Mes développements pour l'agrég de maths (leçons d'algèbre et analyse, option informatique)

Nguyễn Lê Thành Dũng (ENS Ulm, département informatique, promo 2012)

Préparation à l'agrégation de l'ENS Paris-Saclay, 2016–2017

Ce document recense les développements que j'ai travaillés et rédigés pendant mon année de prépa agrég, en vue de l'oral de leçon de mathématiques. (En option D, il y a un unique oral « Mathématiques pour l'informatique » où peuvent tomber à la fois des leçons d'algèbre et des leçons d'analyse.)

Parmi ceux-ci, un certain nombre sont originaux, voire exotiques. On ne les trouvera pas dans les livres classiques de l'agrég, mais j'ai tout de même essayé d'indiquer des références livresques quand c'était possible.

- Dualité lagrangienne et extrema liés en optimisation convexe
- Fonction tangente et permutations zigzag (tiré des développements de Paul Melotti)
- Points à distances impaires, avec le déterminant de Gram
- Étude des automorphismes extérieurs de $\mathfrak{S}_6$
- Les fonctions monotones (continues) sont dérivables presque partout
- Équivalent asymptotique de la fonction thêta et sommes de Gauss (inabouti, il reste une arnaque à régler, qui pourra constituer un exercice pour la lectrice ; envoyez vos suggestions de preuve à `nltd@nguyentito.eu`)

D'autres sont des développements « classiques » mais pour lesquels je propose des preuves améliorées.

- Enveloppe convexe du groupe orthogonal : au niveau agrég, on est censé avoir entendu parler de décomposition en valeurs singulières
- Théorème taubérien fort de Littlewood (saviez-vous qu'il était dû à Littlewood sans Hardy ?) : on découpe moins d'ε en invoquant les sommes de Riemann
- Stabilité asymptotique d'un équilibre (ou « théorème de Liapounov » ; saviez-vous qu'il était dû à Perron ?) : preuve plus directe et concise que celle proposée par le Rouvière

Le reste est relativement classique. On trouvera également une section Idées exclues.

On pourra consulter l'excellent *Histoires hédonistes de groupes et de géométries, tome premier* de Caldero et Germoni pour y trouver d'autres développements pour lesquels j'ai une grande affection, mais que je n'ai pas pris la peine de taper, notamment :

- Revêtement universel $\mathrm{SU}(2) \to \mathrm{SO}(3)$ via les quaternions
- Réciprocité quadratique par double comptage d'une conique sur $\mathbb{F}_q^p$ (trop beau !)
- Existence de la réduction de Frobenius (utilisant l'orthogonalité duale)

Le développement Non-isomorphisme exceptionnel (avec la réduction de Jordan) est également issu de H2G2 tome 1, mais la preuve qui y est donnée est légèrement fausse, c'est pourquoi une version corrigée est rédigée ici. Ce développement gagnerait d'ailleurs à être plus connu, étant donné qu'il se recase dans de nombreuses leçons d'algèbre, faisant intervenir à la fois la réduction des endomorphismes nilpotents, les groupes finis, et les corps finis.

Table des matières

1 Algèbre/géométrie et analyse

1.1 Dualité lagrangienne et extrema liés en optimisation convexe

On montre ici un théorème fondamental en *recherche opérationnelle*, variante du théorème des extrema liés où :

— on a des multiplicateurs de Lagrange *positifs* correspondant à des contraintes d'*inégalité* (on ne pourra donc pas invoquer les sous-variétés) ;

— les conditions nécessaires du premier ordre sont également *suffisantes* grâce à la convexité.

Il est recommandé d'avoir quelques connaissances en optimisation (notamment, l'application à la dualité en programmation linéaire et programmation semi-définie) si on veut présenter ce développement.

Soient $f, g_1, \dots, g_k : \mathbb{R}^n \to \mathbb{R}$ des fonctions *convexes*. On considère le problème de minimisation

$$p = \inf_{x \in F} f(x) \qquad F = \left\{ x \in \mathbb{R}^n \mid g_i(x) \leq 0,\ i = 1, \dots, k \right\}$$

(Vocabulaire : f est la *fonction objectif*, les g_i sont des *contraintes*, F est l'ensemble des *solutions réalisables*).

On appelle *condition de Slater* l'existence d'un $x_0 \in \mathbb{R}^n$ *strictement réalisable*, c'est-à-dire tel que $g_i(x_0) < 0$ pour tout i.

Théorème (Karush–Kuhn–Tucker)**.** *On suppose ici que $f, g_1, \dots, g_k$ sont $\mathscr{C}^1$, et que la condition de Slater est vérifiée. Alors pour tout $x \in \mathbb{F}$, $f(x) = p$ si et seulement s'il existe $\mu_1, \dots, \mu_k \geq 0$ tels que*

$$\nabla f(x) + \sum_{i=0}^{k} \mu_i \nabla g_i(x) = 0 \quad \textit{et} \quad \mu_i g_i(x) = 0 \ \forall i$$

Afin de montrer cela, introduisons le *lagrangien* $\mathscr{L} : \mathbb{R}^n \times \mathbb{R}_+^k \to \mathbb{R}$ et le problème dual associé :

$$\mathscr{L}(x, \mu) = f(x) + \sum_{i=1}^{k} \mu_i g_i(x) \qquad d = \sup_{\mu \in \mathbb{R}_+^k} \inf_{x \in \mathbb{R}^n} \mathscr{L}(x, \mu)$$

Remarque. $p = \inf\limits_{x \in \mathbb{R}^n} \sup\limits_{\mu \in \mathbb{R}_+^k} \mathscr{L}(x, \mu)$.

Démonstration. En effet, si $x \notin F$, alors il existe i tel que $g_i(x) > 0$. $\mathscr{L}(x, (0, \dots, \mu_i, \dots, 0)) \to +\infty$ quand $\mu_i \to +\infty$. Donc $\sup_{\mu \in \mathbb{R}_+^k} \mathscr{L}(x, \mu) = +\infty$ dès que $x \notin F$, et si $x \in F$, le sup est atteint pour $\mu = 0$ soit $\mathscr{L}(x, \mu) = f(x)$. □

Corollaire (Dualité faible)**.** $d \leq p$.

Démonstration. Il s'agit simplement de voir que pour tout x, μ,

$$\inf_y \mathscr{L}(y, \mu) \leq \mathscr{L}(x, \mu) \leq \sup_\nu \mathscr{L}(x, \nu)$$

puis de prendre le sup sur μ à gauche et l'inf sur x à droite. □

Théorème (Dualité forte)**.** *On suppose seulement que $f, g_1, \dots, g_k$, et que la condition de Slater est satisfaite. Alors $p = d$ et le supremum dual est atteint.*

Démonstration. Si $p = -\infty$, la dualité faible permet de conclure directement que $d = -\infty$.

Sinon, il suffit de montrer $p \leq d$, donc de trouver $\mu_1, \dots, \mu_k \geq 0$ tels que pour tout $x \in \mathbb{R}^n$, $\mathscr{L}(x, \mu) \geq p$.

Posons $A, B \subset \mathbb{R}^{k+1}$ définis par

$$A = \left\{(y_1, \dots, y_k, z) \mid \exists x \in \mathbb{R}^n / y_i \geq g_i(x),\ z \geq f(x)\right\} \qquad B = \left\{(y_1, \dots, y_k, z) \mid y_i < 0,\ z < p\right\}$$

Si $(y_1, \dots, y_k, z) \in A \cap B$, alors il existe x tel que $g_i(x) \leq y_i < 0$ pour tout x, donc $x \in F$, et $f(x) \leq z < p$. C'est impossible par définition de p. Ainsi, A et B sont disjoints, avec B ouvert.

Donc il existe un hyperplan séparateur [1] i.e. une forme linéaire φ telle que $\varphi(a) \geq \varphi(b)$ pour tout $a \in A$ et $b \in B$. En coordonnées, φ s'écrit

$$\varphi(y_1, \dots, y_k, z) = \mu_1 y_1 + \dots + \mu_k y_k + \nu z \quad \text{avec} \quad (\mu_1, \dots, \mu_k, \nu) \neq (0, \dots, 0)$$

Pour tout x, en prenant $a = (g_1(x), \dots, g_k(x), f(x))$, et $b = (0, \dots, 0, p) \in \overline{B}$, on a

$$\sum_{i=1}^{k} \mu_i g_i(x) + \nu f(x) \geq \nu p$$

On montre que $\nu > 0$ par disjonction de cas :

— si $\mu = (\mu_1, \dots, \mu_k) \neq 0$, alors l'inégalité ci-dessus, appliquée à x_0 strictement réalisable, nous donne $\nu f(x_0) > \nu p$;

— sinon, $\varphi(g_1(x_0), \dots, g_k(x_0), f(x_0)) > \varphi(0, \dots, 0, p-1)$ nous donne $\nu f(x_0) > \nu(p-1)$.

En divisant par ν, on a finalement : $\mathscr{L}(x, \mu_1/\nu, \dots, \mu_k/\nu) \geq p$. □

Supposons maintenant que $f, g_1, \dots, g_k$ sont $\mathscr{C}^1$.

Les conditions KKT sont nécessaires. Fixons $\mu_1, \dots, \mu_k$ maximisant le dual : $\inf_x \mathscr{L}(x, \mu) = d = p$. Soit x tel que $f(x) = p$. Alors

$$f(x) = p = d \leq \mathscr{L}(x, \mu) = f(x) + \sum_{i=0}^{k} \mu_i g_i(x)$$

Comme $g_i(x) \leq 0$ et $\mu_i \geq 0$ pour tout i, ce qui entraîne l'inégalité réciproque, on a en fait $\mu_i g_i(x) = 0$ pour tout i. Ainsi, en x, $\mathscr{L}(-, \mu)$ atteint la valeur d qui est son minimum, son gradient s'annule donc. Ceci donne immédiatement la condition au premier ordre. □

Les conditions KKT sont suffisantes. Soient $x \in F$ et $\mu \in \mathbb{R}_+^k$ vérifiant ces conditions. Alors, comme $\mathscr{L}(-, \mu)$ est convexe, ses points stationnaires sont ses minima globaux, donc elle atteint son minimum en x. Comme $\mu_i g_i(x) = 0$ pour tout i, le lagrangien vaut $f(x)$:

$$f(x) = \mathscr{L}(x, \mu) = \inf_{x'} \mathscr{L}(x', \mu) \leq \sup_{\mu'} \inf_{x'} \mathscr{L}(x', \mu') = p$$

donc x minimise bien f sur F. □

1. Il faut faire attention aux hypothèses topologiques de la version de Hahn-Banach qu'on utilise ici. Sinon, on pourrait invoquer le théorème de séparation des convexes en dimension finie de Minkowski, qui demande seulement que les deux convexes soient disjoints.

Ci-dessous, une tentative de prouver autrement la dualité forte… comme corollaire du *théorème du minimax de Sion* ; ce théorème pourrait d'ailleurs faire l'objet d'un développement fort intéressant. L'intérêt étant de voir un lien entre condition de Slater et compacité. On suppose donc qu'il existe x_0 strictement réalisable.

On a besoin comme hypothèse supplémentaire que $d > -\infty$ (comment s'en passer ?). On rappelle qu'un sup de fonctions semi-continues inférieurement l'est, et qu'une telle fonction admet un minimum sur tout compact.

Fixons $R > 0$ et posons $\bar{B}_R = \bar{B}(x_0, R)$, qui est convexe compact. Soit

$$p_R = \min_{x \in \bar{B}_R} \sup_{\mu \in \mathbb{R}^k_+} \mathscr{L}(x, \mu) = \sup_{\mu \in \mathbb{R}^k_+} \min_{x \in \bar{B}_R} \mathscr{L}(x, \mu)$$

l'égalité résultant du théorème du minimax.

La première expression donne $p_R = \min_{x \in F \cap \bar{B}_R} f(x)$ (l'ensemble étant non vide puisque x_0 y est).

D'autre part, par la seconde expression, $p_R \geq d$. Comme x_0 est strictement réalisable, quand $\|\mu\| \to +\infty$ en restant dans $\mathbb{R}^k_+$, $\mathscr{L}(x_0, \mu) \to +\infty$. Il existe donc un compact $K \subset \mathbb{R}^k_+$ tel que $\forall \mu \in \mathbb{R}^k_+ \setminus K$, $\mathscr{L}(x_0, \mu) < d \leq p_R$ (et K est indépendant de R, c'est important !). D'où

$$p_R = \max_{\mu \in K} \min_{x \in \bar{B}_R} \mathscr{L}(x, \mu) = \min_{x \in \bar{B}_R} \max_{\mu \in K} \mathscr{L}(x, \mu)$$

Quand $R \to +\infty$, on trouve

$$\inf_{x \in F} f(x) = \inf_{x \in \mathbb{R}^n} \max_{\mu \in K} \mathscr{L}(x, \mu) = \max_{\mu \in K} \inf_{x \in \mathbb{R}^n} \mathscr{L}(x, \mu)$$

où, cette fois-ci, on a utilisé la compacité de K pour appliquer le théorème du minimax à $-\mathscr{L}$! Tout ceci fonctionnant encore avec n'importe quel convexe compact $K' \supseteq K$, en épuisant $\mathbb{R}^k_+$ avec des compacts, on a finalement $p = d$, et de plus, on sait qu'une solution duale optimale μ^* existe.

Question ouverte : peut-on montrer $d > -\infty$ sans utiliser un argument d'hyperplan séparateur ?

1.2 Enveloppe convexe du groupe orthogonal

Je propose ici une démonstration bien plus expéditive que celle qu'on trouve par-ci par-là dans des PDF sur Internet, relativement autosuffisante avec le programme de math spé (pas besoin de théorèmes un peu compliqués à démontrer comme Hahn-Banach géométrique, donc). Mais du coup c'est peut-être un peu court…

On considère $\mathbb{R}^n$ muni de sa norme euclidienne canonique $\|\cdot\|$, $O(n)$ le groupe orthogonal.

Le seul prérequis sera le suivant :

Théorème (Décomposition en valeurs singulières)**.** *Soit $M \in \mathscr{M}_n(\mathbb{R})$, alors il existe $U, V \in O(n)$ et D diagonale à coefficients positifs tels que $M = UDV$.*

Démonstration. On s'est placé dans le cas particulier des matrices carrées, donc il suffit d'enchaîner décomposition polaire et théorème spectral. □

Énonçons également un petit lemme qu'il sera bon d'illustrer avec un **dessin** dans $\mathbb{R}^2$:

Lemme. $\mathrm{Conv}(\{-1,1\}^n) = [-1,1]^n$.

Démonstration. On aimerait parachuter une formule explicite, mais c'est sans doute pénible, vu que ça devra impérativement faire intervenir tous les 2^n sommets de l'hypercube… Sinon, il est clair que $\mathrm{Conv}(-1,1) = [-1,1]$, d'où l'on déduit que

$$\bigcup_{x\in[-1,1]} \mathrm{Conv}(\{x\} \times \{-1,1\}^{n-1}) \subseteq \mathrm{Conv}(\{-1,1\}^n)$$

puis on conclut par récurrence. □

Maintenant, soit $|||\cdot|||$ la norme subordonnée sur $\mathscr{M}_n(\mathbb{R})$ et B la boule unité *fermée* de $\mathscr{M}_n(\mathbb{R})$ pour cette norme.

Théorème. *B est l'enveloppe convexe de $O(n)$.*

Démonstration. Tout d'abord, il est clair que les matrices orthogonales, étant des isométries, sont de norme 1, donc $O(n) \subset B$. B étant convexe, il contient également l'enveloppe convexe de $O(n)$.

Soit $M \in B$. Écrivons sa SVD : $M = UDV$ où $U, V \in O(n)$ et $D = \mathrm{Diag}(d_1, \dots, d_n)$. Comme $|||D||| \leq 1$, on a $|d_i| \leq 1$ pour tout i. Le lemme précédent nous permet donc d'écrire D comme barycentre de la forme $\mathrm{Diag}(\pm 1, \dots, \pm 1)$. Ces matrices sont des symétries orthogonales, elles sont dans $O(n)$. En multipliant par U à gauche et V à droite, on a $M \in \mathrm{Conv}(O(n))$. □

Le théorème est donc en fait simplement la conséquence du fait que la plus grande valeur singulière est égale à la norme subordonnée.

Théorème. *$O(n)$ est l'ensemble des* points extrêmes *de B, c'est-à-dire des points qui ne peuvent pas s'écrire comme barycentres d'autres points de B.*

Ce résultat découle du précédent via le théorème de Krein-Milman [2], mais celui-ci est difficile à montrer.

2. En réalité, on n'a besoin que de la version en dimension finie, plus simple, et démontrée par Minkowski. Cette version nécessite quand même l'existence des hyperplans d'appui, donc utilise le théorème de séparation des convexes (dont la généralisation en dimension infinie est le théorème de Hahn-Banach).

Preuve élémentaire. Vu le résultat précédent, tout point extrême est forcément une matrice orthogonale. Réciproquement, soit $U \in O(n)$.

Posons $\varphi : M \mapsto \mathrm{Tr}(U^{-1}M)$, $\varphi \in \mathscr{M}_n(\mathbb{R})^*$. Pour tout $M \in B$, on a (puisque $\|U^{-1}Me_i\| \leq 1$)

$$\varphi(M) = \mathrm{Tr}(U^{-1}M) = \sum_{i=1}^{n} \langle U^{-1}Me_i \mid e_i \rangle \leq \sum_{i=1}^{n} \|U^{-1}Me_i\| \cdot \|e_i\| \leq n$$

et on a égalité si et seulement si, pour tout i,

— $\|U^{-1}Me_i\| = 1$

— (Cauchy-Schwarz) $U^{-1}Me_i$ et e_i sont positivement liés

soit $U^{-1}Me_i = e_i$ pour tout i. Ce qui est équivalent à $U^{-1}M = I$ ou encore à $M = U$.

Ainsi, d'une part $\varphi(U) = n$, d'autre part, pour tout barycentre $G = \sum_{i=1}^{k} \alpha_i M_i$ avec $M_i \in B \setminus \{U\}$, on a $\varphi(M_i) < n$ pour tout i donc $\varphi(G) < n$. Forcément $U \neq G$: U est un point extrême. □

Conséquence de la preuve : pour chaque point extrême, il existe un hyperplan d'appui intersectant B uniquement en ce point. Ce n'est pas vrai pour tout convexe (faire un dessin).

1.3 Fonction tangente et permutations zigzag

Cf. Richard P. Stanley, *A Survey of Alternating Permutations*. Le développement lui-même est tiré du PDF de Paul Melotti.

Le terme « permutation alternante » pouvant induire en confusion avec le groupe alterné, nous parlerons ici de *permutation zigzag*. Plus précisément, on dira que $\sigma \in \mathfrak{S}_n$ est :

— *haut-bas* si $\sigma(1) > \sigma(2)$, $\sigma(2) < \sigma(3)$, …
— *bas-haut* si $\sigma(1) < \sigma(2)$, $\sigma(2) > \sigma(3)$, …
— *zigzag* si elle est haut-bas ou bas-haut, ou de façon équivalente si $(\sigma(i) - \sigma(i-1))(\sigma(i+1) - \sigma(i)) < 0$ pour tout i.

(Faire un dessin pour illustrer.) On notera leurs ensembles respectifs Z_n^+, Z_n^- et $Z_n = Z_n^+ \cup Z_n^-$, et on prendra comme convention, pour $n \in \{0, 1\}$, $Z_n^+ = Z_n^- = \mathfrak{S}_n$ qui est un singleton.

