matrice A, car $\overline{x} = -A^{-1}b$, et on se rend compte que plus la matrice est difficile à inverser, plus l'algorithme met du temps à converger.

Remarques : • En pratique, on admet que $(A^{-1}d_k, d_k) = 2(f(x_k) - \overline{f})$ et on insiste sur la convexité de f, l'existence et l'unicité du minimum et la dépendance au conditionnement.
• Si on présente la leçon convexité, on présente en détail le lemme de Kantorovitch et on va très vite sur le gradient à pas optimal. Sinon, on admet Kantorovitch.
• Dans le cas général, on peut montrer que si f est fortement convexe et $\mathcal{C}^1$, alors la suite donnée par cette algorithme converge vers le minimum.
• Cet algorithme est dit de descente. C'est un algorithme d'optimisation différentiable, destiné à minimiser une fonction réelle différentiable définie sur un espace euclidien ou, plus généralement, sur un espace hilbertien. Au point courant, un déplacement est effectué le long d'une direction de descente, de manière à faire décroître la fonction.
On peut en citer trois autres : celle de Newton-Raphson appliqué à ∇f, celle de gradient à pas constant (qui converge pour un pas assez petit si f est fortement convexe $\mathcal{C}^1$ et si ∇f est localement lipschitzien) et celle de gradient conjugué.
La méthode de gradient conjugué s'applique à la minimisation de fonctions de la forme $x \in \mathbb{R}^n \mapsto \frac{1}{2}(Ax, x) + (b, x)$. A chaque itération, au lieu de minimiser la fonction sur l'espace vectoriel $\text{Vect}(\nabla f(x_k))$, on la minimise sur $\text{Vect}(\nabla f(x_0), ..., \nabla f(x_k))$. L'algorithme converge donc exactement vers la solution en au plus n itérations.

Chapitre 22

Méthode de Kacmarz

Références : Aucune

Soit $A \in \mathrm{GL}_n(\mathbb{R})$ et $b \in R^n$. On cherche la solution x_∞ du système linéaire $Ax = b$. La méthode de Kacmarz consiste à construire une suite récurrente en projetant sur des hyperplans bien choisis.

Algorithme.
Pour $1 \leqslant i \leqslant n$, on note ${}^t a_i$ la i-ème ligne de la matrice A. On définit les vecteurs "renormalisés" suivants : $u_i = \dfrac{a_i}{\|a_i\|}$ et $\alpha = \left(\dfrac{b_i}{\|a_i\|}\right)_i$.

On considère les hyperplans affines, H_i, de direction $\mathrm{Vect}(u_i)^\perp$, passant par $\alpha_i u_i$. On note Π_i la projection sur $\mathrm{Vect}(u_i)^\perp$. On confondra abusivement le projecteur et sa matrice dans la base canonique.

Soit $x_0 \in \mathbb{R}^n$. On construit la suite $(x_k)_{k\in\mathbb{N}}$ par : pour tout $k \in \mathbb{N}$, x_{k+1} est la projection de x_k sur H_r, où $r \equiv 1 + k\ [n]$, *id est* $x_{k+1} = \Pi_r(x_k) + \alpha_r u_r$.

Lemme.

On a

$$\{x_\infty\} = \bigcap_{i=1}^{n} H_i.$$

Démonstration.
• Soit $z \in H_i$, alors il existe $z_i \in \mathrm{Vect}(u_i)^\perp$ tel que $z = \alpha_i u_i + z_i$. On en déduit que $\langle a_i, z\rangle = b_i$. Ainsi, pour $z \in \bigcap_{i=1}^{n} H_i$, on a : $Az = b$, *id est* $\bigcap_{i=1}^{n} H_i \subset \{x_\infty\}$.
• Pour l'inclusion réciproque, comme $Ax_\infty = b$, on a pour tout i, $\langle a_i, x_\infty\rangle = b_i$, donc $\langle u_i, x_\infty\rangle = \alpha_i$.
Pour conclure, on utilise que

$$\forall i, \mathbb{R}^n = \mathbb{R}u_i \oplus^\perp \mathrm{Vect}(u_i)^\perp.$$

Ainsi $x_\infty = \delta_i u_i + c_i$ avec $c_i \in \mathrm{Vect}(u_i)^\perp$ et le produit scalaire précédent donne $\delta_i = \alpha_i$, donc $x_\infty \in H_i$. □

Lemme.

Soit $u \in \mathbb{R}^n$ un vecteur unitaire. Le projecteur orthogonal sur $\mathrm{Vect}(u)^\perp$ a pour matrice dans la base canonique $\Pi = I_n - u\,{}^t u$. De plus, on a : $\|\Pi\| = 1$ et pour tout $x \notin \mathrm{Vect}(u)^\perp$ on a : $\|\Pi x\| < \|x\|$.

Démonstration. Soit $x \in \mathbb{R}^n$ et $y = \Pi x$ le projeté orthogonal de x sur $\mathrm{Vect}(u)^\perp$. Le vecteur y est caractérisé par :

$$\begin{cases} y \in \mathrm{Vect}(u)^\perp \\ \forall z \in \mathrm{Vect}(u)^\perp, \quad \langle z, y - x\rangle = 0 \end{cases}$$

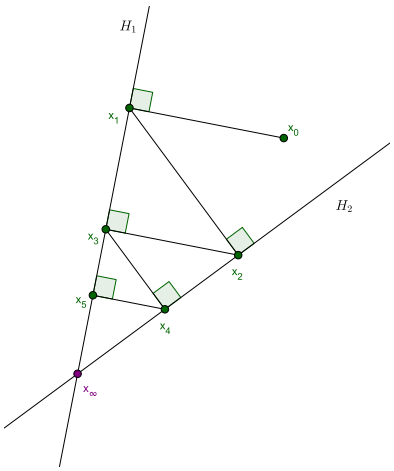


FIGURE 22.1 – Illustration de la méthode.

On pose $\tilde{y} = (I_n - u^{\mathrm{t}}u)x$. D'une part, on a :

$$\begin{aligned}\langle u, \tilde{y}\rangle &= \langle u, x\rangle - \left\langle u, u^{\mathrm{t}}ux\right\rangle \\ &= \langle u, x\rangle - \left\langle u^{\mathrm{t}}uu, x\right\rangle \\ &= \langle u, x\rangle - \langle u, x\rangle \quad \text{car } {}^{\mathrm{t}}uu = 1 \\ &= 0\end{aligned}$$

Ainsi, on a : $\tilde{y} \in \mathrm{Vect}(u)^{\perp}$. D'autre part, pour tout $z \in \mathrm{Vect}(u)^{\perp}$, on a :

$$\begin{aligned}\langle z, x - \tilde{y}\rangle &= \langle z, x\rangle - \langle z, \tilde{y}\rangle \\ &= \langle z, x\rangle - \langle z, x\rangle + \left\langle z, u^{\mathrm{t}}ux\right\rangle \\ &= \left\langle u^{\mathrm{t}}uz, x\right\rangle \\ &= 0 \quad \text{car } {}^{\mathrm{t}}uz = \langle u, z\rangle = 0\end{aligned}$$

Ainsi, on a $\tilde{y} = y$ et $\Pi = I_n - u^{\mathrm{t}}u$.

Pour conclure, soit $x \in \mathbb{R}^n$, d'après le théorème de Pythagore, on a : $\|x\|^2 = \|\Pi x\|^2 + \|(I_n - \Pi)x\|^2$. On en déduit que : $\|\Pi\| = 1$ ainsi que l'inégalité stricte. □

Nous allons maintenant pouvoir nous intéresser à la convergence de cette méthode.

Théorème.

Pour tout $x_0 \in \mathbb{R}^n$, la suite $(x_k)_{k\in\mathbb{N}}$ converge vers x_∞.

Démonstration. On note $\epsilon_k = x_k - x_\infty$ l'erreur d'approximation à l'étape k. On remarque que l'on a $\epsilon_{k+1} = \Pi_r\epsilon_k$. En effet, on a

$$\begin{cases} x_\infty = \alpha_r u_r + \Pi_r x_\infty \ (\text{car } x_\infty \in H_r) \\ x_{k+1} = \Pi_r(x_k) + \alpha_r u_r \end{cases},$$

donc

$$\varepsilon_{k+1} = \Pi_r(x_k) + \alpha_r u_r - \alpha_r u_r - \Pi_r x_\infty = \Pi_r\epsilon_k.$$

Il s'ensuit que la suite $(\|\epsilon_k\|)_k$ est décroissante et minorée par zéro. Elle converge donc. On pose $T = \Pi_n \dots \Pi_1$. Pour tout k, on a : $\|\epsilon_{kn}\| \leqslant \|T\|^k\|\epsilon_0\|$. Il nous suffit donc de montrer que l'on a : $\|T\| < 1$.

Soit $x \in \mathbb{R}^n$ tel que $\|Tx\| = \|x\|$. Cela signifie que pour tout i $\|\Pi_{i+1}(\Pi_i \dots \Pi_1)x\| = \|(\Pi_i \dots \Pi_1)x\|$. Or d'après le lemme 2, on en déduit que pour tout i, $(\Pi_i \dots \Pi_1)x \in \mathrm{Vect}(u_{i+1})^{\perp}$ et $(\Pi_i \dots \Pi_1)x = x$. Il en résulte que $x \in \bigcap_{i=1}^{n} \mathrm{Vect}(u_i)^{\perp}$, *id est* $Ax = 0$. Ainsi $x = 0$.

Ainsi, pour tout $x \in \mathbb{R}^n \setminus \{0\}$, $\|Tx\| < \|x\|$.
Comme on travaille en dimension finie, on a bien $\|T\| < 1$. [1] Ce qui montre la convergence. □

Remarques : • Le calcul d'une matrice Π_i demande $\mathcal{O}(n^3)$ opérations élémentaires. Mais comme on calcule toujours sa valeur en un certain vecteur y, on a juste à calculer $\Pi_i y = y - \langle u, y \rangle u$. Cela fait $\mathcal{O}(n)$ opérations élémentaires.
Ainsi, pour faire une n-itération (calculer Ty), il faut $\mathcal{O}(n^2)$ opérations élémentaires. On est dans le même ordre de grandeur que pour les autres méthodes de résolution approchée de systèmes linéaires (gradient, itératives linéaires...).
• En dimension infinie, le dernier argument du développement est faux. Plaçons-nous dans $(c_0(\mathbb{N}), \|\|_\infty)$ les suites réelles tendant vers 0. Alors pour l'opérateur $Tu = \sum \frac{u_n}{2^{n+1}}$, on a bien $\|Tu\| < \|u\|$ si $u \neq 0$ et $\|T\| = 1$.
• Dans le cas où A est orthogonale, ses lignes sont orthogonales et donc l'algorithme termine en au plus n étapes.
• En fait, l'algorithme marche quand même lorsque A n'est pas inversible et quand b est dans l'image de A. (Merci Thibaut Tardieu)

Adapté du travail de Baptiste Huguet.

1. La boule unité étant compacte, T atteint son maximum dessus.

Chapitre 23

Méthode de Laplace

Références : Rouvière, *Petit guide de calcul différentiel*, ex 113

Théorème.

Soient $a < b \leqslant \infty$, $\varphi : [a,b[\to \mathbb{R}$ de classe $\mathcal{C}^2$ sur $[a,b[$ [a] avec $\varphi' > 0$ sur $]a,b[$, et $f : [a,b[\to \mathbb{C}$ continue en a telle que $f(a) \neq 0$. On suppose de plus qu'il existe $t_0 \in \mathbb{R}$ tel que $e^{-t_0\varphi} f \in L^1(]a,b[)$, alors l'intégrale $F(t) = \displaystyle\int_a^b e^{-t\varphi(x)} f(x)\mathrm{d}x$ est définie pour $t \geqslant t_0$ et

1. si $\varphi'(a) > 0$, alors $F(t) \underset{+\infty}{\sim} \dfrac{1}{\varphi'(a)} \times \dfrac{e^{-t\varphi(a)} f(a)}{t}$,
2. si $\varphi'(a) = 0$ et $\varphi''(a) > 0$, alors $F(t) \underset{+\infty}{\sim} \sqrt{\dfrac{\pi}{2\varphi''(a)}} \times \dfrac{e^{-t\varphi(a)} f(a)}{\sqrt{t}}$.

[a] C'est à dire φ est la restriction d'une fonction $\mathcal{C}^2$ sur un ouvert contenant $[a,b[$.

Démonstration. On peut supposer $t_0 = 0$. En effet, il suffit de poser $\widetilde{f} = e^{-t_0\varphi} f$ et on a l'énoncé voulu.

• L'intégrale F est bien définie.
En effet, φ est croissante, donc pour $t \geqslant 0$,

$$\left|e^{-t\varphi(x)} f(x)\right| \leqslant e^{-t\varphi(a)} \left|f(x)\right| \in L^1.$$

• Commençons par étudier deux exemples : commençons par $a = 0$ et $\varphi(x) = x$.
La continuité de f en 0 donne l'existence de $M > 0$ et $\alpha > 0$ tels que $|f| \leqslant M$ sur $[0,\alpha]$. Alors pour $t > 0$, on a

$$t\int_0^\alpha e^{-tx} f(x)\mathrm{d}x = \int_0^{t\alpha} e^{-y} f\left(\frac{y}{t}\right)\mathrm{d}y \underset{t\to+\infty}{\longrightarrow} \int_0^\infty e^{-y} f(0)\mathrm{d}y = f(0).$$

Le passage à la limite est justifié par le théorème de convergence dominée car $\left|e^{-y} f(\frac{y}{t})\mathbb{1}_{[0,t\alpha]}\right| \leqslant Me^{-y} \in L^1([0,\infty[)$.
Puis comme $f \in L^1$, on a

$$t\left|\int_\alpha^b e^{-tx} f(x)\mathrm{d}x\right| \leqslant te^{-t\alpha}\int_0^b \left|f(x)\right|\mathrm{d}x \underset{t\to+\infty}{\longrightarrow} 0.$$

On a bien

$$\int_0^b e^{-tx} f(x)\mathrm{d}x \sim \frac{f(0)}{t}.$$

Continuons avec un autre exemple : supposons que $a = 0$ et $\varphi(x) = x^2$.
Par la même méthode que précédemment, on a pour $t > 0$

$$\sqrt{t}\int_0^\alpha e^{-tx^2} f(x)\mathrm{d}x = \int_0^{\sqrt{t}\alpha} e^{-y^2} f\left(\frac{y}{\sqrt{t}}\right)\mathrm{d}y \underset{t\to+\infty}{\longrightarrow} \int_0^\infty e^{-y^2} f(0)\mathrm{d}y = \frac{\sqrt{\pi}}{2} f(0).$$

Puis

$$\sqrt{t}\left|\int_\alpha^b e^{-tx^2}f(x)\mathrm{d}x\right| \leqslant \sqrt{t}e^{-t\alpha^2}\int_0^b |f(x)|\,\mathrm{d}x \underset{t\to+\infty}{\longrightarrow} 0.$$

D'où

$$\int_0^b e^{-tx^2}f(x)\mathrm{d}x \sim \frac{\sqrt{\pi}f(0)}{2\sqrt{t}}.$$

• Étudions à présent le premier cas du théorème : $\varphi' > 0$ sur $[a,b[$.
L'idée est de se ramener aux cas vus en exemple.
On pose donc naturellement le changement de variable $u = \varphi(x) - \varphi(a)$ (Comme φ est strictement croissante, on obtient bien un $\mathcal{C}^1$-difféomorphisme.) et on note ψ sa bijection réciproque. Alors on a

$$F(t) = e^{-t\varphi(a)}\int_a^b e^{-t(\varphi(x)-\varphi(a))}f(x)\mathrm{d}x = e^{-t\varphi(a)}\int_0^{\psi^{-1}(b)} e^{-tu}f(\psi(u))\psi'(u)\mathrm{d}u \sim e^{-t\varphi(a)}\frac{f(\psi(0))\psi'(0)}{t}.$$

Or $\psi(0) = a$ et $\psi'(0) = \dfrac{1}{\varphi'(\psi(0))} = \dfrac{1}{\varphi'(a)}$, donc on a bien

$$F(t) \sim \frac{1}{\varphi'(a)} \times \frac{e^{-t\varphi(a)}f(a)}{t}.$$

• Il reste enfin le deuxième cas à traiter : $\varphi'(a) = 0$ et $\varphi''(a) > 0$.
On pose ici $u = \sqrt{\varphi(x) - \varphi(a)}$. On a bien un $\mathcal{C}^1$-difféomorphisme par théorème d'inversion globale car φ est strictement croissante. On note à nouveau ψ l'inverse.
On a alors

$$F(t) = e^{-t\varphi(a)}\int_a^b e^{-t(\varphi(x)-\varphi(a))}f(x)\mathrm{d}x = e^{-t\varphi(a)}\int_0^{\psi^{-1}(b)} e^{-tu^2}f(\psi(u))\psi'(u)\mathrm{d}u \sim e^{-t\varphi(a)}\frac{\sqrt{\pi}f(\psi(0))\psi'(0)}{2\sqrt{t}}.$$

On sait que $\psi(0) = a$, puis

$$(\psi^{-1})'(x) = \frac{\varphi'(x)}{2\sqrt{\varphi(x)-\varphi(a)}} \underset{a^+}{\sim} \frac{(x-a)\varphi''(a)}{2\sqrt{(x-a)^2\varphi''(a)/2}} = \sqrt{\frac{\varphi''(a)}{2}}.$$

Donc $\psi'(0) = \dfrac{1}{(\psi^{-1})'(\psi(0))} = \sqrt{\dfrac{2}{\varphi''(a)}}$ et on retrouve le résultat annoncé :

$$F(t) \underset{+\infty}{\sim} \sqrt{\frac{\pi}{2\varphi''(a)}} \times \frac{e^{-t\varphi(a)}f(a)}{\sqrt{t}}.$$

□

Corollaire (Formule de Stirling)**.**

On a

$$\Gamma(t+1) \underset{+\infty}{\sim} \left(\frac{t}{e}\right)^t \sqrt{2\pi t}.$$

Démonstration. On a

$$\Gamma(t+1) = \int_0^\infty e^{-x}x^t\mathrm{d}x.$$

Pour faire apparaître la forme du théorème, on applique le changement de variable $x = t(u+1)$ pour $t > 0$, ainsi on a

$$\Gamma(t+1) = \int_{-1}^\infty e^{-t(u+1)}t^t(u+1)^t t\mathrm{d}u = t^{t+1}\int_{-1}^\infty e^{-t(u+1-\ln(u+1))}\mathrm{d}u.$$

On pose $f = 1$ et $\varphi(u) = u + 1 - \ln(u+1)$. Alors $\varphi'(u) = 1 - \dfrac{1}{1+u} = \dfrac{u}{1+u}$ et $\varphi''(u) = \dfrac{1}{(1+u)^2}$.
On remarque que $\varphi' > 0$ sur $]0,\infty[$, donc en appliquant le théorème, on a

$$\int_0^\infty e^{-t(u+1-\ln(u+1))}\mathrm{d}u \sim \sqrt{\frac{\pi}{2\varphi''(0)}} \times \frac{e^{-t\varphi(0)}f(0)}{\sqrt{t}} = \sqrt{\frac{\pi}{2t}}e^{-t}.$$

Puis en faisant le changement de variable $v = -u$ dans la seconde intégrale, on a

$$\int_{-1}^{0} e^{-t(u+1-\ln(u+1))}\mathrm{d}u = \int_{0}^{1} e^{-t(1-v-\ln(1-v))}\mathrm{d}v.$$

On pose $\tilde{\varphi}(v) = 1 - v - \ln(1-v)$ et on remarque que le théorème s'applique. On obtient alors

$$\int_{-1}^{0} e^{-t(u+1-\ln(u+1))}\mathrm{d}u \sim \sqrt{\frac{\pi}{2t}}e^{-t}.$$

D'où il vient

$$\Gamma(t+1) \underset{+\infty}{\sim} 2t^{t+1}\sqrt{\frac{\pi}{2t}}e^{-t} = \left(\frac{t}{e}\right)^{t}\sqrt{2\pi t}.$$

□

Remarques : • On a un résultat similaire pour les intégrales du type $\int_a^b e^{it\varphi(x)}f(x)\mathrm{d}x$. On appelle cela la méthode de la phase stationnaire. Le lecteur intéressé pourra regarder le Zuily, Queffelec ou le Zuily.
• Ce développement semble un peu obscure sans l'expliquer un peu. Il faut se dire que φ est croissante et qu'en conséquence, comme l'exponentielle décroît vite, la valeur de l'intégrale est concentrée en $[a, a+\epsilon[$. On applique alors des formules de Taylor pour voir ce que l'intégrale donne.

Chapitre 24

Méthode de la sécante

Références : Demailly, *Analyse numérique et équations différentielles*, p 102

La méthode de Newton est une méthode numérique de recherche de points fixes. L'idée est de remplacer f par sa tangente en x_p. On a ainsi $y = f(x_p) + f'(x_p)(x - x_p)$, et donc l'intersection de la tangente avec l'axe des abscisses $y = 0$ est $x_{p+1} = x_p - \dfrac{f(x_p)}{f'(x_p)}$. Elle est très performante (ordre 2). Néanmoins il est nécessaire de bien connaître la dérivée de f pour pouvoir calculer la suite approximant le zéro définie par $x_{p+1} = x_p - \dfrac{f(x_p)}{f'(x_p)}$. Le but de la méthode de la sécante est d'approximer f' par une corde.

Insérez un dessin ici !

Théorème.

Soit f de classe $\mathcal{C}^2$, a un zéro de f et tel que $f'(a) \neq 0$. On pose $I = [a - r, a + r]$ un intervalle où f' ne s'annule pas, et on définit la suite x_p par

$$x_{p+1} = x_p - \frac{f(x_p)}{\tau_p}, \text{ avec } \tau_p = \frac{f(x_p) - f(x_{p-1})}{x_p - x_{p-1}}.$$

Alors si on note $(s_p)_p$ la suite de Fibonacci de premiers termes $s_0 = s_1 = 1$, il existe K et h des réels positifs tels que pour x_0, $x_1 \in [a - h, a + h]$ distincts, on a

$$|x_p - a| \leqslant \frac{1}{K} \left(K \max(|x_0 - a|, |x_1 - a|)\right)^{s_p}.$$

Démonstration. On note $M_i = \max_I \left|f^{(i)}\right|$, $m_i = \min_I \left|f^{(i)}\right|$, et

$$\tau : \begin{array}{ccc} I \times I & \to & \mathbb{R} \\ (x, y) & \mapsto & \begin{cases} \dfrac{f(y) - f(x)}{y - x} \text{ si } x \neq y \\ f'(x) \text{ si } x \neq y \end{cases} \end{array}.$$

- Étude de τ :

On remarque que $\tau(x, y) = \displaystyle\int_0^1 f'(x + t(y - x))\mathrm{d}t$, donc par les théorèmes sur les intégrales à paramètres, τ est $\mathcal{C}^1$.
On peut alors utiliser le théorème de dérivation sous le signe intégrale car f est $\mathcal{C}^2$:

$$\frac{\partial \tau}{\partial x}(x, y) = \int_0^1 (1 - t) f''(x + t(y - x))\mathrm{d}t \text{ et } \frac{\partial \tau}{\partial y}(x, y) = \int_0^1 t f''(x + t(y - x))\mathrm{d}t.$$

D'où on a $\left|\dfrac{\partial \tau}{\partial x}\right| \leqslant \dfrac{M_2}{2}$ et $\left|\dfrac{\partial \tau}{\partial y}\right| \leqslant \dfrac{M_2}{2}$, et comme f' est de signe constant, $|\tau| \geqslant m_1$.
Pour finir, on a $\left|\tau(x, y) - f'(x)\right| = |\tau(x, y) - \tau(x, x)| = \left|\displaystyle\int_x^y \frac{\partial \tau}{\partial y}(x, t)\mathrm{d}t\right| \leqslant \dfrac{M_2}{2} |y - x|$.

• Raisonnons de la même manière sur $\psi(x,y) = x - \dfrac{f(x)}{\tau(x,y)}$.

Posons $h_p = x_p - a$, alors comme $x_{p+1} = \psi(x_p, x_{p-1})$, on a

$$\forall p \geqslant 1, h_{p+1} = \psi(x_p, x_{p-1}) - a = \psi(a+h_p, a+h_{p-1}) - \psi(a,a).$$

On remarque comme précédemment que

$$h_{p+1} = \int_0^1 h_p \frac{\partial \psi}{\partial x}(a+th_p, a+th_{p-1}) + h_{p-1}\frac{\partial \psi}{\partial y}(a+th_p, a+th_{p-1})\mathrm{d}t.$$

Puis

$$\begin{cases} \dfrac{\partial \psi}{\partial x}(x,y) = 1 - \dfrac{f'(x)\tau(x,y) - f(x)\frac{\partial \tau}{\partial x}}{\tau(x,y)^2} = \dfrac{\tau(x,y) - f'(x)}{\tau(x,y)} + f(x)\dfrac{\frac{\partial \tau}{\partial x}}{\tau(x,y)^2} \\ \dfrac{\partial \psi}{\partial y}(x,y) = f(x)\dfrac{\frac{\partial \tau}{\partial y}}{\tau(x,y)^2} \end{cases}$$

En utilisant les inégalités de la première étape et le fait que $|f(x)| = |f(x) - f(a)| \leqslant M_1 |x-a|$ par les accroissement finis, on a :

$$\begin{cases} \left|\dfrac{\partial \psi}{\partial x}(x,y)\right| \leqslant \dfrac{M_2 |y-x|}{2m_1} + |x-a| \dfrac{M_1 M_2}{2m_1^2} \\ \left|\dfrac{\partial \psi}{\partial y}(x,y)\right| \leqslant |x-a| \dfrac{M_1 M_2}{2m_1^2} \end{cases}$$

On fixe alors $(x,y) = (a+th_p, a+th_{p-1})$ pour $t \in [0,1]$ et $p \geqslant 1$ en supposant que x_p, $x_{p-1} \in I$ (on le montrera à la fin par récurrence), alors $|y-x| \leqslant (|h_p| + |h_{p-1}|)t$ et $|x-a| = |h_p|\, t$, donc

$$\begin{cases} \left|\dfrac{\partial \psi}{\partial x}(x,y)\right| \leqslant \left(\dfrac{M_2}{2m_1}(|h_p| + |h_{p-1}|) + \dfrac{M_1 M_2}{2m_1^2}|h_p|\right) t \\ \left|\dfrac{\partial \psi}{\partial y}(x,y)\right| \leqslant \dfrac{M_1 M_2}{2m_1^2}|h_p|\, t \end{cases}$$

D'où en mettant tout bout à bout :

$$\begin{aligned} |h_{p+1}| &\leqslant \left(\frac{M_2}{2m_1}|h_p|(|h_p| + |h_{p-1}|) + \frac{M_1 M_2}{2m_1^2}|h_p|^2 + \frac{M_1 M_2}{2m_1^2}|h_p|\,|h_{p-1}|\right)\int_0^1 t\mathrm{d}t \\ &= \frac{1}{2}\underbrace{\left(\frac{M_2}{2m_1} + \frac{M_1 M_2}{2m_1^2}\right)}_{K}|h_p|(|h_p| + |h_{p-1}|) \\ &\leqslant K|h_p|\max(|h_p|, |h_{p-1}|). \end{aligned}$$

• Conclusion :

On pose $h = \min(r, \dfrac{1}{K})$, alors pour x_0, $x_1 \in [a-h, a+h]$, on a $|h_2| \leqslant K\dfrac{1}{K}\max(|h_1|, |h_0|) \leqslant h$. Par récurrence, cela légitime tous les calculs du dessus et on a $\forall p \geqslant 1$, $|h_{p+1}| \leqslant |h_p| \leqslant h$ donc

$$\forall p \geqslant 2, |h_{p+1}| \leqslant K|h_p|\,|h_{p-1}|.$$

On a trivialement $|h_p| \leqslant \dfrac{1}{K}(K\max(|h_0|, |h_1|))^{s_p}$ pour $p = 0$ ou $p = 1$.

Pour $p = 2$, on a vu $|h_2| \leqslant K|h_1|\max(|h_1|, |h_0|) \leqslant \dfrac{1}{K}K^2\max(|h_1|, |h_0|)^2$.

Enfin, si on suppose le résultat vrai jusqu'à un rang $p \geqslant 2$, alors

$$|h_{p+1}| \leqslant K|h_p|\,|h_{p-1}| \leqslant K\frac{1}{K}(K\max(|h_0|, |h_1|))^{s_p}\frac{1}{K}(K\max(|h_0|, |h_1|))^{s_{p-1}} = \frac{1}{K}(K\max(|h_0|, |h_1|))^{s_{p+1}}.$$

Le théorème est ainsi démontré. □

Remarques : • Attention à ne pas oublier le cas $p = 2$! La relation $|h_{p+1}| \leqslant K|h_p|\,|h_{p-1}|$ n'est pas forcément vraie pour $p = 1$.

• On dit qu'une suite converge à l'ordre au moins p si il existe $C > 0$ tel que $\forall k \in \mathbb{N}$, $|x_{k+1} - a| \leqslant |x_k - a|^p$. La méthode de Newton est d'ordre 2. Il est difficile de mettre l'équation sous cette forme pour la méthode de la sécante. Néanmoins, on voit (et on vérifie numériquement) que comme $s_p \sim \dfrac{1}{\sqrt{5}}\left(\dfrac{1+\sqrt{5}}{2}\right)^{p+1}$, l'ordre vaut

$\varphi = \dfrac{1+\sqrt{5}}{2} \approx 1,618$. C'est donc une méthode moins rapide que celle de Newton, mais tout de même efficace.
• On a mieux que le théorème, on a trouvé une manière explicite de calculer le h pour avoir la convergence. Mais en pratique, on ne sait pas quel est le zéro de f, donc une question subsiste : comment choisir l'intervalle où on va converger quand on ne sait pas où est le zéro ?
Et bien, c'est difficile ! En pratique, l'algorithme converge tout le temps, mais c'est parce qu'on a de la chance.
• Et en dimensions supérieures ? Il existe des trucs, c'est détaillé dans le Allaire.
• On peut s'inspirer de cette méthode pour l'épreuve de modélisation ! En effet plutôt que de calculer la dérivée de f dans la méthode de Newton, on peut juste poser

$$\frac{f(x+\sqrt{\%eps}) - f(x)}{\sqrt{\%eps}}.$$

On trouve une méthode d'ordre compris entre φ et 2.

Chapitre 25

Méthode des petits pas

Références : Rombaldi, *Éléments d'analyse réelle*, p 221-224

Théorème.

Soit $f :]-1,1[\to \mathbb{R}$, une fonction continue qui admet en zéro le développement limité suivant :

$$\forall x \in]-1,1[,\ f(x) = x - \alpha x^{p+1} + \beta x^{2p+1} + o(x^{2p+1}) \ ,$$

avec $\alpha > 0$, $\beta \neq 0$ et $\gamma = \dfrac{(1+p)\alpha^2}{2} - \beta \neq 0$.
Alors pour tout x_0 assez petit, la suite des itérées de f est bien définie et vérifie :

$$\forall n \geqslant 0,\ x_n = \frac{1}{\sqrt[p]{p\alpha n}} - \frac{\gamma}{p^2\alpha^2 \sqrt[p]{p\alpha}} \frac{\ln(n)}{n \sqrt[p]{n}} + o\left(\frac{\ln(n)}{n \sqrt[p]{n}}\right) \quad .$$

Étape 1 : Montrons que la suite est bien définie.
On peut définir (par prolongement continue) les fonctions continues, g et h telles pour tout $x \in]-1,1[$, on ait :

$$f(x) = xg(x) \quad \text{et} \quad f(x) = x - \alpha x^{p+1} h(x) \quad .$$

On a $g(0) = 1 = h(0)$. Donc on dispose de $\eta > 0$ tel que g et h soient strictement positives sur $]-\eta, \eta[$. En particulier, pour tout $x \in [0, \eta]$, on a :

$$f(x) = xg(x) \geqslant 0 \quad \text{et} \quad f(x) - x = -\alpha x^{p+1} h(x) \leqslant 0 \quad .$$

Ainsi, le segment $[0, \eta]$ est stable par f. Pour tout x_0 dans ce compact, la suite des itérés de f est donc bien définie.

Étape 2 : Montrons que $(x_n)_{n\in\mathbb{N}}$ converge vers 0.
Comme on l'a vu précédemment, pour tout $x \in [0, \eta]$, on a : $f(x) \leqslant x$. La suite $(x_n)_{n\in\mathbb{N}}$ est donc décroissante et minorée par 0. Elle converge donc. Or f étant continue, cette limite est un point fixe de f. Le point 0 est évidemment un point fixe de f et de plus on a : $\forall x \in]0, \eta],\ f(x) < x$. La suite $(x_n)_{n\in\mathbb{N}}$ converge donc vers 0.

Étape 3 : Équivalent de la suite.
Soit $\lambda \in \mathbb{Z}^*$. On définit la suite $(y_n)_{n\in\mathbb{N}}$ par : $\forall y \in \mathbb{N},\ y_n = x_{n+1}^\lambda - x_n^\lambda$. On cherche un λ tel que cette suite admette une limite finie non nulle. Pour tout $n \in \mathbb{N}$, on a :

$$\begin{aligned}
y_n &= (x_n - \alpha x_n^{p+1} + \beta x_n^{2p+1} + o(x_n^{2p+1}))^\lambda - x_n^\lambda \\
&= x_n^\lambda (1 - \alpha x_n^p + \beta x_n^{2p} + o(x_n^{2p}))^\lambda - x_n^\lambda \\
&= x_n^\lambda \left(1 + \lambda(-\alpha x_n^p + \beta x_n^{2p}) + \frac{\lambda(\lambda-1)}{2}\alpha^2 x_n^{2p} + o(x_n^{2p})\right) - x_n^\lambda \\
&= -\alpha\lambda x_n^{p+\lambda} + \lambda\left(\beta + \frac{(\lambda-1)\alpha^2}{2}\right) x_n^{2p+\lambda} + o(x_n^{2p+\lambda})
\end{aligned}$$

Ainsi, la suite $(y_n)_{n\in\mathbb{N}}$ admet une limite finie non nulle pour $\lambda = -p$. On se fixe cette valeur de λ à présent. On a donc :

$$\forall n \in \mathbb{N},\ y_n = \alpha p + p\gamma x_n^p + o(x_n^p) \quad .$$

Par critère de Cesàro, on a :

$$\forall n \in \mathbb{N},\ \frac{x_n^{-p} - x_0^{-p}}{n} = \frac{1}{n}\sum_{k=0}^{n-1} y_k \underset{n\to+\infty}{\longrightarrow} p\alpha.$$

On en déduit alors que :

$$\begin{aligned}
\frac{x_n^{-p}}{np\alpha} &\underset{n\to+\infty}{\longrightarrow} 1 \\
x_n \sqrt[p]{np\alpha} &\underset{n\to+\infty}{\longrightarrow} 1 \\
x_n &\sim \frac{1}{\sqrt[p]{p\alpha n}}
\end{aligned}$$

Étape 4 : second terme du développement.
On a : $\forall n \in \mathbb{N},\ y_n = p\alpha + p\gamma x_n^p(1 + o(1))$. Ainsi, on a :

$$\sum_{k=0}^{n-1} y_k = np\alpha + p\gamma \sum_{k=0}^{n-1} x_n^p(1 + o(1)) \quad .$$

La suite $(x_n^p(1+o(1)))_{n\in_N}$ est positive. Elle est équivalente à la suite $\left(\frac{1}{p\alpha(n+1)}\right)_{n\in\mathbb{N}}$, dont la série diverge. Par sommation des équivalents des séries divergentes, on a :

$$\begin{aligned}
\sum_{k=0}^{n-1} y_k - np\alpha &\sim p\gamma \sum_{k=1}^{n} \frac{1}{p\alpha n} \\
\sum_{k=0}^{n-1} y_k - np\alpha &\sim \frac{\gamma}{\alpha}\ln(n) \\
\sum_{k=0}^{n-1} y_k &= np\alpha + \frac{\gamma}{\alpha}\ln(n) + o(\ln(n)) \\
x_n^{-p} &= np\alpha\left(1 + + \frac{\gamma\ln(n)}{np\alpha^2} + o\left(\frac{\ln(n)}{n}\right)\right) \\
x_n &= \frac{1}{\sqrt[p]{p\alpha n}}\left(1 + \frac{\gamma}{p\alpha^2}\frac{\ln(n)}{n} + o\left(\frac{\ln(n)}{n}\right)\right)^{-1/p} \\
x_n &= \frac{1}{\sqrt[p]{p\alpha n}}\left(1 - \frac{\gamma}{p^2\alpha^2}\frac{\ln(n)}{n} + o\left(\frac{\ln(n)}{n}\right)\right)
\end{aligned}$$

Remarques : Applications aux suites classiques.
• La fonction sinus admet le développement limité suivant en 0 :

$$\sin(x) = x - \frac{1}{3!}x^3 + \frac{1}{5!}x^5 + o(x^5).$$

On est bien dans les conditions de l'énoncé avec $\alpha = \frac{1}{6}$, $\beta = \frac{1}{120}$ et $p = 2$.
La suite des itérés du sinus admet donc pour développement asymptotique :

$$x_n = \sqrt{\frac{3}{n}} - \frac{3\sqrt{3}}{10}\frac{\ln(n)}{n\sqrt{n}} + o\left(\frac{\ln(n)}{n\sqrt{n}}\right) \quad .$$

• La fonction $x \mapsto \ln(1+x)$ admet le développement limité suivant en 0 :

$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} + o(x^3).$$

On est bien dans les conditions de l'énoncé avec $\alpha = \frac{1}{2}$, $\beta = \frac{1}{3}$ et $p = 1$.
La suite de ses itérés admet donc pour développement asymptotique :

$$x_n = \frac{2}{n} + \frac{2}{3}\frac{\ln(n)}{n^2} + o\left(\frac{\ln(n)}{n^2}\right) \quad .$$

Adapté du travail de Baptiste Huguet.

Chapitre 26

Modélisation de suites de variables aléatoires indépendantes

Références : Ouvrard, *Probabilités 2*, p 53-59

Soit $x \in [0,1[$, on pose les suites $(D_n(x))_{n\geqslant 1}$ et $(R_n(x))_{n\geqslant 0}$ définies par

$$\left\{\begin{array}{l} R_0(x) = x \\ Dn(x) = \lfloor 2R_{n-1}(x)\rfloor \\ R_n(x) = 2R_{n-1}(x) - D_n(x) \end{array}\right. .$$

Elles vérifient $D_n \in \{0,1\}$ et $R_n \in [0,1[$.
De plus, par récurrence, on a pour tout $n \in \mathbb{N}$

$$x = \sum_{j=1}^{n} \frac{D_j(x)}{2^j} + \frac{1}{2^n} R_n(x) = \sum_{j=1}^{\infty} \frac{D_j(x)}{2^j}.$$

On a ainsi défini le développement dyadique de $x \in [0,1[$.
Attention, celui-ci est non-unique. Par exemple, $\frac{1}{2} = \sum_{j=2}^{\infty} \frac{1}{2^j}$.

Théorème.

On se place sur $([0,1[, \mathcal{B}([0,1[), \mathbb{P})$ avec $\mathbb{P}$ la restriction de la mesure de Lebesgue sur $[0,1[$.
La suite $(D_n)_n$ est une suite de variables aléatoires iid de loi $b(1/2)$. De plus, pour tout $n \in \mathbb{N}$, R_n suit une loi uniforme sur $[0,1[$ et les variables aléatoires D_1, ..., D_n et R_n sont mutuellement indépendantes.

Démonstration. • Soit $n \in \mathbb{N}^*$ et $\varepsilon^n = (\varepsilon_1, ..., \varepsilon_n) \in \{0,1\}^n$, on note

$$I^n_{\varepsilon^n} = \left[\sum_{j=1}^{n} \frac{\varepsilon_j}{2^j}, \sum_{j=1}^{n} \frac{\varepsilon_j}{2^j} + \frac{1}{2^n}\right[.$$

On remarque que les $I^n_{\varepsilon^n}$ forment une partition de $[0,1[$ et que les D_j sont constants dessus.
On a

$$\bigcap_{j=1}^{n} \{D_j = \varepsilon_j\} = I^n_{\varepsilon^n},$$

donc

$$\mathbb{P}\left(\bigcap_{j=1}^{n} \{D_j = \varepsilon_j\}\right) = \frac{1}{2^n}.$$

Soit J une sous partie finie de $\{1, ..., n\}$, alors en sommant sur J^c, on a

$$\mathbb{P}\left(\bigcap_{j\in J} \{D_j = \varepsilon_j\}\right) = \frac{1}{2^{|J|}}.$$

Et en particulier, on a

$$\mathbb{P}(D_j = \varepsilon_j) = \frac{1}{2}.$$

D'où

$$\mathbb{P}\left(\bigcap_{j\in J}\{D_j = \varepsilon_j\}\right) = \prod_{j\in J}\mathbb{P}(D_j = \varepsilon_j).$$

Comme n et J sont arbitraires, cela prouve exactement que les D_j forment une suite de variables aléatoires indépendantes de loi $b(1/2)$.

- On commence par remarquer que

$$R_n = 2^n id - \sum_{j=1}^{n} 2^{n-j} D_j.$$

Soit f une fonction **positive mesurable** (pour la tribu borélienne), alors pour tout ε^n, on a

$$\begin{aligned}
E\left[f(R_n)\prod_{j=1}^{n}\mathbb{1}_{\{D_j=\varepsilon_j\}}\right] &= E\left[f(2^n id - \sum_{j=1}^{n}2^{n-j}\varepsilon_j)\prod_{j=1}^{n}\mathbb{1}_{\{D_j=\varepsilon_j\}}\right] \\
&= \int_{\mathbb{R}} \mathbb{1}_{I^n_{\varepsilon^n}}(x) f\left(2^n x - \sum_{j=1}^{n}2^{n-j}\varepsilon_j\right)\mathrm{d}\mathbb{P}(x) \\
&= \int_{\mathbb{R}} \mathbb{1}_{I^n_{\varepsilon^n}}\left(\frac{1}{2^n}y + \sum_{j=1}^{n}\frac{\varepsilon_j}{2^j}\right) f(y)\frac{1}{2^n}\mathrm{d}\mathbb{P}(y) \text{ (avec } y = 2^n x - \sum_{j=1}^{n}2^{n-j}\varepsilon_j) \\
&= \frac{1}{2^n}\int_{\mathbb{R}} \mathbb{1}_{[0,1[}(y) f(y)\mathrm{d}\mathbb{P}(y) \\
&= \mathbb{P}\left(\bigcap_{j=1}^{n}\{D_j = \varepsilon_j\}\right)\int_{\mathbb{R}} \mathbb{1}_{[0,1[}(y) f(y)\mathrm{d}\mathbb{P}(y)
\end{aligned}$$

En sommant sur les ε^n, on obtient

$$E[f(R_n)] = \int_{\mathbb{R}} \mathbb{1}_{[0,1[}(y) f(y)\mathrm{d}\mathbb{P}(y).$$

On en déduit donc que R_n suit une loi uniforme.
Puis on peut répéter la même opération qu'auparavant en sommant sur $j \in J^c$ et on obtient

$$E\left[f(R_n)\prod_{j\in J}\mathbb{1}_{\{D_j=\varepsilon_j\}}\right] = \prod_{j\in J}\mathbb{P}(D_j = \varepsilon_j)E[f(R_n)].$$

Cela nous donne l'indépendance de R_n avec D_1, ..., D_n. □

Attention, les R_n ne sont pas indépendantes ! Sinon $D_n = 2R_{n-1} - R_n$ admettrait une densité, ce qui est faux.

Lemme.

Soit Y une variable aléatoire de loi uniforme sur $[0,1[$, F une fonction de répartition et G la fonction - appelée pseudo-inverse de F - définie par

$$\forall t \in \mathbb{R}, G(t) = \inf\{x \in \mathbb{R}, F(x) \geqslant t\}.$$

Alors $G(Y)$ a pour fonction de répartition F.

Démonstration. On a l'équivalence

$$F(x) \geqslant t \Leftrightarrow x \geqslant G(t).$$

Donc comme Y suit une loi uniforme sur $[0,1[$, on a

$$\mathbb{P}(G(Y) \leqslant x) = \mathbb{P}(Y \leqslant F(x)) = F(x).$$

□

Corollaire.

Soit $(\mu_j)_j$ une suite de probabilités sur $(\mathbb{R}, \mathcal{B}(\mathbb{R}))$, alors il existe une suite $(X_j)_j$ de variables aléatoires **indépendantes** définies sur $([0,1[, \mathcal{B}([0,1[), \mathbb{P})$ et telle que X_j suive la loi μ_j.

Démonstration. On va créer une suite de variables aléatoires indépendantes $(Y_j)_j$ de lois uniformes sur $[0,1[$. Ainsi en utilisant le lemme, on aura terminé.

• On reprend les notations précédentes.
En utilisant la bijection $(\mathbb{N}^*)^2 \simeq \mathbb{N}^*$, [1]on peut partitionner $\mathbb{N}^*$ en union d'ensembles infinis

$$\mathbb{N}^* = \bigsqcup_{j \in \mathbb{N}^*} N_j,$$

et on note φ_j l'extractrice donnant les éléments de N_j dans l'ordre croissant.
On pose ensuite

$$Y_j = \sum_{k=1}^{\infty} \frac{1}{2^k} D_{\varphi_j(k)}.$$

• Par **le lemme des coalitions**, les Y_j sont indépendantes car ce sont des fonctions de différents D_k (et les D_k sont indépendantes).

• Montrons que Y_j suit une loi uniforme sur $[0,1[$.
On pose $Y_{j,n} = \sum_{k=1}^{n} \frac{1}{2^k} D_{\varphi_j(k)}$. Comme les D_k sont iid, $Y_{j,n}$ suit la même loi que

$$Z_n = \sum_{k=1}^{n} \frac{1}{2^k} D_k.$$

La suite Z_n tend presque surement vers Z la fonction identité.
De même, Y_j est la limite presque sure des $Y_{j,n}$. On a donc en particulier la convergence en loi, d'où

$$\mathbb{P}(Y_j \leqslant y) = \lim_n \mathbb{P}(Y_{j,n} \leqslant y) = \lim_n \mathbb{P}(Z_n \leqslant y) = \mathbb{P}(Z \leqslant y) = y.$$

Donc Y_j suit une loi uniforme sur $[0,1[$. □

Remarques : • Pour la leçon 249, on peut utiliser les Y_j pour avoir une suite de variables aléatoires iid de loi $b(p)$. Il suffit de poser $X_j = \mathbb{1}_{Y_j \leqslant p}$.
• La fonction de répartition d'une loi exponentielle est

$$F(x) = (1 - \exp(-\lambda x))\mathbb{1}_{[}0, \infty[.$$

Sa pseudo-inverse est alors

$$G(u) = -\lambda^{-1} \log(1-u).$$

De même, pour une loi de Cauchy, on a

$$G(u) = \tan(\pi(u - 1/2)).$$

• Pour les lois discrètes, il faut être plus malin. Si $\mu = \sum p_k \delta_{x_k}$, on se donne U une variable aléatoire uniforme sur $[0,1]$. On pose aussi la suite $(s_k)_k$ définie par $s_0 = p_0$ et $s_{k+1} = s_k + p_{k+1}$.
Alors la variable aléatoire X qui vaut x_k lorsque $U \in]s_{k-1}, s_k]$ suit la loi μ.
• Une utilité d'avoir une infinité de lois uniformes indépendantes est de pouvoir simuler une loi de Poisson de la manière suivante

$$N = \max\{n \in \mathbb{N}^*, U_1 ... U_n > \exp(-\lambda)\} \sim \mathcal{P}(\lambda).$$

1. On peut prendre l'application $(j,k) \mapsto k + \frac{(j+k-2)(j+k-1)}{2}$ par exemple.

Chapitre 27

Partitions d'un entier en parts fixées

Références : Francinou, Gianella, Nicolas, *Oraux X-ENS - Analyse 2*, p199

Théorème.

Soient a_1, ..., a_k des entiers naturels non nuls premiers entre eux. On note u_n le nombre de k-uplets $(x_i)_{i\in[1,k]}$ tels que $\sum a_i x_i = n$. Alors $u_n \underset{n\to\infty}{\sim} \dfrac{1}{a_1...a_k}\dfrac{n^{k-1}}{(k-1)!}$.

Démonstration. • On commence par étudier les séries $\sum_{x_i\in\mathbb{N}} z^{a_i x_i}$. Elles sont définies de rayon de convergence 1 (par le lemme d'Abel).

On peut faire le produit de Cauchy de ces séries pour obtenir la série $\sum_{n=0}^{\infty}\left(\sum_{\substack{(x_i)\in\mathbb{N}^k\\ \sum a_i x_i = n}} 1\right) z^n$ de rayon de convergence supérieur ou égal à 1.[1] On remarque que le terme général de cette série est u_n.

On pose donc la série génératrice $f(z) := \sum_{n=0}^{\infty} u_n z^n = \prod_{i=1}^{k}\left(\sum_{x_i\in\mathbb{N}} z^{a_i x_i}\right) = \prod_{i=1}^{k}\dfrac{1}{1-z^{a_i}}$.

