Les dev' de Dev'
Développements pour l'agrégation de Mathématiques

Loïc Devilliers

3 décembre 2017

Introduction

Ce document rassemble mes développements ainsi que ma répartition (probablement discutable), * veut dire que ce développement n'est pas tapé. J'espère qu'il ne contient pas de grosses fautes de maths, et je m'excuse d'avance pour le nombre de coquilles et de fautes d'orthographe qui peuvent s'y trouver. Vous pouvez m'envoyer ici vos remarques, suggestions, critiques, ainsi que vos pierres (pour la lapidation).

Ces développements ont généralement été tapés après avoir été travaillés, ils sont donc principalement écrits pour rappel et n'ont pas toujours pour but d'être complètement exhaustifs : les détails importants devraient cependant s'y trouver. Les éléments qui sont dans les parties compléments n'ont pas vocation à être expliquées pendant le développement, seulement ce sont à mon avis des choses à savoir démontrer si le jury vous posait la question.

D'une manière générale, lorsque vous travaillez des développements, n'ayez aucune confiance en ce que vous lisez (que ce soit un livre, un bon livre, un pdf trouvé sur le net, ni même ce document). Soyez toujours sûr que vous pouvez justifier le passage d'une ligne à une autre.

Je tiens à bien préciser que ce document a été écrit pendant que je préparais l'agrégation en 2014. En particulier, il est indépendant de ma fonction actuelle de moniteur dans la préparation à l'agrégation de l'ENS Paris-Saclay.

Je remercie tous ceux qui, pendant l'année de préparation à l'agrégation m'ont prodigué des conseils, des suggestions, des améliorations, des corrections. Je remercie en particulier Jill-Jênn de son aide.

Si vous voulez d'excellents conseils pour l'agrégation je vous recommande ce PDF écrit par Jill-Jênn Vie. Vous y trouverez aussi sa propre liste de développements.

Table des matières

Statistiques du document

- Nombre de développements : 41
- Quatre leçons sans développements : les leçons 122, 216, 262 et 263.
- Une leçon avec un seul développement : la leçon 140
- Probabilité pour tomber sur un couplage d'algèbre constitué de deux leçons avec des impasses [1] : 0.12%.
- Probabilité pour tomber sur un couplage d'analyse constitué de deux leçons avec des impasses : 0.3%.
- En moyenne un développement est utilisé 3.97 fois [2]

1. En supposant le tirage uniforme.
2. Sans compter les leçons avec plus de deux développements.

Bibliographie

[Ave83] A. Avez. *Calcul différentiel.* Maîtrise de mathématiques pures. Masson, 1983.

[BMP04] V. Beck, J. Malick, and G. Peyré. *Mathématiques : objectif agrégation.* H&K, 2004.

[Bru05] Sylvain Bruiltet. Un théorème de joris. *RMS*, (1154), 2005.

[Car81] J.C. Carrega. *Théorie des corps : la règle et le compas.* Actualités scientifiques et industrielles. Formation des enseignants et formation continue. Hermann, 1981.

[CG13] P. Caldero and J. Germoni. *Histoires hédonistes de groupes et de géométries.* Number 1 in Mathématiques en devenir. Calvage et Mounet, 2013.

[Cia82] P.G. Ciarlet. *Introduction à l'analyse numérique matricielle et à l'optimisation.* Collection Mathématiques appliquées pour la maîtrise. Masson, 1982.

[Eid09] J.D. Eiden. *Géométrie analytique classique.* Tableau noir. Calvage & Mounet, 2009.

[FG94] S. Francinou and H. Gianella. *Exercices de mathématiques pour l'agrégation : algèbre 1.* Masson, 1994.

[FGN08] S. Francinou, H. Gianella, and S. Nicolas. *Exercices de mathématiques des oraux de l'École polytechnique et des Écoles normales supérieures : Algèbre.* Number vol. 3 in Enseignement mathématiques. Cassini, 2008.

[Gou08] X. Gourdon. *Analyse : Mathématiques pour MP*.* Ellipses Marketing, 2008.

[GT98] S. Gonnord and N. Tosel. *Calcul différentiel : Thèmes d'analyse pour l'agrégation.* CAPES-agrég mathématiques. Ellipses, 1998.

[HL09] F. Hirsch and G. Lacombe. *Eléments d'analyse fonctionnelle : Cours et exercices avec réponses.* Cours et exercices avec réponses. Dunod, 2009.

[Ouv98] J.Y. Ouvrard. *Probabilités : Tome 1, Capes-Agrégation.* Enseignement des mathématiques. Cassini, 1998.

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

[Pey04] G. Peyré. *L'algèbre discrète de la transformée de Fourier : niveau M1.* Ellipses, 2004.

[QZ13] H. Queffélec and C. Zuily. *Analyse pour l'agrégation : Cours et exercices corrigés.* Sciences sup. Dunod, 2013.

[Rou09] F. Rouvière. *Petit guide de calcul différentiel : à l'usage de la licence et de l'agrégation.* Enseignement des mathématiques. Cassini, 2009.

[Szp09] A. Szpirglas. *Mathématiques Algèbre L3 : Cours complet avec 400 tests et exercices corrigés.* Pearson Education, 2009.

[Zav13] M. Zavidovique. *Un Max de Maths : Problèmes pour agrégatifs et mathématiciens, en herbe ou confirmés.* Im-et-Ker. Calvage et Mounet, 2013.

Chapitre 1

Développements

1.1 Densité des polynômes dans $L^2(I, \omega d\lambda)$

Développement

Soit I un intervalle de $\mathbb{R}$, soit ω une fonction de poids [1], on suppose qu'il existe $\alpha > 0$ tel que $x \mapsto e^{\alpha|x|}\omega(x) \in L^1$. $L^2(I, \omega d\lambda)$ est un espace de Hilbert muni du produit scalaire :

$$\langle f \,|g \rangle = \int_I fg\omega d\lambda$$

Les polynômes [2] sont inclus dans $L^2(I, \omega d\lambda)$, alors par le théorème de Gram-Schmidt, on peut construire une famille orthonormale de polynômes$(P_n)_{n\in\mathbb{N}}$ échelonnée en degré.

Théorème 1.1. *Sous ces hypothèses cette famille est une base hilbertienne de* $L^2(I, \omega d\lambda)$

Démonstration : Montrons donc que $\mathbb{R}[X]$ est dense dans $L^2(I, \omega d\lambda)$ pour ça montrons que $\mathbb{R}[X]^\perp = \{0\}$. Soit f, tel que :

$$\forall n \in \mathbb{N} \ \langle f \,|X^n \rangle = 0$$

Il suffit donc de montrer que $f = 0$.
Posons $g = f\omega\mathbb{1}_I$, alors $g \in \mathbb{L}^1$, donc $\hat{g}(z) = \int_\mathbb{R} e^{-izx} f(x)\omega(x)\mathbb{1}_I dx$ est bien défini. Posons $F(z) = \int_I h(z,x)dx$ où $h(z,x) = e^{-izx}f(x)\omega(x)$, posons $D = \{z \in \mathbb{C} \ / \ |\Im z| < \frac{\alpha}{2}\}$, alors le théorème de dérivation holomorphe des intégrales à paramètre nous dit que F est holomorphe sur D, en effet on peut appliquer ce théorème car :

- $\forall x \in I \ z \mapsto h(x,z)$ est holomorphe sur D
- $\forall z \in D \ x \mapsto h(x,z)$ est mesurable
- $\forall z \in D \ x \mapsto h(x,z)$ est majoré en module par $e^{|\alpha|x/2}|f|\omega$ intégrale sur I car $e^{|\alpha|x/2}, f \in L^2(I, \omega d\lambda)$, donc leur produit dans $L^1(I, \omega d\lambda)$.

Donc $F^{(n)}(z) = \int_I \frac{\partial^n h(z,x)}{\partial z} = \int_I (ix)^n e^{-izx} f(x)\omega(x)dx$ alors $\forall n \in \mathbb{N} \ F^{(n)}(0) = 0$, donc F étant holomorphe on a que F est nul sur un voisinage de 0, et donc $F = 0$ sur D, donc sur l'axe des réels et donc $\hat{g} = 0$, par l'injectivité de Fourier on a que $g = 0$, donc $f = 0$ ($\omega > 0$ sur I). $\square$

1. Continue et strictement positive
2. On fera ici un léger abus en confondant polynômes et fonctions polynomiales.

Remarque 1.2. *Est-ce suffisant de supposer que $X^n \in L^2(\omega d\lambda)$? Non !*
$I = \mathbb{R}^{+*}$, $w(x) = e^{-\ln(x)^2}$, $f(x) = \sin(4\pi \ln(x))$ *n'est pas la fonction nulle, pourtant* $\langle X^n \,| f \rangle = 0$ *:*

Tout d'abord on a $x^2 x^{2n} e^{-\ln(x)^2} = e^{-\ln(x)^2 - (2n+2)\ln(x)} \to 0$, donc on a bien $\mathbb{R}[X] \subset L^2(\omega d\lambda)$.

$$\begin{aligned}
\langle X^n \,| f \rangle &= \int_I x^n \sin(4\pi \ln(x)) e^{-\ln(x)^2} dx \quad \text{On pose } y = \ln(x) \\
&= \int_{\mathbb{R}} e^{(n+1)y} \sin(4\pi y) e^{-y^2} dy \\
&= e^{(\frac{n+1}{2})^2} \int_{\mathbb{R}} e^{-(y - \frac{n+1}{2})^2} \sin(4\pi y) dy \quad \text{On pose } u = y - \frac{n+1}{2} \\
&= e^{(\frac{n+1}{2})^2} \int_{\mathbb{R}} e^{-u^2} \sin(4\pi u) du \quad \text{On a une fonction impaire} \\
&= 0
\end{aligned}$$

Donc f n'est pas dans l'adhérence.

Références

[BMP04]

Leçons concernées

- 201
- 202
- 207
- 209
- 213
- 234
- 239
- 240
- 245

1.2 Processus de Galton-Watson

Développement

Partant d'un homme à la génération 0, on définit la génération $n+1$ comme les hommes issus de la génération n. Un homme a un nombre d'enfants qui suit une variable aléatoire. Toutes ces variables aléatoiressont indépendantes et de même loi X. Chaque homme a k enfants avec une probabilité p_k. On suppose $0 < p_0 < 1$, on note $m = \mathbb{E}(X)$.
Soit Z_n le nombre d'hommes à la n-ième génération, on pose $x_n = \mathbb{P}(Z_0)$ et $G(s) = \mathbb{E}(s^X) = \sum p_k s^k$ la fonction génératrice de X.

Théorème 1.3. *Sous ces conditions si $m \leq 1$, le nom de famille va s'éteindre presque sûrement, et si $m > 1$, le nom de famille va s'éteindre avec une probabilité non nulle.*

Démonstration :

- Soit A l'événement la famille s'éteint, $A = \cap\{Z_n = 0\}$ qui est une réunion croissante, donc $\mathbb{P}(A) = \lim \mathbb{P}(Z_n = 0) = \lim x_n$
- On a $Z_{k+1} = X_1 + \ldots + X_{Z_k}$, alors :

$$\begin{aligned}
G_{Z_{k+1}}(s) &= \mathbb{E}\left(\sum_n \mathbb{1}_{Z_k=n} s^{X_1+\ldots+X_{Z_k}}\right) \\
&= \sum \mathbb{E}\left((1_{Z_k=n}) s^{X_1+\ldots+X_{Z_n}}\right) \\
&= \sum \mathbb{P}(Z_k = n)\mathbb{E}(s^{X_1+\ldots+X_{Z_n}}) \\
&= \sum \mathbb{P}(Z_k = n)\mathbb{E}(s^X)^n \\
&= G_{Z_k}(G(s))
\end{aligned}$$

  Donc par une récurrence immédiate on que la fonction génératrice de Z_n est $G \circ \ldots \circ G = G^n$.
- Sur $[0,1]$ on a $G'(s) = \sum p_k k s^{k-1}$ et $G''(s) = \sum p_k k(k-1)s^{k-2}$:
  Comme $p_0 < 1$, il y a au moins un $k \in \mathbb{N}^\star$ tel que $p_k > 0$, par suite G' est strictement positive sur $]0,1]$, donc G est strictement croissante.
  $G'' \geq 0$, donc G est convexe, si $p_0 + p_1 = 1$, alors G est une droite, sinon il existe $k \geq 2$ tel que $p_k > 0$, et donc $G'' > 0$ sur $]0,1[$, donc G est strictement convexe dans ce cas.
- Étudions la suite x_n, $(Z_n = 0) \subset (Z_{n+1} = 0)$ donc x_n est une suite croissante majorée (par 1) donc converge vers p, de plus $x_n = G_n(0) = G \circ G_{n-1}(0) = G(x_{n-1})$ comme G est continue sur $[0,1]$ on a donc par passage à la limite $G(p) = p$, soit u un point fixe, alors $x_1 = p_0 = G(0) < G(u) = u$, alors par récurrence $x_{n+1} = G(x_n) < G(u) = u$, ainsi p est la plus petite racine positive de $G(x) - x = 0$.
- $m = \mathbb{E}X = \lim \frac{g(1)-g(x)}{1-x}$ alors
  — Si $m > 1$, alors il existe α tel que $f(\alpha) < \alpha$) donc $f(x) - x$ s'annule par le théorème des valeurs intermédiaires pour un $p \in]0, \alpha[$ donc la famille s'éteind avec probabilité p (il y a au plus un point fixe dans $[0,1[$ disons $0 < a < b < 1$, par application deux fois du théorème de Rolle, on aurait l'existence d'un $c \in]a,b[$ tel que $G''(c) = 0$ ce qui contredit le caractère strictement convexe de G, en effet il existe $k \geq 2$ tel que $p_k \neq 0$
  — Si $m < 1$, soit s un point fixe de G, par convexité de G, $s = G(s) \geq m(s-1) + 1$, soit $s(1-m) \geq (1-m)$, donc $s \geq 1$, donc $s = 1$, il y a extinction avec probabilité 1.

— Si $m = 1$ et supposons qu'il y ait un point fixe dans $]0,1[$, alors la demi-tangente est en dessous de la courbe, la corde reliant (p,p) à $(1,1)$ et en dessus de $G_{|[p,1]}$ donc $G = Id_{[p,1]}$ mais par prolongement analytique $G = Id$, donc $p_0 = 0$, ce qui est absurde, il y a donc un seul point fixe : 1, et donc extinction presque sûrement.

□

Remarque

On pourrait remarquer que montrer le cas $m = 1$ implique le cas $m < 1$, en effet si on fait des enfants suivant la variable aléatoire X, avec $\mathbb{E}X < 1$, on peut toujours trouver une variable aléatoireY positive telle que $\mathbb{E}X + Y = 1$ dont on est sûr qu'il y aura extinction, mais « qui peut le plus peut le moins », en produisant X enfants au lieu de $X + Y$ on ne risque pas d'échapper à l'extinction.

Leçons concernées

- 223
- 229
- 243
- 244
- 253
- 260
- 261
- 264

1.3 Dénombrement d'une équation diophantienne

Développement

Soit $(a_1, \ldots, a_p)$ des entiers naturels premiers dans leur ensemble, on note S_n le nombre de p-uplets d'entiers naturels de l'équation diophantienne suivante : $a_1 x_1 + \ldots a_p x_p = n$.

Proposition 1.4. $S_n \underset{+\infty}{=} \frac{1}{\alpha_1 \alpha_2 \ldots \alpha_p} \frac{n^{p-1}}{(p-1)!} + O(n^{p-2})$

Démonstration :
On pose $F(X) = \sum\limits_{n \geq 0} S_n X^n = \prod\limits_{i=1}^{p} \sum\limits_{n_l} X^{a_i n_l} = \prod\limits_{i=1}^{p} \frac{1}{1 - X^{\alpha_i}}$ cette fraction rationnelle a pour pôle les racines a_i-ième de l'unité, le pôle 1 est d'ordre p. Les autres sont d'ordre au plus p, si l'un d'eux était d'ordre p, il serait racine de tous les $1 - X^{a_i}$, donc son ordre divise tous les a_i, donc vaut 1. Donc la multiplicité d'un pôle ω différent de 1 de F vérifie $m_\omega \leq p - 1$.

Par décomposition en éléments simples on a en notant P l'ensemble des pôles de F :

$$F(X) = \sum_{\omega \in P} \sum_{k=1}^{m_\omega} \frac{\alpha_{\omega,k}}{(\omega - X)^k}$$

$$(1 - X)^p F(X) = \prod_{i=1}^{p} \frac{1}{1 + X + \ldots + X^{\alpha_i - 1}} \underset{X \to 1}{\to} \frac{1}{a_1 a_2 \ldots a_p} = \alpha_{1,p}$$

$$\begin{aligned}
\frac{1}{(\omega - X)^k} &= \frac{1}{(k-1)!} \left(\frac{1}{\omega - X} \right)^{(k-1)} \\
&= \frac{1}{\omega (k-1)!} \left(\frac{1}{1 - X/\omega} \right)^{(k-1)} \\
&= \frac{1}{\omega (k-1)!} \left(\sum \omega^{-n} X^n \right)^{(k-1)} \\
&= \frac{1}{\omega (k-1)!} \sum_{n \geq k-1} n(n-1) \ldots (n-k+2) \omega^{-n} X^{n-k+1} \\
&= \frac{1}{(k-1)!} \sum_{n \geq 0} (n+1)(n+2) \ldots (n+k-1) \omega^{-n-k} X^n \\
F(X) &= \sum_{\omega \in P} \sum_{k=1}^{m_\omega} \frac{\alpha_{\omega k}}{(k-1)!} \sum_{n \geq 0} (n+1)(n+2) \ldots (n+k-1) \omega^{-n-k} X^n \\
&= \sum_{n \geq 0} \sum_{\omega \in P} \sum_{k=1}^{m_\omega} \beta_{n,\omega,k} X^n \\
S_n &= \sum_{\omega \in P} \sum_{k=1}^{m_\omega} \beta_{n,\omega,k} = \beta_{n,1,p} + \sum_{\omega \in P} \sum_{\substack{k=1 \\ k \neq p}}^{m_\omega} \beta_{n,\omega,k}
\end{aligned}$$

et $\beta_{n,\omega,k} = O(n^{k-1})$, ainsi $S_n = \frac{1}{a_1 a_2 \dots a_p} \frac{n^{p-1}}{(p-1)!} + O(n^{p-2})$

$\square$

Références

[Gou08]

Leçons concernées

- 124
- 126
- 140
- 190
- 224
- 243
- 244

1.4 Polygones constructibles à la règle et au compas

Développement

On cherche à quelle condition sur n on peut construire dans le plan le polygone régulier à n côtés inscrit dans le cercle unité (on assimile le plan aux nombres complexes) dont l'un des sommet est 1 avec uniquement la règle (non gradué) et au compas :

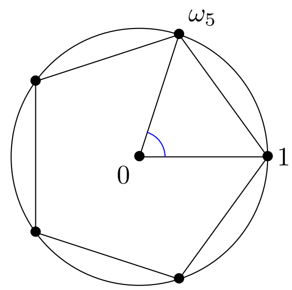

FIGURE 1.1 – Un pentagone régulier inscrit dans le cercle unité dont l'un des sommet et 1 est constructible si et seulement si ω_5 l'est.

Théorème 1.5. *Le polygone à n régulier à n cotés est constructible si et seulement si n est de la forme $n = 2^a p_1 \times \ldots \times p_r$ où les p_i sont des nombres de Fermat premiers distincts (de la forme de $2^\gamma + 1$)*

Démonstration :

- Avec les conditions fixés la construction est équivalente à construire $\omega_n = e^{\frac{2i\pi}{n}}$, on peut écrire $n = 2^a p_1^{a_1} \ldots p_r^{a_r}$, avec $p_1, \ldots, p_r$ des nombres premiers distincts impairs.
- Si ω_n constructible et $d|n$ alors $\omega_d = \omega_n^{\frac{n}{d}}$ constructible, donc les $p_i^{a_1}$ sont constructibles or $\Phi_{p_i^{a_i}}$ est le polynôme minimal de $\omega_{p_i^{a_i}}$ (car $\Phi_{p_i^{a_i}}$ annule $\omega_{p_i^{a_i}}$ et est irréductible sur $\mathbb{Q}[X]$), qui est de degré $(p_i - 1)p_i^{a_i - 1}$ par le théorème de Wantzel ce doit être une puissance de 2, donc $a_i = 1$ et $p_i = 2^\gamma + 1$ est un nombre de Fermat.
- Réciproquement montrons que ces nombres conviennent :
  — ω_{2^a} est constructible, (il suffit de raisonner par récurrence en effectuant des bissectrices au compas)
  — Montrons que $\omega = \omega_p$ est constructible si p est un nombre de Fermat. On considère $G = Aut(\mathbb{Q}[\omega])$, un automorphisme de corps sur $\mathbb{Q}[\omega]$ envoie ω (racine de Φ_p) sur une racine de Φ_p alors on a : $\begin{pmatrix} G & \to & (\mathbb{Z}/p\mathbb{Z})^\star \\ \sigma & \mapsto & m/\sigma(\omega) = \omega^m \end{pmatrix}$ est un isomorphisme de groupe, ainsi G est cyclique d'ordre $p - 1 = 2^q$. Soit σ un générateur de G on pose

$$L_k = \left\{ z \in \mathbb{Q}[w], \sigma^{2^k}(z) = z \right\} \text{ pour } k \in [\![0, q]\!]$$

Pour tout $k \in [\![0, q]\!]$, L_k est un corps, de plus on a :

$$\mathbb{Q} \subset L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_q = \mathbb{Q}[\omega]$$

(car $\sigma^{2^q} = \mathrm{Id}$). Fixons $k \in [\![1, q]\!]$, on a $L_{k-1} \subsetneq L_k$, en effet, posons :

$$x = \sum_{m=0}^{2^{q-k}-1} \sigma^{2^k m}(\omega)$$

i) On a $x \in L_k$ car σ est un morphisme additive et car :

$$\forall m \in [\![0, 2^{q-k}-2]\!] \quad \sigma^{2^k}(\sigma^{2^k m}(\omega)) = \sigma^{2^k(m+1)}(\omega) \text{ et } \sigma^{2^k}(\sigma^{2^k(2^{q-k}-1)}(\omega)) = \sigma^{2^q}(\omega) = \omega$$

ii) De plus, $x \notin L_{k-1}$. En effet, supposons que $x \in L_{k-1}$ alors :

$$\sum_{m=0}^{2^{q-k}-1} \sigma^{2^k m}(\omega) = \sum_{m=0}^{2^{q-k}-1} \sigma^{2^{k-1}+2^k m}(\omega) \tag{1.1}$$

Dans ce cas, on remarque que les termes de ces deux sommes sont des puissances de ω et appartiennent à la base $\mathcal{B}$ de $\mathbb{Q}[\omega]$ où $\mathcal{B} = (1, \omega, \ldots, \omega^{p-1})$. Le membre de gauche de (1.1) a 1 comme coordonnée sur ω, en effet, pour $m \in [\![0, 2^{q-k}-1]\!]$

$$\begin{aligned} \sigma^{2^k m}(\omega) = \omega \quad &\iff \quad \sigma^{2^k m} = \mathrm{Id} \\ &\iff \quad 2^q | 2^k m \\ &\iff \quad 2^{q-k} | m \\ &\iff \quad m = 0 \end{aligned}$$

Tandis que le membre de droite de (1.1) a 0 comme coordonnée sur ω, en effet pour $m \in [\![0, 2^{q-k}-1]\!]$,

$$\begin{aligned} \sigma^{2^{k-1}+2^k m}(\omega) = \omega \quad &\iff \quad \sigma^{2^{k-1}+2^k m} = \mathrm{Id} \\ &\iff \quad 2^q | 2^{k-1}(1+2m) \Longrightarrow 2 | 2^{q+1-k} | (1+2m) \end{aligned}$$

Comme la décomposition d'un vecteur dans la base $\mathcal{B}$ devrait être unique, on obtient alors une contradiction. Ainsi $L_{k-1} \subsetneq L_k$.

En passant par la formule des dimensions on a :

$$2^q = [\mathbb{Q}[\omega] : \mathbb{Q}] = \underbrace{[L_q : L_{q-1}]}_{\geq 2} \underbrace{[L_{q-1} : L_{q-2}]}_{\geq 2} \ldots \underbrace{[L_1 : L_0]}_{\geq 2} \underbrace{[L_0 : \mathbb{Q}]}_{\geq 1}$$

On a donc $[L_k, L_{k-1}] = 2$ pour tout $k \in [\![1, q]\!]$ et $L_0 = \mathbb{Q}$. Par le théorème de Wantzel, ω est constructible.

— Si ω_a et ω_b sont constructibles avec $a \wedge b = 1$ alors ω_{ab} constructible, en effet prenons $au + bv = 1$ avec $u, v \in \mathbb{Z}$, alors $\omega_{ab} = \omega_a^v \omega_b^u$.

□

Complément et remarques

Remarque 1.6. *On a fait ici de la théorie de Galois sans le dire, lorsqu'on a fait correspondre L_k et σ^{2^k}. On aurait pu utiliser un théorème de Galois qui aurait directement affirmer que les L_k étaient deux-à-deux distincts, mais cela aurait été dommage d'utiliser un théorème si fort, alors que dans ce cas particulier il existe une démonstration assez simple.*

Remarque 1.7. *Écrit tel quel c'est peut-être un peu long pour* 15 *minutes. On pourra être plus rapide sur l'argument des coordonnées et faire ça un peu avec les mains, quitte à revenir dessus en cas de questions.*

Prouver qu'un objet est constructible en mathématiques n'est pas la même chose que savoir construire cet objet. Par exemple, comment construire le pentagone régulier ?