Notre but est de montrer le résultat inattendu suivant :

Théorème (Désiré André)**.** *La série génératrice exponentielle des permutations haut-bas est* $G(z) = \tan(z) + \sec(z)$.

En fait, au lieu d'utiliser la série génératrice pour dénombrer nos objets comme d'habitude, ici le sens utile est plutôt l'obtention d'un algorithme pour obtenir les coefficients des séries entières des fonctions tangente et sécante. Il faudrait pour cela dénombrer d'une autre façon les permutations haut-bas, ce qu'on ne fera pas ici.

Proposition. *Pour tout* $n \in \mathbb{N}$, $Z_n^+ \simeq Z_n^-$, *et si* $n \geq 2$, *alors* $Z_n^+ \cap Z_n^- = \varnothing$.

Démonstration. Pour $n \leq 1$, on a égalité. Sinon, la bijection entre Z_n^+ et Z_n^- est réalisée par $\sigma \mapsto (i \mapsto \sigma(n - i + 1))$ (visuellement, c'est une réflexion par rapport à un axe horizontal).

Dès qu'il existe deux éléments dans l'ensemble, on ne peut pas avoir à la fois $\sigma(1) > \sigma(2)$ et $\sigma(1) < \sigma(2)$. □

Proposition. *Pour* $n \in \mathbb{N}$, $Z_{n+1} \simeq \bigsqcup_{G \sqcup D = [\![1,n]\!]} Z_{|G|}^- \times Z_{|D|}^+$.

Démonstration. Soit $\sigma \in Z_{n+1}$ et soit $m = \sigma^{-1}(n+1)$. Posons $G = \sigma([\![1, m-1]\!]) = \{g_1, \dots, g_p\}$ et $D = \sigma([\![m+1, n-1]\!]) = \{d_1, \dots, d_q\}$ ($p = m - 1$, $q = n - m + 1$).

On peut maintenant définir $\sigma_g \in Z_p$ par $\sigma(m - i) = g_{\sigma_g(i)}$, et $\sigma(m + i) = d_{\sigma_d(i)}$. Il faut voir ce qui se passe sur un dessin : à gauche de m, on lit σ_g de droite à gauche, et à droite de m, on lit σ_d de gauche à droite.

Comme la suite $\sigma(m), \sigma(m-1), \sigma(m-2)$ est zigzag et $\sigma(m)$ est maximal, $\sigma_g \in Z_p^-$; de même, $\sigma_d \in Z_q^+$. Si $p \leq 1$ ou $q \leq 1$, on peut se convaincre que ça marche toujours avec la définition choisie de Z_p^- et Z_q^+.

On a ainsi défini une application $Z_{n+1} \longrightarrow \bigsqcup_{G \sqcup D = [\![1,n]\!]} Z_{|G|}^- \times Z_{|D|}^+$, dont on peut se convaincre qu'elle est bijective. □

Nous pouvons maintenant passer au dénombrement. Posons $a_n = |Z_n^+| = |Z_n^-|$ et $b_n = a_n/n!$; la série génératrice exponentielle s'écrit alors $G(z) = \sum_{n \in \mathbb{N}} b_n z^n$. Comme $0 \leq b_n \leq |\mathfrak{S}_n|/n! = 1$, G est de rayon de convergence au moins 1.

La relation de récurrence se réécrit, avec les cardinaux,

$$|Z_{n+1}| = \sum_{G \sqcup D = [\![1,n]\!]} a_{|G|} \cdot a_{|D|} = \sum_{k=1}^{n} \binom{n}{p} a_k a_{n-k} = \sum_{k=1}^{n} n! \frac{a_k}{k!} \frac{a_{n-k}}{k!} \quad \text{d'où} \quad \frac{|Z_{n+1}|}{n!} = \sum_{k=1}^{n} b_k b_{n-k}$$

On voit donc apparaître une convolution, ce qui nous donne envie de reformuler l'identité avec des séries entières. Mais attention au terme $n = 0$! Pour $n \geq 1$, comme $Z_{n+1}^+ \cap Z_{n+1}^- = \varnothing$, on a $|Z_{n+1}| = 2a_{n+1}$ soit $|Z_{n+1}|/n! = 2(n+1)b_{n+1}$. Pour $n = 0$, $|Z_1|/0! = 1 = 2 \times 1 \times b_1 - 1$. Ainsi :

$$\sum_{n\in\mathbb{N}} \frac{|Z_{n+1}|}{n!} z^n = \sum_{n\in\mathbb{N}} 2(n+1)b_{n+1}z^n - 1 = 2G'(z) - 1$$

le rayon de convergence étant au moins 1 pour la même raison que précédemment.

À droite de l'égalité, la convolution devient un produit de Cauchy en prenant la série génératrice ; finalement, on trouve que G est une solution de l'équation différentielle

$$2y' = y^2 + 1 \qquad \text{avec condition initiale} \quad y(0) = 1$$

Par Cauchy-Lipschitz, il existe une unique solution maximale à ce problème. Il suffit donc d'en exhiber une autre définie sur $]-1, 1[$ pour déterminer G sur cet intervalle. Parachutons donc $f(x) = \tan(x) + \sec(x)$; il ne reste qu'à calculer pour conclure.

Corollaire. *$a_n = \sec^{(n)}(0)$ si n est pair, $a_n = \tan^{(n)}(0)$ sinon.*

Démonstration. La fonction tangente est impaire tandis que la sécante est paire. □

1.4 Lemme de Morse

Béni soit ce développement, car il permet de remplir la leçon « Applications des formules de Taylor » en faisant autre chose qu'un développement asymptotique. Référence : exercices 66 et 114 dans Rouvière, *Petit guide de calcul différentiel*.

On note $S_n(\mathbb{R})$ l'espace des matrices symétriques réelles de taille n.

Proposition. *Soit $A \in S_n(\mathbb{R}) \cap \mathrm{GL}_n(\mathbb{R})$. Il existe un voisinage $V \ni A$ et $P \in \mathscr{C}^\infty(V, \mathrm{GL}_n(\mathbb{R}))$ tel que $M = P(M)^T A P(M)$ pour tout $M \in V$.*

Démonstration. Considérons $(A^{-1})S_n(\mathbb{R}) = \{A^{-1}M \mid M \in S_n(\mathbb{R})\}$. C'est un $\mathbb{R}$-espace vectoriel de dimension finie $n(n+1)/2$. $U = \mathrm{GL}_n(\mathbb{R}) \cap (A^{-1})S_n(\mathbb{R})$ en est une partie ouverte.

On considère l'application $\psi : P \in U \mapsto P^T A P \in S_n(\mathbb{R})$. ψ est une application $\mathscr{C}^\infty$ (car polynomiale) entre deux espaces de même dimension. Il s'agit de construire un inverse (à droite) de ψ au voisinage de A ; on voudrait donc appliquer le théorème d'inversion locale. Il suffit pour cela de vérifier que la différentielle est inversible.

Calculons-la : $D\psi(I)(H) = H^T A + AH$. Cette formule montre que si $H \in \mathrm{Ker}(D\psi(I))$, AH est antisymétrique ; or AH est symétrique (car $H \in (A^{-1})S_n(\mathbb{R})$, et l'on comprend pourquoi s'être restreint à cet espace !) donc $AH = 0$ soit $H = 0$ (A inversible). $D\psi(I)$ est donc inversible. □

Corollaire (Réduction $\mathscr{C}^\infty$ des formes quadratiques)**.** *Soit (p, q) la signature de A en tant que forme quadratique non dégénérée. Il existe $Q \in \mathscr{C}^\infty(V, \mathrm{GL}_n(\mathbb{R}))$ telle que pour tout $M \in V$,*

$$M = Q(M)^T \mathrm{Diag}(I_p, -I_q)\, Q(M).$$

Démonstration. Il suffit de combiner le théorème précédent avec la loi d'inertie de Sylvester. □

Théorème (« Lemme » de Morse)**.** *Soit $f \in \mathscr{C}^3(U, \mathbb{R}^n)$ ($U \subseteq \mathbb{R}^n$ ouvert) telle que $f(0) = 0$, $Df(0) = 0$, et $D^2 f(0)$ soit non dégénérée de signature $(p, n-p)$. Alors il existe un changement de coordonnées local $\mathscr{C}^1$ $x \mapsto u$ tel que*

$$f(x) = u_1^2 + \ldots + u_p^2 - u_{p+1}^2 - \ldots - u_n^2$$

Démonstration. On part de la formule de Taylor avec reste intégral[3]. En écriture matricielle,

$$f(x) = \int_0^1 (1-t) x^T H_f(tx) x \, dt = x^T A(x) x \quad \text{où} \quad A(x) = \int_0^1 (1-t) H_f(tx)\, dt$$

$H_f(x)$ étant la hessienne de f en x (formule valable pour x dans un voisinage convexe de 0). f étant $\mathscr{C}^3$, par dérivation sous le signe somme, A est $\mathscr{C}^1$.

$A(0) = H_f(0)$ et cette dernière est inversible par hypothèse. Le théorème démontré précédemment nous donne un voisinage V de $A(0)$ dans $S_n(\mathbb{R})$ et $Q \in \mathscr{C}^\infty(V, \mathrm{GL}_n(\mathbb{R}))$ tels que si $A(x) \in V$, $A(x) = Q(A(x))^T \mathrm{Diag}(I_p, -I_{n-p})\, Q(A(x))$. Et comme A est continue à valeurs dans $S_n(\mathbb{R})$, $U = A^{-1}(V)$ est un voisinage de 0.

Sur ce voisinage, on a donc :

$$f(x) = x^T \cdot Q(A(x))^T \mathrm{Diag}(I_p, -I_{n-p})\, Q(A(x)) \cdot x = u^T \mathrm{Diag}(I_p, -I_{n-p})\, u \quad \text{avec} \quad u = Q(A(x)) \cdot x$$

et c'est bien l'écriture qu'on voulait avoir. L'application $x \in U \mapsto u$ est-elle bien un difféomorphisme ? Elle est $\mathscr{C}^1$, et sa différentielle en 0 vaut $h \mapsto Q(A(0)) \cdot h$, qui est inversible. Quitte à restreindre plus le voisinage de 0, on peut donc avoir un $\mathscr{C}^1$-difféomorphisme par inversion locale. □

3. LE RESTE INTÉGRAL !

1.5 Méthode de Kaczmarz

Référence : à trouver.

Soient $A \in \mathscr{M}_{m,n}(\mathbb{R})$, et $b \in \mathbb{R}^m$. On veut résoudre $Ax = b$ ($x \in \mathbb{R}^n$) itérativement. Pour cela, on pose $(l_1, \dots, l_m)$ les lignes de A, et p_i le projecteur orthogonal sur l'hyperplan affine H_i d'équation $l_i x = b_i$ ($i \in \{1, \dots, m\}$). À partir de $x_0 \in \mathbb{R}^n$ quelconque, on définit par récurrence

$$x_{k+1} = p_{(k+1 \bmod n)}(x_k)$$

(faire un dessin !). On va montrer que la suite (x_k) converge vers une solution (sous réserve d'existence), et même mieux :

Proposition. *Soit S le sous-espace affine des solutions. Supposons que S soit non vide. Alors la suite (x_k) tend vers la solution de $Ax = b$ la plus proche de x_0, soit le projeté orthogonal de x_0 sur S.*

En particulier, s'il existe une unique solution et (x_k) converge vers elle. Par contre, s'il n'y a pas de solutions, on peut voir que la suite ne converge pas.

Démonstration. On a $S = \bigcap_{i=1}^n H_i$. Ainsi, S est aussi l'ensemble des points fixes communs de $p_1, \dots, p_m$. Soit x^* le projeté orthogonal de x_0 sur S ; il s'agit de montrer que $x_k \longrightarrow x^*$ quand $k \to +\infty$.

En posant $y_k = x_k - x^*$, cela revient à montrer $y_k \longrightarrow 0$. On voit que

$$y_{k+1} = p_i(x_k) - x^* = p_i(x_k) - p_i(x^*) = \pi_i(y_k)$$

où π_i est la partie linéaire de p_i, soit la projection orthogonale sur $\mathrm{Ker}(l_i)$.

Notons également H_i' la direction de H_i (qui est un hyperplan vectoriel), et $S' = \bigcap_{i=1}^n H_i'$ la direction de S. Comme tous les π_i stabilisent S', ils stabilisent aussi $F = S'^{\perp}$. Par récurrence, $y_k \in F$ pour tout $k \in \mathbb{N}$.

Pour montrer que $y_k \longrightarrow 0$, on va établir que $\|\Pi_{|F}\| < 1$ où $\Pi = \pi_n \circ \dots \circ \pi_1$. Ensuite, comme $\|\pi_i\| = 1$, on aura $\|y_k\| \leq \|\Pi_{|F}\|^{\lfloor p/n \rfloor} \|y_0\|$, d'où convergence linéaire.

Soit $z \in F$. On a $\|\pi_i(z)\| = \|z\|$ si et seulement si $\pi(z) = z$ soit $z \in \mathrm{Ker}(l_i)$, et $\|\pi_i(z)\| < \|z\|$ sinon (par théorème de Pythagore…). Donc $\Pi(z) = z \Leftrightarrow z \in \bigcap_{i=1}^n \mathrm{Ker}(l_i) = S'$. Comme $F \perp S'$, dès que $z \neq 0$, $\|\Pi(z)\| < \|z\|$. Comme nous sommes en dimension finie, ceci implique que $\|\Pi_{|F}\| < 1$ (par compacité de la sphère unité). □

2 Algèbre (et géométrie)

2.1 Points à distances impaires, avec le déterminant de Gram

Le résultat suivant est tiré d'un petit article : *Are there $n+2$ points in E^n with odd integral distances*, Graham, Rothschild & Straus. Il a été posé comme exercice à l'oral de l'ENS Lyon en 2015. (Peut-être se trouve-t-il dans l'un des Francinou–Gianella…)

Théorème. *Soit $n \in \mathbb{N}^*$. Il existe $n+2$ points distincts à distances entières impaires dans $\mathbb{R}^n$ si et seulement si $n+2 \equiv 0 \mod 16$.*

La preuve originale utilise le *déterminant de Cayley-Menger*, qui permet de calculer le volume de simplexes et généralise ainsi la formule de Héron. On trouvera des détails sur ce fameux déterminant dans le Zavidovique. Nous allons utiliser ici le déterminant de Gram, plus connu, pour éviter des calculs avec des opérations élémentaires sur les lignes et les colonnes.

Preuve du sens direct Soit $n \in \mathbb{N}$ et $x_0, \dots, x_{n+1}$ des points dans $\mathbb{R}^n$ tels que pour tout $i \neq j$, $\|x_i - x_j\| \in 2\mathbb{Z}+1$. Quitte à translater, on peut prendre $x_0 = 0$.

Notons $G = (\langle x_i, x_j \rangle)_{1 \leq i,j \leq n+1}$ la matrice de Gram de $x_1, \dots, x_{n+1}$, J la matrice carrée de taille $n+1$ dont tous les coefficients valent 1, et $A = (a_{ij})_{1 \leq i,j \leq n+1} = I + J$.

Proposition. $\det G = 0$.

Démonstration. Le déterminant de Gram d'une famille liée est toujours nul, et les $x_1, \dots, x_{n+1}$ sont dans $\mathbb{R}^n$ donc sont liés. En effet, si M est la matrice des (x_i) dans une base orthonormale (de taille $n \times (n+1)$), alors $G = M^T M$ a un rang majoré par celui de M, qui est le rang de la famille de vecteurs. □

Proposition. $\det A = n+2$.

Démonstration. J est de rang 1 donc a pour valeur propre 0 avec multiplicité n. On vérifie que $(1, \dots, 1)$ est vecteur propre pour la valeur propre $n+1$, ce qui achève de déterminer le spectre de J. Les valeurs propres de $A = I + J$ sont donc $1, \dots, 1, n+2$, leur produit vaut donc $n+2$. □

On va prouver $\det 2G \equiv \det A \mod 16$, ce qui suffira à conclure avec les deux propositions ci-dessus. Pour cela, regardons ce qu'on peut dire sur $2G$ modulo 16.

Remarque. *Si m est impair, $m^2 \equiv 1 \mod 8$ et $2m^2 \equiv 2 \mod 16$.*

Démonstration. Facile à vérifier à la main ; le second résultat se déduit du premier, pas besoin d'examiner 8 classes de congruence. □

Ainsi, l'identité de polarisation $2\langle x_i, x_j \rangle = \|x_i\|^2 + \|x_j\|^2 - \|x_i - x_j\|^2$ entraîne que les coefficients non diagonaux de $2G$ sont congrus à 1 modulo 8 (remarquer que $\|x_i\|^2 = \|x_i - x_0\|^2$ est bien le carré d'un nombre impair). Quant aux coefficients diagonaux, de la forme $2\|x_i\|^2$, ils sont congrus à 2 modulo 16. Ainsi

$$2G \equiv A + B \mod 16, \qquad B = (b_{ij})_{1 \leq i,j \leq n+1} \in S_{n+1}(\mathbb{Z}),\ b_{ii} = 0,\ b_{ij} \in \{0, 8\}$$

Donc $\det 2G \equiv \det(A+B) \mod 16$ car le déterminant est un polynôme à coefficients entiers en les coefficients de la matrice. Reste à prouver $\det(A+B) \equiv \det A \mod 16$.

Écrivons la formule de Leibniz :

$$\det(A+B) = \sum_{\sigma \in \mathfrak{S}_{n+1}} \varepsilon(\sigma) T_\sigma, \quad T_\sigma = \prod_{i=1}^{n+1} (a_{i\sigma(i)} + b_{i\sigma(i)})$$

$A + B$ étant une matrice symétrique, $T_\sigma = T_{\sigma^{-1}}$ pour tout $\sigma \in \mathfrak{S}_n$ (et en général $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$), et

$$T_\sigma \equiv \prod_{i=1}^{n+1} a_{i\sigma(i)} \mod 8 \quad \text{donc} \quad T_\sigma + T_{\sigma^{-1}} = 2T_\sigma \equiv 2\prod_{i=1}^{n+1} a_{i\sigma(i)} \mod 16.$$

On peut ainsi regrouper les termes de la somme dans $\det(A + B)$ par deux pour montrer la congruence voulue… à l'exception des termes pour $\sigma = \sigma^{-1}$, c'est à dire σ involutif.

Fixons σ une involution et développons T. Étudions les termes comportant au moins un facteur b_i. S'il y en a deux, alors le terme est divisible par 64, donc congru à 0 mod 16. Donc

$$T_\sigma \equiv \prod_{i=1}^{n+1} a_{i\sigma(i)} + \sum_{i=1}^{n+1} t_i \mod 16 \qquad t_i = b_{i\sigma(i)} \prod_{j\neq i} a_{j\sigma(j)} \equiv 0 \mod 8$$

Pour $i \in \{1, \dots, n+1\}$, alors :

— si i est un point fixe de σ, alors $b_{i\sigma(i)} = b_{ii} = 0$ donc $t_i = 0$;

— sinon, σ transpose i et $\sigma(i)$, et $t_i = t_{\sigma(i)}$, toujours par symétrie des matrices A et B.

Finalement, on peut toujours regrouper les termes non nuls par deux, et obtenir que

$$T_\sigma \equiv \prod_{i=1}^{n+1} a_{i\sigma(i)} \mod 16$$

En fin de compte, on a :

$$\det(A + B) \equiv \sum_{\sigma\in\mathfrak{S}_{n+1}} \varepsilon(\sigma) \prod_{i=1}^{n+1} a_{i\sigma(i)} \equiv \det A \mod 16$$

ce qu'il fallait démontrer.

