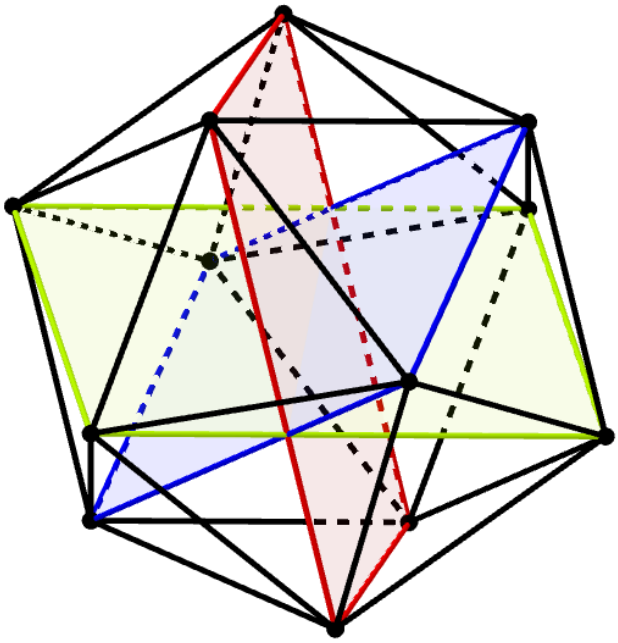
Notes pour l'agrégation de mathématiques

Développements et plans de leçons

Gabriel Pallier



École normale supérieure de Cachan, 2014-2015.

Table des matières

Avant-propos

Ce document rassemble des développements référencés et commentés ainsi que quelques leçons choisies (liste non exhaustive). Les sources, le plus souvent secondaires, font partie de la littérature classique de l'agrégation, d'ouvrages et de revues dédiées à l'enseignement et la culture mathématique. Quand beaucoup de versions existent pour un théorème classique je cite celles qui m'ont été les plus utiles. Rarement, des aspects historiques sont évoqués. Les leçons correspondantes sont signalées, avec la nomenclature du rapport de jury 2014. Il n'y a pas d'ordre, et certains titres sont peu explicites. Le degré de détail des leçons est variable mais, sauf pour quelques unes (signalées par F), moindre que ce qui est attendu à l'oral. Certains plans ne sont qu'esquissés.

Avertissement

Ce texte contient des erreurs. Je reste cependant attentif à ce qu'il y en ait le moins possible. Merci de me les signaler !

Chapitre 0

Développements

1. Théorème fondamental de l'algèbre

Leçons.
126 (ex) Extensions de corps. Exemples et applications.
142 (dev) Algèbre des polynômes à plusieurs indéterminées.
144 (dev) Racines d'un polynôme. Polynômes symétriques élémentaires
Source. Samuel [Sam67, P.53]. Attention coquille, y_j à la place de x_j.
Pré-requis.

(1) Théorème des polynômes symétriques.

(2) L'équation de degré 2 dans $\mathbb{C}$.

(3) Théorème des valeurs intermédiaires.

Théorème 1.1. *Soit $P \in \mathbb{C}[X]$ non constant. Alors P admet une racine dans $\mathbb{C}$.*

Soit $P \in \mathbb{C}[X]$ unitaire. On procède par récurrence sur la valuation 2-adique du degré de P.

(a) Coefficients réels. On introduit un nouveau polynôme $F \in \mathbb{C}[X]$ par

$$F(X) = P(X)\overline{P}(X).$$

Alors $F = \overline{F}$ et donc $F \in \mathbb{R}[X]$ (la sous-$\mathbb{R}$-algèbre des invariants) ; par ailleurs si F possède une racine complexe α, alors α ou $\overline{\alpha}$ est racine de P. On supposera donc P à coefficients réels dans la suite.

(b) Initialisation : degré impair. Soit $P \in \mathbb{R}[X]$ de degré impair, $\tilde{P}$ la fonction polynômiale associée. Alors $\tilde{P}$ est continue sur $\mathbb{R}$, de limite -1 (resp. $+1$) en -1 (resp. $+1$). D'après le théorème des valeurs intermédiaires, $\tilde{P}$ s'annule et P possède une racine réelle.

(c) Un polynôme auxiliaire. Ecrivons $\deg P = d = 2^n q$ avec q impair (une telle écriture est unique). Pour tout $c \in \mathbb{Z}$, posons

$$G_c(X_1,\dots,X_d;X) = \prod_{1 \leqslant i < j \leqslant d} (X - X_i - X_j - cX_iX_j).$$

Alors $G_c \in \mathbb{Z}[X_1,\dots,X_d]^{\mathfrak{S}_d}[X]$. D'après le théorème des polynômes symétriques, on a donc

$$G_c \in \mathbb{Z}[\sigma_1,\dots,\sigma_d][X].$$

En particulier, si $x_1,\dots,x_d$ sont les racines de P (éventuellement non distinctes) dans un corps de décomposition K de P sur $\mathbb{C}$,

$$\begin{aligned} G_c(x_1,\dots,x_d;X) &\in \mathbb{Z}[\sigma_1(x_1,\dots,x_d),\dots,\sigma_d(x_1,\dots,x_d)][X] \\ &= \mathbb{Z}[a_{d-1},\dots,a_0][X] \\ &\subset \mathbb{R}[X]. \end{aligned}$$

(d) Réduction de degré. Le degré en X de G_c est

$$\deg_X G_c = \frac{d(d+1)}{2} = 2^{n-1}q(d+1).$$

Par hypothèse de réccurence, $G_c(x_1, :::, x_d; X)$ possède une racine z dans $\mathbb{C}$, pour tout $c \in \mathbb{Z}$. Il s'agit de l'un des $y_{ij}(c) = x_i + x_j + cx_ix_j$; notons le $y_{i(c)j(c)}(c)$. Puisque $\mathbb{Z}$ est infini, il existe c et c' distincts dans $\mathbb{Z}$ tels que

$$\begin{aligned} i(c) &= i(c') = r \\ j(c) &= j(c') = s. \end{aligned}$$

On sait alors que $y_{rs}(c)$ et $y_{rs}(c')$ sont dans $\mathbb{C}$. Par conséquent, la somme et le produit de x_r et x_s sont dans $\mathbb{C}$. Or x_r et x_s sont racines de

$$X^2 - (x_r + x_s)X + x_rx_s;$$

et tout polynôme de degré 2 à coefficients complexes admet [1] une racine dans $\mathbb{C}$. Conclusion, x_r et x_s sont dans $\mathbb{C}$.

Remarque 1.2. La preuve qu'on présente ici peut être retracée jusqu'à Lagrange en 1772. Voir [Suz06] pour sa place dans l'histoire du théorème fondamental de l'algèbre. La seule objection de Gauss concernait le lieu a priori des racines ; avec le point de vue de l'algèbre moderne ce n'est plus un problème.

Remarque 1.3 (Ariles Remaki). On a utilisé l'axiome du choix (à cause du choix des z_c) si on veut l'éviter on fait simplement varier c dans un ensemble fini assez grand pour appliquer le principe des tiroirs.

Applications du théorème fondamental de l'algèbre. On mentionne les applications directes de l'énoncé « minimaliste » (existence d'une racine)

— (Algèbre linéaire) Soit E un $\mathbb{C}$-espace vectoriel de dimension finie, $u \in L(E)$. Alors u admet un vecteur propre.
— (Géométrie) Soit F un faisceau de quadriques complexe. Alors une quadrique de F au moins est dégénérée.
— (Groupes) $\mathbb{C}^*$ est un groupe divisible (pour tout $Z \in \mathbb{C}^*$, pour tout $n \in \mathbb{N}$, il existe $z \in \mathbb{C}^*$ tel que $Z = z^n$) ; sans requérir l'exponentielle complexe. Ceci permet notamment le lemme de prolongement des caractères.

Autres applications du théorème des polynômes symétriques.

— Dans le lemme de Kronecker (voir le développement 19)
— Polynômes palindromiques (voir le développement 5).
— Soit $f : M_n(\mathbb{C}) \to \mathbb{C}$ une fonction polynômiale telle que $f(AB) = f(BA)$ pour toutes $A; B \in M_n(\mathbb{C})$. Alors f est un polynôme en les coefficients de .

1. En caractéristique 2 rajouter simplement une racine de 1 (i.e. se placer dans le corps de rupture de $X^2 + 1$) suffit pour résoudre toutes les équations du second degré. Attention, la réduction aux coefficients réels du (a) n'est pas susceptible de s'appliquer ici puisqu'elle double le degré.

2. Non-rétraction et point fixe de Brouwer

206: (dev) Points fixes,

207: (dev) Prolongement de fonctions, exemples et applications

209: (dev) Approximation par une suite de polynômes

214: (ex) Inversion locale et fonctions implicites

215: (ex) Applications di□érentiables sur les ouverts de $\mathbb{R}^n$

Source. Gonnord et Tosel [GT98].
Références. Milnor, Rogers [Mil78], [Rog80].
Avertissement. L'ensemble est trop long, il y a de quoi faire deux développements distincts (qui vont naturellement ensemble) : soit la preuve du théorème 2.1 en admettant le lemme de non retraction (plus adapté pour les leçons 206 ou 209), soit la preuve du lemme de non-retraction (alors vu comme un théorème) en suivant la méthode de Milnor-Rogers (lemmes 2.10 et 2.11). Finalement, l'approche du théorème de Brouwer présentée ici est moins élémentaire que la voie combinatoire par le lemme de Sperner [GT98], [AHZ14, p.170], mais elle se case dans plus de leçons.

Théorème 2.1 (Voir aussi le théorème 2.7 pour une variante). *Soit E un espace vectoriel normé réel de dimension finie, B sa boule unité fermé et $f : B \to B$ une fonction continue. Alors, f admet un point fixe.*

Pour la preuve du théorème de Brouwer on s'appuira sur la version suivante du lemme de non rétraction.

Lemme 2.2 (Voir le théorème 2.9 pour une version plus forte). *Soit B la boule unité fermée euclidienne de $\mathbb{R}^n$ et S la sphère unité. Il n'existe pas d'application C^1 de B dans S telle que $f_{|S} = Id_S$.*

Dans toute la preuve, on raisonne par l'absurde en supposant f sans point fixe et on cherche à contredire le lemme de non rétraction.

2.1. 1ère étape : approximation polynômiale.

Lemme 2.3. *Pour tous $\varepsilon > 0$ et $r_2 > 1$ il existe $r_1 < 1$ et $g : B^0(0; r_2) \to B^0(0; r_1)$ de classe C^1 telle que $\sup_{x \in B} |f(x) - g(x)| < \varepsilon$.*

Démonstration. Quitte à changer de norme on peut supposer que la norme est strictement convexe (par exemple, euclidienne) et f se prolonge alors en $\overline{f}$ définie sur $B^0(0; r_2)$ en envoyant $x \in B^0(0; r_2) \setminus B$ sur l'image de sa projection (unique) sur le convexe fermé B. D'après le théorème de Stone et Weierstrass, il existe g polynômiale (en particulier C^1) sur $B^0(0; r_2)$ et telle que $\|g - \overline{f}\| < \varepsilon'$, pour tout ε' (nous verrons plus loin comment fixer ε' en fonction de ε). g est à valeurs dans $B^0(0; 1 + \varepsilon')$: donc $(1 - \varepsilon')g$ est à valeurs dans $B^0\left(0; 1 - \frac{\varepsilon'^2}{2}\right)$ et d'après l'inégalité triangulaire

$$\forall x \in B,\ |(1 - \varepsilon')g(x) - f(x)| \leq \varepsilon' |g(x)| + \varepsilon' - \frac{\varepsilon'^2}{2} + 2\varepsilon'$$

Soit donc $\varepsilon' > 0$ l'unique tel que $\frac{\varepsilon'^2}{2} + 2\varepsilon' = \varepsilon$, $r_1 = 1 - \frac{\varepsilon'}{2}$ et $g = (1 - \varepsilon')g$; le lemme est démontré.

Puisque f n'a pas de point fixe, $\delta(f) = \inf_{x \in B} \|f(x) - x\|$ est strictement positif sur le compact B. Si nous choisissons $\varepsilon < \delta$, l'approximation g à ε près n'aura pas non plus de point fixe, puisque l'inégalité triangulaire implique $\delta(g) \geq \delta(f) - \varepsilon$. On s'est donc ramené à démontrer le théorème de Brouwer pour une fonction C^1 à valeurs dans l'intérieur de B.

2.2. 2ème étape : construction d'une rétraction C^1. Soit g telle que fournie par le lemme précédent, sans point fixe. On suppose la norme euclidienne.

Lemme 2.4. *Pour tout $x \in B$, la demi-droite D_x d'origine $g(x)$ et passant par x (bien définie car $x \neq g(x)$) intersecte la sphère $S(0;1)$ en un unique point, noté $k(x)$. De plus, l'application $x \mapsto k(x)$ est C^1.*

Pour l'existence et l'unicité de $k(x)$, on se place dans le plan vectoriel engendré par x et $g(x)$; puisque $\|g(x)\| \leq r_1 < 1$, l'intersection avec le cercle de rayon 1 est bien définie et unique. Pour le caractère C^1, deux voies se présentent :

2.2.1. *1ère méthode : théorie du discriminant.* Remarquons que le nombre $\lambda(x) = \frac{\|x\|^2 - \langle g(x), x\rangle}{\|x - g(x)\|^2}$ est la solution positive d'une équation de degré 2 dont les coefficients dépendent polynômialement des coordonnées de x et de $g(x)$, donc de manière C^1 des coefficients de x. Or on dispose d'une expression C^1 de la plus grande solution en fonction des coefficients, tant que le coefficient dominant ne s'annule pas et que le discriminant Δ de l'équation est > 0. C'est le cas ici, puisqu'il y a deux solutions distinctes (l'une strictement négative).

2.2.2. *2ère méthode : théorème des fonctions implicites.* Pour le caractère C^1, utilisons le théorème des fonctions implicites : introduisons, pour $t \neq 0$

$$F(x;t) = \|(1-t)g(x) + tx\|^2 - 1$$

F est C^1 au voisinage de x, et

$$\frac{\partial F}{\partial t} = 2\langle (1-t)g(x) + tx; x - g(x)\rangle$$

Si $F(x_0;t_0) = 0$, alors $(1-t)g(x_0) + tx_0 = k(x_0)$. L'annulation de $\frac{\partial F}{\partial t}$ à cette endroit donnerait que $x_0 - g(x_0) \perp k(x_0)$; en particulier, comme $k(x_0)$, x_0 et $g(x_0)$ sont alignés, $g(x_0) \in T_{k(x_0)}S(0;1)$ mais ceci est absurde car $\|g(x_0)\| < 1$. D'après le théorème des fonctions implicites, il existe localement définie sur un voisinage V de x_0, C^1 et telle que $F(x;\lambda(x)) = 0$ pour $x \in V$. Puisque $k(x) = g(x) + \lambda(x)(x - g(x))$, le caractère C^1 de k est démontré.

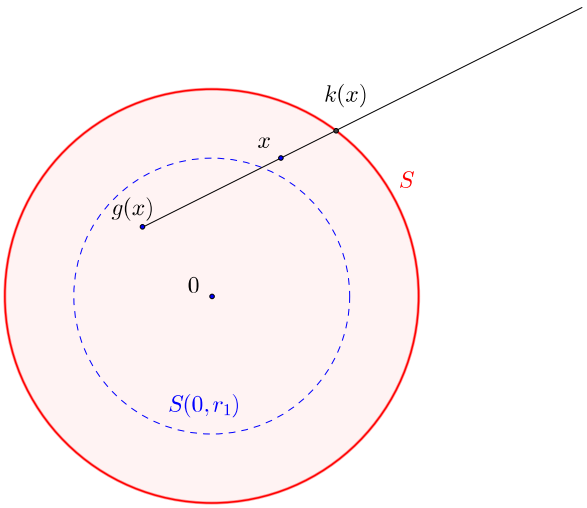


Figure 1. Construction de la rétraction k

2.3. Fin de la preuve. Si $x \in S$, l'unique intersection de D_x avec S est x : donc $k(x) = x$. Nous avons donc construit une rétraction C^1 de B dans S ; ceci est absurde.

Remarque 2.5. Supposons par l'absurde qu'il existe une rétraction $f : B \to S$ seulement supposée continue. D'après le théorème de Brouwer, l'application f admet un point

fixe ; mais ceci est absurde, puisque celui-ci devrait se situer dans l'image S, et $f_{|S}$ est sans point fixe. On a démontré ainsi le lemme de non retraction continu.

Remarque 2.6. En dimension finie, les classes d'homéomorphismes de convexes compacts se réduisent à celles des boules unité fermées. On a donc l'énoncé en apparence plus général :

Théorème 2.7. *Soit C un compact convexe d'un espace vectoriel normé de dimension finie, et $f : C \to C$ une fonction continue. Alors, f admet un point fixe.*

L'avantage de cet énoncé est qu'il se généralise en dimension infinie (c'est le théorème de Schauder), ce qui ne serait pas le cas pour les boules unité fermées.

Application du théorème de Brouwer : le théorème de Perron-Frobenius [GP10, p.66–67].

Théorème 2.8. *Soit $A \in M_n(\mathbb{R})$ dont tous les coefficients $a_{i,j}$ sont positifs. Alors A admet une valeur propre réelle positive.*

Démonstration. Si A n'est pas inversible, 0 est valeur propre ; on supposera donc A inversible dans la suite. Soit H l'hyperplan affine de $\mathbb{R}^n$ d'équation

$$H = \left\{ (x_1, \dots, x_n) \mid \sum_{i=1}^{n} x_i = 1 \right\}.$$

On note H^+ l'intersection de H avec le premier quadrant $Q = \{x_1, \dots, x_n \geq 0\}$. C'est un convexe compact de $\mathbb{R}^n$. Puisque A est à coefficients positifs, le premier quadrant est stable par A. On considère alors la fonction f qui à tout $x \in H^+$ associe

$$f(x) = Ax / \varphi(Ax)$$

où φ est la forme linéaire $e_1^* + \dots + e_n^*$. f est une application continue de H^+ dans H^+. D'après le théorème de Brouwer, elle admet un point fixe v qui est vecteur propre de A.

2.4. Lemme de non-rétraction. Milnor [Mil78] a publié la preuve du lemme suivante qu'il décrit comme « étrange ». Rogers [Rog80] élucide cette preuve, toujours dans le *Monthly*.

Théorème 2.9. *Soit B la boule unité fermée euclidienne de $\mathbb{R}^n$ et S la sphère unité. Il n'existe pas d'application[2] C^1 de B dans S telle que $f_{|S} = Id_S$.*

On raisonne par l'absurde en supposant que f existe.

2.5. Une perturbation de l'identité.

Lemme 2.10. *Pour tout $t \in [0;1]$, $v_t = (1-t)\,Id_B + tf$. Alors, pour t assez petit, v_t réalise un C^1-difféomorphisme de B sur elle-même.*

Démonstration. Par convexité de B, v_t est bien à valeurs dans B pour tout T. De plus, en tant que somme de fonctions C^1, v_t est C_1 et pour tout $x \in B$ nous avons

$$d(v_t)_x = \mathrm{Id} + t\,d(f - \mathrm{Id})_x$$

L'application $d(f - \mathrm{Id})_x$ est continue sur le compact B, elle y est donc bornée (pour une norme quelconque) par $M > 0$. Posons $a = \frac{1}{M+1}$. Alors, pour tout $t \leq a$, nous avons que pour tout $x \in B$, $\mathrm{Id} + t\,d(f - \mathrm{Id})_x$ est inversible. De plus, B étant convexe, l'égalité des accroissements finis donne pour $t \leq a$, $\|v_t(x) - v_t(y)\| \geq \frac{1}{M+1}\|x - y\|$.
Donc v_t est injective ; d'après le théorème d'inversion locale, v_t réalise un C^1-difféomorphisme de B sur son image. Voyons que celle-ci est B. Pour tout $t \leq a$ et $x \in B$ nous avons $\|d(v_t)_x\| \geq \frac{1}{M+1}$. Ainsi, $(v_t)^{-1} : v_t(B) \to B$ est uniformément continue. Par un lemme

2. Rappelons que si $A \subset \mathbb{R}^n$ et $B \subset \mathbb{R}^m$. On écrit $f \in C^1(A;B)$ si $f(A) \subset B$ et s'il existe $U \supset A$ et $\overline{f} : U \to \mathbb{R}^m$ de classe C^1 tels que $\overline{f}_{|A} = f$. Par définition, on pose alors $df = d\overline{f}_{|A}$.

classique, $v_t(B)$ est ouverte[3] et fermée[4] dans B, qui est connexe. On en déduit ce que l'on souhaitait.

2.6. Le lemme de Milnor-Rogers.

Lemme 2.11. *Soit λ la mesure de Lebesgue sur $\mathbb{R}^n$. Alors l'application*

$$\varphi : t \mapsto \int_B \det(dv_t)\, d\lambda$$

est polynomiale.

Démonstration. A $x \in B$ fixé, nous avons $\det((\mathrm{d}v_t)_x) = \det(\mathrm{Id} + t\mathrm{d}(f - \mathrm{Id})_x)$; cette application est polynomiale de degré n, de la forme

$$\det((\mathrm{d}v_t)_x) = \sum_{k=0}^{n} a_k(x)\, t^k.$$

Intégrons sur B contre λ, cela donne

$$\varphi(t) = \sum_{k=0}^{n} \left(\int_B a_k(x)\, (\mathrm{d}x) \right) t^k = \sum_{k=0}^{n} A_k t^k.$$

(c) Fin de la preuve. Pour t assez petit, v_t est un difféomorphisme de B. De plus, par continuité de $t \mapsto v_t$ c'est un difféomorphisme qui préserve l'orientation. Donc

$$\forall t \text{ assez petit}, \quad \lambda(v_t(B)) = \int_B \det(\mathrm{d}v_t)\, \mathrm{d}\lambda = \varphi(t).$$

Mais d'après le premier lemme, $v_t(B) = B$ pour t assez petit de sorte que $\varphi(t)$ est constante sur un intervalle, donc constante partout égale à ω_n volume de B. Mais $v_t(1) = f$, et le rang de $\mathrm{d}f$ est au plus 2 partout (puisque f est à valeurs dans S, $\mathrm{Im}(\mathrm{d}f)_x \subset T_{f(x)}S = x^{\perp}$, donc $\varphi(1) = 0$. C'est une contradiction.

Remarque 2.12. On peut remplacer C^1 par C^k avec $k \in \mathbb{N}^* \cup \{\infty\}$ et conserver la même preuve. Comme noté plus haut, la version C^1 suffit pour démontrer le théorème de Brouwer. En retour, le théorème de Brouwer donne le lemme de non retraction continu.

Remarque 2.13 (Du point fixe de Brouwer à la sphère chevelue). Soit $f : S^{n-1} \to S^{n-1}$ un homéomorphisme de la sphère, $n > 2$. Il découle du théorème de Brouwer que f admet un point fixe (quitte à étendre f à B^n par $\overline{f}(tx) = tf(x)$). Quitte à appliquer cela au flot en petit temps positif d'un champ de vecteurs, on en déduit le théorème de la sphère chevelue : tout champ de vecteur sur la sphère s'annule quelque part.

---

3. Théorème d'inversion locale : f est ouverte (on peut si l'on veut revenir à $\overline{f}$, qui est ouverte sur un voisinage de B)

4. Soit (y_n) une suite de $v_t(B)$ qui converge vers $y \in B$. La suite $x_n = v_t^{-1}(y_n)$ est de Cauchy, donc elle converge vers x dans le complet B. Par continuité, $y = v_t(x)$.

3. Determinant de Smith, application

Leçons.
105 (dev) Groupe des permutations d'un ensemble fini
106 (dev) Groupe linéaire d'un espace vectoriel, sous-groupes de $\mathrm{GL}(E)$
107 (ex) Représentations et caractères d'un groupe fini sur un $\mathbb{C}$-espace vectoriel
150 (dev) Exemples d'actions de groupes sur les espaces de matrices
152 (dev) Déterminant. Applications.
170 (ex) Formes quadratiques sur un espace vectoriel de dimension finie
190 (ex) Méthodes combinatoires, problèmes de dénombrement

Référence. Francinou et al. [FGN14, Algèbre 2]. Voir aussi Mansuy et Mneimné [MM16, 4.6] qui atttribue le théorème 3.1 à Brauer.

Théorème 3.1. *Soient k un corps* de caractéristique nulle *et n un entier naturel non nul. Soient et deux éléments du groupe $\mathfrak{S}_n$, P et P 2 $\mathrm{GL}(n;k)$ les matrices de permutations correspondantes. Alors P et P sont semblables si et seulement si et sont conjuguées dans $\mathfrak{S}_n$.*

Le théorème dit aussi que quand G est cyclique, deux G-ensembles finis sont isomorphes si et seulement si leurs représentations de permutation (obtenues en vectorialisant l'action de G) sont isomorphes.

3.1. L'expression du nombre de cycles de ^{m} en fonction du type cyclique.

Lemme 3.2. *Le nombre de cycles de est la dimension de l'espace $\mathrm{Ker}\,(P \quad I)$.*

Démonstration. Soit $x = \sum x_i e_i$ invariant par P. Alors $P\,(x) = x$ donne que $x_i = x_j$ si $i = {}^m(j)$ pour un certain m, ie si i et j apparaissent dans le même cycle intervenant dans la décomposition de . Réciproquement, si la fonction $i \mapsto x_i$ est constante sur les supports des cycles de , alors x est P-invariant.

Proposition 3.3. *Si l'on écrit $c_\ell(\ )$ le nombre de cycles de longueur ℓ dans , alors le nombre de cycles de ^{m} est*

$$\sum_{\ell=1} \mathrm{pgcd}(\ell; m)\, c_\ell(\ ). \tag{1}$$

Démonstration. Si $_1 \quad _r$ est la décomposition de en produit de cycles disjoints, alors $^m = {}^m_1 \quad {}^m_r$; les ${}^m_i$ se décomposent eux-mêmes en cycles disjoints : si $j \ j = \ell$ alors en écrivant $= (c_0 c_1 \quad c_{\ell-1})$ et en posant $k = \mathrm{pgcd}(\ell; m)$,

$$\begin{aligned} {}^m &= (c_0 c_m \quad c_{\ell-m})\ (c_{m-1} c_{2m-1} \quad c_{\ell-1}) \\ &= \wedge_1 \quad \wedge_k. \end{aligned}$$

où les $\wedge_i$ sont des cycles de longueur $\ell = k$.

En vertu du lemme, si P et P sont semblables alors pour tout $m \in \mathbb{N}$ ^{m} et ^{m} ont même nombre de cycles. Il s'agit de montrer que ceci implique que et ont même type cyclique, i.e. que la matrice intervenant dans l'équation (1) est inversible.

3.2. Déterminant de Smith.

On est ramené à prouver l'inversibilité de la matrice

$$A_n = (\mathrm{pgcd}(i;j))_{1 \leq i;j \leq n}.$$

Lemme 3.4. *Pour tout $n \in \mathbb{N} \setminus \{0\}$,*

$$\det A_n = \prod_{i=1} \varphi(i). \tag{2}$$

Démonstration. Introduisons la matrice d'incidence de la relation de divisibilité : $B = (b_{i;j})$ avec $b_{i;j} = 1_{j|i}$. Il vient

$$\begin{aligned} {}^tB_{i;j} &= \varphi(i)\,1_{i|j} \\ B\,{}^tB_{i;j} &= \sum_{k=1}^{n} 1_{k|i}\,\varphi(k)\,1_{k|j} \\ &= \sum_{k=1}^{n} 1_{k|\mathrm{pgcd}(i;j)}\,\varphi(k) \\ &= \mathrm{pgcd}(i;j)\,; \end{aligned}$$

où l'on a utilisé la formule $\sum_{d|n} \varphi(d) = n$ (φ est la transformée de Möbius de $n \mapsto n$). Par ailleurs B est triangulaire, avec des 1 sur la diagonale, donc

$$\det A_n = (\det B)^2 \det \quad = \det \quad = \varphi(1) \quad \varphi(n)\,.$$

Remarque 3.5. Une manière de « deviner » la relation (2) est de procéder par récurrence. Si p est un nombre premier on obtient (en retranchant p fois la première colonne à la dernière) que $\det A_p = (p \quad 1)\det(A_{p\ 1})$. Le cas général est plus compliqué et fait intervenir une transformée de Möbius.

4. Réciprocité quadratique par les sommes de Gauss

Leçons.

110: (dev) Caractères d'un groupe abélien fini et transformée de Fourier discrète

123: (dev) Corps finis. Applications.

125: (dev) Extensions de corps. Exemples et applications

Source. Serre [Ser70, chapitre I] ou Samuel [Sam67]. Attention aux notations : on prend p et ℓ comme Serre (et non q et p comme Samuel).

Théorème 4.1. *Soient p et ℓ deux nombres premiers impairs distincts. Alors*

$$\left(\frac{p}{\ell}\right)\left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}} \tag{3}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \tag{4}$$

On va approcher à l'aide d'une *somme de Gauss* une racine carrée de ℓ dans une extension adéquate de $\mathbf{F}_p$. Pour tester si la racine obtenue est dans $\mathbf{F}_p$, on lui appliquera l'automorphisme de Frobenius. C'est un peu plus facile pour la loi complémentaire, on commence donc par celle-ci.

4.1. La loi complémentaire. Soit K une extension de décomposition du polynôme $P = X^4 + 1$ sur $\mathbf{F}_p$. Soit ζ une de ses racines dans K. Comme $\zeta^4 = -1$, le nombre $y = \zeta + \zeta^{-1}$ est une racine carrée de 2 dans K. De plus car$K = p$ donc

$$y^p = \zeta^p + \zeta^{-p}.$$

Si $p \equiv 1$ modulo 8, cela entraîne $y^p = y$, donc y est fixe par le Frobenius Frob_p, ce qui revient à a□rmer $y \in \mathbf{F}_p$

Si $p \equiv 3$ modulo 8, $y^p = -y$ et donc $y \in \mathbf{F}_p$.

On remarque par ailleurs que

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{si } p \equiv 1\,(8) \\ -1 & \text{si } p \equiv 3\,(8) \end{cases}$$

Conclusion,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

4.2. Loi de réciprocité quadratique. Soit K une extension de décomposition de $P = X^\ell - 1$ sur $\mathbf{F}_p$, ζ une racine de P dans K. On introduit la somme de Gauss

$$y = \sum_{a \in \mathbf{Z}/\ell\mathbf{Z}} \left(\frac{a}{\ell}\right) \zeta^a.$$

(l'écriture ζ^a avec $a \in \mathbf{Z}/\ell\mathbf{Z}$ a bien un sens, puisque $\zeta^\ell = 1$).

Proposition 4.2. *On a*

$$y^2 = \left(\frac{-1}{\ell}\right)\ell. \tag{5}$$

Démonstration. Calculons

$$y^2 = \sum_{(a;b) \in \mathbf{F}_\ell^{*2}} \left(\frac{ab}{q}\right) \zeta^{a+b} = \sum_{c \in \mathbf{F}_\ell^*} \left(\frac{c}{\ell}\right) \sum_{a \in \mathbf{F}_p} \zeta^{a(1+c)}.$$

On vérifie que

$$\sum_{a \in \mathbf{F}_\ell} \zeta^{a(1+c)} = \begin{cases} \ell & \text{si } c \neq -1 \\ -1 & \text{si } c = -1. \end{cases}$$

Finalement (attention aux signes à cet endroit !)

$$y^2 = \sum_{b \in \mathbf{F}_\ell^\times \setminus \{\pm 1\}} \left(\frac{b}{\ell}\right)(-1) + \frac{1}{\ell}(\ell - 1)$$
$$= \sum_{b \in \mathbf{F}_\ell^\times} \left(\frac{b}{\ell}\right)(-1) - (-1) \frac{1}{\ell} + \frac{1}{\ell}(\ell - 1);$$

le premier terme étant nul car il y a autant de carrés que de non-carrés dans $\mathbf{F}_\ell^\times$, on trouve le résultat escompté.

Or, $y \in \mathbf{F}_p \iff y^p = y$ (puisque $\mathbf{F}_p$ est, dans K, le sous-corps fixé par le Frobenius). Comme nous sommes en caractéristique p,

$$y^p = \sum_{a \in \mathbf{F}_\ell^\times} \left(\frac{a}{\ell}\right) a^p = \sum_{b \in \mathbf{F}_\ell^\times} \left(\frac{bp^{-1}}{\ell}\right) b = \left(\frac{p^{-1}}{\ell}\right) y = \left(\frac{p}{\ell}\right) y.$$

Donc, $\left(\frac{-1}{\ell}\right)\ell$ est un carré modulo p si et seulement si p est un carré modulo ℓ. Finalement

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

Remarque 4.3. Plutôt que de prendre un corps de racine K variant avec ℓ, on peut comme [Ser70] se placer une bonne fois pour toutes dans $\overline{\mathbf{F}_p}$, clôture algébrique de $\mathbf{F}_p$, limite inductive des $\mathbf{F}_{p^{n!}}$. Attention toutefois à bien prendre une racine primitive 8-ième de l'unité dans la preuve de la loi complémentaire. Celle-ci existe bien puisque le polynôme $X^8 - 1$ est séparable sur $\mathbf{F}_p$ (ce ne serait pas le cas de $X^p - 1$, pour prendre un exemple).

Remarque 4.4. Avec la loi de réciprocité quadratique, décider si a est un carré modulo p est un problème algorithmiquement rapide. L'usage du symbole de Jacobi permet même d'éviter d'avoir à décomposer a en facteurs premiers, ce qui ramène le calcul de (a/p) à une complexité comparable à celle de l'algorithme d'Euclide[5]. La recherche effective d'une racine carrée dans $\mathbf{F}_p$ est également de faible complexité une fois que l'on sait calculer des symboles de Legendre (avec l'algorithme de Cippola), contrairement au cas général dans $\mathbf{Z}/n\mathbf{Z}$.

Remarque 4.5. Une autre approche (peut-être plus fidèle à Gauss ?) est de calculer les sommes de Gauss dans $\mathbf{C}$, ce qui oblige à écrire les congruences modulo l'anneau des entiers algébriques $\overline{\mathbf{Z}}$. Toutefois, la relation maîtresse (5) apparaît alors un peu plus naturelle. En effet, si $\zeta = e^{2i\pi/\ell}$, alors

$$y = \sum_{a \in \mathbf{Z}/\ell\mathbf{Z}} \left(\frac{a}{\ell}\right) \zeta^a = \sum_{a \in \mathbf{F}_\ell^\times} \left(\frac{a}{\ell}\right) \zeta^a.$$

Si l'on pose $\chi(a) = \left(\frac{a}{\ell}\right)$ et $\psi(a) = \zeta^a$, alors χ est un caractère multiplicatif (i.e, un élément de $\widehat{\mathbf{F}_p^\times}$) et ψ un caractère additif (i.e., un élément de $\widehat{\mathbf{F}_p}$). La somme de Gauss est (au choix) la transformée de Fourier de $\chi \in L^2(\mathbf{F}_p^\times)$ évaluée en ψ, ou bien encore la transformée de Fourier de $\overline{\chi}$ évaluée en ψ. L'apparition de ℓ dans le carré de y (qui est aussi une transformée de Fourier) s'interprète comme un coefficient de renormalisation. Pour plus de précisions voir le livre de Mérindol [Mer06].

5. Logarithmique d'après un théorème de Lamé.

5. Réciprocité quadratique par le résultant

Leçons.

142: Algèbre des polynômes à plusieurs indéterminées.

143: Résultant. Applications

Source. Mérindol [Mer06, page 389]. Attention aux quelques petites coquilles, il y a plusieurs échanges entre R et S notamment. Voir aussi [Ser70], cf. les commentaires à la fin.

Pré-requis.

(1) La formule du résultant à partir des racines

(2) Le théorème des polynômes symétriques

(3) Les propriétés élémentaires du symbole de Legendre

Théorème 5.1. *Soient p et ℓ deux nombres premiers impairs distincts. Alors*

$$\left(\frac{p}{\ell}\right)\left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}. \tag{6}$$

(a) Un lemme sur les polynômes palindromiques.

Définition 5.2. Soient A un anneau, $P = a_d X^d + \cdots + a_0$ un polynôme de degré d dans $A[X]$. On lui associe son homogénéisé $\tilde{P} \in A[X;Y]$ par

$$\tilde{P}(X;Y) = a_d X^d + a_{d-1} X^{d-1} Y + \cdots + a_1 X Y^{d-1} + a_0 Y^d$$

On dit que P est palindromique si $\tilde{P} \in A[X;Y]^{\mathfrak{S}_{\{X;Y\}}}$. Cela revient à $a_0 = a_d$, $a_1 = a_{d-1}$ etc.

Lemme 5.3. *Si $P \in \mathbb{Z}[X]$ est palindromique de degré d pair, alors il existe $S \in \mathbb{Z}[T]$ de degré $d/2$ tel que*

$$P(X) = X^{d/2} S(X + 1/X).$$

Démonstration. D'après le théorème des polynômes symétriques, l'homogénéisé s'écrit sous la forme

$$\tilde{P}(X;Y) = U(X+Y; XY);$$

où U est de degré $d/2$. Puisque $\tilde{P}$ est homogène de degré pair, et comme les puissances de XY sont de degré pair, il ne peut pas y avoir de puissance impaire de la première variable dans U ; ainsi, il existe V puis W homogènes de degré $d/2$ tels que

$$\tilde{P}(X;Y) = V\left((X+Y)^2; XY\right) = W\left(X^2+Y^2; XY\right).$$

Posons alors $S(X) = W(X;1)$. Dans $\mathbb{Q}(X)$, il vient

$$\begin{aligned} P(X) = \tilde{P}(X;1) = W\left(X^2+1; X\right) &= X^{d/2} W(X + 1/X; 1) \\ &= X^{d/2} S(X + 1/X). \end{aligned}$$

(b) Les polynômes K_p.

Proposition 5.4. *Soit p un nombre premier impair. Le polynôme*

$$P(X) = X^{p-1} + \cdots + X + 1$$

est palindromique. On lui associe V_p tel que $P(X) = X^{(p-1)/2} V_p(X + 1/X)$, unitaire de degré $(p-1)/2$, puis $K_p(Y) = V_p(Y+2)$. Alors

$$K_p(0) = p \tag{7}$$

$$K_p(Y) \equiv Y^{(p-1)/2} \pmod{p}. \tag{8}$$

Démonstration. Pour (7) on calcule directement :

$$K_p(0) = V_p(2) = V_p(1 + 1=1) = p:$$

Pour (8) remarquons que modulo p, d'après le petit théorème de Fermat

$$X^{p\ 1} + \quad + 1 \quad \frac{X^p \quad 1}{X \quad 1} \quad \frac{(X \quad 1)^p}{X \quad 1} \quad (X \quad 1)^{p\ 1};$$

d'où $V_p(X + 1=X) \quad X^{\frac{p\ 1}{2}}(X \quad 1)^{p\ 1} \quad \left[\frac{(X\ 1)^2}{X}\right]^{\frac{p\ 1}{2}} \quad X \quad 2 + X^{\ 1}{}^{\frac{p\ 1}{2}}$, puis $K_p(Y)$ $Y^{\frac{p\ 1}{2}}$.

(c) Loi de réciprocité quadratique.

Proposition 5.5. *Soient p et $\grave{}$ premiers, impairs, distincts. Alors*

$$\left(\frac{\grave{}}{p}\right) = \mathrm{Res}(K_p; K_{\grave{}}): \tag{9}$$

Démonstration. Déjà, $\mathrm{Res}(K_p; K_{\grave{}})$ est dans Z. Soit r un nombre premier qui le divise. Alors les réductions $\overline{K_p}$ et $\overline{K_{\grave{}}}$ modulo r ont une racine commune dans une extension K de $\mathbb{F}_r$. Si L est un corps de décomposition de $T^2 \quad 2T + 1$ sur K, et x une racine de ce polynôme, alors $x + x^{\ 1} \quad 2 =$. Etant données les définitions de K_p et $K_{\grave{}}$, x est racine de $X^p \quad 1$ et $X^{\grave{}} \quad 1$, ce qui est absurde. Donc $\mathrm{Res}(K_p; K_{\grave{}})$ est dans $f \quad 1g$.

Ensuite, on utilise (8) puis (7) de la proposition précédente pour obtenir modulo p

$$\mathrm{Res}(K_p; K_{\grave{}}) \quad \mathrm{Res}\left(Y^{\frac{p\ 1}{2}}; K_q\right) \quad \mathrm{Res}(Y; K_q)^{\frac{p\ 1}{2}}$$

$$K_{\grave{}}(0)^{\frac{p\ 1}{2}}$$

$$\grave{}^{\frac{p\ 1}{2}}:$$

Puisque $\mathrm{Res}(K_p; K_{\grave{}}) = \quad 1$, ceci conclut.

Finalement,

$$\left(\frac{\grave{}}{p}\right) = \mathrm{Res}(K_p; K_{\grave{}}) = \quad (\ 1)^{\frac{\grave{}\ 1}{2}\frac{p\ 1}{2}}\,\mathrm{Res}(K_{\grave{}}; K_p)$$

$$= \quad (\ 1)^{\frac{\grave{}\ 1}{2}\frac{p\ 1}{2}} \quad \left(\frac{\grave{}}{p}\right) :$$

Remarque 5.6. Une grande-aïlleule de cette preuve a été publiée (en français) par Gotthold Eisenstein en 1845 au journal de Crelle [Eis45, p.179] et elle est reprise dans le cours de Serre [Ser70, I, Appendice]. Un calcul montre que le polynôme K_p se scinde sur R et

$$K_p(Y) = \prod_{k=1}^{(p\ 1)=2} \left(Y + 4\sin^2\frac{k}{p}\right);$$

d'où l'on déduit

$$\left(\frac{\grave{}}{p}\right) = 4^{\frac{\grave{}\ 1}{2}\frac{p\ 1}{2}} \prod_{j=1}^{(p\ 1)=2}\prod_{k=1}^{(\grave{}\ 1)=2} \sin^2\frac{k}{\grave{}} \quad \sin^2\frac{k}{p} :$$

La loi de réciprocité quadratique est alors visible sur le produit de droite. Eisenstein décrit sa méthode comme une élimination, opération d'ordre algébrique, ce qui explique le titre « Application de l'Algèbre à l'Arithmétique transcendante ». Il l'applique aux résidus biquadratiques. Voici comment Eisenstein décrit sa preuve : « *Etant proposées deux équations algébriques quelconques, on pourra en éliminer la quantité inconnue x de deux manières di érentes, soit en mettant dans la seconde à la place de x sa valeur tirée de la première, soit en mettant dans la première à la place de x sa valeur tirée de la seconde. Nous ferons voir que les lois de réciprocité pour les résidus quadratiques, cubique et biquadratique [..]*

ne sont que l'interprétation arithmétique du simple fait algébrique dont nous venons de parler. ».

6. Théorème de Stone-Weierstrass

Leçons :

201: Espaces de fonctions

202: Exemples de parties denses et applications

Référence. Hirsch et Lacombe [HL99].

Théorème 6.1. *Soit K un métrique compact. L'algèbre de Banach $C(K;\mathbb{R})$ est munie de la norme uniforme et on se donne A une sous-algèbre. On suppose que pour tous x et y distincts dans K et pour tous $u;v \in \mathbb{R}$ il existe $f \in A$ telle que*[6]

$$\begin{aligned} f(x) &= u \\ f(y) &= v \end{aligned}$$

Alors, A est dense dans $C(K;\mathbb{R})$.

La preuve procède en deux étapes : tout d'abord on montre un cas particulier qui entraîne le fait que que $\overline{A}$ est réticulée, ie

$$f;g \in A \implies \max(f;g);\min(f;g) \in \overline{A}$$

Ensuite on utilise cette propriété pour montrer le théorème, en deux temps.

(a) Un premier lemme.

Lemme 6.2. *La suite de fonctions polynômiale définies par*

$$P_0 = 0;\ P_{n+1}(x) = x + \frac{1}{2}\left(x - P_n(x)^2\right) :$$

converge uniformément vers $r : x \mapsto \sqrt{x}$ sur $[0;1]$

Démonstration. D'après le théorème de Dini, il suffit de montrer que P_n est une suite croissante qui converge simplement vers r sur $[0;1]$. Pour tout $x \in [0;1]$, montrons par récurrence la propostion

$$P_n(x) \leq r(x)$$

C'est vérifié pour $n = 0$; sous l'hypothèse de récurrence il s'agit donc de montrer

$$\frac{1}{2}\left(x - P_n(x)^2\right) \leq \sqrt{x} - P_n(x)$$

ce qui garantira le rang $n+1$.

$$\begin{aligned} \frac{1}{2}\left(x - P_n(x)^2\right) &= \frac{1}{2}\left(\sqrt{x} - P_n(x)\right)\left(\sqrt{x} + P_n(x)\right) \\ &\leq \frac{1}{2}\left(\sqrt{x} - P_n(x)\right)\left(\sqrt{x} + \sqrt{x}\right) \\ &\leq \sqrt{x} - P_n(x) \end{aligned}$$

(la dernière ligne vient de $\sqrt{x} \leq 1$).

(b) Le min et le max.

Proposition 6.3. *Si f et g sont dans A, alors $\max(f;g)$ et $\min(f;g)$ sont dans $\overline{A}$*

Démonstration. Puisque

$$\begin{aligned} \max(f;g) &= \frac{1}{2}(f + g + |f - g|) \\ \min(f;g) &= -\max(-f;-g) \end{aligned}$$

on est ramené à montrer que $f \in A \implies |f| \in \overline{A}$. Soit donc $f \in A$; f est continue sur le compact K donc bornée par R. Remarquons que comme A est une algèbre qui contient les

6. On peut montrer que cette condition équivaut à ce que A soit unifère et séparante, ie pour tous $x \neq y$ il existe f telle que $f(x) \neq f(y)$

constantes, $P(f)$ est dans A pour tout polynôme P. En particulier, on considère la suite de fonctions

$$x \mapsto R \, P_n \left(f(x)^2 / R^2 \right)$$

Comme f^2/R^2 est à valeurs dans $[0;1]$, d'après le lemme précédent cette suite de fonctions converge uniformément vers $|f|$ sur K.

(c) Preuve du théorème. Soit $\varepsilon > 0$ et $f \in C$. On cherche d'abord à approcher f inférieurement. Fixons $x \in K$, commençons par montrer qu'il existe $f_x \in \overline{A}$ telle que

$$f_x(x) = f(x)$$
$$f_x < f + \varepsilon$$

Pour tout $y \in K$, il existe $f_{x;y} \in A$ telle que $f_{x;y}(x) = f(x)$ et $f_{x;y}(y) = f(y)$. Posons

$$\omega_y = \{ f_{x;y} < f + \varepsilon \}$$

Alors ω_y contient y et c'est un ouvert, donc

$$K = \bigcup_{y \in K} \omega_y$$

De ce recouvrement, on peut extraire un sous-recouvrement fini par $\omega_{y_1}, \ldots, \omega_{y_N}$. On pose alors

$$f_x = \min_{k=1}^{N} f_{x;y_k}$$

D'après la proposition précédente, $f_x \in \overline{A}$ et comme les ω_{y_k} recouvrent K, $f_x < f + \varepsilon$.

Remarque 6.4. La méthode itérative du début fonctionne aussi très bien pour rechercher une racine carrée de matrice symétrique définie positive (concrètement, pour la décomposition polaire par exemple).

Applications du théorème de Stone-Weierstrass.

(1) Soit K métrique compact. Alors $C(K)$ est séparable.

(2) Dans la théorie des séries de Fourier : Version « uniforme » du théorème de Féjer ; une formule de Plancherel faible (dans $L^2 \setminus C(\mathbb{T})$) suffisante pour les applications à l'analyse complexe, par exemple le principe du maximum.

(3) Passage du théorème de Brouwer C^1 au théorème de Brouwer continu.

7. Ellipsoïde de John, applications

Leçons.

150: (ex) Exemples d'actions de groupes sur les espaces de matrices (ici la congruence)

158: (dev) Matrices symétriques réelles, matrices hermitiennes

160: (ex) Endomorphismes remarquables d'un espace euclidien

171: (dev) Formes quadratiques réelles

181: (dev) Barycentres dans un espace a□ne réel de dimension finie, convexité. Applications.

203: (ex) Utilisation de la notion de compacité

219: (ex) Extremums : existence, caractérisation, recherche

Sources possibles. [FGN14, Algèbre 3, 3.31, 3.38]

Avertissement. Développement long. On doit donc admettre par exemple la proposition 7.2 qui serait immédiate avec le formalisme de l'algèbre extérieure.

Pré-requis. Un théorème de réduction simultanée de deux formes quadratiques, par exemple dans le Ramis-et-Deschamps [RDO88, Algèbre 2, 1.3.4].

Théorème 7.1. *Soit E un espace euclidien. Soit K une partie relativement compacte de E dont 0 est un point intérieur. Il existe un unique ellipsoïde plein de volume minimal contenant K.*

On désigne par λ la mesure de Lebesgue sur E normalisée pour correspondre à la forme volume de la structure euclidienne.

(a) Volume des ellipsoïdes. Soit $q : E \to \mathbb{R}$ une forme quadratique définie positive ; on lui attache un unique ellipsoïde

$$E_q = \{x \in E \mid q(x) \leq 1\}$$

Il s'agit d'une partie mesurable de E ; on note $V_q = \int_E 1_{E_q} d\lambda$ son volume. $q \mapsto E_q$ déinit une bijection entre l'espace $Q^{++}(E)$ des formes quadratiques définies positives sur E et l'ensemble des ellipsoïdes. Pour tout $q \in Q(E)$, on note $D(q)$ le déterminant d'une matrice de q dans une base orthonormée de E.

Proposition 7.2. *Si q_0 est la forme euclidienne standard de E, alors*[7]

$$V_q = \frac{1}{\sqrt{D(q)}} V_{q_0}. \tag{10}$$

Démonstration. D'après le théorème spectral il existe B une base orthonormée de E telle que si $(x_1, \dots, x_n)$ sont les formes coordonnées de B, on peut écrire $q = \sum_{i=1}^n a_i x_i^2$ avec les $a_i > 0$, et $D(q) = a_1 \cdots a_n$. Puisque B est orthonormée,

$$V_q = \int_{\mathbb{R}^n} 1_{[0;1]}(a_1 x_1^2 + \cdots + a_n x_n^2)\, dx_1 \cdots dx_n.$$

Faisant le changement de variables $y_i = \sqrt{a_i} x_i$, de jacobien $J = \prod_i \sqrt{a_i}$, on trouve

$$V_q = \frac{1}{\sqrt{a_1 \cdots a_n}} \int_{\mathbb{R}^n} 1_{[0;1]}(y_1^2 + \cdots + y_n^2)\, dx_1 \cdots dx_n = \frac{1}{\sqrt{D(q)}} V_{q_0}.$$

7. On ne précise pas V_{q_0}, ce n'est pas utile. Voir cependant la remarque 7.6.

(b) Existence : Compacité. On norme $Q(E)$par $N(q) = \sup_{q_0(x)=1} jq(x)j$. Puis on pose

$$A = \{ q \in Q^+(E) \mid K \quad E_q = \{ q \in Q^+(E) \mid \forall x \in K; q(x) \leq 1 \} :$$

A est borné: 0 est intérieur à K, il existe donc > 0 tel que $B(0;) \quad K$. Ainsi, $q \in A \Rightarrow N(q) \leq 1= .$

A est convexe, fermé dans $Q(E)$: Puisque 0 est intérieur, on a $q > 0$ sur $K \Rightarrow q \in Q^+(E)$ de sorte que $A = \{q \in Q^+(E) \mid \forall x \in K; q(x) \in [0;1]\}$. Il s'ensuit que A est convexe et fermé (en tant qu'intersection de convexes fermés).

A est non vide: Puisque K est relativement compacte, elle est bornée dans E. Donc $tq_0 \in A$, pour t assez petit.

Conclusion: Etant donnés $Q(E)$ est un espace vectoriel normé de dimension finie, et A une partie fermée et bornée, A est compacte, non vide, et la fonction $D : A \to \mathbb{R}$ atteint sa borne supérieure sur A en un certain q. E_q est alors un ellipsoïde de volume minimal, contenant K.

(c) Unicité : Convexité.

Lemme 7.3. *Soient q et q' dans $Q^{++}(E)$. Alors pour tout $\in [0;1]$ on a*

$$D((1 \quad)q + \quad q') > D(q)^1 \quad D(q') \tag{11}$$

Avec égalité ssi $q = q'$.

Démonstration. D'après le théorème de réduction simultanée, il existe une base B_2 de E qui est orthonormée pour E et orthogonale pour q' ; autrement dit q a pour matrice I_n et q', $D = \mathrm{diag}(d_1;:::d_n)$ avec les $d_i > 0$. Puisque l'inégalité 11 à montrer est homogène, on peut se contenter de calculer les déterminants dans la base B (bien qu'elle ne soit pas forcément orthonormée) soit à montrer :

$$\det((1 \quad)I_n + \quad D) > (\det D) \quad :$$

Quitte à prendre les logarithme, on se ramène à montrer

$$\sum_{i=1}^{n} \ln((1 \quad) + \quad d_i) > \quad \ln d_i :$$

Il s'agit simplement de l'inégalité de concavité pour le log entre 1 et d_i. Le cas d'égalité est celui de $d_i = 1$ pour tout i, c'est-à-dire $q = q'$.

Si maintenant $q \neq q'$ dans A sont telles que $D(q) = D(q') = \max_{q \in A \setminus Q^{++}(E)} D$, alors posons $q'' = (q + q')=2$. Comme A est convexe, q'' est dans A et d'après le cas d'inégalité strcte de 11, $D(q'') > D(q)$, ce qui serait absurde.

(d) Une application : forme quadratique invariante. Le résultat précédent joue un rôle fondamental, par exemple dans la théorie des représentations des groupes topologiques compacts (il assure la complète réductibilité) :

Théorème 7.4. *Soit E un espace vectoriel réel de dimension finie, G un sous-groupe compact de $\mathrm{GL}(E)$. Il existe une forme quadratique q définie positive sur E telle que*

$$G \quad O(q) :$$

Démonstration. Donnons une preuve dans le langage des actions de groupes[8]. Soit R l'ensemble des parties de E relativement compactes contenant 0 dans leur intérieur. On dispose d'une action naturelle de G sur E ; celle-ci induit deux actions de G (à gauche et à droite, respectivement) sur $P(E)$ et $F(E;\mathbb{R})$, puis par restriction :

$$\begin{aligned} G \ y \ R \quad & g:K = g(K) \\ Q(E) \ x \ G \quad & (q:g)(x) = q(g(x)) \end{aligned}$$

8. Autre exemple de ce précepte : $\mathbf{SL}(2;\mathbf{Z})$ agit à droite sur les formes quadratiques binaires entières de discriminant < 0, et à gauche sur $\mathbf{H}$; action qui se restreint pour les imaginaires quadratiques, à l'action équivariante sur les racines de la forme deshomogénéisée.

On peut transformer la seconde action en une action à gauche en posant $g{:}q(x) = q\ g^{-1}(x)$. On dispose alors d'un morphisme de G-ensembles $R \to Q(E)$ qui est la propriété de John-Loewner. On cherche un point stable de la 2e action, pour ceci on en cherche un dans le G-ensemble R. C'est ce qui conduit à considérer

$$K_0 = G{:}B = \{g(x) \mid g \in G,\ x \in B\}{:}$$

K est compacte en tant qu'image continue du compact $G \times B$. De plus, 0 est intérieur : on se donne $g \in G$ quelconque, $g{:}B$ contient une boule ouverte centrée en 0. Ainsi $K_0 \in R$ et c'est un point fixe pour la première action : donc si q est la forme quadratique de l'ellipsoïde E_q, q est G-invariante.

Remarque 7.5. On se demande à quoi ressemble cet ellipsoïde, par exemple, si K est un carré ou un triangle équilatéral plein dans $\mathbf{R}^2$, symétrique par rapport à 0. Si E_q est l'ellipsoïde de John-Loewner dans ce cas, par unicité, le groupe des isométries de $\mathbf{R}^2$ laissant stable E_q contient le groupe des isométries de K, qui est plus grand que le groupe des isométries générique d'une conique : E_q est un disque dont la frontière passe par les sommets.

Remarque 7.6 (Au sujet de V_{q_0}). Bien que cela ne soit pas essentiel pour ce qui précède, le « vrai » volume d'une boule euclidienne par rapport à la mesure de Lebesgue standard λ^n est

$$V_n = \frac{2\ \pi^{n/2}}{n\ \Gamma(n/2)} \tag{12}$$

Pour démontrer (12) le manière classique est de calculer de deux manières différentes l'intégrale

$$I_n = \int_{\mathbf{R}^n} e^{-x_1^2 - \cdots - x_n^2}\, dx_1 \cdots dx_n :$$

à l'aide du théorème de Fubini-Tonelli d'une part, à l'aide du changement de variables $r^2 = x_1^2 + \cdots + x_n^2$ d'autre part. En particulier,

$$\frac{V_{n+2}}{V_n} = \frac{n}{n+2}\,\frac{\Gamma(n/2)}{\Gamma(n/2+1)} = \frac{2}{n+2}$$

d'après l'équation fonctionnelle de la fonction Γ. Ceci implique que V_n est maximal pour $n = 5$ ou 6 (en fait $n = 5$) et décroît ensuite ; par ailleurs

$$\lim_{n \to +\infty} V_n = 0{:}$$

En particulier, l'ellipsoïde de John-Loewner du cube $[-1/2; 1/2]^n$ dans $\mathbf{R}^n$ voit son diamètre tendre vers... l'infini (!) quand n grandit.

Remarque au sujet de l'orthogonalisation simultanée de deux formes bilinéaires symétriques (ou quadratiques). Le théorème principal est le suivant

Théorème 7.7. *Soit $(E; \varphi)$ un espace quadratique (ceci suppose φ non dégénérée) de dimension finie et ψ une forme bilinéaire symétrique. On note d_ψ (resp. d_φ) l'application $E \to E^*$ associée à ψ (resp. à φ). Alors il existe une base de E orthogonale pour φ et ψ si et seulement si $u = d_\varphi^{-1} d_\psi$ est diagonalisable.*

Remarque 7.8. d_φ est inversible (φ est non dégénérée) mais ce n'est pas le cas de d_ψ a priori. Noter aussi que u est autoadjoint pour φ.

En corollaire, il découle du théorème spectral et du précédent théorème que si E un espace vectoriel réel, φ et ψ bilinéaires sur E avec φ est définie positive, alors il existe une base orthonormale pour φ, orthogonale pour ψ. On retrouve aussi que si k est quadratiquement clos et u diagonalisable, il existe une base à la fois orthonormale pour φ et orthogonale pour ψ.

8. Théorème de la base de Burnside

Leçons.

101: Exemples de sous-groupes distingués et de groupes quotient. Applications.

104: Groupes finis. Exemples et applications.

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

151: Dimension d'un espace vectoriel

Source. M. Hall, [Hal76, p. 175]. Je dois ce développement à Ariles Remaki.

Théorème 8.1. *Soit P un p-groupe fini et D son sous-groupe de Frattini. On pose $r > 1$ l'entier naturel tel que P/D est d'ordre p^r. Alors*
(i) Toute famille génératrice de P est de cardinal au moins r.
(ii) De toute famille génératrice de P on peut extraire une sous-famille génératrice de cardinal r.

(a) Croissance des normalisateurs.

Lemme 8.2. *Soit M un sous-groupe maximal de P. Alors M est normal et d'indice p dans P.*

Démonstration. On fait agir M sur P/M par translation à gauche. L'équation aux classes modulo p donne

$$0 \quad jP/Mj \quad (P/M)^M \quad (p);$$

où $(P/M)^M$ est l'ensemble des classes fixées par cette action. En particulier, $M \in (P/M)^M$ donc $(P/M)^M > p > 1$. Or $gM \in (P/M)^M$ ssi pour tout m dans M, $mgM = gM$; soit encors $g^{-1}mg \in M$, i.e. $g \in \mathrm{N}_P(M)$. Donc

$$\mathrm{N}_P(M) = jMj \quad (P/M)^M > jMj:$$

Par maximalité[9] de M, $\mathrm{N}_P(M)$ est égal à M ou P. D'après la formule précédente $\mathrm{N}_P(M) = P$ et $M \neq P$. Le quotient P/M est un p-groupe sans sous-groupe propre (toujours par maximalité de M), c'est donc $\mathbb{Z}/p\mathbb{Z}$.

(b) Vectorialisons $A = P/D$. Rappelons que par définition D est l'intersection des sous-groupes maximaux de P.

Proposition 8.3. *D contient toutes les puissances p-ièmes et les commutateurs de P. En d'autre termes A est un groupe abélien p-élémentaire.*

Démonstration. Pour tout M sous-groupe maximal de P, le quotient P/M est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Ceci entraîne que pour tout g dans G, g^p est inclus dans D. En outre on a un morphisme (avec $\mathrm{M}(P)$ l'ensemble des sous-groupes maximaux de P)

$$\begin{array}{ccc} P & \to & \prod_{M \in \mathrm{M}(P)} (P/M) \\ g & \mapsto & (g \bmod M)_M \end{array}$$

Dont le noyau est exactement D, donc une injection

$$A \hookrightarrow (\mathbb{Z}/p\mathbb{Z})^{\mathrm{M}(P)}$$

En particulier, A est abélien donc D contient le sous-groupe dérivé $[P;P]$.

A est naturellement muni d'une structure d'espace vectoriel de dimension r sur le corps $\mathbb{F}_p$.

9. Maximalité que l'on n'avait pas utilisée jusqu'à présent.

(c) Preuve de (i). Soit $fz_1;:::z_sg$ une partie génératrice de P. Puisque le morphisme $: P \to A$ est surjectif, $f\overline{z_1};:::\overline{z_s}g$ est génératrice dans A. Comme A est un espace vectoriel de dimension r, d'après la théorie de la dimension nous avons $s > r$.

(d) Preuve de (ii). Soit $Z = fz_1;:::z_sg$ une partie génératrice de P. D'après le théorème de la base incomplète, on peut extraire de Z une sous-famille $X = fx_1;:::x_rg$ telle que $f\overline{x_1};:::\overline{x_r}g$ est une base de A. Soit donc $H = hx_1;:::x_ri$. Si par l'absurde $H \neq P$, alors il existe M sous-groupe maximal de P tel que $H \subset M$. Mais alors (H) est incluse dans $M=D$.

Remarque 8.4. On peut vérifier directement que $r = 1$ correspond au cas où P est cyclique. A l'inverse, le cas où r est l'exposant de p dans l'ordre de P correspond à $P \simeq \mathbb{F}_p^r$.Par ailleurs une famille génératrice minimale d'un groupe P d'ordre p est de cardinal $\geq$: si $hg_1;:::g_si$ est une telle famille alors

$$f1g \subset hg_1i \subset hg_1;g_2i \subset \cdots \subset hg_1;:::g_si = P$$

Remarque 8.5. Le lemme 8.2 est un cas particulier d'une propriété dite de « croissance des normalisateurs ». Si G est un groupe nilpotent et H un sous-groupe strict, alors $N_G(H) \supset H$. En particulier, les sous-groupes maximaux sont distingués.

Remarque 8.6. On peut reformuler la proposition 5, et faire un parallèle avec le sous-groupe dérivé : dans un p-groupe

- Le dérivé $[P;P]$ est le sous-groupe qui donne le plus grand quotient abélien.
- Le Frattini (P) est le sous-groupe qui donne le plus grand quotient abélien p-élémentaire.

Remarque 8.7. Le sous-groupe de Frattini est aussi l'ensemble des éléments « mous » c'est-à-dire des $g \in G$ tels que pour tout $S \subset G$

$$hS [fggi = G \Rightarrow hSi = G:$$

Remarque 8.8. Il y a une ressemblance intriguante avec le lemme de Nakayama en algèbre commutative (avec le radical de Jacobson à la place du sous-groupe de Frattini).

9. Critère de Klarès

Leçons :

155: Endomorphismes diagonalisables

157: Endomorphismes trigonalisables et nilpotents

Référence : Mansuy et Mneimné [MM16, 6.8].
Pré-requis. Réduction des nilpotents (le « lemme des noyaux itérés »)

Théorème 9.1. *Soit k un corps algébriquement clos, E un k-espace vectoriel de dimension finie, u un endomorphisme de E. On définit ad_u par*

$$\begin{aligned} \mathrm{ad}_u : L(E) &\to L(E) \\ v &\mapsto uv - vu. \end{aligned}$$

Alors, u est diagonalisable si et seulement si

$$\ker \mathrm{ad}_u = \ker \mathrm{ad}_u^2. \tag{13}$$

(a) Sens direct : u semi-simple implique (13). Supposons que u est diagonalisabke : il existe donc $P \in k[X]$ simplement scindé qui annule u. Notons l_u et r_u les endomorphismes définis par

$$\begin{aligned} l_u : v &\mapsto uv \\ r_u : v &\mapsto vu. \end{aligned}$$

Alors, pour tout $v \in L(E)$ nous avons

$$\begin{aligned} P(l_u)(v) &= P(u)v = 0 \\ P(r_u)(v) &= vP(u) = 0. \end{aligned}$$

Donc, P annule l_u et r_u et ces endomorphismes sont diagonalisables. De plus, ils commutent : donc ils sont codiagonalisables, et $\mathrm{ad}_u = l_u - r_u$ est diagonalisable. Il s'ensuit que

$$\ker \mathrm{ad}_u = \ker \mathrm{ad}_u^2.$$

(b) Sens indirect : (13) implique u diagonalisable. Ecrivons $u = \quad +$ la décomposition de Dunford de u, où est semi-simple et nilpotent. k étant algébriquement clos, est diagonalisable. Pour tout $\in \mathrm{sp}$, l'espace propre $E(\ )$ est -stable ; d'après la réduction des endomorphismes nilpotents il existe un base B de $E(\ )$ dans laquelle admet la matrice

$$N = \begin{pmatrix} J_{d_1} & & (0) \\ & \ddots & \\ (0) & & J_{d_r} \end{pmatrix}$$

où J_{d_i} est le bloc de Jordan de taille d_i. Posons alors M la matrice par blocs égale à

$$M = \begin{pmatrix} \mathrm{diag}(1, \ldots, d_1 - 1) & & (0) \\ & \ddots & \\ (0) & & \mathrm{diag}(1, \ldots, d_r - 1) \end{pmatrix}$$

Un calcul de produit par blocs montre alors que

$$N M - M N = N.$$

Soit B la concaténation des bases B et M la matrice par blocs M , puis l'endomorphisme représenté par M dans B. Alors

$$=$$

De plus, les espaces propres de sont -stable, donc = . Il en ressort que

$$\mathrm{ad}_u(\ ) = (\ +\ ) \qquad (\ +\ ) =$$

D'où $\in \mathrm{Im}(\mathrm{ad}_u)$. Maintenant, si $\ker \mathrm{ad}_u = \ker \mathrm{ad}_u^2$ alors $\ker \mathrm{ad}_u \cap \mathrm{im}\, \mathrm{ad}_u = \{0\}$, donc $= 0$ et $u =$, d'où : u est diagonalisable.

Remarque 9.2. Que dire si k n'est plus supposé algébriquement clos ? Le sens direct est toujours valable. Par contre le sens indirect ne l'est plus a priori. Supposons que l'on a (13) et soit K une clôture algébrique de k (En fait, une extension de décomposition de $_u$ su□t). Alors l'endomorphisme u de $E \ _k K$ est diagonalisable ; en particulier u est semi-simple. Prenons comme exemple l'endomorphisme de $\mathbf{R}^2$ associé à la matrice

$$R = \begin{matrix} \cos & \sin \\ \sin & \cos \end{matrix}$$

avec 2 Z. R est diagonalisable sur C mais pas sur R ; en conséquence ker ad = ker ad^2 (En outre, ici est cyclique, donc cet espace est de dimension 2, c'est R[ ] ′ C) mais n'est pas diagonalisable.

Remarque 9.3. On peut voir le critère de Klarès comme procédant de l'équivalence plus générale (sans hypothèse sur le corps de base)

$$u \text{ semi-simple } \quad ( ) \quad \mathrm{ad}_u \text{ semi-simple}$$

Le sens direct est exactement la même preuve que (a). Pour le sens indirect, remarquons qu'en écrivant $u =$ + la décomposition de Dunford de u, nous avons

$$\mathrm{ad}_u = \mathrm{ad} + \mathrm{ad} \tag{14}$$

Alors d'une part ad est semi-simple d'après la preuve du sens direct, d'autre part ad est nilpotente (c'est la di□érence de l et r qui sont nilpotents et commutent). Enfin, pour tout $w \ 2 \ L(E)$, $[l \ ; l \ ] = [r \ ; r \ ] = 0$. Donc ad et ad commutent , (14) est la décomposition de Dunford de ad_u. Si donc ad_u est semi-simple alors ad = 0, et donc ker ad $= L(E)$, ce qui implique que est une homothétie nilpotente ; donc = 0 et u est semi-simple.

Remarque 9.4. On peut résumer les remarques précédentes sous la forme suivante, sans aucune hypothèse sur k.

$$\begin{array}{ccc} u \text{ diagonalisable} & ( ) & \mathrm{ad}_u \text{ diagonalisable} \\ + & [* \ _u \text{ scindé}] & + \\ u^{(K)} \text{ diagonalisable} & ( ) & \ker \mathrm{ad}_u = \ker \mathrm{ad}_u^2 \\ + & [* \ _u \text{ séparable}] & + \\ u \text{ semi-simple} & ( ) & \mathrm{ad}_u \text{ semi-simple} \end{array}$$

Si maintenant k est supposé parfait (par exemple si k est fini, ou de caractéristique nulle), les deux lignes du bas sont équivalentes. Si k est algébriquement clos les deux lignes du haut sont équivalente. Par exemple pour $k = \mathbf{C}$ toutes les assertions sont équivalentes.

Remarque 9.5. Une autre question naturelle est : quels sont les $u \ 2 \ L(E)$ tels que $\ker \mathrm{ad}_u = \ker \mathrm{ad}_{u^2}$? Le noyau de ad_u est le commutant de u que nous noterons $C(u)$. Si u est diagonalisable, alors $u \ 2 \ k \ u^2$ de sorte que $C(u) = C \ u^2$. Réciproquement, utiliser la réduction de Jordan.

10. Constructibilité des polygones réguliers

Leçons.

125: Extensions de corps

: Polynômes irréductibles, corps de rupture

: Utilisation des nombres complexes en géométrie

Référence. Chambert-Loir [CL05].

Di□culté. Le sens indirect est plus facile.

