EXEMPLES DE PARTIES GÉNÉRATRICES D'UN GROUPE

par

Pascal Boyer

Table des matières

prérequis :

1. Généralités et cas commutatif

1.1. Définitions. — Soit G un groupe et S une partie non vide de G ; le groupe $< S >$ engendré par S dans G est le plus petit sous-groupe de G contenant S.
Remarque : l'existence de $< S >$ est assurée par le fait que l'intersection de deux sous-groupes est un groupe : $< S >$ est l'intersection de tous les sous-groupes de G contenant S. Dans le cas où $< S >= G$ on dit que S est *une partie génératrice* de G ; dans ce cas si S est fini, on dit que G est *de type fini*. Dans le cas $G =< S >$ où S est de cardinal 1, on dit que G est *monogène* et si G est fini, il est dit *cyclique*.
Propriété : tout élément $x \in< S >$ s'écrit sous la forme $s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}$ où $n \in \mathbb{N}$ dépend que de x, $s_1, \cdots, s_n \in S$ et $\epsilon_i = \pm 1$. En général cette écriture n'est pas unique.
Question : pour un groupe de type fini le cardinal d'un ensemble S de générateurs de cardinal minimal a-t-il un intérêt quelconque ? Même question pour un groupe qui n'est pas de type fini, en demandant que le groupe engendré par S soit dense.
Remarque : signalons qu'un ensemble de générateur S tel que tout sous-ensemble strict n'est pas générateur, n'est pas forcément de cardinal minimal : par exemple 2 et 3 engendrent $\mathbb{Z}$ alors que ni 2 ni 3 ne sont des générateurs.

1.2. Groupes cycliques. — Tout groupe cyclique de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$; en effet soit $G =< g >$ et considérons le morphisme $f : \mathbb{Z} \to G$ qui à 1 associe g. Par définition le noyau de f est $n\mathbb{Z}$ de sorte que f induit un isomorphisme $\bar{f} : \mathbb{Z}/n\mathbb{Z} \simeq G$.

Proposition 1.1. — *Tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est de cardinal d où d est un diviseur de n. Réciproquement pour tout $d|n$, il existe un unique sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ qui est isomorphe à $\mathbb{Z}/d\mathbb{Z}$.*

Preuve : Le premier point est un cas particulier du théorème de Lagrange. Réciproquement soit H un sous-groupe de $G = \mathbb{Z}/n\mathbb{Z}$; considérons et $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow G/H$, où G/H est le groupe quotient de G par H. Le noyau de ϕ est un sous-groupe de $\mathbb{Z}$ donc de la forme $d\mathbb{Z}$, contenant $\operatorname{Ker}\psi = n\mathbb{Z}$, de sorte que d divise n. Ainsi H est cyclique, engendré par la classe de d ; son ordre est n/d. □

Corollaire 1.2. — *Le groupe engendré par un élément $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est le groupe engendré par $\overline{k \wedge n}$; il est de cardinal $\frac{n}{n \wedge k}$.*

Preuve : Comme k est un multiple de $k \wedge n$, on a l'inclusion $(k) \subset (k \wedge n)$. Réciproquement on écrit une relation de Bezout $uk + vn = n \wedge k$ de sorte que modulo n, $n \wedge k$ appartient au groupe engendré par k et donc $(k \wedge n) \subset (k)$. On en déduit alors que l'ordre de k dans $\mathbb{Z}/n\mathbb{Z}$ qui est par définition le cardinal du groupe engendré par k, est $\frac{n}{n \wedge k}$. □
Remarque : un élément $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est un générateur si et seulement si $k \wedge n = 1$; on notera $\psi(n)$ le cardinal de l'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$, et donc aussi le cardinal des $1 \leq k \leq n$ premiers avec n.