Preuve du sens réciproque Soit $n = 16m - 2$, $m \in \mathbb{N}^*$, plaçons-nous dans l'espace euclidien de dimension n. Soit H un hyperplan et $P_1, \dots, P_n \in H$ les sommets d'un simplexe régulier de centre O, avec $P_iP_j = n/2 = 8m - 1$. On va rajouter à cette famille deux points symétriques par rapport à H, Q et Q', de sorte que le milieu de $[QQ']$ soit O. En prenant $QQ' = 4m - 1$, on peut montrer que $QP_i = Q'P_i = 6m - 1$ pour tout i : on a bel et bien $n + 2$ points à distances impaires.

2.2 Étude des automorphismes extérieurs de $\mathfrak{S}_6$

(Inspiré d'un billet de blog de David Madore.)

Supposons qu'on ait prouvé l'existence d'un automorphisme extérieur (voir à la fin pour une construction). À quoi ressemble l'ensemble de ces automorphismes extérieurs ? Peut-on les décrire tous, de façon combinatoire ? On va présenter ici une description inspirée de celle faite par Sylvester vers 1844 ; au lieu de parler de synthèmes, on utilisera des triples transpositions, qui sont la même chose avec de la structure algébrique en plus.

Pour $x \in \{1, \dots, 6\}$, on note $e(x) = (x\ y_1) \dots (x\ y_5) \in \mathfrak{S}_6$ où $\{y_1, \dots, y_5\} = \{1, \dots, 6\} \setminus \{x\}$. Les éléments la forme $e(x)$ sont appelés *étoiles* et leur ensemble est noté E. e réalise une bijection canonique entre $\{1, \dots, 6\}$ et E.

Proposition. *Toute famille de 5 transpositions distinctes ne commutant pas deux à deux est une étoile.*

Démonstration. Soit $\{\tau_1, \dots, \tau_5\}$ une telle famille. τ_1 et τ_2 ne commutent pas donc $\tau_1 = (a\ b)$, $\tau_2 = (a\ c)$ avec $b \neq c$. De même $\tau_3 = (a'\ b')$, $\tau_4 = (a'\ c')$ avec $b' \neq c'$. τ_1 et τ_3 ne commutent pas non plus, et par l'absurde, si $a' = b$, alors on trouve que τ_2 et τ_3 commutent, contradiction. De même on ne peut pas avoir $a = b'$. Donc $a' = b$. Ainsi $\tau_1, \dots, \tau_4$ ont un élément commun, et on montre facilement que τ_5 aussi. Donc $\{\tau_1, \dots, \tau_5\} = e(a) \in E$. □

Corollaire. *Tout automorphisme qui envoie les transpositions sur des transpositions est intérieur.*

Démonstration. Soit φ cet automorphisme. $\varphi(E) = E$, car « ne pas commuter » est préservé par automorphisme. Posons $g : x \mapsto e^{-1}(\varphi(e(x)))$, $g \in \mathfrak{S}_6$, de sorte que $\varphi(e(x)) = e(g(x))$. Pour tout $a \neq b$, comme $\{(a\ b)\} = e(a) \cap e(b)$, on a $\varphi((a\ b)) = (g(a)\ g(b))$. φ coïncide donc avec $\sigma \mapsto g\sigma g^{-1}$ sur les transpositions, qui engendrent $\mathfrak{S}_6$, donc φ est intérieur. □

Proposition. *Les automorphismes extérieurs de $\mathfrak{S}_6$ échangent transpositions et triples transpositions.*

Démonstration. En effet, ce sont les seules classes de conjugaison d'ordre 2 dont les permutations ont pour signature −1. (Les automorphismes stabilisent $\mathfrak{A}_6$ car c'est le seul sous-groupe distingué non trivial.) □

On peut déjà en déduire que :

Théorème. $\mathrm{Aut}(\mathfrak{S}_6)/\mathrm{Int}(\mathfrak{S}_6) \simeq \mathbb{Z}/2\mathbb{Z}$.

Démonstration. Si $\varphi \in \mathrm{Aut}(\mathfrak{S}_6) \setminus \mathrm{Int}(\mathfrak{S}_6)$ et τ est une transposition, $\varphi(\tau)$ est une triple transposition et $\varphi^2(\tau)$ est une transposition. Ainsi, $\varphi^2 \in \mathrm{Int}(\mathfrak{S}_6)$. □

En fait, on a même un produit semi-direct, mais on va s'intéresser à autre chose.

Soit F l'ensemble des familles de 5 triples transpositions qui ne commutent pas, qu'on appellera *co-étoiles*. Alors $\widehat{\varphi} : X \in E \mapsto \varphi(X) \in F$ est une bijection.

Proposition. *Pour tout $g \in \mathfrak{S}_6$, le diagramme suivant est commutatif :*

$$\begin{array}{ccccc} \{1,\dots,6\} & \xrightarrow{e} & E & \xrightarrow{\widehat{\varphi}} & F \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g(-)g^{-1}} & & \downarrow{\scriptstyle \varphi(g)(-)\varphi(g)^{-1}} \\ \{1,\dots,6\} & \xrightarrow{e} & E & \xrightarrow{\widehat{\varphi}} & F \end{array}$$

Démonstration. Le carré de gauche signifie que la conjugaison sur les étoiles correspond à l'action sur les points, ce qu'on a déjà vu précédemment.

Dans le carré de droite, on veut prouver que $\varphi(gXg^{-1}) = \varphi(g)\varphi(X)\varphi(g^{-1})$, où $X \in E$, donc $X \subset \mathfrak{S}_6$. Mais c'est simplement la propriété de morphisme. □

On en déduit ce diagramme :

$$\begin{array}{ccc} \{1,\dots,6\} & \xrightarrow{\widehat{\varphi^{-1}\circ\varepsilon}} & F \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g(-)g^{-1}} \\ \{1,\dots,6\} & \xrightarrow{\widehat{\varphi^{-1}\circ\varepsilon}} & F \end{array}$$

Ainsi, tout automorphisme extérieur peut s'écrire sous la forme $\varphi(g)(x) = f^{-1}(gf(x)g^{-1})$ avec $f : \{1,\dots,6\} \xrightarrow{\sim} F$ bijective. Or, il y a autant d'automorphismes extérieurs qu'intérieurs (puisque [4] le quotient est $\mathbb{Z}/2\mathbb{Z}$), et $\mathrm{Int}(\mathfrak{S}_6) \simeq \mathfrak{S}_6$ (car on peut retrouver la permutation d'origine à partir de la conjugaison en agissant sur les étoiles !) : il y en a donc 6!, autant que de bijections $\{1,\dots,6\} \xrightarrow{\sim} F$. Donc :

— pour tout f, le φ ainsi défini est bien un automorphisme extérieur ;
— pour tout φ, le f qui convient est unique.

Conclusion Tout automorphisme extérieur de $\mathfrak{S}_6$ se factorise en fait comme la composition de deux isomorphismes entre $\mathfrak{S}_6$ et $\mathfrak{S}(F)$: l'action par conjugaison de $\mathfrak{S}_6$ sur F, et un transfert de structure via une bijection. On a en fait un isomorphisme (qui n'est pas endo) tout à fait canonique entre deux groupes de permutations sur 6 éléments, mais dont les ensembles sous-jacents ne peuvent être identifiés que par un choix non canonique de bijection, induisant alors un automorphisme extérieur.

En langage catégorique, on pourra résumer élégamment tout ceci en disant que l'endofoncteur du groupoïde des ensembles de cardinal 6 qui a tout ensemble X associe les co-étoiles de $\mathfrak{S}(X)$ n'est pas naturellement isomorphe à l'identité.

Une dernière remarque Si deux triples transpositions partagent une transpositions, elles commutent. (En effet, dans $\mathfrak{A}_4$, les doubles transpositions et l'identité forment un sous-groupe isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$, qui est abélien.) Ainsi, les co-étoiles correspondent aux partitions du graphe complet à 6 éléments en 5 triplets d'arêtes disjointes, c'est-à-dire aux *1-factorisations* (un *1-facteur*, aussi appelé *couplage parfait*, est un ensemble d'arêtes tel que chaque sommet soit incident à exactement une arête du couplage ; ici, cela correspond donc aux triples transpositions).

Annexe : construction d'un automorphisme extérieur de $\mathfrak{S}_6$ La construction présentée ici est tirée de Perrin, *Cours d'algèbre*, proposition I.8.11.

Remarque. *Il revient au même trouver un isomorphisme $\varphi : \mathfrak{S}_6 \xrightarrow{\sim} \mathfrak{S}(E)$ qui n'est induit par aucune bijection $\{1,\dots,6\} \to E$.*

(Et remarquons que plus haut, on a bien construit un tel isomorphisme, vers le groupe de permutation des co-étoiles !)

Démonstration. En effet, si $E = \{1,\dots,6\}$, l'isomorphisme (automorphisme, donc) $\mathfrak{S}_6 \to \mathfrak{S}_6$ induit par une permutation σ de $\{1,\dots,6\}$ est exactement la conjugaison par σ (penser à l'action de la conjugaison sur la décomposition en cycles disjoints). On retrouve ainsi les automorphismes intérieurs.

Réciproquement, si $\varphi : \mathfrak{S}_6 \to \mathfrak{S}(E)$ n'est pas induit par une bijection, on a tout de même une égalité de cardinaux entraînant l'existence d'une bijection $f : \{1,\dots,6\} \to E$, et alors quelle que soit f, on vérifie que $\varphi \circ \mathfrak{S}(f)^{-1}$ est un automorphisme extérieur. □

4. Une utilisation du théorème de Lagrange se cache ici. Il faut bien voir que dans tout le développement, on utilise de la théorie des groupes pour éviter d'avoir à faire des dénombrements « à la main »…

Nous allons construire une telle bijection à partir du lemme ci-dessous.

Lemme. *Il existe un sous-groupe $H < \mathfrak{S}_6$ d'indice 6 agissant transitivement sur $\{1, \dots, 6\}$ (pour l'action canonique de $\mathfrak{S}_6$, bien entendu).*

En fait, la situation est la suivante : dans $\mathfrak{S}_n$ pour $n \neq 6$, de tels sous-groupes n'existent pas et les sous-groupes d'indices n sont ceux qui stabilisent un point. Dans $\mathfrak{S}_6$, on a aussi ceux qui stabilisent une co-étoile. La vérification de tout ceci est laissée à la lectrice.

Dans le but d'éviter les raisonnements circulaires, une autre construction de H est présentée ci-dessous.

Démonstration. Faisons agir $\mathfrak{S}_5$ sur ses 5-Sylow par conjugaison. Ceci donne un morphisme de $\mathfrak{S}_5$ dans le groupe des permutations de ces 5-Sylow, qui sont au nombre de 6. Le morphisme est injectif car son noyau ne peut être ni $\mathfrak{S}_5$, ni $\mathfrak{A}_5$: $\mathfrak{S}_5$ s'identifie donc à un sous-groupe H de $\mathfrak{S}_6$, d'indice 6. La transitivité de l'action est garantie par les théorèmes de Sylow. □

Posons maintenant $E = \mathfrak{S}_6/H$ l'ensemble des classes à gauche. $\mathfrak{S}_6$ agit dessus par translation ce qui donne un morphisme $\varphi : \mathfrak{S}_6 \to \mathfrak{S}(E)$. $\mathrm{Ker}(\varphi)$ est distingué dans $\mathfrak{S}_6$, et d'indice au moins 6 (taille d'une orbite), donc c'est $\{\mathrm{id}\}$. φ est ainsi injective, et même bijective entre groupes de même cardinal.

Si f était telle que $\varphi = \mathfrak{S}(f)$, alors le stabilisateur de $H \in E$ pour l'action φ serait le groupe des permutations ayant pour point fixe $f^{-1}(H) \in \{1, \dots, 6\}$. Or ici, le stabilisateur de H contient H, vu comme sous-groupe de $\mathfrak{S}_6$, qui agit transitivement donc dont les éléments n'ont aucun point fixe commun. L'existence d'une telle f est donc impossible. φ est donc un isomorphisme qui n'est pas induit par une bijection.

2.3 Non-isomorphisme exceptionnel (avec la réduction de Jordan)

Dans H2G2 tome 1, ou encore dans le Perrin exercice IV.5.1. Le premier contient des erreurs et le second est un exercice sans correction…

Posons $G = \mathrm{PSL}_4(\mathbb{F}_2)$ et $H = \mathrm{PSL}_3(\mathbb{F}_4)$. On va montrer que :

— $|G| = |H| = 20160$;

— G possède plusieurs classes de conjugaison d'éléments d'ordre 2 ;

— H n'en possède qu'une seule.

En conséquence de ces deux derniers points, $G \not\simeq H$. De plus, on sait que :

Théorème. $\mathrm{PSL}_n(\mathbb{F}_q)$ *est simple sauf pour* $n = 2$ *et* $q = 2, 3$.

Démonstration. C'est long… □

Une fois que nous aurons démontré les affirmations précédentes, ce dernier théorème nous permettra de dire que G et H sont tous deux simples, de même cardinal, et pourtant non isomorphes.

Comment compter les classes de conjugaison ? Rappelons que sur tout corps (pas forcément algébriquement clos), les matrices nilpotentes sont classifiées à similitude près par la réduction de Jordan.

Lemme. *Les classes de similitudes de matrices nilpotentes d'indice 2 dans* $\mathscr{M}_n(K)$ *sont en bijection avec* $\{1, \dots, \lfloor n/2 \rfloor\}$.

Démonstration. Soit une telle classe, elle admet un unique représentant $N = \mathrm{Diag}(J_1, \dots, J_k)$ où les J_i sont des blocs de Jordan, de taille décroissante. $N^2 = 0$ signifie que $J_i^2 = 0$ pour tout i. Les blocs de Jordan sont donc de taille 1 ou 2. On réalise donc la bijection en comptant les blocs d'ordre 2 : il y en a forcément au moins un, sinon $N = 0$, et il peut y en avoir n'importe quel nombre jusqu'à $\lfloor n/2 \rfloor$ (N étant de taille n). □

Corollaire. *Si* K *est de caractéristique 2, il y a* $\lfloor n/2 \rfloor$ *classes de conjugaison d'ordre 2 dans* $\mathrm{GL}_n(K)$.

Démonstration. Soit $A \in \mathrm{GL}_n(K)$. A est d'ordre deux ssi $A \neq I$ et $A^2 = I$, ce qui se réécrit aussi $A^2 - I = 0$ i.e. $(A - I)^2 = 0$ ($K[A]$ étant un anneau commutatif de caractéristique 2), i.e. $A - I$ nilpotente d'indice 2. Et A est conjugué à B (comme éléments du groupe) ssi $A - I$ est semblable à $B - I$ (comme matrices). On est donc ramenés au lemme précédent. □

On a en fait classifié des orbites pour la conjugaison dans $\mathrm{GL}_n(K)$ en prolongeant cette action de groupe à l'espace $\mathscr{M}_n(K)$…

Étude de G On a $G = \mathrm{SL}_4(\mathbb{F}_2)$ car I est la seule homothétie, puis $G = \mathrm{GL}_4(\mathbb{F}_2)$ car $\det A \neq 0 \Leftrightarrow \det A = 1$ (tout ceci parce que $\mathbb{F}_2^* = \{1\}$). Ainsi,

$$|G| = (2^4 - 1)(2^4 - 2)(2^4 - 2^2)(2^4 - 2^3) = 20160.$$

D'autre part, on peut directement appliquer le lemme précédent : il y a $\lfloor 4/2 \rfloor = 2$ classes de conjugaison d'ordre 2.

Étude de H On a tout d'abord $\mathrm{GL}_3(\mathbb{F}_4)/\mathrm{SL}_3(\mathbb{F}_4) \simeq \mathbb{F}_4^*$, puis $H \simeq \mathrm{SL}_3(\mathbb{F}_4)/Z(\mathrm{SL}_3(\mathbb{F}_4))$ avec $Z(\mathrm{SL}_3(\mathbb{F}_4)) \simeq \mathbb{F}_4^*$. En effet, toutes les homothéties sont dans $\mathrm{SL}_3(\mathbb{F}_4)$: pour tout $\lambda \in \mathbb{F}_4^*$, $\det \lambda I = \lambda^3 = 1$ car $\mathbb{F}_4^*$ est un groupe d'ordre 3. Le compte donne

$$|H| = \frac{(4^3-1)(4^3-4)(4^3-4^2)}{3^2} = 20160.$$

Dans $\mathrm{GL}_3(\mathbb{F}_4)$, il y a $\lfloor 3/2 \rfloor = 1$ classe de conjugaison d'ordre 2. Si $A \in \mathrm{SL}_3(\mathbb{F}_4)$ est d'ordre 2, il est donc conjugué à la transvection

$$T = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

ce qui s'écrit $A = PTP^{-1}$ avec $P \in \mathrm{GL}_3(\mathbb{F}_4)$. Peut-on choisir P dans $\mathrm{SL}_3(\mathbb{F}_4)$? Oui, quitte à la multiplier à droite par $\mathrm{Diag}(1, 1, \det P^{-1})$. Tout élément d'ordre 2 est donc conjugué à T dans $\mathrm{SL}_3(\mathbb{F}_4)$.

Passons maintenant au quotient dans $H = \mathrm{PSL}_3(\mathbb{F}_4)$. Soit $A \in \mathrm{SL}_3(\mathbb{F}_4)$ tel que $\overline{A}^2 = \bar{I}$ dans H, c'est-à-dire $A^2 \in Z(\mathrm{SL}_3(\mathbb{F}_4))$. Il existe donc $\lambda \in \mathbb{F}_4^*$ tel que $A^2 = \lambda I$. Soit μ une racine carrée de λ ; il en existe (exactement) une car $x \mapsto x^2$ est un automorphisme (caractéristique 2 + finitude du corps). En posant $B = \mu^{-1}A$, on a $\overline{A} = \overline{B}$ dans H, et $B^2 = I$. B est alors conjugué à T, et en projetant sur le quotient, $\overline{A}$ est conjugué à $\overline{T}$: la classe de conjugaison de ce dernier est donc la seule, CQFD.

2.4 Sous-groupe de Frattini et théorème de la base de Burnside

C'est le problème 3 dans Zavidovique, *Un max de maths*. On propose ici une façon plus courte d'établir les résultats du début.

Théorème (de la base de Burnside)**.** *Toutes les familles génératrices minimales (pour l'inclusion) d'un p-groupe ont même cardinal.*

Lemme. *Soient $H_1, \dots, H_n \trianglelefteq G$ tels que G/H_i soit abélien pour tout i. Alors $G/\bigcap_i H_i$ est abélien.*

Démonstration. En effet, G/H est abélien si et seulement si $D(G) \subseteq H$, où $D(G)$ est le groupe dérivé. □

Fixons maintenant G un p-groupe, c'est-à-dire que $|G| = p^m$ avec p premier.

Lemme. *Soit $H < G$ un sous-groupe strict* maximal. *Alors $H \triangleleft G$ et $G/H \simeq \mathbb{Z}/p\mathbb{Z}$.*

Démonstration. Soit $N_G(H)$ le normalisateur de H dans G. On a $H \subseteq N_G(H) \subseteq G$, or H est maximal, donc soit $N_G(H) = H$, soit $N_G(H) = G$ i.e. $H \triangleleft G$.

