Introduction

Voici les développements qui m'ont accompagné durant mon année de préparation à l'agrégation. Ils sont plus ou moins longs, et plus ou moins difficiles : la classification dépend évidemment de vos goûts.
Certains développements peuvent contenir des erreurs, ou des raisonnements trop rapides ; vous pouvez me le signaler par e-mail.

Bonne lecture, et bonne préparation !

Table des matières

1 Algèbre & Géométrie

1.1 Moyen & semi-classique : groupe d'isométrie du tétraèdre, table de $\mathfrak{S}_4$

(haut)

Référence : AD, Livre sur $\mathfrak{S}_4$, Szpirglas (Algèbre L3) pour le type des isométries, à compléter éventuellement avec H2G2.

Recasages : 101, 105, 108, 160, 161.

Énoncé : On montre que le groupe d'isométries du tétraèdre régulier est isomorphe à $\mathfrak{S}_4$; on en déduit la table de caractères de ce groupe.

Preuve : On commence par faire un **dessin** du tétraèdre, et on appelle A, B, C et D ses sommets. Soit G le groupe des isométries fixant le tétraèdre. G est constitué d'applications affines, donc tout $g \in G$ envoie les points extremaux de T sur ceux de $g(T) = T$: autrement dit, on a par restriction une action de G sur $\{A, B, C, D\}$. Cette action est fidèle, car comme les quatre sommets ne sont pas coplanaires, ils forment un repère affine. Ainsi, on a un morphisme injectif $\phi : G \to \mathfrak{S}_4$. On montre que ϕ est surjectif : pour cela, on montre que $\mathrm{Im}(\phi)$ contient les transpositions. Par symétrie en les lettres, il suffit de montrer qu'il existe $s \in G$ fixant C et D, et envoyant A sur B et inversement. Soit $\mathscr{P}$ le plan contenant C, D et M le milieu de $[AB]$. Alors, comme les médianes d'un triangle équilatéral sont ses hauteurs, le vecteur $\overrightarrow{AB}$ est orthogonal à $\overrightarrow{CM}$ et à $\overrightarrow{DM}$. Comme $(M, \overrightarrow{CM}, \overrightarrow{DM})$ est un repère cartésien de P, on en déduit que $\overrightarrow{AB} \perp \mathscr{P}$. Comme M est le mileu de $[AB]$, on en déduit que la réflexion orthogonale $s_{\mathscr{P}}$ de plan $\mathscr{P}$ est une isométrie de G qui convient. Conclusion : $G \simeq \mathfrak{S}_4$.

On note O le barycentre du tétraèdre. De ce qui précède, on déduit, en considérant la suite suivante (où la deuxième flèche est obtenue en vectorialisant suivant le repère : $(O, \overrightarrow{OA}, \overrightarrow{OB}, \overrightarrow{OC})$) :

$$\mathfrak{S}_4 \longrightarrow G \longrightarrow \mathrm{GL}(3, \mathbf{R}) \longrightarrow \mathrm{GL}(3, \mathbf{C})$$

un morphisme $\rho : \mathfrak{S}_4 \longrightarrow \mathrm{GL}(3, \mathbf{C})$. Autrement dit, on a une représentation de $\mathfrak{S}_4$, dont on note $\theta = \mathrm{Tr}(\rho)$ le caractère.
Déterminons les valeurs que prend θ sur les différentes classes de conjugaison : on les connaît bien grâce aux partitions de 4 (à ce moment, il faut écrire les colonnes de la table de caractères). On a donc $\theta(id) = 3$, et, par ce qui précède, $\theta((12)) = \mathrm{Tr}(s_{\mathscr{P}}) = 1$ (car toute symétrie vectorielle est semblable à $diag(1, 1, -1)$). De plus, l'image de (123) dans G est une rotation d'axe (OD) d'angle $\pm\frac{2\pi}{3}$: ainsi, sa trace est $\theta((123)) = 1+2\cos(\frac{2\pi}{3}) = 0$. Enfin, on a, en utilisant l'égalité $\overrightarrow{OA}+\overrightarrow{OB}+\overrightarrow{OC}+\overrightarrow{OD} = \vec{0}$:

$$\rho((12)(34)) = \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix} \text{ et } \rho((1234)) = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}$$

Donc : $\theta((12)(34)) = \theta((1234)) = 0$.

L'étude précédente nous a donné trois caractères irréductibles non triviaux : en effet, on a un caractère de degré 1 non trivial donné par $\varepsilon = \det \circ \rho$ (il est non trivial car $\varepsilon((12)) = -1$ car une réflexion de l'espace est indirecte). L'autre est donné par θ : en effet, on a :

$$\sum_{g \in \mathfrak{S}_4} |\theta(g)|^2 = 1 \times |3|^2 + 6 \times 1^2 + \ldots = 24 = |\mathfrak{S}_4|$$

Le troisième caractère est donné par la torsion de θ par ε, notée $\theta \otimes \varepsilon$. Enfin, pour compléter la table, on utilise le fait que le dernier caractère irréductible doit vérifier : $\eta(1)^2 + 3^2 + 3^2 + 1^2 + 1^2 = 24$ et $\sum_\chi \chi(1)\chi(g) = 0$ pour $g \neq id$ (ces deux identités proviennent de la décomposition de la régulière).

	1 id	6 (12)	3 (12)(34)	8 (123)	6 (1234)
1	1	1	1	1	1
ε	1	-1	1	1	-1
θ	3	1	-1	0	1
$\theta \otimes \varepsilon$	3	1	-1	0	-1
η	2	0	2	-1	0

1.2 Moyen & original : autour de sous-groupes finis de $\mathbf{GL}_n(\mathbf{Z})$

Référence : (Arnaudies Bertin T2 ?) Recasages : 102, 104, 106, 153, 191.

Remarque : Il y a ici deux développements possibles, un a) et un b). On peut rajouter l'intro (0) pour parler de réseaux (par ex dans la 191)

Énoncé : 0) Réseaux On appelle réseau un sous-groupe de $\mathbf{R}^n$ de la forme $\mathscr{R} = \oplus Z e_i$, où (e_i) est une base de $\mathbf{R}^n$. On définit :

$$G = \text{Isom}(\mathscr{R}) = \{g \in \mathcal{O}_n(\mathbf{R}), g(\mathscr{R}) = \mathscr{R}\}$$

On montre que l'application $g \in G \mapsto \text{Mat}_{(e_i)}(g) \in \text{GL}_n(\mathbf{Z})$ est bien définie : en effet, si $g \in G$, alors $g(\mathscr{R}) \subset \mathscr{R}$ donc les colonnes de $\text{Mat}_{(e_i)}(g)$ sont entières, et $\text{Mat}_{(e_i)}(g) \in \mathcal{M}_n(\mathbf{Z})$; de plus, comme $g^{-1} \in G$, on a aussi : $\text{Mat}_{(e_i)}(g^{-1}) = \text{Mat}_{(e_i)}(g)^{-1} \in \mathcal{M}_n(\mathbf{Z})$, ce qui conclut.
On montre que G est fini : en effet, soit β la forme quadratique sur $\mathbf{R}^n$ telle que (e_i) soit orthonormée pour β. Alors $q(x) = \beta(x,x)$ est une fq définie positive, donc elle induit une norme N. Par équivalence des normes sur $\mathbf{R}^n$, on dispose de $C > 0$ tel que :

$$\forall x = x_1e_1 + \ldots + x_ne_n \in \mathbf{R}^n, N(x) \leq C\|x\|_2$$

Soit $M = \sup_i \|e_i\|_2$. Alors, si $g \in G$, l'image de e_1 est de norme $\|ge_1\|_2 = \|e_1\|_2 \leq M$. Ainsi, ge_1 est à coordonnées entières bornées par C : il n'y a donc qu'un nombre fini de choix pour ge_1 ; de même, pour tout i, il n'y a qu'un nombre fini de choix pour ge_i : ainsi, G est fini.
Dès lors, G est fini et s'identifie à un sous-groupe de $\text{GL}_n(\mathbf{Z})$.

a) Lemme de Serre etc Soit G un sous-groupe fini de $\text{GL}_n(\mathbf{Z})$, et p un entier ≥ 3. Alors le morphisme

$$G \to \text{GL}_n(\mathbf{Z}/p\mathbf{Z})$$

est injectif. Corollaire, le cardinal de G divise $(3^n - 1) \ldots (3^n - 3^{n-1})$. On montre que $\text{GL}_2(\mathbf{F}_3)$ n'est pas (isomorphe à) un sous-groupe de $\text{GL}_2(\mathbf{Z})$.

b) Sous-groupes finis de $\mathbf{GL}_2(\mathbf{Z})$ Les sous-groupes finis de $\text{GL}_2(\mathbf{R})$ sont cycliques ou diédraux. Les sous-groupes finis de $\text{GL}_2(\mathbf{Z})$ sont cycliques d'ordre $1, 2, 3, 4, 6$ ou bien diédraux d'ordre $4, 6, 8$ ou 12.

Preuve :

a) Soit G un tel groupe fini, soit π le morphisme de réduction modulo p. Soit $M \in G$ tel que $\pi(M) = I_n$. Alors on dispose de $M' \in \mathcal{M}_n(\mathbf{Z})$ telle que $M = I_n + pM'$. On a alors :

$$\chi_M = \det(XI_n - (I_n + pM')) = p^n \chi_{M'}\left(\frac{X-1}{p}\right)$$

Autrement dit, on a, notant $\chi_M = P$ et $\chi_{M'} = Q$, alors :

$$P(X) = p^n Q\left(\frac{X-1}{p}\right)$$

Et comme M est d'ordre fini, elle est diagonalisable (dans $\mathbf{C}$) à valeurs propres dans $\mathbf{U}$; donc P est scindé à racines dans $\mathbf{U}$.

On montre par récurrence sur n le prédicat : "$\forall Q \in \mathbf{Z}[X], \forall P \in \mathbf{Z}[X]$ unitaire et à racines de module 1

$$\text{l'égalité } P(X) = p^n Q\left(\frac{X-1}{p}\right) \text{ implique } P = (X-1)^n\text{"}$$

C'est trivial pour $n = 0$. Supposons avoir une telle relation en degré n. Alors : $P(1) = p^n Q(0)$. Or :

$$|P(1)| = \prod_\lambda |1-\lambda| \leq \prod_\lambda 2 < p^n$$

donc forcément, comme $Q(0) \in \mathbf{Z}$, on a : $P(1) = Q(0) = 0$. Ainsi, on peut écrire $P(X) = (X-1)\widetilde{P}(X)$, $Q(X) = X\widetilde{Q}(X)$, et alors $\widetilde{P}, \widetilde{Q}$ satisfont le prédicat en degré $n-1$ (ils sont à coeffs entiers car X et $X-1$ sont unitaires, et la d.e. est alors ok dans $\mathbf{Z}$). Par récurrence, $Q = X^n$ et $P = (X-1)^n$; comme M est diagonalisable, cela donne directement $M = I_n$. Donc $\pi\Big|_G$ est injective.
Pour le corollaire : G s'identifie à un ss-g de $\mathrm{GL}_n(\mathbf{F}_3)$, d'où la divisibilité des cardinaux par le théorème de Lagrange.
Montrons que $\mathrm{GL}_2(\mathbf{Z})$ ne contient pas de sous-groupe isomorphe à $\mathrm{GL}_2(\mathbf{F}_3)$. Soit G un sous-groupe fini de $\mathrm{GL}_2(\mathbf{Z})$. On montre que G ne contient pas d'élément d'ordre 8, à la différence de $\mathrm{GL}_2(\mathbf{F}_3)$.
Soit $M \in G$, on sait que M est d'ordre fini, donc diagonalisable sur $\mathbf{C}$. On peut donc écrire, pour des racines de l'unité λ_i :

$$M \simeq \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

Comme le spectre est stable par conjugaison, on a la distinction de cas suivante :

- Si λ_1 est non réel, alors $\lambda_2 = \overline{\lambda_1}$, et, en notant θ un argument de λ_1, on a alors : $2\cos(\theta) = \mathrm{Tr}(M) \in \mathbf{Z}$. En particulier, on a $\cos(\theta) \in \{\pm 1, \pm\frac{1}{2}, 0\}$ et λ est donc un point de l'hexagone régulier ou de $\{\pm i\}$. Donc $M^6 = I_2$ ou $M^4 = I_2$. En particulier, l'ordre n'est pas 8.
- Si λ_1 est réel, alors c'est une racine de l'unité, donc $\lambda_1 = \pm 1$. De même, λ_2 est réel (par l'absurde) et donc $\lambda_2 = \pm 1$; on en déduit que M est d'ordre 1 ou 2.

Exhibons un élément d'ordre 8 dans $\mathrm{GL}_2(\mathbf{F}_3)$. On a la factorisation suivante, dans $\mathbf{F}_3$:

$$\Phi_8 = X^4 + 1 = (X^2 + X - 1)(X^2 - X - 1)$$

Soit M la matrice compagnon du polynôme $X^2 - X - 1$. Alors on a $\Phi_8(M) = 0$, donc $M^4 = -I_2$; donc M est d'ordre 8.

b) Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbf{R})$. Soit $\langle \cdot, \cdot \rangle$ un produit scalaire sur $\mathbf{R}^n$. Alors $(x, y) = \frac{1}{|G|} \sum_{g \in G} \langle gx, gy \rangle$ est un produit scalaire sur $\mathbf{R}^n$, par convexité des produits scalaires (ou simplement : en vérifiant).
De plus, il est G-invariant : en effet, si $h \in G$, $g \mapsto gh$ est une bijection de G, donc sommer sur g revient à sommer sur gh. Ainsi, via une matrice qui envoie, par congruence, la matrice de $(\cdot, \cdot)$ sur l'identité, G est conjugué à un sous-groupe de $\mathcal{O}_n(\mathbf{R})$. On est donc ramené à déterminer les sous-groupes finis de $\mathcal{O}_n(\mathbf{R})$.

Soit G un sous-groupe fini de $\mathcal{O}_2(\mathbf{R})$. On distingue deux cas :

- Si $G \subset SO_2(\mathbf{R})$, alors G est un sous-groupe fini de $\mathbb{S}^1 \simeq \mathbf{R}/\mathbf{Z}$. Donc, en utilisant la caractérisation des sous-groupes de $\mathbf{R}$, G est cyclique.

- Si $G \not\subset SO_2(\mathbf{R})$, alors G contient une symétrie s. De plus, comme $G^+ = G \cap SO_2(\mathbf{R})$ est d'indice 2 dans G, $G = \langle s, G^+ \rangle$. On montre que G est le groupe d'isométrie d'un n-gone, où n est le cardinal de G^+. Soit M un point de l'axe de S d'affixe non nulle, soit $\mathcal{P}$ le polygone formé des $r^k(M)$, pour $k \in \mathbf{Z}/n\mathbf{Z}$ **(faire des dessins)**. Alors on montre que G est le sous-groupe d'isométries de $\mathcal{P}$, ce qui montrera l'isomorphisme $G \simeq \mathcal{D}_n$. Par cardinalité, il suffit de montrer que G fixe le polygone : or cela est évident, car

$$sr^k(M) = sr^k s^{-1}(M) = r^{-k}(M) \in \mathcal{P}$$

Donc G est cyclique ou diédral.
Pour l'application aux sous-groupes finis de $\mathrm{GL}_2(\mathbf{Z})$, on sait qu'ils seront cycliques ou diédraux. Si G est cyclique, en regardant $G \cup sG$, pour une symétrie $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z})$, on aura un groupe diédral. Donc pour classifier, il suffit de trouver les groupes cycliques, et donc, les ordres possibles.
Soit $M \in G$, on sait que M est d'ordre fini, donc diagonalisable sur $\mathbf{C}$. On peut donc écrire, pour des racines de l'unité λ_i :

$$M \simeq \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

Comme le spectre est stable par conjugaison, on a la distinction de cas suivante :

- Si λ_1 est non réel, alors $\lambda_2 = \overline{\lambda_1}$, et, en notant θ un argument de λ_1, on a alors : $2\cos(\theta) = \mathrm{Tr}(M) \in \mathbf{Z}$. En particulier, on a $\cos(\theta) \in \{\pm 1, \pm\frac{1}{2}, 0\}$ et λ est donc un point de l'hexagone régulier ou de $\{\pm i\}$. Donc $M^6 = I_2$ ou $M^4 = I_2$.
- Si λ_1 est réel, alors c'est une racine de l'unité, donc $\lambda_1 = \pm 1$. De même, λ_2 est réel (par l'absurde) et donc $\lambda_2 = \pm 1$; on en déduit que M est d'ordre 1 ou 2.

Donc l'ordre d'un élément peut être $1, 2, 3, 4$ ou 6. De plus, il y a des égalités pour chacun : $I_2, -I_2, C_{\Phi_3}, C_{\Phi_4}$ et C_{Φ_6} (on vérifie qu'ils sont chacun dans SO_2).
Finalement, les sous-groupes de $\mathrm{GL}_2(\mathbf{Z})$ sont exactement les groupes cycliques d'ordre $1, 2, 3, 4, 6$ et les groupes diédraux $\mathcal{D}_2, \mathcal{D}_3, \mathcal{D}_4, \mathcal{D}_6$.

1.3 Moyen+ & "original" : calcul algébrique de la somme quadratique de Gauss

(haut) Recasages : 102, 151, 154, 155 Référence : Peyré (pour un calcul propre du déterminant).

Énoncé : On calcule, pour n impair

$$\tau_n = \sum_{x \in \mathbf{Z}/n\mathbf{Z}} \zeta^{x^2}$$

(où $\zeta = \exp(\frac{2i\pi}{n})$) On trouve :

$$\tau_n = \begin{cases} \sqrt{n} & \text{si } n \equiv 1 \pmod 4 \\ i\sqrt{n} & \text{si } n \equiv 3 \pmod 4 \end{cases}$$

Pour cela, on étudie la trace de l'opérateur de TF sur le groupe additif $\mathbf{Z}/n\mathbf{Z}$.

Remarques : Voir dev analyse.

Preuve : Soit E le $\mathbf{C}$-espace vectoriel constitué des fonctions $\mathbf{Z}/n\mathbf{Z} \to \mathbf{C}$. On a un endomorphisme $\varphi : E \to E$ de transformée de Fourier : pour $f \in E$, $\varphi(f)$ est définie par la formule suivante pour $y \in \mathbf{Z}/n\mathbf{Z}$:

$$\varphi(f)(y) = \sum_{x \in \mathbf{Z}/n\mathbf{Z}} f(x)\zeta^{xy}$$

Si l'on considère la base B formée des fonctions indicatrices des singletons, on a :

$$\mathrm{Mat}_{B,B}(\varphi) = (\zeta^{(k-1)(l-1)})_{1 \leq k,l \leq n}$$

Ainsi, on a $\tau_n = \mathrm{Tr}(\varphi)$, et on cherche à calculer cette trace.
On a la propriété suivante des caractères ($u \in \mathbf{Z}/n\mathbf{Z}$) :

$$\sum_{y \in \mathbf{Z}/n\mathbf{Z}} \zeta^{ux} = n\delta_{u,0}$$

Cela permet de démontrer (en utilisant l'imparité de n) :

$$\varphi \circ \varphi(f)(z) = nf(-z)$$

Ainsi, φ est annulé par le polynôme $X^4 - n^2$: ce polynôme étant scindé à racines simples, φ est diagonalisable, et ses valeurs propres sont dans $\{\pm\sqrt{n}, \pm i\sqrt{n}\}$; notant a, b, c et d les multiplicités de $\sqrt{n}$, $-\sqrt{n}$, $i\sqrt{n}$ et $-i\sqrt{n}$, on a :

$$\tau_n = (a-b)\sqrt{n} + (c-d)i\sqrt{n}$$

On trouve alors quatre équations pour trouver a, b, c et d. On a d'abord, par dimensions :

$$a + b + c + d = n \qquad (1)$$

De plus, l'espace propre $\ker(\varphi^2 - nid)$ est exactement de dimension $a+b$; or, par la formule montrée précédemment, cet espace propre est exactement l'espace des fonctions paires. Comme n est impair, on a donc :

$$a + b = \frac{n+1}{2} \qquad (2)$$

On peut ensuite calculer le module de τ_n. On a : $|\tau_n|^2 = n((a-b)^2 + (c-d)^2)$. Mais on a aussi :

$$\begin{aligned}
|\tau_n|^2 &= \sum_{x \in \mathbf{Z}/n\mathbf{Z}} \sum_{y \in \mathbf{Z}/n\mathbf{Z}} \zeta^{x^2-y^2} \\
&= \sum_{u \in \mathbf{Z}/n\mathbf{Z}} \sum_{v \in \mathbf{Z}/n\mathbf{Z}} \zeta^{uv} \\
&= n
\end{aligned}$$

où le passage de la première à la deuxième ligne est fait en posant $u = x+y$ et $v = x-y$, ce qui est bijectif car 2 est inversible modulo n (qui est impair), et l'égalité finale est un argument de caractère. On a donc l'équation suivante :

$$(a-b)^2 + (c-d)^2 = 1 \qquad (3)$$

L'équation qui nous manque va être donnée en calculant le déterminant de φ de deux façons. D'abord, en utilisant une base de diagonalisation, on a : $\det(\varphi) = \sqrt{n}^{a+b+c+d} i^{c-d}(-1)^b$. Mais on peut aussi calculer le déterminant de φ, car celui-ci est de Vandermonde. Soit $\mu = e^{\frac{i\pi}{n}}$, de sorte que $\mu^2 = \zeta$. On a alors :

$$\begin{aligned}
\det(\varphi) &= \prod_{0 \le l < k \le n-1} (\zeta^k - \zeta^l) \\
&= \prod_{0 \le l < k \le n-1} \mu^{k+l}(\mu^{k-l} - \mu^{l-k}) \\
&= \prod_{0 \le l < k \le n-1} \left(\mu^{k+l} 2i \sin\left(\frac{(k-l)\pi}{n}\right)\right)
\end{aligned}$$

En particulier, en considérant l'argument de $\det(\varphi)$ (dans $\mathbf{R}/2\pi\mathbf{Z}$), on a :

$$\begin{aligned}
\arg(\det(\varphi)) &= \sum_{0 \le l < k \le n-1} \left((k+l)\frac{\pi}{n} + \frac{\pi}{2}\right) \\
&= \sum_{1 \le k \le n-1} \left(\left(k^2 + \frac{k(k-1)}{2}\right)\frac{\pi}{n} + \frac{\pi k}{2}\right) \\
&= \frac{\pi}{n}\frac{3}{2}\frac{n(n-1)(2n-1)}{6} - \frac{\pi}{n}\frac{(n-1)n}{4} + \frac{\pi}{4}(n-1)n \\
&= \frac{\pi}{4}(n-1)(3n-2)
\end{aligned}$$

Pour terminer, on raisonne modulo 8 : si $n \equiv 1 \pmod 8$, alors l'argument vaut 0, et donc, par la contrainte de l'équation (3), $c = d$, puis b est pair, et $|a-b| = 1$. Or $2\max(a,b) = a+b+|a-b|$, ce qui prouve, en utilisant l'équation (2) : $\{a,b\} = \{\frac{n+3}{4}, \frac{n-1}{4}\}$. Par parité, $b = c = d = \frac{n-1}{4}$ et $a = \frac{n+3}{4}$. Si $n \equiv 5 \pmod 8$, on remplace pair par impair, et 0 par π, la conclusion reste la même ; on fait de même pour $n \equiv 3$ et $7 \pmod 8$. Ainsi, on trouve bien le résultat.

1.4 Difficile & original : théorème d'Iwasawa

Réf : NH2G2, tome 1 p39. Recasages : 101, 103.

Énoncé : Soit G agissant sur X (de cardinal au moins 2) **fidèlement et doublement transitivement** (i.e. : l'action de G sur $X \times X$ a deux orbites : la diagonale et le reste). On suppose

- G est engendré par ses commutateurs ;
- pour un $x \in X$, le stabilisateur G_x contient K abélien distingué dans G_x tel que $\{gkg^{-1}, g \in G, k \in K\}$ engendre G.

Alors G est simple.
Application : $\mathrm{PSL}_2(\mathbf{K})$ est simple si $\mathbf{K}$ est de card ≥ 4, $\mathfrak{A}_5$ est simple.

Preuve : Voici un résumé de la preuve :

- lemme 1 : on montre que si un groupe est distingué, il agit transitivement ou trivialement.
- lemme 2 : on montre que G_x est maximal.
- On prend K' distingué dans G non trivial ; on montre que $K'G_x = G$.
- On montre que $K'K$ est distingué dans G, et qu'il est égal à G.
- On montre que G/K' est abélien, puis trivial.

On commence par deux petits lemmes : soit G agissant sur X doublement transitivement, avec X ayant au moins deux éléments.

Lemme 1 : Si K est distingué dans G, alors il agit soit trivialement, soit transitivement.
En effet, s'il existe $k \in K$ et $x \in X$ tel que $k \cdot x \neq x$, alors si $y \in X$ est distinct de x, on dispose de $g \in G$ tel que $g \cdot (x, k \cdot x) = (x, y)$. Alors $gkg^{-1} \cdot x = y$.

Lemme 2 : Si $x \in X$, G_x est un sous-groupe maximal, et même : si $g \notin G_x$, $G = G_x \cup G_x g G_x$.
En effet, si $h \notin G_x$, on dispose de $g_1 \in G_x$ envoyant $g \cdot x$ sur $h \cdot x$. Alors $g^{-1} g_1^{-1} h \cdot x = x$, donc on dispose de $g_2 \in G_x$ tel que $h = g_1 g g_2 \in G_x g G_x$.

On se place à présent dans les hypothèses du th d'Iwasawa. Soit $K' < G$ un sous-groupe distingué non réduit à 1.

D'abord, par le lemme 2, on a $K'G_x = G_x$ ou G ($K'G_x$ étant un groupe car K' est distingué dans G). Si $K' \subset G_x$, alors K' ne peut agir transitivement : par le lemme 1, il agit trivialement. Par fidélité de l'action, K' est trivial, absurde. Ainsi, $K'G_x = G$.

Ensuite, on montre que $K'K$ est distingué dans $K'G_x = G$. Pour cela, comme $K'K$ est un groupe (car K' est distingué dans G), il suffit de montrer que si $k' \in K'$, $k \in K$, $k_1 \in K'$, $g_1 \in G_x$, le produit $(k_1 g_1)(k'k)(k_1 g_1)^{-1}$ est produit d'élements de K' et K. On a en effet :

$$(k_1 g_1)(k'k)(k_1 g_1)^{-1} = \underbrace{k_1 g_1 k' g_1^{-1} k_1^{-1}}_{\in K'} \underbrace{k_1}_{\in K'} \underbrace{g_1 k g_1^{-1}}_{\in K} \underbrace{k_1^{-1}}_{\in K'} \in K'K$$

Ainsi, $K'K$ contient le groupe engendré par les gkg^{-1}, avec $g \in G$ et $k \in K$: donc $K'K = G$.

Ainsi, $G/K' = K'K/K' \simeq K/(K \cap K')$ (l'iso est donné par la projection $K \to K'K/K'$ canonique). Donc G/K' est abélien ; or il est engendré par les commutateurs, car c'est le cas de G (par hypothèse). Ainsi, G/K' est trivial, donc $K' = G$, ce qui conclut.

Application 1 : Pour le premier exemple, on fait agir $\mathrm{PSL}_2(\mathbf{K})$ sur $\mathbf{P}^1(\mathbf{K})$. L'action est fidèle (non trivial !). On utilise le fait que si pour tout x, x et $u(x)$ sont sur une même droite, alors u est une homothétie). On montre facilement que l'action est doublement transitive (celle de PGL_2 est doublement transitive, on fait juste une dilatation). On prend pour K les classes des $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, $a \in \mathbf{K}$, et x la droite engendrée par le premier vecteur de la base canonique. On a alors $K = G_x$ donc K est distingué dans G_x. On montre que $H := \langle gkg^{-1} \mid g \in G, k \in G \rangle$ est égal à G. Déjà, H contient les unipotentes inférieures (conjuguer par une matrice de permutation). Ensuite, on sait que $\mathrm{SL}_2(\mathbf{K})$ est engendré par les matrices de transvections (c'est le pivot de Gauss) donc $H = G$ (sinon, cf les calculs à la fin).
De plus, on a :

$$\left[\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & b(a^2-1) \\ 0 & 1 \end{pmatrix}$$

Ainsi, le groupe dérivé contient H (prendre $a \notin \{0, 1, -1\}$, et $b = c \times (a^2-1)^{-1}$: c'est ici qu'on utilise l'hypothèse $\mathbf{K} \neq \mathbf{F}_2, \mathbf{F}_3$). Comme il est distingué, par ce qui précède, le groupe dérivé est G. On peut donc appliquer le théorème d'Iwasawa : $\mathrm{PSL}_2(\mathbf{K})$ est simple.