Corollaire 1.3. — *L'ensemble des éléments d'ordre $d|n$ (resp. d'ordre divisant d) dans $\mathbb{Z}/n\mathbb{Z}$ est de cardinal $\psi(d)$ (resp. d). Par ailleurs on a $n = \sum_{d|n} \psi(d)$.*

Preuve : Remarquons tout d'abord que si d ne divise pas n, il n'y a aucun élément d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$. Si d divise n, tous les éléments d'ordre d appartiennent au groupe engendré par $(\frac{n}{d})$ qui est isomorphe, en tant que groupe cyclique d'ordre d, à $\mathbb{Z}/d\mathbb{Z}$. Ainsi les éléments

d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les éléments d'ordre d de $\mathbb{Z}/d\mathbb{Z}$ qui sont en nombre $\psi(d)$.

Cherchons maintenant les éléments d'ordre divisant d dans $\mathbb{Z}/n\mathbb{Z}$ qui sont donc d'ordre divisant $d \wedge n$ et qui appartiennent au groupe engendré par $\frac{n}{n\wedge d}$ isomorphe à $\mathbb{Z}/(n \wedge d)\mathbb{Z}$. Ainsi, comme précédemment, les éléments d'ordre divisant d de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les éléments d'ordre divisant $n \wedge d$ de $\mathbb{Z}/(n \wedge d)\mathbb{Z}$, qui sont en nombre $n \wedge d$.

La dernière égalité découle du dénombrement des éléments de $\mathbb{Z}/n\mathbb{Z}$ selon leur ordre. □

Théorème 1.4. — ***(chinois)*** *Soient n et m des entiers premiers entre eux; l'application $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ qui à un entier k associe sa classe modulo n et m, induit un isomorphisme*

$$\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n \times \mathbb{Z}/m\mathbb{Z}.$$

Preuve : Considérons tout d'abord un élément k du noyau de sorte que n et m divise k et comme $n \wedge m = 1$, d'après le lemme de Gauss $nm|k$. Ainsi le noyau est contenu dans $nm\mathbb{Z}$, l'inclusion réciproque étant évidente de sorte que l'on a une injection de $\mathbb{Z}/nm\mathbb{Z} \hookrightarrow \mathbb{Z}/n \times \mathbb{Z}/m\mathbb{Z}$ qui est un isomorphisme par égalité des cardinaux. □
Remarque : il peut être utile de savoir déterminer un antécédent d'un couple $(\bar{a}, \bar{b}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Pour cela on part d'une relation de Bézout $un + vm = 1$ et on pose $k = unb + vma$; on vérifie aisément que comme $un \equiv 1 \mod m$ et $vm \equiv 1 \mod n$, on a $k \equiv a \mod n$ et $k \equiv b \mod m$. Dans le cas où $n \wedge m = d$, le noyau est $n \vee m\mathbb{Z}$ et l'image

$$\{(a, b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} : \ d|a - b\}.$$

1.5 — L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est aussi muni d'une structure d'anneau déduite de celle de $\mathbb{Z}$; on note $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe multiplicatif de $\mathbb{Z}/n\mathbb{Z}$, i.e. l'ensemble des éléments inversibles muni de la multiplication.

Proposition 1.6. — *Un élément $k \in \mathbb{Z}/n\mathbb{Z}$ appartient à $(\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement s'il est un générateur additif de $\mathbb{Z}/n\mathbb{Z}$. En particulier $(\mathbb{Z}/n\mathbb{Z})^\times$ est de cardinal $\varphi(n)$.*

Preuve : Par définition k est inversible si et seulement s'il existe k' tel que $kk' \equiv 1 \mod n$, i.e. s'il existe $\lambda \in \mathbb{Z}$ tel que $kk' + \lambda n = 1$ ce qui est équivalent à $k \wedge n = 1$ et donc k est un générateur de $\mathbb{Z}/n\mathbb{Z}$. □
Remarque : comme $\mathbb{Z}/n\mathbb{Z}$ est monogène tout morphisme de source $\mathbb{Z}/n\mathbb{Z}$ est déterminé par l'image de $\bar{1}$ de sorte qu'en particulier le groupe $\mathrm{aut}(\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$.