Supposons par l'absurde que $N_G(H) = H$. L'équation aux classes pour l'action de H sur $C(H) = \{gHg^{-1} \mid g \in G\}$ s'écrit :

$$[G : H] = [G : N_G(H)] = |C(H)| = \sum_g [H : N_H(gHg^{-1})]$$

Or $[H : N_H(gHg^{-1})] = 1 \Leftrightarrow g \in H$, et sinon $p \mid [H : N_H(gHg^{-1})]$; en effet,

$$N_H(gHg^{-1}) = N_G(gHg^{-1}) \cap H = gN_G(H)g^{-1} \cap H = gHg^{-1} \cap H$$

En réduisant modulo p l'équation aux classes, on a ainsi $0 \equiv 1 \mod p$, contradiction.

On a donc établi $H \triangleleft G$. G/H est un groupe de cardinal p^k avec $k \geq 1$. Si $k > 1$, alors en prenant $x \in G/H$ d'ordre p, on a $\{1\} \subsetneq \langle x \rangle \subsetneq G/H$, qu'on relève par la projection canonique π en $H \subsetneq \pi^{-1}(\langle x \rangle) \subsetneq G$, contredisant la maximalité de H. Donc $|G/H| = p$. □

Posons maintenant $F(G)$ l'intersection des sous-groupes maximaux de G, qui porte le petit nom de *sous-groupe de Frattini*. D'après ce qui précède, on a immédiatement que $F(G) \triangleleft G$ et $G/F(G)$ est abélien. On notera donc additivement :

$$\overline{g} + \overline{g'} = \overline{gg'} \qquad \overline{g}, \overline{g'} \in G/F(G)$$

Proposition. *Pour tout $\overline{g} \in G/F(G)$, $\overline{g^p} = \overline{1}$.*

Démonstration. Soit $g \in G$ un représentant de $\overline{g}$. Pour $H < G$ maximal, notons $[g]_H$ sa classe dans G/H. Comme $G/H \simeq \mathbb{Z}/p\mathbb{Z}$, on a $[g]_H^p = [1]_H$, soit $g^p \in H$. Ainsi, $g^p \in \bigcap_H H = F(G)$. □

On peut donc définir la loi externe

$$\overline{n} \cdot \overline{g} = \overline{g^n} \qquad \overline{n} \in \mathbb{Z}/p\mathbb{Z},\ \overline{g} \in G/F(G)$$

dont on vérifie[5] qu'il munit $G/F(G)$ d'une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel ! Plus explicitement, on a :

$$\forall (n_i) \in \mathbb{Z}/p\mathbb{Z},\ \forall (\overline{g_i}) \in G/F(G), \quad \sum_i \overline{n_i} \cdot \overline{g_i} = \overline{\prod_i g_i^{n_i}}$$

et cette écriture rend évidente la proposition suivante :

5. Les amateurs d'algèbre commutative auront compris qu'il s'agit de passer au quotient sur la structure de $\mathbb{Z}$-module d'un groupe abélien dont l'annulateur contient l'idéal $p\mathbb{Z}$.

Proposition. *Pour tous* $\overline{g_1}, \dots, \overline{g_k} \in G/F(G)$, $\mathrm{Vect}_{\mathbb{F}_p}\{\overline{g_1}, \dots, \overline{g_k}\} = \langle \overline{g_1}, \dots, \overline{g_k} \rangle$.

Ainsi, les parties génératrices minimales de $G/F(G)$ sont des *bases*, la théorie de la dimension nous dit donc qu'elles ont toutes le même cardinal, soit $d = \dim_{\mathbb{F}_p} G/F(G)$.

Pour conclure, il ne reste plus qu'à montrer ceci :

Proposition. *Si* $\{g_1, \dots, g_k\}$ *est une partie génératrice minimale de* G*, alors* $\{\overline{g_1}, \dots, \overline{g_k}\}$ *est une base de* $G/F(G)$ *sur* $\mathbb{F}_p$.

Démonstration. $\{\overline{g_1}, \dots, \overline{g_k}\}$ est évidemment une famille génératrice ; supposons par l'absurde qu'elle ne soit pas libre.

Dans ce cas, $k > d$ et on peut extraire une base ; sans perte de généralité, disons que $\{\overline{g_1}, \dots, \overline{g_d}\}$ est une base de $G/F(G)$, et en particulier engendre $G/F(G)$ comme groupe abélien. On a alors $\langle \{g_1, \dots, g_d\} \cup F(G) \rangle = G$.

Remarquons cependant que $\langle g_1, \dots, g_d \rangle \neq G$ par minimalité ; il existe donc $H < G$ maximal contenant $\langle g_1, \dots, g_d \rangle$. Comme $F(G) \subseteq H$ par définition, on a $\langle \{g_1, \dots, g_d\} \cup F(G) \rangle \subseteq H$: contradiction. □

2.5 Théorème de Lie-Kolchin

Un long exercice dans H2G2 tome 1, corrigé dans la nouvelle édition (p. 238).

Définition. *Le* groupe dérivé $D(G)$ *d'un groupe G est le sous-groupe engendré par les commutateurs* $[g,h] = ghg^{-1}h^{-1}$. *G est dit* résoluble *s'il existe l tel que* $D^l(G) = \{1\}$.

Proposition. *Pour tout $k \in \mathbb{N}$, $D^k(G) \trianglelefteq G$.*

Démonstration. On montre par récurrence que $D^k(G)$ est stable par tout $\varphi \in \mathrm{Aut}(G)$. Le cas de base $k = 0$ est immédiat. Supposons que $\varphi(D^k(G)) = D^k(G)$; alors φ se restreint en un automorphisme de $D^k(G)$ et la formule $\varphi([g,h]) = [\varphi(g), \varphi(h)]$ $(g,h \in D^k(G))$ montre qu'il stabilise $D^{k+1}(G)$.

Il suffit pour conclure d'appliquer ceci à un automorphisme intérieur de G (mais attention, l'automorphisme restreint sur $D^k(G)$ n'est pas forcément intérieur, d'où la nécessité d'une hypothèse de récurrence plus forte que $D^k(G) \trianglelefteq G$). □

L'objectif est de montrer :

Théorème (Lie–Kolchin)**.** *Soit G un sous-groupe résoluble connexe de* $\mathrm{GL}_n(\mathbb{C})$. *Les matrices de G sont cotrigonalisables. De façon équivalente, G est conjugué à un sous-groupe des matrices triangulaires inversibles.*

Si G est abélien, la conclusion est bien connue. Sinon, $n \geq 2$ et il suffit de montrer que G admet un sous-espace stable non triviale : ainsi, on pourra trigonaliser par blocs et conclure par récurrence forte sur n. Attention, la récurrence nécessite d'utiliser le fait que l'extraction d'un bloc diagonal est un morphisme de groupes continu, et d'utiliser la propriété suivante (admise) :

Proposition. *L'image par un morphisme d'un groupe résoluble est résoluble.*

Supposons donc G non abélien. Soit l minimal tel que $D^l(G) = \{1\}$, alors $l \geq 2$ et $H = D^{l-1}(G)$ est abélien.

H est donc cotrigonalisable, et admet donc un vecteur propre commun v. On pose $V = \mathrm{Vect}(Gv)$ où $Gv = \{Mv \mid M \in G\}$. C'est bien un sous-espace stable par G, et non réduit à $\{0\}$; reste à montrer que $V \neq \mathbb{C}^n$.

Montrons que H agit par homothéties sur V. Fixons $A \in H$. Pour tout $P \in G$, $P^{-1}AP \in A$ $(A = D^{l-1}(G) \lhd G)$; v étant vecteur propre commun $P^{-1}APv = \lambda_P v$ pour un certain $\lambda_P \in \mathbb{C}$, ce qui s'écrit aussi $APv = \lambda_P Pv$.

Maintenant, λ_P est une fonction continue de P : en effet, elle s'écrit $\langle APv, Pv\rangle / \|Pv\|^2$ en utilisant le produit hermitien canonique. L'ensemble $\{\lambda_P \mid P \in G\}$ est donc connexe puisque G l'est. Or les λ_P sont inclus dans le spectre de A, invariant par conjugaison, et discret. Donc λ_P est constant. A est donc une homothétie sur Gv, puis sur V.

Si maintenant $V = \mathbb{C}^n$, alors $A \subseteq \mathbb{C}^* I$. Comme A est un groupe dérivé (car G non abélien !) et $\det[g,h] = 1$, $\det = 1$ sur A. D'où $A \subset \mathbb{U}_n I$, or A est connexe, donc A est le groupe trivial. Contradiction. Ainsi, $\{0\} \subsetneq V \subsetneq \mathbb{C}^n$, et on peut enchaîner sur la récurrence.

Dans cette dernière étape, on a besoin de la propriété suivante :

Proposition. *Le groupe dérivé d'un groupe connexe est connexe.*

Démonstration. Admis. □

2.6 Constructibilité des polygones réguliers

Rappelons que l'ensemble des nombres *constructibles* est la clôture quadratique de $\mathbb{Q}$, et qu'il correspond, d'après le théorème de Wantzel, à l'ensemble des affixes dans $\mathbb{C}$ des points repérables par une construction à la règle non graduée et au compas à partir des points 0 et 1.

Théorème (Gauss–Wantzel)**.** *Soit p un nombre premier impair. $\zeta_p = e^{2\pi i/p}$ est constructible si et seulement si p est de la forme $2^n + 1$.*

Dire que ζ_p est constructible revient à dire qu'on peut construire le polygone régulier à p côtés à la règle et au compas.

Remarque. *Dans ce cas, p est appelé* nombre premier de Fermat *et on montre qu'il s'écrit forcément comme $p = 2^{2^m} + 1$.*

Proposition. *Le polynôme minimal de ζ_p est $\Phi_p(X) = X^{p-1} + ... + 1$.*

Démonstration. On a bien $\Phi_p(\zeta_p) = 0$, et on vérifie l'irréductibilité en appliquant à $\Phi_p(X + 1)$ le critère d'Eisenstein. □

Corollaire. $\deg \zeta_p = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

Preuve du sens direct du théorème. Si ζ_p est constructible, alors il est inclus dans une tour d'extensions quadratiques : $\zeta_p \in K_m \supset K_{m-1} \supset ... \supset K_0 = \mathbb{Q}$ avec $[K_m : K_{m-1}] = 2$. Ainsi, $p - 1 = \deg \zeta_p \mid [K_m : K_{m-1}] \times ... \times [K_1 : K_0] = 2^m$, donc $p = 2^n + 1$ avec $n \leq m$. □

Pour le sens réciproque, nous allons considérer le groupe $\mathrm{Gal}(\mathbb{Q}(\zeta_p))/\mathbb{Q}$ des automorphismes de $\mathbb{Q}(\zeta_p)$.

Proposition. $\mathrm{Gal}(\mathbb{Q}(\zeta_p))/\mathbb{Q} \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

Démonstration. Tout d'abord, tout automorphisme $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p))/\mathbb{Q}$ est uniquement déterminé par l'image de ζ_p. Cette image est forcément une racine de Φ_p. Réciproquement, toute racine z de Φ_p détermine un automorphisme de $\mathbb{Q}(\zeta_p)$ par composition des isomorphismes canoniques $\mathbb{Q}(\zeta_p) \simeq \mathbb{Q}(X)/(\Phi_p) \simeq \mathbb{Q}(z)$.

De plus, les racines de Φ_p, i.e. les racines primitives de l'unité, sont en bijection avec $(\mathbb{Z}/p\mathbb{Z})^\times$, via $\bar{k} \mapsto \zeta_p^k$. Ainsi, $\bar{k} \mapsto (\phi_k : \zeta_p \mapsto \zeta_p^k)$ est une bijection vers $\mathrm{Gal}(\mathbb{Q}(\zeta_p))/\mathbb{Q}$, et on vérifie que c'est un morphisme. □

Preuve du sens réciproque. Supposons que $p = 2^n + 1$. Alors $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq \mathbb{Z}/2^n\mathbb{Z}$. Soit σ un générateur du groupe, alors en notant $G_l = \langle \sigma^{2^l} \rangle$, on a

$$\{1\} = G_n \subset G_{n-1} \subset ... \subset G_0 = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$$

Puis, en posant $K_l = \{x \in \mathbb{Q}(\zeta_p) \mid \sigma^{2^l}(x) = x\}$, qui est un sous-corps, on a :

$$\mathbb{Q}(\zeta_p) = K_n \supseteq K_{n-1} \supseteq ... \supseteq K_0 = \mathbb{Q}$$

À ce stade, on peut conclure immédiatement avec la correspondance de Galois : on a $[K_l : K_{l-1}] = [G_{l-1} : G_l] = 2$, donc on a bien obtenu une tour d'extensions quadratiques correspondant à notre tour de sous-groupes. Ainsi, le résultat est trivial d'un point de vue galoisien.

Pour se passer du théorème fondamental de la théorie de Galois, qui est difficile, on va montrer $[K_l : K_{l-1}] > 1$, puis la multiplicativité des degrés permettra de conclure. Posons $x = \sum_{\tau \in G_l} \tau(\zeta_p)$; il est clair que $x \in K_l$. Supposons par l'absurde que $x \in K_{l-1}$. Alors, en notant $\rho = \sigma^{2^l}$,

$$\sum_{\tau \in G_l} \tau(\zeta_p) = x = \rho(x) = \sum_{\tau \in \rho G_l} \tau(\zeta_p)$$

Or, $G_l \cap \rho G_l = \varnothing$ puisque $\rho \notin G_l$, et on a vu tout à l'heure que $(\tau(\zeta_p),\ \tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}))$ est la famille des racines de Φ_p énumérée sans répétition. Cette famille est égale à $(\zeta_p, \dots, \zeta_p^{p-1})$, qui est une base de $\mathbb{Q}(\zeta_p)$, donc en particulier est libre. La relation de liaison obtenue plus haut et donc impossible ; contradiction. □

3 Analyse

3.1 Les fonctions monotones (continues) sont dérivables presque partout

Un joli résultat suggéré par le rapport de jury d'agrég… mais c'est long ! (Peut-être trop pour 15 minutes ?) Ce qui suit est une tentative de démonstration qui s'inspire princpalement des *Leçons d'analyse fonctionnelle* de Riesz & Szokefalvi-Nagy, la fin étant tirée de *Real Analysis*, Royden (ou Royden & Fitzpatrick pour la dernière édition). À la fin de la section, on trouvera des compléments culturels.

On va se restreindre ici aux fonctions monotones *continues*. Même avec cette hypothèse, ça reste technique, attention !

Théorème. *Soit $f : [0,1] \to \mathbb{R}$ une fonction continue croissante. Alors f est dérivable presque partout.*

Définition. *On notera $\Delta f(x,y) = \dfrac{f(y)-f(x)}{y-x}$ pour $x \neq y$ et $f : \mathbb{R} \to \mathbb{R}$.*

Notation dont l'utilité ne fait aucun doute s'agissant de parler de dérivation d'une fonction d'une variable réelle.

Résultats préliminaires Commençons par deux petites propositions. Pour $U \subseteq \mathbb{R}$ un ouvert, notons $CC(U)$ l'ensemble de ses composantes connexes.

Proposition. *Les composantes connexes de U sont des intervalles ouverts disjoints, en nombre au plus dénombrable, dont la réunion est égale à U.*

Démonstration. Admis, mais c'est classique et facile, donc à savoir démontrer sans hésiter. □

Proposition. *Soit $f : [a,b] \to \mathbb{R}$ croissante et $U \subset [a,b]$ ouvert dans $\mathbb{R}$. Alors*

$$\sum_{]c,d[\in CC(U)} (f(d) - f(c)) \leq f(b) - f(a)$$

les termes de la somme étant positifs. Autrement dit, la variation totale *de f sur $[a,b]$ est $f(b) - f(a)$.*

Démonstration. Supposons dans un premier temps $|CC(U)| < \infty$, soit $CC(U) = \{]c_1, d_1[, \dots,]c_n, d_n[\}$ avec $c_1 < d_1 \leq c_2 < \dots \leq d_n$. Alors pour tout i, $f(d_i) \leq f(c_{i+1})$ car f croissante, donc

$$\sum_{i=1}^{n} (f(d_i) - f(c_i)) = -f(c_1) + (f(d_1) - f(c_2)) + \dots + (f(d_{n-1}) - f(c_n)) + f(d_n) \leq f(d_n) - f(c_1)$$

Dans le cas $CC(U)$ dénombrable, il suffit de passer à la limite sur les sous-familles finies. □

Le lemme qui suit est fondamental dans la preuve du théorème.

Lemme (des rayons du soleil)**.** *Soit $f : [a,b] \to \mathbb{R}$ continue et soit $\alpha \in \mathbb{R}$. Posons*

$$O_g(]a,b[,\alpha) = \left\{x \in]a,b[\,|\, \exists y \in]a,x[\,/\, \Delta f(x,y) < \alpha\right\}$$

$$O_d(]a,b[,\alpha) = \left\{x \in]a,b[\,|\, \exists y \in]x,b[\,/\, \Delta f(x,y) > \alpha\right\}$$

Alors $O_g(]a,b[,\alpha)$ et $O_d(]a,b[,\alpha)$ sont ouverts dans $\mathbb{R}$ et

1. *Pour tout $]c,d[\in CC(O_g(]a,b[,\alpha))$, $\Delta f(c,d) \leq \alpha$.*
2. *Pour tout $]c',d'[\in CC(O_d(]a,b[,\alpha))$, $\Delta f(c',d') \geq \alpha$.*

Il faut ***faire un dessin*** pour voir ce qui se passe : l'hypographe de f est éclairé par un faisceau de rayons parallèles de pente α provenant de la gauche dans le cas 1, la droite dans le cas 2, et les ensembles définis sont les zones à l'ombre (la lumière passant à travers les points de tangence). On peut constater visuellement qu'il y a en fait égalité sauf éventuellement pour $d = b$ ou $c' = a$, mais nous n'aurons pas besoin de le prouver formellement.

Remarquons que (1) découle de (2) appliqué à $x \mapsto -f(-x)$, et qu'on peut se ramener à $\alpha = 0$ quitte à soustraire une fonction linéaire. (Et en considérant $-f$, on peut obtenir deux autres cas, consistant à éclairer l'épigraphe au lieu de l'hypographe.) Ce dernier cas est celui généralement énoncé dans la littérature sous le nom de « rising sun lemma » (en effet, $\alpha = 0$ revient à placer le soleil à l'horizon(tale), et les rayons viennent de la droite i.e. de l'est).

Démonstration du « rising sun lemma ». U est ouvert car les inégalités strictes de fonctions continues définissent des ouverts, et une projection linéaire d'un ouvert sur une coordonnée est un ouvert [6].

Soit $]c, d[\in CC(U)$, on veut maintenant montrer que $f(d) - f(c) \geq 0$. Fixons $\varepsilon > 0$. Par compacité, f atteint son maximum sur $[c + \varepsilon, d]$ en un point x. En particulier $f(x) \geq f(d)$. Or $f(d) \geq f(z)$ pour tout $z > d$ car $d \notin U$. Ainsi $f(x) \geq f(y)$ pour tout $y > x$, bref, aucun point ne peut faire de l'ombre à x : $x \notin U$. Or $[c + \varepsilon, d[\subset U$, donc $x = d$. Autrement dit le maximum est atteint en l'unique point d, d'où $f(c + \varepsilon) < f(d)$, et en passant à la limite $f(c) \leq f(d)$. □

Ceci étant établi, c'est parti pour commencer à parler du théorème principal.

Stratégie d'attaque du théorème Soit $f : [0, 1] \to \mathbb{R}$ continue croissante. Définissons ses *dérivées de Dini*

$$D^+f(x) = \limsup_{y \to x^+} \Delta f(x, y) \qquad D^-f(x) = \limsup_{y \to x^-} \Delta f(x, y)$$

$$D_+f(x) = \liminf_{y \to x^+} \Delta f(x, y) \qquad D_-f(x) = \liminf_{y \to x^-} \Delta f(x, y)$$

f est dérivable en un point x si et seulement si ces quatre limites (1) coïncident et (2) sont finies. Nous allons établir que c'est le cas presque partout. Mais d'abord, faisons le lien avec tout ce dont nous avons parlé avant.