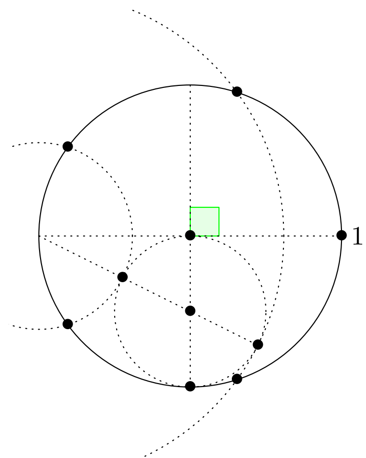

FIGURE 1.2 – Une construction du pentagone régulier : Construire le diamètre perpendiculaire au diamètre qui passe par 1, construire le cercle de centre $-\frac{1}{2}i$ et de rayon $\frac{1}{2}$, puis tracer la droite qui passe par -1 et $-\frac{1}{2}i$. L'intersection de cette droite et ce cercle donne deux points. Tracer les deux cercles de centre -1 et qui passent par chacun de ces points. Les intersections entre le cercle unité et chacun de ces cercles fournissent les points voulus. (Pourquoi ?)

Références

[Car81][FG94]

Leçons concernées

- 102
- 121
- 125
- 141
- 182
- 183

1.5 Sous-groupes compacts de $GL_n(\mathbb{R})$

Développement

Théorème 1.8. *Tout sous groupe compact de $GL_n(\mathbb{R})$ est conjugué à un sous groupe de $O_n(\mathbb{R})$.*

Lemme 1.9. *Soit E un espace vectoriel de dim finie, K un compact convexe de E, et H un sous groupe compact de $GL(E)$, tel que $\forall h \in H\ h(K) \subset K$, alors il existe $k \in K$ point fixe à tous les éléments de H.*

Démonstration : (du lemme)

- Soit $\|\ \ \|$ une norme euclidienne sur E, on pose $N(x) = \sup\limits_{h \in H} \|h(x)\|$ qui est une norme sur E.
- Si $N(x+y) = N(x) + N(y) = \|h(x+y)\|$ pour un $h \in H$
  Alors $N(x+y) \leq \|h(x)\| + \|h(y)\| \leq N(x) + N(y) = N(x+y) = \|h(x+y)\|$
  Donc $\|h(x) + h(y)\| = \|h(x)\| + \|h(y)\|$ et donc $h(x) = \alpha h(y)$, $\alpha > 0$, $x = \alpha y$ (h injective)
- Par compacité de K il existe un élément $a \in K$ de norme minimale.
- S'il y a deux tels points a, $b \in K$, (si $a = \alpha b$ avec $\alpha \in \mathbb{R}^{+*} \setminus \{1\}$ alors $N(a) \neq N(b)$) donc $N(\frac{a+b}{2}) = \frac{1}{2}N(a+b) < \frac{1}{2}(N(a) + N(b)) = N(a)$, or $\frac{a+b}{2} \in K$ (par convexité) de norme $< N(a)$, absurde.
- $\forall h \in H \quad N(h(a)) = N(a)$ (car $g \mapsto g \circ h$ est une bijection sur H), par unicité :
  $\forall h \in H,\ h(a) = a$

□

Démonstration : (du théorème)

- Soit G un sous groupe compact de $GL_n(\mathbb{R})$, on note E l'ensemble des matrices symétriques de $M_n(\mathbb{R})$, on pose $\phi : \begin{pmatrix} G & \to & GL(E) \\ g & \mapsto & s \mapsto gsg^T \end{pmatrix}$ morphisme de groupe continue, et on note $H = \phi(G)$ sous groupe compact de $GL(E)$.
- $P = \{hh^T,\ h \in G\}$ est un compact de E, $K = conv(P)$ est donc compact par le théorème de Carathéodory.
- $\phi_g(\,gh^T) = ghh^Tg^T = (gh)(gh)^T \in P$. Ainsi les éléments de H stabilise P et donc par combinaison convexe, stabilise les éléments de K, on peut donc utiliser le lemme : il existe $s \in K$, tel que $\forall g \in G\ gsg^T = s$.
- $P \subset S_n^{++}$ (ensemble des matrices définies positives) convexe, donc K aussi par combinaison, ainsi $s \in S_n^{++}$, donc il existe $r \in S_n^{++}\ r^2 = s$

$$\begin{array}{rcl} \forall g & \in & G \\ grrg^T & = & rr \\ r^{-1}\,gr(rg^Tr^{-1}) & = & I_n \\ (r^{-1}gr)(r^{-1}gr)^T & = & I_n \\ r^{-1}Gr & \subset & O_n \end{array}$$

□

Complément

Complément 1.10. *Soit $X \subset \mathbb{R}^n$, alors out point de conv(X) s'écrit comme un barycentre d'une famille de $n+1$ points de X.*
Si X est compact alors conv(X) est compact.

Démonstration : Soit $x = \sum_{i=1}^{p} \lambda_i x_i$ une décomposition d'un élément x de *conv*(X) ($\lambda_i > 0$ et $\sum \lambda_i = 1$), avec $p > n+1$, alors la famille $(x_2 - x_1, \dots x_p - x_1)$ est liée, ainsi il existe des a_i non tous nuls tels que $\sum a_i(x_i - x_1) = 0$, on pose $a_1 = -\sum a_i$.
On a alors $x = \sum(\lambda_i + ta_i)x_i$, l'un des $a_i < 0$, soit $t = \min\{-\frac{\lambda_i}{a_i}\ a_i < 0\}$, alors $\mu_i = \lambda_i + ta_i$ sont de somme 1, positif, et comme le min est atteind pour un j on a $\mu_j = 0$.
Ainsi on a une coordonnée en moins et on continue par récurrence. $\square$

Références

[Szp09]

Leçons concernées

- 106
- 150
- 160
- 181
- 203
- 206

1.6 *Table de S_4

Références

[Pey04]

Leçons concernées

- 105
- 107
- 109
- 154
- 161
- 182

1.7 Théorème de Brouwer

Développement

Théorème 1.11. *Soit $n \in \mathbb{N}^\star$, notons B la boule unité fermé de $\mathbb{R}^n$ et S sa sphère unité. Soit $f : B \to B$ continue, alors B admet un point fixe*

Démonstration :

- On suppose $f \in C^1$ sur B [3] et que f n'a pas de point fixe.
  Pour $x \in B$, on note $r(x)$ l'intersection de S avec la demi-droite $[f(x), x[$, alors $r(x) = f(x) + \lambda(x)(x - f(x))$, où $\lambda(x) > 0$ et $\|r(x)\|^2 = 1$, on obtient ainsi une équation en λ du second degré dont le discriminant est strictement positif, donc λ est une application C^1, donc r aussi sur $\mathring{B}$.

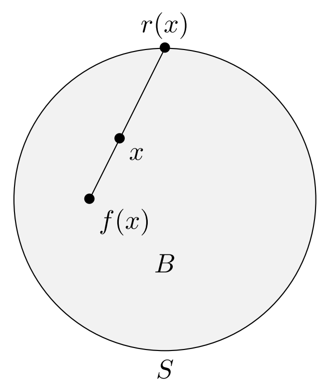

Figure 1.3 – La boule B, ainsi que l'application r.

- On pose
$$F : \begin{pmatrix} B \times [0,1] & \to & B \\ (x,t) & \mapsto & (1-t)x + tr(x) \end{pmatrix}$$
  En particulier, $F(\quad, 0) = id_B$ et $F(\quad, 1) = r$, de plus, pour $x \in S$ et $t \in [0,1]$ on a $F(x,t) = x$.
- Pour $t \in [0,1]$, posons $V(t) = \int_{\mathring{B}} \det \partial_1 F(x,t) dx$. La fonction V est une polynomiale. De plus pour $t = 1$, $\mathring{B} \ni x \mapsto F(x,1) = r$, n'est pas de différentielle inversible en tout point $x \in \mathring{B}$ (car l'image est incluse dans S, qui est d'intérieur vide ce qui contredirait le théorème d'inversion locale si la différentielle était inversible en un point x). Finalement $V(1) = 0$.
- Appliquons le théorème d'inversion globale :
  — Supposons qu'on ait :
$$\forall n \in \mathbb{N}^\star \quad \exists t_n \in \left]0, \frac{1}{n}\right] \quad \exists x_n \in B \text{ tel que } \det \partial_1 F(x_n, t_n) \leq 0$$
  Alors, par extraction de $(x_n)_n$, on aura $\partial_1 F(x,0) \leq 0$, ce qui est impossible. Donc il existe $N \in \mathbb{N}$, tel que pour pour tout $t < \frac{1}{N}$ et pour tout $x \in B$, on ait $\partial_1 F(x,t) > 0$.

3. On dit que f est C^1 si elle est la restriction d'une fonction définie sur un ouvert contenant B qui est C^1.

— $F(\quad, t)$ est injective pour t petit :
$F(x,t) = F(y,t)$, alors $(1-t)\|x-y\| = t\|r(x)-r(y)\| \leq M\|x-y\|$, où $M = \sup_{z\in B}\|dr_z\|$, donc $\|x-y\| \leq \frac{Mt}{1-t}\|x-y\|$, or il existe $\alpha < \frac{1}{N}$ tel que pour $t \leq \alpha$ on ait $\frac{Mt}{1-t} < 1$, ainsi $F(t, \quad)$ est injective pour $0 < t < \alpha$.

— Pour $t < \alpha$, $F(x,t) = x$ pour $x \in S$, par injectivité on a $F(t, \mathring{B}) \bigsqcup S = F(t,B)$ qui est compact donc fermé. Donc $F(t,\mathring{B}) = F(t,B) \bigcap \mathring{B}$ est un fermé de $\mathring{B}$. De plus, $F(t,\mathring{B})$ est un ouvert par le théorème d'inversion locale. Par connexité $F(t,\mathring{B}) = \mathring{B}$.

- Ainsi pour $t < \alpha$, on peut appliquer le théorème d'inversion globale et donc par changement de variable on a $V(t) = V(0) \neq 0$, pour t petit, mais V est une fonction polynomiale, donc $V(1) = V(0) \neq 0$, ce qui est absurde. En conclusion, f a un point fixe.
- Si maintenant f est continue, alors d'après le théorème de Stone-Weierstrass il existe une famille de fonctions polynomiale $(p_n)_n$ tel que $p_n : B \to B$ converge uniformément vers f [4]. Soit x_n un point fixe de p_n, alors par extraction, on peut supposer que $x_n \to x$, alors :

$$|x_n - f(x)| = |p_n(x_n) - f(x)| \leq |f(x) - f(x_n)| + |f(x_n) - p_n(x_n)| \leq |f(x) - f(x_n)| + \|f - p_n\|_\infty \to 0$$

On en conclut que $f(x) = x$.

□

Références

[GT98]

Leçons concernées

- 204
- 206
- 214
- 215
- 253

4. Il faut néanmoins s'assurer que l'on peut trouver p_n tel que $p_n(B) \subset B$ ce qui n'est pas garanti *a priori* par Stone-Weierstrass.. Supposons que l'on ai au contraire $\|p_n\| > 1$ à partir d'un certain rang (sinon il suffit d'extraire). Alors on remplace p_n par $\tilde{p}_n = \frac{p_n}{\|p_n\|_\infty}$, ainsi $\tilde{p}_n : B \to B$, de plus $\tilde{p}_n$ converge encore uniformément vers f. En effet, $\|f - \tilde{p}_n\|_\infty \leq \|f - p_n\|_\infty + \|p_n - \tilde{p}_n\|_\infty \leq \|f - p_n\|_\infty + \|p_n\|_\infty(1 - \frac{1}{\|p_n\|_\infty}) \to 0 + \|f\|_\infty \left(1 - \frac{1}{\|f\|_\infty}\right) \leq 0$.

1.8 Formule sommatoire de Poisson

Développement

Théorème 1.12. *Soit $f \in S(\mathbb{R})$, alors $\sum f(x+n) = \sum \hat{f}(n) e^{2i\pi nx}$*

Démonstration :

- Soit $M > 0$ tel que $|f(x)| \leq \frac{M}{x^2+1}$ pour $x \in \mathbb{R}$. Alors pour $K > 0$ et pour $x \in [-K, K]$, pour tout $n \in \mathbb{Z}$, tel que $|n| > K+1$, on a : $|f(x+n)| \leq \frac{M}{(x+n)^2+1}$, or :
$$\begin{cases} x+n & \geq & -K+|n| & > & 0 & \text{si} & n \geq 0 \\ x+n & < & K-|n| & < & 0 & \text{si} & n < 0 \end{cases}$$
Donc $(x+n)^2 \geq (|n|-k)^2$ Donc $|f(x+n)| \leq \frac{M}{(|n|-K)^2+1}$, on a donc une convergence normale sur $[-K, K]$, donc uniforme, et donc simplement sur tout $\mathbb{R}$, notons F sa limite simple.
- De même $\sum f'(x+n)$ converge uniformément sur $]-K, K[$, on peut donc appliquer le théorème de dérivation sur les suites de fonctions, donc F est de classe C^1 sur $]-K, K[$, et ce pour tout $K > 0$, donc F est de classe C^1 sur $\mathbb{R}$.
- $\sum\limits_{n=-N}^{N} f(x+1+n) = \sum\limits_{n=-N+1}^{N+1} f(x+1)$ en passant à la limite on a $F(x+1) = F(x)$, F est donc 1-périodique.
- Calculons les coefficients de Fourier de F :
$$\begin{aligned} c_n(F) &= \int_0^1 F(t) e^{-2i\pi nt} \\ &= \sum \int_0^1 f(t+n) e^{-2i\pi nt} dt \\ &= \sum \int_n^{n+1} f(t) e^{-2i\pi nt} dt \\ &= \int_{-\infty}^{+\infty} f(t) e^{-2i\pi nt} dt \\ &= \hat{f}(n) \end{aligned}$$
(grâce à la convergence uniforme sur $[0, 1]$)
- F est de classe C^1 donc est égale à sa série de Fourier donc $\sum f(x+n) = \sum \hat{f}(n) e^{2i\pi nx}$

□

Application 1.13. *On pose $T_n = \sum\limits_{k=-n}^{n} \delta_n \in S'(\mathbb{R})$, pour $n \in \mathbb{N}$, alors $(T_n)_n$ converge dans $S'(\mathbb{R})$ vers une distribution δ qui vérifie $\hat{\delta} = \delta$*

Démonstration :

- Soit $\varphi \in S(\mathbb{R})$, alors $T_n(\varphi) \to \sum \varphi(n) = \delta(\varphi)$ (la série est convergente). De plus :
$$|\delta(\varphi)| \leq \sum |\varphi(n)| \leq |f(0)| + \sum_{n \in \mathbb{Z}^\star} \frac{1}{n^2} |n^2 f(n)| \leq ||f||_{0,0} + ||f||_{2,0} \sum_{n \in \mathbb{Z}^\star} \frac{1}{n^2} \leq \left(\frac{\pi^2}{3} + 1 \right) \max(||\varphi||_{2,0}, ||\varphi||_{0,0}$$

- $$\hat{\delta}(\varphi) = \delta(\hat{\varphi}) = \sum \hat{\varphi}(n) = \sum \varphi(n) = \delta(\varphi$$

  Ainsi $\hat{\delta} = \delta$

$\square$

Application 1.14. *On pose $\theta(x) = \sum x^{n^2}$, alors on a $\sqrt{s}\theta(e^{-s\pi}) = \theta(e^{-\pi/s})$*

Démonstration : On applique la formule de Poisson à $f : x \mapsto e^{-\alpha x^2} \in S(\mathbb{R})$, où $\alpha > 0$, $\hat{f}(n) = \int_{-\infty}^{+\infty} e^{-\alpha t^2} e^{-2i\pi nt} dt = \frac{1}{\sqrt{\alpha}} \int_{-\infty}^{+\infty} e^{-u^2} e^{-2i\pi nu/\sqrt{\alpha}} du = \sqrt{\pi/\alpha} e^{-\pi^2 n^2/\alpha}$
En prenant $x = 0$ dans la formule de Poisson on a $\sum e^{-\alpha n^2} = \sqrt{\pi/\alpha} \sum e^{-\pi^2 n^2/\alpha}$, on pose alors $\theta(x) = \sum x^{n^2}$, alors $\sqrt{s}\theta(e^{-s\pi}) = \theta(e^{-\pi/s})$, avec $\alpha = \pi s$. $\square$

Remarque

Remarque 1.15. *Le théorème et les deux applications, cela fait trop on pourra par exemple faire la première application dans les leçons 254, 246 et 255 et la seconde dans les leçons 230 et 241*

Références

[Gou08]

Leçons concernées

- 230
- 241
- 246
- 254
- 255

1.9 Décomposition effective de Dunford

Développement

Théorème 1.16. *Soit $\mathbb{K}$ un corps de caractéristique nulle, soit E un $\mathbb{K}$-espace vectoriel de dimension finie, soit $u \in L(E)$ tel que π_u est scindé, alors il existe un unique couple d'endomorphismes (d, n) vérifiant :*

- $u = d + n$
- *d est diagonalisable*
- *n est nilpotent*
- $dn = nd$

De plus d et n sont des polynômes en u et peuvent être calculés effectivement à l'aide d'un algorithme.

Soit P un polynôme annulateur scindé de u, $P = \prod(X - \lambda_i)^{\alpha_i}$ où les $(\lambda_i)_i$ sont deux à deux distincts, on pose :

$$Q = \frac{P}{\text{pgcd}(P, P')} = \prod(X - \lambda_i)$$

On définit la suite $(u_k)_{k\in\mathbb{N}}$ par $u_0 = u$ et $u_{k+1} = u_k - Q(u_k)Q'(u_k)^{-1}$

Lemme 1.17. *On a pour tout $k \in \mathbb{N}$:*

1. *L'endomorphisme u_k est un polynôme en u.*
2. *L'endomorphisme $Q'(u_k)$ est inversible.*
3. $Q(u_k) \in \left(Q(u)^{2^k}\right)$ *idéal de $\mathbb{K}[u]$ (anneau commutatif).*

Démonstration : (du lemme) Par récurrence

- Pour $k = 0$:
  1. $u_0 = u$ est bien un polynôme en u.
  2. Q et Q' sont premiers entre eux, par Bézout $Id = AQ(u) + BQ'(u)$ et donc $BQ'(u) = Id - AQ(u)$ or $Q(u)$ nilpotent (en effet il existe $r \in \mathbb{N}$ tel que $P|Q^r$, donc $Q^r(u) = 0$), donc $Q'(u)$ est inversible (somme d'un inversible et d'un nilpotent qui commutent).
  3. $Q(u) \in (Q(u))$
- Si la propriété est vrai au rang k :
  1. $Q'(u_k)$ est inversible, $Q'(u_k)^{-1} \in \mathbb{K}[Q(u_n)]$ donc $Q'(u_k)^{-1} \in \mathbb{K}[u]$ (par hypothèse de récurrence), Ainsi :
  $$u_{k+1} = u_k - Q(u_k)Q'(u_k)^{-1} \in \mathbb{K}[u]$$
  2. Par formule de Taylor (pour les polynômes) :
  $Q'(u_{k+1}) - \underbrace{Q'(u_k)}_{\text{inversible}} = (u_{k+1} - u_k)S(u_{k+1}, u_k) = Q(u_k)Q'^{-1}(u_k)R(u) \in \underbrace{(Q(u)^{2^k})}_{\text{nilpotents}}$ Donc $Q'(u_{k+1})$ est inversible.
  3. Par formule de Taylor (pour les polynômes) :
  $Q(u_{k+1}) = \underbrace{Q(u_k) + (u_{k+1} - u_k)Q'(u_k)}_{=0} + \underbrace{(u_{k+1} - u_k)^2}_{u_{k+1}-u_k \in \left(Q(u)^{2^k}\right)} \times T(u_k, u_{k+1}) \in \left(Q(u)^{2^{k+1}}\right)$

□

Démonstration : (du théorème)
$Q(u)$ est nilpotent, donc à partir d'un certain rang $k \in \mathbb{N}$ $Q(u_k) \in (0)$, ie $Q(u_k) = 0$ et donc la suite est stationnaire disons au rang k_0, on pose $d = u_{k_0}$ alors $Q(d) = 0$ ie d est diagonalisable, on pose $n = u - d$ alors

$$n = u_0 - u_{k_0} = \sum_{i=0}^{k_0-1} \underbrace{u_i - u_{i+1}}_{\text{nilpotent}} \text{ est nilpotent}$$

(d, n) sont des polynômes en u donc commutent ainsi on a la décomposition de Dunford.

Soit (d', n') un autre couple, d' commute donc avec n' donc avec u donc avec d (polynôme en u), de même n' commutent avec n, donc :

$$\underbrace{d - d'}_{\text{diagonalisable}} = \underbrace{n' - n}_{\text{nilpotent}} = 0$$

D'où l'unicité. □

Remarques

Remarque 1.18. *On fera attention à l'ordre des étapes dans la récurrence : en effet on utilise le fait que u_{n+1} soit un polynôme en u, dans les étapes 2, et 3, pour dire que $S(u_{n+1}, u_n)$ et $T(u_n, u_{n+1})$ sont bien dans $k[u]$, ce qui est fondamentale pour dire par exemple que $Q'(u_{n+1}) - Q'(u_n) \in (Q(u)^{2^n}) = \{V(u) \circ Q(u)^{2^n}\ V \in k[X]\}$*

Remarque 1.19. *On remarquera bien qu'à aucun moment on a eu besoin de connaître les racines du polynôme. C'est ce qui contribue au caractère effectif de la méthode.*

Remarque 1.20. *Cet algorithme utilise (sans le dire) la méthode de Newton qui d'habitude sert à approximer la solution de $Q(x) = 0$, ici en un nombre fini d'itérations on trouve une solution exacte de cette équation.*

Leçons concernées

- 153
- 155
- 157
- 226
- 232

1.10 Théorème des extrémas liés

Développement

Théorème 1.21. *Soit U un ouvert de $\mathbb{R}^n$, $g_1, ..., g_k$ des fonctions de U dans $\mathbb{R}$ C^1, telles que $(dg_1, ..., dg_k)$ soit une famille libre, on pose $M = \{x \in U \ / \ g_1(x) = g_2(x) = ... = g_k(x) = 0\}$, M est une sous-variété dont le plan tangent en x est $T_xM = \bigcap\limits_{i=1}^{k} \ker dg_{ix}$, soit $f : U \to \mathbb{R}$, C^1 tel que $f_{|M}$ possède un extremum m, alors $df_m \in vect(dg_{1m}, ..., dg_{km})$.*

Démonstration : On note $G : \begin{pmatrix} \mathbb{R}^n & \to & \mathbb{R}^k \\ x & \mapsto & (g_1(x), ...g_k(x)) \end{pmatrix}$ qui est une submersion, donc M est une sous-variété, dont le plan tangent est $T_xM = \ker DG_x = \bigcap\limits_{i=1}^{k} \ker dg_{ix}$

Soit $v \in T_mM$, alors il existe un chemin tracé sur M $\gamma : I \to M$ où I est un intervalle de $\mathbb{R}$ telle que $\gamma(0) = m$ et $\gamma'(0) = v$, alors $f \circ \gamma$ a un extremum en 0, donc $\frac{df \circ \gamma}{dt}(0) = 0$, donc $df_m(v) = 0$, ainsi $v \in \ker df_m$ Donc finalement $T_mM = \bigcap \ker dg_{im} \subset \ker df_m$ on conclut que $df_m \in vect(dg_{1m}, ..., dg_{km})$ grâce au lemme suivant : $\square$

Lemme 1.22. *Soit $\varphi_1, ..., \varphi_k, g$ des formes linéaires sur $\mathbb{R}^n$ telles que $\cap \ker \varphi_i \subset \ker g$, alors $g \in vect(\varphi_1, ..., \varphi_k)$*

Démonstration : On considère $\phi : \begin{pmatrix} \mathbb{R}^n & \mapsto & \mathbb{R}^k \\ x & \mapsto & (\varphi_1(x), ..., \varphi_k(x)) \end{pmatrix}$,
$\psi : \begin{pmatrix} \mathbb{R}^n & \mapsto & \mathbb{R}^{k+1} \\ x & \mapsto & (\varphi_1(x), ..., \varphi_k(x), g(x)) \end{pmatrix}$ applications linéaires qui ont même noyau (par hypothèse), donc par le théorème du rang les images ont même dimension, donc $g \in vect(\varphi_1, ..., \varphi_k)$ $\square$
.

Application 1.23. *Soit $f \in L(\mathbb{R}^n)$, symétrique, alors f est diagonalisable dans une base orthonormée.*

Démonstration : On considère $h : \begin{pmatrix} \mathbb{R}^n & \to & \mathbb{R} \\ x & \mapsto & \langle x \,|f(x) \rangle \end{pmatrix}$ C^1 et $g(x) = ||x||^2 - 1$ h, $g \in C^1$, alors $S^{n-1} = g^{-1}(0)$ est un compact donc h atteint sa borne supérieure en un point y, par le théorème des extrémas liés, $\exists \lambda \in \mathbb{R}$ tel que $dh_y = \lambda dg_y$, donc $\forall v \in \mathbb{R}^n$ $\langle v \,|f(y) \rangle + \langle y \,|f(v) \rangle = \lambda 2 \langle y \,|v \rangle$ par symétrie de f, on a $\forall v \in \mathbb{R}^n$ $\langle f(y) - \lambda y \,|v \rangle = 0$, donc $f(y) = \lambda y$ de plus $y^\perp$ est stable par f (car f symétrique) on conclut donc par récurrence. $\square$

Références

[Ave83]

Leçons concernées

- 159
- 215

1.11 Théorème de Stone-Weierstrass

Développement

Soit X un compact qui a au moins deux éléments.

Lemme 1.24. *Soit H une partie de $C(X,\mathbb{R})$, on suppose que :*

- $\forall (x,y) \in X^2 \; x \neq y \Longrightarrow \; \forall (a,b) \in \mathbb{R}^2 \; \exists h \in H / \left\{ \begin{array}{lcl} h(x) & = & a \\ h(y) & = & b \end{array} \right.$
- $\forall (f,g) \in H^2 \; \sup(f,g), \inf(f,g) \in H$ *(H est dit réticulée).*

Dans ce cas H est dense dans $C(X,\mathbb{R})$ (pour la convergence uniforme).