Corollaire 1.7. — *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n = p$ est premier auquel cas on le notera $\mathbb{F}_p$.*

Théorème 1.8. — ***(de Fermat)*** *Pour tout $n \in \mathbb{Z}$ et $k \wedge n = 1$, on a $k^{\varphi(n)} \equiv 1 \mod n$.*

Preuve : Nous avons vu que le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$ est égal à $\varphi(n)$ et comme l'ordre d'un élément divise le cardinal du groupe, l'ordre de k divise $\varphi(n)$ et donc $k^{\varphi(n)} \equiv 1 \mod n$. □

Proposition 1.9. — *Pour $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, on a*

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1).$$

Preuve : Le théorème chinois donne un isomorphisme

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times;$$

le résultat découle alors du fait que le cardinal des $1 \leq k \leq p^\alpha$ divisible par p est de cardinal $p^{\alpha-1}$ et donc $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. □

En ce qui concerne les $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, on a le résultat suivant que nous admettrons.

Proposition 1.10. — *Pour p premier impair et $\alpha \geq 1$, $(\mathbb{Z}/p^a\mathbb{Z})^\times$ est cyclique et pour $p = 2$, on a*

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}).$$

1.3. Groupes abéliens de type fini. — Tout groupe abélien G est de type fini est isomorphe à $Z^r \times \prod_{i=1}^n \mathbb{Z}/a_i\mathbb{Z}$ où $1 < a_1 | \cdots | a_n$. L'entier r s'appelle le rang de G et les a_i sont ses facteurs invariants.

Remarque : notons que l'entier $r + n$ est le nombre minimal de générateurs nécessaires de G. On pourra par exemple utiliser ce fait pour montrer que le sous-groupe de $GL_2(\mathbb{C})$ engendré par les similitudes

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \quad \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}$$

est isomorphe à $\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Réseaux : ce sont les groupes abéliens de type fini sans torsion. Soit Γ un réseau de V, $\mathbf{e}$ une $\mathbb{Z}$-base de Γ et $\mathbf{v}$ une base de V.

- $\mathbf{v}$ est une $\mathbb{Z}$-base de Γ si et seulement si la matrice de passage de $\mathbf{e}$ à $\mathbf{v}$ appartient à $GL_n(\mathbb{Z})$ ou encore si et seulement s'il existe une matrice $A \in GL_n(\mathbb{Z})$ telle que

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = A \begin{pmatrix} e_1 \\ \ddots \\ e_n \end{pmatrix};$$

- un vecteur $v = (v_i)_{i=1,\cdots,n} \in \mathbb{Z}^n$ peut être complété en une $\mathbb{Z}$-base de $\mathbb{Z}^n$ si et seulement si les v_i sont premiers entre eux ;
- plus généralement $v_1, \cdots, v_r$ des vecteurs de $\mathbb{Z}^n$ peuvent être complétés en une $\mathbb{Z}$-base de $\mathbb{Z}^n$ si et seulement si le pgcd des mineures d'ordre r sont premiers entre eux.

Dans la recherche, en général algorithmique, d'une base la meilleure possible signalons les possibilités suivantes :

- les vecteurs de base le plus courts possibles : réduction de Minkowski
- la famille de vecteurs de base la plus orthogonale possible : réduction de Korkine et Zolotarev
- réduction de Lenstra, Lenstra et Lovasz : étant donnée une base $(e_1, \cdots, e_n)$ on notera $(e_1^*, \cdots, e_n^*)$ la base obtenue par le procédé d'orthonormalisation de Gramm-Schmidt

$$e_i^* = e_i - \sum_{j=1}^{i-1} \mu_{i,j} e_j^*$$

où $\mu_{i,j} = \frac{<e_i|e_j^*>}{||b_j^*||^2}$. La base (e_i) est dite LLL-réduite si $|\mu_{i,j}| \leq 1/2$ et que

$$||e_i^* + \mu_{i,i-1} e_{i-1}^*||^2 \geq \frac{3}{4} ||e_{i-1}^*||^2$$

On dispose alors d'un algorithme dit LLL qui permet de calculer une base LLL-réduite à partir d'une base quelconque : cependant si j'ai bien compris la complexité de cet algorithme est mal comprise.