Remarque. *Soient $a < b$, $x \in]a, b[$ et $\alpha < D_+f(x)$. Alors $x \in O_d(]a, b[, \alpha)$. De même, si $\alpha > D_-f(x)$, alors $x \in O_g(]a, b[, \alpha)$.*

Démonstration. $\limsup_{y \to y^+} \Delta f(x, y) > \alpha$ et $]x, b[$ est un voisinage à droite de x donc il existe $y \in]x, b[$ tel que $\Delta(x, y) > \alpha$: c'est exactement la condition d'appartenance à $O_d(]a, b[, \alpha)$. □

On dispose enfin de tous les outils pour attaquer le cœur de la preuve !

(1) Existence p.p. de la limite. Montrons dans un premier temps que $D^+f \leq D_-f$ presque partout. Pour cela, fixons $\alpha < \beta$ quelconques et posons

$$S_{\alpha,\beta} = \{x \in]0, 1[\mid D_-f(x) < \alpha < \beta < D^+f\}$$

On veut montrer que $S_{\alpha,\beta}$ est de mesure nulle.

En partant de $E_0 =]0, 1[$, nous allons définir par récurrence deux suites de parties de $\mathbb{R}$: pour $n \in \mathbb{N}$,

$$F_n = \bigcup_{I \in CC(E_n)} O_g(I, \alpha) \qquad E_{n+1} = \bigcup_{I \in CC(F_n)} O_d(I, \beta)$$

6. Banach–Schauder en dimension finie !

On a $E_0 \supset F_0 \supset E_1$ ... et le lemme des rayons du soleil (à l'aide une récurrence triviale) garantit que ce sont des ouverts.

Si $x \in S_{\alpha,\beta}$, la remarque établie plus haut nous dit que comme $D_-f(x) < \alpha$, $x \in F_0$, puis comme $D^+f(x) > \beta$, $x \in E_1$, et ainsi de suite… Au bout du compte, $S_{\alpha,\beta} \subset \bigcap_{n\in\mathbb{N}} E_n$ et nous allons montrer que ce dernier ensemble est négligeable.

Soit $n \in \mathbb{N}$. Soit $]a,b[\in CC(F_n)$, le cas 1 du lemme nous dit que $f(b) - f(a) \leq \alpha(b-a)$. Si maintenant $]c,d[\in CC(E_{n+1} \cap]a,b[)$, alors le cas 2 du lemme donne $f(d) - f(c) \geq \beta(d-c)$. En sommant et en appliquant notre majoration de la variation totale, on a :

$$\beta\mu(E_{n+1}\cap]a,b[) = \sum_{]c,d[} \beta\mu(]c,d[) \leq \sum_{]c,d[} (f(d)-f(c)) \leq f(b)-f(a) \leq \alpha\mu(]a,b[)$$

$$\mu(E_{n+1}) \leq \frac{\alpha}{\beta} \sum_{]a,b[} \mu(]a,b[) = \frac{\alpha}{\beta}\mu(F_n) \leq \frac{\alpha}{\beta}\mu(E_n)$$

où μ est la mesure de Lebesgue. Comme $\alpha/\beta < 1$ et $E_0 = [0,1]$ est de mesure finie,

$$\mu(S_{\alpha,\beta}) \leq \mu\left(\bigcap_{n=0}^{\infty} E_n\right) \leq \lim_{n\to\infty} \left(\frac{\alpha}{\beta}\right)^n \mu(E_0) = 0$$

$$\mu\left(\{x \in]0,1[\mid D^+f(x) > D_-f(x)\}\right) = \mu\left(\bigcup_{\alpha,\beta\in\mathbb{Q}} S_{\alpha,\beta}\right) = 0$$

De façon analogue on peut montrer que $D^-f \leq D_+f$ p.p., ce qui suffit à obtenir l'égalité p.p. des quatre dérivées de Dini : en effet, on sait que lim inf $\leq$ lim sup donc $D_+f \leq D^+f$ et $D_-f \leq D^-f$. □

Notons $f'(x)$ cette limite commune qui existe pour tout x hors d'un ensemble de mesure nulle : on définit ainsi une fonction f', qu'on étend arbitrairement à $\mathbb{R}$. f' est à valeurs dans $\mathbb{R}_+ \cup \{+\infty\}$. En effet, f étant croissante, ses taux d'accroissements sont positifs ; et rien ne garantit a priori que la limite de ces taux d'accroissements soit finie. Reste à montrer :

(2) Finitude p.p. de la dérivée. Calculons d'abord, en prolongeant f par $f(1)$ sur $]1,+\infty[$,

$$\int_0^1 \frac{f(x+h)-f(x)}{h}dx = \frac{1}{h}\int_1^{1+h} f(x)\,dx - \frac{1}{h}\int_0^h f(x)\,dx \xrightarrow[h\to 0^+]{f} (1) - f(0)$$

où la dernière égalité est vraie par continuité de f. Comme f' est mesurable (en tant que limite de fonctions mesurables) et positive, on peut l'intégrer et le lemme de Fatou nous donne

$$\int_0^1 f'(x)\,dx \leq \lim_{h\to 0^+} \int_0^1 \frac{f(x+h)-f(x)}{h}dx = f(1)-f(0) < +\infty$$

Ainsi, f' est positive et intégrale, elle est donc finie presque partout. □

Conclusion En excluant d'abord les points où le taux d'accroissement n'a pas de limite, puis ceux où la limite est $+\infty$, on ne s'est privé que d'en semble de mesure nulle, donc : f est dérivable presque partout !

Le théorème se généralise évidemment à un intervalle de définition quelconques (par union dénombrable de segments compacts), et il est tout aussi clair que l'énoncé s'applique aussi pour f décroissante. Par contre, attention, il n'est pas facile de généraliser à f discontinue !

À propos de l'hypothèse de continuité Cette hypothèse était présente dans la première démonstration de ce théorème par Lebesgue en 1904.

Quand f est discontinue, on pourrait vouloir se restreindre à ses intervalles de continuité pour se ramener au cas qu'on a prouvé. Un contre-exemple à cette stratégie naïve est donné par la fonction $f : x \mapsto \sum_{n\in\mathbb{N}} 2^{-n}\mathbb{1}_{[x\geq q_n]}$ où $(q_n)_{n\in\mathbb{N}}$ est une énumération des rationnels. Il faut donc traiter le cas de ce genre de *fonctions de saut* (et en fait, toute fonction monotone est la somme d'une fonction continue et d'une fonction de saut, puisqu'une fonction monotone a un nombre au plus dénombrable de points de discontinuité).

On trouvera chez Royden une preuve directe du cas général (f potentiellement discontinue) utilisant le lemme de recouvrement de Vitali. Dans ce livre, ce théorème est le premier d'une séquence qui aboutit à montrer que pour les fonctions d'une variable réelle la dérivation est bien l'opération inverse de l'intégrale de Lebesgue (presque partout, évidemment).

Dernière remarque culturelle En utilisant la majoration de la variation totale et le lemme des rayons du soleil, on peut aussi démontrer (et ça a quasiment déjà été fait !) que

$$\mu\left(\left\{x \in]0,1[\mid D^+ f(x) \geq \beta\right\}\right) \leq \frac{f(1)-f(0)}{\beta}$$

ce qui aurait pu permettre de traiter la partie finitude (exercice pour la lectrice). Ce résultat est à comparer avec le suivant, utilisé pour démontrer d'autres théorèmes de dérivation presque partout dans le même esprit (cf. par exemple *An introduction to measure theory* de Terence Tao) :

Théorème (Inégalité maximale de Hardy–Littlewood)**.** *Soit $f \in L^1(\mathbb{R})$, et soit $\beta > 0$. Alors*

$$\mu\left(\left\{x \in \mathbb{R} \;\middle|\; \sup_{h>0} \frac{1}{h}\int_x^{x+h} |f(t)|\,dt \geq \beta\right\}\right) \leq \frac{1}{\beta}\int_{\mathbb{R}} |f(t)|\,dt$$

À ce propos, le lecteur est invité à se pencher sur l'énoncé d'un exercice qui m'a été posé au concours d'entrée des ENS, en 2012 :

1. Montrer que tout ouvert de $\mathbb{R}$ est une réunion disjointe dénombrable d'intervalles ouverts.
2. On prend une fonction continue sur un intervalle de $\mathbb{R}$ et on desssine son graphe. On fait arriver de la droite ($x = +\infty$) un faisceau lumineux de rayons parallèles à l'axe des abscisses. Ce faisceau éclaire certaines parties du graphe, le reste étant dans l'ombre (on considérera qu'un rayon arrivant tangent en un extrémum n'est pas bloqué). Montrer que l'ensemble des abscisses des points à l'ombre est une union disjointe d'intervalles ouverts.
3. Soit $(u_n)_{n\in\mathbb{Z}} \in \mathbb{R}^{\mathbb{Z}}$ une suite *sommable*. On pose $u_N^* = \sup_{n\in\mathbb{N}^*} \frac{1}{n}\sum_{k=0}^{n-1} u_{N+k}$.

   Montrer que $\sum_{\substack{N\in\mathbb{Z}\\ u_N^*>0}} u_N \geq 0$.

L'examinateur affirmait que les question (2) et (3) étaient liées. Quatre ans se sont écoulés avant que je ne comprenne ce lien, en travaillant le développement ci-dessus… (Il est toutefois possible de résoudre l'exercice sans voir le lien.) On admirera au passage les contorsions nécessaires pour contourner l'absence de l'intégrale de Lebesgue au programme des classes préparatoires.

3.2 Lemme de Hoeffding

Il existe deux versions de ce lemme : une faible qui s'applique aux variables aléatoires X avec $-c \leq X \leq c$ p.s., et une autre plus forte qui suppose que $a \leq X \leq b$ p.s. La première se démontre simplement par des inégalités de convexité. La seconde admet une preuve plus compliquée, qui présente l'intérêt de se recaser dans la leçon sur les intégrales à paramètre. Dans les deux cas, on peut en déduire une inégalité de concentration, *l'inégalité de Hoeffding*.

Rappelons que pour X une variable aléatoire réelle, la *fonction génératrice des moments* et la *fonction génératrice des cumulants* sont définies respectivement par

$$M_X(t) = \mathbb{E}\left[e^{tX}\right] \quad \text{et} \quad K_X(t) = \ln M_X(t)$$

Si X est bornée p.s., ces fonctions sont définies et même $\mathscr{C}^\infty$ sur $\mathbb{R}$. De plus, X admet des moments à tout ordre, et M_X est la série génératrice exponentielle des moments, d'où le nom. De même, on appelle *cumulants* les quantités $\kappa_n = K_X^{(n)}(0)$.

Proposition. *$\kappa_1 = \mathbb{E}[X]$ et $\kappa_2 = \mathrm{Var}(X)$.*

Démonstration. Calculer en utilisant la dérivation sous le signe $\int$ (ou plutôt $\mathbb{E}$). □

Fixons à partir de maintenant $a < b$, et X une v.a. réelle avec $a \leq X \leq b$ presque sûrement.

Proposition (Inégalité de Popoviciu)**.** $\mathrm{Var}(X) \leq \dfrac{(b-a)^2}{4}$.

Démonstration. $\mathbb{E}[(X-\mu)^2]$ atteint son minimum $\mathrm{Var}(X)$ en $\mu = \mathbb{E}[X]$; prendre $\mu = (a+b)/2$ pour obtenir l'inégalité. □

Lemme (Hoeffding)**.** $K_X(t) \leq t\mathbb{E}[X] + t^2(b-a)^2/8$.

Démonstration. Fixons $t \in \mathbb{R}$. On peut voir que $K_X(t+s) = K_X(t) + K_{Y_t}(s)$ où Y_t est telle que

$$\mathbb{P}_{Y_t} \ll \mathbb{P}_X, \quad \frac{\mathrm{d}\mathbb{P}_{Y_t}}{\mathrm{d}\mathbb{P}_X} = \frac{e^{tX}}{\mathbb{E}\left[e^{tX}\right]}$$

($\mathbb{P}_{Y_t}, \mathbb{P}_X$ étant les mesures images sur $\mathbb{R}$). En particulier $a \leq Y_t \leq b$ p.s. En dérivant par rapport à s deux fois,

$$K_X''(t) = K_{Y_t}''(0) = \mathrm{Var}(Y_t) \leq \frac{(b-a)^2}{4}$$

On considère maintenant t variable et on intègre deux fois ; l'énoncé du lemme en découle immédiatement. □

On complète le développement en présentant l'application à l'inégalité de Hoeffding.

3.3 Polynômes de Bernstein

Référence : Zuily–Quéffélec, *Éléments d'analyse pour l'agrégation*.

Théorème (Bernstein)**.** *Soit $f \in \mathscr{C}([0,1],\mathbb{R})$.*
Pour $n \in \mathbb{N}$ et $x \in \mathbb{R}$, on pose $B_n(x) = \mathbb{E}[f(X_{n,x})]$ où $X_{n,x} \sim \mathrm{Binom}(n,x)$. Alors :

1. *Pour tout $n \in \mathbb{N}$, $B_n : [0,1] \to \mathbb{R}$ est une fonction polynomiale. (B_n est appelé le n-ième polynôme de Bernstein de f.)*
2. $\|B_n - f\|_\infty \underset{n\to\infty}{=} O\left(\omega_f(n^{-1/2})\right)$.

On rappelle que ω_f est le *module de continuité uniforme* de f :

$$\omega_f(h) = \sup_{|x-y|\le h} |f(x) - f(y)|$$

Corollaire (Théorème de Weierstrass)**.** *Les fonctions polynomiales sont denses dans $\mathscr{C}([0,1])$.*

Notons qu'il est utile de connaître le théorème de Stone-Weierstrass plus général pour répondre aux questions sur le développement.

Preuve du corollaire. Soit $f \in \mathscr{C}([0,1])$. D'après le théorème de Heine, f est uniformément continue, ce qui est équivalent à dire que $\omega_f(x) \to 0$ quand $x \to 0^+$. Ainsi, $\|B_n - f\| \to 0$ quand $n \to +\infty$. □

Lemme. *Pour tous $\lambda, h > 0$, $\omega_f(\lambda h) \le \lceil \lambda \rceil \omega_f(h)$.*

Preuve du lemme. On montre d'abord que ω_f est croissante (c'est évident) et sous-additive (par inégalité triangulaire), puis le lemme en découle facilement. □

Preuve du théorème. La polynomialité de B_n est immédiate en écrivant la formule de l'espérance.
Fixons $x \in [0,1]$. On a

$$|B_n(x) - f(x)| = \left|\mathbb{E}\left[f(X_{n,x}) - f(x)\right]\right| \le \mathbb{E}\left[\left|f(X_{n,x}) - f(x)\right|\right] \le \mathbb{E}[\omega_f(|X_{n,x} - x|)]$$

puis en utilisant le lemme,

$$|B_n(x) - f(x)| \le \mathbb{E}\left[\left\lceil \sqrt{n}|X_{n,x} - x| \right\rceil \omega_f\left(\frac{1}{\sqrt{n}}\right)\right] \le \omega_f\left(\frac{1}{\sqrt{n}}\right)\mathbb{E}\left[\sqrt{n}|X_{n,x} - x| + 1\right]$$

Par inégalité de Cauchy-Schwarz (ou convexité de $t \mapsto t^2$, au choix),

$$\mathbb{E}\left[\sqrt{n}|X_{n,x} - x|\right]^2 \le \mathbb{E}\left[n(X_{n,x} - x)^2\right] = n\mathrm{Var}(X_{n,x}) = x(1-x) \le \frac{1}{4}$$

(on rappelle que $X_{n,x} \sim \mathrm{Binom}(n,x)$, et on connaît la variance d'une loi binomiale).
Finalement, on a :

$$\forall x \in [0,1], \quad |B_n(x) - f(x)| \le \frac{3}{2}\omega_f\left(\frac{1}{\sqrt{n}}\right)$$

et le majorant étant indépendant de x, c'est fini. □

Proposition. *La majoration de la vitesse de convergence est optimale à un facteur près.*

Zuily–Quéffelec fait ça avec l'inégalité de Khintchine, mais on peut aussi invoquer le théorème central limite (qui est plus difficile, mais plus connu) ; en fait, on n'a besoin que de la version pour les variables de Bernouilli, appelée « théorème de Moivre–Laplace » et qui peut être prouvée sans fonctions caractéristiques.

Démonstration. Soit $f : x \in [0,1] \mapsto |x - 1/2|$, on va montrer que $|f(1/2) - B_n(1/2)| = \Omega(\omega_f(n^{-1/2}))$. Remarquons d'abord que f est 1-lipschitzienne, donc $\omega_f(h) \leq h$.

Pour cela, posons $X_n = X_{n,1/2}$. Le TCL nous dit que $2\sqrt{n}(X_n - 1/2) \xrightarrow{\text{loi}} \mathscr{N}(0,1)$. Donc

$$\sqrt{n}\left|B_n\left(\frac{1}{2}\right) - f\left(\frac{1}{2}\right)\right| = \mathbb{E}\left[\sqrt{n}\left|X_n - \frac{1}{2}\right|\right] \xrightarrow[n\to+\infty]{} \frac{1}{2}\mathbb{E}[|Y|] > 0 \quad \text{avec } Y \sim \mathscr{N}(0,1).$$

□

3.4 Récurrence d'une marche aléatoire via séries de Fourier

Un théorème célèbre, avec une preuve étrangement moins célèbre et pourtant stylée, que j'ai découverte dans le cours de processus aléatoires de Josselin Garnier et qui est également trouvable sur Internet.

Théorème (Pólya). *La marche aléatoire symétrique sur $\mathbb{Z}^d$ est* récurrente *si et seulement si $d \leq 2$.*

Précisons ce que signifie « récurrente ». Cette marche aléatoire est définie par la suite de v.a. $S_n = X_1 + ... + X_n$ où les (X_i) sont iid uniformes parmi $\{\pm e_1, ..., \pm e_d\}$. Soit N le nombre de passages à l'origine : $N = \text{Card}\{n \in \mathbb{N} \mid S_n = 0\}$. On dit que la marche est récurrente quand $\mathbb{E}[N] = +\infty$.

Premières remarques On a $\mathbb{E}[N] = \mathbb{E}\left[\sum_{n=0}^{\infty} \mathbb{1}_{\{S_n=0\}}\right] = \sum_{n=0}^{\infty} \mathbb{P}(S_n = 0)$.
On peut ne garder que les termes pairs dans cette somme. En effet, pour tout $n \in \mathbb{N}$, on établit facilement que $\sum_{i=1}^{d} \langle S_n, e_i \rangle \equiv n \mod 2$, ce qui entraîne que $S_n \neq 0$ quand n est impair.
On cherche donc une expression pour $\mathbb{P}(S_n = 0)$, $n = 2m$ avec $m \in \mathbb{N}$.