Démonstration : Soit $f \in C(X,\mathbb{R})$, et soit $\epsilon > 0$
$\forall x \in X, \forall y \neq x \, \exists h_y \in H \; / \left\{ \begin{array}{lcl} h_y(x) & = & f(x) \\ h_y(y) & = & f(y) \end{array} \right.$ Notons $O_y = \{z / h_y(z) > f(z) - \epsilon\}$ ouvert de X, et $x, y \in O_y$ ainsi on a :

$$X = \bigcup_{y \in X \setminus \{x\}} O_y$$

Par compacité on a alors :

$$\exists y_1, \ldots, y_m \in X \; / \; X = \bigcup_{i=1}^{m} O_{y_i}$$

On pose alors $g_x = \sup_{i \in [|1,m|]} (h_{y_i}) \in H$. Ainsi $g_x(x) = f(x)$ et $g_x(z) > f(z) - \epsilon$

On pose maintenant $\Omega_x = \{z \in X \; / \; g_x(z) < f(z) + \epsilon\}$ est un ouvert et $x \in \Omega_x$.
Et ce pour tout $x \in X$. Donc par compacité on a :

$$X = \bigcup_{i=1}^{n} \Omega_{x_i}$$

Finalement posons $g = \inf_{i \in [|1,n|]} (g_{y_i}) \in H$.
$\forall z \in X \; f(z) - \epsilon < g(z) < f(z) + \epsilon$, donc $N_\infty(f-g) < \epsilon$
$\square$

Théorème 1.25 (Stone-Weierstrass réel)**.** *Soit H une sous-algèbre de $C(X,\mathbb{R})$ séparante (c'est-à-dire que pour tous $x, y \in X$, si $x \neq y$, alors il existe $h \in H$ tel que $h(x) \neq h(y)$) et contenant les fonctions constantes alors H est dense dans $C(X,\mathbb{R})$*

Démonstration :

- Soit h tel que $h(x) \neq h(y)$, on pose $g(t) = a + \frac{h(x)-h(t)}{h(x)-h(y)}(b-a)$ alors $g \in H$, et $g(x) = a$, et $g(y) = b$.
- Sur $[-1,1]$ il existe une suite de fonctions polynomiales (P_n) qui converge uniformément vers $x \mapsto |x|$.
  Soit $f \in \overline{H} \setminus \{0\}$, alors $P_n\left(\frac{f}{N_\infty(f)}\right) \to \frac{|f|}{N_\infty(f)}$ de manière uniforme. Donc :

$$N_\infty(f) P_n\left(\frac{f}{N_\infty(f)}\right) \to |f|$$

Ainsi $|f|$ est limite d'éléments du fermé $\overline{H}$ donc $|f| \in \overline{H}$, dès que $f \in \overline{H}$.

$$\left\{\begin{array}{lcl} \sup(f,g) & = & \frac{f+g+|f-g|}{2} \in \overline{H} \\ \inf(f,g) & = & \frac{f+g-|f-g|}{2} \in \overline{H} \end{array}\right.$$

Donc $\overline{H}$ est ainsi réticulé, donc est dense mais aussi fermé, on a alors $\overline{H} = C(X, \mathbb{R})$.
□

Théorème 1.26 (Stone-Weierstrass complexe)**.** *Toute sous algèbre H de $C(X, \mathbb{C})$ séparante, auto-conjuguée (stable par conjugaison) contenant les fonctions constantes est dense dans $C(X, \mathbb{C})$*

Démonstration : $H_{\mathbb{R}} = \{h \in H \ h(X) \subset \mathbb{R})\}$, pour $f \in H$ on a $\left\{\begin{array}{lcl} \Re(f) & = & \frac{f+\overline{f}}{2} \in H \\ \Im(f) & = & \frac{f-\overline{f}}{2i} \in H \end{array}\right.$ $H_{\mathbb{R}}$ est de plus séparante car soit $h \in H$ tel que $h(x) \neq h(y)$ alors $\Re(h)$ ou $\Im(h)$ sépare x, y, par le lemme précédent $H_{\mathbb{R}}$ est dense dans $C(X, \mathbb{R})$, or $C(X, \mathbb{C}) = C(X, \mathbb{R}) + iC(X, \mathbb{R})$, donc H est dense dans $C(X, \mathbb{R})$ □

Compléments

Complément 1.27. *Il existe $(P_n)_n$ une suite de polynômes qui converge uniformément vers $| \quad |$ sur $[-1, 1]$.*

Démonstration : On définit $P_0 = 0$ et par récurrence $P_{n+1} = P_n + \frac{1}{2}(X^2 - P_n(X)^2)$, alors par récurrence on montre que $0 \leq P_n(x) \leq |x|$, ainsi (P_n) est une suite croissante, majoré donc converge en tout point. La limite simple f vérifiant $x^2 - f(x)^2$, donc il y a convergence simple vers $| \quad |$ mais par le théorème de Dini la convergence est uniforme. □

Complément 1.28. *(Démonstration du théorème de Dini). Quitte à changer f_n en $\pm(f_n - f)$ on peut supposer $(f_n)_n$ décroissante vers 0, alors $V_n = \{x \in X \ f_n(x) \leq \epsilon\}$ est un ouvert, et $X = \cap V_n$, par compacité $X = \bigcup\limits_{1 \leq i \leq N} V_i = V_N$ par décroissance, ainsi $f_N < \epsilon$, par décroissance pour tout $n \geq N$ on a $0 \leq f_n < \epsilon$*

Application 1.29.
- *Toute fonction continue réelle sur un compact est limite uniforme d'une suite de polynôme réels.*
- *Si $X \subset]0, 1[$ est compact alors toute fonction continue est limite uniforme d'une suite de polynômes à coefficients entiers*
- *Les fonctions 2π périodiques continues de $\mathbb{R}$ dans $\mathbb{C}$ sont limites uniformes de polynômes trigonométriques.*
- *Toute fonction continue sur un compact est limite uniforme de fonctions lipschitziennes.*

Références

[HL09]

Leçons concernées

- 201
- 202
- 203
- 209
- 246

1.12 Théorème de Joris

Développement

Définition 1.30. *Soit A anneau commutatif et B un sous-pseudo anneau de A* [5]*, on dit que B satisfait (P), si : $\forall a \in A, \forall r \gg 0\ a^r \in B \Longrightarrow a \in B$*

Théorème 1.31 (de transfert admis)**.** *Si B respecte P, alors $B[[X]]$ respecte P (dans $A[[X]]$)*

Lemme 1.32. *Soit $f \in C^\infty(\mathbb{R})$, et $a \in \mathbb{R}$ tel que $f^{(k)}(a) = 0$ pour $0 \leq k \leq n-1$, alors il existe $g \in C^\infty(\mathbb{R})$ tel que $f(x) = (x-a)^n g(x)$ de plus $g(a) = \frac{f^{(n)}(a)}{n!}$*

Démonstration : Par formule de Taylor : $f(x) = (x-a)^n \underbrace{\int_0^1 \frac{u^{n-1}}{(n-1)!} f^{(n)}(a + (x-a)u)\, du}_{\in C^\infty(\mathbb{R})}$ □

Lemme 1.33. *Soit D un ouvert de $\mathbb{R}$, $f, g \in C^\circ(\mathbb{R})$ vérifiant f est dérivable sur D et $f' = g$ sur D et $f = g = 0$ sur D^c, alors $f \in C^1$ et $f' = g$*

Démonstration : Soit $x \in D^c$, on pose $\tau(y) = \frac{f(y)}{y-x}$ ($= 0$ si $y \notin D$) sinon soit $]\alpha, \beta[$ la composante connexe de y dans D, supposons $y \geq x$, alors par le théorème des accroissements finis on a $|f(y) - f(\alpha)| \leq \sup |g||y-a| \leq \sup |g||y-x|$, et donc $\tau(y) \leq \sup |g| \to 0$, donc f est dérivable en x et $f'(x) = 0 = g(x)$.

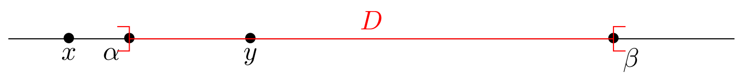

FIGURE 1.4 – Représentation de la composante connexe de D contenant y, dans le cas où $y \in D$ et $x \leq y$.

□

Définition 1.34. *Soit $g \in C^\circ(\mathbb{R})$, on définit les points plats par :*

$$P(g) = \left\{ a \in \mathbb{R} \quad \textit{tel que} \quad \forall \gamma > 0 \quad \lim_{x \to a} \frac{g(x)}{|x-a|^\gamma} = 0 \right\}$$

- $a \in P(g) \Longrightarrow g(a) = 0$
- $\forall k \in \mathbb{N}^\star \quad P(g) = P(g^k)$
- Si $g \in C^\infty(\mathbb{R})$, $P(g) = \bigcap_{n \in \mathbb{N}} (g^{(n)})^{-1}(\{0\})$ fermé.

Théorème 1.35. *Soit $f : \mathbb{R} \to \mathbb{R}$ vérifiant $\forall r \geq 2\ f^r \in C^\infty$, alors $f \in C^\infty$.*

Démonstration :

5. C'est-à-dire que B vérifie toutes les propriétés d'un sous-anneau sauf éventuellement $1 \in B$

- $f = \sqrt[r]{f^r} \in C^0$ pour r impair.
- On pose $D = P(f)^c = P(f^2)^c$ ouvert (f^2 est C^∞).
- $A = C^\circ(D)$, $B = \{f \in A / \exists g \in C^\circ(\mathbb{R})$ vérifiant $f = g_{|D}$ et $g_{|D^c} = 0\}$, alors B satisfait (P) car :
  Si $f^r \in B$ (pour un r impair, alors $f^r = g_{|D}$ pour un certain $g \in C^\circ(\mathbb{R})$, alors $f = \sqrt[r]{g^r}_{|D}$
- f est C^∞ sur D : soit $a \in D$, une dérivée de f^2 ne s'annule pas en a, donc d'après le lemme de divisibilité $f^2(x) = (x-a)^n g_2(x)$, où $g_2 \in C^\infty$ et $g_2(a) \neq 0$, de même $f^3(x) = (x-a)^m g_3(x)$, on a alors $f(x) = \frac{f^3(x)}{f^2(x)} = (x-a)^{m-n}\frac{g_3(x)}{g_2(x)}$ sur un voisinage de a par continuité en a on a $m - n \geq 0$, donc $f \in C^\infty$ sur un voisinage de a.
- On considère $J : \begin{pmatrix} C^\infty(D) & \to & A[[X]] \\ g & \mapsto & \sum \frac{g^{(n)}}{n!}X^n \end{pmatrix}$ est un morphisme d'anneaux
- $J(f_{|D})^r = J(f^r_{|D}) \in B[[X]]$, donc par le théorème de transfert $J(f_{|D}) \in B[[X]]$, donc $f^{(n)} = g_{n|D}$ où $g_n \in C^\circ(\mathbb{R})$
- Par récurrence $f \in C^n$ et $f^{(n)} = g_n$

□

Complément

Ce théorème de transfert a été admis dans ce développement mais il est bon à mon avis de savoir le démontrer :

Théorème 1.36 (de transfert)**.** *Si B respecte P, alors $B[[X]]$ respecte P (dans $A[[X]]$)*

Démonstration :

- $f^r = a_0^r + \ldots \in B[X]$, donc $\forall r \gg 1 a_0^r \in B$ i.e. $a_0 \in B$
- $B' = \{a \in A / \forall m \in \mathbb{N}\, a_0 a^m \in B\}$ alors $a_0 B' \underset{m=1}{\subset} B \underset{a_0 a^m \in B}{\subset} B'$ et $1 \underset{a_0 \in B}{\in} B'$:
  Soit $a, b \in B'$: $\forall r \geq 2$ $(a_0(ab)^m)^r = (a_0^{r-2})(a_0 a^{rm})(a_0 b^{rm}) \in B$, et donc $a_0(ab)^m \in B$ ie $ab \in B'$
  $a_0(a-b)^m = \sum_{k=0}^{m} \binom{m}{k}(-1)^{m-k} a_0(a^k b^{m-k}) \in B$, ie $a - b \in B'$.
- Par récurrence forte on suppose que $a_k \in B'$ pour $0 \leq k \leq n$, on pose $f_n = \sum_{k=0}^{n} a_k X^k \in B'[X]$,

$$\forall r \gg 2 \quad a_0 f^r (f - f_n)^{m(r+1)} = \sum_{k=0}^{m(r+1)} (-1)^k \binom{m(r+1)}{k} f^{m(r+1)-k+r}(a_0 f_n^k) \in B[[X]]$$

  Donc $(a_0 a_{n+1}^m)^{r+1} \in B, \forall r \gg 0$, donc $a_0 a_{n+1}^m \in B\ \forall m$, ie $a_{n+1} \in B'$ ce qui conclut la récurrence.
- $a_0 f^k \in B[[X]]$ et donc $(f - a_0)^r = f^r + \sum_{k=0}^{r} (-1)^k \binom{r}{k} a_0^k f^{r-k} \in B[[X]]$
- On pose $f_n = a_n + a_{n+1}X + \ldots$, $f_0 = f$, et $f_{n+1}X = f_n - a_n$, par récurrence si $f_n^r \in B[[X]]$, alors $a_n \in B$ et $(X f_{n+1})^r \in B[[X]]$, donc $f_{n+1}^r \in B[[X]]$, donc $f \in B[[X]]$

□

Complément 1.37. *Si $f^n \in \mathcal{C}^\infty$ seulement pour $n \geq N$ pour $N \in \mathbb{N}$ N plus grand que deux alors f est encore $\mathcal{C}^\infty$*

Démonstration : Il suffit de constater que $(f^{n-1})^r$ pour $n \geq N$ est $\mathcal{C}^\infty$ pour $r \geq 2$ (car $r(n-1) \geq 2n-1 \geq n \geq N$ et donc en utilisant le théorème $f^{n-1} \in \mathcal{C}^\infty$, puis on descend jusqu'à montrer que f^2 est $\mathcal{C}^\infty$ et donc que $f \in \mathcal{C}^\infty$ $\square$

Complément 1.38. *Soit $(a_i)_{1 \leq i \leq N}$ des entiers positifs premiers dans leur ensemble tel que $f^{a_i} \in \mathcal{C}^\infty$, alors $f \in \mathcal{C}^\infty$*

Démonstration : En effet on sait que l'équation $n = \sum a_i b_i$ aura une solution avec $b_i \in \mathbb{N}$ (grâce par exemple à ce développement), et donc $f^n = \prod (f^{a_i})^{b_i}$ sera $\mathcal{C}^\infty$ comme produit de fonctions $\mathcal{C}^\infty$ $\square$

Exemple 1.39. *Si f^2, et f^3 sont $\mathcal{C}^\infty$, alors f l'est.*

Références

[Bru05]

Leçons concernées

- 124
- 207
- 218
- 228
- 239

1.13 Théorème de la base de Burnside

Développement

Soit G un p-groupe, on note par Spec(G) l'ensemble des sous-groupes de G maximaux. Étudions ces sous-groupes maximaux :

Lemme 1.40. *Soit H un sous groupe maximal, alors $H \lhd G$, et $G/H = \mathbb{Z}/p\mathbb{Z}$.*

Démonstration .

- *On fait agir H sur G/H par multiplication des classes à gauche, on a par la formule des classes : $0 \equiv Card(G/H) \equiv Card(G/H)^H$ [mod p], ainsi $p | Card(G/H)^H$.*

$$gH \in (G/H)^H \iff \forall h \in H\ hgH = gH \iff HgH = gH \iff Hg = gH \iff g \in N_G(H)$$

Ceci démontre que $N_G(H)/H$ est en bijection avec $(G/H)^H$ donc par égalité des cardinaux :

$$CardN_G(H) = CardH \times \underbrace{Card(G/H)^H}_{\geq p}$$

Ainsi, $Card(N_G(H)) > CardH$ donc :

$$H \subsetneq N_G(H) \subset G$$

Par maximalité $N_G(H) = G$, d'où $H \lhd G$.

- *Comme H est maximal G/H n'a pas de sous groupe propre (correspondance des sous groupes de G/H), donc G/H est cyclique et pour des raisons de cardinalité $G/H = \mathbb{Z}/p\mathbb{Z}$.*

□

Théorème 1.41. *Les parties génératrices minimales de G ont le même cardinal.*

Démonstration . *Posons*

$$\varphi(G) = \bigcap_{H \in Spec(G)} H$$

Alors $\varphi(G)$ est un sous-groupe distingué de G, notons $\pi : G \to G/\varphi(G)$ la projection canonique. Soit $H \in Spec(G)$, G/H est abélien (voir lemme 1.40), donc $D(G) \subset H$ [6], donc $D(G) \subset \varphi(G)$, donc $(G/\varphi(G), +)$ est abélien, en particulier c'est un $\mathbb{Z}$-module.
Soit $H \in Spec(G)$, on note $\sigma : G \to G/H = \mathbb{Z}/p\mathbb{Z}$ la projection canonique. Pour tout $x \in G$, $\sigma(x^p) = p\sigma(x) = 0$, ainsi $x^p \in \ker \sigma = H$, ainsi

$$\forall x \in G, \quad x^p \in \varphi(G) \text{ donc } p\pi(x) = 0$$

Ainsi la structure de $\mathbb{Z}$-module sur $(G/\varphi(G), +, \cdot)$ passe au quotient, $(G/\varphi(G), +, \cdot)$ est en fait un $\mathbb{F}_p$-espace vectoriel de dimension finie, dont toutes les familles génératrices minimales (pour la structure d'espace-vectoriel donc pour celle de groupe) sont des bases, et en particulier ont donc le même cardinal.□

On a démontré le théorème dans le cas particulier de $G/\varphi(G)$, le lemme suivant conclut la preuve :

Lemme 1.42. *$(g_i)_{i\in I}$ est génératrice de G si et seuleemnt si $(\pi(g_i))_{i\in I}$ est génératrice de $G/\varphi(G)$.*

6. On note $D(G)$ le groupe dérivé de G.

Démonstration . $\Longrightarrow$ *: Évident car π est surjectif.*
$\Longleftarrow$ *: Si (g_i) pas génératrice, on crée une suite de sous-groupes :*

$$H_0 = \langle (g_i)_i \rangle \subsetneq H_1 \subsetneq ... \subsetneq H_n \subsetneq G$$

Ce processus s'arrête nécessairement (car G est un groupe fini et a donc qu'un nombre fini de sous-groupes).
On a donc construit $H \in Spec(G)$ qui contient les (g_i), ainsi $\varphi(G) \subset H \subsetneq G$, et $\pi(H) \subsetneq \pi(G)$, (par correspondance des sous groupes de $G/\varphi(G)$), ainsi $\pi(H) \supset (\pi(g_i))_{i\in I}$ n'est pas une famille génératrice.$\square$

Remarque 1.43. *Présenté à l'oral de la leçon d'algèbre (101), note : 18.25/20*
Seule question posée lors de ce développement : « Ré-expliquez pourquoi $G/H = \mathbb{Z}/p\mathbb{Z}$. ».

Remarque

Il faut savoir bien mettre en place la formule des classes, de plus il faut savoir démontrer la caractérisation des sous-groupes de G/H par les sous-groupes de G contenant H.

Leçons concernées

- 101
- 103
- 104
- 108
- 151

1.14 Automorphismes de S_n

Développement

On définit $\mathrm{Int}(S_n)$ comme l'ensemble des automorphismes intérieurs de S_n. Posons l'application suivante :

$$\Psi : \begin{pmatrix} S_n & \to & \mathrm{Int}(S_n) \\ \alpha & \mapsto & \sigma \mapsto \alpha\sigma\alpha^{-1} \end{pmatrix}$$

Alors Ψ est un morphisme surjectif, et bijectif dès que $n \geq 3$: $S_n \simeq \mathrm{Int}(S_n)$, de plus $\mathrm{Int}(S_n) \lhd Aut(S_n)$

Lemme 1.44. *Soit $\varphi \in Aut(S_n)$. On définit T_k comme l'ensemble des éléments de S_n qui sont produits d'exactement k transposition(s) à supports disjoints. Si $\varphi(T_1) \subset T_1$, alors $\varphi \in Int(S_n)$*

Démonstration . *Écrivons les images par φ des premières transpositions :*

$$\begin{array}{lcll} \varphi(1,2) & = & (a_1, a_2) & \\ \varphi(1,3) & = & (c,b) & \textit{mais } (1,2),\ (1,3) \textit{ ne commutent pas.} \\ \varphi(1,3) & = & (a_1, a_3) & \textit{donc leurs images non plus donc support non disjoints.} \\ \varphi(2,3) & = & (a_2, a_3) & \\ \varphi(1,4) & = & (a_1, a_4) & (1,4) \textit{ commute avec } (2,3) \textit{ mais pas } (1,2)\textit{, donc de même pour leurs images.} \end{array}$$

Par une récurrence, on montre que $\varphi(1,i) = (a_1, a_i)$, où $a_i \notin \{a_1, ..., a_{i-1}\}$. Posons alors $\alpha(i) = a_i$, on a que $\alpha \in S_n$. De plus, $\varphi(1,i) = (\alpha(1), \alpha(i)) = \alpha(1,i)\alpha^{-1}$. Donc on a

$$\varphi_{|G} = \Psi(\alpha)_{|G} \text{ où } G = \{(1,i), \quad i \in [\![1,n]\!]\}$$

Comme G est une famille génératrice de S_n, on a $\varphi = \Psi(\alpha) \in Int(S_n)$.$\square$

Théorème 1.45. *Pour $n \neq 6$, on a $Aut(S_n) = Int(S_n)$.*

Démonstration . *Soit $\varphi \in Aut(S_n)\backslash Int(S_n)$ et τ une transposition. Alors, $\varphi(\tau)$ est encore d'ordre deux (par automorphie), donc est dans l'un des T_k, de plus les automorphismes laissent stables les classes de conjugaison, donc $\varphi(T_1) = T_k$ (avec $k \geq 2$). En particulier, T_1 aura le même cardinal que T_k soit :*

$$\begin{array}{rcl} \binom{n}{2} & = & \frac{1}{k!}\binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2k+2}{2} \\ \frac{n(n-1)}{2} & = & \frac{n(n-1)\ldots(n-2k+1)}{2^k k!} \\ 2^{k-1} & = & (n-2)\ldots(n-k+1)\frac{(n-k)!}{(n-2k)!k!} \\ 2^{k-1} & = & (n-2)\ldots(n-k+1)\binom{n-k}{k} \end{array}$$

Donc $k = 3$, ainsi $4 = (n-2)\binom{n-3}{3}$, $24 = (n-2)(n-3)(n-4)(n-5)$ donc $n = 6$. On conclut par contraposée. $\square$

Théorème 1.46. *De plus, $Aut(S_6) \neq Int(S_6)$, plus précisément $Aut(S_6)/Int(S_6) = \mathbb{Z}/2\mathbb{Z}$.*

Démonstration .
- *On considère l'action fidèle transitive de $\mathbb{P}GL_2(\mathbb{F}_5)$ sur $\mathbb{P}^1(\mathbb{F}_5)$, ainsi on a un morphisme injectif $\Pi : \mathbb{P}GL_2(\mathbb{F}_5) \to S(\mathbb{P}^1(\mathbb{F}_5)) = S_6$, $|\mathbb{P}GL_2(\mathbb{F}_5)| = \frac{24\times 20}{4} = 120$. Ainsi, l'image de Π, noté N, est un sous-groupe d'indice $\frac{6!}{120} = 6$ de S_6 qui ne stabilise aucun élément élément de $[\![1,6]\!]$.*
- *Posons f le morphisme suivant :*

$$f : \begin{pmatrix} S_6 & \to & S(S_6/N) \simeq S_6 \\ \sigma & \mapsto & (\alpha N \mapsto \sigma\alpha N) \end{pmatrix}$$

  Soit $\sigma \in \ker f$, alors $N = \sigma N$, et donc $\sigma \in N$, ainsi $\ker f \subset N$, $\ker f \lhd S_6$, $|\ker f| \leq 120$, f est donc injectif, et donc $f \in Aut(S_6)$, (quitte à renumérotant en prenant $N = 1$).
  $\forall \sigma \in N$, $f(\sigma)(1) = 1$, si on avait $f = \varphi_a$, alors $f(\sigma)(1) = 1 = a\sigma a^{-1}(1)$, donc $a^{-1}(1) = \sigma a^{-1}(1)$, donc tout les éléments de N stabilisent $a^{-1}(1)$ ce qui est absurde donc $f \in Aut(S_6)\setminus Int(S_6)$.
- *Soit $\varphi \in Aut(S_n) \setminus Int(S_n)$, alors par le lemme 1.44, $f^{-1} \circ \varphi(T_1) = T_1$, et donc $f^{-1} \circ \varphi \in Int(S_6)$, ie $\varphi \in fInt_(S_6)$. Il y a donc deux classes de $Aut(S_6)$ modulo $Int(S_6)$.*

□

Compléments

Remarque 1.47. *On peut aussi s'intéresser aux automorphismes de A_n pour $n \neq 6$ on a aussi des automorphismes « pseudo-extérieurs »de la forme $\sigma \mapsto \tau \circ \sigma \circ \tau^{-1}$, où $\tau \in S_n \setminus A_n$, et c'est tout. Donc pour $n \neq 6$ on a :*

$$Aut(A_n)/Int(A_n) = \mathbb{Z}/2\mathbb{Z}$$

Pour $n \neq 6$ on a d'autres types d'automorphismes extérieurs : les automorphismes extérieurs de S_6 restreint à A_6 [7], ainsi que ceux-là composés avec des automorphismes « pseudo-extérieurs ». Finalement on a :

$$Aut(A_6)/Int(A_6) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Démonstration . *(rapide) Pour le démontrer on procédera de la même manière si un trois-cycle est envoyé sur un trois-cycle, alors l'automorphisme est intérieur ou « pseudo extérieur ». Et en notant T_k l'ensemble des permutations produit de k 3-cycles à supports disjoints, si $|T_k| = |T_1$ alors par un argument combinatoire on a $k = 1$ si $n \neq 6$, et $k \in \{1, 2\}$ si $n = 6$. Puis on vérifiera que l'automorphisme extérieur à S_6 trouvé précédemment envoie bien un 3-cycle sur un produit de deux 3-cycles. En bourrinant par exemple ; on peut programmer tout ça avec un logiciel de calcul formel comme Sage :*