Pré-requis. Critère d'Eisenstein ; notion de constructibilité. Notions sur les p-groupes (existence d'une suite de composition à quotients d'ordre p).

Théorème 10.1 (Gauss). *Le polygone régulier à n côtés est constructible à la règle et au compas si et seulement si n se décompose sous la forme*

$$n = 2^{\quad} p_1 \quad p_s; \tag{15}$$

où les p_i sont des nombres premiers de Fermat (c'est-à-dire de la forme $2^{2^r} + 1$) distincts.

On dira que 2 C est constructible s'il existe une suite d'extensions quadratiques

$$\mathbf{Q} = K_0 \quad K_1 \qquad K_r = K_{r\ 1}(\ ):$$

Les nombres constructibles forment un sous-corps de C que nous noterons L. Il s'agit du plus petit sous-corps de C contenant Q et quadratiquement clos. Le théorème revient à caractériser les racines de l'unité qui sont constructibles.

(a) Nombres de Fermat.

Lemme 10.2. *Si $2^m + 1$ est premier, alors m est une puissance de 2.*

Démonstration. Dans le cas contraire, soit p premier impair tel que $m = pm'$. Modulo $2^{m'} + 1$

$$2^m + 1 \quad 2^{m'\ p} + 1 \quad (\ 1)^p + 1 \quad 0:$$

Donc $2^{m'} + 1$ divise $2^m + 1$, et $m' < m$: $2^m + 1$ n'est pas premier.

(b) Degrés de certaines extensions cyclotomiques.

Proposition 10.3. *Soit $n = p$ où p est un nombre premier, > 1. Alors si est racine primitive n-ième de l'unité dans* C*, l'extension* $\mathbf{Q}(\ )/\mathbf{Q}$ *est de degré $'(n) = p^{\ 1}(p\ 1)$.*

Démonstration. Le polynôme

$$P = \frac{X^p\ 1}{X^{p\ 1}\ 1} = X^{p\ 1(p\ 1)} + \ + X^{p\ 1} + 1$$

annule ; il su□t de montrer qu'il est irréductible, ce qui assurera que c'est son minimal et que $[\mathbf{Q}(\ ) : \mathbf{Q}]$ est égal à son degré, à savoir $'(n)$. Or, dans $\mathbf{Z}[X]/(p) \ ' \ \mathbf{F}_q[X]$ nous avons

$$\overline{P}(X + 1) = \frac{(X + 1)^p\ 1}{(X + 1)^{\ 1}\ 1} = \frac{X^p}{X^{p\ 1}} = X^{'(n)}:$$

Donc, si l'on écrit $P(X + 1) = X^{'(n)} + a_{'(n)\ 1}X^{'(n)\ 1} \quad + a_1X + a_0$, nous avons $p \mid a_i$ pour tout $i < p\ 1$ et $a_0 = p$. D'après le critère d'Eisenstein, $P(X + 1)$, donc P, est irréductible[10].

10. Une preuve directe ne prend pas beaucoup plus de place. Si $P(X + 1)$ n'est pas réductible, alors en écrivant $P(X + 1) = Q(X)S(X)$, on a par factorialité de $\mathbf{F}_p[X]$, $\overline{Q} = X^q$ et $\overline{R} = X^{p\ 1\ q}$ avec $0 < q < p\ 1$. Mais alors p divise $Q(0)$ et $R(0)$, donc p^2 divise $P(1)$, ce qui n'est pas.

(c) La condition nécessaire. Ecrivons C l'ensemble des $n \in \mathbb{N}^*$ tels que que le nombre complexe $\zeta_n = e^{2i\pi/n}$ est constructible.

Proposition 10.4. *Soit $n \in C$. n se décompose sous la forme (15).*

Démonstration. Soit p premier impair et divisant n. Alors $p \in C$. En particulier le degré de ζ_p sur $\mathbb{Q}$ est une puissance de 2. D'après la proposition 10.3, p est de la forme $2^m + 1$ et d'après le lemme 10.2, p est un nombre de Fermat. En outre, si p^2 divise n alors $\zeta_{p^2} \in C$; mais ceci ne peut se produire que si $\varphi(p^2)$ est une puissance de 2 ; or $p \mid \varphi(p^2)$, donc $p = 2$ est la seule possibilité.

(d) La condition suffisante. Par exemple à l'aide des formules de duplication du cosinus, on montre par récurrence sur k que $2^k \in C$ pour tout k.

Lemme 10.5. *Si m et n dans C sont premiers entre eux, alors $mn \in C$.*

Démonstration. Soient u, v tels que $um + vn = 1$. Alors on vérifie que

$$\zeta_n^v \zeta_m^u = \zeta_{nm}$$

Puisque ζ_n^v et ζ_m^u sont dans le corps L des nombres constructibles, c'est aussi le cas de ζ_{mn} et le mn-gone est constructible.

Conformément au lemme précédent, il reste seulement à montrer que si p est un nombre premier de Fermat, alors $p \in C$.

Lemme 10.6. *Soit p un nombre premier. Alors l'ordre du groupe G des $\mathbb{Q}$-automorphismes de $\mathbb{Q}(\zeta_p)$ divise $p - 1$.*

Démonstration. Le polynôme $P = X^{p-1} + \cdots + 1$ annule tous les ζ_p^i pour $1 \leq i \leq p-1$. Puisqu'il est irréductible, c'est leur minimal et les ζ_p^i sont les seuls conjugués de ζ_p sur $\mathbb{Q}$ dans $\mathbb{C}$. Tout $\sigma \in G$ est la donnée univoque de i tel que $\sigma(\zeta) = \zeta^i$, de sorte qu'on a un morphisme injectif (le caractère cyclotomique)

$$\chi : G \to (\mathbb{Z}/p\mathbb{Z})^*$$

D'après le théorème de Lagrange $|G|$ divise $p - 1$.

En particulier, si p est un nombre premier de Fermat alors G est un 2-groupe (en fait il est isomorphe à $\mathbb{F}_p^*$ donc cyclique d'ordre $p - 1$). Or nous avons le

Lemme 10.7. *Soit H un groupe d'ordre 2^r. Alors il existe une suite de sous-groupes*

$$\{1\} = G_r \subset G_{r-1} \subset \cdots \subset G_1 \subset G_0 = H$$

avec $|G_i| = 2^{r-i}$ pour tout i.

Nous ne démontrerons pas ce lemme ici ; il relève de la théorie des groupes et s'obtient par récurrence, en se servant de l'existence d'un centre non trivial.

Pour finir, soit K_s le sous-corps de $\mathbb{Q}(\zeta_p)$ fixé par le sous-groupe G_s pour tout s. Alors

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_{r-1} \subset K_r = \mathbb{Q}(\zeta_p)$$

En accord avec le théorème de la base télescopique, il suffit de montrer que $K_i \subset K_{i+1}$ pour que toutes les extensions soient quadratiques et conclure.

Remarque 10.8. La proposition 10.3 est un cas particulier du théorème de Gauss concernant l'irréductibilité sur $\mathbb{Q}$ des polynômes cyclotomiques pour tout n (ici pour $n = p$).

Remarque 10.9. La fin va plus vite en admettant la correspondance de Galois : l'extension cyclotomique $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ est galoisienne de groupe de Galois cyclique d'ordre 2^r, il existe une filtration de sous-groupes (G_s) de $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ cycliques d'ordre 2^s, et en posant $K_s = \mathbb{Q}(\zeta_p)^{G_{r-s}}$ on a la tour d'extension quadratiques voulues. Il y a encore du travail pour rendre ceci constructif.

Remarque 10.10. La construction de l'heptadécagone régulier est dûe à Gauss en 1796 à l'âge de 19 ans. Il est difficile de tirer de la preuve précédente une construction effective.

Remarque 10.11. Les premiers nombres de Fermat sont

$$p = 3; 5; 17; 257; 65537$$

et en fait... ce sont les seuls connus.

11. Déterminant et conique

Leçons.

152: (3) Déterminant. Exemples et applications

162: (2) Systèmes d'équations linéaires.

180: (3) Coniques. Applications

181: (3) Barycentres dans un espace a□ne réel

Référence. Eiden, géométrie analytique classique p. 94 [Eid09]. Je dois ce développement à Loïc Devilliers.

Di□culté. Attention à ne pas faire d'erreur de calculs dans les produits matriciels à la fin.

Prérequis. Principe de prolongement des identités algébriques (en partie redémontré)

Théorème 11.1. *Soit P un plan a ne sur un corps k, ABC un triangle non plat de P, M et N dans $P \setminus \{A;B;C\}$. On note $M_A;M_B;M_C$ (de même $N_A;N_B;N_C$) les incidences de M sur (BC), (CA) et (AB) par rapport à A, B et C, prises éventuellement à l'infini. Alors il existe une conique C de P passant par les six points de $\overline{P}$*

$$M_A;M_B;M_C;N_A;N_B;N_C$$

11.1. Equation générique d'une conique ne passant pas par A, B et C dans les coordonnées barycentriques. Les points A, B et C sont non alignés donc $A;\overrightarrow{AB};\overrightarrow{AC}$ forme un repère du plan a□ne P dans lequel l'équation générale d'une conique en coordonnées $(u;v)$ est

$$u^2 + uv + v^2 + u + v + = 0$$

où les constantes $:::$ sont non toutes nulles. Exprimons u et v en fonction des coordonnées barycentrique $(X;Y;Z)$ dans le repère $(A;B;C)$:

$$u = \frac{Y}{X+Y+Z}$$
$$v = \frac{Z}{X+Y+Z};$$

de sorte qu'en remplaçant dans l'équation précédente, on obtient une équation homogène [11] de degré 2 en 3 variables

$$aX^2 + bY^2 + cZ^2 + dYZ + eZX + fXY = 0$$

avec $A;:::F$ non tous nuls.

11.2. Un système linéaire. Si l'on note $(x;y;z)$ (resp. $(x';y';z')$) les coordonnées barycentriques de M et N, alors M_A est l'intersection de (AM) et (BC) d'équations barycentriques

$$(AM) : f(X;Y;Z) \mid 9 \quad 2k;\ Y = x;\ Z = Zg$$
$$(BC) : f(X;Y;Z) \mid X = 0g$$

On en déduit des coordonnées barycentriques :

$$M_A(0;y;z) \quad M_B(x;0;z) \quad M_C(x;y;0)$$
$$N_A(0;y';z') \quad N_B(x';0;z') \quad N_C(x';y';0)$$

11. Ceci n'est pas un mystère. Introduire des coordonnées barycentrique dans le reprère A, B, C c'est comme identifier P à un hyperplan a□ne pas vectoriel du $\mathbf{R}$-vectorialisé sur $fA;B;Cg$, et en même temps à une partie de son projectif.

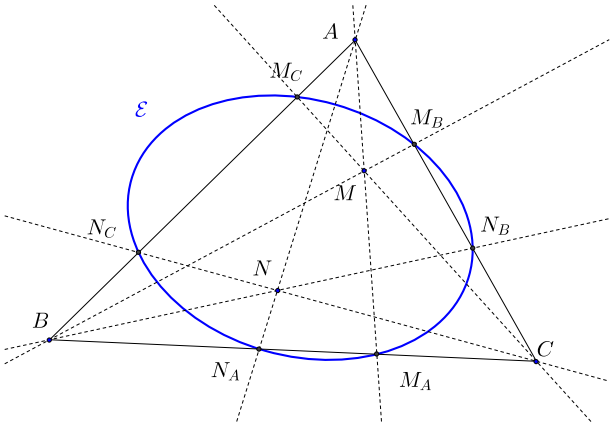


Figure 2. Déterminant et conique

De sorte que la condition d'existence de $A;:::F$ se ramène au système de six équations linéaires à six inconnues

$$(S):\begin{cases} by^2+cz^2+dyz=0\\ ax^2+cz^2+ezx=0\\ ax^2+by^2+fxy=0\\ by'^2+cz'^2+dy'z'=0\\ ax'^2+cz'^2+ez'x'=0\\ ax'^2+by'^2+fx'y'=0 \end{cases}$$

11.3. Fin de la preuve. On doit montrer que le déterminant correspondant au système (S) est nul : pour cela on écrit

$$= \begin{matrix} P & Q \\ R & S \end{matrix}$$

où $P;Q;R;S$ sont des matrices 3 3.

$$P=\begin{pmatrix} 0 & y^2 & z^2\\ x^2 & 0 & z^2\\ x^2 & y^2 & 0 \end{pmatrix}\qquad Q=\begin{pmatrix} yz & 0 & 0\\ 0 & zx & 0\\ 0 & 0 & xy \end{pmatrix}$$

$$R=\begin{pmatrix} 0 & y'^2 & z'^2\\ x'^2 & 0 & z'^2\\ x'^2 & y'^2 & 0 \end{pmatrix}\qquad S=\begin{pmatrix} y'z' & 0 & 0\\ 0 & z'x' & 0\\ 0 & 0 & x'y' \end{pmatrix}$$

Lemme 11.2. *On a la formule de déterminant par blocs*

$$= \det(SP \quad QR) \tag{16}$$

Démonstration. Commençons par supposer S inversible. Alors

$$\begin{matrix} I_3 & QS^{-1} \\ 0 & I_3 \end{matrix} \begin{matrix} P & Q \\ R & S \end{matrix} = \begin{matrix} P & QS^{-1}R & 0 \\ & R & S \end{matrix}$$

Comme le déterminant de la matrice à gauche est 1, on a

$$= \det P \quad QS^{-1}R \det(S) = \det(SP \quad QR)$$

En e□et, on a bien $SQS^{-1}R = QR$ car Q et S, diagonales, commutent. Pour le cas général, soit K un corps infini contenant k (K existe toujours : prendre par exemple la limite inductive des $\mathbb{F}_{q^{n!}}$ si $k \simeq \mathbb{F}_q$). On considère

$$P = (\quad \det(SP \quad QR)) \quad \det S = (\quad \det(SP \quad QR)) \quad x'^2y'^2z'^2$$

vu comme un élément de $A = K[x; x'; y; y'; z; z']$. La fonction polynômiale $P : K^6 \to K$ est nulle sur K^6, et K est infini, donc P est nul[12]. Puisque A est intègre, soit on a (16) soit $x'^2 y'^2 z'^2 = 0$, ce qui n'est pas, donc on a (16).

Il reste maintenant à calculer . Appliquant (16) on obtient

$$= \det \begin{pmatrix} 0 & y'z'y^2 & y'z'z^2 \\ x'z'x^2 & 0 & x'z'z^2 \\ x'y'x^2 & x'y'y^2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & yzy'^2 & yzz'^2 \\ xzx'^2 & 0 & xzz'^2 \\ xyx'^2 & xyy'^2 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & yy'(yz' & yz') & zz'(zy' & z'y) \\ xx'(z'x & zx') & 0 & zz'(x'z & xz') \\ xx'(y'x & yx') & yy'(x'y & xy') & 0 \end{pmatrix}$$

$$= xx'yy'zz' \begin{pmatrix} 0 & yz' & yz' & zy' & z'y \\ z'x & zx' & 0 & x'z & xz' \\ y'x & yx' & x'y & xy' & 0 \end{pmatrix} = 0$$

La somme des colonnes étant nulle.

12. Ce fait se démontre par récurrence, à l'aide d'une pseudo-division euclidienne

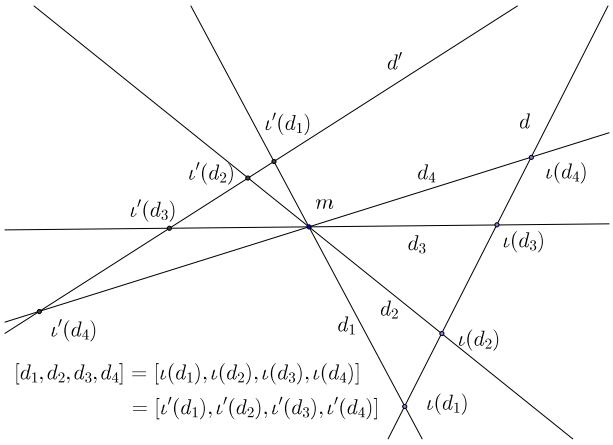


Figure 3. Incidence et perspective

12. Hexagramme de Pascal

Leçons.

127: (3) Droite projective et birapport

159: (3) Formes linéaires et dualité

180: (3) Coniques. Applications

Références. Audin, Géométrie L3 -M1 [Aud12].

Prérequis : Définitions d'une incidence et d'une perspective.

Di□cultés. Le changement de paramétrage d'une conique est bien une homographie ; ne pas confondre les points a, b, c, d, e, f.

Théorème 12.1. *Soit C une conique projective propre, a, b, c, d, e et f six points dans l'image de C. Les droites ab et de, bc et ef, cd et fa s'intersectent en trois points alignés*

Remarque 12.2. Par dualité projective le théorème de Pascal correspond à celui de Brianchon : si un hexagone a tous ses côtés tangents à une conique propre, alors ses diagonales sont concourantes.

(a) Birapport, incidence et perspectives. On désigne par P un plan projectif, $P = P(E)$.

Lemme 12.3. *Soit m un point et d une droite de P ne passant pas par m. L'incidence $: m^? \; ! \; d$ est une homographie.*

Démonstration. Il faut montrer que l'incidence provient d'un isomorphisme linéaire $E^? \; ! \; E$. Soit $(e_1; e_2; e_3)$ une base de E telle que $m = p(e_1)$ et $p(e_2); p(e_3)$ sont dans d. Soit $` \; 2 \; E^?$, on écrit $` = ae_1^2 + be_2^2 + ce_3^2$. Alors $p^?(`) \; 2 \; m^?$ s'écrit $a = 0$, et l'intersection de $p^?(`)$ avec $d = p(he_2; e_3 i)$ est $p((\; ce_2 + be_3))$. Finalement, on pose

$$f : ae_1^2 + be_2^2 + ce_3^2 \; ! \; ae_1 \quad ce_2 + be_3:$$

En particulier, si l'on se donne 4 droites $d_1; : : : d_4$ de $m^?$ et d dans $P^?$, les birapports $[d_1; d_2; d_3; d_4]$ et $[\; (d_1); \; (d_2); \; (d_3); \; (d_4)]$ sont égaux.

Lemme 12.4. *Soit m un point, d et d^0 deux droites de P ne passant pas par m. La perspective $: d \; ! \; d$ est une homographie.*

Démonstration. Si l'on pose l'incidence $m^? \; ! \; d$ et ^{0} l'incidence $m^? \; ! \; d^0$ alors $= {}^0 \quad {}^1$. On conclut par le lemme précédent.

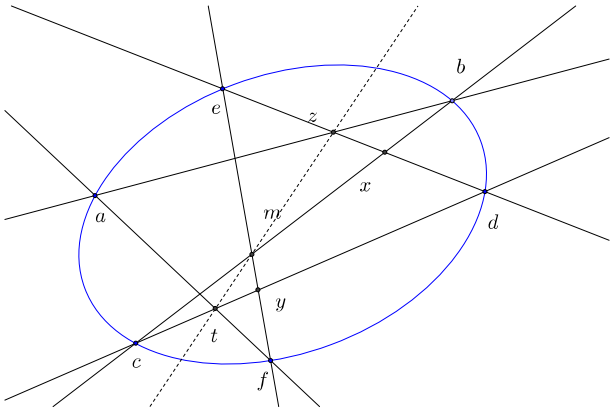


Figure 4. L'hexagramme de Pascal

On a résumé la situation des deux lemmes sur la figure suivante (d et d' sont figurées comme deux sécantes des d_i concourrantes dans un plan a□ne dont on imagine que P est la complétion projective).

(b) Conique, paramétrage et droite projective. Si les types des coniques projectives propres peuvent être variés (selon la classification des formes quadratiques sur le corps de base ; pour R ou C ce n'est pas le cas) intrinsèquement ce sont toutes des variétés projectives isomorphes (paramétrées par $\hat{k}$) :

Lemme 12.5. *Soit C une conique propre, m un point de C. Tout élément d de $m^?$ rencontre l'image de C en un autre point exactement, ntons le $_m(d)$. Alors l'application $_m : m^? \ ! \ C$ est un paramétrage de C ; les changements de paramétrages*

$$_n{}^1 \quad _m : m^? \ ! \ n^?$$

sont des homographies.

(c) Preuve du théorème de Pascal. Elle se ramène à présent à une égalité de deux birapports : Notons z l'intersection de ab et ed, x l'intersection de bc et ed, y l'intersection de cd et ef, t l'intersection de cd et af (figure). Alors

$$\begin{aligned} & & [z;x;d;e] \\ \text{(incidence } b^? \quad ed) &= [bz;bx;bd;be] \\ \text{(changement de points)} &= [ba;bc;bd;be] \\ \text{(changement de paramétrage } b^? \ ! \ f^?) &= [fa;fc;fd;fe] \\ \text{(incidence } f^? \quad cd) &= [t;c;d;y] \end{aligned}$$

Finalement, la perspective à travers m applique ed sur cd et envoie $z;x;d$ respectivement sur $t;c;d$; étant donnée l'égalité des birapports e est envoyé sur y autrement dit z, m et t sont alignés.

---

13. Théorème des deux carrés

Leçons :

121: Nombres premiers

122: Anneaux principaux

Référence : Francinou, Gianella, Nicolas [FGN14, Algèbre 1] ou Jean-Pierre Serre, *Compléments d'arithmétique* (notes polycopiées, sans ISBN).

Avertissement. La version précise (expression de $r_2(n)$) ne rentre pas dans le temps imparti. Dans la leçon « Anneau principaux » il ne faut pas dissimuler qu'en réalité seule la factorialité de $\mathbb{Z}[i]$ compte.

Théorème 13.1. *L'anneau $A = \mathbb{Z}[i]$ des entiers de Gauss est euclidien pour le stathme $N(z) = z\bar{z}$. En outre, les irréductibles de A sont (à association près)*
- Les nombres premiers p congrus à 3 modulo 4
- Les $z \in A$ tels que $N(z)$ est premier.

Corollaire 13.2 (Théorème des deux carrés). *L'entier $n \in \mathbb{N}$ est somme de deux carrés si et seulement si pour tout $p \in P$ congru à 3 modulo 4, $v_p(n)$ est pair. Plus précisément, le nombre de décompositions de n en sommes de deux carrés de $\mathbb{Z}$ est donné par*

$$r_2(n) = 4(d_1(n) - d_3(n)) \tag{17}$$

où $d_i(n)$ est le nombre de diviseurs de n congrus à i mod 4.

(a) Preuve du théorème. On prouve à l'aide du plongement $\mathbb{Z}[i] \hookrightarrow \mathbb{C}$ et de la nature géométrique de N que A est euclidien[13] : Soient a et b dans A avec $b \neq 0$, alors on écrit

$$a/b = x + iy = x_0 + iy_0 + (x - x_0) + i(y - y_0)$$

avec $x_0, y_0 \in \mathbb{Z}$ et $|x - x_0| \leq 1/2$, $|y - y_0| \leq 1/2$. Posons $q = x_0 + iy_0$, il vient $a = qb + r$ avec

$$N(r) = N(b)\,|x - x_0|^2 + |y - y_0|^2 \leq N(b)/2 < N(b)$$

Lemme 13.3. *Soit $p \in P$. S'équivalent*
(i) p est irréductible dans A
(ii) $p \equiv 3$ modulo 4
(iii) p n'est pas somme de deux carrés.

Démonstration. (ii) $\Rightarrow$ (iii) s'obtient par congruence modulo 4, les uniques carrés dans $\mathbb{Z}/4\mathbb{Z}$ étant $\bar{0}$ et $\bar{1}$. Montrons (iii) $\Rightarrow$ (i) par contraposition : si $p = zz'$ avec $z, z' \notin A^\times$ alors en notant $z = a + ib$ nous avons

$$N(p) = p^2 = N(z)\,N(z').$$

Ceci impose $N(z) = N(z') = p$, d'où $a^2 + b^2 = p$, soit : (iii).

(i) $\Rightarrow$ (ii) demande un peu plus de travail. A est euclidien donc principal, et p est irréductible dans A ssi $A/(p)$ est un corps. Or il y a un isomorphisme d'anneaux astucieux (aussi utilisé dans le cours de Perrin) lié au double quotient :

$$A/(p) \simeq \mathbb{Z}[X]/(p, X^2 + 1) \simeq \mathbb{F}_p[X]/(X^2 + 1) \tag{18}$$

Comme $\mathbb{F}_p[X]$ est principal, $\mathbb{F}_p[X]/(X^2 + 1)$ est un corps ssi $X^2 + 1$ est irréductible, autrement dit si $X^2 + 1$ n'a pas de racine dans $\mathbb{F}_p$. Il reste à voir que si $p \equiv 1$ modulo

13. La même preuve s'adapte pour $\mathbf{Z}[j]$, $\mathbf{Z}\left[i, \frac{p}{2}\right]$ par exemple mais attention, pas pour n'importe quel anneau d'entiers quadratiques imaginaires ; ceux-ci ne sont d'ailleurs pas principaux en général, voir [Che14, chapitre 4].

4 alors 1 est un carré dans $\mathbb{F}_p$. Observons alors que[14] $(p-1)! \equiv -1 [p]$ (regrouper les éléments avec leurs inverses) puis que

$$((p-1)/2)!^2 \equiv (-1)^{\frac{p-1}{2}} (p-1)! \equiv -1 [p]$$

si p est congru à 1 modulo 4.

Remarque 13.4. Pour (i) $\Leftrightarrow$ (ii) on peut aussi utiliser la factorialité de A et de $\mathbb{F}_p[X]$ (notion plus faible) et observer que d'après les isomorphismes (18), $A/(p)$ est intègre ssi $\mathbb{F}_p[X]/(X^2+1)$ est intègre, ce qui donne en définitive la même chose.

Démontrons à présent le théorème :

(1) Nombres premiers. D'après le lemme, si $p \equiv 3 \bmod 4$ il est irréductible dans A ; mais par ailleurs, si $p \equiv 1 \bmod 4$ il est somme de deux carrés, d'où $p = a^2 + b^2 = (a+ib)(a-ib)$ et p n'est pas irréductible dans A.

(2) Si $N(z)$ est premier alors z est irréductible (vue la multiplicativité de N). Réciproquement, soit z un irréductible de A et $p \in P$ divisant $N(z)$. Alors $p \mid z\bar{z}$. Si $p \in P_3$ alors p est irréductible, donc $p \mid z$ ou $p \mid \bar{z}$; mais alors $p \mid z$ et $p = z$. On peut donc supposer $p \in P_1$ mais alors $p = y\bar{y}$ d'après ce qui précède, ce qui contredit l'irréductibilité de z.

(b) Preuve du théorème des deux carrés. Soit n un entier naturel. On écrira

$$n = 2^{\alpha_1} p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s} \tag{19}$$

sa décomposition en facteurs premiers avec les $p_i \equiv 1 \bmod 4$ et les $q_i \equiv 3 \bmod 4$. On notera $n \in \Sigma_2$ si n est somme de deux carrés.

(b.1) Si $n \in \Sigma_2$ alors β_i est pair pour tout $i \in \{1;\dots;s\}$. Ecrivons $n = a^2 + b^2$ et soit $q \in P_3$ divisant n. Alors en posant $z = a + ib$, $n = N(z) = z\bar{z}$ est divisible par q, donc (puisque q est irréductible dans A) $q \mid z$, ie $q \mid a$ et $q \mid b$. Donc $q^2 \mid a^2 + b^2 = n$, et $n/q^2 = (a/q)^2 + (b/q)^2$ de sorte que $n/q^2 \in \Sigma_2$. Par une réccurence immédiate, $\alpha_q(n)$ est pair.

(b.2) Si β_i est pair pour tout $i \in \{1;\dots;s\}$ alors $n \in \Sigma_2$. D'après la multiplicativité de N, Σ_2 est stable par multiplication ; il suffit donc d'écrire n comme un produit d'éléments de Σ_2. D'après le lemme, tous les p_i sont sommes de deux carrés. Ecrivons $p_i = a_i^2 + b_i^2 = z_i\overline{z_i}$ avec $z_i = a_i + b_i$.

— Si α est pair alors

$$n = 2^{\alpha/2} \left(a_1^2 + b_1^2\right)^{\beta_1} \cdots \left(a_r^2 + b_r^2\right)^{\beta_r} \left(q_1^2\right)^{\beta_1/2} \cdots \left(q_s^2\right)^{\beta_s/2} :$$

— Si α est impair alors $n = 1^2 + 1^2 + n-2$ et $n-2 \in \Sigma_2$ d'après ce qui précède.

(c) Le nombre de décompositions en sommes de deux carrés. D'après ce qui précède, décomposer n en somme de deux carrés, c'est décomposer n en produit de deux termes conjugués dans l'anneau $\mathbb{Z}[i]$. Par exemple,

$$65 = 5 \cdot 13 = (2+i)(2-i)(3+2i)(3-2i) :$$

Les éléments $2-i$ et $3-2i$ étant irréductibles (car de norme première). On peut décomposer ce produit de deux manières :

$$\begin{aligned} 65 &= [(2+i)(3+2i)][(2-i)(3-2i)] \\ &= [4+7i][4-7i] \\ &= 4^2 + 7^2 \\ &= [(2+i)(3-2i)][(2-i)(3+2i)] \\ &= [8-i][8+i] \\ &= 8^2 + 1^2 : \end{aligned}$$

14. Ce fait caractérise les nombres premiers ; il est parfois connu sous le nom de théorème de Wilson

Soit $n \in \mathbb{N}^*$ impair et écrivons la décomposition de n dans $\mathbb{Z}[i]$:

$$\begin{aligned} n &= p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s} \\ &= (1+i)^{\alpha_0} (1-i)^{\alpha_0} (a_1+ib_1)^{\alpha_1} \cdots (a_r+ib_r)^{\alpha_r} \\ &\quad (a_1-ib_1)^{\beta_1} \cdots (a_r-ib_r)^{\beta_r} q_1^{\beta_1} \cdots q_r^{\beta_r}. \end{aligned}$$

Si maintenant $n = zz$ alors pour tout irréductible π de A, $v_\pi(z) = v_{\bar\pi}(z)$ et $v_\pi(z) + v_{\bar\pi}(z) = v_\pi(n)$, donc nous pouvons écrire :

$$\begin{aligned} z &= (a_1+ib_1)^{\gamma_1} \cdots (a_r+ib_r)^{\gamma_r} \\ &\quad (a_1+ib_1)^{\beta_1-\gamma_1} \cdots (a_r+ib_r)^{\beta_r-\gamma_r} q_1^{\beta_1/2} \cdots q_s^{\beta_s/2} \end{aligned}$$

avec $0 \leq \gamma_0 \leq \alpha_0$ et $0 \leq \gamma_i \leq \alpha_i$ pour tout $i \in \{1,\dots,r\}$. Finalement donc,

$$r_2(n) = (1+\alpha_1) \cdots (1+\alpha_r). \tag{20}$$

Remarque 13.5. Il existe un argument combinatoire pour démontrer le lemme 13.3 dû à D. Zagier [Zag90]. Il consiste à se donner p un nombre premier congru à 1 modulo 4. ; puis on introduit l'ensemble

$$S = \{(x,y,z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}.$$

On vérifie que S est fini[15], et non vide (il contient $(1,1,\frac{p-1}{4})$). Soit f la fonction de S dans S définie par

$$f(x,y,z) \mapsto \begin{cases} (x+2z,z,y-x-z) & \text{si } x < y-z \\ (2y-x,y,x-y+z) & \text{si } y-z < x < 2y \\ (x-2y,x-y+z,y) & \text{si } x > 2y. \end{cases}$$

Alors on peut montrer que f est involutive et possède exactement un point fixe ; de telle sorte que l'on a une action de $\mathbb{Z}/2\mathbb{Z} = \{\mathrm{id}, f\}$ sur S, et d'après l'équation aux classes le cardinal de S est impair. Finalement g l'involution de S donnée par

$$(x,y,z) \mapsto (x,z,y)$$

admet un point fixe ; donc p est somme de deux carrés. Cette preuve est proche de l'esprit des arguments de non-annulation de caractéristique d'Euler consistant à se ramener à un comptage de points fixe (modulo 2), en topologie différentielle.

Remarque 13.6 (Le problème du disque de Gauss). Si la fonction $r_2(n)$ est localement erratique, sa moyenne de Cesaro converge. En effet

$$R_2(N) = 1 + \sum_{n=1}^{N} r_2(n)$$

est exactement le nombre de points à coordonnées entières dans le disque fermé de rayon $\sqrt{N}$. On en déduit que $R_2(N) = \pi N + O(\sqrt{N})$, puis

$$\frac{1}{N} \sum_{n=1}^{N} r_2(n) = \pi + O\left(N^{-1/2}\right). \tag{21}$$

L'amélioration de l'exposant $1/2$ dans le terme de reste de (21) est un problème au long cours. Il est connu qu'on ne pourra pas faire mieux que $N^{3/4+}$ (Hardy, Landau).

Remarque 13.7 (Densités supérieures des sommes de carrés). A partir du théorème et moyennant le cas particulier [Che14, Exercice 9.9][16] suivant du théorème de densité de

15. Si $(x,y,z) \in S$ alors $xyz \neq 0$ (p est premier), donc $x,y,z > 1$. Il s'ensuit que $p = x^2 + 4yz > \max(x,y,z)$, d'où $S \subset \{1,\dots,p\}^3$ et c'est donc un ensemble fini.

16. Cela donne une densité de Dirichlet mais c'est tout aussi bien (même mieux) pour ce que nous voulons faire.

Cebotarev a□rmant que les nombres premiers s'équirépartissent entre 1 et 3 modulo 4, on montre que l'ensemble des sommes de deux carrés a densité naturelle nulle dans N :

$$\limsup_{N \to +\infty} \frac{1}{N} \left| \left(\{1, \dots, N\} \right) \right| = 0. \tag{22}$$

Remarque 13.8 (Trois carrés). Soit Σ_3 l'ensemble des sommes de trois carrés. Gauss a montré [Ser70, IV, appendice] que pour tout $n \in \mathbb{N}$, $n \in \Sigma_3$ si et seulement si n n'est pas la forme $4^a(8b - 1)$ où a et b sont des entiers naturels.

Remarque 13.9. Tout nombre entier est somme de quatre carrés (voir [Sam67, 5.7] – ceci découle aussi du théorème de la remarque précédente), et il existe également une formule donnant le nombre de décomposition en somme de quatre carrés.

Remarque 13.10. A quoi ressemble $A/(p)$ quand $p - 1$ modulo 4 ? Le polynôme $X^2 + 1$ est scindé, disons

$$X^2 + 1 = (X - u)(X + u);$$

avec $u \in \mathbb{F}_p$ et d'après le lemme des restes chinois $A \simeq \mathbb{F}_p - \mathbb{F}_p$. C'est un anneau non intègre.

14. Géométrie des nombres, applications

Référence. Hindry [Hin08].
Di□culté. Ecrire le bon réseau dans la leçon.
Pré-requis. Le volume de la b.u. euclidienne de dimension 4 est ^{2}=2.

Théorème 14.1. *Soit un réseau de* $\mathbf{R}^n$ *et* K *un convexe symétrique mesurable*[17] *de* $\mathbf{R}^n$. *On suppose que*

$$\text{vol}(K) > 2^n \text{covol}(\ ) \tag{23}$$

ou bien, que K *est compact et que*

$$\text{vol}(K) > 2^n \text{covol}(\ ) : \tag{24}$$

Alors $K \setminus$ *n'est pas réduit à* 0.

Corollaire 14.2. *Tout nombre entier naturel est somme de quatre carrés.*

(a) Preuve du théorème de Minkowski. Quitte à e□ectuer un changement de variables linéaire ' envoyant sur $\mathbf{Z}^n$, ce qui multiplie les deux côtés de l'inégalité par $\frac{1}{\text{covol}(\ )}$ on peut supposer que $= \mathbf{Z}^n$.

Lemme 14.3. *Sous les hypothèses du théorème et avec* $= \mathbf{Z}^n$ *il existe* s *et* t *dans distincts tels que* $s + \frac{K}{2} \setminus t + \frac{K}{2}$ *est non vide.*

Démonstration. Posons $C = [0;1[^n$; on peut alors écrire

$$K/2 = \bigsqcup_{s \in \mathbf{Z}^n} (K/2) \setminus (s + C)$$

de sorte que par -additivité et invariance de la mesure par translation

$$\text{vol}(K/2) = \sum_{s \in \mathbf{Z}^n} \text{vol}\left(s + \frac{K}{2}\right) \setminus C :$$

Maintenant, si par l'absurde les parties $s + \frac{K}{2}$ sont toutes disjointes, le dernier terme correspond à

$$\text{vol}\left(\bigsqcup_{s \in} \left(s + \frac{K}{2}\right) \setminus C\right) \leqslant \text{vol}(C) = 1 :$$

Mais $\text{vol}(K/2) = 2^{\ n}\text{vol}(K) > 1$ par hypothèse, ce qui constitue une contradiction.

On en déduit le premier cas du théorème de Minkowski : soient s et t dans , distincts et $x \in s + \frac{K}{2} \setminus t + \frac{K}{2}$; alors

$$x = s + \frac{u}{2} = t + \frac{v}{2}$$

de sorte que $u = 2(t - s) + v$ avec u et v dans K. Puisque K est convexe symétrique, $\frac{u-v}{2} \in K$ donc $s - t \in K$ mais $s - t \in$, $s \neq t$. Pour finir, si K est compact alors $K(1 + 1/m)$ rencontre $f0g$ pour tout $m > 1$; mais alors soit x_m dans cette intersection, (x_m) est bornée donc admet une valeur d'adhérence x ; est discret et K compact donc $x \in \setminus K$, non nulle.

17. Avez-vous déjà rencontré un convexe non mesurable ?

(b) Deux lemmes.

Lemme 14.4. *Soit* N*? l'ensemble des sommes de quatres carrés. est multiplicativement stable*

Démonstration. Soient x et y dans . Dans le sous-anneau de H

$$A = \; a + bi + cj + dk \; j \; (a;b;c;d) \; 2 \; \mathbb{Z}^4$$

on peut écrire $x = N(a)$ et $y = N(b)$. Or N est multiplicative ; donc $xy = N(ab)$, $xy \; 2$

Lemme 14.5. *Soit p premier impair ;* 1 *est somme de deux carrés dans* $\mathbb{F}_p$

Démonstration. Soit C l'ensemble des carrés de $\mathbb{F}_p$. C est de cardinal $\frac{p+1}{2}$ donc d'après le principe des tiroirs, $1 + C$ et C s'intersectent ; 1 est somme de deux carrés.

(d) Théorème des quatres carrés. Conformément à la multiplicativité évoquée plus haut, et étant donné que $2 \; 2$ il reste seulement à montrer la

Proposition 14.6. *Soit p un nombre premier impair, alors p 2 .*

Démonstration. Soient a et b tels que $p \; j \; a^2 + b^2 + 1$. On considère le réseau

$$= \; x \; 2 \; \mathbb{Z}^4 \; j \; x_3 \quad ax_1 + bx_2 \; (p) \; ; \quad x_4 \quad bx_1 \quad ax_2 \; (p)$$

Une $\mathbb{Z}$ base de étant constituée par les vecteurs

$$(e_1;e_2;e_3;e_4) = \begin{matrix} 0\,2 & 3 & 2 & 3 & 2 & 3 & 31 \\ 1 & 0 & 0 & 0 & 0 & & \\ B6\,0 & 7 & 6\,1 & 7 & 6\,0 & 7 & 6\,0\,7C \\ B6\,7 & 6 & 7 & 6 & 7 & 6 & 7C \\ @4\,a & 5 & 4\,b & 5 & 4\,p & 5 & 4\,0\,5A \\ b & & a & & 0 & & p \end{matrix}$$

Donc le covolume de est p^2 ; on choisit > 0 afin que $\frac{2}{2}^4 = 2^4p^2$; la boule euclidienne $B(0; \;)$ de $\mathbb{R}^4$ rencontre en $(x_1;:::x_4)$ non nul. Nous avons d'une part, modulo p

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 \quad & x_1^2 + x_2^2 + (ax_1 + bx_2)^2 + (bx_1 \quad ax_2)^2 \\ & x_1^2 + x_2^2 + \; a^2 + b^2 \; x_1^2 + \; a^2 + b^2 \; x_2^2 + 2 \; (ab \quad ba) \; x_1x_2 \\ & 0 \end{aligned}$$

et d'autre part

$$\begin{aligned} 0 < x_1^2 + x_2^2 + x_3^2 + x_4^2 \; < \quad & {}^2 \\ = \quad & \frac{4^{p}\overline{2}}{}p < \frac{6p}{3} = 2p \end{aligned}$$

Donc $p \; 2$.

Remarque 14.7. On peut éviter de recourir à l'anneau H en prenant $n = p_1 \quad p_r$ sans facteur carré ; puis

$$= \; \Big\backslash_{i=1} \; {}_i$$

où

$${}_i = \; x \; 2 \; \mathbb{Z}^4 \; j \; x_3 \quad ax_1 + bx_2 \; (p_i) \; ; \quad x_4 \quad bx_1 \quad ax_2 \; (p_i) \; :$$

Il vient alors

$$\text{covol} \; (\;) \; 6 \; \prod_i \; \text{covol} \; (\; {}_i) = \; \prod_i \; p_i^2 = n^2$$

puis on conclut. Si n a des facteurs carrés, on écrit $n = \; {}^2n_0$ et on applique ce qui précède à n_0.

15. Critère dual de densité (Hahn-Banach)

Leçons.

202: Exemples de parties denses et applications

208: Espaces vectoriels normés, applications linéaires continues

209: Approximation d'une fonction par des polynômes ou polynômes trigonométriques (en application du théorème de Weierstrass)

244: Fonctions développables en série entière, fonctions analytiques. Propriété de la somme (en application du principe des zéros isolés).

Référence. Gonord et Tosel [GT96], Brézis [BCL99].

Théorème 15.1. *Soit E un espace vectoriel normé (réel), V un sous-espace. S'équivalent*

(i) V est dense dans E

(ii) Pour toute[18] $\in E'$, $\ell_{|V} = 0 \Longrightarrow \ell = 0$

Exemple 15.2. Soit $A \subset]1;+1[$ une partie fermée. Alors A admet un point d'accumulation dans $]1;+1[$ si et seulement si la famille de fonctions

$$f_a : x \mapsto \frac{1}{x - a}_{a \in A}$$

engendre un espace vectoriel dense dans $E = C([0;1])$ muni de la norme uniforme.

(a) Du théorème de Hahn-Banach géométrique au critère dual de densité. Le sens (i) $\Longrightarrow$ (ii) du théorème est le plus immédiat car il relève en fait d'un contexte beaucoup plus général : dans un espace topologique, une fonction est nulle dès qu'elle est nulle sur une partie dense. Montrons le sens (ii) $\Longrightarrow$ (i) par contraposition à l'aide de la première forme géométrique du théorème de Hahn Banach : supposons que V n'est pas dense dans E et soit $x \in E \setminus \overline{V}$. Alors $\overline{V}$ est un convexe fermé, $\{x\}$ est compact, et $\overline{V}$ et $\{x\}$ dont disjoints de sorte qu'il existe $\ell \in E'$ telle que $\sup_{\overline{V}} < \ell(x)$. Vu que $\overline{V}$ est un sous-espace de $\mathbb{R}$ distinct de $\mathbb{R}$, $\overline{V} = \{0\}$ et $V \subset \ker \ell$ tandis que $x \notin \ker \ell$ implique $\ell \neq 0$.

(b) Application. Commençons par supposer que A admet un point non isolé $a_0 \in]1;+1[$. Posons $E = C([0;1])$ et $V = \mathrm{Vect}_{a \in A}\{f_a\}$. Soit ℓ une forme linéaire continue sur E qui s'annule sur V ; conformément au critère dual de densité on cherche à montrer que $\ell = 0$. D'après le théorème de Weierstrass, l'espace W des fonctions polynômiales est dense dans E. Le sens (i) $\Longrightarrow$ (ii) du théorème garantit qu'il suffit de montrer

$$\ell_{|W} = 0 \tag{25}$$

Notons $e_n : x \mapsto x^n$ pour tout $n \in \mathbb{N}$ et introduisons la fonction

$$\varphi(z) = \sum_{k=0}^{+\infty} \langle e_n, \ell \rangle z^n.$$

Le rayon de convergence est supérieur à 1 puisque $|\langle e_n, \ell \rangle| \leq \|\ell\| \|e_n\| = \|\ell\|$ pour tout n de sorte que φ est analytique sur $]-1;1[$. D'après le principe des zéros isolés il suffit de montrer que les zéros de φ s'accumulent sur un point intérieur à $]-1;1[$. Or pour tout $a \in A$

$$\begin{aligned}\varphi(1/a) &= \sum_{k=0}^{+\infty} \langle e_n, \ell \rangle \frac{1}{a^n} \\ &= \sum_{k=0}^{+\infty} \left\langle \frac{e_n}{a^n}, \ell \right\rangle\end{aligned}$$

18. comme « esure de Radon ». Voir la suite pour comprendre

et $\frac{e_n(x)}{a^n} = \frac{x}{a}^n$; or $a > 1$ donc la série de fonctions de terme général $f_n(x) = (x=a)^n$ converge normalement vers

$$f : x \mapsto \frac{1}{1 \quad x=a} = \frac{a}{a \quad x}$$

Par continuité de sur E, $'(1=a) = hf_a; \ i = 0$. Puisque les zéros de $'$ possèdent un point d'accumulation dans $]\ 1;1[$, $' = 0$ et on a le résultat escompté.

(c) Seconde application : espaces de Banach séparables.

Théorème 15.3. *Soit E un espace de Banach tel que E^0 est séparable. Alors E est séparable.*

Démonstration. Soit $(\ _n)$ une suite dénombrable et dense dans E^0. Pour tout n il existe x_n de norme 1 dans E tel que

$$h\ _n; x_n i > \frac{1}{2} k\ _n k$$

Soit alors L_0 le $\mathbb{Q}$ -espace vectoriel engendré par les x_n. Il est dénombrable (c'est une union croissante dénombrable des $\mathrm{Vect}_{\mathbb{Q}} fx_i; 0 \ 6 \ i \ 6 \ ng$ qui sont des $\mathbb{Q}$-ev de dim finie, donc dénombrable).

Si L est le $\mathbb{R}$-espace vectoriel engendré par les x_n, alors L_0 est dense dans L : pour tout $v \ 2 \ L$ on peut écrire $v = \sum v_i x_i$ pour un nombre fini de v_i non nuls ; puis les approximer avec une précision aribitraire par des rationnels. Il suffit donc de vérifier que L est dense dans E, ce que l'on fait à l'aide du critère dual de densité. Soit $\ 2 \ E^0$ qui s'annule sur L. Vu que $(\ _n)$ est dense, pour tout > 0 on peut trouver n tel que $k\ _n \quad k < \ $. On a alors

$$\frac{1}{2} k\ _n k \quad h\ _n; x_n i = h\ _n \quad ; x_n i + h\ ; x_n i$$

Mais comme s'annule sur L, le dernier terme est nul et $jh\ _n \quad ; x_n ij \quad k\ _n \quad k < \ $. On a ainsi montré que

$$k\ k \quad k\ _n k + k \quad \ _n k < 2 + \ = 3$$

Donc $= 0$.

Remarque 15.4. Attention, un espace de Banach E peut être séparable sans que son dual topologique E^0 le soit. Ainsi, l'espace $`^1(\mathbb{N})$ est séparable (l'ensemble des suites à support fini forme une partie dense) ; mais son dual topologique $E^0 \ ' \ `^1(\mathbb{N})$ n'est pas séparable : l'ensemble des indicatrices $f1_X g_{X \ \mathbb{N}}$ forme une partie de cardinal c dont les éléments sont à distance mutuelle 1.

En revanche, d'après ce qui précède, si E est un espace de Banach reflexif, E est séparable si et seulement si E^0 est séparable (puisque son dual E^{00} est lui-même séparable).

Autre application (et non des moindres...) du critère de densité par dualité :

Proposition 15.5 (Brézis [BCL99]). *Soit un ouvert de $\mathbb{R}^N$, la mesure de Lebesgue sur . Alors $C_c(\ )$ est dense dans $L^p(\ )$ quand $p < 1$.*

La stratégie générale de preuve est la suivante : on montre que toute forme linéaire sur L^p qui s'annule sur C_c, est nulle. Les formes linéaires sur L^p s'identifient à L^{p^0}.

16. Théorème d'Ascoli-Arzela

Leçons.

2: Suites et séries de fonctions

2: Application de la notion de densité.

2: Prolongement de fonctions.

Référence. Aucune !

Di□culté. Attention à l'ordre des étapes : d'abord on prolonge la limite, ensuite on montre que la convergence était uniforme en réalité, selon le précepte : convergence simple et équicontinuité donnent convergence uniforme.

Pré-requis.

(1) K métrique compact, F un complet, $A \subset C(K;F)$. Alors A est uniformément équicontinue sur K ssi A est équicontinue en tout $x \in K$ (la preuve est similaire à celle du théorème de Heine).

(2) Une version du théorème de Tychonov : un produit dénombrable de métriques compacts, muni de la topologie produit, est métrisable et compact. Celui-ci peut être avantageusement remplacé par un argument diagonal direct (c'est juste un peu plus technique).

(3) Théorème de prolongement des applications uniformément continues sur une partie dense d'un espace métrique, à valeurs dans un complet.

Théorème 16.1. *Soit K un métrique compact, F un espace métrique complet, $A \subset C(K;F)$. S'équivalent*

(i) A est relativement compacte dans $C(K;F)$

(ii) A est uniformément équicontinue sur K et pour tout $x \in K$ la partie $A(x) = \{f(x) \mid f \in A\}$ est relativement compacte dans F.

Remarque 16.2. Nécessité de la dernière condition : prendre pour A l'ensemble des fonctions constantes. Il est toutefois possible de l'a□aiblir un peu (en apparence) par ex. si F est de dimension finie, il su□t que $A(x_0)$ soit bornée pour un unique $x_0 \in K$.

Remarque 16.3. On a une version généralisée en prenant X métrique, dénombrable à l'infini, $C(X;F)$ muni de la norme de la convergence uniforme sur tous les compacts.

On commence par démontrer le sens (ii) $\Rightarrow$ (i) ; à cet e□et on utilise la caractérisation séquentielle, c'est-à-dire que l'on se donne une suite $(f_n) \in A^{\mathbf{N}}$ dont il s'agit de montrer qu'elle possède une valeur d'adhérence dans $C(K;F)$.

Notation : Pour tout $B \subset C(K;F)$ équicontinue en $x \in K$ (resp. uniformément équicontinue sur K) et $\varepsilon > 0$ on appellera module d'équicontinuité de B pour ε en x (resp. module d'uniforme équicontinuité de B pour ε sur K) la quantité

$$\begin{aligned} \omega_{B;x}(\varepsilon) &= \sup\{\delta > 0 \mid \forall y \in K,\ \forall f \in B,\\ &\qquad d_K(x;y) < \delta \Rightarrow d_F(f(x);f(y)) < \varepsilon\}\\ \omega_B(\varepsilon) &= \sup\{\delta > 0 \mid \forall x \in K,\ \forall y \in K,\ \forall f \in B,\\ &\qquad d_K(x;y) < \delta \Rightarrow d_F(f(x);f(y)) < \varepsilon\} \end{aligned}$$

(a) Utilisation de la précompacité de K. K est un espace métrique compact, donc pour tout $N \in \mathbf{N}^*$ il existe R_N une partie finie de K telle que

$$K = \bigcup_{r \in R_N} B(r;1/N)$$

Comme dans [QZ02] nous disons que R_N est un $\frac{1}{N}$-réseau de K. En particulier la partie $R = \bigcup_N R_N$ est dénombrable et dense dans K qui est ainsi séparable.

(b) Une limite simple f d'une suite extraite, sur R. Par hypothèse, les parties $\overline{A(r)}$ pour tout r dans R sont compactes. D'après le théorème de Tychonov, l'espace $\prod_{r \in R} \overline{A(r)}$ muni de la topologie produit, est métrisable et compact. Par conséquent il existe une sous-suite $f_{(n)}$ qui converge vers une limite f simplement[19] sur R.

(c) Prolongement de f. Montrons que f est uniformément continue sur R, ce qui permettra de la prolonger à tout K. Soit $\varepsilon > 0$, η module d'uniforme équicontinuité de A sur K pour $\varepsilon/3$ et $r, r' \in R$ tels que $d(r, r') < \eta$. Alors pour n assez grand

$$d\left(f_{(n)}(r), f(r)\right) < \varepsilon/3$$
$$d\left(f_{(n)}(r'), f(r')\right) < \varepsilon/3$$

Par l'inégalité triangulaire on a que $d(f(r), f(r')) < \varepsilon$, ce qu'il fallait. On notera toujours f le prolongement à K.

(d) En fait la convergence était uniforme. Déjà, vu que f est uniformément continue sur A on a que $A \cup \{f\}$ est encore uniformément continue. Soit $\varepsilon > 0$, η' module d'uniforme équicontinuité de $A \cup \{f\}$ sur K pour $\varepsilon/3$ et N tel que $1/N < \eta'$. La convergence de $f_{(n)}$ vers f est uniforme sur le réseau R_N (qui est fini) donc pour $n > n_0$ assez grand

$$\forall r \in R_N,\ d\left(f_{(n)}(r), f(r)\right) < \varepsilon/3$$

Soit maintenant $x \in K$ quelconque ; il existe $r \in R_N$ tel que $d(x, r) < \varepsilon/3$, et nous avons alors les 3 inégalités

$$\forall n > n_0,\ d\left(f_{(n)}(r), f(r)\right) < \varepsilon/3$$
$$d\left(f_{(n)}(r), f_{(n)}(x)\right) < \varepsilon/3$$
$$d\left(f(r), f(x)\right) < \varepsilon/3$$

D'après l'inégalité triangulaire $d_F\left(f_{(n)}(x), f(x)\right) \leq \varepsilon$. Conclusion, $f_{(n)} \to f$ uniformément sur K.

(e) La réciproque. L'évaluation

$$\begin{aligned} \mathrm{ev}_x : C(K, F) &\to F \\ f &\mapsto f(x) \end{aligned}$$

est linéaire continue ; si $\overline{A}$ est compacte c'est aussi le cas de $\overline{A}(x) = \overline{A(x)}$ pour tout $x \in K$. Si par l'absurde A n'est pas uniformément équicontinue, alors il existe $\varepsilon > 0$ et $(x_n, y_n, f_n) \in K^2 \times A^{\mathbb{N}}$ telle que

$$d_K(x_n, y_n) \leq 1/n$$
$$d_F\left(f_n(x_n), f_n(y_n)\right) > \varepsilon$$

Puisque K^2 est compact et vue la première inégalité, la suite (x_n, y_n) converge vers un certain (x, x) sur sa diagonale. Soit $f \in \overline{A} \subset C(K, F)$ valeur d'adhérence de la suite (f_n) ; alors comme on devrait avoir pour n assez grand $d_F\left(d_F\left(f_n(x_n), f_n(y_n)\right)\right) \leq \varepsilon$.

Les applications du théorème d'Ascoli.

(1) [HL99] (Compacité d'un opérateur à noyau) Soient X et Y des compacts de $\mathbb{R}^n$ et $K \in C(X \times Y)$. On pose pour tout $f \in C(X)$

$$Tf(y) = \int_X K(x, y) f(x)\, \mathrm{d}x$$

T envoie $C(X)$ dans $C(Y)$ et d'après le théorème d'Ascoli, T est un opérateur compact.

19. Attention, la topologie produit n'est pas induite par la norme $\|\cdot\|_1$ sur R de sorte que cette convergence n'est pas uniforme a priori. Sinon il serait assez facile de conclure très vite !

17. Théorème de Cauchy-Peano-Arzela

Leçons.

202: Utilisation de la notion de compacité

208: Théorème de point fixe

220: Equations di□érentielles

253: Convexité en analyse

Référence.

(1) Théorème de Schauder : RMS - 1999 (écrit Ulm-Lyon 98), corrigé dans le tome 7. L'énoncé est repris dans [Pom94], Cours d'analyse p.80 (attention les notations di□èrent, on prendra ici celles de Pommellet qui sont plus simples).

(2) Théorème de Cauchy-Peano : pas de référence connue.

Di□culté. Manque de référence

Pré-requis. Théorème de Brouwer (ce pré-requis est conséquent)

Théorème 17.1. *Soit C un compact convexe d'un espace vectoriel normé E. Toute application continue $f : C \to C$ admet un point fixe.*

Corollaire 17.2. *(Théorème de Cauchy-Peano-Arzela) Soit E un espace vectoriel normé de dimension finie*[20]*, $F : \mathbb{R} \times E \to E$ continue, $y_0 \in E$ et $t_0 \in \mathbb{R}$. Le problème de Cauchy*

$$\begin{cases} y'(t) = F(t, y(t)) \\ y(t_0) = y_0 \end{cases} \tag{26}$$

admet une solution (non unique a priori) définie sur $]t_0 - \alpha ; t_0 + \alpha[$ pour un certain $\alpha > 0$.

(a) Un argument de précompacité. Soit $\varepsilon > 0$ un réel. $f(C)$ est un métrique compact, en particulier il est précompact et il existe un nombre fini de points $a_1, \dots, a_n$ tels que

$$f(C) \subset \bigcup_{i=1}^{n} B(a_i, \varepsilon) \tag{27}$$

On pose dans tout ce qui suit $F = \mathrm{Vect}_i(a_i)$ et $C' = C \setminus F$. Puisque F est de dimension finie, il est complet, donc fermé dans E, et C' est fermé dans le compact C. Il s'ensuit que C' est compact. Par ailleurs, C et F sont convexe donc C' est convexe.

(b) Approximation par projection dans C'. Pour tout $i \in \{1, \dots, n\}$ et $x \in E$, nous posons $\varphi_i(x) = \max(0, \varepsilon - \|x - a_i\|)$ puis $\varphi = \sum_i \varphi_i$. D'après l'inclusion (27), φ est strictement positive sur $f(C)$; on introduit alors

$$p(y) = \frac{1}{\varphi(y)} \sum_{i=1}^{n} \varphi_i(y)\, a_i$$

Il s'agit d'un barycentre des points a_i ; par convexité de C', il y est. Puisque les a_i à distance moindre de ε de y sont les seuls tels que $\varphi_i(y) < 0$, et par convexité de l'application $\|\cdot - y\|$ nous avons $\|p(y) - y\| < \varepsilon$ pour tout y.

(c) Théorème de Schauder. Pour tout N entier on prend $\varepsilon = 1/N$ et le convexe C' correspondant par la construction précédente. D'après le théorème de Brouwer dans C', la fonction $p_{1/N} \circ f : C' \to C'$ admet un point fixe x_N et nous avons

$$\|x_N - f(x_N)\| = \|p_{1/N}(f(x_N)) - f(x_N)\| < 1/N$$

. Puisque C est métrique compact, la suite (x_N) admet une valeur d'adhérence x_1 et par passage à la limite dans l'inégalité précédente, x_1 est un point fixe pour f.

20. Attention, cette hypothèse est importante (contrairement à Cauchy-Lipschitz qui s'énoncerait dans un Banach quelconque). Une raison pour cela est que le théorème de point fixe de Schauder requiert compacité, là où celui de Banach-Picard se contente de complétude.

(d) Preuve du théorème de Cauchy-Peano. Il faut trouver « le bon convexe compact » pour appliquer le théorème de Schauder.

Lemme 17.3. *Avec les notations des hypothèses du corollaire 17.2, il existe des constantes réelles r; ; M telles que si C est l'ensemble des fonctions M-lipschitziennes sur $[t_0 \quad ; t_0 + \ ]$, valant y_0 en t_0 et à valeurs dans $\overline{B}(y_0; r)$ alors l'application*

$$T : y \mapsto \left(t \mapsto y_0 + \int_{t_0}^{t} F(s; y(s))\, ds \right)$$

est à valeurs dans C.

Démonstration. Fixons $r > 0$ et $_0 > 0$, puis

$$M = \sup_{[t_0 \quad ; t_0 + \ ] \ \overline{B}(y_0; r)} jFj$$

Il existe $2 \ ]0; \ _0[$ tel que $M \quad < r$. Quitte à prendre un tel , on a la propriété voulue : Ty est M-lipschitzienne et par conséquent à valeurs dans $\overline{B}(y_0; r)$.

Par ailleurs, C est convexe (ceci provient de la convexité de $\overline{B}(y_0; r)$). De plus, d'après le théorème d'Ascoli, C est compact : ses éléments sont M-lipschitz donc forment une partie équicontinue fermée. D'après le théorème de Schauder, il existe y telle que $Ty = y$; ceci signifie que y est solution de l'équation différentielle (26).

Remarque 17.4. Un exemple de non-unicité de la solution de (26) est donné par l'équation scalaire

$$y' = jyj$$

avec < 1. Pour > 1 il y a unicité d'après le théorème de Cauchy-Lipschitz.

18. Algébricité et mesure d'irrationalité

Leçons.

230: Séries numériques

Référence. [Duv07]

Définition 18.1. Soit un nombre réel. On dit que est de Liouville si pour tout $n \geq 2$ N il existe un rationnel $r = p/q$ distinct de tel que

$$\left| \frac{p}{q} \right| \leq \frac{1}{q^n}.$$

Théorème 18.2. *Les nombres de Liouville sont transcendants.*

Corollaire 18.3. *Le nombre*

$$= \sum_{n=0}^{+\infty} 2^{-n!}$$

est transcendant.

Théorème 18.4. *L'ensemble des nombres de Liouville forme un G_δ - dense de la droite réelle, de mesure de Lebesgue nulle.*

(a) Une contraposée précisée du théorème 18.2. La proposition suivante relie le degré d'algébricité à la mesure d'irrationalité :

Proposition 18.5. *Soit $\in$ Q algébrique de degré d. Alors il existe $K > 0$ une constante telle que pour tout rationnel p/q distinct de ,*

$$\left| \frac{p}{q} \right| > \frac{K}{q^d} \tag{28}$$

Démonstration. Soit P_0 le polynôme minimal de sur Q. Quitte à multiplier P_0 par un entier k assez grand, on a un annulateur $P = kP_0$ dans $\mathbb{Z}[X]$. Pour tout rationnel r distinct de , $P(r) \neq 0$; en effet

- Si est rationnel alors $\deg P = 1$ et est l'unique racine de P
- Sinon P_0 est irréductible (Q[ ] est intègre), et en particulier il n'a pas de racine rationnelle.

Par ailleurs, si l'on écrit $P = a_0 + \cdots + a_d X^d$ alors il est visible que $P\left(\frac{p}{q}\right) = s/q^d$ où s est un entier, pour tout rationnel p/q. s est non nul pour r distinct de d'après l'argument qui précède, donc $|P(p/q)| > 1/q^d$. Or, d'après l'inégalité des accroissements finis on a que

- Si $|p/q| \leq 1$, $|P(p/q)| \leq \sup_{[-1;+1]} |P'|$ $\frac{p}{q}$
- Sinon $|p/q| > 1$

De sorte que quitte à poser $K = \min\left(1; 1/\sup_{[-1;+1]} |P'|\right)$ on a l'inégalité voulue.

Remarque 18.6. On peut ainsi en déduire que $e \notin$ Q. En effet, pour tout $n > 1$ on a que

$$\sum_{k=0}^{2n+1} \frac{(-1)^k}{k!} < \frac{1}{e} < \sum_{k=0}^{2n} \frac{(-1)^k}{k!}$$

de sorte que $\frac{1}{e} - \sum_{k=0}^{2n} \frac{(-1)^k}{k!} < \frac{1}{(2n+1)!} = \frac{1}{2n+1}\frac{1}{(2n)!}$, $(2n)!$ étant plus grand que le dénominateur du rationnel à droite. Pour tout $K > 0$ il existe n tel que $K > \frac{1}{2n+1}$, ce qui conclut.

(b) Preuve du corollaire. Il nous faut évaluer le reste :

$$\sum_{n=0}^{N} 2^{-n!} = \sum_{n=N+1}^{+\infty} 2^{-n!} \leq \sum_{k=(N+1)!}^{+\infty} 2^{-k!} = 2^{-(N+1)!}$$

Avec $2^{-(N+1)!} = \frac{2}{(2^N)^{N+1}}$. On en déduit que est un nombre de Liouville. En particulier il est transcendant d'après ce qui précède.

Remarque 18.7. On peut contruire comme cela une infinité non dénombrable de nombre de Liouville (et donc de nombres transcendants, ce qui est compatible avec l'argument de Cantor[21]). Partons en effet de l'ensemble $P_1(\mathbf{N})$ des parties infinies de N. Il est indénombrable puisque c'est le complémentaire de l'ensemble $P_f(\mathbf{N})$ des parties finies - dénombrable - dans $P(\mathbf{N})$ - non dénombrable. Pour tout $E \in P_1(\mathbf{N})$ on pose

$$_E = \sum_{n \in E} 2^{-n!}$$

Alors il est clair que $E \mapsto {}_E$ est injective et que ${}_E$ est un nombre de Liouville.

(c) Sur la grosseur de l'ensemble .

Lemme 18.8. *est un G-dense de* R.

Démonstration. Notons $B(x;r)$ la boule ouverte de centre x et de rayon r, épointée de x. Alors nous pouvons écrire

$$= \bigcap_{n>1} \bigcup_{p \in \mathbf{Z};\, q>1} B\left(\frac{p}{q}; \frac{1}{q^n}\right) = \bigcap_{n>1} {}_n$$

${}_n$ est ouvert en tant qu'union d'ouverts ; ${}_n$ est dense puisque quel que soit $x \in$ R il existe (r_m) une suite de rationnels distincts de x tendant vers x ; quitte à écrire $r_m = p_m/q_m$ et à poser

$$s_m = r_m + \frac{1}{2q_m^n}$$

on a que $s_m \in {}_n$ pour tout m et $s_m \to x$. Il s'ensuit que est un G-dense de R au sens de la théorie de Baire.

Définition 18.9. Soit un nombre réel. Sa mesure d'irrationnalité $\in [1;+\infty]$ est donnée par

$$= \sup \{ s \in \mathbf{R} \mid \exists (r_n);\ r_n \neq ;\ |r_n - | < q_n^{-s} \}$$

En particulier est de Liouville si $( ) = +\infty$.

Proposition 18.10. *Soit ${}_0 > 2$. L'ensemble des nombres réels de mesure d'irrationnalité $> {}_0$ est de mesure de Lebesgue nulle.*

Démonstration. Notons S cet ensemble ; S est clairement invariant par translation d'un entier relatif, il suffit donc de montrer que $(S \cap [0;1]) = 0$. Pour cela, on écrit

$$S \cap [0;1] = \limsup_q A_q$$

où

$$A_q = \bigcup_{p=0}^{q} B\left(p/q; q^{-{}_0}\right)$$

On a alors que A_q est Lebesgue-mesurable et $(A_q) = \frac{2q}{q^{{}_0}} = 2q^{1-{}_0}$. Pour ${}_0 > 2$, la suite (A_q) est sommable et d'après le lemme de Borel-Cantelli (la partie « facile ») $(\limsup A_q) = 0$.

21. **R** est indénombrable, tandis que le corps des nombre réels algébriques est dénombrable...

Remarque 18.11. On peut aussi montrer (à l'aide du principe des tiroirs de Dirichlet, du lemme du corps convexe de Minkowski, ou bien de manière effective à l'aide du développement en fraction continue) que tout irrationnel admet une mesure d'irrationnalité > 2. Conjointement au résultat précédent, ce ci implique que pour presque tout $x \in \mathbb{R}$, $\mu(x) = 2$, et invite à poser une mesure plus fine de la qualité de l'approximation diophantienne, pour les réels de mesure d'irrationalité 2 :

(29) $$m(x) = \inf_{r_n \neq a} \liminf_n \; |x - r_n| \, q_n^2 \; :$$

19. Un théorème de Kronecker et une application

106: Groupe des nombres complexes de module 1

1??: Fonctions symétriques élémentaires

Référence : Deschamps-Warusfel pour le théorème. Aucune pour le corollaire.
Di□culté : *. Il y a de nombreuses manières de s'y prendre selon la leçon. L'utilisation du résultant est intéressante en soi mais placer ce développement dans « Résultant » est quand même légèrement abusif (à bien justifier en tout cas). L'application à la preuve du corollaire 19.2 est à ma connaissance originale.

Théorème 19.1. *Soit $P \in \mathbb{Z}[X]$ unitaire de degré n. On suppose que les racines de P dans $\mathbb{C}$ sont de module 1. Alors, il existe un entier m tel que toutes les racines de P sont dans $\{0\} \cup U_m$.*

Corollaire 19.2 (Minkowski?). *Pour G un sous-groupe fini de $GL(n;\mathbb{Z})$, les morphismes de projection canoniques*

$$G \to GL(n;\mathbb{F}_p)$$

sont injectifs pour $p > 3$. Pour $p = 2$ le noyau est de taille au plus 2^n.

19.1. Un premier lemme, trois démonstrations.

Lemme 19.3. *Soit $P \in \mathbb{Z}[X]$ unitaire. On note $\alpha_1, \dots, \alpha_n$ ses racines dans $\mathbb{C}$ (éventuellement non distinctes) et pour tout $k \in \mathbb{N}$, on pose*

$$P_k(X) = \prod_{i=1}^{n} X - \alpha_i^k$$

Alors, $P_k \in \mathbb{Z}[X]$.

Preuve 1 (avec matrice compagne). Soit $C_P \in M_n(\mathbb{C})$ la matrice compagne associée à P. On trigonalise C_P dans $GL_n(\mathbb{C})$; cela donne une matrice T de forme triangulaire supérieure, avec les racines $\alpha_1, \dots, \alpha_n$ de P sur la diagonale. P_k est encore le polynôme caractéristique χ_{T^k} ; or T^k est semblable à une matrice de $M_n(\mathbb{Z})$, ceci conclut.
Preuve 2 (avec le théorème des polynômes symétriques). Ecrivons $c_{k;p}$ le coe□cient de degré p dans P_k. Alors nous pouvons écrire

$$c_{k;p} = (-1)^{k-p} \binom{n}{k-p} \sigma_{k,\dots,k}(\alpha_1, \dots, \alpha_n).$$

Puisque $\binom{n}{k-p} X_1^k \cdots X_n^k \in \mathbb{Z}[X_1, \dots, X_n]^{S_n}$, il existe $Q \in \mathbb{Z}[X]$ tel que

$$\binom{n}{k-p} X_1^k \cdots X_n^k = Q\left(\sigma_1^{(n)}(X_1, \dots, X_n), \dots, \sigma_1^{(n)}(X_1, \dots, X_n)\right).$$

Par spécialisation en les α_i on trouve que $c_{k;p}$ est un polynôme en les $\sigma_j^{(n)}(\alpha_1, \dots, \alpha_n)$ qui sont les coe□cients de P. Ce sont donc des entiers.
Preuve 3 (avec le résultant). Posons $Q(X;Y) = Y^k - X$ et voyons Q et P dans $\mathbb{Z}[Y][X]$. Le résultant correspondant à l'élimination de la variable X correspond à

$$R(X) = \mathrm{Res}_Y(P;Q) = \prod_{i=1}^{n} Q(X;\alpha_i) = (-1)^{\frac{n(n-1)}{2}} P_k(X)$$

et retrouve bien que R est dans l'anneau de base, à savoir $\mathbb{Z}[X]$.