Utilisation de la fonction caractéristique Si φ est la fonction caractéristique de X_1, alors celle de S_n est égale à φ^n (somme de v.a. indépendantes).

$$\forall x \in \mathbb{R}^d, \quad \varphi(x) = \mathbb{E}\left[e^{i\langle x, X_1\rangle}\right] = \sum_{j=1}^{d} \left(\frac{1}{2d} e^{ix_j} + \frac{1}{2d} e^{-ix_j}\right) = \frac{1}{d} \sum_{j=1}^{d} \cos(x_i)$$

Pour en déduire les probabilités recherchées on utilise :

Lemme. *Soit $k = (k_1, ..., k_d) \in \mathbb{Z}^d$. On a la formule des coefficients de Fourier :*

$$\mathbb{P}(S_n = k) = \frac{1}{(2\pi)^d} \int_{[-\pi,\pi]^d} \varphi_n(x) e^{-i\langle k, x\rangle}$$

En fait, φ_n est une série de Fourier d-dimensionnelle normalement convergente dont les coefficients sont les $\mathbb{P}(S_n = (k_1, ..., k_d))$. Ce n'est pas anecdotique : la preuve qu'on est en train de dérouler repose fondamentalement sur un passage au domaine de Fourier [7] pour convertir une convolution de mesures en produit de fonctions, c'est complètement dans l'esprit de l'analyse de Fourier. Mais ici, pas besoin de toute cette théorie, il suffit de calculer :

Preuve du lemme.

$$\int_{[-\pi,\pi]^d} \varphi_n(x) e^{-i\langle k,x\rangle} dx = \int_{[-\pi,\pi]^d} \mathbb{E}\left[e^{i\langle S_n, x\rangle} e^{-i\langle k,x\rangle}\right] dx = \mathbb{E}\left[\int_{[-\pi,\pi]^d} e^{i\langle S_n - k, x\rangle} dx\right] = \mathbb{E}\left[(2\pi)^d \mathbb{1}_{\{S_n=k\}}\right]$$

où on a pu intervenir $\int$ et $\mathbb{E}$ grâce au théorème de Fubini appliqué à une fonction bornée, donc intégrable sur un produit d'espaces de mesure finie. □

7. Ici les « fréquences » (le dual) sont dans le tore et le « temps » (le primal) est discret ; on est habitués à l'autre sens, mais c'est juste l'involutivité de la dualité de Pontriaguine. Les anglophones parlent de « discrete-time Fourier transform », à ne pas confondre avec la transformée de Fourier discrète d'un signal *fini*.

Ainsi, en se souvenant que φ est à valeurs réelles, ses puissances paires sont positives (!), et

$$(2\pi)^d \mathbb{E}[N] = \sum_{m=0}^{\infty} \int_{[-\pi,\pi]^d} \varphi(x)^{2m} dx = \int_{[-\pi,\pi]^d} \frac{dx}{1-\varphi(x)^2}$$

par convergence monotone, l'expression finale étant valable parce que $|\varphi(x)| < 1$ presque partout. (Si on avait gardé les termes impairs (qui peuvent être négatifs), comme c'est le cas dans certaines références, l'interversion série-intégrale aurait été plus dure à justifier ; il faut une astuce dans ce cas…)

Étude d'une intégrale et conclusion Il s'agit donc de savoir si cette intégrale est finie ou non. $1/(1-\varphi^2)$ part à l'infini exactement aux points où il y a un problème de convergence à savoir $|\varphi| = 1$, soit $(0, \dots, 0)$ ainsi que les 2^d points $(\pm\pi, \dots, \pm\pi)$; et elle est continue en-dehors de ces points. Ces derniers points sont des anti-périodes de φ, donc des périodes de $1/(1-\varphi^2)$: il suffit donc d'étudier l'intégrabilité en 0, sur un voisinage $B(0,\varepsilon)$ où $0 < \varepsilon < \pi$.

Pour $x \to 0$,

$$1 - \varphi(x) = \frac{1}{d}\sum_{j=1}^{d}(1-\cos x_j) \sim -\frac{1}{d}(x_1^2 + \dots + x_d^2)$$

d'où

$$\frac{1}{1-\varphi(x)^2} = \frac{1}{(1+\varphi(x))(1-\varphi(x))} \sim \frac{2d}{\|x\|^2}$$

Finalement, reste à étudier l'intégrabilité de $\|x\|^{-2}$. Un passage en coordonnées polaires et le théorème de Tonelli donnent

$$\int_{B(0,\varepsilon)} \|x\|^{-2}\, dx = \int_{]0,\varepsilon[\times S^{d-1}} r^{-2} \cdot r^{d-1}\, dr\, d\omega = \mathrm{Vol}(S^{d-1}) \int_0^{\varepsilon} r^{d-3}\, dr$$

Ce qui est infini exactement quand $d < 3$, CQFD.

Petit détail : le cas $d = 1$ semble nécessiter un traitement particulier, mais le calcul est bien légal à condition de considérer que $S^0 = \{\pm 1\}$ (c'est bien la convention habituelle) et de prendre pour mesure 0-dimensionnelle la mesure de comptage. Les « coordonnées polaires » correspondent alors à la décomposition en signe et valeur absolue, qui est bien un difféomorphisme entre $\mathbb{R}^*$ et $S^0 \times \mathbb{R}_+^*$!

Si le temps permet… On expliquera pourquoi dans une chaîne de Markov irréductible, un état est récurrent si et seulement si tous le sont, et que dans ce cas, tous les états sont presque sûrement atteints. Ainsi, on a montré qu'un ivrogne qui se déplace dans le plan peut être (presque) sûr de rentrer chez lui.

3.5 Gaussiennes, inversion de Fourier et théorème de continuité de Lévy

Notre but est de montrer, dans le cas $d = 1$ (mais toutes les preuves se généralisent sans mal à d quelconque) :

Théorème (Inversion de Fourier). *Soit $f \in L^1(\mathbb{R}^d)$. Si $\hat{f} \in L^1(\mathbb{R}^d)$, on a pour presque tout $x \in \mathbb{R}^d$:*

$$f(x) = \frac{1}{(2\pi)^d} \int_{\mathbb{R}} \hat{f}(\xi) e^{i\xi \cdot x} \, d\xi = \hat{\hat{f}}(-x).$$

En soi, la démonstration est un peu courte, donc on combine généralement ça avec le calcul de la transformée de Fourier d'une gaussienne (résultat utilisé dans la preuve). C'est utile pour faire rentrer le développement dans la leçon « Illustrer par des exemples quelques méthodes de calcul d'intégrales … », mais pour les autres circonstances, on propose ici un autre complément (suggéré par N. Clozeau) : appliquer la formule d'inversion pour prouver le théorème de continuité de Lévy (sur une variable aléatoire dans $\mathbb{R}$ quelconque, pas forcément à densité !).

Préliminaires sur les gaussiennes On définit la gaussienne d'écart-type $\sigma > 0$ comme $g_\sigma : x \mapsto (\sigma\sqrt{2\pi})^{-1} \exp(-x^2/2\sigma^2)$. On a $g_\sigma \in \mathscr{S}(\mathbb{R})$, donc elle est intégrable tout comme toutes ses dérivées.

Lemme. *Pour tout $f \in L^1(\mathbb{R})$, $g_\sigma * f \xrightarrow[\sigma \to 0]{} f$ dans $L^1(\mathbb{R})$.*

Démonstration. Admis. Cette propriété découle du fait que les gaussiennes sont des approximations de l'unité. □

Attention, convergence L^p n'entraîne pas convergence presque partout ! Par contre, d'une suite qui converge dans L^p, on peut extraire une sous-suite qui converge vers la même limite presque partout, d'où :

Corollaire. *Il existe une suite σ_n décroissante tendant vers 0 telle que $g_{\sigma_n} * f \to f$ p.p.*

(Rappel : toute série absolument convergente dans L^p converge p.p., ça sert dans la preuve de complétude.)

Proposition (Transformée de Fourier des gaussiennes). $\widehat{g_\sigma}(\xi) = \exp\left(-\dfrac{\sigma^2\xi^2}{2}\right) = \dfrac{\sqrt{2\pi}}{\sigma} g_{1/\sigma}(\xi)$.

Démonstration. Il y en a plein, choisissez celle qui vous plaît. Une façon simple est d'utiliser le théorème de dérivation sous le signe intégral pour montrer que c'est une solution de l'équation différentielle $y' = -\sigma^2 xy$. Comme $\widehat{g_\sigma}(0) = 1$ on peut parachuter la solution $\sqrt{2\pi}/\sigma \cdot g_{1/\sigma}$, Cauchy-Lipschitz linéaire assurant l'unicité. □

En itérant deux fois, on a bien $\widehat{\widehat{g_\sigma}} = 2\pi g_\sigma$ (le signe moins a disparu car g_σ est paire) : la formule d'inversion de Fourier est vérifiée par les gaussiennes.

Inversion de Fourier, cas général Soit $f \in L^1(\mathbb{R})$ telle que $\hat{f} \in L^1(\mathbb{R})$. On pose

$$F_\sigma(x) = \int_{\mathbb{R}} \widehat{g_\sigma}(\xi) \hat{f}(\xi) e^{i\xi x} d\xi$$

Un calcul rapide (on écrit la formule intégrale pour $\hat{f}$, puis on utilise Fubini) entraîne que

$$F_\sigma(x) = \widehat{\widehat{g_\sigma}} * f(\xi)$$

On observe que $\widehat{g_\sigma} \longrightarrow 1$ ponctuellement quand $\sigma \to 0$; en passant à la limite sur la suite σ_n du lemme préliminaire, on trouve l'égalité presque partout de la formule d'inversion de Fourier. Pour ce faire on a besoin crucialement que $\hat{f} \in L^1(\mathbb{R})$ pour que le théorème de convergence dominée s'applique.

Application : théorème de continuité de Lévy Rappelons tout d'abord que pour vérifier une convergence en loi, il suffit de tester sur un ensemble de fonctions dont l'adhérence contient $\mathscr{C}_c(\mathbb{R})$, espace de fonctions continues à support compact, alors que la définition de cette convergence fait intervenir les fonctions continues bornées. C'est moralement un argument de densité mais attention, $\mathscr{C}_c(\mathbb{R})$ n'est pas dense dans $\mathscr{C}_b(\mathbb{R})$ pour la norme uniforme !

Théorème (Lévy)**.** *Soit X une variable aléatoire réelle de fonction caractéristique φ, et $(X_n)_{n\in\mathbb{N}}$ une suite de v.a. réelles dont on notera les fonctions caractéristiques φ_n pour $n \in \mathbb{N}$. Alors $X_n \to X$ en loi si et seulement si $\varphi_n \to \varphi$ simplement.*

Démonstration. Le sens direct est évident, prouvons la réciproque. Soit $f \in \mathscr{C}_c^\infty(\mathbb{R})$ (qui est bien dense dans $\mathscr{C}_c(\mathbb{R})$), alors en particulier $f \in \mathscr{S}(\mathbb{R})$ donc f et $\hat{f}$ sont intégrables. Par conséquent, on peut écrire la formule d'inversion de Fourier sur f, puis prendre une espérance :

$$\forall n \in \mathbb{N},\ \mathbb{E}[f(X_n)] = \mathbb{E}\left[\frac{1}{2\pi}\int_{\mathbb{R}} \hat{f}(\xi)e^{i\xi X_n}\,d\xi\right] = \frac{1}{2\pi}\int_{\mathbb{R}} \mathbb{E}\left[\hat{f}(\xi)e^{i\xi X_n}\right]d\xi = \frac{1}{2\pi}\int_{\mathbb{R}} \hat{f}(\xi)\varphi_n(\xi)\,d\xi$$

où l'on a interverti espérance et intégrale par le théorème de Fubini (à justifier). (Au fond, on n'a fait que constater que la transformation de Fourier préserve le produit scalaire.) On peut faire le même calcul pour $\mathbb{E}[f(X)]$, puis comme $|\varphi_n| \leq 1$ et $\hat{f} \in L^1(\mathbb{R})$, le théorème de convergence dominée et notre hypothèse de convergence des φ_n nous donnent

$$\mathbb{E}[f(X_n)] \xrightarrow[n\to\infty]{} \frac{1}{2\pi}\int_{\mathbb{R}} \hat{f}(\xi)\varphi(\xi)\,d\xi = \mathbb{E}[f(X)].$$

□

3.6 Formule de Poisson et formule d'inversion de la fonction thêta

On commence par un résultat qui lie séries de Fourier et transformée de Fourier : 2π-périodiser une fonction revient à garder ses pulsations entières. (Existe aussi en version « 1-périodiser = garder les fréquences entières ».)

Théorème (Formule sommatoire de Poisson)**.** $\forall f \in \mathscr{S}(\mathbb{R}),\ \forall t \in \mathbb{R},\ \sum_{n\in\mathbb{Z}} f(t+2\pi n) = \frac{1}{2\pi}\sum_{n\in\mathbb{Z}} \hat{f}(n)e^{int}$.

Remarque. *Cette égalité se lit aussi comme la transformée de Fourier du peigne de Dirac.*

Démonstration. On vérifie sans difficulté que la série à gauche est normalement convergente sur tout compact, et qu'il en va de même de sa dérivée. Elle définit donc une fonction de $\mathscr{C}^1(R/2\pi\mathbb{Z})$; celle-ci est donc égale à sa série de Fourier.

Il suffit ensuite de calculer les coefficients de Fourier, une interversion série-intégrale (permise par la convergence normale) faisant apparaître la transformée de Fourier de f. □

Voici maintenant une application classique à la *fonction θ de Jacobi*. On peut notamment en déduire l'équation fonctionnelle de la fonction ζ de Riemann ; cf. le développement suivant pour une autre conséquence surprenante.

Théorème. *Soit $\theta : x \mapsto \sum_{n\in\mathbb{Z}} e^{-\pi n^2 x}$. Alors $\theta(1/x) = \sqrt{x}\theta(x)$ pour tout $x \in \mathbb{R}_+^*$.*

Remarque. *La fonction θ est analytique sur le demi-plan $\{\Re(z) > 0\} \subset \mathbb{C}$, et l'identité s'étend par unicité du prolongement analytique à ce demi-plan, où il existe une unique détermination de la racine carrée coïncidant avec celle sur $\mathbb{R}_+^*$.*

La preuve fera intervenir les gaussiennes $g_\sigma : t \mapsto (\sigma\sqrt{2\pi})^{-1}\exp(-t/2\sigma^2)$, et on utilisera (cf. développement « inversion de Fourier ») :

Proposition (Transformée de Fourier d'une gaussienne)**.** $\widehat{g_\sigma}(\omega) = \exp\left(-\frac{\sigma^2\omega^2}{2}\right)$.

Preuve de l'équation fonctionnelle. Fixons $x \in \mathbb{R}_+^*$.

$$\theta(x) = \sum_{n\in\mathbb{Z}} \sigma(x)\sqrt{2\pi}\cdot g_{\sigma(x)}(2\pi n) \quad \text{où} \quad \sigma(x)^2 = \frac{2\pi}{x}.$$

$g_{\sigma(x)}$ étant dans $\mathscr{S}(\mathbb{R})$, la formule de Poisson peut s'appliquer :

$$\theta(x) = \frac{\sigma(x)\sqrt{2\pi}}{2\pi}\sum_{n\in\mathbb{Z}} \widehat{g_{\sigma(x)}}(n) = \frac{\sigma(x)}{\sqrt{2\pi}}\sum_{n\in\mathbb{Z}} \exp\left(-\frac{\sigma(x)^2n^2}{2}\right) = \frac{1}{\sqrt{x}}\sum_{n\in\mathbb{Z}} \exp\left(-\frac{\pi n^2}{x}\right) = \frac{\theta(1/x)}{\sqrt{x}}.$$

□

Application (Un développement asymptotique)**.** $\sum_{n\in\mathbb{Z}} x^{n^2} \underset{x\to 1^-}{\sim} \sqrt{\frac{\pi}{-\ln x}}$

Démonstration. On a une série entière de rayon de convergence 1, donc elle est bien définie au voisinage à droite de 1. Écrivons l'équation fonctionnelle pour $x \in]0,1[$

$$\sum_{n\in\mathbb{Z}} x^{n^2} = \theta\left(\frac{-\ln x}{\pi}\right) = \sqrt{\frac{\pi}{-\ln x}}\,\theta\left(\frac{\pi}{-\ln x}\right)$$

Il suffit de vérifier que $\theta(u) = 1 + 2\sum_{n=1}^{\infty} e^{-\pi n^2 u} \to 1$ quand $u \to +\infty$ ($u = -\pi/\ln x$) et c'est bon… □

3.7 Équivalent asymptotique de la fonction thêta et sommes de Gauss

…ou comment caser un morceau de preuve de la réciprocité quadratique (!) dans des leçons d'analyse. Référence livresque : Richard Bellman[8], *A brief introduction to theta functions*. Voir aussi l'article d'Anders Karlsson, *Applications of heat kernels on abelian groups : $\zeta(2n)$, quadratic reciprocity, Bessel integrals*, qui raconte également d'autres applications fort jolies de cette fameuse fonction thêta. Cependant, aucun des deux ne fournit de preuve rigoureuse complète.

On renvoie au développement précédent (Formule de Poisson et formule d'inversion de la fonction thêta) pour la définition de la fonction θ de Jacobi et son équation fonctionnelle. Dans tout ce qui suit, on fixe $p, q \in \mathbb{N}^*$ premiers entre eux. La *somme de Gauss* associée est :

$$S(p,q) = \sum_{k \in \mathbb{Z}/q\mathbb{Z}} \exp(-i\pi k^2 p/q)$$

On va montrer le résultat suivant, à partir duquel la loi de réciprocité quadratique (!) se déduit :

Théorème (Réciprocité des sommes de Gauss)**.** $\sqrt{p}S(p,q) = e^{-i\pi/4}\sqrt{q}\overline{S(q,p)}$, *i.e.*

$$\frac{1}{\sqrt{q}} \sum_{k \in \mathbb{Z}/q\mathbb{Z}} \exp\left(\frac{-i\pi k^2 p}{q}\right) = \frac{e^{-i\pi/4}}{\sqrt{p}} \sum_{k \in \mathbb{Z}/p\mathbb{Z}} \exp\left(\frac{i\pi k^2 q}{p}\right)$$

Cette identité exacte peut en fait être obtenue à partir d'un équivalent asymptotique de $\theta(x + ip/q)$ pour $x \to 0^+$.

Lemme. *Soit $k \in \mathbb{N}^*$. Quand $x \to 0^+$,* $\displaystyle\sum_{l=0}^{+\infty} \exp(-\pi(k+lq)^2 x) \sim \frac{1}{2q\sqrt{x}}$.

Démonstration. La fonction $f : t \mapsto \exp(-\pi(k+tq)^2 x)$ est décroissante et intégrable sur $\mathbb{R}_+$, donc par comparaison série-intégrale,

$$\sum_{l \geq 1} f(l) \leq \int_0^{+\infty} f(t)\,dt \leq \sum_{l \geq 0} f(l) \quad \text{soit} \quad 0 \leq \sum_{l \geq 0} f(l) - \int_0^{+\infty} f(t)\,dt \leq f(0) = e^{-\pi k^2 x} \leq 1$$

Calculons l'intégrale :

$$\int_0^{+\infty} \exp(-\pi(k+tq)^2 x)\,dt = \frac{1}{q\sqrt{\pi x}} \int_{k\sqrt{\pi x}}^{+\infty} e^{-u^2}\,du \underset{x \to 0^+}{\sim} \frac{1}{2q\sqrt{x}} \qquad (u = \sqrt{\pi x}(k+tq))$$

□

Proposition. *Quand $x \to 0^+$,* $\displaystyle\theta\left(x + i\frac{p}{q}\right) \sim \frac{S(p,q)}{q\sqrt{x}}$.