Théorème 1.11. — *(Hermite)* Γ *possède une base* $e_1, \cdots, e_n$ *telle que*

$$N(e_1).\cdots.N(e_n) \leq (\frac{4}{3})^{n(n-1)/2} \det \Gamma$$

Remarque : on rappelle que l'inégalité d'Hadamard donne que $\det \Gamma \leq N(e_1).\cdots.N(e_n)$. En déduire alors qu'il existe un vecteur non nul de Γ de norme inférieure ou égale à $(\frac{4}{3})^{n(n-1)/2} \det(\Gamma)^{1/n}$.
Remarque : l'algorithme LLL a de nombreuses applications, notamment en cryptographie (cf. l'attaque du sac à dos).

1.4. Un groupe abélien non de type fini. — Notons $G = \mathbb{Q}/\mathbb{Z}$ qui est clairement de torsion et pas de type fini puisque tout groupe de torsion de type fini est fini. Soit alors

$$G_p = \bigcup_{n\geq 1} \frac{1}{p^n}\mathbb{Z}/\mathbb{Z} = \frac{1}{p}\mathbb{Z}/\mathbb{Z} \subset \frac{1}{p^2}\mathbb{Z}/\mathbb{Z} \subset \cdots \subset \frac{1}{p^n}\mathbb{Z}/\mathbb{Z} \subset \cdots$$

Lemme 1.12. — G_p *est l'unique pro-p-groupe de Sylow de* G.

Preuve : Remarquons tout d'abord que G_p est un groupe : soient $x, y \in G$ alors il existe n et m tels que $x \in \frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$ et $y \in \frac{1}{p^m}\mathbb{Z}/\mathbb{Z}$ et donc pour $r = \max\{n, m\}$, $x, y \in \frac{1}{p^r}\mathbb{Z}/\mathbb{Z}$ qui est un groupe et donc $x - y \in G_p$. Par ailleurs si $x \in G$ est d'ordre une puissance de p, alors clairement $x \in G_p$. □

Lemme 1.13. — *Les sous-groupes stricts de* G_p *sont les* $\frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$.

Preuve : Pour tout $n \geq 0$, $\frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$ est un sous-groupe de G_p. Réciproquement soit H un sous-groupe de G_p et supposons que H ne soit pas de la forme $\frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$ de sorte que pour tout n, il existe $x \notin \frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$. Soit m tel que $x \in \frac{1}{p^m}\mathbb{Z}/\mathbb{Z}$ avec donc $m > n$ de sorte que $p^{m-n}x$ est un générateur de $\frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$ et donc $\frac{1}{p^n}\mathbb{Z}/\mathbb{Z} \subset H$ et finalement $H = G_p$. □

Lemme 1.14. — *Tout sous-groupe* H *de* G *est la somme directe de ses sous-groupes de Sylow* $H_p = H \cap G_p$.

Preuve : Soit $x \in H$ et n tel que $x \in \frac{1}{n}\mathbb{Z}/\mathbb{Z} \simeq \prod_p \frac{1}{p^{\alpha_p}}\mathbb{Z}/\mathbb{Z}$ où $n = \prod_p p^{\alpha_p}$ et donc $x = \sum_p x_p$ avec $x_p = \frac{n}{p^{\alpha_p}}x \in H \cap G_p$. Ainsi $H \subset \bigoplus_p H_p$, l'inclusion réciproque étant évidente. □
Remarque : $\mathbb{Q}/\mathbb{Z}$ est isomorphe au sous-groupe de torsion de $SO(2, \mathbb{R}) \simeq \mathbb{U}$. Par ailleurs le groupe dual de G_p est isomorphe à l'anneau des entiers p-adiques $\mathbb{Z}_p$ que l'on peut obtenir aussi comme la limite projective des $\frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$.