19.2. Principe des tiroirs. Comme mentionné plus haut, les coe□cients $c_{k;p}$ de P_k sont des polynômes symétriques en les $_i$. Puisque les $_i$ sont en module borné par 1, il s'ensuit par utilisation de l'inégalité triangulaire que

$$jc_{k;p}j \quad 6 \quad \begin{matrix} n \\ p \end{matrix} \tag{30}$$

Puisque $P \ 2 \ Z[X]$, la majoration (30) entraîne que les P_k parcourent un ensemble fini ; il existe donc une sous-suite $P_{'(k)}$ stationnaire. Si est une racine de P, alors $^{'(k)}$ est une racine de $P_{'(k)}$. Comme les $P_{'(k)}$ on au plus n racines distinctes, il existe $k < k^0$ tels que $^{'(k)} = {}^{'(k^0)}$. Posant $m = {}' (k^0) \quad {}' (k)$ on a bien que $\ 2 \ f0g \ [\ U_m$.

19.3. Lemme. Soit G tel que dans l'énoncé du corollaire, et soit $g \ 2 \ G \ \backslash \ \ker$, où $: GL(n; Z) \ ! \ GL(n; F_p)$ est la projection canonique. Alors $g = I + ph$, où $h \ 2 \ M_n(Z)$; il s'ensuit que

$$_g(X) = \det \ X I_{M_n(\mathbf{Z}[X])} \quad g \ = \ _h(p(X \quad 1))$$

les racines complexes de $_g$ sont dans U (puisque par exemple, g est d'ordre fini), donc celles de $_h$ sont dans D ; or ce polynôme est unitaire à coe□cients dans Z. D'après le théorème de Kronecker démontré précédemment, toutes les racines de $_h$ sont nulles, donc h est nilpotente. Mais alors $I + ph$ est la décomposition de Dunford de g ; et comme g est diagonalisable, $h = 0$.

20. Table de caractères et simplicité du groupe A_5

Référence. Colmez [Col11], problème annexe corrigé. Attention au conflit de notation avec U (préferer $\mathcal{U}$ dans un premier temps...)

*Di culté ***.* L'ensemble est trop long. On pourra admettre la partie sur les classes de conjuguaison, ainsi que les identités trigonométriques $\cos\frac{2}{5} = \frac{1}{4}\sqrt{5}$ et $\cos\frac{4}{5} = \frac{1+\sqrt{5}}{4}$.

Pré-requis.

(1) Les relations de Schur-Frobenius (orthogonalité des caractères)

(2) Théorèmes de Sylow (conjuguaison des p-Sylow)

Théorème 20.1. *Le groupe* A_5 *possède exactement* 5 *classes de conjuguaison :*
- C_1 *(identité) de cardinal* 1
- C_3 *(les* 3*-cycles) de cardinal* 20
- $C_{2;2}$ *(les doubles transpositions) de cardinal* 15
- C_5 *formée de* 12 *des* 5*-cycles*
- C_5^0 *formée des* 12 5*-cycles restants.*

En outre
(i) Ces classes sont stables par passage à l'inverse
(ii) A_5 *est simple.*
(iii) Sa table de caractères est donnée par

	C_1	C_3	$C_{2;2}$	C_5	C_5^0
1	1	1	1	1	1
U	4	1	0	1	1
V	5	1	1	0	0
W	3	0	1	$'$	$\bar{}$
W'	3	0	1	$\bar{}$	$'$

Table 1. Table de caractères du groupe A_5 (avec $'$ et $\bar{}$ les deux racines complexes du polynôme $X^2 \quad X \quad 1$)

20.1. Classes de conjuguaison de A_5.

Lemme 20.2. *Soit* C *une classe de conjuguaison de* S_n*. S'il existe* $_0$ *2* C *telle que le centralisateur de* $_0$ *dans* S_n *contient une transposition, alors* C *est encore une classe de conjuguaison de* A_n*.*

Démonstration. Soit dans C qui vérifie les hypothèses du lemme. Puisque est conjuguée à $_0$ dans S_n, son centralisateur Centr( ) est conjugué dans S_n a celui de $_0$; lui aussi contient une transposition, notons la . Quelle que soit ^{0} *2* C il existe *2* S_n telle que

$$^0 = \quad ^1 = \quad (\quad)^{\ 1}$$

Puisque ou est dans A_n, et ^{0} sont encore conjuguées dans A_n.

Dans A_5, tout 3-cycle $(a_1a_2a_3)$ ou toute double transposition $(a_1a_2)(a_3a_4)$ possède une transposition dans son centralisateur (prendre (b_1b_2) avec $fb_1;b_2g = f1;:::5g \quad fa_ig$ dans le premier cas, (a_1a_2) dans le second) de sorte que C_3 et $C_{2;2}$ forment bien des classes de conjuguaison de A_5.

Soit $= (a_1a_2a_3a_4a_5)$ un 5-cycle de A_5. On souhaite étudier son centralisateur. D'après le principe de conjuguaison,

$$^1 = (\quad (a_1) \quad (a_2) \quad (a_3) \quad (a_4) \quad (a_5))$$

pour toute *2* A_5 ; en particulier on constate que *2* Centr( ) ssi *2* $h\ i$ qui est de cardinal 5. D'après l'équation aux classes, la classe de conjuguaison de dans A_5 est de cardinal 60=5 = 12. De plus elle est contenue dans l'ensemble des 5-cycles.

Conclusion : les 5-cycles (qui sont au nombre de 24) se répartissent en exactement deux classes de conjuguaison dans A_5, et on a la liste complète des classes de conjuguaison de A_5 :

$$A_5 = C_1 \ t \ C_3 \ t \ C_{2;2} \ t \ C_5 \ t \ C_5^0$$

Enfin, d'après les théorèmes de Sylow, les 5-Sylow de A_5 sont conjugués entre eux, et de cardinal 5. On en déduit que si est un 5-cycle, est conjugué à $^1 = ^4$ mais pas à ^{2} ni ^{3} qui sont par contre conjugués entre eux. On en déduit que C_5 et C_5^0 sont stables par passage à l'inverse.

20.2. Dimensions des représentations irréductibles. La représentation régulière de A_5 contient d_i fois la représentation irréductible $_i$, où d_i est le degré de $_i$. On peut donc écrire

$$60 = d_1^2 + d_2^2 + d_3^2 + d_4^2 + d_5^2$$

Puisque la représentation triviale est de degré $1 = d_1$, on est ramené à décomposer 59 en somme de 4 carrés. Pour cela, on observe que les carrés modulo 8 sont 0, 1 et 4 ; puis que

$$59 \quad 3 \quad 0 + 1 + 1 + 1 \quad (8)$$

Il s'agit là de la seule décomposition possible ; des considérations sur la taille des nombres en présence donnent

$$59 = 4^2 + 5^2 + 3^2 + 3^2$$

et cette écriture est unique. A ce stade, nous pouvons remplir la première colonne de la table de caractère.

20.3. Bornes sur les caractères ; simplicité de A_5. Les relations de Schur-Frobenius indiquent que si T est la matrice correspondant à la table de caractère de A_5 nous avons

$$(T^?T) \quad \text{Diag}\,(jC_1j\,;jC_3j\,;jC_{2;2}j\,;jC_5j\,;jC_5^0j) = jA_5j\,I_5$$

D'où nous tirons que $T^?T$ est la matrice diagonale de termes les cardinaux des centralisateurs :

$$T^?T = \text{Diag}\,(60;3;4;5;5)$$

En particulier, pour tout 6= 1 caractère irréductible et C 6= C_1, nous avons que $j \quad (C)j^2 \ 6$ 5, de sorte que pour tout $g \ 2 \ C$, $j \quad (g)j \ 6 \ \sqrt{5} < 3$. Puisque les représentations irréductibles sont de degré > 3, ceci donne que A_5 est un groupe simple[22].

20.4. La représentation irréductible de dimension 4. On part de la représentation de permutation tautologique P de A_5 sur $\mathbb{C}^5 = \mathbb{C}e_1 + \quad + \mathbb{C}e_5$. L'espace $\ker(e_1^? + \quad + e_5^?)$ est bien stable, c'est l'orthogonal de la droite des invariants pour le produit hermitien usuel qui est préservé par A_5. On désigne par U la sous-représentation associée. Pour montrer qu'elle est irréductible, calculons son caractère : de $P = U \quad 1$ on tire $_U = _P \quad 1$, or $_P(\ )$ est le nombre de ses points fixes ; donc

$$\begin{aligned}
_U(C_1) &= 5 \quad 1 = 4 \\
_U(C_3) &= 2 \quad 1 = 1 \\
_U(C_{2;2}) &= 1 \quad 1 = 0 \\
_U(C_5) &= 0 \quad 1 = \quad 1 \\
_U(C_5^0) &= 0 \quad 1 = \quad 1
\end{aligned}$$

22. Si N était un sous-groupe propre distingué, soit une représentation irréductible non triviale de $G=N$ (qui existe avec la formule de Burnside car $G=N$ non trivial...) On considère $\sim =$ où $: G \ ! \ G=N$ est la surjection canonique ; $\sim$ est encore irréductible, et contient les classes C_j qui composent N dans son noyau de sorte que si est son caractère, (C_j) est le degré de . Tout ceci est exclu par la borne précédente.

On obtient

$$\begin{aligned} \langle \chi_U, \chi_U \rangle &= \frac{1}{60}\left(4^2 + 20 \quad 1^2 + 15 \quad 0^2 + 2 \quad 12 \quad (-1)^2\right) \\ &= \frac{1}{60}(16 + 20 + 24) \\ &= 1 \end{aligned}$$

Ceci indique que χ_U est irréductible ; ainsi $\chi_U = \chi_4$ et c'est la représentation irréductible de degré 4.

20.5. Les représentations irréductibles de dimension 3. Puisque $\mathbf{1}$ est l'unique représentation irréductible de dimension 1 de A_5, toutes les autres représentations envoient A_5 dans le groupe spécial linéaire. Si donc $\rho : A_5 \to W$ et $\rho' : A_5 \to W'$ sont les deux représentations irréductibles de dimension 3 alors pour tout $g \in A_5$ d'ordre m les valeurs propres de $\rho(g)$ et $\rho'(g)$ sont des racines m-ièmes de l'unité non dont le produit vaut 1 et la somme est de module $\leqslant 3$. En particulier :

(1) Si $g \in C_3$ alors les valeurs propres de $\rho(g)$ sont 1, j et j^2 (où $j = e^{2i\pi/3}$) de sorte que $\chi_W(C_3) = \chi_{W'}(C_3) = 1 + j + j^2 = 0$

(2) Si $g \in C_4$ alors les valeurs propres de $\rho(g)$ sont 1, i et $-i$ de sorte que $\chi_W(C_{2,2}) = \chi_{W'}(C_{2,2}) = 1 + i - i = 1$.

(3) Pour les deux classes C_5 et C_5^0 qui sont stables par passage à l'inverse comme mentionné plus haut, les valeurs propres possibles sont respectivement $1, \zeta, \zeta^{-1}$ ou $1, \zeta^2, \zeta^{-2}$ avec $\zeta = e^{2i\pi/5}$. Ceci permet de lever l'indétermination sur C_5 et C_5^0 : on décidera par exemple

$$\begin{aligned} \chi_W(C_5) &= \chi_{W'}(C_5^0) = 1 + \zeta + \zeta^{-1} \\ \chi_W(C_5^0) &= \chi_{W'}(C_5) = 1 + \zeta^2 + \zeta^{-2}. \end{aligned}$$

Calculons :

$$\begin{aligned} (1 + \zeta + \zeta^{-1})^2 &= 1 + \zeta^2 + \zeta^{-2} + 2\zeta + 2\zeta^{-1} + 2 \\ &= (1 + \zeta + \zeta^2 + \zeta^{-2} + \zeta^{-1}) + 1 + \zeta + \zeta^{-1} + 1 \\ &= 1 + 1 + \zeta + \zeta^{-1} \end{aligned}$$

De sorte que $1 + \zeta + \zeta^{-1} = \varphi$ et $1 + \zeta^2 + \zeta^{-2} = -\varphi^{-1}$.

On remplit ainsi les deux dernières lignes du tableau.

20.6. Les représentations irréductibles de dimension 5. Pour retrouver le caractère manquant χ_V on utilise la décomposition de la représentation régulière

$$\chi_{\mathrm{reg}} = \mathbf{1} + 4\chi_U + 5\chi_V + 3\chi_W + 3\chi_{W'} = 60\,\chi_1.$$

On en déduit

$$\begin{aligned} \chi_V(C_3) &= \frac{1}{5}(60 \quad 4 \quad 1) = 12 \\ \chi_V(C_{2,2}) &= \frac{1}{5}(60 \quad 3 \quad (-1) \quad 3 \quad (-1)) = 12 \\ \chi_V(C_5) &= \frac{1}{5}(60 \quad 4 \quad (-1) \quad 3 \quad (\varphi' + -\varphi)) = 0 \\ \chi_V(C_5^0) &= \frac{1}{5}(60 \quad 4 \quad (-1) \quad 3 \quad (-\varphi + \varphi')) = 0. \end{aligned}$$

20.7. Remarques.

20.7.1. *Les deux représentations irréductibles de dimension* 3. Bien que non isomorphes, les deux représentations irréductibles de dimension 3 diffèrent d'un automorphisme extérieur. Les représentations de dimension 4 et 5 ne « voient » pas cet automorphisme extérieur parce que les groupes $SO(4)$ et $SO(5)$ sont assez grands pour la conjuguer.

20.7.2. *Tables de caractères des extensions centrales.* Le groupe $A_5 \simeq \mathrm{PSL}(2;\mathbb{F}_5)$ possède deux extensions centrales d'ordre 120 : le produit direct $A_5 \times \mathbb{Z}/2\mathbb{Z}$ qui est le groupe des isométries de l'icosaèdre régulier, et le relevé dans $\mathrm{SU}(2)$, appelé groupe icosaédral binaire (aussi isomorphe à $\mathrm{SL}(2;5)$). La table de caractères de A_5 aide à retrouver celle de ces deux groupes.

Pour le groupe $[3;5] = A_5 \times \mathbb{Z}/2\mathbb{Z}$, il y a outre les représentations ρ_U déjà mentionnées, la représentation ε de dimension 1 et tous leur produits tensoriels.

Les degrés des représentations restantes de $2I$ ont leur somme des carrés égale à 60 ; ce sont donc nécessairement $2;2;4$ et 6. La représentation de dimension 4 est obtenue par opération sur les quaternions.

	C_1	C_3	$C_{2;2}$	C_5	C_5^0	fsg	C_3s	$C_{2;2}s$	C_5s	C_5^0s
1	1	1	1	1	1	1	1	1	1	1
ε	1	1	1	1	1	1	1	1	1	1
ρ_U	4	1	0	1	1	4	1	0	1	1
ρ_V	5	1	1	0	0	5	1	1	0	0
ρ_W	3	0	1	φ	$\bar{\varphi}$	3	0	1	φ	$\bar{\varphi}$
$\rho_{W'}$	3	0	1	$\bar{\varphi}$	φ	3	0	1	$\bar{\varphi}$	φ
$\rho_U \otimes \varepsilon$	4	1	0	1	1	4	1	0	1	1
$\rho_V \otimes \varepsilon$	5	1	1	0	0	5	1	1	0	0
$\rho_W \otimes \varepsilon$	3	0	1	φ	$\bar{\varphi}$	3	0	1	φ	$\bar{\varphi}$
$\rho_{W'} \otimes \varepsilon$	3	0	1	$\bar{\varphi}$	φ	3	0	1	$\bar{\varphi}$	φ

Table 2. Table de caractères du groupe $[3;5]$

21. Intégrale de Fresnel et sommes de Gauss complexes

Leçons.

110: Représentations et caractères des groupes abéliens finis

246: Séries de Fourier

Référence: [QZ02]

Théorème 21.1. *Soit* $G_n = \sum_{k=1}^{n} e^{\frac{2ik^2}{n}}$ *la n-ième somme de Gauss. Alors :*

$$G_n = \begin{cases} \sqrt{n} & \text{si } n \equiv 1 [4] \\ 0 & \text{si } n \equiv 2 [4] \\ i\sqrt{n} & \text{si } n \equiv 3 [4] \\ (1+i)\sqrt{n} & \text{si } n \equiv 0 [4] \end{cases} \tag{31}$$

On note $T = \mathbb{R}/\mathbb{Z}$.

Lemme 21.2. *Soit* $f \in C^1_{pm} \cap C(T)$*; alors*

$$\frac{1}{n}\sum_{k=0}^{n-1} f\left(\frac{k}{n}\right) = \sum_{m\in\mathbb{Z}} \hat{f}(mn) \tag{32}$$

Démonstration. D'après le théorème de convergence normale, la famille $\hat{f}(mn)$ est sommable et f est somme de sa série de Fourier. En particulier, en notant $\omega = e^{\frac{2i\pi}{n}}$ nous avons

$$f(k/n) = \sum_{r\in\mathbb{Z}} \hat{f}(r)\,\omega^{rk};$$

d'où le résultat demandé :

$$\sum_{k=0}^{n-1} f\left(\frac{k}{n}\right) = \sum_{k=0}^{n-1}\sum_{r\in\mathbb{Z}} \hat{f}(r)\,\omega^{rk} = \sum_{r\in\mathbb{Z}} \hat{f}(r) \underbrace{\sum_{k=0}^{n-1} \omega^{rk}}_{\substack{n \text{ si } n\mid r; \\ 0 \text{ sinon}}}.$$

On applique le lemme à $f \in C^1_{pm} \cap C(T)$ qui à x associe $e^{2i\pi nx^2}$ sur $[0;1]$: par convergence absolue de $\hat{f}(mn)$ nous pouvons scinder la somme en deux :

$$\frac{G_n}{n} = \sum_{m\in\mathbb{Z}} \hat{f}(2mn) + \sum_{m\in\mathbb{Z}} \hat{f}((2m+1)n)$$

(1) Calcul de la première somme

$$\begin{aligned} \sum_{m\in\mathbb{Z}} \hat{f}(2mn) &= \sum_{m\in\mathbb{Z}} \int_0^1 e^{2i\pi nx^2 - 4i\pi nmx}\,dx \\ &= \sum_{m\in\mathbb{Z}} e^{-2i\pi nm^2} \int_0^1 e^{2i\pi n(x-m)^2}\,dx \\ &= \sum_{m\in\mathbb{Z}} \int_m^{m+1} e^{2i\pi nx^2}\,dx \\ &= \int_1^{+\infty} e^{2i\pi nx^2}\,dx. \end{aligned}$$

L'existence de cette intégrale (semi-convergente) étant justifiable par le calcul

$$\int_1^A e^{2ix^2}\,dx = \int_1^{A^2} \frac{e^{2iu}}{2\sqrt{u}}\,du = \left[\frac{e^{2iu}}{2i\sqrt{u}}\right]_1^{A^2} + \int_1^{A^2} \frac{3e^{2iu}}{4u^{3/2}}\,du$$

Posant $I = \int_{-1}^{+1} e^{2i\pi x^2}\mathrm{d}x$, on obtient finalement

$$\sum_{m\in\mathbf{Z}} \hat{f}(2mn) = \frac{I}{\sqrt{n}}.$$

(2) Calcul de la seconde somme :

$$\begin{aligned}\sum_{m\in\mathbf{Z}} \hat{f}((2m+1)n) &= \sum_{m\in\mathbf{Z}} \int_0^1 e^{2i\pi nx^2 - 2i\pi(2m+1)x}\mathrm{d}x\\ &= \sum_{m\in\mathbf{Z}} e^{-2i\pi n\frac{(2m+1)^2}{2}} \int_0^1 e^{2i\pi n\left(x-\frac{2m+1}{2}\right)^2}\mathrm{d}x\\ &= \sum_{m\in\mathbf{Z}} e^{-in\frac{\pi}{2}} \int_{m+1/2}^{m+3/2} e^{2i\pi n\left(x-\frac{2m+1}{2}\right)^2}\mathrm{d}x\\ &= i^{-n}\frac{I}{\sqrt{n}};\end{aligned}$$

où l'on a utilisé que $(2m+1)^2 \equiv 1 [4]$.

Nous avons donc

$$\forall n > 1,\ G_n = \left(1 + i^{-n}\right) I\sqrt{n} \tag{33}$$

En particulier, $1 = G_1 = (1-i)I$, ce qui donne l'identité

$$\int_{-1}^{+1} e^{2i\pi x^2}\mathrm{d}x = \frac{1+i}{2}$$

Puis

$$G_n = \frac{\left(1-i^n\right)(1+i)}{2}\sqrt{n}.$$

Remarque 21.3. Si p est un nombre premier impair, remarquons que

$$G_p = \sum_{k=0}^{p-1} e^{\frac{2i\pi k^2}{p}} = \sum_{j=0}^{p-1} \left(\sum_{i\in\mathbf{F}_p} \mathbf{1}_{i^2\equiv j [p]}\right).$$

Or, le nombre de racines carrées de a modulo p est donné par $1 + \left(\frac{a}{p}\right)$, d'où

$$G_p = \sum_{a\in\mathbf{F}_p} \left(\frac{a}{p}\right) e^{\frac{2i\pi a}{p}} + \sum_{a\in\mathbf{F}_p} e^{\frac{2i\pi a}{p}} = \sum_{a\in\mathbf{F}_p} \left(\frac{a}{p}\right) e^{\frac{2i\pi a}{p}}.$$

Remarque 21.4. Si on fait tendre n vers $+\infty$ dans le lemme, on obtient $c_0(f)$ comme limite de sommes de Riemann :

$$\lim_{n\to+\infty} \frac{1}{n}\sum_{k=0}^{n-1} f\left(\frac{k}{n}\right) = \lim_{n\to+\infty} \sum_{m\in\mathbf{Z}} \hat{f}(mn) = \hat{f}(0) = \int_{\mathbf{T}} f.$$

22. Equation de la chaleur sur le cercle

Référence: [FGN14, Analyse 4, 1.28]

Soit $u_0 \in C^1_{pm} \setminus C(T)$; on s'intéresse aux solutions $u : T \times \mathbb{R} \to \mathbb{R}$ de l'équation

$$\begin{cases} \frac{\partial u}{\partial t} &= \frac{\partial^2 u}{\partial x^2} \\ u(x;0) &= u_0(x) \end{cases} \tag{34}$$

Théorème 22.1. *Il existe une unique solution à l'équation (34), qui soit continue sur $T \times \mathbb{R}$ et C^2 sur $T \times \mathbb{R}_+^*$. De plus, cette solution est C^1 sur $T \times \mathbb{R}_+^*$, et elle est bornée si et seulement si u_0 est constante.*

Analyse : La fonction de deux variables

$$(x;t) \mapsto u(x;t)e^{-inx}$$

est C^2 sur $T \times \mathbb{R}_+$ et continue sur $T \times \{0\}$; on pose donc $c_n(t) = \int_T u(x;t)e^{-inx}\mathrm{d}x$, et $C_n = c_n(u_0)$.

D'après le théorème de continuité sous le signe $\int$ sur un compact, c_n est continue sur $\mathbb{R}_+$.

D'après le théorème de dérivation sous le signe $\int$ sur un compact, c_n est de classe C^1 sur $\mathbb{R}_+$, et

$$\begin{aligned} c_n'(t) &= \int \frac{\partial u}{\partial t}(x;t)e^{-inx}\mathrm{d}x \\ &= \int_T \frac{\partial^2 u}{\partial x^2}(x;t)e^{-inx}\mathrm{d}x \\ &= -4\pi^2 n^2 c_n(t) \end{aligned}$$

Par conséquent, pour tout $n \in \mathbb{Z}$ nous avons

$$c_n(t) = C_n e^{-4\pi^2 n^2 t}$$

Synthèse : Posons $_n(x;t) = C_n e^{-4\pi^2 n^2 t}e^{inx}$, et $u(x;t) = \sum_{n=-1}^{+1} {}_n(x;t)$. Alors $_n$ est C^1 sur $T \times \mathbb{R}_+$, et

$$\frac{\partial^{k+l}\ {}_n}{\partial^k x \partial^l t} = P(x;n;t)e^{-4\pi^2 n^2 t + inx}$$

où P est polynômiale ; par conséquent la série $\sum_{n=-1}^{+1} \frac{\partial^{k+l}\ {}_n}{\partial^k x \partial^l t}$ est uniformément convergente, et $u(x;t)$ est de classe C^1. D'après ce qui précède et par injectivité de F, c'est l'unique solution.

Si u est définie sur $T \times \mathbb{R}$, alors d'après l'analyse précédente il s'agit encore de

$$u(x;t) = \sum_{n=-\infty}^{+\infty} C_n e^{-4\pi^2 n^2 t + inx}$$

Mais alors (F est de norme 1)

$$|C_n| e^{-4\pi^2 n^2 t} \leq \|u_0\|_{L^1(T)}$$

pour tout $t \in \mathbb{R}$; en particulier en faisant tendre t vers $-\infty$, $C_n = 0$ dès que $n \neq 0$, et u_0 est constante.

Remarque 22.2. La quantité $C_0 = c_0(t)$ est préservée (conservation de l'énergie)

Remarque 22.3. Même en prenant u_0 très régulière (par exemple, réel-analytique) il n'est pas dit que la solution est définie pour les temps négatifs.

23. Nombres de Catalan

Leçons :

124: Anneau des séries formelles,

190: Combinatoire, dénombrement

Référence :
— Knuth Oren Patashnik, Concrete math (pour la série génératrice)
— Engel, Problem solving strategies (pour la méthode combinatoire directe)
Di□culté : **. L'argument combinatoire est délicat, ne pas se précipiter.
Temps : 9 minutes pour la série génératrice, 5 minutes pour le principe de réflexion.

Théorème 23.1. *Soit* (c_n) *la suite des nombres de Catalan définie par*

$$\begin{cases} c_0 = 1 \\ \forall n > 0 \quad c_{n+1} = \sum_{k=0}^{n} c_k c_{n-k} \end{cases} \tag{35}$$

Alors, pour tout $n \in \mathbb{N}$,

$$c_n = \frac{1}{n+1}\binom{2n}{n}$$

Remarque 23.2. Les nombres de Catalan interviennent très souvent dans le dénombrement de structures de données récursives ; ainsi, le nombre c_n est

(1) Le nombre d'arbres binaires à n noeuds

(2) Le nombre d'expressions bien parenthésées avec $2n$ parenthèses

(3) Le nombre de marches aléatoires (Nord, Est) de $(0;0)$ à $(n;n)$ qui restent en-dessous de la diagonale.

Il y a des correspondances bijectives naturelles entre ces trois ensembles.

Remarque 23.3. Soit X une variable de Bernoulli de paramètre $1/2$ (noté $X \sim 1/2$) et X_n sa moyenne. La probabilité que X_n soit restée $> 1/2$ entre 0 et N tend vers 0 quand $N \to +\infty$.

(a) Par une méthode de série génératrice. Soit C la série génératrice des nombres de Catalan :

$$C = \sum_{n>0} c_n X^n$$

On va traduire algébriquement la relation de récurrence et l'intitialisation :

$$C^2 = \sum_{n>0}\left(\sum_{k=0}^{n} c_k c_{n-k}\right) X^n$$

$$XC^2 = \sum_{n>1} c_n X^n = C - 1$$

Donc C est solution d'une équation du second degré à coe□cients dans $\mathbb{Q}[[X]]$:

$$XC^2 - C + 1 = 0$$

On va la résoudre dans $\mathbb{Q}((X))$. Il s'agit de déterminer si $\Delta = 1 - 4X$ possède une racine carrée[23] dans $\mathbb{Q}((X))$.

(1) L'élément $-4X \in 2\mathbb{Q}[[X]]$ est de valuation 1 ; donc il est substituable et $S \mapsto S(-4X)$ est un morphisme d'algèbre de $\mathbb{Q}[[X]]$ (en fait, un automorphisme)

23. Il y a au plus deux racines, puisque $\mathbf{Q}((X))$ est un corps et en particulier un anneau commutatif intègre.

(2) D'autre part

$$\begin{aligned}(1+X)^{\frac{1}{2}\ 2} &= \exp\ \frac{1}{2}\mathrm{Log}\,(1+X)^{\ 2}\\ &= \exp(\mathrm{Log}\,(1+X))\\ &= 1+X\end{aligned}$$

La dernière ligne provient de ce que $\mathrm{Log}\,(1+X)$ est la réciproque de exp 1. Donc les racines carrées de $1+X$ sont $(1+X)^{\frac{1}{2}}$.

Finalement, admet 2 racines carrées, qui sont

$$R = (1+X)^{\frac{1}{2}}\ (\ 4X) = \sum_{n>0} \binom{1=2}{n}\ (\ 4)^n X^n$$

Remarque 23.4. Si $S(0) \neq 0$ et si $S(0)$ est un carré dans K , alors S est un carré dans $K[[X]]$.

Remarquons que $R_+(0) = 1$ (substituer à droite ne change pas le terme constant) tandis que $R\ (0) = 1$. Nous voulons un élément de $\mathbb{Q}[[X]]$; on a donc nécessairement

$$C = \frac{1\ R_+}{2X}$$

On en tire l'expression de c_n : pour $n > 1$

$$\begin{aligned}c_n &= \frac{1}{2}\binom{1=2}{n+1}\ (\ 4)^{n+1}\\ &= (\ 1)^n \frac{4^{n+1}}{2}\frac{(1=2)\ (\ 1=2)\ \cdots\ ((1\ n)=2)}{(n+1)!}\\ &= \frac{2^n(2n!)}{2^n n!(n+1)!} = \frac{1}{n+1}\binom{2n}{n}\end{aligned}$$

(b) Vérification combinatoire « directe » : le principe de réflexion. On connaît la solution et on va s'en servir. Conformément à la troisième interprétation combinatoire, on voit c_n comme le nombre de trajets allant de $(0;0)$ à $(n;n)$ tout en restant en-dessous de la diagonale. Il est équivalent de montrer que le nombre de chemins qui traversent cette diagonale est égal à [24]

$$\binom{2n}{n}\ \frac{1}{n+1}\binom{2n}{n} = \frac{n}{n+1}\binom{2n}{n} = \binom{2n}{n+1}$$

Ce qui est encore le nombre de chemins de $(\ 1;1)$ à $(n;n)$. On va donc essayer d'établir une bijection f entre

— l'ensemble $C^{(n;n)}_{(\ 1;1)}$ des chemins de $(\ 1;1)$ à $(n;n)$

— l'ensemble $C^{0\ (n;n)}_{(0;0)}$ des chemins de $(0;0)$ à $(n;n)$ qui rencontrent la droite : $y = x+1$ au moins une fois.

Pour tout 2 $C^{(n;n)}_{(\ 1;1)}$, soit P le premier point où rencontre . On pose $f(\ )$ dont le tracé est identique à celui de avant P, et est son symétrique par rapport à avant P. On vérifie sans peine que $f(\ )$ 2 $C^{0\ (n;n)}_{(0;0)}$. Réciproquement, si est pris dans $C^{0\ (n;n)}_{(0;0)}$ alors quitte à poser le symétrique de par rapport à avant le premier point de rencontre de , nous avons que $= f(\ )$. Ceci conclut la preuve combinatoire.

Figure 5. La bijection f

24. Pour la dernière égalité de cette ligne, voir que

$$n\binom{2n}{n} = (n+1)\binom{2n}{n\ \ 1} = (n+1)\binom{2n}{n+1}$$

24. Icosaèdre, synthèmes et $\mathrm{Out}(\mathfrak{S}_6)$

Leçons.

104: (3) Groupes finis

105: (2) Groupe symétrique

127: (3) Droite projective et birapport

Références.

Pré-requis.

(1) Simplicité du groupe $\mathfrak{A}_6$.

(2) Si $'$ automorphisme de $\mathfrak{S}_n$ envoie transposition sur transposition, alors $'$ est intérieur.

La démonstration du fait que la suite exacte ci-dessous est scindée ne rentre pas dans le temps imparti pour un développement.

Théorème 24.1. *L'action tautologique de* $\mathrm{PGL}_2(\mathbb{F}_5)$ *sur* $\mathrm{P}^1(\mathbb{F}_5)$ *identifie* $\mathrm{PGL}_2(\mathbb{F}_5)$ *à un sous-groupe transitif de* $\mathfrak{S}_6$ *isomorphe à* $\mathfrak{S}_5$.

Théorème 24.2. *Il existe une suite exacte courte,* scindée

$$f1g \;!\; \mathfrak{S}_6 \;!\; \mathrm{Aut}(\mathfrak{S}_6) \;!\; \mathbb{Z}=2\mathbb{Z} \;!\; f1g: \tag{36}$$

24.1. Preuve du théorème 24.1 d'après [Per96]. $\mathrm{PGL}_2(\mathbb{F}_5)$ opère fidèlement sur les droites vectorielles de $\mathbb{F}_5^2$; modulo une indexation de celles-ci par $f1;:::;6g$ il s'identifie à $H \quad \mathfrak{S}_6$. Par ailleurs

$$jHj = \frac{1}{\mathbb{F}_5} j\mathrm{GL}_2(\mathbb{F}_5)j = \frac{5^2 \quad 1 \quad 5^2 \quad 5}{4} = 120:$$

Donc H est d'indice 6 dans $G = \mathfrak{S}_6$. G opère par translations à gauche sur l'ensemble $G=H$ des classes à gauche ; fHg est fixe, ce qui donne un morphisme

$$\begin{aligned} : G &\;!\; \mathfrak{S}(G=H) \\ H &\;!\; \mathrm{Stab}_G fHg \end{aligned}$$

dont le noyau $K = \ker = \bigcap_{x2G} xHx^{\ 1}$ est distingué dans G. $\mathfrak{A}_6$ est simple, donc les sous-groupes distingués de $\mathfrak{S}_6$ sont $f1g$, $\mathfrak{A}_6$ et $\mathfrak{S}_6$. Puisque K est contenu dans H, il est au moins d'indice 6, donc trivial et est injectif. Vue l'égalité des cardinaux, on a

$$H \;' \mathrm{Stab}_G fHg \;' \mathrm{Stab}_{\mathfrak{S}_6} f1g \;' \mathfrak{S}_5:$$

24.2. Construction d'un automorphisme extérieur de $\mathfrak{S}_6$; la suite exacte. D'après ce qui précède, il existe $: \mathfrak{S}_6 \;!\; \mathfrak{S}_6$ un morphisme qui envoie H sur le sous-groupe H_1 stabilisant 1. Puisque ces deux sous-groupes ne sont pas conjugués (H est transitif, H_1 non), est extérieur ; nous avons donc $\mathrm{Aut}(\mathfrak{S}_6) \not= \mathrm{Int}(\mathfrak{S}_6)$.

Proposition 24.3. $\mathrm{Int}(\mathfrak{S}_6)$ *est d'indice* 2 *dans* $\mathrm{Aut}(\mathfrak{S}_6)$

Démonstration. Notons T_i la classe des produits de i transpositions disjointes dans $\mathfrak{S}_6$ ($i \;2\; f1;2;3g$). Puisque tout automorphisme préserve l'ordre des éléments, et envoie classe de conjuguaison sur classe de conjuguaison, on a un morphisme naturel

$$: \mathrm{Aut}(\mathfrak{S}_6) \;!\; \mathfrak{S}(T_1;T_2;T_3)$$

T_2 est dans $\mathfrak{A}_6$ qui est un sous-groupe caractéristique de $\mathfrak{S}_6$ (c'est le sous-groupe dérivé) donc elle est fixée. Par ailleurs le noyau de est égal à $\mathrm{Int}(\mathfrak{S}_6)$ puisque $'$ est intérieur dès qu'il envoie transposition sur transposition. Conclusion, d'après le premier théorème d'isomorphisme :

$$\mathrm{Aut}(\mathfrak{S}_6)=\mathrm{Int}(\mathfrak{S}_6) \;' \mathrm{Im}(\ ) \quad \mathrm{Stab}(T_2) \;' \mathfrak{S}_2$$

En définitive, on a une suite exacte

$$f1g \;!\; \mathrm{Int}(\mathfrak{S}_6) \;!\; \mathrm{Aut}(\mathfrak{S}_6) \;!\; \mathbb{Z}=2\mathbb{Z} \;!\; f1g$$

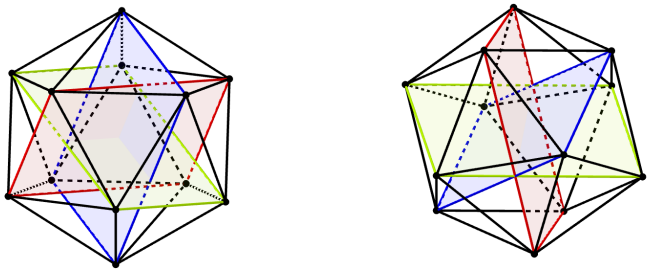


Figure 6. Synthème droite et synthème tordue.

Puisque $\mathrm{Int}(S_6) \simeq S_6/Z(S_6) \simeq S_6$, on a ce qu'on voulait. En particulier, $\mathrm{Aut}(S_6)$ est d'ordre $2 \cdot 6! = 1440$.

24.3. Interprétation géométrico-combinatoire. Pour progresser dans la compréhension de $\mathrm{Aut}(S_6)$ et notamment montrer que (36) est scindée on a besoin de travailler un peu plus concrètement.

Rappelons que l'icosaèdre régulier I possède 12 sommets, donc 6 grandes diagonales. Notons leur ensemble Ω. Une duade est une paire de diagonales de l'icosaèdre et une synthème est une partition de Ω en trois duades. (On peut se représenter une duade comme un rectangle d'or.) Il y a 15 duades et 15 synthèmes ; le graphe d'incidence R des duades et des synthèmes est donc formé sur 30 sommets. L'action du groupe $\mathrm{Iso}^+(I)$ sur les synthèmes n'est pas transitive, comme on peut le voir sur la figure 6.

Définition 24.4. Une pentade synthématique est une collection de 5 synthèmes telle que chaque duade appartient à une et une seule synthème.

Lemme 24.5. *Il y a* 6 *pentades synthématiques.*

Soit $\mathcal{P}$ l'ensemble des pentades synthématiques.

Lemme 24.6. *L'homomorphisme* $S_5 \to S_{\mathcal{P}}$ *associé à l'action tautologique de* S_5 *sur les pentades synthèmatiques est un isomorphisme.*

24.4. $\mathrm{P}^1\mathbf{F}_5$ et l'icosaèdre abstrait. Soit $S = \mathbf{F}_5^2 \setminus \{0\}$ et $[S] = S/\{\pm 1\}$. Notons que $[S]$ possède $\frac{25-1}{2} = 12$ éléments. On introduit le graphe G_+ d'ensemble de sommets $[S]$ dans lequel il y a une arête $[s][s']$ si et seulement si

$$\frac{\det(s,s')}{5} = 1,$$

i.e. si le déterminant de la paire de représentant s et s' est un carré non nul dans $\mathbf{F}_5$ (notons que -1 est un carré modulo 5, donc ce symbole est bien défini). On vérifie que G_+ est un graphe régulier non orienté de valence 5 sur 12 sommets, c'est donc le graphe sous-jacent à l'icosaèdre abstrait (qui est l'ensemble partiellement ordonné obtenu en remplissant les triangles et munissant le tout de la relation d'incidence).

Proposition 24.7. *Dans toute réalisation géométrique maximalement symétrique de l'icosaèdre abstrait, le triplet de paires* $\{(ab),(cd),(ef)\}$ *forme une synthème droite si et seulement si les birapports* $[abcd],[abef],[cdef]$ *sont tous égaux à* -1.

25. Quaternions, groupes SU (2) et SO (3)

Leçons.

101: (3) Actions de groupes

103: (2) Exemples de sous-groupes distingués et de groupes quotient

160: (3) Endomorphismes remarquables d'un espace euclidien

161: (3) Isométries d'un espace a□ne euclidien de dimension finie. Applications en dimension 2 et 3

182: (2) Utilisation des nombres complexes en géométrie

183: (3) Utilisation des groupes en géométrie

Référence. Perrin, Kosmann-Schwarzbach
Di□culté **.
Pré-requis. Existence de l'algèbre à division H ; son centre est R.

Théorème 25.1. *Il existe un isomorphisme de groupes topologiques*[25]

$$\mathrm{SU}(2;\mathbb{C}) = f \quad 1g \;!\; \mathrm{SO}(3)$$

(a) Le groupe G. On rappelle que l'application $\mathbb{H} \quad \mathbb{H} \;!\; \mathbb{R}$, $(q;q^0) \;7!\; \mathrm{Re}(q\overline{q^0})$ est une forme bilinéaire symétrique définie positive, qui induit une norme euclidienne N sur l'algèbre à division H. R est en somme directe, orthogonale pour cette forme, avec l'espace P des quaternions purs. N est multiplicative sur H et le noyau de N est appelé groupe des quaternions unitaires, noté G.
Preuve de la multiplicativité de N [Per96]. On se donne $q;q^0 \; 2 \; \mathbb{H}$; alors comme N est à valeur dans R central dans H

$$N(qq^0) = qq^0\overline{qq^0} = qq^0\overline{q^0}\,\overline{q} = N(q^0)\,q\overline{q} = N(q^0)\,N(q)$$

Proposition 25.2. *Pour tous $q \; 2 \; G$ et $s \; 2$ H, on a $N(qs\overline{q}) = N(s)$. En particulier, G opère sur* H *par isométries pour N via*

$$q:s = qs\overline{q}$$

En outre R *est stable pour cette action, ce qui induit un morphisme continu $s : G \;!$ SO $N_{jP} \quad '$ SO (3).*

1ère preuve (si l'on a construit H comme une sous-algèbre de $M_4(\mathbb{R})$). Par définition

$$\begin{aligned} N(qs\overline{q}) &= \mathrm{Re}(qs\overline{q}) \\ &= \frac{1}{4}\mathrm{tr}_{\mathbb{H}=\mathbb{R}}(qs\overline{q}) \\ &= \frac{1}{4}\mathrm{tr}_{\mathbb{H}=\mathbb{R}}(\overline{q}qs) \\ &= N(s) \end{aligned}$$

2ème preuve (on utilise que R est dans le centre de H). Puisque R est le centre de H et $\overline{q} = q^{\;1}$ pour tout $q \; 2 \; G$, R est stable pour cette action. Son orthogonal $\mathbb{R}^{?N} = P$ l'est donc aussi.

(b) Un premier isomorphisme. Comme le centre de H est exactement R, $\ker s = G \setminus \mathbb{R} = f \quad 1g$. Par ailleurs, montrons que s est surective. Il su□t de montrer qu'elle atteint une partie génératrice, par exemple l'ensemble des renversements. Si l'on se donne $q \; 2 \; G \setminus P$ alors on vérifie que $q^2 \; 2 \; \mathbb{R}$ donc $q^2 = \quad 1$ et $s(q)^2 = 1$; il s'agit d'un renversement et puisque q est stable, c'est le renversement d'axe q dans SO N_{jP} . Conclusion, on a un isomorphisme de groupes

$$(37) \qquad : G = f \quad 1g \;'\; \mathrm{SO}(3)$$

25. En fait, de groupes de Lie

Mieux, c'est un isomorphisme de groupes topologique : En e□et est continu (par définition du quotient $G=f\ 1g$) et bijectif, partant d'un compact à valeur dans un séparé ; c'est un homéomorphisme [26]

(c) Groupe des quaternions unitaires et $\mathrm{SU}(2;\mathrm{C})$. Quitte à choisir une copie de C dans H (par exemple, $\mathrm{R}1+\mathrm{R}i$) on peut voir H comme un C-espace vectoriel de dimension 2 (attention, a priori il y a deux structure, une à droite et une à gauche) de base $(1;j)$. L'opération de G sur H par translation à gauche est C-linéaire pour la structure vectorielle à droite et induit un morphisme injectif $T : G \ ! \ \mathrm{GL}(2;\mathrm{C})$. On calcule que la matrice de $+j$ est

$$T_q = \begin{pmatrix} & \\ & \end{pmatrix}$$

où $j\ j^2 + j\ j^2 = 1$; l'image est donc $\mathrm{SU}(2;\mathrm{C})$ tout entier et on a un isomorphisme de groupes topologiques

$$G \ ' \ \mathrm{SU}(2;\mathrm{C}) \tag{38}$$

.

Remarque 25.3. On a aussi un isomorphisme

$$\mathrm{PSO}(4) \ ' \ (G=f\ 1g) \ (G=f\ 1g) \ ' \ \mathrm{SO}(3) \ \mathrm{SO}(3)$$

Remarque 25.4. La suite exacte courte

$$1 \ ! \ f\ 1g \ ! \ \mathrm{SU}(2) \ ! \ \mathrm{SO}(3) \ ! \ 1$$

ne se scinde pas. En e□et, si on avait une section $: \mathrm{SO}(3) \ ! \ \mathrm{SU}(2)$ d'image H alors on aurait pour tout $p\ 2\ G$, p ou p dans H. Mais alors si p est dans $G \setminus P$ on aurait $p^2 = (\ p)^2 = \ 1$ dans H, ce qui est absurde.

Remarque 25.5. G est simplement connexe (c'est une 3-sphère) et $: G \ ! \ \mathrm{SO}(3)$ est un revêtement. De fait G est (un représentant du) revêtement universel de $\mathrm{SO}(3)$ qui a pour groupe fondamental $\ker \ ' \ \mathrm{Z}=2\mathrm{Z}$.

Remarque 25.6. Les groupes de Lie réels $\mathrm{SO}(3)$ et $\mathrm{SU}(2)$ partagent la même algèbre de Lie $\mathrm{so}(3) \ ' \ \mathrm{su}(2)$ bien qu'ils soient non isomorphes.

Remarque 25.7. $\mathrm{SU}(2)$ n'est pas seulement topologiquement une 3-sphère, il l'est encore géométriquement. En e□et la métrique invariante par translation qui a le plus d'isométries est la métrique riemannienne standard induite par R^4 (les translations dans G sont des rotations de S^3). Sa forme volume est la mesure de Haar.

---

26. Il su□t de montrer (par exemple) que $'$ est fermée. Soit F fermé de $G=f\ 1g$; alors F est compact (fermé dans un compact) et **SO** (3) est séparé, donc $'(F)$ est compact ; en particulier il est fermé.

26. Marche aléatoire sur $\mathbb{Z}^n$, théorème de Polya

Référence. [ZR13] attention coquilles : dans la question 3, remplacer $\frac{1}{1\ q}$ par $\frac{q}{1\ q}$ et dans la question 5, $1\quad y^2$ par $1\quad y^2=2$; puis à la fin, remplacer « la série des p_j converge ssi $n\ 6\ 2$ » par $n > 2$.

Di□culté ***. L'ensemble est trop long ; il faut admettre par exemple la proposition 26.3 et le lemme qui précède.

Pré-requis. Formule d'inversion de Fourier

Théorème 26.1. *Soit M une marche aléatoire*[27] *sur $\mathbb{Z}^n$, telle qu'il existe* e *une* $\mathbb{Z}$*-base du réseau $\mathbb{Z}^n$ avec $M(0) = 0$ et*

$$8i\ 2\ f1;:::ng8\ \ 2\ f\ \ 1g;\ \mathrm{P}(M(t+1) = x + \ \mathrm{e}_i\ j\ M(t) = x) = \frac{1}{2n}$$

Alors

- Si $n\ 6\ 2$, M est presque sûrement récurrente : elle passe presque sûrement une infinité de fois par 0 (et en fait, par n'importe quel $x\ 2\ \mathbb{Z}^n$).

- Si $n > 3$, M est presque sûrement transiente : elle passe presque sûrement un nombre fini de fois par 0.

La stratégie globale de la preuve correspond à se ramener à un problème d'intégrabilité. Concrètement, on pose $p_j = \mathrm{P}(M(j) = 0)$, puis on montre successivement que

$$0 \text{ est transient} \quad ( ) \quad \sum_{\mathbb{Z}^j} p_j < +1$$

$$( ) \quad \int_{B(0;1)\ \mathbf{R}^n} \frac{\mathrm{d}x}{kxk^2} < +1$$

$$( ) \quad n > 2$$

(Remarquons que le sens indirect de la première équivalence résulte simplement du lemme de Borel-Cantelli. En e□et si l'on écrit $A_j = (M(j) = 0)$ alors

$$f0 \text{ est récurrent}g = \limsup_j A_j$$

(a) La première équivalence. On notera q_k (resp. u_k) la probabilité que la marche aléatoire repasse au moins (resp. exactement) k fois par 0.

Lemme 26.2. *Posons $q = q_1$. Alors les suites (q_k) et (u_k) admettent les expressions*

$$q_k = q^k \tag{39}$$

$$u_k = q^k(1\quad q) \tag{40}$$

Démonstration. (39) s'obtient par récurrence sur k : on écrit que

$$\begin{aligned}\mathrm{P}(k+1 \text{ retours en } 0) &= \mathrm{P}(k+1 \text{ retours en } 0 j k \text{ retours en } 0)\\ &\quad \mathrm{P}(k \text{ retours en } 0)\\ &= qq_k\end{aligned}$$

Puis $u_k = q_k\quad q_{k+1}$ et on déduit ainsi (40) de (39) (u_k et q_{k+1} correspondent à des évènements disjoints dont l'union est de probabilité q_k).

Proposition 26.3. *Soit $p_j = \mathrm{P}(M(j) = 0)$. Alors M repasse presque sûrement une infinité de fois par 0 ssi* P *p_j diverge.*

---

27. Formalisation : M est une variable aléatoire définie sur l'univers des mots d'alphabet $= f\ \mathbf{e}_i g$, muni de la tribu cylindrique, probabilisé par

$$\mathbf{P}(! \ \ ^?) = (2n)^{\ j\ !\ j}$$

L'existence de ces objets n'est nullement immédiate.

Démonstration. Désignons par N la variable aléatoire qui compte le nombre de retours à l'origine. Alors

$$\mathrm{E}[N] = \sum_{k \in \mathbf{N}} k u_k = (1-q) \sum_{k \in \mathbf{N}} k q^k = \frac{q(1-q)}{(1-q)^2} = \frac{q}{1-q}$$

En effet

$$\sum_{k>1} k q^{k-1} = \left(\sum_k X^k \right)'_{X=q} = \left(\frac{1}{1-X} \right)'_{X=q} = \frac{1}{(1-q)^2}$$

D'autre part, N est somme des N_k variables aléatoires de Bernoulli caractéristiques de l'évenement $M(k) = 0$ donc

$$\mathrm{E}[N] = \sum_k \mathrm{E}[N_k] = \sum_j p_j$$

(b) Fonction caractéristique de $M(j)$. On pose

$$F_j(x) = \mathrm{E}\left[e^{i\langle M(j); x \rangle} \right] = \sum_{r \in \mathbf{Z}^n} e^{i\langle r; x \rangle} \mathrm{P}(M(j) = r)$$

qui est bien définie car $e^{i\langle M(j);x\rangle}$ est une variable aléatoire bornée, donc admet un moment d'ordre 1. Si on pose $e(j) = M(j) - M(j-1)$ les variables aléatoires $e(j)$ sont indépendantes et

$$F_j(x) = \mathrm{E}\left[e^{i\langle \sum_{k=1}^{j} e(k); x \rangle} \right] = \prod_{k=1} e^{i\langle e(k); x \rangle} = F_1(x)^j$$

où

$$F_1(x) = \frac{1}{n} \sum_{i=1} \cos(x_i)$$

D'après la formule d'inversion de Fourier[28] on peut retrouver la loi de $M(j)$ à partir de F_j via

$$\begin{aligned} \mathrm{P}(M(j) = z) &= \frac{1}{(2\pi)^n} \mathcal{F}(F_j)(z) \\ &= \frac{1}{(2\pi)^n} \int_{[0;2\pi]^n} F_j(x) e^{-i\langle z; x \rangle} \mathrm{d}x \end{aligned}$$

En particulier,

$$p_j = \mathrm{P}(M(j) = 0) = \frac{1}{(2\pi)^n} \int_{[0;2\pi]^n} F_1(x)^j \, \mathrm{d}x \tag{41}$$

(c) La fonction ; fin de la preuve. D'autre part, soit la fonction génératrice[29] des p_j définie pour tout réel < 1 par

$$(r) = \sum_{j \in \mathbf{N}} p_j r^j$$

28. Dans quels espaces ? $L^2(\mathbf{Z}^n)$ $ $L^2(\mathbf{T}^n)$ si l'on veut, mais en fait on n'a pas besoin d'un espace aussi grand. Il suffit de

support fini (compact) $\overset{F}{!}$ polynômes trigonométriques

29. Attention, cette terminologie est dangereuse. Il ne s'agit pas de la série génératrice d'une variable aléatoire discrète au sens des probabilités.

D'après la proposition 26.3 et le théorème de convergence monotone de Beppo-Levi, le caractère récurrent de 0 est lié à l'existence d'une limite finie en 1 pour la fonction . On replace 41 dans l'expression de , cela donne

$$(r) = \sum_{j \in \mathbf{N}} \frac{r^j}{(2\ )^n} \int_{[0;2\ ]^n} F_1(x)^j \, \mathrm{d}x$$

Puisque $kF_1k_{\ 1}\ 6\ 1$, on a bien pour tout $r < 1$

$$\sum_{j \in \mathbf{N}} \frac{r^j}{(2\ )^n} \int_{[0;2\ ]^n} F_1(x)^j \ \mathrm{d}x\ 6 \sum_{j \in \mathbf{N}} r^j = \frac{1}{1\quad r} < 1$$

Donc, d'après le théorème de Fubini-Lebesgue (pour la mesure de comptage sur N et la mesure de Lebesgue sur $[0;2\ ]^n$)

$$\begin{aligned}(r) &= \frac{1}{(2\ )^n} \int_{[0;2\ ]^n} \left(\sum_{j \in \mathbf{N}} r^j F_1(x)^j \right) \mathrm{d}x \\ &= \frac{1}{(2\ )^n} \int_{[0;2\ ]^n} \frac{\mathrm{d}x}{1\quad rF_1(x)}\end{aligned}$$

Ainsi, 0 est récurrent ssi $\frac{1}{1\quad rF_1}$ est intégrable sur $[0;2\ ]^n$. Remplaçant F_1 par son expression, on s'aperçoit que les seuls lieu de divergence sont les coins de cet hypercube. On peut donc se contenter d'étudier $\frac{1}{1\quad rF_1}$ au voisinage de 0 : ici à l'aide de la formule de Taylor-Young à l'ordre 4 pour la fonction cos

$$\begin{aligned}F_1(x) &= \frac{1}{n} \sum_{i=1}^{n} \cos(x_i) \\ &= 1\quad \frac{1}{2} \sum_{i=1}^{n} x_i^2 + O\left(x_1^4 + \quad + x_n^4\right) \\ &= 1\quad kxk^2 =2 + O\left(kxk^4\right)\end{aligned}$$

Pour passer de $O\left(x_1^4 + \quad + x_n^4\right)$ dans la deuxième ligne à $O\left(kxk^4\right)$ dans la troisième, on a utilisé l'inégalité de Cauchy-Schwarz :

$$x_1^4 + \quad + x_n^4\ 6\ n^2\ \left(x_1^2 + \quad + x_n^2\right)^2$$

Finalement, 0 est récurrent ssi $\int_{[0;1]^n} \frac{\mathrm{d}x}{kxk^2} < 1$

L'intégrande est radiale ; quitte à e□ectuer le changement de variables $r = kxk$ et à poser A_n la surface de la $(n\quad 1)$-sphère euclidienne on se ramène à

$$\int_{B(0;1)} \frac{\mathrm{d}x}{kxk^2} = \int_0^1 A_n \frac{r^{n\ 1}}{r^2} \mathrm{d}r < 1 \quad () \quad n \quad 3 > \quad 1 \quad () \quad n > 2$$

On retrouve bien la condition voulue.

---

27. Méthode de Newton pour les polynômes

Référence. [CLF96] Attention, il y a un léger oubli dans le corrigé de la question 2 : $f''(z_n) = O(1)$ est utilisé sans justification adéquate.

Di□culté ***. Développement technique. Ne pas oublier de dériver deux fois à droite de $_r$.

Théorème 27.1. *Soit P un polynôme à coe cients réels, $_1;:::;_r$ ses racines dans $\mathbb{C}$ de multiplicités $m_1;:::m_r$. On suppose que $_r$ est réelle que que pour tout $i \in f1;:::r\ \ 1g$, $\mathrm{Re}(_i) \leq _r$. On considère la méthode de Newton associée à P :*

$$\begin{cases} x_0 > _r \\ x_{n+1} = x_n \quad \frac{P(x_n)}{P'(x_n)} \end{cases}$$

Alors $x_n \to _r$ et plus précisément :

- Si $_r$ est racine simple alors pour tout $c > 0$,

$$x_n \quad _r = o(c^n) \tag{42}$$

- Si $_r$ est racine multiple alors il existe > 0 tel que

$$x_n \quad _r \quad 1 \quad \frac{1}{m_r}^n \tag{43}$$

(a) Etude de la fonction $f(x) = x \quad \frac{P(x)}{P'(x)}$. D'après le théorème de Gauss-Lucas les racines de P' et P'' sont dans $\mathrm{Conv}_i(_i)$, lui-même contenu dans $fz\ j\ \mathrm{Re}(z) \leq _r g$, de sorte que P' et P'' sont strictement positives sur $]_r; 1[$. La fonction f est bien définie et deux fois dérivable sur $]_r; +1[$; de plus nous avons $f(x) < x$ pour $x > _r$. Au voisinage à droite de $_r$, on a que

$$\begin{aligned} \frac{P'(x)}{P(x)} = \sum_{i=1}^{\not} \frac{m_i}{x \quad _i} &= \frac{m_r}{x \quad _r} + \sum_{i<r} \frac{m_i}{_i \quad _r} + o(1) \\ &= \frac{m_r}{x \quad _r} + O(1) \end{aligned}$$

Ceci indique que f se prolonge par continuité en $_r$ avec $f(_r) = _r$. Par ailleurs le calcul de la dérivée donne

$$\begin{aligned} 8x > _r; \quad f'(x) &= 1 \quad \frac{P'(x)^2 \quad P(x)P''(x)}{P'(x)^2} \\ &= \frac{P(x)P''(x)}{P'(x)^2} = \frac{P'(x)}{P(x)} \quad ^1 \frac{P''(x)}{P'(x)} \\ &= \sum_{i=1}^{\not} \frac{m_i}{x \quad _i} \quad ! \quad ^1 \quad 0 \quad @ \sum_{i=1}^{\not} \frac{m_i}{x \quad _i} \quad \frac{1}{_i} + \sum_{j=1}^{\not} \frac{n_j}{x \quad _j} \quad 1 \quad A \end{aligned}$$

où les $_j$ sont les racines de P' (avec multiplicités n_j) qui ne sont pas des racines de P ; celles ci sont de partie réelle $< _r$. Quand $x \to _r$ on obtient

$$\lim_{x \to _r^+} f'(x) = 1 \quad \frac{1}{m_r}$$

D'après le théorème de prolongement de la dérivée, on en déduit que f est C^1 sur $[_r; +1[$ avec[30] $f'(_r) = 1 \quad \frac{1}{m_r}$. Par ailleurs $f' > 0$ donc f est croissante

30. Autre argument peut-être plus direct. f' est une fraction rationnelle sans pôle en $_r$ (sinon f en aurait un aussi). Puisque $x \not\to \frac{1}{x}$ est dérivable de dérivée $\frac{1}{x^2}$ on en déduit que

$$\begin{aligned} f(x) &= x \quad \frac{m_r}{x \quad _r} \quad ^1 + O\ (x \quad _r)^2 \\ &= x \quad \frac{x \quad _r}{m_r} + O\ (x \quad _r)^2 \end{aligned}$$

(b) Convergence de la méthode de Newton. f est croissante sur $[\ _r; +1[$, et $f(x) < x$ pour tout $x >\ _r$, donc (par une récurrence immédiate) $x_n >\ _r$ pour tout n et la suite (x_n) est décroissante ; x_n converge vers une limite $\grave{}$ et par continuité de f, nous avons que $f(\grave{}) = \grave{}$ donc $\grave{} =\ _r$. Pour la rapidité de la convergence, deux cas se présentent

(1) $_r$ est une racine simple ; alors $f'(\ _r) = 0$. Puisque f est continue sur $[\ _r; x_n]$ et dérivable sur $]\ _r; x_n[$, d'après l'égalité des accroissements finis il existe y_n dans ce dernier intervalle tel que

$$x_{n+1}\ \ _r = f(x_n)\ \ f(\ _r) = f'(y_n)(x_n\ \ _r)$$

Puisque $y_n\ !\ _r$ quand $n\ !\ 1$, nous avons que

$$\lim_{n\ !\ +1} \frac{x_{n+1}\ \ _r}{x_n\ \ _r} = f'(\ _r) = 0 \tag{44}$$

La convergence (42) s'ensuit directement

(2) $_r$ est une racine multiple. Puisque f est de classe C^1 sur $[\ _r; x_n]$ et deux fois dérivable sur $]\ _r; x_n[$, d'après la formule de Taylor-Lagrange à l'ordre 2 il existe z_n dans ce dernier intervalle tel que

$$\begin{aligned} x_{n+1}\ \ _r &= f'(\ _r)(x_n\ \ _r) + \frac{1}{2}f''(z_n)(x_n\ \ _r)^2 \\ &= (x_n\ \ _r)\ \ f'(\ _r) + \frac{f''(z_n)}{2}(x_n\ \ _r) \end{aligned}$$

Or il faut remarquer que $f''(x)$ est une fraction rationnelle de x qui n'a pas de pôle en $_r$ (sinon ce serait aussi le cas de f') En particulier nous pouvons écrire $f''(z_n) = O(1)$. Il ressort que

$$\ln(x_{n+1}\ \ _r) = \ln(x_n +\ _r) + u_n$$

où u_n est une suite sommable ; on en déduit ce que l'on souhaitait.

Remarque 27.2. Dans le cas où $_r$ est racine simple, on peut dire mieux en poussant à l'ordre 2 :

$$x_{n+1}\ \ _r = \frac{1}{2}f''(z_n)(x_n\ \ _r)^2$$

Avec $f''(z_n)$ qui converge vers une constante : on dit que la convergence est quadratique. Ceci est à rapprocher du lemme de Hensel pour les zéros simples des polynômes à coefficients dans $\mathbb{Z}_p$.

Remarque 27.3. Si $_r$ est racine multiple, il y a plusieurs méthodes pour se ramener à une convergence quadratique :

- Si P a des coefficients raisonnables (par exemple dans $\mathbb{Q}$) il est possible de mener à bien en temps fini le calcul exact de $R = \text{pgcd}(P; P')$ unitaire ; alors $_r$ est racine simple de R
- Sinon, on utilise la technique d'accélération de convergence d'Aitken.

Ceci nous dit que quand $x\ !\ _r$

$$\frac{f(x)\ \ _r}{x\ \ _r} = 1\ \ \frac{1}{m_r} + O\ (x\ \ _r)^2$$

Autrement dit f est dérivable en $_r$ de dérivée $1\ \ \frac{1}{m_r}$; puisque f est une fraction rationnelle, f est C^1 sur $[1; 1[$.

28. Théorème de réalisation de Borel

Leçons.

207: Prolongement de fonctions

228: Continuité et dérivabilité des fonctions réelles de la variable réelle

241: Suites et séries de fonctions

Référence. Rouvière

Di□culté *.

Pré-requis. Théorème de prolongement de la dérivée. Formule de Leibniz. Convergence normale.

Théorème 28.1. *Soit* (a_n) *une suite réelle. Il existe* $' \in C^1(\mathbb{R})$ *telle que* $'^{(m)}(0) = a_m$ *pour tout* $m \in \mathbb{N}$.

Remarque 28.2. Comparer avec le cas complexe, où la condition devient (critère d'Hadamard)

$$\limsup_{m \to +\infty} (a_m/m!)^{1/m} < +\infty$$

C'est évidemment une condition su□sante dans le cas réel (on peut alors remplacer C^1 par réel-analytique).

Corollaire 28.3. *Soit* $[\ ;\ ]$ *un segment de* $\mathbb{R}$ *et* $' \in C^1([a;b])$ *(ce qui signifie que toutes les dérivées ont des limites finies à droite en et à gauche en). Il existe* $\in C^1(\mathbb{R})$ *telle que* $_{|[\ ;\ ]} = '$.

(a) Existence de fonction plateau.

Lemme 28.4. *Il existe* $f \in C^1$ *telle que* $f(x) = 1$ *si* $|x| \leq 1/2$ *et* 0 *si* $|x| \geq 1$.

Démonstration. On part de la fonction

$$g : x \mapsto \begin{cases} \exp\left(\frac{1}{1-x^2}\right) & |x| < 1 \\ 0 & |x| > 1 \end{cases}$$

g est C^1 : les dérivées de g sur $]-1;1[$ sont de la forme $g^{(m)}(x) = r(x)\exp\left(\frac{1}{1-x^2}\right)$ et par les théorèmes usuels de comparaison

$$g^{(m)}(x) \underset{x \to -1}{=} o(1)$$

De sorte que l'on peut conclure à l'aide du théorème de prolongement de la dérivée. Soit h la primitive de g telle que $h(-1) = 0$; alors h est C^1 et constante égale à $\int_{\mathbb{R}} g$ sur $[1; +\infty[$. Quitte à renormaliser h pour $k \geq k_1$, puis à poser

$$f(x) = h(16 + 4x)\, h(16 - 4x)$$

on vérifie que f possède les propriétés voulues.

(b) Analyse. Inspiré par le cas analytique, nous recherchons $'$ sous la forme

$$'(x) = \sum_{k=0}^{+\infty} f(\ _k x)\, a_k \frac{x^k}{k!}$$

l'espoir étant que fixer les $_k > 0$ ultérieurement permettra d'éviter la divergence de cette série de fonctions et de ses dérivées. On pose donc

$$f_k(x) = f(\ _k x)\, a_k \frac{x^k}{k!}$$

et on cherche à borner les dérivées de f_k. D'après la formule de Leibniz

$$f_k^{(m)}(x) = a_k \sum_{p=0}^{\infty} \binom{m}{p} \binom{m}{k}\ ^p f^{(p)}(\ _k x)\, \frac{x^{k\ p}}{(k\ p)!}$$

Pour $|x| > 1/\varepsilon_k$, f_k et toutes ses dérivées sont nulles. Pour $|x| \leq 1/\varepsilon_k$ nous avons en posant $M_m = \sup_{p=0}^{m} \|f^{(p)}\|_1$, pour $m \leq k$

$$f_k^{(m)}(x) \leq |a_k| M_m 2^m \varepsilon_k^{m-p} \frac{k!}{(k-m)!} = |a_k| M_m 2^m \frac{k!}{(k-m)!}$$

En particulier, si l'on fixe $\varepsilon_k = \max(1, |a_k|)$ on a que pour $k > m$, $\varepsilon_k^{m-k} |a_k| \leq 1$ et $f_k^{(m)}(x) \leq \frac{2^m M_m}{(k-m)!}$. La série de fonctions $\sum_{k>m} f_k^{(m)}$ converge donc normalement sur $\mathbb{R}$, ceci pour tout $m > 0$. On en déduit que f est bien définie et C^1, et que $f^{(m)}$ s'obtient par sommation des $f_k^{(m)}$. Puisque par ailleurs, nous avons

$$f_k^{(m)}(0) = \delta_{m,k} a_k$$

la fonction f convient bien.

(c) Preuve du corollaire. D'après le théorème de réalisation de Borel, il existe φ (resp. ψ) définie sur $\mathbb{R}$ telle que $\varphi^{(m)}(\alpha) = \varphi^{(m)}(\beta)$ pour tout m (de même pour ψ). On pose ensuite

$$\tilde{\varphi}(x) = \begin{cases} \varphi(x) & x < \alpha \\ \varphi(x) & \alpha \leq x \leq \beta \\ \psi(x) & x > \beta \end{cases}$$

D'après le théorème de prolongement de la dérivée, $\tilde{\varphi}$ est C^1 sur $\mathbb{R}$.

29. Une application du théorème de Banach-Steinhaus

Référence: :

Théorème de Banach et Steinhaus. Commençons par rappeler l'énoncé du théorème de Banach et Steinhaus

Théorème 29.1. *Soient E un espace de Banach, F un espace vectoriel normé, $(\varphi_i)_{i\in I}$ une famille (pas forcément dénombrable) d'applications linéaires continues de E dans F. Alors*

- *Soit* $\sup_{i\in I} |||\varphi_i||| < +\infty$
- *Soit, il existe $x \in E$ tel que la famille $(\varphi_i(x))_{i\in I}$ n'est pas bornée dans F.*

Démonstration. Si $\sup_{i\in I} |||\varphi_i||| = M < +\infty$, il est clair que pour tout x dans E, et i dans I, $\|\varphi_i(x)\| \leq M\|x\|$. C'est l'autre sens qui est moins automatique, il fait intervenir la complétude de E et le lemme de Baire.

Sinon, plaçons nous dans le second cas, et posons

$$\Omega_k = \{x \in E \mid \sup_{i\in I} \|\varphi_i(x)\| > k\}$$

Ω_k est ouvert (c'est l'union sur $i \in I$ des $\|\varphi_i\|^{-1}]k;+\infty[$ qui sont ouverts par continuité des φ_i).

Si tous les Ω_k sont denses, le lemme de Baire assure que $\bigcap \Omega_k$ est dense, en particulier non vide. Prenant x dans cette intersection, on en déduit que $\sup_{i\in I} \|\varphi_i(x)\| = +\infty$, autrement dit la famille (φ_i) est non uniformément bornée.

