Kit à l'usage de la préparation de l'agrégation

Etienne Machiels

2022-2024

Sommaire

1 Introduction **3**

2 Comment préparer le concours de l'agrégation ? **4**
2.1 Conseils généraux . . . 4
2.2 Méthode "de brute" . . . 5
2.3 La méthode "à la cool" . . . 5
2.4 La méthode "pile ou face" . . . 5

3 Algèbre et Géométrie **6**
3.1 Loi de réciprocité quadratique par les sommes de Gauss . . . 6
3.2 Théorème de Cauchy et condition pour qu'un sous groupe soit distingué . . . 9
3.3 Irréductibilité des polynômes cyclotomiques . . . 10
3.4 Théorème de Gauss-Lucas et une application . . . 11
3.5 L'exponentielle réalise un homéomorphisme entre $S_n(\mathbb{R})$ et $S_n^{++}(\mathbb{R})$ . . . 12
3.6 Classification des groupes simples d'ordre 60 . . . 13
3.7 Un critère de diagonalisation de matrices: le critère de Klarès . . . 14
3.8 Théorème fondamental de l'algèbre (d'Alembert-Gauss) . . . 16
3.9 Théorème de Frobenius-Zolotarev . . . 18
3.10 Théorème de Chevalley-Warning et une application . . . 20
3.11 Un problème de dénombrement sur les corps finis : Le problème de Kakeya . . . 22
3.12 Théorème de Wedderburn : Les corps finis sont tous commutatifs . . . 24
3.13 Théorème de Sylow version opération de groupes . . . 26

4 Analyse et Probabilités **28**
4.1 Densité des polynômes orthogonaux dans $L^2(\mathbb{R}, \rho)$ . . . 28
4.2 Théorème d'inversion locale . . . 30
4.3 Calcul de l'intégrale de Gauss par une équation différentielle . . . 32
4.4 Calcul d'une intégrale par le théorème des résidus . . . 34
4.5 Théorème de Fischer-Riesz . . . 37
4.6 Théorème de projection sur un convexe fermé et une application dans $L^2(\mathbb{R})$ . . . 39
4.7 Méthode de gradient à pas optimal . . . 41
4.8 Exemple d'un connexe, non connexe par arcs . . . 44
4.9 Théorème de Weierstrass par les polynômes de Bernstein . . . 46
4.10 Formule sommatoire de Poisson et formule d'inversion de Fourier dans l'espace de Schwarz . . . 48
4.11 Calcul des $\zeta(2k)$ et développement asymptotique des nombres de Bernoulli . . . 51
4.12 Formule d'Euler-MacLaurin . . . 53
4.13 Théorème des fonctions implicites . . . 56
4.14 Inégalité de Hoeffding . . . 57
4.15 Théorème central limite + applications . . . 59
4.16 Indécomposabilité de la loi de Poisson . . . 62

5 Résultats bonus **63**
5.1 Un groupe contenant 80% d'éléments d'ordre 2 est abélien . . . 63
5.2 Groupe dont Aut(G) est réduit au neutre . . . 64
5.3 Le groupe multiplicatif d'un corps fini est cyclique . . . 65
5.4 Théorème de d'Alembert-Gauss (version Analyse) . . . 66
5.5 Calcul de la dimension d'un espace vectoriel et problème de dénombrement . . . 67
5.6 Equivalence des normes en dimension finie . . . 68
5.7 Automorphisme de corps de $\mathbb{R}$ . . . 69
5.8 Lien entre loi exponentielle et géométrique . . . 70
5.9 Une fonction réelle continue 1-périodique et $\sqrt{2}$ périodique est constante . . . 71
5.10 Lemme de Wirtinger . . . 72
5.11 Nombres de Pisot . . . 73
5.12 Un test pour comparer deux nombres rationnels qui marche presque tout le temps . . . 74
5.13 Calcul géométrique du produit ab . . . 76
5.14 Une fonction convexe inattendue . . . 77

6 Tableau recasage **78**
6.1 Recasage Algèbre . . . 78
6.2 Recasage Analyse . . . 79

1 Introduction

J'ai initialement crée ce document afin de regouper et de constater l'évolution de mes développements au fur et à mesure de l'année. Je le partage désormais si cela peut servir à d'autres, tant mieux! Dans la mesure du possible, j'ai essayé de détailler au maximum les démonstrations afin de ne pas perdre de temps à comprendre le raccourci qu'à pu prendre l'auteur dans les bouquins. Beaucoup de ces développements sont classiques et très abordable, ceux-ci permettent une certaine sécurité à l'oral de l'agrégation. J'ai référencé dans quelles leçons les développements peuvent rentrer, mais ce classement est largement subjectif, de plus la numérotation des leçons varient en fonction des années, donc faites vous votre propre idée. Du moment que vous arrivez à justifer concrètement l'interêt d'un développement dans une leçon, celui-ci à toujours sa place. Aussi, cette liste ne correspond pas à l'entiereté de mes developpements, j'avoue ne pas avoir eu le courage de tous les recopier...

J'ai également essayé d'inclure les thèmes des énoncés et démonstrations qui, dans la mesure où le résultat ne servirait pas de développement, pourrait servir à apparaître dans les leçons appropriées (attention cela dit, tout résultat énoncé en leçon doit savoir être démontré, au moins partiellement).

La première partie est faite de conseils pour l'agrégation, je ne prétends pas avoir la science infuse, ni tout savoir de ce concours, je témoigne de mon expérience mais la finalité est avant tout de travailler par soi-même.

Enfin, une dernière partie est consacrée à des résultats complémentaires, que j'aime bien ou que je trouve important, mais qui sont trop courts pour faire des développements. Je vous laisse découvrir ça.

Remerciements chaleureux à tout le laboratoire Jean Leray de Nantes, particulièrement à Sylvain Gervais et François Nicoleau, dont leur investissement dans la préparation à l'agrégation n'a d'égal que leur gentillesse.

Bonne lecture et bonne préparation ! (Attention aux coquilles)

2 Comment préparer le concours de l'agrégation ?

Le concours de l'agrégation se décompose majoritairement en deux grandes épreuves, l'écrit et l'oral.

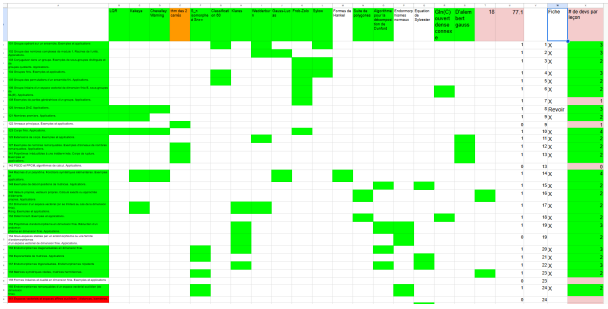
Pour ce qui est de l'écrit, je n'ai que très peu de conseils à donner, si ce n'est connaître par coeur les énoncés des théorèmes usuels tels qu'en analyse par exemple, convergence dominée, dérivation sous le signe intégral, théorème des résidus... Je pense que l'essentiel des révisions se fait en regardant les sujets des autres années et en essayant de rédiger au moins les parties 1 et 2.

Pour ce qui est de l'oral, c'est une autre paire de manche.

2.1 Conseils généraux

Pour avoir passer deux fois les oraux, les principaux conseils que je peux donner aux agrégatifs sont les suivants:

- S'organiser. La préparation peut être un travail de longue haleine, avec beaucoup de charge mentale. Au début de l'année, créez-vous un tableau (excel ou papier), notez les développements que vous souhaitez mettre dans chaque leçon. Cela permet de se rendre compte de son avancée. Vous pouvez même mettre en place un planning, par exemple, deux leçons et un développement par semaine etc... Par exemple, voici



à quoi ressemblait mon tableur à la fin de l'année, les leçons en vertes représentent les leçons préparées, la couleur des développements indiquent à quel point je les connais, les cases vertes indiquent le recasages des développements dans chaque leçon etc. (Comme on peut le voir, malgré deux années de préparation, j'avais encore quelques impasses...)

- Les développements. A l'oral, le développement représente les 3/4 du temps d'autonomie au tableau, en ce sens, il ne faut rien laisser au hasard. S'il y a bien quelque chose à préparer pendant l'année, ce sont les developpements. Rien ne sert de prendre des choses bien compliquées, prenez ce qui vous plaisir, apprenez le bien, et prenez du recul.

- Allez en cours. Conseil bête, mais allez en cours! Faites les exos, écoutez les corrections. Cette année, je me baladais toujours avec un petit carnet, tous les exercices qui sortaient de l'ordinaire étaient notés dedans, ceux-ci pouvant servir à illustrer de façon originale les leçons.

- Investissez-vous! L'année est difficile, autant la rendre le plus agréable possible! Discutez et travaillez avec vos camarades, évitez de travailler tout seul. Echangez avec vos professeur·e·s, prenez les leçons qu'ils vous proposent! Pendant l'année, des leçons sont distribuées, partagez avec les autres mais prenez-en! Et surtout celles qui vous font peur. Par exemple, cette année j'ai présenté la leçon 191 (de la géométrie beurk) et c'était super! C'est la meilleure façon de progresser. Aussi, allez écouter vos camarades présenter leur leçon.

A mon sens, il y a différentes façons de prépaper l'agrégation.

2.2 Méthode "de brute"

La méthode la plus simple pour bien travailler l'oral et obtenir l'agrégation: préparer chaque leçon. S'adonner à la tâche de toutes les rédiger une à une, retenir les références utilisées, les développements. Avec cette méthode, c'est sûr vous aurez des leçons de prédilection, mais peu importe le tirage, vous serez toujours armé pour présenter quelque chose de solide. Cette méthode est en revanche très chronophage, elle vous demande de vous intéressez à des sujets que vous aviez mis de côté toute votre scolarité, d'être à l'aise partout. C'est beaucoup de travail mais un investissement presque sûr.

2.3 La méthode "à la cool"

Cette méthode est celle que j'ai utlisée. Je ne rédigeais pas chaque leçon, mais je m'attardais sur la leçon en notant ce que je voulais mettre dedans, je m'aidais des plans présents sur internet pour rédiger mon propre plan, je feuilletais les livres à la recherche d'éléments que je mettrai dans le plan. A la fin, j'écris sur une fiche le plan, avec pour chaque partie quelles références j'utilisais. C'est un travail moins minutieux que la méthode précédente, mais si on tombe sur une leçon que l'on a préparé, on connaît la structure du plan et les références, ce qui est suffisant pour faire son plan en 3h.

2.4 La méthode "pile ou face"

Celle-là est fortement déconseillé. Elle consiste à croire qu'avec deux devs dans chaque leçon, cela suffit et que l'on peut improviser un plan en 3h le jour J. Alors oui c'est possible si l'on tombe sur une leçon que l'on aime bien. J'ai passé deux fois l'agrégation, la première fois, je connaissais quelques plans, mais j'utilisais surtout cette méthode, et bien j'ai du la repasser. En plus, cela entrâine un stress considérable car au final, on n'est prêt sur rien.

3 Algèbre et Géométrie

3.1 Loi de réciprocité quadratique par les sommes de Gauss

Difficulté : Moyenne
Thèmes : Extension de corps, nombres premiers, racines de polynômes, racines de l'unité.
Leçons concernées: **120**, **104**, **121**, **123**
Références : Serre, Cours d'arithmétique

Enoncé 1. *Soient p et q deux nombres premiers impairs. Alors*

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

Considérons $\mathbb{L}$ le corps de décomposition de $X^q - 1$ sur $\mathbb{F}_p$ et soit ω une racine primitive q-ème de l'unité dans $\mathbb{L}$. Posons alors

$$y = \sum_{x\in\mathbb{F}_q} \left(\frac{x}{q}\right)\omega^x.$$

L'élément y a bien un sens, au sens où sa définition ne dépend pas du réprésentant des x choisis.

Lemme 1.

$$y^2 = (-1)^{\frac{q-1}{2}} q.$$

Démonstration. On a

$$y^2 = \sum_{t\in\mathbb{F}_q} \left(\frac{t}{q}\right) w^t \sum_{z\in\mathbb{F}_q} \left(\frac{z}{q}\right) w^z.$$

Comme le symbole de Legendre est multiplicatif,

$$y^2 = \sum_{t,z\in\mathbb{F}_q} \left(\frac{tz}{l}\right) w^{t+z}.$$

En effectuant le changement de variable $u = t + z$ (notons que u parcourt tous les éléments de $\mathbb{F}_q$), on obtient alors

$$y^2 = \sum_{u\in\mathbb{F}_q} \omega^u \left(\sum_{t\in\mathbb{F}_q^*} \left(\frac{t(u-t)}{q}\right)\right) \qquad \text{(Notons que si } t = 0\text{, tous les termes valent 0.)}$$

Donc, si $t \neq 0$,

$$\left(\frac{t(u-t)}{q}\right) = \left(\frac{-t^2}{q}\right)\left(\frac{1-ut^{-1}}{q}\right) = \left(\frac{t^2}{q}\right)\left(\frac{-1}{q}\right)\left(\frac{1-ut^{-1}}{q}\right) = 1\cdot(-1)^{\frac{q-1}{2}}\left(\frac{1-ut^{-1}}{q}\right).$$

On a alors

$$(-1)^{\frac{q-1}{2}} y^2 = \sum_{u\in\mathbb{F}_q} \mathrm{C}_u \omega^u$$

avec

$$\mathrm{C}_u = \sum_{t\in\mathbb{F}_q^*} \left(\frac{1-ut^{-1}}{q}\right).$$

Si $u = 0$, $\mathrm{C}_0 = \sum_{t\in\mathbb{F}_q^*} \left(\frac{1}{q}\right) = \sum_{t\in\mathbb{F}_q^*} 1 = l - 1$. Sinon, posons $s = 1 - ut^{-1}$.

Comme t parcourt $\mathbb{F}_q^*$, s atteint $\mathbb{F}_q \setminus \{1\}$. Or, comme dans $\mathbb{F}_q^*$, il y a autant d'éléments qui sont des carrés que d'éléments qui n'en sont pas, on a $\sum_{s\in\mathbb{F}_q} \left(\frac{s}{q}\right) = 0$. Ainsi

$$\mathrm{C}_u = \sum_{s\in\mathbb{F}_q} \left(\frac{s}{q}\right) - \left(\frac{1}{q}\right) = -\left(\frac{1}{q}\right) = -1.$$

Finalement, on obtient

$$(-1)^{\frac{q-1}{2}} y^2 = \sum_{u\in\mathbb{F}_q} \mathrm{C}_u \omega^u = q - 1 - \sum_{u\in\mathbb{F}_q^*} \omega^u = q.$$

En effet, soit $\mathrm{S} = \sum_{u\in\mathbb{F}_q} \omega^u$ et soit $y \in \mathbb{F}_q^*$. Comme $\mathbb{F}_q$ est un corps, la somme S est invariante par translation, *i.e.*, $\mathrm{S} = \sum_{x\in\mathbb{F}_q} \omega^{x+y} = \omega^y \sum_{x\in\mathbb{F}_q} \omega^x = \omega^y \,\mathrm{S}$. Comme ω et y sont non nuls, ω^y est non nul donc $\mathrm{S} = 0$. Dans notre cas, la somme est restreinte à $\mathbb{F}_q^*$. Il manque donc le terme en $w^0 = 1$. D'où $\sum_{u\in\mathbb{F}_q^*} \omega^u = -1$ □

Lemme 2.

$$y^{p-1} = \left(\frac{p}{q}\right).$$

Démonstration.

$$y^p = \left(\sum_{x\in\mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x\right)^p.$$

Comme l'équation a lieu dans $\mathbb{L}$ qui est un corps de caractéristique de p (comme extension de $\mathbb{F}_p$), il vient, en utilisant l'identité du première année $(x+y)^p = x^p + y^p$,

$$y^p = \sum_{x\in\mathbb{F}_q} \left(\frac{x}{q}\right)^p \omega^{xp}.$$

De plus, comme p est impair (le symbole de Legendre est à valeur dans + ou -1)

$$\left(\frac{x}{q}\right)^p = \left(\frac{x}{q}\right).$$

En effectuant alors le changement de variable $z = xp$, il vient

$$\begin{aligned} y^p = \sum_{x\in\mathbb{F}_q} \left(\frac{x}{q}\right)^p \omega^{xp} &= \sum_{z\in\mathbb{F}_q} \left(\frac{zp^{-1}}{q}\right) \omega^z \\ &= \sum_{z\in\mathbb{F}_q^*} \left(\frac{z}{q}\right)\left(\frac{p^{-1}}{q}\right) \omega^z \\ &= \left(\frac{p^{-1}}{q}\right) \sum_{z\in\mathbb{F}_q^*} \left(\frac{z}{q}\right) \omega^z \\ &= \left(\frac{p^{-1}}{q}\right) y \\ &= \left(\frac{p}{q}\right) y. \end{aligned}$$

Comme y est non nul (invoquer le 1er lemme par exemple), en multipliant par y^{-1} de chaque côte, cela conclut. □

Enfin, pour conclure sur la loi de réciprocité quadratique

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

Remarque 3.1. Bon, soyons honnête, parmi la myriade de preuves sur le marché pour cette énoncé, celle-là est loin d'être très élégante. En revanche, ce qu'elle illustre, c'est le passage dans un corps plus gros, dans lequel on fait les calculs qui nous intéressent, avant de revenir vers ce qui nous intéresse. Il faudra être d'une grand rigueur lors de l'écriture d'égalité et garder en tête la caractéristique dans laquelle on travaille. Enfin, dernière remarque terminologique, pour cette démonstration, Serre utilise dans son livre les lettres p et l mais elles se ressemblent trop au tableau donc j'ai opté pour p et q. Pour bien comprendre à quoi ce théorème sert, je conseille la page wikipédia de la loi de réciprocité quadratique, où c'est très bien expliqué.

3.2 Théorème de Cauchy et condition pour qu'un sous groupe soit distingué

Difficulté : Facile
Thèmes : Actions de groupes, sous-groupe distingué, groupes finis, groupe symétrique
Leçons concernées : **101**, **104**, **105**
Références : Ulmer, Théorie des groupes, Alessandri, Thèmes de géométrie.

Enoncé 2. *Soit G un groupe fini et p un diviseur premier de $|G|$, alors le nombre de solutions de l'équation $x^p = 1_G$ est divisible par p. En particulier, il existe un élément d'ordre p.*

Démonstration. Notons $n = |G|$ et soit p un diviseur premier de $|G|$. Considérons l'ensemble $X = \{(x_1, \dots, x_p) \in G^p, \quad x_1 \cdots x_p = 1_G\}$. Cet ensemble a cardinal n^{p-1}. Considérons désormais l'action à gauche du groupe cyclique $H = \langle (1\,2\,3 \cdots p) \rangle$ sur X :

$$\begin{aligned} H \times X &\longrightarrow X \\ (\sigma, (x_1, \dots, x_p)) &\mapsto (x_{\sigma(1)}, \dots, x_{\sigma(p)}). \end{aligned}$$

Les orbites pour cet action divise le cardinal de H donc ont cardinal 1 ou p. Or, les orbites de taille 1 sont exactement les solutions de l'équation $x^p = 1_G$. Ecrivant l'équation aux classes en notant s le nombre d'orbites de taille p et r le nombre d'orbites de taille 1, il vient

$$n^{p-1} = r + sp.$$

En résuisant modulo p on a $r = 0 \mod p$. Or le p-uplet $(1_G, \dots, 1_G)$ est une orbite de taille 1. Donc $r = kp$ □

Enoncé 3. *Soit G un groupe fini et soit p le plus petit diviseur premier de $|G|$. On suppose qu'il existe un sous groupe $H < G$ d'indice p dans G. Alors H est distingué dans G. En particulier, tout sous-groupe d'indice 2 est distingué.*

Démonstration. Considérons l'action naturelle de G à gauche sur G/H:

$$\begin{aligned} G \times G/H &\longrightarrow G/H \\ (g, P) &\longmapsto gP. \end{aligned}$$

Etudions le noyau du morphisme ρ associé à l'action:

$$K := \ker\rho = \{g \in G, \forall P \in G/H, gP = P\}.$$

En particulier, en considérant $P = H$, on voit que le noyau doit au moins stabiliser H, d'où $K \subset H$. De plus, le premier théorème d'isomorphisme nous donne que $G/K \sim \mathrm{Im}(\rho) \subset S(G/H)$. En passant au cardinal

$$\frac{|G|}{|K|} = p!.$$

Comme p est le plus petit diviseur premier de $|G|$, par le lemme d'Euclide, on a $\frac{|G|}{p}$ divise $|K|$. Or, $\frac{|G|}{p} = |H|$ puisque H est d'indice p dans G. D'où $|H|$ divise $|K|$, ce qui conclut $H = K \triangleleft G$ □

Remarque 3.2. Lors de ma première année de préparation à l'agrégation, j'espérais présenter cela. Au final, avec du recul, je pense que c'est un peu trop bas niveau, mais en tout cas, ces deux théorèmes illustrent à merveille les actions de groupes donc je le laisse.

3.3 Irréductibilité des polynômes cyclotomiques

Difficulté : Facile-Moyen
Thèmes : Extensions de corps, racines de l'unité, polynômes à une indeterminée.
Leçons concernées : **141**, **102**, **125**
Références : Gozard, Théorie de Galois

Lemme 3. *Soient P, A, B trois éléments non nuls de $\mathbb{Q}[X]$. On suppose que $P \in \mathbb{Z}[X]$, que $P = AB$, et que P et A sont unitaires. Alors A et B appartiennent à $\mathbb{Z}[X]$.*

Preuve du lemme. Clairement, B est lui aussi unitaire. Notons

$$A(X) = X^n + \sum_{i=0}^{n-1} a_i X^i, \quad a_i \in \mathbb{Q}.$$

Et pour chaque i, notons $a_i = \frac{p_i}{q_i}$, avec $p_i \wedge q_i = 1$. Soit q le PPCM des q_i. Alors

$$A(x) = X^n + \frac{1}{q}\sum_{i=0}^{n-1} z_i X^i, \quad z_i \in \mathbb{Z}.$$

Sans perte de généralité on peut supposer que le PGCD des z_i et q est 1. Notant alors $A_1(X) = qA(X)$, on a alors $A_1 \in \mathbb{Z}[X]$ et le polynôme A_1 est primitif puisque

$$A_1(x) = qX^n + \sum_{i=0}^{n-1} z_i X^i.$$

Effectuant le même raisonnement sur B, il existe $r \in \mathbb{N}^*$ tel que $B(X) = \frac{1}{r}B_1(X)$ avec $B_1 \in \mathbb{Z}[X]$ primitif. Donc

$$qrP = A_1 B_1.$$

Comme d'après le lemme de Gauss, le produit de polynômes primitifs est primitif, A_1B_1 est primitif. Or, le contenu de qrP est qr car P est unitaire. Donc $qr = 1$, soit $q = r = 1$. Ainsi, $A = A_1 \in \mathbb{Z}[X]$, et $B = B_1 \in \mathbb{Z}[X]$. □

Enoncé 4. *Soit $\Phi_n = \prod_{\xi^n=1,\, \xi \text{ prim}} (X - \xi)$. Alors Φ est irréductible sur $\mathbb{Q}$*

Démonstration. Soit ω une racine primitive n-ème de l'unité dans $\mathbb{C}$ et soit f son polynôme minimal. Le polynôme $X^n - 1$ est annulateur de ω donc f divise $X^n - 1$ dans $\mathbb{Q}$, donc il existe $h \in \mathbb{Q}[X]$ tel que $f(X)h(X) = X^n - 1$. Or f unitaire et $X^n - 1 \in \mathbb{Z}[X]$ implique que $h \in \mathbb{Z}[X]$.
On va désormais montrer que si u est une racine de f et p un nombre premier avec n, alors u^p est racine de f également.
Soit u une racine de f. Comme f divise $X^n - 1$, $u^n - 1 = 0$ donc u est une racine n-ème de l'unité dans $\mathbb{C}$ donc u^p aussi, d'où $0 = f(u^p)h(u^p)$. Supposons que $f(u^p) \neq 0$. Alors par intégrité, $h(u^p) = 0$. On sait que f est unitaire irréductible sur $\mathbb{Q}$, donc le polynôme minimal de u est f. Ainsi, f divise $h(X^p)$ dans $\mathbb{Q}[X]$, *i.e.*, il existe $g \in \mathbb{Q}[X]$, $h(X^p) = f(X)g(X)$. Par le lemme, g est en fait dans $\mathbb{Z}[X]$. Projetant la dernière égalité modulo p, il vient

$$\overline{h(X^p)} = \overline{h}(X)^p = \overline{f}(X)\overline{g}(X).$$

Soit ϑ un facteur irréductible de $\overline{f}$ dans $\mathbb{F}_p[X]$. ϑ divise donc $\overline{h}^p$ donc divise $\overline{h}$ donc ϑ^2 divise $\overline{f}\,\overline{h} = X^n - \overline{1}$ dans $\mathbb{F}_p[X]$. Par conséquent, $X^n - 1$ possède une racine double dans son corps de décomposition, ce qui est absure car son polynôme dérivé est nX^{n-1} qui est premier avec $X^n - 1$. Donc $f(u^p) = 0$.
Enfin, comme ω est racine de f, et pour tout nombre premier p avec n, ω^p est racine de f, on a $\deg f \geq \varphi(n)$. Or, f divise Φ_n et $\deg \Phi_n = \varphi(n)$ donne $f = \Phi_n$ ce qui conclut. □

3.4 Théorème de Gauss-Lucas et une application

Difficulté : Facile
Thèmes : Polynôme, barycentres, racines d'un polynôme, nombres complexes de module 1.
Leçons concernées : **102**, **181**, **144**
Références : FGN, Oraux X-ENS Algèbre 1

Enoncé 5. *Soit $P \in \mathbb{C}[X]$ non constant. Alors l'ensemble des racines de P' est contenu dans l'ensemble convexe des racines de P.*

Démonstration. Soit $P = \lambda \prod_{k=1}^{r} (X - \lambda_k)^{n_k}$, $\lambda_i \in \mathbb{C}$.

On a alors $P' = \lambda \prod_{k=1}^{r} n_k (X - \lambda_k)^{n_k - 1} \prod_{k \neq l} (X - \lambda_k)^{n_l}$. Considérons la fraction rationnelle $\frac{P'}{P}$:

$$\frac{P'}{P} = \sum_{k=1}^{r} \frac{n_k}{X - \lambda_k}.$$

Soit z une racine de P'. Si z est aussi racine de P, il n'y a rien à dire. Sinon,

$$\begin{aligned} 0 = \frac{P'(z)}{P(z)} &= \sum_{k=1}^{r} \frac{n_k}{z - \lambda_k} \\ &= \sum_{k=1}^{r} n_k \frac{\overline{z - \lambda_k}}{|z - \lambda_k|^2} \\ &= \sum_{k=1}^{r} n_k \frac{z - \lambda_k}{|z - \lambda_k|^2}. \end{aligned}$$

Ainsi, en notant $m := \sum_{k=1}^{r} \frac{n_k}{|z - \lambda_k|}$, on a $z = \sum_{k=1}^{r} \alpha_i \lambda_i$, où $\alpha_i = \frac{1}{m} \frac{n_i}{|z - \lambda_i|^2}$, et $\sum \alpha_i = 1$. Donc z est un barycentre en les λ_i, les racines de P ce qui conclut. □

Application 1. *Le plus grand entier n tel que le polynôme $(X+1)^n - X^n - 1$ a l'ensemble de ses racines non nuls de module 1 est 7.*

Démonstration. Si $n = 2$, $P = 2X$ a une unique racine 0. Soit $n \geq 3$, $P' = n(X+1)^{n-1} - nX^{n-1}$. Soit z une racine de P', z est donc non nulle et on a alors $\left(\frac{z+1}{z}\right)^{n-1} = 1$. Ainsi, il existe $k \in [\![0, k-2]\!]$ tel que

$$\frac{z+1}{z} = e^{\frac{2ik\pi}{n-1}}.$$

De plus, $k \neq 0$ car $z + 1 \neq z$. On en déduit alors que les $n - 2$ racines de P' sont

$$z_k = \frac{e^{\frac{-ik\pi}{n-1}}}{2i \sin(\frac{k\pi}{n-1})}.$$

Maintenant, si toutes les racines non nuls de P sont de module 1, par le théorème de Gauss-Lucas, les racines de P', elles, sont dans le disque unité. On a $|z_1| = \frac{1}{2\sin(\frac{k\pi}{n-1})} > 0$. Et pour $n \geq 8$, on a aussi

$$2\sin(\frac{\pi}{n-1}) < 2\sin\frac{\pi}{6} = 1.$$

Donc $|z_1| > 1$ et $n \geq 8$ ne convient pas. Pour $n = 7$, $P = (X+1)^7 - X^7 - 1$ est degré 6. On peut vérifier facilement que $0, -1, j, j^2$ sont racines de P, et que j et j^2 sont racines de P' donc au moins racines double de P, on a donc trouvé les 6 racines de P, ce qui conclut. □

Remarque 3.3. Il y a une autre application au théorème de Gauss-Lucas que je trouve assez belle : Si P est un polynôme non constant tel que P'' divise P, alors les racines de P sont toutes alignées dans $\mathbb{C}$. Par contre, je n'ai plus la référence, demandez à vos profs !