2. Exemples non commutatifs

2.1. Le groupe symétrique. — Si on cherche les générateurs les plus simples possibles, on se tourne vers les transpositions et on peut montrer les résultats suivants :
(i) les transpositions engendrent $\mathfrak{S}_n$;
(ii) les transpositions $(i\ i+1)$ engendrent $\mathfrak{S}_n$;
(iii) les transpositions $(1\ i)$ engendrent $\mathfrak{S}_n$.

Dans les deux derniers cas, on remarque qu'on ne peut pas enlever des transpositions : si (iii) on enlève $(1\ k)$ alors toute permutation dans le groupe engendré par les autres laisse k invariant ; dans (ii) ce sont les sous-ensembles $[1,k]$ et $[k+1,n]$ qui sont stables. On peut en fait montrer le résultat suivant.

Proposition 2.1. — *(cf. [?]) Soit $\{\tau_1,\cdots,\tau_r\}$ un ensemble de transpositions qui engendrent $\mathfrak{S}_n$, alors $r\geq n-1$.*

Remarque : si on s'autorise à prendre d'autres permutations, on note que $(1\ 2)$ et $(1\ 2\cdots n)$ engendrent $\mathfrak{S}_n$; évidemment comme $\mathfrak{S}_n$ n'est pas commutatif pour $n\geq 3$, on ne peut pas trouver un seul générateur. On note à ce propose que le cardinal minimal d'un système de générateurs ne donne aucun renseignement sur la taille du groupe ni sur ses sous-groupes. En effet tout groupe peut être vu comme un sous-groupe de $\mathfrak{S}_n$ de sorte que si G est un groupe abélien fini nécessitant r générateurs, il est un sous-groupe d'un groupe ne nécessitant que deux générateurs.

Proposition 2.2. — *Pour $n\geq 3$, $\mathcal{A}_n$ est engendré par les 3-cycles.*

Application : : pour $n\geq 5$, $\mathcal{A}_n$ est simple. Comme tous les 3 cycles sont conjugués dans $\mathcal{A}_n$, il suffit de montrer que tout sous-groupe distingué de $\mathcal{A}_n$ contient un 3-cycle.

2.2. Le groupe linéaire. — $SL_n(K)$ est engendrée par les transvections élémentaires relativement à la base canonique

Remarque : les matrices de permutation ne sont pas utiles puisqu'elles s'obtiennent à partir des matrices de transvections. Pour les faire entrer dans le jeu :

- pour $M\in\mathbb{M}_{p,n}(K)$ de rang $r>0$, alors il existe $Q\in SL_n(K)$ (qui est donc produit des $T_{i,j}(\lambda)$ et $\sigma\in\mathfrak{S}_n$ tels que $QMP_\sigma=\begin{pmatrix} I'_r & A\\ 0 & 0\end{pmatrix}$ où P_σ est la matrice de permutation associée à σ et $I'_r=I_r$ si $r<p$ et $I'_r=\mathrm{diag}(1,\cdots,1,\alpha)$ (la matrice de permutation sert à permuter les colonnes quand on moment de pivoter sur cette colonne celle-ci est combinaison linéaire des précédentes). Si on ne s'autorise pas à pivoter les colonnes on obtient une matrice échelonnée cf. plus loin
- décomposition de Bruhat : $T(n,\mathbb{C})\backslash GL(n,\mathbb{C})/T(n,\mathbb{C})\simeq\mathfrak{S}_n$ où $T(n,\mathbb{C})$ désigne l'ensemble des matrices triangulaires supérieures. On interprète ce résultat en termes de drapeaux : l'ensemble des classes de paires de drapeaux complets sous l'action de $GL(n,\mathbb{C})$, est en bijection avec $\mathfrak{S}_n$.
- soit M un élément de $GL_n(K)$, alors $MD_n(\det M^{-1})$ est un produit de transvections élémentaires (moins de n^2) relativement à la base canonique
- si on autorise toutes les transvections et pas seulement les $T_{i,j}(\lambda)$ alors pour $1_E\neq f\in SL(E)$ qui n'est pas une affinité (resp. une affinité) alors f est produit de r (resp. $r+1$) transvections avec $r=n-\dim_K\mathrm{Ker}(f-1_V)$ et que ce nombre est minimal.