Sinon, l'un des Ω_k, disons Ω_{k_0} est non-dense dans E, et donc son complémentaire contient une boule ouverte $B(x;\varepsilon)$. Pour tout y dans E de norme inférieure à ε, et pour tout i dans I,

$$\|\varphi_i(y)\| = \|\varphi_i(x+y) - \varphi_i(x)\| \leq \|\varphi_i(x)\| + \|\varphi_i(x+y)\| \leq 2k_0$$

Ceci implique

$$\sup_{i\in I} |||\varphi_i||| \leq \frac{2k_0}{\varepsilon} < +\infty$$

Divergence d'une série de Fourier. Soit $E = C_2(\mathbb{R};\mathbb{C})$ muni de la norme uniforme. C'est un espace de Banach. On considère la suite d'applications

$$\begin{aligned} \ell_n : E &\to \mathbb{C} \\ f &\mapsto \sum_{k=-n}^{n} c_n(f) \end{aligned}$$

où $c_n(f)$ est le coefficient de Fourier d'ordre n, à savoir

$$c_n(f) = \frac{1}{2\pi}\int_0^{2\pi} f(t)e^{-int}dt$$

Proposition 29.2. *La suite $(|||\ell_n|||)_{n\in\mathbb{N}}$ n'est pas bornée.*

Démonstration. On peut réécrire la somme des coefficients de Fourier jusqu'à n à l'aide du noyau de Dirichlet sous la forme suivante :

$$\ell_n(f) = \frac{1}{2\pi}\int_0^{2\pi} \frac{\sin\left((2n+1)\frac{t}{2}\right)}{\sin\frac{t}{2}} f(t)\,dt = \frac{1}{2\pi}\int_0^{2\pi} D_n(t)\,f(t)$$

Nous avons $|||\ell_n||| \geq \frac{1}{2\pi}\int |D_n(t)|dt$. Prenons alors $\varepsilon > 0$, et

$$f_\varepsilon(t) = \frac{D_n(t)}{|D_n(t)| + \varepsilon}$$

La fonction f a pour avantage d'être à la fois un élément de E, et d'approcher le signe de D_n. On vérifie que $kf\ k \quad 1$ d'une part, et d'autre part que

$$k`_n(f\ )k = \int \frac{D_n^2(t)}{jD_n(t)j + } \quad !\ \int \quad jD_n(t)j\,dt$$

Conclusion,

$$\begin{aligned} jjj`_n jjj &= \frac{1}{2} \int \quad jD_n(t)j\,dt \\ &= \frac{1}{} \int \quad \frac{\sin((n+1=2)\,t)}{\sin(t=2)}\,dt \\ &\quad \frac{2}{} \int_0^{} \quad \frac{\sin((n+1=2)\,t)}{t}\,dt \\ &\quad \frac{2}{} \int_0^{(n+1=2)} \quad \frac{\sin t}{t}\,dt \end{aligned}$$

Or, nous avons

$$\int_0^{+1} \frac{j\sin tj}{t}dt \quad \int_0^{+1} \frac{\sin^2 t}{t}dt \quad \int_{=2}^{+1} \frac{\cos^2 u}{u}du$$

où l'on a fait le changement de variables $u = t + \ =2$ pour la dernière inégalité, et

$$\int_{=2}^{+1} \frac{\cos^2 t + \sin^2 t}{t}dt = \int_{=2}^{+1} \frac{dt}{t} = +1$$

D'où

$$\int_0^{(n+1=2)} \frac{j\sin tj}{t}dt \quad ! \quad \int_0^{+1} \frac{j\sin tj}{t}dt$$

on en déduit la propriété demandée[31].

Corollaire 29.3. *Il existe f 2 E telle que la série de Fourier $\sum c_n(f)\,e^{int}$ diverge en 0.*

Le corollaire résulte de la proposition et du théorème de Banach et Steinhaus.

Remarque 29.4. Le résultat précédent est non constructif ; toutefois nous pourrions trouver un exemple f concret. Le théorème de convergence simple de Dirichlet donne comme

31. On pourrait montrer, plus précisément, que quand x tend vers $+1$ nous avons

$$\int_0^{x} \frac{j\sin tj}{t}dt \quad \frac{2}{}x$$

30. Lemme de Morse à deux variables

Leçons.

214: (2) Inversion locale, fonctions implicites. Applications.

215: (3) Applications di érentiables sur un ouvert de R^n

217: (2) Sous-variétés de R^n. Applications

218: (3) Application des formules de Taylor

Référence. Rouvière
Di culté *.
Pré-requis. Lemme d'inversion locale
Formule de Taylor avec reste intégral à plusieurs variables

Théorème 30.1. Soit $f : R^2 ! R$ de classe C^3. On suppose que la forme hessienne $d^2f(0)$ est non dégénérée. Alors il existe un di éomorphisme $' : V ! W$ où V et W sont des voisinages de 0 dans R^2 tel que $'(0) = 0$ et si $'(x;y) = (u(x;y); v(x;y))$ on a

$$f(x;y) = f(0) + df(0)(x;y) \quad u(x;y)^2 \quad v(x;y)^2 \tag{45}$$

où les signes dépendent de la signature de $d^2f(0)$.

Lemme 30.2. Il existe $,$ et $$ des fonctions C^1 sur un voisinage de 0 telles que

$$f(x;y) = f(0) + df(0)(x;y) + (x;y)x^2 + 2(x;y)xy + (x;y)y^2$$

Démonstration. D'après la formule de Taylor avec reste intégral à l'ordre 2, nous pouvons écrire

$$\begin{aligned} f(x;y) &= f(0) + df(0)(x;y) + \int_0^1 (1-t)\, d^2f(tx;ty)(x;y)^2\, dt \\ &= f(0) + df(0)(x;y) \\ &\quad + \int_0^1 (1-t)\,\partial_{11}f(tx;ty)\,x^2\,dt + \int_0^1 (1-t)\,\partial_{22}f(tx;ty)\,y^2\,dt \\ &\quad + 2\int_0^1 (1-t)\,\partial_{12}f(tx;ty)\,xy\,dt \end{aligned}$$

On pose ainsi

$$\begin{aligned} (x;y) &= \int_0^1 (1-t)\,\partial_{11}f(tx;ty)\,dt \\ (x;y) &= \int_0^1 (1-t)\,\partial_{12}f(tx;ty)\,dt \\ (x;y) &= \int_0^1 (1-t)\,\partial_{22}f(tx;ty)\,dt \end{aligned}$$

La fonction f est C^3, donc les fonctions $[0;1] \times R^2 ! R$, qui à $(t;x;y)$ associent $(1-t)\,\partial_{ij}f(tx;ty)$ sont C^1 par composition. D'après le théorème de dérivation sous le signe $\int$ pour paramètre dans un localement compact, $,$ et $$ sont C^1. En outre

$$(0) = \partial_{11}f(0); \quad (0) = \partial_{12}f(0); \quad (0) = \partial_{22}f(0)$$

Ensuite, on procède à la réduction de la forme $(; ;)$; plus précisément on montre que celle-ci peut s'e ectuer de manière C^1 assez proche de l'origine.

Commençons par supposer que $\partial_{11}f(0)$ et $\partial_{22}f(0)$ sont non tous deux nuls. Quitte à changer f en f on peut supposer que $(0) > 0$. Par continuité de $$, celle ci est non nulle

sur un voisinage V de 0. On écrit alors

$$\begin{aligned}(x;y)\,x^2 + 2\ (x;y)\,xy &+ (x;y)\,y^2 = (x;y)\left[x^2 + \frac{2\ (x;y)}{(x;y)}xy + \frac{(x;y)}{(x;y)}y^2\right] \\ &= (x;y)\left[x + \frac{(x;y)}{(x;y)}y\right]^2 + \frac{^2 - (x;y)}{^2\,(x;y)}y^2\end{aligned}$$

Posons

$$\begin{aligned}u(x;y) &= \sqrt{(x;y)}\,x + \frac{(x;y)}{\sqrt{(x;y)}}y \\ v(x;y) &= \frac{\sqrt{(^2 -)\,(x;y)}}{\sqrt{(x;y)}}y\end{aligned}$$

où $= 1$ (ceci dépend de la signature de $d^2f(0)$). Alors u et v sont C^1 par composition. De plus

$$\begin{pmatrix}\frac{@u}{@x} & \frac{@u}{@y} \\ \frac{@v}{@x} & \frac{@v}{@y}\end{pmatrix} = \begin{pmatrix}\sqrt{(0)} & \cdot \\ 0 & \sqrt{\frac{^2 - (0)}{(0)}}\end{pmatrix}$$

Qui est de déterminant non nul. D'après le lemme d'inversion locale, quitte à restreindre V, $'$ réalise un di éomorphisme de V sur W et on a l'expression voulue.

Il reste à traiter le cas où $@_{11}f(0) = @_{22}f(0) = 0$. Quitte à poser $X = x + y$ et $Y = x - y$ et à changer de variables, on se ramène au cas précédent (une forme quadratique non dégénérée sur $\mathbb{R}^2$ admet au plus deux droites isotropes).

Remarque 30.3. La preuve générale dans le cas où $\mathbb{R}^n$ remplace $\mathbb{R}^2$ est plus technique mais pas fondamentalement di érente. Il s'agit essentiellement de montrer qu'il existe : $V \to GL(n;\mathbb{R})$ de classe C^1 telle que si A est la matrice de la forme quadratique obtenue à l'aide de la formule de Taylor reste intégral,

$$^t(x)\,A(x)\,(x) = {}^t(0)\,A(0)\,(0) = I_{p;q}$$

où $(p;q)$ est la signature de $d^2f(0)$.

31. Théorème de Wedderburn

Thèmes : anneaux, corps

Outils : techniques vectorielles sur les corps, équation aux classes, polynômes cyclotomiques

Références : Perrin, Blanchard (les corps non commutatifs)

On lit souvent la phrase « les corps seront supposés commutatifs ». Pour éviter la confusion, les anneaux à division (ie, où tout élément possèdent un inverse) portent parfois le nom de corps gauche.

L'exemple le plus important de corps non commutatif est peut-être la $\mathbb{R}$-algèbre $\mathbb{H}$ des quaternions de Hamilton. Certaines propriétés usuellement énoncées pour les corps commutatifs entrent en défaut.[32]

Le théorème de Wedderburn stipule que cette distinction entre corps et corps gauche n'est en réalité pas effective dans le cas fini :

Théorème 31.1. Les corps gauches finis sont des corps.

Démonstration. La preuve suivante est dûe à Witt. Elle se déroule en 4 étapes. On désigne par k un corps gauche fini.

(a) k est un espace vectoriel sur son centre. Les techniques vectorielles s'appliquent toujours dans le cas des corps gauches : si $k_1 \subset k_2$ est une extension de corps gauche, et si k_1 est commutatif [33], k_2 est muni d'une structure de k_1 - espace vectoriel donnée par l'addition sous-jacente et la loi de multiplication externe

$$\begin{aligned} k_1 \times k_2 &\to k_2 \\ (\lambda_1, \lambda_2) &\mapsto \lambda_1 \cdot \lambda_2 = \lambda_1 \lambda_2 \end{aligned}$$

Remarque 31.2. On peut aussi introduire une structure de k_1-espace vectoriel sur k_2 par $\lambda_1 \cdot \lambda_2$. Celle-ci est a priori différente de la précédente[34].

Le centre Z du corps gauche k est un corps commutatif de cardinal q. Comme k est un Z-espace vectoriel, $|k| = q^n$ pour $q > 2$ et un certain n. Il s'agit dans la suite de montrer que $n = 1$, autrement dit $k = Z$.

(b) Formule des classes pour l'action de conjugaison de k^*. Le groupe des inversibles k^* agit sur lui-même par conjugaison. L'orbite de $x \in k^*$ est notée $\omega(x)$; elle est réduite à $\{x\}$ si et seulement si $x \in Z^*$. On note par ailleurs k_x le stabilisateur de x, augmenté de l'élément $\{0\}$. k_x est un sous-corps gauche de k, qui est une sous-extension de k/Z. On peut donc écrire $|k_x| = q^{d_x}$ pour un certain $d_x \in \{1, \dots, n\}$. De plus, l'inclusion $k_x^* \subset k^*$ implique $q^d - 1 \mid q^n - 1$, ce qui n'arrive que[35] quand $d \mid n$. On dénombre les orbites $\omega(x)$ de la manière suivante :

$$|\omega(x)| = \frac{|k^*|}{|k_x^*|} = \frac{q^n - 1}{q^{d_x} - 1}$$

L'équation aux classes s'écrit, avec (x_i) un système représentatif des orbites non singletonnes et $d_i = d_{x_i}$:

$$q^n - 1 = |k^*| = |Z^*| + \sum_{i=1}^{k} |\omega(x_i)| = q - 1 + \sum_{i=1}^{k} \frac{q^n - 1}{q^{d_i} - 1} \tag{46}$$

Avec les d_i diviseurs stricts de n pour tout i.

---

32. On prendra ainsi garde au fait que le sous-groupe $H = \{1, i, j, k\}$ de $\mathbb{H}^*$ n'est pas cyclique, contrairement à tout sous-groupe fini d'un corps (commutatif), comme par exemple $\{1, i\}$ dans le groupe $\mathbb{C}^*$, cf critère de cyclicité.

33. On peut se passer de cette hypothèse, toutefois nous préférons garder nos espaces vectoriels sur des corps commutatifs

34. Les dimensions (au sens large) sont les mêmes

35. Traduisons dans $Z = q^d - 1 \mid Z : q^n - 1$, soit en effectuant la divsion euclidienne de n par d, $q^r - 1$ avec le reste r tel que $0 \leq r < d$; mais l'ordre de q est d, donc $r = 0$ et $d \mid n$.

(c) $\Phi_n(q)$ divise $q^n - 1$; n de la preuve. Par définition des polynômes cyclotomiques sur $\mathbb{Z}$,

$$X^n - 1 = \prod_{m \mid n} \Phi_m(X)$$

En particulier, pour tout d diviseur de n,

$$\prod_{m \mid n,\ m \nmid d} \Phi_m(X) = \frac{X^n - 1}{X^d - 1}$$

Si d est un diviseur strict, cette identité donne que $\Phi_n(q)$ divise $\frac{q^n - 1}{q^d - 1}$ dans $\mathbb{Z}$.

Reprenons l'équation aux classes : $\Phi_n(q)$ divise $\frac{q^n - 1}{q^{d_i} - 1}$ pour tout i, donc $\Phi_n(q) \mid q - 1$. En particulier, nous avons

$$|\Phi_n(q)| \leq q - 1 \tag{47}$$

Cette inégalité est absurde si $n > 2$, puisque par définition $\Phi_n(q)$ est le produit des $q - \zeta_l$, où $\zeta_1, \ldots, \zeta_{\varphi(n)}$ sont les racines primitives n-ièmes de l'unité dans $\mathbb{C}$. Or on a alors que pour tout l, $|q - \zeta_l| > |q - 1| = q - 1$, donc $|\Phi_n(q)| > (q-1)^{\varphi(n)} \geq q - 1$.

Corollaire 31.3. Soit A un anneau intègre fini (pas nécessairement commutatif) de caractéristique p. Alors A est un corps ; plus précisément A est isomorphe au corps de décomposition de $X^{|A|} - X$ sur $\mathbb{F}_p$.

Lemme 31.4. Soit A un anneau intègre fini. Alors, A est un corps.

Démonstration. Soit $a \in A$ non nul et considérons l'application de multiplication

$$\begin{aligned} \varphi_a : A &\to A \\ x &\mapsto ax \end{aligned}$$

φ_a est un homomorphisme du groupe additif sous-jacent de a, et $\ker \varphi_a = \{x \in a \mid ax = 0\}$. Par intégrité de A, $\ker \varphi_a$ est réduit à $\{0\}$ et φ_a est injectif (donc surjectif, car A est fini). Il s'ensuit qu'il existe $b \in A$ tel que $\varphi_a(b) = 1_A$, c'est-à-dire que b est un inverse de A.

Nous savons maintenant que tout anneau intègre fini est un corps ; en particulier, c'est un espace-vectoriel sur son sous-corps premier $\mathbb{F}_p$ (où p est la caractéristique de A) et il est de cardinal $q = p^n$. On invoque alors le théorème de structure des corps finis :

Théorème 31.5. Soit k un corps de caractéristique p et de cardinal $q = p^n$. Alors k est isomorphe au corps de décomposition $D_{\mathbb{F}_p}(X^q - X)$, qui est par définition formé par l'ensemble des racines de $\mathbb{F}_p$ dans la clôture algébrique $\overline{\mathbb{F}_p}$.

32. A_5 est l'unique groupe simple d'ordre 60

Leçons.

101: (1) Groupe opérant sur un ensemble

104: (2) Groupes finis

106: (2) Groupe symétrique

Références. Perrin exercice F.6 p. 40

Difficulté *. Attention, on est tenté à un moment d'utiliser la simplicité de A_6 mais ce n'est pas nécessaire (et c'est même assez inélégant puisqu'on montre par la suite celle de A_5).

Théorème 32.1 Il existe un unique groupe simple d'ordre 60 à isomorphisme près, c'est le groupe A_5.

(a) Si G est un groupe simple d'ordre 60, alors $G \simeq A_5$. G est d'ordre $60 = 2^2 \cdot 3 \cdot 5$ donc ses 5-Sylow sont d'ordre 5. D'après les théorèmes de Sylow, le nombre n_5 de 5-Sylow divise 12 et est congru à 1 modulo 5 ; de plus les 5-Sylow sont tous conjugués donc $n_5 \neq 1$ (sinon le 5-Sylow serait unique et distingué).

Finalement, $n_5 = 6$ et on a une action de G sur l'ensemble S de ses 5-Sylow. Puisque G est simple, cette action est triviale ou fidèle ; puisqu'elle est transitive, elle n'est pas triviale, donc on a un plongement de G dans S_6. Dans la suite on identifiera G à son image par le plongement.

G est simple et d'ordre non premier, donc il n'est pas abélien. Ceci implique $[G, G] = G$, donc $G \subset A_6$, qui est d'ordre

$$360 = 2^3 \cdot 3^2 \cdot 5$$

G n'est pas distingué dans A_6 : vu qu'il possède un élément d'ordre 5, si c'était le cas il contiendrait tous les 5-Sylow de A_6 qui sont au nombre de 24 et s'intersectent mutuellement, ce qui donne 72 éléments et constitue une absurdité notable[36].

Par conséquent, l'action par translation à gauche de G sur A_6/G est non triviale. Puisque G est d'indice 6 et comme la classe à gauche G est fixe pour cette action, G agit non trivialement sur $(A_6/G) \setminus G$ qui est de cardinal 5. Cette action est fidèle et $G \simeq A_5$.

(b) Le groupe A_5 est simple. Soit H un sous-groupe distingué non trivial de A_5.

Si H contient un élément d'ordre 2, il les contient tous, car les doubles transpositions sont conjuguées dans A_5. En effet, deux doubles transpositions σ et σ' ayant même structure de cycle, elles sont conjuguées dans S_5 ; on peut donc écrire $\sigma = \tau \sigma' \tau^{-1}$. Si $\tau \in A_5$, c'est bon, sinon on écrit $\tau = \tau_1 \tau_2$ où τ_1 et τ_2 sont des transposition à support disjoints, et on remplace τ par τ_1. Or, il existe 20 éléments d'ordre 2 dans A_5, donc $|H| > 21$, mais comme par ailleurs $|H|$ divise 60, on doit avoir $|H| = 30$ ou 60. En particulier, d'après le lemme de Cauchy, H contient un élément d'ordre 3, et donc A_5

Maintenant, si H possède un élément d'ordre 5, H contient un 5-Sylow de A_5. Mais, comme 5-Sylow de A_5 sont conjugués, H contient tous[37] les éléments d'ordre 5. Il y en a 24, donc par le même argument que précédemment, $H = A_5$.

Remarque 32.2 En fait il n'existe pas de groupe simple non banal (i.e., pas cyclique d'ordre premier) d'ordre < 60. Après 60, le plus petit groupe simple est d'ordre 168 ; il s'agit (au choix) de $GL_3(F_2) \simeq PSL_2(F_7)$ (groupe des isomorphismes du plan de Fano, ou de la droite projective sur F_7). On trouvera de jolies démonstrations (malheureusement toutes les deux un peu trop longues pour un développement) dans [Per96] et surtout dans [Mer06]).

36. Argument à retenir (sinon au pire on dit que A_6 est simple)

37. Attention, cela ne veut pas dire que tous les éléments d'ordre 5 sont conjugués (contrairement au cas des éléments d'ordre 2) !

Remarque 32.3. On peut vérifier que si G est un groupe simple d'ordre < 100 alors G est d'ordre 60 (voir pour cela [FG94] par exemple) : on exclut d'abord les p-groupes, les groupes d'ordre p^2q, pq ou congru à 2 modulo 4 (dans ce dernier cas les 2-Sylow sont cycliques, ce qui entraîne l'existence d'un morphisme non trivial vers $\{\pm 1\}$). Les autres se traitent à la main en regardant l'action (triviale ou transitive) sur les p-Sylow pour p bien choisi. Le fait que le plus petit groupe simple est d'ordre 60 figure (sans preuve) dans la lettre d'Evariste Galois à Auguste Chevalier la veille de son duel.

33. Les sous-groupes finis de $SO(3)$

Leçons.

101 Actions de groupes

104 Groupes finis. Exemples et applications.

Référence. [Aud12], c'est aussi fait dans [FGN14, Algèbre 1].

Difficulté ***. Ce développement est trop long pour être fait en entier, il faut choisir d'admettre des morceaux. L'obtention de (48) paraît dans tous les cas difficilement contournable.

Théorème 33.1. Les sous-groupes finis de $SO(3)$ qui ne laissent aucune droite stable se répartissent en 3 classes de conjuguaison (qui sont aussi classes d'isomorphisme).

- Les groupes tétraédriques, isomorphes à A_4
- Les groupes octaédriques, isomorphes à S_4
- Les groupes dodécaédriques, isomorphes à A_5.

Soit G un sous-groupe fini d'ordre n de $SO_3(\mathbb{R})$. On suppose $n > 1$. Soit S la sphère unité de $\mathbb{R}^3$ euclidien. On pose

$$= \{(g,x) \in (G \setminus \{id\}) \times S \mid g.x = x\}$$

et X son image par la projection sur S.

(a) Une conséquence de la formule des classes. Les éléments de X sont les points de S fixés par un élément non trivial de G ; soit encore, les intersections de S avec les axes de rotation des éléments de G différents de l'identité. En particulier, G stabilise X : si $g.x = x$ alors pour tout $h \in G$,

$$hgh^{-1}.(h.x) = h.(g.x) = h.x$$

Soient $P_1, \dots, P_k$ les orbites pour cette action $G \curvearrowright X$ et e_i l'ordre du stabilisateur d'un représentant de P_i (dans une même orbite, les stabilisateurs sont conjugués).

Proposition 33.2. Avec les notations ci-dessus, nous avons

$$k - 2 + \frac{2}{n} = \sum_{i=1}^{k} \frac{1}{e_i} \tag{48}$$

Démonstration. On va compter de deux manières, l'une depuis G, l'autre depuis X :

D'une part, puisque chaque $g \in G \setminus \{id\}$ a exactement deux points fixes dans S, $|| = 2(n-1)$. D'autre part, on a

$$|| = \sum_{x \in X} (|\mathrm{Stab}_G(x)| - 1)$$

(vu qu'on enlève l'identité). En regroupant selon les orbites, et en utilisant la formule des classes $|P_i| = \frac{|G|}{e_i}$, nous avons :

$$|| = \sum_{i=1}^{k} |P_i|(e_i - 1) = \sum_{i=1}^{k} \frac{n}{e_i}(e_i - 1) = n \sum_{i=1}^{k} 1 - \frac{1}{e_i}$$

Finalement, de

$$|| = 2(n-1) = n \sum_{i=1}^{k} 1 - \frac{1}{e_i}$$

en divisant par n des deux côtés on tire la formule voulue.

Corollaire 33.3. Avec les notations ci-dessus, $2 \leq k \leq 3$

Démonstration. L'équation maîtresse (48) est absurde si $k = 1$ puisqu'alors $k - 2 + \frac{2}{n} < 0$. Tandis que si $k > 4$ alors

$$k - 2 + \frac{2}{n} > k - 2 > k/2 > \sum_{i=1}^{k} \frac{1}{e_i}$$

puisque les e_i sont > 2.

(b) Restrictions données par l'équation (48) : Groupe réductibles. Si $k = 2$ alors l'équation maîtresse donne $e_1 = e_2 = n$ (observer qu'on est dans le cas d'égalité de $\frac{2}{n} \leq \frac{1}{e_1} + \frac{1}{e_2}$). G opère trivialement sur X, qui possède deux éléments. La droite qui passe par ces deux pôles est stable, G n'est pas irréductible. On supposera donc $k > 3$ dans la suite, ce qui donne

$$1 + \frac{2}{n} = \frac{1}{e_1} + \frac{1}{e_2} + \frac{1}{e_3} \tag{49}$$

Quitte à réordonner, on suppose $e_1 \leq e_2 \leq e_3$. On voit que nécessairement $e_1 = 2$ et $e_2 \leq 3$. Par ailleurs, si $e_1 = e_2 = 2$, $e_3 = n/2$. On peut écrire $P_3 = \{x, x'\}$; les éléments envoyant x sur x' sont d'ordre 2, ce sont des renversements et il y en a $n > 2$. Quitte à supposer $n > 3$ (sinon G n'est pas irréductible), il y en a plusieurs et $x' = -x$; donc Rx est G-stable et G n'est pas irréductible.

En poursuivant l'analyse, on obtient que les seuls triplets possibles pour (e_1, e_2, e_3) sont

$$(2, 3, 3) \tag{50}$$

$$(2, 3, 4) \tag{51}$$

$$(2, 3, 5) \tag{52}$$

(c) Sous groupes finis irréductibles de $SO(3)$.

Lemme 33.4. (Lemme des stabilisateurs) Soit $x \in P_i$. Le groupe $H = \mathrm{Stab}_G\{x\}$ est cyclique d'ordre e_i.

Démonstration. H est un sous-groupe de $SO(3)$ laissant Rx stable, donc $(Rx)^\perp$ aussi. On conclut d'après le théorème de structure des sous-groupes finis de $SO(2)$ (cycliques !)

Définition 33.5. Soient p et q deux entiers naturels non nuls. A similitude près il existe au plus un polyèdre régulier convexe dont les faces sont des p-gones et qui se rencontrent au nombre de q en chaque sommets. On le désigne par $\{p, q\}$.

(1) $e_1 = 2$, $e_2 = 3$, $e_3 = 3$, $n = 12$. L'orbite P_2 possède $12/3 = 4$ éléments $x_1, \ldots, x_4$. Soit σ non neutre dans le stabilisateur de x_1 : il est d'ordre 3 et induit une permutation non triviale, donc un 3-cycle, sur x_2, x_3, x_4. On en déduit que x_3 et x_4 sont situés sur des grands cercles C_3 et C_4 intersectant (x_1x_2) en x_1 avec un angle $\frac{2}{3}$. Ceci impose que les x_i forment un tétraèdre régulier. Réciproquement on vérifie que le groupe des isométries positives d'un tétraèdre régulier est isomorphe à A_4.

(2) $e_1 = 2$, $e_2 = 3$, $e_3 = 4$, $n = 24$. L'orbite P_3 possède $24/4 = 6$ éléments $x_1, \ldots, x_6$ dont les stabilisateurs sont d'ordre 4, cycliques d'après le lemme des stabilisateurs. De plus, un élément d'ordre 3 de G induit une permutation des x_i formée de deux 3-cycles. G est le groupe des isométries d'un octaèdre régulier (dont les sommets forment P_3), ou encore d'un cube dont les sommets forment P_2.

(3) $e_1 = 2$, $e_2 = 3$, $e_3 = 5$, $n = 60$. D'après ce qui précède, il s'agit d'assurer l'existence d'un polyèdre régulier à 12 faces pentagonales. On considère l'enveloppe convexe des 20 points de la forme

$$\begin{matrix} 1 & 1 & 1 \\ \leftarrow & ' & 0 \\ 0 & \leftarrow & ' \\ ' & 0 & \leftarrow \end{matrix}$$

Dont on peut véri er qu'ils forment bien un polyèdre appelé dodécaèdre régulier. Les centres des faces forment un icodaèdre régulier.

---

34. Théorème de Chevalley-Warning

Leçons :

123: Corps nis.

142: Algèbre des polynômes à plusieurs indéterminées

Référence : Serre, Cours d'arithmétique chap. 1 (attention, le style est très concis)

Pré-requis : Le groupe F_q est cyclique

Théorème 34.1. K est un corps ni de cardinal q et de caractéristique p. Soient

$$f \in K[X_1;:::X_n]$$

une famille nie de polynômes dont la somme des degrés totaux est $< n$, et soit V l'ensemble de leurs zéros communs dans K^n. On a alors

(53) $$jVj \equiv 0 (p)$$

Notation : Pour tout $F \in K[X_1;:::X_r]$ on écrira

$$S(F) = \sum_{(x_1;:::;x_r)\in K^r} F(x_1;:::x_r)$$

Il s'agit a priori d'un élément de K. On identi era le sous-corps premier de K à $Z=pZ$.

(a) Un lemme sur les sommes de puissances.

Lemme 34.2. Soit u un entier naturel. La somme

$$S(X^u) = \sum_{x\in K} x^u$$

est égale à 1 si $q-1 \mid u$ et $u > 1$, elle est égale à 0 sinon

Remarque 34.3. Attention : on prend comme convention $0^0 = 1$ même s'il pourrait être tentant de le prendre égal à 0 pour un énoncé momentanément plus simple.

Démonstration. Soit $u > 1$ divisible par $q-1$; on a $0^u = 0$ et $x^u = 1$ si $x \neq 0$ (puisque l'ordre multiplicatif de x divise $jK^j = q-1$); donc $S(X^u) = (q-1)\cdot 1 = -1$. Réciproquement, si u n'est pas divisible par $q-1$, soit $y \in K^*$ un générateur (qui existe car K^* est cyclique). y est alors tel que $y^u \neq 1$. Mais alors

$$\sum_{x\in K} x^u = \sum_{x\in K} (xy)^u = y^u \sum_{x\in K} x^u$$

D'où $S(X^u) = 0$.

(b) Théorème de Chevalley-Warning. Posons

$$P = \prod_{} 1 - f^{q-1} \in K[X_1;:::X_n]$$

et soit $x \in K^n$. Si $x \in V$, tous les $f(x)$ sont nuls et $P(x) = 1$; si $x \notin V$, il existe tel que $f(x) \neq 0$, et alors $f(x)^{q-1} = 1$ de sorte que $P(x) = 0$: P est la fonction indicatrice de V. On a donc $S(P) \in Z=pZ$, et

$$jVj \equiv S(P) (\mathrm{mod}\ p)$$

On est donc ramené à montrer que $S(P) = 0$. Puisque la somme des degrés de $f$es est $< n$, nous avons :

$$\deg P < n(q-1)$$

Donc P est somme de monômes $aX^u = aX_1^{u_1} \cdots X_n^{u_n}$ avec $0 \neq a \in K$ et $\sum u_i < n(q-1)$. Pour un tel monôme

$$S(X^u) = \sum_{x_1\in K} \cdots \sum_{x_n\in K} x_1^{u_1} \cdots x_n^{u_n} = \prod_i S(X^{u_i})$$

L'un des u_i est nécessairement $< q-1$; d'après le lemme $S(X^{u_i})$, puis $S(X^u)$, puis $S(P)$ est nul.

Corollaire 34.4. Sous les mêmes hypothèses, et si les f sont sans termes constant (en particulier, s'ils sont homogènes de degré $d > 1$), alors les f ont un zéro en commun non trivial.

En effet, $|V|$ est divisible par p et non nul puisque $0 \in V$.

Remarque 34.5. On retrouve ainsi que toute forme quadratique q en $n > 3$ variables a un zéro non trivial. En termes géométriques : toute conique sur un corps $\mathbb{K}$ ni admet un point rationnel.

Donnons une autre application, qui est un cas particulier d'un théorème d'Erdös-Ginzburg-Ziv :

Proposition 34.6. Soit p un nombre premier et $a_1, \dots, a_{2p-1}$ des éléments de $\mathbb{Z}/p\mathbb{Z}$. Parmi les a_i, il en existe p dont la somme est nulle.

Démonstration. Posons

$$f_1 = \sum_{i=1}^{2p-1} a_i X_i^{p-1}$$

$$f_2 = \sum_{i=1}^{2p-1} X_i^{p-1}$$

Le point 0 de $\mathbb{F}_p^{2p-1}$ est racine commune de f_1 et f_2 et $\deg f_1 + \deg f_2 = 2p-2 < 2p-1$; d'après le théorème de Chevalley-Warning $V(f_1, f_2)$ est de cardinal au moins p, en particulier elle contient $x = (x_1, \dots, x_{2p-1})$ non nul. L'équation $f_2(x) = 0$ indique qu'exactement p des x_i sont non nuls ; mais alors si on note ceux-là $x_{i_1}, \dots, x_{i_p}$ nous avons

$$a_{i_1} + \cdots + a_{i_p} = a_{i_1} x_{i_1}^{p-1} + \cdots + a_{i_p} x_{i_p}^{p-1} = f_1(x) = 0$$

Le cas général s'en déduit par récurrence

Proposition 34.7. On peut remplacer p par $n > 1$ quelconque dans la proposition précédente

Démonstration. On procède par récurrence forte. Supposons la propriété montrée pour $2, \dots, n-1$. Si n est premier il n'y a rien à montrer, sinon $n = pn'$ avec p premier et $n' < n$. On écrit alors

$$2n-1 = p(2n'-1) + p - 1$$

Soient $a_1, \dots, a_{2n-1}$ dans $\mathbb{Z}/n\mathbb{Z}$. Par application répétée de la proposition pour p, il existe $E_1, \dots, E_{2n'-1}$ dans $\{1, \dots, 2n-1\}$ disjoints et de cardinaux p tels que pour tout i,

$$\sum_{x \in E_i} x \in p\mathbb{Z}/n\mathbb{Z}$$

D'après l'hypthèse de récurrence sur n', il existe $E_{i_1}, \dots, E_{i_{n'}}$ tels que la somme des éléments dans les E_{i_k} est 0. On a ainsi $pn' = n$ éléments de somme nulle parmi les a_i.

Remarque 34.8. On peut vérifier que $2n-1$ est optimal dans la proposition précédente. En effet soient a_i les $2n-2$ éléments définis par $a_i = 0$ pour $1 \leq i < n$ et $a_i = 1$ pour $n \leq i \leq 2n-2$; alors on vérifie que l'on ne peut pas extraire de somme nulle de n éléments. Il est également possible d'évaluer le nombre de sous-ensembles de $\{1, \dots, 2n\}$ dont la somme est divisible par n [ZR13].

35. Algorithme de Berlekamp

Leçons.

122: Anneau principaux

151: Dimension d'un espace vectoriel

123: Corps nis

155: Polynômes d'endomorphisme

Référence. [HL12] Attention coquille au début de la deuxième partie de l'algorithme : il faut lire $a \in A^F$ et non pas $a \in A$.

Soit p un nombre premier. L'algorithme de Berlekamp répond au

Problème 35.1. Factoriser $P \in \mathbb{F}_p[X]$ unitaire en produit d'irréductibles unitaires de $\mathbb{F}_p[X]$.

L'algorithme de Berlekamp proprement dit ne s'appliquant que sur les polynômes sans facteurs carrés, on cherche tout dabord ici à obtenir une décomposition du type

$$P = Q_1 \cdots Q_r$$

où Q_1 est la partie sans facteur carrée de P (i.e. le produit des irréductibles divisant P), Q_2 celle de P/Q_1, etc. puis à appliquer l'algorithme de Berlekamp sur les Q_i.

(a) Où l'on se ramène à P sans facteur carré. Observons que si $Q^2 \mid P$ alors $Q \mid \operatorname{pgcd}(P, P')$; la première étape est donc de calculer $S = \operatorname{pgcd}(P, P')$ à l'aide de l'algorithme d'Euclide.

(1) $S = P$; puisque $\deg P' = \deg P - 1$ ceci signifie que $P' = 0$, autrement dit $P \in \ker D = k[X^p]$ (où D est l'endomorphisme de dérivation). On peut alors écrire

$$P = \sum_{k=0}^{n} a_k X^{pk} = \left(\sum_{k=0}^{n} a_k X^k \right)^p = R^p$$

et on reprend avec R ; nous avons bien $\deg R = (\deg P)/p < \deg P$.

(2) $S \neq P$; alors $\deg S < \deg P$ et on recommence avec S et P/S

(b) Où l'on obtient le nombre d'irréductibles divisant P. On suppose dorénavant P sans facteur carrés et on écrit

$$P = P_1 \cdots P_s$$

sa décomposition en produit d'irréductible (inconnus à ce stade). D'après le lemme chinois des restes, il existe un isomorphisme

$$\begin{aligned} \varphi : A = \mathbb{F}_p[X]/(P) &\to \prod_{i=1}^{s} \mathbb{F}_p[X]/(P_i) \simeq \prod_i \mathbb{F}_{p^{\deg P_i}} \\ \overline{Q} &\mapsto (Q \bmod P_i) \end{aligned}$$

Si l'on dénote par F le morphisme de Frobenius $a \mapsto a^p$ de A (et pareil celui de $\prod_i \mathbb{F}_p[X]/(P_i)$) alors à droite $(A)^F = \prod_{i=1}^{s} \mathbb{F}_p \simeq \mathbb{F}_p^s$ de sorte que

$$s = \dim \ker(F - I_A) = \deg P - \operatorname{rg}(F - I_A)$$

L'entier s se calcule à l'aide de l'algorithme du pivot (complexité cubique). En particulier, on sait décider algorithmiquement (et assez rapidement) que P est irréductible : ce n'est pas le cas dès que l'on trouve deux vecteurs linéairement indépendants dans A^F. Rappelons que ceci donne un critère assez pratique d'irréductibilité pour les polynômes à valeurs dans $\mathbb{Z}$ (on choisit p qui ne divise pas le coefficient dominant, on réduit modulo p...)

(c) Décomposition de P en produit d'irréductible. Supposons que P n'est pas irréductible ; alors il existe $Q \in \mathbb{F}_p[X]$ de degré $< \deg P$ tel que $\overline{Q} \in A^F$, autrement dit $P \mid Q^p - Q$. De l'identité

$$X^p - X = \prod_{x \in \mathbb{F}_p} (X - x)$$

on tire, en spécialisant dans $\mathbb{F}_p[Q]$,

$$P \mid \prod_{x \in \mathbb{F}_p} (Q - x)$$

Puisque les $Q - x$ sont premiers entre eux deux à deux (leurs différences sont des polynômes constants) chaque P_i divise un et un seul des $Q - x$. Ainsi,

$$P = \prod_{x \in \mathbb{F}_p} \operatorname{pgcd}(P, Q - x)$$

Puisque $\deg Q - x \leq \deg Q < \deg P$, on a bien décomposé P en un produit de polynômes de degrés strictement plus petits ; de sorte que l'algorithme termine.

---

36. Caractères et groupes abéliens nis

Leçon.

102: Nombres complexes de module 1, sous-groupe des racines de l'unité

Références. [Ser70] ou [Col11].

Di culté **. La principale di culté est de faire les choses dans un ordre cohérent (qui varie beaucoup selon les références). Il n'est pas entièrement satisfaisant d'obtenir l'isomorphisme de G avec son bidual en utilisant le théorème de structure.

Pré-requis : Caractères des groupes cycliques G ' Ĝ quand G est cyclique

Théorème 36.1. Soit G un groupe abélien ni. G est isomorphe à un produit direct de groupes cycliques.

Le théorème précédent appelle un énoncé d'unicité. Il existe pour les produits de groupes cycliques, deux formes normales :

(1) La forme G ' Z=a$_1$Z Z=a$_r$Z où les a$_i$ sont soumis à a$_1$ j j a$_r$ (appelés facteurs invariants du groupe G)

(2) La forme G ' Z=p$_1^{1}$Z Z=p$_s^{s}$: produit de p-groupes (les p$_i$ ne sont pas forcément distincts).

Les deux formes s'obtiennent l'une l'autre par application du lemme chinois. Elles sont analogues respectivement à la réduite de Frobenius et la réduite de Jordan pour les endomorphismes (i.e. les k[X]-modules t.f. de torsion, tandis que les groupes abéliens nis sont les Z-modules t.f. de torsion).

On se propose de démontrer ce théorème via la théorie des caractères

(a) Lemme de prolongement des caractères.

Lemme 36.2. Soit G un groupe abélien ni, H un sous-groupe. Alors on a une suite exacte[38]

$$f1g ! \hat{G}=H ! \hat{G} ! \hat{H} ! f1g$$

où est la restriction.

Démonstration. Il est équivalent de montrer que tout 2 Ĥ se prolonge en 2 Ĝ. On procède par récurrence sur l'indice n de H dans G.

- Si G = H il n'y a rien à prouver
- Sinon, soit x 2 G H ; x^n est dans H. Soit ! 2 C tel que ! ^{n} = (x^n) ; ! existe puisque C est un groupe divisible[39]. Posons H^0 le sous-groupe engendré par H et x ; tout élément de H^0 s'écrit sous la forme xh^t avec t 2 Z et on pose

$$^0(h^0) = (h) ! ^t$$

On véri e que cela ne dépend pas de h choisi. L'indice de H^0 dans G étant strictement plus petit que celui de H, on conclut par récurrence.

38. On dit que est un foncteur exact de G.

39. C'est vraiment le point crucial en fait ; ce n'est pas si évident quand on y ré echit. Il faut par exemple le théorème fondamental de l'algèbre, ou bien la surjectivité de l'exponentielle complexe.

(b) L'isomorphisme $G \simeq \widehat{\widehat{G}}$. D'après le lemme de prolongement des morphismes nous avons

$$\widehat{G} = \widehat{G/H} \quad H^\perp$$

Pour tout H sous-groupe cyclique ; en outre $H^\perp = |H|$. On en déduit par une récurrence immédiate que $\widehat{\widehat{G}} = |G|$ pour tout groupe abélien.

Introduisons l'application

$$\begin{aligned} : G &\to \widehat{\widehat{G}} \\ x &\mapsto (\chi \mapsto \chi(x)) \end{aligned}$$

Proposition 36.3. est un isomorphisme de groupes.

Démonstration. On vérifie sans problème que est un homomorphisme. D'après ce qui précède, G et son bidual ont même ordre, donc il suffit de s'assurer de l'injectivité de . Soit $x \neq 1$ dans G, il s'agit de montrer qu'il existe $\chi \in \widehat{G}$ tel que $\chi(x) \neq 1$. On prend un caractère non trivial de $H = \langle x \rangle$ et on le prolonge à G d'après le lemme de prolongement des caractères.

(c) Le théorème de structure : existence.

Lemme 36.4. G et $\widehat{G}$ ont même exposant.

Démonstration. Vu l'isomorphisme $G \simeq \widehat{\widehat{G}}$ il suffit de démontrer que l'exposant N' de $\widehat{G}$ divise l'exposant N de G. Pour tout $\chi \in \widehat{G}$, et $x \in G$ nous avons $\chi^N(x) = x^N = \chi(1) = 1$ ce qui donne ce qu'on voulait[40]

Démontrons à présent le théorème par récurrence sur l'ordre de G.

Le résultat est acquis si G est trivial.

Supposons G non trivial et soit N son exposant. D'après le lemme qui précède il existe χ_1 d'ordre N et $\chi_1(G) = \mu_N$. Soit donc $x_1 \in G$ tel que $\chi_1(x_1) = e^{2i/N}$ (ou tout autre générateur de μ_N) ; x_1 est d'ordre N. On va montrer que G est produit direct de $H = \langle x_1 \rangle$ et de $\ker \chi_1$, ce qui permettra de conclure.

χ_1 induit un isomorphisme de H_1 sur μ_N ; soit son inverse. Si $x \in G$ alors $a = (\chi_1(x))$ est dans H_1 et $b = a^{-1}x$ est dans $\ker \chi_1$ ce qui montre que $G = H_1 G_1$. Par ailleurs, $H_1 \cap G_1$ est réduit à $\{1\}$ puisque χ_1 restreint à H_1 est injectif. Ceci conclut.

(d) Le théorème de structure : unicité. Supposons que

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \quad \mathbb{Z}/n_r\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \quad \mathbb{Z}/m_s\mathbb{Z}$$

où les entiers m_i et n_j sont soumis aux conditions $n_1 | \quad | n_r$ et $m_1 | \quad | m_s$.

Lemme 36.5. Soient $n, d > 1$. Alors

$$d(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/\frac{n}{n \wedge d}\mathbb{Z}$$

Démonstration. $d(\mathbb{Z}/n\mathbb{Z})$ est l'image de $\mathbb{Z}/n\mathbb{Z}$ par le morphisme de groupes $_d : x \mapsto d.x$. Donc, c'est un groupe cyclique (en tant que quotient de cyclique) ; il s'agit de calculer le cardinal de $\ker _d$. Par définition, c'est l'ensemble des éléments tels que $d.x = 0$ dans $\mathbb{Z}/n\mathbb{Z}$; donc le groupe des éléments dont l'ordre divise n et d. On a donc,

$$\ker _d \simeq \mathbb{Z}/(n \wedge d)\mathbb{Z}$$

d'où l'isomorphisme recherché.

40. On peut aussi voir G comme un $\mathbb{Z}/N\mathbb{Z}$-module, et identifier $\widehat{G}$ à G^-.

Appliquons le lemme pour dénombrer d_G à l'aide des deux décompositions, on trouve

$$\prod_{i=1}^{r} \mathrm{pgcd}(d; n_i) = \prod_{j=1}^{s} \mathrm{pgcd}(d; m_j)$$

Ce sont deux écritures de $|G| = |d_G|$. En particulier, pour $d = m_s n_r$, cela donne

$$\prod_{i=1}^{r} n_i = \prod_{j=1}^{s} m_j$$

tandis que pour $d = m_s$, on obtient

$$\prod_{i=1}^{r} \mathrm{pgcd}(n_i ; m_s) = \prod_{j=1}^{s} m_j$$

Ceci implique que, pour tout i, $\mathrm{pgcd}(n_i ; m_s) = n_i$, autrement dit $n_i \mid m_s$. En particulier,

$$n_r \mid m_s$$

Par symétrie, $n_r = m_s$. On conclut par récurrence.

Remarque 36.6. Le théorème de structure conjugué au lemme de prolongement des caractères donne en retour l'isomorphisme $G \simeq \hat{G}$. Celui-ci n'est pas canonique.

Remarque 36.7. On déduit facilement du théorème $G \simeq \hat{G}$ et des relations

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} |G| & \text{si } x = 1 \\ 0 & \text{si } x \neq 1 \end{cases} \tag{54}$$

les relations d'orthogonalité des caractères (cas particulier des relations de Schur Frobenius)

$$\sum_{x \in G} \chi(x) = \begin{cases} |G| & \text{si } \chi = 1 \\ 0 & \text{si } \chi \neq 1 : \end{cases} \tag{55}$$

En particulier, on retrouve le lemme d'indépendance de Dedekind : $\chi_1, \ldots, \chi_n$ sont distincts ssi linéairement indépendants sur $\mathbb{C}$ (ce qui s'obtient élémentairement [FGN14]). (55) peut aussi se voir comme procédant des relations plus générales d'orthogonalité des caractères de représentations irréductibles : si χ et χ' sont deux représentations de caractères χ et χ' alors

$$\frac{1}{|G|} \sum_{x \in G} \chi(x) \overline{\chi'(x)} = \dim_{\mathbb{C}} [V_\chi^{V_{\chi'}}]^G$$

(Identifier la somme de gauche au rang d'un projecteur sur l'espace des G-morphisme, invariant de la représentation χ'. D'après le lemme de Schur quand χ et χ' ceci est 1 si $\chi \simeq \chi'$ et 0 sinon .

37. Théorème de Kakutani commutatif

Leçons: : 206 Théorèmes de point xe ; exemples et applications. 202 (parties denses), utiliisation de la notion de compacité

Références: : Gonnord Tosel

Théorème 37.1. Soit E un espace a ne normé et K un compact convexe non vide de E. Soit $(T_i)_i$ une famille d'applications a nes continues de E dans E laissant K stable. Alors, les T_i admettent un point xe commun.

37.1. (a) T a ne continue stabilisant K, a un point xe. Soit $x \in K$ quelconque et posons x_n l'équibarycentre des $T^k x$ pour $k \in \{0; \dots; n-1\}$. Alors

$$x_n - Tx_n = \frac{1}{n}(x - T^n x) \tag{56}$$

Donc $\|Tx_n - x_n\| \leq D/n$, où D est le diamètre de K (ni, puisque K est compact). De plus, comme K est un métrique compact, il existe une sous-suite $(x_{\varphi(n)})_{n\in\mathbb{N}}$ et $y \in K$ tels que

$$x_{\varphi(n)} \xrightarrow[n\to+\infty]{} y$$

Par continuité de l'application T, nous avons $Ty = y$, et T admet un point xe.

37.2. (b) Cas d'un nombre ni d'applications. Soit $n > 2$ et $(T_i)_{1\leq i\leq n}$ une famille d'applications a nes laissant K stable. On procède par récurrence sur n. Soit donc Y l'ensemble des points xes collectifs de $T_1; \dots; T_{n-1}$

$$Y = \bigcap_{i=1}^{n-1} \{y \in K;\ T_i y = y\}$$

On véri e alors que :

(1) Y est non vide par hypothèse de récurrence

(2) Y est convexe, car les T_i sont a nes

(3) Y est fermé, car les T_i sont continues. Puisque $Y \subset K$, Y est compact.

(4) Y est stable par T_n, qui permute les éléments de Y :

$$\forall y \in Y,\ \forall i \in \{1; \dots; n-1\},\ T_i T_n y = T_n T_i y = T_n y$$

D'après le cas (a), T_n possède un point xe dans Y, ce qu'il fallait montrer.

37.3. (c) Cas général. Notons Y_i l'ensemble des points xés par T_i. Alors, si par l'absurde

$$\bigcap_{i\in I} Y_i = \varnothing$$

D'après la propriété de Borel & Lebesgue on peut extraire de cette intersection vide de fermés une intersection nie toujours vide ; autrement dit une partie nie sans point xe collectif. Ceci contredit (b).

Remarque 37.2. (a) est encore valable sans l'hypothèse T a ne ; c'est le théorème de Schauder.

Remarque 37.3. L'hypothèse de compacité de K est nécessaire : par exemple si $K = E$ on peut considérer une translation.

Remarque 37.4. D'après le théorème de Krein & Milmann, pour véri er qu'une application a ne laisse stable K il su t de véri er qu'elle envoie ses points extrémaux dans K.

38. Processus de Galton-Watson

Leçons :

253: Utilisation de la convexité en analyse

260: Espérance et moments d'une variable aléatoire

264: Variables aléatoires discrètes

Références : Cotrell & al., exercices de probabilité.

Difficulté **. On s'intéresse au nombre de descendants d'un individu après t générations (arbre généalogique descendant) donné par la variable aléatoire Z_k, sachant que chaque individu se reproduit et donne lieu à des descendant en nombre suivant les mêmes lois $Z \quad Z_1$, indépendantes.

Théorème 38.1. Posons $m = \sum kp_k = E[Z] \in \mathbb{R}[\{+1\}$ et supposons $P(Z \neq 1) < 1$. Alors

- Si $m \quad 1$ il y a extinction avec probabilité 1
- Si $m > 1$ il existe $x < 1$ tel que $P(Z_t = 0) \to x$ quand $t \to +1$

Lemme 38.2. Soit (X_n) une suite de variables iid à valeurs dans $\mathbb{N}$ et soit N à valeurs dans $\mathbb{N}$ indépendante des X_n. On pose

$$Z = \sum_{n=1}^{N} X_n$$

(somme aléatoire de variables aléatoires). Alors, en posant G_X (resp. G_N, G_Z) la fonction génératrice de X_n nous avons

$$G_Z = G_N \quad G_X$$

Démonstration. Par définition

$$G_Z(s) = \sum_{k=0}^{+\infty} P(Z = k)\, s^k = \sum_{k=0}^{+\infty} s^k \sum_{n=0}^{+\infty} P(Z = k; N = n) \tag{57}$$

Or $\{Z = k\} \cap \{N = n\} = \{S_n = k\} \cap \{N = n\}$ où $S_n = X_1 + \quad + X_n$ et les variables Z et S_n sont indépendantes. Il s'ensuit que

$$P(Z = k; N = n) = P(S_n = k)\, P(N = n)$$

De plus, par positivité on peut intervertir les sommes dans l'expression de G_Z, cela donne

$$\begin{aligned} G_Z(s) &= \sum_{n=0}^{+\infty} P(N = n) \sum_{k=0}^{+\infty} P(S_n = k)\, s^k \\ &= \sum_{n=0}^{+\infty} P(N = n)\, G_{S_n}(s) \\ &= \sum_{n=0}^{+\infty} P(N = n)\, G_X(s)^n \\ &= G_N \quad G_X(s) \end{aligned}$$

Revenons à la preuve du théorème : nous avons

$$Z_{t+1} \sum_{n=1}^{Z_t} Z_{(n)}$$

où les $Z_{(i)}$ désignent des copies iid de la loi Z. Par conséquent

$$G_{Z_{t+1}} = G_{Z_t} \quad G_Z$$

Puis par une récurrence immédiate $G_{Z_t} = G_Z^{\circ t}$ où l'exposant $\circ t$ signifie qu'on a composé t fois.

Remarque 38.3. A ce stade remarquons que par la formule de dérivée d'une composée, nous avons

$$E[Z_t] = G'_{Z_t}(1) = G'_Z(1)^t = m^t$$

(cette quantité étant éventuellement infinie). En particulier, si $m < 1$ nous avons déjà que $E[Z_t] \to 0$, ce qui implique $P(Z_t = 0) \to 1$.

Plus précisément, $P(Z_t = 0) = G_{Z_t}(0) = G_Z^{\circ t}(0)$. Comme G_Z est continue et $G_Z(0) > 0$, la suite $G_Z^{\circ t}(0)$ est croissante et converge vers la plus petite solution positive x de l'équation $G_Z(s) = s$.

(1) $m > 1$ (au sens large). Dans ce cas $G_Z(s) < s$ pour s au voisinage à gauche de 1, et par conséquent $x < 1$.

(2) $m \leq 1$. Puisque G_Z est une fonction convexe (elle est analytique sur $]0;1[$ à coefficients positifs et non affine), elle est strictement au-dessus de sa tangente en 1, et $x = 1$

Remarque 38.4. En fait, l'équation $G_Z(x) = x$ possède au plus deux solutions. Ceci est lié au

Lemme 38.5. Soit $g : I \to \mathbb{R}$ une fonction convexe. Si g s'annule en trois points distincts de I alors elle est nulle.

Cette observation n'est pas nécessaire pour le théorème, toutefois elle est intéressante en vue d'une généralisation. Si la génération 0 est constitué de p individus distincts, alors la probabilité d'extinction en temps long va quand même converger vers x (ceci même si p et m sont très grands).

39. Intégrale de Dirichlet par une équation di érentielle

Leçons.

221: Equations di érentielles linéaires

235: Problèmes d'interversions de limites et d'intégrales

236: Illustrer par des exemples quelques méthodes de calcul d'intégrale

239: Fonctions dé nies par une intégrale dépendant d'un paramètre

Référence. [FGN14, Analyse 3] Attention, la variation des constantes n'est pas appliquée, l'énoncé demande seulement de véri er la solution qu'il donne

Théorème 39.1. La fonction $t \mapsto \frac{\sin t}{t}$ est d'intégrale semi-convergente sur $\mathbb{R}_+$ et

$$\int_0^{+1} \frac{\sin t}{t} dt = \frac{}{2} \tag{58}$$

(a) Introduction de la fonction $'$; premières propriétés. On dé nit $'$ par

$$\forall x > 0,\ '(x) = \int_0^{+1} \frac{e^{\ tx}}{1+t^2} dt$$

(a.1) $'$ est continue sur $\mathbb{R}_+$. Pour tout $x > 0$, pour tout $t > 0$, nous avons l'inégalité $0 \leq \frac{e^{\ tx}}{1+t^2} \leq \frac{1}{1+t^2}$. Or $t \mapsto \frac{1}{1+t^2}$ est intégrable sur $\mathbb{R}_+$, et $x \mapsto e^{\ tx}$ est continue pour tout $x > 0$. D'après le théorème de continuité sous le signe $\int_{\mathbb{R}}$, $'$ est continue sur $\mathbb{R}_+$.

(a.2) $'$ est C^1 sur $\mathbb{R}_+$. Posons $f(x;t) = \frac{e^{\ tx}}{1+t^2}$. Alors f est in niment dérivable sur $\mathbb{R}_+$ $\mathbb{R}_+$, et $\frac{\partial^n f}{\partial x^n}(x;t) = (\ 1)^n t^n \frac{e^{\ tx}}{1+t^2}$. En particulier, pour tout $x > A > 0$, on a $\frac{\partial^n f}{\partial x^n}(x;t) \leq \frac{t^n}{1+t^2} e^{\ At}$. Cette fonction de la variable t étant clairement intégrable sur $\mathbb{R}_+$, $'$ est C^1 sur $[A; +1[$ et

$$\forall x > 0,\ '^{(n)}(x) = (\ 1)^n \int_0^{+1} \frac{t^n}{1+t^2} e^{\ xt} dt$$

(a.3) Comportement au voisinage de $+1$. Il découle du théorème de convergence dominée que $\lim_{+1} ' = 0$

(b) Une équation di érentielle linéaire ; variation des constantes. D'après l'expression de $'^{00}$ précédemment obtenue, nous avons que

$$\forall x > 0,\ '^{00}(x) + '(x) = \int_0^{+1} e^{\ tx} dt = \left[\frac{e^{\ tx}}{x} \right]_0^{+1} = \frac{1}{x}$$

Nous somes en présence d'une équation di érentielle du second ordre à coe cients constants, que nous traduisons sous la forme vectorielle

$$Y'(x) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} Y(x) + \begin{pmatrix} 0 \\ 1=x \end{pmatrix}$$

Deux solutions particulières de l'équation homogène $y'' + y = 0$ sont bien sûr

$$Y_1(x) = \begin{pmatrix} \cos x \\ \sin x \end{pmatrix}$$

$$Y_2(x) = \begin{pmatrix} \sin x \\ \cos x \end{pmatrix}$$

Appliquons la méthode de la variation des constantes : on cherche sous la forme $(x)\cos x + (x)\sin x$, en imposant le système linéaire $'(x)Y_1(x) + 'Y_2(x) = B(x)$. Sous forme matricielle, cela revient à

$$\begin{pmatrix} \cos x & \sin x \\ \sin x & \cos x \end{pmatrix} \begin{pmatrix} ' \\ ' \end{pmatrix} = B$$

, d'où

$$^0(x) = \frac{\sin x}{x}$$
$$^0(x) = \frac{\cos x}{x}$$

Lemme 39.2 Soit $x > 0$. Les intégrales $\int_x^{+1} \frac{\sin t}{t} dt$ et $\int_x^{+1} \frac{\cos t}{t} dt$ sont semi-convergentes.

Démonstration. Il su t de le montrer pour $\int_x^{+1} \frac{e^{it}}{t} dt$. On intègre par parties :

$$\int_x^X \frac{e^{it}}{t} dt = i\frac{e^{it}}{t}\Big|_x^X + i\int_x^X \frac{e^{it}}{t^2} dt$$

Le premier terme a pour limite $ie^{ix} = x$, et le second terme est une intégrale absolument convergente.

Nous pouvons donc écrire

$$\begin{aligned} 8x > 0;\ '(x) &= \cos x \int_x^{+1} \frac{\sin t}{t} dt \quad \sin x \int_x^{+1} \frac{\cos t}{t} dt \\ &= \int_x^{+1} \frac{\cos x \sin t \quad \sin x \cos t}{t} dt \\ &= \int_x^{+1} \frac{\sin(t \quad x)}{t} dt \end{aligned}$$

(c) Evaluation de ' en 0. Par dé nition de ' nous avons

$$'(0) = \int_0^{+1} \frac{dt}{1+t^2} = [\arctan u]_0^{+1} = \frac{}{2}$$

Et par ailleurs, d'après la continuité de ' en 0 et l'expression obtenue plus haut

$$'(0) = \lim_{x!\ 0} '(x) = \lim_{x!\ 0} \cos x \int_x^{+1} \frac{\sin t}{t} dt \quad \sin x \int_x^{+1} \frac{\cos t}{t} dt$$

D'une part nous avons

$$\lim_{x!\ 0} \cos x \int_x^{+1} \frac{\sin t}{t} dt = \int_0^{+1} \frac{\sin t}{t} dt$$

Il reste donc à montrer que

$$\lim_{x!\ 0} \sin x \int_x^{+1} \frac{\cos t}{t} dt = 0$$

On coupe l'intégrale en deux parties :

$$\begin{aligned} \int_x^{+1} \frac{\cos t}{t} dt \quad 6 & \int_x^1 \frac{\cos t}{t} dt + \int_1^{+1} \frac{\cos t}{t} dt \\ 6 \quad & |\ln x| + \int_1^{+1} \frac{\cos t}{t} dt \end{aligned}$$

De sorte que $\sin x \int_x^{+1} \frac{\cos t}{t} dt = O(x \ln x)$; en particulier on a ce que l'on souhaitait.

40. Expression générale de la résolvante

Leçons.

221: Equations di érentielles linéaires

2??: Interversions de limites et d'intégrales

2..: Suites et séries de fonctions

Références.

Di culté *.

Théorème 40.1. Soit A une sous-algèbre de $\mathcal{M}_p(\mathbb{R})$, $A \in C^0(\mathbb{R}; A)$ et $R(t)$ la résolvante associée au système $X' = AX$ entre 0 et t. Alors

$$R(t) = I_p + \sum_{n=1}^{+\infty} \int_0^t \int_0^{t_1} \cdots \int_0^{t_{n-1}} A(t_n) A(t_{n-1}) \cdots A(t_1)\, dt_1 dt_2 \cdots dt_n \tag{59}$$

En particulier, si A est abélienne[41], alors

$$R(t) = \exp \int_0^t A(s)\, ds \tag{60}$$

Montrons que

$$\tilde{R}(t) = I_p + \sum_{n=1}^{+\infty} \int_0^t \int_0^{t_1} \cdots \int_0^{t_{n-1}} A(t_n) A(t_{n-1}) \cdots A(t_1)\, dt_1 dt_2 \cdots dt_n \tag{61}$$

est bien dé nie : on sait (par réordonnement) que

$$V_n = \mathrm{Vol}\{(t_1, \ldots, t_n) \mid 0 \leq t_1 \leq \cdots \leq t_n \leq t\} = \frac{t^n}{n!}$$

On pose pour tout $n > 1$, $_n$ le terme général de la série de fonctions dé nissant $\tilde{R}$ dans 61, on a d'une part, si $k\,k$ est une norme d'algèbre :

$$\|_n(t)\| \leq \int_{0 \leq t_1 \leq \cdots \leq t_n \leq t} \|A(t_n) A(t_{n-1}) \cdots A(t_1)\|\, dt_1 dt_2 \cdots dt_n \leq \frac{t^n}{n!} \left(\sup_{[0;t]} \|A(t)\|\right)^n$$

Montrons à présent que les $_n$ sont de classe C^1 : il s'agit de dériver

$$\begin{aligned}
{}_n'(t) &= \frac{d}{dt}\left(\int_{0 \leq t_1 \leq \cdots \leq t_n \leq t} A(t_n) A(t_{n-1}) \cdots A(t_1)\, dt_1 dt_2 \cdots dt_n\right) \\
&= \frac{d}{dt}\left(\int_0^t A(t_n) \left(\int_{0 \leq t_1 \leq \cdots \leq t_{n-1} \leq t_n} A(t_{n-1}) \cdots A(t_1)\, dt_1 dt_2 \cdots dt_{n-1}\right) dt_n\right) \\
&= \frac{d}{dt}\int_0^t A(t_n)\, {}_{n-1}(t_n)\, dt_n \\
&= A(t)\, {}_{n-1}(t)
\end{aligned}$$

Cet expression est encore valable si $n = 1$ car on a alors par calcul direct $_1'(t) = A(t) = A(t)\, {}_0(t)$ avec ${}_0 = I_p$. Donc, par convergence normale sur tout $[0; T]$ de la série des $_n$ et de leurs dérivées, on a que $\tilde{R}$ est de classe C^1, et par l'expression des dérivées

$$\tilde{R}'(t) = A(t) \sum_{n=0}^{+\infty} {}_n(t) = A(t)\tilde{R}(t)$$

41. Quand A est abélienne, c'est encore une algèbre de Lie et $R(t)$ se promène dans son groupe de Lie ; réciproquement si G est un groupe de Lie linéaire réel et $: \mathbb{R} \to G$ alors est solution d'une équation di érentielle homogène $' = a(t)$ où $a(t) \in g$.

Avec la condition initiale $R'(0) = I_p$, ceci permet d'identifier R' à la résolvante R. Signalons que l'expression 61 est moins mystérieuse si l'on se rappelle, même vaguement, d'une preuve du théorème de Cauchy-Lipschitz. En effet, ce n'est guère plus qu'un théorème de point fixe, point fixe que l'on atteint par itérations d'une certaine application contractante, ce à quoi correspond le procédé de sommation des Ω_n dont la série converge vers la résolvante.

Si A est commutative, on peut changer l'ordre dans les produits, de sorte que

$$\forall \sigma \in \mathfrak{S}_n,\ \Omega_n(t) = \int_0^t \int_0^{t_n} \cdots \int_0^{t_2} A(t_{\sigma(n)}) A(t_{\sigma(n-1)}) \cdots A(t_{\sigma(1)})\, dt_{\sigma(1)}\, dt_{\sigma(2)} \cdots dt_{\sigma(n)}$$

Sommant ces égalités sur toutes les permutations, et divisant par $n! = |\mathfrak{S}_n|$, on obtient

$$\Omega_n(t) = \frac{1}{n!} \int_{[0;t]^n} A(\tau_1) \cdots A(\tau_n)\, d\tau_1 \cdots d\tau_n$$

Puis, par le théorème de Fubini sur pavé compact

$$\Omega_n(t) = \frac{1}{n!} \left(\int_0^t A(\tau)\, d\tau \right)^n$$

Finalement

$$R(t) = \sum_{n=0}^{+\infty} \Omega_n(t)\, dt = \sum_{n=0}^{+\infty} \frac{1}{n!} \left(\int_0^t A(\tau)\, d\tau \right)^n = \exp\left(\int_0^t A(\tau)\, d\tau \right)$$

Exemple 40.2 Soient a, b, c des fonctions scalaires $\mathcal{C}^0$ sur $\mathbb{R}$, et $(x_0, y_0, z_0) \in \mathbb{R}^3$: Résoudre l'équation

$$\begin{aligned} x' &= ax + by + cz & x(0) &= x_0 \\ y' &= cx + ay + bz & y(0) &= y_0 \\ z' &= bx + cy + az & z(0) &= z_0 \end{aligned}$$

41. Réciprocité quadratique par dénombrement d'une quadrique

Leçons :

101: (3) Actions de groupes

123: (2) Corps nis. Applications (mais, incompatible avec Réciprocité quadratique par somme de Gauss)

170: (3) Formes quadratiques.

190: (2) Combinatoire, problèmes de dénombrement.

Référence: Caldero-Germoni, Groupes et géométries, p. 181

Di culté: ***

Théorème 41.1. Soient p et ℓ deux nombres premiers impairs distincts. Alors

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

(a) Une première quadrique. Posons

$$C = \left\{ (x_0, \dots, x_{\ell-1}) \in F_p^{\mathbb{Z}/\ell\mathbb{Z}} ; \sum_{i \in \mathbb{Z}/\ell\mathbb{Z}} x_i^2 = 1 \right\},$$

Il s'agit d'une quadrique de l'espace vectoriel F_p^ℓ liée à la forme quadratique ayant pour matrice l'identité dans la base canonique. $\mathbb{Z}/\ell\mathbb{Z}$ agit sur $F_p^{\mathbb{Z}/\ell\mathbb{Z}}$ par permutation circulaires des coordonnées $g : x_k = x_{k+g}$ et cette action se fait par éléments de $O(q)$; en particulier C est préservée et l'équation aux classes donne, modulo ℓ

$$\begin{aligned} |C| &\equiv \left|C^{\mathbb{Z}/\ell\mathbb{Z}}\right| \\ &= \left|\left\{ x \in F_p \mid -x^2 = 1 \right\}\right| \\ &\quad \left|\left\{ x \in F_p \mid -1 x^2 = 1 \right\}\right| \\ &\equiv 1 + \left(\frac{-1}{p}\right) \end{aligned}$$

Ayant fait le changement de variables $x \mapsto x^{-1}$ entre la deuxième et la troisième ligne (on a bien $p - \ell$), la dernière ligne ayant lieu car dans F_p, le nombre de racines carrées de ℓ est $1 + (\ell/p)$ (vu que p est impair).

(b) Une deuxième quadrique.

Lemme 41.2. Posons $\ell_0 = (\ell - 1)/2$; alors l'espace quadratique $E = F_p^{\mathbb{Z}/\ell\mathbb{Z}}, q$ admet pour décomposition

$$E \simeq H^{\ell_0} \perp (-1)^{\ell_0} E$$

où H est le plan hyperbolique sur F_p.

Démonstration. Etant donnée la classi cation des formes quadratiques non dégénérées sur les corps nis, il su t de véri er que

$$\det(-E) = (-1)^{\ell_0} \det H^{\ell_0}$$

ce qui est bien le cas puisque $\det H^{\ell_0} = (\det H)^{\ell_0} = (-1)^{\ell_0}$.

Corollaire 41.3. Soit q^0 la forme quadratique donnée sur F_p^ℓ par

$$q^0(x_1,\dots,x_{\ell-1},y_1,\dots,y_{\ell-1},z) = 2\sum_{i=1}^{\ell-1} x_i y_i + (-1)^{\ell-1} z^2$$

et soit C^0 la conique d'équation $q^0(x) = 1$. Alors $|C^0| = |C|$.

Démonstration. Daprès le lemme q et q^0 sont équivalentes. En particulier, C^0 est l'image de C par un automorphisme linéaire.

(c) Dénombrement de C^0 et n de la preuve. Dénombrer C^0, c'est compter les éléments $x = (x_1,\dots,x_{\ell-1},y_1,\dots,y_{\ell-1},z) \in F_p^\ell$ tels que $q^0(x) = 1$.