Application 2 : On fait agir $G = \mathfrak{A}_5$ sur $X = [\![1, 5]\!]$. On prend $x = 5$ et $K = V_4$ (le groupe de Klein, inclus dans $\mathfrak{A}_4$, le stabilisateur de x). L'action est doublement transitive (facile). Le groupe est engendré par ses commutateurs (car les 3-cycles sont des commutateurs). De plus, le groupe K engendre, via conjugaison par G, tout G, et ce car G est engendré par les doubles transpositions.

$$\begin{pmatrix} 1 & 0 \\ \frac{d-1}{b} & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \frac{a-1}{b} & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad (b \neq 0)$$

$$\begin{pmatrix} 1 & 0 \\ \frac{1-a}{a} & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a^{-1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

1.5 Moyen & original : Sous-groupe de Frattini, cardinal des familles génératrices d'un p-groupe

Référence : Serre, groupes finis, Debreil, groupes finis et treillis de leurs sous-g et Zavidovique Recasages : 104, 108, 121

Énoncé : Soit G un groupe fini, on définit le sous-groupe de Frattini, et on montre que si G est un p-groupe, alors toutes les parties génératrices ont, quitte à enlever des éléments superflus, le même cardinal.

Preuve : Le sous-groupe de Frattini de G est :

$$\Phi_G = \bigcap_{M \text{ maximal}} M$$

où un sous-groupe M est dit maximal si, pour tout sous-groupe N de G, $M \subset N \subset G$ implique $N = M$ ou G. On peut remarquer que, comme l'ensemble des sous-groupes maximaux de G est stable sous $Aut(G)$, le sous-groupe de Frattini est caractéristique, et donc distingué.
Si S est une partie de G, et $H = \langle S \rangle$ est le sous-groupe engendré par S, alors on a $H = G \iff H\Phi_G = G$. En effet, si H est distinct de G, alors il est inclus dans un sous-groupe maximal, dans lequel est aussi inclus $H\Phi_G$. En particulier, S engendre G ssi son image dans G/Φ_G l'engendre.

À présent, on suppose que G est un p-groupe. On montre que G/Φ_G a une structure de $\mathbf{F}_p$-espace vectoriel.

On commence par montrer que tout sous-groupe de G d'indice p est distingué dans G : si M est un tel sous-groupe, alors M est le noyau du morphisme $G \to \mathfrak{S}_{G/M}$ induit : pour cela, on regarde le cardinal.

Puis, on montre que les sous-groupes maximaux de G sont d'indice p. Pour cela, on raisonne par récurrence sur le cardinal (ou plutôt sa valuation p-adique) de G : si $M \subset G$ est maximal, on distingue deux cas :

- si M contient $Z(G)$, alors $M/Z(G)$ est un sous-groupe maximal de $G/Z(G)$, ce qui conclut.
- Sinon, on dispose de $x \in Z(G)$ pas dans M. Son ordre divise le cardinal du groupe : c'est une puissance de p. Alors $G = \langle M, x \rangle$ par maximalité ; on en déduit, en regardant $\langle M, x^p \rangle$ que l'ordre de x est exactement p. Alors $\langle M, x \rangle \simeq M \times C_p$ par construction.

Ainsi, on a une injection **de groupes** (par les deux lemmes d'avant) :

$$G/\Phi_G \longrightarrow \prod_{M \text{ maximal}} G/M$$

Comme le deuxième est abélien et $p.x = 0$ pour tout x dans le deuxième, on en déduit que G/Φ_G est abélien et muni d'une structure de $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$-espace vectoriel.
Ainsi, si S engendre G, quitte à retirer des éléments de S pour que l'image de $S \to G/\Phi_G$ soit une base de G/Φ_G, S a exactement $\dim_{\mathbf{F}_p}(G/\Phi_G)$ éléments.

Remarque : Le théorème n'est pas vrai pour un groupe n'étant pas un p-groupe. Par exemple, $\mathfrak{S}_4$ est engendré par $S = \{(1234), (12)\}$ et par $S' = \{(12), (23), (34)\}$ mais on ne peut enlever d'éléments à S'. De même, $\mathbf{Z}$ est engendré par $\{1\}$ et par $\{2, 3\}$.
Cette propriété ne caractérise pas les p-groupes, car pour p premier, le groupe diédral $\mathcal{D}_p$ la vérifie.

1.6 Moyen & original : Théorème de Lie-Kolchin

Réf : NH2G2 I (p238) Recasages : 106, 154, 156.

Énoncé : Tout groupe connexe et résoluble de $\mathrm{GL}_n(\mathbf{C})$ est simultanément trigonalisable.

On rappelle qu'un groupe G est dit résoluble si la suite $(D^n(G))$ des groupes dérivés stationne au groupe trivial. (attention, le critère de la résolution par des groupes dont les quotients successifs sont abéliens *cycliques* ne fonctionne pas ici car le groupe est infini (mais celle par des groupes dont les quotients sont abéliens si)).

Preuve : Soit G un tel groupe. On a donc, pour un certain $\ell \geq 1$: $D^\ell(G) = 1$ et $D^{\ell-1}(G) \neq 1$. Alors :

1. Si G est un groupe topologique connexe, alors $D(G)$ est caractéristique et connexe. (**on peut admettre cette étape**)
2. $A = D^{\ell-1}(G)$ est abélien non trivial, et donc : $V = \{$vecteurs propres communs aux éléments de $A\}$ est non vide.
3. Pour $v \in V$ et $a \in A$, on note $\chi_v(a)$ le scalaire tel que $av = \chi_v(a)v$. Alors on montre que V est G-stable et : $\forall g \in G, a \in A, \chi_{g(v)}(a) = \chi_v(g^{-1}ag)$. On en déduit que χ_v est constant sur A, et est préservé sous l'action de G : $\chi_v = \chi_{g(v)}$.
4. On regarde le sous-espace engendré par les $g(v)$, puis on récurre (sur n, et pas sur ℓ...).

Voici une preuve des différents points :

1. On sait que $D(G)$ est stable sous $Aut(G)$ (car $Aut(G)$ envoie une partie génératrice (les commutateurs) sur elle-même) ; de plus, si X est l'ensemble des commutateurs de G, X est l'image continue du connexe $G \times G$, donc X est connexe, et donc $D(G) = \cup_{n\in\mathbf{Z}} X^n$ est connexe par union avec un élément commun (X^n est le produit de n éléments (ou inverses d'éléments si $n < 0$) de X).

2. Par hypothèse, $A \neq 1$ et $D(A) = 1$, donc A est abélien non trivial. On montre que les éléments de A ont un vecteur propre commun (en fait, cela est vrai même si A n'est pas forcément un groupe). Déjà, c'est vrai si A n'est constitué que d'homothéties. Ensuite, si A a un élément qui n'est pas une homothétie, alors il admet une valeur propre (on est sur $\mathbf{C}$, un corps algébriquement clos), et un espace propre associé non trivial E_λ. Alors A stabilise E_λ : on travaille sur E_λ. Ainsi, par récurrence sur la dimension de l'espace, A admet bien un vecteur propre commun.

3. On veut avoir $gv \in V$, donc on doit calculer agv ; on a, pour $a \in A$:

$$(g^{-1}ag)v = \chi_v(g^{-1}ag)v$$

ie : $a(g(v)) = \chi_v(g^{-1}ag)g(v)$, ce qui signifie que $g(v) \in V$ et $\chi_{g(v)}(a) = \chi_v(g^{-1}ag)$.
L'application $g \to \chi_v(g^{-1}ag)$ est continue, car χ_v est continue sur le stabilisateur de la droite engendrée par v (sur lequel χ_v s'obtient par projection sur $\mathbf{C}v$ par rapport à un supplémentaire). De plus, l'égalité précédente montre qu'elle est à valeurs dans le spectre de a : elle est donc à valeurs discrètes. Ceci prouve qu'elle est constante, et $\chi_v = \chi_{g(v)}$ pour tout g.

4. On note W le sous-espace engendré par les $(g(v))_{g\in G}$. Si $W = \mathbf{C}^n$, alors cela implique que A est uniquement constitué d'homothéties. Si G est abélien, alors $G = A$, et c'est terminé. Sinon, alors $\ell \geq 2$, donc A est un groupe dérivé : en particulier, le déterminant est trivial sur A, et donc A est isomorphe à un sous-groupe des racines n-ièmes de 1 dans $\mathbf{C}$. Donc $A = 1$ par connexité : c'est absurde. Donc soit c'est fini, soit $W \neq \mathbf{C}^n$.
   W est alors un espace G-stable, donc la matrice d'un élément de G dans $\mathbf{C}^n \simeq W \bigoplus W'$ est de la forme suivante, pour une matrice inversible P :
   $$g = P \begin{pmatrix} \rho(g) & \star \\ 0 & \rho'(g) \end{pmatrix} P^{-1}$$
   Alors $\rho(G)$ et $\rho'(G)$ sont des sous-groupes de $\mathrm{GL}_k(\mathbf{C})$ (resp $\mathrm{GL}_{n-k}(\mathbf{C})$) connexes résolubles (en effet, l'image d'un groupe résoluble est résoluble, facile). Par récurrence, ils sont simultanément trigonalisables, ce qui permet de conclure en concaténant des bases de trigo.

Remarques :

- Ce théorème est un théorème projectif : si G est un sous-groupe connexe résoluble de $\mathrm{GL}_n(\mathbf{C})$, alors son image dans $\mathrm{PGL}_n(\mathbf{C})$ a un point fixe commun dans $\mathbf{P}(\mathbf{C}^n)$.
- Soit $T_n(\mathbf{C})$ le sous-groupe de $\mathrm{GL}_n(\mathbf{C})$ formé des matrices triangulaires supérieures. Alors $T_n(\mathbf{C})$ est résoluble (un crochet envoie e_1 sur e_1, un double crochet fixe (e_1, e_2), etc). On a donc montré que $T_n(\mathbf{C})$ était, à conjuguaison près, le seul sous-groupe résoluble connexe maximal de $\mathrm{GL}_n(\mathbf{C})$ (au même titre que $\mathcal{O}_n(\mathbf{R})$ est le seul sous-groupe compact maximal de $\mathrm{GL}_n(\mathbf{R})$ à conjuguaison près).
- Le théorème est faux si on enlève l'hypothèse de connexité : par exemple, le groupe diédral $D_n \subset \mathrm{GL}_2(\mathbf{C})$ n'est pas simultanément trigonalisable, car sinon, il fixerait une droite ; par le théorème de Maschke, il fixerait un supplémentaire de cette droite, et il serait donc simultanément diagonalisable, donc abélien ; c'est faux.

1.7 Moyen & classique : sous-groupes compacts de $\mathrm{GL}_n(\mathbf{R})$

(haut) Recasages : 103, 106, 150, 170, 171, 181, 203, 208. But : Tout sous-groupe compact de $\mathrm{GL}_n(\mathbf{R})$ est conjugué à un sous groupe de $\mathcal{O}_n(\mathbf{R})$.

Deux versions pour méthodes géométriques : théorème du point fixe de Kakutani (cf Szpirglas), et ellipsoïde de John (cf FGN Algèbre 3).

Énoncé :

a) On montre le théorème de point fixe de Kakutani :
Soit G compact, V espace vectoriel de dim finie, $\rho : G \to \mathrm{GL}(V)$ morphisme continu et $K \subset V$ un compact convexe non vide stable sous-l'action de G. Alors : $\exists x \in K, \forall g \in G, \rho(g)x = x$.
On en déduit que tout sous-groupe compact de $\mathrm{GL}_n(\mathbf{R})$ est conjugué à un sous-groupe de $\mathcal{O}_n(\mathbf{R})$.

b) On montre le théorème de l'ellipsoïde de John :
Si K est un compact d'intérieur non vide, alors il existe un unique ellipsoïde centré en 0 de volume minimal contenant K.
On en déduit que tout sous-groupe compact de $\mathrm{GL}_n(\mathbf{R})$ est conjugué à un sous-groupe de $\mathcal{O}_n(\mathbf{R})$.

Preuve :

a) Pour le théorème de Kakutani : on note H l'image de ρ par G, qui est donc un ss-g compact.
On regarde $N(x) = \sup_{u \in H} \|u(x)\|_2$ (avec $\|\|_2$ une norme euclidienne) : c'est bien défini (par compacité de H et continuité de l'évaluation en x $H \to \mathbf{R}^n$), c'est une norme sur E (en effet, tous les axiomes sont vérifiés car $\|\|_2$ est une norme).
De plus, il y a égalité dans l'inégalité triangulaire ssi x et y sont positivement liés. En effet, si $x, y \in \mathbf{R}^n$, on a :

$$\|u(x+y)\|_2 \leq \|u(x)\|_2 + \|u(x+y)\|_2 \leq N(x) + N(y)$$

Or, comme $N(x+y) = \|u(x+y)\|_2$ pour un certain $u \in H$ (toujours par compacité), on en déduit que si $N(x+y) = N(x) + N(y)$, alors a fortiori, pour ce u :

$$\|u(x) + u(y)\|_2 = \|u(x)\|_2 + \|u(x+y)\|_2$$

Ce qui implique, par égalité de l'inégalité triangulaire euclidienne, que $u(x)$ et $u(y)$ soient positivement liés. Comme u est inversible, cela implique que x et y soient positivement liés.
Comme K est compact, il existe $x \in K$ minimisant N sur K. Montrons que x est point fixe commun de H. Déjà, on a, comme $v \mapsto uv$ est une bijection de H :

$$N(u(x)) = \sup_{v \in H} \|vu(x)\|_2 = \sup_{v' \in H} \|v'\|_2 = N(x)$$

De plus, on a $u(x) \in K$ par hypothèse, et donc par convexité : $\frac{1}{2}(x+u(x)) \in K$. Et, en prenant la norme :

$$N\left(\frac{x+u(x)}{2}\right) \leq \frac{N(x) + N(u(x))}{2} = N(x)$$

Donc on a égalité dans l'inégalité triangulaire, et on en déduit que x et $u(x)$ sont positivement liés ; enfin, comme ils sont de mêmes normes, ils sont égaux, on a donc bien $u(x) = x$.

Pour le corollaire, on prend $\rho(g)(q) = q \circ g^{-1}$ sur les formes quadratiques (autrement dit, on regarde l'action naturelle). C'est bien dans $\mathrm{GL}(\mathcal{Q}(\mathbf{R}^n))$, et c'est continu.
Notons O l'orbite du produit scalaire canonique sous l'action de G. Alors O est compact par image continue de G. Ainsi, $K = Conv(O)$ est un convexe compact par le théorème de Carathéodory, non vide. Donc il existe $q \in K$ fixé par tous les éléments de H. On a donc $G \subset \mathcal{O}(q)$: pour conclure, il suffit donc de montrer que q est définie positive. Mais on a $O \subset \mathcal{Q}^{++}(\mathbf{R}^n)$ (car touit élément conjugué à un produit scalaire en est un), donc $K \subset \mathcal{Q}^{++}(\mathbf{R}^n)$ par convexité de ce dernier : cela permet de conclure.

b) Pour q définie positive, je regarde $\mathcal{E}_q = \{x, q(x) \leq 1\}$, et $\mathcal{Q}_K = \{q \in \mathcal{Q}^{++}(\mathbf{R}^n), K \subset \mathcal{E}_q\}$. Alors $\mathcal{Q}_K$ est non vide (car K est borné), fermé (car si $q_n \in \mathcal{Q}_K \to q$, et $x \in K$, $q(x) = \lim q_n(x) \leq 1$)), convexe (facile) et borné (car K est d'intérieur non vide, donc son diamètre est ≥ 0, alors que le diamètre de $\mathcal{E}_q$ tend vers l'infini si q tend vers l'infini). Par le théorème de Heine-Borel, $\mathcal{Q}_K$ est compact ; de plus, $q \mapsto \det(q)$ est strictement log-concave sur $\mathcal{Q}^{++}(\mathbf{R}^n)$; en effet, cela est une conséquence de l'orthogonalisation. simultanée. (**à admettre éventuellement**)
J'en déduis que $\det$ a un unique maximum sur le compact $\mathcal{Q}_K$: ce maximum correspond donc bien à un volume minimal.

Pour la conséquence, on prend G un sous-groupe compact de $\mathrm{GL}_n(\mathbf{R})$, et on pose $K = \bigcup_{g\in G} gB$, avec B la boule unité fermée de $\mathbf{R}^n$ pour une norme. C'est un compact (image continue de $G \times B$) d'intérieur contenant 0. Ainsi, il existe une unique q telle que $K \subset \mathcal{E}_q$ et $\mathcal{E}_q$ soit de volume minimal. Soit $g \in G$, regardons $q \circ g^{-1}$: c'est toujours défini positif, et son volume est $|\det(g)|^n$. Or G est compact, donc $\det(G)$ est un sous-groupe compact de $\mathbf{R}_+^\star$: ce dernier étant isomorphe (en tant que groupe topologique) à $\mathbf{R}$, on en déduit que $|\det(G)| = 1$, donc le volume est préservé. De plus, si $x \in K$, on a $g^{-1}x \in K$ par définition, donc $q \circ g^{-1} \in \mathcal{Q}_K$. Par unicité, on a directement $G \subset \mathcal{O}(q)$.

1.8 Moyen & semi-classique : Version faible du théorème de Dirichlet par les polynômes cyclo/corps finis

(haut) Référence : Hindry (ne le fait pas tout à fait pareil, il regarde les racines). Recasages : 120, 121, 123, 125, 141

Énoncé : Soit Φ_n le n-ème polynôme cyclotomique, q la puissance d'un nombre premier premier à n. Alors, dans $\mathbf{F}_q$, Φ_n est le produit de d polynômes irréductibles (différents par séparabilité) de mêmes degrés $m = \frac{\varphi(n)}{d}$, et m vaut l'ordre de $q \in (\mathbf{Z}/n\mathbf{Z})^\times$.
Applications :

- Φ_n est irréductible sur $\mathbf{F}_q$ ssi q engendre $(\mathbf{Z}/n\mathbf{Z})^\times$.
- $\Phi_8 = X^4 + 1$ est irréductible dans $\mathbf{Q}[X]$, mais jamais dans $\mathbf{F}_q[X]$.
- Φ_n a une racine dans $\mathbf{F}_q$ ssi $q = 1 \pmod n$ ssi Φ_n est scindé dans $\mathbf{F}_q$.
- Si n est un entier naturel non nul, il y a une infinité de nombres premiers congrus à $1 \pmod n$.

Preuve : On écrit : $\Phi_n = \prod_{i=1}^d P_i$ la décomposition en irréductibles. Soit $i \in \{1, \dots, d\}$, soit ζ une racine d'un P_i dans un corps de rupture $L = \mathbf{F}_q(\zeta)$. Alors $\deg(P_i) = [L : K] =: m$ (dépendant de i a priori). Alors on a $\Phi_n(\zeta) = 0$, donc ζ est d'ordre divisant n. De plus, $X^n - 1$ est à racines simples, (car premier à sa dérivée) donc les $(\Phi_d)_{d|n}$ sont premiers entre eux : en particulier, ζ n'annule aucun des autres Φ_d, ce qui prouve que ζ est d'ordre n.
Par le théorème de Lagrange, on a $n \mid |L^*| = q^m - 1$, ie : $q^m = 1 \pmod n$. Montrons que m est minimal en ce sens. Si m' est l'ordre de q, alors $L' = \{x \in L, x^{q^{m'}} = x\} = L^{\mathrm{Frob}^{m'}}$ est une sous-extension de $L/\mathbf{F}_q$ contenant ζ : c'est égal à L. Donc $m' = m$. Ainsi, m est bien l'ordre de q modulo n.

Pour la version faible de Dirichlet : on a $\Phi_n(0) = 1$ pour tout n, donc pour tout entier N, N est premier avec $\Phi_n(N)$ (car N divise $\Phi_n(N) - \Phi_n(0)$). De plus, comme Φ_n est un polynôme, il n'y a qu'un nombre fini de a tels que $\Phi_n(a) = \pm 1$. Il existe des nombres premiers $= 1 \pmod n$: en effet, on prend N tel que $\Phi_n(N) \neq \pm 1$, puis n'importe quel diviseur premier de $\Phi_n(N)$ convient. S'il n'y avait qu'un nombre fini de premiers congrus à $1 \pmod n$, notés $p_1 \dots, p_k$ alors on prend $N = \ell p_1 \dots p_k$, pour un ℓ tel que $\Phi_n(N) \neq \pm 1$; si p est un diviseur premier à $\Phi_n(N)$, alors par ce qui précède, $p = 1 \pmod n$, et p est premier à N : c'est impossible.

Remarque : Si $n \geq 3$, il existe une infinité de nombres premiers non congrus à $1 \pmod n$: en effet, il y en a (2 par exemple) et s'il y en avait un nombre fini, disons $p_1, \dots, p_k$, alors $2np_1 \dots p_k - 1$ aurait un diviseur premier non congru à $1 \pmod n$.

Remarque 2 : Factoriser Φ_n dans $\mathbf{F}_p$ revient à trouver la décomposition de $p\mathcal{O}_K$ en produit d'idéaux premiers de $\mathcal{O}_K$, où $K = \mathbf{Q}(\zeta_n)$ est la n-ème extension cyclotomique. En particulier, p est totalement décomposé ssi $p \equiv 1 \pmod n$, et p reste premier dans $\mathcal{O}_K$ ssi p engendre $(\mathbf{Z}/n\mathbf{Z})^\times$.

1.9 Facile & semi-classique : suite de polygones du plan qui converge vers un point

(haut) Recasages : 102, 149, 155, 181, 191.

Énoncé : Soit $P = (P_0 \dots P_{n-1})$ un n-gone quelconque du plan affine réel. On considère la transformation $P \mapsto P'$ qui à un polygone associe le polygone constitué des milieux des côtés. L'itération de cette transformation converge (au sens où chaque point du polygone converge vers) l'isobarycentre O.

Preuve : Soit $P_j^{(m)}$, pour $j \in \mathbf{Z}/n\mathbf{Z}$, les sommets du polygone à l'itération m. On vectorialise par rapport à O, et on identifie $(P_j^{(m)})_j$ à un point de $\mathbf{C}^n$. La transformation revient donc à faire :

$$(z_j) \mapsto (\frac{z_{j-1} + z_j}{2})$$

Autrement dit, notant $z = (z_j)$, les coordonnées de $P^{(m)}$ seront :

$$A^m z \qquad \text{où } A = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & & & & (0) \\ & \frac{1}{2} & \frac{1}{2} & & & \\ & & \ddots & \ddots & & \\ & & & \frac{1}{2} & \frac{1}{2} & \\ & & (0) & & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & & & & & \frac{1}{2} \end{pmatrix}$$

On détermine A^m ; pour cela, on peut écrire $A = \frac{1}{2}(I_n + J)$, où $J = \begin{pmatrix} 0 & 1 & & & & (0) \\ & 0 & 1 & & & \\ & & \ddots & \ddots & & \\ & & & 0 & 1 & \\ (0) & & & & 0 & 1 \\ 1 & & & & 0 & 0 \end{pmatrix}$

On cherche à réduire la matrice J, ce qui permettra de réduire la matrice A. Ce qu'on peut remarquer, c'est que la transformation décrite envoie un polygone régulier sur un polygone régulier ; autrement dit, pour $k \in [\![0, n-1]\!]$, on est amené à considérer : $v^k = (1, \omega^k, \dots, \omega^{(k-1)(n-1)}$, où $\omega = \exp(\frac{2i\pi}{n})$. On vérifie alors : $v^k = \omega^k v^k$. Ainsi, on a trouvé n vecteurs propres associés à des valeurs propres distinctes : un résultat simple nous dit alors que J est diagonalisable, et que ses valeurs propres sont ω^k, et même que $(v^k)_{k \in [\![0,n-1]\!]}$ est une base de diagonalisation de J, donc de A. On a ainsi, pour une matrice $P \in \mathrm{GL}_n$:

$$A = P\mathrm{diag}(\frac{1+1}{2}, \frac{1+\omega}{2}, \dots, \frac{1+\omega^{n-1}}{2})P^{-1}$$

Or on a : $1 + \omega^k = e^{\frac{ik\pi}{n}} \times 2\cos\left(\frac{k\pi}{n}\right)$. Ainsi,

$$\left|\frac{1+\omega^k}{2}\right| = \cos\left(\frac{k\pi}{n}\right)$$

et donc :

$$\forall k \neq 0, \left(\frac{1+\omega^k}{2}\right)^m \underset{m\to\infty}{\longrightarrow} 0$$

Ceci prouve que A^m converge (au sens des applications linéaires) vers le projecteur sur $\ker(A - I_n)$ parallèlement à $\oplus_k \ker(A - \frac{1}{2}(1+\omega^k)I_n)$. Autrement dit, ce projecteur est celui sur Vect(v^0) parallèlement à son supplémentaire Vect$(v^1, \dots, v^{n-1})$.
Revenons à notre problème : on écrit $z = z^0 + z^1 + \ldots + z^{n-1}$ cette décomposition, on a alors, comme la somme des racines d-èmes de l'unité est nulle pour d divisant n :

$$\forall k \neq 0, \sum_{i=0}^{n-1} v_i^k = 0$$

Et donc on a : $z^0 = \left(\frac{1}{n}\sum_{i=0}^{n-1} z_i\right) v^0$.
Or, comme O est l'isobarycentre du polygone, on a $\sum_i z_i = 0$, ce qui prouve donc que $A^m z$ converge vers le vecteur nul : autrement dit, la suite de polygones converge bien vers le point O.

Remarque 1 : Concernant la projection sur les points fixes : on utilise ici le fait que cet espace est de dimension 1, puis on utilise une petite astuce. En général, si on a un endom u sur E annulé par PQ, avec P et Q premiers entre eux, alors si $UP + VQ = 1$ est une relation de Bézout associée, on a la décomposition :

$$E = \ker(P(u)) \oplus \ker(Q(u))$$

et les projecteurs sont donnés par $p_P = (VQ)(u)$ et $p_Q = (UP)(u)$.
Ici, on a $P = X - 1$ et $Q = \frac{X^n - 1}{X-1}$. La division euclidienne de Q par P donne ainsi, pour S un polynôme[1] :

$$Q = PS + n$$

donc $V = \frac{1}{n}$ et $U = -\frac{S}{n}$ conviennent, et $p_P = \frac{1}{n}\sum_i u^i$, autrement dit pour J :

$$z^0 = \frac{1}{n}\sum_i J^i z = \frac{1}{n}\begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix} z$$

Remarque 2 : On peut changer l'énoncé : par exemple, on peut remplacer le milieu par le centre de gravité du triangle formé par 3 points consécutifs, etc...

1. égal à $X^{n-2} + 2X^{n-3} + \ldots + n - 1$

1.10 Moyen & semi-classique : Démonstration des formules de Newton, et applications

Références : Mansuy & Mneimné, Réduction des endom, et Cassini algèbre 1. Mneimné, réduction des endom pour la dernière.
Recasages : 144, 153, 157.
Application : résolution d'équations non linéaires, ou exo 5.27 de Cassini 1, ou encore : M nilpotente ssi $\forall k \geq 1, \mathrm{Tr}(M^k) = 0$.