Démonstration. Par une interversion de sommes, justifiée par la sommabilité de la famille considérée, on obtient facilement que

$$\sum_{n \in \mathbb{N}^*} \exp\left(-\pi n^2 \left(x + i\frac{p}{q}\right)\right) = \sum_{k=1}^{q} \left(\sum_{l \in \mathbb{N}} \exp(-\pi(k+lq)^2 x)\right) \exp\left(\frac{-i\pi k^2 p}{q}\right)$$

8. Un analyste qui a aussi eu une carrière fructueuse de mathématicien appliqué : il est l'inventeur de la *programmation dynamique*, qui est au programme de l'agrég option D en algorithmique, mais intervient aussi en recherche opérationnelle et théorie du contrôle.

Grâce au lemme, on sait que les sommes intérieures sont équivalentes à $1/2q\sqrt{x}$, donc

$$\theta\left(x+i\frac{p}{q}\right) = 1 + 2\sum_{n\in\mathbb{N}^*} \exp\left(-\pi n^2\left(x+i\frac{p}{q}\right)\right) \underset{x\to 0^+}{\sim} \frac{S(p,q)}{q\sqrt{x}}$$

□

Maintenant, écrivons l'équation fonctionnelle de θ :

$$\theta\left(\frac{1}{x+ip/q}\right) = \sqrt{x+i\frac{p}{q}} \times \theta\left(x+i\frac{p}{q}\right) \underset{x\to 0^+}{\sim} e^{i\pi/4}\sqrt{\frac{p}{q}} \times \frac{S(p,q)}{q\sqrt{x}}$$

D'autre part, on a

$$\frac{1}{x-ip/q} \underset{x\to 0^+}{=} x\frac{q^2}{p^2} + i\frac{q}{p} + O(x^2)$$

Arnaquons maintenant allègrement en considérant que notre équivalent asymptotique, valable quand $z \to ip/q$ en suivant une demi-droite parallèle à $\mathbb{R}_+$, le reste en suivant un courbe qui finit par être tangente à cette demi-droite. Alors

$$\theta\left(\frac{1}{x+ip/q}\right) = \overline{\theta\left(\frac{1}{x-ip/q}\right)} \underset{x\to 0^+}{\sim} \frac{\overline{S(q,p)}}{p\sqrt{xq^2/p^2}}$$

On voit donc apparaître du $S(q,p)$! En simplifiant et en comparant nos deux équivalents asymptotiques, on obtient l'identité arithmétique désirée.

Pour que ça marche vraiment, il faudrait étendre le cadre de validité du lemme, en faisant une comparaison série-intégrale plus subtile, peut-être en utilisant une formule du genre

$$\int_0^{+\infty} f(t)\,dt - \sum_{n=1}^{+\infty} f(n) = \int_0^{+\infty} (t - \lfloor t \rfloor) f'(t)\,dt$$

On pourrait dire qu'en fin de compte, on obtient la loi de réciprocité quadratique par une comparaison série-intégrale !

3.8 Théorème taubérien fort de Littlewood

Référence : Gourdon, *Analyse*. La preuve astucieuse du Gourdon a été découverte par Jovan Karamata ; elle figure déjà telle quelle dans un livre de 1939, *The Theory of Functions* de Titchmarsh. On propose ici une variante de la méthode de Karamata avec moins de découpage d'ε, en utilisant des sommes de Riemann ainsi qu'en sortant un peu du programme de prépa. (Sans doute ne suis-je pas la première personne à découvrir cette astuce, mais je n'ai pas de référence.)

Pour présenter ce développement, il faut un peu de culture sur les théorèmes abéliens et taubériens, en particulier savoir énoncer le théorème d'Abel radial ou angulaire, dont le résultat suivant est une réciproque partielle.

Théorème (Littlewood[9])**.** *Soit $(a_n) \in \mathbb{R}^n$ telle que $a_n = O(1/n)$ quand $n \to +\infty$. En particulier, la série entière $F(x) = \sum_{n\in\mathbb{N}} a_n x^n$ a un rayon de convergence au moins 1.*

Alors, si $F(x) \to c \in \mathbb{R}$ quand $x \to 1^-$, alors $\sum_{n\in\mathbb{N}} a_n$ est convergente et vaut c.

Exemple. $1 - \dfrac{1}{2} + \dfrac{1}{3} - \dfrac{1}{4} + \ldots = \ln 2$.

Il suffit de montrer le théorème pour $c = 0$, quitte à soustraire c à a_0.

Stratégie globale Soit Θ l'ensemble des fonctions $\theta : [0,1] \to \mathbb{R}$ telles que

— $\displaystyle\sum_{n\in\mathbb{N}} a_n\theta(x^n)$ converge pour $0 \le x < 1$;

— $\displaystyle\sum_{n\in\mathbb{N}} a_n\theta(x^n) \xrightarrow[x\to 1^-]{} 0$.

Remarquons que Θ est un espace vectoriel.

On va montrer que $g = \mathbb{1}_{[1/2,1]} \in \Theta$, ce qui établira le théorème : en effet, dans ce cas,

$$\forall N \in \mathbb{N},\ S_N = \sum_{n=0}^{N} a_n = \sum_{n=0}^{\infty} a_n g(x_N^n) \quad \text{avec } x_N = 2^{-1/N} \xrightarrow[N\to+\infty]{} 1^-$$

et par composition de limites $S_N \to 0$ quand $N \to +\infty$.

Lemme. *Si P est un polynôme s'annulant en 0, alors $P \in \Theta$.*

Démonstration. Par linéarité, il suffit de le montrer pour les monômes. Si $\theta(x) = x^k$ pour $k \ge 1$, alors comme $(x^n)^k = x^{nk} = (x^k)^n$, on a $\sum_{n\in\mathbb{N}} a_n f(x^n) = \theta(x^k)$, puis on conclut par composition de limites. □

Lemme. *Si $f : [0,1] \to \mathbb{R}$ est continue par morceaux (ou plus généralement bornée et Riemann-intégrable[10]), alors*

$$(1-x)\sum_{n=0}^{\infty} x^n f(x^n) \xrightarrow[x\to 1^-]{} \int_0^1 f(t)\,dt$$

Démonstration. La série se réécrit $\sum_{n=0}^{\infty}(x^n - x^{n+1})f(x^n)$ et on reconnaît donc une somme de Riemann infinie associée à la subdivision $]0,1] = \bigcup_{n\in\mathbb{N}}]x^{n+1}, x^n]$! Comme la finesse de cette subdivision est $1 - x$, et tend vers 0 quand $x \to 1^-$, la somme de Riemann converge vers l'intégrale.

Ceci est légèrement une arnaque dans la mesure où le théorème habituel de convergence des sommes de Riemann est énoncé pour des subdivisions finies, mais on peut montrer qu'il est aussi valable pour des subdivisions dénombrables. □

9. À ne pas confondre avec le théorème taubérien de Hardy–Littlewood, qui parle de convergence au sens de Cesàro ! La méthode de Karamata pouvant aussi être appliquée pour démontrer ce théorème.

10. Remarque culturelle : une fonction bornée est Riemann-intégrable si et seulement si son ensemble de points de discontinuités est de mesure nulle.

Écrivons maintenant $g(x) = x + x(1-x)h(x)$ où, pour $x < 1/2$, $h(x) = 1/(x-1)$, et pour $x \geq 1/2$, $h(x) = 1/x$.

Les fonctions polynomiales étant denses dans $L^1([0,1])$ (corollaire du théorème de Weierstrass), il existe $Q \in \mathbb{R}[X]$ tel que $\|h - Q\|_1 < \varepsilon$. Posons alors $P(X) = X + X(1-X)Q(X)$: c'est une approximation de g. (Au passage, tout polynôme P avec $P(0) = 0$ et $P(1) = 1$ s'écrit sous cette forme, ce qui motive l'introduction de h.)

On a alors :

$$\left|\sum_{n\in\mathbb{N}} a_n g(x^n) - \sum_{n\in\mathbb{N}} a_n P(x^n)\right| \leq \sum_{n\in\mathbb{N}} |a_n| \cdot |g - P|(x^n) = \sum_{n\in\mathbb{N}} |a_n| \cdot x^n(1-x^n) \cdot |h - Q|(x^n)$$

Comme $1 - x^n = (1-x)(1 + ... + x^{n-1}) \leq n(1-x)$, $|a_n|(1-x^n) \leq n|a_n|(1-x)$. Or $n|a_n| = O(1)$ par hypothèse. Donc il existe $M > 0$ tel que

$$\left|\sum_{n\in\mathbb{N}} a_n g(x^n) - \sum_{n\in\mathbb{N}} a_n P(x^n)\right| \leq M(1-x) \sum_{n\in\mathbb{N}} x^n |h - Q|(x^n)$$

Soit :

$$\left|\sum_{n\in\mathbb{N}} a_n g(x^n)\right| \leq \left|\sum_{n\in\mathbb{N}} a_n P(x^n)\right| + M(1-x) \sum_{n\in\mathbb{N}} x^n |h - Q|(x^n)$$

En passant à la limite avec les lemmes précédents, sachant que $P \in \Theta$ et que $|h - Q|$ est continue par morceaux :

$$\limsup_{x\to 1^-} \left|\sum_{n\in\mathbb{N}} a_n g(x^n)\right| \leq 0 + M \int_0^1 |h(t) - Q(t)|dt = M\|h - Q\|_1 < M\varepsilon$$

D'où, finalement,

$$\sum_{n\in\mathbb{N}} a_n g(x^n) \xrightarrow[x\to 1^-]{} 0$$

3.9 Théorème du point fixe de Brouwer $\mathscr{C}^1$

Soit $n \geq 2$ un entier. On note D^n la boule unité fermée de $\mathbb{R}^n$, et $S^{n-1} = \partial D^n$ la sphère unité.

Théorème (Brouwer)**.** *Toute application $f \in \mathscr{C}^1(D^n, D^n)$ admet un point fixe.*

Remarque. *On en déduit le théorème pour $f \in \mathscr{C}^0(D^n, D^n)$.*

Preuve de la remarque. On approxime f par une suite de fonctions $\mathscr{C}^1$ qui convergent uniformément ; chacune admet un point fixe, et on extrait une sous-suite convergente.

Attention : il faut s'assurer que les approximations de f soient bien à valeur dans D^n et non dans une boule de rayon $1 + \varepsilon$. □

S'il existait un contre-exemple f au théorème, alors on pourrait définir la rétraction

$$r : x \mapsto \frac{f(x) - x}{\|f(x) - x\|}$$

qui contredirait le lemme suivant :

Lemme (de non-rétraction $\mathscr{C}^1$)**.** *Il n'existe pas de fonction $r \in \mathscr{C}^1(D^n, S^{n-1})$ telle que $r \restriction_{S^{n-1}} = \mathrm{id}$.*

Remarque. *En topologie algébrique, on prouve que D^n et S^{n-1} n'ont pas le même type d'homotopie ; une conséquence est qu'il n'existe pas non plus de rétraction $\mathscr{C}^0$.*

Preuve du lemme. Par l'absurde, soit r un contre-exemple. Posons, pour $t \in [0, 1]$, $f_t = (1-t)\mathrm{id} + tr$, et définissons

$$P(t) = \int_{D^n} \det J_{f_t}(x)\, dx = \int_{D^n} \det((1-t)I + tJ_r(x))\, dx$$

où $J_r(x)$ désigne la matrice jacobienne de r au point x.

La seconde expression montre que la fonction P est *polynomiale*, ce qui résulte de la polynomialité du déterminant en développant l'intégrande. Comme $r(D^n)$ est d'intérieur vide, J_r s'annule partout (contraposée du théorème d'inversion locale) donc $P(1) = 0$.

Soit maintenant $t \in [0, 1/(1+M)[$ où $M = \sup |||J_r|||$. Alors pour tout $x \in D^n$, $1 - t > tM \geq |||tJ_r|||$, donc J_{f_t} est inversible (propriété classique des algèbres de Banach). De plus, si $f_t(x) = f_t(y)$, alors

$$(1-t)(x-y) = t(r(y) - r(x)) \quad \text{d'où} \quad (1-t)\|x-y\| = t\|r(x) - r(y)\| \leq tM\|x-y\|$$

par inégalité des accroissements finis. Ceci contredit $1 - t > tM$ à moins que $\|x - y\| = 0$: f est donc injective.

Le théorème d'inversion globale nous dit donc que f_t est un difféomorphisme pour des petites valeurs de t. Ainsi, la formule de changement de variable s'applique immédiatement à la définition de $P(t)$ (ou presque ! modulo une valeur absolue qu'on évacue en vérifiant que l'intégrande est toujours positive), et donne $P(t) = \mathrm{Vol}(f_t(D^n))$.

Que peut-on dire sur l'image de f_t ? Tout d'abord, comme D^n est compact, $f_t(D^n)$ est compacte, donc fermée dans D^n. $f_t(D^n) \setminus S^{n-1}$ est donc un fermé relatif de la boule ouverte. Souvenons-nous maintenant que r est une rétraction : on a donc $f_t(S^{n-1}) = S^{n-1}$, d'où par injectivité $f_t(D^n) \setminus S^{n-1} = f_t(D^n \setminus S^{n-1})$. Le membre de droite est un ouvert, car $D^n \setminus S^{n-1}$ est un ouvert de $\mathbb{R}^n$ et f_t un difféomorphisme local. $f_t(D^n \setminus S^{n-1})$ est donc à la fois ouvert et fermé relativement à $D^n \setminus S^{n-1}$, et non vide, donc par connexité, on a finalement $f_t(D^n) = D^n$.

Mais alors, la fonction polynomiale P est constante égale à $\mathrm{Vol}(D^n)$ sur $[0, 1/(1+M)[$, donc l'est partout. Or $\mathrm{Vol}(D^n) \neq 0$ et $P(1) = 0$, contradiction. □

3.10 Théorème d'existence de Cauchy-Peano par méthode de point fixe

Théorème (Schauder)**.** *Soit K une partie compacte convexe non vide d'un espace vectoriel normé. Alors toute application continue $f : K \to K$ admet un point fixe.*

En dimension finie, ce n'est autre que le théorème de point fixe de Brouwer. Le théorème suivant donne un exemple d'application dans un espace de fonctions de dimension infinie.

Théorème (Cauchy–Peano)**.** *Soit $f : I \times U, \mathbb{R}^d$ où I est un intervalle ouvert contenant 0 et $U \subseteq \mathbb{R}^d$ ouvert. Soit $y_0 \in U$. Si f est* continue*, alors le problème de Cauchy*

$$y'(t) = f(t, y(t)) \quad y(0) = y_0$$

admet au moins une solution locale au voisinage de 0.

Preuve du théorème de Cauchy–Peano. Le problème est équivalent à l'équation intégrale

$$y(t) = y_0 + \int_0^t f(u, y(u))\, du = \Phi(y)(t) \qquad \Phi : y \mapsto \left(t \mapsto y_0 + \int_0^t f(u, y(u))\, du \right)$$

donc se formule comme recherche d'un point fixe de l'application Φ. Reste à savoir sur quel espace cette application est définie…

Fixons $a > 0$ tel que $[-a, a] \subset I$ et $\bar{B}(y_0, a) \subset U$. Sur le compact $[-a, a] \times \bar{B}(y_0, a)$, $|f|$ atteint un maximum M. Soit $b = \min(a, a/M)$. Posons

$$K = \left\{ y \in \mathscr{C}([-b, b], \bar{B}(y_0, a)) \;\middle|\; y \text{ } M\text{-lipschitzienne} \right\}$$

Il est clair que K est non vide (il contient l'application $t \mapsto y_0$) et convexe. K est compact en vertu du théorème d'Ascoli : les fonctions dans K sont toutes à valeurs dans un même compact, et équicontinues car elles ont la même constante de Lipschitz.

Pour appliquer le théorème de Schauder, il ne reste qu'à montrer que Φ est bien définie et continue sur K et que $\Phi(K) \subseteq K$. Soit $y \in K$. Puisque y est à valeurs dans $\bar{B}(y_0, a) \subset U$, $f(t, y(t))$ est définie pour tout t, ce qui assure que $\Phi(y)$ est définie. Pour $-b \leq s < t \leq b$,

$$|\Phi(y)(s) - \Phi(y)(t)| \leq \int_s^t |f(u, y(u))|\, du \leq M(t - s) \quad \text{car} \quad (u, y(u)) \in [-a, a] \times \bar{B}(y_0, a)$$

d'où le caractère M-lipschitzien. De plus, comme $\Phi(y)(0) = y_0$, on en déduit que $\Phi(y)$ est à valeurs dans $\bar{B}(y_0, Mb) \subseteq \bar{B}(y_0, a)$. Donc $\Phi(y) \in K$.

Enfin, pour ce qui est de la continuité,

$$\|\Phi(y) - \Phi(z)\| \leq \int_{-b}^{b} |f(u, y(u)) - f(u, z(u))|\, du \xrightarrow[z \to y]{} 0$$

par convergence dominée (domination sur $[-b, b]$ par $2M$) ou par un argument de convergence uniforme plus long à détailler. □

Preuve du théorème de Schauder. On va admettre le théorème de Brouwer (cf. développement « théorème de Brouwer $\mathscr{C}^1$ »)) et se ramener au cas de la dimension finie.

Soit $\varepsilon > 0$. Par précompacité, K peut être recouvert par un nombre fini de boules ouvertes de rayon ε et de centres $x_1, \ldots, x_n$. Soit $C = \mathrm{Conv}(x_1, \ldots, x_n) \subseteq K$; c'est un compact convexe en dimension finie car $C \subset \mathrm{Vect}(x_1, \ldots, x_n)$.

C est ainsi une ε-approximation de K par un convexe compact ; approximons maintenant f en posant

$$g_\varepsilon : x \in C \mapsto \frac{\sum_{i=1}^n h_i(f(x))x_i}{\sum_{i=1}^n h_i(x)} \quad \text{où} \quad h_i(x) = \min(0, \varepsilon - \|x - x_i\|) \geq 0$$

Il est clair que si g_ε est bien définie (i.e. son dénominateur ne s'annule jamais), alors elle est continue.

Soit $x \in K$. Comme $h_i(f(x)) > 0 \Leftrightarrow d(f(x), x_i) < \varepsilon$, $g_\varepsilon(x)$ est un barycentre à poids strictement des points de $x_1, \dots, x_n$ à distance $< \varepsilon$ de $f(x)$. De tels points existent par la condition de recouvrement. Ainsi :

— $g_\varepsilon(x)$ est bien défini ;
— c'est un barycentre des $x_1, \dots, x_n$, donc $g_\varepsilon(x) \in C$;
— $\|g_\varepsilon(x) - f(x)\| < \varepsilon$ par convexité de $B(f(x), \varepsilon)$.

Ainsi, $g_\varepsilon \in \mathscr{C}(C, C)$. Par le théorème de Brouwer, g_ε admet un point fixe x_ε. La famille $(x_\varepsilon)_{\epsilon>0}$ admet une valeur d'adhérence $x_0 \in K$. Montrons que x_0 est un point fixe de f.

Pour tout $\varepsilon > 0$, $\|f(x_\varepsilon) - x_\varepsilon\| = \|f(x_\varepsilon) - g(x_\varepsilon)\| < \varepsilon$. En passant à la limite sur une suite $(\varepsilon_n)_{n\in\mathbb{N}}$ telle que $\varepsilon_n \to 0$ et $x_{\varepsilon_n} \to x_0$, on a $\|f(x_0) - x_0\| = 0$, soit $f(x_0) = x_0$. □

Moralement, on a démontré et utilisé une version plus fine de la propriété suivante :

Proposition. *Si K est une partie compacte d'un espace vectoriel normé E, alors pour tout $\varepsilon > 0$, il existe un sous-espace $F \subset E$ de dimension finie tel que K soit compris dans le voisinage d'épaisseur ε de F.*

3.11 Stabilité asymptotique d'un équilibre

On prouve ici que pour montrer qu'un point d'équilibre est asymptotiquement stable, il suffit de linéariser à son voisinage et de vérifier que c'est le cas du système linéarisé.