(1) Tous les y_i sont nuls. Le choix des x_i est indi érent, ce qui donne $p^{\ell-1}$ possibilités, et z doit être racine de $(-1)^{\ell-1}$. Le nombre de tels points est donc

$$N_1 = p^{\ell-1}\left(1 + (-1)^{\ell-1}\right) = p^{\frac{\ell-1}{2}}\left(1 + (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}}\right)$$

(2) L'un des y_i, disons y_j, est non nul. Comme p est impair, $2y_j$ est encore non nul. Une fois xés les $x_1,\dots,x_{\ell-1}$ et z, il reste à choisir $(y_1,\dots,y_{\ell-1})$ dans un hyperplan a ne de $F_p^{\ell-1}$. Le nombre de tels points est

$$N_2 = p^{\ell-1}\left(p^{\ell-1} - 1\right)$$

En comparant les deux cardinaux, on obtient nalement modulo ℓ

$$1 + \frac{\ell}{p}\left(p^{\frac{\ell-1}{2}} - 1 + (-1)^{\frac{\ell-1}{2}\frac{p-1}{2}} + p^{\frac{\ell-1}{2}}\left(p^{\frac{\ell-1}{2}} - 1\right)\right) \equiv p^{\ell-1} + \frac{p}{\ell}\left(-1\right)^{\frac{\ell-1}{2}\frac{p-1}{2}}$$

Où l'on a remplacé $p^{\frac{\ell-1}{2}}$ par $\frac{p}{\ell}$ conformément à l'identité d'Euler. D'après le petit théorème de Fermat, $p^{\ell-1} \equiv 1$, ce qui donne nalement

$$\frac{\ell}{p} \equiv \frac{p}{\ell}\left(-1\right)^{\frac{\ell-1}{2}\frac{p-1}{2}} \pmod{\ell}$$

Puisque les deux quantités sont ± 1, la loi de réciprocité quadratique est démontrée.

42. Action de $SL(2;Z)$ sur H et formes quadratiques binaires

Référence. [Ser70, chapitre 6] pour l'action de $SL(2;Z)$ sur H. Pour l'équivariance des actions, c'est assez bien fait dans [Tri13] mais avec des notations plutôt opaques.

Difficulté ***. C'est trop long pour un développement. Il est plus raisonnable de contenter de parler de l'action de $SL(2;Z)$ sur H, et mentionner le reste dans la leçon.

Théorème 42.1. Le groupe $G = SL(2;Z)$ opère (à gauche) par homographies sur le demi-plan de Poincaré via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z = \frac{az+b}{cz+d}$$

De plus, si l'on pose

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$D = \left\{ z \in H \;\middle|\; \frac{1}{2} \leq \mathrm{Re}(z) < \frac{1}{2};\ |z| > 1 \text{ ou } (|z| = 1 \text{ et } \mathrm{Re}(z) \leq 0) \right\}$$

Alors

(i) Pour tout $z \in H$ il existe $g \in \langle S, T \rangle$ tel que $g \cdot z \in D$

(ii) $z \in D$ est l'unique dans son orbite dans D [42]

(iii) S et T engendrent G

Théorème 42.2. Le groupe $G = SL(2;Z)$ opère (à droite) par congruence sur l'ensemble Q des formes quadratiques binaires réduites [43] de discriminant < 0 par

$$q \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} (x;y) = q(ax+by; cx+dy)$$

De plus, si on note G l'ensemble des formes réduites au sens de Gauss, c'est à dire

$$G = \{ q = (a;b;c) \mid a < b \leq a \leq c;\ b \geq 0 \text{ si } a = c \}$$

Alors

(i) Pour tout $q \in Q$ il existe $g \in \langle S, T \rangle$ tel que $q \cdot g \in Q$

(ii) Si q et $q \cdot g$ sont dans G alors $g = \pm I$, sauf éventuellement si $q(x) = x^2 + x + 1$ ou $x^2 + 1$.

(iii) S et T engendrent G.

42.1. Deux actions équivariantes. On montre ici que la restriction de la première action aux entiers quadratiques de H est équivariante à la seconde (passée à gauche). Posons $H_2 = \{ z \in H \mid \deg_Q(z) = 2 \}$ et

$$\begin{aligned} H_2 &\to Q \\ z &\mapsto ((x;y) \mapsto (x - zy)(x - \bar{z}y)) \\ \frac{b + i\sqrt{-(q)}}{2a} &\leftarrow\!\shortmid\ q = (a;b;c) \end{aligned}$$

où Δ est l'entier minimal tel que $f(z) = (a;b;c)$ avec $a;b;c \in Z$ premiers entre eux dans leur ensemble. On peut voir H_2 comme inclus dans la sphère de Riemann $\hat{C}$ sur laquelle $PSL(2;C)$ opère naturellement :

$$\begin{aligned} H_2 &\to \hat{C} \\ z &\mapsto [z : 1] \end{aligned}$$

---

42. Plus précisément : si z et $g \cdot z$ sont dans D alors $g = \pm I$, sauf éventuellement si $z = j$ et $g \in \langle T \rangle$ ou si $z = i$ et $g = T$.

43. Ce sont les formes quadratiques binaires sur Z de la forme $ax^2 + bxy + cy^2$ avec $a > 0$ et a, b et c premiers entre eux dans leur ensemble

Puis $SL(2;Z)$ agit sur $\hat{C}$ via les morphismes

$$SL(2;Z) \quad PSL(2;Z) \,!\, PSL(2;C) \,!\, S(H_2)$$

En e et H_2 est stable pour cette action. Concrètement si $g = \begin{smallmatrix} a & b \\ c & d \end{smallmatrix}$ avec $ad \quad bc = 1$, et $z \ 2 \ H_2$ on pose

$$g:z = \frac{az + b}{cz + d}$$

Maintenant, montrons que $z^0 = g:z$ est racine[44] de $g:q$ ssi z est racine de q :

$$(g:q)(z^0;1) = 0 \quad () \quad q(az^0 + b; cz^0 + d) = 0$$
$$() \quad q(z;1) = 0$$

Il reste à voir que l'ensemble G des formes réduites au sens de Gauss correspond au domaine fondamental D. Soit donc $q = (a;b;c)$ réduite au sens de Gauss ; on note et $^-$ les racines dans C de $aX^2 + bX + c$, et on suppose par exemple $2 \ H$. Alors $^- = c=a > 1$ (puisque $a > 0$ et $c > a$). De plus

$$\mathrm{Re}( ) = \frac{+ \ ^-}{2} = \frac{b}{2a}$$

Donc on a bien $1=2 \ 6 \ < \ 1=2$; et nalement si $c = a$ alors $j \ j = 1$ et $b > 0$ donne $\mathrm{Re}( ) \ 6 \ 0$. Conclusion

$$q \ 2 \ G \quad () \quad \ 2 \ D$$

42.2. Lemme. Le lemme suivant peut servir à prouver l'invariance de H sous l'action par homographies réelles[45]

Lemme 42.3. Soit $z \ 2 \ H$, $g = \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \ 2 \ SL(2;R)$. Alors

$$\mathrm{Im}(g:z) = \frac{\mathrm{Im}(z)}{jcz + dj^2} \tag{62}$$

Démonstration. C'est un calcul :

$$\begin{aligned} g:z \quad \overline{g:z} &= \frac{az + b}{cz + d} \quad \frac{a\bar{z} + b}{c\bar{z} + d} \\ &= \frac{(az + b)(c\bar{z} + d) \quad (a\bar{z} + b)(cz + d)}{jcz + dj^2} \\ &= \frac{(ad \quad bc)z + (bc \quad ad)\bar{z} + acjzj^2 \quad acjzj^2 + bd \quad bd}{jcz + dj^2} \\ &= \frac{ad \quad bc}{jcz + dj^2}(z \quad \bar{z}) = 2i\,\mathrm{Im}(z) : \end{aligned}$$

42.3. On peut atteindre D depuis tout H à l'aide de S et T seulement.

Lemme 42.4. Soit $z \ 2 \ H$. Il existe $g \ 2 \ hS;Ti$ tel que $g:z \ 2 \ D$.

Démonstration. L'ensemble $cz + d \ j \ (c;d) \ 2 \ Z^2$ est discret donc ni dans tout compact. En particulier il existe $g_0 \ 2 \ hS;Ti$ tel que

$$\mathrm{Im}(g_0:z) = \max \{ \mathrm{Im}(g:z) \ ; \ g \ 2 \ hS;Ti \}$$

Quitte à remplacer g_0 par $T^n g_0$ pour $n \ 2 \ Z$ adéquat, on peut supposer que $\frac{1}{2} \ 6 \ \mathrm{Re}(g_0:z) < \frac{1}{2}$. On a alors $jg_0:zj > 1$; en e et si ce n'était pas le cas $Sg_0:z$ serait de partie réelle strictement plus grande. Maintenant, si $jg_0:zj = 1$ et $\mathrm{Re}(g_0:z) < 0$, $Sg_0:z$ est bien dans D.

44. Projection dans $\hat{C}$ du cône isotrope de q vue comme une forme complexe

45. Il y a aussi un argument topologique : $\hat{R}$ est stable, $\hat{C} \ n \hat{R}$ a exactement deux composantes connexes ; donc il su t de voir que i est envoyé dans H, par exemple.

42.4. Si z et z^0 dans D sont dans la même orbite sous $SL(2;Z)$, alors ils sont égaux. Par symétrie on peut supposer que $\mathrm{Im}(z^0) > \mathrm{Im}(z)$ de sorte que si $z^0 = g.z$ alors $|cz+d| \leq 1$. Ceci exclut $|c| > 2$ et laisse comme seuls cas possibles[46] $c = 0;1$

(1) $c = 0$. Dans ce cas $d = a = \pm 1$; quitte à changer g en $-g$ on peut supposer $a = d = 1$. Mais alors g est de la forme T^n et $\mathrm{Re}(z^0) - \mathrm{Re}(z) = n \in 2Z$, de sorte que l'on ne peut pas avoir simultanément g et g^0 dans D.

(2) $c = 1$. Dans ce cas $|z+d| \leq 1$; ceci n'est possible que si $d = 0$ (auquel cas g est de la forme $T^n S$) et donne alors $|z| = 1$, $\mathrm{Re}(z) \leq 0$, mais alors $\mathrm{Re}(Sz) \in [0;1/2]$ et $z = j$ ou c'est absurde; ou bien, si $d = \pm 1$ et on conclut de même avec cette fois-ci la possibilité $z = i$.

46. C'est $PSL(2;Z)$ qui agit dèlement donc on peut changer c en $-c$ sans changer l'opération de g

43. Théorème de Lie-Kolchin

Leçons :

106: Groupe linéaire, sous-groupes de $GL(E)$

154: Sous-espaces stables

157: Endomorphismes trigonalisables et nilpotents

Référence : [CL05]

Di culté : **.

Théorème 43.1. Soit $E = \mathbb{C}^n$, G un sous-groupe connexe résoluble de $GL(E)$. Alors tous les éléments de G sont simultanément trigonalisables.

Remarque 43.2. En termes de représentations des groupes topologiques, ceci équivaut à : toute représentation continue, irréductible, d'un groupe connexe résoluble, est de dimension 1.

43.1. Plan de la démonstration. On procède par double récurrence sur n et r, où n est la dimension de l'espace et r l'entier minimal tel que $D^r(G) = \{Id\}$. On commence par un

Lemme 43.3. Soit G un groupe topologique connexe. Le sous-groupe $D(G)$ est connexe.

Démonstration. L'ensemble S des commutateurs est connexe, en tant qu'image continue du connexe $G \times G$. Posons S^m l'ensemble des produits $s_1 \cdots s_m$ avec $s_i \in S$. On écrit alors

$$D(G) = \bigcup_{m=0}^{+\infty} S^m$$

Puisque les S^m sont connexes d'intersection deux à deux non vide, $D(G)$ est connexe.

43.2. Le cas irréductible : récurrence sur r. Commençons par supposer qu'il n'existe pas de sous-espace G-stable di érent de $\{0\}$ ou $\mathbb{C}^n$ et montrons que $n = 1$. On écrit $G_r = D^r(G)$ et on procède par récurrence sur r. L'initialisation $r = 1$ correspond au résultat classique avec G abélien (On prend v un vecteur propre d'un élément, il engendre une droite G-stable). On suppose donc $r > 1$ et on pose $H = D^{r-1}(G)$. H est un sous-groupe caractéristique, donc distingué, dans G.

Lemme 43.4. Soit V le sous-espace de $\mathbb{C}^n$ engendré par les vecteurs propres communs à tous les éléments de H ; alors $V = \mathbb{C}^n$. En particulier H est codiagonalisable.

Démonstration. H est abélien donc $V \neq 0$ d'après le cas d'initialisation. Il su t de montrer que V est G-stable. Pour tout v vecteur propre commun aux éléments de H nous pouvons écrire

$$\forall h \in H,\ h.v = \chi_h(v)\, v$$

Comme $H \subset G$, pour tout $h \in H$ et $g \in G$ il existe $h' \in H$ tel que $hg = gh'$.

$$h.(g.v) = gh'.v = g\,\chi_{h'}(v)\, v = \chi_{h'}(v)\, g.v$$

Donc, V est G-stable. D'après le théorème de la base trop complète il existe $(v_1, \ldots, v_n)$ une base de V telle que v_i est vecteur propre de tous les h dans H : H est codiagonalisable.

Lemme 43.5. Avec les notations ci-dessus, $H \subset Z(G)$

Démonstration. Soit $h \in H$; les $g^{-1}hg$ sont codiagonalisable avec même valeurs propres que celles de h, donc en nombre fini ($\leq n!$) et l'orbite $O = \{g^{-1}hg\}$ de h sous l'action de G est discrète. On a une application $G \to O$, $g \mapsto g^{-1}hg$ continue, d'un connexe à valeurs dans un discret donc constante égale à h.

Soit $h \in H$, W un espace propre de h. h commute avec tous les éléments de G, donc W est G-stable et $W = \mathbb{C}^n$; nalement H est un sous-groupe d'homothéties. Maintenant, $H \cap D(GL(\mathbb{C}^n)) = SL(\mathbb{C}^n)$ donc H est isomorphe à un sous-groupe de $_n(\mathbb{C})$. Par ailleurs H est connexe d'après le lemme donc H est trivial, ce qui est absurde.

43.3. Le cas général : récurrence sur n. On suppose $n > 1$. D'après ce qui précède il existe une droite vectorielle G-stable, notons la $\mathbb{C}e_1$ et complétons en une base $(e_1; : : : e_n)$ de $\mathbb{C}^n$. Dans cette base, les éléments de G sont sous la forme

$$[g] = \begin{matrix} (g) & ? \\ (0) & [g_2] \end{matrix}$$

L'application $g \mapsto g_2$ est un morphisme de groupes d'après la formule du produit par blocs. Par ailleurs elle est continue. Son image G_2 est un sous-groupe connexe, résoluble (c'est un quotient de G) de $GL\left(\mathbb{C}^{n-1}\right)$. Ceci conclut la récurrence.

Remarque 43.6. Le groupe T_n des matrices de la forme $I + T$ où T est triangulaire supérieure stricte dans $M_n(\mathbb{C})$, est connexe (c'est un sous-espace a ne) et résoluble. Pour voir qu'il est résoluble, observer que l'on a une décomposition en produit semidirect

$$T_n = \mathbb{C}^{n-1} \rtimes T_{n-1}$$

et que ces deux groupes sont résolubles ($\mathbb{C}^{n-1}$ est abélien ; T_{n-1} par hypothèse de récurrence, T_1 étant trvial). Donc T_n véri e les hypothèses du théorème de Lie-Kolchin, ce qui est assez peu utile vu qu'il est déjà construit sous la forme triangulaire supérieure.

Remarque 43.7. En fait on a seulement besoin de G Zariski-connexe, ce qui est plus faible.

Remarque 43.8. En théorie des algèbres de Lie, l'analogue est le théorème de Lie (qui n'implique cependant l'énoncé ici que pour les sous-groupes connexes fermés). L'énoncé analogue est incorrect pour les groupes nilpotents (avec triangulaire supérieur strict dans la conclusion), cependant, le théorème d'Engel donne une sorte de remplacement.

44. Inégalité de Carleman

Leçons: : Séries numériques

Références: :

Théorème 44.1 Soit $\sum a_n$ une série convergente de termes positifs. On pose

$$b_n = (a_1 \cdots a_n)^{1/n}$$

Alors $\sum b_n$ est convergente ; de plus si $a \neq 0$

$$\sum_{n>0} b_n < e \sum_{n>0} a_n \tag{63}$$

et la constante e est optimale.

44.1. Inégalité arithmético-géométrique. Tout d'abord, $b_n \leq \frac{1}{n}\sum_{k=1}^{n} a_k$, mais ceci ne suffit pas : une série peut très bien converger sans que la série des moyennes de Cesaro ne converge. En revanche,

$$b_n^n = \frac{1}{n!}(a_1 (2a_2) \cdots (na_n))$$

D'où

$$b_n \leq \frac{1}{n}(n!)^{1/n} \sum_{k=0}^{n} k a_k$$

44.2. Inégalité (large) de Carleman. Pour tout $N \in \mathbb{N}$,

$$\begin{aligned}\sum_{n=0}^{N} b_n &\leq \sum_{n=0}^{N} \frac{1}{n}(n!)^{1/N} \sum_{k=0}^{n} k a_k \\ &= \sum_{k=0}^{N} k a_k \sum_{n=k}^{N} \frac{1}{n}(n!)^{1/n}\end{aligned}$$

Il s'agit de majorer $(n!)^{1/n}$. D'après la formule de Stirling, $n!^{1/n} \sim n/e$. Plus précisément, montrons

Lemme 44.2 Pour tout $n > 1$ nous avons

$$\frac{n+1}{e}^{n} \leq n! \tag{64}$$

Démonstration. Par récurrence sur n : c'est vrai pour $n = 1$. Par ailleurs

$$\begin{aligned}\frac{n+2}{e}^{n+1} \frac{e}{n+1}^{n} &= e^{-1}(n+2) \frac{n+2}{n+1}^{n} \\ &= e^{-1}(n+1) \frac{n+2}{n+1}^{n+1} \\ &\geq e^{-1}(n+1)\, e = n+1\end{aligned}$$

En effet, la suite $(1+1/n)^n$ croît en convergeant vers e.

Finalement

$$\begin{aligned}\sum_{n=0}^{N} b_n &\leq \sum_{k=0}^{N} k a_k \sum_{n=k}^{+\infty} \frac{1}{n}(n!)^{-1/n} \\ &\leq \sum_{k=1}^{N} k a_k \sum_{n=k}^{+\infty} \frac{1}{n}\frac{e}{(n+1)} \\ &= \sum_{k=1}^{N} k a_k \sum_{n=k}^{+\infty} \frac{e}{n} - \frac{e}{n+1} \\ &= e \sum_{k=1}^{N} a_k\end{aligned}$$

Par passage à la limite quand $N \to +\infty$, on obtient l'inégalité

$$\sum_{n>0} b_n \leq e \sum_{n>0} a_n$$

44.3. Optimalité de la constante e. On a besoin d'une inégalité du même type que (64) mais dans l'autre sens :

Lemme 44.3. Pour tout ε tel que $0 < \varepsilon < e$ il existe $n_1 \in \mathbb{N}$ tel que pour $n > n_1$

$$n! \geq \left(\frac{n+1}{e}\right)^n$$

Démonstration. Posons $u_n = \left(\frac{n+1}{e}\right)^n$. D'après un calcul précédent

$$\frac{u_{n+1}}{u_n} = \frac{1}{e}(n+1)\left(\frac{n+2}{n+1}\right)^{n+1} \geq \frac{e}{e}(n+1)$$

Soit $\varepsilon > 0$ tel que $e - \varepsilon > 1 + \varepsilon > 1$. Pour $n > n_0$ assez grand,

$$\frac{u_{n+1}}{u_n} > (1+\varepsilon)\frac{(n+1)!}{n!}$$

De sorte que, toujours pour $n > n_0$:

$$\frac{u_n}{n!} > (1+\varepsilon)^{n-n_0}\frac{u_{n_0}}{n_0!}$$

Maintenant, il existe n_1 assez grand tel que $(1+\varepsilon)^{n_1-n_0} u_{n_0}/n_0! \geq 1$.

Remarque 44.4. On peut aussi obtenir le lemme directement à l'aide de la formule de Stirling.

Posons $a_n^{(N)} = 1/n$ si $n \in N$ et 0 sinon. Alors $b_n^{(N)} = (n!)^{-1/n}$ si $n \in N$ et 0 sinon. Pour tout $\varepsilon > 0$ nous avons pour N assez grand

$$\forall n \in \{n_1, \ldots, N\},\ b_n^{(N)} \geq \frac{e-\varepsilon}{n+1}$$

d'après le lemme précédent. Ce qui donne finalement

$$\begin{aligned}\sum_{n=1}^{+\infty} b_n^{(N)} &= \sum_{n=1}^{N} b_n \\ &= \sum_{n=1}^{n_1-1} b_n + \sum_{n=n_1}^{N} b_n \\ &\geq \sum_{n=n_1}^{N} \frac{e-\varepsilon}{n+1}\end{aligned}$$

D'après les résultats usuels sur la série harmonique, la dernière somme est équivalente à $\ln N$ quand on fait $N \to +\infty$. D'un autre côté

$$\sum_{n=1}^{+\infty} a_n^{(N)} \sim \ln N$$

De sorte que, pour tout $\varepsilon > 0$, il existe N tel que

$$\sum_{n=1}^{+\infty} b_n^{(N)} \leq \sum_{n=1}^{+\infty} a_n^{(N)}$$

Donc e est la constante optimale.

44.4. Inégalité stricte. Nous savons que l'inégalité arithmético-géométrique est stricte dès qu'on l'applique à des nombres distincts. D'après le calcul mené en (b), le cas d'égalité dans (63) ne peut être atteint que si a_k est égal à une constante c pour tout k.

(1) $c = 0$. Alors $a = 0$

(2) $c > 0$. Alors $a_n = c/n$ mais cette série diverge.

44.5. Compléments. Il existe une version intégrale, à savoir : Pour toute $f : \mathbb{R}_+^* \to \mathbb{R}_+$ positive mesurable,

$$\int_0^{+\infty} \exp\left(\frac{1}{x}\int_0^x \ln f(t)\,dt\right) dx \leq e \int_0^{+\infty} f(x)\,dx.$$

45. L^p est complet

Leçons: : 234 (Espaces L^p), 205 (espaces complets), 241 (suites et séries de fonctions)

Références: : [Bré83] [RRC87]

Définition 45.1. Soit E un espace mesuré de mesure positive Pour tout $p \in [1;+\infty]$ on définit $L^p(E)$ comme l'ensemble des applications $f : E \to \mathbb{R}$ telle que $|f|^p$ est intégrable sur E contre (ou μ-essentiellement bornées si $p = \infty$), quotienté par l'égalité μ-presque partout. L^p est un espace vectoriel, muni de la norme[47]

$$\|f\|_{L^p} = \left(\int_E |f|^p\right)^{1/p}$$

Théorème 45.2. $L^p(E)$ est un espace de Banach.

45.1. 1er cas : $p = 1$. Soit (f_n) une suite de Cauchy de L^1. Pour tout $k \in \mathbb{N}^*$ il existe N_k entier naturel tel que

$$\forall n,m > N_k,\ \|f_n - f_m\|_{L^1} \leq \frac{1}{k} \tag{65}$$

Soit $\tilde{f_n}$ un représentant de la classe de f_n pour tout n, et posons

$$A_{n,m}(k) = \left\{x \in E;\ |\tilde{f_n}(x) - \tilde{f_m}| \geq \frac{1}{k}\right\}.$$

Les parties $A_{n,m}(k)$ sont de mesure nulle pour $n,m > N_k$; d'après la propriété de sigma-additivité, nous avons

$$\mu\left(\bigcup_{k>1} \bigcup_{n,m>N_k} A\right) = 0. \tag{66}$$

Posons A cette union de mesure nulle. La première inégalité se particularise sur $E \setminus A$ et donne

$$\forall n,m > N_k, \forall x \in E \setminus A,\ |f_n(x) - f_m(x)| \leq \frac{1}{k} \tag{67}$$

En d'autres termes, pour tout $x \in E \setminus A$, la suite $\tilde{f_n}(x)$ est de Cauchy. $\mathbb{R}$ étant complet, elle admet une unique limite que nous noterons $\tilde{f}(x)$. Par passage à la limite dans l'inégalité (67) avec $k = 1$ quand $m > N_1$ tend vers $+\infty$, nous avons que $|f - f_{N_1}| \leq 1$ partout sur $E \setminus A$, donc $\tilde{f}$ est essentiellement bornée ; elle définit une unique classe $f \in L^1$. Il reste à voir que $f_n \to f$ en norme L^1 ; pour cela il suffit de montrer que $\tilde{f_n}$ converge vers $\tilde{f}$ uniformément sur $E \setminus A$. Pour tout $\varepsilon > 0$ on prend k tel que $1/k < \varepsilon$; puis en faisant tendre $m > N_k$ vers $+\infty$ on obtient

$$\forall n > N_k,\ \forall x \in E \setminus A,\ |\tilde{f_n}(x) - \tilde{f}(x)| \leq \varepsilon$$

qui est ce qu'on souhaitait.

45.2. 2ème cas : $p < 1$.

Lemme 45.3. Soit $(g_n)_{n>0}$ une suite de fonctions $E \to \mathbb{R}$ positives et μ-mesurables. Alors

$$\left\|\sum_{n=0}^{+\infty} g_n\right\|_{L^p} \leq \sum_{n=0}^{+\infty} \|g_n\|_{L^p} \tag{68}$$

47. Ceci résulte de l'inégalité de Minkowski

Démonstration. Déjà, la série $g = \sum_{n=0}^{+\infty} g_n$ est mesurable en tant que limite supérieure de fonctions mesurables ; l'intégrale $\int_E |g|^p$ est donc bien définie dans $\overline{\mathbb{R}_+}$, ce qui autorise le (léger) abus de notation $\|g\|_{L^p}$. Maintenant, nous avons pour tout N en vertu d'une récurrence immédiate de l'inégalité de Minkowski

$$\left\| \sum_{n=0}^{N} g_n \right\|_{L^p} \leq \sum_{n=0}^{N} \|g_n\|_{L^p}$$

Le théorème de convergence monotone de Beppo-Levi (pour le terme de gauche) et la définition de la série $\sum_{n=0}^{+\infty} \|g_n\|_{L^p}$ (pour le terme de droite) permettent le passage à la limite de cette inégalité dans $\overline{\mathbb{R}_+}$ quand $N \to +\infty$.

Soit à présent (f_n) une suite de Cauchy de L^p ; il existe une sous-suite $(f_{n_k})_{k>0}$ telle que $\|f_{n_{k+1}} - f_{n_k}\|_{L^p} \leq 1/2^k$. D'après le lemme, la série de terme général $g_k = f_{n_{k+1}} - f_{n_k}$ converge μ-presque partout vers une fonction $g \in L^p$. Pour μ-presque tout x dans E, nous avons donc que $(f_{n_k}(x))$ est de Cauchy, et converge vers une limite $f(x)$. Exactement comme dans le preimer cas, on montre que $f \in L^p$, puis que $f_{n_k} \to f$ en norme L^p.

Pour finir, observons que puisque (f_n) est de Cauchy, elle converge si et seulement si elle possède une valeur d'adhérence ; nous avons montré que f est limite d'une sous-suite, donc

$$f_n \to f$$

en norme L^p.

Rappel : preuve des inégalités de Hölder et de Minkowski.

Définition 45.4. Soit $p \in [1; +\infty]$, on appelle exposant conjugué de p et on note p' le nombre tel que

$$\frac{1}{p} + \frac{1}{p'} = 1$$

Théorème 45.5. (Inégalité de Hölder) Soient $f \in L^p$ et $g \in L^{p'}$. Alors $fg \in L^1$ et

$$\int_E |fg| \leq \|f\|_{L^p} \|g\|_{L^{p'}} \tag{69}$$

Démonstration. Rappelons l'inégalité de Young (qui s'obtient à l'aide de la concavité de la fonction log) :

$$\forall x, y \geq 0, \quad xy \leq \frac{x^p}{p} + \frac{y^{p'}}{p'}$$

L'inégalité de Young appliquée partout sur E à $|f|$ et $|g|$ avec $\lambda > 0$ donne

$$\int_E |fg| \leq \frac{\lambda^{p-1}}{p} \|f\|_{L^p}^p + \frac{1}{p'\lambda} \|g\|_{L^{p'}}^{p'}$$

Le terme de droite est dérivable par rapport à λ et il est minimisé pour $\lambda = \|g\|_{L^{p'}}^{p'/p} \|f\|_{L^p}^{-1}$. On obtient alors l'inégalité de Hölder.

46. Isométries in nitésimales et isométries globales

Leçons: : 214 (inversion locale, fonctions implicites), 215 (Calcul di),

Références: : [?]

Théorème 46.1. Soit E un espace euclidien et$f : E ! E$ de classeC^1 dont la di érentielle est partout dans O (E). Alors f est une isométrie a ne de E (en particulier, df est constante égale à sa partie linéaire).

1ère étape :f est localement une isométrie :

Lemme 46.2. Soit a 2 E ; alors il existeU_a voisinage ouvert dea dans E tel que pour tous x; y 2 U_a nous ayons :

$$kf(x) \quad f(y)k = kx \quad yk$$

Démonstration. L'inégalité $kf(x) \quad f(y)k \ 6 \ kx \quad yk$ est celle des accroissements nis appliquée sur le segment[x; y], et elle est valable sans restriction surx et y puisque E est convexe. Par ailleurs, commef est C^1 et de di érentielle df_a 2 O (E), le lemme d'inversion locale assure l'existence d'un ouvertU_a contenant a tel que f réalise un C^1-di éomorphisme de U_a sur $V = f(U_a)$; par conséquent$f^{\ 1} : V ! U_a$ est di érentiable et sa di érentielle est encore à valeurs dans le groupeO (E) (puisque par la formule de composition $df^{\ 1}_{f(x)} \quad df_x = Id$ pour tout x 2 U_a. Quitte à restreindre V (et donc U_a) à une boule ouverte centrée enf (a), on peut supposer queV est convexe ; donc par la même inégalité des accroissement nis, $f^{\ 1}(x^0) \quad f^{\ 1}(y) \quad k \ x^0 \quad y^0k$ pour tous $x^0; y^0$ 2 V. Appliquant ceci à $x^0 = f(x)$ et $y^0 = f(y)$ on obtient l'égalité voulue.

2ème étape : df est localement constante.

Lemme 46.3. Pour tout h; l 2 E, pour tous x; y 2 U_a nous avons

$$hdf_x(h) ; df_y(l)i = hh; li$$

Démonstration. D'après le lemme précédent$kf(x) \quad f(y)k = kx \quad yk$. Di érencions par rapport à x dans la direction h ; cela donne

$$2hdf_x(h) ; f(x) \quad f(y)i = hh; x \quad yi$$

Di érencions par rapport à y dans la direction l, cela donne

$$2hdf_x(h) ; df_y(l)i = \quad 2hh; li$$

On obtient bien ce que l'on souhaitait.

A présent montrons que df est constante sur U_a. Nous avons $hdf_x(h) ; df_y(l)i = hh; li$ mais aussi $hdf_x(h) ; df_x(l)i = hh; li$ pour tous h; l 2 E puisque df_x 2 O (E). Par conséquent$(df_x \quad df_y)(l) ? df_x(h)$ pour tous h; l ; donc $df_x = df_y$

3ème étape : Conclusion. df est localement constante surE, donc constante (E est connexe) égale à 2 O (E). Par intégration sur les segments, pour tousx et y dans E nous avons $f(y) \quad f(x) = \ (x \quad y)$. Par ailleurs est une isométrie ; doncf est une isométrie a ne de partie linéaire . En particulier, f est bijective.

Remarque 46.4. Si df est partout dans SO (E) alors f est un déplacement deE.

Remarque 46.5. La propriété de rigidité est perdue dès que l'on se donne un groupe un peu plus grand à la place deO (E). Par exemple, pour df 2 Sim(E) (groupe des similitudes directe) : considérer que toutes les applications holomorphes de$\mathbb{R}^2$ conviennent.

Remarque 46.6. Si f est seulement supposéeC^2, une preuve sans le lemme d'inversion locale est présentée dans [Rou03, Exercice 98].

47. Prolongement de Tietze

Leçons:

207: Prolongement de fonctions

241: Suites et séries de fonctions

Références: Schwarz, Topologie et analyse fonctionnelle ; Gourdon analyse

Théorème 47.1. Soit E un espace métrique, F un fermé de E, $[a;b]$ un intervalle compact de $\overline{R}$ et $f : F \to [a;b]$ une application continue. Alors, il existe

$$g : E \to [a;b]$$

continue, qui prolonge f sur F.

Remarque 47.2. Ce théorème est, plus largement, valable pour tous les espaces E topologiques dans lesquels deux fermés disjoints possèdent des voisinages ouverts disjoints. Un tel espace est dit normal ; en particulier, un espace métrique est normal. Les espaces normaux sont par ailleurs caractérisables par la propriété de prolongement précédente.

47.1. Lemme d'interpolation.

Lemme 47.3. Soit E un espace métrique, soient A et B deux parties fermées disjointes de E, a et b deux réels. Alors il existe une fonction f continue sur E qui vaut a sur A et b sur B.

Démonstration. Quitte à composer à droite par une application affine, il suffit de prouver le lemme pour $a = 0$ et $b = 1$. On utilise pour cela la distance à A et la distance à B, en posant pour tout $x \in E$

$$f(x) = \frac{d(x;A)}{d(x;A) + d(x;B)}$$

Cette fonction est bien définie puisque comme A et B sont disjoints et fermés nous avons

$$d(x;A) = 0 \iff x \in A \implies x \notin B \implies d(x;B) \neq 0$$

de sorte que $d(x;A) + d(x;B) > 0$ pour tout x (Remarquons que le lemme serait faux si l'on supposait A et B ouvertes).

Remarque 47.4. Parmi les espaces topologiques, ce lemme est encore une caractérisation des espaces normaux.

47.2. Preuve du théorème.

Lemme 47.5. Soient $E; F; f$ telle que dans les hypothèses du théorème, avec $F \to [\ ;\ ]$ continue. Alors il existe $\hat{f} : E \to [-1/3; 1/3]$ continue telle que

$$\forall x \in F,\ |f(x) - \hat{f}(x)| \leq \frac{2}{3} \tag{70}$$

Démonstration. On pose

$$A = \left\{ x \in F \mid f(x) \leq -\frac{1}{3} \right\}$$
$$B = \left\{ x \in F \mid f(x) \geq \frac{1}{3} \right\}$$

A et B sont fermés et disjoints dans E ; d'après le lemme, il existe $\hat{f}$ continue sur E à valeurs dans $[-1/3; 1/3]$ telle que $\hat{f}_{|A} = -1/3$, $g_{0|B} = 1/3$. Ensuite, quitte à disjoindre les cas pour tout $x \in F$, nous avons $\sup_F |f - \hat{f}| \leq 2/3$.

Nous pouvons à présent démontrer le théorème. On se donne $f : F \to [-1;1]$ continue ; par récurrence sur n entier naturel, nous définissons

$g_0 = \hat{f}$ telle que fournie par le lemme précédent

Pour tout $n \in \mathbb{N}$, $g_{n+1} = f \setminus g_n$.
Alors, par itération du lemme, nous avons d'une part

$$\sup_E |g_n| \leq \left(\frac{1}{3}\right)\left(\frac{2}{3}\right)^n$$

Et, d'autre part

$$\sup_F \left| f - \sum_{k=0}^{n} g_k \right| \leq \left(\frac{2}{3}\right)^n \tag{71}$$

La série de fonctions de terme général (g_k), à valeurs dans l'espace complet $\mathbb{R}$, est normalement convergente. Donc, sa somme

$$g = \sum_{k=0}^{+\infty} g_k$$

est bien définie et continue sur E. De plus, par passage à la limite quand n tend vers $+\infty$ dans l'inégalité (71), $g = f$ sur F.

Remarque 47.6. On peut, dans les hypothèses, remplacer l'espace d'arrivée de $\mathbb{R}$ par $\mathbb{C}$ (ou par $\mathbb{R}^d$) ; le théorème est toujours valable. En revanche, si l'on suppose que l'espace d'arrivée doit être $\mathbb{C}^*$, une obstruction d'ordre topologique apparaît. En effet, si $S^1 = F \subset E = \mathbb{C}$, il n'existe pas de prolongement continu à tout $\mathbb{C}$ de l'identité sur S^1, à valeur dans $\mathbb{C}^*$. En effet, supposons qu'il existe $g : \mathbb{C} \to \mathbb{C}^*$ dont la restriction à S^1 vaut l'identité. Alors, quitte à diviser $g(x)$ par sa norme pour tout x, on peut considérer que g est à valeurs dans S^1. Quitte à poser $h_t(x) = (1-t)x + tg(x)$ poue tout x dans B^1 et $t \in [0;1]$, on a construit une rétraction de B^1 sur S^1, ce qui est absurde (d'après le lemme de non retraction). Toutefois, d'après le théorème du degré de Hopf (on a ici, en fait, seulement besoin d'un cas élémentaire), si g est de degré 0, elle se prolonge à tout $\mathbb{C}$.

Applications.

(1) Conjointement au théorème du point fixe de Brouwer, le théorème de Tietze-Urysohn est un ingrédient dans une preuve du théorème de Jordan.

(2) Les sous-groupes compacts de $GL(n;\mathbb{R})$ sont (des points réels de groupes) algébriques, [MMT86, Theorem 3.7.1].

48. Images des exponentielles

Références. [ZR13] On a un peu simplifié le passage de $\mathbb{C}$ à $\mathbb{R}$.
Pré-requis. $\exp : \mathbb{C} \to \mathbb{C}$ est surjective.

Théorème 48.1. On considère l'application $\exp : M_n(K) \to GL(n;K)$
(i) Si $K = \mathbb{C}$, exp est surjective. De plus pour toute $A \in GL(n;\mathbb{C})$ il existe $C \in \mathbb{C}[A]$ telle que $\exp(C) = A$
(ii) Si $K = \mathbb{R}$ exp atteint exactement les carrés de $GL(n;\mathbb{R})$. Plus précisément, si $A \in GL(n;\mathbb{R})$ est de la forme C^2 alors il existe $B \in \mathbb{R}[C]$ tel que $\exp(B) = A$.

48.1. Nil et Uni.

Lemme 48.2. Soit K le corps $\mathbb{R}$ ou $\mathbb{C}$. Alors, exp réalise un homéomorphisme de $Nil_n = \{N \in M_n(K) ; N$ est nilpotente$\}$ vers l'ensemble $Uni_n = I_n + Nil_n$ des matrices unipotentes

Démonstration. Introduisons les polynômes

$$E(X) = \sum_{k=0}^{n-1} \frac{X^k}{k!}$$

$$L(X) = \sum_{k=1}^{n-1} \frac{(-1)^{k+1}}{k} (X-1)^k :$$

Puisque l'indice de nilpotence est majoré par n, nous avons pour toute $N \in Nil_n$, $\exp(N) = E(N)$, et $E(N)$ est une matrice unipotente ($E(N) - I$ est une somme de matrices nilpotentes qui commutent). De même, pour toute $U \in Uni_n$, $L(U)$ est nilpotente.

Nous allons montrer qu'il existe R et S dans $\mathbb{Q}[X]$ tels que

$$L \circ E(X) = X + X^n R(X)$$
$$E \circ L(X) = X + (X-1)^n S(X) :$$

Puisque X^n (resp. $(X-1)^n$) annule tout Nil_n (resp. Uni_n) ceci impliquera $L \circ E_{|Nil_n} = Id_{Nil_n}$ et $E \circ L_{|Uni_n} = Id_{Uni_n}$. E et L étant continus, ceci attestera que 'il s'agit d'homéomorphismes. Par développement limité aux voisinages de 0 et 1

$$\exp(x) =_{x\to 0} E(x) + O(x^n)$$
$$\ln(x) =_{x\to 1} L(x) + O((x-1)^n) :$$

D'où pour $x \to 0$

$$\begin{aligned} L \circ E(x) &= L(\exp(x) + O(x^n)) \\ &= \ln(\exp(x)) + O((E(x)-1)^n) + O(x^n) \\ &= x + O(x^n) : \end{aligned}$$

Tandis que pour $x \to 1$

$$\begin{aligned} E \circ L(x) &= E(\ln(x) + O((x-1)^n)) \\ &= \exp(\ln x + O((x-1)^n)) + O\left(\ln x + O((x-1)^n)\right)^n \\ &= x(1 + O(x-1)^n) + O((x-1)^n) \\ &= x + O((x-1)^n) : \end{aligned}$$

Nous avons donc

$$L \circ E(x) - x =_{x\to 0} O(x^n) :$$

Donc $L \circ E - X = X^n R(X)$ où $R \in \mathbb{Q}[X]$. De même,

$$E \circ L(x) - x =_{x\to 1} O((x-1)^n) :$$

Donc $E \circ L - X = (X-1)^n S(X)$ où $S \in \mathbb{Q}[X]$.

48.2. Le cas complexe. Soit maintenant $A \in GL(n;C)$; nous la décomposons sous la forme $A = D + N = D\,I_n + D^{-1}N = DU$, où $A = D + N$ est la décomposition de Dunford. D'après le lemme précédent, $U = \exp(N')$ avec $N' \in C[A]$, N' nilpotente.

D'un autre côté, il existe $P \in GL(n;C)$ tel que $P^{-1}D^2P = \mathrm{diag}(\lambda_1;\dots;\lambda_n)$, les λ_i dans C^*. Comme exp est surjective sur C^*, il existe $\mu_1;\dots;\mu_n$ tels que $\exp(\mu_i) = \lambda_i^2$. On pose donc

$$= P^{-1}\mathrm{diag}(\mu_1;\dots;\mu_n)P$$

Il existe $\in C_{n-1}[X]$ interpolateur de Lagrange aux points $(\mu_i;\mu_i)$ de sorte que $= (D)$ et $\in C[A]$. Finalement, $+N \in C[A]$ et puisque $C[A]$ est commutative,

$$\exp(+N) = A$$

48.3. Le cas réel. Si $A \in GL(n;R)$ est une exponentielle, alors c'est un carré : soit en effet B telle que $A = \exp B$, on prend $C = \exp(B/2)$, alors $A = C^2$.

Réciproquement, soit $A = C^2$ un carré de $GL(n;R)$. Alors $A = C\overline{C}$; C est l'exponentielle d'une matrice complexe, il existe donc B_0 et un polynôme P tels que $B_0 = P(C)$ et $\exp(B_0) = C$ d'après ce qui précède. On pose $B = B_0\overline{B_0}$; alors B_0 et $\overline{B_0}$ commutent et $\exp(B) = A$. De plus, $B \in C[C]$ comme requis.

Remarque 48.3. On peut retrouver la surjectivité de l'exponentielle complexe à partir du cas (i) du théorème. Le corps C s'injecte dans $M_2(R)$ via

$$\begin{aligned} ' : C &\to M_2(R) \\ x+iy &\mapsto \begin{pmatrix} x & y \\ y & x \end{pmatrix} \end{aligned}$$

Soit donc $z \in C^*$. C'est un carré dans C^*, disons $z = ^2$. Maintenant, $'(z) = '(\ )^2$, et donc $'(z)$ est un carré de $GL(2;R)$. D'après le théorème, nous pouvons écrire $(z) = \exp C$, avec $C = Q('(\ ))$ pour un certain polynôme $Q \in R[X]$. Mais $'$ est un automorphisme d'algèbre, donc $C = '(Q(\ )) \in \mathrm{Im}\,'$. Finalement, si l'on prend $= '^{-1}(C)$, alors $\exp = z$.

Remarque 48.4. On peut également obtenir l'identité $L\ E_{j\mathrm{Nil}_n} = \mathrm{Id}_{\mathrm{Nil}_n}$ en travaillant dans l'agèbre $K[[X]]$ des séries formelles. Les spécialisations

$$\begin{aligned} K[[X]] &\to M_n(K) \\ F &\mapsto F(N) \end{aligned}$$

sont possibles parce que N est nilpotent. Pour l'identité inverse on peut faire de même dans $K[[X-1]]$.

Remarque 48.5. On peut donner une seconde preuve plus topologique. On désigne par C le groupe des inversibles de l'algèbre de Banach $C[A]$; soit $C = C[A] \cap GL(n;C)$. Ce groupe est connexe (car connexe par arcs). L'application exponentielle est un morphisme de $C[A]$ vers C ; d'après le théorème d'inversion locale elle est ouverte, et donc surjective.

49. Il n'y a pas de groupe simple d'ordre $864 = 2^5 \cdot 3^3$

Référence. [Isa08] (qui traite le cas d'ordre $2^6 \cdot 7^3$)

Difficulté. ** S'il s'agit d'un développement, le théorème 49.1 peut être admis.

Théorème 49.1 (Sylow). Soit G un groupe d'ordre $p^n m$, p premier tel que $p \nmid m$. Alors G possède un sous-groupe d'ordre p^n. De plus, le nombre de tels sous-groupes est congru à 1 modulo p.

Pour le théorème suivant on note $n_p(G)$ le nombre de p-Sylow du groupe fini G.

Théorème 49.2 (Raffinement sur le nombre de p-Sylow, [Isa08]). Soit G un groupe fini d'ordre $p^n m$, $p \nmid m$, qui ne normalise pas ses p-Sylow. Soit $P = S \cap T$ une intersection de cardinal maximal p^k entre deux Sylows S et T de G. Alors

$$n_p(G) \equiv 1 (p^{k+1}).$$

49.1. Preuve de Wielandt d'une partie des théorèmes de Sylow.

Démonstration du théorème 49.1 d'après [Per96, Exercice I.C.2]. On introduit pour la preuve l'ensemble X des parties de G de cardinal p^n et Y l'ensemble des p-Sylow de G. Pour $E \in X$, on note $G_E = \mathrm{Stab}_G(E)$.

Soit donc $E \in X$ et soit $x \in E$, puisque E est stable par G_E on a une injection $G_E \to E$ qui à g associe gx. Donc $|G_E| \leq |E| = p^n$. Si $|G_E| = p^n$ alors l'application précédente est une bijection, donc $E = G_E x$ avec $G_E \in Y$. Réciproquement si E est de la forme Sx avec $x \in G$ et $S \in Y$ alors on a que $G_E = S$.

Soit Ω l'ensemble des orbites de X sous G et $(E_1, \dots, E_r)$ des représentants. Alors d'après l'équation aux classes nous pouvons écrire

$$|X| = \sum_{\omega \in \Omega} |\omega| = \sum_{i=1}^{r} \frac{|G|}{|G_{E_i}|}.$$

Modulo p, $|G|/|G_{E_i}|$ est congru à m si $|G_{E_i}| = p^n$, autrement dit si $E_i \in Y$, et à 0 sinon, d'où la congruence voulue. Le cardinal de X ne dépend pas de la structure de groupe sur G ; on peut donc supposer $G = \mathbb{Z}/n\mathbb{Z}$, dans ce cas nous savons d'après la section 401 qu'il existe un unique sous-groupe d'ordre p^n, ie $|Y| = 1$, ce qui donne $|X| \equiv m\ (p)$. Finalement, $m \equiv |Y| \equiv m\ (p)$, et $p \nmid m$, donc $|Y| \equiv 1\ (p)$. En particulier, il existe un p-sous-groupe de Sylow et leur nombre est congru à 1 modulo p.

49.2. Conjuguaison et nombre des Sylow.

Soit p un nombre premier.

Théorème 49.3. Soit G un groupe fini, $P < G$ un p-groupe et $S < G$ un p-Sylow de G. Il existe $g \in G$ tel que $P < gSg^{-1}$. En particulier, les p-Sylow de G sont conjugués, et ce sont les p-sous-groupes maximaux pour l'inclusion.

Démonstration. Ecrivons $|G| = p^n m$ avec m non divisible par p. Examinons l'opération de P sur G/S par translations à droite. Les orbites ont des cardinaux diviseurs de l'ordre de P, donc multiples de p dès qu'elles sont non réduites à un élément. Mais leur somme est égale à m. Donc une orbite est réduite à un point, disons que c'est Sg. Alors $sgp \in Sg$ pour tout $s \in S$ et $p \in P$, donc $P \subset gSg^{-1}$.

Proposition 49.4. Le nombre de p-Sylow est $|G : \mathrm{Norm}_G(S)|$ si S est un p-Sylow quelconque. En particulier il divise l'ordre de G.

C'est une conséquence imédiate du fait que l'action de G par conjuguaison est transitive sur les p-Sylow. Si G est le normalisateur de S, il n'y a qu'un seul p-Sylow.

Lemme 49.5. Soit P un p-Sylow de G. Tout p-sous-groupe de $\mathrm{Norm}_G(P)$ est contenu dans P.

Démonstration. Par définition, P est normal dans $\mathrm{Norm}_G(P)$; il y est donc l'unique p-Sylow et d'après le théorème 49.3, il contient tout p-sous-groupe.

49.3. Preuve du théorème 49.2. Soit S un Sylow de G. Dans l'action de S par conjuguaison sur les Sylow de G, l'orbite de T pour T di érent de S a pour cardinal $|S : Q|$, où $Q = \mathrm{Norm}_G(T) \cap S$. Mais Q est un p-sous-groupe de $\mathrm{Norm}_G(T)$, il est donc contenu dans T d'après le Lemme 49.5. On en déduit que $|S : Q|$ est une puissance de p supérieure à p . Finalement l'orbite de S est de cardinal 1. Donc $n_p(G) \equiv 1$ modulo p .

49.4. Pas de groupe simple d'ordre 864.

Lemme 49.6 ([Isa08, Corollary 1.3]) Soit G un groupe simple. Si G contient un sous-groupe d'ordre m, alors l'ordre de G divise $m!$.

Démonstration. Soit H le sous-groupe en question. Si $H = 1$ ou $H = G$ il n'y a rien à montrer. Il y a une action non triviale, donc dèle (vu que G est simple) de G sur G/H. D'après le théorème de Lagrange l'ordre de G divise $|S_{G/H}| = m!$.

Soit maintenant G un groupe simple d'ordre 864. On note n_2 et n_3 ses nombres de 2- et de 3-Sylow respectivement. Nous savons d'après le théorème 49.1 que $n_3 \equiv 1 (3)$ et $n_3 \mid 32$. Puisque G est simple, nous avons que n_3 est égal à 4 ou 16. En particulier, n_3 n'est pas congru à 1 modulo 3^2, donc d'après le théorème 49.2 G possède deux 3-Sylow (notons les S et T) dont l'intersection $P = S \cap T$ est d'indice 3 dans les deux. Puisque 3 est le plus petit facteur premier divisant l'ordre de S et T (c'est le seul), P est normal dans S et dans T. Introduisons $N = \mathrm{Norm}_G(P)$. D'après ce qui précède, S et T sont dans N, donc $n_3(N) > 1$. Puisque $n_3(N) \equiv 1 (3)$, on a que $n_3(N) > 4$. Mais aussi, $n_3(N)$ divise $|N| = 27$, qui est une puissance de 2. On en déduit que N est d'ordre au moins $4 \cdot 27$, donc d'indice au plus 8 dans G. Mais $|G|$ ne divise pas $8!$ (ni a fortiori $m!$ pour $m < 8$. Contradiction avec le lemme.

Commentaires. D'après un théorème de Burnside, les groupes d'ordre $p^a q^b$ sont résolubles. La preuve utilise la théorie des caractères ; on sait de nos jours l'éviter, mais c'est technique [Isa08, Chapitre 7]. Pour les groupes d'ordre pq, p^2q, la version simple du théorème de Sylow su t. 864 nous semble bien adapté pour illustrer l'intérêt du théorème car il a beaucoup plus de diviseurs. D'ailleurs il y a beaucoup de groupes d'ordre 864, il y en a

$$\mathrm{gnu}(864) = 4725$$

d'après [CDO08, Table 3] (véri cation sur de petits nombres de la conjecture des gnous gallopants).

Chapitre 1

Leçons

101. F Groupe opérant sur un ensemble. Exemples et applications.

Développements possibles.
3 Déterminant de Smith
7 Ellipsoïde de John, applications.
8 Théorème de la base de Burnside.

I. Langage des actions de groupes.
I.1. Dé nitions.

Définition 101.1 Soit G un groupe et X un ensemble. Une action de G sur X est la donnée de $(G; X) ! X$ notée $(g; x) 7! g:x$ telle que $1:x = x$ et $g:(h:x) = gh:x$ pour tous $g; h 2 G$ et $x 2 X$.

De manière équivalente, c'est un homomorphisme de groupes $: G ! S_X$. Vues les données (groupe et ensemble) en présence il est parfois plus naturel d'encoder une action par $(X; G) ! X$; on parle d'action à droite, et l'on requiert $(x:gh = x:g):h$.
Par exemple si X est muni d'une action de G à gauche, on munira l'espace des fonctions sur X à valeur dans R d'une action de G à droite.
Si X est muni d'une action à gauche de G on dit de X que c'est un G-ensemble.

Définition 101.2 L'action est dèle si est injectif, transitive si pour tous $x; y 2 X$ il existe $g 2 G$ tel que $g:x = y$, libre si $f g 2 G : g:x = x g$ est trivial pour tout $x 2 X$.

Définition 101.3 Soit $(G; X) ! X$ une action. L'orbite de $x 2 X$ est $O(x) = f g:x : g 2 G g$ (en particulier, une action est transitive si elle n'a qu'une orbite). Le stabilisateur de x est $Stab_G(x) = f g 2 G : g:x = x g$.

Lemme 101.4 Les stabilisateurs d'éléments d'une même orbites sont conjugués, en particulier s'ils sont nis, ils ont le même cardinal.

Définition 101.5 (G-morphismes et invariants). Soient X et Y deux G-ensembles ; $f : X ! Y$ est G-équivariante si $f(g:x) = g:f(x)$. On dit aussi de f que c'est un G-morphisme, ou qu'il entrelace les actions. Si Y est équipé de l'action triviale on dit que f est un invariant.

Exemple 101.6 Exemple d'invariant : le birapport.

I.2. Notions construites à partir de groupe opérant.

Exemple 101.7 Espace a ne : c'est un espace vectoriel qui agit.

Exemple 101.8 ([Per96]) Espace homogène $G=H$: ce sont les G-ensembles transitifs.

Exemple 101.9 Produit semidirect : Etant donnés deux groupes N et H et une action de H sur N par automorphismes, on forme un produit semidirect.

Proposition 101.10 Soient $N o H$ et $M o H$ deux produits semidirects. Si $f : N ! M$ est un homomorphisme de groupes H-équivariant, alors f s'étend en un homomorphisme des produits semi-directs.

(La proposition est utile quand on veut énumérer les produits semidirects.)
On voit ainsi l'absence d'équivariance comme une obstruction à étendre les morphismes .

I.3. Action et classi cation.

Exemple 101.11 Exemples venant de l'algèbre linéaire :r -équivalence, similitude, congruence (matrices).

On cherche des invariants pour une action de groupe. Parfois cela su t à résoudre le problème de l'équivalence (exemple : réduction/classi cation de Jordan).

II. Applications combinatoires et théorie des groupes. Souvent les groupes sont dé nis par leurs actions (ex : groupe linéaire, groupe symétrique). Par renversement du principe précédent, un invariant peut aider à dé nir un groupe. Exemple : Groupe orthogonal.

II.1. Application aux groupes nis.

Proposition 101.12 (Formule des classes)Soit G un groupe agissant sur$X$. Soit l'espace des orbites. Alors

$$jX j = jGj \sum_{! \ 2} \frac{1}{jG_! j}$$

où $jG_! j$ désignej $Stab_G(x)j$ pour n'importe quel $x \ 2 \ !$.

Proposition 101.13 Soit G un p-groupe ni. Le centre de G est non trivial.

Proposition 101.14 (Cauchy) Soit G un groupe ni, p un nombre premier qui divise l'ordre de G. Alors, G possède un élément d'ordre$p$.

Théorème de la base de Burnside : voir développement 8.

II.2. Formule de Burnside. Application au dénombrement.

Proposition 101.15 Soit G un groupe ni agissant dans$X$ et l'espace des orbites. Alors

$$j \ j = \frac{1}{jGj} \sum_{g2 \ G} j^g X j$$

où $^g X$ désigne l'ensemble des éléments xés par$g$.

Exemple 101.16 Il y a 24 façons de peindre6 faces d'un dodécaèdre en noir et6 faces en blanc (à isométrie près).

Exemple 101.17 Il y a 76 colliers de perles avec4 perles bleues,3 noires et2 blanches.

II.3. Isomorphismes exceptionnels.Exemples $PGL_2(F_5) \simeq S_5$ ou encore$SO_3(\mathbb{R}) \simeq SU_2(\mathbb{C})=f \ 1g$

III. Actions et représentations.

III.1. Représentation de permutation. Points xes. Actions transitive, doublement transitives. Soit k un corps. Soit une action de$G$ dans l'ensemble ni X, et soit E l'espace des sommes formelles d'éléments de$X$ à coe cients dans le corps$k$. On forme une représentation de$G$ dans$V$ en posant

$$g: \sum_x {}_x x = \sum_x {}_x g:x:$$

Exemple 101.18 La représentation régulière (gauche) est la représentation de permutation associée à l'action de$G$ sur lui-même par translation à gauche.

III.2. Représentations de permutation des groupes cycliques.Voir le développement 8.

IV. Utilisation des G-morphismes en géométrie.

IV.1. De l'ellipsoïde de John aux sous-groupes compacts maximaux de$GL_n(\mathbb{R})$.

IV.2. Action de $SL_2(\mathbb{Z})$ sur $\mathbb{H}$ et classi cation des formes quadratiques binaires entières.

Compléments hors leçon. En terme de théorie des catégories, une action du groupe G sur l'ensemble$X$ peut être vue comme un groupoïde avec espace d'objets$X$ muni d'un foncteur vers$G$ (vu comme groupoide) qui étiquette la èche $x \to g:x$ par g. Les actions sont donc dans un sens des groupes généralisés.

102. F Groupe des nombres complexes de module 1

Au préalable de cette leçon, on suppose construits
- Le corps R des nombres réels, par exemple comme complétion de $\mathbb{Q}$ pour la valeur absolue $|\ |_1$
- Le corps C, comme sous-algèbre à involution de $M_2(R)$.
- L'exponentielle réelle, les fonctions trigonométriques cos et sin, ainsi que leurs développements en séries entières.

.

I. Le groupe U.

I.1. Dé nition.

Proposition 102.1. L'application $N : C \to R_+, z \mapsto z\bar{z}$ est un morphisme de groupes en restriction à C. On note U son noyau ; c'est un groupe abélien compact, homéomorphe au cercle unité de R^2. En particulier, U est connexe.

Théorème 102.2. La série $\exp : z \mapsto \sum_{n=0}^{+\infty} z^n/n!$ converge normalement sur tout compact de C et dé nit un morphisme de groupes surjectif vers C. On a $\exp(i\ ) = \cos\ + i \sin$ et $\exp(x + iy) = e^x \exp(iy)$ pour x et y réels, en particulier $\ker \exp = 2i\ Z$.

Le seul point délicat est la surjectivité et il y a essentiellement deux manières de la prouver. L'une (ad hoc) est de construire une détermination du logarithme. L'autre est d'utiliser un peu de topologie et montrer que $\exp$ est ouverte, par exemple avec le théorème d'inversion locale, puis d'image ouverte et fermée dans C.

Corollaire 102.3. Le groupe U est isomorphe à R/Z. En particulier, c'est un groupe divisible.

I.2. Les sous-groupes de U.

Proposition 102.4. Les sous-groupes de U sont cycliques ou denses dans U.

Soit p un nombre premier. $Z[1/p]/Z$ est un sous-groupe (dense) de U. U contient des sous-groupes abéliens libres de tout rang.

Proposition 102.5. Soit G un groupe de type ni. Alors G se plonge dans U si et seulement si $G = C \quad Z^r$ où C est un groupe cyclique et $r > 0$. En particulier, les sous-groupes nis de U sont cycliques.

II. Le groupe U_n.

II.1. Polygone réguliers convexes.

On munit C de la structure euclidienne. L'enveloppe convexe de $e^{2k\ i/n}\ ; k \in Z$ est un polygone régulier.

Théorème 102.6. Soit P un polygone régulier convexe non dégénéré du plan euclidien R^2 à sommets dans Z^2. Alors P est un carré.

La preuve utilise que l'anneau $Z[i]$ est factoriel. Voir pour cela le développement 13.

II.2. Théorème de Kronecker sur les polynômes à racines dans le disque unité.

Voir le développement 19.

II.3. Représentations complexes des groupes cycliques.

Voir la leçon 110. Application : transformée de Fourier rapide [Dem08].

III. Aspects arithmétiques.

III.1. Polynôme cyclotomiques.

Définition 102.7. Soit $n > 2$. On dé nit le polynôme $_n(X) \in C[X]$ par

$$_n(X) = \prod_{\in Z_n} (X \quad)$$

où Z_n est l'ensemble des racines primitives n-ièmes de l'unité.

Proposition 102.8. $_n(X) \in Z[X]$.

Théorème 102.9 (Dirichlet faible). Il existe une infinité de nombres premiers de la forme $an + 1$, $a > 1$.

Théorème 102.10 (Gauss). $\Phi_n(X)$ est irréductible.

III.2. Constructibilité. Voir le développement 10.

IV. Le groupe des quaternions unitaires. Développement 25.

Proposition 102.11 Les sous-groupes connexes fermés de $\mathbb{H}$ sont isomorphes à $\{1\}$, U ou V et ceux de la seconde famille sont classifiés par leur algèbre de Lie, une droite de quaternions purs.

Remarque 102.12 V contient des semi-groupes libres non abéliens.

103. F Exemples de sous-groupes distingués et de groupe quotient.

Le but est de ne pas faire une leçon sur les groupes simples (qui ont plus leur place dans les leçons sur les groupes linéaires et les groupes symétriques). On s'intéresse ici plutôt aux groupes nilpotents et résolubles. Bien que la théorie de Galois soit un peu au-delà du programme de l'agrégation, c'est elle qui a motivé l'introduction de ces notions, jusqu'à la terminologie (en partie), il ne semble donc pas vain de la mentionner comme application. Cette leçon comporte beaucoup de dé nitions et peu de théorèmes substantiels hors applications ; il est donc bon de connaître des exemples instructifs pour l'agrémenter ou elle restera insipide.

I. Dé nitions et premiers exemples.

I.1. Sous-groupe distingué.

Définition 103.1. Soit G un groupe et H un sous-groupe de G. On appelle ensemble des classes à gauches suivant H dans G l'ensemble $\{gH\}_{g\in G}$, noté G/H. De même, $H\backslash G = \{Hg^{-1}\}_{g\in G}$ est l'ensemble des classes à droite.

En termes d'actions de groupe (leçon 101), G/H est l'espace des orbites pour l'action par translation à droite de H dans G. Naturellement, G opère (à gauche) sur G/H. On a les mêmes énoncés à droite.

Définition 103.2. H est distingué (ou normal) dans G, noté $H \trianglelefteq G$, si pour tout $g \in G$, $gHg^{-1} = H$. De manière équivalente, H est distingué dans G si les partitions de G en classes à gauche ou à droite suivant H coïncident. (On parle parfois de décomposition propre dans ce cas.)

Définition 103.3 (Normalisateur). Soit H un sous-groupe de G. On appelle normalisateur de H dans G, et on note $N_G(H)$, le sous-groupe $\{g \in G : gHg^{-1} = H\}$. C'est le plus grand sous-groupe de G dans lequel H est normal.

Définition 103.4 (Sous-groupe caractéristique.) Le sous-groupe H de G est caractéristique s'il est stable par tout automorphisme de G. Un sous-groupe caractéristique est distingué. La réciproque n'est pas valable.

Exemple 103.5. Soit G un groupe. Le groupe $\mathrm{Inn}(G)$ des automorphismes intérieurs de G est distingué dans le groupe $\mathrm{Aut}(G)$.

Exemple 103.6. Les sous-groupes d'indice 2 sont distingués. Si G est ni, les sous-groupes d'indice p de G, où p est le plus petit diviseur de l'ordre, sont distingués.

I.2. Groupe quotient.

Proposition 103.7. Soit H un sous-groupe distigué de G. Alors G/H est muni d'une loi de groupe, $(gH)\,(g'H) = gg'H$. On l'appelle le groupe quotient. Le morphisme $G \to G/H$, $g \mapsto gH$ est dit canonique.

Proposition 103.8 (Premier théorème d'isomorphisme pour les groupes.) Soit $\varphi : G \to H$ un morphisme de groupes surjectif. Alors $\ker \varphi \trianglelefteq G$, et $H \simeq G/\ker \varphi$.

Proposition 103.9 (Second théorème d'isomorphisme pour les groupes.) Soit $\{S, N\}$ une paire de sous-groupes de G, avec $N \trianglelefteq G$. Alors SN est un sous-groupe, $S \cap N$ est normal dans S, et

$$SN/N \simeq S/(S \cap N).$$

Attention, parfois le premier théorème est appelé « fondamental » et le second théorème « premier théorème ». C'était le cas dans l'ancien traité d'algèbre de Van der Waerden.

Exemple 103.10. $\mathrm{PGL}(2;\mathbb{C}) = \mathrm{PSL}(2;\mathbb{C})$.

II. Groupe dérivé et abélianisé. Deux exemples : groupe linéaire, groupe symétrique.

Proposition 103.11. $D(S_n) = A_n$

Proposition 103.12. $D(\mathrm{GL}(n;k)) = \mathrm{SL}(n;k)$ sauf cas particuliers.

Sous-corps	degré	Gal(L=)	Gal(=Q) (si galoisienne)
K	6	f idg	S_3
K_1	3	h $_1$i	non galois.
K_2	3	h $_2$i	non galois.
K_3	3	h $_3$i	non galois.
K^0	2	A_3	Z=2Z
Q	1	S_3	f 1g

Table 1. Correspondance de Galois pour le corps de décomposition K de X^3 2 sur Q. Les $_i$ sont les transpositions dans S_3, mes K_i des plongements du corps de rupture.

II.1. Groupes nilpotents et résolubles.
II.2. Les p -groupes. Sous-groupe de Frattini. Théorème de la base de Burnside.
II.3. Suites scindées, produit semidirect.
II.4. Groupes topologiques.

III. Application : théorie de Galois.
III.1. Extensions galoisiennes.

Proposition 103.13 Soit L une extension de degré n in d'un corps K ni ou de caractéristique nulle. On note G le groupe des K -automorphismes de L. S'équivalent :
(i) K est le corps des invariants de G.
(ii) Pour tout x dans L, le polynôme minimal de x sur K est scindé sur L
(iii) L est engendré par les racines d'un polynôme sur K
Dans ce cas, on dit que l'extension L=K est galoisienne, et que G est son groupe de Galois, noté Gal(L=K). Par ailleurs G est d'ordre n.

Exemple 103.14 $Q[X]= X^2+1$ est une extension galoisienne de Q, mais ce n'est pas le cas de $Q[X]= X^3$ 2 .

III.2. Correspondance de Galois.

Théorème 103.15 Soit k est un corps de caractéristique nulle ou ni. L est une extension galoisienne de k de groupe de Galois G. Soit E l'ensemble des extensions intermédiaires de L=k et G l'ensemble des sous-groupes de G. Pour tout K 2 E, l'extension L=K est galoisienne et les applications

$$\begin{array}{ccc} E & & G \\ K & \mapsto & \mathrm{Gal}(L/K) \\ L^H & & H \end{array}$$

sont bijectives, décroissantes pour l'inclusion et réciproque l'une de l'autre ; de plus pour que K=k soit galoisienne, il faut et il su t que Gal(L=K) E G, auquel cas

$$\mathrm{Gal}(K/k) \simeq G/\mathrm{Gal}(L/K) \tag{72}$$

Remarque 103.16 Quand on parle d'extension du corps K, il s'agit de désigner un corps L plus gros le contenant ; mais quand on parle d'extension de groupe de H il s'agit plus souvent d'un groupe G dont H est un quotient. Ceci est conforme à la correspondance de Galois : si L est une extension galoisienne de K, les groupes Gal(L=k) pour K=k galoisienne sont des extension des groupes Gal(K=k).

III.3. Corps nis. Toute extension de degré n in sur F_q est unique à isomorphisme près, et isomorphe au corps de décomposition du polynôme X^{q^n} X sur F_q ; $\mathrm{Gal}(F_{q^n}/F_q)$ est d'ordre n. L'automorphisme de Frobenius

$$\begin{array}{rccc} \mathrm{Frob}_q : & F_{q^n} & \to & F_{q^n} \\ & x & \mapsto & x^q \end{array}$$

est un F_q-automorphisme de F_{q^n} dont le corps fixe est exactement F_q ; il est d'ordre exactement n, donc engendre tout le groupe de Galois de F_{q^n}/F_q. On a donc un isomorphisme

$$\begin{aligned} \mathrm{Gal}(F_{q^n}/F_q) &\simeq \mathbb{Z}/n\mathbb{Z} \\ \mathrm{Frob}_q^m &\mapsto \overline{m} \end{aligned}$$

et les extensions de corps finis sont cycliques. L'élément Frob_q^m fixe le sous-corps $F_{q^{\mathrm{pgcd}(n;m)}}$; la correspondance de Galois et la description des sous-groupes des groupes cycliques permet de décrire le treillis des sous-corps de F_{q^n} contenant F_q en parallèle du treillis des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

corps K	degré	$\mathrm{Gal}(F_{q^n}/K)$	$\mathrm{Gal}(K/F_q)$
F_{q^n}	n	$\{0\}$	$\mathbb{Z}/n\mathbb{Z}$
F_{q^m} $(m \mid n)$	m	$\mathbb{Z}/(n/m)\mathbb{Z}$	$\mathbb{Z}/m\mathbb{Z}$
F_q	1	$\mathbb{Z}/n\mathbb{Z}$	$\{0\}$

Table 2. Correspondance de Galois pour les extensions finies de corps finis

104. Groupes finis. Exemples et applications.

Références. [Per96, FG94, Isa08]
Voir l'annexe B pour le contenu de cette leçon.

Commentaires. Cette leçon aborde le problème de la classification, au moins pour en faire ressortir la difficulté. Ceci motive la recherche de classes plus restreintes (cycliques, abéliens, nilpotents, résolubles, parfaits, simples).

I. Exemples fondamentaux.

(1) Groupes cycliques. Treillis des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$. Critère de cyclicité. Le sous-groupes finis de $k^\times$. Stabilité par passage au sous-groupe, quotient. Lemme chinois.

Voir l'annexe B.

(2) Groupes abéliens. Théorème de structure.

(3) Groupes symétriques. Théorème de Cayley. Groupes linéaires.