• Étudions les pôles de f.
Les pôles sont les racines a_i-èmes de l'unité. Le pôle 1 est évidemment de multiplicité k.
Montrons que les autres pôles sont de multiplicité strictement inférieure à k.
Par le théorème de Bézout, il existe u_1, ..., u_k tels que $\sum u_i a_i = 1$.[2]

Si ω est une racine de l'unité de multiplicité k, alors $\omega^{a_i} = 1$ donc $\omega = \omega^{\sum u_i a_i} = \prod_{i=1}^{k}(\omega^{a_i})^{u_i} = 1$.

• Décomposons en éléments simples f :
On note $P = \{\omega_1, ..., \omega_p\}$ les pôles de f avec $\omega_1 = 1$.
Alors il existe $\alpha \in \mathbb{C}^*$ et $c_{i,j} \in \mathbb{C}$ tels que $f(z) = \dfrac{\alpha}{(1-z)^k} + \sum_{\substack{i\in[1,p]\\ j\in[1,k-1]}} \dfrac{c_{i,j}}{(\omega_i - z)^j}$.

• Pour $\omega \in P$, $\dfrac{1}{(\omega - z)^j}$ est développable en série entière pour $|z| < 1$.

On a déjà pour $|z| < 1$, $\dfrac{1}{\omega - z} = \dfrac{1}{\omega}\dfrac{1}{1-\frac{z}{\omega}} = \sum_{n=0}^{\infty}\dfrac{z^n}{\omega^{n+1}}$.

Donc en dérivant : $\dfrac{(j-1)!}{(\omega-z)^j} = \sum_{n=j-1}^{\infty}\dfrac{n!}{(n-j+1)!}\dfrac{z^{n-j+1}}{\omega^{n+1}}$.

1. Le rayon de convergence du produit de Cauchy est supérieur ou égal au minimum des rayons de convergence des séries entières étudiées.

2. $\sum a_i\mathbb{Z}$ est un idéal de $\mathbb{Z}$ qui est principal, donc il est engendré par un élément m. Or m divise a_i pour tout i et ils sont premiers entre eux donc $m = 1$.

Donc $\frac{1}{(\omega-z)^j} = \sum_{n=0}^{\infty} \binom{n+j-1}{n} \frac{z^n}{\omega^{n+j}}$.

- Conclusion :

On déduit en identifiant les coefficients que $u_n = \alpha \binom{n+k-1}{n} + \sum_{\substack{i\in[1,p]\\ j\in[1,k-1]}} \frac{c_{i,j}}{\omega_i^{n+j}} \binom{n+j-1}{n}$.

Or $\binom{n+j-1}{n} = \frac{1}{(j-1)!}(n+j-1)...(n+1) \sim \frac{n^{j-1}}{(j-1)!}$, donc $u_n = \alpha \binom{n+k-1}{n} + o(n^{k-1}) \sim \alpha \frac{n^{k-1}}{(k-1)!}$.

Puis on a $\lim_{\substack{z\to 1\\ z<1}} (1-z)^k f(z) = \alpha$.

Et $(1-z)^k f(z) = \prod_{i=1}^{k} \frac{1-z}{1-z^{a_i}} = \prod_{i=1}^{k} \frac{1}{1+z+...+z^{a_i-1}}$, donc $\alpha = \frac{1}{a_1...a_k}$.

On en déduit $u_n \sim \frac{1}{a_1...a_k} \frac{n^{k-1}}{(k-1)!}$. □

Remarques : • On adapte la preuve avec des séries formelles et des fractions rationnelles selon la leçon. J'ai préféré l'écrire avec les séries entières pour bien faire apparaître où intervient l'étude des convergences.

• En faisant cette preuve, on a aussi trouvé une méthode de calcul de u_n ! Il suffit de trouver la décomposition en éléments simples explicite de f, puis d'en déduire u_n avec la formule

$u_n = \alpha \binom{n+k-1}{n} + \sum_{\substack{i\in[1,p]\\ j\in[1,k-1]}} \frac{c_{i,j}}{\omega_i^{n+j}} \binom{n+j-1}{n}$.

Par exemple, si on veut décomposer 100 euros en pièces de 1 ou 2 euros, on écrit la décomposition en éléments simples de $\frac{1}{(1-x)(1-x^2)}$ et on trouve $u_n = \frac{n+1}{2} + \frac{1+(-1)^n}{4}$. En particulier, $u_{100} = 51$. C'est logique, on peut choisir entre 0 et 50 pièces de 2 euros, et on compense comme on veut avec les pièces de un euro.

Chapitre 28

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

Références : Francinou, Gianella, Nicolas, *Oraux X-ENS - Algèbre 3*, p130

On considère ici la norme subordonnée associée à la norme euclidienne sur E. On rappelle qu'un espace euclidien est un espace vectoriel muni d'un produit scalaire de dimension finie (notée n ici).

Théorème.

Soit E un espace euclidien et $B = \{u \in \mathcal{L}(E), |||u||| \leqslant 1\}$, alors les points extrémaux de B sont les éléments de $\mathrm{O}(E)$.

On rappelle qu'un point extrémal u de B est un point tel que $B \setminus \{u\}$ est convexe. Sur un dessin, on voit que les points extrémaux de la boule unité de $\mathbb{R}^2$ sont les points du cercle.

Démonstration. Soit $u \in \mathrm{O}(E)$, comme $|||\mathrm{O}(E)||| = \{1\}$, on a bien $u \in B$.
Supposons que $u = \frac{1}{2}(v+w)$ avec $v, w \in B$. Si on montre que cela implique $v = w$, on aura fini. En effet, si $B \setminus \{u\}$ n'était pas convexe, on pourrait trouver un segment $[v, w]$ contenant u et dont les bords sont dans $B \setminus \{u\}$. Quitte à découper notre segment, on peut se ramener au cas où u est au milieu du segment, c'est à dire $u = \frac{1}{2}(v+w)$. Donc si on prouve que $v = w = u$, on aura une absurdité.
Soit x de norme 1, alors $1 = \|x\| = \|u(x)\| \leqslant \frac{1}{2}(\|v(x)\| + \|w(x)\|) \leqslant \frac{1}{2}(|||v||| + |||w|||) \leqslant 1$.
On a donc égalité ! En particulier, pour tout x unitaire, $\|v(x) + w(x)\| = \|v(x)\| + \|w(x)\|$. Donc $v(x) = \lambda_x w(x)$ avec $\lambda_x > 0$ [1]. Or $\|v(x)\| = \|w(x)\| = 1$ donc $\lambda_x = 1$.
$v(x) = w(x)$ pour tout x unitaire donc par linéarité, $v = w$ et u est bien un point extrémal de B.

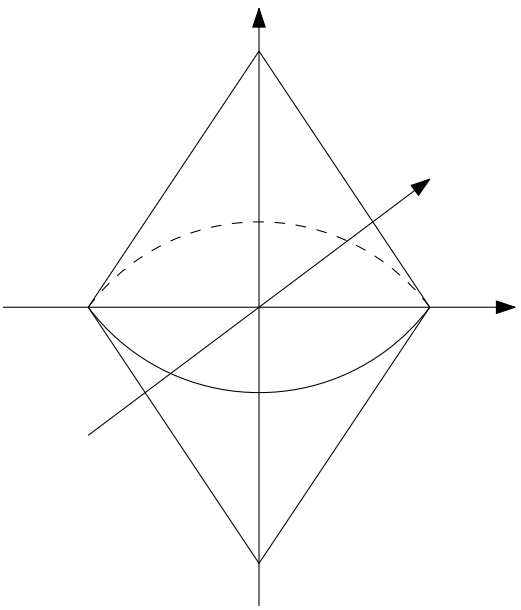
Réciproquement, soit $u \in B$ tel que $u \notin \mathrm{O}(E)$. Montrons que u n'est pas extrémal.
On note A la matrice de u dans une base orthonormée de E. En utilisant la décomposition polaire (sur $\mathcal{M}_n(\mathbb{R})$, on peut écrire $A = OS$ avec $O \in \mathrm{O}_n(\mathbb{R})$ et $S \in \mathcal{S}_n^+(\mathbb{R})$.
En utilisant le théorème de réduction des matrices symétriques, on a $S = PD^{\mathrm{t}}P$ avec $P \in \mathrm{O}_n(\mathbb{R})$ et $D = \mathrm{Diag}(d_1, ..., d_n)$ avec $0 \leqslant d_1 \leqslant ... \leqslant d_n$.
De plus, $|||A||| = |||OS||| = |||S||| = \sqrt{d_n^2} = d_n$ [2] et $u \in B$ donc $|||A||| \leqslant 1$. Donc $\forall i$, $d_i \in [0, 1]$.
Par hypothèse, A n'est pas orthogonale, donc $S \neq I_n$, donc $d_1 < 1$. On peut donc écrire $d_1 = \frac{a+b}{2}$ où $-1 \leqslant a < b \leqslant 1$ (on prend $a \geqslant -1$ et pas $a \geqslant 0$ pour le cas où $d_1 = 0$).
On pose alors $D_1 = \mathrm{Diag}(a, d_2, ..., d_n)$ et $D_2 = \mathrm{Diag}(b, d_2, ..., d_n)$.
On a $D_1 \neq D_2$ et $A = \frac{1}{2}(OPD_1{}^{\mathrm{t}}P + OPD_2{}^{\mathrm{t}}P)$.

1. En effet, on a $\|v(x) + w(x)\|^2 = \|v(x)\|^2 + \|w(x)\|^2 + 2\|v(x)\|\|w(x)\| = \|v(x)\|^2 + \|w(x)\|^2 + 2(v, w)$. Donc $(v, w) = \|v(x)\|\|w(x)\|$. L'égalité dans Cauchy-Schwarz donne que $v(x) = \lambda_x w(x)$.
Puis $\|w(x)\|^2 \lambda_x = (v, w) = \|v(x)\|\|w(x)\| \in \mathbb{R}^+$, donc λ_x est positif.

2. On rappelle que sur les matrices, la norme 2 donne $|||M||| = \sqrt{\rho({}^{\mathrm{t}}MM)}$ où ρ est le rayon spectral, c'est à dire la valeur propre maximale.

Ici on est plutôt content, on a écrit A comme le milieu d'un segment. Néanmoins, il faut encore montrer que les bornes de ce segment sont dans B.
Soit X de norme 1, alors $\left\|OPD_i{}^tPX\right\|^2 = {}^tXPD_i{}^tP{}^tOOPD_i{}^tPX = {}^t({}^tPX)D_i^2({}^tPX)$.
Or $\left\|{}^tPX\right\| = 1$ car P est orthogonale et X est unitaire.
En notant $Y = {}^tPX$, on a ${}^tYD_i^2Y = \sum_{j=2}^{n} d_j^2y_j^2 + d_i^0y_1^2$ avec $d_i^0 = a^2$ si $i = 1$ et b^2 si $i = 2$.
De plus, les coefficients de D_i^2 sont tous compris entre 0 et 1, donc ${}^tYD_i^2Y \leqslant \sum_{j=1}^{n} y_j^2 = 1$. On en déduit que $OPD_1{}^tPX$ et $OPD_2{}^tPX$ sont dans B.
Donc $A = \frac{1}{2}(OPD_1{}^tP + OPD_2{}^tP)$ est le milieu de deux éléments distincts de B. Donc A n'est pas un point extrémal ! □

Remarques : • Un théorème de Krein-Milman affirme qu'un convexe compact de $\mathbb{R}^n$ est toujours l'enveloppe convexe de l'ensemble de ses points extrémaux (voir FGN analyse 3). Donc ici, la boule unité de $\mathcal{L}(E)$ est l'enveloppe convexe de $\mathrm{O}(E)$.
En particulier, on en déduit que tout élément de $\mathcal{L}(E)$ est combinaison linéaire d'éléments de $\mathrm{O}(E)$. Il existe donc une base de $\mathcal{L}(E)$ constituée d'éléments de $\mathrm{O}(E)$. (Merci à Alexandre Bailleul pour cette idée.)
• On rappelle que $\mathrm{O}(E)$ n'est pas l'ensemble des éléments de norme 1.
• En dimension 1, le résultat est simple. En effet, $\mathcal{L}(E)$ s'identifie à $\mathbb{R}$ et B au segment $[-1, 1]$. D'autre part, $\mathrm{O}(E)$ n'est constitué que de $\pm I_1$ soit 1 et -1.
• En dimension 2, $\mathrm{O}(E)$ s'identifie à deux cercles disjoints : l'un représentant l'ensemble des angles des rotations de $\mathrm{SO}(E)$ et l'autre représentant l'ensemble des angles des axes de symétries de $\mathrm{O}(E) \setminus \mathrm{SO}(E)$. B s'identifie donc à un compact convexe de dimension 4 tel que ses points extrémaux soient deux cercles.
On peut préciser cette vision. En effet, si $A \in \mathrm{SO}_2$ alors $-A \in \mathrm{SO}_2$. Il en va de même pour l'autre composante connexe. Donc les cercles sont centrés autour de 0.
On peut ensuite projeter en dimension 3 pour obtenir que la boule unité est un double cône (deux cônes collés par leur base circulaire) dont la hauteur évolue de 0 à 1 (et de manière symétrique sur celui du bas). On peut faire de jolis dessins de ces doubles toupies évolutives pour "voir" la boule.



La double toupie

Chapitre 29

Polygones réguliers constructibles

Références : Mercier, *Cours de Géométrie*, p 428-429 et 433-436

Théorème.

Soit p un nombre premier impair, $\alpha \in \mathbb{N}^*$.
Alors le polygone régulier à p^α côtés est constructible si et seulement si $\alpha = 1$ et p est un nombre premier de Fermat (c'est à dire que p est un nombre premier qui s'écrit sous la forme $1 + 2^{2^\beta}$, où $\beta \in \mathbb{N}$).

Démonstration. On pose $q = p^\alpha$. On rappelle que le polygone régulier à q côtés $\mathcal{P}_q$ est constructible ssi $\omega = \exp\left(\frac{2i\pi}{q}\right)$ est constructible ssi $\cos\left(\frac{2\pi}{q}\right)$ est constructible.

$\Rightarrow$ On suppose que $\mathcal{P}_q$ est constructible.
Alors, par le théorème de Wantzel [1], on obtient : $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^m$, où $m \in \mathbb{N}^*$.
Aussi, le polynôme cyclotomique Φ_q étant le polynôme minimal de ω, on a :

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg \Phi_q = \varphi(q) = p^{\alpha-1}(p-1).$$

On obtient $2^m = p^{\alpha-1}(p-1)$.
Comme p est impair, il vient $\alpha = 1$, puis $p = 1 + 2^m$; montrons que m est une puissance de 2.
On écrit alors $m = \lambda 2^\beta$, avec $\beta \in \mathbb{N}$ et $\lambda \in \mathbb{N}^*$ impair ; on a alors $p = 1 + \left(2^{2^\beta}\right)^\lambda$.
Or, λ étant impair, on a $1 + X \big| 1 + X^\lambda$ dans $\mathbb{Z}[X]$ (car (-1) est racine). D'où $1 + 2^{2^\beta} \Big| p$ et donc, comme p est premier, on en déduit $\lambda = 1$.
p est bien un nombre premier de Fermat.

$\Leftarrow$ • On note $n = 2^\beta$, de sorte que $p = 1 + 2^n$, et $\omega = \exp\left(\frac{2i\pi}{p}\right)$.
On a : $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg \Phi_p = p - 1 = 2^n$.
On va vouloir trouver une suite d'extensions quadratiques menant à $\mathbb{Q}(\omega)$.
On note $G = \mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$; et si $g \in G$, alors g fixe $\mathbb{Q}$ et est entièrement déterminé par $g(\omega)$.
On a $\omega^p = 1$, donc $g(\omega)^p = 1$ et $g(\omega)$ est une racine de l'unité.
Les automorphismes de G sont donc de la forme $g_i(\omega) = \omega^i$ (avec $i \neq 0$) et on vérifie facilement que ce sont bien des automorphismes. On a donc

$$G = \left\{ g_i : \omega \mapsto \omega^i \middle| i \in [\![1, p-1]\!] \right\}.$$

On pose

$$\varphi : \begin{array}{ccc} G & \to & (\mathbb{Z}/p\mathbb{Z})^\times \\ g_i & \mapsto & i \end{array}.$$

1. Le théorème de Pierre-Laurent Wantzel, énoncé en 1837, donne une condition nécessaire et suffisante pour qu'un nombre soit constructible à la règle et au compas : il faut et il suffit que ce nombre appartienne à une extension de $\mathbb{Q}$ qui soit le terme d'une suite d'extensions quadratiques.
Pour le montrer, il suffit de voir que les points constructibles sont des intersections de cercles et droites, donc des racines de polynômes de degré 2. Les nombres constructibles sont donc dans des tours d'extensions quadratiques.

Alors
$$\varphi(g_i \circ g_j) = \varphi(g_{ij}) = ij = \varphi(g_i)\varphi(g_j),$$
donc φ est un isomorphisme de groupes. G est donc un **groupe cyclique** (C'est le résultat le plus important de cette preuve.).

• Désormais, g désignera un générateur de G.
Pour $i \in [\![0, n]\!]$, on note $K_i = \text{Ker}\left(g^{2^i} - id\right)$; c'est un sous-corps de $\mathbb{Q}(\omega)$.
De plus, $\forall i \in [\![0, n-1]\!], g^{2^{i+1}} = \left(g^{2^i}\right)^2$ implique $K_i \subseteq K_{i+1}$.

• Montrons que $K_0 = \mathbb{Q}$.
Les $(\omega^j)_{1 \leqslant j \leqslant p-1}$ forment une $\mathbb{Q}$-base de $\mathbb{Q}(\omega)$, donc $\left(g^i(\omega)\right)_{0 \leqslant i \leqslant p-2}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\omega)$.
Soit $a \in K_0$, $\exists a_0, \ldots, a_{p-2} \in \mathbb{Q}$,
$$a = a_0\omega + ... + a_{p-2}g^{p-2}(\omega),$$
mais
$$a = g(a) = a_{p-2}\omega + a_0 g(\omega) + ... + a_{p-1}g^{p-2}(\omega).$$
Il vient $a_0 = a_1 = ... = a_{p-2}$, donc
$$a = a_0(\omega + ... + g^{p-2}(\omega)) = -a_0 \in \mathbb{Q}.$$
Donc $K_0 = \mathbb{Q}$.

• Montrons que K_i est une extension quadratique de K_{i-1}.
Pour montrer que $\forall i \in [\![0, n-1]\!], K_i \neq K_{i-1}$, on considère l'élément $b = \sum_{k=0}^{2^{n-i}-1} g^{k2^i}(\omega)$.
On a :
$$g^{2^i}(b) = \sum_{k=0}^{2^{n-i}-1} g^{(k+1)2^i}(\omega) = \sum_{k=1}^{2^{n-i}-1} g^{k2^i}(\omega) + g^{2^n}(\omega) = \sum_{k=1}^{2^{n-i}-1} g^{k2^i}(\omega) + \omega = b.$$
Donc $b \in K_i$.
Puis
$$g^{2^{i-1}}(b) = \sum_{k=0}^{2^{n-i}-1} g^{k2^i+2^{i-1}}(\omega) \neq b$$
car on a décalé tous les indices de 2^{i-1} ; les coordonnées de b dans la famille des g^{k2^i} ne sont que des zéros.
On en déduit alors qu'on a la suite d'extensions :
$$\mathbb{Q} = K_0 \underset{\neq}{\subset} K_1 \underset{\neq}{\subset} \ldots \underset{\neq}{\subset} K_n = \mathbb{Q}(\omega).$$

Mais $2^n = [\mathbb{Q}(\omega) : \mathbb{Q}] = \prod_{i=0}^{n-1} \underbrace{[K_{i+1} : K_i]}_{\geqslant 2}$.
Ainsi, $\forall i \in [\![0, n-1]\!], [K_{i+1} : K_i] = 2$.

• Conclusion
Par le théorème de Wantzel, tous les éléments de $\mathbb{Q}(\omega)$ sont donc constructibles. [2]

□

Lemme.

→ Soit $n \geqslant 3$, alors $\mathcal{P}_n$ est constructible ssi $\mathcal{P}_{2n}$ est constructible.
→ Soit $n, m \geqslant 3$ sont premiers entre eux, alors $\mathcal{P}_{nm}$ est constructible ssi $\mathcal{P}_n$ et $\mathcal{P}_m$ le sont.

2. Pour revenir à $\cos\frac{2\pi}{p}$, il suffit d'écrire $\cos\frac{2\pi}{p} = \frac{\omega + \omega^{-1}}{2} \in \mathbb{Q}(\omega)$, donc $\cos\frac{2\pi}{p}$ est constructible. En fait, on a même $K_{n-1} = \mathbb{Q}\left(\cos\frac{2\pi}{p}\right)$.

Démonstration. • Si $\mathcal{P}_{2n}$ est construit, on prend un point sur deux et on obtient les sommets de $\mathcal{P}_n$.
Réciproquement, si on a $\mathcal{P}_n$, on trouve le centre du polygone en construisant les médiatrices des côtés, puis on cherche les intersections du cercle circonscrit avec les médiatrices de chaque côté. Cela donne les sommets de $\mathcal{P}_{2n}$.
• Si $\mathcal{P}_n$ et $\mathcal{P}_m$ sont construits, on trouve une relation de Bézout $un + vm = 1$, ce qui donne $\dfrac{2\pi}{mn} = u\dfrac{2\pi}{m} + v\dfrac{2\pi}{n}$.
Il suffit de reporter u fois le premier angle et v fois le deuxième pour obtenir l'angle voulu. (On reporte juste u fois le côté associé à l'angle $\dfrac{2\pi}{m}$ sur le cercle, puis v fois l'autre et on aura alors le côté associé à l'angle voulu, donc un des côtés de $\mathcal{P}_{nm}$.)
Réciproquement, si $\mathcal{P}_{nm}$ est construit, on ignore $m-1$ sommets consécutifs sur m pour obtenir $\mathcal{P}_n$ et vice versa pour $\mathcal{P}_m$. □

Théorème (Gauss-Wantzel)**.**

Les seuls polygones réguliers à n côtés constructibles sont ceux pour lesquelles n est de la forme $n = 2^m p_1 ... p_k$ avec $m \in \mathbb{N}$ et p_i des nombres **premiers** de Fermat **distincts**.

Remarques : • C'est beau !
• Les seuls nombres premiers de Fermat connus à ce jour sont 3, 5, 17, 257, 65537. Il a été montré qu'il était très probable que ce soit les seuls.
• Pour faire ce développement, il faut savoir reprouver que $\mathbb{Q}(\omega)$ est un $\mathbb{Q}$ espace vectoriel de dimension $p - 1 = \varphi(p)$. Il faut aussi savoir reprouver que $(\omega, ..., \omega^{p-1})$ en forme une base.
Il faut faire attention à prendre comme exemple non trivial le plus simple $\mathbb{Q}(j)$. Pour $\mathbb{Q}(i)$, ça ne marche pas car i est une racine quatrième de l'unité et 4 n'est pas premier !

Adapté du travail de Florian Lemonnier.

Chapitre 30

Polynômes irréductibles de $\mathbb{F}_q$

Références : Francinou, Gianella, *Exercices de mathématiques pour l'agrégation - Algèbre 1*, 5.10 et 3.11

Théorème.

Soit $n \in \mathbb{N}^*$, on note $A(n,q)$ l'ensemble des polynômes irréductibles unitaires de degré n de $\mathbb{F}_q[X]$ et $I(n,q)$ le cardinal de $A(n,q)$, alors

— $X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P$,

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

— On a l'équivalent $I(n,q) \sim \frac{q^n}{n}$,

— Il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_q$.

Démonstration. • Soit d un diviseur de n, $P \in A(d,q)$ et x une racine de P dans $\overline{F_q}$, alors $[\mathbb{F}_q(x) : \mathbb{F}_q] = d$ et donc $\mathbb{F}_q(x)$ est isomorphe à $\mathbb{F}_{q^d}$. En particulier, x est racine de $X^{q^d} - X$ car $\mathbb{F}_{q^d}$ est le corps de décomposition de ce polynôme. Or $X^{q^d} - X | X^{q^n} - X$ car $d|n$, donc x est racine de $X^{q^n} - X$. [1]
Les polynômes irréductibles étant à racines simples sur $\overline{F_q}$, on a $P | X^{q^n} - X$. [2]
Par décomposition en irréductibles, on a donc $\prod_{d|n} \prod_{P \in A(d,q)} P | X^{q^n} - X$.

• Soit P un diviseur irréductible unitaire de $X^{q^n} - X$, on note d son degré et on choisit x une de ses racines sur $\mathbb{F}_{q^n}$ (où P est scindé). Alors on a la tour d'extensions de corps $\mathbb{F}_q \subset \mathbb{F}_q(x) \subset \mathbb{F}_{q^n}$, donc par le théorème de

1. En effet, on sait que $X^{q^d} - X$ est à racines simples, et si x en est une racine, alors $x^{q^n} = x^{(q^d)^{\frac{n}{d}}} = x^{q^d (q^d)^{\frac{n}{d}-1}} = x^{(q^d)^{\frac{n}{d}-1}} = \ldots = x$
2. On utilise le résultat suivant :

Lemme.

Si K est un corps fini ou de caractéristique nulle, et si $P \in K[X]$ est un polynôme irréductible, alors P est à racines simples dans la clôture algébrique $\overline{K}$ de K.

Démonstration. Si P a une racine double α, alors $P = (X-\alpha)^2 Q$, donc $X - \alpha | P'$ et $X - \alpha | P \wedge P'$, donc comme P est irréductible et $P \wedge P' | P$, on a $P' = 0$.
Si K est de caractéristique nulle, cela implique $P = cste$, ce qui est absurde.
Si K est de caractéristique p, alors $P = R(X^p)$. Or si K est fini, le Frobenius est un automorphisme et $P = R_0(X)^p$ (en changeant les coefficients avec le Frobenius), ce qui est absurde.

□

En fait, on vient de prouver que les corps finis et les corps de caractéristique nulle sont parfaits, càd que toutes leurs extensions sont séparables. On peut trouver un théorème plus général dans le Calais à la page 44.

Il est bon de savoir que c'est faux en général si K est un corps infini de caractéristique p non nulle. Par exemple, $P(T) = T^p - X$ est irréductible sur le corps $\mathbb{F}_p(X)$ par un argument de degré. Mais si on prend une racine α dans une extension, alors $X = \alpha^p$ et $P(T) = T^p - \alpha^p = (T-\alpha)^p$.

la base télescopique : $[\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. Donc $d = [\mathbb{F}_q(x) : \mathbb{F}_q] | n$.
De plus, comme $X^{q^n} - X$ est à racines simples, chaque facteur irréductible, n'apparaît qu'une fois.
On en déduit donc que $\prod_{d|n} \prod_{P \in A(d,q)} P = X^{q^n} - X$ car notre décomposition contient bien tous les polynômes irréductibles (car il faut $d|n$ et chacun d'eux n'apparaît qu'une fois) et de plus les membres des deux côtés sont unitaires.

- En regardant les degrés dans l'égalité précédente, on voit que $q^n = \sum_{d|n} dI(d,q)$. On a besoin de la formule d'inversion de Möbius pour poursuivre. [3]

Lemme (Première formule d'inversion de Möbius)**.**

Soit $f : \mathbb{N}^* \to \mathbb{R}$ et $g : n \in \mathbb{N}^* \mapsto \sum_{d|n} f(d)$, alors

$$\forall n \geqslant 1, f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Démonstration. On passe d'une somme à l'autre en posant le changement de variable $d' = \frac{n}{d}$ dans la somme.
Prouvons donc $f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$.

→ Soit $k = p_1^{\alpha_1} ... p_r^{\alpha_r}$ avec $r > 0$, alors $\sum_{d|k} \mu(d) = \mu(1) + \sum_{i=1}^{r} \sum_{1 \leqslant \gamma_1 < ... < \gamma_i \leqslant r} \mu(p_{\gamma_1} ... p_{\gamma_r}) = 1 + \sum_{i=1}^{r} \sum_{1 \leqslant \gamma_1 < ... < \gamma_i \leqslant r} (-1)^i =$
$\sum_{i=0}^{r} (-1)^i \binom{r}{i} = (1-1)^r = 0.$

→ On a $\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{d' | \frac{n}{d}} f(d') = \sum_{dd'|n} \mu(d) f(d') = \sum_{d'|n} f(d') \sum_{d | \frac{n}{d'}} \mu(d)$. Or on a vu que si $\frac{n}{d'} \neq 1$, alors $\sum_{d | \frac{n}{d'}} \mu(d) = 0$, donc $\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = f(n) \sum_{d|1} \mu(d) = f(n)$. □

- Ceci étant fait, on a $I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$. Puis pour l'équivalent, on pose $r_n = \sum_{d|n, d \neq n} \mu\left(\frac{n}{d}\right) q^d$, alors
$|r_n| \leqslant \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} q^d = \frac{q^{\lfloor \frac{n}{2} \rfloor + 1} - q}{q-1}$.
En particulier, $|r_n| \leqslant \frac{q^{\lfloor \frac{n}{2} \rfloor + 1}}{q-1}$ donc $|r_n| = o(q^n)$. Ainsi, comme $I(n,q) = \frac{q^n + r_n}{n}$, on a l'équivalent voulu.

- On a vu que $\sum_{d|n, d \neq n} q^d < q^n$. Donc $I(n,q) > 0$.

Cela donne l'existence de polynômes irréductibles de tout degré. □

Corollaire.

Toute extension **de degré fini** sur $\mathbb{F}_q$ est une extension simple, normale et séparable.

Démonstration. • Une extension est simple si elle peut s'écrire sous la forme $\mathbb{F}_q(x)$.
Soit $\mathbb{K}$ une extension de degré fini de $\mathbb{F}_q$. Par unicité des corps finis, si n est le degré de $\mathbb{K}$, alors $\mathbb{K} = \mathbb{F}_{q^n}$. Comme il existe des polynômes irréductibles de tout degré, $\mathbb{F}_{q^n}$ est un corps de rupture d'un polynôme irréductible de degré n sur $\mathbb{F}_q$. Cela prouve le résultat.

3. On rappelle que la fonction de Möbius est définie par $\mu(n) = 0$ si n a un facteur irréductible carré, et $\mu(n) = (-1)^r$ si $n = p_1 ... p_r$ avec les p_i tous distincts et irréductibles.

• Une extension est normale si tout polynôme irréductible de $\mathbb{F}_q$ admettant une racine dans cette extension est scindé.
Soit P un tel polynôme et x une telle racine. Notons n le degré de P. Alors la formule du théorème montre que P est scindé sur $\mathbb{F}_{q^n}$. Or $\mathbb{F}_q(x)$ est un sous-corps de $\mathbb{F}_{q^n}$ de degré n. Donc $\mathbb{F}_q(x) = \mathbb{F}_{q^n}$ et l'extension est normale.

• Une extension $\mathbb{K}$ est séparable si le polynôme minimal sur $\mathbb{F}_q$ de tout élément α de $\mathbb{K}$ n'a que des racines simples dans un corps de décomposition.
On a vu que $\mathbb{F}_q$ est parfait. Donc toute extension de $\mathbb{F}_q$ est séparable. □

Chapitre 31

Quelques ordres moyens

Références : Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, p 40-41

Un ordre moyen d'une fonction arithmétique $f : \mathbb{N} \to \mathbb{R}$ (une suite numérique donc) toute fonction élémentaire de variable réelle g telle que

$$\sum_{1 \leqslant n \leqslant x} f(n) \sim \sum_{1 \leqslant n \leqslant x} g(n).$$

On va chercher quelques développements asymptotiques de ces sommes partielles et en déduire des ordres moyens.
On étudiera les fonctions

$$\sigma(n) = \sum_{d|n} d \text{ et } \varphi(n).$$

Dans toute la suite, quand cela s'avérera nécessaire, on notera $\mathcal{O}_u$ un $\mathcal{O}$ uniforme en x. Ainsi on pourra permuter sommations et $\mathcal{O}$.

Théorème.

Un ordre moyen de σ est $x \mapsto \dfrac{\pi^2}{12}x$ et on a

$$\sum_{n \leqslant x} \sigma(n) = \frac{\pi^2}{12}x^2 + \mathcal{O}(x \ln(x)).$$

Démonstration. On réécrit les sommations pour commencer.

$$\begin{aligned}
\sum_{n \leqslant x} \sigma(n) &= \sum_{n \leqslant x} \sum_{d|n} d \\
&= \sum_{dm \leqslant x} d \\
&= \sum_{m \leqslant x} \frac{1}{2} \left\lfloor \frac{x}{m} \right\rfloor \left(\left\lfloor \frac{x}{m} \right\rfloor + 1 \right) \\
&= \frac{1}{2} \sum_{m \leqslant x} \left(\frac{x}{m} \right)^2 + \sum_{m \leqslant x} \frac{x}{m} \mathcal{O}_u(1) + \sum_{m \leqslant x} \mathcal{O}_u(1) \\
&= \frac{x^2}{2} \sum_{m \leqslant x} \frac{1}{m^2} + \mathcal{O}(x) \sum_{m \leqslant x} \frac{1}{m} + \mathcal{O}(x)
\end{aligned}$$

Lemme.

On a

$$\sum_{m\leqslant x}\frac{1}{m^2}=\frac{\pi^2}{6}+\mathcal{O}\left(\frac{1}{x}\right)$$

et

$$\sum_{m\leqslant x}\frac{1}{m}=\ln(x)+\mathcal{O}(1).$$

Démonstration. Soit $m\geqslant 1$, alors

$$\int_m^{m+1}\frac{1}{t^2}\mathrm{d}t\leqslant\frac{1}{m^2}\leqslant\int_{m-1}^{m}\frac{1}{t^2}\mathrm{d}t.$$

Donc

$$\int_{\lfloor x\rfloor+1}^{\infty}\frac{1}{t^2}\mathrm{d}t=\frac{1}{\lfloor x\rfloor+1}\leqslant\sum_{m>x}\frac{1}{m^2}\leqslant\int_{\lfloor x\rfloor}^{\infty}\frac{1}{t^2}\mathrm{d}t=\frac{1}{\lfloor x\rfloor}.$$

Il vient

$$\sum_{m\leqslant x}\frac{1}{m^2}=\frac{\pi^2}{6}+\mathcal{O}\left(\frac{1}{\lfloor x\rfloor}\right)=\frac{\pi^2}{6}+\mathcal{O}\left(\frac{1}{x}\right).$$

Puis le développement de la série harmonique donne

$$\sum_{m\leqslant x}\frac{1}{m}=\ln(\lfloor x\rfloor)+\mathcal{O}(1)=\ln(\lfloor x\rfloor)+\mathcal{O}(1).$$

Or

$$\ln(\lfloor x\rfloor)=\ln(x+\mathcal{O}_u(1))=\ln(x)+\ln\left(1+\mathcal{O}_u\left(\frac{1}{x}\right)\right)=\ln(x)+\mathcal{O}_u\left(\frac{1}{x}\right)=\ln(x)+\mathcal{O}(1)$$

d'où le résultat. □

On a alors

$$\sum_{n\leqslant x}\sigma(n)=\frac{x^2}{2}\left(\frac{\pi^2}{6}+\mathcal{O}\left(\frac{1}{x}\right)\right)+\mathcal{O}(x\ln(x))=\frac{\pi^2}{12}x^2+\mathcal{O}(x\ln(x)).$$

□

Théorème.

Un ordre moyen de φ est $x\mapsto\frac{\pi^2}{3}x$ et on a

$$\sum_{n\leqslant x}\varphi(n)=\frac{3}{\pi^2}x^2+\mathcal{O}(x\ln(x)).$$

Démonstration. On utilise la formule d'inversion de Moëbius appliquée à $n=\sum_{d|n}\varphi(d)$, cela donne

$$\varphi(n)=\sum_{md=n}\mu(d)m.$$

Les mêmes calculs que précédemment donnent

$$\begin{aligned}\sum_{n\leqslant x}\varphi(n)&=\sum_{n\leqslant x}\sum_{md=n}\mu(d)m\\&=\sum_{d\leqslant x}\mu(d)\sum_{m\leqslant\frac{x}{d}}m\\&=\sum_{d\leqslant x}\frac{\mu(d)}{2}\left\lfloor\frac{x}{m}\right\rfloor\left(\left\lfloor\frac{x}{m}\right\rfloor+1\right)\\&=\frac{x^2}{2}\sum_{d\leqslant x}\frac{\mu(d)}{d^2}+\mathcal{O}(x\ln(x)).\end{aligned}$$

La question est : que vaut $\sum_{d\leqslant x}\frac{\mu(d)}{d^2}$?

La somme $\sum_{d\geqslant 1}\frac{\mu(d)}{d^2}$ converge absolument, ainsi que $\sum_{d\geqslant 1}\frac{1}{d^2}$, et on a

$$\left(\sum_{d\geqslant 1}\frac{\mu(d)}{d^2}\right)\left(\sum_{k\geqslant 1}\frac{1}{k^2}\right)=\sum_{n=1}^{\infty}\frac{1}{n^2}\sum_{d|n}\mu(d)=1,$$

cette dernière égalité venant de $\sum_{d|n}\mu(d)=\delta_{n,1}$.

On a donc

$$\sum_{d\leqslant x}\frac{\mu(d)}{d^2}=\sum_{d\geqslant 1}\frac{\mu(d)}{d^2}-\sum_{d>x}\frac{\mu(d)}{d^2}=\frac{6}{\pi^2}+\mathcal{O}(1)\sum_{d>x}\frac{1}{d^2}=\frac{6}{\pi^2}+\mathcal{O}\left(\frac{1}{x}\right).$$

D'où

$$\sum_{n\leqslant x}\varphi(n)=\frac{3}{\pi^2}x^2+\mathcal{O}(x)+\mathcal{O}(x\ln(x))=\frac{3}{\pi^2}x^2+\mathcal{O}(x\ln(x)).$$

□

Remarques : • On peut rajouter la preuve de l'inversion de Moebius comme ce développement est un peu court.
• Les ordres moyens sont souvent les renseignements les plus simples à déterminer sur une fonction arithmétique.
• On peut aussi trouver un ordre moyen de $\tau(n)=\sum_{d|n}1$: c'est $x\mapsto\ln(x)+2\gamma-1$. On a même

$$\sum_{n\leqslant x}\tau(n)=x(\ln(x)+2\gamma-1)+\mathcal{O}(\sqrt{x}).$$

C'est aussi dans le Tenenbaum, il faut démontrer le lemme de l'hyperbole mais cela ne pose pas de difficulté.

Sur une idée d'Alexandre Bailleul.

Chapitre 32

Réduction des endomorphismes normaux

Références : Gourdon, *Les maths en tête - Algèbre*, p260
`http://mp.cpgedupuydelome.fr/` (pour le lemme pratique)
Francinou, Gianella, Nicolas, *Oraux X-ENS - Algèbre 3*, p65 (pour l'exponentielle)

Théorème.

Soit E un espace euclidien et $u \in \mathcal{L}(E)$ un endomorphisme normal, alors il existe une base orthonormée $\mathcal{B}$ de E dans laquelle

$$\mathrm{mat}_{\mathcal{B}}(u) = \begin{pmatrix} \lambda_1 & & & & & & \\ & \ddots & & & & & \\ & & \lambda_r & & & & \\ & & & \tau_1 & & & \\ & & & & \ddots & & \\ & & & & & \tau_s & \end{pmatrix} \text{ avec } \lambda_i \in \mathbb{R} \text{ et } \tau_j = \begin{pmatrix} a_j & -b_j \\ b_j & a_j \end{pmatrix} \in \mathcal{M}_2(\mathbb{R}).$$

On commence par énoncer le lemme fondamental (amélioré) qui fait tout marcher !

Lemme.

- Soit $u \in \mathcal{L}(E)$ normal et F un sous-espace vectoriel de E stable par u, alors F est stable par u^* et $F^\perp$ est stable par u et u^*.
- Si u est normal, alors pour tout sous espace F stable par u, $u_{|F}$ est normal.

Démonstration. Je reprends une preuve assez intuitive trouvée à l'adresse suivante : `http://mp.cpgedupuydelome.fr/document.php?doc=Fiche%20-%20R%C3%A9duction%20des%20endomorphismes%20normaux.txt`.
On écrit la matrice de u dans une base orthonormée adaptée à la décomposition $E = F \oplus F^\perp$. Elle est de la forme $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$. Le fait que $F^\perp$ est stable par u^* est trivial : il suffit de regarder la transposée. Le but est donc de montrer que $B = 0$.
u est normal, donc ${}^tAA = A{}^tA + B{}^tB$. En passant à la trace, on trouve $\mathrm{Tr}({}^tBB) = 0$. Or $(M, N) \mapsto \mathrm{Tr}({}^tMN)$ est un produit scalaire, donc ici on a $\|B\| = 0$, donc $B = 0$.
On a ainsi $F^\perp$ est stable pour u, et donc stable pour u^*.

Pour le deuxième point, on reprend les calculs et on s'aperçoit que ${}^tAA = A{}^tA$, donc $u_{|F}$ est normal. □

Démonstration. On va faire une récurrence sur n la dimension de E.
Pour $n = 1$, le résultat est évident.
Soit $n \geqslant 2$, supposons le résultat vrai jusqu'au rang $n-1$ et montrons le au rang n.

Cas 1 : u admet une valeur propre réelle λ.
L'espace E_λ est de dimension supérieure ou égale à 1 et est stable par u. Donc $E_\lambda^\perp$ est stable par u donc $u_{|E_\lambda^\perp}$ est normal. Il existe donc par hypothèse de récurrence (comme $\dim(E_\lambda^\perp) < n$) une base orthonormée $\mathcal{B}_2$ dans laquelle la matrice de $u_{|E_\lambda^\perp}$ est jolie. On prend n'importe quelle base orthonormée $\mathcal{B}_1$ de E_λ et on a u de la forme voulue dans la base $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$.

Cas 2 : u n'a aucune valeur propre réelle.
Soit $Q = X^2 + \alpha X + \beta$ un diviseur irréductible de χ_u, on pose $N = \ker(Q(u))$.

• On a $N \neq \{0\}$. En effet, $Q = (X - \lambda)(X - \overline{\lambda})$. Donc comme λ est une valeur propre complexe de u, on a $\det(u - \lambda id) = 0$. D'où il vient $\det(Q(u)) = 0$. Donc $N \neq \{0\}$.

• Soit $x \in N$, on pose $F = \mathrm{Vect}_{\mathbb{R}}(x, u(x))$. Comme u n'a pas de valeurs propres réelles, $\dim(F) = 2$. De plus, F est stable par u car $u(x) \in F$ et $u(u(x)) = -\alpha u(x) - \beta x \in F$ car $x \in N = \mathrm{Ker}(Q(u))$.
On peut donc définir $u_{|F}$ et c'est un endomorphisme normal.

• On se donne une base orthonormale $\mathcal{B}_1$ de F. On note $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ la matrice de $u_{|F}$ dans cette base.

La condition $u_{|F}$ normal implique $a^2 + b^2 = a^2 + c^2$ et $ab + cd = ac + bd$. Donc $b = \pm c$.
Si $b = c$, le polynôme caractéristique est $\chi(X) = X^2 - (a+d)X + ad - b^2$ et son discriminant est $\Delta = (a-d)^2 + 4b^2$.
Δ est positif donc on a au moins une valeur propre réelle pour $u_{|F}$, donc pour u, ce qui est absurde.
Donc $b = -c$.
La deuxième égalité donne $(a - d)b = 0$. Si $b = 0$, la matrice est diagonale, donc on a une valeur propre réelle.
Donc $b \neq 0$ et $a = d$. La matrice de $u_{|F}$ est donc de la forme $\tau = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

• Conclusion :
On prend une base orthonormée $\mathcal{B}_2$ mettant $u_{|F^\perp}$ sous la forme voulue. Puis en concaténant $\mathcal{B}_1$ et $\mathcal{B}_2$, on obtient une base orthonormée dans laquelle la matrice de u est sous la forme demandée.
Ainsi la récurrence est prouvée. □

Remarque : • On peut appliquer ce théorème pour prouver les théorèmes de réduction des matrices orthogonales, antisymétriques et symétriques (théorème spectral). On en applique deux d'un coup juste après !

Et maintenant, une petite application sympa dont on fait la démonstration rapidement si on a le temps.

Corollaire.

La fonction exponentielle $\exp : \mathcal{A}_n(\mathbb{R}) \mapsto \mathrm{SO}_n(\mathbb{R})$ est surjective.

Démonstration. • Pour montrer qu'elle est définie, prenons $A \in \mathcal{A}_n(\mathbb{R})$, on a ${}^t\exp(A) = \exp({}^tA) = \exp(-A) = \exp(A)^{-1}$, donc $\exp(A) \in \mathrm{O}_n(\mathbb{R})$.
Puis $\det(\exp(A)) = \exp(\mathrm{Tr}(A)) = \exp(0) = 1$ donc $\exp(A) \in \mathrm{SO}_n(\mathbb{R})$.

• Soit $M = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & R_{\theta_1} & & \\ & & & & \ddots & \\ & & & & & R_{\theta_s} \end{pmatrix} \in \mathrm{SO}_n(\mathbb{R})$ avec $R_{\theta_i} = \begin{pmatrix} \cos(\theta_i) & -\sin(\theta_i) \\ \sin(\theta_i) & \cos(\theta_i) \end{pmatrix}$ (quitte à mettre des blocs R_π pour le nombre pair de -1.

Alors on a $M = \exp(B)$ avec $B = \begin{pmatrix} 0 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ & & & \theta_1 J & & \\ & & & & \ddots & \\ & & & & & \theta_s J \end{pmatrix} \in \mathcal{A}_n(\mathbb{R})$ avec $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Il suffit maintenant d'observer la compatibilité de l'exponentielle avec le changement de base pour conclure. □

Remarque : on voit alors que $\mathcal{A}_n(\mathbb{R})$ est l'algèbre de Lie associé au groupe de Lie $\mathrm{SO}_n(\mathbb{R})$.

Chapitre 33

Simplicité de $\mathrm{SO}_3(\mathbb{R})$

Références : Caldero, Germoni, *Histoires hédonistes de groupes et de géométrie*, p237

On va commencer par prouver quelques propriétés sur $\mathrm{SO}_n(\mathbb{R})$ que l'on utilisera dans la suite pour prouver la simplicité de $\mathrm{SO}_3(\mathbb{R})$. On conclura sur l'éventuelle simplicité des autres groupes spéciaux orthogonaux.

Théorème.

$\mathrm{SO}_n(\mathbb{R})$ est compact et connexe (par arcs).

Démonstration. 1) On définit l'application ϕ qui à $M \in \mathcal{M}_n(\mathbb{R})$ associe ${}^tMM$. Elle est continue car chacune des composantes est un polynôme en les coefficients de la matrice en entrée. Donc $\mathrm{SO}_n(\mathbb{R}) = \phi^{-1}\{I_n\} \cap \overset{-1}{\det}\{1\}$ est fermé.
D'autre part, on prend la norme liée au produit scalaire $(A, B) = \mathrm{Tr}({}^tAB)$ sur l'espace des matrices et on remarque que $\|M\| = \sqrt{\mathrm{Tr}({}^tMM)} = \sqrt{n}$ pour $M \in \mathrm{SO}_n(\mathbb{R})$. Donc $\mathrm{SO}_n(\mathbb{R})$ est borné (pour toute norme car elles sont équivalentes).
Comme on est en dimension finie, $\mathrm{SO}_n(\mathbb{R})$ est compact.

2) Continuons avec la connexité. Soit $M \in \mathrm{SO}_n(\mathbb{R})$, on va créer un chemin continu liant M à I_n. Ainsi on pourra relier deux matrices par un chemin continu en passant par l'identité.
Le théorème de réduction donne l'existence d'une matrice $P \in \mathrm{O}_n(\mathbb{R})$ telle que

$$M = P \begin{pmatrix} I_r & & & & \\ & -I_{2p} & & & \\ & & R_{\theta_1} & & \\ & & & \ddots & \\ & & & & R_{\theta_s} \end{pmatrix} {}^tP \text{ avec } R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

On pose alors pour $t \in [0,1]$, $N(t) = \begin{pmatrix} I_r & & & & & & \\ & R_{t\pi} & & & & & \\ & & \ddots & & & & \\ & & & R_{t\pi} & & & \\ & & & & R_{t\theta_1} & & \\ & & & & & \ddots & \\ & & & & & & R_{t\theta_s} \end{pmatrix}$.
Ainsi $\gamma(t) := PN(t){}^tP$ est une application continue de $[0,1]$ dans $\mathrm{SO}_n(\mathbb{R})$ qui relie M à I_n. □

On peut maintenant prouver le théorème suivant.

Théorème.

$\mathrm{SO}_3(\mathbb{R})$ est un groupe simple.

Démonstration. Soit $H \lhd \mathrm{SO}_3(\mathbb{R})$ non trivial, il nous faut montrer que $H = \mathrm{SO}_3(\mathbb{R})$. On admet que les retournements engendrent $\mathrm{SO}_3(\mathbb{R})$. Ceux-ci sont conjugués dans $\mathrm{SO}_3(\mathbb{R})$ (donc l'ensemble des retournements est stable par automorphisme intérieur). On en déduit que si H contient un retournement, comme il est distingué, il les contient tous et donc $H = \mathrm{SO}_3(\mathbb{R})$.