Théorème. *Considérons le système différentiel autonome*

$$x'(t) = f(x(t)) \qquad f \in \mathscr{C}^1(R^n, R^n)$$

Supposons que 0 soit un point d'équilibre et que $Df(0)$ ait toutes ses valeurs propres de partie réelle strictement négatives. Alors il existe un voisinage V de 0 tel que pour tout solution vérifiant $x(0) \in V$, $x(t) \to 0$ quand $t \to +\infty$.

Ce résultat est semble-t-il dû à Perron. C'est aussi un cas particulier du *théorème de stabilité de Lyapunov*. La démonstration par construction d'une fonction de Lyapunov est présentée dans le Rouvière, qui renvoie vers Coddington & Levinson, *Theory of Ordinary Differential Equations*, pour une preuve plus expéditive ; c'est cette dernière qui est présentée ici.

On va utiliser le *lemme de Grönwall* sous la forme intégrale simplifiée suivante :

Lemme. *Soient $\alpha \in \mathscr{C}^0(I, \mathbb{R})$ croissante, $\beta \in \mathscr{C}^0(I, \mathbb{R}_+)$ et $u \in \mathscr{C}^0(I)$ ($0 \in I$) vérifiant*

$$\forall t \geq 0,\ u(t) \leq \alpha(t) + \int_0^t \beta(s)u(s)\,ds.$$

Alors pour tout $t \geq 0$,

$$u(t) \leq \alpha(t) \exp\left(\int_0^t \beta(s)\,ds\right)$$

Démonstration. Admis. L'astuce est de multiplier par le facteur intégrant $e^{-\beta t}$ … □

Stabilité du système linéarisé Posons $A = Df(0)$, alors $f(x) = Ax + g(x)$ avec $g(x) = o(|x|)$.

Si y est une solution du système $y'(t) = Ay(t)$, alors $y(t) = \exp(tA)y(0)$ pour tout t. On voudrait montrer que $\exp(tA) \to 0$ quand $t \to +\infty$.

En fixant $\mu < 0$ tel que $\mu > \Re(\lambda)$ pour toute valeur propre λ de A, on montre que :

$$\exists M > 0 \mid \forall t \geq 0,\ \|\exp(tA)\| \leq Me^{\mu t}$$

pour une norme d'opérateur induite par une norme quelconque sur $\mathbb{R}^n$.

Extension au système original Soit x une solution définie sur un intervalle ouvert I, contenant l'origine. On a $(\exp(-tA)x(t))' = \exp(-tA)g(x(t))$ d'où en intégrant

$$\exp(-tA)x(t) = x(0) + \int_0^t \exp(-sA)g(x(s))\,ds$$

$$x(t) = \exp(tA)x(0) + \int_0^t \exp((t-s)A)g(x(s))\,ds$$

En prenant la norme et en appliquant la majoration de l'exponentielle,

$$x(t) \leq Me^{\mu t}|x(0)| + \int_0^t Me^{\mu(t-s)}|g(x(s))|\,ds$$

Comme $g(x) = o(|x|)$ au voisinage de 0, on peut écrire $|g(x)| = |x|h(x)/M$ avec $h(x) \geq 0$ et $h(x) = o(1)$, ce qui donne :

$$\forall t \in I,\ e^{-\mu t}|x(t)| \leq M|x(0)| + \int_0^t e^{-\mu s}|x(s)| \cdot h(x(s))\, ds$$

Le lemme de Gronwall donne alors

$$|x(t)| \leq M|x(0)| \exp\left(\int_0^t (h(x(s)) + \mu)\, ds\right)$$

Tant que la trajectoire de x reste suffisamment proche de l'origine, $h(x(s)) + \mu < 0$ et ainsi x reste bornée… on voit d'où vient la stabilité.

Pour formaliser ça, considérons $U = B(0, r)$ un voisinage de 0 tel que $h(U) \subseteq]\mu/2, -\mu/2[$, et $V = B(0, r/M)$. On va établir que les trajectoires partant de $x(0) \in V$ sont asymptotiquement stables. Posons

$$T = \inf\{T > 0 \mid \forall t \in [0, T[,\ x(t) \text{ définie},\ x(t) \in U\}$$

Si $x(0) \in V$, alors $T > 0$. Supposons maintenant $T < +\infty$. Pour $t \in [0, T[$, on a alors $|x(t)| < M|x(0)|$ soit $x(t) \in U$. Par théorème de sortie de tout compact, x est définie en T, et même sur un voisinage à droite de T. Il n'en faut pas beaucoup plus pour montrer que x reste dans U à droite de T, d'où contradiction : par l'absurde, $T = +\infty$.

Ainsi, x est définie sur $\mathbb{R}_+$, et décroit exponentiellement.

3.12 Méthode de Newton pour les polynômes

Incontournable… Références : mix entre Rouvière (qu'on consultera pour une très bonne explication des points fixes attractifs / superattractifs / répulsifs) et Chambert-Loir–Fermigier (pour les polynômes).

Soit P un polynôme unitaire scindé sur $\mathbb{R}$ (par commodité, on va supposer $\deg P \geq 2$) :

$$P(x) = (x-\xi_1)^{m_1} \dots (x-\xi_r)^{m_r} \qquad \xi_1 < \dots < \xi_r$$

On cherche une racine de P par la *méthode de Newton* : on part d'un point x_0 et on calcule par récurrence

$$x_{n+1} = f(x_n) \qquad f(x) = x - \frac{P(x)}{P'(x)}$$

Le cas particulier des polynômes présente deux intérêts :

— Si $x_0 > \xi_r$, on tombe toujours sur la racine ξ_r. Ainsi, la convergence n'est pas seulement locale. C'est vrai généralement pour des fonctions convexes.

— Les hypothèses usuelles de la méthode de Newton comportent que $P'(\xi_r) \neq 0$, donc que ξ_r est une racine simple. Pour une racine multiple, on va voir qu'on a quand même convergence, mais avec une vitesse plus lente.

La récurrence est bien définie Par le théorème de Gauss–Lucas, P' et P'' ont leurs racines dans $[\xi_1, \xi_r]$. Donc, sur $]\xi_r, +\infty[$, $P' > 0$ et $P'' > 0$, P est strictement croissante et strictement convexe, et f est bien définie.

Par stricte convexité, pour $x_n > \xi_r$, $x_{n+1} = f(x_n) > \xi_r$. Pour le voir, il suffit de faire un dessin : la courbe de P est au-dessus de la tangente qui relie $(x_{n+1}, 0)$ et $(x_n, P(x_n))$. Formellement : $P(x_n) = (x_n - x_{n+1})P'(x_n)$ d'une part; d'autre part $P(x_n) = P'(y)(x_n - \xi_r)$ avec $y \in]\xi_r, x_n[$ par accroissements finis, or $P'(y) < P'(x_n)$ par convexité donc $x_n - x_{n+1} < x_n - \xi_r$.

Ainsi, $f :]\xi_r, +\infty[\to]\xi_r, +\infty[$ est bien définie, il en va de même de la suite (x_n). Celle-ci est donc (strictement) minorée par ξ_r, et de plus décroissante : elle converge.

Convergence vers un point fixe de f Montrons que f peut être prolongée en ξ_r. $m = m_r \geq 1$ étant la multiplicité de la racine ξ_r, on a $P(\xi_r + h) = a_m h^m + O(h^{m+1})$ et $P'(\xi_r + h) = m a_m h^m + O(h^m)$ donc

$$\frac{P(\xi_r + h)}{P'(\xi_r + h)} \sim \frac{h}{m} \qquad \text{d'où} \qquad f(\xi_r + h) = \xi_r + \left(1 - \frac{1}{m}\right) h + o(h)$$

f se prolonge donc par continuité sur $[\xi_r, +\infty[$ par $f(\xi_r) = \xi_r$; comme c'est une fraction rationnelle, $f \in \mathscr{C}^\infty([\xi_r, +\infty[)$. De plus, $f'(\xi_r) = 1 - 1/m$. ξ_r étant l'unique point fixe sur cet intervalle, $x_n \to \xi_r$ quand $n \to +\infty$.

Cas d'une racine simple C'est le cas usuel : comme $f'(\xi_r) = 0$, le point fixe est superattractif.

Par la formule de Taylor–Lagrange à l'ordre 2 :

$$\forall n \in \mathbb{N},\ \exists z_n \in]\xi_r, x_n[\,/\, x_{n+1} - \xi_r = f(x_n) - f(\xi_r) = \frac{f''(z_n)}{2}(x_n - \xi_r)^2$$

Donc la convergence est au moins *quadratique* :

$$\frac{x_{n+1} - \xi_r}{(x_n - \xi_r)^2} \xrightarrow[n \to +\infty]{} \frac{f''(\xi_r)}{2} \qquad \text{soit} \qquad x_{n+1} - \xi_r = O\left((x_n - \xi_r)^2\right)$$

i.e. le nombre de chiffres significatifs de l'approximation double à peu près à chaque itération.

Cas d'une racine multiple Maintenant, $f'(\xi_r) > 0$, le point fixe est attractif et la convergence sera donc *linéaire*. En effet, on s'y prend de la même façon qu'avant, mais à l'ordre 1 :

$$\forall n \in \mathbb{N},\ \exists z_n \in]\xi_r, x_n[\ /\ x_{n+1} - \xi_r = f(x_n) - f(\xi_r) = f'(z_n)(x_n - \xi_r)$$

$$\frac{x_{n+1} - \xi_r}{x_n - \xi_r} \xrightarrow[n\to+\infty]{} f'(\xi_r) = 1 - \frac{1}{m} < 1$$

En étudiant à l'ordre 2, on peut avoir plus de précisions :

Proposition. *Il existe $\lambda > 0$ tel que $x_n - \xi_r \sim \lambda(1 - 1/m)^n$.*

Démonstration. On écrit Taylor–Lagrange :

$$\forall n \in \mathbb{N},\ \exists z_n \in]\xi_r, x_n[\ /\ x_{n+1} - \xi_r = f'(\xi_r)(x_n - \xi_r) + \frac{f''(z_n)}{2}(x_n - \xi_r)^2$$

$$\frac{x_{n+1} - \xi_r}{x_n - \xi_r} = f'(\xi_r)\,(1 + O(x_n - \xi_r))$$

On montre, en s'aidant de la convergence linéaire précédemment établie, que $x_n - \xi_r = O(c^n)$ pour $1-1/m < c < 1$, puis que $\prod_n (1 + O(x_n - \xi_r))$ converge. On conclut par produit téléscopique. □

4 Idées exclues

4.1 Unicité de la topologie de $\mathbb{R}$-EVT séparé en dimension finie

(EVT = *espace vectoriel topologique*, c'est-à-dire espace vectoriel muni d'une topologie rendant continues les lois de compositions interne et externe.)

Évidemment, $\mathbb{R}$ est considéré avec sa topologie usuelle, et ça marche aussi pour les $\mathbb{C}$-EVT.

Théorème. *Le $\mathbb{R}$-espace vectoriel $\mathbb{R}^n$ n'admet qu'une seule topologie de $\mathbb{R}$-EVT séparé, qui est la topologie produit.*

Remarque. *Les topologies non séparées sont obtenues comme topologie initiale d'une projection sur un quotient séparé et sont donc en bijection avec les sous-espaces vectoriels (prendre l'adhérence de $\{0\}$).*

Un résultat qui généralise l'équivalence des normes et clôt la question. Fait dans les premières pages de Bourbaki, *Espaces vectoriels topologiques*, dans le cadre général des corps valués non discrets.

4.2 Lemme de Hensel, ou méthode de Newton p-adique

Violemment hors-programme, dommage, c'est plus original que la méthode de Newton usuelle et c'est de la jolie algèbre en plus… Un PDF de Keith Conrad raconte ça super bien.

Définition. *On appelle* entier p-adique *une suite $(a_n)_{n\in\mathbb{N}^*}$ avec $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ et $\pi_n(a_{n+1}) = a_n$ pour $n \in \mathbb{N}^*$, où $\pi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ est la projection canonique.*

Proposition. *Les entiers p-adiques forment un sous-anneau de $\prod_{n\in\mathbb{N}^*} \mathbb{Z}/p^n\mathbb{Z}$, de caractéristique nulle. Cet anneau est noté $\mathbb{Z}_p$.*

Définition. *Le* corps des nombres p-adiques $\mathbb{Q}_p$ *est le complété de $\mathbb{Q}$ pour la distance $d_p(x,y) = p^{-v_p(x-y)}$.*

Proposition. *La boule fermée de centre 0 et de rayon 1 dans $\mathbb{Q}_p$ est un sous-anneau isomorphe à $\mathbb{Z}_p$.*

Lemme (Hensel)**.** *Soient $f \in \mathbb{Z}_p[X]$ et $a \in \mathbb{Z}/p\mathbb{Z}$ tels que dans $\mathbb{Z}/p\mathbb{Z}$, on ait $f(a) = 0$ et $f'(a) \neq 0$. Alors il existe un unique $\alpha \in \mathbb{Z}_p$ tel que $f(\alpha) = 0$ et dont la classe dans $\mathbb{Z}/p\mathbb{Z}$ soit a.*

Corollaire. *Soient $f \in \mathbb{Z}[X]$ et $a \in \mathbb{Z}$ tels que $f(a) \equiv 0 \mod p$ et $f'(a) \not\equiv 0 \mod p$. Alors pour tout $n \in \mathbb{N}^*$, il existe $\alpha \in \mathbb{Z}$ tel que $f(\alpha) \equiv 0 \mod p^n$ et $\alpha \equiv a \mod p$.*

On a deux procédés d'itération légèrement différents pour relever des solutions dans un $\mathbb{Z}/p^n\mathbb{Z}$ plus grand : l'un est la méthode de Newton, l'autre ressemble à la preuve du théorème d'inversion locale.

4.3 Fonctions invariantes d'une équation différentielle linéaire

Un développement inspiré par une remarque dans *Ten lessons I wish I had learned before I started teaching differential equations* (item 3) de Gian-Carlo Rota. Voir la fin pour plus de remarques culturelles.

En vrai, c'est assez décevant comme truc.

On considère ici l'équation différentielle linéaire homogène

$$y''(t) + p(t)y'(t) + q(t) = 0 \qquad (p, q : \mathbb{R} \to \mathbb{R})$$

dont on notera $S \subset \mathscr{C}^2(\mathbb{R}, \mathbb{R})$ l'espace des solutions.

Si $f : \mathbb{R}^{2k} \to \mathbb{R}$ ($k \in \mathbb{N}^*$ quelconque), on abrégera

$$f[y, z](t) = f\left(y(t), \dots, y^{(k)}(t), z(t), \dots, z^{(k)}(t)\right)$$

et on appellera f une *fonction invariante* si, pour toute base de S (i.e. système fondamental de solutions) (y, z),

$$\forall L \in \mathrm{GL}(S),\ \exists \lambda(L) \in \mathbb{R} / \forall t \in \mathbb{R},\ f[Ly, Lz](t) = \lambda(L) \cdot f[Ly, Lz](t)$$

Autrement dit, une fonction invariante est indépendante du système fondamental de solution choisi, à un facteur constant (par rapport au temps) près.

On peut remarquer que les coefficients de l'équation sont en fait des fonctions invariantes (avec $\lambda(L) = 1$) puisque

Un autre exemple de fonction invariante est le *wronskien*

$$W[y, z](t) =$$

L'invariance du wronskien découle immédiatement du lemme suivant :

Lemme. *Soit (y, z) une base de S, $L \in \mathrm{GL}(V)$. Alors, pour tout $t \in \mathbb{R}$,*

$$W[Ly, Lz](t) = (\det L) \cdot W[y, z](t)$$

Ici, donc $\lambda(L) = \det(L)$.

Démonstration. Comme (y, z) est une base, on peut y décomposer Ly et Lz :

$$Ly = ay + bz \quad Lz = cy + dz$$

Dans la base (y, z), la matrice de L est donc

$$M = abcd$$

donc $\det L = \det M$.

Maintenant, soit $t \in \mathbb{R}$. Évaluons ces relations, ainsi que celles obtenues en dérivant, au point t. On obtient

$$plif = plaf \times plouf$$

d'où, en prenant le déterminant,

$$tadaaa$$

□

Nous en venons maintenant au théorème principal : en un certain sens, ces fonctions invariantes suffisent à engendrer toutes les autres.

Théorème. *Soit f une fonction invariante, alors il existe $g : \mathbb{R} \to \mathbb{R}$ et $h : \mathbb{R}^{2l} \to R$ tels que pour toute base (y, z),*

$$\forall t \in \mathbb{R},\ f[y,z](t) = g(W[y,z](t))h[p,q](t)$$

Commençons par un résultat d'algèbre linéaire.

Proposition. *Soit $\phi : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ un morphisme de groupes. Alors il existe $\psi : \mathbb{R}^* \to \mathbb{R}^*$ tel que $\phi = \psi \circ \det$.*

Démonstration. Soit T une transvection, alors T^2 est aussi une transvection, donc T est semblable à T^2. Comme ϕ est à valeurs dans un groupe abélien, on a donc $\phi(T)^2 = \phi(T)$, soit $\phi(T) = 1$ dans $\mathbb{R}^*$.

Comme les transvections engendrent $\mathrm{SL}_n(\mathbb{R})$, on a $\phi(\mathrm{SL}_n(\mathbb{R})) = \{1\}$. ϕ passe donc au quotient comme morphisme $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \to \mathbb{R}^*$. Or le déterminant réalise un isomorphisme entre $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R})$ et $\mathbb{R}^*$… □

Maintenant, fixons f une fonction invariante et (y, z) une base. On peut voir que si $f[y,z](t) \neq 0$ pour un certain t, alors les $\lambda(L)$ sont uniques, non nuls, et réalisent un morphisme de groupes vers $\mathbb{R}^*$. On a alors, par le lemme précédent, $\lambda(L) = g(\det L)$ pour tout $L \in GL(S)$.

Soit $t \in \mathbb{R}$. Il existe un système fondamental $(u_t, v_t) \in S^2$ tel que $u(0) = v'(0) = 1$, $u'(0) = v(0) = 0$, de sorte que $W[u,v](t) = 1$. Soit $L_t \in \mathrm{GL}(S)$ telle que $L_t u_t = y$ et $L_t v_t = z$. Alors

$$f[y,z](t) = \lambda(L) \cdot f[u_t, v_t](t) \quad \text{avec} \quad \lambda(L) = g(\det L_t) = g\left(\frac{W[y,z](t)}{W[u_t,v_t](t)}\right) = g(W[y,z](t))$$

en utilisant le lemme sur le wronskien démontré plus haut.

On a donc notre facteur $g(W)$, reste à trouver h telle que

$$\forall t \in \mathbb{R},\ h[p,q](t) = W[u_t, v_t](t)$$

Pour cela, remarquons qu'on a $y'' = -py' - qy$, suite à quoi $y''' = -py'' - p'y' - qy' - q'y = p(py' + qy) - p'y' - qy' - q'y$, etc. Par récurrence, il existe une suite de polynômes P_n tels que…

ENFIN BREF VOILÀ

Remarque. *Ce théorème est l'analogue du théorème fondamental sur les polynômes symétriques, qui dit qu'un polynôme symétrique en les solutions d'une équation polynomiale s'exprime comme polynôme en les coefficients de l'équation.*

Culture, biblio, etc. Publié dans les annales scientifiques de l'ENS par un matheux oublié par l'Histoire.