II. Fragments de théorie.

(1) Application de la théorie des actions de groupes ; théorie combinatoire des groupes finis. Théorèmes de Sylow.

(2) Les p-groupes. Les p-groupes sont nilpotents.

(3) Extensions. Produit semidirect. Isomorphismes entre produits semi-directs. Groupes dihédraux. Groupes d'ordre pq.

(4) Transfert. Applications : entiers n tels que tout groupe d'ordre n est cyclique (resp. abélien). Groupes d'ordre 2015.

III. Applications.

(1) Géométrie : sous-groupes finis de $SO(3)$ et polyèdres réguliers.

(2) Algèbre : Extensions galoisiennes finies, correspondance de Galois. Application : polygones constructibles. Extensions de corps finis [On reprend le treillis du début].

105. Groupe symétrique. Applications

[Per96]

I. Le groupe symétrique.

(1) Dé nition, ordre [par l'équation aux classes]. Intérêt théorique : théorème de Cayley.

(2) Représenter les permutations : tableaux, décomposition en cycles. Application au calcul de l'inverse.

(3) Applications de la décomposition en cycle : Ordre des éléments. Principe de conjuguaison.

II. Signature, groupe alterné.

(1) Signature : dé nitions équivalentes. Groupe alterné. Le groupe alterné est le sous-groupe dérivé.

(2) Application : théorie des déterminants. Orientation d'un e.v. réel.

III. Propriétés algébriques.

(1) Parties génératrices de S_n et de A_n. Présentation de S_n. Activité : Alice et Bob jouent dans le groupe symétrique.

(2) La simplicité de A_n, $n > 5$. Corollaire, S_n pas résoluble pour $n > 5$.

(3) Les automorphismes de S_n. Le cas de S_6 : $PGL(2; F_5)$ s'identi e à un sous-groupe transitif.

IV. Représentations.

(1) Polynômes symétriques. Théorème des polynômes symétriques. Une application.

(2) Représentations de permutation. DEV : théorème de Brauer

106. Groupe linéaire, sous-groupe de $GL(E)$

I. Le groupe linéaire. Quelques sous-groupes et quotient.

(1) Dé nitions : Endomorphismes / Matrices. Principe de conjuguaison.

(2) Parties génératrices (on exclut certains cas nis). Centre.

(3) Déterminant et sous-groupes, quotientPGL ;PSL .

(4) Dénombrements (cas des corps nis). Etude et dévissage de$GL(2; F_3)$

II. Opérations sur $M_n(k)$.

(1) Action à gauche.

(2) Conjuguaison. Théorème de plongement. DEV : matrices de permutations et théorème de Brauer

(3) Réduction des endomorphismes. Isomorphismes entre groupes linéaires.

(4) Congruence.

III. Aspects topologiques .

(1) Densité. Principe de densité algébrique. Application : $_{AB} = _{BA}$

(2) Théorème de Lie-Kolchin.

Commentaires. Attention

Le groupe des automorphismes de$GL(E)$ est compliqué en général (à la di érence des automorphismes de$L(E)$). En particulier, il ne sont pas tous intérieurs (sauf quelques cas nis ; penser à $M \mapsto ({}^tM)^{-1}$ où M est la matrice dans une base).

107. Représentations et caractères complexes d'un groupe ni

Références : [Elk02], [Col11].

I. Notion de représentation.

(1) Dé nition. Exemple ; représentations tautologique. Représentation régulière.

(2) G morphismes. Somme directe.

(3) Semi-simplicité (représentations complexes). Théorème de Maschke. Contre-exemple en caractéristiquep non première à l'ordre du groupe.

(4) Représentations de permutation. Illustration : théorème de Brauer.

II. Représentations irréductibles et théorie des caractères.

(1) Lemme de Schur

(2) Caractères. Orthogonalité des caractères.

(3) Tables de caractères. DEV : caractères de $\mathfrak{A}_5$. Applications à la simplicité.

(4) (Eventuellement) propriétés d'intégralité des caractères.

III. Le cas abélien.

(1) Groupe dual. Application : représentations des groupes d'ordre 8. DEV : Théorème de structure.

(2) Transformée de Fourier. Exemple : sommes de Gauss.

Commentaire. Le théorème de Maschke (semi-simplicité) et le lemme de Schur (représentation irréductibles) sont di cilement contournables. Il faut aborder la pratique de comment dresser une table de caractères.

110. F Caractères et transformée de Fourier discrète

I. Caractères et groupe dual.

I.1. Dé nitions, exemples. G est un groupe etk un corps.

Définition 110.1 Un caractère deG sur k est un morphisme de groupesG ! k . L'ensemble des caractères forme un groupe appelé groupe dual deG (sur k), noté Ĝ.

Exemple 110.2 La signature : S_n ! f 1g, le caractère de Legendre $(\overline{x}) = \frac{x}{p}$ pour x 2 $(Z=pZ)^?$.

Proposition 110.3 (Indépendance linéaire des caractères)Les caractères $_1; : : : _n$ sont distincts ssi ils sont linéairement indépendants surk.

Corollaire 110.4 Si G est ni alors Ĝ aussi et Ĝ 6 jGj.

Corollaire 110.5 Soit K=k une extension nie de degrén, L=k une extension. Les plongementsK ! L sont linéairement indépendants.

I.2. Caractères des groupes abéliens nis.On prendra ici k algébriquement clos, G abélien et ni.

Remarque 110.6 Les groupes abéliens d'exposantN sont desZ=NZ-modules. On a alors un isomorphisme

$$\hat{G} ' \mathrm{Hom}_{Z=NZ}(G; Z=NZ) = G-:$$

En particulier, si G est d'exposantp premier, le dualĜ s'identi e en tant qu'espace vectoriel au dual F_p-linéaire $G^?$.

Proposition 110.7 Soit G un groupe cyclique d'ordreN : G = $\langle 1; ; : : : ^{N-1} \rangle$. Soit ! une racine primitive N-ième de l'unité dansk. Alors les caractères deG sur k sont les

$$` \mapsto ^k = ! ^{k`}:$$

En particulier, Ĝ ' Z=NZ (mais cet isomorphisme n'est pas naturel).

Lemme 110.8 Si G est abélien ni, il est produit direct de groupes cycliques.

Lemme 110.9 Si G et H sont abéliens alorsĜ H ' Ĝ Ĥ.

Théorème 110.10 Les groupesG, G- et G— sont isomorphes. De plus,G et G— sont naturellement isomorphes via

$$\begin{aligned} G &\to G— \\ g &\mapsto (\mapsto (g)) \end{aligned}$$

Remarque 110.11 G est abélien ssijGj = Ĝ .

I.3. Orthogonalité des caractères complexes.[Elk02].

Lemme 110.12 Si k = C alors 8(; g) 2 Ĝ G, $\overline{(g)} = (g)^{-1}$

Proposition 110.13 (G abélien) Les éléments deĜ forment une base orthonormée de l'espace des fonctionsG ! C pour le produit hermitien

$$\langle '; \rangle = \frac{1}{jGj} \sum_{g2G} ' (x) \overline{(x)}$$

Cet espace est appelé$L^2(G)$. Par bidualité les éléments deG vus dansG— forment une base orthonormale de$L^2(G—)$

I.4. Caractères et représentations.

Lemme 110.14 (Schur) Si k est algébriquement clos et $s(i ; V)$ est une représentation irréductible de G, alors $\mathrm{End}_G(V) ' k$.

Proposition 110.15 Les caractères de G s'identifient exactement aux représentations complexes irréductibles de l'abélianisé $G=[G;G]$.

Remarque 110.16 En pratique, la première chose à déterminer pour dresser une table de caractères est le groupe $\hat{G^{ab}}$.

Exemple 110.17. Si $G = S_n$, $\hat{G} ' Z=2Z$. Si $G = H_8$ ou D_4, $\hat{G} ' K_4 = (Z=2Z)^2$.

II. Analyse harmonique sur un groupe abélien ni. G est un groupe abélien ni

II.1. La transformation de Fourier.

Définition 110.18 L'espace $L^2[G]$ est muni de deux structures d'algèbre :

$$' (g) = ' (g) (g)$$
$$'? (g) = \sum_{h2G} ' (h) h^{1}g$$

Définition 110.19 Soit $f 2 L^2(G)$. On appelle transformée de Fourier de f, notée $\hat{f}$, l'élément de $L^2 \hat{G}$ dé nie par

$$\hat{f}( ) = p\frac{1}{jGj} \sum_{g2G} f (g) \overline{(g)} = p\overline{jGj} hf; i_{L^2(\hat{G})}$$

Théorème 110.20 La transformation de Fourier $F : L^2(G) ! L^2 \hat{G}$ admet les propriétés suivantes :

(i) F est un isomorphisme isométrique.

(ii) Pour tout $f 2 L^2(G)$,

$$f = p\frac{1}{jGj} \sum_{2\hat{G}} \hat{f}( )$$

(iii) Pour tous $f; g 2 L^2(G)$ nous avons $\widehat{f ? g} = \hat{f} \hat{g}$

Remarque 110.21 L'application $F ( ) : f 7! \hat{f}( )$ est l'unique extension de en un morphisme d'algèbres $(C[G] ; ?) ! C$.

II.2. Formule de Poisson.

Définition 110.22 Soit $H G$ un sous-groupe de G. On note $H^]$ et on appelle orthogonal de H le sous-groupe

$$H^] = \{ 2 \hat{G}; 8h 2 H; (h) = 1 \}$$

Remarque 110.23 On a un isomorphisme $H^] ' \hat{G=H}$ donné par la factorisation des $2 H^]$ à travers $: G ! G=H$.

Théorème 110.24 Avec les notations précédentes, on a pour tout $f 2 L^2[G]$

$$8g 2 G; \sum_{h2H} f (gh) = \frac{jHj}{jGj} \sum_{2H^]} \hat{f}(^{-}) (g)$$

Remarque 110.25 Soit $f 2 C^1_{pm} \setminus C(R=Z)$, $(c_k)_{k2Z}$ ses coe cients de Fourier ; alors [QZ02]

$$\frac{1}{n} \sum_{k=0}^{n1} f (k=n) = \sum_{m2Z} c_{mn} (f) \quad (73)$$

Entrée: P, Q dans $\mathbb{C}[X]$ (en représentation creuse) de degré $d_p, d_q \leq N = 2^p$

Sortie: Le polynôme $PQ \in \mathbb{C}[X]$

(1) Evaluer P et Q en les ω^i, $0 \leq i \leq 2N-1$ (Coût : $\Theta(N \log N)$ opérations arithmétiques dans $\mathbb{C}$)

(2) Calculer $P(\omega^i) Q(\omega^i)$ (Coût $\Theta(N)$)

(3) Interpoler par transformée de Fourier inverse (Coût : $\Theta(N \log N)$).

Cet algorithme est également efficace pour multiplier de grands entiers : un entier écrit en base b est l'évaluation en b du polynôme P qui a pour coefficients ses chiffres.

Algorithme 1 : Principe de la transformée de Fourier rapide pour la multiplication de P et Q (Cooley, Tukey).

II.3. Transformée de Fourier rapide. On dispose d'un échantillon de valeurs $f[n]_{n=0}^{n=N-1}$ d'un signal temporel $f(t)$ aux temps n. On l'identifie à un élément de $\mathbb{C}^N$, puis de

$$(\mathbb{C}[Z/NZ], +) \simeq \mathbb{C}[X]/(X^N - 1) :$$

Sa transformée de Fourier discrète relative à $\omega \in \mu_N(\mathbb{C})$ est $\hat{f} = \mathcal{F}(f)$ correspondant.

Proposition 110.26 Le polynôme trigonométrique

$$f(x) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \hat{f}[k] \omega^{kx}$$

est interpolateur de f aux temps $n = 0, \dots, N-1$.

Théorème 110.27 (FFT - transformée de Fourier rapide, [Dem08]) Supposons $N = 2^p$. On pose $f^0[n] = f[2n]$ et $f^1[2n+1]$ pour $n \in \{0, \dots, N/2 - 1\}$. On note $\hat{f}^0$ et $\hat{f}^1$ les transformées de Fourier discrètes de f^0 et f^1 dans $\mathbb{C}^{N/2}$. Alors (en posant $n' = n - N/2$)

$$\hat{f}[n] = \hat{f}^0[n] + \omega^n \hat{f}^1[n] \qquad 0 \leq n < N/2$$
$$\hat{f}[n] = \hat{f}^0[n'] - \omega^n \hat{f}^1[n'] \qquad N/2 \leq n < N$$

Proposition 110.28 Le coût C_N du calcul (en opérations arithmétiques dans $\mathbb{C}$) de $\hat{f}$ est donné par $2C_{N/2} + bN$, où b est une constante. En particulier

$$C_N = \Theta(N \log N) :$$

Exemple 110.29 Soient P et $Q \in \mathbb{C}[X]$ de degré $N = 2^p - 1$ à multiplier. L'algorithme FFT permet de rapporter la complexité à $N \log N$ (voir algorithme)

III. Caractères dans les corps finis. k est un corps algébriquement clos. On distingue les caractères additifs sur $\mathbb{F}_q$ (i.e. les éléments de $\hat{\mathbb{F}}_q$) et les caractères multiplicatifs.

Définition 110.30 Soit $\mathbb{F}_q$ un corps fini de caractéristique p. Soit ω une racine primitive p-ième de l'unité dans k. Alors tout caractère additif $\chi \in \hat{\mathbb{F}}_q$ est de la forme

$$\chi_a(x) = \omega^{\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax)}$$

pour $a \in \mathbb{F}_q$. En particulier $a \mapsto \chi_a$ est un homomorphisme de $\mathbb{F}_q$ sur $\hat{\mathbb{F}}_q$.

Définition 110.31 Soient $\chi \in \hat{\mathbb{F}}_q$ et $\psi \in \hat{\mathbb{F}}_q$. On définit leur somme de Gauss par

$$G(\chi, \psi) = \sum_{x \in \mathbb{F}_q} \chi(x) \psi(x) :$$

Théorème 110.32 (Loi de réciprocité quadratique) Soient ℓ et p deux nombres premiers impairs distincts. Alors

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

	$\{1\}$	$\{-1\}$	$\{i\}$	$\{j\}$	$\{k\}$
1	1	1	1	1	1
χ_{10}	1	1	1	1	1
χ_{01}	1	1	1	1	1
χ_{11}	1	1	1	1	1
χ	2	2	0	0	0

Table 3. Table de caractères de H_8. Les 4 premières lignes correspondent aux caractères du groupe abélien K_4.

Remarque 110.33 Si $k = \mathbb{C}$ alors $G(\ ,\ ) = F_{mul}(\ )(\ )$ et $G(\ ,\ ) = F_{add}(\ )(\ )$ à condition d'inclure $L^2(F_q)$ dans $L^2(F_q)$ pour la seconde égalité.

Proposition 110.34 Si $k = \mathbb{C}$, $! = e^{2i/p}$ et $\ $ est le caractère de Legendre sur F_p, p premier impair on a

$$G(\ ,\ _1) = \begin{cases} p & \text{si } p \equiv 1 (4) \\ ip & \text{si } p \equiv 3 (4). \end{cases}$$

Compléments.

Remarque 110.35 Les groupes H_8 et D_8 ont même table de caractères, bien qu'étant non isomorphes. Cela est lié au fait que ces deux extensions centrales de K_4 sont isoclines, c'est-à-dire que les applications $G/Z(G) \times G/Z(G) \to [G,G]$ induites par le commutateurs sont les mêmes pour ces deux groupes.

IV. Autres directions et développements envisageables.
Codes cycliques et décryptage des codes BCH [Dem08]
Calcul exact des sommes de Gauss complexes [QZ02]
Transformée de Fourier dans un anneau (presque) quelconque [Dem08]
Constructibilité des N-gones pour N nombre de Fermat
Théorème de la base normale.

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

Références. [Per96, Dem08]

I. Commentaires. L'anneau véritable ici, c'est $\mathbb{Z}$. L'étude de ses quotients est utile pour comprendre son arithmétique.

II. I Anneau $\mathbb{Z}/n\mathbb{Z}$.

(1) Le groupe $\mathbb{Z}/n\mathbb{Z}$. Lemme chinois (version groupes).

(2) Automorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$. Indicatrice d'Euler.

121. F Nombres premiers. Applications

I. Nombres premiers.

I.1. Théorème fondamental de l'Arithmétique.

Définition 121.1 Soit $2 \mathbb{Z}$, $\neq 1$. On dit que $$ est irréductible ssi pour tous $n; m \in \mathbb{Z}$, $= nm$ implique $n = 1$ ou $m = 1$.

Remarque 121.2 $$ est irréductible ssi l'anneau $\mathbb{Z}/( )$ est un corps noté $\mathbb{F}$.

Théorème 121.3 (Théorème fondamental de l'arithmétique) L'anneau $\mathbb{Z}$ est factoriel ; c'est-à-dire que pour tout $n \in \mathbb{Z}$ on peut écrire

$$n = {}_1{}^{1} \quad {}_r{}^{r}$$

où les $_i$ sont irréductibles et distincts ; de plus cette décomposition est unique à l'ordre près des $_i$.

Corollaire 121.4 Soit $p \in \mathbb{Z}$. Les propositions suivantes sont équivalentes

(i) p est irréductible

(ii) Pour tous $n; m \in \mathbb{Z}$ nous avons $p \mid nm \Rightarrow p \mid n$ ou $p \mid m$.

En d'autres termes $\mathbb{Z}/(p)$ est un corps $\Leftrightarrow$ $\mathbb{Z}/(p)$ est intègre. On dit alors que p est premier.

Remarque 121.5 Dans un anneau intègre, (i) implique (ii) est un fait général. (ii) implique (i) est lié au fait que $\mathbb{Z}$ est factoriel.

Dans la suite on supposera $p \in \mathbb{N}$ premier (sans perte de généralité puique p et $-p$ sont associés).

Remarque 121.6 (et algorithme) soit $n > 2$ et d le plus petit diviseur de n di érent de 1. Alors, d est premier. On en déduit l'algorithme du crible d'Erathosthène.

Proposition 121.7 2 et 3 sont premiers ; le nombre $\frac{\ln 2}{\ln 3}$ est irrationnel.

I.2. Valuation p-adique. pgcd, ppcm.

Définition 121.8 La valuation p-adique de $n \in \mathbb{N}^{?}$ est le plus grand entier $$ tel que $p^{} \mid n$. Elle est notée $_p(n)$.

Proposition 121.9 Le pgcd et le ppcm de n et m s'expriment à partir des valuations par

$$\text{pgcd}(n; m) = \prod_{p \in \mathbb{P}} p^{\min(\,{}_p(n);\,{}_p(m))}$$

$$\text{ppcm}(n; m) = \prod_{p \in \mathbb{P}} p^{\max(\,{}_p(n);\,{}_p(m))}$$

Remarque 121.10 Ces écritures n'ont pas d'intérêt e ectif. Décomposer m et n en facteurs premiers est beaucoup plus coûteux que calculer leur pgcd (ou de manière équivalente leur ppcm) avec l'algorithme d'Euclide.

Remarque 121.11 La valuation p-adique se prolonge naturellement au corps des fractions $\mathbb{Q}$.

I.3. Le corps $\mathbb{F}_p$. Caractéristique.

Définition 121.12 Soit A un anneau intègre unitaire ; il existe un unique morphisme $\mathbb{Z} \to A$. Son noyau est de la forme (p) où $p = 0$ ou un nombre premier appelé caractéristique de A.

Remarque 121.13 Si A est un anneau de caractéristique $p > 0$, c'est une $\mathbb{F}_p$-algèbre. Si A est ni, la dimension de A est nie. En particulier, tout corps ni est de cardinal $q = p$ avec $p \in \mathbb{P}$.

Proposition 121.14 (Fermat). Pour tout $n \in \mathbb{N}$ nous avons

$$n^p \equiv n \ [p].$$

Corollaire 121.15 Soit A un anneau de caractéristique $p \neq 0$. L'application $F : x \mapsto x^p$ est un endomorphisme $\mathbb{F}_p$-linéaire de A. Si A est un corps, F est injectif.

Proposition 121.16 Le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p-1$.

I.4. Fonctions arithmétiques.

Définition 121.17. $f : \mathbb{N}^* \to \mathbb{N}$ est dite arithmétique si $f(nm) = f(n)f(m)$ dès que $n \wedge m = 1$.

Proposition 121.18 Une fonction arithmétique est entièrement déterminée par son image en les nombres premiers.

Exemple 121.19 Les fonctions suivantes sont arithmétiques :
- $\sigma_k(n) = \sum_{d|n} d^k$. En particulier σ_0 (nombre de diviseurs) et σ_1 (somme des diviseurs)
- $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$, via le théorème des restes chinois.
- $\mu(n)$ définie par $\mu(p) = -1$ et $\mu(p^2) = 0$ si p est premier.
- $r_2(n)$ nombre de décomposition en sommes de deux carrés.

Proposition 121.20 Le nombre (resp. la somme) des diviseurs de n est donné par le produit (infini)

$$\sigma_0(n) = \prod_{p \in \mathbb{P}} (1 + \nu_p(n)) \tag{74}$$

$$\sigma_1(n) = \prod_{p \in \mathbb{P}} \frac{p^{1+\nu_p(n)} - 1}{p - 1}. \tag{75}$$

Proposition 121.21 La fonction indicatrice d'Euler admet l'expression suivante :

$$\varphi(n) = n \prod_{p \in \mathbb{P},\ p|n} \left(1 - \frac{1}{p}\right). \tag{76}$$

II. Répartition des nombres premiers.

II.1. Le théorème d'Euclide.

Théorème 121.22 L'ensemble $\mathbb{P}$ est infini.

Corollaire 121.23 Il existe une suite (u_n) d'entiers dont toutes les sous-suites (u_{k_n}) sont stationnaires, mais qui n'est pas stationnaire.

Corollaire 121.24 La fonction indicatrice d'Euler tend vers $+\infty$.

III. Identité d'Euler, théorème de Legendre.

Définition 121.25 La fonction ζ de Riemann est définie dans le demi-plan $\Omega = \{\mathrm{Re}\, z > 1\}$ par l'expression

$$\zeta(s) = \sum_{n \geq 1} n^{-s}. \tag{77}$$

Elle définit une fonction holomorphe de la variable complexes, sans pôle sur ce demi-plan.

Théorème 121.26 (Euler). La fonction $1/\zeta$ admet sur Ω le développement

$$\frac{1}{\zeta(s)} = \prod_{p \in \mathbb{P}} (1 - p^{-s}) = \sum_{n \geq 1} \mu(n) n^{-s} \tag{78}$$

Corollaire 121.27. La série $\sum_{p \in \mathbb{P}} 1/p$ est divergente, et

$$\liminf_{n \to +\infty} \frac{\varphi(n)}{n} = 0. \tag{79}$$

Théorème 121.28 (Théorème de raréfaction de Legendre)Notons $\pi(n)$ le nombre de nombres premiers$\leq n$. Alors

$$\lim_{n\to+\infty} \frac{\pi(n)}{n} = 0 : \tag{80}$$

Démonstration. Soit $\varepsilon > 0$. D'après le corollaire précédent, il existe$N$ tel que $\varphi(N)/N \leq \varepsilon$. Puisque les nombres premiers plus grands que$N$ sont premiers àN, ils ont seulement$\varphi(N)$ résidus possibles modulo$N$. On en déduit que$\limsup \pi(n)/n \leq 2\varepsilon$.

Remarque 121.29 Un résultat plus fin (mais nettement plus difficile) est le théorème des nombres premiers (conjecturé par Gauss et démontré par Hadamard et De la Vallée Poussin en 1896) : $\pi(n) \sim n/\ln(n)$.

IV. Progressions arithmétiques.

Définition 121.30 Soit U_n le groupe des racines de l'unité dans$\mathbb{C}$. $\zeta \in U_n$ est dite primitive si elle engendreU_n. On définit le n-ième polynôme cyclotomique par

$$\Phi_n = \prod_{\text{primitive}} (X - \zeta) :$$

Proposition 121.31 Pour tout $n \in \mathbb{N}$ nous avons que
(i) $\Phi_n \in \mathbb{Z}[X]$
(ii) Si p premier divise $\Phi_n(a)$ mais pas $\Phi_n(d)$ pour tout $d \mid n$, $d < n$, alors $p \equiv 1 [n]$

Théorème 121.32 (Version faible du théorème de la progression arithmétique). Soit n un entier naturel. Alors il existe une infinité de nombres premiers de la forme $kn + 1$, où k est entier.

Remarque 121.33 On ne sait pas actuellement s'il existe une infinité de nombres premiers de la forme$n^2 + 1$

V. Critères de primalité. Ici n est un entier naturel ; on cherche à décider sa primalité.

V.1. Critères « parfaits ».

Proposition 121.34 n est premier ssi n n'admet aucun diviseur $d \leq \sqrt{n}$.

Théorème 121.35 (Wilson) . n est premier ssi $(n-1)! \equiv -1 [n]$.

Les deux critères précédents permettent donnent un résultat certain, mais ils ne sont pas praticables pour$n$ grand.

V.2. Test de Fermat.

Proposition 121.36 S'il existe a, $1 \leq a \leq n-1$ tel quea^{n-1} n'est pas congru à1 modulo n, alors n n'est pas premier (et a est appelé témoin de Fermat).

Remarque 121.37 La réciproque est fausse, le test n'est pas parfait ; le plus petit contre-exemple est le nombre de Carmichael561. Mais un témoin de Fermat suffit. Le calcul dea^{n-1} est peu coûteux (exponentiation rapide).

Définition 121.38 n est dit pseudo-premier en base$b$ si b et n sont premiers entre eux et si $b^{n-1} \equiv 1 [n]$.

Exemple 121.39 $1729 = 12^3 + 1$ est pseudo-premier en bases$2, 3, 5$. Il n'est pas premier (divisible par $12 + 1$).

V.3. Test de Miller-Rabin.

Théorème 121.40 Soit $n > 1$ un entier impair. Ecrivons $n - 1 = 2^s t$ avec t impair. S'il existe a tel que $1 < a < n$, $a^t \not\equiv 1 [n]$ et $a^{2^i t} \not\equiv -1 [n]$ pour $i = 0, 1, \ldots, s$ alors n n'est pas premier (et a est appelé témoin de Miller).

Exemple 121.41 2 est témoin de Miller pour 561

Le test de Miller-Rabin est probabiliste, toutefois on peut montrer (Rabin) que si $n > 9$ n'est pas premier, alors il admet au moins $n - 2 - E(\varphi(n)/4)$ témoins de Miller. Donc si n passe k fois le test de Miller avec succès pour des a aléatoires, il est probablement premier avec (pseudo) probabilité d'erreur 4^{-k}.

122. Anneaux principaux

I. Dé nitions, premières propriétés.

(1) Idéaux, idéaux principaux. Ordre sur les idéaux principaux dans un anneau intègre. Exemple : les fonctions qui s'annulent en 0 dans $C^1(R)$ (lemme de Hadamard).

(2) Anneaux factoriels. Anneaux noetheriens. Anneaux principaux. Equivalence p irréductible $\Leftrightarrow$ $A/(p)$ est un corps. Les anneaux euclidiens sont principaux. Exemples : Z et $Z[i]$

II. Exemples, contre-exemples.

(1) L'anneau $A[X]$ est principal (et euclidien) ssi A est un corps.

(2) $Z[X]$ factoriel non principal ; un anneau euclidien non principal [Per96].

123. Corps nis

Référence. [Dem08, Per96]

Commentaire. L'existence des F_q pour q non premier peut attendre un peu, parce que ses propriétés essentielles ne la nécessitent pas et aident à comprendre sa construction ainsi que son unicité. Dans les applications, on veille à faire intervenir F_q et pas seulement F_p.

Le théorème de Wedderburn est important en soi mais ce n'est pas le coeur du sujet.

I. I Existence et unicité des F_q.

(1) Caractéristique, sous-corps premier. Les corps F_p. K est un F_p-ev. Exemple : $F_4 ' Z[j]=(2)$.

(2) Le groupe F_q est cyclique d'ordre q 1. Morphisme de Frobenius.

(3) Existence et unicité : corps de décomposition de $X^q X$ sur F_p.

II. II Corps nis et polynômes.

(1) Théorème de l'élément primitif. Polynômes irréductibles sur F_q et corps de rupture. Théorème de Gauss F_q est un corps parfait. Correspondance de Galois pour les corps nis.

(2) Application 1 des polynômes sur corps nis : algorithme de Berlekamp (DEV). Réduction modulo p.

(3) Application 2 des polynômes sur corps nis : partage de secret de Shamir.

(4) Polynômes à plusieurs indéterminées. Théorème de Chevalley-Warning (DEV). Application : Erdös-Ginzburg-Ziv.

III. III Carrés dans les corps nis.

(1) Loi de réciprocité quadratique par les sommes de Gauss. Algorithme de Cippola.

(2) Théorème de Frobenius-Zolotarev.

IV. IV Corps nis et géométrie.

(1) Quelques isomorphismes exceptionnels.

124. F Séries formelles

Référence : [Bou07, Chapitre 4, Ÿ4].

I. L'algèbre $A[[X]]$ et ses opérations. A est un anneau unitaire commutatif intègre.

I.1. Dé nition. $A[X]$ est la A-algèbre des suites presque nulles d'éléments de A munie du produit de convolution. On écrira $P = \sum p_n X^n$ et $Q = \sum q_n X^n$ des éléments génériques de $A[X]$.

Définition 124.1. On appelle ordre de $P \in A[X]$ l'entier

$$!(P) = \max \{ n \in \mathbb{N} ; X^n \mid P \}$$

Si $P = 0$, on pose $!(P) = +\infty$.

Proposition 124.2. $!$ est une valuation sur $A[X]$, autrement dit pour tous $P, Q \in A[X]$

(i) $!(P) = +\infty \Rightarrow P = 0$,
(ii) $!(P+Q) \geq \min(!(P), !(Q))$
(iii) $!(PQ) = !(P) + !(Q)$

Définition 124.3. $(P_n) \in A[X]^{\mathbb{N}}$ est une suite de Cauchy si pour tout $k \in \mathbb{N}$ on a $!(P_n - P_m) > k$ pour n, m assez grands.

Définition 124.4. $A[[X]]$ est l'ensemble des suites de Cauchy pour $!$, quotienté par la relation $(P_n) \sim (Q_n) \Leftrightarrow !(P_n - Q_n) \to +\infty$. Les propriétés (i) à (iii) permettent d'assurer à $A[[X]]$ une structure de A-algèbre.

Remarque 124.5. La suite $(P_n) \in A[X]^{\mathbb{N}}$ converge dans $A[[X]]$ dès que $!(P_{n+1} - P_n) \to +\infty$. En particulier tout élément de $A[[X]]$ peut s'écrire de manière unique sous la forme $\sum_{n \geq 0} a_n X^n$, où $a_n \in A$ pour tout $n \geq 0$.

On écrira $S = \sum s_n X^n$, $T = \sum t_n X^n$, ... des éléments génériques de $A[[X]]$

Remarque 124.6. $ST = \sum_{(p,q) \in \mathbb{N}^2} s_p t_q X^{p+q}$. La somme a un sens puisque le nombre de monôme de valuation $\leq k$ est fini pour tout k.

I.2. Substitution d'une série formelle dans une autre.

Proposition 124.7. $A[[X]]$ est intègre.

Proposition 124.8. Soient $S, T \in A[[X]]$. Alors la série de terme général $(s_n T^n)$ converge dans $A[[X]]$ si et seulement si $S \in A[X]$ ou $t_0 = 0$. Sa somme est par dé nition

$$S(T) = S \circ T = \sum_{n \geq 0} s_n T^n$$

appelée substituée de T dans S.

Proposition 124.9. Soit T telle que $t_0 = 0$. Alors $S \mapsto S \circ T$ est un A-homomorphisme de $A[[X]]$ laissant A stable.

Remarque 124.10. On peut toujours substituer 0 et $S(0) = s_0$.

Proposition 124.11. Si T et U sont substituables, $(S \circ T) \circ U = S \circ (T \circ U)$

II. Propriétés algébriques de $K[[X]]$. A partir de maintenant, K est un corps.

II.1. Inversibilité, propriétés arithmétiques.

Remarque 124.12 (fondamental). $(1 - X)^{-1} = \sum_{n \geq 0} X^n$

Théorème 124.13. $A[[X]]^\times = \{ S \in K[[X]] ; s_0 \in A^\times \}$ DEV 1 (th 124.13 ! cor 124.15)

Corollaire 124.14. L'inclusion naturelle $K[X] \hookrightarrow K[[X]]$ se prolonge en une inclusion de $K(X)_0$ (anneau des fractions rationnelles sans pôle en 0) dans $K[[X]]$

Corollaire 124.15 Les idéaux de $K[[X]]$ sont principaux et de la forme (X^n).
L'arithmétique de $K[[X]]$ est complètement décrite par $v : S \mapsto T \mapsto v(S) \mapsto v(T)$.
En particulier, $K[[X]]$ n'a qu'un seul idéal maximal $m = (X)$, et les irréductibles de $K[[X]]$ sont X et ses associés.
$K[[X]]$ est un anneau euclidien pour le stathme v.

Remarque 124.16 $K[[X]]/m \simeq K$. Ceci assure $K[[X]] \simeq K^0[[X]] \Rightarrow K \simeq K^0$

Exemple 124.17 La famille $(U_n)_{n\in\mathbb{N}}$ des polynômes de Tchebychev de deuxième espèce est dé nie par

$$\sum_{n>0} U_n(X)Z^n = \frac{1}{1 - 2XZ + Z^2}$$

U_n est bien dé nie et dans $\mathbb{Z}[X]$ car le polynôme $1 - 2XZ + Z^2 \in \mathbb{Z}[X][[Z]]$ est de terme constant inversible.

II.2. Série dérivée. On supposera dorénavant car$K = 0$.

Définition 124.18 Soit D l'endomorphisme du K-ev $K[[X]]$ dé ni par $D(1) = 0$ et $D(X^n) = nX^{n-1}$. DS est appelée série dérivée de S, notée aussi S'. D est une dérivation de $K[[X]]$ de noyau K et $D^n S(0) = n!s_n$

Proposition 124.19 Il existe une unique $E \in \operatorname{Ker}(D - I)$ telle que $e_0 = 1$. Elle est appelée série exponentielle, notée

$$\exp = \sum_{n>0} \frac{X^n}{n!}$$

Proposition 124.20 Soient $\lambda, \mu \in K$. Alors si S et T sont substituables, $\exp(S + T) = \exp(S)\exp(T)$.

En découlent, toutes les identités remarquables trigonométriques
II.3. Série réciproque. Rappelons que$X$ est neutre pour la loi

Théorème 124.21 (inversion locale pour les séries formelles) Soit $S \in K[[X]]$. Alors pour qu'il existe une série formelle T telle que $S \circ T = X$, il faut et il suf t que S soit associé à X, autrement dit $S(0) = 0$ et $S'(0) \neq 0$.
De plus, dans ce cas T est unique et $T \circ S = X$. T est appelée réciproque de S, notée S^{-1}.

Remarque 124.22 Ce théorème possède une preuve constructive.

Corollaire 124.23 Si $S \circ X$ alors $U \mapsto U \circ S$ est un automorphisme d'algèbre d'inverse $V \mapsto V \circ S^{-1}$

Exemple 124.24 La série formelle $\exp - 1 = \sum_{n>1} X^n/n!$ admet pour réciproque la série

$$\sum_{n>1} \frac{(-1)^{n+1}}{n} X^n$$

notée $\operatorname{Log}(1 + X)$.

Définition 124.25 Soit $\alpha \in K$; on pose $(1 + X)^\alpha = \exp(\alpha \operatorname{Log}(1 + X))$

Proposition 124.26 (formule du binôme généralisée) Le développement en série formelle de $(1 + X)^\alpha$ est

$$(1 + X)^\alpha = \sum_{n>0} \binom{\alpha}{n} X^n$$

où $\binom{\alpha}{n} = 1$ si $n = 0$ et $\frac{1}{n!}\alpha(\alpha - 1)\cdots(\alpha - n + 1)$ sinon.

II.4. Corps des fractions.

Proposition 124.27. Le corps des fractions de $K[[X]]$, noté $K((X))$, est isomorphe à l'algèbre des suites de $K^{\mathbb{Z}}$ à support minoré, muni du produit de convolution. La valuation v s'y prolonge.

Remarque 124.28 Pour tout $F \in K((X)) \setminus K[[X]]$ nous avons $F^{-1} \in K[[X]]$

Proposition 124.29 On a l'isomorphisme de groupes

$$\mathbb{Z} \times K[[X]]^\times \simeq K((X))^\times$$

Théorème 124.30 L'inclusion $K(X)_0 \hookrightarrow K[[X]]$ se prolonge en $K(X) \hookrightarrow K((X))$. Ses éléments sont caractérisés par

$$F \in K((X)) \iff \exists N \in \mathbb{N}, \exists n_0 \in \mathbb{N}, \exists \varphi \in K^{\mathbb{N}^*} \setminus \{0\}, \forall n > n_0, \varphi(f_{n+1}, \dots, f_{n+N}) = 0$$

III. Applications.

III.1. Spécialisation en les endomorphismes localement nilpotents.

Définition 124.31 Soit E un K-ev, $u \in \mathcal{L}(E)$ est localement nilpotent s'il existe n_x tel que $u^{n_x}(x) = 0$ pour tout $x \in E$.

Remarque 124.32 En dimension finie, u est nilpotent ssi u est localement nilpotent.

Exemple 124.33 (i) L'opérateur de dérivation D restreint à $K[X]$. (ii) L'opérateur de différenciation sur les suites polynômiales.

Proposition 124.34 Soit u localement nilpotent ; alors il existe un morphisme de K-algèbres $\varphi_u : K[[X]] \to \mathcal{L}(E)$ qui à S associe

$$x \mapsto \sum_{n \leq n_x} s_n u^n(x)$$

L'image est notée $K[[u]]$; elle est isomorphe à $K[[X]]/(X^p)$ pour

Exemple 124.35 (Formule de Taylor pour les polynômes) Soit $a \in K$, on note $\tau_a(P) = P(X + a)$. Alors $\tau_a \in K[[D]]$ et plus précisément

$$\tau_a = \exp(aD)$$

Remarque 124.36 On peut montrer que $K[[D]]^\times \simeq K[[X]]^\times$. On peut montrer $K[[D]]$ est le commutant de D (à rapprocher de ce que $K[C]$ est le commutant de C pour C un endomorphisme cyclique).

III.2. Série génératrice en combinatoire. A une suite $u \in K^{\mathbb{N}}$ on associe naturellement sa série génératrice $U = \sum_{n>0} u_n X^n$. L'intérêt d'une telle écriture est que les relations de récurrence sur la suite u_n vont se traduire en des relations algébriques vérifiées par U dans $K[[X]]$.

DEV 2

Exemple 124.37. (nombres de Catalan) Soit c la suite d'entiers définie par $c_0 = 1$ et pour tout $n \in \mathbb{N}$,

$$c_{n+1} = \sum_{k=0}^{n} c_k c_{n-k}$$

Alors,

$$c_n = \frac{1}{n+1}\binom{2n}{n}$$

Exemple 124.38 Le nombre de manière de paver un rectangle de taille $3 \times n$ (n pair) avec des dominos de taille 2×1 est

$$u_n = \sum_{k \in \mathbb{Z}} \binom{n/2 + k}{n/2 - k} 2^k$$

Exemple 124.39 (Partitions d'un entier en parts xées) Soit $_1;:::;_p$ des entiers naturels non nuls premiers entre eux dans leur ensemble. Pour tout $n \in \mathbb{N}$, on pose

$$p(n) = \left| \left\{ (n_1;:::;n_p) \in \mathbb{N}^p \mid \sum_{i=1}^{p} n_p \ _p = n \right\} \right|$$

Alors,

$$p(n) \quad \prod_{i=1}^{p} \ _i^{\ !\ 1} \ \frac{n^{p\ 1}}{(p\ 1)!}$$

IV. Compléments.

IV.1. Substitution et spécialisation. $A[[X]]$ est le complété de $A[X]$ pour la métrique (X)-adique. Le contexte général pour qu'il existe une spécialisation de $A[[X]]$ élément d'une A-algèbre A est que celle-ci soit complète pour la métrique $(\ )$-adique. En particulier, la spécialisation en $T \in A[[X]]$ est possible ssi $A[[T]]$ est complet pour la topologie (T)-adique, autrement dit si la topologie (T)-adique sur $A[[X]]$ est moins ne que la topologie (X)-adique, et équivaut alors à la substitution de T. Ceci éclaire la condition $T(0) = 0$ et la notation $S \ T = S(T)$.

IV.2. Automorphismes de la K-algèbre $K[[X]]$. L'anneau $K[[X]]$ possède un unique idéal maximal m, ce qui en fait un anneau local. Tout automorphisme de $K[[X]]$ préserve m et envoie donc (X) sur l'un de ses associés ; il est de la forme $R_S : U \mapsto U \ S$ où $! (S) = 1$ et d'inverse $R_{S \ 1}$. De fait nous pouvons écrire

$$\mathrm{Aut}(K[[X]]) \simeq K[[X]]$$

où $K[[X]]$ est le groupe des éléments réciproquables de l'algèbre $K[[X]]$.

Anneaux de valuation discrète. L'anneau $A[[X]]$ est un anneau de valuation discrète.

Autres développements possibles.

(1) Nombres de Bernoulli, propriété fondamentale des polynômes de Bernoulli.

(2) Formule de réversion de Lagrange, théorème de Schur.

(3) Théorème d'inversion locale pour les fonctions analytiques.

(4) Nombre de surjections, nombres de Bell, nombre de Stirling de 2e espèce.

126. Extensions de corps. Exemples et applications.

127. Exemples d'équations diophantiennes

Références.

Commentaires. Le seul cas pour lequel on peut développer une théorie générale est le degré 1, il ne faut pas le négliger. En particulier on pourra augmenter le nombre de variables progressivement pour voir quelles sont les propriétés de l'anneau $\mathbb{Z}$ impliquées. Pour l'existence et la structure des solutions, la principalité de $\mathbb{Z}$ suffit mais pour trouver les solutions il faut utiliser que $\mathbb{Z}$ est euclidien (algorithme de Gauss). Les exemples fondamentaux de degré 2 sont l'équation de Pythagore et les équations de Pell-Fermat.

I. Équations diophantienne de degré 1.

(1) $\mathbb{Z}$ est intègre. Une variable.

(2) $\mathbb{Z}$ est factoriel. Deux variables.

(3) $\mathbb{Z}$ est principal. Systèmes linéaires en entiers : théorème de la base adaptée, existence de la forme normale de Smith. [Sam67] [DTLQ14]

(4) $\mathbb{Z}$ est euclidien. Algorithme de résolution des systèmes linéaires en entiers. [DTLQ14]

II. Équations diophantiennes de degré 2.

(1) L'équation de Pythagore $x^2 + y^2 = z^2$. Paramétrisation des solutions.[Sam67]

(2) Les équations de Pell $x^2 - dy^2 = 1$. Lemme d'approximation de Dirichlet, théorème d'existence. Lien avec le développement de $\sqrt{d}$ en fraction continue.[Hin08].

(3) Le théorème des deux carrés $x^2 + y^2 = m$, $m \in \mathbb{N}$. Propriétés arithmétiques de l'anneau $\mathbb{Z}[i]$. La fonction $r_2(n)$.[Per96?]

(4) Formes quadratiques binaires entières. Nombres premiers représentés. Classification au sens de Gauss (vue comme une conséquence de l'action du groupe modulaire sur $\mathbb{H}$).

III. Compléments.

(1) L'équation de Fermat $x^m + y^m = z^m$. Inexistence de solutions pour $m = 4$. Théorème de Germain : si p est un nombre premier de Germain, pas de solutions en entiers $xyz \not\equiv 0 \ (p)$.

(2) Géométrie des nombres : Réseaux. Lemme du corps convexe de Minkowski. Applications : théorème des deux carrés, théorème des quatre carrés.

(3) Equations diophantiennes dans $\mathbb{N}$. Le cas du degré 1 : équivalent du nombre de solutions. Séries génératrices.

Autre développement possible. Equation de Ramanujan-Nagel [FG94].

141. F Polynômes irréductibles

A est un anneau commutatif intègre. On rappelle que A [X] est un anneau commutatif intègre contenant A et que A [X] = A . On suppose connue la propriété universelle de l'algèbre A [X].

I. Premières propriétés.

I.1. Eléments irréductibles, racines.

Définition 141.1 Soit P 2 A [X]. S'équivalent :
(i) P 6= 0 et pour tous Q; R 2 A [X], P = QR implique Q 2 A ou R 2 A
(ii) L'idéal (P) est maximal parmi les idéaux propres de A [X].
(iii) L'anneau quotient A [X]=(P) est un corps.

On dit alors que : P est irréductible dans A [X]

Exemple 141.2 Tout polynôme de degré 1 est irréductible.

Proposition 141.3 A corps) A [X] principal) A [X] euclidien

Définition 141.4 Soit B un sous-anneau de A et P 2 B [X]. On dit que r 2 A est racine de P si P (r) = 0 .

Proposition 141.5 Soit k un corps, P 2 k [X]. Alors si r est racine de P , (X r) divise P dans k [X].

Corollaire 141.6 Si P 2 k [X] est irréductible et de degré > 1, alors il n'a pas de racine dans k. En particulier, si k est algébriquement clos, les irréductibles de k [X] sont les polynômes de degré 1.

Théorème 141.7 C est algébriquement clos. En particulier, les irréductibles de R [X] sont :
- Les polynômes de degré 1
- Les polynômes de degré 2 de discriminant < 0

I.2. Lemme du contenu et conséquences ici A est un anneau à pgcd.

Définition 141.8 Soit $P = \sum a_k X^k$ un élément de A [X] et c un pgcd des a_k ; on dit que c est un contenu de P , noté c = c(P) (dé ni à association près). On dit que P est primitif si c(P) 1.

Lemme 141.9 (du contenu) Supposons A factoriel. Alors c(P) c(Q) = c(PQ)

Théorème 141.10 Soit K le corps de fraction de A ; on dispose d'une inclusion naturelle A [X] K [X], et les irréductibles de A [X] sont :
- les irréductibles de A
- les polynômes primitifs irréductibles de K [X]

Théorème 141.11 Si A est factoriel alors A [X] est factoriel.

Corollaire 141.12 Si A est factoriel, alors P est irréductible dans A [X] dès que l'anneau A [X]=(P) est intègre.

I.3. Critère d'Eisenstein et applications.

Théorème 141.13 (Critère d'Eisenstein) Soit A un anneau factoriel et K = Fr (A), $P = \sum a_k X^k$ à coe cients dans A. Soit p un irréductible de A ; on note (k) la valuation p-adique de a_k. Alors, si
(i) (k) > 1 pour k < n
(ii) (n) = 0
(iii) (0) = 1
Le polynôme P est irréductible sur K [X] (et même, dans A [X], s'il est primitif)

Exemple 141.14 (i) Pour tout entier p premier, $X^2 - p$ est irréductible (et donc, $\sqrt{p}$ est irrationnel)
(ii) Le polynôme $X^4 + 1$ est irréductible sur Z.

II. Techniques corporelles.

II.1. La réduction modulo p.

Proposition 141.15 Soit $P \in \mathbb{Z}[X]$ dont le coefficient dominant n'est pas divisible par p. Alors, si la réduction de P dans $\mathbb{F}_p$ est irréductible, P est irréductible sur $\mathbb{Z}$.

Remarque 141.16 Le polynôme $\Phi_8 = X^4 + 1$ est irréductible sur $\mathbb{Q}$ mais réductible dans tous les $\mathbb{F}_p$.

Définition 141.17 Soient $d = \sum d_{1,i} = \sum d_{2,j}$ deux partitions de l'entier d. On dit que d_1 est plus fine que d_2 si pour tout i il existe $i_1, \dots, i_r$ tels que $d_{2,i} = \sum_l d_{1,i_l}$.

Proposition 141.18 Soit $P \in \mathbb{Z}[X]$ unitaire de degré d ; P_1 et P_2 ses réductions modulo p_1 et p_2. On suppose que

$$P_1 = \Phi_{1,1} \cdots \Phi_{1,r}$$
$$P_2 = \Phi_{2,1} \cdots \Phi_{2,s}$$

sont leurs décompositions en produits d'irréductibles de $\mathbb{F}_{p_1}[X]$, éventuellement non distincts. On en déduit

$$d = \sum_{i=1}^{r} \deg \Phi_{1,i} = \sum_{j=1}^{s} \deg \Phi_{2,j}$$

Si les deux partitions de l'entier d associées à ces décompositions n'ont pas de partition moins fine en commun non triviale, alors P est irréductible sur $\mathbb{Z}$.

II.2. Corps de rupture.

Définition 141.19 Soit $P \in k[X]$ un polynôme irréductible. Une extension K de k est appelée extension de rupture de P si $K = k(\alpha)$ où $P(\alpha) = 0$.

Proposition 141.20 Il existe un corps de rupture unique à isomorphisme près (c'est le corps $k[X]/(P)$)

Remarque 141.21 L'unicité à isomorphisme près ne signifie pas qu'il y a unicité des corps de rupture dans une extension algébrique. Par exemple, considérons le polynôme $P = X^3 - 2$ sur $\mathbb{Q}$ (irréductible d'après le critère d'Eisenstein) ; le corps de rupture admet 3 plongements dans $\overline{\mathbb{Q}}$ à savoir $\mathbb{Q}(\sqrt[3]{2})$ (totalement réel), $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$

II.3. Quelques critères d'irréductibilité.

Proposition 141.22 Soit P un polynôme de degré n. Si P n'a pas de racine dans une extension de degré $\leq n/2$, alors P est irréductible.

Remarque 141.23 L'usage le plus fréquent de cette proposition est le cas $n = 3$; un polynôme de degré 3 est irréductible s'il n'a pas de racine.

Théorème 141.24 Soit $P \in k[X]$ un polynôme irréductible de degré n et K une extension de k de degré m premier à n. Alors, P est encore irréductible dans $K[X]$.

Exemple 141.25 $X^3 + X + 1$ (irred sur $\mathbb{Q}$ mais aussi sur $\mathbb{Q}(i)$)

Compléments.

Anneaux intégralement clos.

Définition 141.26 A est intégralement clos si tout polynôme irréductible unitaire de $A[X]$ possède une racine dans A.

Exemple 141.27 L'anneau $\mathbb{Z}$. L'anneau $\mathcal{O}_K$ des entiers du corps de nombres K.

Théorème 141.28 Tout anneau factoriel est integralement clos.

Algorithme de Berlekamp. L'algorithme de Berlekamp permet de factoriser un polynôme $P \in \mathbb{F}_q[X]$ en produit d'irréductibles sur $\mathbb{F}_q$.

142. Algèbre des polynômes à plusieurs indéterminées. Applications

143. Résultant. Applications

144. Racines de polynômes. Polynômes symétriques.

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

151. F Dimension d'un espace vectoriel

Références.

Commentaires. Les applications de la théorie de la dimension sont extrêmement nombreuses mais on n'y pense pas forcément.

Attention. Pour la théorie de la dimension, on se tiendra a une unique référence (par exemple [RDO88]) pour éviter tout cercle vicieux.

Dans toute la leçon, k est un corps commutatif et E est un k-espace vectoriel. I est un ensemble d'indices.

I. Théorie de la dimension.

I.1. Famille libre, famille génératrice.

Définition 151.1 $k^{(I)}$ est l'espace vectoriel des familles de scalaires $(s_i)_{i \in I}$ à support ni.

Définition 151.2 Soit $x = (x_i)_{i \in I}$ une famille de vecteurs de E. On dispose d'une application

$$\begin{aligned} \varphi_x : k^{(I)} &\to E \\ (\lambda_i) &\mapsto \sum_{i \in I} \lambda_i x_i \end{aligned}$$

φ_x est appelée application linéaire attachée à la famille x. Par dé nition, $\mathrm{Vect}(x_i)$ est l'image de φ .

Exemple 151.3 $E = L(F)$, $u \in L(E)$ et $x_i = u^i$ pour tout $i \in \mathbb{N}$. Alors φ_x est l'application de spécialisation en u. C'est encore un morphisme de k-algèbres, si l'on identi e $k^{(I)}$ à $k[X]$. Son image est $k[u]$.

Définition 151.4 On dit que la famille (x_i) est :
- génératrice, si φ_x est surjective
- libre, si φ_x est injective

Si (x_i) n'est pas libre, elle est dite liée. Si (x_i) est libre et génératrice, on dit que c'est une base. Une sur-famille (resp. une sous-famille) d'une famille génératrice est génératrice (resp. libre).

Exemple 151.5 (i) La famille de fonctions $(t \mapsto e^{\lambda_i t})_{i \in I}$ pour λ_i une famille de réels distincts deux à deux, est libre.

(i) Soient K et L deux corps ; une famille de morphismes $f_i : K \to L$ est libre ssi les f_i sont distincts (lemme de Dedekind)

Proposition 151.6 L'image d'une famille génératrice par une application surjective est génératrice. L'image d'une famille libre par une application linéaire injective est libre. L'image d'une base par un isomorphisme est une base.

Remarque 151.7. En particulier, une famille génératrice l'est encore dans un sous-espace qui la contient ; une famille est libre dans un espace qui contient E.

II. Dimension nie.

Proposition 151.8. Une famille composée d'un unique vecteur x_0 est libre si et seulement si $x \neq 0$.

En d'autres termes (et contrairement aux modules) il n'y a pas d'élément de torsion.

Proposition 151.9. Les assertions suivantes s'équivalent :
(i) e est une base
(ii) e est une famille génératrice minimale
(iii) e est une famille libre maximale.

Lemme 151.10. Soit $(e_i)_{1 \leq i \leq n}$ une famille. Alors, toute famille de cardinal $n+1$ formée de combinaisons linéaire de termes de e est liée.

Définition 151.11. On dit que E est de dimension nie, s'il admet une famille génératrice nie.

Proposition 151.12 (Théorème de la base incomplète). Soient $J \subset I$ telles que $(e_i)_{i \in J}$ est libre, $(e_j)_{j \in I}$ est génératrice. Alors il existe L telle que $J \subset L \subset I$ et (e_L) soit une base de e.

Théorème 151.13 (Théorème de la dimension - cas de la dimension nie). Tout espace vectoriel de dimension nie admet une base nie. De plus, le cardinal des bases est le même, il est appelé dimension de E et noté $\dim_k E$.

III. Caractérisation des bases, classi cation.

Proposition 151.14. Soit (e_i) une famille de E avec $\dim E = n$. Les conditions suivantes sont équivalentes :
(i) (e_i) est génératrice et de cardinal n
(ii) (e_i) est libre de cardinal n
(iii) (e_i) est une base de E

Corollaire 151.15 (Théorème de classi cation). Deux espaces vectoriels de dimension nie sont isomorphes si, et seulement si ils ont même dimension.

Proposition 151.16. Soit $u \in L(E;F)$ où E et F sont de dimension nie et de même dimension. Alors u est injective ssi u est surjective ssi u est bijective.

Corollaire 151.17. Soit A une k-algèbre de dimension nie. Alors A est un corps (éventuellement non commutatif) si et seulement si A est intègre.

Remarque 151.18. Il y a une analogie avec le cas des applications entre ensembles nis. L'analogue du dernier corollaire est qu'un anneau commutatif intègre ni est un corps.

IV. Dimension et rang. Si E n'est pas de dimension nie, on écrira $\dim_k E = +\infty$. On adopte doénavant l'ordre et les règles de calcul usuel (addition et multiplication) dans $\overline{\mathbb{N}} = \mathbb{N} \cup \{+\infty\}$: $n + +\infty = n \times +\infty = +\infty$, $n \leq +\infty$ pour tout $n \in \overline{\mathbb{N}}$.

V. Sous-espaces, supplémentaire.

Proposition 151.19. Soit F un sous-espace vectoriel de E. Alors

$$\dim F \leq \dim E$$

Théorème 151.20. Si E est de dimension nie, F admet un supplémentaire G dans E, et

$$\dim E/F = \dim G \leq \dim E$$

V.1. Produit et somme.

Proposition 151.21 Soient E et F deux k-espaces vectoriels ; alors

$$\dim E \quad F = \dim E + \dim F$$

Proposition 151.22 Soient $E_1, \ldots, E_n$ des ssev de E de dimension nie, alors

$$\dim \sum_i E_i \leq \sum \dim E_i$$

avec égalité si et seulement si la somme est directe.

Proposition 151.23 (Changement de corps de base) Soit k^0 un sous-corps de k. Alors E et k sont des k^0-espace vectoriels. De plus,

$$\dim_{k^0} E = (\dim_{k^0} k) \quad (\dim_k E)$$

Corollaire 151.24 Impossibilité de la trisection de l'angle et de la duplication du cube.

DEV 2

V.2. Rang et théorème du rang.

Définition 151.25 Si E est de dimension nie, le rang de la famille (x_i), noté $\mathrm{rg}(x_i)$ est la dimension de $\mathrm{Vect}(x_i)$. C'est un entier plus petit que $\dim E$.

Décrire un algorithme de détermination pratique du rang.

Définition 151.26 Soit $u \in L(E;F)$. Si $\mathrm{Im} u$ est de dimension nie, on dit que u est de rang ni, et on note $\mathrm{rg} u = \dim \mathrm{Im} u$.

Le premier théorème d'isomorphisme donne alors la

Proposition 151.27 Si E est de dimension nie, alors toute application linéaire partant de E est de rang ni $\leq \dim E$. De plus,

$$\dim E = \mathrm{rg} u + \dim \ker u$$

Exemple 151.28 La suite d'espace vectoriels $E_0 \xrightarrow{u_0} \quad \xrightarrow{u_{p-1}} E_p$ de dimension nie est dite exacte si $\mathrm{Im}\, u_i = \ker u_{i+1}$ pour tout $i < p \quad 1$. On a alors la relation d'Euler-Poincaré

$$\sum_{i=0}^{p} (-1)^i \dim E_i = 0$$

Exemple 151.29 (Formule de Grassmann généralisée) Soient $F_1, \ldots, F_p$ des ssev de E de dimension nie. Alors

$$\dim \sum_{i=1}^{p} F_i = \sum_{i=1}^{p} \dim F_i \quad \sum_{i,j} \dim F_i \cap F_j + \quad + (-1)^{p-1} \dim \bigcap_{i=1}^{p} F_i$$

VI. Dualité en dimension nie.

VI.1. Dualité.

Définition 151.30 Soit E un k-espace vectoriel. Son dual E^* est l'espace $L(E;k)$. On note $\varphi(x) = \langle x, \varphi \rangle$ pour tout $(x, \varphi) \in E \quad E^*$

Théorème 151.31 Si E est de dimension nie, E^* aussi et $\dim E = \dim E^*$. Plus précisément, si (e_i) est une base de E alors il existe une unique famille (e_i^*) telle que $\langle e_i, e_j^* \rangle = \delta_{ij}$ appelée base duale.

Corollaire 151.32 L'application linéaire de bidualité $\quad : E \to E^{**}$ qui à x associe $\varphi \mapsto \langle x, \varphi \rangle$ est un isomorphisme si E est de dimension nie.

Proposition 151.33 Soit E, F deux espaces vectoriel de dimension nie. Alors $L(E;F)$ est de dimension nie, et

$$\dim L(E;F) = (\dim E)(\dim F)$$

De plus, si (e_i) est une base de E et (f_i) une base de F, une base de $L(E;F)$ est donnée par la famille

$$(f_j e_i^*)_{1 \leq i \leq \dim E;\ 1 \leq j \leq \dim F}$$

152. Déterminant. Exemples et applications

I. Notion de déterminant.

(1) Formes linéaires alternées sur un module libre de type ni. Applications à la théorie de la dimension.

(2) Matrices et déterminants. Invariance par extension des scalaires. Polynôme caractéristique.

(3) Techniques élémentaires de calcul. Comatrice. Formule de Cauchy-Binet.

(4) Calcul algorithmique : approche modulaire.

II. Applications en algèbre et géométrie.

(1) Determinant de Smith et thm Brauer.

(2) Discriminant ; équivalence des formes quadratiques (sur un corps ni).

(3) Déterminant et conique.

(4) Résultant de deux polynômes. Applications.

(5) Volume des ellipsoïdes. Ellipsoïde de John.

III. Application au calcul di érentiel dans R^n.

(1) Interprétation géométrique dans R^n (gure)

(2) Jacobien ; formule du changement de variables.

(3) Wronskien. Wronskien généralisé. Thm Sturm.

153. Polynômes d'endomorphisme en dimension nie

I. Référence [MM16].

II. Commentaire. Il y a deux niveaux de lecture pour cette leçon : élémentaire et version $k[X]$-module

III. Polynômes d'endomorphisme.

(1) L'algèbre $k[u]$. Polynôme minimal. Eléments inversibles, éléments nilpotents.

(2) Matrices. Polynôme caractéristique.

(3) Sous-espaces stables$_u$ et $_u$. Sous-espaces cyclique (dé nition). Endomorphisme cyclique. Théorème de Hamilton-Cayley.

IV. Polynômes d'endomorphisme et décomposition.

(1) Lemme de décomposition des noyaux

(2) décomposition de Dunford (avec polynômialité des projecteurs spectraux). Application : critère de nilpotence de Cartan.

(3) Exponentielle de matrice ; image.

V. Polynôme d'endomorphisme et réduction d'endomorphisme.

(1) Existence d'un vecteur primitif

(2) Théorème de réduction de Frobenius.

(3) Les racines ; la réduction de Jordan.

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

155. F Endomorphismes diagonalisables

I. Dé nitions, premières propriétés. Dans toute la leçon, E est un k-ev de dimension nie n. u est un endomorphisme de E.

I.1. Dé nitions.

Définition 155.1 Soit $A \in M_n(k)$. A est encore un élément de $M_n(k[X])$; le polynôme caractéristique de A est par dé nition

$$\chi_A = \det(XI_n - A) \in k[X]$$

Le polynôme caractéristique χ_u est le polynôme caractéristique d'une matrice de u ; il ne dépend pas de la matrice choisie.

Proposition 155.2 Soit $\lambda \in C$. S'équivalent
(i) $\chi_u(\lambda) = 0$
(ii) $\exists x \in E \setminus \{0\}$, $u(x) = \lambda x$
Dans ce cas, λ est dite valeur propre de u (noté $\lambda \in \mathrm{sp}\, u$) et l'espace $E_\lambda(u) = \ker(u - \lambda I)$ est appelé espace propre.

Remarque 155.3 Si $P \in k[X]$ est annulateur de u et $\lambda \in \mathrm{sp}\, u$ alors $P(\lambda) = 0$

Définition 155.4 Soit $\lambda \in k$. La dimension $d_\lambda(u) = \dim E_\lambda(u)$ est appelée multiplicité géométrique. La valuation de χ_u sur $X - \lambda$ est appelée multiplicité algébrique.

Proposition 155.5 Les espaces propres de u sont en somme directe. Lorsque cette somme coïncide avec E, on dit que u est diagonalisable.

Définition 155.6 Une base de diagonalisation est une base de E formée de vecteurs propres. La matrice de u diagonalisable dans l'une de ses bases de diagonalisation est diagonale.

Définition 155.7 On dit que $A \in M_n(k)$ est diagonalisable si elle admet une matrice diagonale dans sa $GL_n(k)$-orbite (pour l'action par conjuguaison), ou de manière équivalente, si elle représente un endomorphisme diagonalisable.

I.2. Premiers critères de diagonalisabilité.

Définition 155.8 u est semi-simple si tout espace u-stable admet un supplémentaire u-stable.

Théorème 155.9 S'équivalent
(i) u est diagonalisable
(ii) χ_u est scindé, et $\forall \lambda \in \mathrm{sp}\, u$, $m_\lambda(u) = d_\lambda(u)$.
(iii) un polynôme simplement scindé annule u
(iv) un polynôme scindé annule u, et u est semi-simple.

Remarque 155.10 (ii) est une reformulation. (iii) et (iv) découlent par contre du lemme de décomposition des noyaux.

Exemple 155.11 Un idempotent est annulé par $X(X-1)$; il est diagonalisable. Une symétrie est annulée par $X^2 - 1 = (X+1)(X-1)$; elle est diagonalisable si car $k \neq 2$.

Si u est diagonalisable, $P(u)$ est diagonalisable pour tout $P \in k[X]$

Proposition 155.12 (Critère des polynômes d'endomorphisme) u est diagonalisable si et seulement si

$$\forall P \in k[X],\ P(u) = 0 \Rightarrow P(u) \text{ nilpotent}$$

En d'autre termes, l'idéal annulateur de u dans $k[X]$ est radical.

II. Compléments.

II.1. Décomposition de Jordan & Dunford, applications.

Théorème 155.13 Supposons que $_u$ est scindé. Alors u s'écrit de manière unique sous la forme

$$u = d + n$$

où d est diagonalisable, n est nilpotent et $d; n$ commutent. d et n sont alors des polynômes en u.

Proposition 155.14 (Critère de Klarès) On pose

$$\begin{aligned} ad_u : L(E) &\to L(E) \\ v &\mapsto uv - vu \end{aligned}$$

Alors u est diagonalisable ssi $\ker ad_u = \ker ad_u^2$.

II.2. Commutant. Endomorphismes codiagonalisables.

Proposition 155.15 Si v commute à u alors les espaces propres de u sont v-stables.

Corollaire 155.16 Si u est diagonalisable, alors v commute à u (noté $v \in C(u)$) ssi v laisse stables les espaces propres de u. En particulier,

$$\dim C(u) = \sum_{\lambda \in k} (\dim \ker(\lambda I - u))^2$$

Théorème 155.17 Soient u et v deux endomorphismes diagonalisables qui commutent. Alors il existe une base de diagonalisation commune de u et v.

Application : soit G un p-groupe abélien fini. Alors G est isomorphe à un produit direct de p-groupes cycliques (via la représentation de G dans les matrices de permutation).

II.3. Aspects topologiques.

Définition 155.18 u est dit régulier s'il possède n valeurs propres distinctes.
Un endomorphisme régulier est diagonalisable.

Proposition 155.19 $k = \mathbb{C}$. L'ensemble des endomorphismes réguliers est un ouvert dense de $L(E)$. En particulier les endomorphismes diagonalisables forment un G_δ-dense (au sens de la théorie de Baire)

Proposition 155.20 (Caractérisation topologique de la diagonalisabilité) A est diagonalisable si, et seulement si, la classe de similitude de A est fermée dans $M_n(\mathbb{C})$.

II.4. Algèbre bilinéaire. k est $\mathbb{R}$ ou $\mathbb{C}$. Supposons E euclidien (resp. hermitien) muni d'un produit scalaire (resp. hermitien) $\langle ; \rangle$, c'est-à-dire d'un isomorphisme $E \simeq E^*$ qui transporte le crochet de dualité. On rappelle que u possède alors un unique adjoint (qui est l'image de $^t u \in L(E^*)$).

Définition 155.21 u est normal ssi $uu^* = u^*u$

Lemme 155.22 Si u est normal, il est semi-simple. De plus, le supplémentaire u-stable de la définition 155.8 peut être choisi orthogonal.

Théorème 155.23 $k = \mathbb{C}$. u est normal ssi il admet une base orthonormée de diagonalisation. De manière équivalente :
(i) u est diagonalisable ssi il est normal pour un produit hermitien.
(ii) Les matrices normales sont les $U(n; \mathbb{C})$-orbites des matrices diagonales, pour l'action par conjuguaison, ou par congruence.

Application : les groupes $SO(n; \mathbb{R})$ et $SU(n; \mathbb{C})$ sont connexes.

III. Applications.

III.1. Systèmes di érentiels linéaires.

Définition 155.24. Soit I un intervalle de $\mathbb{R}$. Un système di érentiel linéaire est la donnée d'une équation di érentielle du type

$$X' = A(t)X(t)$$

où $A(t) \in \mathcal{M}_n(\mathbb{R})$.

Théorème 155.25. Supposons que A est $\mathcal{C}^1$ à valeurs dans une sous-algèbre $\mathcal{A}$ commutative. Alors X est donné sur I par

$$X(t) = \exp\left(\int_{t_0}^{t} A(t)\,dt\right) X(t_0)$$

Exemple 155.26. Soient a, b, c des fonctions scalaires $\mathcal{C}^0$ sur $\mathbb{R}$, et $(x_0, y_0, z_0) \in \mathbb{R}^3$. L'équation

$$\begin{array}{rcll} x' &=& ax + by + cz & x(0) = x_0 \\ y' &=& cx + ay + bz & y(0) = y_0 \\ z' &=& bx + cy + az & z(0) = z_0 \end{array}$$

admet pour solution

$$\begin{array}{rcl} u(t) &=& u_0 \exp\left(\int_0^t (a(s) + b(s) + c(s))\,ds\right) \\ v(t) &=& v_0 \exp\left(\int_0^t a(s) + j^2 b(s) + j c(s)\,ds\right) \\ w(t) &=& w_0 \exp\left(\int_0^t a(s) + j b(s) + j^2 c(s)\,ds\right) \end{array}$$

III.2. Réduction des matrices d'adjacence.

Définition 155.27. Une fête F est la donnée d'un ensemble ni P (de personnes) muni d'une relation binaire A (appelée amitiée) symétrique et nulle part ré exive. Une matrice d'incidence $(f_{p;q}) \in \mathcal{M}_P(\mathbb{R})$ de F est dé nie par $f_{p;q} = [pAq]$

Proposition 155.28. Une matrice d'incidence est diagonalisable.

Théorème 155.29 (Théorème de l'amitié). Soit $F = (P; A)$ un fête à n personnes. On suppose que pour toute paire $\{p; p'\}$ P d'éléments distincts il existe un unique p'' tel que

$$pAp'' \wedge p'Ap''.$$

Alors

(i) $n \quad 2$ modulo 3

(ii) Il existe $h \in P$ appelé hôte de F tel que $\forall p \neq h;\ hAp$.

156. Exponentielle de matrice

Dans toute la leçon, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Définition 156.1 La série de fonctions de terme général $A \mapsto \frac{A^k}{k!}$ est normalement convergente sur tout compact de l'algèbre de Banach $\mathcal{M}_n(\mathbb{K})$. Sa somme est une application continue, appelée exponentielle.

Remarque 156.2 Si $n = 1$, cette définition coïncide avec l'usuelle sur $\mathbb{R}$ ou $\mathbb{C}$.

Proposition 156.3 Pour tout $A \in \mathcal{M}_n(\mathbb{K})$, $\exp(A) \in \mathbb{K}[A]$; autrement dit $\exp A$ est un polynôme en A.

Remarque 156.4 Ce polynôme dépend de A.