• Pourquoi les retournements sont-ils conjugués ?
Soient r_D et $r_{D'}$ deux retournements de droites respectives D et D'. On choisit d et d' deux vecteurs unitaires engendrant chacun leur droite associée. On peut ensuite trouver une base orthonormée de $D^\perp$: (e_1, e_2) (et de même on peut trouver (e'_1, e'_2) base de $D'^\perp$). Finalement on obtient deux bases orthonormées (d, e_1, e_2) et (d', e'_1, e'_2). La matrice de passage de l'une à l'autre est donc orthogonale. Quitte à poser $d'' = -d'$, on a une matrice de passage de déterminant 1, donc dans $\mathrm{SO}_3(\mathbb{R})$.

• Pourquoi les retournement engendrent-ils $\mathrm{SO}_3(\mathbb{R})$?
C'est une conséquence du théorème de Cartan-Dieudonné [1]. Ce théorème affirme que le groupe $\mathcal{O}_n(\mathbb{R})$ est engendré par les réflexions. Un élément $u \in \mathrm{SO}_3(\mathbb{R})$ est donc le produits d'un nombre pair de réflexions (pair car son déterminant est 1). On peut toutes les multiplier par (-1). Or si τ est une réflexion, alors $-\tau$ est un retournement (il suffit de diagonaliser les matrice pour s'en rendre compte). Donc u est un produit de retournements.

• Pourquoi H contient-il un retournement ?
Soit $h \in H$ non trivial, on pose $\phi : \begin{array}{ccc} \mathrm{SO}_3(\mathbb{R}) & \to & \mathbb{R} \\ g & \mapsto & \mathrm{Tr}(ghg^{-1}h^{-1}) \end{array}$.
— $\phi(I_3) = 3$ donc $3 \in \mathrm{Im}(\phi)$,
— $\mathrm{SO}_3(\mathbb{R})$ est connexe donc $\phi(\mathrm{SO}_3(\mathbb{R}))$ est un intervalle contenant 3,
— $\mathrm{SO}_3(\mathbb{R})$ est compact donc $\phi(\mathrm{SO}_3(\mathbb{R})) = [a, b]$ avec $a \leqslant 3 \leqslant b$,
— la trace d'un élément de $\mathrm{SO}_3(\mathbb{R})$ est de la forme $1 + 2\cos(\theta)$, donc $\phi(\mathrm{SO}_3(\mathbb{R})) = [a, 3]$ avec $a \in [-1, 3]$.

Supposons que $a = 3$, alors $\forall g \in \mathrm{SO}_3(\mathbb{R})$, $ghg^{-1}h^{-1} = I_3$ (le théorème de réduction donne qu'il y a une unique matrice de $\mathrm{SO}_3(\mathbb{R})$ de trace 3). Donc $h \in Z(\mathrm{SO}_3(\mathbb{R})) = I_3$ [2]. C'est absurde !

Donc $a < 3$, donc il existe $n \in \mathbb{N}^*$ tel que $a < 1 + 2\cos\left(\frac{\pi}{n}\right) < 3$ (car $3 = \lim\limits_{n\to\infty} 1 + 2\cos\left(\frac{\pi}{n}\right)$). On note g_n tel que $\phi(g_n) = 1 + 2\cos\left(\frac{\pi}{n}\right)$. Alors $h_n := g_n h g_n^{-1} h^{-1} \in H$ (car $h^{-1} \in H$ et $g_n h g_n^{-1} \in H$ car H est distingué) et est une rotation d'angle $\pm\frac{\pi}{n}$.
Donc h_n^n est dans H et est une rotation d'angle π, donc un retournement. □

Remarque : qu'en est-il des autres groupes spéciaux orthogonaux ?
Si n est pair, $< \pm I_n > \lhd \mathrm{SO}_n(\mathbb{R})$ donc $\mathrm{SO}_n(\mathbb{R})$ n'est pas simple. On pose ainsi naturellement les groupes $\mathrm{PSO}_n(\mathbb{R}) = \begin{cases} \mathrm{SO}_n(\mathbb{R})/ < \pm I_n > & \text{si } n \text{ est pair} \\ \mathrm{SO}_n(\mathbb{R}) & \text{si } n \text{ est impair} \end{cases}$.
On peut alors montrer que $\mathrm{PSO}_n(\mathbb{R})$ est simple pour $n = 3$ et $n \geqslant 5$. C'est faux pour $n = 4$ car $\mathrm{PSO}_4(\mathbb{R}) \simeq \mathrm{SO}_3(\mathbb{R}) \times \mathrm{SO}_3(\mathbb{R})$ (en le faisant agir sur les quaternions, fait dans H2G2). Pour $n = 2$, $\mathrm{SO}_2(\mathbb{R})$ est abélien donc $\mathrm{PSO}_2(\mathbb{R})$ aussi ; en particulier, il n'est pas simple.
• Pour prouver les cas de simplicité de $\mathrm{PSO}_n(\mathbb{R})$, on utilise le même type de démonstration que celle vue ici. On se ramène même à la simplicité de $\mathrm{SO}_3(\mathbb{R})$. Pas mal comme application tout de même, non ?

1. À ce sujet on pourra lire `http://florian.bouguet.free.fr/doc/developpements/cartan_dieudonne.pdf`.
2. En effet, soit $u \in Z(\mathrm{SO}_3(\mathbb{R}))$, alors pour toute droite D de l'espace, si on note r_D le retournement de droite D, on a $r_D = u r_D u^{-1} = r_{u(D)}$. On en déduit $D = u(D)$ pour toute droite D de l'espace. C'est un exo de sup classique de montrer qu'alors, u est une homothétie. Il n'y a qu'une homothétie dans $\mathrm{SO}_3(\mathbb{R})$, c'est l'identité.

Chapitre 34

Solution élémentaire de l'équation de Schrödinger

Références : Bony, *Cours d'analyse - Théorie des distributions et analyse de Fourier*, p 187-189 + p 150
Zuily, *Éléments de distributions et d'équations aux dérivées partielles*, p 115 + p 108-109

Théorème.

L'équation de Schrödinger possède une solution élémentaire tempérée à support dans $\{t \geqslant 0\}$. Il s'agit de la distribution E donnée par :

$$\forall \varphi \in \mathcal{S}(\mathbb{R} \times \mathbb{R}^n), \quad \langle E, \varphi \rangle = e^{-in\pi/4} \int_0^\infty \frac{1}{(4\pi t)^{n/2}} \left(\int_{\mathbb{R}^n} e^{i\|x\|^2/4t} \varphi(t,x) \mathrm{d}x \right) \mathrm{d}t.$$

Démonstration. • Analyse
Supposons que E soit solution de

$$\partial_t E - i\Delta_x E = \delta_0.$$

On applique la transformée de Fourier partielle à cette équation pour obtenir

$$\partial_t \widetilde{E} + i\|x\|^2 \widetilde{E} = \widetilde{\delta_0}.$$

Explicitons $\widetilde{\delta_0}$:

$$\langle \widetilde{\delta_0}, \varphi \rangle = \langle \delta_0, \widetilde{\varphi} \rangle = \widetilde{\varphi}(0,0) = \int_{\mathbb{R}^n} \varphi(0,x) \mathrm{d}x.$$

On est tenté de poser comme solution

$$E = \widetilde{\mathcal{F}}^{-1} \left(H(t) e^{-it\|\xi\|^2} \right).$$

Ainsi le H permettra d'obtenir le dirac en dérivant avec la formule des sauts et l'exponentielle vérifiera l'équation.

• Synthèse
Posons E comme précédemment. On a alors pour $\varphi \in \mathcal{S}(\mathbb{R} \times \mathbb{R}^n)$,

$$\begin{aligned}
\langle \partial_t E - i\Delta_x E, \widetilde{\varphi} \rangle &= \langle \partial_t \widetilde{E} + i\|x\|^2 \widetilde{E}, \varphi \rangle \\
&= \langle \widetilde{E}, -\partial_t \varphi + i\|x\|^2 \varphi \rangle \\
&= \int_{\mathbb{R}^n} \int_0^\infty e^{-it\|x\|^2} \left(-\partial_t \varphi(t,x) + i\|x\|^2 \varphi(t,x) \right) \mathrm{d}t\mathrm{d}x \\
&= \int_{\mathbb{R}^n} \left[-e^{-it\|x\|^2} \varphi(t,x) \right]_0^\infty \mathrm{d}x \\
&= \int_{\mathbb{R}^n} \varphi(0,x) \mathrm{d}x \\
&= \langle \delta_0, \widetilde{\varphi} \rangle.
\end{aligned}$$

On a donc bien, comme la transformée de Fourier partielle est une bijection sur $\mathcal{S}$ [1],

$$\partial_t E - i\Delta_x E = \delta_0.$$

• Explicitons la distribution E.
On a posé

$$\widetilde{E} = H(t)e^{-it\|\xi\|^2}.$$

Donc en appliquant la transformée de Fourier, on a

$$\check{E} = \frac{1}{(2\pi)^n} H(t)\widetilde{\mathcal{F}}\left(e^{-it\|\xi\|^2}\right).$$

On a à présent besoin d'un lemme.

Lemme.

On a pour $t \in \mathbb{R}^{+*}$,

$$\mathcal{F}\left(e^{-it\|\xi\|^2}\right) = \left(\frac{\sqrt{\pi}}{\sqrt{t}} e^{-i\frac{\pi}{4}}\right)^n e^{i\frac{\|x\|^2}{4t}}.$$

Si on a ce lemme, alors

$$\check{E} = \frac{1}{(2\pi)^n} H(t) \left(\frac{\sqrt{\pi}}{\sqrt{t}} e^{-i\frac{\pi}{4}}\right)^n e^{i\frac{\|x\|^2}{4t}}.$$

Or pour $\varphi \in \mathcal{S}(\mathbb{R}\times\mathbb{R}^n)$, on a

$$\begin{aligned}
\langle E, \varphi\rangle &= \langle \check{E}, \check{\varphi}\rangle \\
&= e^{-in\pi/4} \int_0^\infty \frac{1}{(4\pi t)^{n/2}} \left(\int_{\mathbb{R}^n} e^{i\|x\|^2/4t}\varphi(t,-x)\mathrm{d}x\right)\mathrm{d}t \\
&= e^{-in\pi/4} \int_0^\infty \frac{1}{(4\pi t)^{n/2}} \left(\int_{\mathbb{R}^n} e^{i\|x\|^2/4t}\varphi(t,x)\mathrm{d}x\right)\mathrm{d}t
\end{aligned}$$

On en déduit donc le résultat :

$$E = \check{E} = \frac{H(t)}{(4\pi t)^{n/2}} e^{-i\frac{n\pi}{4}} e^{i\frac{\|x\|^2}{4t}}.$$

□

Passons à présent à la preuve du lemme.

Démonstration. On commence par fixer t.
La transformée de Fourier de $T = e^{-it\|\xi\|^2}$ est bien définie car c'est une fonction de L^∞, donc de $\mathcal{S}'$.
Néanmoins, comme elle n'est pas dans $\mathcal{S}$, on ne peut pas calculer simplement sa transformée de Fourier.

On se place à présent dans $\mathcal{S}(\mathbb{R}^n)$ et $\mathcal{S}'(\mathbb{R}^n)$.
On pose $T_\varepsilon = e^{-\varepsilon\|\xi\|^2}e^{-it\|\xi\|^2} \in \mathcal{S}'(\mathbb{R}^n)$.
Soit $\varphi \in \mathcal{S}(\mathbb{R}^n)$, alors par convergence dominée, on a

$$\langle T_\varepsilon, \varphi\rangle = \int e^{-\varepsilon\|\xi\|^2}e^{-it\|\xi\|^2}\varphi(\xi)\mathrm{d}\xi \underset{\varepsilon\to 0}{\to} \int e^{-it\|\xi\|^2}\varphi(\xi)\mathrm{d}\xi = \langle T, \varphi\rangle.$$

Donc $T_\varepsilon \to T$ dans $\mathcal{S}'$. Comme la transformée de Fourier est continue, il vient $\mathcal{F}T_\varepsilon \to \mathcal{F}T$ dans $\mathcal{S}'$.
Mais $T_\varepsilon \in \mathcal{S}$ et la transformée de Fourier sur $\mathcal{S}'$ n'est qu'un prolongement de celle sur $\mathcal{S}$. On en déduit

$$\begin{aligned}
\mathcal{F}T_\varepsilon &= \int_{\mathbb{R}^n} e^{-\varepsilon\|\xi\|^2}e^{-it\|\xi\|^2}e^{-i(x,\xi)}\mathrm{d}\xi \\
&= \prod_{j=1}^n \int_{\mathbb{R}} e^{-(\varepsilon+it)y^2}e^{-ix_j y}\mathrm{d}y
\end{aligned}$$

1. On n'oublie surtout pas de le mettre dans le plan ! Ce n'est pas une chose évidente !

On sait que si $z \in \mathbb{R}^{+*}$, alors

$$\int_{\mathbb{R}} e^{-zy^2} e^{-ix_j y} \mathrm{d}y = \frac{\sqrt{\pi}}{\sqrt{z}} e^{-\frac{x_j^2}{4z}}.$$

En utilisant le théorème d'holomorphie sous le signe intégrale, on montre que $z \mapsto \int_{\mathbb{R}} e^{-zy^2} e^{-ix_j y} \mathrm{d}y$ se prolonge de manière holomorphe sur $\Re(z) > 0$. De même, $z \mapsto \frac{\sqrt{\pi}}{\sqrt{z}} e^{-\frac{x_j^2}{4z}}$ se prolonge de manière holomorphe sur $\Re(z) > 0$ en utilisant une bonne détermination du logarithme.
Par principe de prolongement analytique, comme elles coïncident sur l'axe réel, on a

$$\int_{\mathbb{R}} e^{-(\varepsilon+it)y^2} e^{-ix_j y} \mathrm{d}y = \frac{\sqrt{\pi}}{\sqrt{\varepsilon+it}} e^{-\frac{x_j^2}{4(\varepsilon+it)}}.$$

Et enfin, il vient

$$\mathcal{F}T_\varepsilon = \left(\frac{\sqrt{\pi}}{\sqrt{\varepsilon+it}}\right)^n e^{-\frac{\|x\|^2}{4(\varepsilon+it)}}$$

D'une part, $\sqrt{\varepsilon+it} \to e^{i\frac{\pi}{4}}\sqrt{t}$. D'autre part, $e^{-\frac{\|x\|^2}{4(\varepsilon+it)}} \to e^{i\frac{\|x\|^2}{4t}}$ dans $\mathcal{S}'$ par convergence dominée (il suffit de l'écrire).

On a donc bien le résultat attendu

$$\mathcal{F}T = \left(\frac{\sqrt{\pi}}{\sqrt{t}} e^{-i\frac{\pi}{4}}\right)^n e^{i\frac{\|x\|^2}{4t}}.$$

□

Théorème.

Si $A \in \mathcal{E}'(\mathbb{R}^n)$ est telle qu'il existe une solution élémentaire $E \in \mathcal{D}'(\mathbb{R}^n)$, c'est à dire telle que $A * E = \delta$, alors pour tout $f \in \mathcal{E}'(\mathbb{R}^n)$, il existe au moins une solution à $A * u = f$.
De plus, il existe au plus une solution $u \in \mathcal{E}'(\mathbb{R}^n)$ et si elle existe, c'est $E * f$.

Démonstration. Comme les supports de A et f sont compacts, le produit de convolution suivant est défini et on peut utiliser l'associativité :

$$A * (E * f) = (A * E) * f = \delta * f = f.$$

On a donc une solution définie par $u = E * f$.
De plus, si on a une solution u à support compact, alors comme les supports de u et A sont compacts, on peut écrire

$$u = \delta * u = (A * E) * u = (E * A) * u = E * (A * u) = E * f.$$

Cela donne l'unicité. □

Comme $(\partial_t - i\Delta_x)\delta$ est une distribution à support compact, et comme $(\partial_t - i\Delta_x)\delta * u = \partial_t u - i\Delta_x u$ pour $u \in \mathcal{D}'(\mathbb{R}^n)$ [2], on peut appliquer notre théorème à l'équation de Schrödinger. On a ainsi pour tout $f \in \mathcal{E}'(\mathbb{R}^n)$ au moins une solution sur $\mathbb{R}^n$ à

$$\partial_t u - i\Delta_x u = f.$$

De plus, l'unique solution à support compact - si elle existe - est $E * f$.

Remarques : • Attention ! E n'est quasiment jamais à support compact ! Ce n'est pas parce que $u = E * f$ est compact que nécessairement E acquière aussi cette propriété.
• Il n'existe pas toujours de solution à support compact de $A * u = f$, par exemple si $f = \delta$, alors nécessairement, s'il existe une solution dans $\mathcal{E}'$, c'est E. Et on peut prouver que toute EDP à coefficients constants non tous nuls possède une infinité de solutions élémentaires et qu'elles ne sont **jamais** à support compact dès que l'ordre de l'équation vaut au moins 1.
• Et le lien avec la physique, où est-il ?
L'équation physique de Schrödinger est

$$H\psi = i\hbar\partial_t\psi.$$

2. Bony, p 144-145

ψ est la fonction d'onde d'une particule libre. Sa norme au carré est la densité de probabilité de la position de la particule.

H est l'hamiltonien du système. Il vérifie $H = \dfrac{\widehat{p}^2}{2m} + V$ avec $\widehat{p}$ la quantité de mouvement vectorielle et V le potentiel.

On peut démontrer que $\widehat{p} = -i\hbar\nabla_x$. Ainsi, à potentiel nul, on a une équation similaire à celle étudiée :

$$\partial_t\psi - i\hbar\Delta_x\psi = 0.$$

Pour des détails supplémentaires, le lecteur peut (ou pas) regarder le Claude Cohen-Tannoudji et le Basdevant, Dalibard, Joffre.

• Il n'est pas si clair que à t fixé,

$$\mathcal{F}\left(e^{-it\|\xi\|^2}\right) = \widetilde{\mathcal{F}}\left(e^{-it\|\xi\|^2}\right).$$

Pour une fonction de $\mathcal{S}$, c'est évident. Il suffit donc de passer la transformée de Fourier de l'autre côté du crochet et cela donne le résultat. (Merci à Léo Vivion pour cette remarque.)

• On peut appliquer le même raisonnement (mais c'est plus simple) pour trouver une solution élémentaire de l'équation de la chaleur. C'est la distribution

$$E(t,x) = H(t)(4\pi t)^{-n/2}e^{-\|x\|^2/4t}.$$

Chapitre 35

Sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$

Références : Ulmer, *Théorie des groupes*, p 138

Théorème.

Si G est un sous-groupe fini non trivial du groupe $\mathrm{SO}_3(\mathbb{R})$ des rotations de $\mathbb{R}^3$, alors G est isomorphe à l'un des groupes $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{D}_m$, $\mathcal{A}_4$, $\mathcal{S}_4$ ou $\mathcal{A}_5$ (avec $m \geqslant 2$).

Démonstration. • Les éléments de G sont des rotations, donc tout élément de $G \setminus \{id\}$ a une droite de points fixes : l'axe de la rotation. On appelle pôles ses deux intersections avec $\mathbb{S}^2$. On note X l'ensemble des pôles et on montre facilement que G induit une action sur X.
En effet, si $x \in X$ est un pôle de $g \neq id$, alors pour $h \in G$, $h(x)$ est un pôle pour hgh^{-1}, donc on a stabilité. Les autres axiomes sont trivialement vérifiés.
On a $2 \leqslant |X| \leqslant 2(n-1)$ en notant $n = |G|$ car G est non trivial et chaque $g \in G \setminus \{id\}$ a exactement deux pôles.
On note r le nombre d'orbites, alors la formule de Burnside donne

$$r = \frac{1}{|G|}\left(|X^{id}| + \sum_{g \neq id} |X^g|\right) = \frac{1}{n}\left(|X| + \sum_{i=1}^{n-1} 2\right) = \frac{1}{n}(|X| + 2(n-1)).$$

L'encadrement précédent donne $2 \leqslant r \leqslant 4\left(1 - \frac{1}{n}\right) < 4$. D'où $r \in \{2, 3\}$.

• Supposons $r = 2$, il y a deux orbites X_1 et X_2. La formule des classes donne $2 = \frac{1}{n}(|X_1| + |X_2| + 2(n-1))$ donc $|X_1| + |X_2| = 2$ et donc $|X_1| = |X_2| = 1$. Toutes les rotations de G ont donc le même axe de rotation, celui passant par les deux pôles ainsi trouvés. On en déduit que G peut se voir comme un sous-groupe fini de rotations de $\mathrm{SO}_2(\mathbb{R})$. C'est donc un groupe cyclique [1] et alors $G \simeq \mathbb{Z}/n\mathbb{Z}$.

• Si $r = 3$, on nomme X_1, X_2, X_3 les orbites et on note n_i le cardinal du stabilisateur d'un représentant x_i de X_i. Le pôle x_i est par définition laissé fixe par au moins un $g \neq id$ donc $n_i \geqslant 2$.
On suppose $|X_1| \geqslant |X_2| \geqslant |X_3|$, alors comme $|X_i| = \frac{n}{n_i}$, on a $\frac{1}{n_1} \geqslant \frac{1}{n_2} \geqslant \frac{1}{n_3}$.
La formule de Burnside donne $3 = \frac{1}{n}(|X| + 2(n-1))$, donc $|X| = n + 2$.
En utilisant la formule des classes, il vient

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} = 1 + \frac{2}{n}.$$

On a donc $\frac{3}{n_1} \geqslant 1 + \frac{2}{n} > 1$, d'où $n_1 = 2$ car on a vu que $n_i \geqslant 2$. On en déduit :

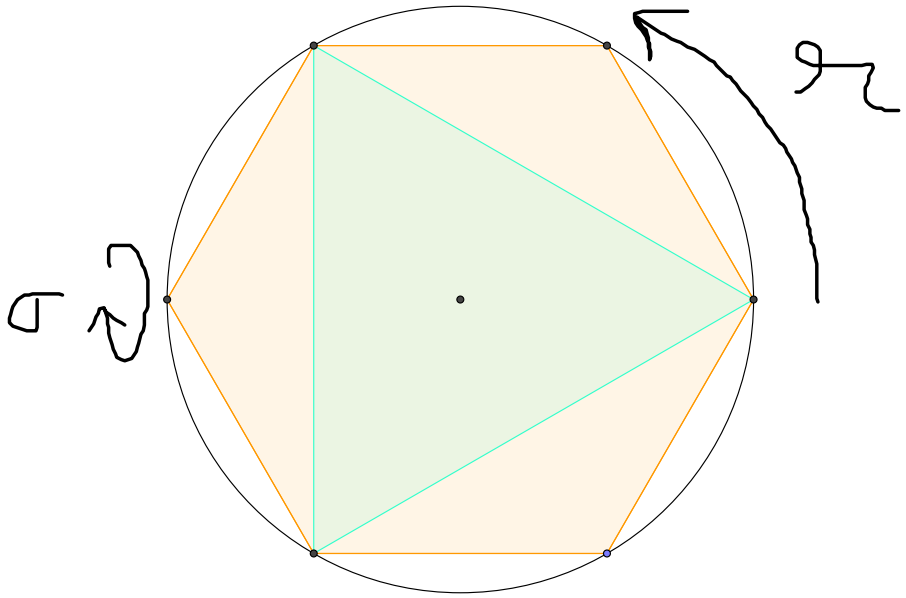
$$\frac{1}{n_2} + \frac{1}{n_3} = \frac{1}{2} + \frac{2}{n}.$$

1. On considère φ le morphisme de groupes qui à une rotation dans $\mathrm{SO}_2(\mathbb{R})$ d'angle θ envoie $e^{i\theta}$ dans $\mathbb{C}^*$. Alors $\varphi(G)$ est un sous groupe fini de $\mathbb{C}^*$. On sait alors que forcément $\varphi(G) = \mathbb{U}_n$ donc G est cyclique.

Donc $\frac{2}{n_2} \geqslant \frac{1}{2} + \frac{2}{n} > \frac{1}{2}$ et $n_2 \in \{2, 3\}$.
Si $n_2 = 2$, on a $n_3 = \frac{n}{2}$ et si $n_2 = 3$, alors $\frac{1}{n_3} = \frac{1}{6} + \frac{2}{n} > \frac{1}{6}$. Comme $n_3 \geqslant n_2 = 3$, on a $n_3 \in \{3, 4, 5\}$.
On arrive donc à la disjonction de cas suivante :

1. $n_1 = 2$, $n_2 = 2$, $n_3 = \frac{n}{2}$ et $n = |G|$ est pair,
2. $n_1 = 2$, $n_2 = n_3 = 3$ et G est d'ordre 12,
3. $n_1 = 2$, $n_2 = 3$, $n_3 = 4$ et G est d'ordre 24,
4. $n_1 = 2$, $n_2 = 3$, $n_3 = 5$ et G est d'ordre 60.

→ Cas 1 :
Comme $n_3 = \frac{n}{2} \geqslant n_2 = 2$, on a $n \geqslant 4$.
Si $n = 4$, $G \simeq \mathbb{Z}/4\mathbb{Z}$ ou $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{D}_2$.
Dans l'autre cas, on a $|X_3| = \frac{n}{n_3} = 2$. Il n'y a donc que deux pôles v et $-v$ dans X_3 (car $G_v = G_{-v}$ donc $|\mathrm{Orb}(v)| = |\mathrm{Orb}(-v)| = 2$ et il n'y a qu'une seule orbite de ce cardinal car $n \neq 4$). Le stabilisateur H de ces deux pôles est donc, par le même raisonnement que pour $r = 2$, un groupe cyclique de rotations dans $v^\perp$ de cardinal $\frac{n}{2}$.
Puis comme $X_3 = \{v, -v\}$ est une orbite, il existe un élément σ de $G \setminus H$ qui envoie v sur $-v$. Nécessairement c'est une rotation d'angle π d'axe inclus dans $v^\perp$. On dessine son axe dans le plan $v^\perp$ et on rajoute le polygone régulier donné par les rotations de H.
σ agit comme une symétrie axiale dans le plan $v^\perp$.
On remarque donc que $\mathbb{D}_{\frac{n}{2}} \subset G$ et par un argument de cardinal, $\mathbb{D}_{\frac{n}{2}} \simeq G$.



Sur le dessin ci-dessus [2], on peut mieux comprendre les deux cas précédents pour $n = 6$. On a un axe de rotation privilégié v et un polygone régulier à 6 côtés dans le plan orthogonal à cet axe. Alors soit on considère seulement les rotations $\{r^k, k \in [\![1, 6]\!]\}$ de ce polygone et on a le groupe $\mathbb{Z}/n\mathbb{Z}$, soit on prend un sous polygone régulier à 3 côtés (un triangle), et on n'a plus que 3 rotations mais on ajoute les symétries $\{r^{2k}\sigma, k \in [\![1, 3]\!]\}$, ce qui nous donne le groupe diédral $\mathbb{D}_{\frac{n}{2}}$. X_1 est le triangle bleu et X_2 est le triangle formé par les 3 autres sommets de l'hexagone.

→ Cas 2 :
On rappelle que les seuls groupes d'ordre 12 sont à isomorphisme près, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{D}_6$, $\mathcal{A}_4$ et Dic_3.

2. Au passage, c'est probablement le dessin le plus moche de l'univers...

Les éléments de G sont tous d'ordre un, deux ou trois car ils sont tous dans un stabilisateur. Il n'y a donc pas d'élément d'ordre 6, ce qui écarte les trois premiers cas facilement.
De plus, Dic_3 a un élément d'ordre 4, donc il est aussi éliminé.
Ainsi $G \simeq \mathcal{A}_4$.

→ Cas 3 :
Les éléments de G sont d'ordre 2, 3 ou 4. X_2 a 8 éléments et pour $v \in X_2$, $G_v = G_{-v}$, donc $|\mathrm{Orb}(v)| = |\mathrm{Orb}(-v)|$. Comme les orbites sont de cardinaux distincts, ces 8 pôles forment 4 axes de rotations qui sont donc d'ordre 3 (les rotations, pas les pôles). On a donc exactement quatre 3-Sylow/axes.
Comme les p-Sylow sont conjugués, on a une action transitive du groupe sur ces 3-Sylow par conjugaison, en notant $X_2 = \{\pm P_1, \pm P_2, \pm P_3, \pm P_4\}$ les axes de rotation :

$$\varphi : \begin{array}{ccc} G & \to & \mathcal{S}_4 \\ g & \mapsto & \left(G_{\pm P_i} \mapsto g G_{\pm P_i} g^{-1}\right) \end{array}.$$

Alors soit $g \in \mathrm{Ker}(\varphi)$, alors $gG_{\pm P_i}g^{-1} = G_{\pm P_i}$ pour tout i.
Soit $r \in G_{\pm P_i}$, alors $grg^{-1}(g(\pm P_i)) = g(\pm P_i)$. Donc grg^{-1} est une rotation d'axe $g(\pm P_i)$ qui par hypothèse est aussi une rotation d'axe $\pm P_i$. Donc g fixe quatre droites distinctes. g est donc l'identité.

→ Cas 4 :
$\mathcal{A}_5$ est l'unique groupe simple d'ordre 60, montrons donc que G est simple.
On rappelle que $60 = 2^2 \times 3 \times 5$. Donc les 3-Sylow ont 3 éléments, les 5-Sylow ont 5 éléments et les 2-Sylow ont 4 éléments.
X_1 contient 30 pôles d'ordre 2. Par cardinalité des orbites, il contient 15 axes de rotations d'ordre 2.
En itérant ce raisonnement, on a quinze éléments d'ordre 2, dix 3-Sylow et six 5-Sylow.

Supposons que G ait un sous-groupe distingué propre H.
Si $5 \mid |H|$, par le théorème de Cauchy, H contient un élément d'ordre 5, donc un 5-Sylow. Il les contient donc tous car les 5-Sylow sont conjugués. Comme les 5-Sylow sont ici isomorphes à $\mathbb{Z}/5\mathbb{Z}$, ils sont d'intersection deux à deux réduite à id (sinon ils seraient égaux car tout élément différent de id est générateur). On en déduit que H a au moins $1 + 6 \times 4 = 25$ éléments, donc $|H| = 30$.
On remarque que $3|30$ donc H contient un élément d'ordre 3. Donc $H = G$. Absurde.

Si $3|H$, H contient au moins $1 + 10 \times 2 = 21$ éléments donc il est de cardinal 30. On a donc $5|H$ et on obtient $G = H$.

H est donc soit de cardinal 2, soit de cardinal 4.
Si $|H| = 2$, $H = \langle\sigma\rangle$ et comme H est distingué, $\forall g \in G, g\sigma g^{-1} = \sigma$. Donc toutes les rotations de G ont même axe. C'est impossible car sinon il n'y aurait que deux orbites.
Si $|H| = 4$, alors H est l'unique 2-Sylow (sinon il n'est pas distingué).
Tout élément d'ordre 2 est dans un 2-Sylow, car sinon le sous groupe d'ordre 2 engendré par cet élément serait maximal pour l'inclusion et serait donc un 2-Sylow. Or il y a 15 éléments d'ordre 2, donc il ne peut y avoir un unique 2-Sylow. □

Remarques : • Si on se donne un polyèdre régulier, on peut étudier les isométries positives de sa sphère circonscrite conservant les sommets du polyèdre (les isométries propres). Celles-ci forment des sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$. Les groupes d'isométries positives des solides de Platon sont :
— $\mathcal{A}_4$ pour le tétraèdre,
— $\mathcal{S}_4$ pour le cube et l'octaèdre,
— $\mathcal{A}_5$ pour le dodécaèdre et l'icosaèdre.
Les polyèdres réguliers ayant le même groupe d'isométries sont en fait duaux, c'est à dire qu'en prenant un couple de tels polyèdres, si on relie les centres des faces de l'un, on obtient l'autre. On voit vite cette propriété avec le tétraèdre qui est son propre dual, et avec le cube qui engendre un octaèdre comme dual.
• Le groupe d'isométries de l'octaèdre est $\mathcal{S}_4$, pourtant par les deux premiers cas vus précédemment, on a vu que l'on pouvait faire agir des groupes d'isométries isomorphes à $\mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{D}_2$ sur les sommets de l'octaèdre. C'est logique car ces deux groupes s'injectent dans $\mathcal{S}_4$: un 4-cycle engendre un sous-groupe cyclique d'ordre 4 de $\mathcal{S}_4$ et $\mathbb{D}_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ peut être vu comme le sous-groupe de $\mathcal{S}_4$ engendré par deux transpositions à supports disjoints.
• Ce développement est trop long, il vaut mieux s'arrêter au cas 3 et faire quelques dessins de polyèdres ensuite pour conclure.
• En fait, cette classification marche de la même manière pour les sous-groupes finis de $\mathrm{PGL}_2(\mathbb{C})$. C'est le

théorème de Dickson. On peut trouver des éléments de réponse à ce sujet sur la page de Matthieu Romagny : `https://perso.univ-rennes1.fr/matthieu.romagny/agreg/exo/ss_gr_finis_PGL2.pdf`.
• Ces sous-groupes finis ne sont pas distingués car $\mathrm{SO}_3(\mathbb{R})$ est simple.

Chapitre 36

Table de $\mathcal{S}_4$

Références : Rauch, *Les groupes finis et leurs représentations*, 4.4

Nous allons déterminer la table de caractère de $\mathcal{S}_4$.

Tout d'abord, on sait qu'il y a cinq classes de conjugaison dans $\mathcal{S}_4$, qui correspondent aux types de la permutation. Ainsi, il y a la classe uniquement composée de l'identité, la classe comprenant les 6 transpositions, celle comprenant les 8 3-cycles, celles comprenant les 6 4-cycles et enfin celle comprenant les 3 doubles transpositions. [1] Il y a donc 5 caractères irréductibles. On connaît maintenant la taille de la table de caractères de $\mathcal{S}_4$.

• Caractères irréductibles de degré 1 :

On connaît deux représentations irréductibles de degré 1 : la représentation triviale **1** et la signature ε. On peut remplir les deux premières lignes de la table :

$\mathcal{S}_4$	1 Id	6 (12)	8 (123)	6 (1234)	3 (12)(34)
1	1	1	1	1	1
ε	1	-1	1	-1	1

• Premier caractère irréductible de degré 3 :

On va donner une interprétation géométrique de la représentation associée. Soit T un tétraèdre régulier de l'espace euclidien, centré en l'origine. On note (e_1, e_2, e_3, e_4) ses sommets. On note $Is(T)$ le groupe des isométries du tétraèdre. On a alors l'isomorphisme suivant :

$$\begin{array}{rll} \varphi : \mathcal{S}_4 & \to Is(T) & \\ \sigma & \mapsto u : \quad T & \to T \\ & \qquad e_i & \mapsto e_{\sigma(i)} \end{array}$$

Pour montrer que φ est définie, il suffit de la définir pour les transpositions et de la prolonger par morphisme de groupe. On voit alors $\varphi((12))$ comme la symétrie par rapport à l'hyperplan passant par e_3, e_4 et le milieu du segment $[e_1, e_2]$.
φ est injective car un élément de son noyau fixe un repère affine, donc est l'identité, et elle est surjective par construction. [2]
En pratique, on n'utilise pas que φ est un isomorphisme mais c'est joli donc on le dit quand même !

Comme $Is(T) \hookrightarrow \mathrm{O}(\mathbb{C}^3) \subset \mathrm{GL}(\mathbb{C}^3)$, φ induit une représentation de degré 3 de $\mathcal{S}_4$. On note χ_3 le caractère associé : $\forall \sigma \in \mathcal{S}_4, \chi_3(\sigma) = \mathrm{Tr}(\varphi(\sigma))$. On calcule alors, dans la base (e_1, e_2, e_3) (sachant $e_4 = -e_1 - e_2 - e_3$) :

1. On les compte à l'oral en utilisant les arguments de combinatoire classiques : on a un point fixe à choisir parmi 4 éléments, etc...

2. Pendant la préparation, on fait un tétraèdre en papier brouillon, et on fait ce morceau de la preuve dessus en le montrant au jury.

$$\varphi(12) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\chi_3(12) = 1$$

$$\varphi(123) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$\chi_3(123) = 0$$

$$\varphi(1234) = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}$$

$$\chi_3(1234) = -1$$

$$\varphi((12)(34)) = \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix}$$

$$\chi_3((12)(34)) = -1$$

On vérifie que χ_3 est irréductible en calculant :

$$\langle \chi_3, \chi_3 \rangle = \frac{1}{|\mathcal{S}_4|} \sum_{\sigma \in \mathcal{S}_4} |\chi_3(\sigma)|^2 = \frac{1}{24}(3^2 + 6 \times 1^2 + 6 \times (-1)^2 + 3 \times (-1)^2) = 1$$

On peut alors compléter une ligne supplémentaire de la table [3] :

$\mathcal{S}_4$	1 Id	6 (12)	8 (123)	6 (1234)	3 (12)(34)
1	1	1	1	1	1
ε	1	-1	1	-1	1
χ_3	3	1	0	-1	-1

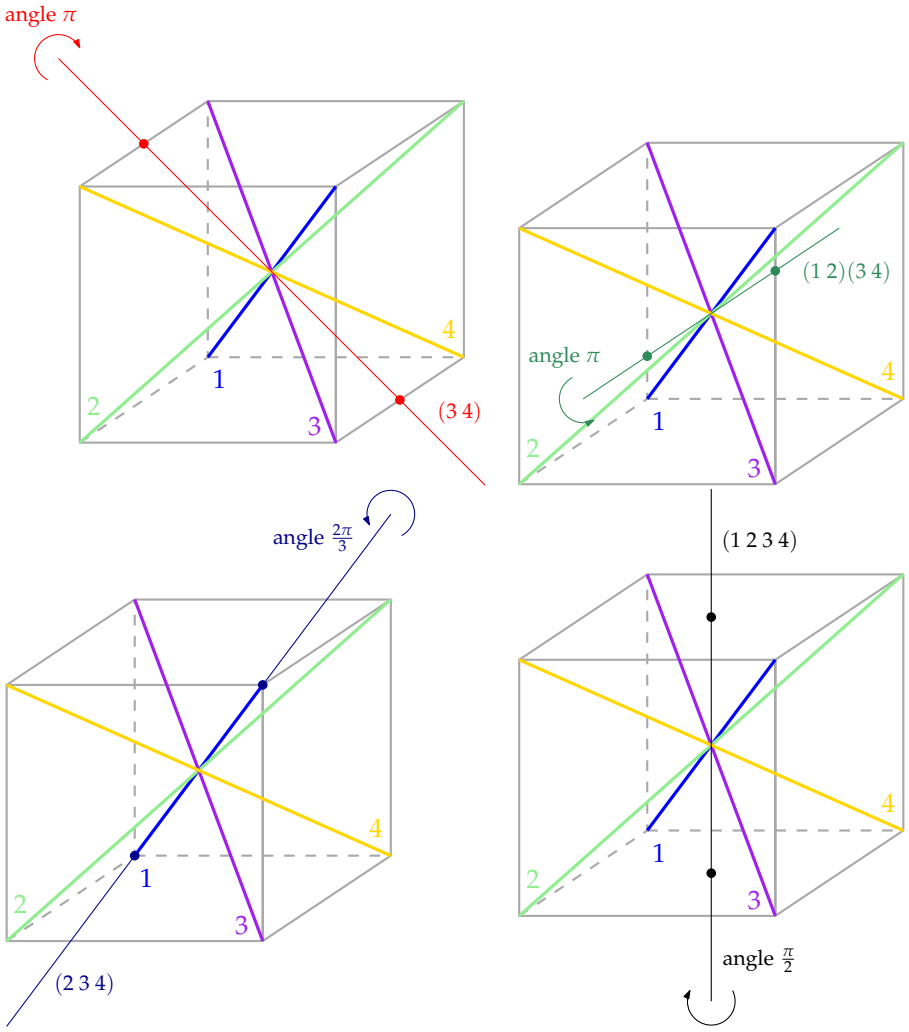
• Second caractère irréductible de degré 3 :

$\mathcal{S}_4$ est aussi isomorphe au groupe $Is^+(C)$ des isométries positives du cube.
En effet, on sait qu'une grande diagonale du cube est envoyée par une isométrie positive du cube sur une autre grande diagonale (car les isométries préservent les distances). L'action de $Is^+(C)$ sur les quatre grandes diagonales induit un morphisme $f : Is^+(C) \to \mathcal{S}_4$.
La rotation d'axe joignant les centres de deux arêtes opposées et d'angle π permute deux diagonales, laisse invariantes les deux autres. On a donc toutes les transpositions dans $\mathrm{Im}(f)$, donc f est surjective.
Ensuite, si une isométrie du cube u laisse globalement invariante chaque grande diagonale, chaque sommet du cube est donc invariant ou envoyé sur son opposé. On montre que si un sommet est envoyé sur son opposé, alors tous les sommets le sont (sinon on ne conserve pas les distances), et que la seule isométrie ayant cette propriété est la symétrie par rapport au centre du cube, donc une isométrie négative. f est donc injective, et finalement bijective.

Il existe donc un isomorphisme ψ de $\mathcal{S}_4$ dans $Is^+(C)$. Comme $Is^+(C) \hookrightarrow \mathrm{SO}(\mathbb{C}^3) \subset \mathrm{GL}(\mathbb{C}^3)$, ψ induit une représentation sur $\mathcal{S}_4$, dont le caractère sera noté χ_3'.

3. On peut aussi définir le caractère χ_3 comme celui attaché à la représentation standard de $\mathcal{S}_4$, qui est irréductible. On a alors : $\forall \sigma \in \mathcal{S}_4, \chi_3(\sigma) =$ (nombre de points fixes de σ) $- 1$. C'est plus rapide !

Pour tout σ dans $\mathcal{S}_4$, $\psi(\sigma)$ est donc une rotation, dont on connaît la trace : $\mathrm{Tr}(\psi(\sigma)) = \chi_3^{'}(\sigma) = 1+2\cos(\frac{2\pi}{k})$, où k désigne l'ordre de σ [4].



On calcule alors :

$$\chi_3^{'}(12) = 1 + 2\cos(\frac{2\pi}{2}) = -1$$

$$\chi_3^{'}(123) = 1 + 2\cos(\frac{2\pi}{3}) = 0$$

$$\chi_3^{'}(1234) = 1 + 2\cos(\frac{2\pi}{4}) = 1$$

$$\chi_3^{'}((12)(34)) = 1 + 2\cos(\frac{2\pi}{2}) = -1$$

On vérifie que $\chi_3^{'}$ est irréductible en calculant :

$$\langle \chi_3^{'}, \chi_3^{'} \rangle = \frac{1}{|\mathcal{S}_4|} \sum_{\sigma \in \mathcal{S}_4} |\chi_3^{'}(\sigma)|^2 = \frac{1}{24}(3^2 + 6 \times (-1)^2 + 6 \times 1^2 + 3 \times (-1)^2) = 1$$

.

On peut maintenant compléter une nouvelle ligne de la table [5] :

4. Si r est une rotation d'ordre k, il existe un réel θ et une base orthonormée dans laquelle r s'écrit : $\begin{pmatrix} R_\theta & 0 \\ 0 & 1 \end{pmatrix}$ avec $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. Comme $R_\theta^n = R_{n\theta}$, on déduit $\theta = \frac{2\pi}{k}$ mod 2π.
Puis comme on a un isomorphisme de groupes, l'ordre de la permutation et de la rotation associée sont les mêmes.

5. On peut voir la représentation ψ comme $\mathrm{Hom}(\varphi, \epsilon)$. On a alors $\chi_3^{'} = \varepsilon\chi_3$. Le calcul de $\langle \chi_3^{'}, \chi_3^{'} \rangle$ donne $\langle \chi_3, \chi_3 \rangle$ qui vaut 1. Encore une fois, cette méthode est plus rapide !

$\mathcal{S}_4$	1 Id	6 (12)	8 (123)	6 (1234)	3 (12)(34)
1	1	1	1	1	1
ε	1	-1	1	-1	1
χ_3	3	1	0	-1	-1
χ_3'	3	-1	0	1	-1

• Dernier caractère irréductible :

Pour trouver le degré du dernier caractère irréductible, on utilise la formule $\sum_{\chi \text{irréductible}} \deg(\chi)^2 = |\mathcal{S}_4| = 24$. Le dernier caractère irréductible χ_2 est donc de degré $\sqrt{24 - 2 \times 1^2 - 2 \times 3^2} = 2$. On finit en utilisant l'orthogonalité des colonnes d'une table de caractères. En effet, si σ et τ ne sont pas dans la même classe de conjugaison, on a $\sum_{\chi \text{irréductible}} \overline{\chi(\sigma)}\chi(\tau) = 0$.

Finalement, on a la table de caractères complète de $\mathcal{S}_4$:

$\mathcal{S}_4$	1 Id	6 (12)	8 (123)	6 (1234)	3 (12)(34)
1	1	1	1	1	1
ε	1	-1	1	-1	1
χ_2	2	0	-1	0	2
χ_3	3	1	0	-1	-1
χ_3'	3	-1	0	1	-1

Remarques : • En fait, $(1234)^2 = (13)(24)$, donc on peut obtenir cette double transposition en faisant une rotation d'angle π au centre d'une face du cube.

• Pour mieux voir la rotation d'angle $\frac{2\pi}{3}$ dans le cas du 3-cycle, on peut dessiner le tétraèdre inscrit dans le cube dont un des sommets est sur l'axe de rotation.

• On peut également trouver la représentation irréductible de degré 2 comme suit. Notons V_4 le groupe engendré par les doubles transpositions de $\mathcal{S}_4$. V_4 est distingué dans $\mathcal{S}_4$, et comme $D(\mathcal{S}_4) = \mathfrak{A}_4 \not\subset V_4$, le quotient $\mathcal{S}_4/V_4$ est isomorphe à $\mathcal{S}_3$, seul groupe d'ordre 6 non commutatif. L'image par la projection $\mathcal{S}_4 \longrightarrow \mathcal{S}_4/V_4 \simeq \mathcal{S}_3$ d'une transposition est une transposition (car d'ordre 2 dans $\mathcal{S}_3$), l'image d'un 3-cycle est un 3-cycle (car d'ordre 3 dans $\mathcal{S}_3$), l'image d'un 4-cycle est une transposition (car d'ordre 2 dans $\mathcal{S}_3$), et enfin l'image d'une double transposition est l'identité de $\mathcal{S}_3$ (car V_4 est le noyau de la projection).

La représentation standard $\overline{\rho_2}$ de $\mathcal{S}_3$, de degré 2, induit une représentation ρ_2 de $\mathcal{S}_4$. Précisément, si $\overline{\sigma}$ désigne la classe de $\sigma \in \mathcal{S}_4$ modulo V_4, on a une représentation $\rho_2 : \mathcal{S}_4 \longrightarrow \mathrm{GL}(\mathbb{C}^2)$ définie par : $\forall \sigma \in \mathcal{S}_4, \rho_2(\sigma) = \overline{\rho_2}(\overline{\sigma})$. Notons χ_2 le caractère associé à la représentation ρ_2 de $\mathcal{S}_4$ et $\overline{\chi_2}$ le caractère associé à la représentation standard $\overline{\rho_2}$ de $\mathcal{S}_3$. On a : $\forall \sigma \in \mathcal{S}_4$, $\chi_2(\sigma) = \overline{\chi_2}(\overline{\sigma})$.

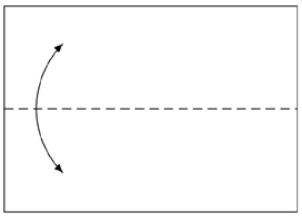
Cependant, on connaît $\overline{\chi_2}$. En effet, le caractère θ associé à la représentation de permutation de $\mathcal{S}_3$ se décompose en $\theta = \mathbf{1} + \overline{\chi_2}$. En outre, $\forall \sigma \in \mathcal{S}_3$, $\theta(\sigma) =$ nombre de points fixes de σ. On en déduit les valeurs de $\overline{\chi_2}$:

$\mathcal{S}_3$	1 Id	3 (12)	2 (123)
$\overline{\chi_2}$	2	0	-1

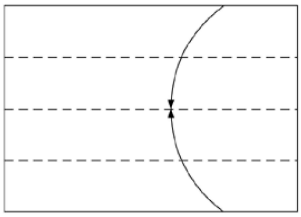
On peut calculer les valeurs de χ_2, et vérifier que $\langle \chi_2, \chi_2 \rangle = 1$, donc que χ_2 est irréductible. C'est en fait général : pour G un groupe fini et H un sous-groupe distingué de G, une représentation irréductible de G/H remonte en une représentation irréductible de G.

• Il y a une manière assez simple de faire un tétraèdre avec de la force, de la fougue, de la tendresse, ainsi qu'une feuille de papier. La voici !

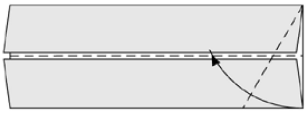
1
Prendre une feuille A4 et marquer le pli central.