3.5 L'exponentielle réalise un homéomorphisme entre $\mathrm{S}_n(\mathbb{R})$ et $\mathrm{S}_n^{++}(\mathbb{R})$

Difficulté : Facile
Thèmes : Théorème spectral, diagonalisation, exponentielle de matrices.
Leçons concernées : **152**, **155**, **157**, **158**
Références : Caldero, NH2G2

Enoncé 6. *L'application exp* : $\mathrm{S}_n(\mathbb{R}) \to \mathrm{S}_n^{++}(\mathbb{R})$ *est un homéomorphisme.*

Il y a 5 choses à montrer : définition de l'application, surjectivité, injectivité, continuité, continuité de l'inverse.

Démonstration. Montrons que l'application est bien définie. Soit $S \in \mathrm{S}_n$. Par le théorème spectral, il existe $P \in \mathrm{O}_n(\mathbb{R})$ tel que $S = P\mathrm{diag}(\lambda_i)P^{-1}$, où $\mathrm{diag}(\lambda_i)$ est une matrice diagonale dont les coefficients sont les valeurs propres de S (donc dans $\mathbb{R}$). On a alors

$$\exp(S) = P\mathrm{diag}(e^{\lambda_i})P^{-1} = P\mathrm{diag}(e^{\lambda_i})^t P \in \mathrm{S}_n^{++}(\mathbb{R}),$$

car $e^{\lambda_i} > 0$ pour tout i et P est orthogonale. Donc l'exponentielle envoie bien $\mathrm{S}_n(\mathbb{R})$ dans $\mathrm{S}_n^{++}(\mathbb{R})$ et par restriction de l'exponentielle de matrices usuelle, elle reste continue.
Montrons désormais la surjectivité. Considérons $B \in \mathrm{S}_n^{++}(\mathbb{R})$. On a donc $B = P\mathrm{diag}(\mu_i)P^{-1}$, avec $P \in \mathrm{O}_n(\mathbb{R})$ et $\mu_i > 0$ pour tout i. Donc la matrice A définie par $A = P\mathrm{diag}(\log(\mu_i))P^{-1}$ est symétrique et l'on a $\exp(A) = B$, d'où la surjectivité.
Pour l'injectivité, supposons que l'on ait $\exp(A) = \exp(A')$, avec $A, A' \in \mathrm{S}_n(\mathbb{R})$. Considérons Q un polynôme interpolateur de Lagrange tel que $Q(e^{\lambda_i}) = \lambda_i$, où les λ_i sont les valeurs propres de A. On a alors, puisque $\exp(A)$ est un polynôme en A, A' qui commute avec

$$Q(\exp(A')) = Q(\exp(A)) = PQ(\mathrm{diag}(\lambda_i))P^{-1} = A$$

Donc A' commute avec A. Ces deux matrices sont donc co-diagonalisables. Il existe donc $R \in \mathrm{GL}_n(\mathbb{R})$ tel que $A = R\mathrm{diag}(\mu_i)R^{-1}$ et $A' = R\mathrm{diag}(\mu_i')R^{-1}$. Comme $\exp(A) = \exp(A')$, nécessairement, $e^{\mu_i} = e^{\mu_i'}$ pour tout i. L'injectivité de l'exponentielle réelle permet de conclure.
Enfin, montrons la bi-continuité. On va passer par la caractérisation séquentielle de la continuité. Soit $(B_p)_p = (\exp(A_p))_p$ une suite de $\mathrm{S}_n^{++}(\mathbb{R})$ qui converge vers $B = \exp(A) \in \mathrm{S}_n^{++}(\mathbb{R})$. Il s'agit de montrer que $A_p \to A$. Comme la suite (B_p) converge, elle est bornée (pour toute norme) et donc en particulier pour la norme $|||\cdot|||_2$, définie par:

$$|||M|||_2 = \sqrt{\rho({}^tMM)}.$$

Or, pour $M \in \mathrm{S}_n^{++}(\mathbb{R})$, on a :

$$|||M|||_2 = \sqrt{\rho({}^tMM)} = \sqrt{\rho(M^2)} = \rho(M) = \max\{\mathrm{Spec}(M)\}.$$

Donc tous les spectres des B_p sont majorés par une constante C. En appliquant le même raisonnement à B_p^{-1}, on constate que les spectres des B_p sont minorés par une constante C'. Par suite, toutes les valeurs propres des B_p sont incluses dans le compact $[C, C'] \subset]0, +\infty[$. Ainsi, les valeurs propres des A_p sont alors incluses dans le compact $[\log(C'), \log(C)]$. La suite (A_p) est donc également bornée. Montrons que A est l'unique valeur d'adhérence de (A_p). Supposons qu'on ait une sous suite $(A_{\varphi(p)})$ qui converge vers $\bar{A}$. On a $\exp(A_{\varphi(p))} = B_{\varphi(p)}$ pour tout p. On en déduit alors, par continuité et injectivité de l'exponentielle, que $\exp(\bar{A}) = B = \exp(A)$ et donc $A = \bar{A}$. Comme dans une espace vectoriel de dimension finie, une suite bornée qui n'a qu'une valeur d'adhérence converge vers celle-ci, cela conclut. □

Remarque 3.4. Par deux fois j'ai présenté ce developpement à l'agrégation. Ce que j'en ai retenu, c'est que le jury demande systématiquement d'expliquer la continuité de l'exponentielle de matrices, d'expliciter le polynôme interpolateur, et pourquoi la norme 2 revient au rayon spectral dans le cas des matrices symétriques.

3.6 Classification des groupes simples d'ordre 60

Difficulté : Facile
Thèmes : Théorème de Sylow, action de groupe, groupe quotient, groupe symétrique
Leçons concernées : **101**, **103**, **104**, **105**
Références : Szpirglas, Mathématiques L3 Algèbre

Enoncé 7. *Soit G un groupe simple d'ordre 60. Alors G est isomorphe à A_5.*

Démonstration. L'idée est de faire agir G sur un ensemble de cardinal 5, par exemple G/H, avec H un sous-groupe d'indice 5 dans G. Commençons par montrer qu'un tel H existe.
Supposons par l'absurde qu'il n'existe pas de sous groupe strict de G d'indice inférieur ou égal à 5. On a

$$60 = 2^2 \cdot 3 \cdot 5.$$

Considérons N_2 l'ensemble des 2-Sylow de G, et n_2 son cardinal. Par les théorèmes de Sylow, on a n_2 qui divise 15. De plus, l'action par conjugaison de G sur N_2 est transitive (les p-Sylow étant tous conjugués). On a alors par la formule des classes, pour x un 2-Sylow quelconque:

$$|G| = |\mathrm{Stab}_x| \ |O_x| = |\mathrm{Stab}_x| \ n_2.$$

Le stabilisateur étant un sous-groupe de G, n_2 est donc l'indice du stabilisateur d'un 2-Sylow quelconque. Si $n_2 = 1$, alors le 2-Sylow est distingué dans G ce qui est absurde par hypothèse. Par hypothèse, on a nécessairement $n_2 = 15$ car sinon, on aurait un sous groupe d'indice ≤ 5. On a alors 15 2-Sylow.
Considérons maintenant S_1 et S_2, deux 2-Sylow distincts de G. Montrons que leur intersection est réduit au neutre. Soit $g \in S_1 \cap S_2$. D'après la classification des groupes finis d'ordre 4, tous les 2-Sylow sont abéliens, donc le centralisateur de g, $C(g)$, contient $S_1 \cup S_2$. Cette réunion est de cardinal ≥ 4 puisque S_1 et S_2 sont disctincts, et comme $C(g)$ contient S_1, son cardinal est un multiple de 4 (par le théorème de Lagrange). Les multiples de 4 qui divisent 60 sont respectivement 12,20 et 60. D'après l'hypothèse qu'on a faite au départ, on a nécessairement, $C(g) = 60$. Donc g est dans le centre. Si $g \neq e$, alors le centre est non trivial et distingué dans G, absurde car G est simple. Donc $g = e$. Mais alors, on a

$$|\{x \in G, \ \mathrm{ord}(x) = 2 \text{ ou } \mathrm{ord}(x) = 4\}| = 15 \ (4-1) = 45.$$

On a fini avec les 2-Sylow. Regardons maintenant les 5-Sylow. Les théorèmes de Sylow donnent directement que le nombre de 5-Sylow, n_5, vaut 6. Chaque 5-Sylow est cyclique d'ordre 5 et d'intersection le neutre deux à deux. En effet, s'ils avaient un élément non trivial en commun, cet élément serait nécessairement générateur des deux groupes car 5 est premier. Ainsi,

$$|\{x \in G, \ \mathrm{ord}(x) = 5\}| = 6 \ (5-1) = 24.$$

Or, $45 + 24 = 69 > 60$. Absurde. Donc G admet un sous-groupe strict d'indice ≤ 5.
Supposons désormais que G admette un sous groupe d'indice ≤ 4, et montrons que c'est impossible. Soit H un tel sous-groupe. Alors G agit naturellement et non trivialement à gauche sur l'ensemble G/H et induit un morphisme (non trivial)

$$\Phi : G \longrightarrow S_{|G/H|}.$$

Comme G a cardinal 60 et $S_{|G/H|}$ a cardinal $\leq 4! = 24$, le morphisme Φ n'est pas injectif, ce qui signifie que $\ker \Phi$ est non trivial. Donc G admet un sous-groupe distingué. Absurde!
On a alors montré qu'il existe un sous groupe H d'indice égal à 5 dans G. Par le même raisonnement, on dispose d'un morphisme Ψ de G dans $S_{|G/H|}$. G étant simple, le morphisme est injectif. Or, $S_{|G/H|}$ a cardinal 120 et G cardinal 60. Donc par le 1er théorème d'isomorphisme, G est isomorphe à un sous-groupe d'indice 2 dans $S_{|G/H|}$. Par unicité du morphisme signature, on a G isomorphe à $A_{|G/H|} \simeq A_5$ □

Remarque 3.5. Il y a deux subtilités dans ce développement. La première est d'expliquer pourquoi les actions à la fin de la preuve sont non triviales. Et pourquoi, le centre est réduit au neutre (notez que dans $\mathbb{Z}/p\mathbb{Z}$, le centre est non trivial mais le groupe est simple par exemple.) Sinon, c'est mon développement préféré, il est simple à apprendre, simple à comprendre, et un régal à présenter!

3.7 Un critère de diagonalisation de matrices: le critère de Klarès

Difficulté : Moyenne
Thèmes : Endormorphismes diagonalisables, formes (bi)linéaire, dimension d'un espace vectoriel, endormorphisme nilpotent, commutant, décomposition de Dunford
Leçons concernées : **152**, **156**
Références : Caldero, Carnet de voyage en Algébrie

Enoncé 8. *Soit A une matrice de $\mathcal{M}_n(\mathbb{K})$, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On suppose que le polynôme caractéristique de A est scindé sur $\mathbb{K}$. Alors A vérifie*

$$A \text{ est diagonalisable } \iff \ker(Comm_A) = \ker(Comm_A)^2.$$

où $(Comm_A)$ désigne l'endormorphisme de $\mathcal{M}_n(\mathbb{K})$ qui envoie une matrice X sur $AX - XA$.

Démonstration. Commençons par le sens direct en supposant que A est diagonalisable. Montrons que (Comm_A) est diagonalisable. On sait qu'il existe un polynôme $P \in \mathbb{K}[X]$ scindé simple tel que $P(A) = 0$. Appelant respectivement L_A et R_A les endormorphismes de $\mathcal{M}_n(\mathbb{K})$ de multiplication à gauche (respectivement à droite), on a les propriétés suivantes, pour tout $k \in \mathbb{N}$

$$L_A^k = L_{A^k}, \quad R_A^k = R_{A^k}.$$

par associativité de la multiplication de matrices. Donc, par suite,

$$P(L_A) = L_{P(A)} = L_0 = 0_{\mathcal{L}(\mathcal{M}_n(\mathbb{K}))}, \quad P(R_A) = R_{P(A)} = R_0 = 0_{\mathcal{L}(\mathcal{M}_n(\mathbb{K}))}$$

L'associativité de la multiplication de matrices donnent également que $R_A \circ L_A(X) = L_A \circ R_A(X)$, pour tout $X \in \mathcal{M}_n(\mathbb{K})$. Donc L_A et R_A commutent, ces deux endormorphismes sont donc annulés par un scindé simple et commutent, ils sont donc codiagonalisables, et leur différence, (Comm_A), est donc diagonalisable. Il est clair qu'on a l'inclusion $\ker(\mathrm{Comm}_A) \subset \ker(\mathrm{Comm}_A)^2$. Montrons l'inclusion réciproque. Comme (Comm_A) stabilise son noyau, (Comm_A) induit une application $f = (\mathrm{Comm}_A)|_{\ker(\mathrm{Comm}_A)}$. Celle-ci est diagonalisable comme restriction d'application diagonalisable. De plus, si $x \in \ker(\mathrm{Comm}_A)$, on a:

$$0 = (\mathrm{Comm}_A)(x) = (\mathrm{Comm}_A)^2(x) = f^2(x),$$

car $\ker(\mathrm{Comm}_A)$ commute avec lui même, donc f est nilpotente et diagonalisable donc nulle au sens des applications linéaires, ce qui implique que $\ker(\mathrm{Comm}_A)^2 = \ker(\mathrm{Comm}_A)$.
Montrons désormais l'implication réciproque en supposant $\ker(\mathrm{Comm}_A) = \ker(\mathrm{Comm}_A)^2$. Commençons par montrez

$$\ker(\mathrm{Comm}_A) \cap \mathrm{Im}(\mathrm{Comm}_A) = \{0\}.$$

Soit $X \in \ker(\mathrm{Comm}_A) \cap \mathrm{Im}(\mathrm{Comm}_A)$. Il existe $Y \in \mathcal{M}_n(\mathbb{K})$ tel que $(\mathrm{Comm}_A)(Y) = X$. En composant cette égalité par (Comm_A), il vient alors

$$(\mathrm{Comm}_A)^2(Y) = (\mathrm{Comm}_A)(X) = 0.$$

puisque X est également dans le noyau par hypothèse. Ainsi, $(\mathrm{Comm}_A)^2(Y) = 0$ mais puisque $\ker(\mathrm{Comm}_A) = \ker(\mathrm{Comm}_A)^2$, $(\mathrm{Comm}_A)^2(Y) = (\mathrm{Comm}_A)(Y) = 0$. D'où $X = 0$. Maintenant introduisons la forme bilinéaire Φ définie pour tout $X, Y \in \mathcal{M}_n(\mathbb{K})$ par $\Phi(X, Y) = \mathrm{Tr}(XY)$. Elle est symétrique par les propriétés de la trace et non dégénérée par le fait que si X est non nul, on peut toujours trouver la bonne matrice Y tel que le produit XY a une trace non nul. Montrons alors que

$$\ker(\mathrm{Comm}_A)^\perp = \mathrm{Im}(\mathrm{Comm}_A).$$

Le fait que Φ soit non dégénéré nous donne que ces deux espaces vectoriels ont la même dimension. En effet, par le théorème du rang,

$$\dim \ker(\mathrm{Comm}_A)^\perp = \dim \mathcal{M}_n(\mathbb{K}) - \dim \ker(\mathrm{Comm}_A) = \dim \mathrm{Im}(\mathrm{Comm}_A). \tag{1}$$

Il suffit alors de montrer une seule inclusion. Soit $Y \in \mathrm{Im}(\mathrm{Comm}_A)$, il existe $X \in \mathcal{M}_n(\mathbb{K})$ tel que $Y = AX - XA$. Donc pour toute matrice Z qui commute avec A, *i.e.*, $Z \in \ker(\mathrm{Comm}_A)$, il vient

$$\mathrm{Tr}(YZ) = \mathrm{Tr}(AXZ - XAZ) = \mathrm{Tr}(A(XZ) - (XZ)A) = 0.$$

Donc Y est bien orthogonal à toutes les matrices de noyau pour la forme bilinéaire Φ. Ecrivons pour finir la décomposition de Dunford $A = D + N$, avec D diagonalisable et N nilpotente. Pour conclure la démonstration, il suffit de montrer que $N = 0$. Pour cela, on va montrer que $N \in \ker(\mathrm{Comm}_A)^\perp$. Soit $Z \in \ker(\mathrm{Comm}_A)$. Par définition de Z, Z commute avec A. De plus, par un corollaire de la décomposition de Dunford, N est un polynôme en A donc commute avec A également. Donc N et Z commutent, et le produit NZ est donc nilpotent, et $\mathrm{Tr}(NZ) = 0$. Par l'égalité 1, on a donc que $N \in \mathrm{Im}(\mathrm{Comm}_A)$. Or, N commute avec A donc $N \in \ker(\mathrm{Comm}_A) \cap \mathrm{Im}(\mathrm{Comm}_A) = \{0\}$ ce qui conclut la preuve. □

Remarque 3.6. Cette preuve utilise beaucoup de notions du programme et donc, d'un point de vue optimisation des developpements, on se régale. En revanche, la première question est de se dire, mais bordel à quoi ça sert ?? Après m'être posé la question, je dirais que d'un point de vue numérique, savoir si une matrice est diagonalisable est une tâche assez ardue, en revanche, savoir si deux noyaux sont égaux revient à faire deux pivots de Gauss.

3.8 Théorème fondamental de l'algèbre (d'Alembert-Gauss)

Difficulté : Moyenne
Thèmes : Extensions de corps, racines d'un polynôme, polynômes symétriques
Leçons concernées : **125**, **144**, **141**
Références : Berhuy, Algèbre : Le grand combat

Enoncé 9. *Tout polynôme non constant de $\mathbb{C}[X]$ admet une racine dans $\mathbb{C}$.*

Démonstration. Commençons par le cas où $P \in \mathbb{R}[X]$. Sans perte de généralité, on peut supposer que P est unitaire. Nous allons alors démontrer le résultat par récurrence sur $n = v_2(\deg P)$, la 2-valuation du degré de P. Pour tout $n \geq 0$, on pose H_n la propriété suivante:

> Tout polynôme $P \in \mathbb{R}[X]$ unitaire non constant à coefficients réelles tel que $v_2(\deg P) \leq n$ admet une racine dans $\mathbb{C}$.

Commençons par l'initialisation, *i.e.*, le cas $n = 0$. Dans ce cas, le degré de P est impair et donc les limites de la fonction polynômiale associée à P vérifie respectivement

$$\lim_{x \to -\infty} P(x) = -\infty, \qquad \lim_{x \to +\infty} P(x) = +\infty.$$

Donc, par le théorème des valeurs intermédiaires, il existe $\alpha \in \mathbb{R}$, tel que $P(\alpha) = 0$. Supposons donc que H_n est vraie et montrons que H_{n+1} est vraie. Soit P un polynôme unitaire non constant à coefficients réelles tel que $v_2(\deg P) \leq n+1$. Ecrivons $d = \deg P = 2^k s$, où s est impair et $k \in \{0, \dots, n+1\}$. Si $k = 0$, on applique H_0 et c'est fini, on peut donc supposer $k \geq 1$.
Soit $\mathbb{L}$ une extension de décomposition de P sur $\mathbb{R}$. Sur $\mathbb{L}$, P est scindé, on peut donc écrire

$$P = (X - \alpha_1) \cdots (X - \alpha_d), \quad \alpha_i \in \mathbb{L}$$

Soit c un réel fixé dans $\mathbb{R}$ et posons

$$Q_c = \prod_{1 \leq i < j \leq d} (X - (\alpha_i + \alpha_j + c\alpha_i\alpha_j) \in \mathbb{L}[X].$$

Si l'on montre que Q est à coefficients réels, on pourra appliquer l'hypothèse de récurrence car $\deg Q_c = |\{(i,j),\ 1 \leq i < j \leq d\}| = \frac{d(d-1)}{2} =$ et $v_2(\deg Q_c) = k - 1$. Soit alors a un coefficient de Q_c. D'après les relations coefficients racines, $a = \pm\sigma(y_{i,j})$ où $y_{i,j} = \alpha_i + \alpha_j + c\alpha_i\alpha_j$ et σ est un polynôme symétrique élémentaire en les $d' = \frac{d(d-1)}{2}$ variables $(Y_{i,j})_{1 \leq i < j \leq d}$.
Considérons l'unique morphisme d'anneau

$$\begin{aligned} \Psi :\ \mathbb{R}[Y_{i,j},\ 1 \leq i < j \leq d] &\to \mathbb{R}[X_1, \dots, X_d] \\ Y_{i,j} &\mapsto X_i + X_j + cX_iX_j \end{aligned}$$

et notons $\tilde{\sigma} = \Psi(\sigma)$. On a alors $\tilde{\sigma}(x_1, \dots, x_d) = \sigma(y_{i,j}) = \pm a$. Il faut alors montrer que $\tilde{\sigma}$ est symétrique. Puisque S_d est engendré par les transpositions, on va montrer que $\tilde{\sigma}$ est invariant par toute transposition. Soit alors $\tau = (pq)$, avec par exemple $p < q$. Notons $\tilde{\sigma}^\tau$ la polynôme obtenu en permutant X_p et X_q. Cette transposition induit une permutation $\tilde{\tau}$ de $\{Y_{i,j},\ 1 \leq i \leq j \leq d\}$. Non seulement τ envoie un $Y_{i,j}$ sur un $Y_{k,l}$ mais ceci de façon surjective, donc bijective. Puisque σ est symétrique en les $Y_{i,j}$, on obtient :

$$\tilde{\sigma}^\tau(X_1, \dots, X_d) = \tilde{\sigma}^\tau(Y_{i,j}) = \sigma(Y_{i,j}) = \tilde{\sigma}(X_1, \dots, X_d)$$

donc $\tilde{\sigma}$ est bien symétrique. Il existe donc $T \in \mathbb{R}[X_1, \dots, X_d]$ tel que $\tilde{\sigma}(X_1, \dots, X_d) = T(\Sigma_1, \dots, \Sigma_d)$, où les $\Sigma_1, \dots, \Sigma_d$ sont les polynômes symétriques élémentaires en les $(X_1, \dots, X_d)$. De là, on obtient

$$a = \pm\sigma(y_{i,j}) = \pm\tilde{\sigma}(x_1, \dots, x_d) = \pm T(\bar{\Sigma_1}, \dots, \bar{\Sigma_d})$$

où $\bar{\Sigma_k} = \Sigma_k(x_1, \dots, x_d)$. Or, $\bar{\Sigma_k}$ est, au signe près, le $(d-k)$ème coefficient de P, donc dans $\mathbb{R}$. Puisque T est à coefficients réelles, on en déduit que a est réel aussi, donc Q_c est à coefficients réels, cela pour tout $c \in \mathbb{R}$.

Par hypothèse de récurrence, Q_c admet donc une racine, notée z dans $\mathbb{C}$. Comme $\mathbb{C} \subset \mathbb{K}$, et que les racines de Q_c sont les $y_{i,j}$, il existe $(i(c), j(c)) \in \{1, \dots, d\}^2$ tel que $Q_c(y_{i(c),j(c)}) = 0$. Or, l'application qui à c associe le couple $(i(c), j(c))$ n'est pas injective. Il existe donc c et c' tel que $(i(c), j(c)) = (i(c'), j(c'))$. Notant (k, l) ce couple, il vient

$$x_k + x_l + c x_k x_l = z_c \in \mathbb{C}, \qquad \text{et} \qquad x_k + x_k + c' x_l x_k = z_{c'} \in \mathbb{C}$$

Par conséquent, le produit

$$\Pi = x_k x_l = \frac{z_c - z_{c'}}{c - c'} \in \mathbb{C}$$

et la somme

$$\Sigma = x_k + x_l = z_c - c\Pi \in \mathbb{C}$$

Enfin, comme $(X - x_l)(X - x_k) = X^2 - \Sigma X + \Pi$, x_k et x_l sont les racines dans $\mathbb{K}$ d'un polynôme de degré deux à coefficients dans $\mathbb{C}$. La résolution classique des équations polynômiales de degré deux donnent alors que x_k et x_l sont dans $\mathbb{C}$. On a donc extrait deux racines de P dans $\mathbb{C}$. On conclut alors par principe de récurrence.

Il reste enfin à traiter le cas où le polynôme P de départ est à coefficients dans $\mathbb{C}$. Dans ce cas, il suffit de considérer le polynôme $P\overline{P}$. Ce polynôme est à coefficients dans $\mathbb{R}$ (pour s'en convaincre, calculer le conjugué de ce polynôme). Appliquant la démonstration précédente à ce polynôme, on extrait deux racines complexes de $P\overline{P}$. Par intégrité de $\mathbb{R}$, les racines sont soit, des racines de P, soit de $\overline{P}$. Dans le premier cas, on est content, dans l'autre, il suffit de prendre le conjugué de la racine pour trouver une racine de P. Cela conclut entièrement le théorème. □

Remarque 3.7. Dans la littérature, la partie sur les polynômes symétriques est souvent résumé en quelques lignes, où j'avoue ne pas comprendre grand chose. Elle est donc en théorie bien expliqué, grâce à la preuve que m'a transmise Mr Gervais (Merci Monsieur).

3.9 Théorème de Frobenius-Zolotarev

Difficulté : Moyenne
Thèmes : Signature d'une permutation, symbole de Legendre, corps finis, groupe dérivé et commutateur, parties génératrices d'un groupe.
Leçons concernées : **105**, **108**
Références : Beck, Objectif Agrégation

Enoncé 10. *Soit p un nombre premier impair et E un espace vectoriel sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ de dimension finie. Pour tout $u \in \mathrm{GL}(E)$, on a*

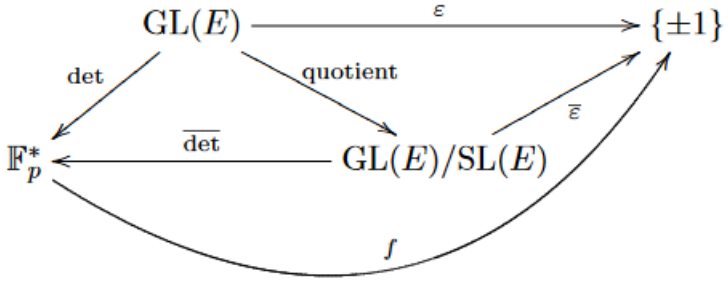
$$\varepsilon(u) = \left(\frac{\det(u)}{p}\right).$$

Commençons par une petite explication. Soit $u \in \mathrm{GL}(E)$. u permute un ensemble fini de vecteurs, on peut donc le voir comme un élément du groupe symétrique. On peut alors se demander quel est la signature de cette permutation, c'est tout l'objet de cet énoncé.

Démonstration. Observons pour commencer que le morphisme det : $\mathrm{GL}(E) \to \mathbb{F}_p^*$ se factorise par la propriété universel du quotient en un morphisme $\overline{\det}$ défini de $\mathrm{GL}(E)/\mathrm{SL}(E)$ dans $\mathbb{F}_p^*$ car, par définiton, $\mathrm{SL}(E)$ est exactement le noyau du déterminant. De plus, ce morphisme est un isomorphisme puisqu'il est surjectif au départ.
Montrons maintenant que le groupe dérivé de $\mathrm{GL}(E)$ est égal à $\mathrm{SL}(E)$. Pour cela, nous allons utiliser le fait que $\mathrm{SL}(E)$ est engendré par les transvections et que toutes transvections est un commutateur. On rappelle qu'une application linéaire f est une transvection s'il existe une base adaptée de E dans laquelle f s'écrive

$$\begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & \ddots & & & \vdots \\ \vdots & \vdots & \ddots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & 0 & 0 \\ 0 & 0 & \cdots & \cdots & 1 & 1 \\ 0 & 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

En particulier, deux transvections sont toujours conjuguéees (dans $\mathrm{GL}(E)$). Soit alors f une transvection, et considérons f^2. Si $(e_1, \ldots, e_n)$ est une base adaptée à f, alors $(e_1, \ldots, 2e_{n-1}, e_n)$ est une base adaptée à f^2. Donc f^2 est une transvection. De plus, comme f et f^2 sont conjuguées, il existe $u \in \mathrm{GL}(E)$, tel que $f^2 = ufu^{-1}$, ou de façon équivalente, $f = ufu^{-1}f^{-1}$. On a alors montré que toute transvection est un commutateur, ce qui donne l'inclusion $\mathrm{SL}(E) \subset D(\mathrm{GL}(E))$. Maintenant, tout commutateur étant de déterminant égal à 1, on a l'inclusion réciproque donc l'égalité. Or, on sait que le groupe dérivé est un sous groupe distingué du groupe de départ, ainsi l'application ε : $\mathrm{GL}(E) \to \{\pm 1\}$ se factorise par le quotient $\mathrm{GL}(E)/\mathrm{SL}(E)$ en un morphisme $\bar{\varepsilon} = \varepsilon \circ \pi$, où π est la projection canonique sur le groupe quotient. Résultat, on obtient le graphique suivant



On a donc un morphisme de groupes f : $\mathbb{F}_p^* \xrightarrow{\overline{\det}^{-1}} \mathrm{GL}(E)/\mathrm{SL}(E) \xrightarrow{\bar{\varepsilon}} \{\pm 1\}$ de tel sorte que $f \circ \det = \varepsilon$. Pour conclure la démonstration, il faut alors montrer que pour tout $x \in \mathrm{GL}(E)$, $f(x) = \left(\frac{x}{p}\right)$. Pour cela, on va alors

montrer qu'il existe un unique morphisme non trivial de $\mathbb{F}_p^*$ dans $\{\pm 1\}$, et que f en est un. Comme le symbole de Legendre est un tel morphisme, nécessairement, ceux-ci coïncident.
Tout d'abord, on sait (voir 5.3) que $\mathbb{F}_p^*$ est cyclique. Soit ω un générateur de $\mathbb{F}_p^*$ et soit ϕ un morphisme dans $\{\pm 1\}$. Comme ϕ est uniquement determiné par l'image de ω, si $\phi(\omega) = 1$, ϕ est trivial. Sinon, ϕ est non trivial, on a alors unicité d'un morphisme non trivial. Maintenant, montrons que f est non trivial. Pour cela, il suffit de considérer un $u \in \mathrm{GL}(E)$ particulier tel que $\varepsilon(u) = f(\det(u)) = -1$. En tant qu'espace-vectoriel, E est isomorphe à $\mathbb{F}_q$, le corps à $q = p^n$ éléments. Soient η un générateur de $\mathbb{F}_q$ et u l'endormorphisme défini par $u(x) = \eta x$. Comme $\mathbb{F}_q = \{1, \eta, \eta^2, \dots, \eta^{p^n-2}\}$, u coïncide avec le cycle $(1\ \eta\ \eta^2 \dots \eta^{p^n-2})$. C'est un cycle de longueur pair donc sa signature vaut -1, ce qui conclut. □

Remarque 3.8. A un moment donné, on utilise de manière essentielle que le groupe $\{\pm 1\}$ est abélien. Je laisse au lecteur la tâche de déterminer où cela intervient

3.10 Théorème de Chevalley-Warning et une application

Difficulté : Facile
Thèmes : Corps finis, racines d'un polynôme, dénombrement
Leçons concernées : **120**, **123**, **142**, **144**, **190**.
Références : Serre, Cours d'arithmétique pour l'énoncé, Zavidovique, Un max de maths pour l'application.