7. En effet la restriction à un tel automorphisme à A_6 aura pour image un sous groupe d'indice 2 de S_6, donc nécessairement A_6.

```
K=GF(5) #Fabrication du sous-groupe N
A=MatrixSpace(K,2,2)
B=MatrixSpace(K,2,1)
L=[]
P=[]
M=[B([0,1]),B([1,0]),B([1,1]),B([2,1]),B([3,1]),B([4,1])]
for C in A:
   if det(C)==0:
      c=1
   else:
      c=0
      for k in [2..4]:
         for D in P:
            if C==k*D:
               c=c+1
   if c==0:
      P[len(P):]=[C]
      N=[0,0,0,0,0,0]
      for i in [0..5]:
         for j in [0..5]:
            for k in K:
               if M[j]==k*C*M[i]:
                  N[i]=j+1
      L[len(L):]=[Permutation(N,6)]

Q=[] #Fabrication du groupe quotient
S=SymmetricGroup(6)
R=[]
for s in S:
   if (s in R)==false:
      print s
      M=[]
      for a in L:
         p=S(a)*s
         M[len(M):]=[p]
         R[len(R):]=[p]
      Q[len(Q):]=[M]
   if len(Q)==6:
      break
@interact #Calcul de l'automorphisme
def psi(s=input_box((1,2,3))):
   p=S(s)
   O=[0,0,0,0,0,0]
   for i in [0..5]:
      a=Q[i][0]*p
      for j in [0..5]:
         if (a in Q[j])==true.
            O[i]=j+1
   b=S(Permutation(O,6))
   return(b)
```

aut.py

Résultat :

$$(1,5,4)(2,3,6)$$

□

Références

[Per96]

Leçons concernées

- 101
- 103
- 104
- 105
- 108

1.15 Théorèmes de Weierstrass et d'Osgood

Développement

Théorème 1.48 (Weierstrass)**.** *Soit U un ouvert de $\mathbb{C}$ et soit $(f_n)_n$ une suite de fonction holomorphes convergeant vers f uniformément sur tout compact, alors f est holomorphe sur U et f_n' converge uniformément vers f' sur tout compact de U.*

Démonstration : Soit T un triangle, alors $\int_{\partial T} f(z)dz = \lim \int_{\partial T} f_n(z)dz = 0$, donc f est holomorphe sur U (Morera)

□

Théorème 1.49 (d'Osgood)**.** *Soit U un ouvert de $\mathbb{C}$ et $(f_n)_n$ une suite de fonctions holomorphes sur U qui converge simplement sur U, alors il existe un ouvert dense de U sur lequel f est holomorphe*

Démonstration :

- Soit O un ouvert de U, par continuité des (f_n) on définit pour $k \in \mathbb{N}$, $F_k = \{x \in O, \forall n, |f_n(x)| \leq k\}$ est un fermé de U, de plus (F_k) est une suite croissante pour l'inclusion. Pour tout $x \in O$, $f_n(x) \to f(x)$ donc $(|f_n(x)|)_{n\in\mathbb{N}}$ est une suite bornée disons par un certain k entier naturel, donc $x \in F_k$, donc $O = \bigcup\limits_{k\in\mathbb{N}} F_k$
- O est un espace de Baire (car ouvert de $\mathbb{C}$) donc par le théorème de Baire il existe un k tel que $\mathring{F_k} \neq \emptyset$ dans O, mais O est un ouvert de $\mathbb{C}$ donc $\mathring{F_k} \neq \emptyset$ dans $\mathbb{C}$. Soit Ω une boule ouverte dans $\mathring{F_k}$, grâce à la formule de Cauchy on a :

  $$\forall z \in \Omega,\ \forall n \in \mathbb{N},\ f_n(z) = \frac{1}{2i\pi}\int_{\partial\Omega} \frac{f_n(w)}{w-z}dw$$

  De plus les (f_n) sont uniformément bornées sur Ω en module par k on a ainsi :
  $\forall w \in \partial\Omega\ \frac{f_n(w)}{w-z} \to \frac{f(w)}{w-z}$
  $\forall w \in \partial\Omega |\frac{f_n(w)}{w-z}| \leq \frac{k}{|w-z|} \leq \frac{k}{d(z,\partial\Omega)}$ or $w \mapsto \frac{k}{d(z,\partial\Omega)}$ est une fonction constante donc intégrable sur $\partial\Omega$ (compacte). Donc par convergence dominée $f_n(z) \to \frac{1}{2i\pi}\int_{\partial\Omega} \frac{f(w)}{w-z}dw$ donc par unicité de la limite on a $f(z) = \frac{1}{2i\pi}\int_{\partial\Omega} \frac{f(w)}{w-z}dw$ donc par le théorème de Morera f est holomorphe sur Ω et ce pour tout Ω boule ouverte dans $\mathring{F_k}$, donc f est holomorphe sur $\mathring{F_k}$
- Notons maintenant V la réunion de tous les ouverts sur lequel f est holomorphe, V est ouvert et par propriété locale de l'holomorphie f est holomorphe sur V, de plus $V \cap O \neq \emptyset$ et ce pour tout ouvert O de U, ce qui prouve que V est dense.

□

Références

[Zav13]

Leçons concernées

- 205
- 235
- 241
- 245
- 247

1.16 Sous-espaces de $C(\mathbb{R}, \mathbb{R})$ stables par translation

Développement

Théorème 1.50. *Soit F un sous-espace vectoriel de $E = C(\mathbb{R}, \mathbb{R})$ de dimension finie n, les translations de E sont les endomorphismes définis pour $a \in \mathbb{R}$ par :*

$$t_a : \begin{pmatrix} E & \to & E \\ f & \mapsto & x \mapsto f(x+a) \end{pmatrix}$$

F est stable par toutes les translations si et seulement si F est exactement l'espace des solutions d'une équation différentielle linéaire homogène d'ordre n à coefficients constants.

Démonstration . *Si F est l'espace des solutions d'une équation différentielle homogène d'ordre n, alors par le théorème de Cauchy-Lipschitz F est de dimension n et est stable par translations. Si F est stable par translations, soit $(f_1, \dots, f_n)$ une base de F, alors :*

$$\forall a \in \mathbb{R} \quad \forall (i,k) \in [\![1,n]\!]^2 \quad \exists b_{ik}(a) \in \mathbb{R} \text{ tel que } \forall x \in \mathbb{R} \quad f_i(x+a) = \sum_{k=1}^{n} b_{ik}(a) f_k(x)$$

On pose $B(a) = (b_{ik})_{i,k}$ et $F_k(x) = \int_0^x f_k(t)dt$, $F_k \in C^1$, alors on a en intégrant $F_i(x+a) - F_i(a) = \sum\limits_{k=1}^{n} b_{ik}(a) F_k(x)$

De plus la famille $(F_i)_i$ est libre car : $\left(\sum\limits_{i=1}^{n} a_i F_i = 0 \underset{\text{en dérivant}}{\Longrightarrow} \sum\limits_{i=1}^{n} a_i f_i = 0 \right)$

Lemme 1.51. *Il existe $(x_1, \dots, x_n) \in \mathbb{R}^n$ / $A = (F_i(x_j))_{1 \le i,j \le n}$ soit inversible.*

Démonstration . *On pose $G = vect(F_1, \dots, F_n)$, soit $x \in \mathbb{R}$, on pose $\delta_x : \begin{pmatrix} G & \to & \mathbb{R} \\ f & \mapsto & f(x) \end{pmatrix} \in G^\star$, considérons $H = (\delta_x)_{x \in \mathbb{R}}$ alors $H^\perp = \{0\}$ (f tel que $\delta_x(f) = 0$, $\forall x \Longrightarrow f = 0$), or :*

$$\dim G^\star = n = \dim(vect(H)) + \underbrace{\dim(H^\perp)}_{0}$$

Ainsi H est une famille génératrice de $G^\star$, donc on peut trouver $(x_1, \dots, x_n)$, tel que $(\delta_{x_1}, \dots, \delta_{x_n})$ soit une base de $G^\star$, soit $(g_1, \dots, g_n)$ sa base antéduale, on note A la matrice de passage de $(g_1, \dots, g_n)$ à $(F_1, \dots, F_n)$, alors $F_i = \sum\limits_{k=1}^{n} a_{ki} g_k$, soit $F_i(x_j) = \sum\limits_{k=1}^{n} a_{ki} \underbrace{g_k(x_j)}_{\delta_{kj}} = a_{ji} \square$

On pose $C(a) = (F_i(x_j + a) - F_i(a))_{1 \le i,j \le n}$ alors on reconnaît : $C(a) = B(a)A$. Les F_i sont C^1, et donc $a \mapsto C(a)$ aussi, donc $a \mapsto B(a) = C(a)A^{-1}$ aussi, donc b_{ij} aussi, ainsi :

$$a \mapsto f_i(a) = \sum_{k=1}^{n} b_{ik}(a) f_k(0) \in C^1$$

De plus, en dérivant en a au point 0, *on a* $f_i'(x) = \sum_{k=1}^{n} b_{ik}'(0) f_k(x)$ *donc* $f_i' \in F$, *donc en notant* $D : C^\infty \to C^\infty$ *l'endomorphisme de dérivation, on a* $D(F) \subset F$.

On note π *le polynôme minimal de* $D_{|F}$, *et* $d = d^\circ \pi$, *alors* $F = \ker \pi(D_{|F}) \subset \ker \pi(D)$, *on a donc que* $n = \dim F \leq \dim \ker \pi(D) = d$ *par le théorème de Cauchy-Lipschitz. De plus,* $d \leq n$ *(le degré du polynôme minimal est plus petit que la dimension de l'espace, par Cayley-Hamilton).*

Donc finalement $n = d$, *et donc* $F = \ker \pi(D)$ *est donc exactement l'ensemble des solutions de l'équation différentielle linéaire homogène d'ordre* n *à coefficients constant donné par le polynôme* π. $\square$

Leçons concernées

- 151
- 154
- 159
- 221
- 228

1.17 Loi de réciprocité quadratique

Développement

Théorème 1.52. *Soient p, q deux nombres premiers impairs distincts on a :*

$$\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right) \times (-1)^{\frac{(p-1)(q-1)}{4}}$$

Démonstration :

- $|\{x \in \mathbb{F}_q \,/\, px^2 = 1\}| = 1 + \left(\frac{p}{q}\right)$
- Notons $S = \{(x_1, \ldots, x_p) \in \mathbb{F}_q^p \mid \sum x_i^2 = 1\}$, alors le groupe $(\mathbb{Z}/p\mathbb{Z}, +)$ agit sur les éléments de S par permutation circulaire :

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

  Il y a alors deux types d'orbites :
  - Celles où il y a un élément avec deux coordonnées différentes, soit x un représentant d'une telle orbite, alors $\mathrm{stab}(x)$ est un sous-groupe strict de $\mathbb{Z}/p\mathbb{Z}$, et donc $\mathrm{stab}(x) = \{0\}$, et donc $|\omega(x)| = \frac{|\mathbb{Z}/p\mathbb{Z}|}{\mathrm{stab}(x)} = p$
  - Celles dont toutes les coordonnées sont égales entre elles, on a donc $px_1^2 = 1$

  Ainsi $S \equiv 1 + \left(\frac{p}{q}\right) + 0 \mod p$
- Posons $d = \frac{p-1}{2}$, $a = (-1)^d$, et $A = diag\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, a\right) \in M_p(\mathbb{F}_q)$

  I_p et A sont deux symétriques inversibles de même déterminant donc sont congruentes, donc il existe $P \in GL_p(\mathbb{F}_q)$ tel que $I_n = P^T AP$, or $X \in S$ si et seulement si $X^T I_n X = 1$ si et seulement si $(PX)^T A(PX) = 1$, ainsi si on note $S' = \{Y \,/\, Y^T AY = 1\}$, on a $|S| = |S'|$.
  Notons $y = (y_1, z_1, y_2, z_2, \ldots y_d, z_d, t)$ un élément de $\mathbb{F}_q^p$, alors $y \in S'$ si et seulement si $2(y_1 z_1 + \ldots y_d z_d) + at^2 = 1$, dénombrons de tels éléments :
  - Si $y_1 = y_2 = \ldots = y_d = 0$, alors il y a $1 + \left(\frac{a}{q}\right)$ façons de choisir t, et q^d façons de choisir les z_i, soit $q^d \left(1 + \left(\frac{a}{q}\right)\right)$
  - Dans le cas où l'un des y_i est non nul, alors on a $q^d - 1$ choix pour les y_i, q possibilités pour t, et à $y_1, \ldots, y_d, t$ fixés on a $z = (z_1, \ldots z_d)$ qui doit appartenir à un hyperplan affine de $\mathbb{F}_q^d$, soit q^{d-1} possibilités. Ce qui fait en tout $q^d(q^d - 1)$

  Ainsi :

  $$\begin{aligned}
  |S'| &= q^d \left(1 + \left(\frac{a}{q}\right) + q^d - 1\right) \\
  &= q^d \left(\left(\frac{a}{q}\right) + q^d\right) \\
  &\equiv \left(\frac{q}{p}\right)^2 + \left(\frac{q}{p}\right)\left(\frac{a}{q}\right) \mod p \\
  &\equiv 1 + \left(\frac{q}{p}\right)\left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \mod p \\
  |S| &\equiv 1 + \left(\frac{q}{p}\right) \times (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \mod p
  \end{aligned}$$

- Ainsi $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \times (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \mod p$, d'où l'égalité (les nombres étant à valeurs dans $\{-1, 1\}$).

$\square$

Remarques

Ce développement est très joli, il utilise des actions de groupes, du dénombrement, la classification des formes quadratiques sur les coprs finis. Et c'est pour moi l'occasion de vous conseiller l'excellent livre Histoire hédonistes de groupes et géométries.

Références

[CG13]

Leçons concernées

- 101
- 121
- 150
- 170

1.18 Déterminant et conique

Développement

Soient 3 points P_1, P_2, P_3 non alignés dans un plan affine d'un corps K de caractéristique nul. On se place dans les coordonnées barycentriques du repère qu'ils forment. Soient M, N de coordonnées barycentriques (x, y, z) (x', y', z') distincts des trois points.
On suppose que la droite (P_iM) intercepte la droite (P_jP_k) i, j, k étant deux à deux distincts et on note M_i le point d'intersection de même pour N.

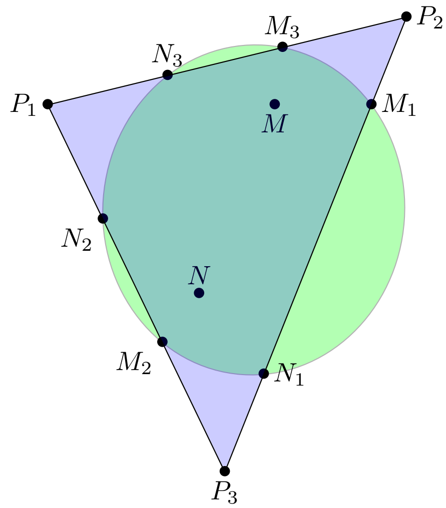

FIGURE 1.5 – Le triangle $P_1P_2P_3$, les points M et N, ainsi que la conique (ici une ellipse) passant par N_i, M_i pour $i \in [\![1, 3]\!]$.

Théorème 1.53. *Sous ces conditions les points $M_1, M_2, M_3, N_1, N_2, N_3$ sont sur une même conique.*

Démonstration :

- Dans les coordonnées cartésiennes du repère $(P_1, \overrightarrow{P_1P_2}, \overrightarrow{P_1P_3})$ une conique C est définie par le lieu des points de coordonnées (u, v) vérifiant $au^2 + buv + cv^2 + du + ev + f = 0$ où (a, b, c) n'est pas le triplet nul.
  Le passage des coordonnées barycentriques (X, Y, Z) dans le repère $(P_1,\ P_2,\ P_3)$ aux coordonnées cartésiennes est donné par $u = \frac{Y}{X+Y+Z}$ et $v = \frac{Z}{X+Y+Z}$ en remplaçant on obtient que la conique C est le lieu des points de coordonnées barycentriques (X, Y, Z) vérifiant : $\alpha X^2 + \beta Y^2 + \gamma Z^2 + \delta YZ + \epsilon XZ + \zeta XY = 0$ où $\alpha, \beta, \gamma, \delta, \epsilon, \zeta$ ne sont pas tous nuls.
- Les points $P_1(1, 0, 0)$ $M(x, y, z)$ et $M_1(0, y_1, z_1)$ (sa première coordonnée est nulle car M_1 est sur la droite P_2P_3) sont alignés donc leur déterminant est nul ainsi (y_1, z_1) est proportionnel à (y, z) donc égal (par homogénéité). Donc M_1 est sur C si et seulement si $\beta y^2 + \gamma z^2 + \delta yz = 0$ par permutation des points on obtient un système de 6 équations d'inconnues $(\alpha, \beta, \ldots, \zeta)$ dont le déterminant est :

$$\Delta = \begin{vmatrix} 0 & y^2 & z^2 & yz & 0 & 0 \\ x^2 & 0 & z^2 & 0 & xz & 0 \\ x^2 & y^2 & 0 & 0 & 0 & xy \\ 0 & y'^2 & z'^2 & y'z' & 0 & 0 \\ x'^2 & 0 & z'^2 & 0 & x'z' & 0 \\ x'^2 & y'^2 & 0 & 0 & 0 & x'y' \end{vmatrix} = \begin{vmatrix} A & B \\ C & D \end{vmatrix}$$

avec B et D des matrices commutantes (car diagonales).

Lemme 1.54. $\begin{vmatrix} A & B \\ C & D \end{vmatrix} = \det DA - BC$

Démonstration : Si $\det D \neq 0$ alors : $\begin{pmatrix} I_n & -BD^{-1} \\ 0 & I_n \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A - BD^{-1}C & 0 \\ C & D \end{pmatrix}$

donc $\begin{vmatrix} A & B \\ C & D \end{vmatrix} = \det D \det(A - BD^{-1}C) = \det(DA - BC)$ (car B, D commutent)

Sinon on pose $P = \det D \times \left(\begin{vmatrix} A & B \\ C & D \end{vmatrix} - \det DA - BC \right) \in K[x, x', y, y', z, z']$ est le polynôme nul, par intégrité de $K[x, x', y, y', z, z']$, on obtient $\begin{vmatrix} A & B \\ C & D \end{vmatrix} = \det(DA - BC)$ □

- D'après le lemme 1.54, on a donc :

$$\begin{aligned} \Delta &= \begin{vmatrix} 0 & yy'(yz' - zy') & zz'(zy' - yz') \\ xx'(xz' - zx') & 0 & zz'(zx' - xz') \\ xx'(xy' - xy') & yy'(yx' - xy') & 0 \end{vmatrix} \\ &= xx'yy'zz' \begin{vmatrix} 0 & (yz' - zy') & (zy' - yz') \\ (xz' - zx') & 0 & (zx' - xz') \\ (xy' - xy') & (yx' - xy') & 0 \end{vmatrix} \\ &= 0 \text{ en faisant } C_1 + C_2 + C_3 \to C_1 \end{aligned}$$

- Donc le déterminant est nul, donc il existe une solution non nulle, ce qui donne bien une conique.

□

Remarques

Remarque 1.55. *Ce développement présente à mon sens deux intérêts : l'utilisation des coordonnées homogènes pour avoir des équations symétriques, et de donner une application pratique à la formule des déterminants par blocs 2×2 (ici on a donné une preuve plus simple en utilisant la structure polynomiale de la situation).*

Remarque 1.56. *Je profite de ce développement pour signaler que le livre de [Eid09] est une vraie merveille.*

Références

[Eid09]

Leçons concernées

- 152
- 162
- 180
- 181

1.19 Dénombrement des polynômes irréductibles unitaires dans $\mathbb{F}_q$

Développement

Soit $\mathbb{F}_q$ un corps de caractéristiques p, on note I_q^n le nombre de polynômes irréductibles, unitaires de $\mathbb{F}_q[X]$ de degré n. On note μ la fonction de Möbius, multiplicative : $\mu(mn) = \mu(m)\mu(n)$ si m et n sont premiers entre eux.

Lemme 1.57. *Soit G un groupe abélien et $f : \mathbb{N}^\star \to G$ et $g : \mathbb{N}^\star \to G$, si $f(n) = \sum\limits_{d|n} g(d)$, alors $g(n) = \sum\limits_{d|n} \mu(\frac{n}{d}) f(d)$*

Démonstration :

- $S(n) = \sum\limits_{d|n} \mu(d)$, $S(1) = 1$, et $S(n) = 0$ $n \geq 2$, S est multiplicative, et $S(p^\alpha) = 0$, pour p premier et $\alpha \geq 1$
- $\sum\limits_{d|n} \mu(d) f(\frac{n}{d}) = \sum\limits_{d|n} \mu(d) \sum\limits_{d'|\frac{n}{d}} g(d') = \sum\limits_{d'|n} g(d') S(\frac{n}{d}) = g(n) \times 1$

□

Proposition 1.58. $X^{q^n} - X = \prod\limits_{d|n} \prod\limits_{P \in I_q^d} P$

Démonstration :

- Il est clair que $X^{q^n} - X$ n'a pas de carrés dans sa décomposition en éléments irréductibles, car il est scindé à racines simples
- Soit P un polynôme irréductible divisant $X^{q^n} - X$ de degré d, soit x une racine de P dans une clôture algébrique du corps, alors P (étant irréductible) est le polynôme minimal de x, on a alors $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)] \underbrace{[\mathbb{F}_q(x) : \mathbb{F}]}_{d}$, donc $d|n$
- Réciproquement soit $d|n$ et P un polynôme irréductibles de degré d : soit x une racine de P, donc P est son polynôme minimal, ainsi $\mathbb{F}_q(x) = \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$, car $d|n$ ainsi toute racine de P est racine de $X^{q^n} - X$, par séparabilité $P | X^{q^n} - X$

□

Théorème 1.59. *Le nombre de polynômes irréductibles unitaires dans $\mathbb{F}_q$ de degré n est :*

$$\frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

Démonstration : En passant au degré dans la proposition précédente on a :

$$q^n = \sum_{d|n} d I_q^d$$

On utilise alors la formule d'inversion de Möbius on a donc

$$nI_q^n = \sum_{d|n} \mu\left(\frac{d}{n}\right) q^d$$

□

Application 1.60. *I_q^n est toujours non nul, donc on peut toujours trouver un polynôme irréductible de degré n sur $\mathbb{F}_p$ et on peut donc construire $\mathbb{F}_{p^n}$ par quotient.*

Références

[FG94]

Leçons concernées

- 123
- 125
- 141
- 190

1.20 Simplicité $SO_n(\mathbb{R})$ pour n impair

Développement

Théorème 1.61. *$SO_n(\mathbb{R})$ est un groupe simple, pour n impair.*

Démonstration :

- Soit $G \lhd SO_n(\mathbb{R})$, différent de $\{I_n\}$, et soit $\omega \in G \setminus \{I_n\}$, $V = \ker(\omega - I_n)$, alors $1 \leq d = dimV \leq n-1$, (en effet $\omega \neq I_n$ et ω est semblable à $Diag(R_{\theta_1}, ..., R_{\theta_s}, I_d, -I_k)$, $(R_\theta \in SO_2(\mathbb{R}) \setminus \{\pm I_n\})$, alors par $\det \omega = 1$ on a k pair, et par imparité de n on a $d \geq 1$
- Soient $(e_1, ..., e_n)$ la base canonique de $\mathbb{R}^n$, pour $I \subset [|1, n|]$ de cardinal d on pose $W_I = vect\{e_i \quad i \in I\}$, ainsi il est clair que $\mathbb{R}e_i = \bigcap_{I/i \in I} W_I$, réindexons les éléments de la forme W_I en $W_1, ..., W_r$
- Soit $(f_1, ..., f_d)$ une base orthonormée de V (par Gram-Schmidt), que l'on complète en une base orthonormée de $\mathbb{R}^n$: $(f_1, ... f_n)$, idem pour W_i : $(f'_1, ..., f'_n)$ on considère l'application linéaire $g_i : (f_k \mapsto f'_k) \in O_n(\mathbb{R})$, et quitte à changer f'_n en $-f'_n$, $g_i \in SO_n(\mathbb{R})$ et $g_i(V) = W_i$, on pose $\omega_i = g_i \omega g_i^{-1} \in G$, alors $\ker(\omega_i - I_n) = W_i$
- Considérons $\varphi : \begin{pmatrix} SO_n(\mathbb{R}) & \to & G \\ g & \mapsto & g\omega_1 g^{-1}\omega_1^{-1} ... g\omega_r g^{-1}\omega_r^{-1} \end{pmatrix} \in C^1$

  De plus $(I_n + h)\omega(I_n + h)^{-1}\omega^{-1} = I_n + h - \omega h \omega^{-1} + o(\|h\|)$, donc

$$d\varphi_{I_n} : \begin{pmatrix} so_n(\mathbb{R}) & \to & so_n(\mathbb{R}) \\ h & \mapsto & rh - \sum_{i=1}^{r} \omega_i h \omega_i^{-1} \end{pmatrix}$$

$$h \in \ker d\varphi_{I_n} \iff hr = \sum_{i=1}^{r} \omega_i h \omega_i^{-1}$$

  Soit $h \in \ker d\varphi_{I_n}$ on considère la norme euclidienne $\|A\| = \sqrt{tr^t AA}$ qui est invariante par conjugaison par un élément de $O_n(\mathbb{R})$, on a :

$$\|hr\| = \left\| \sum_{i=1}^{r} \omega_i h \omega_i^{-1} \right\| \leq \|\omega_i h \omega_i^{-1}\| + \left\| \sum_{j=1,\, j \neq i}^{r} \omega_j h \omega_j^{-1} \right\| \leq \sum_{j=1}^{r} \|\omega_j h \omega_j^{-1}\| = r\|h\|$$

  Il y a donc égalité dans l'inégalité triangulaire d'une norme euclidienne donc :

$$\begin{aligned} \exists \lambda > 0 \quad \omega_i h \omega_i^{-1} &= \lambda \sum_{j=1,\, j \neq i}^{r} \omega_j h \omega_j^{-1} \\ (1+\lambda)\omega_i h \omega_i^{-1} &= \lambda \sum_{j=1}^{r} \omega_j h \omega_j^{-1} = \lambda r h \\ \|(1+\lambda)\omega_i h \omega_i^{-1}\| &= \lambda \|rh\| \\ (1+\lambda)\|h\| &= \lambda r \|h\| \end{aligned}$$

- Ainsi $h = 0$ ou $1 + \lambda = \lambda r$ dans tous les cas $h = \omega_i h \omega_i^{-1}$, donc h commute avec ω_i et ce $\forall i$. Donc h stabilise $W_i = \ker(\omega_i - I_n)$ donc stabilise par intersection $\mathbb{R}e_i$, donc h est diagonalisable tout en étant antisymétrique ($h \in T_{I_n}O_n(\mathbb{R}) = so_n(\mathbb{R})$), donc $h = 0$, donc on peut appliquer le théorème d'inversion locale : φ est un C^1-difféomorphisme local sur un ouvert de I_n de $SO_n(\mathbb{R})$ dans un ouvert de G, en particulier G est d'intérieur non vide

- $G = \bigcup_{g \in G} g\overset{\circ}{G}$ est ouvert car $x \mapsto xg$ est un homéomorphisme donc transforme un ouvert en un ouvert.
- $SO_n(\mathbb{R}) \setminus G = \bigcup_{g \notin G} gG$ est réunion d'ouvert donc est ouvert, ainsi G est à la fois ouvert et fermé de $SO_n(\mathbb{R})$.
- Enfin $SO_n(\mathbb{R})$ est connexe par arc (grâce à la décomposition des matrices de $SO_n(\mathbb{R})$ on peut les relier continûment à I_n) donc connexe, donc $G = SO_n(\mathbb{R})$.