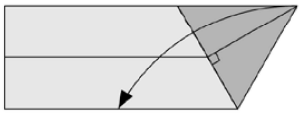
2
Plier chaque côté jusqu'au pli central.



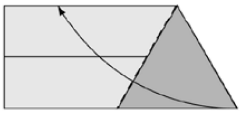
3
Amener le coin inférieur droit sur le pli central en partant de l'angle du haut.



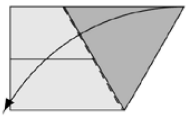
4
Amener le coin supérieur sur le côté inférieur.



5
Replier le long du pli marqué en 3.

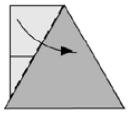


Plier à nouveau.

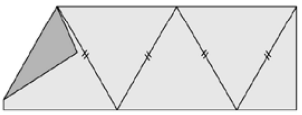


Répéter cette opération une dernière fois.

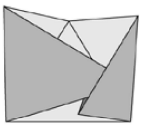
6
Plier le dernier triangle.



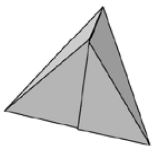
7
Déplier à plat en gardant le coin supérieur gauche plié.



8
Enrouler, puis rentrer le triangle de gauche dans le petit de droite.



9
Le tétraèdre est assemblé.



Extrait de « Pliages et mathématiques », ACL-Editions

Adapté du travail de Thibaut Tardieu et Florian Lemonnier.

Chapitre 37

Théorème central limite

Références : Ouvrard, *Probabilités 2*, p323

Théorème (Théorème central limite)**.**

Soit $(X_n)_{n\in\mathbb{N}}$ une suite de v.a. *iid* de carré intégrable. On note $m = \mathbb{E}[X]$, $\sigma^2 = \mathbb{V}ar(X)$ et $(S_n)_{n\in\mathbb{N}}$ la somme des X_n. On a alors :

$$\frac{S_n - nm}{\sqrt{n\sigma}} \Longrightarrow \mathcal{N}(0,1) \quad .$$

Quitte à recentrer et réduire les variables, on peut supposer que $m = 0$ et $\sigma^2 = 1$. La démonstration va utiliser le théorème de Paul Lévy. On note φ_n la fonction caractéristique de $\frac{S_n}{\sqrt{n}}$ et on va montrer que la suite $(\varphi_n)_n$ converge vers la fonction caractéristique de la loi normale.

• **Étape 1 :** Soient $(a_n)_n$ et $(b_n)_n$ deux suites de nombres complexes de modules inférieurs à 1, on a :

$$\forall n \in \mathbb{N}^*, \quad \left|\prod_{i=1}^n a_i - \prod_{i=1}^n b_i\right| \leqslant \sum_{i=1}^n |a_i - b_i| \quad .$$

Le résultat est évident pour $n = 1$. Soit $n \geqslant 1$, on a :

$$\begin{aligned}\left|\prod_{i=1}^{n+1} a_i - \prod_{i=1}^{n+1} b_i\right| &\leqslant \left|\prod_{i=1}^{n+1} a_i - a_{n+1}\prod_{i=1}^{n} b_i\right| + \left|a_{n+1}\prod_{i=1}^{n} b_i - \prod_{i=1}^{n+1} b_i\right| \\ &\leqslant |a_{n+1}|\left|\prod_{i=1}^{n} a_i - \prod_{i=1}^{n} b_i\right| + \left|\prod_{i=1}^{n} b_i\right||a_{n+1} - b_{n+1}| \\ &\leqslant \left|\prod_{i=1}^{n} a_i - \prod_{i=1}^{n} b_i\right| + |a_{n+1} - b_{n+1}|\end{aligned}$$

Par récurrence on a le résultat. [1]

• **Étape 2 :** Soit X une v.a. $\mathbb{L}^2$, alors on a :

$$\forall t \in \mathbb{R}, \quad \left|\varphi_X(t) - \left(1 + it\mathbb{E}[X] - \frac{t^2}{2}\mathbb{E}[X^2]\right)\right| \leqslant t^2\mathbb{E}\left[\min\left(X^2, |t|\frac{|X^3|}{6}\right)\right] \quad .$$

1. pas de référence, c'est à connaître par ♡ ...

D'après la formule de *Taylor-Laplace* à l'ordre 1, pour tout réel x, on a :

$$e^{ix} = 1 + ix - x^2 \int_0^1 (1-u)e^{iux}\mathrm{d}u$$
$$e^{ix} - \left(1 + ix - \frac{x^2}{2}\right) = -x^2 \int_0^1 (1-u)[e^{iux} - 1]\mathrm{d}u$$
$$\left|e^{ix} - \left(1 + ix - \frac{x^2}{2}\right)\right| \leqslant x^2$$

De même, en poussant la formule à l'ordre 2, pour tout réel x, on a :

$$e^{ix} = 1 + ix - \frac{x^2}{2} - i\frac{x^3}{2} \int_0^1 (1-u)^2 e^{iux}\mathrm{d}u$$

$$\left|e^{ix} - \left(1 + ix - \frac{x^2}{2}\right)\right| \leqslant \frac{|x^3|}{6}$$

On a donc la majoration suivante : $\forall x \in \mathbb{R}, \quad \left|e^{ix} - \left(1 + ix - \frac{x^2}{2}\right)\right| \leqslant \min\left(x^2, \frac{|x^3|}{6}\right)$. On obtient le résultat en appliquant cette inégalité à tX et on effectue l'inégalité de Jensen ($x \mapsto |x|$ est convexe).

• **Étape 3 :** Application à φ_n.

Soit $t \in \mathbb{R}$ et $n \in \mathbb{N}^*$, on a : $\varphi_n(t) = \varphi_{S_n}\left(\frac{t}{\sqrt{n}}\right) = \left(\varphi_X\left(\frac{t}{\sqrt{n}}\right)\right)^n$, par propriétés sur les fonctions caractéristiques (somme de v.a. indépendante et multiplication par une constante). D'après les deux étapes précédentes, on a :

$$\begin{aligned}\left|\varphi_n(t) - \left(1 - \frac{t^2}{2n}\right)^n\right| &= \left|\left(\varphi_X\left(\frac{t}{\sqrt{n}}\right)\right)^n - \left(1 - \frac{t^2}{2n}\right)^n\right| \\ &\leqslant n\left|\varphi_X\left(\frac{t}{\sqrt{n}}\right) - \left(1 - \frac{t^2}{2n}\right)\right| \\ &\leqslant n\frac{t^2}{n}\mathbb{E}\left[\min\left(X^2, \frac{|t|}{6\sqrt{n}}|X^3|\right)\right]\end{aligned}$$

D'après le théorème de convergence dominée (dont les hypothèses sont vérifiées) on a :

$$\left|\varphi_n(t) - \left(1 - \frac{t^2}{2n}\right)^n\right| \underset{n\to+\infty}{\longrightarrow} 0 \quad .$$

En outre, on a :

$$\forall t \in \mathbb{R}, \quad \left(1 - \frac{t^2}{2n}\right)^n \underset{n\to+\infty}{\longrightarrow} e^{-\frac{t^2}{2}} \quad .$$

On a donc :

$$\forall t \in \mathbb{R}, \quad \varphi_n(t) \underset{n\to+\infty}{\longrightarrow} e^{-\frac{t^2}{2}} \quad .$$

Le théorème de Paul Lévy permet de conclure.

Adapté du travail de Baptiste Huguet.

Chapitre 38

Théorème d'extension

Références : Saux Picart, *Cours de calcul formel - Algorithmes fondamentaux*, p 148

On sait que si P et Q sont deux polynômes admettant une racine commune, alors leur résultant est nul en cette racine. Le calcul du résultant permet donc de trouver toutes les racines possibles.
Néanmoins les racines du résultant ne se remontent pas toutes en racines des polynômes. C'est ce que permet d'étudier le théorème d'extension.

Théorème.

Soit $\mathbb{K}$ un corps algébriquement clos et soient P, Q deux polynômes de $\mathbb{K}[Y_1, ..., Y_k][X]$, on note $P = \sum_{i=0}^{m} a_i X^i$ et $Q = \sum_{i=0}^{n} b_i X^i$ avec m, $n \neq 0$ et a_i, $b_i \in \mathbb{K}[Y_1, ..., Y_k]$.
Si $(\alpha_1, ..., \alpha_k, \alpha)$ est tel que $P(\alpha_1, ..., \alpha_k, \alpha) = Q(\alpha_1, ..., \alpha_k, \alpha) = 0$, alors $\mathrm{Res}_X(P, Q)(\alpha_1, ..., \alpha_k) = 0$.
Réciproquement, si $\mathrm{Res}_X(P, Q)(\alpha_1, ..., \alpha_k) = 0$, alors une des propositions suivantes est vérifiée :

1. $\exists \alpha \in \mathbb{K}$, $P(\alpha_1, ..., \alpha_k, \alpha) = Q(\alpha_1, ..., \alpha_k, \alpha) = 0$,
2. $P(\alpha_1, ..., \alpha_k, X) = 0$,
3. $Q(\alpha_1, ..., \alpha_k, X) = 0$,
4. $a_m(\alpha_1, ..., \alpha_k) = b_n(\alpha_1, ..., \alpha_k) = 0$.

Pour prouver ce théorème, on va utiliser l'application suivante :

$$\Phi : \begin{array}{ccc} \mathbb{K}[Y_1, ..., Y_k][X] & \to & \mathbb{K}[X] \\ U & \mapsto & U(\alpha_1, ..., \alpha_k, X) \end{array}$$

Pour voir sa compatibilité avec le résultant, on a le résultat suivant.

Lemme.

Soient A, B deux anneaux, et φ un morphisme d'anneau de A dans B, alors si on note p et q les degrés respectifs de $\varphi(P)$ et $\varphi(Q)$, on a

$$\varphi(\mathrm{Res}_X(P, Q)) = \begin{cases} \varphi(a_m)^{n-q} \mathrm{Res}_X(\varphi(P), \varphi(Q)) & \text{si } \varphi(a_m) \neq 0, \\ \varphi(b_n)^{m-p} \mathrm{Res}_X(\varphi(P), \varphi(Q)) & \text{si } \varphi(b_n) \neq 0, \\ 0 & \text{si } \varphi(a_m) = \varphi(b_n) = 0. \end{cases}$$

Démonstration. Le résultant est défini comme le déterminant de la matrice de Sylvester. On a donc, comme le déterminant est un polynôme :

$$\varphi(\mathrm{Res}_X(P, Q)) = \varphi(\det(Sylv(P, Q))) = \det(\varphi(Sylv(P, Q))).$$

Si on note a'_i et b'_i les images des a_i et b_i par φ, alors

$$\varphi(Sylv(P,Q)) = \begin{pmatrix} a'_m & & & & 0 & & \\ \vdots & \ddots & & & b'_q & \ddots & \\ a'_0 & & \ddots & & \vdots & \ddots & 0 \\ & \ddots & & a'_m & b'_0 & & b'_q \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & a'_0 & & & b'_0 \end{pmatrix}.$$

Supposons $a'_m \neq 0$, alors en développant par rapport aux premières lignes, on a

$$\det(\varphi(Sylv(P,Q))) = (a'_m)^{n-q} \det(Sylv(\varphi(P),\varphi(Q))).$$

Il vient

$$\varphi(\mathrm{Res}_X(P,Q)) = (\varphi(a_m))^{n-q} \mathrm{Res}_X(\varphi(P),\varphi(Q)).$$

Si $a'_m = 0$ et $b'_n = 0$, la formule précédente marche encore car $\varphi(\mathrm{Res}_X(P,Q)) = 0$.
Enfin si $a'_m = 0$ et $b'_n \neq 0$, on a par le même raisonnement

$$\varphi(\mathrm{Res}_X(P,Q)) = (\varphi(b_n))^{m-p} \mathrm{Res}_X(\varphi(P),\varphi(Q)).$$

□

Passons à la preuve du théorème !

Démonstration. $\Leftarrow$: Si $P(\alpha_1,...,\alpha_k,\alpha) = Q(\alpha_1,...,\alpha_k,\alpha) = 0$, alors α est racine de $\Phi(P)$ et $\Phi(Q)$, donc $\mathrm{Res}_X(\Phi(P),\Phi(Q)) = 0$. Le lemme donne alors $\Phi(\mathrm{Res}_X(P,Q)) = 0$, donc $\mathrm{Res}_X(P,Q)(\alpha_1,...,\alpha_k) = 0$.

$\Rightarrow$: Supposons que $\mathrm{Res}_X(P,Q)(\alpha_1,...,\alpha_k) = 0$.

• Si $\Phi(a_m) \neq 0$, alors le lemme donne $\Phi(a_m)^{n-q} \mathrm{Res}_X(\Phi(P),\Phi(Q)) = 0$, donc $\mathrm{Res}_X(\Phi(P),\Phi(Q)) = 0$. On en déduit que soit $\Phi(Q) = 0$ (cas 3), soit $\Phi(Q) \neq 0$ et $\Phi(P)$ et $\Phi(Q)$ ont une racine commune α. Alors $(\alpha_1,...,\alpha_k,\alpha)$ est racine commune de P et Q.

• Si $\Phi(b_n) \neq 0$, on peut refaire le raisonnement pour tomber sur les cas 1 ou 3.

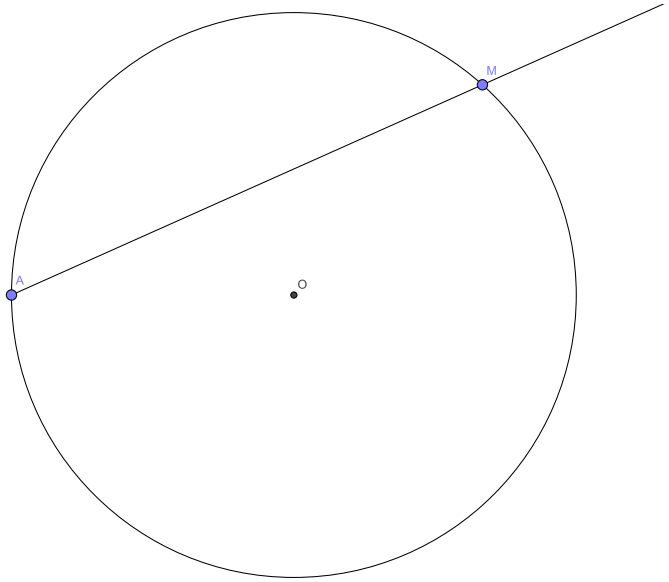
• Si $\Phi(a_m) = \Phi(b_n) = 0$, on est dans le cas 4. □

Application : Paramétrisation du cercle
On tente de trouver une paramétrisation du cercle centré en 0 et de rayon 1. Pour cela, on choisit un point A sur le cercle (ici $(-1,0)$). L'intersection d'une droite de pente $t \in \mathbb{R}$ passant par A - et non-tangente au cercle - avec le cercle est appelée $M(t)$. $M(t)$ est donc racine de $P = X^2 + Y^2 - 1$ et $Q = Y - t(X+1)$.
Pour trouver une expression en t des coordonnées de $M(t)$, on fait un résultant :

$$\mathrm{Res}_Y(P,Q) = \begin{vmatrix} 1 & 1 & 0 \\ 0 & -t(X+1) & 1 \\ X^2-1 & 0 & -t(X+1) \end{vmatrix} = P(t(X+1))) = (1+t^2)X^2 + 2t^2X + t^2 - 1$$

Pour calculer ce résultant rapidement, on a utilisé la formule magique avec les racines : on a juste à faire le produit des $P(\alpha_i)$ avec α_i les racines de Q.

On trouve deux racines au polynôme obtenu : $X = -1$ (qui correspond au point A), et $X = \dfrac{1-t^2}{1+t^2}$. Finalement, la paramétrisation du cercle est donnée ici par $M(t) = \left(\dfrac{1-t^2}{1+t^2}, \dfrac{2t}{1+t^2}\right)$.



Refaisons maintenant le raisonnement à l'envers ! Supposons que j'ai la paramétrisation précédente, et que je veuille trouver une équation de la courbe décrite par cette paramétrisation. Puis-je remonter les racines du résultant en racines des deux polynômes ?
On pose $P = (1+t^2)X + t^2 - 1$ et $Q = (1+t^2)Y - 2t$, alors

$$\mathrm{Res}_t(P,Q) = \begin{vmatrix} X+1 & 0 & Y & 0 \\ 0 & X+1 & -2 & Y \\ X-1 & 0 & Y & -2 \\ 0 & X-1 & 0 & Y \end{vmatrix} = 4(X^2+Y^2-1).$$

Les zéros du résultant décrivent le cercle $\mathcal{C}(0,1)$, or $M(t)$ paramétrise le cercle privé du point A. Le point A représente le cas 4 du théorème, c'est à dire que comme $\Phi(P) = -2$ et $\Phi(Q) = -2t$, le terme dominant a disparu dans les deux polynômes.

Remarques : • Pour illustrer les cas 2 et 3 du théorème, on peut juste prendre $P = (Y_1 - \alpha_1)P'$ car alors $a_i' = 0$ pour tout i et la matrice de Sylvester est de déterminant nul (pareil pour Q pour le cas 3).

Chapitre 39

Théorème de Cartan - Von Neumann

Références : Gonnord, Tosel, *Thèmes d'analyse pour l'agrégation - Calcul différentiel*, p 81-84

Théorème (Théorème de Cartan-Von Neumann)**.**

Tout sous-groupe fermé de $\mathrm{GL}_n(\mathbb{R})$ est une sous-variété de $\mathcal{M}_n(\mathbb{R})$.

Démonstration. Soit G un sous-groupe fermé de $\mathrm{GL}_n(\mathbb{R})$. Le but de la preuve est de trouver pour chaque point g de G un $\mathcal{C}^1$-difféomorphisme local φ envoyant un voisinage ouvert U de 0 dans $\mathcal{M}_n(\mathbb{R})$ sur un voisinage ouvert V de g dans $\mathrm{GL}_n(\mathbb{R})$ et un sous-espace vectoriel $\mathcal{L}_G$ de $\mathcal{M}_n(R)$ tel que $\varphi(U \cap \mathcal{L}_G) = V \cap G$.

- On peut se restreindre au cas où $g = I_n$.

En effet, l'application t_g : $\begin{array}{ccc} \mathcal{M}_n(\mathbb{R}) & \longrightarrow & \mathcal{M}_n(\mathbb{R}) \\ h & \longmapsto & gh \end{array}$ est un $\mathcal{C}^\infty$-difféomorphisme (global).
Si on trouve φ un difféomorphisme de $V(0) \subset \mathcal{M}_n(\mathbb{R})$ dans $V(I_n) \subset G$, alors $t_g \circ \varphi$ est un difféomorphisme entre un voisinage de 0 et un voisinage de $g \in G$.

- On pose $\mathcal{L}_G = \{M \in \mathcal{M}_n(\mathbb{R}), \forall t \in \mathbb{R}, e^{tM} \in G\}$. C'est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$.

La seule chose non triviale à vérifier est la stabilité par la somme.

L'exponentielle est $\mathcal{C}^\infty$. De plus, $D\exp(0) = I_n$ est un isomorphisme, donc exp induit un $\mathcal{C}^1$-difféomorphisme d'un voisinage de 0 sur un voisinage de I_n. On appelle L son inverse.
On voit que $DL(I_n) = I_n$. La définition de la différentiabilité donne alors $L(I_n + H) = H + o(H)$. [1]

Soit $k \in \mathbb{N}^*$, on a $e^{\frac{A}{k}} e^{\frac{B}{k}} = I_n + \dfrac{A+B}{k} + o\left(\dfrac{1}{k}\right)$. Donc pour k assez grand, on peut utiliser la formule d'inversion précédente et écrire $e^{\frac{A}{k}} e^{\frac{B}{k}} = \exp\left(L\left(e^{\frac{A}{k}} e^{\frac{B}{k}}\right)\right)$.
Il vient

$$\begin{aligned} \left(e^{\frac{A}{k}} e^{\frac{B}{k}}\right)^k &= \exp\left(kL\left(e^{\frac{A}{k}} e^{\frac{B}{k}}\right)\right) \\ &= \exp\left(kL\left(I_n + \frac{A+B}{k} + o\left(\frac{1}{k}\right)\right)\right) \\ &= \exp\left(k\left(\frac{A+B}{k} + o\left(\frac{1}{k}\right)\right)\right) \\ &= \exp(A+B) + o(1). \end{aligned}$$

Donc $\lim\limits_{k\to\infty} \left(e^{\frac{A}{k}} e^{\frac{B}{k}}\right)^k = e^{A+B}$.

Soient maintenant A et B dans $\mathcal{L}_G$, alors $\forall t \in \mathbb{R}$, e^{tA}, $e^{tB} \in G$. On a alors $\lim\limits_{k\to\infty} \left(e^{\frac{tA}{k}} e^{\frac{tB}{k}}\right)^k = e^{t(A+B)}$. Or $\forall k$, $e^{\frac{tA}{k}} e^{\frac{tB}{k}} \in G$ et G est fermé, donc $e^{t(A+B)} \in G$. On en déduit donc que $A + B \in \mathcal{L}_G$.

1. En fait, L est le logarithme matriciel et on peut le définir directement par $L(I_n + M) = \sum\limits_{i=0}^{\infty} \dfrac{(-1)^i M^{i+1}}{i+1}$ pour $\|M\| < 1$.

→ On pose S un supplémentaire de $\mathcal{L}_G$ dans $\mathcal{M}_n(\mathbb{R})$, puis on pose φ qui à $X = L + M \in \mathcal{L}_G \oplus S$ associe $e^L e^M \in \mathrm{GL}_n(\mathbb{R})$. φ est $\mathcal{C}^\infty$, $\varphi(0) = I_n$ et $\varphi'(0) = I_n$. On peut appliquer le théorème d'inversion local.
Il existe U un voisinage ouvert de 0 dans $\mathcal{M}_n(\mathbb{R})$ tel que φ est un $\mathcal{C}^1$-difféomorphisme de U sur un voisinage ouvert de I_n, $V = \varphi(U) \subset \mathrm{GL}_n(\mathbb{R})$.
Néanmoins on veut avoir $\varphi(U \cap \mathcal{L}_G) = V \cap G$. On sait déjà que $\varphi(\mathcal{L}_G) \subset G$, donc $\varphi(U \cap \mathcal{L}_G) \subset V \cap G$. On va donc montrer que quitte à restreindre U, si $\varphi(X) \in G$, alors $X \in \mathcal{L}_G$, ainsi le théorème sera prouvé !

• Montrons qu'il n'existe pas de suite $(M_k)_k$ de $S \setminus 0$ de limite nulle et telle que pour tout k, $e^{M_k} \in G$.
Si c'est le cas, on pose la suite $\varepsilon_k = \dfrac{M_k}{\|M_k\|}$. Elle évolue dans la sphère unité fermée et dans S, donc quitte à extraire une sous suite, on peut supposer qu'elle converge (vers $\varepsilon \in S$ de norme 1). Montrons que $\varepsilon \in \mathcal{L}_G$. On aura alors $\varepsilon \in \mathcal{L}_G \cap S = \{0\}$, ce qui est absurde.
Soit $t \in \mathbb{R}$, on a $e^{t\varepsilon} = \lim\limits_k \exp\left(t\dfrac{M_k}{\|M_k\|}\right)$. Si on pose $\dfrac{t}{\|M_k\|} = \lambda_k + \mu_k$ avec $\lambda_k \in \mathbb{Z}$ et $|\mu_k| < \dfrac{1}{2}$, on obtient $\exp\left(t\dfrac{M_k}{\|M_k\|}\right) = \underbrace{e^{\lambda_k M_k}}_{=(e^{M_k})^{\lambda_k} \in G} \underbrace{e^{\mu_k M_k}}_{\to 1}$.[2]
On a donc $e^{t\varepsilon} = \lim\limits_k e^{\lambda_k M_k}$ et comme G est fermé, $e^{t\varepsilon} \in G$.

• Conclusion : Supposons que l'on ne peut restreindre U tel que si $\varphi(X) \in G$ et $X \in U$, alors $X \in \mathcal{L}_G$. Alors pour tout $k \in \mathbb{N}^*$, on dispose de $Y_k \in V \cap G \cap B(I_n, \dfrac{1}{k})$ tel que son antécédent $X_k = \varphi^{-1}(Y_k)$ n'appartienne pas à $\mathcal{L}_G$. On dispose donc de deux suites $(s_k)_k \in (S\setminus\{0\})^{\mathbb{N}^*}$ et $(l_k)_k \in \mathcal{L}_G^{\mathbb{N}^*}$ telles que l'on ait : $\forall k \in \mathbb{N}^*, \quad X_k = l_k + s_k$.
Par continuité de φ^{-1}, ces deux suites sont de limite nulle. De plus pour tout k,on a : $\varphi(X_k) = e^{l_k} e^{s_k} = Y_k \in G$.
Dans ce cas, $e^{s_k} = e^{-l_k} Y_k \in G$ donc par le point précédent, on a une absurdité.
Il existe donc un ouvert U contenant 0 tel que $\varphi(U \cap \mathcal{L}_G) = \varphi(U) \cap G$ et tel que φ induise un $\mathcal{C}^1$-difféomorphisme sur U. □

Remarques : • $\mathcal{L}_G$ peut être égal à $\{0\}$. En fait, c'est le cas si et seulement si G est discret, donc si et seulement si G est une variété de dimension nulle (c'est à dire un ensemble de points isolés). Il vaut mieux le préciser à l'oral car certains mathématiciens pensent que c'est un abus que de parler de variétés de dimension nulle.
• L'ensemble $\mathcal{L}_G$ est en fait une sous-algèbre pour la multiplication interne du crochet de Lie (même démo que pour la stabilité par la somme). On l'appelle l'algèbre de Lie associée à G.
• La courbe $t \to \exp(tM)$ pour $M \in \mathcal{L}_G$ est une courbe dans G passant par I_n. Son vecteur tangent en $t = 0$ est M. Donc $\mathcal{L}_G \subset T_{I_n} G$. Or ils ont même dimension, donc l'espace tangent à I_n est l'algèbre de Lie.
• Applications (Mneimné-Testard) : SL_n, $\mathrm{SO}_n/\mathrm{O}_n$ sont des sous-variétés de $\mathbb{R}^{n^2}$, les algèbres de Lie correspondantes sont les matrices de trace nulle et les matrices antisymétriques. Les dimensions de ces sous-variétés sont donc $n^2 - 1$ et $\dfrac{n(n-1)}{2}$. Les comportements de SO_n et O_n sont les mêmes car SO_n est un ouvert de O_n.
• C'est un développement dangereux... Il faut connaître un minimum de théorie de Lie pour le faire.

2. $\exp(\mu_k M_k)$ tend vers 1 puisque M_k tend vers 0 et μ_k borné.

Chapitre 40

Théorème de Cauchy-Lipschitz

Références : Demailly, *Analyse numérique et équations différentielles*, p 132-133 et 141-142
`http://www.math.univ-toulouse.fr/~fboyer/_media/enseignements/agreg/cours_edo_agreg_fboyer.pdf`

Théorème.

Soit I un intervalle ouvert de $\mathbb{R}$, Ω un ouvert de $\mathbb{R}^m$ et $f : I \times \Omega \to \mathbb{R}^m$ une application continue et localement lipschitzienne en la seconde variable.
Alors, si $t_0 \in I$ et $y_0 \in \Omega$ sont donnés, le problème de Cauchy suivant admet une unique solution maximale.

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

Démonstration. • Cylindre de sécurité [1]
Comme I et Ω sont ouverts, il existe $C_0 = [t_0 - T_0, t_0 + T_0] \times \overline{B}(y_0, r_0)$ un cylindre inclus dans $I \times \Omega$.
Comme f est localement lipschitzienne en la seconde variable, on peut choisir r_0 assez petit pour que f soit k-lipschitzienne sur C_0.
De plus, sur C_0, f est bornée par une constante M.
Soit $T \leqslant T_0$, et y une solution du problème de Cauchy définie au moins sur $I_0 \subset [t_0 - T, t_0 + T]$. Supposons qu'elle sorte du cylindre $C = [t_0 - T, t_0 + T] \times \overline{B}(y_0, r_0)$ au temps $\tau \in [t_0 - T, t_0 + T]$ alors, par continuité,

$$r_0 = \|y(\tau) - y_0\| = \left\| \int_{t_0}^{\tau} y'(u) \mathrm{d}u \right\| \leqslant TM.$$

Donc si $T \leqslant \min\left(T_0, \frac{r_0}{M}\right)$, alors toute solution définie sur $I_0 \subset [t_0 - T, t_0 + T]$ reste dans la boule $\overline{B}(y_0, r_0)$.
On nommera cylindre de sécurité l'ensemble $C = [t_0 - T, t_0 + T] \times \overline{B}(y_0, r_0)$.

• Existence locale de la solution
On note $\mathcal{F} = \mathcal{C}([t_0 - T, t_0 + T], \overline{B}(y_0, r_0))$ [2] et pour $y \in \mathcal{F}$, on appelle $\phi(y)$ la fonction définie sur $[t_0 - T, t_0 + T]$ comme suit :

$$\phi(y)(t) = y_0 + \int_{t_0}^{t} f(u, y(u)) \mathrm{d}u.$$

Comme $\mathcal{F}$ muni de la norme uniforme est une partie complète, et comme $\phi : \mathcal{F} \to \mathcal{F}$, on va appliquer un théorème de point fixe.
Soient y_1, $y_2 \in \mathcal{F}$,

$$\begin{aligned} |\phi(y_1) - \phi(y_2)|(t) &= \left| \int_{t_0}^{t} (f(u, y_1(u)) - f(u, y_2(u))) \, \mathrm{d}u \right| \\ &\leqslant k \int_{t_0}^{t} |y_1(u) - y_2(u)| \, \mathrm{d}u \\ &\leqslant kT \|y_1 - y_2\| \end{aligned}$$

1. Faire un dessin.
2. Ce n'est pas un espace vectoriel !!! C'est un fermé dans un complet néanmoins.

Donc $\|\phi(y_1) - \phi(y_2)\| \leqslant kT \|y_1 - y_2\|$. Et en particulier, si on choisit $T < \dfrac{1}{k}$, alors ϕ est **contractante**.
On a donc existence et unicité d'une solution au problème de Cauchy sur $[t_0 - T, t_0 + T]$.

- Unicité locale

Soient y_1 et y_2 deux solutions définies sur des intervalles ouverts I_1 et I_2 contenant $[t_0 - T, t_0 + T]$.
Soit $J = \{t \in I_1 \cap I_2, y_1(t) = y_2(t)\}$, on va montrer que $J = I_1 \cap I_2$ par connexité.
On sait déjà que $[t_0 - T, t_0 + T] \subset J$ par l'unicité vue précédemment, donc J est **non vide**.
Comme $J = (\widetilde{y_1} - \widetilde{y_2})^{-1}(0)$ (en notant $\widetilde{y_i}$ la restriction de y_i à $I_1 \cap I_2$), J est **fermé**.
Soit $t_1 \in J$, alors y_1 et y_2 sont solutions du nouveau problème de Cauchy

$$(P') : \begin{cases} y'(t) = f(t, y(t)) \\ y(t_1) = y_1(t_1) \end{cases}$$

En adaptant le début de la preuve, on voit qu'on a égalité de y_1 et y_2 sur un voisinage $[t_1 - T', t_1 + T']$ de t_1.
Donc J est **ouvert**.

Comme $I_1 \cap I_2$ est connexe, on a $J = I_1 \cap I_2$, ce qui donne l'unicité locale.

- Construction de la solution maximale

On considère $J = \bigcup_{(\tilde{I}, y) \in S} \tilde{I}$ avec S l'ensemble des $(\tilde{I}, y)$ solution du problème de Cauchy. On définit alors y^* sur J par $y^*(x) = y(x)$ si $(\tilde{I}, y)$ est solution et $x \in I$. On peut faire ça par unicité locale.
La solution y^* est ainsi maximale. □

Remarques : • Si la condition local-lipschitz n'est pas vérifiée, on n'a plus l'unicité.

$$\begin{cases} y'(t) = \sqrt{y(t)} \\ y(0) = 0 \end{cases}$$

On trouve à ce problème une infinité de solutions de la forme $y(t) = \dfrac{(t - t_0)^2}{4} \mathbb{1}_{[t_0, +\infty[}(t)$.
• Si f est seulement continue, le théorème de Cauchy-Arzela-Peano donne l'existence d'une solution. Ce théorème se prouve avec Ascoli et Schauder.

Chapitre 41

Théorème de Frobenius-Zolotarev

Références : Beck, Malick, Peyré, *Objectif Agrégation*, p.251

Théorème (Frobenius-Zolotarev)**.**

Soient p un nombre premier impair et $n \in \mathbb{N}^*$. On a alors :

$$\forall u \in \mathrm{GL}_n(\mathbb{F}_p),\ \varepsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où ε désigne la signature de u vu comme permutation de l'ensemble $\mathbb{F}_p^n$. [a]

a. Celle-ci est bien définie car $\mathrm{GL}_n(\mathbb{F}_p) \hookrightarrow \mathcal{S}(\mathbb{F}_p^n) \simeq \mathcal{S}_{p^n} \simeq \mathcal{S}(\mathbb{F}_{p^n})$ et ε est un morphisme de groupes donc n'est pas affecté par le choix des isomorphismes précédents.

On rappelle la définition du symbole de Legendre. Soit p un nombre premier et a un entier quelconque, alors on a :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si} \quad a \equiv 0[p] \\ 1 & \text{si} \quad a \text{ est un carré dans } \mathbb{F}_p \\ -1 & \text{sinon} \end{cases} .$$

Le but de la démonstration est de factoriser la signature. Nous allons faire cela en deux étapes.

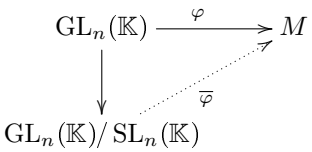
Lemme.

Soient $\mathbb{K}$ un corps et M un groupe abélien (on suppose que $\mathbb{K} \neq \mathbb{F}_2$ ou bien que $n > 2$). Pour tout morphisme $\varphi : \mathrm{GL}_n(\mathbb{K}) \to M$, il existe un unique morphisme $\delta : \mathbb{K}^* \to M$ tel que l'on ait : $\varphi = \delta \circ \det$.

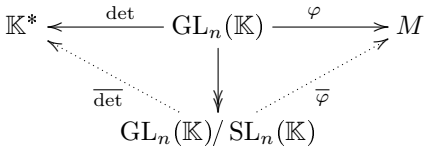
Démonstration. Puisque $\mathbb{K} \neq \mathbb{F}_2$, on a : $D(\mathrm{GL}_n(\mathbb{K})) = \mathrm{SL}_n(\mathbb{K})$. Pour tout x, y dans $\mathrm{GL}_n(\mathbb{K})$, on a :

$$\varphi([x,y]) = [\varphi(x), \varphi(y)] = e \quad ,$$

car M est un groupe abélien. Ainsi tous les commutateurs de $\mathrm{GL}_n(\mathbb{K})$ sont dans le noyau de φ. Or les commutateurs engendrent le groupe dérivé. Ainsi le groupe dérivé de $\mathrm{GL}_n(\mathbb{K})$ est inclus dans le noyau de φ. D'après la propriété universelle du quotient, il existe un unique morphisme $\overline{\varphi}$ qui rend le diagramme suivant commutatif.



De plus le noyau du morphisme det : $\mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$ est exactement $\mathrm{SL}_n(\mathbb{K})$. D'après la propriété universelle et le premier théorème d'isomorphisme, il existe un unique isomorphisme $\overline{\det}$ qui fasse commuter le diagramme suivant :



On pose $\delta = \overline{\varphi} \circ \overline{\det}^{-1}$. On obtient l'égalité voulue.

Pour l'unicité, on sait que le déterminant est surjectif, donc toute l'image de δ est fixée par φ. □

Dans notre cas, pour M on a le groupe $\{\pm 1\}$ qui est abélien. On dispose donc d'un unique morphisme δ tel que l'on ait : $\varepsilon = \delta \circ \det$. Il faut à présent montrer que δ est le symbole de Legendre.

Lemme.

Soit p un nombre premier impair. Le symbole de Legendre est l'unique morphisme non trivial de $\mathbb{F}_p^*$ dans $\{\pm 1\}$.

Démonstration. Le symbole de Legendre est bien un morphisme de groupe entre $\mathbb{K}^*$ et $\{\pm 1\}$. En effet, pour $a \in \mathbb{F}_p^*$, on a $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$. De plus, ce n'est pas un morphisme trivial. En effet, l'ensemble des carrés de $\mathbb{F}_p^*$ est égal à l'image du morphisme $\psi : x \in \mathbb{K}^* \mapsto x^2$. Le noyau de ce morphisme est $\{\pm 1\}$ et donc d'après le premier théorème d'isomorphisme, il n'y a que $\dfrac{p-1}{2}$ carrés dans $\mathbb{F}_p^*$.

Réciproquement, soit $\alpha : \mathbb{F}_p^* \to \{\pm 1\}$ un morphisme non trivial. D'après le premier théorème d'isomorphisme, le noyau de α est un sous-groupe d'indice 2 de $\mathbb{F}_p^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Or pour tout diviseur d de $p-1$ il existe un unique sous-groupe de $\mathbb{Z}/(p-1)\mathbb{Z}$ d'indice d[1] . On note H cet unique sous-groupe d'indice 2. Soit x un élément de $\mathbb{F}_p^* \backslash H$. On a alors la partition suivante : $\mathbb{F}_p^* = H \bigsqcup xH$. On a alors :

$$\alpha(g) = \begin{cases} 1 & \text{si } g \in H \\ -1 & \text{sinon} \end{cases}$$

Le morphisme α est donc entièrement déterminé. Il existe donc au plus un morphisme non trivial entre $\mathbb{F}_p^*$ et $\{\pm 1\}$, c'est le symbole de Legendre. □

Pour conclure il faut encore montrer que δ est non trivial. Pour cela il suffit d'exhiber un automorphisme dans $\mathrm{GL}_n(\mathbb{F}_p)$ de signature -1. En temps que $\mathbb{F}_p$-espaces vectoriel, $\mathbb{F}_p^n$ et $\mathbb{F}_{p^n}$ sont isomorphes. Il suffit donc de trouver une bijection $\mathbb{F}_p$-linéaire de $\mathbb{F}_{p^n}$ de signature -1. Soit g un générateur du groupe cyclique $\mathbb{F}_{p^n}^*$. La permutation $x \mapsto gx$ agit comme le (p^n-1)-cycle $(g, g^2, \ldots, g^{p^n-1})$. Cette permutation est de signature -1 car $p^n - 1$ est pair. Ce qui achève la démonstration.

Corollaire.

Soit p un nombre premier impair, on a : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ et $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Démonstration. On définit l'isomorphisme u suivant :

$$\begin{array}{rccc} u : & \mathbb{F}_p & \to & \mathbb{F}_p \\ & x & \mapsto & 2x \end{array}$$

1. Car il existe un unique sous groupe d'ordre $\dfrac{n}{d}$, voir Calais, p.100

Son déterminant est égal à 2. Il ne reste plus qu'à calculer la signature de la permutation engendrée. Pour cela il suffit de compter le nombre d'inversion. [2]

x	0	1	2	...	$\frac{p-1}{2}$	$\frac{p+1}{2}$	...	$p-2$	$p-1$
$u(x)$	0	2	4	...	$p-1$	1	...	$p-4$	$p-2$

On remarque qu'il n'y a pas d'inversion entre deux éléments inférieurs à $\frac{p-1}{2}$ ou supérieurs à $\frac{p+1}{2}$.
Soit $k \geqslant \frac{p+1}{2}$, k voit sa position relative à $p-k$ éléments inversée par u. Le nombre d'inversions est donc

$$\sum_{k=\frac{p+1}{2}}^{p-1} p-k = \sum_{l=0}^{\frac{p-1}{2}} l = \frac{p^2-1}{8} \quad .$$

En appliquant le théorème de Frobenius-Zolotarev, on obtient donc le résultat.

Pour le deuxième résultat du théorème, on peut faire le même raisonnement avec $u : x \mapsto -x$. On peut alors soit compter le nombre d'inversions (en bidouillant un peu), soit se rendre compte que cette application s'écrit comme un produit de $\frac{p-1}{2}$ transpositions. □

Remarques : • Dans le Objectif agrégation, ils prennent $n > 2$, mais comme p est choisi impair, on peut prendre $n \geqslant 1$, ce qui nous autorise à utiliser Frobenius-Zolotarev dans le corollaire.
• Montrons que $D(\mathrm{GL}_n(\mathbb{K})) = \mathrm{SL}_n(\mathbb{K})$ pour $\mathbb{K}$ un corps à au moins 3 éléments et $n \geqslant 2$. (FGNal2)
On note $D_i(a)$ la matrice de dilatation avec comme coefficient a sur la i-ème ligne de la diagonale. $T_{i,j}(b)$ est la transvection de coefficient b.
Par des calculs, on remarque que

$$[D_i(a), T_{i,j}(b)] = T_{i,j}((a-1)b).$$

Comme $(a-1)b$ parcourt $\mathbb{K}$ si a est différent de 0 et 1 (d'où la nécessité d'avoir au moins trois éléments dans le corps), toute transvection est un commutateur.
$\mathrm{SL}_n(\mathbb{K})$ est engendré par les transvections donc cela termine la preuve.
Remarquons que ce résultat est aussi vrai pour $\mathbb{K} = \mathbb{F}_2$ et $n \geqslant 3$.
• Une autre application consiste à calculer la signature du morphisme de Frobenius F sur $\mathbb{F}_q$.
On sait que F est d'ordre n. La théorie de Galois donne l'existence d'un élément x de $\mathbb{F}_q$ tel que $(x, F(x), ..., F^{n-1}(x))$ forme une base de $\mathbb{F}_q$. La matrice de F dans cette base est une simple matrice de permutation dont le déterminant est $(-1)^{n+1}$.
Le théorème de Frobenius Zolotarev donne alors, en sachant que $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,

$$\varepsilon(F) = \left(\frac{(-1)^{n+1}}{p}\right) = (-1)^{\frac{(p-1)(n+1)}{2}}.$$

Adapté du travail de Baptiste Huguet et complété par les recherches de Mario Goncalves Lamas et Anne-Elisabeth Falq.

2. En effet, c'est clair au vu de la définition : $\varepsilon(u) = \prod_{i \neq j} \frac{u(j)-u(i)}{j-i} \in \{\pm 1\}$.

Chapitre 42

Théorème de Grothendieck

Références : : Zavidovique, *Un Max de Math*, p180
Rudin, *Analyse Fonctionelle*, p114 (pour la correction de la fin de la preuve)

Théorème.

Soit (Ω, μ) un espace de probabilité. Soit S un sous espace vectoriel fermé de $L^p(\mu)$ qui soit inclus dans $L^\infty(\mu)$. Alors S est de dimension finie.

Démonstration. Le principe de la preuve est de se ramener dans le cadre hilbertien de $L^2(\mu)$ afin de pouvoir utiliser les propriétés associées : bases hilbertiennes, théorème de Pythagore...

- Montrons qu'il existe un $K > 0$ tel que : $\forall f \in S, \|f\|_\infty \leqslant K \|f\|_p$.

On définit l'application

$$\begin{array}{rccc} i : & (S, \|.\|_\infty) & \to & (S, \|.\|_p) \\ & f & \mapsto & f \end{array} .$$

Il s'agit de montrer que i est une application ouverte. L'application i est linéaire et bijective. Pour tout f dans S[1], $|f(x)| \leqslant \|f\|_\infty$ *µpp*. Ainsi, on a :

$$\|f\|_p = \left(\int_\Omega |f|^p \mathrm{d}\mu \right)^{1/p} \leqslant \left(\int_\Omega \|f\|_\infty^p \, \mathrm{d}\mu \right)^{1/p} = \|f\|_\infty \, (\mu(\Omega))^{1/p} = \|f\|_\infty \quad .$$

Ce qui montre que i est continue[2]. De plus S étant fermé dans l'espace de Banach $L^p(\mu)$, alors $(S, \|.\|_p)$ est lui-même un espace de Banach. Soit une suite $(f_n)_{n\in\mathbb{N}}$ dans S qui converge au sens de $L^\infty(\mu)$ vers une fonction $f \in L^\infty(\mu)$. Par continuité de l'application i, la suite $(i(f_n))_{n\in\mathbb{N}}$ converge vers $i(f)$ au sens de $L^p(\mu)$. Or $(S, \|.\|_p)$ est un espace de Banach, donc $f \in S$. Donc S est fermé dans $L^\infty(\mu)$. Ainsi $(S, \|.\|_\infty)$ est aussi un espace de Banach.

L'application i est donc une application linéaire continue surjective entre deux espaces de Banach. D'après le théorème de l'application ouverte, i est donc ouverte, *id est* il existe $K > 0$ tel que $\forall f \in S, \|f\|_\infty \leqslant K \|f\|_p$.

- Montrons qu'il existe un $M > 0$ tel que : $\forall f \in S, \|f\|_\infty \leqslant M \|f\|_2$.

Comme on travaille sur un espace de probabilité, $L^\infty(\mu)$, et donc S, est inclus dans $L^2(\mu)$. Si $p = 2$, le résultat est immédiat. Sinon, on doit distinguer les cas.

Si $p < 2$. On peut effectuer l'inégalité de Hölder avec $\dfrac{2}{p} > 1$. Pour toute fonction $f \in S$, on a :

$$\|f\|_p^p = \int_\Omega |f|^p \mathrm{d}\mu \leqslant \left(\int_\Omega |f|^{p.2/p} \mathrm{d}\mu \right)^{p/2} (\mu(\Omega))^{1-p/2} = \|f\|_2^p \quad .$$

En passant à la racine p-ième et en utilisant l'étape précédente, on obtient : $\forall f \in S, \|f\|_\infty \leqslant K \|f\|_2$.

1. on confondra f et un de ses représentants.
2. On dit que l'injection $L^\infty \hookrightarrow L^p$ est topologique

Si $p > 2$. Soit $f \in S$, on a : $|f(x)|^p \leqslant \|f\|_\infty^{p-2} |f(x)|^2$ μpp. On a donc :

$$\|f\|_p^p = \int_\Omega |f|^p(x)\mathrm{d}\mu(x) \leqslant \|f\|_\infty^{p-2} \int_\Omega |f|^2(x)\mathrm{d}\mu(x) = \|f\|_\infty^{p-2} \|f\|_2^2 \quad .$$

En utilisant la première étape, on obtient : $\forall f \in S, \|f\|_\infty \leqslant K^{p/2} \|f\|_2$.

On pose $M = \max(K, K^{p/2})$. On a alors : $\forall f \in S, \|f\|_\infty \leqslant M \|f\|_2$.

• Soient n un entier et $(f_i)_{1\leqslant i\leqslant n}$ une famille de S, orthonormée dans $L^2(\mu)$. Montrons que pour tout n-uplet $(c_1, \ldots, c_n) \in \mathbb{R}^n$ et pour μ presque tout $x \in \Omega$ on a :

$$\left|\sum_{i=1}^n c_i f_i(x)\right| \leqslant M\sqrt{\sum_{i=1}^n c_i^2} \quad .$$

On prend les c_i dans $\mathbb{Q}$ qui est un ensemble dénombrable dense (pour la norme 2) dans $\mathbb{R}$.
Comme $\mathbb{Q}^n$ est dénombrable, on a l'existence de $\Omega' \subset \Omega$ de mesure pleine tel que pour tout $(c_i)_i$ dans $\mathbb{Q}^n$ et pour tout $x \in \Omega'$ on a :[3]

$$\left|\sum_{i=1}^n c_i f_i(x)\right| \leqslant \left\|\sum_{i=1}^n c_i f_i\right\|_\infty \quad .$$

Or d'après l'étape précédente et comme $\sum_{i=1}^n c_i f_i \in S$ (car S est un espace vectoriel),

$$\left\|\sum_{i=1}^n c_i f_i\right\|_\infty \leqslant M \left\|\sum_{i=1}^n c_i f_i\right\|_2 \quad .$$

De plus d'après le théorème de Pythagore, on a :

$$\left\|\sum_{i=1}^n c_i f_i\right\|_2^2 = \sum_{i=1}^n c_i^2 \|f_i\|_2^2 \quad .$$

Comme la famille $(f_i)_{1\leqslant i\leqslant n}$ est normée, alors pour tout $1 \leqslant i \leqslant n, \|f_i\|_2^2 = 1$. Ainsi, on a :

$$\forall (c_i)_i \in \mathbb{Q}^n, \forall x \in \Omega', \left|\sum_{i=1}^n c_i f_i(x)\right| \leqslant M\sqrt{\sum_{i=1}^n c_i^2} \quad .$$

Puis comme $(c_i)_i \mapsto \sum_{i=1}^n c_i f_i(x)$ est continue à x fixé (car polynomiale en les c_i) et $(c_i)_i \mapsto \sqrt{\sum_{i=1}^n c_i^2}$ l'est aussi, on a par densité :

$$\forall (c_i)_i \in \mathbb{R}^n, \forall x \in \Omega' \left|\sum_{i=1}^n c_i f_i(x)\right| \leqslant M\sqrt{\sum_{i=1}^n c_i^2} \quad .$$

• Conclusion.
Pour tout $x \in \Omega'$, on pose pour $1 \leqslant i \leqslant n, c_i = f_i(x)$. On a alors :

$$\sum_{i=1}^n f_i(x)^2 \leqslant M\sqrt{\sum_{i=1}^n f_i(x)^2}$$
$$\left(\sum_{i=1}^n f_i(x)^2\right)^2 \leqslant M^2 \sum_{i=1}^n f_i(x)^2$$
$$\sum_{i=1}^n f_i(x)^2 \leqslant M^2$$

3. En effet, pour tout (c_i) dans $\mathbb{Q}^n$, on dispose de $\Omega_{(c_i)_i}$ tel que l'inégalité soit vérifié. Il suffit donc de vérifier que l'intersection dénombrable de mesurables pleins est pleine, ou de même qu'une union dénombrable de négligeables est négligeable.
Or $\mu\left(\bigcup \mathcal{N}_k\right) \leqslant \sum \mu(\mathcal{N}_k) = 0$, donc c'est bon !