Énoncé : Soit K un corps, soit $\lambda_1, \ldots, \lambda_n \in \mathbf{K}$, et, pour $k \geq 0$, $s_k = \sum_i \lambda_i^k$ (où $s_0 := n$) les sommes de Newton. On note également a_k les coefficients du polynôme $P = \prod_i (X - \lambda_i)$; en terme de fonctions symétriques élémentaires, on a donc $a_{n-k} = (-1)^k \sigma_k \quad (k \geq 1)$.
Alors on a les relations suivantes

$$\forall k \geq n, \quad \sum_{j=0}^{n} a_j s_{k-n+j} = 0 \qquad (1)$$

$$\forall k \in [\![1, n]\!], \quad \sum_{j=0}^{k} a_{n-k+j} s_j = (n-k) a_{n-k} \qquad (2)$$

Application : Si A est une matrice 3×3 annulé par un polynôme scindé [2], alors :

$$6 \det(A) = \mathrm{Tr}(A)^3 - 3\mathrm{Tr}(A)\mathrm{Tr}(A^2) + 2\mathrm{Tr}(A^3)$$

Preuve : On sait que la matrice compagnon associée à P,

$$C_P = \begin{pmatrix} 0 & 0 & \ldots & \ldots & 0 & -a_0 \\ 1 & \ddots & & & \vdots & -a_1 \\ 0 & \ddots & \ddots & & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots \\ 0 & & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \ldots & \ldots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

La matrice compagnon est la matrice de la multiplication par $\overline{X}$ dans $\mathbf{K}[X]/(P(X))$ dans la base $(\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}})$: en particulier, elle est annulée par P. Ainsi, pour la (1), on a :

$$0 = \mathrm{Tr}(P(C_P)C_P^{k-n}) = \sum_{j=0}^{n} a_j \mathrm{Tr}(C_P^{k-n+j})$$

Or C_P est annulée par P scindé, donc C_P est trigonalisable, et C_P est semblable à $diag(\lambda_1, \ldots, \lambda_n) +$ T, où T est triangulaire supérieure. En particulier, on a $\mathrm{Tr}(C_P^\ell) = \sum_{j=1}^n \lambda_j^\ell$ pour tout ℓ, d'où la formule (1).
Pour la formule (2), on introduit la suite de polynômes donnés par :

$$Q_{n-k} = \sum_{j=0}^{k} a_{n-k+j} X^j \quad (k \in [\![0, n]\!])$$

2. Cette condition est artificielle, on peut toujours se placer sur un corps de décomposition de π_A

Par le même argument que précédemment, le membre de gauche de (2) est exactement $\mathrm{Tr}(Q_k(C_P))$. On a $Q_0 = P$, $Q_n = 1$, et $Q_{n-k} - XQ_{n-k+1} = a_{n-k}$. On en déduit, en téléscopant (attention à distinguer X et Y dans les calculs), une identité dans $\mathbf{K}(X)[Y]$:

$$P(X) = (X - Y)(\sum_{k=0}^{n-1} Q_{k+1}(Y)X^k) + Q_0(Y)$$

Ce qui donne, en "évaluant" en C_P pour Y :

$$P(X)I_n = (XI_n - C_P)\sum_{k=0}^{n-1} Q_{k+1}(C_P)X^k I_n$$

Ainsi :

$$P(X)(XI_n - C_P)^{-1} = \sum_{k=0}^{n-1} Q_{k+1}(C_P)X^k I_n$$

D'où, en prenant la trace (et en utilisant le fait que $XI_n - C_P$ est trigonalisable) :

$$\sum_{j=1}^{n} \frac{1}{X - \lambda_j} P(X) = \sum_{k=0}^{n-1} \mathrm{Tr}(Q_{k+1}(C_P))X^k$$

Dans le terme de gauche, on reconnaît $\frac{P'}{P}$: ainsi, on a :

$$P'(X) = \sum_{k=0}^{n-1} \mathrm{Tr}(Q_{k+1}(C_P))X^k$$

dans $\mathbf{K}(X)$, donc aussi dans $\mathbf{K}[X]$ car les deux sont des polynômes; autrement dit, la relation (2) est prouvée.

Pour l'application : on sait que A est trigonalisable sur $\mathbf{K}$, on note λ_1, λ_2 et λ_3 ses valeurs propres; on garde les mêmes notations. On a alors, en appliquant la formule pour $k = 3, 2$ et 1 :

$$\begin{cases} a_0s_0 + a_1s_1 + a_2s_2 + a_3s_3 & = & 0 \\ a_1s_0 + a_2s_1 + a_3s_2 & = & a_1 \\ a_2s_0 + a_3s_0 & = & 2a_2 \end{cases}$$

On en déduit, comme $s_k = \mathrm{Tr}(A^k)$, $a_2 = -\mathrm{Tr}(A)$ et $a_3 = 1$:

$$2a_1 = \mathrm{Tr}(A)^2 - \mathrm{Tr}(A^2)$$

En multipliant la première équation par 2, et comme $s_0a_0 = -3\det(A)$, on a :

$$-6\det(A) + (\mathrm{Tr}(A)^2 - \mathrm{Tr}(A^2))\mathrm{Tr}(A) - 2\mathrm{Tr}(A)\mathrm{Tr}(A^2) + 2\mathrm{Tr}(A^3) = 0$$

ce qui conclut en arrangeant les termes.

1.11 Facile & classique : marche aléatoire sur le N-gone régulier

(haut) Référence : ? Recasage : 149, 155, 261, 262.

Énoncé : Soit N un entier impair supérieur ou égal à 3. Soit (X_n) une suite de variables aléatoires à valeurs dans $\mathbf{Z}/N\mathbf{Z}$ telle que $X_0 = 0$ ps et :

$$\forall k \in \mathbf{Z}/N\mathbf{Z}, \mathbb{P}\left(X_{n+1} = k \pm 1 \mid X_n = k\right) = \frac{1}{2}$$

Alors, quand $n \to \infty$, $X_n \longrightarrow \mathcal{U}(\mathbf{Z}/N\mathbf{Z})$ en loi.

Preuve : Soit, pour $n \geq 0$, p_n défini par :

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

Alors la formule des probas totales montre que $p_{n+1} = Ap_n$, où :

$$A = \begin{pmatrix} 0 & 1/2 & 0 & \dots & 1/2 \\ 1/2 & 0 & 1/2 & (0) & \\ & \ddots & \ddots & \ddots & \\ & & & & 1/2 \\ 1/2 & 0 & \dots & 1/2 & 0 \end{pmatrix}$$

Autrement dit, A est la matrice avec des $1/2$ sur la sur et sous-diagonale, avec un en haut-droite et en bas-gauche. On peut écrire

$$A = \frac{1}{2}(J + J^{-1})$$

avec

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

J est la (transposée de) la matrice compagnon de $X^n - 1$, donc son polynôme minimal est $X^N - 1$: ainsi, elle a N valeurs propres distinctes, les ω^k (avec $\omega = e^{2i\pi/N}$), pour $k \in \{0, \dots, N-1\}$, et est donc diagonalisable. On peut donc écrire :

$$J = \sum_{k=0}^{N-1} \omega^k Q_{\omega_k}$$

avec q_{ω_k} la matrice du projecteur spectral. On en déduit :

$$A = \sum_{k=0}^{N-1} \cos(2k\pi/N) Q_{\omega_k}$$

Et donc :

$$A^n = \sum_{k=0}^{N-1} \cos(2k\pi/N)^n Q_{\omega_k}$$

Or, comme N est impair, tous les $\cos$ sauf le premier ont une valeur absolue < 1, donc ils tendent tous vers 0 ; ainsi, on a :

$$A^n \longrightarrow Q_1$$

Dès lors, on en déduit :

$$p_n \longrightarrow Q_1(p_0)$$

Comme A est symétrique réelle, ses projecteurs spectraux sont des projecteurs orthogonaux [3] ; comme $\mathrm{Im}(Q_1)$ est la droite engendrée par $\pi =^t (1, 1 \ldots, 1)$, on en déduit :

$$Q_1(p_0) = \frac{\langle p_0, \pi\rangle}{\langle \pi, \pi\rangle}\pi = \frac{1}{N}\pi$$

Et donc on a :

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

Ce qui prouve bien, l'espace d'états étant discret, la convergence en loi de X_n.

3. Voir le développement sur la suite de polygones pour une méthode d'algèbre linéaire et non bilinéaire.

1.12 Moyen & semi-classique : forme normale de Smith

Référence : Beck Malick Peyré, Objectif Agrégation Recasages : 122, 126, 150, 162

Énoncé : Soit A un anneau euclidien, de stathme φ. Toute matrice U de $\mathcal{M}_n(A)$ s'écrit :

$$U = PDQ^{-1}$$

où $D = diag(d_1, d_2, \dots, d_n)$ et P, Q sont des matrices de $\mathrm{GL}_n(A)$, où $d_1|d_2 \dots |d_n$. Application pour les équations diophantiennes linéaires. On présente l'algorithme avec $A = \mathbf{Z}$ (muni de son stathme $|n|$) et $U = \begin{pmatrix} 4 & 8 & 4 \\ 4 & 13 & 11 \\ 4 & 16 & 13 \end{pmatrix}$ (cf remarque).

Preuve : On exhibe un algorithme qui permet, en restant dans la même classe de similitude, de se ramener à une matrice diagonale comme cherchée. On rappelle que les matrices de transvection et de permutation sont dans $\mathrm{GL}_n(A)$, donc les opérations $L_i \longleftarrow L_i + aL_j$ et $L_i \longleftrightarrow L_j$ sont permises (et pareil avec les colonnes).
L'algorithme fonctionne en 5 étapes :

1. Si $M = 0$, c'est fini.

2. Sinon, on permute les lignes et les colonnes pour que $\varphi(a_{1,1})$ soit le plus petit stathme de toute la matrice.

3. Première colonne : pour i entre 2 et n, faire :

   a) Effectuer la division euclidienne de $u_{i,1}$ par $u_{1,1}$: $u_{i,1} = u_{1,1}q + r_i$. Faire l'opération élémentaire $L_i \longleftarrow L_i - qL_1$.

   b) Si $r_i \neq 0$, faire $L_i \longleftrightarrow L_1$ et retourner en 3a).

   c) Si $r_i = 0$, passer à la ligne suivante si $i \neq n$, et à l'étape 4 si $i = n$.

4. Première ligne : pour j entre 2 et n faire :

   a) Effectuer la division euclidienne de $u_{1,j}$ par $u_{1,1}$: $u_{1,j} = u_{1,1}q + r'_j$. Faire l'opération élémentaire $C_j \longleftarrow C_j - qC_j$.

   b) Si $r'_j \neq 0$, faire $C_j \longleftrightarrow C_1$ et retourner en 3a) **(et non pas en 4a)!!)**.

   c) Si $r'_j = 0$, passer à la colonne suivante si $j \neq n$, et à l'étape 5 si $j = n$.

5. À ce stade, la première ligne et la première colonne sont nulles, sauf en première position.

   a) S'il existe $i_1 \geq 2$ et $j_1 \geq 2$ tels que u_{i_1,j_1} n'est pas divisible par $u_{1,1}$, alors faire $C_1 \longleftarrow C_1 + C_{i_1}$ et retourner en 3.

   b) Sinon, appliquer l'algorithme avec la matrice extraite $(u_{i,j})_{i,j\geq 2}$.

$$\begin{pmatrix} 4 & 8 & 4 \\ 4 & 13 & 11 \\ 4 & 16 & 8 \end{pmatrix} \xrightarrow[1,2,3]{} \begin{pmatrix} 4 & 8 & 4 \\ 0 & 5 & 7 \\ 0 & 8 & 4 \end{pmatrix} \xrightarrow[4ac)]{} \begin{pmatrix} 4 & 0 & 0 \\ 0 & 5 & 7 \\ 0 & 8 & 4 \end{pmatrix}$$
$$\xrightarrow[5a)]{} \begin{pmatrix} 4 & 0 & 0 \\ 5 & 5 & 7 \\ 8 & 8 & 4 \end{pmatrix} \xrightarrow[3a)]{} \begin{pmatrix} 4 & 0 & 0 \\ 1 & 5 & 7 \\ 8 & 8 & 4 \end{pmatrix}$$
$$\xrightarrow[3b)]{} \begin{pmatrix} 1 & 5 & 7 \\ 4 & 0 & 0 \\ 8 & 8 & 4 \end{pmatrix} \xrightarrow[3ac)]{} \begin{pmatrix} 1 & 5 & 7 \\ 0 & -20 & -28 \\ 8 & 8 & 4 \end{pmatrix}$$
$$\xrightarrow[3ac)]{} \begin{pmatrix} 1 & 5 & 7 \\ 0 & -20 & -28 \\ 0 & -24 & -52 \end{pmatrix} \xrightarrow[4ac)]{} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -20 & -28 \\ 0 & -24 & -52 \end{pmatrix}$$
$$\xrightarrow[5b)]{} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & -72 \end{pmatrix}$$

On montre que l'algorithme termine : pour cela, on a besoin de trouver un entier naturel qui décroît strictement après chaque étape. Les étapes impliquent que $\varphi(u_{1,1})$ décroît à chaque étape, mais pas forcément strictement. Comme $\varphi(u_{1,1})$ décroît strictement à chaque passage en $3)b)$, il n'y en a qu'un nombre fini, et donc on passe forcément au moins une fois à l'étape 4. À chaque passage $4 \to 3$, $\varphi(u_{1,1})$ décroit strictement, donc il n'y a qu'un nombre fini de tels passages : ainsi, on passe forcément à l'étape 5. Enfin, après chaque passage $5 \to 3$, l'étape $3)b)$ puis $3)a)$ fait diminuer strictement $\varphi(u_{1,1})$: donc on ne passe qu'un nombre fini de fois en $5)a)$, ce qui prouve qu'on arrive forcément en $5)b)$ à terme : par récurrence sur l'entier n, on arrive bien à la forme voulue : cqfd.

Remarque : Pour obtenir la matrice de l'exemple, je suis parti d'un cas où on va à l'étape $5)a)$: $\begin{pmatrix} 4 & 0 & 0 \\ 0 & 5 & 7 \\ 0 & 8 & 4 \end{pmatrix}$ puis j'ai mis des coefficients divisibles par le terme en $(1,1)$ sur la première colonne : $\begin{pmatrix} 4 & 0 & 0 \\ 4 & 5 & 7 \\ 4 & 8 & 4 \end{pmatrix}$. Enfin, j'ai fait $C_2 \longleftarrow C_2 + 2C_1$ et $C_3 \longleftarrow C_3 + C_1$: $\begin{pmatrix} 4 & 8 & 4 \\ 4 & 13 & 11 \\ 4 & 16 & 8 \end{pmatrix}$.

1.13 Description de $\mathcal{O}(p,q)$

Référence : NH2G2 tome 1 Recasages : 156, 160, 170, 171.

Énoncé : Soit p, q des entiers naturels non nuls. Alors on a un homéomorphisme :

$$\mathcal{O}(p,q) \simeq \mathcal{O}(p) \times \mathcal{O}(q) \times \mathbf{R}^{pq}$$

En particulier, $\mathcal{O}(p,q)$ a quatre composantes connexes. Faire l'exemple de $\mathcal{O}(1,2)$ qui préserve la forme de Lorentz où la variable d'espace est plane.

Preuve : On rappelle que $\mathcal{O}(p,q)$ est un groupe, c'est le stabilisateur de

$$I(p,q) = diag(\underbrace{1,\dots,1}_{p}, \underbrace{-1,\dots,-1}_{q})) = I_p \oplus (-I_q)$$

pour l'action par congruence. De plus, le principe de conjugaison (et la classification des fq sur $\mathbf{R}$) assure que tous les groupes d'isométries d'une forme quadratique de signature (p,q) sont conjugués à $\mathcal{O}(p,q)$.

On utilisera beaucoup les deux faits suivants, qu'il est bon d'admettre avant le développement :

lemme 1 $\exp : \mathscr{S}_n(\mathbf{R}) \longrightarrow \mathscr{S}_n^{++}(\mathbf{R})$ est un homéomorphisme.

Montrer que $\exp$ est une bijection est assez simple (l'injectivité demandant un peu de travail), en utilisant le théorème spectral; pour montrer la continuité de l'inverse, on prend (A_m) telle que $\exp(A_m) \longrightarrow \exp(A)$, alors on a aussi, par continuité de l'inverse, que $\exp(-A_m) \longrightarrow \exp(-A)$. Ainsi, comme le spectre d'une suite de matrices symétriques bornée est majoré (par e^C, où C domine $\|M\|_2$), il résulte que le spectre des (A_m) est majoré, et minoré en utilisant $(-A_m)$: donc (A_m) est bornée. Mais la seule valeur propre possible de cette suite est A, donc $A_m \longrightarrow A$.

lemme 2 (décomposition polaire) On a un homéomorphisme :

$$\begin{gathered}\mathscr{S}_n^{++}(\mathbf{R}) \times \mathcal{O}(n) \longrightarrow \mathrm{GL}_n(\mathbf{R}) \\ (S,O) \mapsto SO\end{gathered}$$

En effet, la réciproque est donnée par $M \mapsto (\sqrt{M^tM}, M(\sqrt{M^tM})^{-1})$, où la racine est un homéo $\mathscr{S}_n^{++}(\mathbf{R}) \longrightarrow \mathscr{S}_n^{++}(\mathbf{R})$ en utilisant le lemme 1 et le fait que la multiplication par $\frac{1}{2}$ est un homéo dans $\mathscr{S}_n(\mathbf{R})$.

On peut donc passer au développement : on montre que $\mathcal{O}(p,q)$ est stable par décomposition polaire, i.e. que, si (S,O) est la décompostion polaire de M, alors :

$$M \in \mathcal{O}(p,q) \iff (S,O) \in (\mathscr{S}_n^{++}(\mathbf{R}) \cap \mathcal{O}(p,q)) \times (\mathcal{O}(n) \cap \mathcal{O}(p,q))$$

Pour cela, il suffit de montrer que S est dans $\mathcal{O}(p,q)$. On note $T = M^tM$, on a $T^2 = S$. On remarque que $\mathcal{O}(p,q)$ est stable par transposée : en effet :

$$M \in \mathcal{O}(p,q) \iff MI_{(p,q)}\,{}^tM = I_{(p,q)} \iff {}^tM^{-1}I_{(p,q)}M^{-1} = I_{(p,q)} \iff ({}^tM)^{-1} \in \mathcal{O}(p,q)$$

Cela prouve que $T \in \mathcal{O}(p,q)$. Ensuite, on montre que $\mathcal{O}(p,q)$ est stable par racine carrée. Pour cela, on écrit $T = \exp(U)$. On a alors :

$$\begin{aligned}
\exp(U) \in \mathcal{O}(p,q) &\iff \exp(U) I_{(p,q)} \exp({}^tU) = I_{(p,q)} \\
&\iff I_{(p,q)} \exp(U) I_{(p,q)}^{-1} = \exp(-U) \text{ on utilise la symétrie de } U \\
&\iff \exp(I_{(p,q)} U I_{(p,q)}^{-1}) = \exp(-U) \\
&\iff I_{(p,q)} U I_{(p,q)}^{-1} = -U \text{ (par le lemme 1, en utilisant le fait que } I_{(p,q)} \in \mathcal{O}(n)) \\
&\iff I_{(p,q)} \frac{U}{2} I_{(p,q)}^{-1} = -\frac{U}{2} \\
&\iff \exp\left(\frac{U}{2}\right) \in \mathcal{O}(p,q)
\end{aligned}$$

Donc finalement, comme $S = \exp\left(\frac{U}{2}\right)$, on en déduit que $S \in \mathcal{O}(p,q)$.

Ainsi, la décomposition polaire induit un homéo :

$$\mathcal{O}(p,q) \simeq (\mathscr{S}_n^{++}(\mathbf{R}) \cap \mathcal{O}(p,q)) \times (\mathcal{O}(n) \cap \mathcal{O}(p,q))$$

Il reste à détailler les deux termes de ce produit.

D'après les équivalences précédentes, on a, pour $U \in \mathscr{S}_n(\mathbf{R})$:

$$\exp(U) \in \mathcal{O}(p,q) \iff I_{(p,q)} U = -U I_{(p,q)}$$

Ainsi, en écrivant $U = \begin{pmatrix} U_1 & U_2 \\ {}^tU_2 & U_3 \end{pmatrix}$, on trouve :

$$\exp(U) \in \mathcal{O}(p,q) \iff \begin{pmatrix} U_1 & U_2 \\ -{}^tU_2 & -U_3 \end{pmatrix} = \begin{pmatrix} -U_1 & U_2 \\ -{}^tU_2 & U_3 \end{pmatrix} \iff U_1 = 0_p \text{ et } U_3 = 0_q$$

Finalement $\mathscr{S}_n^{++}(\mathbf{R}) \cap \mathcal{O}(p,q) \simeq \mathcal{M}_{p,q}(\mathbf{R})$ via exp et $U_2 \mapsto \begin{pmatrix} 0 & U_2 \\ {}^tU_2 & 0 \end{pmatrix}$.

Si $O \in \mathcal{O}(n)$, alors

$$O \in \mathcal{O}(p,q) \iff [O, I_{(p,q)}] = 0 \iff O = O_p \oplus O_q \qquad \text{avec } O_p \in \mathcal{O}(p) \text{ et } O_q \in \mathcal{O}(q)$$

où la dernière équivalence est une simple reformulation du fait que si un endomorphisme commute avec un autre, il stabilise ses espaces propres. Finalement, on a bien l'homéomorphisme désiré.

1.14 Moyen & classique : Théorème de Perron Frobenius avec deux applications

Recasages : 149, 226. Référence : D. Serre, Matrices.

Énoncé : On suppose que $A > 0$; soit ρ le rayon spectral de A (valeur propre de plus grand module). Alors $\rho > 0$, ρ est une valeur propre simple de A, elle est dominante (i.e. : toutes les autres valeurs propres ont un module $< \rho$) et il existe un unique vecteur v à coordonnées positives tel que $Av = \rho v$ et $\|v\|_1 = 1$: on l'appelle vecteur de Perron-Frobenius associé à A.

Application 1 : Soit $G = (E = \{1, \dots N\}, V)$ un graphe orienté. On définit la matrice des liens L par : $l_{i,j} = \frac{1}{d_j}$ si $j \to i \in V$ (où d_i est le nombre de liens sur la page i), et 0 sinon. Cette matrice est stochastique positive, mais pas > 0. On définit J la matrice avec des 1 partour et $G = (1-\alpha)\frac{1}{N}J + \alpha L$. Alors G a un vecteur propre positif pour la valeur propre 1, et celui-ci est unique sous la condition que la somme des coefficients soit 1. On le trouve par la méthode de la puissance : $\mu_\infty = \lim G^n \mu$. On calcule les puissances de G en utilisant le fait que L est une matrice creuse : cela permet de calculer $G\mu$ en $\bar{l}N$ opérations où $\bar{l}$ est le nombre moyen de liens.

Application 2 : $y(t) = e^{tA} y_{init}$, et v, ϕ sont les vecteurs de Perron-Frobenius de A et A^T (vérifier qu'ils existent) tq $\langle v, \phi \rangle = 1$, alors :

$$y(t)e^{-\rho t} \underset{t \to +\infty}{\longrightarrow} \langle y_{init}, \phi \rangle v$$

Preuve : On définit $\mathscr{C} := \{x \in \mathbf{R}^n, \forall j, x_j \geq 0\}$; c'est un fermé. On note π le vecteur colonne avec que des 1. On montre :

$$\forall x \in \mathscr{C}, 0 \leq \langle Ax, \pi \rangle \leq \langle x, \pi \rangle \underbrace{\sup_j \left(\sum_{i=1}^n a_{i,j} \right)}_{:=M} \tag{1}$$

En effet, le premier membre est évident car tout est positif ; et le second membre se montre via l'égalité :

$$\langle Ax, \pi \rangle = \sum_{i=1}^n \sum_{j=1}^n a_{i,j} x_j \leq M \sum_{i=1}^n x_i$$

On note ensuite

$$\mathscr{E} := \{t \geq 0, \exists x \in \mathscr{C} \backslash \{0\}, Ax - tx \in \mathscr{C}\}$$

Alors :

- $\mathscr{E}$ est un intervalle : en effet, si $t \in \mathscr{E}$, on dispose de $x \in \mathscr{C}$ non nul tel que $Ax - tx \in \mathscr{C}$. Alors, comme $\mathscr{C}$ est stable par somme, si $t' < t$, on a $Ax - t'x = Ax - tx + (t - t')x \in \mathscr{C}$. Dès lors, si $t \in \mathscr{E}$, on a $[0, t] \subset \mathscr{E}$: cela prouve que $\mathscr{E}$ est étoilé par rapport à 0, c'est donc un connexe de $\mathbf{R}$, donc un intervalle.

- $\mathscr{E}$ est fermé : en effet, si $t_n \to t_\infty$, avec $t_n \in \mathscr{E}$, alors pour tout n, on dispose d'un $x_n \in \mathscr{C} \backslash \{0\}$ "correspondant" : on peut, quitte à diviser x_n par sa norme, supposer que $\|x_n\|_1 = 1$ pour tout n. Alors (x_n) est à valeurs dans la sphère unité, qui est compacte ; on peut en extraire $x_{\varphi(n)} \to x_\infty$ (avec $\|x_\infty\| = 1$). Alors on a :

$$\forall n, Ax_{\varphi(n)} - t_{\varphi(n)} x_{\varphi(n)} \in \mathscr{C}$$

Or ce terme tend vers $Ax_\infty - t_\infty x_\infty$, et $\mathscr{C}$ est fermé : on en déduit que $t_\infty \in \mathscr{E}$ pour $x_\infty \in \mathscr{C}$ (une nouvelle fois car $\mathscr{C}$ est fermé).

- $\mathscr{E}$ est borné : en effet, on a vu en (1) :

$$\forall x \in \mathscr{C}, \langle Ax - Mx, \pi \rangle \leq 0$$

Donc pour $t > M$, on a $t \notin \mathscr{E}$.

- $\mathscr{E}$ n'est pas réduit à 0 : en effet, les coordonnées de $A\pi$ sont toutes strictement positives (car $a_{i,j} > 0$) ; ainsi, il existe $t > 0$ tel que $A\pi - t\pi \in \mathscr{C}$ (on peut invoquer le fait que $\{x \in \mathbf{R}^n, \forall j, x_j > 0\}$ est un ouvert).

Ainsi, $\mathscr{E} = [0, \rho]$, pour un $\rho > 0$.
Soit $x \in \mathscr{C} \backslash \{0\}$ tel que $Ax - \rho x \in \mathscr{C}$. On montre alors que $Ax = \rho x$; supposons que ce ne soit pas le cas, notons $y = Ax - \rho x$. Alors comme y est non nul et comme $a_{i,j} > 0$ pour tout i, j, toutes les coordonnées de Ay sont strictement positives : ainsi, on a $Ay \in \overset{\circ}{\mathscr{C}}$, et on dispose de $\varepsilon > 0$ tel que :

$$Ay - \varepsilon Ax \in \mathscr{C}$$

Comme $Ay - \varepsilon Ax = A(Ax) - (\rho + \varepsilon)Ax$, et $Ax \in \mathscr{C} \backslash \{0\}$ (pour la même raison que pour y), on en déduit que $\rho + \varepsilon \in \mathscr{E}$, absurde.

On a donc montré que ρ était valeur propre de A, et qu'il existait un vecteur propre à coeffs positifs.

Soit $z \in \mathbf{C}^n$ un vecteur propre de A associé à la valeur propre $\lambda > 0$. Alors on a, par l'inégalité triangulaire :

$$|Az|_i = \left| \sum_{j=1}^{n} a_{i,j} z_j \right| \leq (A|z|)_i$$

Comme on a $|Az| = |\lambda||z|$, on a :

$$A|z| - |Az| = A|z| - |\lambda||z| \in \mathscr{C}$$

En particulier, on a $|\lambda| \in \mathscr{E}$, donc :

$$|\lambda| \leq \rho$$

Étudions le cas d'égalité : $|\lambda| = \rho$ ssi il y a égalité dans l'inégalité triangulaire, i.e. si les $(a_{i,j}z_j)_j$ sont positivement liés, ou, ce qui revient au même puisque $a_{i,j} > 0$, ssi les (z_j) sont positivement liés. On peut alors écrire $z = |z|e^{i\theta}$, et alors $|z|$ est aussi valeur propre de A pour λ. Mais comme A est à coefficients positifs et $|z|$ aussi, on a $\lambda \geq 0$, et donc $\lambda = \rho$. Ainsi ρ est bien la plus grande valeur propre de A, et elle est dominante.
On montre enfin que $\dim(\ker(A - \rho id)) = 1$; soit z un vecteur propre pour ρ, on suppose : $\langle v, z \rangle = 0$ (où v a été défini avant). Alors on a vu que $|z|$ était vecteur propre de A pour ρ : de plus on a $z = |z|e^{i\theta}$ pour un θ, donc $\langle v, |z| \rangle = 0$. Or $v = \frac{1}{\rho}Av$ est à coefficients > 0, donc $|z| = 0$, et $z = 0$. Ainsi, l'orthogonal de v dans $\ker(A - \rho id)$ est 0, ce qui prouve :

$$\rho \text{ est simple et } \ker(A - \rho id) = \mathbf{C}v$$

Application 1 : Le caractère stochastique de la matrice A est une conséquence de la définition. En revanche, elle est rarement à coefficients strictement positifs... C'est pourquoi on introduit $G =$

$(1-\alpha)\frac{1}{N}J+\alpha L$: alors le théorème de Perron-Frobenius s'applique à G ; comme G est stochastique, on a $\rho \leq 1$. De plus, l'application $\mu \mapsto G\mu = \alpha L\mu + (1-\alpha)\begin{pmatrix} \frac{1}{N} \\ \vdots \\ \frac{1}{N} \end{pmatrix}$ est contractante dans $\mathbf{R}^N$; elle admet donc un unique point fixe, ce qui prouve que 1 est vecteur propre de G. Ainsi, 1 est valeur propre simple, et le vecteur cherché est exactement le vecteur de Perron-Frobenius de G.

Le calcul de $G\mu = \alpha L\mu+(1-\alpha)\begin{pmatrix} \frac{1}{N} \\ \vdots \\ \frac{1}{N} \end{pmatrix}$ peut se faire, en utilisant le fait que L est une matrice creuse, en $\sim \bar{l}N$ étapes. Ainsi, on obtient un algo d'approximation de v.