Enoncé 11. *On fixe $q = p^k$ une puissance d'un nombre premier. Soit (f_α) une famille de polynôme de $\mathbb{F}_q[X_1, \dots, X_n]$ de tel sorte que*

$$\sum_\alpha \deg(f_\alpha) < n.$$

Alors l'ensemble V des zéros communs des f_α dans $\mathbb{F}_q$ est congru à 0 modulo p

Démonstration. Posons $P = \prod_\alpha (1 - f_\alpha^{q-1})$ et soit $x \in \mathbb{F}_q^n$. Si $x \in V$, tous les f_α sont nuls et donc $P(x) = 1$. Si $x \notin V$, il existe un polynôme pour lequel $f_\alpha(x) = a \neq 0$. Or $a^{q-1} = 1$ ce qui implique que $P(x) = 0$. Ainsi, en posant $S(f) = \sum_{x \in \mathbb{F}_q^n} f(x)$, on a alors

$$|V| = S(P) \ mod \ p.$$

Il reste alors à montrer que $S(P) = 0$.
L'hypothèse $\sum \deg f_\alpha < n$ entraîne

$$\deg P \leq n(q-1).$$

De plus, P est combinaison linéaire de monôme $X^u = X_1^{u_1} \cdots X_r^{u_r}$, avec $\sum u_i \leq n(q-1)$. Il suffit alors de montrer que pour chacun de ces monômes, on a $S(X^u) = 0$. Or

$$S(X^u) = \sum_{x \in \mathbb{F}_q^n} \prod_i X_i^{u_i} = \prod_i \sum_{x \in \mathbb{F}_q^n} X_i^{u_i} = \prod_i S(X_u^{u_i})$$

Par le principe des tiroirs, il existe i_0 tel que $u_{i_0} < q - 1$. Or, considérant y un générateur de $\mathbb{F}_q$, l'automorphisme de $\mathbb{F}_q^*$ défini par $x \mapsto yx$ est un isomorphisme. Il vient alors

$$S(X_{i_0}^{u_{i_0}}) = \sum_{x \in \mathbb{F}_q^*} x^{u_{i_0}} = \sum_{yx \in \mathbb{F}_q^*} x^{u_{i_0}} = y^{u_{i_0}} \sum_{x \in \mathbb{F}_q^*} x^{u_{i_0}} = y^{u_{i_0}} S(X_{i_0}^{u_{i_0}})$$

D'où $S(X_{i_0}^{u_{i_0}}) = 0$ et par suite, $S(X^u) = 0$. □

Application. Toute forme quadratique sur un corps fini a plus de 3 variables admet un 0 non trivial.

La preuve découle directement de l'énoncé

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

Démonstration. Traitons dans un premier cas le cas où n est un nombre premier. Posons

$$P_1(X_1, \dots, X_{2p-1}) = \sum_{i=1}^{2p-1} X_i^{p-1}, \quad P_2(X_1, \dots, X_{2p-1}) = \sum_{i=1}^{2p-1} \bar{a_i} X_i^{p-1}, \ P_1, P_2 \in \mathbb{F}_p[X_1, \dots, X_{2p-1}]$$

Par le théorème de Chevalley-Warning, comme 0 est racine commune de ces deux polynômes, il existe au moins p racines communes. Considérons $x = (x_1, \dots x_{2p-1})$ une telle racine non triviale. L'évaluation de P_1 en x nous donne que pour chaque i, on a soit $x_i^{p-1} = 0$ ou 1 selon si x_i est nul ou non. Donc $P_1(x) = 0$ si et seulement s'il existe p ou 0 coordoonnées non nuls dans x. Comme $x \neq 0$, on a exactement p coordonnées non nuls dans x. L'évaluation de P_2 en x donne quant à elle

$$0 = P_2(x) = \sum_{i=1}^{2p-1} \bar{a_i} \delta_{x_i^{p-1}, 1}.$$

Ce qui donne le résultat voulu.
Revenons au cas général, que l'on va démontrer par récurrence. Pour $n = 1$, il n'y a rien à montrer. Supposons le résultat acquis pour $d < n$. Si n est premier, on conclut par ce qui précède, sinon, on écrit $n = pn'$, avec p premier (notons que $p, n' < n$). Remarquons également que $2n - 1 = (2n' - 1)p + p - 1$. Appliquant l'hypothèse de récurrence aux entiers $a_1, \dots, a_{2p-1}$, on peut trouver un ensemble E_1 de p entiers dont la somme est divisible par p, et de la même façon, on peut construire un ensemble E_2, disjoint de E_1, constitué lui aussi de p entiers parmi les $2n - 1 - p$ entiers restants dont la somme est aussi divisible par p. On continue alors jusqu'à ce qu'il reste $2p - 1$ entiers, c'est-à-dire exactement $2n' - 1$ fois. Notant S_i la somme des entiers dans E_i, on peut alors écrire $S_i = pS'_i$. En appliquant encore une fois l'hypothèse de récurrence aux S'_i, on trouve alors n' indice $k_1, \dots, k_{n'}$ tels que

$$n' \mid \sum_{i=1}^{n'} S'_{k_i}.$$

Considérons alors la réunion des E_{k_i}, cette réunion possède $pn' = n$ éléments. Notons les $a_{l_1}, \cdots, a_{l_n}$. Ils vérifient alors

$$\sum_{i=1}^{n} a_{l_i} = \sum_{j=1}^{n'} S_{n_j} = p \sum_{j=1}^{n'} S'_{n_j}.$$

On a alors bien $pn' = n \mid \sum_{i=1}^{n} a_{l_i}$, ce qui conclut. Remarquons que $n - 1$ zéros et $n - 1$ uns fournissent un exemple d'ensemble à $2n - 2$ éléments dont on ne peut pas trouver n éléments dont la somme est divisible par n. □

3.11 Un problème de dénombrement sur les corps finis : Le problème de Kakeya

Difficulté : Moyenne mais long développement
Thèmes : Dualité, dénombrement, corps finis, dimension d'un espace vectoriel.
Leçons concernées : **190**, **144**, **148**, **123**,
Références : Certaines idées de la preuve se trouvent dans le 131 développement pour l'oral, en revanche, cette version est une version non probabiliste.

Afin d'énoncer la proposition, commençons par parler un peu du problème. Initialement, le problème de Kakeya consiste à retourner une aiguille de longueur 1 sur le plan $\mathbb{R}^2$. La question étant "Quelle est l'aire minimal à couvrir pour retourner une aiguille". Généralisant l'idée selon laquelle, lorsque que l'on retourne l'aiguille, on a nécessairement parcouru toutes les directions du plan, on se demande alors, étant donné un espace affine sur un corps fini $\mathbb{F}_q$ de dimension n, combien de points doit-on prendre pour s'assurer d'avoir une droite contenant chacune des directions de l'espace affine ? Un tel espace est appelé espace de Kakeya. Formellement,

Definition 3.1. *Soit E un espace vectoriel de dimension n sur $\mathbb{F}_q$. On appelle espace de Kakeya un ensemble $K \subset E$ tel que, pour tout direction non triviale v de E, il existe un point $y \in E$ tel que la ligne*

$$L_{y,v} = \{y + tv,\ t \in \mathbb{F}_q\}$$

est dans K.

On souhaite alors minimiser le cardinal de K. Et c'est tout le sujet de l'énoncé suivant

Enoncé 12. *Soit K un ensemble de Kakeya sur E. Alors le cardinal de K vérifie*

$$|K| \geq \frac{1}{n!}|\mathbb{F}_q|^n.$$

La démonstration fait appel à deux résulats

Lemme 4. *Soit d un entier positif et $E \subset \mathbb{F}_q^n$ un ensemble tel que $|E| < \binom{n+d}{n}$. Alors il existe un polynôme $P \in \mathbb{F}_q[X_1, \dots, X_n]$ de degré au plus d, non trivial tel que P s'annule sur E.*

Preuve du premier lemme. Considérons $\mathbb{F}^E = \{f,\ f : E \to \mathbb{F}\}$ l'ensemble des applications de E dans $\mathbb{F} = \mathbb{F}_q$. Alors cet ensemble à une structure de $\mathbb{F}$-espace vectoriel. E étant fini, on peut ordonner arbitrairement ses éléments, par exemple tel que $E = \{e_i, i = 1, \dots, |E|\}$. Ainsi, une application $f \in \mathbb{F}^E$ est uniquement determiné par l'image par f des e_i, et donc la dimension de $\mathbb{F}^E$ comme $\mathbb{F}$ espace vectoriel est $|E|$. Considérons alors

$$\begin{aligned} \Phi : \mathbb{F}[X_1, \dots, X_n] &\longrightarrow \mathbb{F}^E \\ P &\mapsto \Phi(P). \end{aligned}$$

où pour $x \in E, \Phi(P)(x) = P(x)$. Cette application est linéaire mais la dimension de $\mathbb{F}_q[X_1, \dots, X_n]_d$ en tant que $\mathbb{F}$ espace vectoriel vérifie, en vertu de 5.5,

$$\dim \mathbb{F}_q[X_1, \dots, X_n]_d = \binom{n+d}{n} > |E|$$

donc Φ ne peut pas être injective, ce qui conclut le premier lemme □

Lemme 5. *Soit $P \in \mathbb{F}_q[X_1, \dots, X_n]$ de degré au plus $q-1$ s'annulant sur un ensemble de Kakeya K. Alors $P = 0$.*

Démonstration du deuxième lemme. Supposons par l'absurde que P soit non nul. Comme il s'annule sur un ensemble non vide, il est également non constant. P s'écrit alors

$$P = \sum_{a_1 + \dots + a_n \leq d} C_{a_1, \dots, a_n} X_1^{a_1} \cdots X_n^{a_n}.$$

avec d le degré de P. Notons alors

$$P_d = \sum_{a_1 + \dots + a_n = d} C_{a_1, \dots, a_n} X_1^{a_1} \cdots X_n^{a_n}.$$

la composante de degré d de P (comme P n'est pas constant, $\exists\, a_1, \dots, a_n \geq 0$ tel que $\sum a_i = d$ et $C_{a_1,\dots,a_n} \neq 0$). Soit alors v une direction quelconque de $\mathbb{F}_q^n$. Puisque K est un ensemble de Kakeya, il existe $y \in \mathbb{F}_q^n$ tel que $\{y + tv,\ t \in \mathbb{F}_q\} \subset K$. Puisque P s'annule sur K, on a

$$P(y + tv) = 0,\ \forall t \in \mathbb{F}_q.$$

Mais, en particulier, si l'on voit $P(y + tv)$ comme un élément de $\mathbb{F}_q[t]$, P est toujours de degré $d < q$. Or, un polynôme de degré d ayant strictement plus de d racines est nul. De cela on tire

$$P_d(t) = \sum_{a_1+\cdots+a_n=d} C_{a_1,\dots,a_n} t^d v_1^{a_1} \cdots v_n^{a_n} = 0.$$

et donc

$$\sum_{a_1+\cdots+a_n=d} C_{a_1,\dots,a_n} v_1^{a_1} \cdots v_n^{a_n} = 0.$$

et cela, pour toute direction arbitraire v. Ainsi, fixant les $n-1$ premières composantes de v et laissant variable la dernière, le polynôme à une indeterminée

$$\widetilde{P_d(v_n)} = \sum_{a_1+\cdots+a_n=d} C_{a_1,\dots,a_n} v_1^{a_1} \cdots v_n^{a_n} = 0.$$

est de degré $\leq d$ et s'annule pour tout $v_n \in \mathbb{F}$. De la même façon que précedemment, $\widetilde{P_d}$ est nulle, il vient alors

$$\sum_{a_1+\cdots+a_n=d} C_{a_1,\dots,a_n} v_1^{a_1} \cdots v_{n-1}^{a_{n-1}} = 0.$$

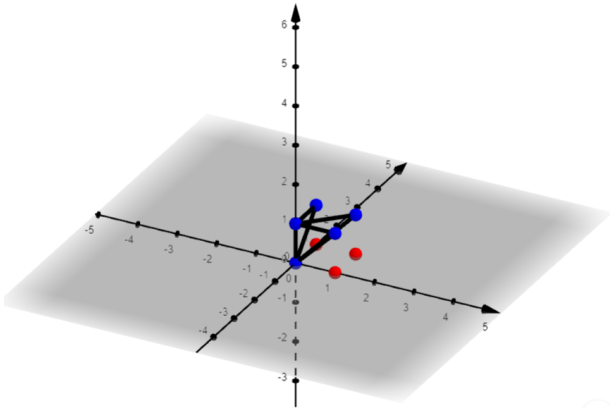
En itérant ce processus, on finit par obtenir que $C_{a_1,\dots,a_n} = 0$. Contradiction, donc $P = 0$ □

Démonstration de l'énoncé. Supposons qu'il existe un ensemble de Kakeya K de cardinalité au plus $\binom{n+q-1}{n}$, où $q = |\mathbb{F}_q|$. Le premier lemme assure l'existence d'un polynôme non nul de degré au plus $q-1$ qui s'annule sur K, mais le deuxième lemme assure l'inverse. Donc K vérifie nécessairement $|K| \geq \binom{n+q-1}{n}$. Or,

$$\binom{n+q-1}{n} = \frac{(n+q-1)!}{(q-1)!n!} = \frac{1}{n!} \prod_{j=q}^{n+q-1} j = \frac{q(q+1)\cdots(q+n-1)}{n!} = \frac{q^n}{n!} + O(q^{n-1}).$$

□

Remarque 3.9. Ce développement est un petit bijou qui vous fera briller aux yeux du jury. Il est original, pas si compliqué, on peut faire des dessins, il est extrêmement recasable. Le seul problème est qu'il n'y pas de référence, mais je vous assure que si vous vous plongez dedans, vous ne le regretterez pas et qu'il s'apprend facilement. Aussi, ce developpement utilise de façon non triviale 5.5, la preuve n'est pas dure mais il faut la connaître si ce devéloppement est présenté. Si vous ne voyez pas à quoi ressemble un ensemble de Kakeya, voilà un exemple



En bleu un ensemble de Kakeya dans $\mathbb{F}_2^3$

De manière générale, pour savoir combien de directions il y a sur $\mathbb{F}_q^n$, on fait agir par translation $\mathbb{F}_q^*$ sur $\mathbb{F}_q^n \backslash \{0\}$, et deux éléments sont dans la même orbite si et seulement s'ils sont colinéaires, si bien que la formule des classes donne alors que le nombre de directions est $\frac{q^n-1}{q-1}$ (qui est bien un entier).

3.12 Théorème de Wedderburn : Les corps finis sont tous commutatifs

Difficulté : Moyenne
Thèmes : Extensions de corps, action de groupes, polynômes cyclotomiques, racines de l'unité.
Leçons concernées : **101**, **102**
Références : Perrin, Cours d'Algèbre (Gourdon, Algèbre pour le lemme)

Lemme 6. *Soient $\mathbb{L}_1 \subset \mathbb{L}_2$ deux corps finis, avec $\mathbb{L}_1$ commutatif, alors il existe $k \in \mathbb{N}$ tel que $|\mathbb{L}_2| = |\mathbb{L}_1|^k$.*

Démonstration. $\mathbb{L}_1$ est sous-corps commutatif de $\mathbb{L}_2$ donc $\mathbb{L}_2$ est un $\mathbb{L}_1$-espace vectoriel de dimension k finie. Le corps $\mathbb{L}_2$ est donc isomorphe comme $\mathbb{L}_1$-espace vectoriel à $\mathbb{L}_1^k$. □

Enoncé 13. *Tout corps fini est commutatif.*

Démonstration. Considérons un corps $\mathbb{K}$, pas nécessairement commutatif, et soit Z son centre

$$Z = \{a \in \mathbb{K},\ \forall x \in \mathbb{K}, ax = xa\}.$$

Z est un sous corps commutatif de $\mathbb{K}$ de cardinal $q \geq 2$, ($0_{\mathbb{K}}$ et $1_{\mathbb{K}} \in Z$). Donc par le lemme, $|\mathbb{K}| = q^n$.
Supposons $\mathbb{K}$ non commutatif, donc $n > 1$. Alors $\mathbb{K}^*$ opère sur lui-même par conjugaison. Pour $x \in \mathbb{K}^*$, on note O_x l'orbite de x. On pose également $\mathbb{K}_x = \{y \in \mathbb{K},\ yx = xy\}$ le centralisateur de x. $\mathbb{K}_x$ est un sous-corps de $\mathbb{K}$ (pas nécessairement commutatif) et le stabilisateur de l'action décrite ci-dessus est $\mathbb{K}_x^*$. Comme $Z \subset \mathbb{K}_x$, on a $|\mathbb{K}_x| = q^d$.
Remarquons que d divise nécessairement n. En effet, l'inclusion $\mathbb{K}_x^* \subset \mathbb{K}$ entraîne $q^d - 1$ divise $q^n - 1$. Et si on écrit $n = pd + r$ la division de n par d, on a alors:

$$\begin{aligned} q^n - 1 = (q^d)^m q^r - 1 &= ((q^d - 1) + 1)^m q^r - 1 \\ &\equiv q^r - 1 \quad [q^d - 1]. \end{aligned}$$

Par suite, il existe donc $k \in \mathbb{Z}$ tel que

$$q^n - 1 = k(q^d - 1) + q^r - 1.$$

$q^d - 1$ est non nul puisque $q \geq 2$ et $d \geq 1$ et $0 \leq q^r - 1 < q^d - 1$.
Donc $q^r - 1$ est le reste de la division euclidienne de $q^n - 1$ par $q^d - 1$. Ce reste est nul si et seulement si $r = 0$, ou de façon équivalente, si d divise n.
Revenons à notre action par conjugaison. La formule de Burnside donne alors

$$|O_x| = \frac{|\mathbb{K}^*|}{|\mathbb{K}_x^*|} = \frac{q^n - 1}{q^d - 1}.$$

De plus, par définition des polynômes cyclotomiques dans $\mathbb{Z}$, on a

$$q^n - 1 = \prod_{m|n} \Phi_m(q), \qquad q^d - 1 = \prod_{m|d} \Phi_m(q).$$

donc

$$\frac{q^n - 1}{q^d - 1} = \prod_{m|n, m\nmid d} \Phi_m(q).$$

Pour $d \neq n$, on a n qui divise n mais pas d, donc on observe que $\Phi_n(q)$ divise $\frac{q^n-1}{q^d-1}$.
Ecrivons désormais l'équation aux classes. Celle-ci donne :

$$|\mathbb{K}^*| = |Z^*| + \sum_{x \notin Z/\sim} |O_x|.$$

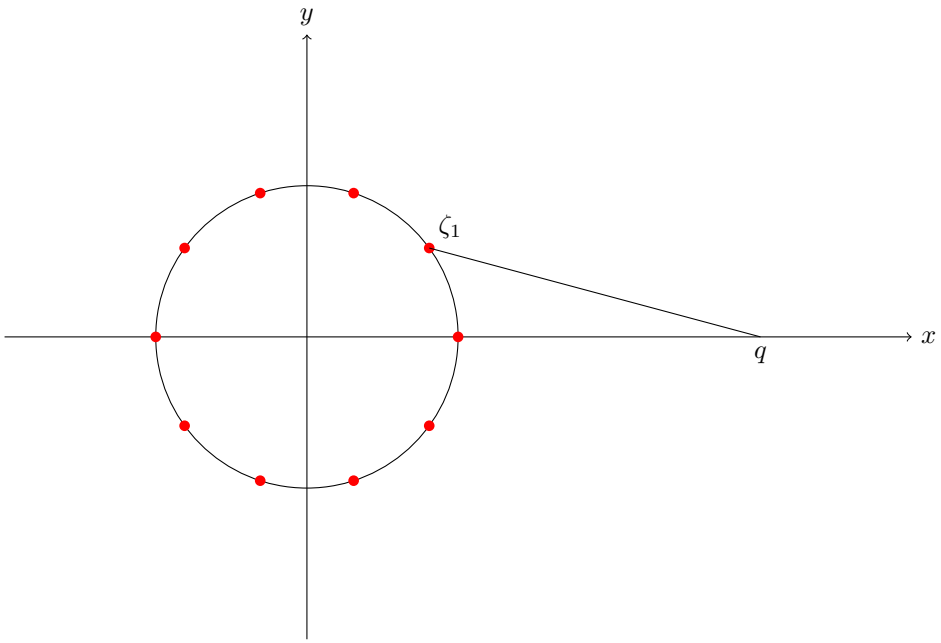
Dire que x n'est pas dans Z signifie que l'on a $d \neq n$ et

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1}.$$

où la somme porte sur certains diviseurs (stricts) de n. Comme $\Phi_n(q)$ divise q^n-1 et $\frac{q^n-1}{q^d-1}$, $\Phi_n(q)$ divise $q-1$. En particulier, $|\Phi_n(q)| \leq q-1$.
Pour conclure, on a

$$\Phi_n(q) = (q-\zeta_1)\cdots(q-\zeta_l).$$

où les ζ_i sont les racines primitives n-èmes de l'unité dans $\mathbb{C}$. Elles vérifient donc pour tout $i, |\zeta_i| = 1$ et $\zeta_i \neq 1$ puisque $n \neq 1$. Mais alors pour tout $i, |q-\zeta_i| > q-1$ (Essentiel de faire un dessin ici) et donc $|\Phi_n(q)| \geq (q-1)^l \geq q-1$. Contradiction. Donc $n = 1$. □



3.13 Théorème de Sylow version opération de groupes

Difficulté : Moyenne
Thèmes : Actions de groupes, Conjugaison, groupes finis
Leçons concernées : **101**, **103**, **104**
Références : Perrin, Cours d'Algèbre

Enoncé 14. *Soit G un groupe fini tel que $|G| = p^\alpha m$, avec $p \wedge m = 1$, p premier et $\alpha \geq 1$. Soit n_p le nombre de p-Sylow de G. Alors*

1. $n_p \geq 1$
2. *Tous les p-Sylows de G sont conjugués et tout conjugué d'un p-Sylow en est un autre,*
3. $n_p = 1 \ mod \ p$,
4. n_p *divise* m.

Remarque 3.10. Pour $G = \mathrm{GL}_n(\mathbb{F}_p)$, $H = \{A \in \mathrm{GL}_n(\mathbb{F}_p), A = (a_{i,j})_{i,j}, a_{i,i} = 1, a_{i,j} = 0 \text{ si } j < i\}$, on a

$$|G| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}), \quad |H| = p^{\frac{n(n+1)}{2}} k, \ k \wedge p = 1.$$

Donc H est un p-Sylow de G.

Remarque 3.11. Puisque G est fini, par le théorème de Cayley, on peut injecter G dans S_n. De la même façon, S_n s'injecte dans $\mathrm{GL}_n(\mathbb{F}_p)$ via les matrices de permutation. On va utiliser ce fait là à travers le lemme suivant.

Lemme 7. *Soit H un sous-groupe de G, et S un p-Sylow de G. Alors il existe a dans G tel que le sous-groupe $aSa^{-1} \cap H$ soit un p-Sylow de H.*

Preuve du lemme. G agit sur l'ensemble G/S naturellement à gauche. Le stabilisateur d'un élément aS de G/S est aSa^{-1}. On peut restreindre cette action à H et le stabilisateur de l'action induite est alors $aSa^{-1} \cap H$. De plus, pour tout $a \in G$, $aSa^{-1} \cap H$ est un p-Sylow de H si et seulement si l'indice de ce sous groupe dans H est premier avec p. Or, la formule des classes appliquée à l'action de H donne alors

$$m = |G/S| = \sum_{a \in R} |O_{aS}| = \sum_{a \in R} \left| \frac{H}{aSa^{-1} \cap H} \right|.$$

En particulier, il existe au moins un $a \in R \subset G$ tel que $\left|\frac{H}{aSa^{-1} \cap H}\right|$ soit premier avec p, sinon p diviserait m, absurde. □

Démonstration.

1. Comme G est un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$ par la première remarque, et que $\mathrm{GL}_n(\mathbb{F}_p)$ admet un p-Sylow, d'après le lemme, G admet un p-Sylow.

2. Soit H et S deux p-Sylows de G. D'après le lemme, il existe a dans G tel que $H \cap aSa^{-1}$ soit un p-Sylow de H. Or, $H \cap aSa^{-1} \subset H$ et ce sont deux p-groupes de même cardinal, on a donc $H \cap aSa^{-1} = H$ d'où $aSa^{-1} = H$.

3. Notons X l'ensemble des p-groupes de G. Alors $n_p = |X|$. Soit S un p-groupe de G. S agit par conjugaison sur X par restriction de l'action de G (bien définie d'après 2). La formule des classes pour cette action donne

$$|X| = n_p = \sum_{x \in X/\sim} |O_x| = |X^S| + \sum_{x \in X/\sim, \mathrm{Stab}_x \neq S} \left| \frac{S}{\mathrm{Stab}_x} \right|$$

La somme de droite est divisible par p puisque c'est l'indice d'un certain sous groupe d'un p-groupe. Il reste donc à montrer que $|X^S| = 1$. Puisque S est stable par l'action, il est clair que $|X^S| \geq 1$. Soit alors $T \in X^S$. Soit N le sous-groupe de G engendré par S et T. Pour tout $n \in S \cup T$, $nTn^{-1} = T$ puisque $T \in X^S$. Donc T est distingué dans N puisque T commute avec les éléments de T et S. Or, T et S sont deux p-Sylow de N (puisque ce sont deux p-Sylow de G) donc d'après (2), T est l'unique p-Sylow de N et donc $T = S$. Par suite, $X^S = 1$.

4. Enfin, soit S un p-Sylow de G. La formule des classes donnent

$$n = |G| = \mathrm{Stab}(G) \cdot \mathrm{O}_S.$$

Or $\mathrm{O}_S = n_p$ donc $n_p | n$.

□

4 Analyse et Probabilités

4.1 Densité des polynômes orthogonaux dans $L^2(\mathbb{R}, \rho)$

Difficulté : Moyenne
Thèmes : Transformée de Fourier, principe du prolongement analytique, théorème d'holomorphie sous le signe intégrale, bases hilbertiennes.
Leçons concernées : **234**, **250**, **213**, **245**.
Références : Beck, Objectif Agrégation

Definition 4.1. *Soit I un intervalle de $\mathbb{R}$. On appelle fonction poids une fonction $\rho : I \to \mathbb{R}$ mesurable, strictement positive et telle que*

$$\forall n \in \mathbb{N}, \quad \int_I |x|^n \rho(x) \mathrm{d}x < +\infty.$$

On note $L^2(I, \rho)$ l'espace des fonctions intégrables de carré intégrable pour la mesure de densité ρ par rapport à la mesure de Lebesgue.

Enoncé 15. *Soient I un intervalle de $\mathbb{R}$ et ρ une fonction poids. On suppose qu'il existe $\alpha > 0$ tel que*

$$\int_I e^{\alpha|x|} \rho(x) \mathrm{d}x < +\infty.$$

Alors les polynômes orthogonaux associés à ρ forment une base hilbertienne de $L^2(I, \rho)$.