Ceci étant vrai pour μ presque tout $x \in \Omega$, on peut intégrer sur Ω.

$$\int_\Omega \sum_{i=1}^{n} f_i(x)^2 \mathrm{d}\mu(x) \leqslant M^2 \mu(\Omega)$$
$$\sum_{i=1}^{n} \|f_i\|_2^2 \leqslant M^2$$
$$n \leqslant M^2$$

Toute famille orthonormée de S est donc de taille finie, inférieure à M^2. Ainsi S est de dimension finie, inférieure à M^2. □

Remarques : • On peut donner un contre-exemple à l'inégalité fausse du Zavidovique. On se place sur $[0,1]$. On prend $f_1 = 1$ et $f_2 = -\mathbb{1}_{]0,1]}$.
Alors pour tout $x \in [0,1]$, $|f_i|(x) \leqslant \|f_i\|_\infty$, mais

$$|f_1 + f_2|(0) > \|f_1 + f_2\|_\infty .$$

• Le théorème de l'application ouverte est une des principales applications du théorème de Baire. Celui-ci permet d'ailleurs de montrer le théorème de Banach-Steinhaus.
En application du théorème de l'application ouverte, il y a le théorème des isomorphismes de Banach (Tout opérateur continu bijectif sur des Banach est bicontinu.), le théorème d'équivalence des normes comparables, le théorème du graphe fermé et la non-surjectivité de la TF de L^1 dans $\mathcal{C}^0$.

Adapté du travail de Baptiste Huguet.

Chapitre 43

Théorème de Liapounov

Références : Rouvière, *Petit guide de calcul différentiel*, p143

Théorème.

On se donne y une fonction de $\mathbb{R}^+$ définie comme solution du système $\begin{cases} y' &= f(y) \\ y(a) &= x \end{cases}$ où $f : \mathbb{R}^n \to \mathbb{R}^n$ est $\mathcal{C}^1$ et $f(a) = 0$. On suppose que $\Re(\mathrm{Sp}(Df(a))) \subset \mathbb{R}^{-*}$, alors a est point d'équilibre attractif du système différentiel.

On ne fera la preuve que dans le cas $a = 0$ pour simplifier.

Démonstration. On pose z la solution du système linéarisé $\begin{cases} z' &= Az \\ z(0) &= x \end{cases}$ avec $A := Df(0)$.
L'idée de la preuve est de transporter l'asymptotique stabilité de 0 du système linéarisé pour le vrai système différentiel, et cela en créant une nouvelle norme appropriée.

- On appelle $(\lambda_i)_{1 \leqslant i \leqslant k}$ les valeurs propres de A. Il existe $a > 0$ tel que pour tout i, $\Re(\lambda_i) < -a$.

On sait que $\mathbb{C}^n = \bigoplus_{1 \leqslant i \leqslant k} \mathrm{Ker}((A - \lambda_i I_n)^{m_i})$. Donc pour tout $x \in \mathbb{R}^n$, on peut le décomposer sous la forme $x = x_1 + ... + x_k$ avec $x_i \in \mathrm{Ker}((A - \lambda_i I_n)^{m_i})$.
On a $e^{tA} x_i = e^{t\lambda_i} e^{t(A - \lambda_i I_n)} x_i = e^{t\lambda_i} \sum_{p=0}^{m_i} \frac{t^p}{p!} (A - \lambda_i I_n)^p x_i$.
Donc en prenant une norme sous multiplicative, on a
$\left\| e^{tA} x_i \right\| \leqslant e^{t\Re(\lambda_i)} \sum_{p=0}^{m_i} \frac{|t|^p}{p!} \left\| A - \lambda_i I_n \right\|^p \|x_i\| \leqslant e^{-at} \sum_{p=0}^{m_i} \frac{|t|^p}{p!} \left\| A - \lambda_i I_n \right\|^p \max_j \|x_j\|$.
Il vient $\left\| e^{tA} x \right\| \leqslant \left(\sum_{i=1}^{k} \sum_{p=0}^{m_i} \frac{|t|^p}{p!} \left\| A - \lambda_i I_n \right\|^p \right) e^{-at} \max_j \|x_j\|$.
On a alors $\left\| e^{tA} x \right\| \leqslant CP(|t|) e^{-at} \|x\|$ avec P un polynôme et C une constante d'équivalence qui va bien entre les normes $\|.\|$ et $\|x\|_* := \max \|x_j\|$.

Comme $z(t) = e^{tA} x$ est la solution du linéarisé, on a $\|z(t)\| \leqslant CP(|t|) e^{-at} \|x\|$, donc 0 est un point d'équilibre attractif du linéarisé.

- On définit $b(x, y) := \int_0^{\infty} (e^{tA} x, e^{tA} y) \mathrm{d}t$.

Cette fonction est bien définie car $|(e^{tA} x, e^{tA} y)| \leqslant \left\| e^{tA} x \right\| \left\| e^{tA} y \right\| \leqslant C^2 e^{-2at} P(|t|)^2 \|x\| \|y\|$ qui est intégrable.
On vérifie que c'est un produit scalaire (car e^{tA} est inversible) et on pose $q(x) = b(x, x)$ la forme quadratique associée.

- On veut montrer qu'il existe α, $\beta > 0$ tels que $q(y) \leqslant \alpha \Rightarrow q(y)' \leqslant -\beta q(y)$.

→ On sait que $\nabla q(x)(y) = 2b(x,y)$ donc $\nabla q(x)(Ax) = 2b(x,Ax) = \int_0^\infty 2(e^{tA}x, e^{tA}Ax)\mathrm{d}t$.
Or $2(e^{tA}x, e^{tA}Ax) = \frac{\mathrm{d}(\|e^{tA}x\|^2)}{\mathrm{d}t}$, donc $\nabla q(x)(Ax) = 2b(x,Ax) = -\|x\|^2$.

→ On note $r(y) = f(y) - Ay$ la "différence" entre le système étudié et le linéarisé.
Alors $q(y)' = \nabla q(y).f(y) = 2b(y, f(y)) = 2b(y, A(y)) + 2b(y, r(y))$.
Or on a vu $2b(y, A(y)) = -\|y\|^2$, donc $q(y)' = -\|y\|^2 + 2b(y, r(y))$.

→ Soit $\varepsilon > 0$, on a $r(y) = f(y) - Ay = f(y) - f(0) - Df(0)y$. Par définition de la différentielle, $r(y) = o(\sqrt{q(y)})$ donc il existe $\alpha > 0$ tel que $q(y) \leqslant \alpha \Rightarrow \sqrt{q(r(y))} \leqslant \varepsilon\sqrt{q(y)}$ (on choisit juste d'exprimer ce fait avec la norme $\sqrt{q}$.).
On a alors par Cauchy-Schwarz : $|b(y, r(y))| \leqslant \sqrt{q(y)}\sqrt{q(r(y))}$. Donc si $q(y) \leqslant \alpha$, alors $|b(y, r(y))| \leqslant \varepsilon q(y)$.
D'autre part, comme $\sqrt{q}$ et $\|.\|$ sont équivalentes, il existe C tel que $Cq(y) \leqslant \|y\|^2$.
On en déduit donc que si $q(y) \leqslant \alpha$, $q(y)' = -\|y\|^2 + 2b(y, r(y)) \leqslant -(C - 2\varepsilon)q(y)$. On note $\beta = C - 2\varepsilon$ et on choisit ε assez petit pour que $\beta > 0$.

• Pour finir, montrons que si $q(x) \leqslant \alpha$ alors pour tout $t \in \mathbb{R}^+$, $q(y(t)) \leqslant \alpha$. En particulier, la solution $y(t)$ sera globale car bornée.
En effet, si ce n'était pas le cas, on aurait l'existence de $t_0 > 0$ tel que $q(y(t_0)) = \alpha$ et pour $t > t_0$ assez proche de t_0, on ait $q(y(t)) > \alpha$. Or $q(y)'(t_0) \leqslant -\beta q(y) < 0$, donc $q(y)$ est décroissante dans un voisinage de t_0 par continuité, donc ce serait absurde.

• Conclusion : si $q(x) \leqslant \alpha$, on a pour tout $t \in \mathbb{R}^+$, $q(y(t)) \leqslant \alpha$, donc $q(y)'(t) \leqslant -\beta q(y)(t)$. Le lemme de Gronwall donne alors $q(y)(t) \leqslant e^{-\beta t}q(x)$.
Il est maintenant clair au vu de cette formule que 0 est un point d'équilibre attractif du système différentiel.
□

Remarque : • On peut prouver que si $Df(0)$ possède une valeur propre de partie réelle strictement positive, alors 0 est instable pour le système différentiel.
• Une application de ce théorème est l'équation de Van der Pol, présente dans le X-ENS - analyse 4.
• Il est bon de connaître quelques contre-exemples sur ce sujet dans le cas où on a une valeur propre de partie réelle nulle. On en donne quelques-uns ici partant du point $(0,0)$.

— NL instable, L instable :
$$(\text{NL}) : \begin{cases} x' = y \\ y' = -y^2 \end{cases} \text{ et } (\text{L}) : \begin{cases} X' = Y \\ Y' = 0 \end{cases}$$
On a
$$(\text{NL}) : \begin{cases} x(t) = x_0 + \ln(1 + y_0 t) \\ y(t) = \dfrac{y_0}{1 + y_0 t} \end{cases} \text{ et } (\text{L}) : \begin{cases} X(t) = X_0 + Y_0 t \\ Y(t) = Y_0 \end{cases}$$

— NL stable, L instable :
$$(\text{NL}) : \begin{cases} x' = y \\ y' = -y^{\frac{3}{2}} \end{cases} \text{ et } (\text{L}) : \begin{cases} X' = Y \\ Y' = 0 \end{cases}$$
On a
$$(\text{NL}) : \begin{cases} x(t) = x_0 + 2\sqrt{y_0} - \dfrac{4\sqrt{y_0}}{2 + \sqrt{y_0}t} \\ y(t) = \left(\dfrac{2\sqrt{y_0}}{2 + \sqrt{y_0}t}\right)^2 \end{cases} \text{ et } (\text{L}) : \begin{cases} X(t) = X_0 + Y_0 t \\ Y(t) = Y_0 \end{cases}$$

— NL stable, L stable :
$$(\text{NL}) : \{x' = -x^3 \text{ et } (\text{L}) : \{X' = 0$$
On a
$$(\text{NL}) : \left\{x(t) = \frac{x_0}{\sqrt{1 + 2x_0^2 t}} \text{ et } (\text{L}) : \{X(t) = X_0\right.$$

— NL instable, L stable :
$$(\text{NL}) : \{x' = x^3 \text{ et } (\text{L}) : \{X' = 0$$
On a
$$(\text{NL}) : \left\{x(t) = \frac{x_0}{\sqrt{1 - 2x_0^2 t}} \text{ et } (\text{L}) : \{X(t) = X_0\right.$$

Chapitre 44

Théorème de Molien

Références : Leichtnam, *exercices corrigés de Mathématiques posés à l'oral des concours de Polytechnique et des ENS - Tome algèbre et géométrie*, p 95

Théorème.

On note $A = \mathbb{C}[X_1, ..., X_n]$ et A_k l'espace des polynômes homogènes de A de degré k. On se donne G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$.
Pour $g \in G$, on pose $\sigma_g : \begin{array}{ccc} A & \to & A \\ P(X) & \mapsto & P({}^t gX) \end{array}$ (où on considère X comme un vecteur colonne), alors $\forall k \in \mathbb{N}$, σ_g induit un automorphisme de A_k et si on note $A_k^G := \{P \in A_k, \forall g \in G, \sigma_g(P) = P\}$, $a_k = \dim(A_k)$ et $a_k(G) = \dim(A_k^G)$, alors on a l'égalité suivante dans $\mathbb{C}[[Z]]$:

$$\frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I_n - Zg)} = \sum_{k=0}^{\infty} a_k(G) Z^k.$$

Démonstration. • Montrons que σ_g induit un automorphisme sur chaque A_k.
Il est déjà clair que σ_g est un morphisme d'algèbre. [1] Puis on remarque que $\sigma_{gg'} = \sigma_g \circ \sigma_{g'}$ et $\sigma_e = Id$. On a ainsi $(\sigma_g)^{-1} = \sigma_{g^{-1}}$ et $\sigma_g \in \mathrm{Aut}(A)$.
Enfin σ_g envoie un monôme de degré k sur un polynôme homogène de degré k, donc $\sigma_g(A_k) \subset A_k$. On peut donc construire la restriction de σ_g à A_k. Or σ_g est injectif (sur A donc sur A_k), par égalité des dimensions, σ_g induit un automorphisme sur chaque A_k.
En fait, on a montré que $\sigma : \begin{array}{ccc} G & \to & GL(A) \\ g & \mapsto & \sigma_g \end{array}$ définit une représentation de G et que l'on peut définir les représentations induites $\sigma_{|A_k}$ sur les A_k [2].

• Montrons à présent que $\dfrac{1}{\det(I_n - Zg)} = \displaystyle\sum_{k=0}^{\infty} \chi_k(g) Z^k$ où $\chi_k(g) = \mathrm{Tr}(\sigma_{|A_k}(g))$ est le caractère de $\sigma_{|A_k}$ en g.
Le groupe G est fini, donc par le théorème de Lagrange, $\forall g \in G$, $g^{|G|} = e$. Il en résulte que le polynôme $X^{|G|} - 1$ annule toutes les matrices de G, mais il est scindé à racines simples, donc pour $g \in G$, il existe $u \in \mathrm{GL}_n(\mathbb{C})$ telle que ugu^{-1} soit diagonale. On a $\chi_k(g) = \mathrm{Tr}(\sigma_{|A_k}(g)) = \mathrm{Tr}(\sigma_{|A_k}(u)\sigma_{|A_k}(g)\sigma_{|A_k}(u^{-1})) = \chi_k(ugu^{-1})$. [3] En fait, on peut juste dire que les caractères sont des fonctions centrales, ce qui évite d'écrire ces formules.
On peut donc supposer g diagonale : $g = \mathrm{Diag}(\lambda_1, ..., \lambda_n)$. Alors

$$\frac{1}{\det(I_n - Zg)} = \prod_{i=1}^{n} \frac{1}{1 - \lambda_i Z} = \prod_{i=1}^{n} \sum_{p=0}^{\infty} \lambda_i^p Z^p = \sum_{p=0}^{\infty} v_p Z^p$$

avec $v_p = \displaystyle\sum_{k_1 + ... + k_n = p} \lambda_1^{k_1} ... \lambda_n^{k_n}$.
Puis on remarque que pour $k_1 + ... + k_n = p$, on a $\sigma_{|A_p}(g)(X_1^{k_1} ... X_n^{k_n}) = (\lambda_1^{k_1} ... \lambda_n^{k_n}) X_1^{k_1} ... X_n^{k_n}$, donc si on prend

1. Attention, $\sigma_h(P({}^t gX)) = P({}^t g {}^t hX)$. C'est l'indéterminée X qui est multipliée par ${}^t h$!
2. C'est en fait une action de groupe.
3. On peut faire cela en étendant l'ensemble de définition de σ à $\mathrm{GL}_n(\mathbb{C})$. On vérifie que les identités faites auparavant sont toujours vérifiées.

la base de A_k constituée des $X_1^{k_1}...X_n^{k_n}$ avec $k_1 + ... + k_n = p$, alors on voit que $\chi_p(g) = \mathrm{Tr}(\sigma_{|A_p}(g)) = v_p$.
La formule précédente donne donc $\dfrac{1}{\det(I_n - Zg)} = \sum_{k=0}^{\infty} \chi_k(g) Z^k$.

- Pour conclure, on utilise le lemme suivant.

Lemme.

Soit $\rho : G \to \mathrm{GL}(V)$ une représentation d'un groupe G fini avec V un $\mathbb{C}$-espace vectoriel de dimension finie, alors

$$\dim(V^G) = \frac{1}{|G|} \sum_{g \in G} \chi(g).$$

Si on applique ce lemme à $\sigma_{[A_k}$, on a $\dim(A_k^G) = a_k(G) = \dfrac{1}{|G|} \sum_{g \in G} \chi_k(g)$.

On a donc

$$\frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I_n - Zg)} = \frac{1}{|G|} \sum_{g \in G} \sum_{k=0}^{\infty} \chi_k(g) Z^k = \sum_{k=0}^{\infty} \frac{1}{|G|} \sum_{g \in G} \chi_k(g) Z^k = \sum_{k=0}^{\infty} a_k(G) Z^k.$$

□

Prouvons à présent le lemme.

Démonstration. On pose $p_G = \dfrac{1}{|G|} \sum_{g \in G} \rho(g) \in \mathrm{GL}(V)$ l'opérateur de Reynolds.[4] Alors en utilisant la bijection $h \mapsto gh$, on a $\rho(h) p_G(v) = p_G(v)$, donc $p_G(V) \subset V^G$. Comme $p_G(v) = v$ pour $v \in V^G$, on a $p_G(V) = V^G$.
De plus, en sommant, on a $p_G \circ p_G = p_G$, donc p_G est un projecteur sur V^G. En trouvant une bonne base pour le projecteur, on a vite $\mathrm{rg}(p_G) = \mathrm{Tr}(p_G) = \dim(V^G)$, donc, en appliquant l'application trace à p_G, on a $\dim(V^G) = \dfrac{1}{|G|} \sum_{g \in G} \chi(g)$. □

Remarques : • Le théorème de Molien donne le lien entre un objet simple : le déterminant, et les $a_k(G)$ qui sont les dimensions des sous-espaces d'invariants.
• La série des invariants est nommée série de Molien.
• On a l'impression qu'il serait plus naturel de poser $\sigma_g(P)(X) = P(gX)$ mais ça n'est pas le cas ! Par exemple, prenons le 3-cycle (123). Sa matrice de permutation associée est

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

Si on se place dans $\mathbb{C}[X_1, X_2, X_3]$, on a

$$P(AX) = \begin{pmatrix} X_3 \\ X_1 \\ X_2 \end{pmatrix} \text{ et } P({}^tAX) = \begin{pmatrix} X_2 \\ X_3 \\ X_1 \end{pmatrix}.$$

La deuxième approche donne la permutation intuitive.
• Faisons un exemple avec $\mathcal{S}_3$:
On considère l'action classique de $\mathcal{S}_3$ sur $\mathbb{R}^3$ pour obtenir un sous-groupe fini de matrices dans $\mathrm{GL}_3(\mathbb{C})$.
Alors $\det(I_3 - Z\sigma_e) = (1-Z)^3$, $\det(I_3 - Z\sigma_{(12)}) = \det \begin{pmatrix} 1 & -Z & 0 \\ -Z & 1 & 0 \\ 0 & 0 & 1-Z \end{pmatrix} = (1-Z)(1-Z^2)$ et enfin $\det(I_3 - Z\sigma_{(123)}) = \det \begin{pmatrix} -Z & 0 & 1 \\ 1 & -Z & 0 \\ 0 & 1 & -Z \end{pmatrix} = (1-Z^3)$. Comme le déterminant est invariant sur les classes de

4. Ouioui, c'est le même qu'en mécanique des fluides ! Mais au lieu de moyenner un flot sur l'action d'un groupe de translations en temps, on moyennise une représentation sur son groupe associé.

conjugaison, on a :

$$\sum_{k=0}^{\infty} a_k(\mathcal{S}_3)Z^k = \frac{1}{6}\left(\frac{1}{(1-Z)^3} + \frac{3}{(1-Z)(1-Z^2)} + \frac{2}{1-Z^3}\right) = \frac{1}{(1-Z)(1-Z^2)(1-Z^3)}.$$

En fait, on peut étendre ce résultat à $\mathcal{S}_n$ avec $\sum_{k=0}^{\infty} a_k(\mathcal{S}_n)Z^k = \frac{1}{(1-Z)...(1-Z^n)}$.

• Pour $\mathcal{A}_3$, on a

$$\sum_{k=0}^{\infty} a_k(\mathcal{A}_3)Z^k = \frac{1}{3}\left(\frac{1}{(1-Z)^3} + \frac{2}{1-Z^3}\right) = \frac{1+Z^3}{(1-Z)(1-Z^2)(1-Z^3)}.$$

On peut aussi étendre ce résultat à $\mathcal{S}_n$ avec $\sum_{k=0}^{\infty} a_k(\mathcal{A}_n)Z^k = \frac{1+Z^{\frac{n(n-1)}{2}}}{(1-Z)...(1-Z^n)}$.

• On peut montrer que si A^G est engendré par des polynômes homogènes f_1,...,f_r de degrés d_1,...,d_r, alors la série de Molien de G est le développement en série formelle d'une fraction rationnelle de la forme

$$\frac{F(Z)}{(1-Z^{d_1})...(1-Z^{d_r})}, \text{ avec } F \in \mathbb{Z}[Z].$$

Le théorème de Molien permet d'avoir une idée de où chercher les invariants.

• On rappelle que le fait que A^G soit engendré par des polynômes homogènes f_1,...,f_r veut juste dire que pour tout $P \in A$, il existe $Q \in \mathbb{C}[Y_1, ..., Y_r]$ tel que

$$P(X_1, ..., X_n) = Q(f_1(X_1, ..., X_n), ..., f_r((X_1, ..., X_n)).$$

A^G est engendrée en tant qu'**algèbre**.

• Pour l'exemple de $\mathcal{S}_n$, les invariants de A sont les polynômes symétriques et ils sont engendrés par les polynômes symétriques élémentaires $\Sigma_i = \sum_{1 \leqslant k_1 < ... < k_i \leqslant n} X_1^{k_1}...X_n^{k_n}$. On a bien $\deg(\Sigma_i) = i$, ce qui confirme les résultats précédents.

• Pour $\mathcal{A}_n$, on peut montrer que les polynômes invariants sous son action sont engendrés par les polynômes symétriques élémentaires et le polynôme de Vandermonde (de degré n). Il faut un peu modifier la fraction rationnelle précédente pour le faire apparaître en multipliant par $(1-Z^n)$ au numérateur et au dénominateur. C'est à dire

$$\sum_{k=0}^{\infty} a_k(\mathcal{A}_n)Z^k = \frac{(1+Z^{\frac{n(n-1)}{2}})(1-Z^n)}{(1-Z)...(1-Z^{n-1})(1-Z^n)^2}.$$

Chapitre 45

Théorème de Pascal

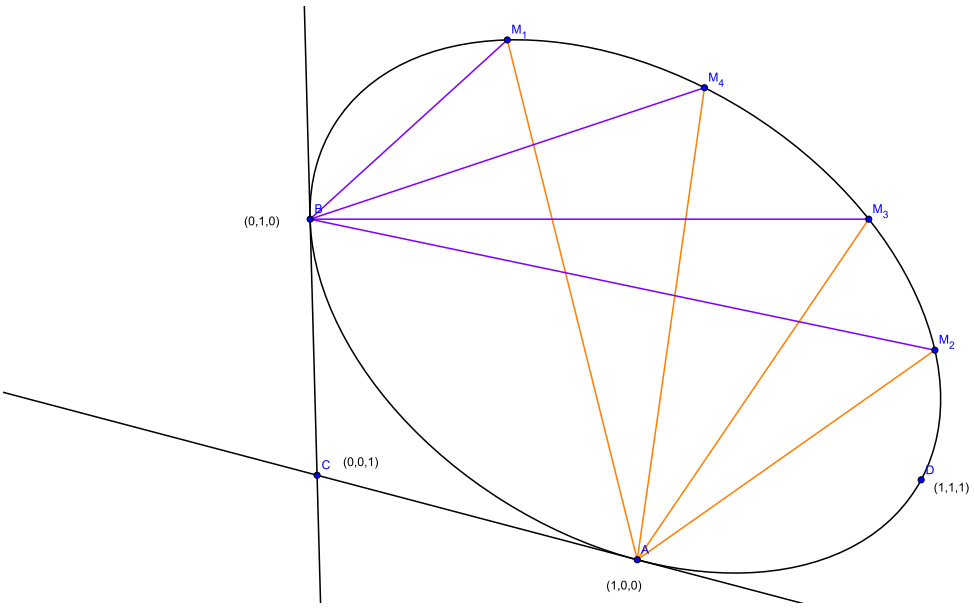
Références : Ladegaillerie, *Géométrie affine, projective, euclidienne et anallagmatique*, p 418 et p 420-421

Attention ! Ce développement utilise des notions complexes. Si on le fait, il faut préciser dans le plan ce qu'est le birapport de quatre droites concourantes, la formule du birapport dans le cas des droites utilisées ici, et le fait que les homographies de coniques sont fixées par l'image de trois points distincts.

Le birapport se définit sur une droite projective. Sur $\mathbb{P}_1(\mathbb{C})$, il n'y a pas de problème, mais sur $\mathbb{P}_2(\mathbb{R})$, il faut prendre les quatre points projectifs sur une droite projective. Cela revient à se fixer un point de $\mathbb{R}^2$, puis à regarder toutes les droites passant par ce point. Cela forme une droite projective. Quatre points projectifs de $\mathbb{P}_2(\mathbb{R})$ alignés sur une même droite projective sont donc quatre droites se coupant en un même point.

Proposition.

Soit $\mathcal{C}$ une conique propre et M_1, M_2, M_3, M_4 quatre points sur cette conique. Alors pour tout $M \in \mathcal{C}$ différent des M_i, le birapport $[(MM_1), (MM_2), (MM_3), (MM_4)]$ garde la même valeur. On le note $[M_1, M_2, M_3, M_4]$.

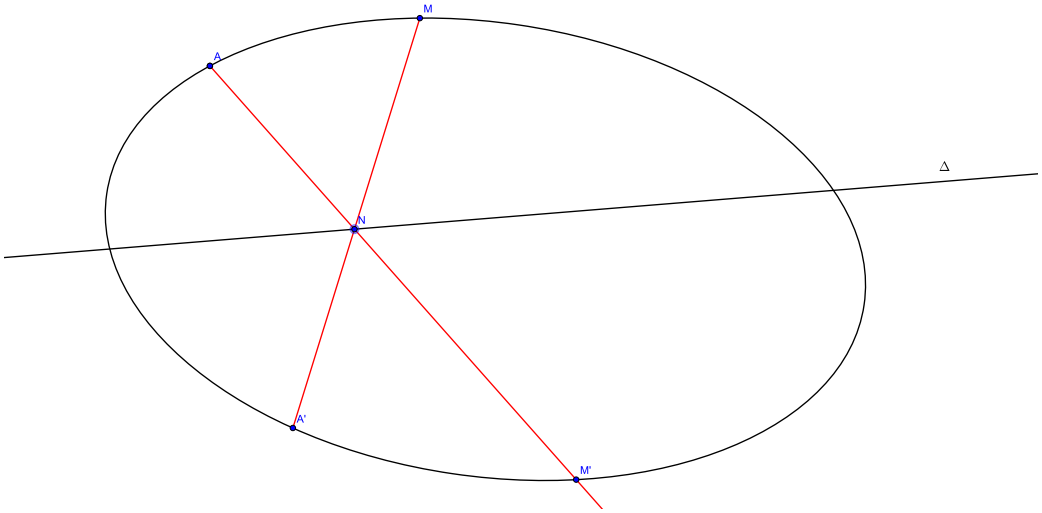


Démonstration. On se donne deux points A et B distincts sur $\mathcal{C}$ et non confondus avec les M_i, puis on construit C comme sur la figure et on prend un nouveau point D distincts des précédents n'importe où sur $\mathcal{C}$. On définit

le repère projectif (A, B, C, D) : $A(1,0,0)$, $B(0,1,0)$, $C(0,0,1)$ et $D(1,1,1)$. Alors l'équation de la conique dans ce repère est $XY - T^2 = 0$. [1]
La droite (AM_k) a une équation de la forme $aX + bY + cT = 0$. On évalue en A pour trouver $a = 0$, puis comme la droite $T = 0$ est (AB) et $B \neq M_k$, on a $b \neq 0$. On peut donc mettre l'équation de droite sous la forme $Y - \lambda_k T = 0$. De même, les droites (BM_k) peuvent se mettre sous la forme $X - \mu_k T = 0$.
On peut montrer [2] que $[(AM_1), (AM_2), (AM_3), (AM_4)] = [\lambda_1, \lambda_2, \lambda_3, \lambda_4]$ par une formule donnant le birapport sur un faisceau de deux droites. Il en va de même pour le birapport des (BM_i) et des μ_i.
Puis on remarque que les coordonnées de M_k vérifient $XY - T^2 = 0$ et $Y - \lambda_k T = 0$ donc ses coordonnées sont $(1 : \lambda_k^2 : \lambda_k)$. On a de même ses autres coordonnées avec les μ_k : $M_k(\mu_k^2 : 1 : \mu_k)$.
En comparant les coordonnées (multiplier le premier par μ_k et le second par λ_k), on s'aperçoit qu'il faut $\lambda_k \mu_k = 1$.
On pose l'homographie $h(z) = \dfrac{1}{z}$ alors $[\lambda_1, \lambda_2, \lambda_3, \lambda_4] = [h(\lambda_1), h(\lambda_2), h(\lambda_3), h(\lambda_4)] = [\mu_1, \mu_2, \mu_3, \mu_4]$.
Cela conclut la preuve. □

Proposition.

On appelle homographie d'une conique $\mathcal{C}$ toute bijection de $\mathcal{C}$ qui conserve le birapport.
Une homographie h d'une conique propre $\mathcal{C}$ possède un axe, c'est à dire une droite Δ telle que si on se donne $A \in \mathcal{C}$ et $A' = h(A)$, alors pour tout $M \in \mathcal{C}$, $h(M)$ est construit comme l'intersection avec $\mathcal{C}$ de la droite passant par A et par l'intersection de Δ et $(A'M)$.
Toute homographie de coniques est alors caractérisée par un couple de points homologues A et $A' = h(A)$ et l'axe de l'homographie.



Démonstration. • Soit h une application comme définie sur le dessin. Alors h est une bijection et elle conserve le birapport. En effet, prenons quatre points distincts M_i sur $\mathcal{C}$ alors leur birapport est celui des $(A'M_i)$, donc celui des $(A'N_i)$. Puis on sait par définition du birapport que celui-ci vaut le birapport des N_i. [3] Le birapport est donc égal à celui des (AN_i) puis à celui des (AM_i') et enfin à celui des M_i' par le même raisonnement.

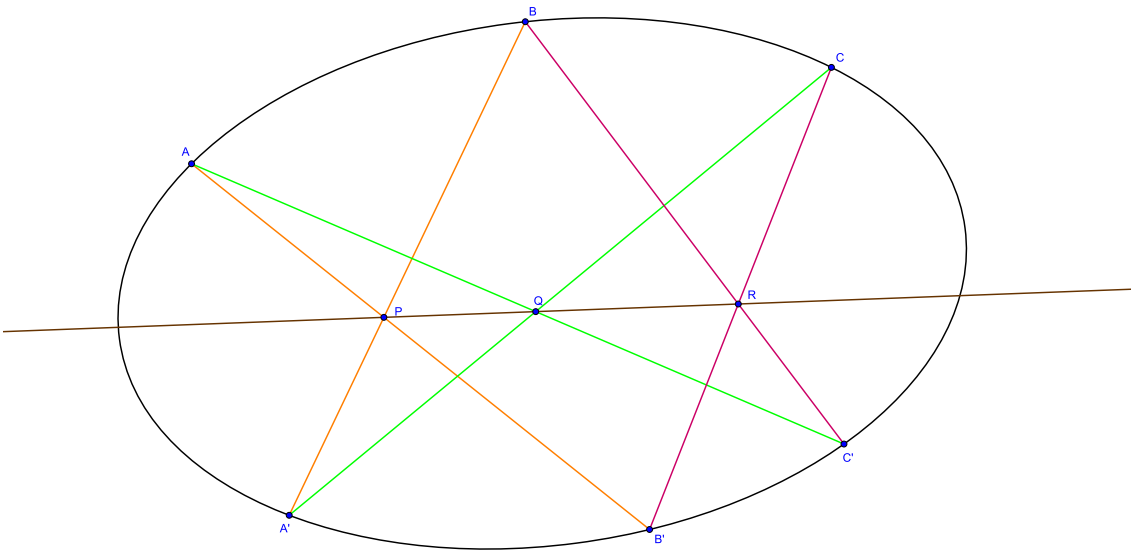
• Réciproquement, soit h une homographie de la conique $\mathcal{C}$. On se donne trois points A, B, C de $\mathcal{C}$ distincts et on note A', B', C' leurs images par h. On note R l'intersection de (AB') avec $(A'B)$ et S celle de (AC') avec

1. Il suffit d'écrire le polynôme homogène définissant $\mathcal{C}$, d'écrire les tangentes en B et C et d'évaluer pour trouver des conditions simples sur les coefficients.
2. Ladegaillerie, p 131 : on connaît la formule en excluant le point à l'infini (on fait $T = 1$ et les équations précédentes donnent des coordonnées de points sur une droite projective.). Pour prendre en compte celui-ci, il faut faire des déterminants 2×2. Bref ça ne vaut pas le coup d'être détaillé...
3. Ladegaillerie, p 55/119, par Thalès.

$(A'C)$. On appelle Δ la droite (RS). Alors h est l'homographie d'axe Δ et telle que $A' = h(A)$ car elle coïncide avec cette homographie en trois points A, B et C. □

Théorème (Hexagramme de Pascal)**.**

On se donne six points distincts A, B, C, A', B', C' dont trois ne sont pas alignés, alors ces six points sont sur une même conique propre $\mathcal{C}$ si et seulement si les intersections P, Q, R de (AB') et $(A'B)$, (BC') et $(B'C)$, (CA') et $(C'A)$ sont alignées.



Démonstration. • Si les six points sont sur un conique propre, alors il existe une unique homographie envoyant A sur A', B sur B' et C sur C'. Cette homographie peut être définie comme celle d'axe (PQ) et envoyant A sur A', ou celle d'axe (PR) et envoyant B sur B'. On a donc $(PQ) = (PR)$ donc l'axe passe par P, Q et R. Ils sont bien alignés.

• Réciproquement, on définit $\mathcal{C}$ l'unique conique propre passant par les cinq premiers points (existe car au moins trois points ne sont pas alignés), et Δ la droite passant par P, Q et R. Alors l'homographie de $\mathcal{C}$ d'axe Δ et envoyant A sur A', transforme C en le point de la droite (AC') sur $\mathcal{C}$. Puis l'homographie de $\mathcal{C}$ d'axe Δ et envoyant B sur B', transforme C en le point de la droite (BC') sur $\mathcal{C}$. Ces homographies ont même axe et envoient A sur A' : elles sont donc égales.
Les droites (AC') et (BC') s'intersectent uniquement en C', donc l'image de C par cette homographie est C', et donc C' se trouve sur $\mathcal{C}$. □

Remarques : • Dans tout ce développement, je me place dans $\mathbb{R}^2$ que j'injecte dans $\mathbb{P}_2(\mathbb{R})$ en choisissant une droite à l'infini. Quand je ne rajoute pas projectif après les objets géométriques que j'utilise, c'est que je les considère dans $\mathbb{R}^2$.
• Je redéfinis les homographies sur un ensemble de $\mathbb{P}_2(\mathbb{R})$ de même cardinal qu'une droite projective dans ce développement. On peut montrer (Ladegaillerie, p 151) que ces nouvelles homographies vérifient toujours les propriétés des "vraies" homographies, comme le fait qu'il existe une unique homographie envoyant trois points distincts sur trois autres.
• Dans le théorème de Pascal, l'ordre des points est indifférent, ce qui veut dire que d'autres intersections de droites sont aussi alignées.
• Le théorème de Pappus est l'analogue du théorème de Pascal pour une conique dégénérée en deux droites sécantes. Pour le prouver, on montre de même qu'une homographie de droites a un axe, puis le reste du raisonnement est le même.
• Si le développement est trop court (aha quelle blague !), on peut prouver que l'équation de la conique est bien $XY - T^2$, ou on peut prouver qu'une homographie de droites a un axe.

Chapitre 46

Théorème de structure des groupes abéliens finis

Références : Colmez, *Éléments d'analyse et d'algèbre (et de théorie des nombres)*, p 250-252

On rappelle que l'exposant d'un groupe G est le plus petit entier n tel que pour tout $g \in G$, $g^n = e$. Comme pour tous $g, h \in G$, gh est un élément d'ordre $\text{ppcm}(o(g), o(h))$ **car G est abélien**, l'exposant est donc le ppcm des ordres des éléments du groupe, et aussi le plus grand des ordres des éléments du groupe.

Théorème.

Si G est un groupe abélien fini, alors il existe $r \in \mathbb{N}$ et des entiers N_1, ..., N_r, où N_1 est l'exposant de G et $N_{i+1} | N_i$ tels que

$$G \simeq \prod_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}.$$

Comme G est un groupe abélien fini, les classes de conjugaisons n'ont qu'un élément. On a donc $n = |G|$ représentations irréductibles de degré 1 par Burnside.
Puis on remarque que les caractères irréductibles sont des morphismes. Ce sont donc des éléments de $\widehat{G}$, le groupe abélien des morphismes de G dans $\mathbb{C}^*$.
Réciproquement, tout élément de $\widehat{G}$ fournit une représentation irréductible, donc un caractère irréductible.
$\widehat{G}$ est donc le groupe des caractères irréductibles de G.

Lemme.

On pose l'application

$$i : \begin{array}{ccc} G & \to & \widehat{\widehat{G}} \\ g & \mapsto & (\chi \mapsto \chi(g)) \end{array},$$

alors i est un isomorphisme de groupes.

Démonstration. i est bien un morphisme de groupes car les caractères sont des morphismes.
En effet,

$$i(gh)(\chi) = \chi(gh) = \chi(g)\chi(h) = i(g)(\chi)i(h)(\chi).$$

On a vu que $\widehat{G}$ est l'ensemble des caractères irréductibles. Il est donc de même cardinal que G. On a $\left|\widehat{G}\right| = \left|\widehat{\widehat{G}}\right|$, en appliquant le même raisonnement aux éléments de $\widehat{\widehat{G}}$, qui sont les caractères irréductibles sur $\widehat{G}$ **car $\widehat{G}$ est abélien**.
D'où $|G| = \left|\widehat{\widehat{G}}\right|$.
Il suffit de montrer que i est injectif.

Soit $g \in G$ tel que $i(g)(\chi) = 1 = i(e)(\chi)$. Alors $\forall \chi \in \widehat{G}$, $\chi(g) = \chi(e) = 1$.
On décompose $\mathbb{1}_{\{g\}}$ dans la base des caractères.

$$\begin{aligned}\mathbb{1}_{\{g\}} &= \sum_{\chi\in\widehat{G}} \langle \mathbb{1}_{\{g\}}, \chi\rangle \chi \\ &= \sum_{\chi\in\widehat{G}} \frac{1}{G} \sum_{h\in G} \overline{\mathbb{1}_{\{g\}}(h)}\chi(h)\chi \\ &= \frac{1}{G}\sum_{\chi\in\widehat{G}} \chi(g)\chi \\ &= \frac{1}{G}\sum_{\chi\in\widehat{G}} \chi\end{aligned}$$

On a donc en évaluant en e :

$$\mathbb{1}_{\{g\}}(e) = \frac{1}{G}\sum_{\chi\in\widehat{G}} \chi(e) = 1.$$

D'où $g = e$ et i est bien injective. □

Lemme.

G et $\widehat{G}$ ont même exposant.

Démonstration. Soit N l'exposant de G, on a $\forall \chi \in \widehat{G}$, $\forall g \in G$,

$$\chi^N(g) = \chi(g)^N = \chi(g^N) = \chi(1) = 1.$$

L'exposant de $\widehat{G}$ est inférieur ou égal à N.
On peut appliquer le même raisonnement à $\widehat{G}$ pour obtenir que N est inférieur ou égal à l'exposant de $\widehat{G}$ (car G et $\widehat{\widehat{G}}$ ont même exposant par le lemme précédent).
Cela donne le résultat. □

Passons à la preuve du théorème.

Démonstration. Démontrons le théorème par récurrence sur $n = |G|$.
Pour $n = 1$, le résultat est évident.
On suppose $n > 1$, notons N_1 l'exposant de G.

• Par le lemme précédent, il existe un élément $\chi_1 \in \widehat{G}$ d'ordre N_1. On a donc $\forall g \in G$, $\chi_1(g)^{N_1} = 1$.
Donc $\chi_1(G)$ est un sous-groupe des racines N_1-ièmes de l'unité et on a égalité car χ_1 est d'ordre exactement N_1.

Soit $x_1 \in G$ tel que $\chi_1(x_1) = \exp\left(\frac{2i\pi}{N_1}\right)$ et soit p l'ordre de x_1.
On sait que p divise N_1. Puis $\chi_1(x_1^p) = 1 = \exp\left(\frac{2ip\pi}{N_1}\right)$, donc N_1 divise p et finalement x_1 est d'ordre N_1.

• On pose $H_1 = \langle x_1\rangle$. Montrons que $G \simeq H_1 \times \mathrm{Ker}(\chi_1)$. Comme $H_1 \simeq \mathbb{Z}/N_1\mathbb{Z}$ et $|\mathrm{Ker}(\chi_1)| < n$, on aura le résultat en appliquant l'hypothèse de récurrence.
En effet, si on décompose $\mathrm{Ker}(\chi_1)$ en $\prod_{i=2}^{r} \mathbb{Z}/N_i\mathbb{Z}$ avec $N_{i+1}|N_i$, alors comme les éléments de G sont d'ordre divisant N_1, on aura $G \simeq \prod_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}$ avec $N_{i+1}|N_i$.

χ_1 induit un morphisme surjectif α de H_1 sur $\mathbb{U}_{N_1}$, puis par égalité des cardinaux, α est un isomorphisme.
Soit $x \in G$, alors

$$x = \alpha^{-1}(\chi_1(x))\left(\alpha^{-1}(\chi_1(x))\right)^{-1} x.$$

Par définition de α, $\alpha^{-1}(\chi_1(x)) \in H_1$.
Puis

$$\chi_1\left(\left(\alpha^{-1}(\chi_1(x))\right)^{-1} x\right) = \chi_1\left(\left(\alpha^{-1}(\chi_1(x))\right)^{-1}\right)\chi_1(x) = (\chi_1(x))^{-1}\chi_1(x) = 1,$$

donc $\left(\alpha^{-1}(\chi_1(x))\right)^{-1} x \in \mathrm{Ker}(\chi_1)$.
On a donc bien $G = H_1 \mathrm{Ker}(\chi_1)$.
On a aussi $H_1 \cap \mathrm{Ker}(\chi_1) = \{e\}$ car χ_1 est injectif sur H_1.
Il vient donc que $G \simeq H_1 \times \mathrm{Ker}(\chi_1)$, ce qui termine la preuve. □

Remarques : • On peut déduire de ce résultat le théorème de structure des groupes abéliens de type fini. On applique le théorème précédent au sous-groupe de torsion T, puis on peut prouver qu'on peut écrire $G \simeq T \times L$ avec L sans torsion. On montre en se donnant une base que L est isomorphe à $\mathbb{Z}^d$. Cela donne le résultat.
• Ce résultat peut être généralisé en le théorème de structure des modules de type fini sur les anneaux principaux.

Adapté du travail de Alexandre Bailleul.

Chapitre 47

Théorème de Weierstrass

Références : Zuily, Queffélec, *Analyse pour l'agrégation*, p 518-519 (et p 114-115)

Théorème.

Soit $f : [0,1] \to \mathbb{C}$ continue. On lui associe ses polynômes de Bernstein définis pour tout $n \geqslant 1$ par

$$B_n = \sum_{k=0}^{n} \binom{n}{k} X^k (1-X)^{n-k} f\left(\frac{k}{n}\right).$$

Alors pour tout $n \geqslant 1$,

$$||f - B_n||_\infty \leqslant \frac{3}{2}\omega\left(\frac{1}{\sqrt{n}}\right),$$

où ω est le module de continuité uniforme de f [a]. De plus, cette estimation est optimale.

a. Pour tout $h \in \mathbb{R}$, $\omega(h) = \sup_{|x-y| \leqslant h} (|f(x) - f(y)|)$. Celui-ci tend vers 0 en 0 par uniforme continuité de f (théorème de Heine). On le définit sur $\mathbb{R}$ pour ne pas avoir de problème ensuite.

Démonstration. Commençons par fixer un $x \in [0,1]$. On considère une suite $(X_n)_n$ de variables aléatoires indépendantes de Bernoulli de paramètre x. Pour $n \geqslant 1$ on notera

$$S_n = \sum_{k=1}^{n} X_k.$$

Remarquons que l'on a, pour $n \geqslant 1$,

$$\mathbb{E}(S_n) = nx,$$
$$\mathrm{Var}(S_n) = nx(1-x),$$

et

$$\mathbb{E}\left(f\left(\frac{S_n}{n}\right)\right) = \sum_{k=0}^{n} \binom{n}{k} x^k (1-x)^{n-k} f\left(\frac{k}{n}\right) = B_n(x).$$

Soit $n \geqslant 1$. Par le constat précédent on peut écrire

$$\begin{aligned} |f(x) - B_n(x)| &= \left|\mathbb{E}\left(f(x) - f\left(\frac{S_n}{n}\right)\right)\right| \\ &\leqslant \mathbb{E}\left(\left|f(x) - f\left(\frac{S_n}{n}\right)\right|\right) \\ &\leqslant \mathbb{E}\left(\omega\left(\left|x - \frac{S_n}{n}\right|\right)\right). \end{aligned}$$

On aura besoin du lemme suivant :

Lemme.

Pour tous $\lambda, h \in [0,1]$, on a $\omega(\lambda h) \leqslant (\lambda+1)\omega(h)$.

Démonstration. La fonction ω est croissante. En effet, si $h \leqslant h'$ alors

$$\{|f(x)-f(y), |x-y| \leqslant h\} \subset \{|f(x)-f(y), |x-y| \leqslant h'\}$$

d'où $\omega(h) \leqslant \omega(h')$.

Ensuite, celle-ci est sous-additive :

Soient t_1 et t_2 dans $[0,1]$ tels que $t_1+t_2 \in [0,1]$. Soient u et v dans $[0,1]$ tels que $|u-v| \leqslant t_1+t_2$ et $u \leqslant v$, et soit w dans $[0,1]$ tel que $|u-w| \leqslant t_1$ et $|v-w| \leqslant t_2$. (On peut prendre $w = u+t_1$ par exemple)

Alors on a

$$\begin{aligned} |f(u)-f(v)| &\leqslant |f(u)-f(w)| + |f(w)-f(v)| \\ &\leqslant \omega(t_1)+\omega(t_2) \end{aligned}$$

d'où $\omega(t_1+t_2) \leqslant \omega(t_1)+\omega(t_2)$ en passant à la borne supérieure.
On en déduit par une récurrence immédiate que si $n \in \mathbb{N}$ et $h \in [0,1]$ sont tels que $nh \in [0,1]$ alors $\omega(nh) \leqslant n\omega(h)$.

Soit donc λ et h dans $[0,1]$. Comme $\lfloor\lambda\rfloor \leqslant \lambda \leqslant \lfloor\lambda\rfloor + 1$ on obtient

$$\begin{aligned} \omega(\lambda h) &\leqslant \omega((\lfloor\lambda\rfloor+1)h) \\ &\leqslant (\lfloor\lambda\rfloor+1)\omega(h) \\ &\leqslant (\lambda+1)\omega(h). \end{aligned}$$

□

Par le lemme on a

$$\omega\left(\left|x-\frac{S_n}{n}\right|\right) \leqslant \left(\sqrt{n}\left|x-\frac{S_n}{n}\right|+1\right)\omega\left(\frac{1}{\sqrt{n}}\right).$$

Ainsi, en utilisant l'inégalité de Cauchy-Schwarz ($||.||_1 \leqslant ||.||_2$ comme on a une mesure de probabilité), on obtient

$$\begin{aligned} |f(x)-B_n(x)| &\leqslant \omega\left(\frac{1}{\sqrt{n}}\right)\mathbb{E}\left(\sqrt{n}\left|x-\frac{S_n}{n}\right|+1\right) \\ &= \omega\left(\frac{1}{\sqrt{n}}\right)\left(1+\sqrt{n}\left\|x-\frac{S_n}{n}\right\|_1\right) \\ &\leqslant \omega\left(\frac{1}{\sqrt{n}}\right)\left(1+\sqrt{n}\left\|x-\frac{S_n}{n}\right\|_2\right). \end{aligned}$$

De plus, $\mathbb{E}\left(\frac{S_n}{n}\right) = x$ donc $\left\|x-\frac{S_n}{n}\right\|_2$ n'est autre que la racine carrée de la variance de $\frac{S_n}{n}$, qui vaut $\frac{1}{n^2}\mathrm{Var}(S_n) = \frac{1}{n^2}nx(1-x) = \frac{x(1-x)}{n}$.