Définition 156.5 Soient $A, B \in \mathcal{M}_n(\mathbb{K})$. On appelle crochet de Lie de A et B et on note $[A, B]$ la matrice $AB - BA$.

Proposition 156.6 Pour toutes $A, B \in \mathcal{M}_n(\mathbb{K})$ nous avons :
(i) Si $[A, B] = 0$ alors $\exp(A)\exp(B) = \exp(A + B)$
(ii) $\exp(A) \in GL(n, \mathbb{K})$ et $(\exp(A))^{-1} = \exp(-A)$
(iii) $\forall P \in GL(n, \mathbb{K})$, $\exp(PAP^{-1}) = P\exp(A)P^{-1}$
(iv) $\exp({}^tA) = {}^t\exp A$ et si $\mathbb{K} = \mathbb{C}$, $\exp(\overline{A}) = \overline{\exp(A)}$
(v) Si A est triangulaire supérieure avec coefficients diagonaux $a_1, \dots, a_n$, alors $\exp(A)$ est triangulaire supérieure avec coefficients diagonaux $\exp(a_1), \dots, \exp(a_n)$.
(vi) $\det(\exp(A)) = \exp(\operatorname{tr} A)$
(vii) $\exp(\operatorname{diag}(A_1, \dots, A_r)) = \operatorname{diag}(\exp(A_1), \dots, \exp(A_r))$

Remarque 156.7. (i) est possiblement en défaut si $AB \neq BA$, ce qui peut arriver dès que $n > 2$. Prendre A le projecteur sur e_1 et B telle que $Be_2 = e_1$ et $Be_1 = 0$; alors $\exp(AB) = AB \neq \exp A + \exp B$.
- Si $A = D + N$ est la décomposition de Dunford de A alors $\exp(A) = \exp(D)\exp(N)$

Proposition 156.8 $\operatorname{sp}_{\mathbb{C}} \exp(A) = \{\exp(\lambda) ; \lambda \in \operatorname{sp}_{\mathbb{C}} A\}$

Corollaire 156.9 $\exp(At) \xrightarrow[t \to +\infty]{} 0 \iff \forall \lambda \in \operatorname{sp}_{\mathbb{C}} A, \operatorname{Re}\lambda < 0$.

Proposition 156.10 A est diagonalisable $\iff$ $\exp(A)$ est diagonalisable

I. Sous-groupes de $GL(n, \mathbb{K})$.

I.1. Sous-groupes à un paramètre.

Rappelons que les $\exp(\lambda\ )$ sont tous les morphismes continus de $(\mathbb{R}, +)$ vers $(\mathbb{R}^*, \times)$. Plus généralement :

Proposition 156.11 Soit φ un morphisme de $\mathbb{R}$ dans $GL(n, \mathbb{K})$ continu. Alors il existe $A \in \mathcal{M}_n(\mathbb{R})$ telle que $\varphi(t) = \exp(At)$

Exemple 156.12 (i) Pour N nilpotente, le sous-groupe de $GL(2, \mathbb{K})$ de la forme $I + \lambda N$ avec $\lambda \in \mathbb{R}$.
(ii) Le sous-groupe $SO(2, \mathbb{R}) = \{\exp(Jt)\}_{t \in \mathbb{R}}$ où J est la matrice de rotation d'angle $= 2$.

I.2. Algèbre de Lie d'un sous-groupe fermé de $GL(n, \mathbb{K})$.

Proposition 156.13 Soient $A, B \in \mathcal{M}_n(\mathbb{K})$; alors
(i) $\lim_{p \to +\infty} (I + A/p)^p = \exp(A)$
(ii) $\lim_{p \to +\infty} (\exp(A/p)\exp(B/p))^p = \exp(A + B)$
(iii) $\lim_{p \to +\infty} \left(\exp\frac{A}{p}\exp\frac{B}{p}\exp\frac{-A}{p}\exp\frac{-B}{p}\right)^{p^2} = \exp([A, B])$

Théorème 156.14 Si G est un sous-groupe fermé de $GL(n, \mathbb{K})$, alors l'ensemble

$$\mathfrak{g} = \{A \in \mathcal{M}_n(\mathbb{K}) ; \forall t \in \mathbb{R}, \exp(tA) \in G\}$$

forme un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$, stable par le crochet de Lie. On l'appelle l'algèbre de Lie de G.

Exemple 156.15 (i) Si $G = GL(n;K)$ alors $\mathfrak{g} = M_n(K)$ (vue comme algèbre de Lie, on la note $\mathfrak{gl}(n;K)$).
(ii) Si $G = SL(n;K)$ alors $\mathfrak{g} = \mathfrak{sl}_n(K) = \ker \mathrm{tr}$
(iii) Si $G = SO(n;R)$ alors $\mathfrak{g} = A_n(R)$
(iv) Si G est $\{ni\}$ alors $\mathfrak{g} = \{0\}$.

II. Image de l'exponentielle.
II.1. Différentiabilité.

Proposition 156.16 L'application $\exp_R$ (resp. $\exp_C$) est différentiable de n^2 (resp. $2n^2$) variables réelles sur $M_n(K)$, de différentielle $\mathrm{Id}_{M_n(K)}$ en l'identité.

Corollaire 156.17 exp réalise une difféomorphisme local d'un voisinage de 0 dans $M_n(K)$ sur un voisinage de I_n dans $GL(n;K)$.

Proposition 156.18 Il existe V voisinage de I_n dans $GL(n;K)$ tel que tout sous-groupe de $GL(n;K)$ contenu dans V est trivial.

II.2. Image.

Remarque 156.19 exp n'est pas injective (sauf si $n = 1$ et $K = R$)

Proposition 156.20 Soit $A \in M_n(K)$; alors $\exp(A) = I_n \Leftrightarrow \mathrm{sp}_C(A) \subset 2i\pi\mathbb{Z}$

Définition 156.21 Nil_n est l'ensemble des matrices nilpotentes de $M_n(K)$. $\mathrm{Uni}_n = \{I_n + N ;\ N \text{ nilpotente}\}$ est l'ensemble des matrices unipotentes de $M_n(K)$

Proposition 156.22 exp réalise un homéomorphisme de Nil_n sur Uni_n :

Théorème 156.23 (i) $\exp_C$ est surjective sur $GL(n;C)$
(ii) $M \in GL(n;R)$ est une exponentielle de matrice réelle $\Leftrightarrow \exists A \in GL(n;R) ;\ M = A^2$.

Corollaire 156.24 (Divisibilité dans les groupes linéaires) Soit $A \in GL(n;C)$ et $p > 1$; alors A admet une racine p-ième. Pour $A \in GL(n;R)$, A admet une racine p-ième pour tout p si et seulement si A est un carré.

Proposition 156.25 $GL(n;C)$ est connexe ; les classes de similitude de $M_n(C)$ sont connexes.

Remarque 156.26 On retrouve ce fait directement à partir de générateurs de $GL(n;C)$.

III. Systèmes différentiels linéaires.
III.1. Définition et théorème de Cauchy-Lipschitz.

Définition 156.27 Un système différentiel linéaire est la donnée de deux applications $A \in C^0(R;M_n(K))$ et $B \in C^0(R;M_{n;1}(K))$ et d'une équation de la forme

$$X'(t) = A(t)X(t) + B(t) \tag{81}$$

Remarque 156.28 Ce cas englobe celui des équations différentielles linéaires scalaires d'ordre n (avec pour A une matrice compagnon)

Théorème 156.29 Soit $t_0 \in R$. Si A est localement lipschitzienne, l'équation (81) avec la condition initiale $X(t_0) = X_0$ admet une unique solution sur un intervalle I contenant t_0.

Proposition 156.30 S'il existe $a;b \in R_+$ telles que $\|A(t)\| \leq at + b$ pour tout t, alors l'équation (81) admet des solutions sur tout R, uniques à condition initiale donnée.

III.2. Lien avec l'exponentielle.

Proposition 156.31 Soit $(A;B)$ un système différentiel et supposons que A est à valeurs dans une sous-algèbre commutative de $M_n(K)$. Alors la solution générale de l'équation est donnée par $X(t) = \exp\left(\int_{t_0}^{t} A(s)\,ds\right) X_0 + \int_{t_0}^{t} \exp\left(\int_{u}^{t} A(s)\,ds\right) B(u)\,du$

Définition 156.32 Soit $(A;B)$ un système différentiel vérifiant les hypothèses du théorème 156.29 et de la proposition 156.30. On définit la résolvante $R_{t_1}^{t_2}$ par $X(t_2) = R_{t_1}^{t_2} X(t_1)$ pour X solution de l'équation homogène $X' = A(t)X$.

Remarque 156.33 $W(t) = \det R(t)$ est le wronskien. Nous avons $W(t) = \exp \int_{t_0}^{t} \operatorname{tr} A(s)\,ds$. De plus, les conditions suivantes sont équivalentes

(i) $W(t_0) \neq 0$

(ii) $W(t) \neq 0$ pour tout $t \in I$

III.3. Vers la formule de Baker-Campbell-Hausdorff.

Proposition 156.34 Soient $A;B$ telles que $[A;[A;B]] = [B;[A;B]] = 0$. Alors

$$\exp(A)\exp(B) = \exp\left(A + B + \frac{[A;B]}{2}\right) :$$

157. Endomorphismes trigonalisables. Endomorphismes nilpotents.

Commentaire. On aborde ici la réduction dans la direction de la réduction de Jordan, dont la réduction des nilpotents appporte l'information combinatoire essentielle.

I. Dé nitions.

(1) Drapeaux. Drapeaux stables. Endomorphismes trigonalisables$u$ trigonalisable $\Leftrightarrow$ u scindé. Application : $\det \exp(u)$. Version matricielle.

(2) Endomorphismes nilpotents. Caractérisations. Réduction des endomorphismes nilpotents : Le lemme des noyaux itérés

II. Réduction.

(1) Lemme de décomposition des noyaux, projecteurs spectraux et décomposition de Dunford. Applications : images exponentielle. Critère de nilpotence de Cartan.

(2) Réduction de Jordan. Application : Critère de diagonalisabilité de Klarès. Tableaux de Young. Les carrés de$GL(n;R)$

(3) Co-réduction. Théorème de Lie Kolchin

III. Aspects topologiques ($k = C$).

(1) Densité des diagonalisables. Application : Hamilton-Cayley.

(2) Caractérisation des classes nilpotentes.

170. Formes quadratiques. Orthogonalité, isotropie.

Références. [Aud12], [Per96]

On cherche la plus grande généralité (tout en excluant la caractéristique 2). Un peu comme pour les représentations ou la réduction, il est utile de penser une forme quadratique comme une structure supplémentaire sur un espace vectoriel : notion d'espace quadratique. Toutefois l'in uence du corps de base est dans le cas des formes quadratiques nettement plus pregnante. sur F_p recèlent des aspects arithmétiques.

I. Formes bilinéaires symétriques.

(1) Dé nition. Orthogonalité. Formes non dégénérées : isomorphisme de E avec son dual. Application : représenter les crochets de dualité. Polarité par rapport à une quadrique.[Aud12]

(2) Isotropie : dé nitions, premières propriétés.

(3) Forme matricielle. Base orthogonale.

(4) L'algorithme de mise sous carrés de Gauss.

II. Formes quadratiques.

(1) Dé nition. Isotropie.

(2) Elements de classi cation : Sur C, sur R (loi d'inertie de Sylvester) sur les corps nis. DEV : réciprocité quadratique.

(3) Plans hyperbolique. Existence de la décomposition hyperbolique + anisotrope. Théorème de simpli cation de Witt [Aud12].

(4) Orthogonalisation simultanée [RDO88] (tome 2). Exemples.

(5) Groupes orthogonaux ; groupes classiques ? []

III. Formes quadratiques et arithmétique des entiers.

(1) Formes quadratiques binaires : dé nition, propriétés.

(2) Classi cation : théorème de Gauss.

190. Méthodes combinatoire, problèmes de dénombrement

Références. [GKP94]

I. Approche élémentaire.

(1) Ensemble ni, cardinal. Bijections.

(2) Lemme des bergers. Application cardinal deHK, H et K sous-groupes de$G$. Principe des tiroirs. Application : une fq de rang > 2 sur F_q représente tout. Crible de Poincaré. Application : expression de$'(n)$.

(3) Nombres d'injection, de surjections, de bijections de$f1;:::ng$ vers $f1;:::pg$

II. Dénombrement de quelques ensembles. Application.

(1) Action de groupes. Théorie combinatoire des groupes. Equ. aux classes. Application sérieuse : les$p$-groupes ont un centre non trivial. Application pas sérieuse : preuve de Zagier du th. deux carrés. Formule de Burnside, une application au nombre de colliers.

(2) Espaces vectoriels et a nes sur les corps nis. Groupes linéaires sur un corps ni.

(3) Application : loi de réciprocité quadratique [CG13].

(4) Combinatoire du groupe symétrique. Grands cycles.

(5) Chevalley-Warning et Erdös-Ginzburg-Ziv.

(6) Nombre de points entiers dans un cercle. Comportement asymptotique de$_2(n)$.

III. Séries génératrices.

(1) Notions sur l'algèbre des séries formelles.

(2) Application : nombres de Catalan.

201. Espaces de fonctions. Exemples, applications

Références.

Commentaire. X espace topologique, E espace vectoriel, $F(X;E)$ espace de fonctions ; on rajoute progressivement de la structure (topologie, mesure, struct. di érentielle...) sur X et sur E. La leçon doit répondre à la question : quel est l'avantage de voir une fonction dans un espace de fonctions ? Plusieurs réponses :

- savoir approcher par des fonctions plus simples, voire savoir décomposer sur une base (au sens hilbertien) ;
- savoir bien formuler les problèmes d'EDP ou d'equa. di . : la fonction est une inconnue

C'est pourquoi on cherche complétude + à caractériser les parties denses et les parties compactes

I. Espaces de fonctions continues. X topologique, E e.v.n

(1) Complétude : théorèmes de transfert (si E Banach $C(X;E)$ Banach)

(2) Parties denses. DEV : théorème de Stone-Weierstrass Applications

(3) Caractéristation des parties compactes (X métrique). Théorème d'Ascoli. Applications : opérateurs à noyau. Sous-espaces fermés de fonctions régulières dans $C([0;1])$ (avec Banach-Steinhaus)

II. Espaces L^p. X topologique mesuré (espace borélien), $E = \mathbb{R}$

(1) Complétude : théorème de Riesz-Fischer [BCL99]

(2) Parties denses : $C_c(\ )$ dense dans L^p si $p < 1$ [BCL99]. Dualité L^p L^q

(3) Parties compactes : Riesz-Frechet-Kolmogorov

(4) L'espace $L^2(\ )$. Application : théorème de Radon-Nikodym, version faible [BMP05]. La version forte est dans [RRC87] DEV : Densité des polynômes orthogonaux.

(5) Espaces de Sobolev (et plus si a nités !) théorème Lax-Milgram, application : EDP

III. Espaces de fonctions holomorphes. $X =$ ouvert de $\mathbb{C}$, $E = \mathbb{C}$

(1) Complétude, parties compactes : théorèmes de Weierstrass et de Montel [AM04].

202. Exemples de parties denses et applications

Références. [Bré83, BMP05, RRC87]

Commentaire. Si A est dense dans X il rencontre chaque ouvert, ce qui matérialise dans X la topologie de X. La densité doit permettre le prolongement à X de certaines propriétés (égalités, inégalités...) vraies sur A (ce principe ne se réduit pas à l'Analyse). Par ailleurs A est d'autant plus facile à manier qu'il est petit, par exemple dénombrable. Il est donc utile de chercher des parties denses, petites si possible.

I. Densité dans $\mathbb{R}$, application.

(1) $\mathbb{Z}[1/t]$ est dense dans $\mathbb{R}$, développement des réels en base t

(2) $\mathbb{Q}$ est dense dans $\mathbb{R}$ (par construction !), développement en fractions continues.

II. Densité dans les espaces vectoriels normés.

(1) Sous-espaces denses. Critère de densité par dualité de Hahn-Banach.

(2) Densité dans les espaces de fonctions continues. DEV th. de Stone-Weierstrass

(3) Densité dans les espaces l^p. L'espace de Hilbert séparable.

III. Densité et prolongement.

(1) Unicité du prolongement continu. Applications

(2) Existence (applications uniformément continues sur une partie dense d'un complet). Applications : intégrale de Riemann des fonctions régées. DEV théorème d'Ascoli. Inversion de Fourier dans L^1.

203. Utilisation de la notion de compacité

Références. [Pom94, BMP05, Bré83]

Attention. (rapport de jury) Ne pas faire une leçon sur la notion de compacité.

Commentaire. Beaucoup de résultats d'existence en analyse (de limites, de min, de max, de solutions...) reposent sur des arguments de compacité.

I. Dé nition ;

(1) Compacité métrique : propriété de Bolzano-Weierstrass. Equivaut à Précompact + complet.

(2) Compacité topologique : propriété de Borel-Lebesgue.

II. Applications à la topologie et à l'analyse fonctionnelle.

(1) Théorème d'équivalence des normes en dimension nie

(2) Théorème de compacité de Riesz. Application : montrer que certains espaces sont de dimension nie.

(3) Densité dans $C(K)$: théorème de Stone-Weierstrass

III. Applications au calcul di érentiel et aux équations di érentielles.

(1) Zéros isolés (pour les non analytiques, di injective). Théorème de Hadamard-Levy (caractérisation des di éo de $\mathbb{R}^n$)

(2) Théorème du point xe de Schauder et théorème de Cauchy-Peano-Arzela

IV. Applications en algèbre et géométrie.

(1) Les sous-groupes compacts de $GL(E)$

(2) Isomorphismes de groupes topologiques compacts

V. Illustrations.

204. Connexité. Exemples et applications

I. Notion de connexité.

(1) Dé nitions et caractérisations. Notion de composante connexe.

(2) Connexité par arcs. Equivalence pour les ouverts de $\mathbb{R}^n$ (connexité par arcs a nes, etc.)

II. La connexité dans $\mathbb{R}$.

(1) Les connexes de $\mathbb{R}$ sont les intervalles. Théorème des valeurs intermédiaires, application : Théorème fondamental de l'algèbre.

(2) Applications de la connexité de $\mathbb{R}$: un critère d'analycité.

III. Application de la connexité.

(1) Topologie : classes d'homéomorphisme. Théorème de relèvement, Brouwer en dimension 2.

(2) Calcul di érentiel : Inversion globale à partir de l'inversion locale . Exemple : lemme de non rétraction. Théorème de Hadamard-Levy (dans le cas $\mathbb{C}^2$). Surjectivité de l'exponentielle sur $\mathbb{C}$. Sur $GL(n;\mathbb{C})$.

(3) Groupes classiques. Exemple : $SO(3)$ est connexe. Théorème de Lie-Kolchin.

(4) Localisation des racines : théorème de Gerschgörin précisé (avec la continuité des racines de polynômes) [MM16].

208. Espaces vectoriels normés. Applications linéaires continues.

I. Notion d'espace vectoriel normé.

(1) Dé nition. Tout e.m est isométrique à une partie d'e.v.n. Exemples. Dessins de boule unité.

(2) La dimension nie. Compacité de la boule unité pour la norme sup, application : équivalence des normes en dimension nie. Tout compact convexe symétrique est la b.u. d'une norme. Tout compact convexe d'intérieur non vide est homéomorphe à la b.u. fermée. Application : di érents énoncés du théorème de Brouwer.

(3) Théorème de compacité de Riesz. Application.

II. Espace de Banach.

(1) Dé nition. Théorème de transfert

(2) Théorème de Banach-Steinhaus. Application 1 : normes de l'opérateur d'interpolation. Application 2 : sous-espaces de $C([0;1])$ fermés formés de fonctions régulière. Cas semblable avec hölderiennes ?

(3) Théorèmes de graphe fermé et de l'application ouverte. Application 1 : séries de Fourier, non surjectivité de F sur c_0 [?]. Application 2 [BCL99] supplémentaires topologiques. Thm Grothendieck .

230. Séries de nombres réels et complexes

Références. Pour la base du cours, Arnaudies-Fraysse [AF91]. Pour les exemples et applications : [Duv07, FGN14].

Commentaire. Cette leçon s'oriente avant tout vers la question de la convergence des séries numériques. Plus que la pertinence des exemples, leur bon placement est très important (pas trop tôt). Insister sur la notion d'absolue convergence qui motive l'étdude des séries à termes positifs (II.1). Signaler la parenté avec la théorie des intégrales semi-convergentes : somme en cascade vs identi cation d'une primitive, sommation par paquets vs changement de variable, transformation d'Abel vs intégration par parties.

I. Notion de série numérique.

(1) Dé nitions : sommes partielle, série convergente, divergente, restes. CN$u_n \to 0$, pas su sant, exemple.

(2) Linéarité de la somme

(3) Critère de Cauchy. Par la contraposée : divergence de la série harmonique. Application : séries absolument convergentes

II. Techniques sur les séries numériques.

(1) Séries à termes positifs : comparaison, équivalents. Série de Riemann pour ≤ 1. Application : dev asymptotique (3 termes) de la série harmonique. Formule de Stirling. Critères de Cauchy, d'Alembert, Raab-Duhamel (facultatif)

(2) Regroupement des termes ou sommation par paquets. Série de Riemann pour > 1.

(3) Les séries alternées. Application $\sum (-1)^n/(n + (-1)^n)$ convergente pour $> 1/2$

(4) La transformation d'Abel. Exemple : $\sum \sin n/n$

(5) La comparaison série intégrale. Application 1 : séries de Bertrand. Application 2 : $\sum \sin(\pi\sqrt{n})$. Encadrement des restes. Faire un dessin. La formule sommatoire d'Euler Maclaurin à l'ordre 1.

III. Compléments et applications.

(1) Convergence permutative et convergence absolue [FGN14, AF91]

(2) Quelques inégalités : Hardy, Knopp, Carleman

(3) Représentation des nombres réels. En base $\neq$ [AF91]. Application : ensemble de Cantor. Série de Engel [FGN14, Analyse 1]. Caractérisation des rationnels par le développement en série de Engel, application e est irrationnel.

(4) Approximation dophantienne. Théorème de Liouville reliant le degré d'algébricité à la mesure de transcendance [Duv07]. Application : il existe une in nité non dénombrable de nombres de Liouville.

233. Analyse numérique matricielle

Référence. [BCL99, AK02, Cia98].

Commentaire. Les deux problèmes sont la résolution des systèmes linéaires (au sens exact ou moindres carrés) et la recherche des valeurs propres, mais il ne faut pas croire qu'ils sont indépendants : par exemple signaler l'e et du rayon spectral sur la convergence des méthodes itératives. Ne pas oublier de mentionner des applications (di érences nies par la discrétisation du Laplacien par exemple)

I. Norme matricielles, conditionnement.

(1) Dé nition, exemple, contre-exemple.

(2) Formule du rayon spectral [MMT86]

(3) Conditionnement et systèmes linéaires [AK02]

II. La résolution des systèmes linéaires [AK02].

(1) Rappels sur les méthodes directes : LU, Cholesky, QR. complexité.

(2) Méthode itérative : principe. Jacobi, Gauss-Seidl. Relaxation.

(3) Convergence des méthodes itératives.

(4) Interprétation matricielle de la méthode de gradient à pas constant.

III. Localisation et calcul des valeurs propres.

(1) Lemme d'Hadamard. Disques de Gerschgörin. Version précisée (nombre de valeurs propres à l'aide de th. Rouché + connexité par arcs). Ovales de Cassini. [MM16]

(2) Calcul : méthode de la puissance, puissance inverse. Applications au calcul des racines de polynômes.

234. Espaces L^p

I. Référence. [BCL99]

Commentaire. Comme dans la leçon espaces de fonctions on se concentre sur la complétude (Riesz-Fischer), la recherche de parties denses et la caractérisation des parties compactes (Riesz-Fréchet-Kolmogorov). Brézis considère $L^p(\ )$ où est un ouvert de R^N. C'est un cadre convenable pour la leçon mais il faut savoir le justi er : espaces de Sobolev.

II. I Espaces L^p.

(1) Inégalité de Young. Inégalités de Hölder et de Minkowski.

(2) Espace L^p pour une mesure - nie. Théorème de Riesz-Fischer.

(3) Formes linéaires sur L^p ; la dualité L^p L^{p^0}, re exivité, uniforme convexité ; le cas de L^1. Densité de $C_c(\ )$ dans $L^p(\ )$.

III. II Convolution.

(1) Inégalités de convolution.

(2) Suites régularisantes. Densité de C_c^1 dans L^p.

IV. III Compléments.

(1) Topologie faible. $`^1$ a la propriété de Schur.

(2) Théorème de Riesz-Fréchet-Kolmogorov (avec Ascoli)

235. Problèmes d'interversions de limites et d'intégrales

Commentaire. Plan quelque peu stéréotypé : interversion limite/limite, limite/intégrale, intégrale/intégrale. Sachant que la partie II est le coeur du sujet, et que II et III ont une intersection non vide : les intégrales impropres sont des limites. Cette leçon doit faire sentir progressivement l'e cacité des hypothèses de complétude en analyse.

I. Interversion de limites.

(1) Exemples, contre-exemples.

(2) Convergence uniforme dans un espace de Banach et théorème de la double limite.

(3) Dérivées partielles. Lemme de Schwarz.

II. Interversion de limites et d'intégrales.

(1) Une approche élémentaire : continuité de l'intégrale sur compact.

(2) Convergence monotone et convergence dominée.

(3) Continuité, dérivabilité, holomorphie sous $\mathbb{R}$. Intégrales à paramètres ; transformée de Fourier et de Laplace (une variable).

(4) Retour sur les séries de fonctions.

III. Interversions d'intégrales.

(1) Approche élémentaire : Fubini sur pavé compact.

(2) Fubini-Tonelli, Fubini-Lebesgue.

(3) Intégrales impropres.

IV. IV Applications.

(1) Une application à la théorie des EDL : Expression générale de la résolvante

(2) Une application aux probabilités : le théorème de Polya.

(3) Stabilité de l'espace de Schwarz par transformée de Fourier.

236. Méthodes de calcul d'intégrales

Références. [CLF96]

I. Fonctions de la variable réelle - techniques standard.

(1) Primitive usuelles. Fractions rationnelles ; fractions rationnelles en fonctions trigonométriques.

(2) Intégration par parties. Exemples : intégrales de Wallis. Application à la formule de Stirling.

(3) Changement de variables. Exemples.

(4) Interversion série intégrale. Exemple : $\int_0^1 \frac{\ln x}{x-1} dx$.

II. Méthodes d'analyse complexe.

(1) Applications de la formule de Cauchy homotope

(2) Application de la formule des résidus.

III. Techniques avancées.

(1) Intégrales à paramètre ; transformée de Laplace. Théorèmes taubériens.

(2) Equations di érentielles. Transformée de Fourier de la gaussienne.

(3) Intégrales multiples. Exemple : calcul du volume de lan-boule euclidienne.

246. F Séries de Fourier

Préliminaires. Le groupe topologique $T = R=Z$, est compact et de mesure 1, pour la mesure issue de sur R. On a donc la suite d'inclusions ($1 < p < 1$, $K = R$ ou C)

$$C_K(T) \quad L^1_K(T) \quad L^p_K(T) \quad L^1_K(T): \tag{82}$$

Définition 246.1 $f : R \to K$ est C^k par morceaux si elle est C^k sur $R \setminus D$ où D est fermé discret et si $f^{(k)}$ admet des limites nies à gauche et à droite en tout point de D.

Définition 246.2 Soit $f \in C(T)$, alors f est C^k (resp. C^k par morceaux) si $f_{R \to T}$ est C^k (resp. C^k par morceaux). Elle est C^1 (par morceaux) si C^k (par morceaux) pour tout k.

I. Convolution, convergence des sommes de Fourier.

I.1. Dé nitions.

Définition 246.3 Soit $n \in Z$, on dé nit $e_n : t \mapsto e^{i2nt} \in C^1(T)$. puis, pour $f \in L^1(T)$

$$\forall n \in Z;\ c_n(f) = \int_T f(t)\, e_n(-t)\, dt \tag{83}$$

est le n-ième coe cient de Fourier de f (aussi nôté $\hat{f}(n)$).

Remarque 246.4 Quand f est à valeurs réelles, on utilise plus souvent les coe cients de Fourier trigonométriques $a_n(f) = c_n(f) + c_{-n}(f)$ et $b_n(f) = i(c_n(f) - c_{-n}(f))$ avec $n \in N$.

Exemple 246.5 (Fonction créneau, gure ??) Soit $\in C_{R;pm}(T)$ impaire, valant 1 sur $0; \frac{1}{2}$. Alors $c_0(\ ) = 0$, et pour $n \neq 0$

$$c_n(\ ) = \frac{(-1)^n - 1}{i\,n};\ a_n(\ ) = 0;\ b_n(\ ) = \frac{2[(-1)^n - 1]}{n} \tag{84}$$

Exemple 246.6 (Fonction triangle, gure ??) Soit $\in C \setminus C^1_{pm}(T)$ paire, telle que $(x) = x - \frac{1}{4}$ sur $0; \frac{1}{2}$. Alors $c_0(\ ) = 0$, et pour $n \neq 0$

$$c_n(\ ) = \frac{(-1)^n - 1}{2(n)^2};\ a_n(\ ) = \frac{(-1)^n - 1}{(n)^2};\ b_n(\ ) = 0 \tag{85}$$

I.2. Convolution et noyaux.

Définition 246.7 Soient $f; g \in L^1(T)$. On dé nit $f ? g$ par $\forall x \in T;\ f ? g(x) = \int_T f(t)\, g(x - t)$. On a alors $f ? g \in L^1(T)$.

Proposition 246.8 $(L^1(T); ?)$ est une algèbre de Banach commutative. De plus, nous avons par dé nition

$$\forall f \in L^1(T); \forall n \in Z;\ f ? e_n = c_n(f)\, e_n \tag{86}$$

Autrement dit, e_n est vecteur propre de $f ?$ pour la valeur propre $\hat{f}(n)$.

La suite $\hat{f} \in C^Z$ est bornée par $\|f\|_{L^1}$, et plus précisément :

Proposition 246.9 L'application

$$F : \begin{cases} L^1(T) & \to C^Z_b \\ f & \mapsto \hat{f} \end{cases}$$

est un morphisme continu de C-algèbres de $(L^1(T); ?)$ vers C^Z_b munie du produit terme à terme et de la norme $\|\ \|_1$.

Proposition 246.10 On appelle noyau de Dirichlet D_N et de Féjer K_N à l'ordre N, les polynômes trigonométriques suivants :

$$D_N(t) = \sum_{n=-N}^{N} e_n(t) = \frac{\sin((2N+1)\ t)}{\sin(t)} \tag{87}$$

$$K_N(t) = \frac{1}{N}\sum_{n=0}^{N-1} D_n(t) = \frac{1}{N}\frac{\sin^2(Nt)}{\sin^2(t)} \tag{88}$$

On appelle somme de Fourier (resp. de Fejer) de $f \in L^1(T)$ à l'ordre N, la convolution $S_N(f) = D_N ? f$ (resp. $_N(f) = K_N ? f$). Les sommes de Fejer sont la moyenne de Cesaro des sommes de Fourier.

Remarque 246.11 La famille d'opérateurs $D_N ?$ n'est pas bornée. D'après le théorème de Banach-Steinhaus, il existe $f \in L^1(T)$ telle que $S_N(f)$ diverge en norme L_1. La famille d'opérateurs $_N : f \mapsto S_N(f)(0)$ n'est pas non plus bornée pour f dans $C(T)$.

Théorème 246.12 Si f est continue, alors $_N(f) \to f$ uniformément sur T. Si $f \in L^p(T)$ avec $p < 1$ alors $_N(f) \to f$ en norme L^p.

Remarque 246.13 Le point (i) constitue une preuve e ective du théorème de Weierstrass sur la densité de l'algèbre des polynômes trigonométriques.

Corollaire 246.14 Le morphisme F est injectif.

I.3. Théorème de convergence normale.

Corollaire 246.15 Si la série de terme général $(c_n(f)\,e_n)$ converge normalement, alors sa somme est égale à f dans $L^1(T)$. En particulier, ℓ^1 est contenu dans l'image de F.

Exemple 246.16 Pour la fonction triangle , on a $kc_n(\ )k = O\left(n^{-2}\right)$, donc $S_n(\ ) \to$ uniformément sur T. En particulier $\sum_{n\in Z} c_n(\ ) = (0) = 1=4$, d'où $\sum_{k\geq 1}(2k+1)^{-2} = {}^2=8$.

Définition 246.17 Soit $F \in L^1(R)$; on dé nit sa transformée de Fourier $\hat{F}$ par $\hat{F}(x) = \int_R F(t)\, e^{-2i\pi xt}\, dt$.

Proposition 246.18 (Formule sommatoire de Poisson) Soit $F \in C(R)$ telle que $F(x) = o(x^{-})$ en 1, où > 1. On suppose que $\sum_{n\in Z} \hat{F}(n) < 1$. Alors

$$\sum_{n\in Z} F(n) = \sum_{n\in Z} \hat{F}(n) \tag{89}$$

II. Lemme de Riemann-Lebesgue et conséquences.

II.1. Convergence ponctuelle.

Théorème 246.19 Pour toute $f \in L^1(T)$, $c_n(f) \to 0$ en 1.

Remarque 246.20 F n'est pas surjective sur l'espace S_0 des suites qui tendent vers 0 en 1

Proposition 246.21 (Dirichlet). Soit $f \in L^1(T)$ qui admet en x_0 des limites à droite et à gauche $f(x_0^-)$, et telle que les fonctions $: h \mapsto \frac{1}{h}\left(f(x_0 - h) - f(x_0^-)\right)$ dé nies pour $h > 0$ sont intégrables au voisinage de 0. Alors

$$S_N(f)(x_0) \to \frac{1}{2}\left(f(x_0^+) + f(x_0^-)\right) : \tag{90}$$

Corollaire 246.22 Si f est de la classe C^1 par morceaux et à sauts symétriques, alors $S_N(f) \to f$ simplement sur T.

Exemple 246.23 Pour la fonction créneau , $S_n(\ )(1=4) \to (1=4) = 1$, d'où $\sum_{k\geq 1}(-1)^k=k = = 4$.

Remarque 246.24 La convergence ponctuelle des sommes de Fejer a lieu dès que est réglée, vers la demi-somme des limites à droite et à gauche.

II.2. Régularité et coe cients de Fourier.

Proposition 246.25 Soit $k \geq 2$ N, $f \in C^1_{pm} \cap C(T)$; alors f^0 est dé nie presque partout sur T, de sorte qu'elle dé nit bien une unique classe encore notée f^0 dans $L^1(T)$, et

$$c_n(f^0) = 2i\pi n c_n(f) \tag{91}$$

Exemple 246.26 La fonction créneau est la dérivée de la fonction triangle $\in C^1_{pm} \cap C(T)$. On véri e $c_n(\ ) = 2i\pi n c_n(\ )$

Corollaire 246.27 Si $f \in C^k(T)$, alors $\hat{f}(n) = o(|n|^{-k})$ en $\pm\infty$. Si $\hat{f}(n) = o(|n|^{-k-2})$ alors $f \in C^k(T)$

III. L'espace de Hilbert $L^2(T)$.

III.1. Structure hilbertienne.

Proposition 246.28 $L^2(T)$ est un espace de Hilbert.

$$\forall f \in L^2(T),\ c_n(f) = \int_T f(t)\,\overline{e_n}(t)\,dt = \langle f, e_n\rangle \tag{92}$$

Proposition 246.29 La famille $(e_n)_{n\in\mathbb{Z}}$ est orthonormée. En particulier, si $f \in L^2(T)$ alors $\hat{f} \in \ell^2(\mathbb{Z})$, et

$$\|\hat{f}\|_{\ell^2} \leq \|f\|_{L^2} \tag{93}$$

(inégalité de Bessel)

Corollaire 246.30 Soit $f \in C^1_{pm}(T) \cap C(T)$. Alors la série de terme général $S_N(f)$ converge normalement vers f.

Remarque 246.31 On retrouve sans calcul que $S_n(\ ) \to$ uniformément sur T.

III.2. Théorème de Parseval.

Proposition 246.32 La famille forme $(e_n)_{n\in\mathbb{Z}}$ forme une base hilbertienne de $L^2(T)$. En particulier, F induit un isomorphisme isométrique de $L^2(T)$ sur ℓ^2 (égalité de Parseval).

Exemple 246.33 L'égalité de Parseval appliquée à donne $\sum_{k\geq 1} k^{-4} = \pi^4/90$.

Corollaire 246.34 (Inégalité de Wirtinger). Soit $f \in C^1_{pm} \cap C([0;1];\mathbb{C})$; alors

$$\int_0^1 |f|^2 \leq \left(\int_0^1 f\right)^2 + \frac{1}{2}\int_0^1 |f'|^2. \tag{94}$$

IV. Applications.

IV.1. Sommes de Gauss.

Proposition 246.35 Soit $f \in C^1_{pm} \cap C(T)$; alors

$$\frac{1}{n}\sum_{k=0}^{n-1} f\left(\frac{k}{n}\right) = \sum_{m\in\mathbb{Z}} \hat{f}(mn). \tag{95}$$

Corollaire 246.36 Soit $G_N = \sum_{i=1}^{N-1} e^{\frac{2i\pi n i^2}{N}}$ la N-ième somme de Gauss. Alors :

$$G_N = \frac{1+i^n}{1-i}\sqrt{n}. \tag{96}$$

DEV 21

Remarque 246.37 Si $N = p$ est premier impair, $G_p = \sum_{a\in F_p} \left(\frac{a}{p}\right) \zeta^a$ où $\zeta = e^{2i\pi/n}$. Ceci permet de montrer la loi de réciprocité quadratique.

IV.2. Equation de la chaleur. Soit $u_0 \in C^1_{pm} \setminus C(T)$; on s'intéresse aux solutions $u : T \times \mathbb{R} \to \mathbb{R}$ de l'équation

$$\begin{cases} \frac{\partial u}{\partial t} - 4\frac{\partial^2 u}{\partial x^2} = 0 & (x;t) \in T \times \mathbb{R} \\ u(x;0) = u_0(x) & \forall x \in T \end{cases} \tag{97}$$

DEV 22

Théorème 246.38 Il existe une unique solution à l'équation (97), qui soit continue sur $T \times \mathbb{R}_+$ et C^2 sur $T \times \mathbb{R}_+$. De plus,

(i) Cette solution est C^1 sur $T \times \mathbb{R}_+$.

(ii) Elle dé nie et bornée sur $T \times \mathbb{R}$ si et seulement siu_0 est constante.

(iii) $u(\cdot\,;t) \to c_0(u_0)$ uniformément sur T quand$t \to +1$

Remarque 246.39 La solution de l'équation de la chaleur est donnée par

$$u(\cdot\,;t) = \#(\cdot\,;t) \star u_0 \tag{98}$$

où $\#$ est la fonction theta de Jacobi$\#(z;t) = \sum_{n \in \mathbb{Z}} e^{n^2 t + inz}$

Eléments non traités.

- Noyaux de Gibbs et de Jackson
- Phénomène de Gibbs (au voisinage des discontinuités)
- Etude des opérateurs de convolution dans $L^2(T)$; leur compacité, leurs espaces propres [HL99].

Autres développement possibles.

- Développement eulérien de la cotangente et calcul des premiers (2p)
- Développement en série de Fourier des polynômes de Bernoulli
- Inégalité de Bernstein
- Formule sommatoire de Poisson en lien avec la transformée de Fourier
- Tératologie : Séries de Fourier lacunaires.

Annexe A

Formes quadratiques

Cours de Claudine Picaronny donné en janvier-février 2015 à l'ENS Cachan, rédigé par Gabriel Pallier. Quelques remarques et exercices ont été ajoutés. Toutes les erreurs sont imputables au rédacteur.

301. Formes bilinéaires symétriques

Une référence pour ce cours est le chapitre 5 de [Per96]. Toutefois la portée est ici un peu moins générale. En particulier on se contente d'étudier les formes bilinéaires, et pas les formes hermitiennes, ni les formes alternées.

I. Orthogonalité, dualité. Soient k un corps, E un k-ev de dimension $n < 1$.

Définition 301.1 Une forme bilinéaire symétrique sur E est une application $: E \quad E \to k$ telle que

(99) $\qquad 8(x;y) \in E \quad E; \qquad (x; \quad); \quad (\quad ;y) \quad \in E^{?}$

(100) $\qquad 8(x;y) \in E \quad E \qquad (x;y) = \quad (y;x):$

Une forme bilinaire symétrique dé nit une notion d'orthogonalité : pour tous $x;y \in E$, on écrit $x ? y$ si $(x;y) = 0$. Si $X \quad E$ on écrira

(101) $\qquad X^{?} := f y \in E; \ 8x \in X; x ? yg:$

C'est un espace vectoriel appelé orthogonal de X. De plus, nous avons

(102) $\qquad X^{?} \quad = \quad \setminus_{x \in X} \quad f x g^{?};$

(103) $\qquad \mathrm{Vect}(X) \qquad X^{??}:$

Remarque 301.2 Si l'on n'impose pas la symétrie à il existe a priori deux notions d'orthogonalité, l'une à droite et l'autre à gauche. La relation ? est toutefois symétrique si l'on exige $(x;y) = 0 \ =) \quad (y;x) = 0$ comme dans [Per96].

Définition 301.3 On appelle $E^{?}$ le noyau de , noté ker . Lorsque ker $= f0g$ on dit que est non dégénérée. Le rang de est la codimension de $E^{?}$ dans E.

Remarque 301.4 Une forme bilinéaire symétrique dé nit une application linéaire $\overline{\ }$ de E dans $E^{?}$:

$$\overline{\ }: E \quad ! \quad E^{?}$$
$$x \quad 7! \quad f y \ 7! \ B(x;y)g:$$

Le noyau de $\overline{\ }$ est exactement ker . Si est non dégénérée, $\overline{\ }$ est injectif. Comme nous sommes en dimension nie, $\dim E = \dim E^{?}$ et $\overline{\ }$ est alors bijectif. En résumé, on a un isomorphisme

$$S_2(E) \quad ' \quad L \quad (E; E^{?})$$
$$7! \quad \overline{\ }$$

qui envoie les non dégénérées sur les isomorphismes. Le crochet de dualité est transporté sur .

II. Restriction.

Proposition 301.5. Soit une forme bilinéaire symétrique non dégénérée, un sous-espace vectoriel de . Alors l'application linéaire qui fait commuter le diagramme suivant

$$\begin{array}{ccc} E & \xrightarrow{\ \ } & E^* \\ \| & & \# \\ F & \xrightarrow{\ \ } & F^* \end{array}$$

est un morphisme surjectif de noyau .

Démonstration. est injective, donc (restriction) est surjective, et est surjective donc est surjective. De plus par dé nition

$$\begin{aligned} \ker &= \{x \in E ; \forall y \in F, (x)(y) = 0\} \\ &= \{x \in E ; \forall y \in F, (x,y) = 0\} \\ &= F^\perp . \end{aligned}$$

Corollaire 301.6. Si est non dégénérée, alors pour tout sous espace nous avons
(i) $\dim F + \dim F^\perp = n$
(ii) $F = F^{\perp\perp}$.

Démonstration. (i) est le théorème du rang appliqué à l'application . (ii) est dû à l'inclusion $F \subset F^{\perp\perp}$ et à la complémentarité des dimensions dans .

Proposition 301.7. Soit un sous-espace de . Une forme bilinéaire symétrique sur dé nit par restriction une forme linéaire sur , dont le noyau est $F \cap F^\perp$.

Démonstration. Par dé nition

$$\ker = \{x \in F ; \forall y \in F, (x,y) = 0\} = F \cap F^\perp .$$

Attention. Les formes dé nies positives restent dégénérées quand restreintes à un sous-espace, mais ce n'est pas un fait général pour les formes bilinéaires symétriques non dégénérées. Par exemple $(x,y) = xy$ sur $\mathbb{R}^2$.

III. Isotropie (dé nitions).

Définition 301.8. On dit que est isotrope (pour) si est dégénérée, ce qui équivaut à $F \cap F^\perp \neq \{0\}$. est totalement isotrope si $= 0$, ce qui équivaut à $F \subset F^\perp$.

Remarque 301.9. totalement isotrope $\Rightarrow$ isotrope. Pour une droite vectorielle , les deux notions sont équivalentes.

Définition 301.10. On dit que $x \in E$ non nul est isotrope si Kx est isotrope. x est isotrope ssi $(x,x) = 0$. L'ensemble des vecteurs isotropes (augmenté de) forme un cône appelé cône isotrope de la forme .

Exemple 301.11. $E = k^2$, $(x,y) = x_1y_1 - x_2y_2$. Alors $(x,x) = x_1^2 - x_2^2$; il y a deux droites isotropes

Proposition 301.12. On suppose non dégénérée. Soit un sous-espace de , il y a équivalence entre
(1) est non dégénérée
(2) $F \cap F^\perp = \{0\}$
(3) $E = F \oplus F^\perp$
(4) $^{\perp}$ est non dégénérée.

Démonstration. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1) sont contenues dans les preuves précédentes. Le corollaire 301.6 donne que (2) et (3) sont vraies pour si et seulement si elles sont vraies pour , et donc (2) $\Leftrightarrow$ (4).

IV. Ecriture matricielle. Mise sous carrés. Soit $B = (e_1; \dots : e_n)$ une base de E. Si x et y se décomposent sur cette base sous la forme $x = x_1 e_1 + \quad + x_n e_n$ et $y = y_1 e_1 + \quad + y_n e_n$ alors

$$(x; y) = \sum_{i;j} x_i y_j \quad (e_i; e_j) = {}^t X \left(\quad (e_i; e_j) \right)_{i;j} Y;$$

où X et Y sont les vecteurs colonnes contenant les coordonées de x et y respectivement.

La matrice $S = \left(\quad (e_i; e_j) \right)$ est symétrique. Elle est appelée matrice de la forme bilinéaire symétrique dans la base B. La matrice de sur une base B^0 est alors de la forme

$$S^0 = {}^t P S P;$$

où P est la matrice de passage de B vers B^0 (qui contient en colonne les coordonnées des vecteurs de B dans B^0)

Remarque 301.13 En termes d'action de groupe : $GL(n; k)$ agit par congruence sur $S_n(k)$, via

$$P : S = {}^t P S P:$$

L'ensemble des matrices d'une forme quadratique est une orbite pour cette action : c'est une classe de congruence.

Attention. Ne pas confondre la relation de congruence et celle de similitude.

Une équation du sous-espace $\ker$ dans la base B est

$$\{ y \in E \mid SY = 0 \} = \{ y \in E \mid Y \in \ker S \};$$

où Y contient les coordonnées de y dans B. En particulier, est non dégénérée ssi S est inversible. Dans ce cas, on constate que toutes les matrices de ont un même déterminant modulo k^{*2}.

Définition 301.14 Le discriminant ( ) est la classe du déterminant d'une matrice de , modulo k^{*2}.

Remarque 301.15 Si F est un supplémentaire de $\ker$ alors $_F$ est non dégénérée. On peut alors éventuellement défnir le discriminant de F comme le discriminant de $_F$ (qui ne dépend pas du supplémentaire choisi).

Définition 301.16 La base B est dite orthogonale pour la forme bilinéaire symétrique si la matrice de dans B est diagonale. Ceci équivaut à $(e_i; e_j) = 0$ si $i \neq j$.

Exemple 301.17 $k = F_2$. On considère la forme bilinéaire symétrique de matrice dans la base canonique

$$S = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} :$$

Alors, pour tous $x = x_1 e_1 + x_2 e_2$

$$\begin{matrix} x_1 & x_2 \end{matrix} \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \begin{matrix} x_1 \\ x_2 \end{matrix} = 2 x_1 x_2 = 0:$$

Une telle forme bilinéaire symétrique ne peut pas admettre de base orthogonale.

En fait, la caractéristique 2 est la seule obstruction :

Théorème 301.18 Soit k un corps de caractéristique $\neq 2$. Alors une forme bilinéaire symétrique admet une base orthogonale.

1ère démonstration. Par récurrence sur $n = \dim E$; c'est clair pour $n = 1$.

Si $= 0$ alors toute base est orthogonale pour . Dans le cas contraire montrons le lemme suivant

Lemme 301.19 Si est non nulle, il existe $e \in E$ tel que $(e; e) \neq 0$.

Démonstration. $(e + f; e + f) = (e; e) + 2 \quad (e; f) + \quad (f; f)$. Puisque 2 est inversible dans k, pour tout $x \in E$

$$(x; x) = 0 \implies = 0:$$

Soit donc e tel que $(e;e) \neq 0$ et

$$\begin{aligned} H &= \{ke\}^? \\ &= \{x \in E;\ (x;e) = 0\}. \end{aligned}$$

Alors H est un hyperplan et

$$E = \{ke\} \overset{?}{\oplus} H.$$

On conclut par hypothèse de récurrence.

2ème démonstration : algorithme de mise sous carré de Gauss. Soit une forme bilinéaire symétrique donnée dans les coordonnées par le polynôme homogène de degré 2

$$(x;x) = \sum_i a_i x_i^2 + \sum_{i<j} b_{ij}\, x_i x_j.$$

On cherche à écrire $(x;x) = \sum_i x_i^2$. On procède encore par récurrence sur n.
1er cas : $\exists i; a_i \neq 0$. Quitte à permuter, on peut supposer que c'est a_1. On écrit $(x;x)$ sous la forme $P(x_1;\dots;x_n)$ où P est un polynôme homogène de degré 2 en n indéterminées

$$a_1 x_1^2 + x_1 \sum_{j=2}^{n} b_{1j}\, x_j + Q_1(x_2;\dots;x_n)$$

où Q_1 est un polynôme homogène de degré 2 en $n-1$ indéterminées. On cherche à faire apparaître le début d'un carré :

$$a_1 \left(x_1 + \sum_{j=2}^{n} \frac{b_{1j}}{2} x_j\right)^2 - a_1 \left(\sum_{j=2}^{n} \frac{b_{1j}}{2} x_j\right)^2 + Q_1(x_2;\dots;x_n).$$

Posons $\varphi_1(x_1;\dots;x_n) = x_1 + \sum_{j=2}^{n} \frac{b_{1j}}{2} x_j$. Par hypothèse de récurrence il existe $\varphi_2;\dots;\varphi_r$ formes linéaires en $x_2;\dots;x_n$ linéairement indépendantes et telles que

$$Q_1(x_2;\dots;x_n) = \sum_{k=1}^{r} \lambda_k \varphi_k(x_2;\dots;x_n)^2.$$

Remarque 301.20 La matrice des φ_i dans la base des $dx_i^? = dx_i$ est de la forme

$$T = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ ? & [\varphi_2] & \cdots & [\varphi_r] \end{pmatrix} \begin{matrix} dx_1 \\ \vdots \end{matrix}.$$

2ème cas : a_i est nul pour tout i. Quitte à permuter les variables on peut suppose que $b_{12} \neq 0$ (sinon il n'y a rien à montrer).

$$\begin{aligned} & b_{12} x_1 x_2 + x_1 \sum_{j=3}^{n} b_{1j}\, x_j + x_2 \sum_{j=3}^{n} b_{2j}\, x_j + Q_2(x_3;\dots;x_n) \\ = & \ b_{12} \left(x_1 + \sum_{j=3}^{n} \frac{b_{2j}}{b_{12}} x_j\right)\left(x_2 + \sum_{j=3}^{n} \frac{b_{1j}}{b_{12}} x_j\right) - \frac{1}{b_{12}} \left(\sum_{j=3}^{n} \frac{b_{1j}}{b_{12}} x_j\right)\left(\sum_{j=3}^{n} \frac{b_{2j}}{b_{12}} x_j\right) \\ & + Q_2(x_3;\dots;x_n) \\ = & \ \frac{b_{12}}{4} \left(x_1 + x_2 + \sum_{j=3}^{n} \frac{b_{1j} + b_{2j}}{b_{12}} x_j\right)^2 - \frac{b_{12}}{4} \left(x_1 - x_2 + \sum_{j=3}^{n} \frac{b_{2j} - b_{1j}}{b_{12}} x_j\right)^2 \\ & + Q_3(x_3;\dots;x_n) \end{aligned}$$

où Q_3 est un polynôme homogène de degré 2 en les $n-2$ variables $x_3, \dots, x_n$ que l'on peut mettre sous carrés par hypothèse de récurrence :

$$\varphi_1(x_1, \dots, x_n) = x_1 + x_2 + \sum_{j=3}^{n} \frac{b_{1j} + b_{2j}}{b_{12}} x_j$$

$$\varphi_2(x_1, \dots, x_n) = x_1 - x_2 + \sum_{j=3}^{n} \frac{b_{2j} - b_{1j}}{b_{12}} x_j$$

$$Q(x_1, \dots, x_n) = \sum_{i=3}^{r} \lambda_i \varphi_i(x_3, \dots, x_n).$$

Remarque 301.21 La matrice des φ_i dans la base des $e_i^* = dx_i$ est de la forme

$$T = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 1 & -1 & 0 & \cdots & 0 \\ ? & ? & [\varphi_3] & & [\varphi_r] \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ dx_1 \\ \vdots \end{matrix}$$

V. Orthogonalisation simultanée. La référence est [RDO88] tome 2, pages 35-36.

Théorème 301.22 Soient φ et ψ non dégénérée et $d_\varphi, d_\psi : E \to E^*$ associés. Il existe une base de E à la fois φ-orthogonale et ψ-orthogonale ssi $u = d_\psi^{-1} d_\varphi$ est diagonalisable.

302. Formes quadratiques

A partir d'ici, k est de caractéristique $\neq 2$

I. Définitions.

Définition 302.1 Une forme bilinéaire symétrique définit une unique application $q : E \to k, x \mapsto \varphi(x,x)$ appelée forme quadratique associée à φ.

On a montré plus haut que q caractérise φ (ceci fait l'objet du lemme 19). φ est parfois appelée forme polaire associée à q. On parle de noyau, caractère non dégénéré, discriminant, base orthogonale, matrices... de la forme q comme de sa forme polaire. En fin, on dit que q représente le scalaire λ s'il existe $x \in E$ non nul tel que $q(x) = \lambda$. On désignera aussi occasionnellement le couple (E, q) par E.

Le groupe linéaire de E agit sur l'ensemble des formes quadratiques par

$$\forall u \in GL(E),\ u \cdot q = q \circ u^{-1}.$$

(Le u^{-1} est là pour avoir une action à gauche.) Le stabilisateur de q pour cet action est noté $O(q)$ et appelé groupe orthogonal de q.

Définition 302.2 On dit que deux formes quadratiques q et q' sont équivalentes s'il existe u un automorphisme de E tel que $q \circ u^{-1} = q'$, autrement dit si q et q' sont dans une même orbite pour l'action précédente. L'ensemble des u tels que $q \circ u^{-1} = q'$ forme une classe (à gauche) dans $GL(E)/O(q)$.

Remarque 302.3 Deux formes quadratiques équivalentes représentent les mêmes scalaires. En outre elles possèdent le même ensemble de matrices ; donc la même matrice, dans des bases éventuellement différentes.

Proposition 302.4 Soit R un système de représentants de k^*/k^{*2}. Alors, toute forme quadratique non dégénérée admet une matrice diagonale à coefficients dans R.

Corollaire 302.5 Il y a un nombre fini de classes d'équivalence de formes quadratiques non dégénérées sur E ssi k^{*2} est d'indice fini dans k^*.

II. Classification des formes quadratiques.

II.1. Le cas $k = \mathbb{C}$ (et les corps quadratiquement clos). Il y a une seule classe de formes quadratiques non dégénérées. Les formes quadratiques sont entièrement classifiées par leur rang $r \in \{0, \dots, n\}$. Il existe $n+1$ classes de formes sur $\mathbb{C}^n$.

Remarque 302.6. Ceci est vrai plus généralement, lorsque $k = k^2$, ce qui est toujours valable quand k est algébriquement clos, mais aussi par exemple pour le corps K des nombres complexes constructibles à la règle et au compas (qui est la plus petite extension de $\mathbb{Q}$ dans laquelle chaque élément non nul admet deux racines carrées). De tels corps sont dits quadratiquement clos.

Remarque 302.7. On peut montrer que $\mathbb{C}$ est quadratiquement clos seulement à l'aide des écritures algébriques des nombres complexes : pas besoin de l'exponentielle complexe.

II.2. Le cas $k = \mathbb{R}$ (et les corps euclidiens). On a l'isomorphisme de groupes $\mathbb{R}^* = \mathbb{R}^{*2} \cdot \{\pm 1\}$. Quitte à permuter les vecteurs d'une base orthonormale fournie par la proposition 302.4, toute forme quadratique non dégénérée q admet une matrice de la forme

$$I_{r,s} = \begin{pmatrix} I_r & (0) \\ (0) & -I_s \end{pmatrix}, \quad r + s = n.$$

Définition 302.8. ($k = \mathbb{R}$) Soit q une forme quadratique ; q est dite définie positive si $q(x) > 0$ dès que $x \neq 0$; elle est définie négative si $-q$ est définie positive. On écrit $q > 0$ (resp. $q < 0$) le fait que q est définie positive (resp. négative).

Une forme définie positive est non dégénérée (elle est même anisotrope).

Exemple 302.9. $E = \mathbb{R}^n$, q donnée par

$$q\left(\sum_i x_i e_i\right) = \sum_i x_i^2$$

est appelée forme euclidienne attachée à la base canonique.

Soit q une forme quadratique définie positive. Sur une base orthogonale, elle admet une matrice de la forme $I_{r,s}$. Or, elle ne représente pas -1, donc $s = 0$. Il existe donc une unique classe d'équivalence de formes définies positives.

Proposition 302.10. Soit q une fqnd sur un espace vectoriel réel. Alors il existe un unique couple (r, s) avec $r + s = n$ tel que q admette dans une certaine base la matrice

$$I_{r,s} = \begin{pmatrix} I_r & 0_{r,s} \\ 0_{s,r} & -I_s \end{pmatrix}$$

Précisément

$$r = \max\{\dim F;\ F \text{ sev de } E;\ q_F > 0\}$$
$$s = \max\{\dim F;\ F \text{ sev de } E;\ q_F < 0\}.$$

Remarque 302.11. Cette proposition reste valable si q est non dégénérée, à condition de considérer les matrices

$$I_{r,s,n} = \begin{pmatrix} I_r & (0) & \\ & -I_s & \\ (0) & & 0_{n-r-s} \end{pmatrix}.$$

Pour la preuve, remarquons que l'existence est déjà acquise via le théorème d'existence d'une base orthogonale ; nous voulons seulement montrer l'unicité. Commençons par le

Lemme 302.12. Soient F et G deux sev tels que $q_F > 0$ et $q_G < 0$. Alors $F + G = F \oplus G$, ie F et G sont en somme directe.

Démonstration. Soit $x \in F \cap G$; alors $q(x) > 0$ puisque $x \in F$, mais aussi $q(x) \leq 0$ puisque $x \in G$; donc x est isotrope ; mais puisque $q_F > 0$, $x = 0$.

Soit donc $E = F_0 \oplus G_0$ une décomposition avec $q_{|F_0} > 0$ et $q_{|G_0}$ (on sait qu'une telle décomposition existe). S'il existe un sev F tel que $\dim F > \dim F_0$ et sur lequel q est définie positive, alors en vertu du lemme

$$F + G_0 = F \oplus G_0;$$

donc $\dim F = \dim F_0$, on a démontré l'unicité.

Le nombre de classes de formes sur E est donc exactement le nombre de couples d'entiers naturels $(r;s)$ avec $r+s \leq n$, soit $n(n+1)/2$. Le couple $(r;s)$ est appelé signature de la forme quadratique q. Il s'obtient (par exemple) à l'aide de l'algorithme de mise sous carrés de Gauss.

Remarque 302.13 Il existe une notion de forme définie positive sur tout corps ordonnés ; en outre ces corps sont réels (i.e. -1 n'est pas somme de carrés). Un corps réel k est euclidien si $k^{\times 2}$ est d'indice 2 dans $k^\times$. Sur un corps euclidien, la classification des formes quadratiques est la même que sur $\mathbb{R}$. Par exemple il en est ainsi du corps K_0 des réels constructibles à la règle et au compas.

Remarque : Réduction simultanée de deux formes quadratiques sur un corps euclidien. Il existe un théorème de réduction simultanée pour deux formes quadratiques q et q' si $q > 0$ sur un corps euclidien. En particulier deux formes quadratiques définies positives admettent une base orthogonale (mais pas orthonormée) en commun. Cf, par exemple, [Tau21], exercice 1 du thème XIII (sous forme matricielle).

II.3. Le cas $k = F_q$ (q impair). On sait dans ce cas que $k^\times = k^{\times 2}$ est d'ordre 2. Si α est un non carré de F_q on peut alors prendre $R = \{1, \alpha\}$

Proposition 302.14 Soit q une forme quadratique de rang ≥ 2 sur k. Alors q représente tous les scalaires

Démonstration. Soit $\lambda \in F_q$ quelconque. Dans une base orthogonale pour q on peut écrire

$$q\left(\sum_i x_i e_i\right) = a_1 x_1^2 + a_2 x_2^2 + \cdots$$

et on peut supposer $a_1, a_2 \neq 0$. Les ensembles

$$S_1 = \{a_1 x^2; x \in F_q\}$$
$$S_2 = \{\lambda - a_2 x^2; x \in F_q\}$$

sont tous deux de cardinal $\frac{q+1}{2}$ (car a_1 et a_2 sont non nuls) ; d'après le principe des tiroirs ils possèdent une intersection non vide.

Remarque 302.15 Il s'agit également d'une conséquence directe du théorème de Chevalley-Warning appliqué à q et à λ.

Théorème 302.16 (k corps fini) Soit q une forme quadratique non dégénérée sur E. Alors q admet comme matrice soit I_n, soit

$$\begin{pmatrix} I_n & 0 \\ 0 & \end{pmatrix}$$

et ces deux cas s'excluent mutuellement selon la valeur du discriminant de q. En particulier, les formes sont entièrement classifiées par leur discriminant.

Corollaire 302.17 (k fini) Deux formes quadratiques non dégénérées sont équivalente ssi elles ont même discriminant. En particulier, il y a deux classes d'équivalence par rang.

Démonstration. Par récurrence sur $\dim E$. Pour $n = 1$ c'est toujours vrai (quel que soit le corps d'ailleurs). Soit q un fqnd sur E ; d'après la proposition il existe $v \in E$ tel que $q(v) = 1$. Ainsi

$$E = \langle v \rangle \oplus \langle v \rangle^\perp$$

Corps	Invariants (en dim n)	Nombre de classes d'équivalence
$\mathbb{C}$	rang $r \in \{0, \dots, n\}$	$n+1$
$\mathbb{R}$	signature (r,s) ; $r+s \leq n$	$n(n+1)/2$
$\mathbb{F}_q$	rang et discriminant : r;	$2n+1$
$\mathbb{Q}$	beaucoup (symboles sur les $\mathbb{Q}_p$ etc.)	1

Table 1. Aperçu de la classification des formes quadratiques

Alors $q_{|\mathrm{Vect}(e_1,f_1)^\perp}$ est non dégénérée, et on peut lui appliquer l'hypothèse de récurrence ; de plus

$$q_{|\mathrm{Vect}(e_1,f_1)^\perp} = (-q).$$

II.4. Le cas $k = \mathbb{Q}$. C'est nettement plus difficile que dans les cas précédents ; en effet d'après le théorème fondamental de l'arithmétique

$$\mathbb{Q}^\times = \{\pm 1\} \times \prod_{p \in P} (\mathbb{Z}/2\mathbb{Z})$$

où P est l'ensemble des nombres premiers, de sorte que $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ est infini (et possède même la puissance du continu).

D'après le théorème d'Ostrowski [Col11], toutes les valeurs absolues sur $\mathbb{Q}$ sont la valeur absolue usuelle ou la valeur absolue p-adique

$$|r|_p = 2^{-v_p(r)}$$

et les complétions pour ces valeurs absolue sont $\mathbb{Q}_1 = \mathbb{R}$ et les $\mathbb{Q}_p$ corps p-adiques. La classification des formes quadratiques sur les $\mathbb{Q}_p$ (avec $p \in P \cup \{1\}$) permet en retour la classification sur $\mathbb{Q}$. C'est le principe de Hasse notamment le th. de Hasse-Minkowski [Ser70, Chapitre 4].

$$\begin{array}{ccc} \mathbb{Q}_p & & \mathbb{Q}_1 = \mathbb{R} \\ & \nwarrow & \\ & \mathbb{Q} & \end{array}$$

II.5. Résumé. Le tableau suivant récapitule l'influence du corps de base sur la classification des formes quadratiques dans les cas étudiés

303. Isotropie (car $k \neq 2$)

I. Indice, Lagrangiens. On appellera ici un sous-espace vectoriel totalement isotrope, un *seti* pour abréger. On rappelle que cela signifie $F \subset F^\perp$. Si F est un seti de q, on a nécessairement

$$\dim F \leq \frac{\dim E}{2}.$$

Définition 303.1. On appelle indice de la forme quadratique non dégénérée q et on note $\nu(q)$ le maximum de la dimension d'un seti. Si $\nu(q) = 0$ on dit que q est anisotrope.

Exemple 303.2. $k = \mathbb{R}$, q une forme définie positive. Alors q est anisotrope.

Définition 303.3. Soit (V,q) de dimension paire $2n$. Alors un seti de dimension n est appelé un Lagrangien.

II. Plans hyperboliques.

Définition 303.4. Soit (P,q) un plan. On dit que P est hyperbolique s'il existe une base sur laquelle la matrice de q est

$$J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Proposition 303.5 On a l'équivalence des assertions
(i) P est hyperbolique ;
(ii) q admet la matrice $I_{1;1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$;
(iii) Q est non dégénérée et admet un vecteur isotrope.

Démonstration. Pour l'équivalence (i) $\Leftrightarrow$ (ii) il s'agit de montrer que $I_{1;1}$ et J sont congruentes. On peut aussi remarquer que

$$X^2 - Y^2 = 2xy$$

avec $x = \frac{X - Y}{2}$, $y = X + Y$. Pour (i) $\Rightarrow$ (iii) observons que $\det J = -1 \neq 0$ et donc q est non dégénérée et que les deux vecteurs de base sont isotropes.

Supposons (iii) et soit $e \in P$ isotrope pour q. On note φ la forme bilinéaire symétrique associée à q. Comme q est non dégénérée, il existe $g \in P$ tel que $\varphi(e;g) \neq 0$. Quitte à diviser g par $\varphi(e;g)$, on peut supposer $\varphi(e;g) = 1$, et comme $\varphi(e;e) = 0$, le couple $(e; g + \lambda e)$ forme une base pour tout λ, et vérifie $\varphi(e; g + \lambda e) = 1$. Il reste à trouver λ pour que $q(g + \lambda e) = 1$, mais

$$q(g + \lambda e) = q(g) + \lambda^2 q(e) + 2\lambda = q(g) + 2\lambda$$

donc $\lambda = -q(g)/2$ convient.

Remarque 303.6 Si $k = \mathbb{R}$ (ou un corps euclidien) l'implication (iii) $\Rightarrow$ (ii) est immédiate à la suite de la classification énoncée plus haut q est de rang 2 et elle n'est ni définie positive, ni définie négative. Donc sa signature est $(1;1)$.

Les deux droites isotropes d'un plan hyperbolique sont ses deux Lagrangiens.

III. Espaces hyperboliques.

Théorème 303.7 Soit $(E;q)$ un espace vectoriel muni d'une forme quadratique. Les propriétés suivantes s'équivalent :
(i) E est somme directe de plans hyperboliques (pour les restrictions de q) ;
(ii) q admet l'une des matrices suivantes (où $\sim$ désigne la relation de congruence) :

$$\begin{pmatrix} I_r & 0 \\ 0 & I_r \end{pmatrix} \qquad \begin{pmatrix} 0 & I_r \\ I_r & 0 \end{pmatrix} \qquad \operatorname{diag}(J;\dots;J) :$$

(iii) q est non dégénérée et possède un Lagrangien
On dit alors que $(E;q)$ est un espace hyperbolique.

Remarque 303.8 Cette proposition contient le cas précédent du plan hyperbolique.

Au vu de la preuve précédente, (i) $\Leftrightarrow$ (ii) est clair. (i) $\Rightarrow$ (iii) également : prendre le sous-espace engendré par les premiers vecteurs de base de la deuxième matrice. (iii) $\Rightarrow$ (ii) se démontre par récurrence sur r : le cas $r = 1$ étant acquis, il s'agit d'établir le

Lemme 303.9 Sous l'hypothèse (iii), il existe (e_i) une base du Lagrangien, complétée en $(e_1;\dots;e_n;f_1;\dots f_n)$ telle que pour tous $i;j$ on ait

(104) $$\varphi(e_i;f_j) = \delta_{ij}$$
(105) $$\varphi(f_i;f_i) = \varphi(e_i;e_i) = 0$$

Démonstration. $\operatorname{Vect}(e_1;\dots e_{k-1}) \subset \operatorname{Vect}(e_1;\dots e_k)$ donc

$$\{e_1;\dots e_k\}^\perp \subset \{e_1;\dots e_{k-1}\}^\perp :$$

Ainsi, il existe g dans E tel que $g \in \{e_1;\dots e_{k-1}\}^\perp \cap \{e_1;\dots e_k\}^\perp$, c'est-à-dire que

$$\varphi(g;e_i) = 0 \text{ tant que } i \neq k-1$$
$$\varphi(g;e_k) \neq 0 :$$

Quitte à diviser g par $\varphi(g;e_k)$ on peut supposer $\varphi(g;e_k) = 1$.

$$\forall k \geq 2,\ K,\ (g + e_k, e_k) = 1$$
$$(g + e_k, e_i) = 0 \qquad i \in \{1, \dots, k-1\}.$$

On a $(g + e_k, g + e_k) = q(g) + 2\lambda_k$. Soit donc $\lambda_0 = -q(g)/2$, on pose alors $f_k = g + \lambda_0 e_k$. On vérifie alors les relations (104) et (105)

Ceci achève la preuve du théorème de caractérisation des espaces hyperboliques. En fait, le lemme précédent nous donne un peu mieux, à savoir la

Proposition 303.10 Soit q une forme quadratique non dégénérée sur E. Soit F un sev maximal pour l'inclusion. Alors il existe deux sous espaces vectoriels H et A tels que $E = H \overset{\perp}{\oplus} A$ avec H hyperbolique contenant F comme Lagrangien, et (A, q) anisotrope.