Application 2 : Comme ${}^TA$ est aussi à coefficients positifs, elle admet un vecteur de Perron-Frobenius ϕ.

1.15 Moyen & original : degré de représentation, nombre de classes de conjugaison et cardinal du groupe

Référence : NH2G2 Tome 2 ou Serre, Représentations linéaires des groupes finis.
Recasage : 103, 104, 144, (153)

Énoncé : Soit ρ une rep irréductible de G fini, de degré d. Alors $d \mid |G|$.
Application : si G est un groupe fini de cardinal impair, le nombre k de classes de conjugaison de G vérifie $k \equiv |G| \pmod 8$.

Remarque : En fait, on a même : $d \mid [G : Z(G)]$ mais c'est plus difficile.

Preuve : Si C est une classe de conjugaison, alors on peut définir $\chi(C)$. Soient $C_1, \ldots C_k$ les différentes classes de conjugaison. Pour $i \in [\![1, k]\!]$, on note z_i défini par :

$$z_i = \sum_{s \in C_i} \rho(s)$$

alors z_i vérifie, comme C_i est une classe de conjugaison : $\forall g, \rho(g) z_i \rho(g^{-1}) = z_i$. Ainsi, par le lemme de Schur [4], on dispose de $\lambda_i \in \mathbf{C}$ tel que $z_i = \lambda_i id_{\mathbf{C}^{d_i}}$. En prenant la trace, on a :

$$\lambda_i d = \mathrm{Tr}(z_i) = \sum_{s \in C_i} \chi(s) = |C_i| \chi(C_i)$$

On montre que λ_i est un entier algébrique. Vue l'expression de z_i, on dispose de $A = (a_{h,k})_{h,k \in G} \in \mathcal{M}_n(\mathbf{Z})$ telle que

$$\forall h \in G, z_i \rho(h) = \sum_{k \in G} a_{h,k} \rho(g)$$

Et, comme on a aussi $z_i \rho(h)$, cela prouve que λ_i est racine du polynôme caractéristique de A : ainsi, λ_i est un entier algébrique. Enfin, on a :

$$\begin{aligned}
\sum_{j=1}^{k} \lambda_j \overline{\chi(C_j)} &= \frac{1}{d} \sum_{j=1}^{k} d \lambda_j \overline{\chi(C_j)} \\
&= \frac{1}{d} \sum_{j=1}^{k} |C_j| \chi(C_j) \overline{\chi(C_j)} \quad \text{par l'identité au dessus} \\
&= \frac{1}{d} \sum_{g \in G} \chi(g) \overline{\chi(g)} \\
&= \frac{|G|}{d} \quad \text{par orthonormalité}
\end{aligned}$$

Or :

- λ_j est un entier algébrique pour tout j
- $\overline{\chi(C_j)}$ est un entier algébrique, car $\chi(C_j)$ est un entier algébrique (car $\rho(g)$ est diagonalisable, à valeurs propres annulées par $X^n - 1$, donc sa trace est un entier algébrique), et car tout polynôme à coefficients entiers annulant $\chi(C_j)$ annulera aussi son conjugué.

4. qu'on peut redémontrer en considérant le noyau et l'image, qui sont G-stables, donc triviaux

- L'ensemble des entiers algébriques est un anneau.

Ainsi, $\frac{|G|}{d}$ est un entier algébrique. Mais c'est aussi un rationnel : cela implique qu'il est dans $\mathbf{Z}$. Conclusion : $d \mid |G|$.

Pour l'application, on prend un tel groupe G d'ordre n impair. On sait que, notant d_i les degrés des représentations irréductibles de G (pour $i \in [\![1,k]\!]$: il y en a autant que de classes de conjug), on a [5] :

$$n = \sum_{i=1}^{k} d_i^2$$

Or $d_i \mid n$ par ce qu'on vient de voir, et donc est impair. Ainsi, on a

$$d_i \equiv \pm 1 \text{ ou } \pm 3 \pmod 8$$

et

$$n \equiv \sum_{i=1}^{k} d_i^2 \equiv \sum_{i=1}^{k} 1 = k \pmod 8$$

ce qui conclut.

5. Cette identité se montre en regardant la représentation régulière de G : sa trace est nulle partout sauf en 1_G où elle vaut n ; on conclut en la décomposant sur la base des caractères irréductibles.

1.16 Difficile & original : indicateur de Frobenius-Schur

Référence : Serre, Représentations linéaires des groupes finis ; NH2G2 tome 2
Recasage : 101, 154, 158, 159, 170.

Énoncé : Soit $\rho : G \to \mathrm{GL}(V)$ une représentation irréductible, de caractère χ. Alors, s'équivalent :

(i) χ est à valeurs réelles

(ii) Il existe une forme bilinéaire non nulle fixée par $\rho(G)$.

(iii) Il existe une forme bilinéaire non dégénérée fixée par $\rho(G)$.

De plus si ces conditions sont réunies, les prop suivantes sont équivalentes :

(i) ρ se réalise sur $\mathbf{R}$: dans une base (e_i) de V, pour tout g, $\mathrm{Mat}_{e,e}(\rho(g))$ est à coeff réels.

(ii) Il existe une forme bilinéaire symétrique non nulle fixée par $\rho(G)$.

(iii) L'indicateur de Frobenius-Schur vaut 1, i.e. :

$$\frac{1}{|G|}\sum_{g\in G}\chi(g^2) = 1$$

Ainsi, on montre que $\mathcal{D}_4$ et $\mathbb{H}_8$ ne sont pas isomorphes (bien qu'ils aient même table de caractère).

Preuve : Pour la première, on a un isomorphisme de représentations $\mathrm{Bil}(V;\mathbf{C}) \to \mathrm{Hom}(V, V^*)$ (le vérifier !) ; ainsi, par le lemme de Schur, les trois premières propositions sont équivalentes à $\mathrm{Hom}(V, V^*)^G \neq 0$ (pour la (iii), remarquer que tout élément non nul de cet Hom est inversible, car son noyau et son image sont G-stables).
Pour la deuxième proposition, on a la décompostion en espaces G-stables :

$$\mathrm{Bil}(V;\mathbf{C}) = \mathrm{Sym}(V) \oplus \mathrm{A}(V)$$

et le caractère induit sur $\mathrm{Sym}(V)$ vaut, en g, notant (λ_i) les valeurs propres de $\rho(g)$:

$$\sum_{1\leq i<j\leq n}\overline{\lambda_i\lambda_j} + \sum_{i=1}^{n}\overline{\lambda_i\lambda_i} = \frac{\chi(g^{-2}) + \chi(g^{-1})^2}{2}$$

Ainsi, $(iii) \iff (ii)$, en utilisant le fait que $\frac{1}{|G|}\sum_g \chi(g)^2 = (\chi,\chi) = 1$.
Il reste à montrer $(i) \iff (ii)$: on procède par double implication :

- $(i) \implies (ii)$: Soit $(e_1,\ldots,e_n)$ une base comme demandée. Soit $V_0 = \bigoplus_i \mathbf{R}e_i$. Soit β la forme bilinéaire telle que (e_i) soit orthonormée. Alors la forme

  $$\widetilde{\beta} = \frac{1}{|G|}\sum_{g\in G} g\cdot\beta$$

  est G-invariante, et symétrique. De plus, comme V_0 est G-stable, sa restriction à V_0 est un produit scalaire : elle est donc non nulle.

- $(ii) \implies (i)$: Soit B une forme bilinéaire symétrique invariante par G. Soit $\langle \cdot, \cdot \rangle$ un produit hermitien invariant par G (qu'on peut construire en moyennant). Alors, par représentation de Riesz, pour une unique application $\varphi : V \to V$ antilinéaire, on a :

  $$\forall x, y \in V, B(x, y) = \langle \varphi(x), y \rangle$$

  De plus, une telle application φ commute alors avec l'action de G : en effet, pour $x, y \in V$, on a :

  $$\begin{aligned} \langle \varphi(gx), gy \rangle &= \beta(gx, gy) \\ &= \beta(x, y) \quad \text{(car } \beta \text{ est invariante par } G\text{)} \\ &= \langle \varphi(x), y \rangle \\ &= \langle g\varphi(x), gy \rangle \quad \text{(car le produit scalaire est invariant par } G\text{)} \end{aligned}$$

  On a alors, pour $x, y \in V$:

  $$B(\varphi(x), y) = \langle \varphi^2(x), y \rangle = \langle \varphi(x), \varphi(y) \rangle$$

  Donc, en échangeant x et y, on trouve : φ^2 est hermitien, et $\langle \varphi^2(x), x \rangle = \langle \varphi(x), \varphi(x) \rangle > 0$: φ^2 est défini positif. Donc il existe un unique hermitien défini positif v tel que $\varphi^2 = v^2$. On pose alors $\sigma = \varphi v^{-1}$: comme v est polynomiale en φ, on a $\sigma^2 = 1$: c'est une symétrie (en voyant V comme un $\mathbf{R}$-espace vectoriel). On note V_0 et V_1 les sous-espaces propres de σ, on a $V_1 = iV_0$ (car : $\sigma(x) = x \iff \sigma(ix) = -ix$), et donc :

  $$V = V_0 \oplus_{\mathbf{R}} iV_0$$

  Comme σ est polynomiale en φ, elle commute à tous les éléments de G, et cette décomposition est donc G-stable. Cela conclut.

1.17 Moyen & original : nombre de solutions non singulières d'une équation quadratique modulo N

Réf : Hindry, p17-18-19 Recasages : 120, 123, 126, 170.

Énoncé : Soit $Q : (x_1, \dots x_n) \mapsto \sum_{1\leq i,j\leq n} b_{ij}x_ix_j$ une forme quadratique en n variables à coeff entiers non dégénérée (sur $\mathbf{Q}^n$). Soit, pour N entier, $\mathscr{C}(N) = \{x \in (\mathbf{Z}/N\mathbf{Z})^n, Q(x) = 0$ et $\mathrm{pgcd}(x_1, \dots, x_n, N) = 1\}$ et $c(N) = \mathrm{Card}(\mathscr{C}(N))$. Alors, pour N impair premier avec D_Q (le déterminant de $(b_{ij})_{1\leq i,j\leq n}$) :

$$c(N) = N^{n-1}\prod_{p|N}\frac{p^{n-1} - 1 + \varepsilon_p(p-1)p^{\frac{n}{2}-1}}{p^{n-1}}$$

où $\varepsilon_p = \begin{cases} 0 & \text{si } n \text{ est impair} \\ \left(\frac{(-1)^{\frac{n}{2}}D_Q}{p}\right) & \text{si } n \text{ est pair} \end{cases}$.

Preuve : On procède en trois étapes :

1. Si $N = p$ est premier : On a une forme quadratique sur $(\mathbf{F}_p)^n$, et on cherche à déterminer le cardinal de son cône $\mathscr{C}(Q) \cup \{0\}$; par l'algorithme de Gauss, on peut se ramener au cas où $Q(x) = \sum_{i=1}^n a_ix_i^2$, où tous les a_i sont non nuls car $D_Q \equiv \prod a_i \pmod p$, et $D_Q \not\equiv 0 \pmod p$. On a alors :

$$\begin{aligned} c(p) + 1 &= \sum_{x_1,\dots,x_n\in\mathbf{F}_p} \delta_{Q(x_1,\dots,x_n),0} \\ &= \frac{1}{p}\sum_{x_1,\dots,x_n\in\mathbf{F}_p}\sum_{a\in\mathbf{F}_p}\exp\left(\frac{2i\pi}{p}aQ(x_1,\dots,x_n)\right) \\ &= p^{n-1} + \frac{1}{p}\sum_{x_1,\dots,x_n\in\mathbf{F}_p}\sum_{a\neq 0}\exp\left(\frac{2i\pi}{p}aQ(x_1,\dots,x_n)\right) \\ &= p^{n-1} + \frac{1}{p}\sum_{x_1,\dots,x_n\in\mathbf{F}_p}\sum_{a\neq 0}\prod_{i=1}^n\exp\left(\frac{2i\pi}{p}aa_ix_i^2\right) \\ &= p^{n-1} + \frac{1}{p}\sum_{a\neq 0}\prod_{i=1}^n\underbrace{\sum_{x_i\in\mathbf{F}_p}\exp\left(\frac{2i\pi}{p}aa_ix_i^2\right)}_{:=\tau(aa_i)} \end{aligned}$$

On admet (provisoirement) le lemme suivant :
lemme : On a :

- $\tau(a) = \left(\frac{a}{p}\right)\tau(1)$,
- $|\tau(1)|^2 = p$
- $\tau(1)^2 = \left(\frac{-1}{p}\right)$

On a donc :

$$\begin{aligned} c(p) + 1 &= p^{n-1} + \frac{1}{p}\sum_{a\neq 0}\prod_{i=1}^n\left(\frac{aa_i}{p}\right)\tau(1) \\ &= p^{n-1} + \frac{1}{p}\left(\frac{D_Q}{p}\right)\tau(1)^n\sum_{a\neq 0}\left(\frac{a}{p}\right)^n \end{aligned}$$

Or $\sum_{a\neq 0}\left(\frac{a}{p}\right) = 0$ si n est impair, et $p-1$ sinon. Si n est pair, on a $\tau(1)^{\frac{n}{2}} = \left(\frac{-1}{p}\right)^n p^{\frac{n}{2}}$. On a donc bien :

$$c(p) = p^{n-1} + \varepsilon_p p^{\frac{n}{2}-1}(p-1) - 1$$

2. Si M et N sont premiers entre eux, alors le lemme chinois affirme que si $x_1, \dots, x_n \in \mathbf{Z}/(MN)\mathbf{Z}$, on a $Q(x) \equiv 0 \pmod{NM}$ ssi $Q(x) \equiv 0 \pmod{N}$ et $\pmod{M}$; de plus, la condition de pgcd se comporte de la même façon. Ainsi, la bijection $(\mathbf{Z}/MN\mathbf{Z})^n \to (\mathbf{Z}/M\mathbf{Z})^n \times (\mathbf{Z}/N\mathbf{Z})^n$ induit une bijection $\mathscr{C}(MN) \to \mathscr{C}(M) \times \mathscr{C}(N)$, et on en déduit : $c(MN) = c(M)c(N)$.

3. Pour conclure, on calcule, pour p ne divisant pas D_Q et $m \geq 1$, $c(p^m)$. On a une application : $\pi : x \in \mathscr{C}(p^{m+1}) \to (x \pmod{p^m}) \in \mathscr{C}(p^m)$: montrons qu'elle est surjective et que chaque fibre est de card p^{n-1}. Soit $x_0 \in \mathscr{C}(p^m)$, $a_0 \in \mathbf{Z}$ tel que $Q(x_0) \equiv p^m a_0 \pmod{p^{m+1}}$, et $z \in \mathbf{Z}$, on a :

$$\begin{aligned} x_0 + p^m z \in \mathscr{C}(p^{m+1}) &\iff Q(x_0) + 2b_Q(x_0, z) + p^{2m}Q(z) \equiv 0 \pmod{p^{m+1}} \\ &\iff a_0 + b_Q(x_0, z) \equiv 0 \pmod{p} \end{aligned}$$

C'est l'équation d'un hyperplan (en effet, la forme linéaire $z \in \mathbf{F}_p \mapsto b_Q(x_0, z)$ est non nulle car p ne divise pas D_Q) affine dans $\mathbf{F}_p^n$: il y a donc p^{n-1} solutions z modulo p, et donc : $\mathrm{Card}(\pi^{-1}(x_0)) = p^{n-1}$. Ainsi, par récurrence immédiate : $c(p^m) = p^{(m-1)(n-1)}c(p)$.

Finalement, pour N vérifiant l'énoncé, en utilisant l'étape 2 :

$$\begin{aligned} c(N) &= \prod_{p\mid N} c(p^{v_p(N)}) \\ &= \prod_{p\mid N} p^{(v_p(N)-1)(n-1)}c(p) \\ &= N^{n-1} \prod_{p\mid N} \frac{c(p)}{p^{n-1}} \end{aligned}$$

ce qui conclut.

Pour le lemme : si a est un carré et b est un non-carré, alors :

$$\begin{aligned} \tau(a) + \tau(b) &= 2 + \sum_{x\neq 0} \exp\left(\frac{2i\pi}{p} a x^2\right) + \sum_{x\neq 0} \exp\left(\frac{2i\pi}{p} b x^2\right) \\ &= 2 + 2\sum_{x\neq 0} \exp\left(\frac{2i\pi}{p} x\right) \qquad \text{(chaque élément est représenté deux fois)} \\ &= 0 \end{aligned}$$

Donc $\tau(a) = \left(\frac{a}{b}\right)$ pour tout a.
Pour la deuxième partie : l'application $(x, y) \in (\mathbf{F}_p)^2 \mapsto (x+y, x-y) \in (\mathbf{F}_p)^2$ est bijective car $p \neq 2$; ainsi, on a :

$$\tau(1)\overline{\tau(1)} = \sum_{x,y} \exp\left(\frac{2i\pi}{p}(x^2 - y^2)\right) = \sum_{u,v} \exp\left(\frac{2i\pi}{p} uv\right) = p$$

La troisième partie s'en déduit, car $\overline{\tau(1)} = \tau(-1) = \left(\frac{-1}{p}\right)\tau(1)$.

1.18 Moyen & original : CNS d'existence d'une matrice vérifiant une équation polynomiale

Référence : ? ?

Énoncé : Soit $\mathbf{K}$ un corps, et $P \in \mathbf{K}[X]$ un polynôme irréductible de degré d. On note $\mathbf{L}$ le corps de décomposition de P sur $\mathbf{K}$, et on note $G = \mathrm{Aut}(\mathbf{L}/\mathbf{K})$. On suppose que l'action de G sur les racines de P est libre. Alors :

$$\exists M \in \mathcal{M}_n(\mathbf{K}) \iff d \mid n$$

Application : $\exists M \in \mathcal{M}_n(\mathbf{R}), M^2 = -I_n$ ssi n est pair.
Si $M \in \mathcal{M}_n(\mathbf{Q})$ vérifie $M^p = I_n$ (avec p premier), et si $p-1 \not| n$, alors M a un point fixe non nul dans $\mathbf{Q}^n$.

Preuve : On procède par double implication.

Supposons qu'il existe une telle matrice M. Soit $\mathbf{L}$ le [6] corps de décomposition de P sur $\mathbf{K}$. Alors, on sait (par construction du corps de décomposition par succession de corps de rupture) que $G = \mathrm{Aut}(\mathbf{L}/\mathbf{K})$ agit transitivement sur les racines de P dans $\mathbf{L}$.
La matrice M, vue dans $\mathcal{M}_n(\mathbf{L})$, est annulée par P, qui est scindé sur $\mathbf{L}$, et à racines simples (car P est irréductible, donc $\mathrm{pgcd}(P, P') = 1$). Ainsi, M est $\mathbf{L}$-diagonalisable ; soit S son spectre (c'est un ensemble de couples (λ, n_λ)). On a, notant $\Delta = \mathrm{diag}(S)$, l'existence de $Q \in \mathrm{GL}_n(\mathbf{L})$ telle que :

$$M = Q\Delta Q^{-1}$$

Soit $\sigma \in G$; on peut appliquer σ à chaque coefficient des matrices. Comme σ est un automorphisme de corps, il préserve les multiplications et les inverses (il est injectif) ; ainsi, on a :

$$\sigma(M) = \sigma(Q)\sigma(\Delta)\sigma(Q)^{-1}$$

Mais comme $M \in \mathbf{K}$, on a $\sigma(M) = M$. Par unicité du spectre, on a donc :

$$\forall \sigma \in G, \sigma(S) = S$$

Ainsi, on peut regrouper les éléments de S en orbites, et on en déduit :

$$n = \sum_{\lambda \in S} n_\lambda = \sum_{\lambda \in S/G} n_\lambda [G : \mathrm{Stab}(\lambda)]$$

Or G agit librement sur les racines de P, donc $\mathrm{Stab}(\lambda) = 1$, et :

$$n = |G| \sum_{\lambda \in S/G} n_\lambda$$

Pour finir, on montre que $|G| = d$: en effet, soit x une racine de P dans $\mathbf{L}$; comme l'action de G sur les racines de P est transitive, le polynôme

$$Q(X) = \prod_{\sigma \in G} (X - \sigma(x))$$

6. comme tous les corps de décomposition sont isomorphes, l'article défini convient

a exactement les mêmes racines que P dans $\mathbf{L}$, et comme les deux sont scindés à racines simples (on utilise le fait que l'action est libre), on en déduit que $Q = P$, puis que $|G| = d$. Ainsi :

$$d \mid n$$

Réciproquement, supposons que $d \mid n$; alors, en écrivant $M = \begin{pmatrix} \widetilde{M} & \dots & \dots & (0) \\ \vdots & \widetilde{M} & & \vdots \\ \vdots & & \widetilde{M} & \vdots \\ (0) & \dots & \dots & \widetilde{M} \end{pmatrix}$, il suffit de faire le cas $d = n$; pour cela, on écrit $P = X^d + a_{d-1}X^{d-1} + \dots a_0$, et on note m l'endom de multiplication par $\overline{X}$ dans l'anneau quotient $\mathbf{K}[X]/(P)$. En notant $\widetilde{M}$ la matrice de m dans la base $(\overline{1}, \overline{X}, \dots, \overline{X^{d-1}})$ (c'est la matrice compagnon de P), on a $P(\widetilde{M}) = 0$.

Pour les applications :

- On prend $P = X^2 + 1$, on a alors $\mathbf{L} = \mathbf{C}$ et $G = \mathbf{Z}/2\mathbf{Z}$ agit transitivement et librement sur $\{\pm i\}$: on peut appliquer la propriété.
- On prend $\Phi_p = \frac{X^p - 1}{X - 1}$, de degré $p - 1$. On a alors $\mathbf{L} = \mathbf{Q}(\zeta_p)$, où $\zeta_p = \exp(2i\pi/p)$. Alors $G = (\mathbf{Z}/p\mathbf{Z})^\times$: en effet, si $\sigma \in G$, alors σ est entièrement déterminée par $\sigma(\zeta_p)$, qui est une racine de Φ_p. On a ainsi un isomorphisme :

  $$\sigma \in G \mapsto (\mathbf{Z}/p\mathbf{Z})^\times \ni k, \sigma(\zeta_p) = \zeta_p^k$$

  On vérifie que l'action est libre : en effet, toutes les racines de Φ_p engendrent $\mathbf{L}$, donc si σ en fixe une, elle fixe $\mathbf{L}$, et donc : $\sigma = id$.
  Soit $M \in \mathcal{M}_n(\mathbf{Q})$, avec $M^p = I_n$ et $p - 1 \not| n$. Alors, M est annulée par $(X - 1)\Phi_p(X)$, donc par le lemme des noyaux :

  $$\mathbf{Q}^n = \ker(M - I_n) \oplus \ker(\Phi_p(M))$$

  La restriction $M\Big|_{\ker(\Phi_p(M))}$ est alors bien définie, et annulée par Φ_p ; par la propriété, on a donc $p - 1 \mid \dim(\ker(\Phi_p(M)))$. Ainsi, on en déduit $\dim(\ker(M - I_n)) \neq 0$, et donc M a un point fixe dans $\mathbf{Q}^n$.

1.19 Moyen & classique : deux équations diophantiennes

Réf : Hindry, chap III.

Énoncé : On explicite les triplets (x, y, z) primitifs (ie : tels que $\mathrm{pgcd}(x, y, z) = 1$) tels que :

$$x^2 + y^2 = z^2 \qquad \text{(triplets pythagoriciens)}$$

On en déduit que l'équation diophantienne :

$$x^4 + y^4 = z^2$$

n'a pas de solution entière non triviale.

Preuve : On commence par la détermination des triplets pythagoriciens primitifs. On raisonne par analyse-synthèse.

- *Analyse* Soit (x, y, z) un tel triplet; comme la fonction carré est paire, on peut les supposer positifs. On a, en étudiant les carrés modulo 4 :

  $$z^2 \equiv 0 \text{ ou } 1 \pmod 4$$

  Ainsi, x et y ne peuvent pas être simultanément impairs (car on aurait alors $x^2 + y^2 \equiv 2 \pmod 4$), ni être pairs (car alors z^2, donc z serait aussi pair, et le triplet ne serait pas primitif). Par symétrie des rôles en x et y, on peut supposer x impair et y pair. On a alors $\mathrm{pgcd}_{\mathbf{Z}}(x, y) = 1$: en effet, si p premier divise x et y, il divise z^2 donc z, et c'est impossible.
  On a, dans $\mathbf{Z}[i]$:

  $$z^2 = (x + iy)(x - iy)$$

  Soit d un pgcd de $x + iy$ et $x - iy$ dans $\mathbf{Z}[i]$: l'existence est assurée car $\mathbf{Z}[i]$ est euclidien. Alors d divise $2x$ et d divise $2iy$, donc d divise $2y$. Comme x et y sont premiers entre eux dans $\mathbf{Z}$, on dispose de $u, v \in \mathbf{Z}$ tels que $1 = xu + yv$. On en déduit que d divise 2. Mais d divise z^2, donc d divise $\mathrm{pgcd}_{\mathbf{Z}}(2, z^2)$ (toujours par Bézout), i.e. d divise 1. Ainsi, $x + iy$ et $x - iy$ sont premiers entre eux.
  L'anneau $\mathbf{Z}[i]$ est factoriel (car euclidien), donc comme $x + iy$ et $x - iy$ sont premiers entre eux et que leur produit est un carré, on en déduit que ce sont eux-mêmes des carrés à unité près. Ainsi, on dispose de $u, v \in \mathbf{Z}$ et $\lambda \in \mathbf{Z}[i]^\times$ tels que :

  $$x + iy = \lambda(u + iv)^2$$

  Comme $\lambda \in \{\pm 1, \pm i\}$ et comme x est impair, on en déduit, quitte à échanger u et v :

  $$\begin{cases} x &=& u^2 - v^2 \\ y &=& 2uv \\ z &=& u^2 + v^2 \end{cases}$$

  On peut supposer $u, v \geq 0$. De plus, par primitivité de (x, y, z), on a forcément $\mathrm{pgcd}(u, v) = 1$, et u et v doivent être de parités différentes et on doit avoir $u \geq v$ car $x \geq 0$.

- *Synthèse* Si u et v sont deux entiers naturels premiers entre eux de parités différentes, alors le triplet $(u^2 - v^2, 2uv, u^2 + v^2)$ est bien primitif (à vérifier oralement). De plus, on a bien :

  $$(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2$$

  donc c'est un triplet pythagoricien.

Pour l'application, on suppose qu'il existe une solution (x, y, z) non triviale (qu'on peut supposer positive), et on trouve une solution (x', y', z'), telle que $0 < z' < z$. Cela concluera par descente infinie. On distingue deux cas :

- Si (x, y, z) n'est pas primitif, on dispose de p premier divisant x, y et z. Alors $p^4 \mid z^2$, ce qui montre $p^2 \mid z$. Le triplet $(x/p, y/p, z/p^2)$ convient alors.

- Si (x, y, z) est primitif, alors (x^2, y^2, z) aussi : en effet, si p divise les trois, il divise x et y, absurde. Ainsi, (x^2, y^2, z) est pythagoricien primitif ; par symétrie $x \longleftrightarrow y$, on peut supposer x impair. On dispose alors de u, v comme avant tels que :

$$\left\{ \begin{array}{ccc} x^2 & = & u^2 - v^2 \\ y^2 & = & 2uv \\ z & = & u^2 + v^2 \end{array} \right.$$

  Alors, comme u et v sont premiers entre eux, (x, v, u) est pythagoricien primitif, avec x impair ; on dispose donc de u', v' comme avant tels que :

$$\left\{ \begin{array}{ccc} x & = & u'^2 - v'^2 \\ v & = & 2u'v' \\ u & = & u'^2 + v'^2 \end{array} \right.$$

  Alors :
$$(y/2)^2 = u'v'(u'^2 + v'^2)$$
  donc, comme $\mathrm{pgcd}(u', v') = \mathrm{pgcd}(u', u'^2 + v'^2) = \mathrm{pgcd}(v', u'^2 + v'^2) = 1$, par factorialité, u', v' et $u'^2 + v'^2 = u$ sont des carrés : ainsi, on dispose de $x', y', z' > 0$ tels que $u = z'^2$, $u' = x'^2$ et $v' = y'^2$. Alors on a :
$$x'^4 + y'^4 = z'^2$$
  et $z' \leq u \leq u^2 < u^2 + v^2 = z$; cela conclut.

1.20 Facile & classique : dimension du commutant

Réf : Cassini Algèbre 2.