□

Remarques

Remarque 1.62. *Présenté à l'oral d'analyse (204). Note : 17/20 (en utilisant directement la stricte convexité de la norme euclidenne au lieu de la redémontrer sans le dire en passant par le cas d'égalité dans l'inégalité de Cauchy-Schwarz).*
Seule question posée lors de cette oral à propos de ce développement : « pourquoi $SO_n(\mathbb{R}) \setminus G = \bigcup_{g \notin G} gG$ *? »*

Références

[GT98]

Leçons concernées

- 160
- 204
- 214
- 217

1.21 Méthode du gradient optimal

Développement

Soit $J : \mathbb{R}^p \to \mathbb{R}$ C^1 que l'on suppose elliptique c'est-à-dire :

$$\exists \alpha > 0 \ / \ \langle \nabla J(x) - \nabla J(y) \,|\, x - y \rangle \geq \alpha \|x - y\|^2 \ \forall x, \ y \in \mathbb{R}^n$$

On cherche à approximer de manière itérative le minimum de J.

Théorème 1.63. *On définit la méthode du gradient à pas optimal par $u_0 \in \mathbb{R}^p$ et $u_{n+1} = u_n - \rho(u_n)\nabla J(u_n)$ où $\rho(u_n)$ vérifie : $\frac{d}{d\rho} J(u_n - \rho \nabla J(u_n)) = 0$*
Alors J admet un minimum, cette méthode est bien définie et u_n tend vers le minimum de J

Démonstration :

- Par la formule de Taylor on a :

$$\begin{aligned}
J(v) - J(u) &= \int_0^1 \langle \nabla J(u + t(v-u)) \,|\, v - u \rangle \, dt \\
&= \langle \nabla J(u) \,|\, v - u \rangle + \int_0^1 \frac{1}{t} \langle \nabla J(u + t(v-u)) - \nabla J(u) \,|\, t(v-u) \rangle \, dt \\
&\geq \langle \nabla J(u) \,|\, v - u \rangle + \int_0^1 \alpha t \|u - v\|^2 dt \\
J(v) - J(u) &\geq \langle \nabla J(u) \,|\, v - u \rangle + \frac{\alpha}{2} \|u - v\|^2
\end{aligned}$$

  Donc pour $v \neq u$ on a $J(v) - J(u) > \langle \nabla J(u) \,|\, v - u \rangle$ et donc J est strictement convexe, de plus pour $u = 0$ on a : $J(v) \geq J(0) + \langle \nabla J(0) \,|\, v \rangle + \frac{\alpha}{2}\|v\|^2 \geq J(0) - \|\nabla J(0)\| \times \|v\| + \frac{\alpha}{2}\|v\|^2 \to +\infty$
- En dehors d'un compact $J > J(0)$, et dans ce compact il y a un minimum, soit donc u est un minimum de J, alors on a : $J(v) - J(u) > \langle \nabla J(u) \,|\, v - u \rangle = 0$, donc le minimum est unique.
- Par restriction à une droite affine, on a encore une fonction strictement convexe sur $\mathbb{R}$ donc atteint son minimum en un point unique, donc la méthode est bien définie.
- En dérivant par rapport à ρ on a $\langle \nabla J(u_n) \,|\, \nabla J(u_n - \rho \nabla J(u_n)) \rangle = 0$ soit $\langle \nabla J(u_n) \,|\, \nabla J(u_{n+1}) \rangle = 0$ donc $\langle u_{n+1} - u_n \,|\, J(u_{n+1}) \rangle = 0$, donc $J(u_n) - J(u_{n+1}) \geq \frac{\alpha}{2}\|u_{n+1} - u_n\|^2$
- $J(u_n)$ est une suite décroissante et minorée par $J(u)$ donc converge, ainsi $J(u_n) - J(u_{n+1}) \to 0$.
- Mais alors u_n est borné, (car sinon $J(u_{n_p}) \to +\infty$) Heine sur un compact : ∇J est uniformément continue, $u_{n+1} - u_n \to 0$ donc $\nabla J(u_{n+1}) - \nabla J(u_n) \to 0$.
- $\|\nabla J(u_n)\|^2 = \langle \nabla J(u_n) \,|\, \nabla J(u_n) \rangle = \langle \nabla J(u_n) \,|\, \nabla J(u_n) - J(u_{n+1}) \rangle \leq \|\nabla J(u_n)\| \times \|\nabla J(u_n) - \nabla J(u_{n+1})\|$ donc $\nabla J(u_n) \to 0$ et
- $\alpha\|u_n - u\|^2 \leq \langle \nabla J(u_n) - \nabla J(u) \,|\, u_n - u \rangle \leq \|\nabla J(u_n)\| \times \|u_n - u\|$ Ainsi $\|u_n - u\| \leq \frac{1}{\alpha}\|\nabla J(u_n)\|$ donc $u_n \to u$.

$\square$

Complément

Complément 1.64. *Soit $A \in S_n^{++}$ et $b \in \mathbb{R}^n$, considère $J(u) = \frac{1}{2}\langle Au \,|\, u \rangle - \langle b \,|\, u \rangle$ alors la méthode du gradient converge vers X où $AX = b$.*

Démonstration : Tout d'abord $J \in C^1$ et $\nabla J(u) = Au - b$, donc pour le minimum X (s'il existe) on a $AX = b$ de plus et on a :

$$\langle \nabla J(u) - \nabla J(v) \,|u - v \rangle = \langle A(u-v) \,| u - v \rangle \geq \lambda \|u - v\|^2$$

Pour λ la plus petite valeur propre de A, on a donc le caractère elliptique.
De plus on cherche à avoir $0 = \langle \nabla J(u_{n+1}) \,| \nabla J(u_n) \rangle = \langle Au_n - A\left(\rho(u_n)\nabla J(u_n)\right) - b \,| Au_n - b \rangle$ on pose $v_n = Au_n - b$ alors on a $\|w_n\|^2 - \rho(u_n) \langle Aw_n \,| w_n \rangle = 0$, donc $\rho(u_n) = \frac{\|w_n\|^2}{\langle Aw_n | w_n \rangle}$ □

Références

[Cia82]

Leçons concernées

- 219
- 226
- 229
- 253

1.22 Théorème de Grothendieck

Développement

Théorème 1.65. *Soit $p \geq 1$ et (Ω, μ) un espace probabilisé. Soit F un sous-espace vectoriel fermé de $L^p = L^p(\Omega, \mu)$ inclus dans $L^\infty(\mu)$, alors F est un espace vectoriel de dimension finie.*

Démonstration :

- Considérons $i : F \to L^\infty$. Soit $(f_n, i(f_n))_n$ une suite d'éléments du graphe de i qui converge vers $(f, g) \in F \times L^\infty$. Alors $f_n \overset{L^p}{\to} f$, et donc par extraction f_{n_k} converge vers f presque partout, ainsi $f = g$, donc le graphe de i est fermé, donc d'après le théorème du graphe fermé (F est un fermé d'un complet donc complet, tout comme L^∞) i est une forme linéaire continue, donc il existe K tel que :
$$\forall f \in F \quad \|f\|_\infty \leq K\|f\|_p$$
- Si $p < 2$, alors $\int_\Omega |f|^p d\mu \leq (\int_\Omega |f^p|^{\frac{2}{p}})^{\frac{p}{2}}) \int_\Omega d\mu)^{\frac{2-p}{2}}$, ainsi $\|f\|_p \leq \|f\|_2$, ainsi :
$$\|f\|_\infty \leq K\|f\|_2$$
Si $p \geq 2$, alors pour presque tout $x \in \Omega$, donc $|f(x)|^p \leq \|f\|_\infty^{p-2}|f(x)|^2$, et donc : $\|f\|_p^p \leq \|f\|_\infty^{p-2}\|f\|_2^2$, ainsi : $\|f\|_\infty \leq K^p\|f\|_p^p \leq K^p\|f\|_\infty^{p-2}\|f\|_2^2$ d'où :
$$\|f\|_\infty \leq K^{p/2}\|f\|_2$$
En posant $M = max(K, K^{\frac{p}{2}})$ on a :
$$\|f\|_\infty \leq M\|f\|_2$$
- $F \subset L^\infty \subset L^2$
- Soit $(f_i)_{1 \leq i \leq n}$ une famille orthonormée dans L^2 de fonction de F. Pour $c \in \mathbb{Q}^n$, on considère N_c de mesure nulle telle que pour $x \in \Omega \setminus N_c$ on ait :
$$|\sum c_k f_k(x)| \leq \|\sum c_k f_k\|_\infty$$
Et On pose $\Omega' = \Omega \setminus (\bigcup_{c \in \mathbb{Q}^n} N_c)$ de mesure 1.
$\forall x \in \Omega' \quad \forall c \in \mathbb{Q}^n$ on a :
$$|\sum c_i f(x)| \leq \|\sum c_i f_i(x)\| \leq \|\sum c_i f_i\|_\infty \leq M\|\sum c_i f_i\|_2 = M\sqrt{\sum |c_i|^2}$$
Par densité de $\mathbb{Q}^n$ dans $\mathbb{R}^n$ on a encore :
$$\forall x \in \Omega' \, \forall c \in \mathbb{R}^n \quad |\sum c_i f_i(x)| \leq M\sqrt{\sum |c_i|^2}$$
- Prenons maintenant $c_i = f(x)$, on a alors :
$$\left(\sum f_i(x)^2\right)^2 \leq M \sum f_i(x)^2$$
Soit : $\sum f_i^2(x) \leq M^2$, que l'on intègre sur Ω' de mesure 1, on a ainsi $n \leq M^2$, donc F est de dimension finie.

$\square$

Attention

Remarque 1.66. *On fera attention : il semble qu'il y ait une erreur dans le livre de Zavidovique, ce n'est pas parce qu'on a* $|f_i(x)| \leq \|f_i\|_\infty$ *pour tout* x *et pour tout* i*, que cette inégalité est encore vraie pour des combinaisons linéaires de ces* f_i*, (on peut trouver des contre-exemples).*

Références

[Zav13]

Leçons concernées

- 205
- 208
- 213
- 234

1.23 Marche aléatoire en dimension ≥ 3

Développement

Théorème 1.67. *Soit $d \geq 3$, on définit une marche aléatoire sur $\mathbb{Z}^d$ par $X_0 = 0_d$ et par $X_{n+1} = X_n + \theta_n$ où les (θ_n) est une suite de variables aléatoires indépendantes suivant la uniforme à valeurs dans $\{\pm e_1, \dots \pm e_d\}$, ou $(e_1, \dots, e_d)$ est la base canonique de $\mathbb{R}^d$, alors $\mathbb{P}(X_n = 0$ une infinité de fois$) = 0$.*

Démonstration :

- On calcule φ la fonction caractéristique de θ_1 :

$$\varphi(t) = \frac{1}{2d} \sum \exp(i \langle t \,|e_j \rangle) + \exp(-i \langle t \,|e_j \rangle) = \frac{1}{d} \sum_t \cos t_j$$

  Alors par indépendances des θ_n on a :

$$\varphi_{X_n}(t) = \varphi(t)^n = \sum_{k \in \mathbb{Z}^d} \mathbb{P}(X_n = k) \exp(itk)$$

- En utilisant le fait que la somme de tous les possibles soit égale à 1 on a :

$$\frac{1}{(2\pi)^d} \int_{[-\pi,\pi]^d} \sum |\mathbb{P}(X_n = k) \exp(itk)| = \frac{1}{(2\pi)^d} \int_{[-\pi,\pi]^d} dt = 1$$

  On peut donc appliquer Fubini :

$$\frac{1}{(2\pi)^d} \int_{[-\pi,\pi]^d} \varphi_{X_n}(t) dt = \sum_k \mathbb{P}(X_n = k) \frac{1}{(2\pi)^d} \int_{[-\pi,\pi]^d} \exp(itk) dt = \mathbb{P}(X_n = 0_d)$$

- Puis en utilisant le théorème de convergence montone on a :

$$\sum \mathbb{P}(X_{2n} = 0_d) = \sum \frac{1}{(2\pi)^d} \int_{[-\pi,\pi]^d} \varphi(t)^{2n} dt = \frac{1}{(2\pi)^d} \int_{[-\pi,\pi]^d} \sum \varphi(t)^{2n} dt$$

  Or pour presque tout $t \in \mathbb{R}^d$, $|\varphi(t)| < 1$, donc $\sum \varphi(t)^{2n} = \frac{1}{1-\varphi^2(t)}$

- Montrons que $\frac{1}{1-\varphi^2}$ est intégrable sur $[-\pi, \pi]^d$, pour cela il suffit de montrer que c'est le cas au voisinage de[8] $(\pm\pi, \dots, \pm\pi)$ et de 0_d mais on a $\varphi\left(t + \sum_i \pm e_i \pi\right) = -\varphi(t)$ donc par translation il suffit de le faire en 0_d :
  $\varphi \in C^\infty$ par développement limité on a :

$$\varphi(t) = \frac{1}{d} \left(\sum_i 1 - \frac{t_i^2}{2} + o(t_i) \right) = 1 - \frac{||t||^2}{2d} + o(||t||^2)$$

  Donc $\varphi^2(t) = 1 - ||t||^2/d + o(||t||^2)$ donc $\frac{1}{1-\varphi^2(t)} \sim \frac{d}{||t||^2}$ est intégrable en 0_d car $2 < d$, ainsi $\sum \mathbb{P}(X_{2n} = 0_d) < +\infty$.

8. Attention les $\pm$ ne sont pas forcément les mêmes au sein d'un même vecteur.

- Notons pour $k \in \mathbb{Z}^d$, $N_k = |n \in N \ / \ X_n = k| = \sum \mathbb{1}_{\{X_n = k\}}$, alors $\mathbb{E}N_0 = \sum \mathbb{P}(X_n = 0) < +\infty$, donc $\mathbb{P}(N_0 = +\infty) = 0$ et ainsi $\mathbb{P}(N_0 < +\infty) = 1$.
- Pour $k \in \mathbb{Z}^d$, $l = \sum |k_j|$, alors $\mathbb{P}(X_l = -k) > 0$, et pour $n \geq l$ on a :

$$\begin{array}{rcl} \mathbb{P}(X_{n-l} = k \text{ et } X_n = 0) & = & \mathbb{P}(X_{n-l} = k \text{ et } \theta_{n-l+1} + \dots \theta_n = -k) \\ & = & \mathbb{P}(X_{n-k} = k)\mathbb{P}(X_l = -k) \\ & \leq & \mathbb{P}(X_n = 0) \end{array}$$

  Et par somme on a :

$$\mathbb{P}(X_l = -k) \sum \mathbb{P}(X_n = k) \leq \sum_{n \geq l} \mathbb{P}(X_n = 0) < +\infty$$

  Donc de même $\mathbb{P}(N_k < +\infty) = 1$.
- Soit $m \in \mathbb{N}$, alors $\mathbb{P}(\exists n / \ \forall p \geq n \ X_p \notin [-m, m]^d) = \mathbb{P}\left(\bigcap_{k \in [-m,m]^d} N_k < +\infty \right) = 1$

  Ainsi $\mathbb{P}(||X_n|| \to +\infty) = \lim_{m \to +\infty} \mathbb{P}(\exists n / \ \forall p \geq n \ X_p \notin [-m, m]^d) = 1$

□

Leçons concernées

- 235
- 247
- 260
- 261

1.24 Théorème de Chevalley-Warning

Développement

$\mathbb{F}_q$ un corps de caractéristique p.

Lemme 1.68. *Soit $m \in \mathbb{N}$, tel que $m = 0$ ou $q - 1 \not| m$ alors :* $\sum\limits_{x \in \mathbb{F}_q} x^m = 0$

Démonstration :

- Si $m = 0$: trivial.
- Si $q - 1 \not| m$: soit g un générateur de $\mathbb{F}_q^\star$: $\sum\limits_{x \in \mathbb{F}_q} x^m = \sum\limits_{x \in \mathbb{F}_q} (gx)^m = g^m \sum\limits_{x \in \mathbb{F}_q} x^m$ Avec $g^m \neq 1$ (car l'ordre de g est $q - 1$ qui ne divise par m), donc $\sum\limits_{x \in \mathbb{F}_q} x^m = 0$.

□

Théorème 1.69 (Chevalley-Warning)**.** *Soient $P_1, \ldots, P_r \in \mathbb{F}_q[X_1, ..., X_n]$ non nuls, on pose $V(P_1, ...P_r)$ l'ensemble des zéros communs aux polynômes $P_1, \ldots P_r$, alors :*

$$\sum_{i=1}^{r} d^\circ P_i < n \Longrightarrow p | Card(V(P_1, \ldots, P_r))$$

Démonstration :

- On pose $S(x) = \prod(1 - P_i^{q-1})$ est la fonction caractéristique de $V(P_1, ..., P_r)$:
  En effet si x annule tous les P_i, alors $S(x) = 1$, réciproquement si $P_i(x) \neq 0$, alors $P_i(x)^{q-1} = 1$ et donc $S(x) = 0$.
- Si S est le polynôme nul, alors le résultat est clair
- Sinon $\exists A \subset \mathbb{N}^n$ fini et non vide tel que $S(X) = \sum\limits_{\alpha \in A} c_\alpha X_1^{\alpha_1} X_2^{\alpha_2} ... X_n^{\alpha_n} \quad c_\alpha \in \mathbb{F}_q^\star$
  Alors on calcule : $\sum\limits_{x \in \mathbb{F}_q^n} S(x) = \sum\limits_{\alpha \in A} c_\alpha \sum\limits_{x \in \mathbb{F}_q^n} x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n}$
- Fixons un $\alpha \in A$ alors on a : $\sum\limits_{x \in \mathbb{F}_q^n} x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n} = \prod\limits_{i=1}^{n} \sum\limits_{x_i \in \mathbb{F}_q} x_i^{\alpha_i}$
  De plus : $d^\circ S = \sum\limits_{i=1}^{r} (q-1) d^\circ P_i < n(q-1)$ ainsi $\forall \alpha \in A$, $d^\circ X_1^{\alpha_1} X_2^{\alpha_2} ... X_n^{\alpha_n} < n(q-1)$, donc par contraposée l'un des $\alpha_i < (q-1)$, donc par le lemme 1, on a que $\sum\limits_{x \in \mathbb{F}^q} x^{\alpha_i} = 0$
- Et ce pour tout $\alpha \in A$, donc $\sum\limits_{x \in \mathbb{F}_q} S(x) = 0$, et S est la fonction indicatrice de $V(P_1, ..., P_r)$, ainsi $p|\mathrm{Card}V(P_1, ..., P_r)$

□

Application 1.70. *Soient $n \in \mathbb{N}^\star$ et $a_1, \ldots a_{2n-1}$ des éléments de $\mathbb{Z}/n\mathbb{Z}$, alors il existe n éléments parmi ces $2n - 1$ dont la somme est nulle.*

Démonstration :

- Dans le cas où $n = p$ est premier on pose $f_1 = \sum_{i=1}^{2p-1} a_i X_i^{p-1}$, $f_2 = \sum_{i=1}^{2p-1} X_i^{p-1}$ On peut alors appliquer le théorème de CW, et comme $(0, \dots, 0)$ est une racine commune il en existe une non triviale : $(x_1, \dots, x_{2p-1})$, $f_2(x_1, \dots, x_{2p-1}) = 0$ il y a donc exactement p x_i qui sont non nul, et donc on conclut en utilisant f_1.
-

□

Application 1.71. *Si on se place dans $\mathbb{P}^{n-1}(\mathbb{F}_q)$ où $n \geq 3$, alors toute conique est non vide*

Démonstration : En effet soit $F = 0$ une conique projective de $\mathbb{P}^{n-1}(\mathbb{F}_q)$, $F \in \mathbb{F}_q[X_1, X_2, ..., X_n]$ est un polynôme homogène de degré 2, et $2 < 3 \leq n$, alors par CW le nombre de zéros de ce polynôme est un multiple de p, or $(0, ..., 0)$ est déjà racine évidente, donc il existe des zéros non triviaux à F et donc des points à la conique dans $\mathbb{P}^{n-1}(\mathbb{F}_q)$ □

Comme par exemple la conique d'équation $X^2 + Y^2 + Z^2 = 0$ alors que dans $\mathbb{P}^2(\mathbb{R})$ c'est une conique vide.

Remarque 1.72. *Je propose de faire en développement uniquement le théorème de Chevalley-Warning et l'application pour le cas premier. On pourra écrire en remarque que le cas non premier se démontre également (à condition de savoir le faire en cas de question du jury).*

Références

[Zav13]

Leçons concernées

- 120
- 123
- 126
- 142

1.25 Théorème de Frobenius-Zolotarev

Développement

Théorème 1.73. *Soit $p \geq 3$ un nombre premier, V un $k = \mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension finie, alors pour $u \in GL(V)$ on a $\epsilon(u) = \left(\frac{\det u}{p}\right)$*

Démonstration :

- Soit M un groupe abélien, soit $\varphi : GL(V) \to M$ un morphisme, alors comme $p \geq 3$, on a que $D(GL_n(k)) = SL_n(k)$, et $\varphi(aba^{-1}b^{-1}) = \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1} = 1$, donc $SL_n(k) \subset \ker\varphi$, donc φ se factorise en un unique morphisme $\overline{\varphi} : GL_n(k)/SL_n(k) \to M$, $\varphi = \overline{\varphi} \circ \pi$, où $\pi : GL_n(k) \to GL_n(k)/SL_n(k)$.
  De même pour $\det : GL_n(k) \to k^\star$ surjectif, dont le noyau est $SL_n(k)$, donc $\overline{\det} : GL_n(k)/SL_n(k) \to k^\star$ est en fait un isomorphisme. $\det = \overline{\det} \circ \pi$.
  Donc $\varphi = \overline{\varphi} \circ \overline{\det}^{-1} \circ \overline{\det} \circ \pi = \alpha \circ \det$. Où $\alpha : \mathbb{Z}/p\mathbb{Z}^\star \to M$.
- Le symbole de Legendre est un morphisme non trivial de $\mathbb{Z}/p\mathbb{Z}^\star$ car il y a $\frac{p-1}{2}$ carrés, soit $\alpha : \mathbb{Z}/p\mathbb{Z}^\star \to \{-1, 1\}$ un morphisme non trivial, alors $\ker\alpha$ est un sous-groupe d'indice 2 de $\mathbb{Z}/p\mathbb{Z}^\star$, or $\mathbb{Z}/p\mathbb{Z}^\star$ est un groupe cyclique, donc possède un seul groupe de cardinal $\frac{p-1}{2}$ (p est impaire), donc $\ker\alpha = \{x^2, x \in \mathbb{Z}/p\mathbb{Z}\}$, donc $\alpha = 1$ sur les carrés et -1 sur les non carrés, donc α est le symbole de Legendre.
- Considérons le morphisme $\epsilon : GL(V) \to \{-1, 1\}$, ainsi par le premier point, il existe un morphisme de groupe $\alpha : \mathbb{Z}/p\mathbb{Z}^\star \to \{-1, 1\}$ tel que $\epsilon = \alpha \circ \det$, montrons alors que ϵ n'est pas un morphisme trivial, on pose $d = \dim V$, et on considère $\mathbb{F}_q$, où $q = p^d$, alors V et $\mathbb{F}_q$ sont des $\mathbb{Z}/p\mathbb{Z}$ espaces vectoriels isomorphes, or $\mathbb{F}_q^\star$ est cyclique, soit g un générateur de ce groupe. Posons $u : x \mapsto gx \in GL(\mathbb{F}_q)$, alors u fixe 0, et $g \mapsto g^2 \mapsto g^3 \ldots g^{q-1} = 1 \mapsto g$, donc $\epsilon(u) = (-1)^q = -1$ (car $q = p^d$ est impair), donc ϵ est non trivial, donc α non plus, donc α est le symbole de Legendre. Ainsi $\epsilon(u) = \left(\frac{\det u}{p}\right)$, pour tout $u \in GL(V)$.