De plus, on a l'unicité de la dimension de H dans une telle écriture. C'est par exemple une conséquence du résultat suivant (théorème de Witt [Per96, Chapitre 8]) que nous ne démontrerons pas :

Théorème 303.11 Soient F et F' deux sous-espaces vectoriels, soit $u : F \to F'$ un isomorphisme tel que $\forall x \in F,\ q(u(x)) = q(x)$. Alors $\exists \theta \in O(q)$ tel que $\theta_{|F} = u$.

En revanche, l'existence de la décomposition $H \overset{\perp}{\oplus} A$ donne le

Corollaire 303.12 (E, q) est hyperbolique ssi il admet un Lagrangien.

Démonstration. Le sens direct découle de la définition. Pour le sens indirect, soit L un Lagrangien. Soit H un sous-espace de dimension $2\dim L$ tel que $q_{|H}$ est hyperbolique (qui existe d'après le lemme 303.9) Alors $\dim H = \dim E$ donc $H = E$ et q est hyperbolique.

Exemple 303.13 q dont une matrice est

$$\begin{pmatrix} 0 & B \\ {}^tB & 0 \end{pmatrix},$$

avec $\det B \neq 0$, est hyperbolique.

IV. Influence du corps de base.

IV.1. Les corps quadratiquement clos.

Lemme 303.14 Une forme quadratique anisotrope est de rang 1.

Démonstration. Tout nombre est un carré !

Proposition 303.15 Soit F un sev im. Soit H hyperbolique admettant F comme Lagrangien. Soit $E = H \overset{\perp}{\oplus} A$ la décomposition de E associée, où q_A est anisotrope. Alors $\dim A$ est le reste de $\dim E$ dans la division par 2.

Corollaire 303.16 $\dim F = \dim(q) = \frac{\dim E}{2}$. De plus il s'agit de la dimension commune de tous les sev im.

IV.2. $k = \mathbb{R}$.

Lemme 303.17 On suppose $k = \mathbb{R}$. Une forme anisotrope est soit définie positive, soit définie négative.

Démonstration. Montrons la contraposée. Soient u et v non nuls tels que $q(u)\,q(v) \leq 0$. On peut supposer que u et v sont linéairement indépendants (sinon ils sont isotropes) et on considère l'ensemble des

$$v_t = (1 - t)\,v + tu$$

qui sont donc tous non nuls. D'après le théorème des valeurs intermédiaires il existe t tel que $v_{t?}$ est isotrope.

Remarque 303.18 C'est aussi une conséquence immédiate de la classification. Une fqnd ni définie positive ni définie négative admet un plan hyperbolique, donc un vecteur isotrope.

Proposition 303.19 Soit F un setim. H un sous-espace hyperbolique admettant F comme Lagrangien et $E = H \perp A$ la décomposition associée. Alors

$$\dim F = \min(r, s)$$

En particulier :
Si $r > s$ alors q_A est définie positive
Si $r = s$ alors $A = \{0\}$ et q est hyperbolique
Si $r < s$ alors q_A est définie négative.

Corollaire 303.20 Tous les setim ont même dimension ; $\delta(q) = \min(r, s)$.

IV.3. Corps finis ($k = \mathbb{F}_\ell$, où ℓ puissance d'un nombre premier impair). On a démontré plus haut qu'une forme quadratique de rang 3 n'est pas anisotrope (conséquence du principe des tiroirs).

Proposition 303.21 Supposons $\dim E$ impaire. Soit F un setim, $E = H \perp A$ la décomposition associée (où F est un Lagrangien de H). Alors

$$\dim F = \frac{\dim E - 1}{2}$$

et A est une droite vectorielle.

Démonstration. $\dim A$ est impair (même parité que $\dim E$) et $\dim A \in \{0; 1; 2\}$.

Le cas de dimension paire est plus délicat :

Proposition 303.22 Supposons $\dim E = 2m$. Il y a deux possibilités
- Soit E est hyperbolique : tous les setim ont dimension m
- Soit E est non hyperbolique, et tous les setim ont dimension $m - 1$.

304. Exercices d'application

I. Mise sous carrés.

Exercice 304.1 Mettre sous carrés le polynôme homogène

$$P(x; y; z; t) = xy + xt + yz + 2zt.$$

Solution.

$$\begin{aligned} xy + xt + yz + 2zt &= (x + z)(y + t) - zt + 2zt \\ &= \frac{1}{4}(x + z + y + t)^2 - \frac{1}{4}(x - y + z - t)^2 + zt \\ &= \frac{1}{4}\left[(x + y + z + t)^2 - (x - y + z - t)^2 + (z + t)^2 - (z - t)^2\right] \end{aligned}$$

En termes matriciels, ceci s'écrit

$${}^tP \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \\ 1 & 0 & 2 & 0 \end{pmatrix} P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Avec

$$P = \frac{1}{2}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{pmatrix}.$$

Exercice 304.2 [Tau94] Soit K un corps $K = \mathbb{R}$ ou $\mathbb{C}$. On pose

$$E(K) = \{(x; y; z) \in K^3; x^2 + 2y^2 + 2z^2 + 2xy + 2xz = 0\}$$

Est-ce que $E(K)$ est un sous-espace vectoriel de K^3 ?

Solution. La mise sous carrés de Gauss donne

$$\begin{aligned} x^2 + 2y^2 + 2z^2 + 2xy + 2xz &= (x + y + z)^2 + (x - y)^2 \\ &= X^2 + Y^2 \end{aligned}$$

avec $X = x + y + z$, $Y = x - y$ et $Z = z$, donc
Si $K = \mathbb{R}$, $E(K)$ est une droite vectorielle (d'équation $X = Y = 0$)
Si $K = \mathbb{C}$, $E(K)$ est l'ensemble d'équation

$$X = \pm iY$$

soit l'union de deux plans vectoriels ; ce n'est pas un sous-espace vectoriel.

II. Formes quadratiques réelles. Signature.

Exercice 304.3 [Tau21] Quelle est la signature de la forme quadratique réelle donnée dans un système de coordonnées par

$$q(x_1, \dots, x_n) = \sum_{i \neq j} x_i x_j$$

Solution 1. Une matrice de cette forme quadratique est

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

Posons

$$P = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & 0 \end{pmatrix} \in GL(n, \mathbb{R}).$$

Alors

$$P^{-1}QP = \begin{pmatrix} n-1 & 0 & \cdots & 0 \\ 0 & -1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & -1 \end{pmatrix}$$

donc la signature de Q est $(1, n-1)$.

Exercice 304.4 Soit, pour tout $A \in M_n(\mathbb{R})$, $q(A) = \operatorname{tr} A^2$. Montrer que q est une forme quadratique sur $M_n(\mathbb{R})$ et déterminer sa signature.

Solution. L'application $(A, B) \mapsto \operatorname{tr}(AB)$ est bien une forme bilinéaire symétrique donc q est une forme quadratique. Ecrivons $M_n(\mathbb{R})$ sous la forme

$$M_n(\mathbb{R}) = S_n(\mathbb{R}) \oplus A_n(\mathbb{R})$$

On considère la base $\mathcal{B}_S$ de $S_n(\mathbb{R})$ formée des $\frac{1}{\sqrt{2}}(E_{ij} + E_{ji})$ et la base $\mathcal{B}_A$ de $A_n(\mathbb{R})$ formée des $\frac{1}{\sqrt{2}}(E_{ij} - E_{ji})$. Dans la base $\mathcal{B} = \mathcal{B}_S \sqcup \mathcal{B}_A$ de $M_n(\mathbb{R})$, la matrice de q est

$$\begin{pmatrix} I_{n(n+1)/2} & \\ & -I_{n(n-1)/2} \end{pmatrix}$$

Donc q est non dégénérée (ce que l'on pouvait voir directement) et de signature $\left(\frac{n(n+1)}{2}, \frac{n(n-1)}{2}\right)$.

Remarque 304.5. L'espace $M_n(R)$ se décompose aussi sous la forme

$$M_n(R) = D_n(R) \oplus T_n^+(R) \oplus T_n^-(R)$$

où $D_n(R)$ est l'espace des matrices diagonales, qui est anisotrope pour q, et $T_n^+(R)$ (resp. $T_n^-(R)$) est l'espace des matrices triangulaires supérieures strictes (resp. inférieures strictes) qui est un Lagrangien de l'espace hyperbolique

$$H = T_n^+(R) \oplus T_n^-(R)$$

III. Isotropie.

Exercice 304.6. [Per96] Soit (P, q) un plan. Montrer que q est hyperbolique ssi P possède exactement deux droites isotropes.

Solution. Si q est hyperbolique, soit (e_1, e_2) une base dans laquelle la matrice de q est J. Alors

$$q(xe_1 + ye_2) = 2xy = 0 \iff x = 0 \text{ ou } y = 0$$

Réciproquement, supposons que q admet exactement deux droites isotropes distinctes $_1$ et $_2$. Soient e_1 et e_2 non nuls pris respectivement dans $_1$ et $_2$ et la forme bilinéaire symétrique associée ; alors $(e_1, e_2) =$ donc quitte à diviser e_1 par la matrice de q dans la base (e_1, e_2) est J.

IV. Matrices symétriques.

Exercice 304.7. Soit A la matrice symétrique réelle dé nie par $a_{i,j} = \min(i, j)$. Montrer que A est dé nie positive.

Solution 1. Par récurrence sur n : c'est visible pour $n = 1$ (et même pour $n = 2$ si l'on veut) puis on pose

$$P = T_{n\ 1;n}(\ 1)$$

On véri e alors que ${}^tP A_n P$ possède une forme diagonale par blocs

$${}^tP A_n P = \begin{pmatrix} A_{n\ 1} & 0 \\ 0 & 1 \end{pmatrix}$$

Solution 2. Soit B telle que $b_{i,j} = 1$ si $j > i$ et 0 sinon, alors on remarque que $A = {}^tBB$.

Exercice 304.8. (Caractéristaion de Sylvester) Soit S une matrice symétrique réelle d'ordre n. Montrer que les conditions suivantes sont équivalentes

(i): S est dé nie positive

(ii): Pour tout $k \in \{1; \dots; n\}$, $_k(S) > 0$, où

$$_k(S) = \det(s_{ij})_{1 \leq i,j \leq k}$$

Solution. Par récurrence sur n :
L'équivalence de (i) et (ii) est clairement valable pour $n = 1$

(i) $\Rightarrow$ (ii) au rang n : Supposons $S \in S_n^{>0}(R)$: Alors $_n(S) > 0$ (c'est le produit des valeurs propres de S) et la sous-matrice formée des $(n\ 1)$ premières lignes et colonnes est encore dé nie positive ; d'après l'hypothèse de récurrence (i) $\Rightarrow$ (ii) au rang $n\ 1$, et $_k(S) > 0$ pour $k \leq n\ 1$, donc (ii).

(ii) $\Rightarrow$ (i) au rang n : S se présente sous la forme

$$S = \begin{pmatrix} S^0 & ? \\ ? & s_{n;n} \end{pmatrix}$$

où $s_{n;n} > 0$. Posons alors

$$P = \begin{pmatrix} 1 & 0 & & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ \frac{s_{n;1}}{s_{n;n}} & 0 & \frac{s_{n;n\ 1}}{s_{n;n}} & 1 \end{pmatrix}$$

Ceci donne

$$SP = \begin{pmatrix} ? & ? \\ 0 & s_{n;n} \end{pmatrix} :$$

Puis, comme S est symétrique,

$${}^tPSP = \begin{pmatrix} S^{00} & 0 \\ 0 & s_{n;n} \end{pmatrix}$$

où S^{00} est dé nie positive (véri er que S^{00} est > 0, cela revient à explrimer $_n > 0$) donc dé nie positive par hypothèse de récurrence. On en déduit ce que l'on souhaitait.

Exercice 304.9 Soit n un entier naturel. Déterminer les composantes connexes par arcs de $S_n(\mathbb{R}) \setminus GL(n;\mathbb{R})$.

Annexe B

Groupes finis

401. Un critère de cyclicité pour les groupes finis

I. Sous-groupes des groupes cycliques. Les groupes cycliques sont les groupes monogènes finis[1]. Ce sont, à isomorphisme près, les groupes $\mathbb{Z}/n\mathbb{Z}$. Rappelons qu'en vertu du lemme de Bezout $\mathbb{Z}/n\mathbb{Z}$ est engendré par la classe de $a \in \mathbb{Z}$, pour tout a premier à n. En conséquence $\mathbb{Z}/n\mathbb{Z}$ possède exactement $\varphi(n)$ générateurs, où φ est la fonction indicatrice d'Euler.

Si la classe des groupes cyclique n'est pas stable par produit direct[2], elle l'est toutefois par passage au sous-groupe et par quotient[3].

Remarque 401.1. On prendra garde à ce qu'un groupe G peut ne posséder que des sous-groupes et quotients propres cycliques sans l'être pour autant : par exemple le groupe symétrique S_3 a des sous-groupes propres isomorphes à $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$. Ceci est encore faux même si l'on suppose G abélien ; ainsi, $(\mathbb{Z}/p\mathbb{Z})^2$ a tous ses sous-groupes propres cycliques sans l'être pour autant.

Lemme 401.2. Soit d un diviseur de n. Alors $\mathbb{Z}/n\mathbb{Z}$ possède un unique sous-groupe H_d d'ordre d. En conséquence, il existe exactement $\varphi(d)$ éléments d'ordre d, et[4]

$$n = \sum_{d \mid n} \varphi(d) \tag{106}$$

Démonstration. Soit $\pi : G \to G$ qui à x associe $d \cdot x = x + \cdots + x$; π est un morphisme. Si H_d et H_d' sont deux sous-groupes de cardinal d, alors par le théorème de Lagrange $H_d, H_{d'} \subset \ker \pi$. Il reste à voir que $|\ker \pi| = d$; pour cela on peut relever π en $\overline{\pi} : \mathbb{Z} \to \mathbb{Z}$ et constater que $|\mathrm{Im}\ \pi| = |d\mathbb{Z}/n\mathbb{Z}| = n/d$.

Pour l'identité (106), on peut séparer les éléments de $\mathbb{Z}/n\mathbb{Z}$ selon leur ordre :

$$n = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} 1 = \sum_{d \mid n} \sum_{\langle x \rangle = H_d} 1 = \sum_{d \mid n} \varphi(d)$$

II. Enoncé du critère de cyclicité. Le critère de cyclicité suivant énonce une réciproque du lemme précédent :

Proposition 401.3. Soit G un groupe fini. On suppose que pour tout entier d, il existe au plus d éléments x tels que $x^d = 1$ dans G. Alors, G est cyclique.

Remarque 401.4. D'après le théorème de Lagrange, les seuls entiers d tels que l'équation $x^d = 1$ admette des solutions sont diviseurs de $n = |G|$.

Remarque 401.5. L'hypothèse de finitude de G est importante. En effet, $\mathbb{Z}^2$ n'a aucun élément d'ordre fini plus grand que 2 ; mais il n'est pas monogène pour autant.

---

1. Pour certains auteurs, $\mathbb{Z}$ est aussi un groupe cyclique.
2. Rappelons que d'après le lemme chinois, $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z}$ est cyclique si et seulement si n et m sont premiers entre eux
3. Soit $G \simeq \mathbb{Z}/n\mathbb{Z}$ avec $n > 1$. Soit $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ le morphisme de surjection canonique. Alors $G' = \pi^{-1}(G)$ est un sous-groupe de $\mathbb{Z}$ qui contient $\ker \pi = n\mathbb{Z}$, ie $G' = m\mathbb{Z}$ avec $m \mid n$.
   Si H est un quotient de $\mathbb{Z}/n\mathbb{Z}$, notons φ la projection $\mathbb{Z}/n\mathbb{Z} \to H$; alors $\varphi \circ \pi$ est un morphisme surjectif de $\mathbb{Z}$ vers H. Il s'ensuit que $H \simeq \mathbb{Z}/m\mathbb{Z}$. L'inclusion $\ker(\varphi \circ \pi) \supset \ker \pi$ implique par ailleurs $m \mid n$.
4. On peut traduire l'égalité suivante comme suit : l'identité de $\mathbb{N}$ est la transformée de Möbius de l'indicatrice d'Euler

Le cas d'application le plus important est sans doute le

Corollaire 401.6. Si k est un corps commutatif, alors tout sous-groupe fini de $k^?$ est cyclique. En particulier, nous avons l'isomorphisme

$$F_p^? \simeq \mathbb{Z}/(p-1)\mathbb{Z}$$

En effet, les éléments d'ordre d dans $k^?$ sont contenus dans l'ensemble des racines de $X^d - 1$, qui est au plus de cardinal d.

III. Preuves du critère de cyclicité.

III.1. Par l'identité (106). Soit G tel que dans la proposition. Pour tout d un diviseur de n, on note $\psi(d)$ le nombre d'éléments de G qui ont pour ordre exactement d.

S'il existe x d'ordre d dans G, alors tous les éléments $x^{d'}$ du groupe $H = \langle x \rangle$ vérifient $x^{d'd} = 1_G$; donc H contient tous les éléments d'ordre d', pour d' divisant d. Par ailleurs $H \simeq \mathbb{Z}/d\mathbb{Z}$, donc il y a exactement $\psi(d')$ éléments d'ordre d'.

Finalement, on trouve que

$$\psi(d) \in \{0, \psi(d)\}$$

Comme on peut encore écrire

$$n = \sum_{d|n} \psi(d)$$

La comparaison de cette écriture avec (106) conduit à $\psi(d) = \varphi(d)$ pour tout d. En particulier, $\psi(n) = \varphi(n) > 0$, et il existe un élément d'ordre n : G est cyclique.

III.2. Une autre preuve dans le cadre abélien. On fera ici l'hypothèse supplémentaire que G est abélien

Lemme 401.7. Soient x et y d'ordres respectifs a et b dans G abélien. On suppose que a et b sont premiers entre eux. Alors xy est d'ordre ab.

Démonstration. D'une part $(xy)^{ab} = x^{ab}y^{ab} = 1$; donc l'ordre de xy divise ab; d'autre part pour tout $r \in \mathbb{Z}$, on a que

$$(xy)^r = 1_G \Rightarrow (xy)^{ra} = 1_G \Rightarrow x^{ra}y^{ra} = 1_G \Rightarrow b \mid ra \Rightarrow b \mid r$$

Le même raisonnement montre que $a \mid r$ et ainsi, l'ordre de xy est ab.

Remarque 401.8. On voit ainsi facilement que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est cyclique quand $(a, b) = 1$. En effet, $(\overline{1}, \overline{1})$ est d'ordre ab, donc c'est un générateur.

Proposition 401.9. Soit N le ppcm des ordres des éléments du groupe G. Alors il existe un élément x d'ordre N dans G.

Démonstration. Ecrivons $N = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$; pour tout i entre 1 et s il existe $x_i \in G$ d'ordre $p_i^{\alpha_i} m_i$ avec $p_i \nmid m_i$. Posant $y_i = x_i^{m_i}$, l'ordre de y_i est $x_i^{\alpha_i}$. D'après le lemme précédent itéré, $x = x_1 \cdots x_s$ est d'ordre N.

Tout ce qui précède s'applique à n'importe quel groupe abélien ; le nombre N est appelé exposant. Il reste à voir que si G vérifie les hypothèses du critère 401.3, alors x est un générateur de G. Tous ses éléments de G vérifiant alors $x^N = 1_G$ on a nécessairement $|G| \leq N$, donc $|G| = |\langle x \rangle|$ et finalement $G = \langle x \rangle$.

IV. Remarques.

IV.1. Sous-groupes multiplicatif d'un corps. On a vu que tout sous-groupe du groupe multiplicatif d'un corps k est cyclique. C'est le cas, en particulier, du groupe des racines n-ièmes de l'unité. Une conséquence est le

Corollaire 401.10. Soit k un corps commutatif. Alors le groupe $\mu_n(k)$ des racines n-ièmes de l'unité dans $k^?$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$, pour un certain d divisant n.

Démonstration. On se place dans le corps K de décomposition du polynôme $P = X^n - 1$ sur k. P étant primitif, ses racines dans K sont toutes distinctes (on peut le constater en calculant le pgcd de P et P'). Il y en a donc n. Maintenant, $\mu_n(k)$ est un sous-groupe de $\mu_n(K) \simeq \mathbb{Z}/n\mathbb{Z}$.

Le résultat est déjà très bien connu dans $\mathbb{C}$, où l'on obtient les racines à l'aide de l'exponentielle complexe. Dans $\mathbb{F}_p$, il donne le critère suivant :

Proposition 401.11 Soit p un nombre premier et d un entier. Alors

$$\#\mu_d(\mathbb{F}_p) = \begin{cases} \{1\} & \text{si } d-p \quad 1 \\ \mathbb{Z}/d\mathbb{Z} & \text{si } d \mid p \quad 1 \end{cases}$$

Il faut prendre garde au fait que le corollaire devient faux si l'on remplace k par un corps gauche (ie, non commutatif). Par exemple, le groupe H des quaternions, d'ordre 8, n'est pas cyclique (et pas même abélien). Le défaut ne vient pas de ce que $H^\times$ n'est pas abélien, mais bien du fait que H n'est pas commutatif ; ainsi le polynôme $X^4 \quad 1$ admet 8 racines dans H.

En particulier, attention à la fausse preuve suivante du théorème de Wedderburn : Soit k un corps fini ; $k^\times$ est fini, donc $k^\times$ est cyclique, donc abélien, donc k est commutatif !

On a bien sûr besoin de l'hypothèse de commutativité de k pour affirmer que $k^\times$ est cyclique.

IV.2. Hypothèse de finitude. L'hypothèse de finitude est importante. En effet $\mathbb{Z}^2$ possède 0 éléments d'ordre d, pour tout d. Pour autant, il n'est pas monogène.

402. Produit semi-direct, dévissage

Thèmes : : Décomposition des groupes, classification des groupes finis

Outils : : Action de groupe, théorèmes de Sylow

Références : : [Per96], [FG94]

I. Le produit HK. Soit G un groupe, H et K des sous-groupes. Il est en général faux que la partie

$$HK = \{hk \mid h \in H,\ k \in K\}$$

est un sous-groupe. De même, rien ne garantit a priori que[5] $HK = KH$.

Toutefois, ces deux particularités sont équivalentes

Proposition 402.1 HK est un sous-groupe si, et seulement si, $HK = KH$

Démonstration. Si HK est un groupe, il est stable par passage à l'inverse. Pour tous $h \in H$ et $k \in K$, $(hk)^{-1} = k^{-1}h^{-1}$ et cet élément est dans KH, donc $HK \subset KH$; par ailleurs, soient $k \in K$ et $h \in H$. Alors $(kh)^{-1}$ est dans HK, donc kh est dans HK. Finalement $HK = KH$.

Maintenant, si $HK = KH$, alors pour tous $h, h' \in H$ et $k, k' \in K$, remarquons que $(hk)^{-1} \in HK$ et il existe h'', k'' tels que

$$(hk)(h'k') = h(kh')k' = h(h''k'')k' = (hh'')(k''k') \in HK$$

Donc, HK est un groupe (et KH aussi).

En outre, nous savons dénombrer les parties HK et KH :

Proposition 402.2 Soient H et K des sous-groupes finis. Alors

$$\#HK = \#KH = \frac{\#H \ \#K}{\#H \cap K}$$

En particulier, si $\#H$ et $\#K$ sont premiers entre eux, $\#HK = \#H \ \#K$.

5. Soit $H = \{\mathrm{Id}, (12)\}$ et $K = \{\mathrm{Id}, (13)\}$ dans le groupe symétrique S_3. On vérifie que

$$HK = \{\mathrm{Id}, (12), (13), (321)\} \text{ et } KH = \{\mathrm{Id}, (12), (13), (123)\}$$

et que ces deux parties de S_3 ne sont pas des groupes (elles sont de cardinal 4 qui ne divise pas 6).

Démonstration. Considérons l'application de multiplication

$$\begin{aligned} : H \quad K &! \quad HK \\ (h;k) &7! \quad hk \end{aligned}$$

Voyons que les bres de cette application sont de cardinal $jH \setminus K j$. Soit $x 2 HK$, on peut écrire $x = h_0k_0$ avec $(h_0;k_0) 2 H \quad K$. Maintenant

$$hk = h_0k_0 \quad () \quad hk = h_0k_0 \quad () \quad h_0{}^{1}h = k_0k^{1}$$

Par conséquent, pour tout $h 2 H$, il existe k tel que $hk = x$ si et seulement si $h_0{}^{1}h 2 K$, ie $h 2 h_0(H \setminus K)$; et dans ce cas k est uniquement déterminé par $k = h^{1}x$. On obtient ainsi la formule demandée.

En particulier, si les cardinaux $jH j$ et $jK j$ sont premiers entre eux, d'après le théorème de Lagrange le seul cardinal possible de $H \setminus K$ est 1 ; par conséquent $jHK j = jH jjK j$ dans ce dernier cas.

II. Critère de décomposition en produit direct.

Théorème 402.3. Soient H et K deux sous-groupes de G tels que[6] $[H;K] = f1g$ et $H \setminus K = f1g$. Alors $HK = hH;K i$ et on a l'isomorphisme de groupes

$$HK ' H \quad K$$

En particulier, si G est ni et si $jGj = jH jjK j$ alors $G ' H \quad K$.

Démonstration. Soient H et K tels que dans l'énoncé. D'après la proposition précédente, puisque $[H;K] = f1g$ on a en particulier $HK = KH$, donc HK est un groupe. HK est contenu dans $hH;K i$ et contient H et K ; donc $HK = hH;K i$. On véri e de plus que l'application est un isomorphisme.

Remarque 402.4. $[H;K] = f1g$ implique que $hkh^{1} = k$ pour tout $k 2 k$ (et $khk^{1} = h$ pour tout $h 2 H$), donc en particulier

$$H \quad \mathrm{Norm}_G(K) \quad \text{et} \quad K \quad \mathrm{Norm}_G(H)$$

Dès que l'on sait qu'un sous groupe N est distingué dans G, il est donc intéressant de chercher le noyau K du morphisme de l'opération par conjuguaison $G \quad N$. Si G est ni et si K est de cardinal $jGj = jN j$, en vertu de la proposition précédente, $HK = G$ et on obtient alors une décomposition de G en produit direct.

II.1. Application : sous-groupe du groupe multiplicatif d'un corps. On se propose de retrouver ici un résultat obtenu à l'aide du critère de cyclicité :

Lemme 402.5. Soit G un sous-groupe du groupe multiplicatif d'un corps. Les p-sous-groupes de G sont cycliques.

Démonstration. Soit P un p-sous-groupe de G, d'ordre p . Notons p l'exposant de P. Alors, les éléments de P véri ent tous $x^{p} = 1$; ce sont donc tous des racines de $X^{p} \quad 1$. Mais ce polynôme est de degré p ; nous avons donc $p = p$, et P est cyclique.

En particulier, les p-Sylow de G sont tous cycliques. Comme G est abélien, il est produit direct de ses p-Sylow. Or ceux ci sont d'ordres premiers entre eux. Donc G est cyclique.

III. Produit semi-direct.

6. Rappelons que $[H;K]$ est par dé nition le sous-groupe de G engendré par les $hkh^{1}k^{1}$ avec $h 2 H$ et $k 2 K$.

III.1. Dé nition interne . Soient N et K des sous-groupes de G. Comme dans les hypothèses du théorème, on suppose que K normalise N et que $N \setminus K$ est trivial ; toutefois, on ne suppose pas a priori que l'action par conjuguaison de H sur N est triviale. Celle-ci se fait par automorphismes, qui sont intérieurs du point de vue de G mais peuvent être extérieurs du point de vue de H.

Le groupe NK est toujours un sous-groupe de G, égal à $hN; K i$ mais non isomorphe a priori à $N \quad K$ (à part quand l'action $H \quad N$ est triviale). On dit que NK est un produit semi-direct de N et de K. Si G est ni et si K est d'indice jNj, on dit que $G = NK$ est une décomposition de G en produit semi-direct.

Exemple 402.6 (Groupe diédral). Soit $n > 3$, on note D_{2n} le groupe des isométries du [7] n-gone régulier dans le plan a ne euclidien. D_{2n} contient un sous-groupe R cyclique d'ordre n, qui est le groupe des rotations. R est normal dans G, d'indice 2 (c'est le noyau du déterminant de l'application orthogonale associée, ou bien si l'on préfère, de la signature des permutation des sommets associées). Si s est une symétrie, s est d'ordre 2 et engendre un groupe S d'ordre 2, qui lui n'est pas distingué dans G, ni même normalisé par R. Regardons l'action par conjugaison $S \quad R$; celle-ci conjugue les rotations en leur inverse, autrement dit l'automorphisme intérieur $' _s \ 2 \ \mathrm{Int}\ (G)$, restreint à R, est l'automorphisme d'inversion $r \ 7! \ r^{\ 1}$ (toujours présent dans un groupe commutatif). Nous avons donc une décomposition en produit semi-direct non direct $D_{2n} = RS$.

III.2. Dé nition externe . Soient N et H deux groupes, et $' : H \ ! \ \mathrm{Aut}\ (N)$ une action de H sur N. On pose $G = N \ o_{'} \ H$, et on appelle produit semi-direct de N et H relativement à $'$, l'ensemble $N \quad H$ muni de la structure de groupe donnée par

$$(n; h) \ (n^0; h^0) = (\ n \ (h{:}n^0) \ ; hh^0)$$

Par exemple, le groupe diédral D_{2n} est dé ni par

$$D_{2n} = Z=nZ \ o_{'} \ Z=2Z$$

où $' : Z=2Z \ ! \ \mathrm{Aut}\ (Z=nZ)$ est le morphisme qui envoie le générateur de $Z=2Z$ sur $g \ 7! \ g^{\ 1}$.

On retrouve le cas du produit direct lorsque $\mathrm{Im}' = f\mathrm{Id}_G g$. Il n'existe pas forcément de produit semi-direct non direct entre N et H ; c'est par exemple le cas quand jGj et $j\mathrm{Aut}\ (N)j$ sont premiers entre eux (car alors, toute action de H sur N par automorphismes est triviale). Ceci motive l'étude générale des groupes d'automorphismes, en particulier ceux des groupes simples.

IV. Isomorphismes entre produits semi-directs. On rencontre parfois l'écriture $G = N \ o \ H$ sans mention de $'$; cette écriture peut être ambigüe, sauf quand par exemple il n'existe qu'un seul morphisme non trivial de H vers $\mathrm{Aut}\ (N)$; on signi e alors implicitement que le produit n'est pas direct. Il peut aussi se produire que deux produits semi-directs selon des morphismes di érents soient en fait isomorphes. La proposition suivante donne un critère simple d'isomorphisme pour les produits semi-directs :

Proposition 402.7. Soient $'; \ $ des opérations de H sur N qui di èrent d'un automorphisme au départ, c'est-à-dire qu'il existe $\ 2 \ \mathrm{Aut}\ (H)$ tel que

$$' = \ $$

Alors, les produits semi-directs $N \ o \ H$ et $N \ o_{'} \ H$ sont isomorphe, via l'application donnée sur les couples par

$$\begin{aligned} : \ N \ o_{'} \ H \ &! \quad N \ o \quad H \\ (n; h) \ &7! \quad (n; \ (h)) \end{aligned}$$

En particulier, si tous les morphismes non triviaux de H vers $\mathrm{Aut}\ (N)$ di èrent d'un automorphisme au départ, la notation $N \ o \ H$ ne désigne qu'une seule classe d'isomorphismes de groupes.

7. du ou d'un n-gone régulier ? On s'autorise ici à dire du car le n-gone est une gure de géométrie semblable

Démonstration. Calculons

$$\begin{aligned}(n;h)\,(n';h') &= (n;\ (h))(n';\ (h')) \\ &= (n\ \ (h)(n');\ (h)\ \ (h')) \\ &= (n'\ (h)(n');\ (hh')) \\ &= [(n;h)(n';h')]\ :\end{aligned}$$

Exemple 402.8 Il existe deux morphismes non triviaux de $Z=3Z$ vers $Z=6Z\ '\ \mathrm{Aut}\ (Z=7Z)$: $'$ qui envoie 1 sur 2 et $\ $ qui envoie 1 sur 4. Les deux produits semi-directs $Z=7Z\ o_{'}\ Z=3Z$ et $Z=7Z\ o\ \ Z=3Z$ sont en fait isomorphes, via $\ = '\ \ $ avec $\ :x\ 7!\ x^{\ 1}$.

Proposition 402.9 Soient $'$, $\ $ des opérations de H sur N conjuguées à l'arrivée, c'est-à-dire qu'il existe $u\ 2\ \mathrm{Aut}\ (N)$ tel que

$$8x\ 2\ H;\ '\ (x) = u^{\ 1}\ \ (x)\ \ u$$

Alors, les produits semi-directs $N\ o\ \ H$ et $N\ o_{'}\ H$ sont isomorphes, via l'application donnée sur les couples par

$$:\ N\ o_{'}\ H\ \ !\ \ \ N\ o\ \ H$$

Remarque 402.10 Si N et H sont commutatifs et si G est un produit semi-direct non direct de N par H, G n'est pas commutatif. Toutefois, on peut avoir isomorphisme entre un produit direct et le produit semi direct correspondant, si N ou H n'est pas supposé abélien. Ainsi, on a l'isomorphisme

$$S_3\ \ Z=2Z\ '\ \ S_3\ o\ Z=2Z$$

car S_3 n'a pas d'automorphisme extérieur.

V. Suites exactes courtes et produit semi-direct. Soit une suite exacte courte de groupes

$$1\ !\ \ N\ !\ \ G\ !\ \ H\ !\ \ 1$$

On dit que G est une extension de N par $H\ '\ G=N$.

Supposons qu'il nous soit donné un groupe G et que nous cherchions à le décomposer, c'est-à-dire à l'écrire comme un produit direct ou semi-direct. On suit alors à peu de choses près les 3 étapes suivantes :

V.1. Rechercher des sous-groupes distingués N dans G. Pour rechercher des sous-groupes, on dispose de plusieurs outils : citons, par exemple

(1) La recherche du centre

(2) Le calcul de la suite centrale

(3) Le calcul de la suite dérivée

(4) Les théorèmes d'existence de Sylow (si le groupe est ni)

(5) Le théorème d'existence de p-sous-groupes (si G est un p-groupe)

Pour montrer la distinction, on peut utiliser l'un des critères de distinction suivant :

Proposition 402.11 Soit G un groupe, H un sous-groupe

(i) Si H est central il est distingué dans G, et si $H = Z(G)$ le quotient n'est pas monogène, sauf s'il est trivial

(ii) Si H est d'indice 2, il est distingué dans G

(iii) Si G est ni, si H est d'indice p où p est le plus petit diviseur premier de jGj, alors H est distingué dans G

(iv) Si H contient le sous-groupe dérivé $D(G) = [G;G]$, il est distingué (et le quotient est abélien).

(v) Si H est l'unique p-sous-groupe de Sylow de G, il est distingué[8] dans G

8. Et même, caractéristique dans G. En fait, on montre plus généralement qu'un sous-groupes de Hall (ie, un sous-groupe dont l'indice dans G est premier à l'ordre) est caractéristique dès qu'il est distingué dans G.

Démonstration. (i) est immédiat, puisque $Z(G)$ est par définition l'ensemble des éléments fixes dans l'action $G \times G \to G$ par conjuguaison. En outre, supposons que $H = Z(G)$ et que G/H est monogène avec H central. Alors il existe $t \in G$ dont la classe engendre G/H tel que l'on puisse écrire

$$G/H = \{t^k H\}_{k \in \mathbb{N}}$$

à présent, si g et g' sont deux éléments quelconques de G, nous pouvons écrire

$$gg' = t^k h t^{k'} h' = t^{k+k'} hh' = t^{k'} h' t^k h = g'g$$

finalement $G = Z(G)$ et l'extension est triviale.

Dans le cas (ii), nous voyons que si $g \in G \setminus H$, $gH = Hg = G \setminus H$. Donc H est distingué.

Pour (iii), remarquons que $p \leq q$, où q est le plus petit diviseur du cardinal de H. On écrit ensuite l'action par transation à gauche de H sur l'ensemble des classes G/H, ce qui donne

$$p = \sum_{\omega \in H \setminus (G/H)} |\omega|$$

Or les cardinaux des orbites divisent q ; et l'une d'entre elle au moins (celle de la classe nulle) est réduite à un élément. Donc toutes les orbites sont de cardinal 1 ; l'action est triviale, et le noyau du morphisme $\varphi : H \to S_{G/H}$ est total. Or

$$\ker \varphi = \bigcap_{g \in G} gHg^{-1}$$

Donc H est distingué dans G.

Une dernière manière de montrer que H est distingué est de chercher un système générateur dont tous les éléments sont distingués.

V.2. Rechercher une section. C'est souvent l'étape la plus délicate. Notons que même l'existence d'un sous-groupe distingué n'a en général aucune raison de donner lieu à une suite exacte scindée. Citons par exemple le cas de H_8 :

$$1 \to \{\pm 1\} \to H_8 \to (\mathbb{Z}/2\mathbb{Z})^2 \to 1$$

Le sous-groupe $\{\pm 1\}$ est distingué dans H_8 (c'est son centre) mais ne donne lieu à aucun produit semi-direct non direct (puisque $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z})$ est trivial) ; or H_8 est non abélien donc il ne s'écrit pas sous la forme $\mathbb{Z}/2\mathbb{Z} \times H$ où H est abélien.

V.3. Etudier l'opération par conjuguaison de H sur N. Dans l'idéal, celle-ci est triviale et nous avons une décomposition en produit direct. Citons un lemme facile à obtenir et très utile dans ce sens

Lemme 402.12 Soit G un groupe fini, N un sous-groupe de G d'ordre p, où p est le plus petit facteur premier de G. Alors, si N est distingué dans G, il est central. En particulier, si la suite

$$1 \to N \to G \to G/N \to 1$$

admet une section, alors G est un produit direct $N \times H$.

On obtient ainsi par exemple la

Proposition 402.13 Soit G un groupe abélien fini, alors G est produit direct de ses sous-groupes de Sylow

Démonstration. Par récurrence sur le nombre de facteurs premiers

- Si G est un p-groupe, le résultat est évident.

- Sinon, $|G| = pq$. Par hypothèse de récurrence, G contient un sous-groupe H d'ordre q qui est produit direct de ses p'-Sylow pour $p' \neq p$. Par ailleurs d'après le théorème de Sylow, G contient un p-Sylow S. Comme les cardinaux sont premiers entre eux, $H \cap S = \{1\}$, $HS = G$ et par commutativité de G, $G \simeq S \times H$.

Remarque 402.14 En particulier, si tous les sous-groupes de Sylow de G sont cycliques, G est cyclique. On retrouve ainsi que tout sous-groupe ni de $k^?$ est cyclique : si S est l'un de ses p-Sylow, avec S d'ordre p , S contient un élément d'ordre p (sinon, tous ses éléments sont racines de $X^{p-1} - 1$, ce qui constitue une absurdité).

Remarque 402.15 Plus généralement, les groupes ni qui sont produits directs de leurs sous-groupes de Sylow sont nilpotents (nis). Nous étudierons les groupes nilpotents plus loin.

403. Quelques groupes d'automorphismes.

Soit $\in \mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$. Dans $(\mathbb{Z}/p\mathbb{Z})^n$ tous les éléments sont d'ordre divisant p donc ce groupe abélien est muni d'une structure d'espace vectoriel sur $\mathbb{F}_p$; véri ons que est $\mathbb{F}_p$-linéaire : soit $\in \mathbb{F}_p$ et $x \in (\mathbb{Z}/p\mathbb{Z})^n$, alors $f(\cdot x) = f(x + \cdots + x) = f(x) + \cdots + f(x) = \cdot f(x)$.

Remarque 403.1 Plus généralement, tout morphisme entre deux groupes abéliens d'exposant p est encore un morphisme pour la structure vectorielle. On s'en resservira dans la suite.

On se propose de calculer les groupes d'automorphismes de V_4, S_3, D_4 (dihédral d'ordre 8), $\mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z}$ et H_8.

(i): $G = V_4$: D'après la remarque précédente, $\mathrm{Aut}(G) \simeq GL(2; \mathbb{F}_2) \simeq S_3$

(ii): $G = S_3$: Les transposition sont les seuls éléments d'ordre 2 et un automorphisme préserve l'ordre ; il permute donc les transpositions. Ceci entraîne que tout automorphisme est intérieur ; et ainsi $\mathrm{Aut}(G) \simeq S_3/Z(S_3) \simeq S_3$.

(iii): $G = D_4$: Le groupe D_4 est d'indice 2, donc distingué, dans D_8 et l'action de ce dernier par automorphismes intérieurs dans D_4 se factorise par le centralisateur de D_4 dans D_8, dont on véri e que c'est $\{1\}$.

Remarque 403.2 Si $n > 2$ on peut montrer que

$$\mathrm{Aut}(D_n) \simeq \mathbb{Z}/n\mathbb{Z} \rtimes_{\mathrm{id}} \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) :$$

(iv): $G = H_8$. Ecrivons $G = \{1; i; j; k\}$ avec les règles de calcul habituelles $i^2 = j^2 = k^2 = 1$, $ij = k$. Posons S l'ensemble

$$S = \{ i \quad j \quad k\}$$

formant les sommets d'un cube dans l'espace des quaternions purs. Le groupe des automorphismes de H_8 agit sur S via

$$\cdot : (i + j + k) = \cdot (i) + \cdot (j) + \cdot (k) :$$

Comme le sous-groupe $\{1\}$ de H_8 est caractéristique (c'est le sous-groupe dérivé, ou encore, le centre) il est stable, donc xe (puisque de groupe d'automorphismes trivial) par $\mathrm{Aut}(H_8)$. Par conséquent l'action $\mathrm{Aut}(H_8)$ S passe au quotient de S par $\{1\}$ et induit une action sur l'ensemble des diagonales de S, que l'on peut encore indexer par les sommets d'un tétraèdre régulier :

$$= \overline{i + j + k}; \overline{i \quad j \quad k}; \overline{\quad i \quad j + k}; \overline{\quad i + j \quad k}$$

On a donc un morphisme

$$: \mathrm{Aut}(H_8) \to S \simeq S_4$$

est injectif puisque $\{i; j; k\}$ forme un système de générateur de H_8 ; Déjà, $\mathrm{Aut}(G)$ contient comme sous-groupe $\mathrm{Int}(G) \simeq G/Z(G) \simeq V_4$. Par ailleurs, $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ agit sur $\{i; j; k\}$ par permutations circulaires, et cette action s'étend en un plongement dans $\mathrm{Aut}(G)$. Les deux groupes ci-dessus engendrent A_4 . Considérons maintenant $\cdot : H_8 \to H_8$ tel que $\cdot(1) = 1$; $\cdot(\quad 1) = \quad 1$; $\cdot(\quad i) = \quad j$; $\cdot(\quad j) = \quad i$ et $\cdot(\quad k) = \quad k$. On véri e que $\cdot$ est un automorphisme de H_8 qui induit une permutation circulaire (donc impaire) de . On en déduit que est un automorphisme, et $\mathrm{Aut}(H_8) = S_4$.

G	V_4	S_3	D_4	H_8
$\mathrm{Aut}(G)$	S_3	S_3	D_4	S_4
$\mathrm{Out}(G)$	S_3	1	$\mathbb{Z}/2\mathbb{Z}$	S_3

Table 1. Automorphismes de groupes de petits ordres. On donne aussi le groupe $\mathrm{Out}(G)$ des (classes d') automorphismes extérieurs.

404. Groupes de petits ordres

I. Groupes d'ordre 12. Dans tout ce qui suit, G est un groupe d'ordre 12. On raisonne par analyse-synthèse. D'après les théorèmes de Sylow nous savons que le nombre n_2 de 2-Sylow divise 3 et est impair ; donc $n_2 \in \{1, 3\}$. D'autre part le nombre de 3-Sylow divise 4 et est congru à 1 modulo 3, donc $n_3 \in \{1, 4\}$.

I.1. 1er cas : Il existe un unique 2-Sylow. Soit D le 2-Sylow de G et T un 3-Sylow. Comme D et T sont de cardinaux premiers entre eux, $D \cap T$ est trivial, et $G = DT$. De plus, D est distingué dans G donc G est un produit-semi-direct de D et T. En vertu de la classification des groupes d'ordre 4, nous savons que $D \simeq \mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Dans le premier cas $\mathrm{Aut}(G) \simeq (\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$ et tout morphisme de T vers $\mathrm{Aut}(D)$ est trivial ; alors $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et d'après le lemme chinois G est cyclique. Dans le second cas, $\mathrm{Aut}(G) \simeq \mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$; si $\varphi : T \to \mathrm{Aut}(D)$ est un morphisme, alors soit il est trivial auquel cas $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, soit c'est un plongement dont l'image correspond au sous-groupe A_3. Il existe deux tels plongements et ils diffèrent d'un automorphisme (l'inversion) au départ, ce qui donne les produits semi-directs isomorphes entre eux et $G \simeq V_4 \rtimes \mathbb{Z}/3\mathbb{Z}$.

I.2. 2e cas : Il existe trois 2-Sylow. Il ne peut pas y avoir 4 groupes de 3-Sylow, car ceux ci ne s'intersectant qu'en l'identité cela ferait 8 éléments d'ordre exactement 3 ce qui ne laisse que 4 éléments d'ordre 1, 2 ou 4 ce qui n'est pas assez pour trois 2-Sylow. Donc le 3-Sylow T est unique, et il est distingué dans G. Si D est un sous-groupe de 2-Sylow, comme son indice est égal à l'ordre de T, $G = TD$ et G est un produit semi-direct de T par D. Si D est isomorphe à V_4 alors les morphismes de D vers $\mathrm{Aut}(T) \simeq \mathbb{Z}/2\mathbb{Z}$ sont classifiés dans $M_{1;2}(\mathbb{F}_2)$ qui est d'ordre 4 ; tous ceux qui sont non triviaux diffèrent d'un automorphisme au départ, et donnent la classe de groupes G_4. En fin, si D est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ alors écrivons $D = \{1, s, s^2, s^3\}$ et $\mathrm{Aut}(T) = \{\mathrm{id}, t\}$; il existe un unique morphisme non trivial de D vers $\mathrm{Aut}(T)$, qui donne la classe de groupes G_5.

I.3. Classes d'isomorphismes. Les groupes G_1, G_2, G_3, G_4, G_5 sont bien deux à deux non isomorphes car à chaque fois caractérisés par le nombre ou les classes d'isomorphismes de leurs sous-groupes de Sylow. Il reste à faire le lien avec les groupes particuliers :

(1) Géométriquement, A_4 s'identifie au groupe des isométries du tétraèdre et le sous-groupe des doubles transpositions s'identifie alors au sous-groupe formé par l'identité et les renversements ayant pour axes les droites passant par le milieux de deux arêtes opposées. Donc $A_4 \simeq G_3$.

(2) Dans $S_3 \times \mathbb{Z}/2\mathbb{Z}$, il y a bien 3 deux Sylow isomorphes à V_4 ; ce sont les groupes engendrés par $(\tau, \bar{0})$ et $(1, \bar{1})$ où τ est une transposition. Donc $S_3 \times \mathbb{Z}/2\mathbb{Z} \simeq G_4$; par ailleurs il s'agit là du groupe des isométries d'un prisme à base triangulaire. Remarquons en outre que tous les groupes du type $S_3 \rtimes \mathbb{Z}/2\mathbb{Z}$ sont encore isomorphes à ce groupe.

(3) Le groupe dihédral D_{12} possède plusieurs sous-groupes isomorphes à V_4 ; ce sont ceux engendrés par deux réflexions d'axe orthogonaux. Donc $D_{12} \simeq G_4$

I.4. Conclusion. Il existe cinq groupes d'ordre 12 à isomorphisme près ; ce sont

$$G_1 : \mathbb{Z}/12\mathbb{Z}$$
$$G_2 : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$
$$G_3 : V_4 \rtimes \mathbb{Z}/3\mathbb{Z} \simeq A_4$$
$$G_4 : \mathbb{Z}/3\mathbb{Z} \rtimes V_4 \simeq S_3 \times \mathbb{Z}/2\mathbb{Z} \simeq D_{12}$$
$$G_5 : \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$$

où V_4 est le groupe de Klein $(\mathbb{Z}/2\mathbb{Z})^2$; tous les poduits semi-directs des trois dernières lignes ne désignant à chaque fois qu'une seule classe d'isomorphisme.

II. Groupes d'ordre 18. Soit G un groupe d'ordre 18, T un 3-Sylow ; il est d'indice 2 donc distingué dans G, et si s est un élément d'ordre 2 (qui existe d'après le lemme de Cauchy) alors $G = T \langle s \rangle$, G est produit semi-direct de T par s. Conformément à la classi cation des groupes d'ordre p^2, T est soit cyclique soit isomorphe à $(\mathbb{Z}/3\mathbb{Z})^2$.
1er cas : $T \simeq \mathbb{Z}/9\mathbb{Z}$. Il existe deux morphismes de $\mathbb{Z}/2\mathbb{Z}$ vers $\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z})$, le morphisme trivial et celui qui à $\bar{1}$ associe $t \mapsto t^{-1}$. Il donnent les classes de groupes

$$G \simeq \mathbb{Z}/18\mathbb{Z}$$
$$G \simeq \mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

2e cas : $T \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. D'après l'exercice 1.4.1, $\mathrm{Aut}(G) \simeq \mathrm{GL}_2(\mathbb{F}_3) \simeq S_4$. Si $\varphi : \mathbb{Z}/2\mathbb{Z} \to S_4$ est un morphisme, l'image de $\bar{1}$ est d'ordre divisant 2, donc 1 ou 2.

(1) $\varphi(\bar{1}) = \mathrm{id}$: φ est trivial, $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

(2) $\varphi(\bar{1})$ est une transposition de S_4. Tous les morphismes de ce type di èrent d'un automorphisme intérieur de S_4 à l'arrivée ; on désignera cette classe d'isomorphisme par

$$G \simeq (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes_1 \mathbb{Z}/2\mathbb{Z}.$$

(3) $\varphi(\bar{1})$ est une double transposition. Tous les morphismes de ce type di èrent d'un automorphisme intérieur de S_4 à l'arrivée ; on désignera cette classe d'isomorphisme par

$$G \simeq (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes_2 \mathbb{Z}/2\mathbb{Z}.$$

Il reste à voir que les deux derniers sous-cas donnent des produits semi-directs qui ne sont pas isomorphes.
Conclusion. Il y a 5 classes d'isomorphisme de groupes d'ordre 18 : deux abéliens, trois non abéliens qui s'écrivent comme produits semi-directs non directs.

Annexe C

Algèbre e ective

601. Interpolation

Ce chapitre aborde l'interpolation polynômiale au sens de Lagrange. On y décrit une application à un procédé de partage de secret. Des aspects de la complexité de l'opération d'interpolation ainsi que leurs conséquences sont également évoqués.

I. Principe de l'interpolation de Lagrange. Soient k un corps, n un entier naturel non nul tel que $n \leq \#k$ (au sens large). On se donne $x_1, \dots, x_n$ des éléments de k distincts. Notons E l'espace vectoriel des polynômes de degré $\leq n-1$ à coe cients dans k, et $\varphi_i : P \mapsto P(x_i)$ la forme linéaire d'évaluation en x_i.

Théorème 601.1. Avec les hypothèses et notations précédentes, la famille $\Phi = (\varphi_1, \dots, \varphi_n)$ forme une base de E^*. De plus, la base antéduale de E est la famille $L = (\ell_i)$ des polynômes de Lagrange

$$\ell_i(X) = \prod_{j \neq i} \frac{X - x_j}{x_i - x_j} \tag{107}$$

En particulier, pour tout n-uplet $(y_1, \dots, y_n) \in k^n$, il existe un unique $P \in E$ appelé interpolateur aux points (x_i, y_i) tel que $P(x_i) = y_i$ pour $1 \leq i \leq n$. Ce polynôme est donné par

$$P(X) = \sum_{i=1}^{n} y_i \ell_i(X) \tag{108}$$

Démonstration. On véri e directement $\langle \ell_i, \varphi_j \rangle = \delta_{i,j}$ pour tous $1 \leq i, j \leq n$, ce qui prouve à la même occasion que (φ_i) et (ℓ_i) sont de rang n, donc des bases respectives de E^* et E.

Dans la suite, on écrira

$$L_{x_1,\dots,x_n}(Y_1, \dots, Y_n, X) = \sum_{i=1}^{n} \ell_i Y_i$$

Il s'agit de l'élément de $k[Y_1, \dots, Y_n, X]$ de degré partiel $n-1$ en X qui se spécialise dans $k[X]$ en les interpolateurs aux (x_i, y_i).

Le calcul de l'interpolateur est implémenté à l'aide de Sage dans l'algorithme 2. Il s'applique à deux listes de scalaires x et y de longueur n pour lesquels il renvoie l'unique interpolateur de degré $\leq n-1$.

Figure 1. Interpolation de Lagrange pour $k = \mathbb{R}$
$[x_i] = [-2, -1, 0, 1, 2, 3]$ et $[y_i] = [4, 0, 8, 3, 9, 7]$

II. Une application au partage de secret.

```
def Lagrange(x,y):
    n = len(x)
    K = x[0].parent().fraction_field()
    var('X') ; R = PolynomialRing(K,'X')
    Interpolateur = R(0)
    # Application de la formule (108)
    for i in range(n):
        l = range(n) ; l.remove(i)
        P = prod((X-R(x[j]))/(x[i]-x[j]) for j in l)
        Interpolateur += y[i]*P
    return Interpolateur

sage: L = Lagrange([1,2,3],[2,5,4]) ; L.expand()
-2*X^2 + 9*X - 5
sage: L.substitute(X=2)
5
```

Algorithme 2 : (Sage) Interpolateur de Lagrange

II.1. Principe. Un chef pirate a caché dans sa jeunesse un trésor sur une île déserte perdue quelque part dans un océan assimilé à un plan affine P sur le corps k (supposé assez grand). Sur son lit de mort, il décide de le léguer à son équipage formé de N pirates novices. Cependant, connaissant la mortalité élevée dans le métier et afin d'éviter que l'un des pirates ne trahisse les $N-1$ autres pour s'emparer seul du trésor, il souhaite que celui-ci ne puisse être retrouvé que par un sous-ensemble quelconque d'au moins n pirates, où $N-n$ est petit devant N. Le chef pirate établit donc un repère de P, l'identifiant ainsi à k^2 et un polynôme $P \in k[X]$ de degré $n-1$ tel que $P(0)$ est l'abscisse et $P(1)$ l'ordonnée[1] de l'île du trésor sur la carte ; puis il confie sa carte à son équipage, et individuellement au pirate i le couple $(x_i ; P(x_i))$ avec les x_i distincts et $x_i \neq 0 ; 1$. Ainsi, les pirates ne pourront retrouver P par interpolation que s'ils sont au moins n à partager leur information.

II.2. Fiabilité. Ce sytème possède un léger inconvénient : $n-1$ pirates avisés et déterminés peuvent quand même situer le trésor sur une droite D. Voici comment ils peuvent s'y prendre : les $n-1$ pirates commencent par calculer

$$V(T) = L_{x_1;\dots;x_{n-1};0}(y_1;\dots;y_{n-1};T;1).$$

Puis ils tracent la courbe d'équation $v = V(u)$ sur la carte (en coordonnées $(u;v)$). Nécessairement le trésor est sur la courbe. Mieux :

Proposition 601.2 $\deg_T V = 1$

Démonstration. Introduisons le polynôme $U(T) = L_{x_1;\dots;x_{n-1};1}(y_1;\dots;y_{n-1};T;0)$. Alors, U et V sont dans $k[T]$ et $U \circ V = V \circ U = T$. Par conséquent, $(\deg U)(\deg V) = 1$.

Ainsi, les pirates peuvent naviguer le long de la droite $D : v = V(u)$ et espérer trouver le trésor au bout d'un temps raisonnable.

Toutefois, le système est totalement inefficace au-delà[2] puisqu'on montre que $n-2$ pirates ne pourront pas retrouver le trésor : d'après le théorème d'interpolation 601.1, pour tout $(u;v)$ dans le plan P, il existe un polynôme P qui interpole les données des $n-2$ pirates et tel que $P(0) = u$, $P(1) = v$.

III. Interpoler, évaluer, multiplier.

1. Par exemple, en choisissant d'abord P de degré $n-1$ aléatoire (au moins si k est infini, cela ne doit pas poser de problème théorique), puis en ajoutant à P une correction affine.

2. Signalons quand même que si k est infini (typiquement si on imagine $k = \mathbb{Q}$ ou $\mathbb{R}$), le choix d'une variable aléatoire pour P peut se réveler délicat. D'abord puisqu'il n'y a pas de loi uniforme ; ensuite parce qu'une information même limitée sur cette variable (par exemple, une borne) de la part des pirates peut aider un petit nombre d'entre eux à estimer P sous des informations partielles.

III.1. *Interpolation, évaluation et division euclidienne.* Evaluer P en $x_1;:::;x_n$, c'est calculer les restes R_i dans la division euclidienne de P par $X \quad x_i$. D'après le lemme chinois des restes, ceci revient encore à calculer P modulo $= (X \quad x_1) \quad (X \quad x_n)$. Ceci peut éventuellement servir pour calculer modulo un polynôme séparable S donc on sait décrire facilement les racines dans une extension de décomposition K de S sur k.

Exemple 601.3. Soit à calculer le reste R du polynôme $P = (\cos + (\sin)X)^n$ de $\mathbf{R}[X]$ modulo $X^2 + 1$. On évalue P en les racines de $X^2 + 1$, à savoir i et i dans $\mathbf{C}$. On trouve $P(i) = e^{in} = \cos n + ni\sin$, $P(i) = e^{in} = \cos n \quad ni\sin$, puis par interpolation

$$R(X) = \cos n + (\sin n)X:$$

Il faut prendre garde à la description de l'extension de décomposition K en question que l'on utilise pour mener les calculs. Si celle-ci est uniquement décrite comme un corps de rupture, la simplification apportée peut être faible, voire illusoire puisqu'on doit quand même mener des divisions euclidiennes. Dans l'exemple précédent, c'est l'existence de l'exponentielle complexe qui joue un rôle important.

Remarque 601.4. L'interpolation, est donc un isomorphisme de $k[X]=( )$ décrit comme une somme directe des $k[X]$-modules simples $k[X]=(X \quad x_i)$, vers E. Ceci revient aussi à munir E d'une structure de $k[X]$-module E . Pour tout $P \ 2 \ k[X]$ et $Q \ 2 \ E$, $P:Q$ est l'unique solution du problème d'interpolation

$$8i; \ P:Q(x_i) = P(x_i)\,Q(x_i):$$

III.2. *La complexité de l'interpolation.*

Définition 601.5. On appelle $\mathrm{CI}(n)$ la complexité en temps[3] du calcul complet de $L_{x_1;:::x_n}$ pour une entrée $fx_1;:::x_ng$ (ou, de manière équivalente, le calcul de tous les $_i$ associés aux x_i).

Proposition 601.6. $\mathrm{CI}(n)$ *vérifie*

$$\mathrm{CI}(n) = O \ n^3 \ : \tag{109}$$

Démonstration. L est la donnée des P^i. Si (f_j) est la base de $E^?$ duale de la base des X^j pour E alors on peut écrire $'_i = \quad x_i^j f_j$. Le calcul des $_i$ est donc équivalent à l'inversion de la matrice de terme général $a_{i;j} = x_i^j$, d'ordre n à coefficients dans k (il s'agit d'une matrice du type de Vandermonde). L'algorithme de Gauss-Jordan effectue cette inversion en temps cubique.

Une fois connus les polynômes de Lagrange $_i$, le calcul d'un interpolateur aux $(x_i;y_i)$ par la formule 108 est de complexité n^2 . En termes matriciels, cela correspond au produit du vecteur ligne $(y_1;:::y_n)$ par la matrice contenant les $_i$ dans la base X^j . Notons qu'il n'est toutefois pas nécessaire de calculer les polynômes de Lagrange si on souhaite seulement évaluer l'interpolateur en $x \ 2 \ k$ donné : on peut spécialiser complètement L, ce qui donne $L_{x_1;:::x_n}(y_1;:::y_n;x) = \sum_{i=1}^{n} y_i \prod_{j\neq i} \frac{x \quad x_j}{x_i \quad x_j}$. Il s'agit d'un calcul qui demandera sans raffinements $3n(n \quad 1) + n \quad 1 = O \ n^2$ opérations dans le corps de base.

Sans surprise, l'interpolation de $P \ 2 \ k[X]$ de degré $n \quad 1$ à partir de n de ses valeurs est en général plus difficile que le problème inverse, à savoir l'évaluation de P en n points qui s'effectue, par exemple, à partir des écritures en schéma de Hörner

$$a_n \ _1 x_i^{n \ 1} + \quad + a_0 = a_0 + x(a_1 + x(a_2 + \quad)) \tag{110}$$

en temps global quadratique. Toutefois, si les x_i sont pris de manière adéquate, et en particulier quand ils forment un sous-groupe cyclique[4] de k , les deux problèmes d'interpolation et d'évaluation se retrouvent considérablement simplifiés, principalement pour deux raisons :

3. On compte ici les opérations (additions, multiplications, calcul d'inverse) dans le corps de base. Il s'agit d'un modèle relativement réaliste si k est un corps fini. Si $k = \mathbf{Q}$ ou $\mathbf{R}$ avec une précision des flottants fixée, une approche modulaire doit permettre de s'en approcher.

4. $E = E_{X^n \ 1}$ n'est alors plus seulement un $k[X]$-module, c'est plus précisément un $k[X]=(X^n \quad 1)$-module, en fait le $k[\mathbf{Z}=n\mathbf{Z}]$-module régulier ou encore la représentation régulière de $\mathbf{Z}=n\mathbf{Z}$. Les opérations

(1) Le calcul des x_i^j est redondant.

(2) L'inversion de la matrice de terme général x_i^j n'est plus un problème ; un calcul direct montre que si $x_i = \omega^i$ où ω est racine n-ième de l'unité

$$\mathcal{F}_i(X) = \frac{1}{n}\sum_{l=1}^{n} x_i^{-l} X^l. \tag{111}$$

L'équation (111) exprime que l'évaluation et l'interpolation en des racines de l'unité sont des problèmes équivalents. L'algorithme de transformée de Fourier rapide (que nous ne décrirons pas plus précisément ici) tire parti de ces fait. Il permet notamment de rapporter la multiplication de deux polynômes à un problème de complexité $\mathcal{O}(n \log n)$ où n est le maximum des degrés.

d'évaluation (resp. d'interpolation) s'identifient à des passages de la base canonique de $L^2(\mathbf{Z}/n\mathbf{Z})$ à la base formée par les caractères de ce groupe ; ce sont ainsi des transformations de Fourier (resp. transformation de Fourier inverse).

Bibliographie

[AF91] J.M Arnaudies and H. Fraysse. *Cours de mathématiques*. classes préparatoires et premier cycle universitaire. Dunod, 1991.

[AHZ14] Martin Aigner, K.H. Hofmann, and Günter M. Ziegler. *Proofs from THE BOOK*. SpringerLink : Bücher. Springer Berlin Heidelberg, 2014.

[AK02] G. Allaire and S.M. Kaber. *Algèbre linéaire numérique*. Mathématiques pour le 2e cycle. Ellipses, 2002.

[AM04] E. Amar and É. Matheron. *Analyse complexe*. Enseignement des mathématiques. Cassini, 2004.

[Aud12] M. Audin. *Géométrie (L3M1)*. Enseignement SUP-Maths. EDP Sciences, 2012.

[BCL99] Haïm Brézis, P.G. Ciarlet, and J.L. Lions. *Analyse fonctionnelle : théorie et applications*. Collection Mathématiques appliquées pour la maîtrise. Dunod, 1999.

[BMP05] V. Beck, J. Malick, and G. Peyré. *Objectif Agrégation*. H&K, 2005.

[Bou07] N. Bourbaki. *Algèbre : Chapitre 4 à 7*. Algèbre. Springer Berlin Heidelberg, 2007.

[Bré83] H. Brézis. *Analyse fonctionnelle : théorie et applications*. Collection Mathématiques appliquées pour la maîtrise. Masson, 1983.

[CDO08] John H. Conway, Heiko Dietrich, and E. A. O'Brien. Counting groups : gnus, moas, and other exotica. *Math. Intelligencer*, 30(2) :6–18, 2008.

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

[Che14] Gaëtan Chenevier. Théorie algébrique des nombres – cours de m1, ecole polytechnique, 2013–2014.

[Cia98] P.G. Ciarlet. *Introduction à l'analyse numérique matricielle et à l'optimisation*. Collection Mathématiques appliquées pour la maîtrise. Dunod, 1998.

[CL05] A. Chambert-Loir. *Algèbre corporelle*. École polytechnique : Mathématiques. École Polytechnique, 2005.

[CLF96] A. Chambert-Loir and S. Fermigier. *Exercices de mathématiques pour l'agrégation : Analyse 3*. Number v. 3 in Agrégation de mathématiques. Masson, 1996.

[Col11] P. Colmez. *Éléments d'analyse et d'algèbre (et de théorie des nombres)*. Mathématiques (École polytechnique (France))). Éd. de l'École Polytechnique, 2011.

[Dem08] M. Demazure. *Cours d'algèbre*. Nouvelle bibliothèque mathématique. Cassini, 2008.

[DTLQ14] G.M. Díaz-Toca, H. Lombardi, and C. Quitté. *Modules sur les anneaux commutatifs : cours et exercices*. Mathématiques en devenir. Calvage & Mounet, 2014.

[Duv07] D. Duverney. *Théorie des nombres : cours et exercices corrigés*. Sciences SUP. : Mathématiques. Dunod, 2007.

[Eid09] Jean-Denis Eiden. *Géométrie analytique classique*. Tableau noir. Calvage & Mounet, 2009.

[Eis45] G. Eisenstein. Applications de l'Algèbre à l'Arithmétique transcendante. *J. Reine Angew. Math.*, 29 :177–184, 1845.

[Elk02] R. Elkik. *Cours d'algèbre*. Mathématiques pour le 2e cycle. Ellipses Marketing, 2002.

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

[FGN14] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Exercices de mathématiques des oraux de l'École polytechnique et des Écoles normales supérieures*. Enseignement des mathématiques. Cassini, 2008–2014.

[GKP94] R.L. Graham, D.E. Knuth, and O. Patashnik. *Concrete Mathematics : A Foundation for Computer Science*. A @foundation for computer science. Addison-Wesley, 1994.

[GP10] Victor Guillemin and Alan Pollack. *Di erential topology*. AMS Chelsea Publishing, Providence, RI, 2010. Reprint of the 1974 original.

[GT96] Stéphane Gonnord and Nicolas Tosel. *Topologie et analyse fonctionnelle : thèmes d'analyse pour l'agrégation*. Number v. 1 in CAPES-agrég mathématiques. Ellipses, 1996.

[GT98] Stéphane Gonnord and Nicolas Tosel. *Calcul di érentiel*. Thèmes d'analyse pour l'agrégation :. Ellipses, 1998.

[Hal76] Marshall Hall. *The Theory of Groups*. AMS Chelsea Publishing Series. AMS Chelsea Pub., 1976.

[Hin08] Marc Hindry. *Arithmétique : Primalité et codes, Théorie analytique des nombres, Equations diophantiennes, Courbes elliptiques*. Tableau noir. Calvage & Mounet, 2008.

[HL99] F. Hirsch and G. Lacombe. *Eléments d'analyse fonctionnelle : cours et exercices avec réponses*. Enseignement des mathématiques. Dunod, 1999.

[HL12] D. Hernandez and Y. Laszlo. *Introduction à la théorie de Galois*. Ecole polytechnique, 2012.

[Isa08] I.M. Isaacs. *Finite Group Theory*. Graduate studies in mathematics. American Mathematical Society, 2008.

[Mer06] Jean-Yves Merindol. *Nombres et algèbre*. Collection Grenoble Sciences. EDP Sciences, 2006.

[Mil78] John Milnor. Analytic proofs of the "hairy ball theorem" and the brouwer fixed point theorem. *The American Mathematical Monthly*, 85(7) :521–524, 1978.

[MM16] Roger Mansuy and Rached Mneimné. *Algèbre linéaire : Réduction des endomorphismes*. Vuibert, 2016.

[MMT86] R. Mneimne, R. Mneimné, and F. Testard. *Introduction à la théorie des groupes de Lie classiques*. Collection Méthodes. Hermann, 1986.

[Per96] D. Perrin. *Cours d'algèbre*. CAPES-agrég mathématiques. Ellipses, 1996.

[Pom94] Alain Pommellet. *Cours d'analyse*. Ellipses, 1994.

[QZ02] H. Que□élec and C. Zuily. *Eléments d'analyse*. Agrégation de mathématiques. Dunod, 2002.

[RDO88] Edmond Ramis, Claude Deschamps, and Jacques Odoux. *Algèbre*. Cours de mathématiques spéciales : classes préparatoires et enseignement supérieur. Masson, 1988.

[Rog80] C. A. Rogers. A less strange version of milnor's proof of brouwer's fixed-point theorem. *The American Mathematical Monthly*, 87(7) :525–527, 1980.

[Rou03] F. Rouvière. *Petit guide de calcul di érentiel : à l'usage de la licence et de l'agrégation*. Enseignement des mathématiques. Cassini, 2003.

[RRC87] W. Rudin, W.A. RUDIN, and Tata McGraw-Hill Publishing Company. *Real and Complex Analysis*. Higher Mathematics Series. McGraw-Hill Education, 1987.

[Sam67] Pierre Samuel. *Théorie algébrique des nombres*. Hermann, Paris, 1967.

[Ser70] Jean-Pierre Serre. *Cours d'arithmétique : par Jean-Pierre Serre*. SUP. Le mathématicien. Presses universitaires de France, 1970.

[Suz06] Je□ Suzuki. Lagrange's proof of the fundamental theorem of algebra. *The American Mathematical Monthly*, 113(8) :705–714, 2006.

[Tau94] P. Tauvel. *Algèbre 2*. Exercices de mathématiques pour l'agrégation. Masson, 1994.

[Tau21] P. Tauvel. *Corps commutatifs et théorie de Galois : Cours et exercices*. Calvage et Mounet, 2021.

[Tri13] M. Trifković. *Algebraic Theory of Quadratic Numbers*. Universitext. Springer New York, 2013.

[Zag90] Don Zagier. A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares. *Amer. Math. Monthly*, 97(2) :144, 1990.

[ZR13] M. Zavidovique and B. Randé. *Un max de maths : problèmes pour agrégatifs et mathématiciens, en herbe ou confirmés*. Im-et-Ker. Calvage & Mounet, 2013.