Énoncé : Soit $\mathbf{K}$ un corps et $A \in \mathcal{M}_n(\mathbf{K})$. Alors, notant $\mathcal{C}(A)$ le commutant de A, on a :

$$\chi_A = \pi_A \iff \mathcal{C}(A) = \mathbf{K}[A]$$

Preuve : On commence par un lemme :
lemme : On a toujours $\dim(\mathcal{C}(A)) \geq n$.
preuve : On commence par remarquer que la dimension de $\mathcal{C}(A)$ est invariante par extension de corps (au sens où le commutant sur Ł a pour Ł-dimension la $\mathbf{K}$-dim de celui sur $\mathbf{K}$) (et ce, parce que le rang d'une famille de vecteurs ne dépend pas du corps, par pivot de Gauss), et qu'elle est invariante en changeant A par PAP^{-1} (car $\mathcal{C}(PAP^{-1}) = P\mathcal{C}(A)P^{-1}$). Ainsi, quitte à se placer sur un corps de décomposition, on peut supposer A triangulaire.
On montre alors que $\dim(\mathcal{C}(A) \cap T_n(\mathbf{K})) \geq n$. Si $X = (x_{i,j})$ est trianguliaire supérieure, alors $AX - XA = 0$ est un système de $\frac{n(n+1)}{2}$ équations, mais les équations diagonales sont $0 = 0$: on a donc au plus $\frac{n(n+1)}{2} - n$ équations libres, ce qui donne un espace de dimension au moins n, d'où le lemme.

Supposons que $\mathcal{C}(A) = \mathbf{K}[A]$. On a alors $\deg(\pi_A) = \dim(\mathbf{K}[A]) \geq n$, donc $\pi_A = \chi_A$ par le théorème de Cayley-Hamilton.
Réciproquement, supposons que $\pi_A = \chi_A$. Montrons qu'il existe $x \in \mathbf{K}^n$ tel que $\pi_{A,x} = \pi_A$; on écrit $\pi_A = P_1^{\alpha_1} \dots P_r^{\alpha_r}$ la décomposition de π_A en irréductibles. On a alors, par le lemme des noyaux, la décomposition en espaces A-stables :

$$\mathbf{K}^n = \bigoplus_{i=1}^{r} \ker(P_i(A)^{\alpha_i})$$

Soit, pour $i \in [\![1, r]\!]$, $x_i \in \ker(P_i(A)^{\alpha_i})$ tel que $P_i^{\alpha_i - 1}(A)x_i \neq 0$: un tel x_i existe car sinon, π_A/P_i serait annulateur. On pose alors $x = \sum_{i=1}^{r} x_i$, et alors ce x_i convient : en effet, pour $P \in \mathbf{K}[X]$, on a :

$$\begin{aligned} P(A)(x) = 0 &\iff \forall i \in [\![1, r]\!], P(A)(x_i) = 0 \\ &\iff \forall i \in [\![1, r]\!], P_i^{\alpha_i} \mid P \\ &\iff \pi_A \mid P \end{aligned}$$

Alors la famille $(x, Ax, \dots, A^{n-1}x)$ est libre, donc est une base de $\mathbf{K}^n$; si $M \in \mathcal{C}(A)$, il existe $P \in \mathbf{K}[X]$ tel que $Mx = P(A)x$. On montre alors, en multipliant par A, que $M = P(A)$, ce qui conclut.

Remarque : On peut montrer qu'en toute généralité, on a $\mathcal{C}(\mathcal{C}(A)) = \mathbf{K}[A]$

2 Analyse

2.1 Facile & classique : Intégrale de Dirichlet par la méthode de Laplace

(haut) Référence : Cassini, Oraux X-ENS, Analyse (2 ou 3 ?) Recasages :

- 228 Continuité, dérivabilité des fonctions réelles d'une variable réelle. Exemples et applications.
- 235 Problèmes d'interversion de limites et d'intégrales
- 236 Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables.
- 239 Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.

Énoncé : On a $\int_0^\infty \frac{\sin(t)}{t}\mathrm{d}t = \frac{\pi}{2}$

Preuve : On commence par remarquer que l'intégrale est bien définie : en fait, elle est semi-convergente. En effet, $\sin$ étant dérivable en 0, le sinus cardinal se prolonge par continuité en 0 où il prend la valeur 1, d'où son intégrabilité locale. De plus, on a, par intégration par parties, pour $\varepsilon > 0, M > \varepsilon$:

$$\int_\varepsilon^M \frac{\sin(t)}{t}\mathrm{d}t = \left[\frac{1-\cos(t)}{t}\right]_\varepsilon^M + \int_\varepsilon^M \frac{1-\cos(t)}{t^2}\mathrm{d}t$$

Le crochet s'annule pour $\varepsilon \to 0, M \to \infty$, et l'intégrande de droite est intégrable sur $[0,\infty[$ (en 0, c'est borné, et en ∞, c'est en $O(t^{-2})$, donc intégrable par critère de Riemann) : dès lors, l'intégrale est semi-convergente.
Soit F la fonction définie sur $\mathbf{R}_+$ par :

$$F(p) = \int_0^\infty \frac{\sin(t)}{t}e^{-pt}\mathrm{d}t$$

La fonction est bien définie, en 0 par ce qui précède, et en $p > 0$ car l'intégrande y est intégrable (c'est continu à décroissance exponentielle).
Par théorème de dérivation sous intégrale, F est même de classe $\mathcal{C}^1$ sur $]0,\infty[$ (pour cela, il suffit de le voir sur $]\varepsilon,\infty[$ pour tout $\varepsilon > 0$), et on a :

$$\begin{aligned}\forall p > 0, F'(p) &= \int_0^\infty -\sin(t)e^{-pt}\mathrm{d}t \\ &= \mathrm{Im}(\frac{1}{i-p}) \\ &= -\frac{1}{1+p^2}\end{aligned}$$

Donc $F + \arctan$ est constante. Par l'inégalité de la moyenne et par l'inégalité $|\sin(t)| \leq |t|$, on a : $\forall p > 0, |F(p)| \leq \frac{1}{p}$. Donc F tend vers 0 en l'infini, donc la constante vaut $\lim_\infty \arctan = \frac{\pi}{2}$.
Pour conclure, il suffit de montrer que F est continue en 0. Pour cela, on fait de nouveau une IPP : si

g est une primitive du sinus cardinal sur $[0, \infty[$, alors pour $p > 0$, on a (en faisant tendre une égalité de primitive à l'infini) :

$$\begin{aligned} F(p) &= \int_0^\infty \frac{\sin(t)}{t} e^{-pt} \mathrm{d}t \\ &= \left[g(t)e^{-pt}\right]_0^\infty + \int_0^\infty g(t)e^{-pt} p \mathrm{d}t \\ &= -g(0) + \int_0^\infty g\left(\frac{u}{p}\right) e^{-u} \mathrm{d}u \end{aligned}$$

En prenant g nulle à l'infini, on a $-g(0) = F(0)$, et l'intégrale au deuxième membre tend vers 0 par le théorème de convergence dominée, car g est bornée et tend vers 0 à l'infini. Donc F est continue en 0, et :

$$\int_0^\infty \frac{\sin(t)}{t} \mathrm{d}t = \frac{\pi}{2}$$

Remarque

- Attention, la fonction $t \mapsto \frac{-\cos(t)}{t}$ n'a pas de limite en 0, il faut donc prendre la bonne primitive dans l'IPP.
- Le sinus cardinal n'est PAS intégrable (il suffit de faire un découpage pour s'en rendre compte).
- Autres méthodes pour calculer cette intégrale : Analyse complexe (regarder $f(z) = \frac{e^{iz}}{z}$ sur un bon contour (qui passe autour de 0)), ou utilisation d'une TF (attention, sinc pas L^1 donc convolution/troncature obligatoire !). Sinon, autre méthode : on a $\int_0^\infty \frac{\sin x}{x} \mathrm{d}x = \frac{\pi}{2}$ par Plancherel, puis une IPP et l'écriture $\frac{1-\cos(2x)}{2} = \sin^2(x)$ permet de conclure.
- En fait, on a montré que si une fonction continue avait une intégrale semi-convergente, alors sa transformée de Laplace est continue en 0.

2.2 Difficile & original : Calcul d'une intégrale elliptique

(haut) Référence : Gourdon Analyse page 188 Recasage : 171, 239, 265, 267.

Énoncé : On note M la moyenne arithmético-géométrique ; alors, pour $u < v$ deux réels strictement positifs :

$$I(u,v) := \int_0^{\frac{\pi}{2}} \frac{\mathrm{d}\varphi}{\sqrt{u^2\cos^2(\varphi) + v^2\sin^2(\varphi)}} = \frac{\pi}{2M(u,v)}$$

On en déduit la longueur du lemniscate de Bernoulli, image par l'inversion de centre 0 de rapport 1 de l'hyperbole $\{x^2 - y^2 = 1\}$ (d'équation en coordonnées polaires $r = \sqrt{\cos(2\theta)}$)

Preuve : On montre que I est invariante en changeant u, v par $\sqrt{uv}, \frac{u+v}{2}$. Pour cela, on fait le changement de variable $t = v\tan(\varphi)$ puis le changement de variable $s = \frac{1}{2}(t - \frac{uv}{t})$ (détail des calculs à la fin). Or I est continue en (u,v) (par le théorème de continuité sous intégrale, en dominant sur chaque $[\varepsilon, \infty[^2$). On en déduit, en passant à la limite (dans $I(u_n, v_n) = I(u,v)$, où u_n, v_n sont les termes pour calculer la MAG) que $I(u,v) = I(M(u,v), M(u,v)) = \frac{\pi}{2M(u,v)}$.

Pour la longueur du lemniscate, on a une paramétrisation donnée par $r = \sqrt{\cos(2\theta)}$. Or, en utilisant les symétries, la longueur du lemniscate est donnée par :

$$\ell = 4\int_0^{\frac{\pi}{4}} \sqrt{r'(\theta)^2 + r(\theta)^2}\mathrm{d}\theta$$

(on a utilisé la formule donnant la vitesse en polaire). Dès lors, en dérivant r :

$$\ell = 4\int_0^{\frac{\pi}{4}} \frac{\mathrm{d}\theta}{\sqrt{1 - 2\sin^2(\theta)}}$$

On fait le changement de variable $2\sin^2(\theta) = \sin^2(\varphi)$, et on trouve alors :

$$\ell = 4\frac{1}{\sqrt{2}}\int_0^{\frac{\pi}{2}} \frac{\mathrm{d}\varphi}{\sqrt{1 - \frac{1}{2}\sin^2\varphi}} = \frac{4}{\sqrt{2}}K\left(\frac{1}{\sqrt{2}}\right)$$

En notant $K(x) = \int_0^{\frac{\pi}{2}}(1 - x^2\sin^2\theta)^{-\frac{1}{2}}\mathrm{d}\theta$. Or on a l'identité suivante : $I(u,v) = \frac{1}{v}K\left(\sqrt{1 - \frac{u^2}{v^2}}\right)$. Ainsi, en prenant $v = \sqrt{2}$ et $u = 1$, on trouve :

$$\ell = \frac{2\pi}{M(1,\sqrt{2})}$$

Pour le premier changement de variable, on a : $t = v\tan\theta$ donc $\mathrm{d}\theta = \frac{1}{v}\frac{\mathrm{d}t}{1+\frac{t^2}{v^2}}$ et, par la formule $\cos^2 = \frac{1}{1+\tan^2}$:

$$u^2\cos^2(\theta) = \frac{u^2}{1 + t^2/v^2} \text{ et } v^2\sin^2(\theta) = \frac{t^2}{1 + t^2/v^2}$$

$$I(u,v) = \int_0^{\infty} \frac{\mathrm{d}t}{\sqrt{(u^2 + t^2)(v^2 + t^2)}}$$

On a aussi :
$$I(\sqrt{uv}, \frac{u+v}{2}) = \frac{1}{2}\int_{-\infty}^{\infty} \frac{\mathrm{d}s}{\sqrt{(uv+s^2)(\frac{1}{4}(u+v)^2+s^2)}}$$
En posant $s = \frac{1}{2}(t - \frac{uv}{t})$, on trouve alors :
$$I(\sqrt{uv}, \frac{u+v}{2}) = I(u,v)$$

2.3 Moyen & semi-classique : Prolongement des transformées de Mellin des fonctions à croissance lente, valeur de la fonction ζ en les entiers négatifs

(haut) Référence : Colmez (p406) Recasages : 207, 239, 245.

Énoncé On admet que $\frac{1}{\Gamma}$ est holomorphe à droite de 0.

Soit f une fonction de classe $\mathcal{C}^\infty$ sur $\mathbf{R}_+$ à décroissance rapide à l'infini ainsi que toutes ses dérivées. Alors sa transformée de Mellin, définie, pour $\mathrm{Re}\,(s) > 0$ par :

$$M(f,s) = \frac{1}{\Gamma(s)} \int_0^\infty f(t) t^s \frac{\mathrm{d}t}{t}$$

admet un prolongement holomorphe à $\mathbf{C}$ tout entier, et vérifie, pour k entier naturel : $M(f,-k) = (-1)^k f^{(k)}(0)$.
Application : la fonction ζ a un prolongement méromorphe sur $\mathbf{C}$, avec un seul pôle d'ordre 1 en 1 (et de résidu 1). On a même : $\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1}$ où (B_n) sont les nombres de Bernoulli ($\frac{t}{e^t-1} = \sum \frac{B_n}{n!} t^n$).

Preuve : On montre que $M(f,\cdot)$ est holomorphe à droite de 0 par le théorème d'holomorphie sous intégrale. On note, pour $\varepsilon > 0$ et $M > \varepsilon$: $I_{\varepsilon,M} = \{z, \varepsilon < \mathrm{Re}\,(z) < M\}$. Alors, si $s \in I_{\varepsilon,M}$ est de partie réelle σ, et si $t \in]0,\infty[$, on a :

$$\left| f(t) t^{s-1} \right| = |f(t)| t^{\sigma-1} \leq |f(t)| (t^{\varepsilon-1} + t^{M-1})$$

Le terme de droite étant intégrable (et ce car f est bornée autour de 0 et à croissance lente à l'infini), le théorème d'holomorphie sous intégrale s'applique (l'intégrande étant holomorphe), et : $M(f,\cdot)$ est holomorphe sur $I_{\varepsilon,M}$, ce pour tout ε, M, donc partout à droite de 0.
Si $\mathrm{Re}\,(s) > 0$, on a par IPP :

$$\int_0^\infty f(t) t^{s-1} \mathrm{d}t = -\frac{1}{s} \int_0^\infty f'(t) t^s \mathrm{d}t$$

ce qui donne, en utilisant l'équation fonctionnelle de Γ :

$$M(f,s) = -M(f', s+1)$$

On en déduit, en remplaçant f par $f^{(k)}$ (qui vérifie les mêmes hyp que f) : $M(f^{(k)}, s) = -M(f^{(k+1)}, s+1)$. Ainsi, on a : $M(f,s) = (-1)^k M(f^{(k)}, s+k)$. Cette équation [7] permet de prolonger de manière holomorphe $M(f,\cdot)$ à droite de $-k$; ainsi, cela étant vrai pour tout k, on a un prolongement de $M(f,\cdot)$ à $\mathbf{C}$ tout entier, qui est holomorphe. Enfin, comme $M(f',1) = \int_0^\infty f'(t)\mathrm{d}t = -f(0)$, on en déduit : $M(f,-k) = (-1)^k f^{(k)}(0)$.

Pour l'application : on a, comme la mesure $\frac{\mathrm{d}t}{t}$ est invariante par multiplication :

$$\forall s, \mathrm{Re}\,(s) > 0 \implies \Gamma(s) = \int_0^\infty e^{-nt} (nt)^s \frac{\mathrm{d}t}{t} = n^s \int_0^\infty e^{-nt} t^s \frac{\mathrm{d}t}{t}$$

7. Il peut être bon de faire un dessin des demi-plans

On en déduit, pour s de partie réelle $\sigma > 1$:

$$\begin{aligned}
\zeta(s) &= \frac{1}{\Gamma(s)} \sum_{n=1}^{\infty} \int_0^{\infty} e^{-nt} t^s \frac{\mathrm{d}t}{t} \\
&= \frac{1}{\Gamma(s)} \int_0^{\infty} \sum_{n=1}^{\infty} e^{-nt} t^s \frac{\mathrm{d}t}{t} \qquad \text{(par Fubini)} \\
&= \frac{1}{\Gamma(s)} \int_0^{\infty} \frac{e^{-t}}{1-e^{-t}} t^s \frac{\mathrm{d}t}{t} \\
&= \frac{1}{\Gamma(s)} \int_0^{\infty} \frac{t}{e^t - 1} t^{s-1} \frac{\mathrm{d}t}{t} \\
&= \frac{1}{s-1} M(f, s-1) \quad \text{avec } f(t) = \frac{t}{e^t - 1}
\end{aligned}$$

Le passage de la première à la deuxième ligne est assuré par l'égalité suivante, par positivité :

$$\sum_{n=1}^{\infty} \int_0^{\infty} e^{-nt} t^{\sigma} \frac{\mathrm{d}t}{t} = \zeta(\sigma)\Gamma(\sigma) < \infty$$

On montre que f vérifie l'énoncé. f est l'inverse d'une fonction holomorphe qui ne s'annule pas autour de 0 donc elle est de classe C^∞ en 0 ; de plus, elle est C^∞ partout ailleurs. On montre, par récurrence sur n, que $f(t) = O(te^{-t})$ en l'infini. On a : $(e^t - 1)f(t) = t$ donc en dérivant n fois, on a, par règle de Leibniz, et en utilisant l'HDR :

$$(e^t - 1)f^{(n)}(t) + O(te^{-t})e^t = O(t)$$

Ce qui conclut en divisant par l'exp.
Ceci permet directement de conclure.

2.4 Moyen & semi-original : Autour de Fourier et de l'analyse complexe

Référence : Queffélec & Queffélec, chapitres III et XI. Recasages : 245, 250, 239, 265.

Énoncé : On démontre, en utilisant diverses méthodes issues de l'analyse complexe, les résultats suivants :

- La transformée de Fourier de $x \mapsto e^{-\frac{x^2}{2}}$ est $\xi \mapsto \frac{1}{\sqrt{2\pi}} e^{-\frac{\xi^2}{2}}$ (par prolongement analytique)
- Si $n \geq 2$, celle de $x \mapsto \frac{1}{1+x^2}$ est $\xi \mapsto \pi e^{-|\xi|}$ (par théorème des résidus).
- Si $f \in L^1(\mathbf{R})$ vérifie : $f(x) = O(e^{-\frac{x^2}{2}})$ et $\widehat{f}(\xi) = O(e^{-\frac{\xi^2}{2}})$, alors f est proportionnelle à la gaussienne. (par un peu plus d'artillerie).

Preuve :

- Je pose $\varphi(x) = e^{-\frac{x^2}{2}}$: c'est bien intégrable ; alors, pour $\xi \in \mathbf{R}$:

$$\begin{aligned}\widehat{\varphi}(\xi) &= \int_{\mathbf{R}} e^{-\frac{x^2}{2}} e^{-i\xi x} \mathrm{d}x \\ &= e^{-\frac{\xi^2}{2}} F(i\xi)\end{aligned}$$

  où $F(z) = \int_{\mathbf{R}} \exp\left(-\frac{(x+z)^2}{2}\right) \mathrm{d}x$. Par invariance par translation de la mesure de Lebesgue, F vaut $\sqrt{2\pi}$ sur $\mathbf{R}$.
  De plus, F est bien définie et est entière : en effet, si $M > 0$, alors pour tout $z \in B(0, M)$, on a :

$$\left| e^{-\frac{(x+z)^2}{2}} \right| = e^{-\frac{x^2}{2}} e^{\frac{1}{2}\mathrm{Re}\left(-xz+z^2\right)} \leq e^{-\frac{x^2}{2}} e^{M^2+M|x|} = O(e^{-\frac{x^2}{4}})$$

  Et pour tout $x \in \mathbf{R}$, la fonction $z \mapsto e^{-\frac{(x+z)^2}{2}}$ est holomorphe sur $B(0, M)$. Ainsi, par le théorème d'holomorphie sous intégrale, F est holomorphe sur $B(0, M)$, et ce pour tout M : donc F est entière.
  Les fonctions entières F et $z \mapsto \sqrt{2\pi}$ coïncident sur $\mathbf{R}$ qui a un point d'accumulation : le principe du prolongement analytique affirme qu'elles sont égales. En particulier, $F(i\xi) = \sqrt{2\pi}$ et $\widehat{\varphi} = \sqrt{2\pi}\varphi$.

- Je pose $\varphi(x) = \frac{1}{1+x^2}$, qui est intégrable, et dont l'intégrale vaut π ; on cherche à calculer

$$\widehat{\varphi}(\xi) = \int_{\mathbf{R}} \frac{e^{-ix\xi}}{1+x^2} \mathrm{d}x$$

  Soit $\xi < 0$. Je pose $f : z \in \mathbf{C} - \{\pm i\} \mapsto \frac{e^{-iz\xi}}{1+z^2}$. Alors f est méromorphe, avec des pôles simples en $\pm i$. On a $\mathrm{Res}(f, i) = \frac{e^{\xi}}{2i}$. Ainsi, en intégrant sur le bord du demi-cercle de rayon $R > 1$ au dessus de l'axe réel, on a, par le théorème des résidus :

$$\int_{-R}^{R} f(x) \mathrm{d}x + \int_0^{\pi} f(Re^{i\theta}) iRe^{i\theta} \mathrm{d}\theta = \pi e^{\xi}$$

Or on a, en utilisant l'inégalité $\sin(\theta) \geq \frac{2\theta}{\pi}$:

$$\begin{aligned}\left|\int_0^\pi f(Re^{i\theta})iRe^{i\theta}\mathrm{d}\theta\right| &\leq \int_0^\pi \left|f(Re^{i\theta})iRe^{i\theta}\right|\mathrm{d}\theta \\ &= \int_0^\pi \frac{R}{R^2-1}e^{\frac{2\theta}{\pi}\xi R}\mathrm{d}\theta \\ &\leq \frac{\pi}{2\xi(R^2-1)}\end{aligned}$$

En particulier, on a : $\int_{\mathbf{R}} f(x)\mathrm{d}x = \pi e^{\xi}$, cqfd.
Pour les $\xi > 0$: on a $\widehat{\varphi}(\xi) = \overline{\widehat{\overline{\varphi}}(-\xi)} = \widehat{\varphi}(-\xi)$, ce qui conclut. Pour $\xi = 0$, on sait que l'intégrale vaut π.

- Pour la dernière : temps à tester.

2.5 Moyen & classique : Prolongement de la fonction ζ et équation fonctionnelle

(haut) Réf : Hindry (p141 puis 154 à 157). Recasages : 245, 246, 265

Énoncé : On montre l'équation fonctionnelle, vérifiée pour $s \in \mathbf{C}$ tel que $\mathrm{Re}(s) \in]0,1[$: notant $\xi(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$, on a :

$$\xi(s) = \xi(1-s)$$

Tel quel, le développement est long : il faut choisir deux des trois étapes, quitte à admettre l'autre.

Preuve : On procède en plusieurs étapes :

- D'abord, on montre que ζ se prolonge en une fonction méromorphe à droite de 0, avec un unique pôle simple en 1 de résidu 1.
- Ensuite, si on veut, on prouve la formule de Poisson et on l'applique pour avoir une équation fonctionnelle pour la fonction θ.
- Enfin, on écrit $\int_0^\infty = \int_0^1 + \int_1^\infty$ et on bidouille un peu.

- On effectue une transformée d'Abel. Soit s un réel > 1. On a :
$$\frac{1}{n^s} = \sum_{k=n}^{\infty}\left(\frac{1}{k^s} - \frac{1}{(k+1)^s}\right)$$
Ainsi, on en déduit :
$$\begin{aligned}
\zeta(s) &= \sum_{n=1}^{\infty}\sum_{k=n}^{\infty}\left(\frac{1}{k^s} - \frac{1}{(k+1)^s}\right)\\
&= \sum_{k=1}^{\infty}\sum_{n=1}^{k}\left(\frac{1}{k^s} - \frac{1}{(k+1)^s}\right) \qquad \text{par positivité}\\
&= \sum_{k=1}^{\infty} k\left(\frac{1}{k^s} - \frac{1}{(k+1)^s}\right)\\
&= \sum_{k=1}^{\infty} k\int_k^{k+1} st^{-s-1}\mathrm{d}t\\
&= s\sum_{k=1}^{\infty}\int_k^{k+1} \lfloor t\rfloor t^{-s-1}\mathrm{d}t\\
&= s\int_1^{\infty} \lfloor t\rfloor t^{-s-1}\mathrm{d}t \qquad \text{par convergence monotone}
\end{aligned}$$
Le dernier terme est une fonction holomorphe de s à droite de 1 par le théorème d'holomorphie sous intégrale. Le principe du prolongement analytique permet d'affirmer que l'égalité est valable pour tout s à droite de 1. Maintenant, si s est à droite de 1, on a :
$$\begin{aligned}
\zeta(s) &= s\int_1^{\infty}(\lfloor t\rfloor - t + t)t^{-s-1}\mathrm{d}t\\
&= s\int_1^{\infty}(\lfloor t\rfloor - t)t^{-s-1}\mathrm{d}t + \frac{s}{s-1}
\end{aligned}$$
Et le premier terme est holomorphe à droite de 0, par le théorème d'holomorphie sous intégrale. Ainsi, on a bien le premier point.

- Soit $f \in \mathcal{S}(\mathbf{R})$, on note $\widehat{f}$ sa transformée de Fourier, donnée par :

$$\widehat{f}(\xi) = \int_{\mathbf{R}} f(x)e^{-2i\pi x\xi}\mathrm{d}x$$

On montre la formule de Poisson :

$$\sum_{n\in\mathbf{Z}} f(n) = \sum_{m\in\mathbf{Z}} \widehat{f}(m)$$

Déjà, les deux sommes sont bien définies car f et $\widehat{f}$ sont toutes deux dans $\mathcal{S}(\mathbf{R})$. Soit F la fonction définie sur $\mathbf{R}$ par :

$$F(x) = \sum_{n\in\mathbf{Z}} f(x+n)$$

Alors F est la somme d'une série de fonctions qui converge uniformément, ainsi que toutes ses dérivées : ainsi, F est bien définie, et est dans C^∞. De plus, F est 1-périodique. Aussi, F est intégrable sur $[0,1]$: on a en effet, par positivité :

$$\int_0^1 |F| = \int_{\mathbf{R}} |f| < \infty$$

On calcule les coefficients de Fourier de F : pour $m \in \mathbf{Z}$, on a par Fubini :

$$\int_0^1 F(x)e^{-2i\pi mx}\mathrm{d}x = \sum_{n\in\mathbf{Z}} \int_0^1 f(x+n)e^{-2i\pi mx}\mathrm{d}x = \widehat{f}(m)$$

F est de classe C^1, donc le théorème de Dirichlet s'applique, et :

$$\forall x \in [0,1], F(x) = \sum_{m\in\mathbf{Z}} \widehat{f}(m)e^{2i\pi mx}$$

On conclut en appliquant en $x = 0$. Soit, pour $u > 0$, $f_u : x \mapsto e^{-\pi ux^2}$, et soit θ définie sur $\mathbf{R}_+^*$ par :

$$\theta(u) = \sum_{n\in\mathbf{Z}} e^{-\pi n^2 u}$$

Comme f_u est dans $\mathcal{S}(\mathbf{R})$ [8], on en déduit :

$$\theta(u) = \sum_{m\in\mathbf{Z}} \widehat{f_u}(m)$$

Or on a $\widehat{f_u} = \frac{1}{\sqrt{u}} f_{\frac{1}{u}}$ (par un calcul via un changement de variable), et donc :

$$\theta(u) = \frac{1}{\sqrt{u}}\theta\left(\frac{1}{u}\right)$$

- Soit s à droite de 1 : on a :

$$\begin{aligned}
\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) &= \sum_{n=1}^{\infty}\int_0^\infty \pi^{-\frac{s}{2}} t^{\frac{s}{2}} e^{-t} n^{-s}\frac{\mathrm{d}t}{t} && \text{(Fubini)}\\
&= \sum_{n=1}^{\infty}\int_0^\infty u^{\frac{s}{2}} e^{-\pi n^2 u}\frac{\mathrm{d}u}{u} && \text{(changement de variable } t = \pi n^2 u\text{)}\\
&= \int_0^\infty u^{\frac{s}{2}} \underbrace{\left(\sum_{n=1}^{\infty} e^{-\pi n^2 u}\right)}_{:=\widetilde{\theta}(u)}\frac{\mathrm{d}u}{u} && \text{(Fubini)}
\end{aligned}$$

8. En effet, les dérivées de la gaussiennes sont de la forme $H_n(x)e^{-x^2/2}$, où H_n est le n-ème polynôme de Hermite.