On a donc

$$|f(x)-B_n(x)| \leqslant \omega\left(\frac{1}{\sqrt{n}}\right)(1+\sqrt{x(1-x)}).$$

Or le polynôme $X(1-X)$ admet son maximum sur $[0,1]$ en $\frac{1}{2}$ (simple étude de fonction), ce maximum valant $\frac{1}{4}$. Finalement,

$$|f(x)-B_n(x)| \leqslant \frac{3}{2}\omega\left(\frac{1}{\sqrt{n}}\right),$$

et la majoration étant uniforme, on a bien

$$||f - B_n||_\infty \leqslant \frac{3}{2}\omega\left(\frac{1}{\sqrt{n}}\right).$$

Pour montrer que cette estimation est optimale, on va exhiber une fonction f telle que pour tout $n \geqslant 1$,

$$||f - B_n||_\infty \geqslant C\omega\left(\frac{1}{\sqrt{n}}\right),$$

où C est une constante strictement positive.

On considère la fonction $f : x \mapsto \left|x - \frac{1}{2}\right|$, continue sur $[0,1]$ et dont le module de continuité uniforme vérifie $\forall h \in [0,1]$, $\omega(h) \leqslant h$ (seconde inégalité triangulaire). En gardant les mêmes notations que précédemment, pour $x = \frac{1}{2}$ et $n \geqslant 1$, on a

$$\begin{aligned}
||f - B_n||_\infty &\geqslant \left|f\left(\frac{1}{2}\right) - B_n\left(\frac{1}{2}\right)\right| \\
&= \mathbb{E}\left(\left|\frac{1}{2} - \frac{S_n}{n}\right|\right) \\
&= \frac{1}{2n}\mathbb{E}\left(|2S_n - n|\right) \\
&= \frac{1}{2n}||\varepsilon_1 + \cdots + \varepsilon_n||_1,
\end{aligned}$$

où pour tout $i \in \{1, ..., n\}$, $\varepsilon_i = 2X_i - 1$ est une variable aléatoire de Rademacher.
On va montrer que $||\varepsilon_1 + \cdots + \varepsilon_n||_1 \geqslant \sqrt{\frac{n}{\mathrm{e}}}$ [1], ce qui prouvera que

$$||f - B_n||_\infty \geqslant \frac{1}{2\sqrt{\mathrm{e}}}\,\omega\left(\frac{1}{\sqrt{n}}\right)$$

et terminera la preuve.

Posons $f = \varepsilon_1 + \cdots + \varepsilon_n$ et $g = \prod_{j=1}^{n}\left(1 + i\frac{\varepsilon_j}{\sqrt{n}}\right)$. On a presque surement

$$|g| = \left|\prod_{j=1}^{n}\left(1 + i\frac{\varepsilon_j}{\sqrt{n}}\right)\right| = \prod_{j=1}^{n}\left(1 + \frac{\varepsilon_j^2}{n}\right)^{1/2} \leqslant \prod_{j=1}^{n}\exp\left(\frac{1}{n}\right)^{1/2} = \sqrt{\mathrm{e}}$$

car pour tout $j \in \{1, ..., n\}$, $\varepsilon_j^2 = 1$ ps et $\forall x \in \mathbb{R}, 1 + x \leqslant \exp(x)$.

De plus,

$$\begin{aligned}
|\mathbb{E}(fg)| &= \left|\sum_{j=1}^{n}\mathbb{E}\left(\varepsilon_j\prod_{k=1}^{n}\left(1 + i\frac{\varepsilon_k}{\sqrt{n}}\right)\right)\right| \\
&= \left|\sum_{j=1}^{n}\left(\prod_{\substack{k=1\\k\neq j}}^{n}\mathbb{E}\left(1 + i\frac{\varepsilon_k}{\sqrt{n}}\right) \times \mathbb{E}\left(\varepsilon_j + \frac{i}{\sqrt{n}}\right)\right)\right| \\
&= \sqrt{n}
\end{aligned}$$

car les ε_k sont centrées et indépendantes.
Finalement, on a $\sqrt{n} = |\mathbb{E}(fg)| \leqslant \mathbb{E}(|fg|) \leqslant ||f||_1||g||_\infty \leqslant \sqrt{\mathrm{e}}||f||_1$, d'où le résultat. □

Remarques : • En pratique, on ne prouve ni la croissance, ni la sous-additivité de ω pour avoir le temps de tout faire.

Adapté du travail d'Alexandre Bailleul.

1. Cette inégalité est appelée inégalité de Khintchine.

Chapitre 48

Théorème des extrema liés

Références : Gourdon, *Les maths en tête - Analyse*, p 317 et p 327
Beck, Malick, Peyré, *Objectif agrégation*, p20 (pour l'interprétation géométrique)

Théorème (Théorème des extrema liés)**.**

Soient f, g_1, ..., g_r des fonctions de classe $\mathcal{C}^1$ d'un ouvert $U \subset \mathbb{R}^n$ dans $\mathbb{R}$. On pose $\Gamma = \{x \in U, g_1(x) = \cdots = g_r(x) = 0\}$.
Si $f_{|\Gamma}$ admet un extremum relatif en $a \in \Gamma$, et si les formes linéaires $Dg_1(a), \ldots, Dg_r(a)$ sont linéairement indépendantes, alors il existe des réels $\lambda_1, \cdots, \lambda_r$, appelés multiplicateurs de Lagrange, tels que

$$Df(a) = \sum_{i=1}^{r} \lambda_i Dg_i(a).$$

Démonstration. • Soit $s = n - r$. On peut identifier $\mathbb{R}^n$ à $\mathbb{R}^s \times \mathbb{R}^r$. On écrit donc les éléments de $\mathbb{R}^n$ comme (x, y) où $x = (x_1, \ldots, x_s)$ et $y = (y_1, \ldots, y_r)$.
Posons $a = (\alpha, \beta) \in \mathbb{R}^s \times \mathbb{R}^r$.
Déjà, $r \leqslant n$ car les formes linéaires $Dg_i(a)$ forment une famille libre et la dimension de l'espace dual de $\mathbb{R}^n$ est n. De plus, si $r = n$, le théorème devient évident car les $Dg_i(a)$ forment une base de $(\mathbb{R}^n)^*$.
On peut donc supposer que $r < n$, ie $s \geqslant 1$.

- Les formes linéaires $(Dg_i(a))_{1 \leqslant i \leqslant r}$ forment une famille libre, ainsi la matrice :

$$\begin{pmatrix} \frac{\partial g_1}{\partial x_1}(a) & \cdots & \frac{\partial g_1}{\partial x_s}(a) & \frac{\partial g_1}{\partial y_1}(a) & \cdots & \frac{\partial g_1}{\partial y_r}(a) \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial g_r}{\partial x_1}(a) & \cdots & \frac{\partial g_r}{\partial x_s}(a) & \frac{\partial g_r}{\partial y_1}(a) & \cdots & \frac{\partial g_r}{\partial y_r}(a) \end{pmatrix}$$

est de rang r [1].
On peut donc en extraire une sous-matrice $r \times r$ inversible. Quitte a changer le nom des variables, on peut supposer que :

$$\det \left(\frac{\partial g_i}{\partial y_j}(a) \right)_{1 \leqslant i,j \leqslant r} \neq 0.$$

Ce qui peut se reformuler, en posant $g := (g_1, \ldots, g_r)$ par : $D_y g(a)$ est inversible.

• D'après le théorème des fonctions implicites, on peut donc trouver un voisinage ouvert U' de α dans $\mathbb{R}^s$, un voisinage ouvert Ω de $a = (\alpha, \beta)$ dans $\mathbb{R}^n$ et une fonction $\varphi = (\varphi_1, \ldots, \varphi_r) : U' \to \mathbb{R}^r$ de classe $\mathcal{C}^1$ tels que :

$$(x \in U', (x, y) \in \Omega \text{ et } g(x, y) = 0) \Leftrightarrow (y = \varphi(x)).$$

En d'autre termes, sur un voisinage de a, les éléments de Γ s'écrivent $(x, \varphi(x))$. Comme $a \in \Gamma$, on a $\beta = \varphi(\alpha)$.

1. Il y a r lignes donc le rang est au plus r. Puis les r lignes sont indépendantes donc le rang est au moins r.

Posons $\psi := (\psi_1, \dots, \psi_n) : x \in U' \subset \mathbb{R}^s \mapsto (x, \varphi(x))$. Alors $\psi(x) \in \Gamma$ par le TFI. Posons également, sur U', $h = f \circ \psi$.
Comme $h(\alpha) = f(a)$, h admet un extremum local en α (car f admet un extremum local sur Γ en a).
Ainsi, pour tout $i \in [\![1, s]\!]$,

$$0 = \frac{\partial h}{\partial x_i}(\alpha) = \sum_{j=1}^{s} \frac{\partial f}{\partial x_j}(\psi(\alpha)) \frac{\partial \psi_j}{\partial x_i}(\alpha) + \sum_{j=1}^{r} \frac{\partial f}{\partial y_j}(\psi(\alpha)) \frac{\partial \psi_{s+j}}{\partial x_i}(\alpha)$$

En remarquant que $\forall j \in [\![1, s]\!]$, $\dfrac{\partial \psi_j}{\partial x_i} = \delta_{i,j}$ et que $\forall j \in [\![1, r]\!]$ $\dfrac{\partial \psi_{s+j}}{\partial x_i} = \dfrac{\partial \varphi_j}{\partial x_i}$. Et comme $a = \psi(\alpha)$, on obtient :

$$\frac{\partial f}{\partial x_i}(a) + \sum_{j=1}^{r} \frac{\partial \varphi_j}{\partial x_i}(\alpha) \frac{\partial f}{\partial y_j}(a) = 0$$

De plus, $g \circ \psi$ est nulle sur U' donc pour tout $k \in [\![1, r]\!]$ c'est également le cas pour $g_k \circ \psi$. Donc, par un calcul similaire à celui du dessus, pour $i \in [\![1, s]\!]$:

$$\frac{\partial g_k}{\partial x_i}(a) + \sum_{j=1}^{r} \frac{\partial \varphi_j}{\partial x_i}(\alpha) \frac{\partial g_k}{\partial y_j}(a) = 0$$

Si on considère donc la matrice :

$$M = \begin{pmatrix} \dfrac{\partial f}{\partial x_1}(a) & \cdots & \dfrac{\partial f}{\partial x_s}(a) & \dfrac{\partial f}{\partial y_1}(a) & \cdots & \dfrac{\partial f}{\partial y_r}(a) \\ \dfrac{\partial g_1}{\partial x_1}(a) & \cdots & \dfrac{\partial g_1}{\partial x_s}(a) & \dfrac{\partial g_1}{\partial y_1}(a) & \cdots & \dfrac{\partial g_1}{\partial y_r}(a) \\ \vdots & & \vdots & \vdots & & \vdots \\ \dfrac{\partial g_r}{\partial x_1}(a) & \cdots & \dfrac{\partial g_r}{\partial x_s}(a) & \dfrac{\partial g_r}{\partial y_1}(a) & \cdots & \dfrac{\partial g_r}{\partial y_r}(a) \end{pmatrix}$$

Les s premiers vecteurs colonnes de M s'expriment, d'après les deux formules aux dérivées partielles ci-dessus, linéairement en fonction de ses r derniers vecteurs colonnes, donc $\operatorname{rg}(M) \leqslant r$. Ainsi les $r+1$ lignes de M forment une famille liée. [2]
Ceci entraine l'existence de réels $\mu_0, \dots, \mu_r$ non tous nuls tels que :

$$\mu_0 Df(a) + \mu_1 Dg_1(a) + \cdots + \mu_r Dg_r(a) = 0$$

Comme la famille $(Dg_i(a))_i$ est libre, $\mu_0 \neq 0$ donc en posant $\lambda_i = -\dfrac{\mu_i}{\mu_0}$ pour $i \in [\![1, r]\!]$, on obtient

$$Df(a) = \sum_{i=1}^{r} \lambda_i Dg_i(a).$$

□

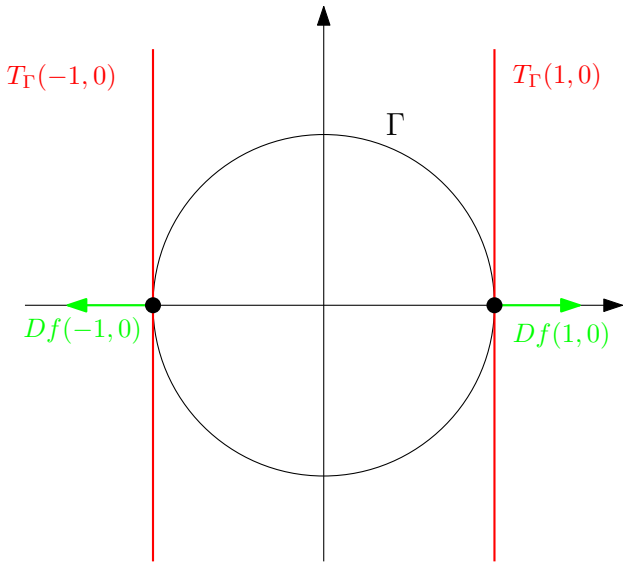
Interprétation géométrique du théorème : (d'après Objectif Agrégation p 20)
$\Gamma \cap V_a$ est une sous-variété pour V_a un certain voisinage de a.
Pour montrer cela, on commence par enlever des coordonnées comme dans la preuve pour obtenir la matrice (Dg_i) de taille $r \times r$ de déterminant non nul. Par continuité du déterminant, il existe un voisinage de a où le déterminant est non nul, donc où les Dg_i sont linéairement indépendants.
Puis on montre si les $Dg_i(x)$ sont linéairement indépendants, alors la matrice $DG(x)$ des $Dg_i(x)$ est surjective (donc on a la submersion voulue). En effet, $\operatorname{Ker}(DG(x)) = \bigcap \operatorname{Ker}(Dg_i(x)) = \bigcap (\nabla g_i(x))^{\perp} = \operatorname{Vect}(\nabla g_i(x))^{\perp}$ et par indépendance, $\operatorname{Vect}(\nabla g_i(x))$ est de dimension r, d'où $\operatorname{Vect}(\nabla g_i(x))^{\perp}$ est de dimension $n - r$. Donc la dimension de l'image est égale à r, ce qui montre la surjectivité.

L'égalité $Df(a) = \sum_{i=1}^{r} \lambda_i Dg_i(a)$ nous donne $\bigcap \operatorname{Ker} Dg_i(a) \subset \operatorname{Ker} Df(a)$. C'est même une équivalence. [3]
La caractérisation de l'espace tangent pour les sous variétés implicites est $\{h \in \mathbb{R}^n, Dg_i(a)h = 0, \forall i\}$. Le

2. Plus précisément, ça vient de $\operatorname{rg}({}^tM) = \operatorname{rg}(M)$, le rang des vecteurs lignes est égal au rang des vecteurs colonnes de M. Cette propriété vient d'elle même en faisant un pivot de Gauss pour se ramener à une matrice avec une diagonale de 1 et des 0 partout.
3. On le montre en utilisant qu'en dimension finie $(F^0)^{\perp} = F$, cf FGNal1 ex 6.27

théorème des extrema liés donne donc que $Df(a)$ est nulle sur l'espace tangent à Γ en a. Cela s'écrit aussi $\forall h \in \Gamma, < Df(a), h >= 0$, donc le vecteur $Df(a)$ est orthogonal à l'espace tangent en a.

→ En exemple, on prend $f(x,y) = x^2$ sur $\Gamma = \{(x,y) \in \mathbb{R}^2, g(x,y) = x^2 + y^2 - 1 = 0\}$. Les points extrémaux sont $(\pm 1, 0)$ et $(0, \pm 1)$ et les vecteurs correspondants sont $Df(\pm 1, 0) = \begin{pmatrix} \pm 2 \\ 0 \end{pmatrix}$ et le vecteur nul pour les deux autres. On a la figure suivante (où sont tracés les espaces tangents **affines**) qui représente l'orthogonalité de Df par rapport à l'espace tangent aux points où Df est non nulle.



En fait, l'exercice sur les directions principales d'une quadrique (Rouvière, ex 129) est la généralisation en dimension 3 de cette vision. On pose $f(x) = \|x\|^2$ et Q la forme quadratique définissant l'ellipsoïde. Alors les points extrémaux sont atteints quand le vecteur x est orthogonal à l'ellipsoïde. Un rapide dessin montre que cela arrive seulement pour les directions principales.

Remarques : • Il existe une version sous-variété de ce théorème présente dans le Avez de calcul différentiel. Elle trivialise la démonstration mais ne donne pas les multiplicateurs de Lagrange. Il y a du travail après.
• Une application du théorème des extrema liés est la preuve de l'inégalité arithmético-géométrique. (Gourdon, p319)
Idée : on pose $f(x_1, \dots, x_n) = x_1 \dots x_n$ et $g(x_1, \dots, x_n) = x_1 + \dots + x_n - s$. On applique le TEL et on trouve $\lambda = \dfrac{f(a)}{a_i}$, donc les a_i sont constants (à $\dfrac{s}{n}$) et $f(x) \leqslant \left(\dfrac{s}{n}\right)^n$ sur l'ensemble $\Gamma = \{x \in (\mathbb{R}^+)^n, \sum x_i = s\}$.
• Une autre application du même type est la mise en boîte à peu de frais de l'exercice 128 du Rouvière.
• Une dernière application est la preuve du théorème spectral. On a juste à maximiser $x \mapsto (u(x), x)$ sur la sphère unité.

Adapté du travail de Laura Gay

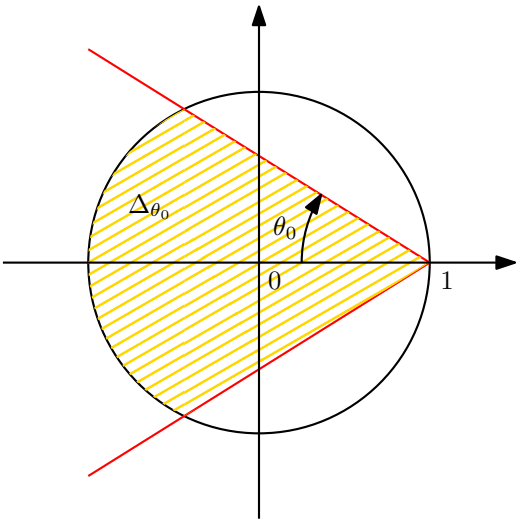
Chapitre 49

Théorèmes d'Abel et taubérien faible

Références : Gourdon, *Les maths en tête - Analyse*, p 249-251
Chambert-Loir, *Exercices de Mathématiques pour l'Agrégation 1*, 6.3

Théorème (Théorème d'Abel)**.**

Soit $f(z) = \sum_{n\geqslant 0} a_n z^n$ une série entière de rayon de convergence $R \geqslant 1$ telle que $\sum_{n\geqslant 0} a_n$ converge.
Soit $\theta_0 \in [0, \frac{\pi}{2}[$ et $\Delta_{\theta_0} = \{z \in B(0,1),\ \exists \rho > 0 \text{ et } \theta \in [-\theta_0, \theta_0] \text{ tels que } 1 - z = \rho e^{i\theta}\}$,
alors $\lim\limits_{\substack{z\to 1 \\ z\in\Delta_{\theta_0}}} f(z) = \sum_{n\geqslant 0} a_n$.



Le domaine Δ_{θ_0}

Démonstration. Soient $S = \sum a_n$ et $R_n = \sum_{k>n} a_k$, on a $a_n = R_{n-1} - R_n$.
Soit $z \in B(0,1)$, alors $f(z) - S = \sum a_n(z^n - 1) = \sum (R_{n-1} - R_n)(z^n - 1) = (z-1)\sum R_n z^n$.
Soit $\varepsilon > 0$, on choisit N tel que $\forall n \geqslant N,\ |R_n| < \varepsilon$.
Alors $|f(z) - S| \leqslant |z-1| \left|\sum_{n=0}^{N} R_n z^n\right| + \varepsilon |z-1| \sum_{n=N+1}^{\infty} |z|^n \leqslant |z-1| \sum_{n=0}^{N} |R_n| + \varepsilon \frac{|z-1|}{1-|z|}$.
Soit $\alpha > 0$ tel que $|z-1| < \alpha \Rightarrow |z-1| \sum_{n=0}^{N} |R_n| < \varepsilon$.
Il ne reste donc plus qu'à majorer $\frac{|z-1|}{1-|z|}$.

On prend $z \in \Delta_{\theta_0}$, donc z est de la forme $1-\rho e^{i\phi}$ avec $\rho > 0$ et $|\phi| \leqslant \theta_0$. On a $|z|^2 = 1 - 2\rho\cos(\phi) + \rho^2$.
D'où $\dfrac{|z-1|}{1-|z|} = \dfrac{|z-1|}{1-|z|^2}(1+|z|) = \dfrac{\rho}{2\rho\cos(\phi)-\rho^2}(1+|z|) \leqslant \dfrac{2}{2\cos(\phi)-\rho} \leqslant \dfrac{2}{2\cos(\theta_0)-\rho}$.
Si on pose $\rho \leqslant \cos(\theta_0)$, on a $\dfrac{|z-1|}{1-|z|} \leqslant \dfrac{2}{2\cos(\theta_0)-\cos(\theta_0)} = \dfrac{2}{\cos(\theta_0)}$.
Conclusion : si on prend $z \in \Delta_{\theta_0}$ et $|z-1| \leqslant \min(\alpha, \cos(\theta_0))$, on a $|f(z)-S| \leqslant \varepsilon\left(1+\dfrac{2}{\cos(\theta_0)}\right)$.
Donc $\lim\limits_{\substack{z\to 1 \\ z\in\Delta_{\theta_0}}} f(z) = S = \sum\limits_{n\geqslant 0} a_n$. □

Applications : • $\sum\limits_{n\geqslant 0} \dfrac{(-1)^n}{2n+1}$ converge comme série alternée grâce au critère de Leibniz.
D'où $\sum\limits_{n\geqslant 0} \dfrac{(-1)^n}{2n+1} = \lim\limits_{\substack{x\to 1 \\ x<1}} \arctan(x) = \dfrac{\pi}{4}$ en appliquant sur la droite réelle le théorème ($\theta_0 = 0$).
• De même, on a $\sum\limits_{n\geqslant 1} \dfrac{(-1)^{n-1}}{n} = \ln(2)$.

On va maintenant démontrer une réciproque partielle du théorème d'Abel dans le cas où $a_n = o\left(\dfrac{1}{n}\right)$ et où on ne demande que la convergence avec $\theta_0 = 0$.

Théorème (Théorème taubérien faible (Alfred Tauber))**.**

Soit $\sum\limits_{n\geqslant 0} a_n z^n$ une série entière de rayon de convergence $R \geqslant 1$ et f sa somme sur le disque unité de $\mathbb{C}$. On suppose qu'il existe S dans $\mathbb{C}$ tel que $\lim\limits_{\substack{x\to 1 \\ x<1}} f(x) = S$, alors si $a_n = o\left(\dfrac{1}{n}\right)$, $\sum\limits_{n\geqslant 0} a_n$ converge et $S = \sum\limits_{n=0}^{\infty} a_n$.

Démonstration. On pose $S_n = \sum\limits_{k=0}^{n} a_k$. Le but est de faire converger S_n vers S. Soit donc $\varepsilon > 0$.
Sur $B(0,1)$, on a $S_n - f(x) = \sum\limits_{k=0}^{n} a_k(1-x^k) - \sum\limits_{k=n+1}^{\infty} a_k x^k$.
Or $(1-x^k) = (1-x)(1+x+...+x^{k-1}) \leqslant (1-x)k$, donc
$|S_n - f(x)| \leqslant (1-x)\sum\limits_{k=0}^{n} k|a_k| + \sum\limits_{k=n+1}^{\infty} \dfrac{k|a_k|}{n+1}|x|^k$.
Puis $(k|a_k|)_k$ converge (vers 0) donc on peut choisir un majorant M de cette suite. On peut aussi choisir N_0 tel que $\forall k \geqslant N_0$, $k|a_k| < \varepsilon^2$.
On a $\forall n \geqslant N_0$, $|S_n - f(x)| \leqslant (1-x)M(n+1) + \dfrac{\varepsilon^2}{n+1}\sum\limits_{k=n+1}^{\infty}|x|^k \leqslant (1-x)M(n+1) + \dfrac{\varepsilon^2}{(n+1)(1-|x|)}$.
Donc $|S_n - f\left(1-\dfrac{\varepsilon}{n+1}\right)| \leqslant (M+1)\varepsilon$.
Pour finir, $f(x)$ converge vers S quand $x \to 1$, donc il existe $N_1 \geqslant N_0$ tel que $|f(1-\dfrac{\varepsilon}{n+1}) - S| < \varepsilon$, $\forall n \geqslant N_1$.
Conclusion : $|S_n - S| \leqslant |S_n - f(1-\dfrac{\varepsilon}{n+1})| + |f(1-\dfrac{\varepsilon}{n+1}) - S| \leqslant (M+2)\varepsilon$. Donc S_n converge vers S. □

Remarques : • Ce théorème reste vrai si on suppose seulement $a_n = \mathcal{O}\left(\dfrac{1}{n}\right)$, c'est le théorème taubérien fort de Hardy-Littlewood. Il se prouve avec le théorème de Weierstrass.
• La réciproque du théorème d'Abel est fausse dans le cas général.
Par exemple, $\sum(-1)^n$ diverge et $\lim\limits_{\substack{z\to 1 \\ |z|<1}} \sum(-1)^n z^n = \lim\limits_{\substack{z\to 1 \\ |z|<1}} \dfrac{1}{1+z} = \dfrac{1}{2}$.

Chapitre 50

Théorèmes de Chevalley-Warning et Erdös-Ginzburg-Ziv

Références : Zavidovique, *Un max de maths*, p 32
Serre, *Cours d'arithmétique*, p 12
Bourgade, *Olympiades internationales de mathématiques - 1976-2005*, p 87

Théorème.

Soient k un corps fini à $q = p^n$ éléments et m un entier naturel non nul. On considère A un ensemble fini et $(f_a)_{a\in A}$ une famille de polynômes de $k[X_1, \dots, X_m]$ telle que

$$\sum_{a\in A} \deg f_a < m.$$

Soit V l'ensemble des racines communes aux polynômes f_a, alors $\#V \equiv 0 \mod (p)$.

Pour commencer, on a besoin de démontrer le lemme suivant sur les sommes de puissances dans les corps finis.

Lemme.

Soit u un entier naturel. Alors :

$$\sum_{x\in k} x^u = \begin{cases} -1 & \text{si } u \geqslant 1 \text{ et } q-1 \text{ divise } u \\ 0 & \text{sinon} \end{cases}.$$

Démonstration. Notons $S(X^u)$ la somme mise en jeu. Si u est nul, le résultat est immédiat tandis que si u est divisible par $q-1$, alors

$$S(X^u) = 0^u + \sum_{x\in k^*} 1 = q - 1 = -1.$$

Enfin, si $u \geqslant 1$ et n'est pas divisible par $q-1$, sachant que k^* est cyclique, il existe $y \in k^*$ tel que y^u soit différent de 1. On a alors :

$$S(X^u) = \sum_{x\in k^*} x^u = \sum_{x\in k^*} (yx)^u = y^u S(X^u).$$

Comme y^u est distinct de 1, il s'ensuit que $S(X^u) = 0$. □

Démonstration. Considérons le polynôme

$$P(X_1, \dots, X_m) = \prod_{a\in A} (1 - f_a^{q-1}(X_1, \dots, X_m)).$$

Remarquons dans un premier temps que P est la fonction caractéristique de V :

- Si $x \in k^m$ vérifient $f_a(x) = 0$ pour tout $a \in A$, alors $P(x) = 1$.
- Si $x \in k^m$ n'est pas un élément de V, il existe $a \in A$ tel que $f_a(x)$ ne vaille pas 0, alors par théorème de Lagrange, $f_a(x)^{q-1} = 1$ et donc $P(x) = 0$.

On en déduit alors que $P \equiv \mathbb{1}_V$, donc

$$S(P) := \sum_{x \in k^m} P(x) \equiv \#V \mod (p).$$

Par hypothèse sur les degrés des polynômes f_a, il vient que $\deg P < m(q-1)$. On peut donc écrire

$$P = \sum_{|u| < m(q-1)} \alpha_u X^u,$$

où les α_u sont des éléments de k. A partir de là :

$$S(P) = \sum_{x \in \mathbb{F}_q^m} \sum_{|u| < m(q-1)} \alpha_u x^u = \sum_{|u| < m(q-1)} \alpha_u S(X^u),$$

avec

$$\forall u \in \mathbb{F}_q^m : S(X^u) = \sum_{(x_1,\dots,x_m) \in \mathbb{F}_q^m} x_1^{u_1} \dots x_m^{u_m} = \left(\sum_{x_1 \in \mathbb{F}_q} x_1^{u_1} \right) \dots \left(\sum_{x_m \in \mathbb{F}_q} x_m^{u_m} \right) = \prod_{i=1}^{m} S(X^{u_i}).$$

Or, si $|u| < m(q-1)$, il existe $i \in [\![1, m]\!]$ tel que $u_i < q-1$ donc d'après le lemme précédent, $S(X^{u_i}) = 0$ ce qui entraîne que $S(P) = 0$ et le résultat s'ensuit. □

A présent, on utilise le théorème de Chevalley-Warning pour démontrer le théorème d'arithmétique d'Erdös-Gizburg-Ziv.

Théorème (Théorème d'Erdös-Gizburg-Ziv)**.**

Soit n un entier naturel non nul. Alors parmi $2n-1$ entiers $a_1, \dots, a_{2n-1}$, on peut en trouver n dont la somme est divisible par n.

Démonstration. Notons EGZ l'ensemble des entiers naturels vérifiant la propriété énoncée dans le théorème précédent. L'objectif est de montrer que EGZ = $\mathbb{N}$.

Soit p un nombre premier. Montrons que p est élément de EGZ. Soient pour cela $a_1, \dots, a_{2p-1}$ des entiers. Considérons les deux polynômes de $\mathbb{F}_p[X]$ suivants :

$$P_1(X_1, \dots, X_{2p-1}) = \sum_{k=1}^{2p-1} X_k^{p-1},$$

$$P_2(X_1, \dots, X_{2p-1}) = \sum_{k=1}^{2p-1} a_i X_k^{p-1}.$$

Ces deux polynômes vérifient $\deg P_1 + \deg P_2 = 2p-2 < 2p-1$ ont $(0, \dots, 0)$ pour racine commune donc d'après le théorème de Chevalley-Warning, ils possèdent une racine commune non nulle $(x_1, \dots, x_{2p-1})$. D'après le théorème de Lagrange, pour tout x de $\mathbb{F}_p$, $x^{p-1} = 1$ si est seulement si x est non nul donc en notant W l'ensemble des indices i pour lesquels x_i est non nul, il vient

$$P_1(x_1, \dots, x_{2p-1}) = \sum_{i \in W} x_i^{p-1} = |W| = 0.$$

Ainsi, $|W|$ est un entier divisible par p vérifiant $1 \leqslant |W| \leqslant 2p-1$ donc $|W| = p$ et on note $W = \{i_1, \dots, i_p\}$. Vient ensuite

$$P_2(x_1, \dots, x_{2p-1}) = \sum_{j=1}^{p} a_{i_j} = 0$$

donc p divise $a_{i_1} + \dots + a_{i_p}$ et le résultat est démontré.

Montrons à présent que EGZ est stable par multiplication. D'après le théorème fondamental de l'arithmétique, la démonstration sera achevée. Soient donc m et n deux éléments de EGZ. Considérons $a_1, \dots, a_{2mn-1}$ entiers. Étant donné que $n \in$ EGZ, il existe $I_1 \subset \{1, \dots, 2mn-1\}$ de cardinal n tel que

$$\sum_{i \in I_1} a_i \equiv 0 \mod (n).$$

De même, il existe $I_2 \subset \{1, \dots, 2mn-1\} \backslash I_1$ de cardinal n tel que

$$\sum_{i \in I_2} a_i \equiv 0 \mod (n).$$

On termine ce procédé après avoir construit l'ensemble d'indices I_{2m-1} car au bout de $2m-2$ étapes, il reste $2nm - 1 - (2m-2)n = 2n-1$ entiers. Pour tout $j \in \{1, \dots, 2m-1\}$, on considère l'entier c_j défini par

$$\sum_{i \in I_j} a_i = c_j n.$$

Alors comme m est un élément de EGZ, on peut considérer $J \subset \{1, \dots 2m-1\}$ de cardinal m tel que

$$\sum_{j \in J} c_j \equiv 0 \mod (m).$$

À partir de là :

$$\sum_{j \in J} \sum_{i \in I_j} a_i = n \left(\sum_{j \in J} c_j \right) \equiv 0 \mod (mn)$$

ce qui termine la démonstration. □

Remarques : • Il faut savoir que la quantité $2n-1$ dans le théorème d'Erdös-Gizburg-Ziv est incompressible comme le montre l'exemple constitué de $n-1$ "0" et $n-1$ "1".
• Il existe une autre méthode plus combinatoire pour démontrer que les nombres premiers sont éléments de EGZ. Étant donnés p un nombre premier et $a_1, \dots a_{2p-1}$ des entiers, on considère pour tout $J \subset \{1, \dots, 2p-1\}$ la somme $S_J = \sum_{i \in J} x_i$. L'idée est alors de calculer de deux manières différentes la quantité

$$\Sigma = \sum_{J \subset \{1,\dots,2p-1\} \ : \ \#J = p} S_J^{p-1}.$$

Tout d'abord, S_J^{p-1} est la somme de divers monômes de degré $p-1$ faisant intervenir k facteurs ($1 \leqslant k \leqslant p-1$) que l'on peut écrire sous la forme $\lambda x_1^{a_{i_1}} \dots x_{i_k}^{a_{i_k}}$. Ce type de monôme se retrouve, avec le même coefficient, dans le développement de S_J pour $\binom{2p-1-k}{p-k}$ ensembles J distincts : il suffi d'avoir pour J un ensemble contenant $i_1, \dots, i_k$ puis de choisir les $p-k$ indices restants dans les $2p-1-k$ indices disponibles. Ainsi, après le développement complet de Σ, tout monôme est un multiple de $\binom{2p-1-k}{p-k}$ donc est divisible par p. L'entier Σ est donc nul dans $\mathbb{F}_p$.
D'autre part, si aucun des S_j n'était divisible par p, on aurait pour tout J, $S_j^{p-1} \equiv 1 \mod (p)$ et σ est non nul modulo p. Ceci continue une contradiction avec le paragraphe précédent donc il existe J de cardinal p tel que $S_J \equiv 0 \mod (p)$.

Adapté du travail de Paul Alphonse, Justine Velly et Joséphine Boulanger

Chapitre 51

Théorèmes de Schauder et de Cauchy-Arzela-Peano

Références : Chambert-Loir, *Analyse 1*, p 79

Théorème.

Soit E un $\mathbb{R}$-espace vectoriel normé. Soit $C \subset E$ un convexe fermé non vide. Soit $f : C \to C$ une application continue telle que $\overline{f(C)}$ est compact dans E.
Alors f admet un point fixe.

La preuve utilise le lemme suivant, un théorème de point fixe en dimension finie s'appuyant sur le théorème de Brouwer. On le prouvera en remarque.

Lemme.

Soit $C \subset \mathbb{R}^n$ $(n \geqslant 1)$ un convexe compact non vide. Soit $f : C \to C$ une application continue.
Alors f admet un point fixe.

Passons à présent à la preuve du théorème de point fixe de Schauder.

Démonstration. Comme C est fermé et $f(C) \subset C$ relativement compact, $\overline{f(C)}$ est un compact de C. On va utiliser la propriété de Borel Lebesgue pour se ramener à un convexe de dimension fini et utiliser notre lemme.
Soit $n \in \mathbb{N}^*$. Il existe $c_1, ..., c_m \in C$ tels que $\overline{f(C)} \subset \bigcup_{i=1}^{m} B(c_i, \frac{1}{n})$. On considère $E_n = \text{Vect}(c_1, ..., c_m)$ et $C_n = \text{Conv}(c_1, ..., c_m)$. En dimension finie, l'enveloppe convexe d'un compact est compacte [1], donc C_n est compact dans E_n qui est de dimension finie.
On va pouvoir appliquer notre lemme à la fonction suivante :

$$\begin{aligned} f_n : C_n &\to C_n \\ : x &\mapsto \sum_{i=1}^{m} \frac{\max(0,\ \frac{1}{n} - ||f(x) - c_i||)}{\sum_{j=1}^{m} \max(0,\ \frac{1}{n} - ||f(x) - c_j||)} c_i \end{aligned}$$

Par le recouvrement de $f(C_n) \subset \overline{f(C)}$, on a que le dénominateur ne s'annule pas sur C_n, de sorte que f_n est bien continue. Par le lemme il existe donc $x_n \in C_n$ tel que $f_n(x_n) = x_n$.

1. Soit $\mathcal{A}$ une partie de $\mathcal{E}$, espace affine de dimension finie n. Le théorème de Carathéodory donne que tout point de $\text{Conv}(\mathcal{A})$ est combinaison convexe d'au plus $n+1$ éléments de $\mathcal{A}$.
On pose K l'ensemble des $n+1$-uplets de $[0,1]^{n+1}$ dont la somme fait 1. K est un compact de $\mathbb{R}^{n+1}$.
On pose

$$f : \begin{array}{ccc} K \times \mathcal{E}^{n+1} & \to & \mathcal{E} \\ ((t_0, ..., t_n), (A_0, ..., A_n)) & \mapsto & t_0 A_0 + ... t_n A_n \end{array},$$

alors f est continue et comme $\text{Conv}(\mathcal{A}) = f(K \times \mathcal{A}^{n+1})$, $\text{Conv}(\mathcal{A})$ est compact.

Montrons pour conclure que f_n vérifie la propriété suivante :

$$\forall x \in C_n,\ ||f_n(x) - f(x)|| \leqslant \frac{1}{n}.$$

Soit donc $x \in C_n$. Comme $f(x) \in \bigcup_{i=1}^{m} B\left(c_i, \frac{1}{n}\right)$ on pose $I = \{i \in \{1, ..., m\},\ f(x) \in B\left(c_i, \frac{1}{n}\right)\}$ et pour $i \in I$ on prend $y_i \in B(0,1)$ tel que $f(x) = c_i + \frac{1}{n} y_i$. On peut alors écrire :

$$\begin{aligned}
\|f_n(x) - f(x)\| &= \left\| \sum_{i\in I} \frac{\frac{1}{n} - ||f(x) - c_i||}{\sum_{j\in I}(\frac{1}{n} - ||f(x) - c_j||)} c_i - f(x) \right\| \\
&= \left\| \sum_{i\in I} \frac{\frac{1}{n} - ||\frac{1}{n} y_i||}{\sum_{j\in I}(\frac{1}{n} - ||\frac{1}{n} y_j||)} (c_i - f(x)) \right\| \\
&= \left\| \sum_{i\in I} \frac{1 - ||y_i||}{\sum_{j\in I}(1 - ||y_j||)} \frac{1}{n} y_i \right\| \\
&\leqslant \sum_{i\in I} \frac{1 - ||y_i||}{\sum_{j\in I}(1 - ||y_j||)} \frac{1}{n} ||y_i|| \\
&\leqslant \frac{\sum_{i\in I}(1 - ||y_i||)}{\sum_{j\in I}(1 - ||y_j||)} \frac{1}{n} \\
&\leqslant \frac{1}{n}
\end{aligned}$$

On peut maintenant mener le raisonnement suivant : comme $f(C)$ est relativement compact dans C, il existe une extractrice φ et $c \in C$ tels que $f(x_{\varphi(n)}) \to c$. Alors

$$\begin{aligned}
||f_{\varphi(n)}(x_{\varphi(n)}) - c|| &\leqslant ||f_{\varphi(n)}(x_{\varphi(n)}) - f(x_{\varphi(n)})|| + ||f(x_{\varphi(n)}) - c|| \\
&\leqslant \frac{1}{\varphi(n)} + ||f(x_{\varphi(n)}) - c|| \to 0
\end{aligned}$$

donc $x_{\varphi(n)} = f_{\varphi(n)}(x_{\varphi(n)}) \to c$. Or f est continue donc $f(x_{\varphi(n)}) \to f(c)$. Comme on a déjà $f(x_{\varphi(n)}) \to c$, on en déduit que $f(c) = c$ ce qu'il fallait démontrer. □

L'application phare du théorème de Schauder est le théorème de Cauchy-Arzela-Peano.

Théorème.

Soit I un intervalle ouvert de $\mathbb{R}$, Ω un ouvert de $\mathbb{R}^n$ et $f : I \times \Omega \to \mathbb{R}^n$ une application continue. Alors, si $t_0 \in I$ et $y_0 \in \Omega$ sont donnés, le problème suivant admet au moins une solution y de classe $\mathbb{C}^1$ définie sur un certain intervalle dans I de la forme $[t_0 - T, t_0 + T]$ avec $T > 0$.

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

Démonstration. • Cylindre de sécurité
Comme I et Ω sont ouverts, il existe $C_0 = [t_0 - T_0, t_0 + T_0] \times \overline{B}(y_0, r_0)$ un cylindre inclus dans $I \times \Omega$.
C_0 est compact donc f est bornée sur C_0 par une constante M.
Soit $T \leqslant T_0$, et y une solution du problème définie au moins sur $I_0 \subset [t_0 - T, t_0 + T]$. Supposons qu'elle sorte du cylindre $C = [t_0 - T, t_0 + T] \times \overline{B}(y_0, r_0)$ au temps $\tau \in [t_0 - T, t_0 + T]$ alors, par continuité,

$$r_0 = \|y(\tau) - y_0\| = \left\| \int_{t_0}^{\tau} y'(u) \mathrm{d}u \right\| \leqslant TM.$$

Donc si $T \leqslant \min\left(T_0, \frac{r_0}{M}\right)$, alors toute solution définie sur $I_0 \subset [t_0 - T, t_0 + T]$ reste dans la boule $\overline{B}(y_0, r_0)$.
On nommera cylindre de sécurité l'ensemble $[t_0 - T, t_0 + T] \times \overline{B}(y_0, r_0)$.

• Application de Schauder
On note $E = \mathcal{C}([t_0 - T, t_0 + T], \mathbb{R}^n)$ et $C = \mathcal{C}([t_0 - T, t_0 + T], \overline{B}(y_0, r_0))$. Alors E est un $\mathbb{R}$-espace vectoriel

normé et C est un convexe fermé non vide.
Pour $y \in C$, on appelle $\phi(y)$ la fonction définie sur $[t_0 - T, t_0 + T]$ comme suit :

$$\phi(y)(t) = y_0 + \int_{t_0}^{t} f(u, y(u))\mathrm{d}u.$$

Par convergence dominée, ϕ est continue, puis comme $MT \leqslant r_0$, on a $\phi : C \to C$.

Supposons que $\phi(C)$ est relativement compacte, alors par le théorème de Schauder, on a existence d'un point fixe dans C de ϕ, c'est à dire une solution à notre équation différentielle définie sur $[t_0 - T, t_0 + T]$.

• $\phi(C)$ est relativement compacte
$[t_0 - T, t_0 + T]$ est compact.
$\phi(C)$ est bornée par r_0 en norme infinie.
Puis si $y \in C$ et t_1, $t_2 \in [t_0 - T, t_0 + T]$ alors

$$\|\phi(y)(t_1) - \phi(y)(t_2)\| = \left\| \int_{t_2}^{t_1} f(u, y(u)))\mathrm{d}u \right\| \leqslant M\,|t_1 - t_2|\,.$$

On en déduit que les fonctions de $\phi(C)$ sont M-lipschitziennes sur $[t_0 - T, t_0 + T]$, donc forment une famille équicontinue.
Le théorème d'Ascoli permet alors de dire que $\phi(C)$ est relativement compacte. □

Remarques : • L'exemple classique d'application de Cauchy-Peano est le problème suivant

$$\begin{cases} y'(t) = \sqrt{y(t)} \\ y\,(0) = 0 \end{cases}$$

On trouve à ce problème une infinité de solutions de la forme $y(t) = \dfrac{(t - t_0)^2}{4}\mathbb{1}_{[t_0, +\infty[}(t)$.
• Voici à présent la preuve du lemme.

Démonstration. La preuve consiste à construire un homéomorphisme entre C et la boule unité fermée de $\mathbb{R}^d$ pour un certain d, le théorème de Brouwer permet alors de conclure.
Tout d'abord, on se ramène au cas où $0 \in \mathring{C}$ de la manière suivante :

- Si $\mathring{C} \neq \varnothing$, soit $c \in \mathring{C}$, alors $C' = C - c$ est un compact convexe de $\mathbb{R}^n$, $f' : x \mapsto f(x + c) - c$ est une application continue de C' dans lui-même, et l'existence d'un point fixe de f équivaut à l'existence d'un point fixe de f'.
- Si $\mathring{C} = \varnothing$, alors il existe un hyperplan affine de E contenant C. En effet, raisonnons par contraposée et montrons que si C contient $(n + 1)$ points affinement indépendants alors C est d'intérieur non vide.
  Soient $c_0, ..., c_n \in C$ des points affinement indépendants ; alors $(c_1 - c_0, ..., c_n - c_0)$ forme une base de $\mathbb{R}^n$. Notant $(e_1, ..., e_n)$ la base canonique de $\mathbb{R}^n$, et $\varphi \in GL(\mathbb{R}^n)$ l'endomorphisme envoyant e_i sur $c_i - c_0$ pour tout i, l'application affine $F : x \mapsto c_0 + \varphi(x)$ réalise un homéomorphisme [2] de $\Delta = \mathrm{Conv}(e_0, e_1, ..., e_n)$ sur $V = \mathrm{Conv}(c_0, ..., c_n)$ où l'on a noté $e_0 = 0$ et $\mathrm{Conv}(x_0, ..., x_n)$ l'enveloppe convexe de $\{x_0, ..., x_n\}$. Reste à voir que Δ est d'intérieur non vide ; comme on est en dimension finie, on dispose de l'équivalence des normes, on montre donc ici que Δ contient une boule pour la norme infinie. Rappelons que, puisque $e_0 = 0$ on a $\Delta = \left\{ \sum_{i=1}^{n} \lambda_i e_i,\ \lambda_i \geqslant 0,\ \sum_{i=1}^{n} \lambda_i \leqslant 1 \right\}$. On pose $x = \sum_{i=1}^{n} \lambda e_i$ pour un $\lambda > 0$ tel que $\dfrac{3n\lambda}{2} \leqslant 1$. Alors $B = B_{||.||_\infty}\left(x, \dfrac{\lambda}{2}\right) \subset \Delta$. En effet, si $y = \sum_{i=1}^{n} y_i e_i \in B$ alors pour tout i, $|\lambda - y_i| < \dfrac{\lambda}{2}$ donc $y_i \in \left]\dfrac{\lambda}{2}, \dfrac{3\lambda}{2}\right[$ donc $y_i \geqslant 0$ et $\sum_{i=1}^{n} y_i \leqslant \dfrac{3n\lambda}{2} \leqslant 1$ donc $y \in \Delta$.
  On considère alors C comme un convexe de $\mathbb{R}^{n-1}$. Par récurrence sur la dimension, initialisée à 0, dimension pour laquelle C est un singleton et le théorème acquis, on peut donc supposer C d'intérieur non vide.