Démonstration. On souhaite montrer qu'une famille est une base hilbertienne de $L^2(I, \rho)$. Considérons donc $f \in \overline{\mathrm{Vect}(\{x^n,\ n \in \mathbb{N}\})}^{\perp}$ et montrons que $f = 0$. Posons la fonction φ définie par

$$\forall x \in \mathbb{R}, \quad \varphi(x) = \begin{cases} f(x)\rho(x), & \text{si } x \in I, \\ 0, & \text{sinon.} \end{cases}$$

Cette fonction est L^1. En effet, puisque pour tout $t \geq 0$, on a $t \leq \frac{1+t^2}{2}$, il vient

$$\forall x \in I, \quad |f(x)|\rho(x) \leq \frac{1}{2}(1 + |f(x)|^2)\rho(x).$$

Comme f est $L^2(I, \rho)$ et ρ est L^1, on a ρf^2 intégrable sur I. On déduit alors que φ est L^1.
Comme on a une fonction L^1, on peut calculer sa transformée de Fourier:

$$\forall x \in \mathbb{R}, \quad \hat{\varphi}(z) = \int_I f(x) e^{-ixz} \rho(x) \mathrm{d}x.$$

Notons à présent $B_\alpha = \{z \in \mathbb{C}, |\mathrm{Im}\ z| < \frac{\alpha}{2}\}$. Montrons que $\hat{\varphi}$ se prolonge en une fonction holomorphe sur B_α.
Posons $g(z, x) = e^{-izx} f(x)\rho(x)$. Pour $z \in B_\alpha$, on a

$$\begin{aligned} \int_I |g(z,x)| \mathrm{d}x &\leq \int_I e^{\alpha|x|/2} |f(x)| \rho(x) \mathrm{d}x. \\ &\leq \left(\int_I e^{\alpha|x|} \rho(x) \mathrm{d}x \right)^{\frac{1}{2}} \left(\int_I |f(x)|^2 \rho(x) \mathrm{d}x \right)^{\frac{1}{2}} < +\infty. \end{aligned}$$

Ainsi, la fonction F, qui à $z \in B_\alpha$ associe $F(z) = \int_I g(z, x) \mathrm{d}x$ est bien définie. De plus,
Pour tout $z \in B_\alpha$, l'application $x \mapsto g(z, x)$ est mesurable,
Pour presque tout $x \in I$, l'application $z \mapsto g(z, x)$ est holomorphe,
Pour tout z tel que $|\mathrm{Im}\ z| < \frac{\alpha}{2}$

$$|g(z, x)| \leq h(x) = e^{\alpha|x|/2} |f(x)| \rho(x).$$

avec $h \in L^1(I)$. Ainsi par le théorème d'holomorphie sou l'intégrale, F est holomorphe sur B_α, connexe de $\mathbb{C}$ et coïncide sur $\mathbb{R}$ avec $\hat{\varphi}$. On peut alors calculer les dérivées successives de F :

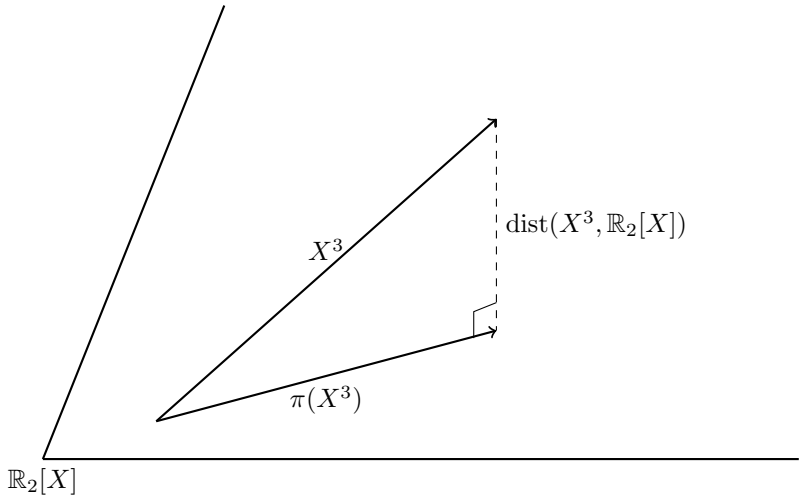
$$\forall n \in \mathbb{N}, \forall z \in B_\alpha, F^{(n)}(z) = (-i)^n \int_I x^n e^{-izx} f(x)\rho(x)\mathrm{d}x.$$

Fixant n, l'évaluation en 0 de cette expression donne

$$F^{(n)}(0) = (-i)^n \int_I x^n f(x)\rho(x)\mathrm{d}x = (-i)^n \langle f, x^n \rangle .$$

Or, ce dernier produit scalaire vaut 0 puisque, par hypothèse, f est dans l'orthogonal des x^n. Mais par unicité du développement en série entière, comme les $F^{(n)}(0)$ sont tous nuls, on a $F = 0$ dans un voisinage de 0. Comme B_α est connexe, il vient par le théorème de prolongement analytique que F est nulle sur tout B_α, donc en particulier sur l'axe réel. L'injectivité de la transformée de Fourier dans L^1 implique alors que $\varphi = 0$ ce qui implique, car $\rho > 0$, que $f = 0$. □

Application. Calcul de minimisation de l'intégrale $\int_{-1}^{1}(x^3 - ax^2 - bx - c)^2\mathrm{d}x$



Démonstration. Pour $\rho = 1$, les polynômes orthogonaux de $L^2(\mathbb{R})$ sont les polynômes de Legendre définis par

$$P_n = \frac{1}{2^n n!}\frac{d^n}{dx^n}\left((x^2-1)^n\right)$$

et par le résultat précédent, c'est une base hilbertienne de $L^2(\mathbb{R})$ (à normalisation près). On peut alors interpréter l'intégrale précédente comme le projeté de $x \mapsto x^3$ sur $\mathbb{R}_2[X]$. La formule de projection donne alors

$$\Pi_{\mathbb{R}_2[X]}(x^3) = < x^3, e_0 > e_0 + < x^3, e_1 > e_1 + < x^3, e_2 > e_2, \quad e_i = \frac{P_i}{\|P_i\|}$$

On conclut alors par le théorème de Pythagore. □

Remarque 4.1. Développement beaucoup proposé à l'oral car beaucoup de recasages possible, il est nécessaire d'être vraiment au point dessus. Le dernier argument cache de gros théorèmes, s'attendre à des questions sur l'injection de Fourier par exemple. Aussi, il faut connaître les familles élémentaires de polynômes tel que Legendre, Laguerre.. qui correspondent chacun à des fonctions de poids bien réfléchis.

4.2 Théorème d'inversion locale

Difficulté : Difficile
Thèmes : Application différentiable, Espaces vectoriels normées, théorème de point fixe.
Prérequis : Théorème de point fixe à paramètres.
Leçons concernées : **214**, **215**.
Références : Laudenbach, Calcul différentiel et intégral

Enoncé 16. *Soient E et F deux espaces de Banach, U un ouvert de E et $a \in U$. Soit $f : U \to F$ une application $\mathcal{C}^1$ telle que $\mathrm{D}f(a)$ soit inversible. Alors il existe un voisinage ouvert U' de a dans U et un voisinage ouvert V' de $f(a)$ dans F tels que la restriction de f à U' soit un $\mathcal{C}^1$-difféomorphisme de U' dans V'.*

Démonstration. Par translation, on se ramène au cas où $a = 0$ et $f(a) = 0$. Par ailleurs, le problème reste inchangé en composant f à gauche par l'isomorphisme linéaire $[\mathrm{D}f(0)]^{-1}$. Noter alors que

$$\mathrm{D}\left([\mathrm{D}f(0)]^{-1} \circ f\right)(0) = [\mathrm{D}f(0)]^{-1} \circ \mathrm{D}f(0) = Id.$$

On se ramène alors à prouver le théorème pour $E = F,\ a = f(a) = 0,\ \mathrm{D}f(0) = Id$.
Posons $\varphi(x) = f(x) - x$ et $T_y(x) = y - \varphi(x) = y - f(x) + x$ pour tout $x \in E$. Afin de montrons qu'on a homéomorphisme, on va commencer par montrer qu'on a au moins une bijection en résolvant $f(x) = y$. Or visiblement, le point x est solution de $f(x) = y$ si et seulement si x est un point fixe de T_y. On va alors montrer qu'un tel x existe par le théorème de point fixe de Picard. □

Lemme 8. *Il existe $r > 0$ tel que la boule ouverte B centrée en 0 de rayon r vérifie*

- *l'adhérence $\bar{B}$ de B dans E est contenue dans U*
- *pour tout $x \in B,\ \|\mathrm{D}\varphi(x)\| \leq \frac{1}{2}$*
- *pour tout $x \in B,\ \mathrm{D}f(x) \in \mathrm{GL}(E)$.*

Preuve du lemme. Point par point, le premier vient du fait que U est un ouvert donc U contient une boule ouverte de rayon ρ, donc $r < \rho$ convient.
Ensuite, comme φ est $\mathcal{C}^1$ et $\mathrm{D}\varphi(0) = 0$, la continuité de l'application $x \mapsto \mathrm{D}\varphi(x)$ en 0 dit qu'il existe $r > 0$ tel que

$$\|x\| < r \Rightarrow \|\mathrm{D}\varphi(x)\| \leq \frac{1}{2}.$$

Enfin, comme $x \mapsto \mathrm{D}f(x)$ est $\mathcal{C}^0$ et comme $\mathrm{D}f(0) \in \mathrm{GL}(E)$, ouvert dans $\mathrm{Endo}(E)$, si r est assez petit, $\mathrm{D}f(x) \in \mathrm{GL}(E)$ pour tout $x \in B$. □

Retour à la démonstration. Reprenons la recherche de point fixe pour T_y. Par l'inégalité des accroissements finis, pour tout $x_1, x_2 \in B$, on a

$$\|\varphi(x_1) - \varphi(x_2)\| \leq \frac{1}{2}\|x_1 - x_2\|.$$

En particulier,

$$\|x\| \leq r \Rightarrow \|\varphi(x)\| \leq \frac{r}{2} \quad \text{et} \quad \|T_y(x)\| \leq \frac{r}{2} + \|y\|.$$

Donc si $\|y\| < \frac{r}{2}$, T_y envoie $\bar{B}$ dans B avec une constante de Lipschitz $\leq \frac{1}{2}$. Comme $\bar{B}$ fermé dans un Banach, $\bar{B}$ est complet pour la métrique induite de E. Par le théorème de point fixe à paramètres, T_y admet un unique point fixe $g(y)$ dans $\bar{B}$ mais en fait, $T_y(\bar{B}) \subset B$, de tel sorte qu'on s'assure que le point fixe de T_y n'est pas sur le bord. De plus, $y \mapsto g(y)$ est continue. En effet, par l'inégalité triangulaire, on a

$$\begin{aligned} d(g(y_1), g(y_2)) &\leq d\left(T_{y_1}(g(y_1)), T_{y_1}(g(y_2))\right) + d\left(T_{y_1}(g(y_2)), T_{y_2}(g(y_2))\right) \\ &\leq \frac{1}{2} d(g(y_1), g(y_2)) + d\left(T_{y_1}(g(y_2)), T_{y_2}(g(y_2))\right) \end{aligned}$$

où le $\frac{1}{2}$ correspond à la constante de Lipschitz de T_y. Ainsi

$$(1-\frac{1}{2})d(g(y_1),g(y_2)) \leq d\left(T_{y_1}(g(y_2)),T_{y_2}(g(y_2))\right).$$

Par la continuité de T_y en $(g(y))$, le majorant de droite peut être rendu arbitrairement petit si y_2 est proche de y_1. Cela traduit la continuité de g en y.
Considérons désormais $V' = \{y \in E,\ \|y\| < \frac{r}{2}\}$, et $U' = B \cap f^{-1}(V')$. Pour $y \in V'$, par ce qui précède, $g(y)$ est l'unique pré-image de y dans B. Donc $f_{|U'}$ est une bijection de U' dans V' et d'inverse g. C'est en fait un homéomorphisme car g est continue. Il reste à montrer que g est différentiable en tout point de V'. Soient $x_1, x_2 \in U'$ et y_1, y_2 leur image dans V'. Ecrivant que f est différentiable en x_1, il vient

$$y_2 - y_1 = \mathrm{D}f(x_1)(x_2 - x_1) + \mathrm{R}(x_2),$$

où x_1 est fixe et x_2 variable. et où le reste x_2 est un $o(\|x_2 - x_1\|)$. Composant cette égalité par $[\mathrm{D}f(x_1)]^{-1}$, il vient

$$x_2 - x_1 = [\mathrm{D}f(x_1)]^{-1}(y_2 - y_1) - [\mathrm{D}f(x_1)]^{-1}\mathrm{R}(x_2). \tag{2}$$

Si on parvient à montrer que $R'(y_2) := [\mathrm{D}f(x_1)]^{-1}\mathrm{R}(x_2)$ est un $o(\|y_2 - y_1\|)$, alors on aura terminé.
Comme l'application linéaire $[\mathrm{D}f(x_1)]^{-1}$ est continue et comme $\mathrm{R}(x_2)$ est un $o(\|x_2 - x_1\|)$, il existe $\delta > 0$ tel que

$$\|x_2 - x_1\| < \delta \Rightarrow \|[\mathrm{D}f(x_1)]^{-1}(\mathrm{R}(x_2))\| \leq \frac{1}{2}\|x_2 - x_1\|.$$

Reportant cela dans (2), il vient :

$$\|x_2 - x_1\| < \delta \Rightarrow \|x_2 - x_1\| \leq \|[\mathrm{D}f(x_1)]^{-1}\|\ \|y_2 - y_1\| + \frac{1}{2}\|x_2 - x_1\|.$$

Prenant $C = 2\|\mathrm{D}f(x_1)^{-1}\|$, il vient

$$\|x_2 - x_1\| \leq C\|y_2 - y_1\|.$$

La continuité de g donne, si $\|y_2 - y_1\|$ assez petit, que $\|x_2 - x_1\| \leq \delta$ et l'inéquation précédente est vérifiée, on peut alors écrire

$$\frac{\|\mathrm{R}(x_2)\|}{\|y_2 - y_1\|} \leq C\frac{\|\mathrm{R}(x_2)\|}{\|x_2 - x_1\|}.$$

Quand y_2 tend vers y_1, $x_2 = g(y_2)$ tend vers x_1 et le majorant de droite tend vers 0, ce qui prouve que $\mathrm{R}(g(y_2))$ est un $o(\|y_2 - y_1\|)$. Reportant cette information dans (2), on obtient

$$x_2 - x_1 = [\mathrm{D}f(x_1)]^{-1}(y_2 - y_1) + o(\|y_2 - y_1\|),$$

ce qui signifie que g est différentiable en y_0 et que sa dérivée est $[\mathrm{D}f(x_1)]^{-1}$. □

4.3 Calcul de l'intégrale de Gauss par une équation différentielle

Difficulté : Moyenne
Thèmes : Théorème de continuité sous l'intégrale, équation différentielle
Leçons concernées : **220 221**, **236**, **239**, **228**
Références : Candelpergher, Calcul intégral

Enoncé 17.

$$\int_{\mathbb{R}} e^{-x^2}\mathrm{d}x = \sqrt{\pi}.$$

Démonstration. Posons pour tout $t>0,\ \varphi(t) = \int_{\mathbb{R}} \frac{e^{-tx^2}}{1+x^2}$. Par le critère de Riemann, cette fonction est clairement bien définie partout. De plus, comme pour tout $t>0,\ x\mapsto \frac{e^{-tx^2}}{1+x^2}$ est mesurable, pour tout $x\in\mathbb{R},\ t\mapsto \frac{e^{-tx^2}}{1+x^2}$ est continue et pour tout $t>0,\ |\frac{e^{-tx^2}}{1+x^2}| \leq \frac{1}{1+x^2}$ intégrable, on a φ qui est continue par le théorème de continuité sous le signe intégrale. Est-elle dérivable ? Par le théorème de dérivabilité sous le signe intégrale, il faut montrer que $|\frac{x^2e^{-tx^2}}{1+x^2}| \leq g(x)$, où g est une fonction intégrable indépendante de t. On peut majorer la quantité précédente par $\frac{x^2}{1+x^2}$ mais cette fonction n'est pas intégrable sur $\mathbb{R}$. Malheureusement, c'est le mieux que l'on puisse faire. Mais il y a un moyen de s'en sortir. En effet, la dérivabilité d'une fonction est une notion locale, il suffit alors de montrer que φ est dérivable sur tout intervalle $]a,b[,\ 0<a<b$. Ainsi,

$$\left|\frac{x^2e^{-tx^2}}{1+x^2}\right| \leq \sup_{t\in]a,b[}\left|\frac{x^2e^{-tx^2}}{1+x^2}\right| \leq e^{-ax^2} = g(x).$$

et g intégrable sur $\mathbb{R}$. On peut alors écrire

$$\forall t>0,\quad \varphi'(t) = \int_{\mathbb{R}} \frac{x^2e^{-tx^2}}{1+x^2}\mathrm{d}x.$$

En réarrangeant, on obtient

$$\begin{aligned}\varphi'(t) &= -\int_{\mathbb{R}} \frac{(1+x^2)e^{-tx^2}}{1+x^2}\mathrm{d}x + \int_{\mathbb{R}} \frac{e^{-tx^2}}{1+x^2}\mathrm{d}x\\ &= -\int_{\mathbb{R}} e^{-tx^2}\mathrm{d}x + \varphi(t)\\ &= -\frac{C}{\sqrt{t}} + \varphi(t).\end{aligned}$$

où C est l'intégrale qu'on cherche à déterminer. La résolution de l'équation différentielle

$$\varphi'(t) - \varphi(t) = -\frac{C}{\sqrt{t}}.$$

avec la condition initiale $\varphi(0) = [arctan(x)]_{-\infty}^{+\infty} = \pi$ donne

$$\begin{aligned}\varphi(t) &= \pi e^t - e^t\int_0^t \frac{C}{\sqrt{u}}e^{-u}\mathrm{d}u\\ &= e^t\left(\pi - 2C\int_0^{\sqrt{t}} e^{-x^2}\mathrm{d}x\right).\end{aligned}$$

Comme $\varphi(t) \leq \int_{\mathbb{R}} e^{-tx^2} = \frac{C}{\sqrt{t}}$, on en déduit $\lim_{t\to+\infty}\varphi(t) = 0$ et donc

$$\lim_{t\to+\infty} 2C\int_0^{\sqrt{t}} e^{-x^2}\mathrm{d}x = \pi.$$

mais également

$$\lim_{t\to+\infty} 2C\int_0^{\sqrt{t}} e^{-x^2}\mathrm{d}x = C^2.$$

D'où, par unicité de la limite, $C^2 = \pi$, ou de façon équivalente,

$$\int_{\mathbb{R}} e^{-x^2}\mathrm{d}x = \sqrt{\pi}.$$

□

Remarque 4.2. La résolution s'effectue assez facilement en résolvant d'abord l'équation homogène puis avec la méthode de la variation de la constante.

4.4 Calcul d'une intégrale par le théorème des résidus

Difficulté : Moyenne
Thèmes : Théorème des résidus, Calcul d'intégral
Leçons concernées : **245**, **236**.
Références : Pas de référence

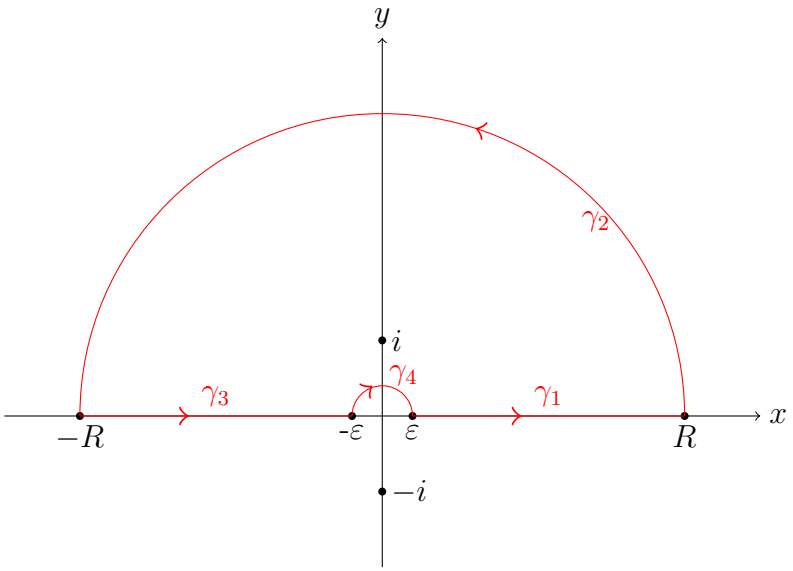
Enoncé 18.

$$\int_0^{+\infty} \frac{\ln^2(t)}{1+t^2}\mathrm{d}t = \frac{\pi^3}{8}.$$

Démonstration. Notons $\Omega = \{z \in \mathbb{C},\ \exists \theta \in]-\frac{3\pi}{2}, \frac{\pi}{2}[, \frac{z}{|z|} = e^{i\theta}\}$ et définissons un logarithme complexe sur Ω

$$\begin{aligned} \log : \Omega &\to \mathbb{C} \\ z &\mapsto \ln|z| + i\theta. \end{aligned}$$

et on notera f la fonction qui à z associe $\frac{\log^2(z)}{1+z^2}$. Cette fonction (méromorphe) a deux pôles dans $\mathbb{C}$, i et $-i$, et un seul dans $\mathbb{C}\backslash\Omega$. Considérons alors $R > 0$, $\varepsilon > 0$ ainsi que le lacet simple suivant



Calculons alors l'intégrale de f le long de chaque composante de γ. Pour γ_2, on a

$$\begin{aligned} \gamma_2 : [0,\pi] &\to \mathbb{C} \\ \theta &\mapsto Re^{i\theta} \end{aligned}$$

Ainsi, si $z = Re^{i\theta}$, $\mathrm{d}z = \theta Re^{i\theta}$, d'où

$$\int_{\gamma_2} f(z)\mathrm{d}z = \int_0^{\pi} \frac{\log^2(Re^{i\theta})}{1+R^2e^{2i\theta}} Re^{i\theta}\mathrm{d}\theta.$$

Passant au module, on obtient alors

$$\begin{aligned} \left|\int_0^{\pi} \frac{\log^2(Re^{i\theta})}{1+R^2e^{2i\theta}} Re^{i\theta}\mathrm{d}\theta\right| &\leq \int_0^{\pi} \frac{|\ln(R)+i\theta|^2}{R^2-1} R\mathrm{d}\theta \\ &= \int_0^{\pi} \frac{\ln^2(R)+\theta^2}{R^2-1} R\mathrm{d}\theta \\ &\leq \pi \sup_{\theta\in[0,\pi]} \frac{\ln^2(R)+\theta^2}{R^2-1} \\ &\underset{R\to+\infty}{\sim} \pi\frac{\log^2(R)}{R^2} R \to 0. \end{aligned}$$

De la même façon on calcule l'intégrale le long de γ_4.

$$\begin{aligned}\gamma_4 :&[0,\pi] \to \mathbb{C}\\ &\theta \mapsto \varepsilon e^{i\theta}\end{aligned}$$

Et ainsi,

$$\begin{aligned}\left|\int_{\gamma_2} f(z)\mathrm{d}z\right| &= \left|\int_0^\pi \frac{\log^2(\varepsilon e^{i\theta})}{1+\varepsilon^2 e^{2i\theta}}\varepsilon e^{i\theta}\mathrm{d}\theta\right|\\ &\leq \int_0^\pi \frac{\log^2(\varepsilon)+\theta^2}{1-\varepsilon^2}\varepsilon\mathrm{d}\theta\\ &\leq \pi\frac{\log^2(\varepsilon)+\theta^2}{1-\varepsilon^2}\varepsilon\\ &\underset{\varepsilon\to 0}{\sim} \pi\log^2(\varepsilon)\varepsilon \to 0.\end{aligned}$$

On a fait la moitié. L'intégrale selon γ_1 donnera l'intégrale que l'on souhaite calculer lorsque ε tend vers 0 et R vers l'infini. Enfin, pour γ_3,

$$\begin{aligned}\int_{\gamma_3} f(z)\mathrm{d}z = \int_{-R}^{-\varepsilon}\frac{\log^2(z)}{1+z^2}\mathrm{d}z &= \int_\varepsilon^{\mathbb{R}}\frac{(\ln(z)-i\pi)^2}{1+z^2}\mathrm{d}z\\ &= \int_\varepsilon^{\mathbb{R}}\frac{\ln^2(z)-2\ln(z)i\pi-\pi^2}{1+z^2}\mathrm{d}z\\ &= \int_\varepsilon^{\mathbb{R}}\frac{\ln^2(z)}{1+z^2}\mathrm{d}z - \int_\varepsilon^{\mathbb{R}}\frac{2\ln(z)i\pi}{1+z^2}\mathrm{d}z - \int_\varepsilon^{\mathbb{R}}\frac{\pi^2}{1+z^2}\mathrm{d}z.\end{aligned}$$

Remarquons deux choses : l'intégrale

$$\int_\varepsilon^{\mathbb{R}}\frac{\pi^2}{1+z^2}\mathrm{d}z$$

est convergente par le critère de Riemann, et sa limite quand $\varepsilon \to 0$ et $R \to \infty$ vaut

$$\int_\varepsilon^{\mathbb{R}}\frac{\pi^2}{1+z^2}\mathrm{d}z \to \pi^2\int_0^{+\infty}\frac{1}{1+z^2}\mathrm{d}z = \frac{\pi^3}{2}.$$

Aussi, l'intégrale

$$\int_\varepsilon^R \frac{2\ln(z)i\pi}{1+z^2}\mathrm{d}z.$$

est à valeur imaginaire pure.
Gardant tous ces résultats en tête, appliquons le théorème des résidus à la fonction f sur l'ouvert étoilé Ω. Comme f est holomorphe sur $\gamma = \cup\gamma_i$, on a

$$\int_\gamma f(z)\mathrm{d}z = 2\mathrm{i}\pi\ \mathrm{Res}(f,\mathrm{i})\ \mathrm{Ind}_\gamma(\mathrm{i}).$$

avec

$$\mathrm{Res}(f,i) = \lim_{z\to i}(z-i)f(z) = \frac{\log^2(i)}{2i} = i\frac{\pi^2}{8}.$$

Donc

$$\int_\gamma f(z)\mathrm{d}z = 2i\pi(i\frac{\pi^2}{8}) = -\frac{\pi^3}{4}.$$

De plus, on a

$$\int_\gamma f(z)\mathrm{d}z = \int_{\gamma_1} f(z)\mathrm{d}z + \int_{\gamma_2} f(z)\mathrm{d}z + \int_{\gamma_3} f(z)\mathrm{d}z + \int_{\gamma_4} f(z)\mathrm{d}z;$$

Passant à la limite sur ε et R, il vient

$$-\frac{\pi^3}{4} = \int_0^{+\infty}\frac{\ln^2(t)}{1+t^2}\mathrm{d}t + 0 - \frac{\pi^3}{2} + \int_0^{+\infty}\frac{\ln^2(t)}{1+t^2}\mathrm{d}t - \int_0^{+\infty}\frac{2\ln(z)i\pi}{1+z^2}\mathrm{d}z.$$

Notant I l'intégrale que l'on souhaite calculer, il vient

$$2I - \int_{\varepsilon}^{\mathbb{R}} \frac{2\ln(z)i\pi}{1+z^2}\mathrm{d}z = \frac{\pi^3}{4}.$$

Or, l'intégrale restante est imaginaire pure comme énoncé précedemment. Par suite, en passant à la partie réelle, on trouve alors $I = \frac{\pi^3}{8}$, ce qui conclut. □

Remarque 4.3. De la conclusion on déduit accessoirement que

$$\int_0^{+\infty} \frac{\ln(t)}{1+t^2}\mathrm{d}t = 0.$$

4.5 Théorème de Fischer-Riesz

Difficulté : Dure
Thèmes : Interversion limite intégrale, espaces L^p, notion de convergence, espaces complets
Leçons concernées : **201**, **205**, **241**, **234**.
Références : Brezis, Analyse fonctionnelle

Enoncé 19. *L'espace* L^p *est de Banach pour tout* $1 \leq p \leq +\infty$

Remarque 4.4. Pour démontrer qu'un espace est de Banach, on procède toujours de la même façon : on considère une suite de Cauchy, on montre que la limite existe, que la limite est dans l'evn, et que la différence entre la suite et sa limite tend vers 0 au sens de la norme.