□

Compléments

Remarque 1.74. *Ce développement peut avoir comme application de cacluler la signature de l'automorphisme de Frobenius.*

Complément 1.75. $D(GL_n(k)) = SL_n(k)$

Démonstration :

- $D(GL_n(k)) \subset SL_n(k)$. Pour l'inclusion réciproque il suffit de montrer qu'une transvection est un commutateur (elles sont toutes conjugués dans $GL_n(k)$) :
- $I_n + (1 - 2^{-1})E_{1,2} = [I_n + E_{1,2}, Diag(2^{-1}, 1, \ldots, 1)]$

□

Complément 1.76. *Soit $n \in \mathbb{N}^\star$, et $G = \mathbb{Z}/n\mathbb{Z}$ le sous-groupe cyclique d'ordre n, et soit $d|n$, alors G a un unique sous groupe d'ordre d.*

Démonstration : Les sous-groupes de G sont en bijection avec les sous groupes de $\mathbb{Z}$ contenant $n\mathbb{Z}$ qui sont les $k\mathbb{Z}$ pour $k|n$, en notant $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la projection canonique on voit que $\pi(k\mathbb{Z})$ est cyclique (car engendré par k) d'ordre $\frac{n}{k}$
$\square$

Références

[BMP04]

Leçons concernées

- 106
- 120
- 121
- 152

1.26 Méthode de la relaxation

Développement

Théorème 1.77. *Soit $A \in S_n^{++}$, $b \in \mathbb{R}^n$, $A = D+T+T^T$ où D diagonale, T triangulaire supérieure strict, $\omega > 0$, $M = \frac{1}{\omega}D + T^T$ et $N = \frac{1-\omega}{\omega}D - T$, $A = M - N$, $F : x \mapsto M^{-1}Nx + M^{-1}b$, et pour $u_0 \in \mathbb{R}^n$ alors on définit la suite (u_n) par $u_{n+1} = F(u_n)$, soit u tel que $Au = b$ alors :*

- *si $\omega \in]0, 2[$ alors $u_k \to u$*
- *si $\omega \geq 2$ alors il existe u_0 tel que u_n diverge*

Démonstration :

- $D_{ii} = A_{ii} = e_i^T A e_i > 0$ car $A \in S_n^{++}$, donc M est bien inversible et $Au = b$ si et seulement si $u = F(u)$
- Si $\omega \in]0, 2[$, alors il existe une norme subordonnée telle que $\|M^{-1}N\| < 1$: En effet notons $\| \quad \|$ la norme subordonnée à $v \mapsto \sqrt{v^T A v}$.
  $\|M^{-1}N\| = \|I_n - M^{-1}A\| = \|v_0 - M^{-1}Av_0\|$ pour un certain v_0 de norme 1, par compacité de la boule unité fermée. On pose $w_0 = M^{-1}Av_0$, $v_0 = A^{-1}Mw_0$, alors :
$$\begin{aligned} \|M^{-1}N\|^2 &= \|v_0 - w_0\|^2 \\ &= v_0^T A v_0 - v_0^T A w_0 - w_0^T A v_0 + w_0^T A w_0 \\ &= 1 - w_0^T M^T (A^{-1T} A) w_0 - w_0^T M w_0 + w_0^T A w_0 \\ &= 1 - w_0^T (M^T + M - A) w_0 \\ &= 1 - \left(\frac{2}{w} - 1\right) w_0^T D w_0 \\ &< 1 \end{aligned}$$
- $\|F^k(u_0) - u\| = \|F^k(u_0) - F^k(u) = \|(M^{-1}N)^k(u_0 - u)\| \leq \|M^{-1}N\|^k \|u_0 - u\| \to 0$
- Soient $\lambda_1, \dots, \lambda_n$ les valeurs propres complexes de $M^{-1}N$, alors :
$$\prod |\lambda_i| = \frac{|\det N|}{|\det M|} = \frac{(\frac{1-\omega}{\omega})^n |\det D|}{\frac{1}{\omega^n}|\det D|} = (1-\omega)^n \geq 1$$
  Donc il existe une valeur propre λ de module ≥ 1, soit $v = v_1 + iv_2$ un vecteur propre associé, on pose $w_1 = v_1 + u$, $w_2 = v_2 + u$ alors $(F^k(w_1))_k$ ou $(F^k(w_2))_k$ diverge, en effet sinon $F^k(v_1 + u) - u = (M^{-1}N)^k v_1 \to 0$, de même $(M^{-1}N)^k v_2 \to 0$ par combinaison linéaire on a donc $\lambda^k v = (M^{-1}N)^k v \to 0$, absurde car $|\lambda| \geq 1$.

□

Références

[Cia82]

Leçons concernées

- 158
- 162
- 208
- 232

1.27 Inversion de Fourier

Développement

Proposition 1.78. *On note* $f(x) = e^{-x^2}$*, alors* $\hat{f} = \sqrt{\pi}e^{-t^2/4}$

Démonstration : Notons $h(x,z) = e^{zx}e^{-x^2}$:

- $z \mapsto h(x,z)$ est holomorphe pour tout $x \in \mathbb{R}$
- $x \mapsto h(x,z)$ est mesurable pour tout $z \in \mathbb{C}$
- Pour $z \in B(0,R)$, on a $|h(x,z)| = e^{xRez - x^2} \leq \begin{cases} e^{-x^2/2} = g(x) & \text{si} \quad |x| \geq 2R \\ e^{|x|R - x^2} = g(x) & \text{sinon} \end{cases}$

Ainsi $g \in L^1(\mathbb{R})$, et donc $F(z) = \int_{\mathbb{R}} e^{zx}e^{-x^2}dx$ est bien définie et holomorphe sur $\mathbb{C}$.
De plus pour z réel $F(z) = \int_{\mathbb{R}} e^{-(x-z/2)^2}e^{z^2/4}dx = e^{z^2/4}\sqrt{\pi}$, par prolongement analytique on a que $F(z) = \sqrt{\pi}e^{z^2/4}$ sur $\mathbb{C}$, or $\hat{f}(t) = F(-it) = \sqrt{\pi}e^{-t^2/4}$.

□

Théorème 1.79. *Soit* $f \in S(\mathbb{R})$*, alors* $f(x) = \frac{1}{2\pi}\int_{\mathbb{R}} e^{itx}\hat{f}(t)dt$

Démonstration :

- Soit $0 < \epsilon_n \to 0$, alors $|e^{itx}e^{-\epsilon_n t^2}\hat{f}(t)| \leq |\hat{f}(t)|$ et $\hat{f} \in L^1$, donc par convergence dominée on a :
  $\frac{1}{2\pi}\int_{\mathbb{R}} e^{itx}\hat{f}(t)dt = \frac{1}{2\pi}\lim \int_{\mathbb{R}} e^{itx - \epsilon_n t^2}\hat{f}(t)dt$
- Or par le théorème de Fubini-Tonelli on a :

$$\int_{\mathbb{R}}\left(\int_{\mathbb{R}} |e^{it(x-y)-\epsilon_n t^2}f(y)|dy\right)dt = \int e^{-\epsilon_n t^2}dt\int |f(y)|dy < +\infty$$

- On peut donc appliquer le théorème de Fubini :

$$\begin{aligned}
\frac{1}{2\pi}\int_{\mathbb{R}} e^{itx-\epsilon_n t^2}\hat{f}(t)dt &= \frac{1}{2\pi}\int_{\mathbb{R}} e^{itx-\epsilon_n t^2}\left(\int_{\mathbb{R}} e^{-ity}f(y)dy\right)dt \\
&= \frac{1}{2\pi}\int_{\mathbb{R}} f(y)dy\int_{\mathbb{R}} e^{it(y-x)}e^{-\epsilon_n t^2}dtdy \\
&= \frac{1}{2\pi\sqrt{\epsilon_n}}\int_{\mathbb{R}} f(y)dy\int_{\mathbb{R}} e^{it\frac{y-x}{\sqrt{\epsilon_n}}}e^{-t^2}dtdy \\
&= \frac{\sqrt{\pi}}{2\pi\sqrt{\epsilon_n}}\int_{\mathbb{R}} f(y)e^{-\frac{(y-x)^2}{4\epsilon_n}}dy \\
&= \frac{1}{\sqrt{\pi}}\int_{\mathbb{R}} f(x+2\sqrt{\epsilon_n}u)e^{-u^2}du \quad u = \frac{y-x}{2\sqrt{\epsilon_n}} \\
&\to f(x)
\end{aligned}$$

Par application de la convergence dominée car $|f(x+2\sqrt{\epsilon_n}u)e^{-u^2}| \leq N_\infty(f)e^{-u^2} \in L^1$.

□

Références

[QZ13]

Leçons concernées

- 236
- 240
- 254
- 255

1.28 Continuité des racines d'une suite de polynômes

Développement

Théorème 1.80. *Soit $(P_m)_{m\in\mathbb{N}}$ une suite de polynômes à coefficients complexes unitaires de degré n, on suppose que $P_m \to P$, alors pour tout m entier naturel on peut mettre P_m ainsi que P de la forme :*

$$\begin{array}{rcl} P_m(X) & = & \prod_{i=1}^{n}(X - x_m^i) \\ P(X) & = & \prod_{i=1}^{n}(X - x^i) \\ \forall i \in [\![1,n]\!] \quad x_m^i & \underset{m\to\infty}{\to} & x^i \end{array}$$

Pour montrer ce théorème on va munir $\mathbb{C}_n[X]$ de la norme N définie par $N\left(\sum_{k=0}^{n} a_i X^i\right) = \sum_{k=0}^{n} |a_i|$.

Lemme 1.81. *Soit $P \in \mathbb{C}_n[X]$, polynôme unitaire de degré n et x une racine de P, alors $|x| \le N(P)$*

Démonstration :

- si $|x| \le 1$, alors $|x| \le 1 \le N(P)$ car P est unitaire.
- Sinon on a $|x| > 1$, ainsi $x^n = -\sum_{k=0}^{n-1} a_i x^i$

  Et donc $x = -\sum_{k=0}^{n-1} a_i x^{i-n+1}$, et donc $|x| \le \sum_{k=0}^{n-1} |a_i| \le N(P)$

□

Lemme 1.82. *Soit $(P_m)_{m\in\mathbb{N}}$ une suite de polynômes à coefficients complexes unitaires de degré n, on suppose que $P_m \to P$, soit x une racine de P, pour tout m entier naturel on note $(x_m^1, x_m^2, ..., x_m^n)$ les racines de P_m comptés avec multiplicités alors on note que :*

$$M = \sup_{m\in\mathbb{N}} N(P_m) < \infty$$

Car $P_m \to P$ donc (P_m) est une suite bornée, on a par le lemme 1.81 que M majore en module tous les x_m^i pour $m \in \mathbb{N}$ et $i \in [\![1,n]\!]$ alors on a que :

$$\forall \epsilon > 0 \, \exists N \in \mathbb{N} \, \forall m \ge N \, \exists i \in [\![1,n]\!] \ / \ |x - x_m^i| < \epsilon$$

Démonstration : Soit $x \in \mathbb{C}$ supposons par l'absurde que :

$$\exists \epsilon > 0 \, \forall N \in \mathbb{N} \, \exists m \ge N \, \forall i \in [\![1,n]\!] \ |x - x_m^i| \ge \epsilon$$

Alors on peut construire une extraction φ tel que :

$$\exists \epsilon > 0 \, \forall m \in \mathbb{N} \, \forall i \in [\![1,n]\!] \ |x - x_{\varphi(m)}^i| \ge \epsilon$$

La suite $\left(\left(x^i_{\varphi(m)}\right)_{i\in[\![1,n]\!]}\right)_{m\in\mathbb{N}}$ est dans $B(0,M)$ compact de $\mathbb{C}^n$: il existe ψ une extraction telle que :

$$\forall i \in [\![1,n]\!]\ x^i_{\psi o\varphi(m)} \underset{m\to\infty}{\to} x^i$$

$$P = \lim P_{\psi o\varphi(m)} = \lim \prod (X - x^i_{\psi o\varphi(m)}) = \prod (X - x^i)$$

Ainsi les racines de P sont exactement les x^i, qui vérifient par passage à la limite $|x - x^i| \geq \epsilon$, donc x n'est pas racine de P, ce qui est absurde. $\square$

Démonstration : (du théorème 1.80)
Raisonnons par récurrence sur n, pour $n = 1$ on a $P_m = X - x_m \to P = X - x$, donc $x_m \to x$, supposons la propriété vrai au rang $n-1$ alors :
Soit x^n une racine de P, par le lemme précédent il existe x^n_m racine de P_m tel que $x^n_m \underset{m\to\infty}{\to} x^n$, on a alors $P = (X-x^n)Q$ et $P_m = (X-x^n_m)Q_m$, si on a que $Q_m \to Q$ il suffit d'appliquer HR(n-1). $\square$

Preuve algébrique que $Q_m \to Q$

On se place dans $\mathbb{C}[a_0, a_1, ..., a_n, x][X]$ soit $P = \sum_{i=0}^{n} a_i X$ dont on fait la division euclidienne en X par $X - x$ (possible car $X - x$ unitaire), alors :

$$P = Q(X - x) + R \text{ où } Q \in \mathbb{C}[a_0, a_1, ..., a_n, x][X] \text{ et } R \in \mathbb{C}[a_0, a_1, ..., a_n, x]$$

En regroupant les termes on a $Q = \sum_{i=0}^{n-1} \tilde{Q}_i(a_0, a_1, ..., a_n, x)X^i$, où $\tilde{Q}_i$ est un polynôme de $\mathbb{C}[a_0, a_1, ..., a_n, x]$, par spécialisation les coefficients de Q_m tendent vers ceux de Q, donc $Q_m \to Q$

Preuve analytique que $Q_m \to Q$

On a $P - P_m = (x^n - x^n_m)Q_m + (X - x^n)(Q - Q_m)$, et le tout est dans $\mathbb{C}_n[X]$, $(X - x^n)(Q - Q_m) \to 0$ (car Q_m est bornée et $(x^n - x^n_m) \to 0$, ainsi $Q - Q_m = \sum_{i=0}^{n-1} a^i_m X^i$, et

$$(X - x^n_m)(Q - Q_m) = a^{n-1}_m X^n + \sum_{i=1}^{n-1} (a^{i-1}_m - x^n a^i_m)X^i - x^n_m a^0_m$$

Dont la norme tend vers 0, on en déduit de proche en proche que $a^i_m \to 0$ donc $Q - Q_m \to 0$

Remarque

Ce théorème aurait été trivial s'il existait des expressions par radicaux des racines en fonction des coefficients, mais Galois et Abel ont démontré que ce n'était pas le cas.

Références

[Gou08]

Leçons concernées

- 144
- 203
- 223
- 241

1.29 Ellipsoïde de John

Développement

Théorème 1.83. *Soit K un compact d'intérieur non vide de $\mathbb{R}^n$, (muni de sa norme $\| \quad \|$ euclidienne canonique). Il existe un unique ellipsoïde centré en 0 de volume minimal contenant K.*

Démonstration :

- On note Q (respectivement Q^+, Q^{++}) l'ensemble des formes quadratiques (respectivement positives, définies positives) de $\mathbb{R}^n$. Pour $q \in Q^{++}$ on note V_q le volume de l'ellipsoïde définie par $\{x \in \mathbb{R}^n \ / \ q(x) \geq 1\}$. Dans une base orthonormée $(e_1, \ldots, e_n)$, tel que $q(x) = \sum a_i x^2$, donc
$$V_q = \int \ldots \int_{\sum a_i x_i^2 \leq 1} dx_1 \ldots dx_n = \int \ldots \int_{t_1^2 + \ldots t_n^2 \geq 1} \frac{1}{\sqrt{a_1 \ldots a_n}} dt_1 \ldots dt_n = \frac{V}{\sqrt{\det q}}$$
(on a fait le changement de variable $t_i = x_i \sqrt{a_i}$ et on note $\det q$ le déterminant commun des matrices de q dans une base orthonormée et V le volume de la boule unité).
- Le problème revient donc à montrer qu'il existe une unique forme quadratique définie positive qui contient K et qui maximise $\det q$.
- On munit Q de la norme $N(q) = \sup\limits_{\|x\| \leq 1} |q(x)|$ et on définit $A = \{q \in Q^+, \ \forall k \in K \ q(k) \leq 1\}$
  - — A est convexe
  - — A est fermé : car $q_n \xrightarrow{N} q$ implique que pour tout $x \in \mathbb{R}$, $q_n(x) \to q(x)$.
  - — A est non vide : $n : \begin{pmatrix} \mathbb{R}^n & \to & \mathbb{R} \\ x & \mapsto & \frac{\|x\|^2}{\sup\limits_{k \in K} \|k\|^2} \end{pmatrix} \in A \cap Q^{++}$
  - — A est bornée : $\mathring{K} \neq \emptyset$, $\exists a \in K \ r > 0$ tel que $B(a, r) \subset K$. Soit $q \in A$ si $\|x\| \leq r$, alors $a + x \in K$ donc :
$$\sqrt{q(x)} = \sqrt{q(x + a - a)} \leq \underbrace{\sqrt{q(x + a)}}_{\leq 1} + \underbrace{\sqrt{q(-a)}}_{\leq 1} \leq 2$$
    Donc $q(x) \leq 4$. Si maintenant $0 < \|x\| \leq 1$, on a $|q(x)| = \frac{1}{r^2} |q(rx)| \leq \frac{4}{r^2}$, donc $N(q) \leq \frac{4}{r^2}$
- $\begin{pmatrix} A & \to & \mathbb{R}^+ \\ q & \mapsto & \det q \end{pmatrix}$ est continue sur le compact A elle atteint son maximum sur A en q_0 donc $\det q_0 \geq \det(n) > 0$ donc $q_0 \in Q^{++}$
- Soit $q \in A$ tel que $\det q = \det q_0$, on suppose que $q \neq q_0$, alors en écrivant ces déterminants dans la base canonique on a : $\det \left(\frac{1}{2}(q + q_0)\right) > \sqrt{\det q_0} \sqrt{\det q} = \det q$, ce qui par convexité de A contredit le fait que q_0 maximise le déterminant. Il y a donc existence et unicité.

□

Complément

Complément 1.84. *Soit A, B deux matrices symétriques réelles définies positives et α, $\beta \in]0, 1[$ vérifiant $\alpha + \beta = 1$ alors :*
$$\det(\alpha A + \beta B) \geq (\det A)^{\alpha} (\det B)^{\beta}$$
Et l'inégalité est stricte si $A \neq B$.

Démonstration :

- $\exists P \in GL_n(\mathbb{R})$ tel que $A = P^T P$ et $B = P^T DB$ avec D matrice diagonale à coefficients diagonaux strictement positifs, ainsi $\det(\alpha B + \beta B) = (\det P)^2 \det(\alpha I_n + \beta d)$ et $(\det A)^\alpha (\det B)^\beta = (\det P)^2 (\det D)^\beta$.
- Il suffit donc de montrer que $\prod(\alpha + \beta d_i) \geq (\prod d_i)^\beta$ ce qui est vérifié par la concavité du logarithme en 1 et en d_i puis par sommation et passage à l'exponentielle.
- Si $A \neq B$, alors l'un des $d_i \neq 1$, et donc on aura une inégalité stricte par stricte concavité du logarithme dans l'une des égalités, mais en sommant avec les autres inégalités (éventuellement larges) on va conserver l'inégalité stricte.

$\square$

Références

[FGN08]

Leçons concernées

- 158
- 170
- 171

1.30 Marche aléatoire en dimension 1 et 2

Développement

Théorème 1.85. *Soit $d \in \{1, 2\}$, on définit une marche aléatoire sur $\mathbb{Z}^d$ par $X_0 = 0_d$ et par $X_{n+1} = X_n + \theta_n$ où $(\theta_n)_n$ est une suite de va indépendantes à valeurs dans $\{\pm e_1, \dots \pm e_d\}$ de loi uniforme, où $(e_1, \dots, e_d)$ est la base canonique de $\mathbb{R}^d$, alors $\mathbb{P}(X_n = 0$une infinité de fois$) = 1$, marche récurrente.*

Démonstration :

- Pour n impair $\mathbb{P}(X_n = 0) = 0$
- Pour $d = 1$ $\mathbb{P}(X_{2n} = 0) = \frac{1}{2^{2n}}\binom{2n}{n} \simeq \frac{1}{2^{2n}}\frac{\sqrt{4\pi n}(2n/e)^{2n}}{2\pi n n^{2n}/e^{2n}} = \frac{1}{\sqrt{\pi n}}$ donc $\sum \mathbb{P}(X_{2n} = 0) = +\infty$
- Pour $d = 2$, $X_n = (Y_n, Z_n)$ et $\theta_n = (\psi_n, \varphi_n)$, alors on change de coordonnées par $\left\{\begin{array}{lcl} U_n & = & \psi_n + \varphi_n \\ V_n & = & \psi_n - \varphi_n \end{array}\right.$, alors $\mathbb{P}(U_n = 1) = \mathbb{P}(\psi_n = 1, \varphi_n = 0) + \mathbb{P}(\psi_n = 0,\ \varphi_n = 1) = \frac{1}{2}$, de même $\mathbb{P}(U_n = -1) = \frac{1}{2}$ de même pour V_n. U_n, V_n sont donc des Bernoulli de paramètre $1/2$. Soient $a, b \in \{1, -1\}$, alors $\mathbb{P}(U_n = a,\ V_n = b) = \mathbb{P}(\theta_n = ((a+b)/1, (a-b)/2)) = \frac{1}{4} = \mathbb{P}(U_n = a)\mathbb{P}(V_n = b)$ les va sont indépendantes.
  $\mathbb{P}(X_{2n} = 0) = \mathbb{P}(\sum U_k = 0, \sum V_k = 0) = \mathbb{P}(\sum U_k = 0)\mathbb{P}(\sum V_k = 0) \sim \frac{1}{\pi n}$ donc $\sum \mathbb{P}(X_{2n} = 0) = +\infty$
- On pose les va $N = |n \in \mathbb{N}, X_n = 0| = \sum \mathbb{1}_{X_n=0}$ et $T_0 = 0$ et par récurrence :
  $$T_{n+1} = \left\{\begin{array}{ll} \inf\{k > T_n, X_k = 0\} & \text{si } T_n < +\infty \\ +\infty & \text{sinon.} \end{array}\right.$$
  On a donc $X_{T_0} = 0$, $X_{T_1} = 0, \dots X_{T_n - 1} = 0$ et donc $\mathbb{P}(N \geq n) = \mathbb{P}(T_{n-1} < +\infty)$ pour $n \geq 1$.
  $$\begin{aligned} \mathbb{P}(T_{n+1} < +\infty) &= \sum_{k\in\mathbb{N}^\star}\sum_{l\in\mathbb{N}^\star}\mathbb{P}(T_n = k, T_{n+1} = k + l) \\ &= \sum_{k\in\mathbb{N}^\star}\sum_{l\in\mathbb{N}^\star}\mathbb{P}(T_n = k)\mathbb{P}(\forall j \in [\![k, k+l-1]\!]\ \theta_k + \dots + \theta_j \neq 0 \quad \theta_k + \dots \theta_{k+l} = 0) \\ &= \sum_{k\in\mathbb{N}^\star}\sum_{l\in\mathbb{N}^\star}\mathbb{P}(T_n = k)\mathbb{P}(T_1 = l) \\ &= \mathbb{P}(T_n < +\infty)\mathbb{P}(T_1 < +\infty) \end{aligned}$$
  Donc par récurrence sur $n \geq 1$ on a $\mathbb{P}(T_n < +\infty) = \mathbb{P}(T_1 < +\infty)^n$
- $+\infty = \sum \mathbb{P}(X_n = 0) = \mathbb{E}(\sum \mathbb{1}_{\{X_n=0\}}) = \mathbb{E}(\sum \mathbb{1}_{\{T_n<+\infty\}}) = \sum \mathbb{P}(T_n < +\infty) = \sum \mathbb{P}(T_1 < +\infty)^n$, donc $\mathbb{P}(T_1 < +\infty) = 1$, donc pour tout $n \geq 0$ on a $\mathbb{P}(T_n < +\infty) = 1$, donc $\mathbb{P}(N \geq n) = 1$, donc $\mathbb{P}(N = +\infty) = \lim \mathbb{P}(N \geq n) = 1$

□

Leçons concernées

- 230
- 249
- 264

1.31 Théorème de Bézout

Développement

Théorème 1.86. *Soit K un corps et soient $P, Q \in K[X,Y]$ premiers entre eux, $d^\circ P = n$, $d^\circ Q = m$, alors $V(P) \cap V(Q)$* [9] *est fini de cardinal plus petit ou égale à $n \times m$.*

Démonstration . • *On pose*

$$\left\{ \begin{array}{llllll} P(X,Y) = \sum_{i=0}^{n'} a_i(X)Y^i & d^\circ_Y P = n' \leq n & \text{alors} & a_{n'}(X) \neq 0 & d^\circ a_i(X) \leq n-i \\ Q(X,Y) = \sum_{i=0}^{m'} b_i(X)Y^i & d^\circ_Y Q = m' \leq m & \text{alors} & b_{m'}(X) \neq 0 & d^\circ b_i(X) \leq m-i \end{array} \right.$$

$$R = Res_Y(P,Q) = det \begin{pmatrix} a_{n'} & 0 & \cdots & 0 & b_{m'} & 0 & \cdots & 0 \\ a_{n'-1} & a_{n'} & \ddots & \vdots & \vdots & b_{m'} & \ddots & \vdots \\ \vdots & a_{n'-1} & \ddots & 0 & \vdots & & \ddots & 0 \\ \vdots & \vdots & \ddots & a_{n'} & b_1 & & & b_{m'} \\ a_0 & & & a_{n'-1} & b_0 & \ddots & \vdots & \vdots \\ 0 & \ddots & & \vdots & 0 & \ddots & b_1 & \vdots \\ \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 & b_1 \\ 0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & b_0 \end{pmatrix}$$

Alors $R_{ij} = \left\{ \begin{array}{lll} a_{n'+j-i} & \text{ou } 0 & \text{si } j \leq m' \\ b_{j-i} & \text{ou } 0 & \text{sinon} \end{array} \right.$ *Donc* $d^\circ R_{ij} \leq \left\{ \begin{array}{ll} n-n'+i-j & \text{si } j \leq m' \\ m+i-j & \text{sinon} \end{array} \right.$

Soit $\sigma \in S_{n'+m'}$,

$$\begin{aligned} d^\circ \prod_{i=0}^{n'+m'} R_{\sigma(j),j} &\leq \sum_{j \leq m'} [n-n'+\sigma(j)-j] + \sum_{j=m'+1}^{n'+m'} [m+\sigma(j)-j] \\ &\leq \sum \sigma(j) - \sum j + (n-n')m' + mn' \leq (n-n')m + mn' = mn \end{aligned}$$

Donc comme $R = \sum \epsilon(\sigma) \prod_{i=0}^{n'+m'} R_{\sigma(j),j}$, *on a que* $0 \leq d^\circ Res_Y(P,Q) \leq nm$. *Car le résultant n'est pas nul, les polynômes sont premiers entre eux et les termes de tête non nuls.*
Soit $(x,y) \in V(P) \cap V(Q)$, *alors* $P(x,Y)$ *et* $Q(x,Y)$ *ont un zéro commun donc* $Res_Y(P,Q)(x) = 0$, *il y a donc au plus* mn *tels* x, *par symétrie il y a au plus* mn y, *donc* $V(P) \cap V(Q)$ *est fini de cardinal au plus* $(nm)^2$.