On suppose donc que $0 \in \mathring{C}$. Cela implique qu'il existe $\varepsilon > 0$ tel que $B(0, \varepsilon) \subset C$. Par ailleurs, comme C est compact il existe $M > 0$ tel que $C \subset B(0, M)$. On considère alors l'application suivante, dite jauge de C :

$$\begin{aligned} \rho : \mathbb{R}^n &\to \mathbb{R}^+ \\ : \ x &\mapsto \inf\{t \geqslant 0 \mid x \in tC\} \end{aligned}$$

Montrons quelques propriétés de ρ :

2. Voir Chambert-Loir

1. $\forall x \in \mathbb{R}^n,\ x \in C \Leftrightarrow \rho(x) \leqslant 1$.
   L'implication directe est claire. Pour l'autre, il faut distinguer deux cas :
   Si $\rho(x) < 1$, alors il existe $t \in [0,1]$ tel que $x \in tC$, donc il existe $c \in C$ tel que $x = tC$. Ainsi $x = (1-t)0 + tc \in C$.
   Si $\rho(x) = 1$, on prend une suite t_n tendant vers 1 telle que $x = t_n c_n$ avec $c_n \in C$. C est compact donc on peut supposer que c_n converge (vers $c \in C$). Alors en passant à la limite, on obtient $x = c \in C$.
2. $\forall x \in \mathbb{R}^n,\ \forall \lambda \in \mathbb{R}^+,\ \rho(\lambda x) = \lambda \rho(x)$.
   En effet, c'est clair pour $\lambda = 0$, et pour $\lambda > 0$ cela résulte de ce que pour tout $t \geqslant 0$: $\lambda x \in tC \Leftrightarrow x \in \dfrac{t}{\lambda} C$.
3. $\forall x \in \mathbb{R}^n,\ \dfrac{||x||}{M} \leqslant \rho(x) \leqslant \dfrac{||x||}{\varepsilon}$. En particulier $\rho(x) = 0 \Leftrightarrow x = 0$.
   En effet, pour tout $x \in \mathbb{R}^n$, $\varepsilon \dfrac{x}{||x||} \in B(0,\varepsilon) \subset C$ donc $x \in \dfrac{||x||}{\varepsilon} C$ donc $\rho(x) \leqslant \dfrac{||x||}{\varepsilon}$.
   Puis pour tout $t \geqslant \rho(x)$ tel que $x \in tC$ on a $\dfrac{x}{t} \in C \subset B(0,M)$ donc $\dfrac{||x||}{t} < M$ donc $\dfrac{||x||}{M} < t$, ainsi : $\dfrac{||x||}{M} \leqslant \rho(x)$.
4. $\forall x, y \in \mathbb{R}^n,\ \rho(x+y) \leqslant \rho(x) + \rho(y)$ et $\forall a, b \in \mathbb{R}^n,\ |\rho(a) - \rho(b)| \leqslant \rho(a-b)$. En particulier, avec 3, ρ est continue sur $\mathbb{R}^n$.
   En effet, pour $x = 0$ ou $y = 0$ le résultat est clair, supposons $\rho(x) > 0$ et $\rho(y) > 0$. Pour tous $t, s > 0$ tels que $x \in tC$ et $y \in sC$ on a $x = tc_x$, $y = sc_y$ avec $c_x, c_y \in C$; comme C est convexe, on a $\dfrac{tc_x + sc_y}{t+s} \in C$ donc $x + y \in (t+s)C$. Passant à la borne inférieure on obtient bien $\rho(x+y) \leqslant \rho(x) + \rho(y)$.
   Soient $a, b \in \mathbb{R}^n$. Supposons $\rho(a) \geqslant \rho(b)$, alors avec $x = a - b$ et $y = b$ l'inégalité précédente donne $|\rho(a) - \rho(b)| = \rho(a) - \rho(b) \leqslant \rho(a-b)$. Le même raisonnement avec $x = a - b$ et $y = a$ quand $\rho(a) \leqslant \rho(b)$ donne finalement le résultat.

On construit alors un homéomorphisme ϕ entre C et $B = \overline{B}(0,1)$ de la manière suivante :

$$\begin{aligned} \phi : C &\to B \\ : x &\mapsto \rho(x)\frac{x}{||x||} \text{ si } x \neq 0, \text{ 0 sinon} \end{aligned}$$

Définissons aussi la fonction ψ, qui sera l'inverse de ϕ :

$$\begin{aligned} \psi : B &\to C \\ : x &\mapsto ||x||\frac{x}{\rho(x)} \text{ si } x \neq 0, \text{ 0 sinon} \end{aligned}$$

Par la propriété 1, ϕ et ψ sont bien à valeurs dans B et C respectivement. Comme ρ est continue et ne s'annule qu'en 0, ϕ et ψ sont continues sur $C\backslash\{0\}$ et $B\backslash\{0\}$ et ne s'annulent qu'en 0. Les inégalités de 3 montrent que ϕ et ψ sont continues en 0. Enfin, la propriété 3 permet d'écrire pour tout $x \in C\backslash\{0\}$ et tout $y \in B\backslash\{0\}$:

$$\begin{aligned} \psi(\phi(x)) = ||\phi(x)||\frac{\phi(x)}{\rho(\phi(x))} = \rho(x)\frac{\rho(x)||x||x}{||x||\rho(x)^2} = x \\ \text{et } \phi(\psi(y)) = \rho(\psi(y))\frac{\psi(y)}{||\psi(y)||} = ||y||\frac{||y||\rho(y)y}{\rho(y)||y||^2} = y \end{aligned}$$

Ainsi ϕ est bien un homéomorphisme de C dans B d'inverse ψ. On peut donc appliquer le théorème de Brouwer à la fonction continue $\phi \circ f \circ \phi^{-1} : B \to B$: elle admet un point fixe $x_0 \in B$, et $\phi^{-1}(x_0) \in C$ est un point fixe de f. □

Adapté du travail de Corentin Caillaud et Karine Beauchard

Chapitre 52

Transformée de Fourier rapide

Références : Cormen, Leiserson, Rivest, Stein, *Algorithmique*, p 827-841

• Problème :
Soient A et B deux polynômes, on veut les multiplier. On suppose qu'ils sont tous deux de degré inférieur ou égal à $n-1$ avec n une puissance de 2.
Si $A(X) = \sum_{j=0}^{n-1} a_j X^j$ et $B(X) = \sum_{j=0}^{n-1} b_j X^j$, alors

$$C(X) = A(X)B(X) = \sum_{j=0}^{2n-1} c_j X^j \text{ avec } c_j = \sum_{k=0}^{j} a_k b_{j-k}.$$

Si on calcule le produit ainsi, on fait $\mathcal{O}(n^2)$ opérations.
On voudrait néanmoins calculer ce produit en $\mathcal{O}(n\log(n))$ opérations.

• Multiplier avec Force, Fougue et Tendresse.
Le polynôme C est de degré inférieur à $2n-1$, il est donc entièrement déterminé par les valeurs prises sur une base du dual de $\mathbb{C}_{2n-1}[X]$.
Si on se donne $2n$ complexes x_i distincts alors les formes linéaires $L_i : P \mapsto P(x_i)$ sont linéairement indépendantes et forment donc une base du dual.
On a ainsi un isomorphisme

$$\begin{array}{ccc} \mathbb{C}_{2n-1}[X] & \to & \mathbb{C}^{2n} \\ P & \mapsto & (P(x_1), ..., P(x_{2n})) \end{array}.$$

De ce constat, on obtient une nouvelle manière de multiplier :

1. On évalue A et B sur une certaine famille $(x_i)_i$ à $2n$ éléments.
2. On multiplie les vecteurs obtenus pour obtenir $C(x_i) = A(x_i)B(x_i)$ ($\mathcal{O}(n)$ opérations).
3. On interpole C à partir des valeurs $C(x_i)$.

Pour évaluer un polynôme en une valeur, on peut utiliser la méthode de Horner :

$$A(x_0) = a_0 + x_0(a_1 + x_0(a_2 + ...)).$$

On a ainsi une évaluation en $\mathcal{O}(n)$ étapes, et donc l'évaluation en $2n$ points de A et B nous coûte $\mathcal{O}(n^2)$ opérations.
On ne parle même pas de l'interpolation qui nécessite l'inversion d'une matrice ($\mathcal{O}(n^3)$) ou le calcul direct par les polynômes de Lagrange ($\mathcal{O}(n^2)$).
La solution à notre problème est donnée par la FFT.

• Évaluation par FFT :
L'idée est de choisir pour les (x_i) les racines de l'unité. On pose $\omega_k^j = \exp\left(\frac{2ik\pi}{j}\right)$. Montrons que l'on peut évaluer A et B en les ω_{2n}^j - $j \in [0, 2n-1]$ - en $\mathcal{O}(n\log(n))$ opérations.

Faisons le pour A :
On pose $A^{[0]}(X) = \sum a_{2j} X^j$ et $A^{[1]}(X) = \sum a_{2j+1} X^j$. Alors $A(X) = A^{[0]}(X^2) + XA^{[1]}(X^2)$.
On doit évaluer $A^{[0]}$ et $A^{[1]}$ en les $(\omega_{2n}^j)^2$. Or $(\omega_{2n}^j)^2 = \omega_n^j = (\omega_{2n}^{n+j})^2$, donc il ne nous reste qu'à faire $2n$

évaluations sur des polynômes de degrés inférieur à $n/2$.

Voici l'algorithme $FFT(A)$:

1. n=degré de A
2. si $n = 1$, retourner A
3. Définition de $A^{[0]}$ et $A^{[1]}$
4. $y^{[0]} = FFT(A^{[0]})$ et $y^{[1]} = FFT(A^{[1]})$
5. Pour $j = 0 : n - 1$ faire
6. $\quad y(j) = y^{[0]}(j) + \omega_{2n}^j y^{[1]}(j)$
7. $\quad y(j+n) = y^{[0]}(j) - \omega_{2n}^j y^{[1]}(j)$
8. renvoyer y

L'avant dernière étape vient juste du fait que

$$A(\omega_{2n}^{n+j}) = A^{[0]}(\omega_n^j) + \omega_{2n}^{n+j} A^{[1]}(\omega_n^j),$$

et $\omega_{2n}^{n+j} = \exp(i\pi)\omega_{2n}^j = -\omega_{2n}^j$.

• Complexité :
On note T la complexité de l'algorithme FFT. Alors, comme les évaluations de $y^{[0]}$ et $y^{[1]}$ requièrent $\mathcal{O}(n)$ opérations, on a

$$T(n) = 2T\left(\frac{n}{2}\right) + \mathcal{O}(n).$$

Écrivons $n = 2^k$, alors on a en divisant par 2^k :

$$\frac{T(2^k)}{2^k} = \frac{T(2^{k-1})}{2^{k-1}} + \mathcal{O}(1).$$

On en déduit que $\frac{T(2^k)}{2^k} = \mathcal{O}(k)$, donc $T(2^k) = \mathcal{O}(k2^k)$.
On a juste à écrire $k = \log_2(n)$ pour obtenir

$$T(n) = \mathcal{O}(n\log(n)).$$

• Interpolation :
Il nous reste à présent à interpoler C à partir des $C(\omega_{2n}^j)$ en $\mathcal{O}(n\log(n))$ opérations.
Cela revient à résoudre le système linéaire suivant :

$$\begin{pmatrix} C(\omega_{2n}^0) \\ C(\omega_{2n}^1) \\ \vdots \\ C(\omega_{2n}^{2n-1}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega_{2n}^1 & \cdots & \omega_{2n}^{2n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \omega_{2n}^{2n-1} & \cdots & \omega_{2n}^{(2n-1)(2n-1)} \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{2n-1} \end{pmatrix}.$$

Appelons V la matrice de Vandermonde à inverser.
On remarque que V^{-1} est donnée par $V_{i,j}^{-1} = \frac{\omega_{2n}^{-ij}}{2n}$.
En effet,

$$(V^{-1}V)_{i,j} = \sum_{k=0}^{2n-1} \frac{\omega_{2n}^{-ik}}{2n} \omega_{2n}^{kj} = \frac{1}{2n} \sum_{k=0}^{2n-1} \omega_{2n}^{k(j-i)} = \delta_{i,j}.$$ [1]

Finalement, on a

$$c_j = \frac{1}{2n} \sum_{k=0}^{2n-1} C(\omega_{2n}^k)\omega_{2n}^{-kj}.$$

Pour calculer C, on doit donc évaluer le polynôme $\widetilde{C}(X) = \frac{1}{2n} \sum_{k=0}^{2n-1} C(\omega_{2n}^k)X^k$ en les $(\omega_{2n}^{-j})_j$. Mais cela, on sait le faire avec la FFT en $\mathcal{O}(n\log(n))$ opérations.

• Conclusion :
On a réussi à multiplier deux polynômes en $\mathcal{O}(n\log(n))$ opérations. Pour cela, on évalue A et B avec la FFT, on fait une multiplication coordonnée par coordonnée, puis on interpole $C = AB$ à nouveau avec la FFT.

1. C'est une série géométrique. Il suffit de calculer.

Remarques : • Il existe beaucoup d'améliorations et de variantes de cet algorithme. On peut en trouver certaines dans le Cormen.
• La grande idée de ce développement est la suivante : "La transformée de Fourier transforme un produit de convolution en un produit.". Une fois cela acquis, tout est assez logique.

Adapté du travail de Alexandre Bailleul et Paul Alphonse.

Chapitre 53

Un anneau principal non euclidien

Références : Perrin, *Cours d'algèbre*, partie II.5

Théorème.

On note $\alpha = \dfrac{1+i\sqrt{19}}{2}$ et $A = \mathbb{Z}[\alpha]$, alors A est un anneau principal, non-euclidien.

Démonstration. **Étape 1 :** α est racine de $P = T^2 - T + 5$, car $\alpha + \overline{\alpha} = 1$ et $\alpha\overline{\alpha} = 5$.
Ainsi, $A = \left\{a + b\alpha \middle| (a,b) \in \mathbb{Z}^2\right\}$ est un sous-anneau de $\mathbb{C}$. [1]
Donc A est intègre ; et comme $\overline{\alpha} = 1 - \alpha$, A est stable par conjugaison.
Pour $z = a + b\alpha \in A$, on définit la norme :

$$N(z) = z\overline{z} = (a+b\alpha)(a+b\overline{\alpha}) = a^2 + ab(\alpha + \overline{\alpha}) + b^2\alpha\overline{\alpha} = a^2 + ab + 5b^2.$$

Alors $N(z) \in \mathbb{N}$ (en réduisant avec la méthode de Gauss), et $N(zz') = N(z)N(z')$.
De plus, $N(z) = 0 \Rightarrow \left(a + \dfrac{b}{2}\right)^2 + \dfrac{19}{4}b^2 = 0 \Rightarrow a = b = 0 \Rightarrow z = 0$.
Soit $z \in A^\times$, alors $N(z)N\left(z^{-1}\right) = 1$ donc $N(z) = 1$.
Alors $\left(a + \dfrac{b}{2}\right)^2 + \underbrace{\dfrac{19}{4}}_{>1} b^2 = 1$, donc $b = 0$ et $a = \pm 1$. Ainsi, $A^\times = \{\pm 1\}$.

Étape 2 : Supposons A euclidien, alors $\exists x \in A\backslash A^\times, \pi_{A/(x)|_{A^\times \cup \{0\}}}$ est surjective.
En particulier, $A/(x)$ est un corps (car des inversibles sont envoyés sur des inversibles) et $\#A/(x) \leqslant 3$, donc $A/(x) = K$, où $K \simeq \mathbb{F}_2$ ou $\mathbb{F}_3$.
On en déduit l'existence d'un morphisme d'anneaux surjectif $\varphi : A \to K$.
Alors $\beta = \varphi(\alpha)$ vérifie $\beta^2 - \beta + 5 = 0$.
Mais cette équation ne possède de solution ni dans $\mathbb{F}_2$, ni dans $\mathbb{F}_3$. [2]
On aboutit à une contradiction, et A n'est donc pas euclidien.

Étape 3 : On introduit une pseudo-division euclidienne.

Lemme.

Soient $a, b \in A\backslash\{0\}$.
Alors il existe $(q,r) \in A^2$, tels que :

1. $N(r) < N(b)$;
2. $a = bq + r$ ou $2a = bq + r$.

Démonstration. Soit $x = \dfrac{a}{b} \in \mathbb{C}$, qu'on écrit aussi $x = u + v\alpha$, où $u, v \in \mathbb{Q}$. On note $n = \lfloor v \rceil$.

1. Car A est un sous-groupe de $\mathbb{C}$, contient 1 et est stable par multiplication.
2. Cela se démontre facilement en cherchant de façon exhaustive.

— Supposons que $v \notin \left]n+\frac{1}{3}, n+\frac{2}{3}\right[$; soient s et t les plus proches entiers de u et v.
Ainsi, $|s-u| \leqslant \frac{1}{2}$ et $|t-v| \leqslant \frac{1}{3}$.
On pose $q = s + t\alpha \in A$ et :

$$N(x-q) = (s-u)^2 + (s-u)(t-v) + 5(t-v)^2 \leqslant \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{9+6+20}{36} = \frac{35}{36} < 1.$$

On pose $r = a - bq = b(x-q)$ et on a $N(r) < N(b)$.

— Supposons désormais que $v \in \left]n+\frac{1}{3}, n+\frac{2}{3}\right[$, alors $2x = 2u + 2v\alpha$ et $2v \in \left]2n+\frac{2}{3}, 2n+1+\frac{1}{3}\right[$ et on est ramené au cas précédent : on peut écrire $2a = bq + r$, avec $N(r) < N(b)$.

□

Étape 4 : Montrons que A est principal.
On a : $A \simeq \mathbb{Z}[T]/(P)$, donc $A/(2) \underset{3}{\simeq} \mathbb{Z}[T]/(2,P) \underset{4}{\simeq} \mathbb{F}_2[T]/(P)$.

Mais $T^2 - T + 5$ est irréductible sur $\mathbb{F}_2$ car de degré 2 sans racine ; donc $A/(2)$ est un corps et (2) est maximal dans A.
Soit $I \neq (0)$ un idéal de A, et soit $a \in I\backslash\{0\}$ de norme $N(a)$ minimale.
Soit $x \in I\backslash(a)$;

→ Si $x = aq + r$ avec $N(r) < N(a)$ ou $r = 0$, alors comme $r \in I$, par minimalité de $N(a)$, on a $r = 0$.
Ainsi $x \in (a)$: contradiction.

→ Ainsi, $2x = aq + r$, et même $2x = aq$ en répétant le procédé qu'on vient à peine de faire.
Comme (2) est maximal, l'idéal (2) est premier, d'où $a \in (2)$ ou $q \in (2)$.
Si $q \in (2)$, alors $q = 2q'$ et $x = aq'$ (par intégrité) donc $x \in (a)$. Contradiction.
Donc $a \in (2)$, c'est à dire : $a = 2a'$.
Comme $q \notin (2)$ et (2) est maximal, on a : $(2,q) = A$, donc $\exists \lambda, \mu \in A, 2\lambda + q\mu = 1$.
Donc $a' = 2\lambda a' + q\mu a' = \lambda a + \mu x \in I$.
Or $0 < N(a') < N(a)$. Contradiction.

Ainsi, $I = (a)$ et A est principal.

□

À présent, prouvons le lemme utilisé.

Lemme.

Soit A un anneau euclidien, alors il existe $x \in A \setminus A^\times$ tel que $\pi_{A/(x)|_{A^\times \cup \{0\}}}$ est surjective.

Démonstration. Si A est un corps, on prend $x = 0$.
Sinon, on prend $x \in A \setminus (A^\times \cup \{0\})$ de stathme minimal parmi les éléments de $A \setminus (A^\times \cup \{0\})$ (existe car le stathme est à valeurs dans $\mathbb{N}$).
Le but est de trouver pour tout $a \in A$, un élément r de $A^\times \cup \{0\}$ tel que $a = r$ dans $A/(x)$. Pour cela on écrit la division euclidienne $a = xq + r$.
Si $r = 0$, c'est bon. Sinon on a $v(r) < v(x)$ donc r est inversible. □

Remarques : • Il est bon de connaître les contre-exemples classiques dans la théorie des anneaux.
— $\mathbb{Z}[i\sqrt{5}]$ est noethérien mais pas factoriel.
— $\mathbb{R}[X_1, X_2, ...]$ est factoriel mais pas noethérien.
— $\mathbb{Z}[X]$ est factoriel non principal.
— $\mathbb{Z}[X]/(2X)$ est noethérien non intègre.

3. Notons $\pi_P : \mathbb{Z}[T] \to \mathbb{Z}[T]/(P)$ et $\pi_{\overline{2}} : \mathbb{Z}[T]/(P) \to (\mathbb{Z}[T]/(P))/(\overline{2})$ les projections canoniques.
Ker $\pi_{\overline{2}} \circ \pi_P = \left\{ f \in \mathbb{Z}[T] \middle| \exists u \in \mathbb{Z}[T], \overline{f} = \overline{2u} \right\} = \{f \in \mathbb{Z}[T] | \exists u, v \in \mathbb{Z}[T], f = 2u + Pv\} = (2,P)$.
Ainsi $\pi_{\overline{2}} \circ \pi_P$ induit un isomorphisme $\mathbb{Z}[T]/(2,P) \simeq (\mathbb{Z}[T]/(P))/(\overline{2}) \simeq A/(2)$.

4. Notons $\pi_2 : \mathbb{Z}[T] \to \mathbb{Z}[T]/(2)$ et $\pi_{\overline{P}} : \mathbb{Z}[T]/(2) \to (\mathbb{Z}[T]/(2))/(\overline{P})$ les projections canoniques.
Ker $\pi_{\overline{P}} \circ \pi_2 = \left\{ f \in \mathbb{Z}[T] \middle| \exists u \in \mathbb{Z}[T], \overline{f} = \overline{Pu} \right\} = \{f \in \mathbb{Z}[T] | \exists u, v \in \mathbb{Z}[T], f = Pu + 2v\} = (2,P)$.
Ainsi $\pi_{\overline{P}} \circ \pi_2$ induit un isomorphisme $\mathbb{Z}[T]/(2,P) \simeq (\mathbb{Z}[T]/(2))/(\overline{P}) \simeq \mathbb{F}_2[T]/(P)$.

• On peut trouver des rappels très clairs à l'adresse suivante :
`http://www.normalesup.org/~crenard/rappelsAnneaux.pdf`
• On peut montrer le même résultat pour $d = 43$, 67 et 163.

Adapté du travail de Florian Lemonnier.

Troisième partie

Développements non utilisés

Chapitre 1

Ancienne version du groupe circulaire

Références : Audin, *Géométrie*, p 203

On définit G le groupe de transformations de $\mathbb{P}_1(\mathbb{C})$ engendré par les homographies et la symétrie $z \mapsto \overline{z}$. Le groupe G contient donc $\mathrm{PGL}_2(\mathbb{C})$ et les inversions.

Théorème.

Le groupe G est exactement l'ensemble des transformations **bijectives** préservant les droites-cercles de $\mathbb{P}_1(\mathbb{C})$.

Démonstration. • On rappelle que pour que quatre points de $\mathbb{P}_1(\mathbb{C})$ soient sur une droite-cercle, il faut et il suffit que leur birapport soit réel. Comme les homographies et la conjugaison conserve le birapport [1], il vient que G conserve les droites-cercles.

• Réciproquement, soit φ une bijection de $\mathbb{P}_1(\mathbb{C})$ préservant les droites-cercles. Pour simplifier, on peut composer φ par une homographie (ce qui ne change pas son appartenance à G) pour que $\varphi(0) = 0$, $\varphi(1) = 1$ et $\varphi(\infty) = \infty$, ainsi elle envoie les cercles sur les cercles et les droites sur les droites.
Commençons par montrer que φ préserve les divisions harmoniques. [2]
Pour cela on va démontrer le lemme suivant :

Lemme.

Soient a, b, $c \in \mathbb{C}$ distincts, pour construire l'unique $d \in \mathbb{P}_1(\mathbb{C})$ tel que $[a, b, c, d] = -1$, il suffit de faire des intersections et des tangentes de droites et de cercles.

Si on prouve ce lemme, on aura terminé car φ préserve la tangence et l'intersection, ainsi que les cercles et les droites. [3] φ ne modifiera pas la figure globale et donc la division harmonique sera conservée.

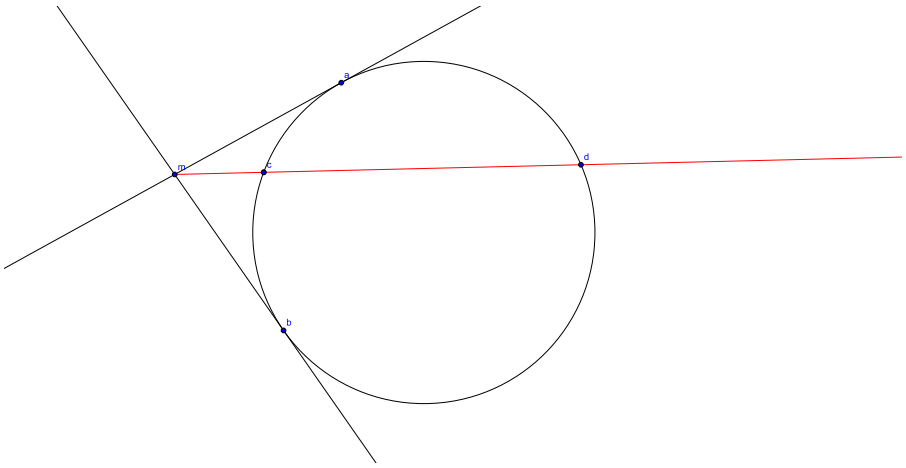
Démonstration. Comme le birapport est réel, les quatre points sont soit cocycliques, soit alignés.

→ Premier cas : a, b, c sont cocycliques.
On peut considérer m l'intersection des tangentes en a et en b (qui peut être à l'infini), alors la deuxième intersection de (mc) avec le cercle est le point d cherché.

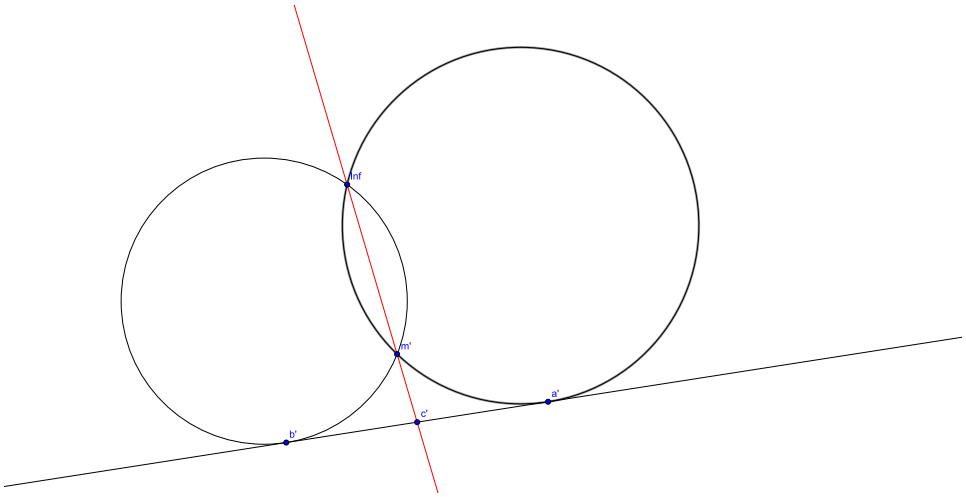
1. Soit h une homographie, f l'unique homographie tel que $[a, b, c, d] = f(d)$ et g l'unique homographie tel que $[h(a), h(b), h(c), h(d)] = g(h(d))$, alors $g \circ h$ est une homographie qui envoie a sur ∞, b sur 0 et c sur 1, donc par unicité $g \circ h = f$, ce qui montre que les homographies conservent le birapport.

2. On rappelle qu'une division harmonique est un quadruplet de points tels que $[a, b, c, d] = -1$. En particulier, si $d = \infty$, $[a, b, c, d] = -1$ donne $\dfrac{c-b}{c-a} = -1$ donc $c = \dfrac{a+b}{2}$, c est le milieu de $[ab]$.

3. En effet, φ envoie une tangente sur une droite qui touche le cercle image. Si elle n'est pas tangente à ce cercle, il y a deux points d'intersections et l'autre point d'intersection n'a pas d'antécédent par φ. De même, l'intersection est préservée car sinon φ envoie deux droites-cercles sécantes sur deux droites-cercles disjoints et le point d'intersection a deux images, ce qui est impossible.



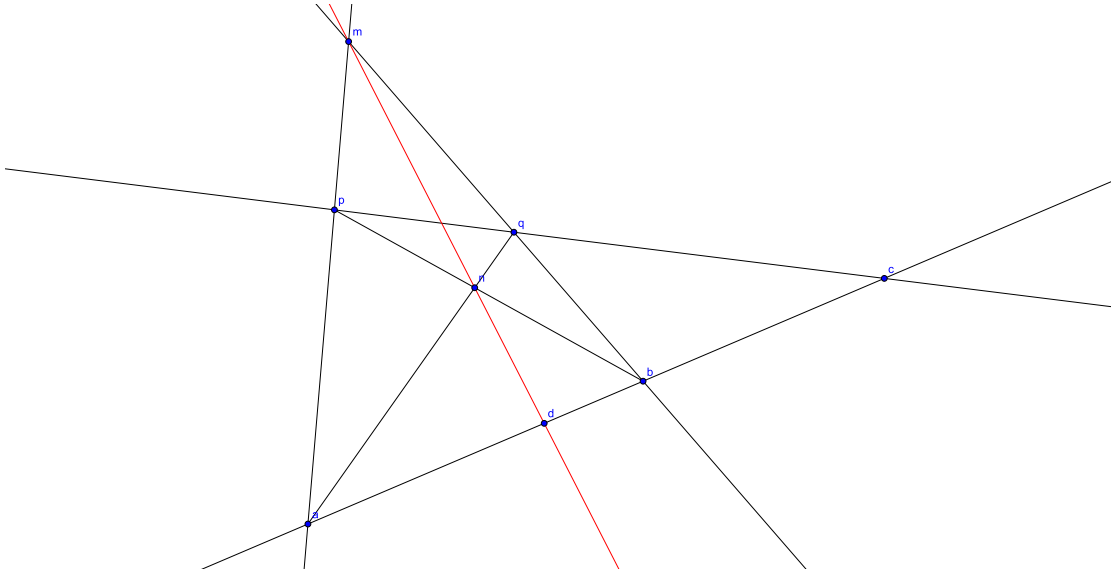
Pour voir cela, on applique une homographie envoyant d à l'infini. On ramène donc l'ancien point à l'infini dans le plan complexe. Nos deux tangentes se transforment en cercles et le cercle devient une droite.



La droite rouge est en fait l'axe radical des deux cercles, donc elle coupe la tangente aux deux en leur milieu. On a donc comme voulu $[a', b', c', \infty] = -1 = [a, b, c, d]$.

→ Second cas : a, b, c sont alignés.
Ici il y a un problème, c peut être situé entre a et b et d peut aussi être à l'infini...
Si quelqu'un peut me dire comment réparer cette preuve, je lui en serai reconnaissant !

Quitte à composer à nouveau par une homographie, on peut supposer b compris entre a et c. On prend m un point différent de l'infini et qui ne soit pas sur la droite (ab). Alors on a un triangle abm. On peut prendre une droite issue de c ne passant ni par m, ni par a et coupant (am) et (bm) en deux points p et q. On note n l'intersection de (pb) et (aq). Alors (mn) coupe (ab) en d le point voulu.



En effet, plaçons nous dans le repère barycentrique (a,b,m), alors si les coordonnées de n sont (α,β,γ) (tous non-nuls et définis à constante multiplicative près), on a $p=(\alpha,0,\gamma)$, $q=(0,\beta,\gamma)$ et $d=(\alpha,\beta,0)$.
À présent, on utilise le fait que p, q et c sont alignés : il existe λ tel que $c=p+\lambda q$. Donc $c=(\alpha,\lambda\beta,(1+\lambda)\gamma)$. Or c est sur la droite (ab), donc $(1+\lambda)\gamma=0$, donc $\lambda=-1$.
Il vient $c=(\alpha,-\beta,0)$ donc

$$[a,b,c,d]=\frac{d-b}{d-a}\times\frac{c-a}{c-b}=-\frac{\alpha}{\beta}\times\frac{\beta}{\alpha}=-1$$

. □

• Fort de ce résultat, nous pouvons maintenant montrer que φ est un morphisme de corps de $\mathbb{C}$.
On a déjà astucieusement modifié φ au départ pour que 0 et 1 soient fixés. On doit juste montrer que φ est additive et multiplicative.
Soient $a,b\in\mathbb{C}$, alors $[a,b,\frac{a+b}{2},\infty]=-1$, donc $[\varphi(a),\varphi(b),\varphi\left(\frac{a+b}{2}\right),\infty]=-1=[\varphi(a),\varphi(b),\frac{\varphi(a)+\varphi(b)}{2},\infty]$, d'où il vient que $\varphi\left(\frac{a+b}{2}\right)=\frac{\varphi(a)+\varphi(b)}{2}$.
En prenant $b=0$, comme $\varphi(0)=0$, il vient $\varphi(a)=2\varphi\left(\frac{a}{2}\right)$. On a donc

$$\varphi(a+b)=\varphi\left(\frac{2a+2b}{2}\right)=\frac{\varphi(2a)+\varphi(2b)}{2}=\frac{2\varphi(a)+2\varphi(b)}{2}=\varphi(a)+\varphi(b)$$

Étudions maintenant la multiplicativité.
Pour cela, on remarque que $[a,-a,a^2,1]=\frac{a^2-a}{a^2+a}\times\frac{1+a}{1-a}=-1$ pour tout $a\in\mathbb{C}$. On a en particulier $[\varphi(a),-\varphi(a),\varphi(a)^2,1]=-1$ et comme φ conserve les divisions harmoniques, $[\varphi(a),\varphi(-a),\varphi(a^2),\varphi(1)]=-1$.
On a $[\varphi(a),-\varphi(a),\varphi(a)^2,1]=[\varphi(a),-\varphi-a),\varphi(a^2),1]$. Donc $\varphi(a^2)=\varphi(a)^2$.
On se rappelle alors astucieusement que $ab=\frac{(a+b)^2-(a-b)^2}{4}$, alors on a

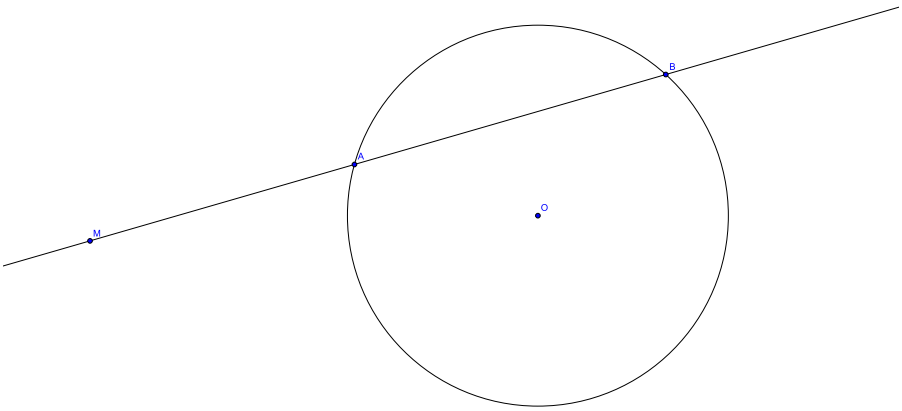
$$4\varphi(ab)=\varphi(4ab)=\varphi((a+b)^2)-\varphi((a-b)^2)=\varphi(a+b)^2-\varphi(a-b)^2=(\varphi(a)+\varphi(b))^2-(\varphi(a)-\varphi(b))^2=4\varphi(a)\varphi(b)$$

Il vient $\varphi(ab)=\varphi(a)\varphi(b)$, donc φ est un morphisme de corps de $\mathbb{C}$.

• Pour finir, φ envoie 0 sur 0, 1 sur 1 et ∞ sur ∞, donc il envoie la droite réelle sur elle-même.
φ est alors uniquement déterminée par $\varphi(i)$, mais $-1=\varphi(i^2)=\varphi(i)^2$, donc $\varphi(i)\in\{1,-1\}$. On en déduit que φ est soit l'identité, soit la conjugaison complexe car $\varphi(a+ib)=a+\varphi(i)b$. Donc $\varphi\in G$. □

Remarques : • Quelques petit rappels :
→ Si f est une isométrie, alors c'est une application affine bijective (voir questions 161). La partie linéaire d'une isométrie est caractérisé par la conservation de la distance, donc du produit scalaire en euclidien. Il résulte de

la théorie de l'adjoint que la partie linéaire vérifie $f^*f = id$ et cela fait le lien avec le groupe orthogonal en choisissant une base.
→ Le théorème à retenir sur le groupe orthogonal est surement son théorème de réduction dont la base est le lemme si F stable par f, alors $F^\perp$ est stable par f^*.
→ Un autre résultat intéressant est le fait que les isométries vectorielles/affines se décomposent en produit d'au plus $n/n+1$ réflexions. On prouve le cas vectoriel par récurrence sur la dimension en trouvant un point fixe x_0 de f et en appliquant l'hypothèse de récurrence sur $x_0^\perp$. Si il n'y a pas de point fixe, on compose par une réflexion d'hyperplan $(x_0 - f(x_0))^\perp$ pour se ramener au premier cas. Pour le cas affine, on trouve un point fixe et on décompose l'isométrie en ce point. Si il n'y a pas de point fixe, on applique la même astuce que auparavant.
→ Une similitude vectorielle est définie par $\|f(x)\| = k\|x\|$ $(k > 0)$; une similitude affine est une application affine de partie linéaire une similitude vectorielle. Dans un plan affine, on peut les mettre sous la forme $z \mapsto az+b$ (directe) et $z \mapsto a\overline{z} + b$ (indirecte) en identifiant le plan à $\mathbb{C}$. Cela est possible grâce au théorème fondamental de décomposition des similitudes : $f = h_k \circ u$ avec h_k une homothétie de rapport k et u une isométrie. Pour le prouver, il suffit de remarquer que $h_k^{-1} \circ f$ conserve la norme donc est une isométrie.
→ Avec ces outils, on peut montrer de manière "non magique" que G conserve les droites-cercles. En effet, soit $\varphi \in G$, alors quitte à composer par une inversion, on peut supposer que $\varphi(\infty) = \infty$. Il en résulte que φ est une similitude que nous savons décomposer en inversions et réflexions. Ainsi G est engendré par les réflexions et inversions. Celles-ci conservent les droites-cercles.
• Le Audin semble trouver évident le fait que toutes les applications préservant les droites/cercles sont bijectives... Je ne vois pas pourquoi ! Il vaut donc mieux le rajouter.
• Il faut maintenant dire un mot à propos de l'axe radical de deux cercles. On définit pour cela la puissance d'un point M par rapport à un cercle de rayon r et de centre O comme $P(M) = OM^2 - r^2$.
On peut alors montrer que pour la figure suivante, on a par la relation de Chasles et Pythagore, $P(M) = \overrightarrow{MA}\overrightarrow{MB}$.
On définit alors l'axe radical de deux cercles comme la droite de points ayant la même puissance par rapport aux deux cercles.
Ramenons-nous au cas nous intéressant. La droite rouge est bien l'axe radical car c'est une droite et elle passe par deux points d'intersections des cercles. Puis en utilisant la relation vue au dessus, on a $P(c') = (c'-a')^2 = (c'-b')^2$, d'où c' est le milieu de a' et b' en développant.



Chapitre 2

Densité des polynômes orthogonaux

Références : Beck, Malick, Peyré, *Objectif agrégation*, p 140
Faraut, *Calcul intégral*, p 163

Soit I un intervalle de $\mathbb{R}$ et ρ une fonction poids. On suppose qu'il existe $a > 0$ tel que

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

Théorème.

Les polynômes orthogonaux associés à ρ forment une base hilbertienne de $L^2(I,\rho)$.

Démonstration. Considérons la fonction

$$\varphi : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \begin{cases} f(x)\rho(x) & \text{si } x \in I \\ 0 & \text{sinon} \end{cases} \end{array}.$$

Étant donné que

$$\forall x \in I : |f(x)|\,\rho(x) \leqslant \frac{1}{2}\left(1 + |f(x)|^2\right)\rho(x),$$

la fonction φ est élément de $L^1(\mathbb{R})$. On peut donc lui associer sa transformée de Fourier $\widehat{\varphi}$ associée au poids ρ. Montrons que $\widehat{\varphi}$ se prolonge en une fonction holomorphe sur

$$B_a = \{z \in \mathbb{C} : |\mathrm{Im}(z)| < a/2\}.$$

Pour cela on considère la fonction

$$g : \begin{array}{ccc} B_a \times I & \to & \mathbb{C} \\ (z,x) & \mapsto & e^{-izx} f(x)\rho(x) \end{array}.$$

Alors :

1. Pour tout $z \in B_a$, la fonction $x \mapsto g(z,x)$ est mesurable.
2. Pour presque tout $x \in I$, la fonction $z \mapsto g(z,x)$ est holomorphe sur B_a.
3. Pour tout $z \in B_a$,
$$|g(z,x)| \leqslant e^{a|x|/2}\,|f(x)|\,\rho(x),$$
la fonction dominatrice étant intégrable sur I par inégalité de Hölder.

Les trois points précédents montrent que la fonction

$$F : \begin{array}{ccc} B_a & \to & \mathbb{C} \\ z & \mapsto & \displaystyle\int_I g(z,x) \end{array}$$

est holomorphe sur B_a. De plus, elle coïncide avec $\widehat{\varphi}$ sur $\mathbb{R}$.

Soit à présent $f \in L^2(I,\rho)$ orthogonale à tous les monômes. D'après le théorème d'holomorphie sous le signe intégral, il vient

$$\forall n \in \mathbb{N} : F^{(n)}(0) = (-i)^n \int_I x^n f(x)\rho(x)\ dx = 0$$

et comme F est holomorphe, elle est nulle sur un voisinage de 0. B_a est connexe donc d'après le principe des zéros isolés, F est identiquement nulle sur B_a. En particulier, $\widehat{\varphi}$ est nulle. Comme φ est intégrable, l'injectivité de la transformée de Fourier sur $L^1(I,\rho)$ montre que φ est nulle. ρ étant une fonction strictement positive, il s'ensuit que f est nulle presque partout sur I.

D'après la caractérisation des parties denses dans les espaces de Hilbert, il s'ensuit que l'ensemble des polynômes orthogonaux est dense dans $L^2(I,\rho)$. En effet, une fonction orthogonale à tous les polynômes orthogonaux est orthogonale à tous les monômes. □

Remarques : • Lorsque l'intervalle I est borné, la démonstration est plus facile grâce au théorème de Weierstrass.
• Un contre-exemple :
Considérons $I =]0,\infty[$ et la fonction poids $\rho : x \mapsto x^{-\ln x}$. Montrons que dans ce cas, les polynômes orthogonaux ne forment pas une base hilbertienne de $L^2(I,\rho)$. Considérons pour cela la fonction

$$f : \begin{array}{ccc} I & \to & \mathbb{R} \\ x & \mapsto & \sin(2\pi \ln x) \end{array}.$$

Soit n un entier naturel. Alors *via* deux changements de variable :

$$\begin{aligned}
\langle f, x^n \rangle &= \int_I x^n \sin(2\pi \ln x) x^{-\ln x}\ dx \\
&= \int_{\mathbb{R}} e^{(n+1)y} \sin(2\pi y) e^{-y^2}\ dy \\
&= e^{(n+1)^2/4} \int_{\mathbb{R}} \exp\left(-\left(y - \frac{n+1}{2}\right)^2\right) \sin(2\pi y)\ dy \\
&= (-1)^{n+1} e^{(n+1)^2/4} \int_{\mathbb{R}} \sin(2\pi t) e^{-t^2}\ dt \\
&= 0
\end{aligned}$$

ainsi, f est une fonction non nulle orthogonale à tous les monômes, ce qui fournit le résultat.

Adapté du travail de Paul Alphonse.

Chapitre 3

Ellipse de Steiner

Références : Mercier, Rombaldi, *Annales du CAPES externe de mathématiques 2009*, p 129-130 + 144-154 + 165-168 (ou dans n'importe quel Mercier contenant le CAPES externe 2009)

Théorème.

Soient $M_1\,(r_1)$, $M_2\,(r_2)$ et $M_3\,(r_3)$ trois points distincts non-alignés du plan affine $\mathcal{P}$ (que l'on identifie à $\mathbb{C}$).
On note $P = (X - r_1)\,(X - r_2)\,(X - r_3)$ et ω, ω' les zéros de P'.
Alors les points $F(\omega)$ et $F'(\omega')$ sont les foyers d'une ellipse tangente aux trois côtés du triangle $M_1M_2M_3$, en leurs milieux (qu'on notera A, B et C).

Démonstration. On va d'abord énoncer et montrer deux lemmes.

Lemme.

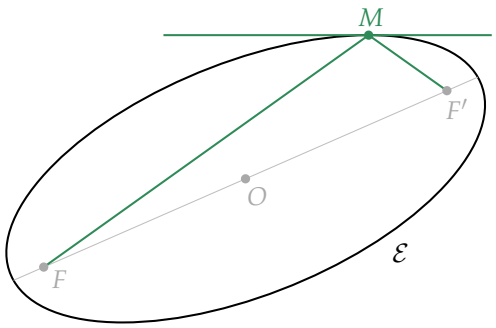
Soient $\mathcal{E}$ une ellipse non-plate et $M \in \mathcal{E}$.
On note F et F' les foyers de $\mathcal{E}$.
Alors la tangente à $\mathcal{E}$ en M est la bissectrice extérieure de $\widehat{FMF'}$. [a]

a. Deux droites ont deux bissectrices. Deux demi-droites ont une bissectrice (que l'on nomme bissectrice intérieure). Si l'on prolonge nos demi-droites, on obtient une deuxième bissectrice qui est la bissectrice extérieure.

Démonstration.

Si O est le centre de l'ellipse, on a la paramétrisation $\overrightarrow{OM(t)} = a\cos t\vec{e_1} + b\sin t\vec{e_2}$ quand $M(t)$ parcourt $\mathcal{E}$.
On dérive l'expression $\left\|\overrightarrow{M(t)F}\right\| + \left\|\overrightarrow{M(t)F'}\right\| = 2a$ et on obtient :

$$\langle \frac{\overrightarrow{M(t)F}}{\left\|\overrightarrow{M(t)F}\right\|}, \frac{\mathrm{d}\overrightarrow{M(t)}}{\mathrm{d}t}\rangle + \langle \frac{\overrightarrow{M(t)F'}}{\left\|\overrightarrow{M(t)F'}\right\|}, \frac{\mathrm{d}\overrightarrow{M(t)}}{\mathrm{d}t}\rangle = 0.$$



Ceci se raccourcit en : $\langle \frac{\overrightarrow{M(t)F}}{\left\|\overrightarrow{M(t)F}\right\|} + \frac{\overrightarrow{M(t)F'}}{\left\|\overrightarrow{M(t)F'}\right\|}, \frac{\mathrm{d}\overrightarrow{M(t)}}{\mathrm{d}t}\rangle = 0$. Mais le premier membre du produit scalaire est le vecteur directeur de la bissectrice intérieure de $\widehat{FMF'}$!
En conséquence : la bissectrice $\left|\begin{array}{l}\text{intérieure}\\ \text{extérieure}\end{array}\right.$ est la $\left|\begin{array}{l}\text{normale}\\ \text{tangente}\end{array}\right.$ à $\mathcal{E}$ en M. □

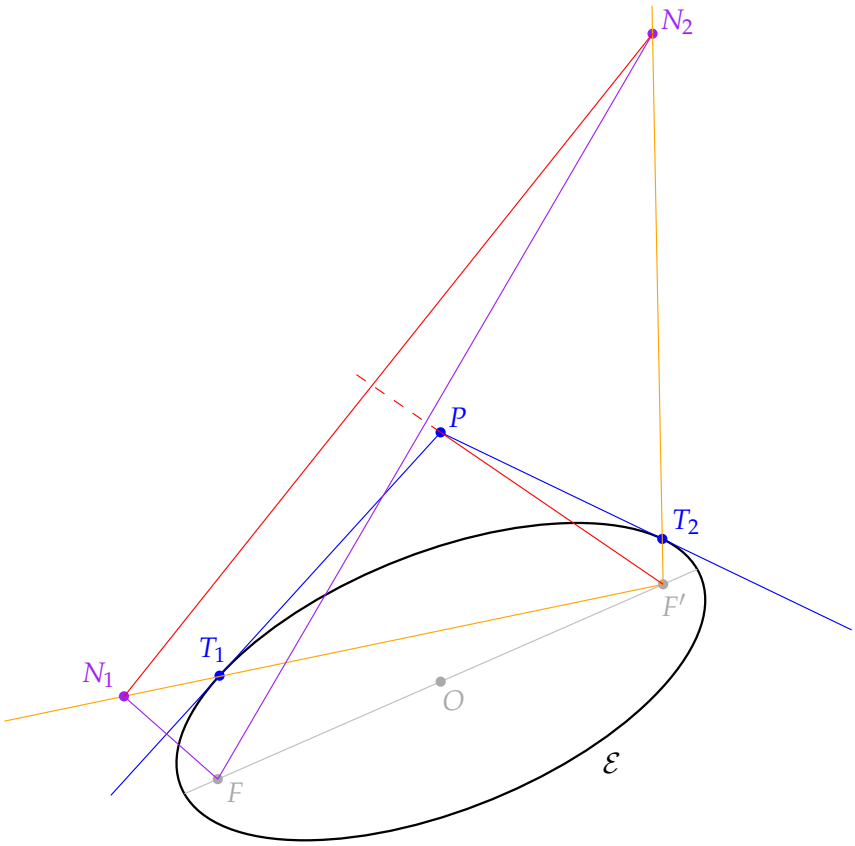
Lemme (Poncelet)**.**

Soit $\mathcal{E}$ une ellipse non-plate de foyers F et F'.
Soit P un point extérieur à $\mathcal{E}$, par lequel passent deux tangentes à $\mathcal{E}$, aux points notés T_1 et T_2.
Alors on a : $\left(\overrightarrow{PT_1}, \overrightarrow{PF}\right) \equiv \left(\overrightarrow{PF'}, \overrightarrow{PT_2}\right)\ [\pi]$.