On a :

$$\widetilde{\theta}(u) = \frac{\theta(u) - 1}{2}$$

Donc, par l'équation fonctionnelle précédente :

$$\widetilde{\theta}(1/u) = \sqrt{u}\widetilde{\theta}(u) + \frac{1}{2}(\sqrt{u} - 1)$$

Ainsi, on en déduit, toujours pour le même s :

$$\begin{aligned}
\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) &= \int_0^1 u^{\frac{s}{2}}\widetilde{\theta}(u)\frac{\mathrm{d}u}{u} + \int_1^\infty u^{\frac{s}{2}}\widetilde{\theta}(u)\frac{\mathrm{d}u}{u} \\
&= \int_1^\infty u^{-\frac{s}{2}}\widetilde{\theta}(1/u)\frac{\mathrm{d}u}{u} + \int_1^\infty u^{\frac{s}{2}}\widetilde{\theta}(u)\frac{\mathrm{d}u}{u} && \text{(changement de variable)} \\
&= \int_1^\infty \widetilde{\theta}(u)\left(u^{\frac{s}{2}} + u^{\frac{1-s}{2}}\right)\frac{\mathrm{d}u}{u} + \frac{1}{s-1} + \frac{1}{s} && (\star)
\end{aligned}$$

Ainsi, on a une identité valable pour $\mathrm{Re}\,(s) > 1$: mais on vérifie que $s \mapsto \int_1^\infty \widetilde{\theta}(u)\left(u^{\frac{s}{2}} + u^{\frac{1-s}{2}}\right)\frac{\mathrm{d}u}{u}$ est holomorphe sur $\mathbf{C}$: pour cela, il suffit de remarquer que

$$\widetilde{\theta}(u) \leq \sum_{n=1}^\infty e^{-\pi n u} = \frac{e^{-\pi u}}{1 - e^{-\pi u}} = O(e^{-\pi u})$$

Et on conclut par holomorphie sous intégrale. Ainsi, l'équation $(\star)$ est valable à droite de 0 en dehors de 1, et comme elle est symétrique en $s \longleftrightarrow 1 - s$, on a bien :

$$\forall s \in \mathbf{C}, \mathrm{Re}\,(s) \in]0,1[\implies \xi(s) = \xi(1-s)$$

2.6 Moyen & semi : linéarisation d'une EDO, stabilité asymptotique des points d'équ.

Recasages : 215, 220, 221. Référence : Rouvière

Énoncé : Soit $y' = f(y)$ un système différentiel ayant un point d'équilibre en un $0 \in \mathbf{R}^n$. On suppose que f est de classe C^1, et on note $A = \mathrm{d}_0 f$. Alors, si 0 est un point d'équilibre asymptotiquement stable de $z' = Az$, c'en est un de $y' = f(y)$.

Exemples : Pour l'équation du pendule amorti :

$$\ddot{\theta} = -\sin\theta - 2\lambda\dot{\theta} \text{ (avec } 0 < \lambda < 1)$$

Attention : Connaître des résultats où ça ne marche pas ! (exemples dans le cas seulement stables, cas du pendule (asympt stable par le dév avant, mais de linéarisé seulement stable))

Preuve : L'idée est de construire une nouvelle norme pour laquelle les boules forment un système de voisinage asympt stables.

La première partie peut être sautée... Déjà, on commence par remarquer que si l'on note $\lambda_1, \ldots, \lambda_k$ les valeurs propres de A, on a la décomposition de Dunford : $A = D + N$ qui permet d'écrire, pour $t \in \mathbf{R}$, comme D et N commutent :

$$e^{tA} = e^{tD} e^{tN}$$

Or e^{tN} est un polynôme en t. Ainsi, si $x \in \mathbf{R}^n$, on a, pour un polynôme P [9] et en notant $|\cdot|$ la norme euclienne sur $\mathbf{R}^n$:

$$\left|e^{tA} x\right| \leq P(|t|) \left|e^{tD} x\right| \leq P(|t|) \sum_{k=1}^{n} e^{t\mathrm{Re}(\lambda_k)} |x|$$

Donc si $\mathrm{Re}\,(\lambda_k) < 0$ pour tout k, alors 0 est un point d'équilibre asymptotiquement stable. Réciproquement, en partant d'un vecteur propre x de A, on montre que si le point est asympt stable, alors $\mathrm{Re}\,(\lambda_k) < 0$.

À présent, on considère

$$b(x, y) = \int_0^\infty e^{tA} x \cdot e^{tA} y \mathrm{d}t$$

et $q(x) = b(x, x)$. Alors :

- En utilisant l'inég de Cauchy-Schwarz et la majoration précédente, on montre que b est bien définie.
- Par linéarité de l'intégrale, b est une forme bilinéaire, évidemment symétrique.
- b est définie positive : en effet, si $x \neq 0$, alors : $\forall t \geq 0$, $e^{tA} x \cdot e^{tA} x \geq 0$, donc $q(x) \geq 0$, avec égalité si l'intégrande est nulle pp, donc partout par continuité, ie si $x = 0$, ce qui n'est pas vérifié.

9. On peut prendre $P(t) = \sum_{k=0}^{n-1} \frac{t^k}{k!} \|N\|^k$

Ainsi, $\sqrt{q}$ est une norme sur $\mathbf{R}^n$.
On sait, par le théorème de Cauchy-Lipschitz, que l'équation $y' = f(y), y(0) = x$ a une (unique) solution maximale ; sur son intervalle de définition, on a, en utilisant la différentielle d'une forme bilinéaire :

$$\begin{aligned}(q(y))' &= 2b(y, f(y)) \\ &= 2b(y, Ay) + 2b(y, r(y)) \qquad \text{(où } r(y) = f(y) - Ay\text{)}\end{aligned}$$

Or, pour $x \in \mathbf{R}^n$:

$$b(x, Ax) = \int_0^\infty \left(e^{tA}x \cdot \frac{\mathrm{d}}{\mathrm{d}t} e^{tA}x \right) \mathrm{d}t = \frac{1}{2} \int_0^\infty \frac{\mathrm{d}}{\mathrm{d}t} |e^{tA}x|^2 \mathrm{d}t = -\frac{1}{2}|x|^2$$

Donc :

$$q(y)' = -|y|^2 + 2b(y, r(y))$$

Comme $\sqrt{q}$ est une norme sur $\mathbf{R}^n$, elle est équivalente à la norme euclidienne canonique, et on dispose de $C > 0$ tel que $\forall x \in \mathbf{R}^n, -|x|^2 \leq -Cq(x)$.
La différentiabilité de f en 0 (en utilisant la norme $\sqrt{q}$) permet de dire que pour tout $\gamma > 0$, il existe $\alpha > 0$ tel que :

$$q(x) \leq \alpha \implies q(f(x) - Ax) \leq \gamma q(y)$$

Autrement dit :

$$q(x) \leq \alpha \implies -|x|^2 + 2b(x, f(x) - Ax) \leq (2\gamma - C)q(x)$$

Donc si $\beta > 0$, et en choisissant γ tel que $2\gamma - C \leq -\beta$, on dispose de $\alpha > 0$ tel que :

$$q(x) \leq \alpha \implies -|x|^2 + 2b(x, f(x) - Ax) \leq -\beta q(x)$$

Pour $r > 0$, on note E_r l'ellipsoïde $\{x, q(x) < r\}$. Ainsi, si $x \in E_\alpha$, le système $y(0) = x, y' = f(y)$ reste dans E_α : en effet, sinon il le quitterait à un t_0 minimal, on aurait alors $q(y(t_0)) = \alpha$, donc $q(y)'(t_0) \leq -\beta q(y)(t_0) < 0$, ce qui montrerait que $q(y)$ décroît autour de t_0, ce qui est absurde car t_0 est le premier instant à quitter E_α. Ainsi, par le lemme de sortie des compacts, y est définie sur $\mathbf{R}_+$. On a même :

$$q(y)' \leq -\beta q(y) \text{ i.e. } q(y(t)) \leq q(x)e^{-\beta t}$$

Ce qui assure la stabilité asymptotique de 0.

2.7 Moyen & semi-classique : une condition suffisante d'existence de solution de l'équation de Burgers

Référence : Di Menza, p82 Recasages : 214, 222, 267.

Énoncé : Soit $u_0 : \mathbf{R} \to \mathbf{R}$ une fonction de classe C^1. On définit

$$T^\star = \begin{cases} \infty & \text{si } u_0 \text{ est croissante} \\ \inf \frac{-1}{u_0'} = \frac{-1}{\inf u_0'} & \text{sinon} \end{cases}$$

Alors le problème

$$\begin{cases} \partial_t u + u \partial_x u &= 0 & x \in \mathbf{R} \quad t \in \mathbf{R}_+ \\ u(x, 0) &= u_0(x) & x \in \mathbf{R} \end{cases}$$

admet une unique solution de classe C^1 sur $\mathbf{R} \times [0, T^\star[$.

Preuve : On procède par analyse-synthèse.
Analyse : Supposons u solution de l'énoncé, avec $T^\star \neq 0$ (pour éviter les trivialités). On utilise la méthode des caractéristiques. Soit, pour $\xi \in \mathbf{R}$, $C_\xi := \{(x(t), t), x'(t) = u(x(t), t)$ et $x(0) = \xi\}$, qui est bien une courbe par unicité du théorème de Cauchy-Lipschitz. Alors, la fonction $f(t) = u(x(t), t)$ reste constante sur C_ξ : en effet, on a :

$$\frac{\mathrm{d}}{\mathrm{d}t} u(x(t), t) = \partial_t u(x(t), t) + x'(t) \partial_x u(x(t), t) = 0$$

Donc, pour $(t, x(t)) \in C_\xi$, on a : $x'(t) = u(x(t), t) = u_0(\xi)$. Cette équation s'intègre en t, et donne : $x(t) = u_0(\xi)t + \xi$.
À présent, on fixe $(x, t) \in \mathbf{R} \times [0, T^\star[$, et on cherche ξ tel que $(x, t) \in C_\xi$. Cela est équivalent à $x = u_0(\xi)t + \xi$, où encore à :

$$F(x, t, \xi) = 0 \text{ où } F(x, t, \xi) = u_0(\xi)t + \xi - x$$

Synthèse : On commence par montrer qu'avec ce choix de $T^\star$, pour $x \in \mathbf{R}$ et $t < T^\star$, on a :

$$\exists! \xi \in \mathbf{R}, F(x, t, \xi) = 0$$

On a : $\partial_\xi F(x, t, \xi) = u_0'(\xi)t + 1 \geq 1 + \inf(u_0')t$. Or si $t < T^\star$, on dispose de $\alpha > 0$ tel que $1 + \inf(u_0')t = \alpha$, et alors l'existence vient du fait que $F(x, t, \xi)$ tend vers l'infini à l'infini, et l'unicité de l'égalité des accroissements finis.
On note ensuite $\xi(x, t)$ un tel ξ, et on montre que $(x, t) \mapsto \xi(x, t)$ est de classe C^1.
En effet, l'application $\varphi : (x, t, \xi) \mapsto (x, t, F(x, t, \xi))$ est de différentielle inversible, donc par le théorème d'inversion locale, c'est un C^1-difféomorphisme local. Ainsi, $(x, t) \mapsto \xi(x, t)$ est localement de classe C^1 (elle coïncide localement avec $(x, t) \mapsto (\varphi^{-1}(x, t, 0))_3$) ; comme être de classe C^1 est une notion locale, cela prouve bien que ξ est de classe C^1.

Alors la fonction $u : (x, t) \mapsto u_0(\xi(x, t))$ sera solution de l'EDP : en effet, par dérivation des fonctions implicites :

$$\partial_x F(x, t, \xi(x, t)) + (\partial_x \xi(x, t)) \partial_\xi F(x, t, \xi(x, t)) = 0$$

$$\text{donc : } \partial_x \xi(x, t) = -\frac{\partial_x F(x, t, \xi(x, t))}{\partial_\xi F(x, t, \xi(x, t))} = \frac{-1}{u_0'(\xi(x, t))t + 1}$$

$$\text{et } \partial_t \xi(x, t) = \frac{u_0(\xi(x, t))}{u_0'(\xi(x, t))t + 1}$$

Donc on a :

$$\partial_t \xi + u_0(\xi) \partial_x \xi = 0$$

ce qui conclut (en multipliant par $u_0'(\xi(x, t))$).

2.8 Facile & original : un système dynamique discret et son analogue continu : méthode d'Euler pour éq de réaction

(haut) Référence : Cassini, Analyse 1 Recasages : 220, 223, 226

Énoncé : Soit $f : \mathbf{R} \to \mathbf{R}$ de classe C^1 telle que $f(0) = f(1) = 0$ pour $x \in]0,1[$, $-x < f(x) < 0$, et $f'(0) \in]-1,0[$. Alors :

- Soit x la solution de $x' = f(x)$ et $x(0) = x_0 \in]0,1[$. Pour n assez grand, le temps d'atteinte t_n de $\frac{1}{n}$ est bien défini, et :
$$t_n \sim -\frac{\log n}{f'(0)}$$
- Soit (x_n) définie par $x_0 \in]0,1[$ et $x_{n+1} - x_n = f(x_n)$. Le premier instant $\varphi(n) \in \mathbf{N}$ vérifiant $x_{\varphi(n)+1} \leq \frac{1}{n}$ satisfait :
$$\varphi(n) \sim -\frac{-\log n}{\log(1 + f'(0))}$$

On fait continu/discret de chaque côté pour éviter de s'embrouiller, mais les deux se ressemblent beaucoup.
Continu : Soit $x_0 \in [0,1]$. Par Cauchy-Lipschitz, on a existence d'une solution autour de $t = 0$; de plus, par unicité dans Cauchy-Lipschitz, x ne peut prendre la valeur 0 ou 1. Ainsi, par le théorème des valeurs intermédiaires, on en déduit que x est à valeurs dans $]0,1[$; ensuite, comme f est négative, x est décroissante. Si x n'était pas définie sur $\mathbf{R}$, mais seulement sur $]a,b[$, avec $b < \infty$, alors, par décroissance, x aurait une limite en b, qui serait donc dans $[0,1]$: on pourrait alors prolonger x en b (ce prolongement serait de classe C^1 par limite de la dérivée, et vérifierait l'EDO), ce qui contredirait la maximalité. Ainsi x est globale.

x est décroissante minorée, elle converge. De plus, par continuité de f, sa limite ℓ vérifie $x'(t) \longrightarrow f(\ell)$. Si $f(\ell) \neq 0$, alors on a, par intégration des équivalents : $x(t) \sim f(\ell)t$, ce qui est absurde car x est bornée. Ainsi, $\ell = 0$ (le cas $\ell = 1$ étant exclu car x est décroissante). Ainsi, les t_n sont bien définis pour n assez grands.

Comme $x(t) \longrightarrow 0$, on a : $f(x(t)) \sim f'(0)x(t)$. Ainsi, $\frac{x'(t)}{x(t)} \sim f'(0)$ (on utilise ici la non-nullité de $f'(0)$!). Comme la fonction $t \mapsto f'(0)$ n'est pas intégrable, on en déduit, par intégration des équivalents : $\log(x(t)) \sim f'(0)t$.
On a $t_n \longrightarrow 0$, par décroissance de x ; ainsi, on en déduit : $-\log n \sim f'(0)t_n$, i.e. :
$$t_n \sim -\frac{\log n}{f'(0)}$$

Discret : La condition $-x < f(x) < 0$ assure la bonne définition de (x_n). La suite est alors décroissante minorée, et elle converge. Par continuité, on a $f(\ell) = 0$ donc $\ell = 0$: ainsi, $\varphi(n)$ est bien définie, et $\varphi(n) \longrightarrow \infty$. On a aussi $f(x_n) \sim f'(0)x_n$, donc, comme $f'(0) \neq -1$: $\frac{x_{n+1}}{x_n} \simeq 1 + f'(0)$, d'où :
$$\log(x_{n+1}) - \log(x_n) \sim \log(1 + f'(0)) \neq 0$$
Par sommation des équivalents, on en déduit : $\log(x_m) \sim m\log(1 + f'(0))$. Or on a :
$$\log(x_{\varphi(n)}) \leq -\log n < \log(x_{\varphi(n)-1})$$
Comme les deux termes latéraux sont équivalents à $\varphi(n)\log(1 + f'(0))$, celui du milieu aussi, d'où :
$$\varphi(n) \sim -\frac{-\log n}{\log(1 + f'(0))}$$

Remarque : Considérons l'exemple de $f(x) = \eta x(1-x)$, où $0 < \eta < 1$. On obtient alors $f'(0) = \eta$. En particulier, si l'on cherche à approcher le modèle $f(x) = x(1-x)$, l'approximation du schéma d'Euler sera de moins en moins bonne à mesure que η augmente.

2.9 Facile & original : indécomposabilité de la loi de Poisson par les séries entières

(haut) Référence : Queffelec, Analyse complexe

Recasages : 241, 243, 245, 261, 264, 266.

Énoncé : Soit Z une variable aléatoire suivant une loi de Poisson de paramètre λ, soient X et Y deux variables indépendantes à valeurs dans $\mathbf{N}$ telles que $X+Y=Z$; alors X et Y suivent des lois de Poisson.

Preuve : Soit G_Z la série génératrice de Z. On a $G_Z = e^{\lambda(s-1)}$ pour tout $s \in \mathbf{C}$. Alors : $G_Z = G_X \times G_Y$. De plus, par définition, G_X et G_Y se développent en série entière, et les coeffs sont positifs. On a en fait : $\mathbb{P}(X=n)\,\mathbb{P}(Y=0) \leq \mathbb{P}(Z=n) = e^{-\lambda}\frac{\lambda^n}{n!}$: pour $n=0$, on a $\mathbb{P}(Z=0) = \mathbb{P}(X=0)\,\mathbb{P}(Y=0) \neq 0$, donc $\mathbb{P}(Y=0) \neq 0$; donc G_X (et G_Y, de la même manière) sont des séries entières de rayon de convergence infini : ce sont des fonctions entières.

De plus, G_X et G_Y ne s'annulent pas, donc elles s'écrivent e^f et e^g. On a alors $f+g = \lambda(s-1)$ (car $f+g-\lambda(s-1)$ est une fonction continue à valeurs dans $2i\pi\mathbf{Z}$, donc constante ; comme G_X et G_Y sont positives sur $\mathbf{R}_+$, on peut supposer $f(x) \in \mathbf{R}$ pour $x \in \mathbf{R}$; ainsi, $f(x)+g(x) \in \mathbf{R}$ pour $x \geq 0$). De plus, comme $X \leq Z$:

$$e^{Re(f(s))} = |\mathbb{E}\left(s^X\right)| \leq \mathbb{E}\left(|s|^Z\right) = e^{\lambda(|s|-1)}$$

Dès lors, $\Re(f(s)) \leq \lambda(|s|-1) \leq \lambda|s|$. La même inégalité étant vraie pour g, on en déduit :

$$|\Re(f(s))| \leq \lambda|s|$$

On peut montrer qu'alors f et g sont des polynômes de degré 1 : en fait on écrit

$$a_n r^n + 0 = \frac{1}{2\pi}\int_0^{2\pi} (f(re^{i\theta}) + \overline{f(re^{i\theta})})e^{-in\theta}\mathrm{d}\theta$$

et ça conclut.

Remarque : La même prop est vraie pour la loi gaussienne, la preuve se généralise (la difficulté étant dans le fait de montrer que les fonctions caractéristiques sont entières).

2.10 Moyen+ & original : calcul de la somme quadratique de Gauss par transformée de Fourier

(haut) Référence : Hindry ou Zuily-Queffelec Recasages : 236, 239, 241, 246

Énoncé : On calcule

$$\tau_n = \sum_{x \in \mathbf{Z}/n\mathbf{Z}} \zeta^{x^2}$$

(où $\zeta = \exp(\frac{2i\pi}{n})$) On trouve :

$$\tau_n = \frac{1+i^{-n}}{1+i^{-1}}\sqrt{n}$$

Preuve : Soit $n \in \mathbf{N}^*$. On pose, **pour $\mathbf{t} \in [\mathbf{0}, \mathbf{1}[$** :

$$f(t) = \sum_{k=0}^{n-1} \exp\left(\frac{2i\pi(t+k)^2}{n}\right)$$

Alors $\tau_n = f(0)$, qu'on cherche à calculer.

Soit $I_n = \int_{-\infty}^{\infty} \exp\left(\frac{2i\pi t^2}{n}\right) \mathrm{d}t := \lim_{A\to\infty} \int_{-A}^{A} \exp\left(\frac{2i\pi t^2}{n}\right) \mathrm{d}t$. Alors par un changement de variable $t^2 = u$, et une IPP, I_n est bien défini. De plus, on vérifie $I_n = \sqrt{n} I_1$.

Pour calculer $f(0)$, on prolonge f en une fonction 1-péridodique, de classe $\mathcal{C}^\infty$ par morceaux (donc, a fortiori, $\mathcal{C}^1$ par morceaux), et, on peut appliquer le théorème de Dirichlet. On a donc :

$$\sum_{m=-j}^{j} \int_0^1 f(t) e^{-2i\pi m t} \mathrm{d}t \underset{j\to\infty}{\longrightarrow} \frac{f(0)+f(1)}{2} = f(0)$$

Mais on trouve aussi, en calculant la somme en séparant les cas m pair et m impair :

$$\sum_{m=-j}^{j} \sum_{k=0}^{n-1} \int_0^1 e^{\frac{2i\pi(t+k)^2}{n}} e^{-2i\pi m t} \mathrm{d}t \underset{j\to\infty}{\longrightarrow} (1+i^{-n}) I_n$$

On en déduit le résultat.

Remarques : Une autre manière de faire ce calcul de manière algébrique (cf dev alg).
Plein de conséquences : Kronecker-Weber quadratique ($\mathbf{Q}(\sqrt{n}) \subset \mathbf{Q}(\zeta_{8n})$) ; loi de réciprocité quadratique (un peu de travail), on a aussi fait le calcul (non trivial !) de l'intégrale de Fresnel I_1.

2.11 Moyen & classique : Extrema liés, applications

Recasages : 159, 214, 215, 219

Énoncé : Soit V un ouvert de $\mathbf{R}^n$, $a \in U$, $f, g_1, \ldots, g_r$ des fonctions de classe $\mathcal{C}^1$ telles que $(\mathrm{d}g_1(a), \ldots, \mathrm{d}g_r(a))$ est une famille libre. Soit Γ le sous-ensemble de V donné par $\Gamma = \{x \in U, g_i(x) = 0 \forall i\}$. Alors si f admet un extremum sur Γ, il existe (des uniques) $\lambda_1, \ldots, \lambda_r \in \mathbf{R}$ tels que :

$$\mathrm{d}f(a) = \sum \lambda_i \mathrm{d}g_i(a)$$

On en déduit le théorème spectral.

Preuve : On commence par montrer :

lemme : Il existe un ouvert $U \ni a$ inclus dans V et un difféo $\Phi : U \to \Phi(U) \subset \mathbf{R}^n$ tel que

$$\Phi(U \cap \Gamma) = \Phi(U) \times (0^p \times \mathbf{R}^{n-p})$$

preuve : Comme la famille $(\mathrm{d}_a g_1, \ldots, \mathrm{d}_a g_p)$ est libre, on dispose de $\varphi_{p+1}, \ldots, \varphi_n$ telle que $(\mathrm{d}_a g_1, \ldots, \mathrm{d}_a g_p, \varphi_{p+1}, \ldots$ soit une base de $(\mathbf{R}^n)^*$. On pose alors :

$$\Phi : x \longmapsto (g_1(x), \ldots, g_p(x), \varphi_{p+1}(x), \ldots, \varphi_n(x))$$

Alors ce qui précède donne que $\mathrm{d}_a\Phi$ est injective, donc inversible ; ainsi, comme Φ est de classe C^1, on dispose d'un ouvert $U \ni a$ tel que $\Phi : U \to \Phi(U)$ soit un difféo, et ce par le théorème d'inversion locale.
Alors, si $x \in U$, on a $x \in \Gamma \iff \Phi(x) \in 0^p \times \mathbf{R}^{n-p}$.

Une conséquence, c'est que les chemins autour de a dans Γ correspondent, par composition par Φ aux chemins autour de $\Phi(a)$ dans $0^p \times \mathbf{R}^{n-p}$: en particulier, en notant $T_a\Gamma$ les dérivées en 0 des chemins sur Γ autour de a, on a :

$$\forall v \in \mathbf{R}^n, v \in T_a\Gamma \iff \mathrm{d}_a\Phi \cdot v \in 0^p \times \mathbf{R}^{n-p}$$

Ainsi, $T_a\Gamma$ est un espace vectoriel de dimension $n - p$, et on a même :

$$T_a\Gamma = \bigcap_{i=1}^{p} \ker(\mathrm{d}_a g_i)$$

Soit f une fonction comme dans l'énoncé ; si γ est un chemin tracé sur Γ autour de a, alors $f \circ \gamma$ a un extremum local en a : on a donc $(f \circ \gamma)'(0) = 0$, i.e. :

$$T_a\Gamma \subset \ker(\mathrm{d}f)$$

On a donc, en terme d'orthogonalité de formes linéaires :

$$\bigcap_{i=1}^{p} \ker(\mathrm{d}_a g_i) = (\mathrm{Vect}(\mathrm{d}_a g_i))^{\perp} \subset f^{\perp}$$

Ceci prouve, par propriétés de l'orthogonal :

$$\mathrm{Vect}(f) \subset \mathrm{Vect}(\mathrm{d}_a g_i)$$

et cela conclut.

Considérons un espace euclidien (de dim finie), et u une application symétrique ; alors $f(x) = \langle u(x), x\rangle$ admet un maximum global sur le compact $\Gamma = \{\langle x, x\rangle - 1\}$: en ce point x, on dispose de λ tel que $\nabla_x f = \lambda(2x)$. Or, comme u est symétrique, $\nabla_x f = 2u(x)$; ainsi, on vient de prouver que u avait une valeur propre.
On note $F = \text{Vect}(x)$: alors F est u-stable, donc $F^\perp$ est u-stable (car u est symétrique). Ainsi, par récurrence sur la dimension, u est diagonalisable en base orthonormée.

Rq : Une autre propriété sympa (en plus de pleins d'inégalités classiques) : soit $g : \mathbf{R}^n \to \mathbf{R}$ de classe C^1 telle que $\Gamma = g^{-1}(0)$ soit borné, et $d_a g$ est non nul pour tout $a \in \Gamma$. Alors tout hyperplan de $\mathbf{R}^n$ se réalise comme plan tangent à Γ en un point.

2.12 Moyen & classique : théorème d'Ascoli, une application pour un micro Sobolev-Reilich-Kondrachov

Recasages :

- 201 Espaces de fonctions. Exemples et applications.
- 203 Utilisation de la notion de compacité.
- 205 Espaces complets. Exemples et applications.
- 241 Suites et séries de fonctions. Exemples et contre-exemples.

Énoncé : On montre que, si (K, d_K) est un compact, et (F, d_F) est un espace complet, alors pour A une partie de $\mathcal{C}^0(K, F)$, si :

(i) $\forall x \in K, A(x) = \{f(x), f \in A\}$ est relativement compacte dans F.

(ii) A est équi-continue (i.e. : $\forall \varepsilon > 0, \exists \delta > 0, \forall x, y \in K, d_K(x, y) < \delta \implies \forall f \in A, d_F(f(x), f(y)) < \varepsilon)$)

alors A est relativement compacte dans $\mathcal{C}^0(K, F)$.
Application : une injection "Sobolev" : l'injection $H^1(]0, 1[) \hookrightarrow \mathcal{C}^0([0, 1])$ est bien définie, continue et compacte (par Ascoli). On en déduit que $H^1 \hookrightarrow L^2$ est compacte.

Preuve : On considère une suite de fonctions (f_n) dans A, et on lui cherche une valeur d'adhérence. Voilà un résumé de la preuve :

- On montre que X est séparable.
- Étant donnée (x_m) dense dans X, on extrait $(f_{\varphi(n)})$ de (f_n) telle que $\forall m \geq 0, f_{\varphi(n)}(x_m) \longrightarrow f(x_m)$ pour $n \to \infty$ et f une fonction.
- On montre que f se prolonge à X tout entier.
- On montre que $f_{\varphi(n)} \to f$ uniformément sur X.