Démonstration. On commence par s'intéresser au cas $p = +\infty$. Soit (f_n) une suite de Cauchy dans L^∞. Comme la suite de Cauchy, pour tout $k > 1$, il existe un entier N_k tel que

$$\|f_m - f_n\|_\infty \leq \frac{1}{k}, \qquad \text{pour} \quad m,\ n \geq N_k.$$

Donc en dehors d'un ensemble négligeable E_k (quitte à choisir un représentant de f_m et f_n qui nous arrange), on a

$$|f_m(x) - f_n(x)| \leq \frac{1}{k}, \quad \forall x \in \Omega \backslash E_k, \quad \forall m,\ n \geq N_k.$$

Enfin, $E = \bigcup E_k$ est de mesure nulle par sigma-additivité et il suit alors que la suite $f_n(x)$ est de Cauchy dans $\mathbb{R}$ donc convergente par complétude de $\mathbb{R}$. Notons $f(x)$ sa limite pour $x \in \Omega \backslash E$. Passant à la limite sur m dans l'inégalité précédente, on obtient

$$|f(x) - f_n(x)| \leq \frac{1}{k}, \quad \forall x \in \Omega \backslash E, \quad \forall n \geq N_k.$$

Donc pour presque tout x, $f(x) \in [\frac{1}{k} - f_n(x), \frac{1}{k} + f_n(x)]$, donc $f \in \mathrm{L}^\infty$ puisque (f_n) l'est et

$$\|f - f_n\|_\infty \leq \frac{1}{k}, \qquad \forall n \geq N_k.$$

Par conséquent, $\|f - f_n\|_\infty \to 0$.
Supposons désormais $1 \leq p < +\infty$. De la même façon, considérons une suite de Cauchy (f_n) dans L^p. Comme les suites de Cauchy ont une unique valeur d'adhérence, il va suffir de montrer qu'une sous suite extraite converge dans L^p. Notons (f_{n_k}) la sous suite de (f_n) vérifiant

$$\|f_{n_{k+1}} - f_{n_k}\|_p \leq \frac{1}{2^k}, \qquad \forall k \geq 1.$$

Une telle sous suite existe. En effet, on procède comme suit : comme (f_n) est de Cauchy, il existe n_1 tel que $\|f_m - f_n\|_p \frac{1}{2}, \quad \forall m, n \geq n_1$, on choisit ensuite $n_2 \geq n_1$ tel que $\|f_m - f_n\|_p \frac{1}{2}, \quad \forall m, n \geq n_2$ et ainsi de suite. Montrons que cette sous suite converge dans L^p. Par soucis de notation, on remplacera désormais la sous suite (f_{n_k}) par uniquement (f_k). Posons alors

$$g_n(x) = \sum_{k=1}^{n} |f_{k+1}(x) - f_k(x)|.$$

Remarquons que cette expression n'est pas définie partout mais presque partout, et que les endroits où elle est définie dépendent de n. En revanche, là où l'expression est bien définie, il est clair que c'est une suite de fonctions croissante et de plus,

$$\|g_n\|_p = \|\sum_{k=1}^{n} |f_{k+1} - f_k|\|_p \leq \sum_{k=1}^{n} \|f_{k+1} - f_k\|_p \leq \sum_{k=1}^{n} \frac{1}{2^k} \leq 1.$$

Donc d'après le théorème de convergence monotone, pour presque tout x, la suite $(g_n(x))$ converge vers une limite finie que l'on note $g(x)$ et $g \in \mathrm{L}^p$. De plus, on a pour $m \geq n \geq 2$ et presque tout x

$$|f_m(x) - f_n(x)| \leq |f_m(x) - f_{m-1}(x)| + \cdots + |f_{n+1}(x) - f_n(x)| \leq g(x) - g_{n-1}(x).$$

Donc pour presque tout x, la suite $(f_k(x))$ est de Cauchy (dans $\mathbb{R}$) et converge donc vers une limite $f(x)$. De plus, pour $n \geq 2$ et pour presque tout x

$$|f(x) - f_n(x)| \leq g(x).$$

Donc f est L^p. Il reste à montrer que $\|f - f_n\|_p \to 0$. On a pour presque tout x, $|f_n(x) - f(x)|^p \to 0$ et $|f_n(x) - f(x)|^p \leq g^p(x)$ majorante intégrable donc par le théorème de convergence dominée,

$$0 = \int_\Omega \lim_{n\to+\infty} |f_n(x) - f(x)|^p \mathrm{d}x = \lim_{n\to+\infty} \int_\Omega |f_n(x) - f(x)|^p \mathrm{d}x = \lim_{n\to+\infty} \|f - f_n\|_p.$$

ce qui conclut le théorème. □

Remarque 4.5. La grosse difficulté de ce théorème est de comprendre et de savoir expliquer comment passer d'un élément de L^p à un élément de $\mathbb{R}$, chose qui est rarement bien expliqué dans les livres. Je conseille vivement d'aller poser des questions aux professeurs pour éclaircir les subtilités.

4.6 Théorème de projection sur un convexe fermé et une application dans $L^2(\mathbb{R})$

Difficulté : Moyenne
Thèmes : Suite de Cauchy, espace de Hilbert, convexité
Leçons concernées : **205**, **213**, **208**, **219**, **253**
Références : Brezis, Analyse fonctionnelle

Enoncé 20. *Soit $K \subset H$ un convexe fermé non vide d'un Hilbert réel H. Alors pour tout $f \in H$, il existe un unique $u \in K$ tel que*

$$|f-u| = \min_{v\in K} |f-v|. \tag{3}$$

De plus, u est caractérisé par la propriété :

$$\begin{cases} u \in K \\ \langle f-u, v-u\rangle \leq 0, \ \forall v \in K. \end{cases} \tag{4}$$

On note alors $u = P_K f$ le projeté de f sur K

Démonstration. Commençons par considérer une suite (v_n) de K vérifiant

$$d_n = |f-v_n| \xrightarrow{n\to+\infty} d = \inf_{v\in K} |f-v|.$$

Montrons que (v_n) est de Cauchy. En appliquant l'identité du parallélogramme avec $a = f-v_n$ et $b = f-v_m$, il vient

$$\left|f - \frac{v_n+v_m}{2}\right|^2 + \left|\frac{v_n-v_m}{2}\right|^2 = \frac{1}{2}(d_n^2+d_m^2).$$

Or, $\frac{v_n+v_m}{2}$ est un barycentre, donc contenu dans le convexe K et donc, $\left|f-\frac{v_n+v_m}{2}\right| \geq d$, par minimalité de d. Par conséquent,

$$\left|\frac{v_n-v_m}{2}\right|^2 \leq \frac{1}{2}(d_n^2+d_m^2) - d^2 \quad \text{et} \quad \lim_{m,n\to+\infty} = 0.$$

(v_n) est donc de Cauchy, et puisque K est fermé dans H, (v_n) converge. Donc, nécessairement, $v_n \to u \in K$ et l'on a $d = |f-u|$. Montrons alors la caractérisation. Supposons que l'on ait (3). Soit $w \in K$. On a

$$v = (1-t)u + tw \in K, \qquad \text{pour } t \in]0,1].$$

et donc

$$|f-u| \leq |f-[(1-t)u+tw]| = |(f-u)-t(w-u)|.$$

En passant au carré, il vient

$$|f-u|^2 \leq |f-u|^2 - 2t\langle f-u, w-u\rangle + t^2|w-u|^2.$$

i.e. $2\langle f-u, w-u\rangle \leq t|w-u|^2$. Quand $t \to 0$, on obtient alors ce qu'on souhaitait.
Inversement, si on suppose u vérifiant 4, on a

$$|u-f|^2 - |v-f|^2 = 2\langle f-u, v-u\rangle - |u-v|^2 \leq 0, \qquad \forall v \in K.$$

d'où 3. □

Remarque 4.6. L'hypothèse sur H réel n'est pas réellement nécessaire. En effet, si on le suppose complexe, il y a juste des conjuguées qui sortent.

Application. Soit $K = \{f \in \mathrm{L}^2(\mathbb{R}),\ f \geq 0 \text{ p.p}\}$. K est un convexe fermé de L^2 et le projeté de $f \in \mathrm{L}^2(\mathbb{R})$ sur K est f_+, sa partie positive.

Démonstration. Montrons déjà que K est un convexe fermé (il est évidemment non vide). Pour convexe, c'est évident puisque qu'une combinaison convexe de deux éléments positifs presque partout reste positive presque partout. Pour fermé, on aura besoin d'un corollaire du théorème de Riesz-Fischer: soit (f_n) une suite de Cauchy de $\mathrm{L}^2(\mathbb{R})$ qui converge au sens L^2 vers une fonction f, il existe une extractrice $n \mapsto \varphi(n)$ tel que $(f_{\varphi(n)})$ converge vers f presque partout. Donc si (f_n) est une suite de Cauchy de K convergeant vers f en norme L^2, pour presque tout $x \in \mathbb{R}$, $f_{\varphi(n)}(x) \to f(x) \geq 0$. Donc K est fermé par la caractérisation séquentielle des fermés.
Enfin, calculons le projeté de $f \in \mathrm{L}^2(\mathbb{R})$. Comme on sait qu'on doit atterir dans K, on se doute que le projeté de f va être f_+, la partie positive de f, et on a toujours $f = f_+ - f_-$, et $f_+ \cdot f_- = 0$ car les deux fonctions sont à support disjoints. Rappelons que les fonctions f_+ et f_- sont respectivements définies par $\max(f, 0)$ et $\max(-f, 0)$. Formellement, si $g \in K$, on a, par la caractérisation du théorème

$$\langle f - f_+, g - f_+ \rangle = \langle -f_-, g - f_+ \rangle = -\langle f_-, f_+ \rangle - \langle f_-, g \rangle = -\langle f_-, g \rangle .$$

Or g et f_- sont positives presque partout, donc $-\langle f_-, g \rangle \leq 0$ pour tout $g \in \mathrm{L}^2(\mathbb{R})$. La caractérisation du théorème nous dit alors que le projeté de f est nécessairement f_+. □

4.7 Méthode de gradient à pas optimal

Difficulté : Moyenne et long
Thèmes : Théorème de point fixe, théorème spectral, calcul différentiel
Leçons concernées : **219**, **226**, **162**, **229**
Références : Bernis, Analyse pour l'agrégation de mathématiques

Enoncé 21. *Soit $A \in \mathcal{M}_n(\mathbb{R})$ une matrice symétrique définie positive, b un élément non nul de $\mathbb{R}^n$. On note Φ la fonctionnelle quadratique:*

$$\forall x \in \mathbb{R}^n, \quad \Phi(x) = \frac{1}{2}\|x\|_A - {}^t xb.$$

Alors l'application Φ atteint son minimum en $\bar{x}$, l'unique solution du système $Ax = b$, et seulement en ce point. De plus, si $a \in \mathbb{R}^n$, $a \neq \bar{x}$, la suite $(x_k)_{k\in\mathbb{N}}$ définie par

$$\begin{cases} x_0 = a \\ \alpha_k = \frac{\|\nabla\Phi(x_k)\|^2}{\|\nabla\Phi(x_k)\|_A^2}, & si\ x_k \neq x_0 \\ \alpha_k = 0, & sinon \\ x_k + 1 = x_k - \alpha_k \nabla\Phi(x_k). \end{cases}$$

converge vers $\bar{x}$. De plus, pour tout entier k,

$$\|x_{k+1} - \bar{x}\| \leq \sqrt{\frac{\lambda_{max}}{\lambda_{min}}} \left(\frac{\lambda_{max} - \lambda_{min}}{\lambda_{max} + \lambda_{min}}\right)^{k+1} \|x_0 - \bar{x}\|.$$

où λ_{max} et λ_{min} sont respectivement la plus grande et la plus petite valeur propre de A

Lemme 9 (Lemme de Kantorovich)**.** *Pour tout élément x non nul de $\mathbb{R}^n$, on a*

$$\frac{\|x\|^4}{\|x\|_{A^{-1}}^2 \|x\|_A^2} \geq 4\frac{\lambda_{max}\lambda_{min}}{(\lambda_{max} + \lambda_{min})^2}.$$

Démonstration. Soit x un élément non nul de $\mathbb{R}^n$. D'après le théorème spectral, la matrice A admet une base orthornormée $(e_1, \ldots, e_n)$ de vecteurs propres. On note λ_i la valeur propre associée au vecteur propre e_i. Remarquons que e_i est aussi un vecteur propre associé de A^{-1} associé à la valeur propre $\frac{1}{\lambda_i}$. Ainsi, en désignant par x_i la i-ème coordonnée de x dans la base $(e_1, \ldots, e_n)$, on a :

$$\begin{aligned} \|x\|_A \|x\|_{A^{-1}} &= \sqrt{\sum_{i=1}^n \lambda_i x_i^2} \sqrt{\sum_{i=1}^n \frac{1}{\lambda_i} x_i^2} \\ &= \sqrt{\frac{\lambda_{\max}}{\lambda_{\min}}} \sqrt{\sum_{i=1}^n \frac{\lambda_i}{\lambda_{\max}} x_i^2} \sqrt{\sum_{i=1}^n \frac{\lambda_{\min}}{\lambda_i} x_i^2} \end{aligned}$$

D'après l'inégalité $ab \leq \frac{1}{2}(a^2 + b^2)$, on a alors

$$\|x\|_A \|x\|_{A^{-1}} \leq \frac{1}{2}\sqrt{\frac{\lambda_{\max}}{\lambda_{\min}}} \sum_{i=1}^n \left(\frac{\lambda_i}{\lambda_{\max}} + \frac{\lambda_{\min}}{\lambda_i}\right) x_i^2.$$

Mais l'application définie par

$$\forall t \in [\lambda_{\min}, \lambda_{\max}], \quad g(t) = \frac{t}{\lambda_{\max}} + \frac{\lambda_{\min}}{t}.$$

est convexe. donc puisque $g(\lambda_{\min}) = g(\lambda_{\max}) = 1 + \frac{\lambda_{\min}}{\lambda_{\max}}$, on a pour tout $t \in [\lambda_{\min}, \lambda_{\max}]$, $g(t) \leq 1 + \frac{\lambda_{\min}}{\lambda_{\max}}$. En reprenant l'inégalité précédente, il vient alors

$$\|x\|_A \|x\|_{A^{-1}} \leq \frac{1}{2}\sqrt{\frac{\lambda_{\max}}{\lambda_{\min}}} \left(1 + \frac{\lambda_{\min}}{\lambda_{\max}}\right) \|x\|^2.$$

En élevant au carré, on trouve

$$\|x\|_A^2\|x\|_{A^{-1}}^2 \leq \frac{1}{4}\frac{\lambda_{\max}}{\lambda_{\min}}\left(1+\frac{\lambda_{\min}}{\lambda_{\max}}\right)^2\|x\|^4$$

ou encore, puisque x est non nul

$$\frac{\|x\|^4}{\|x\|_{A^{-1}}^2\|x\|_A^2} \geq 4\frac{\lambda_{\min}}{\lambda_{\max}}\frac{\lambda_{\max}^2}{(\lambda_{\max}+\lambda_{\min})^2}.$$

□

Démonstration. Passons à la preuve de l'énoncé. Montrons que Φ est différentiable. Soit $h \in \mathbb{R}^n$

$$\begin{aligned}\Phi(x+h) &= \frac{1}{2}\|x+h\|_A^2 - \langle b, x+h\rangle \\ &= \frac{1}{2}\|x\|_A^2 + \langle x, h\rangle + \frac{1}{2}\|h\|_A^2 - \langle b, x\rangle - \langle b, h\rangle \\ &= \Phi(x) + \langle Ax-b, h\rangle + \frac{1}{2}\|h\|_A^2 \\ &= \Phi(x) + \langle Ax-b, h\rangle + o_{\|h\|\to 0}(\|h\|).\end{aligned}$$

puisque en dimension finie toutes les normes sont équivalentes. Donc $\nabla\Phi(x) = Ax - b = A(x-\bar{x})$. Ainsi, puisque un extremum annule nécessairement le gradient de Φ et $\nabla\Phi(\bar{x}) = 0$, on peut conclure que Φ atteint son minimum en ce point puisque pour tout $h \in \mathbb{R}^n$, $\Phi(\bar{x}+h) = \Phi(\bar{x}) + \frac{1}{2}\|h\|_A^2$.
Il reste à montrer la convergence de la suite. Commençons par montrer que α_k est la direction de plus forte descente vers $\bar{x}$. Posons

$$\forall t \in \mathbb{R}, \quad f(t) = \Phi(x_k - t\nabla\Phi(x_k)).$$

En développant, on trouve $f(t) = \Phi(x_k) - t\|\nabla\Phi(x_k)\|^2 + \frac{t^2}{2}\|\nabla\Phi(x_k)\|_A^2$. L'étude de ce polynôme du second degré donne que f atteint son minimum en α_k et donc que c'est la direction de plus faible montée. Notons par ailleurs que cela implique que la dérivée de f s'annule en α_k, ce qui signifie que

$$\begin{aligned}f'(\alpha_k) &= -\|\nabla\Phi(x_k)\|^2 + \alpha_k\|\nabla\Phi(x_k)\|_A^2 \\ &= -\langle\nabla\Phi(x_k), \nabla\Phi(x_k)\rangle + \alpha_k\langle\nabla\Phi(x_k), A\nabla\Phi(x_k)\rangle \\ &= -\langle\nabla\Phi(x_k) - \alpha_k A\nabla\Phi(x_k), \nabla\Phi(x_k)\rangle \\ &= -\langle A(x_k - \alpha_k\nabla\Phi(x_k)) - b, \nabla\Phi(x_k)\rangle \\ &= -\langle\nabla\Phi(x_k - \alpha_k\Phi(x_k)), \nabla\Phi(x_k)\rangle \\ &= -\langle\nabla\Phi(x_{k+1}), \nabla\Phi(x_k)\rangle = 0\end{aligned}$$

Donc deux itérés consécutifs de la suite ont des gradients orthogonaux. Pour alléger les notations, on notera désormais $g_k = \nabla\Phi(x_k)$. Soit $p \in \mathbb{N}$. Evaluons l'erreur entre x_{p+1} et $\bar{x}$:

$$\|x_{p+1} - \bar{x}\|_A^2 = \langle A(x_{p+1}-\bar{x}), x_{p+1} - x_p\rangle + \langle A(x_{p+1}-\bar{x}), x_p - \bar{x}\rangle.$$

D'après ce qui précède,

$$\langle A(x_{p+1}-\bar{x}), x_{p+1} - x_p\rangle = -\alpha_p\langle g_{p+1}, g_p\rangle = 0.$$

Par symétrie de A, il vient alors

$$\begin{aligned}\|x_{p+1} - \bar{x}\|_A^2 &= \langle A(x_{p+1}-x_p), x_p - \bar{x}\rangle + \langle A(x_p - \bar{x}), x_p - \bar{x}\rangle \\ &= \langle x_{p+1} - x_p, A(x_p - \bar{x})\rangle + \|x_p - \bar{x}\|_A^2 \\ &= -\alpha_p\langle g_p, g_p\rangle + \|x_p - \bar{x}\|_A^2 \\ &= -\frac{\|g_p\|^4}{\|g_p\|_A^2} + \|x_p - \bar{x}\|_A^2.\end{aligned}$$

Par ailleurs, on a aussi

$$\|x_p - \bar{x}\|_A^2 = \langle A(x_p - \bar{x}), x_p - \bar{x}\rangle = \left\langle A(x_p - \bar{x}), A^{-1}A(x_p - \bar{x})\right\rangle = \|g_p\|_{A^{-1}}^2.$$

et donc

$$\|x_{p+1} - \bar{x}\|_A^2 = \left(1 - \frac{\|g_p\|^4}{\|g_p\|_A^2 \|g_p\|_{A^{-1}}^2}\right) \|x_p - \bar{x}\|_A^2.$$

D'après le lemme de Kantorovich, on a

$$\left(1 - \frac{\|g_p\|^4}{\|g_p\|_A^2 \|g_p\|_{A^{-1}}^2}\right) \leq 1 - 4\frac{\lambda_{\max}\lambda_{\min}}{(\lambda_{\max} + \lambda_{\min})^2} = \left(\frac{(\lambda_{\max} - \lambda_{\min})^2}{(\lambda_{\max} + \lambda_{\min})^2}\right).$$

Ce qui conclut enfin la démonstration car

$$\|x_{p+1} - \bar{x}\|_A \leq \left(\frac{\lambda_{\max} - \lambda_{\min}}{\lambda_{\max} + \lambda_{\min}}\right) \|x_p - \bar{x}\|_A$$

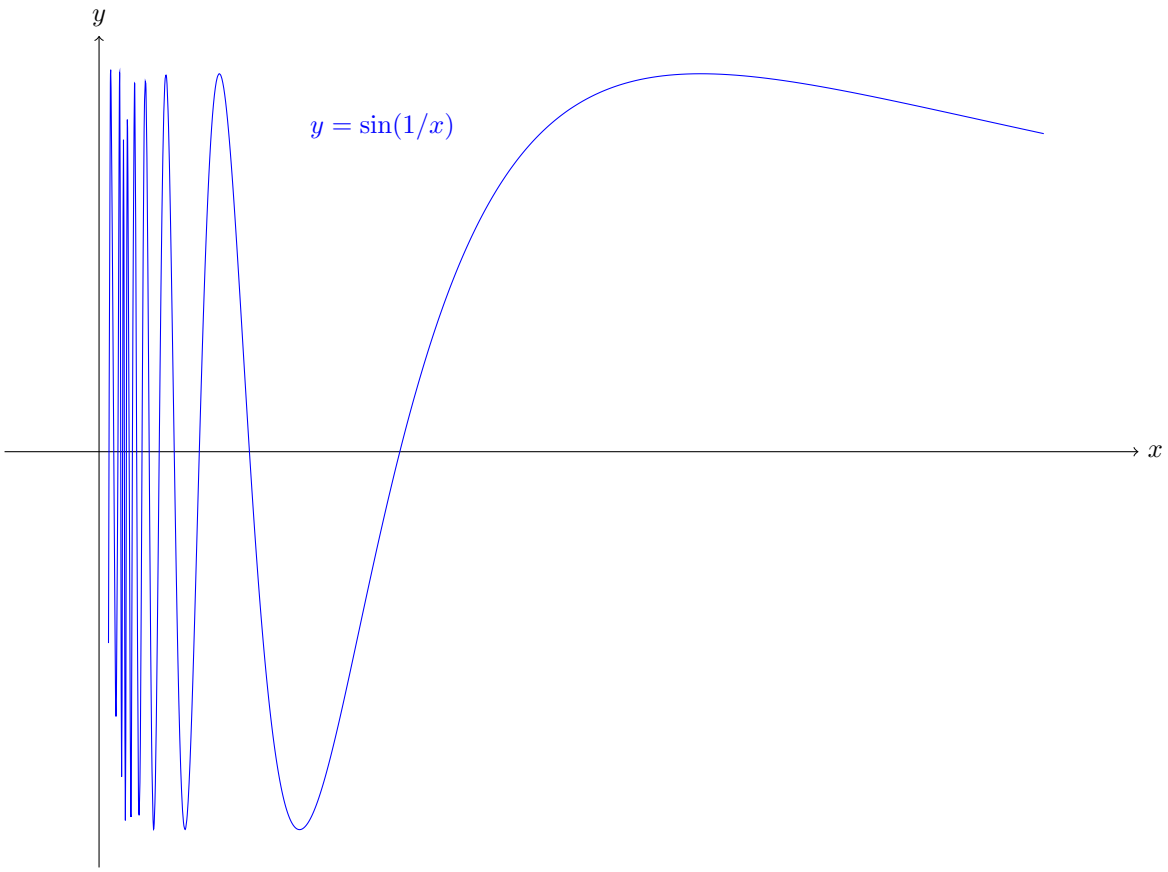
□

Remarque 4.7. Cette preuve est assez longue et il faut l'avoir travaillé assez régulièrement pour pouvoir tout rentrer en 15 minutes. Certains points peuvent être sauté malgré tout.

4.8 Exemple d'un connexe, non connexe par arcs

Difficulté : Facile
Leçons concernées : **204**
Références : Queffelec, Topologie

Enoncé 22. *Soit $A = \{(x, \sin\left(\frac{1}{x}\right),\ x \in \mathbb{R}_+^*\}$ et soit X son adhérence. Alors X est un connexe non connexe par arcs.*



$(x, \sin(1/x))$ sur $]0, 1]$

Démonstration. Commençons par montrer que X est connexe. A est clairement connexe comme image d'un connexe par la fonction continue $f : x \mapsto \left(x, \sin\left(\frac{1}{x}\right)\right)$. De plus, l'adhérence d'un connexe étant connexe, X est connexe. Montrons maintenant que

$$X = \{0\} \times [-1, 1] \cup A.$$

Commeçons par l'inclusion de droite à gauche. Il suffit alors de montrer que tout élément de la forme $(0, y)$, avec $y \in [-1, 1]$ est dans X. Soit c tel que $\sin(c) = y$ et soit $z_n = \left(t_n, \sin\left(\frac{1}{t_n}\right)\right)$, avec $t_n = \frac{1}{c+2\pi n}$. Alors $z_n \in A$ et puisque $\sin\left(\frac{1}{t_n}\right) = y$, la suite (z_n) converge $(0, y)$, d'où $(0, y) \in X$. Réciproquement, soit $z = (x, y) \in X$, alors il existe une suite $(z_n) = (x_n, y_n)$ de A qui converge vers z. Distinguons deux cas

- ou bien $x = 0$ et dans ce cas, puisque $y_n = \sin\left(\frac{1}{x_n}\right) \in [-1, 1]$, on a aussi $y \in [-1, 1]$ et donc $z = (x, y) \in \{0\} \times [-1, 1]$

- ou bien $x > 0$, dans ce cas, soit $\delta = \frac{x}{2}$. A partir d'un certain rang N, on a $z_n \in \bar{B}_{(z,\delta)} \cap A$, pour tout $n > N$. Et la fonction f qui à t associe $\sin\left(\frac{1}{t}\right)$ est continue sur le segment compact $[x - \delta, x + \delta]$. Donc en particulier,

l'image de ce compact est compact et donc fermé. Ainsi

$$y = \lim_{n\to+\infty} y_n = \lim_{n\to+\infty} \sin\left(\frac{1}{x_n}\right) = \lim_{n\to+\infty} f(x_n) = f(x) \in f\left([x-\delta, x+\delta]\right).$$

De cela, on déduit que $(x, y) \in A$.

On va maintenant démontrer que X n'est pas connexe par arcs. Supposons par l'absurde qu'il existe un chemin continu γ de $[0,1]$ dans X tel que $\gamma(0) = (0,0)$ et $\gamma(1) = (1, \sin(1))$. On note alors $\gamma(t) = (u(t), v(t))$ de tel sorte que, si $u(t) \neq 0, v(t) = \sin\left(\frac{1}{u(t)}\right)$. Enfin, on note $t_0 = \sup\{t \geq 0,\ u(t) = 0\}$ le dernier instant où le chemin est sur l'axe des abcisses. Puisque u est continue sur $[0,1]$, en particulier, u est continue en t_0. Donc si (t_n) est une suite de $[0,1]$ qui converge vers t_0 par le bas, il vient nécessairement

$$t_n \to t_0 \Rightarrow u(t_n) \to u(t_0)$$

Or la suite $(u(t_n))$ est constante égal à 0 donc $u(t_0) = 0$.
Soit $a = v(t_0)$. Puisque v est continue, il existe $\varepsilon > 0$ tel que pour tout $t \in [t_0, t_0+\varepsilon], |v(t) - a| < \frac{1}{2}$.
Considérons alors un entier positif n assez grand tel que

$$u(t_0) = 0 < \frac{1}{2\pi n - \frac{\pi}{2}} \leq u(t_0 + \varepsilon).$$

Par application du théorème des valeurs intermédiaires, l'image par u du segment $[t_0, t_0+\varepsilon]$ est un intervalle, et l'inégalité précédente donne alors l'existence d'un temps t_1 et t_2 dans l'intervalle $[t_0, t_0+\varepsilon]$ tel que

$$u(t_1) = \frac{1}{2\pi n - \frac{\pi}{2}}$$
$$u(t_2) = \frac{1}{2\pi n + \frac{\pi}{2}}.$$

On remarque alors que $v(t_1) = -1$ et $v(t_2) = 1$. Soit alors $b \in [-1, 1]$ tel que $|b - a| > \frac{1}{2}$. Par le théorème des valeurs intermédiaires appliqué à v entre t_1 et t_2, il existe un temps $t \in [t_1, t_2] \subset [t_0, t_0+\varepsilon]$ tel que $v(t) = b$ et donc $|v(t) - a| > \frac{1}{2}$. Contradiction! □

Remarque 4.8. Très mauvais recasage....