Démonstration. Si Δ désigne une droite de $\mathcal{P}$, on note σ_Δ la symétrie axiale d'axe Δ.
Ainsi, $\sigma_{(PF)} \circ \sigma_{(PT_1)}$ et $\sigma_{(PT_2)} \circ \sigma_{(PF')}$ sont des rotations de centre de P ; notre but va être de montrer qu'elles sont égales.
On désigne par N_1 et N_2 les symétriques de F par les symétries axiales d'axes (PT_1) et (PT_2).
D'une part, $\sigma_{(PF)} \circ \sigma_{(PT_1)}(N_1) = \sigma_{(PF)}(F) = F$.
D'autre part, comme (PT_1) est tangente à l'ellipse en T_1, c'est la bissectrice extérieure de $\widehat{FT_1F'}$, donc F', T_1 et N_1 sont alignés dans cet ordre.
De même, comme (PT_2) est tangente à l'ellipse en T_2, c'est la bissectrice extérieure de $\widehat{FT_2F'}$, donc F', T_2 et N_2 sont alignés dans cet ordre.
Ainsi, $F'N_1 = F'T_1 + T_1N_1 = F'T_1 + FT_1 = 2a = F'T_2 + FT_2 = F'T_2 + T_2N_2 = F'N_2$.
Aussi, on a : $PN_1 = PF = PN_2$, donc (PF') est la médiatrice de $[N_1N_2]$.
Ainsi, $\sigma_{(PT_2)} \circ \sigma_{(PF')}(N_1) = \sigma_{(PT_2)}(N_2) = F$.
En conséquence, $\sigma_{(PF)} \circ \sigma_{(PT_1)} = \sigma_{(PT_2)} \circ \sigma_{(PF')}$, puis, en regardant les angles de ces rotations :

$$\left(\overrightarrow{PT_1}, \overrightarrow{PF}\right) \equiv \left(\overrightarrow{PF'}, \overrightarrow{PT_2}\right)\ [\pi].$$

□



Démontrons désormais le théorème.

1. On va commencer par vouloir traiter le cas où F et F' sont confondus.
   On a : $P' = 3X^2 - 2(r_1 + r_2 + r_3)X + (r_1r_2 + r_2r_3 + r_3r_1)$.

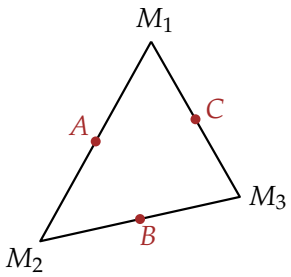
Ainsi, on a les équivalences :

$$\begin{aligned}
P' \text{ a une racine double} &\Leftrightarrow (r_1+r_2+r_3)^2 - 3(r_1r_2+r_2r_3+r_3r_1) = 0\\
&\Leftrightarrow \frac{r_1-r_2}{r_3-r_2} = \frac{r_2-r_3}{r_1-r_3}\\
&\Leftrightarrow \begin{cases} M_1M_2.M_1M_3 = (M_2M_3)^2 \\ \left(\overrightarrow{M_2M_3}, \overrightarrow{M_2M_1}\right) \equiv \left(\overrightarrow{M_3M_1}, \overrightarrow{M_3M_2}\right) \ [2\pi] \end{cases}\\
&\Leftrightarrow \begin{cases} M_1M_2.M_1M_3 = (M_2M_3)^2 \\ M_1M_2 = M_1M_3 \text{ (isocelisme en } M_1) \end{cases}\\
&\Leftrightarrow M_1M_2 = M_2M_3 = M_3M_1\\
&\Leftrightarrow M_1M_2M_3 \text{ est équilatéral}
\end{aligned}$$

Mais le cas du triangle équilatéral est trivial : le cercle inscrit répond à notre problème (il est tangent aux 3 côtés en leurs milieux car les médianes se confondent avec les bissectrices).

2. Désormais, on suppose que $M_1M_2M_3$ n'est pas équilatéral, en conséquence, $F \neq F'$.
On va montrer que $\mathcal{E} = \left\{M \in \mathcal{P} \middle| MF + MF' = AF + AF'\right\}$ répond à notre problème.

   → On a bien $A \in \mathcal{E}$, mais $\mathcal{E}$ est-elle une vraie ellipse, c'est-à-dire non-plate ?
   Pour cela, il suffit de montrer que $A \notin [FF']$.
   Par l'absurde, on suppose que $A \in [FF']$.
   Alors A est barycentre à coefficients positifs de F et F'.
   Mais, par le théorème de Lucas, F et F' sont barycentres à coefficients positifs de M_1, M_2 et M_3 (car P et P' n'ont pas de racine commune).
   Par associativité du barycentre, A est dans l'intérieur strict de $M_1M_2M_3$. Contradiction !



   → On va montrer que (M_1M_2) est tangente à $\mathcal{E}$.
   On note a l'affixe de A, et on calcule $P'(a) = 3(a-\omega)(a-\omega') = (a-r_1)(a-r_2)+(a-r_3)\underbrace{(2a-r_1-r_2)}_{=0}$.
   Ainsi $3(\omega-a)(\omega'-a) = \dfrac{r_2-r_1}{2}\dfrac{r_1-r_2}{2}$, puis $12\dfrac{\omega-a}{r_1-r_2} = \dfrac{r_2-r_1}{\omega'-a}$.
   En passant aux arguments, il vient : $\left(\overrightarrow{M_2M_1}, \overrightarrow{AF}\right) \equiv \left(\overrightarrow{AF'}, \overrightarrow{M_1M_2}\right)\ [2\pi]$.
   Ainsi, $\left(\overrightarrow{M_1M_2}, \overrightarrow{AF}\right) \equiv \left(\overrightarrow{AF'}, \overrightarrow{M_1M_2}\right)\ [\pi]$ donc (M_1M_2) est une bissectrice des droites (AF) et (AF'), nécessairement extérieure à AFF', car sinon (M_1M_2) couperait $[FF']$.
   D'après le lemme 1, (M_1M_2) est tangente à $\mathcal{E}$, en A.

   → On va montrer que (M_1M_3) est tangente à $\mathcal{E}$. [1]
   On a : $P'(r_1) = 3(r_1-\omega)\left(r_1-\omega'\right) = (r_1-r_2)(r_1-r_3)$.
   Ainsi, $3\dfrac{\omega'-r_1}{r_3-r_1} = \dfrac{r_2-r_1}{\omega-r_1}$, donc $\left(\overrightarrow{M_1M_3}, \overrightarrow{M_1F'}\right) \equiv \left(\overrightarrow{M_1F}, \overrightarrow{M_1M_2}\right)\ [2\pi]$.
   On note (M_1T) l'autre tangente à $\mathcal{E}$ issue de M_1. [2]
   Le lemme de Poncelet nous donne : $\left(\overrightarrow{M_1M_2}, \overrightarrow{M_1F}\right) \equiv \left(\overrightarrow{M_1F'}, \overrightarrow{M_1T}\right)\ [\pi]$.
   Donc $\left(\overrightarrow{M_1F'}, \overrightarrow{M_1M_3}\right) \equiv \left(\overrightarrow{M_1M_2}, \overrightarrow{M_1F}\right) \equiv \left(\overrightarrow{M_1F'}, \overrightarrow{M_1T}\right)\ [\pi]$.
   En conséquence, $(M_1M_3) = (M_1T)$ est tangente à $\mathcal{E}$.

   → Enfin, montrons que $C \in \mathcal{E}$. [3]
   On note C' le point de tangence de (M_1M_3) et $\mathcal{E}$.
   Par le lemme 1, (M_1M_3) est bissectrice extérieure de $\widehat{FC'F'}$ en C'.
   Donc G, symétrique de F par rapport à (M_1M_3), vérifie : $G \in (F'C')$, autrement dit $C' \in (F'G)$.
   Ainsi, $C' \in (F'G) \cap (M_1M_3)$.
   Pour montrer que $C = C'$, on va montrer que $C \in (F'G)$.
   En évaluant P' en c, comme on l'avait fait en a précédemment, on obtient que (M_1M_3) est la bissectrice extérieure de l'angle $\widehat{FCF'}$.
   Et donc aussi $C \in (F'G)$.

□

1. On montrerait similairement que (M_2M_3) est tangente à $\mathcal{E}$.
2. Comprenez "autre que (M_1M_2)".
3. On montrerait similairement que $B \in \mathcal{E}$.

Remarques : • L'unicité peut être prouvée en montrant que le cercle incrit est l'unique ellipse vérifiant toutes nos hypothèses pour le triangle équilatéral, puis en envoyant par une homographie toute ellipse de Steiner dans un triangle quelconque sur un cercle inscrit à un triangle équilatéral.
• Le jury attend que le candidat fasse de la géométrie et pas seulement des calculs... Je trouve donc important de donner à l'oral l'idée du premier lemme (dérivation de l'égalité du jardinier) et de démontrer rapidement le théorème de Poncelet, et cela quitte à dire à la fin qu'il suffit de reprendre notre égalité sur P' pour finir la preuve.
• Il y a une autre manière de faire ce développement avec encore plus de calculs dans le Tissier, *Mathematiques Generales*, p 224-227

Adapté du travail de Florian Lemonnier.

Chapitre 4

Exponentielle des matrices symétriques

Références : : Mneimné, Testard, *Introduction à la théorie des groupes de Lie classiques*, p61

Théorème.

L'application exp réalise un homéomorphisme de $\mathcal{S}_n(\mathbb{R})$ sur $\mathcal{S}_n^{++}(\mathbb{R})$.

Démonstration. • Montrons que l'image d'une matrice symétrique est une matrice symétrique définie positive. Soit $A \in \mathcal{S}_n(\mathbb{R})$. La matrice A est orthodiagonalisable en base orthonormée. On dispose de $P \in \mathrm{O}_n(\mathbb{R})$ et d'une matrice diagonale réelle D telles que l'on ait : $A = PD{}^tP$. On a donc : $e^A = Pe^D{}^tP$. D'où il vient que $e^A = {}^t(e^A)$ et que les valeurs propres de e^A sont les exponentielles (réelles) des valeurs propres de A et sont donc réelles strictement positives. Ainsi e^A est bien symétrique définie positive.

- Surjectivité.

Soit $B \in \mathcal{S}_n^{++}(\mathbb{R})$. On dispose de $P \in \mathrm{O}_n(\mathbb{R})$ telle que l'on ait : $B = P \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} {}^tP$, avec les $(\lambda_i)_{1 \leqslant i \leqslant n}$ des réels strictement positifs.

On définit la matrice A comme suit : $A := P \begin{pmatrix} \ln(\lambda_1) & & \\ & \ddots & \\ & & \ln(\lambda_n) \end{pmatrix} {}^tP$. De manière directe on vérifie que $e^A = B$ et que A est une matrice symétrique.

- Injectivité.

Soit A et $\hat{A}$ deux matrices symétriques réelles telles que l'on ait : $e^A = e^{\hat{A}}$.
→ Version MT : en particulier, e^A et $e^{\hat{A}}$ ont le même spectre. Or les éléments du spectre de e^A sont exactement les exponentielles des éléments du spectre de A. Et il en est de même pour $\hat{A}$. Ainsi A et $\hat{A}$ ont le même spectre. [1]
On note $(\lambda_i)_{1 \leqslant i \leqslant n}$ ce spectre. Soit Π un polynôme interpolateur tel que l'on ait : $\forall i \in [\![1, n]\!], \Pi(e^{\lambda_i}) = \lambda_i$.
On montre facilement que $\Pi(e^{\hat{A}}) = \hat{A}$. Donc $\Pi(e^A) = \hat{A}$. De plus A et e^A commutent car e^A est un polynôme en A [2]. Ainsi A et $\hat{A}$ commutent. Étant symétriques, ces deux matrices sont codiagonalisables (dans une base orthonormées commune de vecteurs propres). On dispose de $P \in \mathcal{O}_n(\mathbb{R})$ telle que l'on ait : $A = P \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{pmatrix} {}^tP$ et $\hat{A} = P \begin{pmatrix} \beta_1 & & \\ & \ddots & \\ & & \beta_n \end{pmatrix} {}^tP$, avec $\{\alpha_i / 1 \leqslant i \leqslant n\}$ et $\{\beta_i / 1 \leqslant i \leqslant n\}$ égaux à $\{\lambda_i / 1 \leqslant i \leqslant n\}$. De plus par passage à l'exponentielle, pour tout $i \in [\![1, n]\!]$, on a : $e^{\alpha_i} = e^{\beta_i}$. Ainsi $A = \hat{A}$.
→ Version plus simple : en particulier, e^A et $e^{\hat{A}}$ ont le même spectre. Or les éléments du spectre de e^A sont exactement les exponentielles des éléments de spectre de A. Et il en est de même pour $\hat{A}$. Ainsi A et $\hat{A}$ ont le même spectre. On note $(\lambda_i)_{1 \leqslant i \leqslant n}$ ce spectre. Soit Π un polynôme interpolateur tel que l'on ait : $\forall i \in [\![1, n]\!], \Pi(e^{\lambda_i}) = \lambda_i$.
On a alors $A = \Pi(e^A) = \Pi(e^{\hat{A}}) = \hat{A}$.

1. En fait, ça ne sert pas dans la suite que les matrices ont même spectre...
2. Car e^A est la limite de polynômes de $\mathbb{R}_n[A]$ qui est un sev dans un espace de dim finie, donc fermé.

• Continuité.
La série $\sum \frac{1}{k!}A^k$ converge normalement donc uniformément sur toute boule $B(0,R)$ pour une norme sous-multiplicative. Donc exp est continue sur $B(0,R)$. Elle est donc continue sur $\mathcal{S}_n(\mathbb{R})$. [3]

• Bicontinuité.
Soit une suite $(B_p)_{p\in\mathbb{N}}$ dans $\mathcal{S}_n^{++}(\mathbb{R})$ qui converge vers $B \in \mathcal{S}_n^{++}(\mathbb{R})$. Par bijectivité de l'exponentielle, on dispose d'une suite $(A_p)_{p\in\mathbb{N}}$ dans $\mathcal{S}_n(\mathbb{R})$ et de $A \in \mathcal{S}_n(\mathbb{R})$ telles que l'on ait pour tout p entier $B_p = e^{A_p}$ et $B = e^A$. Le but est de montrer que la suite $(A_p)_{p\in\mathbb{N}}$ converge vers A. on aura donc prouvé la continuité séquentielle de l'inverse de l'exponentielle, et donc sa continuité.

La suite $(B_p)_{p\in\mathbb{N}}$ converge vers B donc en particulier la norme 2 de B_p converge vers celle de B. Donc la plus grande valeur propre de B_p converge vers la plus grande valeur propre de B. En faisant le même raisonnement avec la suite (B_p^{-1}), la plus petite valeur propre de B_p converge vers la plus petite valeur propre de B [4]. Nécessairement les valeurs propres des B_p sont contenues dans un compact de $\mathbb{R}^{+*}$. Les valeurs propres des A_p étant les logarithmes (réels) des valeurs propres des B_p, elles sont aussi contenues dans un compact de $\mathbb{R}$. [5]

Pour tout entier p, on dispose de $Q_p \in \mathrm{O}_n(\mathbb{R})$ et D_p une matrice diagonale telles que l'on ait : $A_p = Q_p D_p {}^{\mathrm{t}}Q_p$. Les suites $(D_p)_{p\in\mathbb{N}}$ et $(Q_p)_{p\in\mathbb{N}}$ sont dans des compacts de $\mathcal{M}_n(\mathbb{R})$. La suite $(A_p)_{p\in\mathbb{N}}$ est donc une suite dans un compact. Elle admet donc des valeurs d'adhérence. Soit φ une extractrice telle que $A_{\varphi(p)} \to \tilde{A}$. Par continuité de l'exponentielle, on a : $e^{\tilde{A}} = e^A$. Par injectivité de l'exponentielle, $\tilde{A} = A$. Ainsi $(A_p)_{p\in\mathbb{N}}$ est une suite dans un compact, qui admet une unique valeur d'adhérence, donc elle converge vers cette valeur d'adhérence. $A_p \to A$. Donc l'exponentielle est bien bicontinue.

Ainsi $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ réalise bien un homéomorphisme.

□

Adapté du travail de Baptiste Huguet.

3. En réalité elle est même analytique.

4. Les B_p sont inversibles car dans $\mathcal{S}_n^{++}$, et l'inverse est une application continue par la formule $B^{-1} = \frac{1}{\det(B)} {}^{\mathrm{t}}\mathrm{com}(B)$.

5. La démonstration du MT est plus complexe : la suite $(B_p)_{p\in\mathbb{N}}$ converge vers B donc la suite de polynôme caractéristique $(\chi_{B_p})_{p\in\mathbb{N}}$ converge vers χ_B. En effet on a continuité de la fonction suivante : $\begin{array}{ccc} \mathcal{M}_n(\mathbb{R}) & \to & \mathbb{R}[X] \\ M & \mapsto & \det(M - XI_n) \end{array}$.
D'après le théorème de Rouché ([MT] chap 2, exo 18), les valeurs propres de B_p convergent vers les valeurs propres de B. Ainsi les valeurs propres des B_p sont contenues dans un compact de $\mathbb{R}^{+*}$.

Chapitre 5

Inégalité de Hardy

Références : Chambert-Loir, Fermigier, Maillot, *Exercices de Mathématiques pour l'agrégation - Analyse 1*, p150

On se place dans $L^p(\mathbb{R}_+)$ avec $p > 1$. Pour toute fonction $f \in L^p(\mathbb{R}_+)$, on définit la fonction F pour presque tout x par :

$$F(x) = \frac{1}{x}\int_0^x f(t)\mathrm{d}t \quad .$$

On a alors le résultat suivant :

Théorème.

La fonction F est dans L^p et sa norme vérifie l'inégalité suivante : $\|F\|_p \leqslant \dfrac{p}{p-1}\|f\|_p$. De plus la constante $\dfrac{p}{p-1}$ est optimale.

Démonstration. Cette démonstration fonctionne par densité. On démontre le théorème pour une classe de fonctions suffisamment régulières, dense dans L^p, puis on prolonge le résultat à L^p.

• Soit $f \in \mathcal{C}^0(\mathbb{R}_+, \mathbb{R}_+) \cap L^p$, une fonction positive. On prolonge alors partout la fonction F en le représentant suivant :

$$F(x) = \begin{cases} f(0) & \text{si} \quad x = 0 \\ \dfrac{1}{x}\displaystyle\int_0^x f(t)\mathrm{d}t & \text{sinon} \end{cases}$$

La fonction F est continue sur $\mathbb{R}_+$ et est de classe $\mathcal{C}^1$ sur $\mathbb{R}_+^*$.
Pour tout $x \in \mathbb{R}_+^*$, on a : $f(x) = (xF(x))' = F(x) + xF'(x)$. D'où l'égalité suivante :

$$\forall x \in \mathbb{R}_+^*,\ F(x) = f(x) - xF'(x) \quad .$$

Soit A un réel strictement positif. Comme toutes les fonctions étudiées sont continues, il est loisible d'intégrer sur le compact $[0, A]$. On a :

$$\int_0^A F^p(x)\mathrm{d}x = \int_0^A F^{p-1}(x)F(x)\mathrm{d}x$$

$$\int_0^A F^p(x)\mathrm{d}x = \int_0^A F^{p-1}(x)f(x)\mathrm{d}x - \int_0^A xF'(x)F^{p-1}(x)\mathrm{d}x \tag{5.1}$$

D'autre part, en réalisant une intégration par partie, on obtient :

$$\begin{aligned}\int_0^A xF'(x)F^{p-1}(x)\mathrm{d}x &= [xF^p(x)]_0^A - \int_0^A F(x)(F^{p-1}(x) + (p-1)xF'(x)F^{p-2}(x))\mathrm{d}x \\ &= AF^p(A) - \int_0^A F^p(x)\mathrm{d}x - (p-1)\int_0^A xF'(x)F^{p-1}(x)\mathrm{d}x\end{aligned}$$

$$\int_0^A F^p(x)\mathrm{d}x = AF^p(A) - p\int_0^A xF'(x)F^{p-1}(x)\mathrm{d}x \tag{5.2}$$

En combinant les équations (5.1) et (5.2), on obtient :

$$\begin{aligned}
\int_0^A F^p(x)\mathrm{d}x &= \int_0^A F^{p-1}(x)f(x)\mathrm{d}x - \frac{1}{p}AF^p(A) + \frac{1}{p}\int_0^A F^p(x)\mathrm{d}x \\
\frac{p-1}{p}\int_0^A F^p(x)\mathrm{d}x &= \int_0^A F^{p-1}(x)f(x)\mathrm{d}x - \frac{1}{p}AF^p(A) \\
\frac{p-1}{p}\int_0^A F^p(x)\mathrm{d}x &\leqslant \int_0^A F^{p-1}(x)f(x)\mathrm{d}x \\
\frac{p-1}{p}\int_0^A F^p(x)\mathrm{d}x &\leqslant \left(\int_0^A F^{(p-1)\frac{p}{p-1}}(x)\mathrm{d}x\right)^{\frac{p-1}{p}}\left(\int_0^A f^p(x)\mathrm{d}x\right)^{1/p} \\
\frac{p-1}{p}\int_0^A F^p(x)\mathrm{d}x &\leqslant \left(\int_0^A F^p(x)\mathrm{d}x\right)^{1-1/p}\left(\int_0^A f^p(x)\mathrm{d}x\right)^{1/p} \\
\frac{p-1}{p}\left(\int_0^A F^p(x)\mathrm{d}x\right)^{1/p} &\leqslant \left(\int_0^A f^p(x)\mathrm{d}x\right)^{1/p}
\end{aligned}$$

En définitive, on a la majoration :

$$\left(\int_0^{+\infty} F^p(x)\mathbb{1}_{[0,A]}(x)\mathrm{d}x\right)^{1/p} \leqslant \frac{p}{p-1}\left(\int_0^{+\infty} f^p(x)\mathrm{d}x\right)^{1/p} \quad .$$

Par convergence monotone [1], on montre que F appartient à L^p et l'on a l'inégalité :

$$\|F\|_p \leqslant \frac{p}{p-1}\|f\|_p \quad .$$

• Soit $f \in \mathcal{C}^0(\mathbb{R}_+,\mathbb{R}) \cap L^p$ (non positive). On pose Φ la fonction $x \mapsto \frac{1}{x}\int_0^x |f|(t)\mathrm{d}t$. La fonction $|f|$ étant continue positive, on peut appliquer le résultat de l'étape précédente. Ainsi Φ appartient à L^p et on a :

$$\|\Phi\|_p \leqslant \frac{p}{p-1}\|f\|_p \quad .$$

De plus $\|F\|_p \leqslant \|\Phi\|_p$ par croissance de l'intégrale. Ainsi pour toute fonction $f \in \mathcal{C}^0(\mathbb{R}_+,\mathbb{R}) \cap L^p$, on a le résultat.

• L'ensemble $\mathcal{C}^0(\mathbb{R}_+,\mathbb{R}) \cap L^p$ est dense dans L^p. Soit $f \in L^p$, on dispose donc d'une suite $(f_n)_{n\in\mathbb{N}}$ qui converge vers f au sens de la norme $\|.\|_p$. Pour presque tout x dans $\mathbb{R}_+$, en appliquant l'inégalité de Hölder, on obtient :

$$\begin{aligned}
|F(x) - F_n(x)| &= \left|\frac{1}{x}\int_0^x (f-f_n)(t)\mathrm{d}t\right| \\
&\leqslant \frac{1}{x}\int_0^{+\infty} \mathbb{1}_{]0,x[}(t)|f-f_n|(t)\mathrm{d}t \\
&\leqslant x^{-\frac{1}{p}}\|f-f_n\|_p
\end{aligned}$$

Ainsi, pour presque tout $x \in \mathbb{R}_+$, $(F_n(x))_{n\in\mathbb{N}}$ converge vers F. De plus en utilisant le lemme de Fatou, on obtient :

$$\begin{aligned}
\int_0^{+\infty} |F(x)|^p\mathrm{d}x &= \int_0^{+\infty} \liminf |F_n(x)|^p\mathrm{d}x \\
&\leqslant \liminf \int_0^{+\infty} |F_n(x)|^p\mathrm{d}x \\
&\leqslant \liminf \left(\frac{p}{p-1}\right)^p \|f_n\|_p^p
\end{aligned}$$

1. En effet, $(F^p(x)\mathbb{1}_{[0,n]})_n$ est une suite croissante de fonctions positives.

Comme cette lim inf est en réalité une limite, on obtient le résultat pour f. Ce qui achève la première partie de la preuve.

- Optimalité.

On définit l'opérateur linéaire $T : \begin{array}{ccc} L^p & \to & L^p \\ f & \mapsto & F \end{array}$.

On a montré que T était un opérateur continu et que sa norme était majorée par la constante $\frac{p}{p-1}$. On va montrer qu'il y a égalité. Soit $s > p$, la fonction $f_s : x \in \mathbb{R}_+^* \mapsto x^{-\frac{1}{s}}$ est dans L^p. Pour tout $x \in \mathbb{R}_+^*$, on a :

$$\begin{aligned} F_s(x) &:= \frac{1}{x}\int_0^x t^{-\frac{1}{s}}\mathrm{d}t \\ &= \frac{1}{x}\left[\frac{s}{s-1}t^{1-1/s}\right]_0^x \\ &= \frac{s}{s-1}x^{-\frac{1}{s}} \\ &= \frac{s}{s-1}f_s(x) \end{aligned}$$

Ainsi, on a : $\|F_s\|_p = \frac{s}{s-1}\|f_s\|_p$. Donc pour tous $s > p$, on a $\frac{s}{s-1} \leqslant \|T\| \leqslant \frac{p}{p-1}$. En faisant tendre s vers p on obtient : $\|T\| = \frac{p}{p-1}$. □

Adapté du travail de Baptiste Huguet.

Chapitre 6

Loi de réciprocité quadratique (avec le résultant)

Références : Mérindol, *Nombres et algèbre*, p 389

Théorème (Loi de réciprocité quadratique)**.**

Soit p et q, deux nombres premiers impairs, distincts. On a : $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$.

Le but est d'exprimer le symbole de Legendre $\left(\frac{p}{q}\right)$ sous la forme d'un résultant de deux polynômes. Pour cela, nous avons besoin d'un lemme portant sur les polynômes.

Lemme.

Soit $R \in \mathbb{Z}[X]$ un polynôme palindromique de degré d pair. Alors, il existe un polynôme $S \in \mathbb{Z}[T]$, de degré $\frac{d}{2}$ tel que l'on ait : $R(X) = X^{d/2} S(X + X^{-1})$.

Démonstration. Les polynômes symétriques élémentaires de $\mathbb{Z}[X,Y]$ sont $\sigma = X+Y$ et $\pi = XY$. Tout polynôme symétrique de $\mathbb{Z}[X,Y]$ s'exprime de manière polynomiale en σ et π, *id est*, si $P \in \mathbb{Z}[X,Y]$ est symétrique, on dispose de $Q \in \mathbb{Z}[X,Y]$ tel que $P(X,Y) = Q(X+Y, XY)$. En particulier, ce résultat est valable pour les polynômes homogènes palindromiques qui sont symétriques.

Soit $R \in \mathbb{Z}[X]$ de degré d pair. On pose $\tilde{R} \in \mathbb{Z}[X,Y]$ son polynôme homogénéisé, définit de la manière suivante : si $R(X) = \sum_{k=0}^{d} a_k X^k$, alors $\tilde{R}(X,Y) = \sum_{k=0}^{d} a_k X^k Y^{d-k}$. On dispose de $Q \in \mathbb{Z}[U,V]$ tel que $\tilde{R}(X,Y) = Q(X+Y, XY)$.

Soit $X^a Y^b$ un monôme de $\tilde{R}$, alors $a+b=d$ et est pair. Donc il n'y a pas de puissance impaire de U dans $Q(U,V)$. De plus $(X+Y)^2 = X^2+Y^2+2XY$ donc on dispose de $\hat{Q} \in \mathbb{Z}[U,V]$ tel que $\tilde{R}(X,Y) = \hat{Q}(X^2+Y^2, XY)$. En outre le degré de Q est $\frac{d}{2}$.

On a : $R(x) = \tilde{R}(X,1) = \hat{Q}(X^2+1, 1)$. Donc $R(x) = X^{d/2}\hat{Q}(X+X^{-1}, 1)$. On pose $S \in \mathbb{Z}[T]$ tel que $S(T) = \hat{Q}(T,1)$. S convient. □

Soit n un entier impair, supérieur à 2. On définit le polynôme $P_n \in \mathbb{Z}[X]$ par $P_n(X) = X^{n-1} + \ldots + X + 1$. C'est un polynôme palindromique de degré pair. On dispose donc de $V_n \in \mathbb{Z}[T]$, de degré $\frac{n-1}{2}$ tel que $P_n(X) = X^{\frac{n-1}{2}} V_n(X+X^{-1})$. On définit enfin $K_n \in \mathbb{Z}[Y]$ par $K_n(Y) = V_n(Y+2)$. Nous avons besoin des résultats suivants sur les polynômes K_n.

Proposition.

i) Pour tout $n > 2$ impair, K_n est unitaire de degré $\dfrac{n-1}{2}$;

ii) Pour tout $n > 2$ impair, $K_n(0) = n$;

iii) Pour tout p premier impair, dans $\mathbb{F}_p[X]$, $K_p(Y) = Y^{\frac{p-1}{2}}$.

Démonstration. i) Cela se vérifie aisément par construction.

ii) On a : $K_n(0) = V_n(2) = V_n(1 + 1/1) = P_n(1) = n$

iii) Pour tout $n > 2$, on a : $P_n(X) = \dfrac{X^n - 1}{X - 1}$. Soit p un nombre premier impair, en se plaçant dans $\mathbb{F}_p[X]$, on a : $X^p - 1 = (X - 1)^p$. Ainsi $P_p(X) = (X - 1)^{p-1}$.

$$\begin{aligned} V_p(X + X^{-1}) &= X^{-\frac{p-1}{2}}(X - 1)^{p-1} \\ &= (X^{-1}(X - 1)^2)^{\frac{p-1}{2}} \\ &= (X + X^{-1} - 2)^{\frac{p-1}{2}} \end{aligned}$$

Et ainsi, dans $\mathbb{F}_p[X]$, on a : $K_p(Y) = Y^{\frac{p-1}{2}}$. □

Nous sommes donc à présent à même d'exprimer le symbole de Legendre comme un résultant.

Proposition.

Soient p et q deux nombres premiers impairs. On a alors :

$$\left(\frac{q}{p}\right) = Res(K_p, K_q) \quad .$$

Démonstration. Si p et q sont égaux le résultat est immédiat car le symbole de Legendre et le résultant sont nuls. On peut donc supposer que p et q sont distincts.

Les polynômes K_p et K_q sont à coefficients entiers, leur résultant est donc un entier. Supposons par l'absurde que ce résultant ne soit pas un élément inversible de $\mathbb{Z}$. Dans ce cas on dispose de $r \in \mathbb{Z}$, nombre premier, qui le divise. En tant que polynôme de $\mathbb{F}_r[X]$, les polynômes K_p et K_q ne sont donc pas premiers entre-eux. On dispose donc d'une extension de corps $\mathbb{L}$ de $\mathbb{F}_r[X]$ et d'un élément $y \in \mathbb{L}$ tel que y soit une racine commune de K_p et K_q.

Quitte à faire une nouvelle extension, on peut supposer que le polynôme $X^2-(y+2)X+1 \in \mathbb{L}[X]$ admette une racine dans $\mathbb{L}$. On la note x. On remarque que x est inversible car il est non nul. ainsi, il vérifie : $x+x^{-1}-2 = y$. On a donc :

$$0 = K_p(y) = V_p(y + 2) = Vp(x + x^{-1}) = x^{-\frac{p-1}{2}} P_p(x) \quad .$$

Ainsi, x est une racine de $X^p - 1$ dans une extension de $\mathbb{F}_r$. C'est de la même manière une racine de $X^q - 1$. Si x était égal à 1, dans ce cas, y serait nul mais ceci est absurde car dans $\mathbb{Z}$, on a $K_p(0) = p$ et $K_q(0) = q$ et p et q ne peuvent pas être tous les deux congrus à 0 modulo r. Donc x est différent de 1. Ceci conduit à une absurdité car 1 est la seule racine p-ième et q-ième de l'unité.

On a donc montrer que le résultant de K_p et K_q était un inversible de $\mathbb{Z}$, *id est* : $Res(K_p, K_q) \in \{-1, 1\}$. Pour conclure on va calculer ce résultant dans F_p.

$$\begin{aligned} Res(K_p, K_q) &= Res(Y^{\frac{p-1}{2}}, K_q) \\ &= [Res(Y, K_q)]^{\frac{p-1}{2}} \\ &= K_q(0)^{\frac{p-1}{2}} \end{aligned}$$

On a donc montré que $Res(K_p, K_q)$ et $\left(\dfrac{q}{p}\right)$ ont la même réduction modulo p. De plus ils sont tous les deux égaux à 1 ou -1. Comme p est impair alors 1 et -1 ont une réduction différente modulo p. Donc on a bien l'égalité annoncée. □

Pour démontrer la loi de réciprocité quadratique, il suffit juste d'utiliser le défaut de symétrie du résultant :

$$\left(\frac{q}{p}\right) = Res(K_p, K_q) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} Res(K_q, K_p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \quad .$$

En plus d'apporter une démonstration de cette loi, la méthode utilisée fournit une expression trigonométrique du symbole de Legendre. En effet, on montre que les racines de V_n sont les $\{\omega_k + \omega_k^{-1}/1 \leqslant k \leqslant \frac{n-1}{2}\}$, où $\omega_k = e^{\frac{2ik\pi}{n}}$. On montre alors que $K_n(Y) = \Pi_{k=1}^{\frac{n-1}{2}}(Y + 4\sin^2\left(\frac{k\pi}{n}\right))$. En utilisant l'expression du résultant avec les racines on obtient l'expression trigonométrique du symbole de Legendre.

Adapté du travail de Baptiste Huguet.

Chapitre 7

Théorème d'Ascoli

Références : Hirsch-Lacombe, *Éléments d'analyse fonctionnelle*

On suppose connu le fait que l'équicontinuité est équivalente à l'uniforme équicontinuité dans $\mathcal{C}(X)$ avec X compact.
C'est bien sur faux dans d'autres espaces de fonctions : par exemple sur $\mathcal{C}(\mathbb{R})$, la fonction carré est continue mais n'est pas uniformément continue. Sur $\mathbb{R}^{+*}$, on a la fonction inverse.

Théorème.

Soit (X,d) un espace métrique compact et $H \subset \mathcal{C}(X)$. On a l'équivalence suivante :

$$H \text{ est relativement compact} \iff H \text{ est bornée et équicontinue.}$$

$\Longrightarrow$ Condition nécessaire.
$\overline{H}$ est une partie compact de $\mathcal{C}(X)$ donc elle est bornée. Ainsi H est bornée. Soit $\varepsilon > 0$, par précompacité de $\overline{H}$, on dispose de $(f_i)_{1\leqslant i\leqslant N}$ dans H tel que l'on ait : $H \subset \bigcup_{i=1}^{N} \mathcal{B}(f_i, \varepsilon/3)$. La famille $(f_i)_{1\leqslant i\leqslant N}$ est finie, elle est donc uniformément équicontinue sur le compact X. On note η le module d'uniforme équicontinuité associé à $\varepsilon/3$. Soit $f \in H$, on dispose de i_0 tel que $f \in \mathcal{B}(f_{i_0}, \varepsilon/3)$. Pour tout$(x,y) \in X^2$ vérifiant $d(x,y) < \eta$, on a donc :

$$|f(x) - f(y)| \leqslant |f(x) - f_{i_0}(x)| + |f_{i_0}(x) - f_{i_0}(y)| + |f_{i_0}(y) - f(y)| \leqslant \varepsilon \quad .$$

Donc H est équicontinue.

Pour le sens réciproque nous allons avoir besoin du lemme suivant.

Lemme.

Soit $(f_n)_{n\in\mathbb{N}}$ une suite équicontinue de $\mathcal{C}(X)$ et $D \subset X$ une partie dense. Si pour tout $x \in D$, la suite $(f_n(x))_{n\in\mathbb{N}}$ converge, alors $(f_n)_{n\in\mathbb{N}}$ converge dans $(\mathcal{C}(X), \|.\|_\infty)$.

Démonstration. On va montrer que la suite $(f_n)_{n\in\mathbb{N}}$ est de *Cauchy* dans $(\mathcal{C}(X), \|.\|_\infty)$ et par complétude de cet espace, elle convergera donc. Soit $\varepsilon > 0$, on dispose de $\eta > 0$ un module d'uniforme équicontinuité associé à $\varepsilon/5$. Par compacité de X, on dispose aussi d'une famille $(x_i)_{1\leqslant i\leqslant N}$ d'éléments de X telle que l'on ait : $X \subset \bigcup_{i=1}^{N} \mathcal{B}(x_i, \varepsilon/5)$. Par densité de D, pour tout $1 \leqslant i \leqslant N$, il existe $y_i \in D \cap \mathcal{B}(x_i, \varepsilon/5)$. Les suites $(f_n(y_i))_{n\in\mathbb{N}}$ sont convergentes donc de *Cauchy*. Ainsi, on a :

$$\exists n_0 \in \mathbb{N}, \forall n,p \geqslant n_0, \forall i, |f_n(y_i) - f_p(y_i)| \leqslant \varepsilon/5 \quad .$$

Soit $x \in X$, on dispose de i tel que $x \in \mathcal{B}(x_i, \varepsilon/5)$. Soit $n,p \geqslant n_0$, on a :

$$\begin{aligned} |f_n(x) - f_p(x)| \leqslant & |f_n(x) - f_n(x_i)| + |f_n(x_i) - f_n(y_i)| + |f_n(y_i) - f_p(y_i)| \\ & + |f_p(y_i) - f_p(x_i)| + |f_p(x_i) - f_p(x)| \\ |f_n(x) - f_p(x)| \leqslant & \varepsilon \end{aligned}$$

En passant au supremum sur les $x \in X$, on obtient : $\forall n, p \geqslant n_0,\ \|f_n - f_p\|_\infty \leqslant \varepsilon$. □

$\Longleftarrow$ Condition suffisante.
H est bornée, donc on dispose de $M > 0$ tel que $\forall f \in H, \|f\|_\infty \leqslant M$. X est compact donc séparable. On dispose donc d'une partie $D \subset X$ dense et dénombrable. Soit $(f_n)_{n\in\mathbb{N}}$ une suite dans H. Pour tout $y \in D$, la suite $(f_n(y))_{n\in\mathbb{N}}$ est une suite dans $[-M, M]$, il existe donc une extractrice φ_y telle que la suite extraite $(f_{\varphi_y(n)}(y))_{n\in\mathbb{N}}$ converge.
D est dénombrable. Par procédé d'extraction diagonale, il existe une extractrice ψ telle que pour tout $y \in D$, $(f_{\psi(n)}(y))_{n\in\mathbb{N}}$ converge. D'après le lemme, $(f_{\psi(n)})_{n\in\mathbb{N}}$ converge dans $(\mathcal{C}(X), \|.\|_\infty)$. Donc H est relativement compact.

Remarques : • Exemples de partie équicontinues de $\mathcal{C}(X)$:
- une partie finie,
- une sous-partie d'une partie équicontinue,
- une union finie de parties équicontinue,
- une suite uniformément convergente de fonctions,
- l'ensemble des fonctions lipschitziennes de constante de Lipschitz fixée.

L'union infinie de parties équicontinues n'est pas forcément équicontinue comme le montre l'exemple de l'ensemble des fonctions lipschitziennes.
• Quelques applications du théorème d'Ascoli :
- le théorème de Cauchy-Arzela-Peano,
- le théorème de Montel (qui donne le théorème de l'application conforme),
- le théorème de Riesz-Fréchet-Kolmogorov
- Les opérateurs à noyau continu de $\mathcal{C}(X)$ dans $\mathcal{C}(Y)$ avec X, Y compacts et pour une mesure finie sur Y sont des opérateurs compacts.

Adapté du travail de Baptiste Huguet.

Chapitre 8

Théorème de Steinhaus

Références : Garet, Kurtzman, *De l'intégration aux probabilités*

Il n'est pas évident d'exhiber des séries entières pour lesquelles le bord du disque de convergence ne contiennent pas de point régulier. Pourtant, c'est un phénomène générique. La démonstration de ce résultat se fait d manière probabiliste. On travaillera dans un espace de probabilité $(\Omega, \mathcal{F}, \mathbb{P})$.

Théorème.

Soient $\sum_{n\geqslant 0} a_n z^n$ une série entière de rayon de convergence 1 et $(X_n)_{n\in\mathbb{N}}$ une suite de variable aléatoire *iid* de loi $\mathcal{U}([0,1])$. Alors presque sûrement, le bord du disque de convergence est une coupure pour la série entière $\sum_{n\geqslant 0} a_n e^{2i\pi X_n z^n}$.

Démonstration.
On souhaite montrer que : $\mathbb{P}(A_r = \varnothing) = 1$, *id est* $\mathbb{P}(A_r \neq \varnothing) = 0$. On note $\mathbb{D}$ le disque ouvert de centre 0 et de rayon 1, Γ son bord et f la somme de la série $\sum_{n\geqslant 0} a_n e^{2i\pi X_n z^n}$, défini sur $\mathbb{D}$. Pour tout $z \in \mathbb{D}$, on note

$$E(z) = \left\{ \omega \in \Omega / \limsup \left| \frac{f^{(n)}(z)}{n!} \right|^{\frac{1}{n}} < \frac{1}{1-|z|} \right\} \quad .$$

- Montrons que l'on a :$\{A_r \neq \varnothing\} = \bigcup_{r\in\mathbb{Q}\cap[0,1]} \bigcup_{\theta\in\mathbb{Q}\cap[0,1]} E(re^{2i\pi\theta})$.

Soit $z \in \mathbb{D}$, alors la série entière $\sum_{n\geqslant 0} \frac{f^{(n)}(z)}{n!} h^n$ a pour rayon de convergence $R(z) \geqslant 1-|z|$ et sa somme coïncide avec $f(z+h)$ pour tout $h \in \mathbb{D}(z, 1-|z|)$. D'après le critère d'Hadamard, on a :

$$\frac{1}{R(z)} = \limsup \left| \frac{f^{(n)}(z)}{n!} \right|^{\frac{1}{n}} \quad .$$

De plus, si jamais l'on a $R(z) > 1-|z|$ alors f se prolonge analytiquement sur $\mathbb{D} \bigcup \mathbb{D}(z, R(z))$. Ainsi pour tout $z \in \mathbb{D}$, on a : $E(z) \subset \{A_r \neq \varnothing\}$. D'où la première inclusion.

Réciproquement, si A_r n'est pas vide, alors on dispose de $u \in \Gamma$ et $\varepsilon > 0$ tel que f se prolonge analytiquement sur $\mathbb{D} \bigcup \mathbb{D}(u, \varepsilon)$. On dispose de $r \in \mathbb{Q} \cap [0,1]$ et $\theta \in \mathbb{Q} \cap [0,1]$ tel que $re^{2i\pi\theta} \in \mathbb{D} \bigcap \mathbb{D}(u, \frac{\varepsilon}{3})$ de sorte que $\mathbb{D}(re^{2i\pi\theta}, \frac{2\varepsilon}{3}) \subset \mathbb{D}(u, \varepsilon)$. On a donc :

$$R(re^{2i\pi\theta}) \geqslant \frac{2\varepsilon}{3} > \frac{\varepsilon}{3} > 1 - |re^{2i\pi\theta}| \quad .$$

Ainsi, on a : $\{A_r \neq \varnothing\} \subset E(re^{2i\pi\theta})$ et donc $\{A_r \neq \varnothing\} = \bigcup_{r\in\mathbb{Q}\cap[0,1]} \bigcup_{\theta\in\mathbb{Q}\cap[0,1]} E(re^{2i\pi\theta})$.

- Montrons que $\forall z \in \mathbb{D}, \quad \mathbb{P}(E(z)) \in \{0,1\}$.

  Soit $n \in \mathbb{N}$, on a :
$$\frac{f^{(n)}(z)}{n!} = \sum_{l=n}^{+\infty} \binom{n+l}{l} a_{n+l} e^{2i\pi X_{n+l}} z^l, \quad \forall z \in \mathbb{D} \quad .$$

La suite des sommes partielles est $\sigma(X_i / i \geqslant n)$-mesurable et convergente. Ainsi, $\frac{f^{(n)}(z)}{n!}$ est une variable aléatoire $\sigma(X_i/i \geqslant n)$-mesurable. Soient $z \in \mathbb{D}$, $N_0 \in \mathbb{N}$ et $N \geqslant N_0$, alors la variable aléatoire $\sup_{n \geqslant N} |\frac{f^{(n)}(z)}{n!}|^{\frac{1}{n}}$ est $\sigma(X_i/i \geqslant N_0)$-mesurable. Ainsi $\limsup |\frac{f^{(n)}(z)}{n!}|^{\frac{1}{n}}$ est une variable aléatoire $\sigma(X_i/i \geqslant N_0)$-mesurable pour tout $N_0 \in \mathbb{N}$. Elle est donc mesurable par rapport à la tribu asymptotique liée à la suite $(X_n)_{n\in\mathbb{N}}$. On en déduit que $E(z)$ est un événement asymptotique. D'après la loi du $0-1$ de Kolmogorov, on a :
$$\forall z \in \mathbb{D}, \quad \mathbb{P}(E(z)) \in \{0,1\} \quad .$$

- Montrons que pour tout $z \in \mathbb{D}$ $\mathbb{P}(E(z))$ ne dépend que de $|z|$.

  Soient $r \in [0,1[$ et $\theta \in [0,1[$, on pose $z = re^{2i\pi\theta}$. On a :
$$\frac{f^{(n)}(z)}{n!} = \sum_{l=n}^{+\infty} \binom{n+l}{l} a_{n+l} e^{2i\pi X_{n+l} + 2i\pi\theta l} r^l \quad .$$

  De plus, on a :
$$\begin{aligned} |\frac{f^{(n)}(z)}{n!}| &= |e^{2i\pi\theta n} \frac{f^{(n)}(z)}{n!}| \\ &= |\sum_{l=n}^{+\infty} \binom{n+l}{l} a_{n+l} e^{2i\pi X_{n+l} + 2i\pi\theta(n+l)} r^l| \end{aligned}$$

On pose $(Y_n)_{n\in\mathbb{N}}$ la suite de variable aléatoire définie par : $\forall n \in \mathbb{N}, \quad Y_n = \{X_n + n\theta\}$, ou $\{\alpha\}$ désigne la partie fractionnaire de α. Les suites $(X_n)_{n\in\mathbb{N}}$ et $(Y_n)_{n\in\mathbb{N}}$ ont la même loi. Pour finir, on pose la fonction mesurable suivante :
$$\begin{array}{rccc} \psi : & [0,1]^{\mathbb{N}} & \to & \bar{\mathbb{R}} \\ & (x_n)_n & \mapsto & \limsup_n |\sum_{k=0}^{+\infty} \binom{n+k}{k} a_{n+k} e^{2i_p i(x_{n+k} + (n+k)\theta)} r \end{array} \quad .$$

Avec cette notation, on a : $E(r) = \{\psi((X_n)_n) < \frac{1}{1-r}\}$ et $E(re^{2i\pi\theta}) = \{\psi((Y_n)_n) < \frac{1}{1-r}\}$. On en déduit donc que $\mathbb{P}(E(r)) = \mathbb{P}(E(re^{2i\pi\theta}))$.

- Conclusion.

Par l'absurde, on suppose que $\mathbb{P}(A_r \neq \varnothing) > 0$. On a donc :
$$\mathbb{P}(\bigcup_{r\in\mathbb{Q}\cap[0,1]} \bigcup_{\theta\in\mathbb{Q}\cap[0,1]} E(re^{2i\pi\theta})) > 0 \quad .$$

On dispose donc de $r_0 \in \mathbb{Q} \cap [0,1]$ et $\theta \in \mathbb{Q} \cap [0,1]$ tel que $\mathbb{P}(E(r_0 e^{2i\pi\theta})) > 0$ D'après les deux étape précédente, on a donc :
$$\forall \theta \in \mathbb{Q} \cap [0,1], \quad \mathbb{P}(E(r_0 e^{2i\pi\theta})) = 1 \quad .$$

Comme $\mathbb{Q}$ est dénombrable, on a donc :
$$\mathbb{P}(E(\bigcap_{\theta\in\mathbb{Q}\cap[0,1]} r_0 e^{2i\pi\theta})) = 1 \quad ,$$

id est presque sûrement, tous les points de Γ sont réguliers. Ceci est absurde car il existe toujours un point singulier. On a donc $\mathbb{P}(A_r \neq \varnothing) = 0$. □

Il est intéressant de remarquer que ce théorème ne permet pas d'exhiber une telle suite $(X_n)_{n\in\mathbb{N}}$.

Adapté du travail de Baptiste Huguet.