- Si $N \geq 1$, par compacité de X on peut recouvrir X par un nombre fini de boules de rayon $\frac{1}{N}$: ainsi on dispose de $(y_M^{(N)})_M$. Alors $(y_M^{(N)})_{N,M}$ est une partie dénombrable dense dans X.
- Soit donc $(x_m)_{m\geq 0}$ dense dans X. Par (ii), pour tout $m \geq 0$, on dispose de φ_m extractrice telle que $f_{\varphi_m(n)}(x_m)$ converge (quand $n \to \infty$). On pose alors $\varphi(n) = \varphi_n \circ \ldots \circ \varphi_0(n)$. Cette extractrice convient.
- On a ainsi défini $f : D \to F$, où $D = \{x_m, m \in \mathbf{N}\}$. Soit $\varepsilon > 0$, et $\alpha > 0$ correspondant dans (ii). Alors :
$$\forall x, x' \in D, \forall n \geq 0, d_X(x, x') < \alpha \implies d_F(f_{\varphi(n)}(x), f_{\varphi(n)}(x')) < \varepsilon$$
Ainsi, on a, en passant à la limite :
$$\forall x, x' \in D, \forall n \geq 0, d_X(x, x') < \alpha \implies d_F(f(x), f(x')) \leq \varepsilon$$
Comme ε a été choisi arbitrairement, cela prouve que f est uniformément continue. Comme F est complet et D est dense, on sait que f se prolonge de manière unique en une fonction uniformément continue sur X tout entier, que l'on notera encore f.

- Soit $\varepsilon > 0$, soit $\alpha > 0$ associé dans (ii). On recouvre X par un nombre fini de boules de rayon $\frac{\alpha}{2}$; dans chaque boule B, il y a au moins un x_m car cette suite est dense. On a alors : $B \subset B(x_m, \alpha)$. Ainsi, on a, pour un N, pour des indices $i_1, \ldots, i_N$:

  $$X = \cup_{j=1}^{N} B(x_{i_j}, \alpha)$$

  On sait que $\forall j \leq N, f_{\varphi(n)}(x_{i_j}) \longrightarrow f(x_{i,j})$. Soit n_0 tel que pour $n \geq n_0$, on a :

  $$\forall j \leq N, d_F(f_{\varphi(n)}(x_{i_j}), f(x_{i_j})) \leq \varepsilon$$

  Alors, pour $n \geq n_0$, on a :

  $$\forall x \in X, d_F(f_{\varphi(n)}(x), f(x)) \leq 3\varepsilon$$

  en effet, si $x \in X$, on dispose de i_j tel que $d(x, x_{i_j}) \leq \alpha$, et on conclut par inég. tri.

Pour l'application, il suffit de vérifier que l'image de la boule unité de H^1 dans C^0 est relativement compacte ; en effet, la condition i) est automatique par continuité de $H^1 \hookrightarrow C^0$, et la ii) est une conséquence de $|u(x) - u(y)| \leq \|u'\|_{L^2}\sqrt{|y - x|}$, qui vient de Cauchy-Schwarz.

2.13 Facile & classique : Théorème de Lax-Milgram, une application

Référence : Di Menza p137, et Bernis pour l'application. Recasage : 205, 208, 213, 222.

Bagage :

- Représentation de Riesz.
- Inégalité de Poincaré dans $]0,1[$ (peut se montrer à l'aide des séries de Fourier).
- $\mathcal{D}(]0,1[)$ dense dans $H_0^1(]0,1[)$ (preuve par convolution).

Énoncé : Soit a une forme bilinéaire sur un espace de Hilbert. On suppose que a est continue et coercive, au sens :

$$\exists \alpha > 0, \forall u \in H, a(u,u) \geq \alpha \|u\|^2$$

Alors, si φ est une forme linéaire continue :

$$\exists! u \in H, \forall v \in H, a(u,v) = \varphi(v)$$

Appli : Si $\alpha \in L^\infty([0,1],\mathbf{R})$, avec $\alpha \geq \alpha_{min}$ pp, pour un $\alpha_{min} > 0$, si $f \in L^2([0,1],\mathbf{R})$ et si $\beta \in C^1([0,1],\mathbf{R})$ vérifie $\beta' \leq 2$, alors l'EDP :

$$\begin{cases} (-\alpha u')' + \beta u' + u & = f \\ \quad u(0) = u(1) & = 0 \end{cases}$$

a une unique solution faible (dans $H^1(]0,1[)$).

Preuve : On commence par le théorème de Lax-Milgram. Si $u \in H$, alors par représentation de Riesz, il existe un unique $Au \in H$ tel que :

$$\forall v \in H, a(u,v) = \langle Au, v \rangle$$

Cela définit donc une application $A : H \to H$. Comme φ est continue, il existe un unique $f \in H$ tel que $\varphi(v) = \langle f, v \rangle$ pour tout v : alors la condition cherchée est équivalente à $Av = f$. Ainsi, il suffit de montrer que A est bijectif.
D'abord, A est injectif : en effet, si $Au = 0$, alors $a(u,u) = 0$, donc $u = 0$ par coercivité. On a en fait, par inégalité de Cauchy-Schwarz :

$$\|Au\|\|u\| \geq a(u,u) \geq \alpha \|u\|^2$$

donc $\|Au\| \geq \alpha \|u\|$. De plus, l'opérateur A est continu : en effet,

$$\forall u \in H, \|Au\|^2 = a(u, Au) \leq \|a\|\|u\|\|Au\|$$

donc A est continu, de norme $\leq \|a\|$.
On montre que AH est fermé (dans H) : si $Au_n \longrightarrow v$, alors

$$\|Au_p - Au_q\| \geq \alpha \|u_p - u_q\|$$

ce qui prouve que, comme (Au_n) est de Cauchy, (u_n) aussi, donc elle converge dans H vers un u_∞.
Alors $Au_\infty = v$ par continuité, donc $v \in AH$, et AH est fermé.
Pour terminer, on montre que $(AH)^\perp = 0$: si $w \in (AH)^\perp$, alors $a(w,w) = 0$, donc $w = 0$. Ainsi,

AH est fermé d'orthogonal nul, donc $AH = H$, et A est surjectif.
Ainsi, A est bijectif, ce qui conclut.

Pour l'application : on écrit la formulation faible du problème. Si $v \in H_0^1(]0,1[)$, alors :

$$\langle (-\alpha u')' + \beta u' + u, v\rangle = \langle \alpha u', v'\rangle + \langle \beta u', v\rangle + \langle u, v\rangle$$

(les crochets sont des crochets L^2).

On définit

$$a : \begin{array}{rcl} H_0^1(]0,1[)^2 & \longrightarrow & H_0^1(]0,1[) \\ (u,v) & \longmapsto & \langle \alpha u', v'\rangle + \langle \beta u', v\rangle + \langle u, v\rangle \end{array}$$

Alors, on vérifie que a est bilinéaire, et continue par définition de la norme H^1. On vérifie enfin que a est coercive : on a en effet, pour $u \in \mathcal{D}(]0,1[)$ [10] :

$$\begin{aligned} \langle \beta u', u\rangle &= \int_0^1 \beta (u'u) \\ &= -\int_0^1 \beta' \frac{u^2}{2} \quad \text{(IPP)} \quad = -\langle \frac{\beta'}{2}, u^2\rangle \end{aligned}$$

Dès lors, par continuité en u, cette identité est vraie pour $u \in H_0^1(]0,1[)$ (on utilise ici la densité de $C^\infty(]0,1[)$ dans $H_0^1(]0,1[)$). Or on a : $-\beta'/2 \geq -1$, et donc, par positivité : $\langle \beta u', u\rangle \geq -\langle u', u'\rangle$. On en déduit :

$$\forall u \in H_0^1(]0,1[), a(u,u) \geq \langle \alpha u', u'\rangle \geq \alpha_{min}\langle u', u'\rangle$$

Or, l'inégalité de Poincaré affirme qu'il existe $C > 0$ tq $\langle u', u'\rangle \geq C\|u\|^2$, ce qui achève de prouver la coercivité.
Ainsi, le théorème de Lax-Milgram s'applique pour a et $\varphi(v) = \langle f, v\rangle$, et on conclut.

10. fonctions C^∞ à support compact

2.14 Moyen & semi-original : Résolution d'une EDP par méthode variationnelle

Réf : Ciarlet ? Recasages : 213, 219, 222, 229, 253
On peut faire seulement le premier résultat, avec les deux trucs admis ça tient. Sinon il y a peut-être des applications plus simples.

Énoncé : Si H est un espace de Hilbert séparable et $J : H \to \mathbf{R}$ est continue, convexe, et coercive (i.e. : $J(x) \underset{\|x\|\to\infty}{\longrightarrow} +\infty$), alors elle atteint son minimum.
Puis on prouve le résultat suivant :
Si $f \in L^2(0,1)$, $\phi : \mathbf{R} \to \mathbf{R}_+$ est strictement convexe et de classe C^1, alors l'équation

$$-u'' + \phi'(u) = f$$

a une solution $u \in H_0^1(0,1) \cap H^2(0,1)$ (et on peut montrer qu'elle est unique mais c'est plus difficile).

Preuve : Soit une telle fonction J, et (x_n) une suite minimisante (*i.e.* $J(x_n) \longrightarrow \inf J$). Comme J est coercive, (x_n) est bornée (par l'absurde). Par un théorème d'analyse fonctionnelle, elle admet une valeur d'adhérence faible [11]. On la note $x_\star$. On montre que $J(x_\star) = \inf J$; soient $\alpha = \inf J$ et $\varepsilon > 0$. On définit $C_\varepsilon = J^{-1}(]-\infty, \ell_\varepsilon])$, avec $\ell_\varepsilon = \begin{cases} \alpha + \varepsilon & \text{si } \alpha > -\infty \\ -\frac{1}{\varepsilon} & \text{sinon} \end{cases}$ (je ne vois pas comment montrer $\alpha \neq -\infty$ a priori...).
Alors C_ε est un convexe (par convexité de J) et est un fermé (fort)(par continuité de J). De plus, pour n assez grand, on a $x_n \in C_\varepsilon$; par un corollaire de la projection sur convexe fermé [12], on en déduit que $x_\star \in C_\varepsilon$.
Cela étant vrai pour tout $\varepsilon > 0$, on en déduit que $J(x_\star) = \alpha$, en particulier $\alpha \neq -\infty$, et le minimum est bien atteint.

Pour l'application à l'EDP : je pose

$$\begin{aligned} J : H_0^1(0,1) &\longrightarrow \mathbf{R} \\ u &\longmapsto \int_0^1 (\frac{u'^2}{2} + \phi(u) - fu) \end{aligned}$$

Alors J est convexe : en effet, $u \mapsto \int_0^1 u'^2 + \phi(u)$ est convexe par somme de telles fonctions, et $u \mapsto \int_0^1 fu$ est linéaire, donc son opposé est convexe.
J est coercive car comme ϕ est positive, on a $J(u) \geq \frac{1}{2}\|u'\|_{L^2}^2 - \langle f, u\rangle_{L^2}$, qui tend vers $+\infty$ quand $\|u\|_{H^1} \to \infty$ (parce que $\|u'\|_{L^2} \geq C\|u\|_{H^1}$ pour un $C > 0$ par l'inégalité de Poincaré).
Enfin, on montre que J est différentiable. Soit $v \in H_0^1(0,1)$; on a, par inégalité triangulaire et inégalité des accroissements finis :

$$\|\phi(u+v) - \phi(u) - v\phi'(u)\|_\infty \leq 2\|\phi'(u)\|_\infty \|v\|_\infty$$

Or $\|v\|_\infty \leq \|v\|_{H^1}$ donc :

$$\left\| \frac{\phi(u+v) - \phi(u) - v\phi'(u)}{\|v\|_{H^1}} \right\|_\infty \leq 2\|\phi'(u)\|_\infty$$

11. Pour montrer ça, on utilise la séparabilité de H, et l'extraction diagonale sur les $(\langle x_n, e_m\rangle)_{n\in\mathbf{N}}$ pour (e_m) une base hilbertienne
12. Pour le démontrer, notant p la projection, on a $\|x_\star - p(x_\star)\|^2 = \lim\langle x_\star - p(x_\star), x_n - p(x_\star)\rangle$, et on conclut car $\langle x_\star - p(x_\star), x_n - p(x_\star)\rangle \leq 0$ pour n assez grand (tel que $x_n \in C_\varepsilon$) (faire un dessin)

De plus, on a, pour tout x tel que $v(x) \neq 0$:

$$\left| \frac{\phi((u+v)(x)) - \phi(u(x)) - v(x)\phi'(u(x))}{\|v\|_{H^1}} \right| \leq \left| \frac{\phi((u+v)(x)) - \phi(u(x)) - v(x)\phi'(u(x))}{v(x)} \right|$$

Et cette quantité tend vers 0 quand $\|v\|_\infty \longrightarrow 0$. Ainsi, ce qui précède permet, de démontrer, par le théorème de convergence dominée :

$$\int_0^1 \frac{\phi(u+v) - \phi(u) - v\phi'(u)}{\|v\|_{H^1}} \underset{\|v\|_{H^1} \to 0}{\longrightarrow} 0$$

Ainsi, comme les deux autres membres sont quadratiques ou linéaires, on en déduit que J est différentiable, et :

$$\forall u, v \in H_0^1(0,1),\ \mathrm{d}_u J(v) = \int_0^1 (u'v' + \phi'(u)v - fv)$$

On peut conclure : comme J vérifie les hypothèses du résultat, elle admet un minimum $u \in H_0^1(0,1)$. Celui-ci vérifie donc $\forall v \in H_0^1(0,1),\ \mathrm{d}_u J(v) = 0$, autrement dit :

$$-u'' + \phi'(u) = f$$

On en déduit que $u'' \in L^2$ (car $f \in L^2$ et $\phi'(u) \in L^\infty(0,1) \subset L^2(0,1)$).

2.15 Moyen & semi-original : Théorème de Bohr-Mollerup

Recasages : 229, 253, 265

Énoncé : On montre que Γ est l'unique fonction $f :]0, \infty[\to]0, \infty[$ vérifiant :

- $f(1) = 1$.
- $\forall x > 0, f(x+1) = xf(x)$.
- f est $\log$-convexe.

Application : formule de Legendre :

$$\Gamma(x) = \frac{2^{x-1}}{\sqrt{\pi}} \Gamma\left(\frac{x}{2}\right) \Gamma\left(\frac{x+1}{2}\right)$$

Preuve : Déjà, on vérifie que Γ vérifie ces trois propriétés : déjà, on a : $\Gamma(1) = \int_0^\infty e^{-t} \mathrm{d}t = 1$; ensuite, une ipp donne l'équation fonctionnelle. Enfin, on montre que Γ est $\log$-convexe ; soit $\lambda \in]0, 1[$, $x, y \in]0, \infty[$, on a :

$$\begin{aligned}
\Gamma(\lambda x + (1-\lambda)y) &= \int_0^\infty t^{\lambda x + (1-\lambda)y} e^{-(\lambda x + (1-\lambda)y)t} \frac{\mathrm{d}t}{t} \\
&= \int_0^\infty \left(t^x e^{-xt}\right)^\lambda \left(t^y e^{-yt}\right)^{1-\lambda} \frac{\mathrm{d}t}{t} \\
&\leq \left(\int_0^\infty t^x e^{-x} \frac{\mathrm{d}t}{t}\right)^\lambda \left(\int_0^\infty t^y e^{-yt} \frac{\mathrm{d}t}{t}\right)^{1-\lambda} \qquad \text{Hölder pour la mesure } \frac{\mathrm{d}t}{t} \\
&= \Gamma(x)^\lambda \Gamma(y)^{1-\lambda}
\end{aligned}$$

Ainsi, la fonction Γ vérifie bien les trois hypothèses. Soit f une fonction vérifiant les trois hypothèses. On a alors, pour n entier naturel > 1, pour $x \in]0, \infty[$, en appliquant l'inégalité des pentes à $\log(f)$ entre $[n-1, n]$, $[n, n+x]$ et $[n, n+1]$, on a :

$$\frac{\log f(n) - \log f(n-1)}{1} \leq \frac{\log f(x+n) - \log f(n)}{x} \leq \frac{\log f(n+1) - \log f(n)}{1}$$

En utilisant les deux premières hypothèses, on a : $\forall n > 0, f(n) = (n-1)!$. Ainsi, notre inéquation devient :

$$\frac{(n-1)^x (n-1)!}{\prod_{k=0}^{n-1}(x+k)} \leq f(x) \leq \frac{n^x (n-1)!}{\prod_{k=0}^{n-1}(x+k)}$$

Les deux termes qui encadrent sont équivalents car $n^x \sim (n-1)^x$: ainsi, ils convergent tous deux vers $f(x)$. Mais ces termes ne dépendent pas de f, donc comme Γ vérifie aussi les hypothèses, ils tendent aussi vers Γ. On a donc :

$$\forall x \in]0, 1], f(x) = \Gamma(x) = \lim_{n \longrightarrow \infty} \frac{n^x (n-1)!}{\prod_{k=0}^{n-1}(x+k)}$$

Par l'hypothèse 2, on en déduit immédiatement que $f = \Gamma$.

Pour l'application : notons f le terme de droite. f est log-convexe par produit de termes log-convexes. De plus, on a :

$$\begin{aligned}\Gamma\left(\frac{1}{2}\right) &= \int_0^\infty \sqrt{x}e^{-x}\frac{\mathrm{d}x}{x} \\ &= \int_0^\infty ue^{-u^2}2\frac{\mathrm{d}u}{u} = \sqrt{\pi}\end{aligned}$$

Ce qui prouve que $f(1) = 1$. Enfin, on a :

$$f(x+1) = \frac{2^x}{\sqrt{\pi}}\Gamma\left(\frac{x+1}{2}\right)\Gamma\left(\frac{x}{2}+1\right) = f(x)$$

(car Γ vérifie la deuxième hypothèse). Cela conclut : par unicité, la formule de Legendre est montrée.

2.16 Moyen & classique : théorème ergodique de Von Neumann

Référence : Beck, Malick, Peyré : objectif agrégation. Recasages : 205, 213, 226.

Énoncé : Soit H un espace de Hilbert, T un endomorphisme continu de H de norme ≤ 1. Soit p le projecteur orthogonal sur $\ker(I-T)$. Alors, quand $n \longrightarrow \infty$:

$$\forall x \in H,\ \frac{1}{n+1}\sum_{k=0}^{n} T^k(x) \longrightarrow p(x)$$

Application : si $f \in L^2_{per}(\mathbf{R}/\mathbf{Z})$ et si $\alpha \notin \mathbf{Q}$, on a la convergence en norme L^2 :

$$\frac{1}{n}\sum_{k=0}^{n-1} f(\cdot + k\alpha) \longrightarrow \int_0^1 f(x)\mathrm{d}x$$

Preuve : Comme T est de norme ≤ 1, si $x \neq 0$, par Cauchy-Schwarz, on a $\langle x, Tx\rangle \leq \|x\|^2$ avec égalité ssi $Tx = x$. Ainsi :

$$Tx = x \iff \langle Tx, x\rangle = \|x\|^2 \iff \langle x, T^\star x\rangle = \|x\|^2 \iff T^\star x = x$$

Où on a utilisé le fait que $\|T^\star\| \leq 1$ car il vaut $\|T\|$.
Ainsi, $\ker(I-T) = \ker(I-T^\star) = \ker((I-T)^\star)$. Or on a $\ker(u^\star)^\perp = \overline{\mathrm{Im} u}$ pour u opérateur (en effet, $\ker(u^\star) = (\overline{\mathrm{Im} u})^\perp$.). Ainsi, on a : $\ker(I-T)^\perp = \overline{\mathrm{Im}(I-T)}$.
La convergence est vraie si $x \in \ker(T-I)$ car la suite est alors constante égale à $p(x)$. Elle est vraie si $x \in \mathrm{Im}(I-T)$: en effet, dans ce cas la somme se téléscope.

Soit $x = p(x) + x_\perp \in H$, et soit $\varepsilon > 0$. On dispose de $y \in \mathrm{Im}(I-T)$ tel que $\|x_\perp - y\| \leq \varepsilon$. Alors on a, par linéarité, pour $n \geq 0$:

$$\frac{1}{n+1}\sum_{k=0}^{n} T^k(x) = p(x) + \frac{1}{n+1}\sum_{k=0}^{n} T^k(y) + \frac{1}{n+1}\sum_{k=0}^{n}(T^k(x_\perp) - T^k(y))$$

Or : $\|T^k(x_\perp) - T^k(y)\| \leq \|T^k\|\varepsilon \leq \varepsilon$. Soit N tel que pour $n \geq N$, on ait $\|\frac{1}{n+1}\sum_{k=0}^{n} T^k(y)\| \leq \varepsilon$. Alors, pour $n \geq N$, on a directement :

$$\|\frac{1}{n+1}\sum_{k=0}^{n} T^k(x) - p(x)\| \leq 2\varepsilon$$

Ce qui conclut.

Pour l'application, on pose $Tf : x \mapsto f(x+\alpha)$. Alors le n-ème coeff de Fourier de Tf vérifie : $c_n(Tf) = e^{-2i\pi n\alpha}c_n(f)$; ainsi, si $\alpha \notin \mathbf{Q}$, $\ker(I-T)$ est l'espace des fonctions constantes pp. On en déduit le résultat.

2.17 Moyen & semi-classique : théorème de Müntz

Référence : Gourdon analyse (et Gourdon algèbre ou Cassini pour le déterminant de Cauchy) Recasages : 152, 161, 201, 209, 213, 234.

Énoncé : Soit (α_n) une suite à termes positifs, strictement croissante, avec $\alpha_0 = 0$ et telle que $\lim_n(\alpha_n) > 1$. Alors $F = \mathrm{Vect}(x^{\alpha_n})$ est dense dans $\mathscr{C}^0([0,1], \mathbf{R})$ ssi $\sum \frac{1}{\alpha_n}$ diverge.

Commentaire : Il faut moduler le développement selon la leçon :

- pour les déterminants, insister sur la place de déterminants (de Gram, de Cauchy) (et éventuellement seulement faire L^2).
- pour les distances d'un euclidien, insister sur le fait que les déterminants nous permettent de faire des calculs de distances (et éventuellement seulement faire L^2).
- pour les espaces de fonctions/approx de fonctions, insister sur le passage L^2/C^0, et comment le gain de structure de L^2 a été profitable.

Preuve : On commence par trouver une CNS pour que F soit dense dans $L^2([0,1])$.
Par le théorème de Weierstrass (polyomial), il suffit de montrer que pour $m \geq 0$, notant $F_n = \mathrm{Vect}(x^{\alpha_1}, \dots x^{\alpha_n})$, on a :

$$d(x^m, F_n) \underset{n\to\infty}{\longrightarrow} 0$$

Or, par les déterminants de Gram, on a :

$$d(x^m, F_n)^2 = \frac{\Delta(x^{\alpha_1}, \dots, x^{\alpha_n}, x^m)}{\Delta(x^{\alpha_1}, \dots, x^{\alpha_n})}$$

avec $\Delta(u_1, \dots, u_k) = \begin{vmatrix} \langle u_1, u_1\rangle & \dots & \langle u_1, u_k\rangle \\ \vdots & & \vdots \\ \langle u_k, u_1\rangle & \dots & \langle u_k, u_k\rangle \end{vmatrix} = \det(\langle u_i, u_j\rangle)$.
Or on a aussi, par déterminant de Cauchy : **(à admettre éventuellement !)** :

$$\det\left(\frac{1}{a_i + b_j}\right) = \frac{\prod_{i<j}(a_j - a_i)(b_j - b_i)}{\prod_{i,j}(a_i + b_j)}$$

Donc :

$$\Delta(x^{\alpha_1}, \dots, x^{\alpha_n}) = \frac{\prod_{i<j}(\alpha_j - \alpha_i)^2}{\prod_{i,j}(\alpha_i + \alpha_j + 1)}$$

et :

$$\Delta(x^{\alpha_1}, \dots, x^{\alpha_n}, x^m) = \frac{\prod_{i<j}(\alpha_j - \alpha_i)^2 \times \prod_i (m - \alpha_i)^2}{\prod_{i,j}(\alpha_i + \alpha_j + 1) \times \prod_i(\alpha_i + m + 1)^2 \times (2m+1)}$$

Donc :

$$d(x^m, F_n) = \frac{1}{\sqrt{2m+1}} \prod_{i=1}^n \frac{|\alpha_i - m|}{\alpha_i + m + 1} = \frac{1}{\sqrt{2m+1}} \prod_{i=1}^n \left|1 - \frac{2m+1}{\alpha_i + m + 1}\right|$$

et ce dernier terme tend vers 0 ssi $\sum \frac{1}{\alpha_n}$ diverge.
En distinguant les cas (α_n) bornée et non bornée, on montre facilement le résultat pour L^2.

En général, on a $\mathrm{Vect}(x^{\alpha_n - 1})$ dense dans L^2 ; ainsi, si P est un polynôme, on prend g proche de P dans ce vect, puis on prend la primitive h de g qui vaut $P(0)$ en 0 (cela est possible car $\alpha_0 = 0$). Alors $h - P$ est uniformément petit par Cauchy-Schwarz (ou : Sobolev !). En résumé, on utilise la suite d'injections : $H^1 \hookrightarrow C^0 \hookrightarrow L^2$.

2.18 Moyen & original : Rolle et polynômes

Réf : Chambert-Loir Analyse 2.

Énoncé : Soit $P = a_nX^n + \ldots + a_0$ et Q deux polynômes scindés sur $\mathbf{R}$. Alors :

(i) Le polynôme $R(X) = a_0Q(X) + a_1Q'(X) + \ldots + a_nQ^{(n)}(X)$ est scindé sur $\mathbf{R}$.

(ii) Si les racines de Q ne sont pas dans $[0, \deg(P)]$, alors $T(X) = a_0Q(0) + a_1Q(1)X + \ldots + a_nQ(n)X^n$ est scindé sur $\mathbf{R}$.

Preuve

(i) Notant ∂ l'opérateur de dérivation, on a : $R = [P(\partial)](Q)$. Commençons par le cas $P = X - \alpha$. On doit montrer que si Q est scindé sur $\mathbf{R}$, alors $Q' - \alpha Q$ aussi. On a, notant $f(x) = Q(x)e^{-\alpha x}$:

$$f'(x) = e^{-\alpha x}(Q'(x) - \alpha Q(x))$$

Ainsi, les racines de $Q' - \alpha Q$ sont exactement les zéros de la dérivée de $Q(x)e^{-\alpha x}$, et la multiplicité de $Q' - \alpha Q$ est celle de f (en tant que fonction analytique) moins un.
FAIRE UN DESSIN DE LA PREUVE

Soit m le degré de Q, et $\lambda_1 < \ldots < \lambda_k$ ses racines, avec multiplicités $m_1, \ldots, m_k$, avec $\sum_{i=1}^k m_i = m$. Notons $f(x) = Q(x)e^{-\alpha x}$. Alors $f^{(m_i)}(\lambda_i) = 0$ pour tout i, donc on a au moins les λ_i zéros de f' avec multiplicité au moins $m_i - 1$, donc $Q' - \alpha Q$ a au moins $\sum_{i=1}^k (m_i - 1) = m - k$ zéros comptés avec multiplicité. Pour montrer que $Q' - \alpha Q$ est scindé sur $\mathbf{R}$, il suffit, par degré, de trouver k autres racines.
On a $f(\lambda_1) = f(\lambda_2)$ donc par le théorème de Rolle, il existe $\mu_1 \in]\lambda_1, \lambda_2[$ tel que $f'(\mu_1) = 0$. En reproduisant, on trouve ainsi $k - 1$ racines réelles.
On peut alors conclure de deux manières : la première, c'est que si S est un polynôme réel ayant $\deg(S) - 1$ racines réelles (comptées avec multiplicité), alors il est scindé sur $\mathbf{R}$. La seconde, c'est en appliquant le théorème de Rolle entre $-\infty$ et λ_1 (ou entre λ_n et $+\infty$) selon le signe de α.
Ainsi, on a que $[(X - \alpha)(\partial)]Q$ est scindé lorsque Q est scindé. Comme P est scindé, on peut écrire $P = a_n \prod_\alpha (X - \alpha)$, et on a alors le résultat par récurrence sur $n = \deg(P)$.