4.9 Théorème de Weierstrass par les polynômes de Bernstein

Difficulté : Facile
Thèmes : Compacité, Probabilité, densité, fonctions continues sur un compact, convergence uniforme.
Leçons concernées : **209**, **201**, **203**
Références : Gourdon, Analyse

Enoncé 23. *Toute fonction continue $f : [a,b] \subset \mathbb{R} \to \mathbb{C}$ est limite uniforme sur $[a,b]$ d'une suite de fonctions de polynômes.*

Démonstration. Commençons par montrer le résultat sur le compact $[0,1]$. Notons $I = [0,1]$ et C l'ensemble des fonctions continues de I dans $\mathbb{C}$. On note, pour toute fonction $f \in C$ et $n \in \mathbb{N}^*$

$$B_n(f) : I \to \mathbb{C}, \quad x \mapsto \sum_{k=0}^{n} f\left(\frac{k}{n}\right) b_n^k(x), \qquad \text{avec} \qquad b_n^k(x) = \binom{k}{n} x^k (1-x)^{n-k}.$$

Soit alors $f \in C$. On va montrer que la suite de polynômes $B_n(f)$ converge uniformément vers f sur $[0,1]$. On doit alors montrer que

$$\lim_{n \to +\infty} \sup_{x \in I} |B_n(f)(x) - f(x)| = 0.$$

Remarquons pour commencer que $B_n(1)$ est l'application constante égal à 1 pour tout x dans I et pour tout n. Cela permet alors d'écrire

$$|B_n(f)(x) - f(x)| = |B_n(f)(x) - B_n(1)(x) f(x)| \leq \sum_{k=0}^{n} \left| f\left(\frac{k}{n}\right) - f(x) \right| b_n^k(x).$$

Traitons cette somme. Tout d'abord, quelques constatations sur f. f est continue sur un compact donc elle est bornée et atteint ses bornes (par le théorème éponyme). Il existe donc $M > 0$ tel que $|f(x)| \leq M, \forall x \in I$. Aussi, f est continue sur un compact donc d'après le théorème de Heine, elle est uniformément continue. Fixons donc un $\varepsilon > 0$, on a alors

$$\exists \eta > 0, \forall (x,y) \in I^2, \ |x-y| < \eta \Rightarrow |f(x) - f(y)| < \varepsilon.$$

Par ce qui précède, scindant la somme comme il se doit, on obtient

$$\begin{aligned} \sum_{k=0}^{n} \left| f\left(\frac{k}{n}\right) - f(x) \right| b_n^k(x) &\leq \sum_{k, \ |\frac{k}{n} - x| \geq \eta} \left| f\left(\frac{k}{n}\right) - f(x) \right| b_n^k(x) + \sum_{k, \ |\frac{k}{n} - x| < \eta} \left| f\left(\frac{k}{n}\right) - f(x) \right| b_n^k(x) \\ &\leq \qquad \varepsilon \left(\sum_{k, \ |\frac{k}{n} - x| < \eta} b_n^k(x) \right) \quad + \quad 2M \left(\sum_{k, \ |\frac{k}{n} - x| \geq \eta} b_n^k(x) \right). \end{aligned}$$

La somme à gauche vérifie

$$\varepsilon \left(\sum_{k, \ |\frac{k}{n} - x| < \eta} b_n^k(x) \right) \leq \varepsilon \left(\sum_{k=0}^{n} b_n^k(x) \right) \leq \varepsilon.$$

Et la somme de droite quant à elle

$$\sum_{k, \ |\frac{k}{n} - x| \geq \eta} b_n^k(x) \leq \frac{1}{\eta^2} \sum_{k=0}^{n} \left(\frac{k}{n} - x \right)^2 b_n^k(x). \tag{5}$$

puisque $|\frac{k}{n} - x| \geq \eta$ implique $\frac{1}{\eta^2} \left(\frac{k}{n} - x \right)^2 \geq 1$. Constatons alors qu'en sortant le $\frac{1}{n}$, cette somme devient alors

$$\sum_{k=0}^{n} \left(\frac{k}{n} - x \right)^2 b_n^k(x) = \frac{1}{n^2} \sum_{k=0}^{n} (k - nx)^2 b_n^k(x).$$

ce qui a tout à l'air d'une variance de loi binomiale. Formellement, si $X \sim \mathcal{B}(x,n)$. Alors,

$$nx(1-x) = \mathbb{V}[X] = \mathbb{E}\left[|X - \mathbb{E}[X]|^2\right] = \sum_{k=0}^{n}(k-nx)^2 b_n^k(x),$$

la dernière égalité provenant du théorème de transfert. On obtient alors

$$\frac{1}{\eta^2}\sum_{k=0}^{n}\left(\frac{k}{n}-x\right)^2 b_n^k(x) = \frac{1}{\eta^2}\frac{x(1-x)}{n} \leq \frac{1}{n\eta^2}.$$

Ce qui permet de conclure, puisque

$$|B_n(f)(x) - f(x)| \leq \varepsilon + \frac{2M}{n\eta^2}.$$

Le majorant étant indépendant de x, il majore aussi son sup. Et quand n grandit, le majorant peut-être rendu arbitrairement petit.
Maintenant, il reste à traiter le cas général dans un intervalle $[a,b]$. Soit donc $[a,b]$ un intervalle de $\mathbb{R}$ et soit

$$\begin{aligned} g :&[0,1] \to [a,b] \\ &t \longmapsto ta + (1-t)b \end{aligned}$$

Alors $f \circ g$ est une application de $[0,1]$ dans $\mathbb{R}$. D'après ce qui précède, il existe donc $(P_n)_n$ une suite de polynômes qui approche uniformément $f \circ g$. Et alors, pour ε assez petit, il existe n assez grand tel que,

$$\sup_{x\in[0,1]} |f(g(x)) - P_n(g(x))| < \varepsilon$$

Or, par changement de variable affine,

$$\sup_{x\in[0,1]} |f(g(x)) - P_n(g(x))| = \sup_{t\in[a,b]} |f(t) - P_n(t)|$$

ce qui conclut la preuve. □

4.10 Formule sommatoire de Poisson et formule d'inversion de Fourier dans l'espace de Schwarz

Difficulté : Moyenne
Thèmes : Convergence normale, Séries de Fourier, Interversion, fonction d'une variable réel, transformée de Fourier
Leçons concernées : **246**, **235**, **241**, **250**, **228**,
Références : Z-Q, Lesfari

Enoncé 24. *Soit $f \in \mathrm{C}^1(\mathbb{R})$ tel que*

$$\sup_{x\in\mathbb{R}} x^2|f(x)| < +\infty \qquad et \qquad \sup_{x\in\mathbb{R}} x^2|f'(x)| < +\infty$$

alors

$$\forall x \in \mathbb{R}, \forall T > 0, \sum_{n\in\mathbb{Z}} f(x+Tn) = \frac{1}{T}\hat{f}\left(\frac{n}{T}\right)\mathrm{e}^{\frac{2i\pi nx}{T}}.$$

Démonstration. Commençons par donner un sens à la série de fonction du membre de droite. Soit $a > 0$, on a, pour tout $T > 0$,

$$\sup_{|x|\leq a}|f(x+Tn)| = \sup_{|y-Tn|\leq a}|f(y)| \leq \sup_{|y|\geq a-T|n|}|f(y)|.$$

Or, il existe $C > 0$ telle que $y^2|f(y)| \leq C$ pour tout $y \in \mathbb{R}$, donc

$$\sup_{|y|\geq a-T|n|}|f(y)| \leq \frac{C}{(T|n|-a^2)}.$$

où l'on a choisi n assez grand de tel sorte que $a-T|n| \neq 0$. La série $\displaystyle\sum_{n\in\mathbb{Z}} f(x+Tn)$ est donc normalement convergente sur tout compact. Notons $g(x)$ sa somme et montrons que g est dévéloppable en série de Fourier en démontrant que g est de classe $\mathcal{C}^1$. Le même raisonnement appliqué à la série $\displaystyle\sum_{n\in\mathbb{Z}} f'(x+Tn)$ assure que cette série est normalement covnergente sur tout compact. La fonction f' étant continue, g est dérivable, de dérivée continue donnée par

$$g'(x) = \sum_{n\in\mathbb{Z}} f'(x+Tn).$$

Donc g est de classe $\mathcal{C}^1$, et elle est T-périodique (un simple ré-indiçage de somme permet de le montrer). D'après le théorème de Jordan-Dirichlet, on a alors

$$\forall x \in \mathbb{R}, \quad g(x) = \sum_{p\in\mathbb{Z}} c_p(g) e^{\frac{2\pi ipx}{T}}.$$

avec

$$c_p(g) = \frac{1}{T}\int_0^T \sum_{n\in\mathbb{Z}} f(x+Tn)e^{\frac{2\pi ipx}{T}}\,\mathrm{d}x.$$

La convergence normale de la série assure la validité de l'interversion série-intégrale et alors

$$c_p(g) = \frac{1}{T}\sum_{n\in\mathbb{Z}}\int_0^T f(x+Tn)e^{\frac{2\pi ipx}{T}}\,\mathrm{d}x = \frac{1}{T}\sum_{n\in\mathbb{Z}}\int_{Tn}^{T(n+1)} f(x)e^{\frac{2\pi ipx}{T}}\,\mathrm{d}x = \frac{1}{T}\hat{f}\left(\frac{n}{T}\right).$$

D'où la formule souhaitée. Notons que l'évaluation en $x = 0$ donne d'autre part

$$\sum_{n\in\mathbb{Z}} f(Tn) = \frac{1}{T}\sum_{n\in\mathbb{Z}}\hat{f}\left(\frac{n}{T}\right).$$

□

Application. Pour tout $f \in \mathrm{S}(\mathbb{R})$, on a, pour tout $x \in \mathbb{R}$

$$f(x) = \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} e^{ix\xi} \hat{f}(\xi) d\xi.$$

En d'autres termes, la transformation de Fourier est injective dans l'espace de Schwartz

Démonstration. Soit $f \in \mathrm{S}(\mathbb{R})$. Soit $T > 0$, d'après ce qui précède, quitte à renormaliser la transformation de Fourier, on a:

$$\sum_{k\in\mathbb{Z}} f(x+kT) = \frac{\sqrt{2\pi}}{T} \sum_{k\in\mathbb{Z}} \hat{f}(k\frac{2\pi}{T}) e^{inx}.$$

En particulier, pour $x = 0$,

$$\sum_{k\in\mathbb{Z}} f(kT) = \frac{\sqrt{2\pi}}{T} \sum_{k\in\mathbb{Z}} \hat{f}(k\frac{2\pi}{T}).$$

Appliquant la formule sommatoire de Poisson au membre de droite il vient

$$\frac{\sqrt{2\pi}}{T} \sum_{k\in\mathbb{Z}} \hat{f}(k\frac{2\pi}{T}) = \frac{\sqrt{2\pi}}{T} \frac{T\sqrt{2\pi}}{2\pi} \sum_{k\in\mathbb{Z}} \hat{\hat{f}}(kT) = \sum_{k\in\mathbb{Z}} \hat{\hat{f}}(kT).$$

D'où

$$\sum_{k\in\mathbb{Z}} f(kT) = \sum_{k\in\mathbb{Z}} \hat{\hat{f}}(kT).$$

Maintenant, l'idée est de faire tendre T vers l'infini. On a

$$\sum_{k\in\mathbb{Z}} f(kT) = f(0) + \sum_{k\in\mathbb{Z}^*} f(kT).$$

Or, f est de Scharwz, donc tend vers 0 plus vite que tout polynôme quand $|x| \to \infty$. Donc en particulier, à partir d'un certain rang, on a $f(n) = O\left(\frac{1}{n^2}\right)$ quand $|n| \to \infty$. Et $f(kT) \to 0$ donc par convergence dominée

$$\lim_{T\to\infty} \sum_{k\in\mathbb{Z}^*} f(kT) = 0.$$

Il en est de même pour $\hat{\hat{f}}$ car c'est une fonction de l'espace de Scharwz aussi. Ainsi

$$f(0) = \hat{\hat{f}}(0) = \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} e^{i\cdot 0\cdot\xi} \hat{f}(\xi) \mathrm{d}\xi.$$

Maintenant, si on applique la formule précédente à l'application $\varphi : t \mapsto f(x+t)$, où x est fixé, on obtient

$$\begin{aligned} f(x) = \varphi(0) = \hat{\hat{\varphi}}(0) &= \int_{\mathbb{R}} \hat{\varphi}(\xi) \mathrm{d}\xi \\ &= \int_{\mathbb{R}} \hat{f}(\xi) \mathrm{e}^{ix\xi} \mathrm{d}\xi \\ &= \frac{1}{2\pi} \hat{\hat{f}}(-x) \end{aligned}$$

Ce qui conclut à l'injectivité de Fourier dans l'espace de Schwartz. □

Application (A éviter si on n'affaiblit pas les hypothèses du théorème)**.**

$$\sum_{n\geq 1} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Démonstration. Soit $\varepsilon > 0$ et posons $f(x) = e^{-2\pi|x|\varepsilon}$. Comme f est intégrable sur $\mathbb{R}$, on peut calculer sa transformée de Fourier explicitement

$$\begin{aligned}\hat{f}(y) &= \int_{\mathbb{R}} e^{-2\pi|x|\varepsilon} e^{-ixy2\pi} \mathrm{d}x \\ &= \int_0^{+\infty} e^{-2\pi x(\varepsilon+iy)} \mathrm{d}x + \int_0^{+\infty} e^{-2\pi x(\varepsilon-iy)} \mathrm{d}x \\ &= \frac{1}{2\pi(\varepsilon+iy)} + \frac{1}{2\pi(\varepsilon-iy)} \\ &= \frac{\varepsilon}{\pi(\varepsilon^2+y^2)}.\end{aligned}$$

La formule sommatoire de Poisson donne alors

$$\sum_{n\in\mathbb{Z}} e^{-2\pi|n|\varepsilon} = \sum_{n\in\mathbb{Z}} \frac{\varepsilon}{\pi(\varepsilon^2+n^2)}.$$

En simplifiant de part et d'autre cette équation, il vient

$$\frac{2}{1-e^{-2\pi\varepsilon}} = \frac{1}{\varepsilon\pi} + 2\frac{\varepsilon}{\pi}\sum_{n\geq 1}\frac{1}{\varepsilon^2+n^2}.$$

Et ainsi,

$$\sum_{n\geq 1}\frac{1}{\varepsilon^2+n^2} = \frac{\pi}{2\varepsilon}\left(\frac{2}{1-e^{2\pi\varepsilon}} - 1 - \frac{1}{\pi\varepsilon}\right).$$

A ce stade, on aimerait alors bien faire tendre ε vers 0. Il faut donc travailler le membre de droite pour pouvoir calculer sa limite. Ecrivant le développement limité de l'exponentielle, il vient

$$\begin{aligned}e^{-2\pi\varepsilon} &= 1 - 2\pi\varepsilon + 2\pi^2\varepsilon^2 - \frac{4}{3}\pi^3\varepsilon^3 + O(\varepsilon^4) \\ 1 - e^{-2\pi\varepsilon} &= 2\pi\varepsilon - 2\pi^2\varepsilon^2 + \frac{4}{3}\pi^3\varepsilon^3 + O(\varepsilon^4) \\ \frac{2}{1-e^{-2\pi\varepsilon}} &= \frac{1}{\pi\varepsilon}\,\frac{1}{1-\pi\varepsilon+\frac{2}{3}\pi^2\varepsilon^2+O(\varepsilon^3)} \\ &= \frac{1}{\pi\varepsilon}\left(1+\pi\varepsilon-\frac{2}{3}\pi^2\varepsilon^2+\pi^2\varepsilon^2+O(\varepsilon^3)\right) \\ &= \frac{1}{\pi\varepsilon}+1+\frac{1}{3}\pi\varepsilon+O(\varepsilon^3).\end{aligned}$$

Finalement, on obtient alors que

$$\frac{\pi}{2\varepsilon}\left(\frac{2}{1-e^{2\pi\varepsilon}} - 1 - \frac{1}{\pi\varepsilon}\right) = \frac{\pi}{2\varepsilon}\left(\frac{1}{\pi\varepsilon}+1+\frac{1}{3}\pi\varepsilon+O(\varepsilon^3) - 1 - \frac{1}{\pi\varepsilon}\right) = \frac{\pi^2}{6} + O(\varepsilon^3) \xrightarrow{\varepsilon\to 0} \frac{\pi^2}{6}.$$

□

4.11 Calcul des $\zeta(2k)$ et développement asymptotique des nombres de Bernoulli

Difficulté : Moyenne
Thèmes : Séries de Fourier, polynômes de Bernoulli, suites et séries de nombres réels
Leçons concernées : **230**, **244**, **246**
Références : El-Amrani, Analyse de Fourier

Enoncé 25. *Pour tout $k \geq 1$, $\zeta(2k) = (-1)^{k-1}\frac{(2\pi)^{2k}}{2\cdot(2k)!}b_{2k}$, où les b_n sont les nombres de Bernoulli.*

Lemme 10. *Il existe une unique suite de polynôme $(B_n[X])_{n\in\mathbb{N}} \in \mathbb{R}[X]$ tels que $B_0 = 1$, $B_n' = nB_{n-1}$ et $\forall n \geq 1, \int_0^1 B_n = 0$.*

Démonstration. Démontrons le résultat par récurrence. Supposons B_{n-1} unique. Alors $B_n = P_n + K$, $\mathbb{K} \in \mathbb{R}$, avec P_n l'unique primitive de nB_{n-1} s'annulant en 0. La constante K est alors donnée par $K = -\int_0^1 P_n(t)\mathrm{d}t$. On remarque que pour $n \geq 2$, cela équivaut à $B_n(0) = B_n(1)$ et que $B_1 = t - \frac{1}{2}$. Les nombres de Bernoulli sont alors $b_n = B_n(0)$. □

Démonstration. Pour démontrer le théorème, considérons l'application de $\mathbb{R}$ dans $\mathbb{R}$ qui a $x \mapsto \frac{B_n(\{x\})}{n!}$. Appelons là f_n. C'est une fonction 1-périodique, et on va montrer que pour $n \geq 2$, elle est continue. La continuité est assuré sur l'intervalle $[0, 1[$, montrons la continuité en 1:

$$\lim_{x\to 1^-} f_n(x) = \frac{B_n(1)}{n!} = \frac{B_n(0)}{n!} = f_n(0).$$

Donc f_n est continue pour $n \geq 2$. De plus, remarquons qu'elle est C^1 par morceaux car polynômiale par morceaux, ce qui sera utile par la suite. Calculons désormais les coefficients de Fourier de f_n. Soit $n \geq 1$, on a

$$c_0(f_n) = \int_0^1 f_n(t)\mathrm{d}t = \int_0^1 \frac{B_n(t)}{n!}\mathrm{d}t = 0.$$

Pour $p \neq 0$, montrons par récurrence que, $\forall n \geq 1, c_p(f_n) = \frac{-1}{(2i\pi p)^n}$.
Pour $n = 1$,

$$\begin{aligned} c_p(f_1) &= \int_0^1 (t - \frac{1}{2})e^{-2i\pi pt}\mathrm{d}t \\ &= \left[(t-\frac{1}{2})\frac{e^{-2i\pi pt}}{-2i\pi p}\right]_0^1 + \int_0^1 \frac{e^{-2i\pi pt}}{2i\pi p}\mathrm{d}t \\ &= \frac{1}{2i\pi p}. \end{aligned}$$

Supposons alors que le résultat soit vrai au rang n.

$$c_p(f_n) = \int_0^1 f_n(t)e^{-2i\pi pt}\mathrm{d}t = \left[f_n(t)\frac{e^{-2i\pi pt}}{-2i\pi p}\right]_0^1 + \int_0^1 f_{n-1}(t)\frac{e^{-2i\pi pt}}{2i\pi p}\mathrm{d}t = 0 + \frac{1}{2i\pi p}c_p(f_{n-1}).$$

Ainsi, par le théorème de Jordan Dirichlet et comme f_n est continue, la série de Fourier de f_n converge vers f partout. Ainsi,

$$\begin{aligned} f_{2p}(t) &= \sum_{p\in\mathbb{Z}^*} c_p(f_{2p})e^{2i\pi pt} \\ &= \sum_{p>0} c_p(f_{2p})(e^{2i\pi pt} + e^{-2i\pi pt}). \end{aligned}$$

En particulier, en évaluant en $t = 0$, on obtient

$$\frac{b_{2k}}{(2k)!} = \sum_{p>0} 2\frac{(-1)^{k-1}}{2^{2k}p^{2k}\pi^{2k}}.$$

Enfin, en réarrangeant, on trouve

$$\sum_{p>0} \frac{1}{p^{2k}} = \zeta(2k) = \frac{b_{2k}\,(-1)^{k-1}\,2^{2k}\,\pi^{2k}}{2\cdot(2k)!}.$$

Enfin, comme $\lim_{k\to\infty} \zeta(2k) = 1$, on a

$$b_{2k} \overset{k\to\infty}{\sim} \frac{2\cdot(2k)!}{(-1)^{k-1}\,2^{2k}\,\pi^{2k}}.$$

□

4.12 Formule d'Euler-MacLaurin

Difficulté : Dure
Thèmes : Intégration, polynômes de Bernoulli, developpement asymptotique
Leçons concernées : **223**, **224**, **226**, **230**, **228**.
Références : Candelpergher, Calcul intégral

Enoncé 26. *Soient $n \in \mathbb{N}$, $n > 1$ et f une fonction indéfiniment dérivable sur $[1, +\infty[$ pour laquelle il existe $M \geq 1$ tel que pour tout $m \geq M$, on ait:*

$$\partial^m f(x) = O\left(\frac{1}{x^2}\right) \quad \text{quand } x \to +\infty.$$

Alors on a, pour tout $m \geq M$

$$f(1) + \cdots + f(n) = T_m(n) + C + R_m(n),$$

où $T_m(n)$ est un terme dépendant de n :

$$T_m(n) = \int_1^n f(x)\mathrm{d}x + \frac{f(n)}{2} + \sum_{k=2}^{m} \frac{(-1)^k B_k}{k!} \partial^{k-1} f(n),$$

C est une constante (indépendante de m et n)

$$C = \frac{f(1)}{2} - \sum_{k=1}^{m} \frac{(-1)^k B_k}{k!} \partial^{k-1} f(1) + (-1)^{m+1} \int_1^{+\infty} \frac{b_m(x)}{m!} \partial^m f(x)\mathrm{d}x.$$

et $R_m(n)$ tend vers 0 quand $n \to +\infty$.

$$R_m(n) = (-1)^m \int_n^{+\infty} \frac{b_m(x)}{m!} \partial^m f(x)\mathrm{d}x.$$

Les B_k sont les nombres de Bernoulli et les b_k sont les polynômes de Bernoulli définis sur $[0, 1[$ et prolongés par 1-périodicité.

Pour ce développement, étant donné la complexité de l'énoncé, on commencera par l'application pour comprendre l'utilité et on démontrera le résultat après.

Application. Observons ce qu'il se passe si $f(x) = \frac{1}{x^2}$. On a $M = 1$, donc pour $m = 7$ par exemple

$$\begin{aligned} 1 + \frac{1}{4} + \cdots + \frac{1}{n^2} &= T_m(n) + C + R_m(n) \\ &= \int_1^n \frac{\mathrm{d}x}{x^2} + \frac{1}{2n^2} - \frac{1}{6n^3} + \frac{1}{30n^5} - \frac{1}{42n^7} + C + O\left(\frac{1}{n^9}\right) \\ &= 1 + C - \frac{1}{n} + \frac{1}{2n^2} - \frac{1}{6n^3} + \frac{1}{30n^5} - \frac{1}{42n^7} + O\left(\frac{1}{n^9}\right) \end{aligned}$$

Cette formule donne une estimation des sommes partielles avec une grande précision. Par exemple, pour $n = 100$, on calcule 5 termes au lieu de 100 avec une précision de l'ordre de 18 chiffres après la virgule. Enfin cela à condition qu'on sache calculer la constante C.

Démonstration. La démonstration de ce résultat est, malgré les apparences, assez simple en réalité. L'idée est la suivante: lorsqu'on réalise une IPP, on intègre souvent la constante 1 en x. Ici, on va plutôt l'intégrer en un polynôme d'intégrale nulle sur $[0, 1]$.

Lemme 11. *Il existe une suite de polynômes (p_n) tel que $p_0 = 1$ et $\partial p_n = p_{n-1}$*

Pour de tels polynômes, si f est infiniment dérivable sur $[0,1]$, on a alors

$$\begin{aligned}\int_0^1 f(x)\mathrm{d}x &= \int_0^1 f(x)p_0(x)\mathrm{d}x \\ &= [f(x)p_1(x)]_0^1 - \int_0^1 f'(x)p_1(x)\mathrm{d}x \\ &= [f(x)p_1(x)]_0^1 - [f'(x)p_2(x)]_0^1 + \int_0^1 \partial^2 f(x)p_2(x)\mathrm{d}x \\ &\dots \\ &= \sum_{k=1}^{m}(-1)^{k-1}[p_k\partial^{k-1}f]_0^1 + (-1)^m\int_0^1 p_m(x)\partial^m f(x)\mathrm{d}x.\end{aligned}$$

Comme chaque terme de la somme fait intervenir des termes de bord des p_n, pour simplifier la formule, on aimerait alors que $p_n(0) = p_n(1)$. En fait on peut prendre les p_n tel que $p_n(0) = p_n(1), \forall n \geq 2$. Cette condition équivaut à

$$\int_0^1 p_n(x)\mathrm{d}x = 0, \quad \text{pour tout } n \geq 1.$$

Par récurrence, on montre que la suite (p_n) vérifie

$$p_{n+1} = \sum_{k=0}^{n} a_k \frac{x^{k+1}}{k+1} + C_{n+1}.$$

Et la condition sur l'intégrale détermine la constante C_{n+1}. Cela prouve l'existence et l'unicité de la suite (p_n). On appelle alors polynômes de Bernoulli les polynômes $x \mapsto B_n(x)$, où $B_n(x)$ est tel que $p_n(x) = \frac{B_n(x)}{n!}$, et les nombres de Bernoulli sont les $B_n = B_n(0)$. Ces nombres vérifient une variété de propriétés, par exemple que pour $k \geq 1$, $B_{2k+1} = 0$. Cela étant dit, la formule écrite précedemment donne alors

$$\int_0^1 f(x)\mathrm{d}x = \frac{f(0)+f(1)}{2} + \sum_{k=2}^{m}\frac{(-1)^{k-1}B_k}{k!}[\partial^{k-1}f]_0^1 + (-1)^m\int_0^1 \frac{B_m(x)}{m!}\partial^m f(x)\mathrm{d}x.$$

On a alors presque terminé. Ayant établi cette égalité sur $[0,1]$, par relation de Chasles, on sait presque estimer $\int_p^q f(x)\mathrm{d}x$. Prolongeant par 1-périodicité les B_k, ce que donne b_k défini par $b_k(x) = B_k(x - [x])$, on a alors

$$\begin{aligned}\int_p^q f(x)\mathrm{d}x = \frac{f(p)}{2} + f(p+1) + \dots + f(q-1) + \frac{f(q)}{2} \\ + \sum_{k=2}^{m}\frac{(-1)^{k-1}B_k}{k!}[\partial^{k-1}f]_p^q + (-1)^m\int_p^q \frac{b_m(x)}{m!}\partial^m f(x)\mathrm{d}x.\end{aligned}$$

Cette formule donne une expression pour l'intégrale de f. Maintenant, en réarrangeant, en prenant $p = 1$ et $q = n$, il vient alors

$$\begin{aligned}f(1) + \dots + f(n) = \int_1^n f(x)\mathrm{d}x + \frac{f(1)+f(n)}{2} + \sum_{k=2}^{m}\frac{(-1)^k B_k}{k!}[\partial^{k-1}f]_1^n \\ + (-1)^{m+1}\int_1^n \frac{b_m(x)}{m!}\partial^m f(x)\mathrm{d}x.\end{aligned}$$

La dernière intégrale dans cette formule n'a aucune raison de tendre vers 0. Utlisant alors l'hypothèse sur les dérivées de f, on s'assure la convergence de l'intégrale, ce qui justifie d'écrire

$$\int_1^n \frac{b_m(x)}{m!}\partial^m f(x)\mathrm{d}x = \int_1^{+\infty}\frac{b_m(x)}{m!}\partial^m f(x) - \int_n^{+\infty}\frac{b_m(x)}{m!}\partial^m f(x)\mathrm{d}x.$$

Et la dernière intégrale, noté $R_m(n)$, est bien une quantité qui tend vers 0 quand n tend vers l'infini. Afin de conclure, il suffit de montrer que le terme

$$C_m = \frac{f(1)}{2} - \sum_{k=2}^{m}\frac{(-1)^k B_k}{k!}\partial^{k-1}f(1) + (-1)^{m+1}\int_1^{+\infty}\frac{b_m(x)}{m!}\partial^m f(x)\mathrm{d}x.$$

est constant. Il est clair qu'il ne dépend pas de n mais en fait, il ne dépend pas non plus de m pour $m \geq M$. En effet, on a

$$\int_1^{+\infty} \frac{b_m(x)}{m!}\partial^m f(x)\mathrm{d}x = \sum_{k=1}^{+\infty}\int_k^{k+1} \frac{b_m(x)}{m!}\partial^m f(x)\mathrm{d}x.$$

et en intégrant par parties

$$\begin{aligned}
&\sum_{k=1}^{+\infty}\int_k^{k+1} \frac{b_m(x)}{m!}\partial^m f(x)\mathrm{d}x \\
&\qquad = \sum_{k=1}^{+\infty}\left[\frac{b_{m+1}(x)}{(m+1)!}\partial^m f(x)\right]_k^{k+1} - \sum_{k=1}^{+\infty}\int_k^{k+1}\frac{b_{m+1}(x)}{(m+1)!}\partial^{m+1}f(x)\mathrm{d}x \\
&\qquad = \sum_{k=1}^{+\infty}\frac{B_{m+1}}{(m+1)!}(\partial^m f(k+1) - \partial^m f(k)) - \int_1^{+\infty}\frac{b_{m+1}(x)}{(m+1)!}\partial^{m+1}f(x)\mathrm{d}x \\
&\qquad = -\frac{B_{m+1}}{(m+1)!}\partial^m f(1) - \int_1^{+\infty}\frac{b_{m+1}(x)}{(m+1)!}\partial^{m+1}f(x)\mathrm{d}x.
\end{aligned}$$

Donc

$$\begin{aligned}
C_m &= \frac{f(1)}{2} - \sum_{k=2}^{m}\frac{(-1)^k B_k}{k!}\partial^{k-1}f(1) + (-1)^{m+1}\int_1^{+\infty}\frac{b_m(x)}{m!}\partial^m f(x)\mathrm{d}x \\
&= \frac{f(1)}{2} - \sum_{k=2}^{m}\frac{(-1)^k B_k}{k!}\partial^{k-1}f(1) + (-1)^{m+1}\left(-\frac{B_{m+1}}{(m+1)!}\partial^m f(1) - \int_1^{+\infty}\frac{b_{m+1}(x)}{(m+1)!}\partial^{m+1}f(x)\mathrm{d}x\right) \\
&= \frac{f(1)}{2} - \sum_{k=2}^{m+1}\frac{(-1)^k B_k}{k!}\partial^{k-1}f(1) + (-1)^{m+2}\int_1^{+\infty}\frac{b_{m+1}(x)}{(m+1)!}\partial^{m+1}f(x)\mathrm{d}x \\
&= C_{m+1}
\end{aligned}$$

Ce qui conclut le développement. □

4.13 Théorème des fonctions implicites

Difficulté : Très dur (je suis nul en calcul diff)
Références : Laudenbach, Calcul différentiel

Enoncé 27. *Soient E_1, E_2 et F des espaces de Banach, deux ouverts U et V respectivement de E_1 et E_2 et une application $f : U \times V \to F$ de classe C^1. On suppose qu'il existe $(a,b) \in E_1 \times E_2$ tels que $f(a,b) = 0$, et que $\frac{\partial f}{\partial y}(a,b)$ est inversible, d'inverse continue (automatique en dimension finie). Alors il existe des voisinages V_a et V_b respectivement de a et de b, et une application $\varphi : V_a \to V_b$ de classe C^1 tel que :*

- $\varphi(a) = b$
- *Pour tout $(x,y) \in V_a \times V_b$, $f(x,y) = 0 \Leftrightarrow y = \varphi(x)$.*