- *Supposons K infini, notons $\{M_1, \ldots M_r\} = V(P) \cap V(Q)$, alors il existe e_2 tel que e_2 soit non colinéaire à $M_i - M_j$, on complète en e_1, tel que (e_1, e_2) soit une base de K^2, on note (X,Y) les coordonnées d'un point dans la base canonique, et (X',Y') les coordonnées d'un*

9. On note $V(P)$ l'ensemble des points d'annulation de P.

point (e_1, e_2), *alors* $\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} X' \\ Y' \end{pmatrix}$, *avec* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *inversible, on note* p *la projection sur* e_1*, parallèlement à* e_2*. Alors,* $p(M_i) = p(M_j)$ *implique* $M_i - M_j \in \ker p = vect(e_2)$ *donc* $i = j$*, de plus* $P(X, Y) = 0$ *si et seulement si* $P(aX' + bY', cX', dY') = 0$ *on note* $\hat{P}(X', Y') = P(aX' + bY', cX', dY')$*, de même pour* Q*, alors* $d^\circ \hat{P} = n$ *et* $d^\circ \hat{Q} = m$*, par ce qui précède il y a au plus* nm *abscisses dans* $V(\hat{P}) \cap V\hat{Q}) = \{M_1, \ldots M_r\}$*, donc* $r \leq nm$*.*
- *Si* K *est fini, alors* $K \subset K(T) = K'$ *et on applique le résultat précédent à* K'*.*

□

Leçons concernées

- 142
- 143
- 152

1.32 Théorème de Liapounov

Développement

Théorème 1.87. *Soit $f : \mathbb{R}^n \to \mathbb{R}^n$ une fonction de classe C^1 tel que $f(0) = 0$ considérons l'équation différentielle $y' = f(y)$ et $y(0) = x$, on suppose que les parties réelles de toutes les valeurs propres de la matrice $A = Df_0$ sont strictement négatives. Alors l'origine est un point d'équilibre attractif du système différentiel : pour tout x voisin de 0 la solution $y(t)$ tend exponentiellement vers 0 quand $t \to +\infty$.*

Démonstration :

- Considérons l'équation différentielle $z' = Az$ tel que $z(0) = x$, on a $z(t) = e^{tA}x$, soit $\| \quad \|$ une norme d'algèbre sur $M_n(\mathbb{C})$ et soit $D + N$ la décomposition de Dunford, alors :

$$\|e^{tA}\| \leq \|e^{tD}\| \times \|e^{tN}\| \leq \|e^{tD}\| \times \left(\sum_{k=0}^{n} \frac{t^k \|N^k\|}{k!}\right) \leq K e^{t \sup Re(\lambda)}(1 + |t|^n)$$

- Considérons a tel que $Re\lambda < -a$, alors on a $e^{t \sup Re(\lambda) + at}(1 + |t|^n) \underset{t \to +\infty}{\to 0}$ donc cette fonction est bornée ainsi $\|z(t)\| \leq Ce^{-at}\|x\|$
- Par Cauchy-Schwarz on a $\left\langle e^{tA}x \,\middle|\, e^{tA}y \right\rangle \leq \|e^{tA}x\| \times \|e^{tA}y\| \leq C^2 e^{-2at}\|x\| \times \|y\|$ qui est intégrable.
  Ainsi $x, y \mapsto b(x, y) = \int_0^\infty \left\langle e^{tA}x \,\middle|\, e^{tA}y \right\rangle dt$ est bien définie, symétrique, positive et si $b(x, x) = 0$, alors par continuité on a $e^{tA}x = 0$, $\forall t \in \mathbb{R}^{+\star}$ ainsi par continuité en $t = 0$ on a que $x = 0$. Donc b est en fait un produit scalaire. On note $q(x) = b(x, x)$.
  $2b(x, Ax) = \int_0^\infty 2 \left\langle e^{tA}x \,\middle|\, e^{tA}Ax \right\rangle dt = \int_0^\infty \frac{d}{dt}\|e^{tA}x\|^2 = -\|x\|^2$
- Notons y une solution maximale solution du problème initiale définie sur $I \subset \mathbb{R}^+$, on pose $r(y) = f(y) - Ay$, alors on a :

$$\begin{aligned} q(y)' &= Dq_y(y') \\ &= 2b(y, y') \\ &= 2b(y, Ay) + 2b(y, r(y)) \\ &= -\|y\|^2 + 2b(y, r(y)) \end{aligned}$$

- $|b(y, r(y))| \leq \sqrt{q(y)}\sqrt{q(r(y))}$

  Comme $r(y) = f(y) - f(0) - Df_0(y) = o(\sqrt{q(y)})$, on a :

$$\forall \epsilon > 0 \; \exists \alpha > 0 \; / \; q(y(t)) \leq \alpha \implies \sqrt{q(r(y(t)))} \leq \epsilon\sqrt{q(y(t))}$$

  Donc $2b(y(t), r(y(t))) \leq 2\epsilon q(y(t))$ pour $q(y(t)) \leq \alpha$
- Les normes $\| \quad \|$ et $\sqrt{q}$ sont équivalentes donc il existe $C > 0$ tel que $Cq(y(t)) \leq \|y(t)\|^2$.
  Ainsi $q(y(t))' \leq (-C + 2\epsilon)q(y(t))$, on pose $\beta = C - 2\epsilon > 0$ pour ϵ suffisamment petit. Donc tant que $q(y(t)) \leq \alpha$ on a $q(y(t))' \leq -\beta q(y(t))$, ce qui est satisfait si la donnée initiale $q(x) < \alpha$: En effet s'il existe un premier t_0 tel que $q(y(t_0)) = \alpha$ on a $q(y_0)'(t) \leq -\beta q(y(t_0)) < 0$ et donc $q(y(t)) > \alpha$ pour t proche de t_0 $t < t_0$, ce qui est une contradiction donc on a $q(y(t)) \leq \alpha$ pour t dans l'intervalle maximale de solution donc $y(t)$ est bornée, donc par le lemme de sortie de tout compact l'intervalle de définition contient $\mathbb{R}^+$, ainsi sur $\mathbb{R}^+$ on a $q(y)' \leq -\beta q(y)$.

- Donc $(e^{\beta t} q(t))' \leq 0$ et donc $q(y(t)) \leq e^{-\beta t} q(x)$

$\square$

Références

[Rou09]

Leçons concernées

- 156
- 220
- 221

1.33 Théorème de Kronecker

Développement

Pour tout $n \in \mathbb{N}$, on pose :

$$A_n = \{P \in \mathbb{Z}[X],\ \text{unitaire de degré } n \text{ tel que } V(P) \subset \overline{D(0,1)}\}$$

Où $V(P)$ désigne les racines de P.

Théorème 1.88. *Soit $P \in A_n$, tel que $P(0) \neq 0$, alors les racines de P sont des racines de l'unité.*

Démonstration : $P = X^n + a_1 X^{n-1} + ... + a_n = \prod (X - \alpha_i)$, $0 < |\alpha_i| \leq 1$, alors

$$|a_i| = \left| \sum_{1 \leq k_1 < k_2 < ... < k_i \leq n} \prod \alpha_j^{k_j} \right| \leq \sum_{1 \leq k_1 < k_2 < ... < k_i \leq n} 1 \leq \binom{n}{i}$$

Donc A_n est finie.
On considère $P_k(X) = \prod (X - \alpha_i^k)$ unitaire dont les racines sont dans $\overline{D(0,1)}$
On note $Q_k(X) = X^k - Y \in \mathbb{Z}[Y][X]$, $R_k(Y)$ le résultant de P et Q_k vu comme des polynômes en X.

$$R_k(Y) = \begin{vmatrix} 1 & & & & 1 & & \\ a_1 & \ddots & & & 0 & \ddots & \\ \vdots & \ddots & \ddots & & \vdots & \ddots & 1 \\ a_n & & \ddots & 1 & 0 & & 0 \\ & \ddots & & a_1 & -Y & \ddots & \vdots \\ & & \ddots & \vdots & & \ddots & 0 \\ & & & a_n & & & -Y \end{vmatrix} = \prod Q_k(\alpha_i) = \prod (\alpha_i^k - Y) = (-1)^n P_k \in \mathbb{Z}[X]$$

Donc $P_k \in A_n$, l'ensemble des racines de tous les polynômes de A_n est fini, donc $\varphi : \begin{pmatrix} \mathbb{N}^\star & \to & \bigcup_{Q \in A_n} V(Q) \\ k & \mapsto & \alpha_i^k \end{pmatrix}$ est non injectif, donc $\exists (k, \ell) \in \mathbb{N}^2$ tel que $k \neq \ell$ et $\alpha_i^k = \alpha_i^\ell$. Ainsi α_i est une racine de l'unité.
$\square$

Corollaire 1.89. *Pour tout $P \in A_n$ on a :*

$$\exists m \in \mathbb{N}, \quad \exists r \in \mathbb{N}, \lambda_1, ... \lambda_r \in Z / P = X^m \prod \Phi_{d_i}^{\lambda_i}$$

Démonstration : Soit m la multiplicité de 0 de P, $P = X^m Q$, où $Q \in \mathbb{Z}[X]$, $Q(0) \neq 0$, unitaire donc $Q \in A_m$, donc les racines de Q sont dans des racines de $X^r - 1$ pour un r bien choisie, donc en considérant la plus grandes des multiplicités des racines de Q, on a que $Q | (X^r - 1)^a$ dans $\mathbb{C}[X]$ et donc dans $\mathbb{Z}[X]$, or $X^r - 1 = \prod_{d|r} \Phi_d$ où les Φ_d sont irréductibles, donc $Q = \prod \Phi_{d_i}^{\alpha_i}$
$\square$

Corollaire 1.90. *Les seuls polynômes de A_n irréductibles sont les Φ_d tel que $\varphi(d) = n$*

Corollaire 1.91. $\phi(n) \to +\infty$

Références

[Szp09]

Leçons concernées

- 102
- 143
- 144

1.34 Ellipse de Steiner

Développement

Théorème 1.92. *Soient A, B, C trois points non alignés du plan complexe, soit $P(X) = (X - A)(X - B)(X - C)$. Alors F_1, F_2 les racines de P' sont les foyers d'une ellipse tangente aux trois côtés du triangle ABC en leurs milieux.*

Lemme 1.93 (de Poncelet)**.** *Soit E une ellipse de foyers F_1, F_2, et soient I, J deux points de l'ellipse dont les tangentes en ces points se coupent en seul point A, alors les angles $\widehat{IAF_1}$ et $\widehat{F_2AJ}$ sont égaux.*

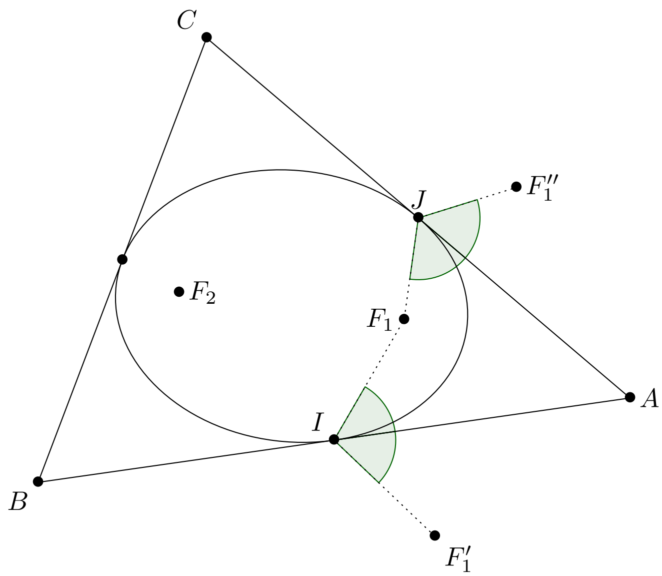

Figure 1.6 – L'ellipse inscrite dans le triangle ABC.

Démonstration :

- La droite (AI) est la bissectrice extérieur de $\widehat{F_1IF_2}$, on note F_1' le symétrique (orthogonal) de F_1 par rapport à (AI), alors les points F_2, I, F_1' sont alignés et $|F_2-F_1'| = |F_2-I|+|I-F_1'| = |F_2 - I| + |I - F_1| = 2a$, de même en notant F_1'' le symétrique de F_1 par rapport à (AJ) on a $|F_2 - F_1''| = 2a$
- Le point F_2 est sur la médiatrice de F_1F_1'', $|F_1' - A| = |F_1 - A| = |F_1'' - A|$, donc A aussi, finalement (AF_2) est la médiatrice de $F_1'F_1''$, on note R_D la symétrie d'axe D.
- Alors $R_{(AJ)} \circ R_{(AF_2)} : F_1' \mapsto F_1'' \mapsto F_1$, de plus $R_{(AF_1)} \circ R_{(AI)} : F_1' \mapsto F_1 \mapsto F_1$

  Donc $R_{(AJ)} \circ R_{(AF_2)} = R_{(AF_1)} \circ R_{(AI)}$ donc $2\widehat{IAF_1} = 2\widehat{F_2AJ}$

□

Démonstration : (du théorème)

- $P'(X)=(X-A)(X-B)+(X-A)(X-C)+(X-B)(X-C)$, donc pour $X=A$ on a $3(A-F_1)(A-F_2)=(A-B)(A-C)$, donc $\frac{B-A}{F_1-A}=3\frac{F_2-A}{C-A}$, donc $\widehat{BAF_1}=\widehat{F_2AC}$.
- On note $F_1'=R_{(AB)}(F_1)$, et $I=(F_2F_1')\cap(AB)$, et $E=\{M\in\mathbb{C}\,/\,|M-F_1|+|M-F_2|=|I-F_1|+|I-F_2|\}$ ellipse de foyers F_1, F_2 qui contient I, de plus $(AI)=(AB)$ est la bissectrice extérieur de $\widehat{F_2IF_1}$, donc la tangente en I de E est (AB).
- Soit $J\in E$ tel que (AJ) soit la tangente en J de E, alors par le lemme 1.93, on a $\widehat{IAF_1}=\widehat{F_2AJ}$ avec $\widehat{IAF_1}=\widehat{BAF_1}=\widehat{F_2AC}$, on a que $J\in[A,C)$, donc (AC) est une tangente de E par symétrie (BC) est une tangente en E.
- On remplace X par $I'=\frac{A+B}{2}$, $3(I'-F_1)(I'-F_2)=(\frac{B-A}{2})(\frac{A-B}{2})$, donc $12\frac{F_1-I'}{A-B}=\frac{B-A}{F_2-I'}$, donc $\widehat{AI'F_1}=\widehat{F_2I'B}$, donc (AB) est la bissectrice extérieur de $\widehat{F_1I'F_2}$, donc $I=I'$, par symétrie E est l'ellipse tangente aux milieux des côtés du triangle.

□

Leçons concernées

- 161
- 180
- 182

1.35 Critère de nilpotence de Cartan

Développement

Soit k un corps de caractéristique nulle, V un k-espace vectoriel de dimension finie n, $B \subset A$ deux sous espaces vectoriels de $L(V)$, on note pour $(t, x) \in L(V)^2$, $ad_t(x) = t \circ x - x \circ t$, $ad_t \in L(L(V))$.

Théorème 1.94. *On pose $T = \{t \in L(V),\, ad_t(A) \subset B\}$. Soit $t \in T$ tel que pour tout $u \in T$ on ait $tr(tu) = 0$ alors t est nilpotent.*

Démonstration :

- Considérons une base $B = (e_1, \ldots, e_n)$ tel que la matrice de t dans cette base soit sous forme de blocs de Jordan, notons aussi $(\lambda_1, \ldots, \lambda_n)$ les valeurs propres, alors si $t = s + n$ est la décomposition de Jordan de t, on a $s(e_i) = \lambda_i e_i$. On pose $F = vect(\lambda_1, \ldots, \lambda_n)$ le $\mathbb{Q}$-sous espace vectoriel de k, soit $\varphi \in F^\star$, on défini u comme l'unique endomorphisme de V qui vérifie $u(e_i) = \varphi(e_i)e_i$ pour $1 \leq i \leq n$.
- Supposons que $u \in T$, les matrices de t, u dans la base B sont triangulaires, on a alors $0 = tr(tu) = \sum \lambda_i \varphi(\lambda_i)$ en composant par φ on a $\sum \varphi(\lambda_i)^2 = 0$ donc $\varphi(\lambda_i) = 0$ pour tout i donc $\varphi = 0$ donc $F^\star = \{0\}$ donc $F = \{0\}$ et donc $\lambda_i = 0$ donc $s = 0$ donc $t = n$ est nilpotent.
- Montrons donc ce que l'on a admis, c'est-à-dire que $u \in T$, montors donc que $ad_u(A) \subset B$, Notons $D_x(v) = x \circ v$, alors $D_x^p(v) = x^p \circ v$, donc $P(D_x) = D_{P(x)}$ pour tout polynôme.
  En particulier si x est diagonalisable on peut choisir un polynôme scindé à racines simples annulateur de x ainsi $P(D_x) = D_0 = 0$, et donc D_x est diagonalisable.
  Ee même si x est nilpotent D_x est nilpotent on peut définir de même G_x de plus G_x et D_x commutent et $ad_x = D_x - G_x$ donc ad_s est diagonalisable et ad_n est nilpotent de plus ad_n et ad_s commutent car n et s commutent, ainsi $ad_t = ad_s + ad_n$, est la décomposition de Dunford de ad_t.
- Il existe $P \in k[X]$ tel que $ad_s = P(ad_t)$ et $P(0) = 0$, de plus :

  $$ad_u(E_{ij}) = (\varphi(\lambda_i) - \varphi(\lambda_j)E_{ij} = \varphi(\lambda_i - \lambda_j)E_{ij} \text{ et } ad_s(E_{ij}) = (\lambda_i - \lambda_j)E_{ij}$$

  Par l'interpolation de Lagrange on obtient $Q \in k[X]$ tel que $Q(\lambda_i - \lambda_j) = \varphi(\lambda_i - \lambda_j)$, alors $ad_u = Q(ad_s)$ (il suffit de vérifier cette relation sur E_{ij}). on pose $R = Q \circ P$, alors $ad_u = R(ad_t)$, de plus $ad_t(A) \subset B \subset A$ si $ad_t^k(A) \subset B$, alors $ad_t^{k+1}(A) \subset ad_t(B) \subset ad_t(A) \subset B$ donc par récurrence $ad_t^k(A) \subset B$, pour tout $k \in \mathbb{N}^\star$ de plus $R(0) = 0$ donc $ad_u(A) \subset B$ par combinaison linéaire et donc $u \in T$.

$\square$

Complément

Complément 1.95. *Soit $u = s + n$ la décomposition de Dunford, alors $s = P(u)$ pour un certain $P \in k[X]$ vérifiant $P(0) = 0$.*

Démonstration : Soit $\chi_u = \prod (X - \lambda_i)^{n_i}$ le polynôme caractéristique de u, d'après le théorème chinois il existe P tel que $P(X) = \lambda_i \mod (X - \lambda_i)^{n_i}$
$E = \oplus N_i$ où N_i est le sous-espace caractéristique associée à λ_i.
Or $s(x_i) = \lambda_i x_i$ pour $x \in N_i$, et $P(u) = \lambda_i I_d + (u - \lambda_i I)^{n_i}$, donc $P(u)(x) = \lambda x_i + 0 = s(x)$, ainsi

$P(u) = s$.
Si 0 est valeur propre, alors $P \equiv 0 \mod X^m$ donc $P(0) = 0$
Sinon on rajoute la condition $P \equiv 0 \mod X$ et un tel P existe encore par le lemme chinois, car $(X, (X-\lambda_1)^{n_1}, \dots (X-\lambda_r)^{n_r})$ sont encore premiers entre eux.
□

Références

[BMP04]

Leçons concernées

- 153
- 157
- 159

1.36 Nombre de zéros d'une équation différentielle linéaire du second ordre

Développement

Théorème 1.96. *Soit $a \in \mathbb{R}^+$ $q \in C^1([a, +\infty[$ $q > 0$, tel que $\int_a^{+\infty} \sqrt{q} = +\infty$ et $q'(x) = \underset{+\infty}{o}(q^{3/2}(x))$, soit y une solution réelle non nulle de $y'' + qy = 0$ sur $[a, +\infty[$ on note $N(x)$ le nombre de zéros de y sur $[a, x]$ alors :*

$$N(x) \sim \frac{1}{\pi} \int_a^x \sqrt{q(u)} du$$

Démonstration :

- Lorsque q est constant, on a une équation facile à résoudre (en cos) et on peut donc compter son nombre de zéros.
- Nombre fini de zéros sur $[a, t]$.
- On pose $\tau(x) = \int_a^x \sqrt{q}$ bijection croissante C^1 de $[a, +\infty[$ sur $[0, +\infty[$, et donc τ^{-1} est une bijection strictement croissante $\in C^1$ de $[0, +\infty[$ sur $[a, +\infty[$, on pose $Y = y \circ \tau^{-1}$, alors $y = Y(\tau)$:
  $y' = \tau' Y(\tau) = \sqrt{q} Y'(\tau)$
  $y'' = \frac{q'}{2\sqrt{q}} Y'(\tau) + q Y''(\tau)$.
  Ainsi $y'' + qy = qY''(\tau) + \frac{q'}{2\sqrt{q}} Y'(\tau) + qY(\tau) = 0$
  Donc Y est solution de $Y'' + \varphi Y' + Y = 0$ où $\varphi = \frac{q'(\tau^{-1})}{2q^{3/2}(\tau^{-1})} \underset{+\infty}{\rightarrow} 0$
- Comme Y est non nulle Y et Y' n'ont pas de zéros en commun, on peut utiliser le théorème du relèvement, ainsi il existe r, θ des fonctions de classe C^1 tel que $Y' + iY = re^{i\theta}$

  $$\begin{aligned} Y = & \quad r \sin\theta & \\ Y' = & \quad r' \sin\theta + r\theta' \cos\theta & = r\cos\theta \\ Y'' = & \quad r' \cos\theta - r\theta' \sin\theta & = -\varphi r \cos\theta - r\sin\theta \end{aligned}$$

  En faisant $cos(\theta)Y' - \sin(\theta)Y''$ on obtient :

  $$0 + r\theta' = \varphi r \cos\theta \sin\theta + r$$

  Ainsi $\theta' = 1 + \varphi \sin\theta \cos\theta$. Donc $|\theta' - 1| \leq \frac{1}{2}|\varphi| \to 0$ ainsi $\theta'(t) \to 1$ donc $\theta(t) \sim t$
- On pose $M(t)$ le nombre de zéros de Y sur $[0, t]$ il existe t_0 tel que $\theta'(t) > 0$ pour $t \geq t_0$.
  $M(t) = |\{u \in [0, t_0] \ / \ \sin(\theta(u)) = 0\}| + |\{u \in [t_0, t] \ / \ \sin(\theta(u)) = 0\}| = K + |\{v \in [\theta(t_0), \theta(t)] \ / \ \sin v = 0\}| = K + |\{k \in \mathbb{Z} \ / \ \theta(t_0) \leq k\pi \leq \theta(t)\}| \sim \frac{\theta(t)}{\pi} \sim \frac{t}{\pi}$
- De plus $N(x) = M(\tau(x)) \sim \frac{\tau(x)}{\pi}$

□

Complément

Théorème 1.97. *Soit I un invervalle de $\mathbb{R}$, $f : I \to \mathbb{C}^\star$ une fonction C^1, alors $f = re^{i\theta}$ avec r, θ des fonctions de classe C^1, de plus r est strictement positive.*

Démonstration : Soit f qui ne s'annule pas. $f(0) = r_0 e^{i\theta_0}$, et $\psi(x) = \int_0^x \frac{f'}{f} + \ln r_0 + i\theta_0$, alors $(fe^{-\psi})' = e^{-\psi}(f' - \psi' f) = 0$, donc $f(x)e^{-\psi(x)} = r_0 e^{i\theta_0} r_0^{-1} e^{-i\theta_0} = 1$ donc $f = e^{\psi} = |f| e^{iIm(\psi)} = re^{i\theta}$ en posant $r = |f|$ et $\theta = Im\psi$, qui sont C^1 $\square$

Références

[Gou08]