(ii) Si $Q(X) = X - \alpha$, on a :

$$\begin{aligned} T(X) &= \sum_{i=0}^n (i - \alpha)a_iX^i \\ &= XP'(X) - \alpha P(X) \end{aligned}$$

Ainsi, si l'on note D l'application linéaire sur $\mathbf{R}[X]$ donnée par $D(P) = XP'$, on a, pour $i \geq 0$: $D(X^i) = iX^i$, et donc, si $Q(X) = \sum_{k=0}^m b_kX^k$, on en déduit :

$$\begin{aligned} T(X) &= \sum_{i=0}^n a_iQ(i)X^i \\ &= \sum_{i=0}^n \sum_{k=0}^m a_ib_ki^kX^i \\ &= \sum_{i=0}^n \sum_{k=0}^m a_ib_kD^k(X^i) \\ &= Q(D)(P) \end{aligned}$$

On est donc ramené au cas $Q(X) = X - \alpha$, où $\alpha \notin [0, n]$. On a alors :

$$T(X) = XP'(X) - \alpha P(X)$$

Notons $\xi_1 < \ldots < \xi_l$ les racines de P, de multiplicités $n_1, \ldots, n_l$. Alors chaque ξ_j est racine de T avec multiplicité $n_j - 1$ (pas racine si $m_j = 1$), ce qui donne donc $n - l$ racines pour T ; de plus, si 0 est racine de P, alors 0 est racine de T pour la même multiplicité : on en a donc $n - l + 1$. Ainsi, pour conclure, il suffit donc d'exhiber l (ou $l - 1$ si $P(0) = 0$) racines distinctes des ξ_j.
Si $P(x) = 0$, alors $T(x) = 0 \iff f(x) := \frac{xP'(x)}{P(x)} = \alpha$. Ainsi, on est amené à étudier la fonction f. On a :

$$\begin{aligned} f(x) &= x \sum_{j=1}^{l} \frac{n_j}{x - \xi_j} \\ &= \sum_{j=1}^{l} n_j \left(1 + \frac{\xi_j}{x - \xi_j}\right) \\ &= n + \sum_{j=1}^{l} \frac{n_j \xi_j}{x - \xi_j} \end{aligned}$$

Ainsi :

$$f(x) = \alpha \iff g(x) := \sum_{j=1}^{l} \frac{n_j \xi_j}{x - \xi_j} + (n - \alpha) = 0$$

La fonction g est continue sur $\mathbf{R} \backslash \{\xi_j\}$, elle tend vers $n - \alpha$ en les deux infinis, et elle vérifie *DESSIN* :

$$\forall j, \lim_{x \to \xi_j^+} g(x) = \begin{cases} +\infty & \text{si } \xi_j > 0 \\ -\infty & \text{si } \xi_j < 0 \\ n - \alpha & \text{si } \xi_j = 0 \end{cases} = - \lim_{x \to \xi_j^-} g(x)$$

En dessinant le graphe de g, on trouve le bon nombre de racines, en allant les chercher autour de 0 si $\alpha < 0$, et autour de $+\infty$ si $n - \alpha < 0$. Cela permet de conclure.

2.19 Difficile & semi : Théorème taubérien de Littlewood

Référence : Choimet & Queffélec, Gourdon analyse.

Long : il faut admettre le :
Lemme admis : Si $\varphi : [0,1] \to \mathbf{C}$ est une fonction continue par morceaux, alors :

$$(1-x)\sum_{n=0}^{\infty} x^n \varphi(x^n) \underset{x\to 1^-}{\longrightarrow} \int_0^1 \varphi$$

Énoncé : Soit (a_n) une suite réelle telle que (na_n) est bornée. On suppose

$$\sum_{k=0}^{\infty} a_n x^n \underset{x\to 1^-}{\longrightarrow} \ell$$

alors $\sum a_n$ converge et $\sum_{n=0}^{\infty} a_n = \ell$.

Preuve : On note E l'ensemble des fonctions $\varphi : [0,1] \to \mathbf{R}$ telles que $\sum a_n x^n$ converge pour tout $x \in [0,1[$ et $\sum_{n=0}^{\infty} a_n x^n \underset{x\to 1^-}{\longrightarrow} \ell\varphi(1)$.
Alors E contient les fonctions polynomiales nulles en 0 : en effet, on vérifie que pour $p \geq 1$, $x \mapsto x^p \in E$, et on conclut par linéarité.
On note $S_N = \sum_{n=0}^{N} a_n$, et g la fonction indicatrice de $[e^{-1}, 1]$. Alors :

$$S_N = \sum_{n=0}^{\infty} a_n g(x_N^n)$$

où g est la fonction indicatrice de $[e^{-1}, 1]$ (**dessin**), et $x_N = e^{-\frac{1}{N}}$. Alors, si l'on montre que $g \in E$, on aura :

$$\lim_{N\to\infty} \sum_{n=0}^{\infty} a_n g(x_N^n) = \ell g(1) = \ell$$

ce qui concluera (le premier terme étant exactement $\lim S_N$).
On cherche à approcher g par un polynôme ; on veut que, tout comme g, une approx fixe 0 et 1. On pose donc : $g(x) = x + x(1-x)h(x)$ avec $h(x) = \begin{cases} -\frac{1}{1-x} & \text{si } x < e^{-1} \\ \frac{1}{x} & \text{si } x \geq e^{-1} \end{cases}$
Pour un polynôme $P(x) = x + x(1-x)Q(x)$, avec Q un autre polynôme, on a :

$$\begin{aligned}\sum_{n=0}^{\infty} |a_n||g(x^n) - P(x^n)| &= \sum_{n=0}^{\infty} |a_n| x^n (1-x^n)|h(x^n) - Q(x^n)| \\ &\leq \sum_{n=0}^{\infty} |na_n|(1-x)x^n|h(x^n) - Q(x^n)|\end{aligned}$$

(en vertu de l'inégalité $1 - x^n \leq n(1-x)$ [13]) Comme (na_n) est bornée, on dispose de $C > 0$ tel que $|na_n| \leq C$ pour tout n. On a donc :

$$\limsup_{x\to 1} \sum_{n=0}^{\infty} |a_n||g(x^n) - P(x^n)| \leq C \limsup_{x\to 1} (1-x)\sum_{n=0}^{\infty} x^n |h(x^n) - Q(x^n)|$$

Rappelons le lemme, et concluons le théorème : soit $\varepsilon > 0$, soit Q un polynôme tel que $\int_0^1 |Q-h| \leq \varepsilon$. Un tel polynôme existe par densité des polynômes dans $L^1([0,1])$. Alors :

$$\limsup_{x\to 1} \sum_{n=0}^{\infty} |a_n||g(x^n) - P(x^n)| \leq C\varepsilon$$

13. par formule de Bernoulli, ou par convexité de $x \mapsto x^n$

Donc pour un certain $\eta > 1$, on a :

$$\forall x \in [1-\eta, 1[, \left| \sum_{n=0}^{\infty} a_n g(x^n) - \sum_{n=0}^{\infty} a_n Q(x^n) \right| \leq 2C\varepsilon$$

Or $Q \in E$ donc pour $x \geq 1 - \eta'$ (avec $\eta' > \eta$ relatif à Q), on a :

$$\forall x \in [1-\eta, 1[, \left| \sum_{n=0}^{\infty} a_n g(x^n) - \ell \right| \leq (2C+1)\varepsilon$$

ce qui montre bien $g \in E$, cqfd.

Pour le lemme : il suffit, comme dans la preuve de la convergence des sommes de Riemann, de le faire pour les fonctions indicatrices d'intervalles ; en l'occurence, ici, les $\mathbf{1}_{[0,b]}$ $(0 < b < 1)$ suffisent. On a alors, pour $x \in]0, 1[$ (attention, $\log(x) < 0$! !) :

$$\sum_{n=0}^{\infty} x^n (1-x) \mathbf{1}_{[0,b]}(x^n) = \sum_{n=\lfloor \frac{\log b}{\log x} \rfloor + 1}^{\infty} x^n (1-x) = x^{\lfloor \frac{\log b}{\log x} \rfloor + 1} \longrightarrow b$$

Remarque : L'énoncé est faux sans hypothèse sur (a_n) : prendre $a_n = (-1)^n$ pour s'en rendre compte.

2.20 Moyen & semi-classique : Étude des zéros de l'EDO de Sturm-Liouville.

Référence : Berthelin, chapitre 8, avec le dernier exercice pour la fin.
Recasages : 204, 220, 221, 228

Énoncé : Soient I un intervalle d'intérieur non vide de $\mathbf{R}$, et les fonctions x et y non nulles, solutions des équations différentielles linéaires :

$$\begin{cases} (a(t)x')' & +r(t)x & = 0 \\ (b(t)y')' & +s(t)y & = 0 \end{cases}$$

avec a, b de classe C^1 sur I, et r et s continues. On suppose que $r \leq s$, et $0 < b \leq a$ sur I. Alors :

- Les zéros de x sont isolés dans I.
- Si $t_1 < t_2$ sont deux zéros consécutifs de x, et si x et y ne sont pas proportionnelles sur $]t_1, t_2[$, alors y a au moins un zéro sur $]t_1, t_2[$.

Application : Soit y solution de $y'' + ty = 0$ sur $\mathbf{R}$. Alors y a au plus un zéro sur $\mathbf{R}_-$, et en a une infinité sur $]0, \infty[$. De plus, notant a_n le nombre de zéros de y sur $]0, n[$, on a :

$$a_n \sim \frac{2}{3\pi} n^{3/2}$$

Preuve : On commence par montrer que les zéros de x sont isolés. Supposons qu'il existe une suite (t_n) de zéros de x telle que $t_n \longrightarrow t_\infty$. Alors par continuité, $x(t_n) \longrightarrow x(t_\infty)$, donc $x(t_\infty) = 0$. On a de plus :

$$0 = \frac{x(t_\infty) - x(t_n)}{t_\infty - t_n} \longrightarrow x'(t_\infty)$$

ainsi, on a $x(t_\infty) = x'(t_\infty) = 0$: par le théorème de Cauchy-Lipschitz, $x = 0$: absurde.

Passons au deuxième point. On suppose que y ne s'annule pas sur $]t_1, t_2[$. Soit W une variante du wronskien, "normalisé", défini sur $]t_1, t_2[$:

$$W = \frac{x}{y}(ax'y - bxy')$$

On a alors :

$$\begin{aligned} W' &= \frac{x}{y}((ax')'y + ax'y' - (by')'x - by'x') + \frac{x'y - xy'}{y^2}(ax'y - bxy') \\ &= \frac{x}{y}(-sxy + ax'y' + rxy - by'x') + ax'^2 - \frac{bxx'y'}{y} - \frac{bxx'y'}{y} + \frac{bx^2y'^2}{y^2} \\ &= x^2(s-r) + \frac{b}{y^2}((xy')^2 - 2xx'yy' + (x'y)^2) + (a-b)(x')^2 \\ &= x^2(s-r) + \frac{b}{y^2}(xy' - x'y)^2 + (a-b)(x')^2 \end{aligned}$$

On a donc, pour $\varepsilon > 0$ petit :

$$W(t_2 - \varepsilon) - W(t_1 + \varepsilon) = \int_{t_1+\varepsilon}^{t_2-\varepsilon} x^2(s-r)\mathrm{d}t + \int_{t_1+\varepsilon}^{t_2-\varepsilon} \frac{b}{y^2}(xy' - x'y)^2\mathrm{d}t + \int_{t_1+\varepsilon}^{t_2-\varepsilon} (a-b)(x')^2\mathrm{d}t$$

Les deux termes latéraux tendent vers les intégrales sur $]t_1, t_2[$: de plus $W(t_1 + \varepsilon) \longrightarrow 0$: en effet, si $y(t_1) \neq 0$, c'est bon ; sinon, on a $y'(t_1) \neq 0$ par Cauchy-Lipschitz, et alors :

$$\frac{x(t_1 + \varepsilon)}{y(t_1 + \varepsilon)} \sim \frac{x'(t_1)}{y'(t_1)}$$

ce qui permet de conclure ; on fait de même en t_2.
Ainsi, $\int_{t_1+\varepsilon}^{t_2-\varepsilon} \frac{b}{y^2}(xy' - x'y)^2 \mathrm{d}t$ admet une limite quand $\varepsilon \to 0$; par convergence monotone, on en déduit que l'intégrande $\frac{b}{y^2}(xy' - x'y)^2$ est intégrable, et on a :

$$0 = \int_{t_1}^{t_2} x^2(s - r)\mathrm{d}t + \int_{t_1}^{t_2} \frac{b}{y^2}(xy' - x'y)^2 \mathrm{d}t + \int_{t_1}^{t_2} (a - b)(x')^2 \mathrm{d}t$$

Dès lors, par positivité :

$$xy' = x'y \text{ pp}$$

ce qui implique que x et y sont proportionnelles sur $]t_1, t_2[$.

Pour l'application : si y admet deux zéros négatifs $t_1 < t_2 \leq 0$. On prend alors $a = b = 1$, et $r(t) = t$ et $s(t) = 0$ sur $]-\infty, 0]$: cela nous dit que toute solution z de $z'' = 0$ a au moins un zéro sur $]t_1, t_2[$: absurde en prenant $z = 1$.
En prenant $a = b = 1, r(t) = 1$ et $s(t) = t$, on a au moins un zéro sur chaque intervalle $]k\pi, (k+1)\pi[$ sur $[1, \infty[$, d'où l'infinité de zéros. De plus, en écrivant : $\forall t \in [n, n+1], n \leq t \leq n+1$, on a, notant b_n le nombre de zéros de $z'' + nz = 0, z(n) = 0, z'(n) = \sqrt{n}$ sur $[n, n+1]$:

$$b_n \leq a_{n+1} - a_n \leq b_{n+1}$$

Or le z précédent vaut $z(t) = \sin(\sqrt{n}(t - n))$, donc ses zéros sont les $n + k\frac{\pi}{\sqrt{n}}$: ainsi :

$$b_n = \lfloor \frac{\sqrt{n}}{\pi} \rfloor \sim \frac{1}{\pi} n^{1/2}$$

Donc on a :

$$a_{n+1} - a_n \sim \frac{1}{\pi} n^{1/2}$$

Or on a, par sommes de Riemann :

$$\sum_{k=0}^{n-1} k^{1/2} \sim \frac{1}{1 + 1/2} n^{1+1/2} = \frac{2n^{3/2}}{3}$$

Et donc, par sommation des équivalents, licite, car le terme est positif non sommable :

$$a_n \sim \frac{2}{3\pi} n^{3/2}$$

3 Probabilités

3.1 Moyen & original : nombre de cycles par les restaurants chinois

(haut) Recasages : 101, 105, 190, 262, 264, 266.

Énoncé : Soit, pour $n \in \mathbf{N}$, Σ_n une variable aléatoire de loi uniforme sur $\mathfrak{S}_n$, et C_n le nombre de cycles de Σ_n. Alors :

$$\frac{C_n}{H_n} \longrightarrow 1 \quad \text{p.s. et } L^2 \qquad\qquad (H_n = 1 + \frac{1}{2} + \ldots + \frac{1}{n})$$

Remarque : On a même : $\frac{K_n - H_n}{\sqrt{H_n}} \longrightarrow \mathcal{N}(0,1)$ en loi.

Preuve : On construit un algorithme pour simuler une loi uniforme sur $\mathfrak{S}_n$. Pour cela, on a une bijection ensembliste :

$$\begin{aligned} \mathfrak{S}_n \times [\![1, n+1]\!] &\to \mathfrak{S}_{n+1} \\ (\sigma, k) &\mapsto \widetilde{\sigma} : j \mapsto \begin{cases} \sigma(j) & \text{si } j \notin \{k, n+1\} \\ n+1 & \text{si } j = k \\ \sigma(k) & \text{si } j = n+1 \end{cases} \end{aligned}$$

En effet, pour le voir il suffit de dire que, pour construire une permutation de $[\![1, n+1]\!]$, il suffit de prendre une permutation de $[\![1, n]\!]$ et de choisir un "voisin" k de $n+1$, où $n+1$ est son propre voisin ssi il est fixe.
Ainsi, par récurrence sur n, on a une bijection $f : [\![1,1]\!] \times [\![1,2]\!] \ldots \times [\![1,n]\!] \simeq \mathfrak{S}_n$, tel que le nombre de cycles de $f(k_1, \ldots, k_n)$ est donné par le nombre de i tels que $k_i = i$. Ainsi, si (K_i) est une suite de variables indépendantes telles que K_i suit la loi uniforme sur $[\![1, i]\!]$, on a que $\Sigma_n = f(K_1, \ldots, K_n)$ suit une loi uniforme sur $\mathfrak{S}_n$.
Ainsi, $C_n = \sum_{i=1}^n K_i$. On a donc $\mathbb{E}(C_n) = H_n$, et :

$$\mathrm{Var}(\frac{C_n}{H_n}) = \frac{1}{H_n^2} \sum_{i=1}^n \frac{1}{i}(1 - \frac{1}{i}) \leq \frac{1}{H_n} \longrightarrow 0$$

ce qui montre la convergence L^2. De plus, par l'inégalité de Bienaymé-Tchebychev, si $\varepsilon > 0$:

$$\mathbb{P}\left(\left|\frac{C_n}{H_n} - 1\right| > \varepsilon\right) \leq \frac{1}{H_n \varepsilon^2}$$

Ce qui montre la convergence en probas (cohérent, car cv L^2). On voudrait appliquer Borel-Cantelli, mais ce n'est pas possible, car le terme de droite n'est pas sommable. Soit, pour $i \geq 0$, $n_i = 2^{i^2}$; alors la somme $\sum_i \frac{1}{H_{n_i} \varepsilon^2}$ est finie, car $H_{n_i} \sim \log(2^{i^2}) = i^2 \log(2)$. Ainsi, par le théorème de Borel-Cantelli :

$$\forall \varepsilon > 0, \mathbb{P}\left(\limsup_i \left(\left|\frac{C_{n_i}}{H_{n_i}} - 1\right| > \varepsilon\right)\right) = 0$$

Or, en comparant les deux évènements :

$$\limsup_i \left(\left|\frac{C_{n_i}}{H_{n_i}} - 1\right| > \varepsilon\right) = \left(\limsup_i \left|\frac{C_{n_i}}{H_{n_i}} - 1\right| > \varepsilon\right)$$

Ce qui donne :

$$\forall \varepsilon > 0, \text{ps, } \limsup_i \left| \frac{C_{n_i}}{H_{n_i}} - 1 \right| \leq \varepsilon$$

On veut faire un échange $\forall \varepsilon \longleftrightarrow$ ps, pour cela il suffit de se ramener à un ensemble dénombrable sur ε, par exemple $\mathbf{Q} \cap]0, +\infty[$. On a donc :

$$\text{ps, } \forall \varepsilon > 0 \in \mathbf{Q}, \limsup_i \left| \frac{C_{n_i}}{H_{n_i}} - 1 \right| \leq \varepsilon$$

Donc :

$$\frac{C_{n_i}}{H_{n_i}} \xrightarrow[ps]{} 1$$

Soit $n \in \mathbf{N}^*$, on dispose de i tel que $n_i \leq n < n_{i+1}$, et ce i tend vers l'infini avec n. De plus, on a $C_{n_i} \leq C_n < C_{n_{i+1}}$ (car l'algo montre que C_n ne peut que croître avec n). Cela donne :

$$\frac{C_{n_i}}{H_{n_{i+1}}} \leq \frac{C_n}{H_n} < \frac{C_{n_{i+1}}}{H_{n_i}}$$

Mais comme $\frac{H_{n_{i+1}}}{H_{n_i}} \sim \frac{(i+1)^2}{i^2} \to 1$, les deux termes encadrant tendent ps vers 1 quand $n \to \infty$; cela montre bien :

$$\frac{C_n}{H_n} \longrightarrow 1 \quad \text{p.s.}$$

3.2 Facile & classique : Borel-Cantelli, pas de mesure de probas "arithmétique" sur $\mathbf{N}^*$

(haut)

Référence : Zavidovique

Énoncé : On montre le lemme de Borel-Cantelli : si (A_n) est une suite d'évènements, alors si $\sum \mathbb{P}(A_n) < +\infty$, $\mathbb{P}(\limsup A_n) = 0$; et si $\sum \mathbb{P}(A_n) = \infty$ et les (A_n) sont indépendants, alors $\mathbb{P}(\limsup A_n) = 1$.
Ensuite, on considère l'ensemble $\Omega = \mathbf{N}^*$, muni de sa tribu discrète. Il n'existe pas de probabilité $\mathbb{P}$ telle que : $\forall n \in \mathbf{N}^*, \mathbb{P}(n\mathbf{N}^*) = \frac{1}{n}$.

Preuve : Soit (A_n) une suite d'évènements telle que $\sum \mathbb{P}(A_n) < \infty$. Par convergence monotone, on sait : $\mathbb{E}(\sum \mathbf{1}_{A_n}) = \sum \mathbb{P}(A_n) < \infty$, donc $\sum \mathbf{1}_{A_n} < \infty$ ps : cela prouve que presque tout x est dans un nombre fini de (A_n), et donc : $\mathbb{P}(\limsup A_n) = 0$.

Soit (A_n) une suite d'évènements **indépendants** telle que $\sum \mathbb{P}(A_n) = \infty$. On montre que $\mathbb{P}(\limsup A_n) = 1$. On a :

$$\limsup A_n = \bigcap_{p\geq 0} \bigcup_{n\geq p} A_n$$

Donc par convergence décroissante, il suffit de montrer : $\forall p \geq 0, \mathbb{P}(\cup_{n\geq p} A_n) = 1$. Or on a :

$$1 - \mathbb{P}\left(\bigcup_{n\geq p} A_n\right) = \mathbb{P}\left(\bigcap_{n\geq p} \overline{A_n}\right) = \prod_{n\geq p}(1 - \mathbb{P}(A_n))$$

le produit infini étant la limite des produits finis. On montre que ce dernier produit est nul : on a en effet $1 - x \leq e^{-x}$ pour $x \in \mathbf{R}$ (par convexité de $\exp$), d'où :

$$\prod_{n=p}^{N}(1 - \mathbb{P}(A_n)) \leq e^{-\sum_{n=p}^{N}\mathbb{P}(A_n)} \underset{N\to\infty}{\longrightarrow} 0$$

Donc :

$$\prod_{n\geq p}(1 - \mathbb{P}(A_n)) = 0$$

ce qui conclut.

On démontre que, notant $\mathcal{P}$ l'ensemble des nombres premiers, on a :

$$\sum_{p\in\mathcal{P}} \frac{1}{p} = \infty$$

Pour cela, pour $N \geq 1$, on a (en vertu de l'égalité $1 + x + \ldots = (1-x)^{-1}$:

$$\prod_{p\in\mathcal{P}, p\leq N} (1 - p^{-1})^{-1} \leq \prod_{p\in\mathcal{P}, p\leq N} (\sum_{i=0}^{n} p^{-i})$$

Or, dans le produit $\prod_{p\in\mathcal{P}, p\leq N}(\sum_{i=0}^{n} p^{-i})$, il apparaît au moins chaque nombre entre 1 et n, et ce par factorialité de $\mathbf{Z}$. Ainsi, on a :

$$\prod_{p\in\mathcal{P}, p\leq N} (1 - p^{-1})^{-1} \geq \sum_{k=1}^{n} \frac{1}{k} \underset{n\to\infty}{\longrightarrow} \infty$$

Comme $\frac{1}{p} \sim -\ln(1-p^{-1})$, on en déduit la divergence de la somme.

Enfin, on montre l'énoncé ; soit $\mathcal{P} = \{p_1, p_2, \dots\}$ une énumération des nombres premiers, et, pour $n \geq 1$, $A_n = p_n\mathbf{Z}$. Supposons qu'une proba $\mathbb{P}$ satisfasse l'énoncé. Alors :

$$\sum_n \mathbb{P}(A_n) = \infty$$

et les (A_n) sont indépendants : en effet, si $m \in A_{p_n} \cap A_{p_{n'}}$, alors $p_n p_{n'} \mid m$, donc $m \in A_{p_n p_{n'}}$. Dès lors, par Borel-Cantelli, on a :

$$\mathbb{P}(\limsup A_n) = 1$$

Or $m \in \limsup A_n$ revient à dire que m a une infinité de diviseurs premiers, donc $\limsup A_n = \emptyset$: on a l'absurdité cherchée.

4 Abandonnés

4.1 Moyen & classique : Inégalités de Kolmogorov

(haut) Référence : Gourdon, Analyse

4.2 Moyen & original : Calculs avec les fonctions multiplicatives

Énoncé : On définit les fonctions L de fonctions multiplicatives. On montre : $L(f \star g, s) = L(f, s)L(g, s)$. On en déduit l'égalité :

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$$

(un peu court...).

4.3 Moyen & classique : critère d'équirépartition de Weyl

(haut)

Référence : Cassini Analyse (2 ?)

4.4 Facile & semi-classique : Linéarisation d'une EDO

(haut)

Référence : Rouvière (chap 3)

Énoncé : Soit $a \in]0, \pi[$, on considère l'équation du pendule sans vitesse initiale et d'angle initial a :

$$\begin{cases} x''(t) & = -\sin(x(t)) \\ x(0) & = a \\ x'(0) & = 0 \end{cases}$$

On montre que ce problème a un une unique solution définie sur $\mathbf{R}$ (contrairement à dans le livre, mais enfin bon...). Soit y le système linéarisé correspondant, on a :

$$\forall t \in \mathbf{R}, |x(t) - y(t)| \leq \frac{a^3}{6}|t|$$

Remarque : Si trop court, regarder l'exo suivant sur Liapounov.

4.5 Facile & classique : calcul d'une intégrale d'une fraction rationnelle en $\sin$ de deux manières

(haut) Référence : Queffelec, Analyse complexe

Énoncé : On a :

$$\forall a \in]-1, 1[, \int_0^{2\pi} \frac{\mathrm{d}t}{1 + a\sin(t)} =$$

Deux méthodes :

- Élémentaire : poser $u = \tan(\frac{t}{2})$
- Avancé : poser $z = e^{it}$ et écrire $z + z^{-1} = 2i\sin(t)$

4.6 Difficile & semi-original : la table de $\mathfrak{S}_n$ est à valeurs entières pour tout n

(haut) Références : H2G2 nouvelle éd tome 2 En fait, pas très difficile mais exigeant en terme de matériel : théorie de Galois.

4.7 Moyen & original : théorème de Minkowski & théorème des quatre carrés de Lagrange

Réf : Hindry Recasages : 126, 181,

Énoncé : Soit Λ est un réseau de $\mathbf{R}^n$, soit C un convexe symétrique borné tel que $\mathrm{vol}(C) > 2^n \mathrm{covol}(\Lambda)$. Alors C contient un élément non nul de Λ. Si C est en plus compacte, alors l'inégalité large suffit.
Corollaire : tout entier est somme de quatre carrés.

4.8 Moyen & original : lemme de Siegel, et application ? ?

Référence : Cassini algèbre 1 Application : approximation diophantienne ? (cf Duverney théorie des nombres).

4.9 Facile & classique : convergence p.s. de série aléatoire

Énoncé : $(X_n)_{n\geq 1}$ indép. centrées de variances u_n, où $\sum_{u_n}$ est une série cv. Alors $\sum X_k$ converge p.s.

Preuve : On montre qu'elle est p.s. de Cauchy : on a, par Bienaymé-Tchebychev et par indépendance :

$$\forall n > m,\ \mathbb{P}\left(|S_n - S_m| \geq c\right) \leq \frac{1}{c^2}\sum_{k=m+1}^{\infty} u_k$$

Mais cette inég est pas terrible...
On pose $T_{m,c} = \inf\{k > m, |S_k - S_m| \geq c\}$. Alors pour $n \geq k > m$, on a :

$$\mathbb{P}\left(T_{m,c} = k\right) \leq \frac{1}{c^2}\mathbb{E}\left((S_k - S_m)^2 \mathbf{1}_{T_{m,c}=k}\right) \leq \frac{1}{c^2}\mathbb{E}\left((S_n - S_m)^2 \mathbf{1}_{T_{m,c}=k}\right)$$

donc :

$$\forall m,\ \mathbb{P}\left(\exists k, |S_k - S_m| \geq c\right) \leq \frac{1}{c^2}\sum_{k=m+1}^{\infty} u_k$$

Donc (en échangeant $\forall c$ et $p.s.$), (S_n) est p.s. de Cauchy.

4.10 Facile & classique A REVOIR : autour du dénombrement

(haut)

Recasages : 105, 152, 190, 243. Réf : Cassini, algèbre 1 pour la première partie, 2 pour la deuxième

Énoncé : Pour $n \geq 1$, on calcule le nombre de dérangements de $[\![1, n]\!]$, on montre qu'il est équivalent à $\frac{n!}{e}$ (par exemple par une série gén). Puis, on calcule :

$$\delta_n = Card\{\text{dérangements pairs}\} - Card\{\text{dérangements impairs}\} = (-1)^{n-1}(n-1)$$

(le voir comme le déterminant de $J_n - I_n$, où J_n est la matrice avec que des 1).

Remarque : On sait (en regardant les lois marginales $(\sigma(i), 1 \leq i \leq n)$) que le nombre de points fixes d'une permutation aléatoire suit une loi binomiale de paramètres $(n, \frac{1}{n})$. Donc le résultat sur l'équivalent en e^{-1} est aussi une conséquence de la convergence en loi des binomiales vers la loi de Poisson de paramètre 1.

4.11 Moyen+ & classique : résolution de l'équation de la chaleur à la mode Green

(haut) Référence : Brézis ? (à vérifier) Recasages : 222, 250.

4.12 Moyen & classique : proba pour que deux entiers soient premiers entre eux

On montre (avec des calculs classiques) que la proba que deux entiers choisis aléatoirement (avec proba uniforme) dans $[\![1, n]\!]$ soient premiers entre eux tend, quand $n \to \infty$, vers $\frac{6}{\pi^2}$. Ce dév est à mettre en lien avec les fonctions L de fct multiplicatives.