De plus, la différentielle de φ en a est donnée par la formule suivante

$$\mathrm{D}\varphi(a) = -\left[\frac{\partial f}{\partial y}(a,b)\right]^{-1} \circ \frac{\partial f}{\partial x}(a,b).$$

Démonstration. Soit $g : U \times V$ définie par $g(x,y) = (x, f(x,y))$. La différentielle $\mathrm{D}g(a,b) : E_1 \times E_2 \to E_1 \times F$ est donnée par

$$\mathrm{D}g(a,b)(h,k) = \left(h, \frac{\partial f}{\partial x}(a,b)(h) + \frac{\partial f}{\partial y}(a,b)(k)\right).$$

On observe alors que cette différentielle est inversible. En effet, si $(h',k') = \mathrm{D}g(a,b)(h,k)$, alors l'inverse est donnée par

$$h = h', \qquad k = \left[\frac{\partial f}{\partial y}(a,b)\right]^{-1}\left(k' - \frac{\partial f}{\partial x}(a,b)(h')\right).$$

Etant inversible, par le théorème d'inversion locale, il existe un voisinage W de (a,b) dans $E_1 \times E_2$, et une boule ouverte B centrée en $(a,0)$ de rayon $r > 0$ dans $E_1 \times F$ tels que $g|_W$ soit un C^1 difféomorphisme de W dans B. Le diffémorphisme inverse de g est de la forme $g^{-1}(x,z) = (x, \Phi(x,z))$. On a alors l'équivalence

$$(x,y) \in W,\ f(x,y) = 0 \Leftrightarrow \|x - a\| < r \text{ et } y = \Phi(x,z).$$

Cela prouve que les solutions de $f(x,y) = 0$ dans W sont les points du graphe de φ, où

$$\varphi(x) = \Phi(x,0).$$

Comme W est ouvert, il existe un voisinage V_a de a ouvert dans E_1 et un voisinage V_b de b, ouvert dans E_2 tels que $V_a \times V_b \subset W$. Comme φ est continue, quitte à rétrécir V_a, on peut supposer $\varphi(V_a) \subset V_b$. Les ouverts V_a et V_b, ainsi que φ ont alors les propriétés énoncées. □

4.14 Inégalité de Hoeffding

Difficulté : Moyen
Thèmes : Probabilités, transformée de Laplace, Inégalité de Markov, convexité
Leçons concernées : **229**, **253**, **261**, **262**, **264**, **266**
Références : Bernis, 40 Développements pour l'agrégation

Enoncé 28. *Soit $(X_n)_{n\geq 1}$ une suite de variables aléatoires réelles, indépendantes, et d'espérance nulle. On suppose qu'il existe une suite de réelles strictement positifs $(c_n)_{n\geq 1}$ telle que pour tout n, on ait*

$$|X_n| \leq c_n, \qquad \mathbb{P}\text{-presque sûrement.}$$

Alors, pour tout $\varepsilon > 0$ et pour tout $n \geq 1$, notant $S_n = \sum X_k$ on a

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

Lemme 12. *Soit X une variable aléatoire réelle, centrée, et bornée presque sûrement par 1. Alors*

$$\mathbb{E}[\exp(tX)] \leq \exp\left(\frac{t^2}{2}\right).$$

Preuve du lemme. Soit $x \in [-1,1]$. Commençons par remarquer que pour tout $t \in \mathbb{R}$, on a

$$\frac{1-x}{2} + \frac{1+x}{2} = 1, \quad \frac{1-x}{2} \in [0,1], \quad \frac{1-x}{2}(-t) + \frac{1+x}{2}(t) = tx.$$

De cela, on tire que l'application $x \mapsto \frac{1-x}{2}(-t) + \frac{1+x}{2}(t)$ est un paramètrage du segment $[-t,t]$ et que c'est une combinaison convexe. Donc par convexité de la fonction exp, il vient

$$\exp(tx) \leq \frac{1-x}{2}\exp(-t) + \frac{1+x}{2}\exp(t).$$

Retournons maintenant aux probabilités. Comme X est bornée par 1, pour tout $u \in \mathbb{R}$, uX est une variable aléatoire bornée, il en va de même pour $\exp(uX)$. Aussi, cela assure l'existence de son espérance. Ainsi,

$$\begin{aligned}
\mathbb{E}[\exp(tX)] &\leq \frac{1}{2}\left(\mathbb{E}[(1-X)\exp(-t) + (1+X)\exp(t)]\right) \\
&\leq \frac{1}{2}\left(\mathbb{E}[(1-X)\exp(-t)] + \mathbb{E}(1+X)\exp(t)]\right) \\
&\leq \frac{1}{2}\left(\exp(-t) + \exp(t)\right) \qquad \text{car } \mathbb{E}[X] = 0 \\
&= \mathrm{ch}(t).
\end{aligned}$$

Or,

$$\mathrm{ch}(t) = \sum_{k=0}^{+\infty} \frac{t^{2k}}{(2k)!} \qquad \text{et} \qquad \exp\left(\frac{t^2}{2}\right) = \sum_{k=0}^{+\infty} \frac{t^{2k}}{2^k\ k!}.$$

et pour tout $k \in \mathbb{N}$, on a

$$2^k\ k! = 2^k(1 \cdot 2 \cdots k) = ((1\cdot 2)\cdot(2\cdot 2)\cdot\cdots\cdot(2\cdot k)) = 2\cdot 4\cdot 6\cdots 2k \leq (2k)!$$

Donc, en raisonnant sur les sommes partielles pour tout n, il vient $\mathrm{ch}(t) \leq \exp\left(\frac{t^2}{2}\right)$ pour tout $t \in \mathbb{R}$, donc

$$\mathbb{E}[\exp(tX)] \leq \exp\left(\frac{t^2}{2}\right).$$

□

Preuve de l'inégalité. Comme l'application $x \mapsto \exp(x)$ est continue de $\mathbb{R}$ dans $\mathbb{R}$, elle est mesurable de $(\mathbb{R}, \mathrm{Bor}(\mathbb{R}))$ dans $(\mathbb{R}, \mathrm{Bor}(\mathbb{R}))$. Ainsi, comme les (X_i) sont indépendants, cela assure que la famille $(\exp(tX_i))$ l'est aussi. De plus, pour tout $k \in \mathbb{N}^*$, la variable aléatoire $\frac{X_k}{c_k}$ est centrée, bornée par 1, ce qui permet de lui appliquer le lemme. De tout cela il vient alors, pour $t \in \mathbb{R}$ et $n \in \mathbb{N}^*$,

$$\begin{aligned}
\mathbb{E}[\exp(tS_n)] &= \mathbb{E}\exp\left(t\sum_{k=1}^{n} X_k\right) && (6)\\
&= \mathbb{E}\left[\prod_{k=1}^{n}\exp(tX_k)\right] && (7)\\
&= \prod_{k=1}^{n}\mathbb{E}\left[\exp\left(tc_k\frac{X_k}{c_k}\right)\right] \qquad \text{par indépendance} && (8)\\
&\leq \prod_{k=1}^{n}\exp\left(\frac{t^2c_k^2}{2}\right) && (9)\\
&\leq \exp\left(\frac{t^2}{2}\sum_{k=1}^{n}c_k^2\right). && (10)
\end{aligned}$$

Nous ne sommes pas loin de conclure. Soit $\varepsilon > 0$. Par croissance de la fonction exponentielle, l'inclusion $\{S_n > \varepsilon\} \subset \{\exp(tS_n) > \exp(t\varepsilon)\}$ entraîne l'inégalité $\mathbb{P}(\{S_n > \varepsilon\}) \leq \mathbb{P}(\{\exp(tS_n) > \exp(t\varepsilon)\})$. De plus, pour tout $t \in \mathbb{R}_+^*$, $\exp(tS_n)$ est une variable aléatoire positive donc on peut lui appliquer Markov:

$$\begin{aligned}
&\mathbb{P}(S_n > \varepsilon)\mathbb{P}(\{\exp(tS_n) > \exp(t\varepsilon)\})\\
&\qquad \leq \exp(-t\varepsilon)\mathbb{E}[\exp(tS_n)]\\
&\qquad \leq \exp\left(\frac{t^2}{2}\sum_{k=1}^{n}c_k^2 - t\varepsilon\right).
\end{aligned}$$

où la dernière inégalité provient de 10. Cette égalité étant vraie pour tout $t \in \mathbb{R}_+^*$, on va essayer de trouver le t_0 optimal. L'application $\varphi : t \mapsto \frac{t^2}{2}\sum_{k=1}^{n}c_k^2 - t\varepsilon$ est un polynôme de degré 2. Il est facile de vérifier que son minimum est atteint en $t_0 = \frac{\varepsilon}{\sum_{k=1}^{n}c_k^2}$ et

$$\varphi(t_0) = \frac{-\varepsilon^2}{2\sum_{k=1}^{n}c_k^2}.$$

Ainsi,

$$\mathbb{P}(S_n > \varepsilon) \leq \exp\left(\frac{-\varepsilon^2}{2\sum_{k=1}^{n}c_k^2}\right).$$

Raisonnement de la même façon sur $\mathbb{P}(\{-Sn > \varepsilon\})$ puisque la suite $(-X_n)$ vérifie les mêmes hypothèses que la suite (X_n) on conclut

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

□

4.15 Théorème central limite + applications

Difficulté : Moyen
Thèmes : Probabilités
Leçons concernées : **218**, **224**, **261**, **262**, **264**, **266**.
Références : Garet-Kurtzmann, De l'intégration aux probabilités

Enoncé 29. *Soit $(X_i)_i$ une suite de variables aléatoire i.i.d dans* L^2. *Soit $m = \mathbb{E}[X_1]$ et $\sigma^2 = \mathrm{Var}[X_1]$. Alors*

$$\lim_{n\to\infty} \frac{S_n - nm}{\sigma\sqrt{n}} \underset{Loi}{=} \mathcal{N}(0,1).$$

Lemme 13. *Pour tout $(u,v) \in \mathbb{C}^2$, on a*

$$|u^n - v^n| \leq n|u-v| \max\{|u|,|v|\}^{n-1}.$$

Preuve du lemme. On a

$$u^n - v^n = (u-v)(u^{n-1} + u^{n-2}v + \cdots + uv^{n-2} + v^{n-1}).$$

En passant au module

$$\begin{aligned} |u^n - v^n| &\leq |u-v| \sum_{j=0}^{n-1} |u|^j |v|^{n-1-j} \\ &\leq n|u-v| \max\{|u|,|v|\}^{n-1}. \end{aligned}$$

□

Démonstration. Sans perte de généralité, on peut supposer que $m = 0$ et $\sigma = 1$. Il faut alors montrer que $\frac{S_n}{\sqrt{n}}$ converge en loi vers $\mathcal{N}(0,1)$. On va montrer que la fonction caractéristique de $\frac{S_n}{\sqrt{n}}$, noté Φ_n converge vers celle de la loi normale. On remarque tout d'abord

$$\begin{aligned} \Phi_n(t) &= \mathbb{E}\left[e^{it\frac{1}{\sqrt{n}}\sum_{i=1}^n X_i}\right] \\ &= \mathbb{E}\left[\prod_{i=1}^n e^{\frac{itX_j}{\sqrt{n}}}\right] \\ &= \prod_{j=1}^n \mathbb{E}[e^{\frac{itX_j}{\sqrt{n}}}], \qquad \text{par indépendance des } X_i \text{ et } X_i \in L^1 \\ &= \prod_{j=1}^n \Phi_{X_j}\left(\tfrac{t}{\sqrt{n}}\right) = \left(\Phi_{X_1}\left(\tfrac{t}{\sqrt{n}}\right)\right)^n. \end{aligned}$$

Comme X_1 est L, le théorème de dérivabilité sous l'intégrale implique que Φ_{X_1} est C^2. En particulier, Φ_{X_1} est 2 fois dérivable en 0 et son développement limité est

$$\Phi_{X_1}(t) = \Phi_{X_1}(0) + \Phi'_{X_1}(0)t + \frac{\Phi''_{X_1}(0)}{2} + o(t^2).$$

Or, $\Phi_X^{(p)}(t) = \mathbb{E}\left[(iX)^p e^{itX}\right]$, donc $\Phi_{X_1}(0) = 1, \Phi'_{X_1}(0) = \mathbb{E}[X_1] = 0$ et $\Phi''_{X_1}(0) = \mathbb{E}[-X^2] = -\mathrm{Var}[X_1] = 1$ donc

$$\Phi_{X_1}(t) = 1 - \frac{t^2}{2} + o(t^2).$$

On va alors utiliser le lemme avec $u = \Phi_{X_1}\left(\frac{t}{\sqrt{n}}\right)$ et $v = 1 - \frac{t^2}{2n}$. Il vient alors

$$\begin{aligned} \left|\Phi_{X_1}^n\left(\frac{t}{\sqrt{n}}\right) - \left(1-\frac{t^2}{2n}\right)^n\right| &\leq n\left|\Phi_{X_1}\left(\frac{t}{\sqrt{n}}\right) - \left(1-\frac{t^2}{2n}\right)\right| \max\left\{\left|\Phi_{X_1}\left(\frac{t}{\sqrt{n}}\right)\right|, \left|1-\frac{t^2}{2n}\right|\right\}^{n-1} \\ &\leq n\ o\left(\frac{t}{\sqrt{n}}\right)^2 \qquad \text{pour } n \text{ assez grand} \\ &\leq o(1) \xrightarrow{n\to\infty} 0 \end{aligned}$$

De cela, on conclut que la fonction caractéristique de $\frac{S_n}{\sqrt{n}}$ tend vers la limite en n de $\left(1-\frac{t^2}{2n}\right)^n$. Or

$$\left(1-\frac{t^2}{2n}\right)^n = e^{-\frac{t^2}{2}}.$$

D'où la convergence en loi ce qui conclut. □

Application.

$$n! \overset{n\to\infty}{\sim} \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

Démonstration. Considérons $(X_i)_i$ une suite de variables aléatoires indépendantes suivant une loi exponentielle de paramètre 1. Soit $S_n = X_1 + \cdots + X_n$. Montrons par récurrence que S_n a pour densité

$$f_n(x) = \frac{x^{n-1}}{(n-1)!}e^{-x}1_{\mathbb{R}_+}(x).$$

Pour $n = 1$, il n'y rien à démontrer. Supposons alors que S_n a pour densité f_n. On va appliquer la méthode de la fonction muette. Soit g mesurable de $(\mathbb{R}, \mathrm{Bor}(\mathbb{R}))$ dans $(\mathbb{R}, \mathrm{Bor}(\mathbb{R}))$, on a

$$\begin{aligned}
\mathbb{E}\left[g(S_n + X_{n+1})\right] &= \int_\Omega g(S_n + X_{n+1})\mathrm{d}\mathbb{P}(w) \\
&= \int_{\mathbb{R}^2} g(s+x)\mathrm{d}\mathbb{P}_{S_n, X_{n+1}} \qquad \text{par le théorème du transfert} \\
&= \int_{\mathbb{R}^2} g(s+x)\mathrm{d}\left(\mathbb{P}_{S_n}\times\mathbb{P}_{X_{n+1}}\right) \qquad \text{par indépendance de } X_{n+1} \text{ et } S_n \\
&= \int_0^{+\infty}\left(\int_0^{+\infty} g(s+x)e^{-x}\frac{s^{n-1}}{(n-1)!}e^{-s}\mathrm{d}x\right)\mathrm{d}s \qquad \text{loi de couple = produit des densités} \\
&= \int_0^{+\infty}\frac{s^{n-1}}{(n-1)!}\left(\int_0^{+\infty} g(s+x)e^{-(s+x)}\mathrm{d}x\right)\mathrm{d}s \\
&= \int_0^{+\infty}\frac{s^{n-1}}{(n-1)!}e^{-s}\left(\int_0^{+\infty} g(u)e^{u}1_{u>s}\mathrm{d}u\right)\mathrm{d}s \\
&= \int_0^{+\infty} g(u)e^{-u}\left(\int_0^{+\infty}\frac{s^{n-1}}{(n-1)!}1_{u>s}\mathrm{d}s\right)\mathrm{d}u \\
&= \int_s^{+\infty} g(u)e^{-u}\left(\int_0^{u}\frac{s^{n-1}}{(n-1)!}\mathrm{d}s\right)\mathrm{d}u \\
&= \int_s^{+\infty} g(u)e^{-u}\frac{u^n}{n!}\mathrm{d}u = \mathbb{E}\left[g(S_{n+1})\right].
\end{aligned}$$

On fixe alors un $x > 0$ et on pose

$$G_n(x) = \mathbb{P}(0 < \frac{S_n - n}{\sqrt{n}} < x).$$

Alors

$$\begin{aligned}
G_n(x) &= \mathbb{P}(n < S_n < \sqrt{n}x + n) \\
&= \int_n^{\sqrt{n}x+n} e^{-t}\frac{t^{n-1}}{(n-1)!}\mathrm{d}t \\
&= \int_0^x \frac{(\sqrt{n}u+n)^{n-1}}{(n-1)!}e^{(-\sqrt{n}u+n)}\sqrt{n}\mathrm{d}u \\
&= e^{-n}\frac{\sqrt{n}n^{n-1}}{(n-1)!}\int_0^x\left(1+\frac{u}{\sqrt{n}}\right)^{n-1}e^{-\sqrt{n}u}\mathrm{d}u \\
&= e^{-n}\frac{n^n\sqrt{2\pi n}}{n!}\frac{1}{\sqrt{2\pi}}\int_0^x\left(1+\frac{u}{\sqrt{n}}\right)^{n-1}e^{-\sqrt{n}u}\mathrm{d}u.
\end{aligned}$$

Or, pour n assez grand,

$$\begin{aligned}\left(1+\frac{u}{\sqrt{n}}\right)^{n-1} e^{-\sqrt{n}u} &= e^{(n-1)\log\left(1+\frac{u}{\sqrt{n}}\right)-\sqrt{n}u} \\ &\overset{n\to\infty}{=} e^{(n-1)\left(\frac{u}{\sqrt{n}}-\frac{u^2}{2n}+o\left(\frac{u}{n}\right)\right)-\sqrt{n}u} \\ &= e^{-\frac{u^2}{2}} e^{-\frac{u}{\sqrt{n}}+\frac{u^2}{2n}+o(1)} \\ &= e^{-\frac{u^2}{2}}.\end{aligned}$$

Egalement, d'après le théorème central limite, $\frac{S_n-n}{\sqrt{n}}$ converge en loi vers une $\mathcal{N}(0,1)$. Donc $G_n(x)$ converge vers la quantité $\mathbb{P}(Y\in[0,x])$, où $Y\sim\mathcal{N}(0,1)$. Or,

$$\mathbb{P}(Y\in[0,x]) = \frac{1}{\sqrt{2\pi}}\int_0^x e^{-\frac{u^2}{2}}\,\mathrm{d}u$$

D'où, nécéssairement, $e^{-n}\frac{n^n\sqrt{2\pi n}}{n!} \xrightarrow[n\to\infty]{} 1$ ou, de façon équivalente, $n!\sim\left(\frac{n}{e}\right)^n\sqrt{2\pi}$. □

Application.

$$\sum_{k=0}^{n}\frac{n^k}{k!} \overset{\infty}{\sim} \frac{e^n}{2}.$$

Démonstration. Soit $(X_i)_i$ une suite de variables aléatoires indépendantes suivant une loi de paramètre 1. Les X_i admettent un moment d'ordre 2 donc sont L^2. Soit $S_n=\sum X_i$, alors S_n suit une loi de Poisson de paramètre n (passer par la fonction caractéristique pour le montrer). Maintenant,

$$\mathbb{P}(S_n\le n) = \sum_{k=0}^{n}\mathbb{P}(S_n=k) = \sum_{k=0}^{n}\frac{n^k}{k!}e^{-n}.$$

De plus, par le théorème central limite, $\frac{S_n-n}{\sqrt{n}}$ converge en loi vers une $\mathcal{N}(0,1)$. En particulier,

$$\mathbb{P}(S_n-n\le 0) = \mathbb{P}\left(\frac{S_n-n}{\sqrt{n}}\le 0\right) \xrightarrow[\infty]{} \frac{1}{2}.$$

Donc

$$e^{-n}\sum_{k=0}^{n}\frac{n^k}{k!} \to \frac{1}{2},$$

ce qui conclut. □

4.16 Indécomposabilité de la loi de Poisson

Difficulté : Moyenne
Thèmes : Séries entières, Série génératrice d'une variable aléatoire, probabilités,
Leçons concernées : **241**, **243**, **245**, **261**, **264**, **266**
Références : Queffelec, Analyse Complexe

On sait que si X et Y sont indépendantes et suivent une loi de Poisson de paramètres λ et μ respectivement, alors la somme $X+Y$ suit une loi de Poisson de paramètre $\lambda+\mu$. Dans ce développement, on montre la réciproque, c'est à dire que si $X+Y$ suit une loi de poisson de paramètre $\lambda+\mu$ avec X et Y indépendantes, alors X et Y suivent indépendamment des lois de Poisson.

5 Résultats bonus

J'ai regroupé dans cette partie des résulats que j'appécie, des exercices sympathiques, trop court pour être developpés mais qui peuvent potentiellement être incorporés dans des leçons.

5.1 Un groupe contenant 80% d'éléments d'ordre 2 est abélien

Difficulté : Difficile, beaucoup de pré-requis, mais qui peut impressionner le jury!
Thèmes : Théorème de Dixon, Théorie des répresentations, Théorie des caractères.

On sait qu'un groupe vérifiant $\forall x \in G, x^2 = 1_G$ est abélien ($xyx^{-1}y^{-1} = xyxy = (xy)^2 = 1_G$). En vérité, si on suppose que G est fini, on a un résultat un peu plus fin :

Enoncé 30. *Soit G un groupe fini. On tire uniformément un élément g parmi G. Si la probabilité $p = \mathbb{P}(g^2 = 1_G) \geq \sqrt{\frac{5}{8}}$, alors G est abélien. En d'autres termes, si un groupe fini G contient au moins 80% éléments d'ordre 2, il est abélien.*

Démonstration. Soit G un groupe fini. Notons $R(h) = \text{Card}(\{g \in G, g^2 = h\}$. $R(h)$ est une fonction de classe. Ainsi, comme les répresentations irréductibles forment une base orthonormée des fonctions centrales sur G, on a $R = \sum_{\chi \text{ irreductible}} \alpha_k \chi_k$. De plus, pour trouver les α_k, il suffit d'évaluer $R(h)$ contre un caractère irréductible:

$$\begin{aligned}
\langle R, \mu \rangle &= \frac{1}{|G|} \sum_{h \in G} \mu(h) R(h) \\
&= \frac{1}{|G|} \sum_{h \in G} (\sum_{g \in G} \delta_{g^2,h}) \mu(h) \\
&= \frac{1}{|G|} \sum_{g \in G} (\sum_{h \in G} \delta_{g^2,h}) \mu(h) \\
&= \frac{1}{|G|} \sum_{g \in G} \mu(g^2).
\end{aligned}$$

Ainsi, en évaluant en $h = 1_G$, il vient $R(1_G) = \frac{1}{|G|} \sum_{\chi} \sum_{g \in G} \chi(g^2)\chi(1_G)$. Notant $v(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g^2)$, la fonction v est appélé indicatrice de Frobenius-Schur. Elle est à valeur dans $\{-1, 0, 1\}$ (admis). Par Cauchy-Schwarz, on a alors

$$\begin{aligned}
R(1_G) &= \sum_{\chi} v(\chi)\chi(1_G) \\
&\leq \left(\sum_{\chi} v^2(\chi) \right)^{\frac{1}{2}} \left(\sum_{\chi} \chi^2(1_G) \right)^{\frac{1}{2}} \\
&\leq \sqrt{k}\sqrt{|G|}.
\end{aligned}$$

où k est le nombre de classe de conjugaison de G. La dernière inégalité venant du fait que v^2 est à valeurs dans 0 ou 1, et qu'il y a autant de classe de conjugaison que des représentations irréductibles. Aussi, commme $|G|$ est égale à la somme des dimensions au carré des représentations irréductibles, cela conclut l'inégalité. Enfin pour conclure, si G n'était pas abélien la probabilité que deux éléments commutent dans un groupe étant $\frac{k}{|G|} \leq \frac{5}{8}$ (théorème de Dixon), on aurait :

$$\mathbb{P}(g^2 = 1_G) = \frac{R(1_G)}{|G|} \leq \sqrt{\frac{k}{|G|}} \leq \sqrt{\frac{5}{8}} \sim 0,79.$$

□

5.2 Groupe dont Aut(G) est réduit au neutre

Enoncé 31. *Soit G un groupe fini dont le groupe des automorphismes est réduit à l'identité. Alors G est isomorphe à $\mathbb{Z}/2\mathbb{Z}$*

Démonstration. Soit $g \in G$. Considérons le morphisme de groupe suivant

$$\begin{aligned} \phi : G &\longrightarrow G \\ h &\mapsto ghg^{-1}. \end{aligned}$$

C'est un automorphisme de G, donc pour tout $h \in G, ghg^{-1} = h$ et cela pour tout $g \in G$. Donc G est abélien. Considérons désormais l'application

$$\begin{aligned} \psi : G &\longrightarrow G \\ g &\mapsto g^{-1}. \end{aligned}$$

Cette application est un "anti-morphisme". Soit $(g,h) \in G^2, \psi(gh) = (gh)^{-1} = h^{-1}g^{-1} = \psi(h)\psi(g) \neq \psi(g)\psi(h)$. Or, on a montré que G etait abélien, donc ψ est un automorphisme de groupe (par unicité de l'inverse dans un groupe). Donc $\forall g \in G, g = g^{-1}$ ou de façon équivalente, tout élément est au plus d'ordre 2. Comme on a montré que G était abélien, il suit par la classification des groupes abéliens finis que G est isomorphe à un $(\mathbb{Z}/2\mathbb{Z})^k$, avec $k \in \mathbb{N}^*$. Supposons par l'absurde que $k > 1$. L'application linéaire qui envoie la base canonique $(e_1, e_2, \ldots, e_k)$ de $(\mathbb{Z}/2\mathbb{Z})^k$ (en tant $\mathbb{F}_2$ espace vectoriel) sur la base $(e_2, e_1, \ldots, e_k)$ est un morphisme de groupes, non trivial car différent de l'identité. Donc pour $k > 1$, Aut$(G) \neq$ Id d'où $k = 1$. □

5.3 Le groupe multiplicatif d'un corps fini est cyclique

Références: Serre, Cours d'arithmétique
Difficulté: Facile

Lemme 14. $n = \sum_{d|n} \varphi(d)$.

Démonstration. Soit d un diviseur de n. Il existe un unique sous groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre, de plus il est cyclique et ses générateurs sont au nombre de $\varphi(d)$. Ainsi, chaque élément de $\mathbb{Z}/n\mathbb{Z}$ génère un sous groupe, ce qui conclut. □

Lemme 15. *Soit G un groupe fini d'ordre n. On suppose que pour tout diviseur d de n, l'ensemble $\{x \in G,\ x^d = 1\}$ a cardinal au plus d. Alors H est cyclique.*

Démonstration. Soit d un diviseur de n. Notons $E_d = \{x \in G,\ x^d = 1\}$. Supposons qu'il existe un élément x d'ordre d. Alors le sous groupe engendré par x a cardinal d et par hypothèse, s'il existe $y \in G, y^d = 1$, alors $y \in H_d := \langle x \rangle$. De plus, le nombre de générateur de H est $\varphi(d)$. Donc finalement, $|E_d| \in \{0, d\}$, selon s'il existe un élément d'ordre d ou non. Or chaque élément de G engendre au moins un des H_d. Ainsi, si pour un certain diviseur d de n, il n'existait pas d'élément d'ordre d, on aurait alors

$$n = |G| = \sum_{d|n} |H_d| < \sum_{d|n} \phi(d) = n.$$

Absurde, donc il existe un élément d'ordre d pour tout diviseur d de n. Or n divise n ce qui conclut. □

Ainsi, si d est un diviseur du cardinal du sous groupe multiplicatif d'un corps et H et H' sont deux groupes d'ordre d. Alors

$$\forall x \in H \cup H', \quad x^d = 1.$$

Le polynôme $X^d - 1$ ayant au plus d racines sur un corps, on a nécessairement que $|H \cup H'| = d$ donc $H = H'$

Remarque 5.1. Résultat très très classique aux multiples applications. Cette preuve là est assez courte, mais en développant le fait que les $\mathbb{Z}/n\mathbb{Z}$ contiennent un unique sous groupe pour chaque diviseur de n, cela peut potentiellement faire un développement.