Leçons concernées

- 220
- 221
- 224

1.37 Table de caractères et simplicité

Développement

Proposition 1.98. *Soient $\chi_1, \ldots, \chi_r$ les caractères irréductibles d'un groupe fini G, alors les sous-groupes distingués de G sont exactement les sous-groupes de la forme $\bigcap_{i\in I} K_{\chi_i}$ où $I \subset \{1, \ldots r\}$ où on a noté $K_\chi = \{g \in G,\ \chi(g) = \chi(e)\}$ pour χ un caractère.*

Lemme 1.99. *Soit $\rho : G \to GL(V)$ une représentation de caractère χ sur V de dimension d, alors $K_\chi = \ker \rho$ (et donc est un sous groupe distingué de G).*

Démonstration : Soit $n = |G|$, alors pour $g \in G$ on a $g^n = e$ donc $X^n - 1$ est un polynôme annulateur scindé à racines simples de $\rho(g)$ donc $\rho(g)$ est diagonalisable à valeurs propres des racines n-ième de l'unité disons $\omega_1, \ldots, \omega_d$. Si $\chi(g) = \chi(e) = d$, alors $\omega_1 + \ldots + \omega_d = d$, donc $\omega_i = 1$, $\forall i$, donc $\rho(g) = Id_V$, réciproquement si $\rho(g) = Id_V$, alors $g \in K_\chi$, on a donc bien $K_\chi = \ker \rho$ $\square$

Démonstration : (du théorème) : On a alors $\bigcap_{i\in I} K_{\chi_i}$ est bien un sous groupe distingué de G.
Réciproquement soit H un sous groupe distingué de G, soit $\rho : G/H \to GL(V)$ la représentation régulière de G/H, soit $\pi : G \to G/H$ la projection canonique, on pose $\hat{\rho} = \rho\circ\pi : G \to GL(V)$, alors :

$$\rho(\pi(g)) = Id_V \iff \pi(g) = e_{G/H} \iff g \in H$$

Donc $\ker(\hat{\rho}) = H = K_{\chi_V}$, décomposons χ_V sur les représentations irréductibles de G : $\chi_V = \sum_{i=1}^{r} a_i\chi_i$, où $a_i \in \mathbb{N}$.
Montrons que $\chi_V(g) = \chi_V(e)$ si et seulement si $a_i\chi_i(g) = a_iX_i(e)\, \forall i$:
Soit $g \in G$ tel que $\chi_V(g) = \chi_V(e)$, alors $|\chi_V(g)| = |\sum a_i\chi_i(g)| \leq \sum a_i\chi_i(e) = \chi_V(e) = |\chi_V(g)|$, par cas d'égalité dans l'inégalité triangulaire on a $a_i\chi_i(g) = a_i\chi_i(e)\, \forall i$, réciproque immédiate.
Posons $I = \{i,\ a_i > 0\}$, alors $H = K_{\chi_V} = \{g \in G/a_i\chi_i(g) = a_i\chi_i(e)\, \forall i\} = \{g \in G,\ \chi_i(g) = \chi_i(e)\, \forall i \in I\} = \bigcap_{i\in I} K_{\chi_i}$. $\square$

Références

[Pey04]

Leçons concernées

- 107
- 109

1.38 Exponentielle de matrice et diagonalisabilité

Développement

Théorème 1.100. *Soit $k = \mathbb{R}$ ou $\mathbb{C}$, soit $A \in M_n(k)$ dont le polynôme caractéristique est scindé alors : A est diagonalisable si et seulement si $\exp(A)$ est diagonalisable.*

Démonstration : Le sens direct est trivial
Si $\exp(A)$ est diagonalisable, on a par Dunford $A = D + N$, et donc $\exp(N) = \exp(A)\exp(-D)$, (car A et D commutent) donc $\exp(A)$ et $\exp(-D)$ commutent et sont diagonalisables, on peut donc les diagonaliser dans une même base, ainsi $\exp(N)$ est diagonalisable ainsi :

$$\underbrace{\exp(N)}_{\text{diagonalisable}} + \underbrace{0}_{\text{nilpotent}} = \underbrace{I_n}_{\text{diagonalisable}} + \underbrace{N + \frac{1}{2}N^2 + \ldots + \frac{1}{(n-1)!}N^{n-1}}_{\text{nilpotent car N l'est}}$$

Par unicité de la décomposition de Dunford $N + \frac{1}{2}N^2 + \ldots + \frac{1}{(n-1)!}N^{n-1} = 0$
Soit X^r le polynôme minimal de N, alors $X^r | X + \frac{1}{2}X^2 + \ldots + \frac{1}{(n-1)!}X^{n-1}$ ce qui est possible que si $r = 1$, et donc $N = 0$ donc $A = D$ est diagonalisable.
□

Application 1.101. *Soit $A \in M_n(\mathbb{C})$ alors : A diagonalisable et $Sp(A) \subset 2\pi i\mathbb{Z}$ si et seulement si* $\exp(A) = I_n$

Démonstration : Le sens direct est trivial
Si $\exp(A) = I_n$, alors $\exp(A)$ est diagonalisable donc par le théorème précédent A est diagonalisable, donc $I_n = \exp(A) = \exp(PDP^{-1}) = P\exp(D)P^{-1}$, avec D diagonale dont l'exponentielle des éléments diagonaux donne donc 1, ainsi $sp(A) \subset 2\pi i\mathbb{Z}$ □

Application 1.102. *Soit $A \in M_n(\mathbb{R})$ dont le polynôme caractéristique est scindé alors : A est diagonale si et seulement si* $\exp(A)$ *est diagonale*

Démonstration : Le sens direct est trivial
Si $\exp(A)$ est diagonale, alors par le théorème A est diagonalisable : $P^{-1}AP = D$ diagonale. Les matrices $\exp(D)$, et $\exp(A)$ sont donc deux matrices diagonales avec sur leur diagonale les exponentielles des valeurs propres de A comptées avec multiplicité algébrique, donc $\exp(A) = Q\exp(D)Q^{-1}$, avec Q une matrice de permutation, quitte à changer D en QDQ^{-1}, on peut supposer que $\exp(A) = \exp(D)$.

Soit $AX = \lambda X$, alors $\exp(A)X = e^\lambda X$, ainsi $\ker(A - \lambda I_n) \subset \ker(\exp(A) - e^\lambda I_n)$ Par diagonalisabilité de A et $\exp(A)$ on a :

$$E = \bigoplus_{\lambda \in sp(A)} \ker(A - \lambda I_n) \subset \bigoplus_{\mu \in sp(\exp(A))} \ker(\exp(A) - \mu I_n) = E$$

De plus, $\exp : \mathbb{R} \to \mathbb{R}$ est injective donc nécessairement :

$$\forall \lambda \in sp(A)\ \ker(A - \lambda I_n) = \ker(\exp(A) - e^\lambda I_n)$$

On fait le même raisonnement pour D et $\exp(D)$ $(= \exp(A))$:

$$\forall \lambda \in sp(D) \ker(D - \lambda I_n) = \ker(\exp(D) - e^{\lambda} I_n)$$

Donc $\ker(A - \lambda I_n) = \ker(D - \lambda I_n)$, pour toute valeur propre de λ, donc $A = D$ est diagonale.
□

Références

[Szp09]

Leçons concernées

- 155
- 156

1.39 Composantes connexes des formes quadratiques réelles

Développement

Soit $(E, \| \quad \|)$ un $\mathbb{R}$-espace vectoriel normé de dimension finie n, soit $Q(E)$, l'ensembdes des formes quadratiques muni de la norme $N : q \mapsto \sup_{\|x\|=1} |q(x)|$, et $\Omega(E)$ l'ensemble des formes quadratiques non dégénéres.

Théorème 1.103. *1. $\Omega(E)$ est un ouvert de $Q(E)$.*

2. Pour tout $q \in Q(E)$, il existe $k > 0$, tel que si $q' \in Q(E)$ et $N(q - q') < k$, alors q' a la même signature que q.

3. Les composantes connexes de $\Omega(E)$ sont les ensembles $\Omega_i(E)$, définis comme l'ensemble des formes quadratiques de signatures $(i, n-i)$, pour i entier naturel compris entre 0 et n.

Démonstration :

2 Soit $q \in \Omega(E)$ de signature $(i, n-i)$, alors il existe F, G deux sous-espaces vectoriels supplémentaires de dimensions i, $n-i$, tel que :
- $q_{|F}$ soit une forme quadratique définie positive
- $q_{|G}$ soit une forme quadratique définie négative,

alors :
- $\sqrt{q_{|F}}$ est équivalente à $\| \quad \|_{|F}$, donc il existe $a > 0$ tel que pour tout $x \in F$ on ait $\sqrt{q(x)} \geq a\|x\|$, donc que $q(x) \geq a^2\|x\|^2$
- $\sqrt{-q_{|G}}$ est équivalente à $\| \quad \|_{|G}$ donc il existe $b > 0$ tel que pour tout $x \in G$ $\sqrt{-q(x)} \geq b\|x\|$ donc que $q(x) \leq -b^2\|x\|^2$

On pose $k = \min(a^2, b^2)$, alors :
- Pour tout $x \in F$ on a $q(x) \geq k\|x\|^2$
- Pour tout $x \in G$ on a $q(x) \leq -k\|x\|^2$

Soit $q' \in Q$ tel que $N(q - q') < k$, alors
- Pour $x \in F \setminus \{0\}$ on a $q(x) - q'(x) < k\|x\|^2$ donc $q'(x) > q(x) - k\|x\|^2 \geq 0$
- Pour $x \in G \setminus \{0\}$ on a $q'(x) - q(x) < k\|x\|^2$ donc $q'(x) < q(x) + k\|x\|^2 \leq 0$

Ainsi q, et q' on la même signature.
Donc $\Omega_i(E)$ est ouvert pour tout i

1 En particulier $\Omega(E)$ est ouvert comme réunion d'ouverts

3 On a $\Omega(E) = \bigcup \Omega_i$, avec les Ω_i ouverts et la réunion est disjointe, il reste à montrer que les Ω_i sont connexes :
Soient q, q' deux éléments de Ω_i, soient $A, B \in M_n(\mathbb{R})$ les matrices de ces formes quadratiques dans une base, alors il existe $P, Q \in O_n(\mathbb{R})$:

$$A = P^T D_i P \text{ et } B = Q^T D_i Q$$

Où D_i est une matrice diagonale avec i 1, et $n-i$ 0 sur la diagonale, alors quitte à changer la première colonne en son opposée on peut supposer que $\det P = \det Q = 1$. Par connexité de $GL_n(\mathbb{R})^+$ il existe γ un chemin continue de P à Q dans $GL_n(\mathbb{R})^+$, et donc un chemin de A à B dans les matrices de signature $(i, n-i)$, ainsi Ω_i est connexe par arcs donc connexe.

□

Complément

Complément 1.104. $GL_n(\mathbb{R})^+$ *est connexe par arcs.*

Démonstration : Soit $A \in GL_n(\mathbb{R})^+$, soit $A = OS$ sa décomposition polaire

- Comme $S_n^+ +$ est convexe, on peut relier S continûment à I_n dans $S_n^+ +$
- $O \in SO_n(\mathbb{R})$, et $SO_n(\mathbb{R})$ est connexe par arcs, ainsi on peut relier continûment 0 à I_n dans $SO_n(\mathbb{R})$

□

Références

[FGN08]

Leçons concernées

- 171
- 204

1.40 Polynômes de Bernstein

Développement

Théorème 1.105. *Soit $f \in \mathcal{C} \circ ([0,1])$, il existe $(p_n)_n$ une suite de fonctions polynomiales qui converge uniformément vers f sur $[0,1]$.*

Démonstration . • *Pour $x \in [0,1]$, et $n \in \mathbb{N}^\star$, on considère $S_{n,x}$ une variable aléatoire qui suit une loi binomiale de paramètres (n,x), et on pose pour $x \in [0,1]$:*

$$p_n(x) = \mathbb{E}\left(f\left(\frac{S_{n,x}}{n}\right)\right) = \sum_{k=0}^{n} \binom{n}{k} x^k (1-x)^{n-k} f\left(\frac{k}{n}\right)$$

p_n est bien une fonction polynomiale sur $[0,1]$.

• *Soit $\epsilon > 0$, par le théorème de Heine :*

$$\exists \alpha > 0 \quad \forall (x,y) \in [0,1]^2 \quad |x-y| \Longleftrightarrow |f(x) - f(y)| < \epsilon$$

Pour $x \in [0,1]$ on a :

$$\begin{aligned} |p_n(x) - f(x)| &= \left|\mathbb{E}\left(f\left(\frac{S_{n,x}}{n}\right) - f(x)\right)\right| \\ &\leq \mathbb{E}\left(\left|f\left(\frac{S_{n,x}}{n}\right) - f(x)\right| \mathbb{1}_{\{|\frac{S_{n,x}}{n} - x| < \alpha\}}\right) + \mathbb{E}\left(\left|f\left(\frac{S_{n,x}}{n}\right) - f(x)\right| \mathbb{1}_{\{|\frac{S_{n,x}}{n} - x| \geq \alpha\}}\right) \\ &\leq \epsilon + 2\|f\|_\infty \mathbb{P}\left(\left|\frac{S_{n,x}}{n} - x\right| \geq \alpha\right) \end{aligned}$$

• *De plus $\mathbb{P}\left(\left|\frac{S_{n,x}}{n} - x\right| \geq \alpha\right) \leq \frac{1}{\alpha^2} Var\left(\frac{S_{n,x}}{n}\right) = \frac{1}{n^2\alpha^2} Var(S_n) = \frac{1}{na^2} Var(X)$, où X est une variable aléatoirequi suit une loi de Bernoulli de paramètre x, donc $Var(X) = x(1-x) \leq \frac{1}{4}$*

• *Ainsi $N_\infty(p_n - f) \leq \epsilon + \frac{\|f\|_\infty}{2n\alpha^2}$*

□

Corollaire 1.106. *Soit $f \in C^\circ([a,b])$ alors f est limite uniforme de polynômes.*

Démonstration . *En effet il existe $(p_n)_n$ qui converge uniformément vers $x \mapsto f(a + x(b-a))$ sur $[0,1]$, donc $t \mapsto p_n\left(\frac{t-a}{b-a}\right)$ converge uniformément vers $t \mapsto f(t)$ sur $[a,b]$.* □

Propriété 1.107. *Soit $(p_n)_n$ une suite de fonctions polynomiales qui converge uniformément sur $\mathbb{R}$ vers f, alors f est une fonction polynomiale.*

Démonstration . *En effet il existe $N \in \mathbb{N}$ tel que $N_\infty(p_n - p_m) \leq 2$ pour $n, m \geq N$, par inégalité triangulaire, donc $p_n - p_m$ est une fonction polynomiale bornée donc constante, donc $p_n = p_N + \alpha_n$, donc $p_n(0) = P_N(0) + \alpha_n \to f(0)$ donc $\alpha \to \alpha$ pour un certain α, ainsi $p_n = p_N + \alpha_n$ converge simplement vers $P_N + \alpha$, donc $f = P_N + \alpha$ est une fonction polynomiale.*□

Attention on ne peut pas vraiment dire que (p_n) est une suite de Cauchy pour la convergence uniforme, en effet les p_n ne sont pas (sauf si ce sont des polynômes constants) des fonctions bornées. Par contre on peut bien dire que $p_n - f$ sera bien borné pour n assez grand, et par l'inégalité triangulaire que c'est le cas de $p_n - p_m$.

Références

[Ouv98]

Leçon concernée

- 249

1.41 *Quadrature de Gauss

Développement

Leçon concernée

- 236

Chapitre 2

Leçons

2.1 Algèbre

101 Groupe opérant sur un ensemble. Exemples et applications

- Loi de réciprocité quadratique
- Automorphismes de S_n
- Théorème de la base de BURNSIDE

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

- Polygones constructibles à la règle et au compas
- Théorème de KRONECKER

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

- Automorphismes de S_n
- Théorème de la base de BURNSIDE

104 Groupes finis. Exemples et applications

- Automorphismes de S_n
- Théorème de la base de BURNSIDE

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

- Automorphismes de S_n
- Table de S_4

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

- Sous-groupes compacts de $GL_n(\mathbb{R})$
- Théorème de Frobenius-Zolotarev

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

- Table de S_4
- Table de caractères et simplicité

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

- Automorphismes de S_n
- Théorème de la base de Burnside

109 Représentations de groupes finis de petit cardinal.

- Table de S_4
- Table de caractères et simplicité

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

- Théorème de Chevalley-Warning
- Théorème de Frobenius-Zolotarev

121 Nombres premiers. Applications.

- Loi de réciprocité quadratique
- Polygones constructibles à la règle et au compas
- Théorème de Frobenius-Zolotarev

122 Anneaux principaux. Exemples et applications.

Impasse

123 Corps finis. Applications.

- Dénombrement des polynômes irréductibles unitaires dans $\mathbb{F}_q$
- Théorème de Chevalley-Warning

124 Anneau des séries formelles. Applications

- Dénombrement d'une équation diophantienne
- Théorème de Joris

125 Extensions de corps. Exemples et applications

- Dénombrement des polynômes irréductibles unitaires dans $\mathbb{F}_q$
- Polygones constructibles à la règle et au compas

126 Exemples d'équations diophantiennes.

- Dénombrement d'une équation diophantienne
- Théorème de Chevalley-Warning

140 Corps des fractions rationnelles à une indéterminée sur un corps commutatifs. Applications.

Impasse

- Dénombrement d'une équation diophantienne

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

- Dénombrement des polynômes irréductibles unitaires dans $\mathbb{F}_q$
- Polygones constructibles à la règle et au compas

142 Algèbre des polynômes à plusieurs indéterminées. Applications.

- Théorème de Bézout
- Théorème de Chevalley-Warning

143 Résultant. Applications.

- Théorème de Bézout
- Théorème de Kronecker

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

- Continuité des racines d'une suite de polynômes
- Théorème de Kronecker

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

- Loi de réciprocité quadratique
- Sous-groupes compacts de $GL_n(\mathbb{R})$

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

- Sous-espaces de $C(\mathbb{R}, \mathbb{R})$ stables par translation
- Théorème de la base de BURNSIDE

152 Déterminant. Exemples et applications.

- Déterminant et conique
- Théorème de BÉZOUT
- Théorème de FROBENIUS-ZOLOTAREV

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

- Critère de nilpotence de CARTAN
- Décomposition effective de DUNFORD

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

- Table de S_4
- Sous-espaces de $C(\mathbb{R}, \mathbb{R})$ stables par translation

155 Endomorphismes diagonalisables en dimension finie.

- Décomposition effective de DUNFORD
- Exponentielle de matrice et diagonalisabilité

156 Exponentielle de matrices. Applications.

- Exponentielle de matrice et diagonalisabilité
- Théorème de LIAPOUNOV

157 Endomorphismes trigonalisables. Endomorphismes nilpotents.

- Critère de nilpotence de CARTAN
- Décomposition effective de DUNFORD

158 Matrices symétriques réelles, matrices hermitiennes.

- Ellipsoïde de JOHN
- Méthode de la relaxation

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

- Critère de nilpotence de Cartan
- Sous-espaces de $C(\mathbb{R},\mathbb{R})$ stables par translation
- Théorème des extrémas liés

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

- Simplicité $SO_n(\mathbb{R})$ pour n impair
- Sous-groupes compacts de $GL_n(\mathbb{R})$

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

- Ellipse de Steiner
- Table de S_4

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

- Déterminant et conique
- Méthode de la relaxation

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

- Loi de réciprocité quadratique
- Ellipsoïde de John

171 Formes quadratiques réelles. Exemples et applications

- Composantes connexes des formes quadratiques réelles
- Ellipsoïde de John

180 Coniques. Applications.

- Déterminant et conique
- Ellipse de Steiner

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

- Déterminant et conique
- Sous-groupes compacts de $GL_n(\mathbb{R})$

182 Applications des nombres complexes à la géométrie.

- Ellipse de Steiner
- Polygones constructibles à la règle et au compas
- Table de S_4

183 Utilisation des groupes en géométrie.

- Polygones constructibles à la règle et au compas
- Table de S_4

190 Méthodes combinatoires, problèmes de dénombrement.

- Dénombrement d'une équation diophantienne
- Dénombrement des polynômes irréductibles unitaires dans $\mathbb{F}_q$

2.2 Analyse

201 Espaces de fonctions : exemples et applications.

- Densité des polynômes dans $L^2(I, \omega d\lambda)$
- Théorème de Stone-Weierstrass

202 Exemples de parties denses et applications.

- Densité des polynômes dans $L^2(I, \omega d\lambda)$
- Théorème de Stone-Weierstrass

203 Utilisation de la notion de compacité.

- Continuité des racines d'une suite de polynômes
- Sous-groupes compacts de $GL_n(\mathbb{R})$
- Théorème de Stone-Weierstrass

204 Connexité. Exemples et applications.

- Composantes connexes des formes quadratiques réelles
- Simplicité $SO_n(\mathbb{R})$ pour n impair
- Théorème de Brouwer

205 Espaces complets. Exemples et applications.

- Théorème de Grothendieck
- Théorèmes de Weierstrass et d'Osgood

206 Théorèmes de point fixe. Exemples et applications.

- Sous-groupes compacts de $GL_n(\mathbb{R})$
- Théorème de Brouwer

207 Prolongement de fonctions. Exemples et applications.

- Densité des polynômes dans $L^2(I, \omega d\lambda)$
- Théorème de Joris

208 Espaces vectoriels normés, applications linéaires continues. Exemples.

- Méthode de la relaxation
- Théorème de Grothendieck

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

- Densité des polynômes dans $L^2(I, \omega d\lambda)$
- Théorème de Stone-Weierstrass

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

- Densité des polynômes dans $L^2(I, \omega d\lambda)$
- Théorème de Grothendieck

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

- Simplicité $SO_n(\mathbb{R})$ pour n impair
- Théorème de Brouwer

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

- Théorème de Brouwer
- Théorème des extrémas liés

216 Étude métrique des courbes. Exemples.

Impasse

217 Sous-variétés de $\mathbb{R}^n$. Exemples.

- Simplicité $SO_n(\mathbb{R})$ pour n impair
- Théorème des extrémas liés

218 Applications des formules de Taylor.

- Théorème de Joris
- Théorème des extrémas liés

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

- Méthode du gradient optimal
- Théorème des extrémas liés

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

- Nombre de zéros d'une équation différentielle linéaire du second ordre
- Théorème de LIAPOUNOV

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

- Nombre de zéros d'une équation différentielle linéaire du second ordre
- Sous-espaces de $C(\mathbb{R}, \mathbb{R})$ stables par translation
- Théorème de LIAPOUNOV

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

- Continuité des racines d'une suite de polynômes
- Processus de GALTON-WATSON

224 Exemples de développements asymptotiques de suites et de fonctions.

- Dénombrement d'une équation diophantienne
- Nombre de zéros d'une équation différentielle linéaire du second ordre

226 Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples et applications.

- Décomposition effective de DUNFORD
- Méthode du gradient optimal

228 Continuité et dérivabilité des fonctions réelle d'unue variable réelle. Exemple et contre-exemples.

- Sous-espaces de $C(\mathbb{R}, \mathbb{R})$ stables par translation
- Théorème de JORIS

229 Fonctions monotones. Fonctions convexes. Exemples et applications.

- Méthode du gradient optimal
- Processus de GALTON-WATSON

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

- Formule sommatoire de POISSON
- Marche aléatoire en dimension 1 et 2

232 Méthodes d'approximation des solutions d'une équation $F(X) = 0$. Exemples.

- Décomposition effective de Dunford
- Méthode de la relaxation

234 Espace L^p, $1 \leq p \leq +\infty$.

- Densité des polynômes dans $L^2(I, \omega d\lambda)$
- Théorème de Grothendieck

235 Suites et séries de fonctions intégrables. Exemples et applications.

- Marche aléatoire en dimension ≥ 3
- Théorèmes de Weierstrass et d'Osgood

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

- Inversion de Fourier
- Quadrature de Gauss

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

- Densité des polynômes dans $L^2(I, \omega d\lambda)$
- Théorème de Joris

240 Produit de convolution, transformation de Fourier. Applications.

- Densité des polynômes dans $L^2(I, \omega d\lambda)$
- Inversion de Fourier

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

- Formule sommatoire de Poisson
- Continuité des racines d'une suite de polynômes
- Théorèmes de Weierstrass et d'Osgood

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

- Dénombrement d'une équation diophantienne
- Processus de Galton-Watson

244 Fonctions développables en série entière, fonctions analytiques. Exemples.

- Dénombrement d'une équation diophantienne
- Processus de Galton-Watson

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

- Densité des polynômes dans $L^2(I, \omega d\lambda)$
- Théorèmes de Weierstrass et d'Osgood

246 Séries de Fourier. Exemples et applications.

- Formule sommatoire de Poisson
- Théorème de Stone-Weierstrass

247 Exemples de problèmes d'interversion de limites.

- Marche aléatoire en dimension ≥ 3
- Théorèmes de Weierstrass et d'Osgood

249 Suites de variables de Bernoulli indépendantes.

- Marche aléatoire en dimension 1 et 2
- Polynômes de Bernstein

253 Utilisation de la notion de convexité en analyse

- Méthode du gradient optimal
- Processus de Galton-Watson
- Théorème de Brouwer

254 Espace de Schwartz $S(\mathbb{R}^d)$ et distributions tempérées. Transformation de Fourier dans $S(\mathbb{R}^d)$ et $S'(\mathbb{R}^d)$.

- Formule sommatoire de Poisson
- Inversion de Fourier

255 Espaces de Schwartz. Distributions. Dérivation au sens des distributions.

- Formule sommatoire de Poisson
- Inversion de Fourier

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

- Marche aléatoire en dimension ≥ 3
- Processus de Galton-Watson

261 Fonctions caractéristique et transformée de Laplace d'une variable aléatoire. Exemples et applications.

- Marche aléatoire en dimension ≥ 3
- Processus de Galton-Watson

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

Impasse

263 Variables aléatoires à densité. Exemples et applications.

Impasse

264 Variables aléatoires discrètes. Exemples et applications.

- Marche aléatoire en dimension 1 et 2
- Processus de Galton-Watson