5.4 Théorème de d'Alembert-Gauss (version Analyse)

Références: Gourdon, Algèbre
Difficulté: Facile

Enoncé 32. *Le corps des nombres complexes est algébriquement clos*

Démonstration. Soit $P \in \mathbb{C}[X]$, que, sans perte de généralité, on peut supposer unitaire. Alors $\exists (a_0, \dots, a_{n-1}) \in \mathbb{C}^n$, $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. En factorisant par X^n, on a aussi
$P = X^n(1 + \frac{a_{n-1}}{X} + \cdots + \frac{a_0}{X^n})$. Donc l'application polynômiale associée à P vérifie

$$\lim_{|z|\to\infty} |P(z)| = +\infty.$$

Donc $\exists M > 0, \forall z \in \mathbb{C}, |z| > M, |P(z)| > |P(0)| + 1$.
En particulier, $\forall z \in B_{(0,M)}, |P(z)| < |P(0)| + 1$. Comme l'application $z \mapsto P(z)$ est polynômiale, en particulier, elle est continue et sa restriction sur la boule de centre 0 et de rayon M est continue sur un compact donc atteint ses bornes, en particulier son minimum, que l'on note z_0. Supposons alors par l'absurde que $P(z_0) \neq 0$. Posons

$$Q(X) = \frac{P(z_0 + X)}{P(z_0)} = \sum_{k=0}^{n} b_k X^k.$$

On a tout de suite $Q(0) = b_0 = 1$ et $b_n \neq 0$. Donc l'ensemble $\{i \in \mathbb{N}, 1 \leq i \leq n, b_i \neq 0\}$ est non vide. Notons k l'infimum de cet ensemble. Ainsi, on peut réecrire

$$Q(z) = 1 + z^k b_k (1 + \varphi(z)), \qquad \varphi(z) \xrightarrow{z\to 0} 0.$$

De plus, l'application $z \mapsto \varphi(z)$ est continue, donc $\exists r > 0, \forall z \in B_{(0,r)}, |\varphi(z)| \leq \frac{1}{2}$.
Ecrivons $b_k = |b_k| e^{i\theta}$. Soient $\rho \in]0, r[$ et $z = \rho e^{\frac{-i(\theta+\pi)}{k}}$. Pour un tel z, $Q(z) = 1 - \rho^k |b_k|[1 + \varphi(z)]$ et par suite,

$$\begin{aligned} |Q(z)| &= \left|1 - \rho^k |b_k| - \rho^k |b_k| \varphi(z)\right| \\ &\leq |1 - \rho^k|\,|b_k| + |b_k|\,|\rho^k \varphi(z)| \\ &\leq |1 - \rho^k|\,|b_k| + \frac{1}{2}|b_k|\,\rho^k. \end{aligned}$$

Quitte à diminuer ρ, on peut supposer $1 - |b_k|\rho^k > 0$, d'où $|Q(z)| \leq 1 - \frac{1}{2}\rho^k |b_k| < 1$. C'est absurde car $|Q(z)| < 1$ s'écrit de façon équivalente $|P(z + z_0)| < |P(z_0)|$, donc $P(z_0) = 0$. □

5.5 Calcul de la dimension d'un espace vectoriel et problème de dénombrement

Enoncé 33. *Soient $\mathbb{K}$ un corps, n et d deux entiers positifs, et $\mathbb{K}[X_1,\dots,X_n]_d$ le $\mathbb{K}$-espace vectoriel des polynômes en n variables de degré au plus d. Alors la dimensions de cet espace vectoriel est $\binom{n+d}{n}$.*

Démonstration. On va chercher à exhiber une base de cet espace vectoriel et calculer son cardinal. De la même façon que

$$\mathrm{Vect}(\{X \mapsto X^k, 0 \leq k \leq n\})$$

engendrent l'espace vectoriel des polynômes de degré au plus n, ici, $\mathbb{K}[X_1,\dots,X_n]_d$ va être engendré par les monômes

$$X^u = X_1^{u_1}\cdots X_n^{u_n}, \quad \sum u_i \leq d.$$

Clairement, cette famille est génératrice, mais elle est également libre. On est donc ramener à montrer le problème de dénombrement suivant

$$\mathrm{Card}\{(a_1,\dots,a_n)\in\mathbb{N}^n,\ \sum a_i \leq d\} = \binom{n+d}{d}.$$

Supposons pour l'instant que $\sum a_i = d$. Imaginons alors un instant que chaque a_i représente un nombre a_i de boules blanches et qu'entre a_i et a_{i+1}, on introduise une boule noire. Un exemple d'une telle configuration serait alors

$$\underbrace{B,B,\dots,B}_{a_1\text{boules blanches}},N,\underbrace{B,B,\dots,B}_{a_2},N,\cdots,N,\underbrace{B,B,\cdots,B}_{a_n}.$$

Maintenant, il est plutôt clair qu'il y a une bijection entre ces représentations de boules et $\{(a_1,\dots,a_n)\in\mathbb{N}^n,\ \sum a_i = d\}$. Remarquons aussi que l'on a $n-1$ boules noires et $n+d-1$ boules au total. Ainsi, trouver un n-uplet d'entiers positifs dont la somme vaut d revient à choisir $n-1$ parmi $n+d-1$. Par suite,

$$\mathrm{Card}\left(\bigcup_{k=1}^{d}\{(a_1,\dots,a_n)\in\mathbb{N}^n,\ \sum a_i = k\}\right) = \sum_{k=1}^{d+1}\binom{n-2+k}{n-1}$$

Or, par récurrence, et en utilisant la propriété suivante

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1},$$

on obtient

$$\sum_{k=1}^{d+1}\binom{n-2+k}{n-1} = \binom{n+d}{n}.$$

□

5.6 Equivalence des normes en dimension finie

Enoncé 34. *En dimension finie, toutes les normes sont équivalentes.*

Démonstration. Soit E un $\mathbb{K}$-espace vectoriel (ici $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$) de dimension finie, et soit $(e_1, \dots, e_n)$ une base de E. Pour tout $x = \sum x_i e_i$, l'application N_0 qui à x associe $N_0(x) = \sup |x_i|$ est une norme sur E. L'objectif va alors être de montrer que tout norme sur E est équivalente à N_0.
Soit N une norme sur E. Désignant par a le réel $\sum_i N(e_i)$, il vient

$$N(x) = N(\sum x_i e_i) \leq \sum N(x_i e_i) = \sum |x_i| N(e_i) \leq a N_0(x), \quad \forall x \in E.$$

Munissons désormais $\mathbb{K}^n$ de la norme produit $\|(x_1, \dots, x_n)\|_\infty = sup|x_i|$. L'application

$$\begin{aligned} \varphi :(\mathbb{K}^n, \|\cdot\|_\infty) &\to (E, N_0) \\ (x_1, \dots, x_n) &\mapsto \sum x_i e_i. \end{aligned}$$

est clairement une isométrie. Donc $S = \{x \in E,\ N_0(x) = 1\}$ est un compact de (E, N_0) comme image de la sphère unité dans $\mathbb{K}^n$ par φ, une application isométrique donc en particulier continue. De plus, d'après les inégalités précedentes

$$|N(x) - N(y)| \leq N(x - y) \leq a N_0(x - y).$$

Ainsi, N_0 est a-lipschitz donc continue. Et de celà, il vient par le théorème des bornes atteintes que

$$b = \inf_{N_0(x)=1} N(x)$$

existe et est différent de 0 par positivité de la norme. Enfin, on conclut que

$$\forall x \in E, x \neq 0, \quad N(x) = N_0(x)\ N\left(\frac{x}{N_0(x)}\right) \geq b N_0(x).$$

□

5.7 Automorphisme de corps de $\mathbb{R}$

Enoncé 35. *Soit Φ un automorphisme du corps $\mathbb{R}$. Alors $\Phi = Id$*

Démonstration. Une première remarque est que Φ laisse nécessairement invariant $\mathbb{Q}$ puisque si $x \in \mathbb{Q}, x = \frac{a}{b}$, on a

$$\Phi(x) = \Phi(\frac{a}{b}) = \Phi(ab^{-1}) = \Phi(a)\Phi(b)^{-1} = \Phi(\underbrace{1 + \cdots + 1}_{a \text{ fois}})\Phi(\underbrace{1 + \cdots + 1}_{b \text{ fois}})^{-1} = ab^{-1} = x.$$

On aimerait bien conclure en disant que Φ est continue, mais on n'en sait rien ! On va en revanche montrer que Φ est croissante. Soit $x > 0$, alors il existe $a \in \mathbb{R}$ tel que $a^2 = x$. Ainsi

$$\Phi(x) = \Phi(a^2) = \Phi(a)^2 > 0.$$

De là, on tire que si $x \geq y$, $x - y \geq 0$ donc $\Phi(x - y) \geq 0$ donc $\Phi(x) \geq \Phi(y)$. Donc Φ est croissante. Supposons alors par l'absurde que $\Phi \neq \text{Id}$. Soit $x \in \mathbb{R}$. Supposons $\Phi(x) < x$. Soit $\alpha \in \mathbb{Q}$ tel que $\Phi(x) < \alpha < x$. De façon équivalente on a aussi $\Phi(x) < \Phi(a) < x$. Absurde puisque Φ est croissante. Sinon, si $x < \Phi(x)$, il existe $\beta \in \mathbb{Q}$ tel que $x < \Phi(\beta) < \Phi(x)$. Absurde aussi puisque $x < \beta$. Donc $\Phi(x) = x, \ \forall x \in \mathbb{R}$. □

5.8 Lien entre loi exponentielle et géométrique

Enoncé 36. *Soit $X \sim \text{Exp}(\lambda),\ \lambda > 0$. Alors $Y = [X]$ suit une loi géométrique de paramètre $p = 1 - e^{-\lambda}$*

Démonstration. Comme $X \sim \text{Exp}(\lambda),\ X$ a pour densité $f_X(x) = \lambda e^{-\lambda x}$. Ainsi

$$\begin{aligned}\mathbb{P}(Y = y) = \mathbb{P}([X] = y) &= \mathbb{P}(y \leq X < y + 1) \\ &= \int_y^{y+1} \lambda e^{-\lambda x} \mathrm{d}x \\ &= e^{-\lambda y}(1 - e^{-\lambda}) \\ &= \left(e^{-\lambda}\right)^y (1 - e^{-\lambda}) = p(1-p)^y\end{aligned}$$

Donc $Y \sim \text{Geo}(1 - e^{-\lambda})$ □

5.9 Une fonction réelle continue 1-périodique et $\sqrt{2}$ périodique est constante

Démonstration. Commençons par calculer les $c_k(f)$ en tant que fonction 1-périodique

$$\begin{aligned} c_k(f) &= \int_0^1 f(t)e^{-ik2\pi t}\mathrm{d}t \\ &= \int_0^1 f(t+\sqrt{2})e^{-ik2\pi t}\mathrm{d}t \\ &= \int_{\sqrt{2}}^{1+\sqrt{2}} f(s)e^{-ik2\pi(s-\sqrt{2})}\mathrm{d}s \\ &= e^{ik2\pi\sqrt{2}}c_k(f). \end{aligned}$$

Or pour $k \neq 0$, $e^{ik2\pi\sqrt{2}} \neq 1$ puisque $\sqrt{2} \notin \mathbb{Q}$ donc $c_k(f) = 0$ pour tout $k \neq 0$. En particulier, comme la série des $|c_k(f)|$ est convergente, le théorème des séries de Fourier pour les fonctions continues conclut que pour tout $x \in \mathbb{R}$, $S(f)(x) = f(x)$. Or, $S(f)(x) = c_0(f)$ donc f est constante □

5.10 Lemme de Wirtinger

Enoncé 37. *Soit $f : \mathbb{R} \to \mathbb{R}, \mathcal{C}^1, 2\pi$ périodique et de moyenne nulle. Alors*

$$\int_0^{2\pi} |f'(t)| \, \mathrm{d}t \geq \int_0^{2\pi} |f(t)| \, \mathrm{d}t$$

avec égalité si et seulement si $f(t) = A\cos(t) + B\sin(t),\ (A, B) \in \mathbb{R}^2$

Démonstration. Comme f est 2π périodique, sa dérivée aussi, et les coefficients de Fourier vérifient $c_n(f') = inc_n(f)$. De plus la formule de Parseval donne pour $f \in \mathrm{L}^2$

$$\sum_{k\in\mathbb{Z}} |c_k(f)|^2 = \frac{1}{2\pi} \int_0^{2\pi} |f(t)|^2 \mathrm{d}t.$$

On en déduit alors

$$\begin{aligned}
\|f'\|_2^2 &= \sum_{n\in\mathbb{Z}} |c_n(f')|^2 \\
&= \sum_{n\in\mathbb{Z}} n^2 |c_n(f)|^2 \\
&= c_0(f) + \sum_{n\in\mathbb{Z}^*} n^2 |c_n(f)|^2 \\
&= \sum_{n\in\mathbb{Z}^*} n^2 |c_n(f)|^2 \\
&\geq \sum_{n\in\mathbb{Z}^*} |c_n(f)|^2 = \|f\|_2^2.
\end{aligned}$$

puisque par hypothèse sur f, $c_0(f) = 0$ □

5.11 Nombres de Pisot

Soit $\alpha > 1$ un entier algébrique irrationnel (*i.e.* α est annulé par un polynôme P unitaire irréductible à coefficients dans $\mathbb{Z}$). On dit que α est un nombre de Pisot si les autres racines de P sont toutes de module strictement plus petit que 1. Soit $\alpha = \alpha_1$ et $\alpha_i,\ i > 1$ les autres racines de P. On pose alors A_m le nombre

$$A_m = \sum_{k=1}^{n} \alpha_i^m.$$

où n correspond au degré du polynôme P. D'après le théorème sur les polynômes symétriques, on a $A_m \in \mathbb{Z}$. On souhaite maintenant calculer la distance de α^m à $\mathbb{Z}$:

$$\min_{k\in\mathbb{Z}} |\alpha^m - k|.$$

Comme A_m est un entier, on en déduit tout de suite

$$\min_{k\in\mathbb{Z}} |\alpha^m - k| \leq |\alpha^m - A_m| \leq |\alpha_2|^m + \cdots + |\alpha_n|^m.$$

Or, comme les autres racines de P sont de module strictement plus petit que 1, le membre de droite tend vers 0 quand m tend vers l'infini. Cela signifie que α^m est arbitrairement proche d'un entier, et que cet entier est A_m. A titre d'exemple, le nombre d'or φ est un nombre de Pisot puisque $\varphi = \frac{1+\sqrt{5}}{2}$ et sa racine conjuguée est φ^{-1}, qui est bien de module inférieur à 1. Et en effet, $\varphi^{20} = 15126,999934$ qui est, en un certain sens, proche d'un entier. On peut faire plusieurs remarques quant à ces nombres. Déjà, les puissances d'un nombre de Pisot sont très mal équiréparti modulo 1 (alors qu'on sait que la suite des $(\alpha k)_k$ l'est pour tout α irrationnel). Aussi, cela permet d'avoir des approximations rationnelles de nombres irrationnels. Par exemple, le nombre $3+\sqrt{10}$ est un nombre de Pisot et on a

$$(3+\sqrt{10})^6 = 27379 + 8658\sqrt{10} \sim A_6 = 54758$$

Et donc

$$\sqrt{10} \sim \frac{27379}{8658}.$$

Notons qu'on peut améliorer l'approximation de $\sqrt{10}$ autant que l'on souhaite en augmentant la valeur de m. Et pour trouver la constance A_6, il suffit d'appliquer l'algorithme pour exprimer le polynôme $X_1^m + \cdots + X_n^m$ en fonction des polynômes symétriques élémentaires. On peut généraliser cet exemple pour toutes les racines d'entier. Supposons que l'on souhaite une approximation de $\sqrt{n}$. Alors, le nombre de $\lfloor n \rfloor + n$ est un nombre de Pisot, puisque son polynôme minimal est $P = (X - \lfloor n \rfloor)^2 - n$ et l'autre racine de P est $\lfloor n \rfloor - n$ qui est bien de module inférieur à 1. On exprime ensuite $(\lfloor n \rfloor + n)^m$ dans la base $(1, \sqrt{n})$ et on calcule A_m pour le polynôme P.

D'un point de vue culture générale cette fois-ci, l'ensemble S des nombres de Pisot est dénombrable (puisque sous ensemble des nombres algébriques sur $\mathbb{Q}$ qui est dénombrable). Il est également fermé dans $\mathbb{R}$ donc comme il est minoré et fermé, S admet un plus petit élément, appelé "nombre plastique", l'unique racine réelle du polynôme $X^3 - X - 1$.

5.12 Un test pour comparer deux nombres rationnels qui marche presque tout le temps

Supposons qu'à la fin d'un examen, la dernière question consiste à comparer les nombres $\frac{3245743}{894365}$ et $\frac{4598974}{968453}$ et qu'il ne vous reste que quelques secondes pour répondre, sans calculatrice. La méthode que je vous présente pourrait alors bien vous sauvez la vie !

Commencez par additionner 3245745 et 968453, puis séparement 4598974 et 894365. Alors, si le premier résultat est plus grand que le deuxième, il y a 11 chances sur 12 que la première fraction soit plus grande!

Plus généralement, on se donne 4 entiers a, b, c, d entre 1 et N, avec N grand. On souhaite alors comparer $\frac{a}{d}$ et $\frac{c}{b}$, et on va montrer que si $a+b > c+d$, alors la première est plus grande avec probabilité 11/12.

Soit alors

$$P_N = \mathbb{P}\{(a,b,c,d) \in \{1,\dots,N\}^4,\ \frac{a}{d} \triangle \frac{c}{b},\ a+b \triangle c+d,\ \triangle \in \{<,>,=\}\}.$$

P_N est la probabilité que le test fonctionne, on va alors calculer la limite de P_N. Afin de calculer P_N, on va classiquement passer par le complémentaire, noté T_N, *i.e.* les nombres ne vérifiant pas les deux inégalités simultanément. Ainsi, un quadruplet (a,b,c,d) appartenant à T_N vérifie donc, au choix,

$$\begin{aligned} a+b \geq c+d \quad &\text{et} \quad ab < cd \\ a+b > c+d \quad &\text{et} \quad ab \leq cd \\ a+b \leq c+d \quad &\text{et} \quad ab > cd \\ a+b < c+d \quad &\text{et} \quad ab \geq cd. \end{aligned}$$

Les deux premiers cas sont sensiblement identiques aux deux suivants. On va donc s'interesser à ceux-ci. Réecrivant, on obtient alors

$$\frac{ab}{c} \leq d < a+b-c \quad \text{ou} \quad \frac{ab}{c} < d \leq a+b-c.$$

Or, dans les deux cas, on a

$$0 < a+b-c-\frac{ab}{c} = \frac{1}{c}(a-c)(c-b).$$

ce qui donne alors

$$1 \leq b < c < a \leq N \quad \text{ou} \quad 1 \leq a < c < b \leq N.$$

Encore une fois, ces deux cas sont identiques, on considéra alors uniquement le premier. On doit alors compter tous les nombres (a,b,c,d) tels que

$$1 \leq b < c < a \leq N \quad \text{et} \quad \left(\frac{ab}{c} \leq d < a+b-c \quad \text{ou} \quad \frac{ab}{c} < d \leq a+b-c\right). \tag{11}$$

Il restera enfin à multiplier ce cardinal par 4 à la fin. Etant donné (a,b,c), on note $\#\{d\}$ le nombre de d vérifiant 11. Ainsi, on a

$$a+b-c-\frac{ab}{c} < \#\{d\} \leq a+b-c-\frac{ab}{c}+1.$$

En effet, il s'agit juste de la longueur de l'intervalle d'entiers où d peut appartenir. Il vient alors, puisque les cas considérés constituent un quart des événements T_N

$$\sum_{a=3}^{N}\sum_{c=2}^{a-1}\sum_{b=1}^{c-1}\frac{1}{c}(a-c)(c-b) < \frac{T_N}{4} \leq \sum_{a=3}^{N}\sum_{c=2}^{a-1}\sum_{b=1}^{c-1}\left\{\frac{1}{c}(a-c)(c-b)+1\right\}$$

Il reste alors à calculer ces sommes horribles, et on trouve

$$\sum_{a=3}^{N}\sum_{c=2}^{a-1}\sum_{b=1}^{c-1}\frac{1}{c}(a-c)(c-b) = \frac{1}{48}(N-2)(N-1)N(N+1)$$

et

$$\sum_{a=3}^{N}\sum_{c=2}^{a-1}\sum_{b=1}^{c-1}1 = \frac{1}{6}(N-2)(N-1)N.$$

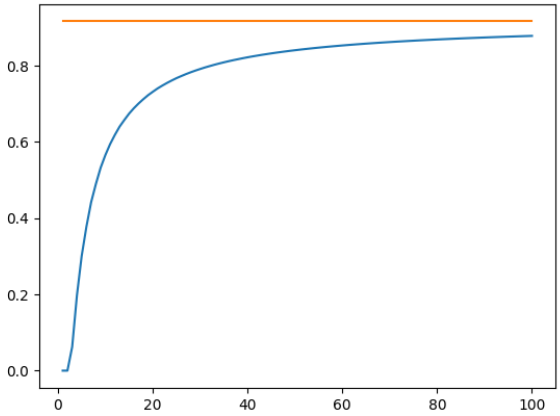
On obtient alors finalement

$$\frac{1}{12}(N-2)(N-1)N(N+1) < T_N \leq \frac{1}{12}(N-2)(N-1)N(N+9).$$

En substituant P_N par $1 - T_N/N^4$, il vient

$$1 - \frac{1}{12}(1-\frac{2}{N})(1-\frac{1}{N})(1+\frac{9}{N}) < P_N \leq 1 - \frac{1}{12}(1-\frac{2}{N})(1-\frac{1}{N})(1+\frac{1}{N}).$$

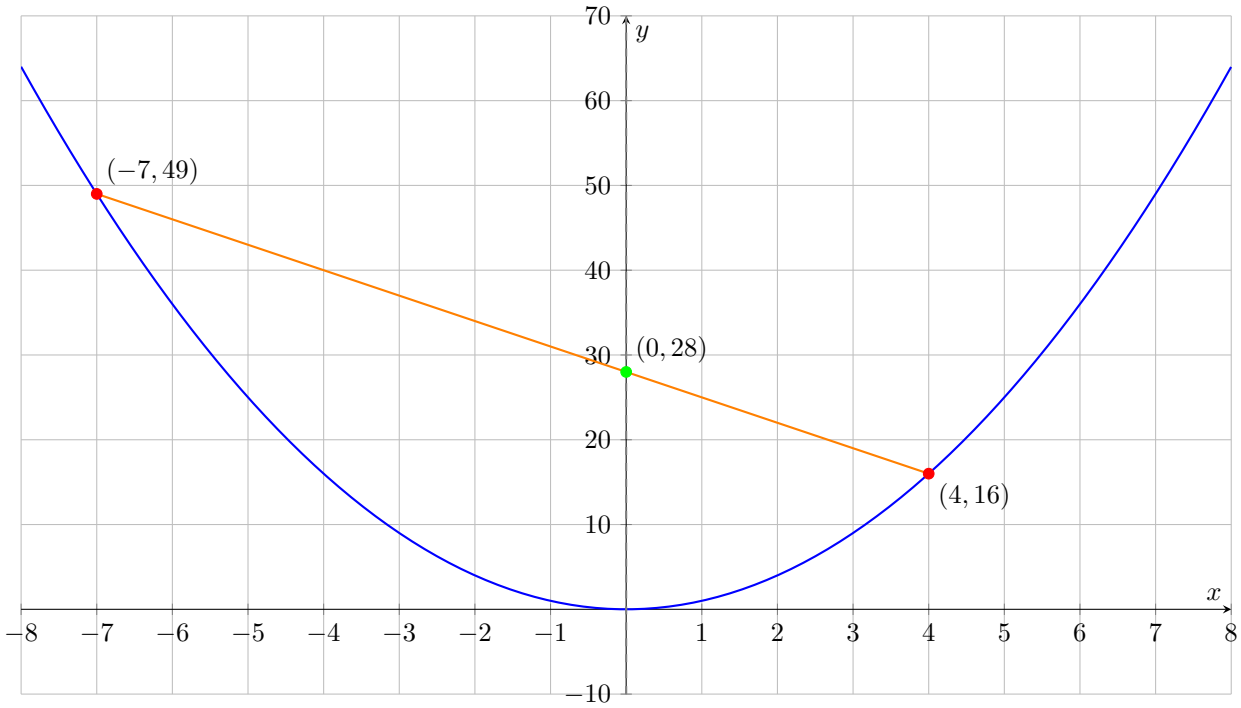
qui tend vers $\frac{11}{12}$ quand N tend vers l'infini. En revanche, on voit que la convergence est assez lente.



Convergence de P_N, pour N de 1 à 100

5.13 Calcul géométrique du produit ab

Que se passe-t-il si étant donné deux nombres positifs a et b, on trace la segment entre $(-a, a^2)$ et (b, b^2) ? Regardons sur le dessin ci-dessous



Le point d'intersection du segment avec la droite d'équation $x = 0$ semble avoir pour coordonnées $(0, ab)$. Montrons ce résultat qui donne un moyen géométrique d'obtenir le produit ab. Soit $(0, y)$ ce point d'intersection, on doit alors résoudre successivement les équations

$$-ta + (1-t)b = 0 \quad \text{puis} \quad ta^2 + (1-t)b^2 = y$$

La première équation donne $t = \frac{b}{a+b}$ et donc

$$y = ta^2 + (1-t)b^2 = \frac{ba^2}{a+b} + \left(1 - \frac{b}{a+b}\right) b^2 = \frac{ba^2}{a+b} + \frac{ab^2}{a+b} = \frac{ab(a+b)}{a+b} = ab.$$

Voilà, ça sert à rien mais c'est joli je trouve.

5.14 Une fonction convexe inattendue

On se propose ici de montrer que l'application

$$\begin{aligned} g \ : \mathrm{S}_n^{++}(\mathbb{R}) &\to \mathbb{R}_+^* \\ A &\mapsto \det(A)^{-\frac{1}{2}}. \end{aligned}$$

est convexe.

Démonstration. L'idée est de considérer l'intégrale

$$I = \int_{\mathbb{R}^n} \mathrm{e}^{-<Ax,x>} \mathrm{d}x.$$

En effet, d'après le théorème spectral, il existe une matrice $P \in \mathrm{O}_n(\mathbb{R})$ tel que $P^{-1}AP = D$, où D est une matrice diagonale avec les valeurs propres de A sur la diagonale. Ainsi,

$$\begin{aligned} I &= \int_{\mathbb{R}^n} \mathrm{e}^{-<Ax,x>} \mathrm{d}x \\ &= \int_{\mathbb{R}^n} \mathrm{e}^{-<PDP^{-1}x,x>} \mathrm{d}x \\ &= \int_{\mathbb{R}^n} \mathrm{e}^{-<DP^{-1}x,P^{-1}x>} \mathrm{d}x. \end{aligned}$$

puisque l'adjoint de P est P^{-1}. On pose alors le changement de variable dans $\mathbb{R}^n, y = P^{-1}x$ dont le déterminant jacobien est égal au déterminant de P qui vaut 1. On a alors

$$\begin{aligned} I &= \int_{\mathbb{R}^n} \mathrm{e}^{-<Dy,y>} \mathrm{d}y \\ &= \int_{\mathbb{R}^n} \mathrm{e}^{-\sum \lambda_j y_j^2} \mathrm{d}y \\ &= \prod_{j=1}^{n} \int_{\mathbb{R}} \mathrm{e}^{-\lambda_j y_j^2} \mathrm{d}y_j. \end{aligned}$$

On reconnaît alors l'intégrale d'une gaussienne, dont on rappelle que

$$\int_{\mathbb{R}} \mathrm{e}^{-ax^2} \mathrm{d}x = \sqrt{\frac{\pi}{a}}.$$

Au final,

$$I = \pi^{\frac{n}{2}} \prod_{j=1}^{n} \frac{1}{\sqrt{\lambda_j}} = \pi^{\frac{n}{2}} \det(A)^{-\frac{1}{2}}.$$

On a donc finalement

$$g(A) = \pi^{-\frac{n}{2}} \int_{\mathbb{R}^n} \mathrm{e}^{-<Ax,x>} \mathrm{d}x.$$

Pour conclure, on prend alors A et $B \in \mathrm{S}_n^{++}(\mathbb{R})$ et $t \in [0,1]$.

$$\begin{aligned} g(tA + (1-t)B) &= \pi^{-\frac{n}{2}} \int_{\mathbb{R}^n} \mathrm{e}^{-<(tA+(1-t)B)x,x>} \mathrm{d}x \\ &= \pi^{-\frac{n}{2}} \int_{\mathbb{R}^n} \mathrm{e}^{-t<Ax,x>} \mathrm{e}^{-(1-t)<Bx,x>} \mathrm{d}x. \end{aligned}$$

On conclut alors par la convexité de l'exponentielle □

6 Tableau recasage

6.1 Recasage Algèbre

	3.1	3.2	3.3	3.4	3.5	3.6	3.7	3.8	3.9	3.10	3.11	3.12	3.13	dev analyse
101		X				X						X	X	
102				X								X		
103									X				X	
104		X				X			X				X	
105						X			X					
106									X					
108									X					
120	X									X	X			
121	X										X			
122														
123	X								X	X	X			
125								X				X		
127								X						
141								X						
142														
144				X						X	X			
148							X				X	X		
149									X					
150							X							
151							X							
152					X		X							
153														4.7
154														
155					X									
156							X							
157					X									4.7
158					X									
159											X			
161														
162														
170										X				
171														
181														
190										X	X			
191											X			

Table 1: Recasage algèbre

6.2 Recasage Analyse

	4.1	4.2	4.3	4.4	4.5	4.6	4.7	4.8	4.9	4.10	4.11	4.12	4.13	4.14	4.15	4.16	dev algèbre
201	X				X				X	X							
203									X								
204								X									
205					X	X											
206							X		X								
208					X	X											
209	X								X								
213	X					X											
214		X											X				
215		X					X						X				
218															X		
219						X	X										
220			X														
221			X														
223												X			X		
224												X			X		
226							X					X					
228			X							X		X					
229							X							X			
230											X	X					
234	X				X												
235					X					X							
236			X	X													
239			X														
241									X	X						X	
243																X	
244											X						
245	X			X												X	
246										X	X						
250	X									X							
253						X								X			
261														X	X	X	
262														X	X		
264														X	X	X	
266														X	X	X	

Table 2: Recasage analyse