Sous-groupes libres de $GL_2(\mathbb{R})$: soient $a,b\geq 2$ des réels : $A=\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}$ et $B=\begin{pmatrix}1 & 0\\ b & 1\end{pmatrix}$. Le groupe $L_{a,b}$ engendré par A et B est libre et discret dans $SL_2(\mathbb{R})$. Si a est transcendant alors $L_{a,a}$ est libre de rang 2 alors que $L_{1,1}$ ne l'est pas.

Remarque : en affine, on rappelle que le groupe affine est le produit semi-direct du sous-groupe des translations par le groupe linéaire que l'on voit comme le sous-groupe fixant un point O.

2.3. Le groupe orthogonal. — Les réflexions par rapport à un hyperplan (resp. les renversements) engendrent $O(n)$ (resp. $SO(n)$ pour $n \geq 3$). Plus précisément

- soit $u \in O(n)$ et $F_u = \{x \in E \ / \ u(x) = x\}$; on note $p_u = n - \dim F_u$. Alors u peut s'écrire comme le produit de p_u réflexions et pas moins ;
- pour $n \geq 3$, tout élément de $SO(n)$ est produit d'au plus n renversements.
- Pour $n = 2$, $SO(2, \mathbb{R}) \simeq \mathbb{R}/\mathbb{Z}$ et ne possède pas de classe génératrice particulière ; signalons que le groupe $\mathbb{Q}/\mathbb{Z}$ étudié plus haut est le groupe de torsion de $SO(2, \mathbb{R})$.

Remarque : soient u_1 et u_2 deux symétries orthogonales de même nature (i.e. tels que $\dim \mathrm{Ker}(u_1 - Id) = \dim \mathrm{Ker}(u_2 - Id)$) ; alors u_1 et u_2 sont conjuguées par $SO(n)$. On obtient ainsi une stratégie pour montrer la simplicité des $SO(n)$ pour $n \geq 3$: il suffit de montrer que tout sous-groupe distingué contient un renversement.

Remarque : la composition de deux rotations de $\mathbb{R}^3$ peut se calculer assez simplement en utilisant les quaternions :

Remarque : en affine il faut absolument savoir jouer avec les isométries en dimension 2 et 3.

Groupes cristallographiques : ca concerne les pavages périodiques, la description des groupes cristallographiques de l'espace euclidien $\mathbb{R}^n$ est réglé par les théorèmes suivants dus à **Bieberbach** :

- le sous-groupe Γ' des translation d'un groupe cristallographique Γ de l'espace euclidien $\mathbb{R}^n$ est d'indice fini engendré et isomorphe à $\mathbb{Z}^n$;
- tout isomorphisme de groupes abstraits entre deux groupes cristallographiques est de la forme $\phi(g) = h \circ g \circ h^{-1}$ où h est une bijection affine de $\mathbb{R}^n$;
- il n'existe qu'un nombre fini de classes d'isomorphisme de groupes cristallographiques (17 en dimension 2, 219 en dimension 3, un meilleure compréhension de la table est toujours un sujet d'actualité.

Remarque : une rotation d'angle α tel $\alpha/\pi \notin \mathbb{Q}$, engendre un sous-groupe dense de $SO(2, \mathbb{R})$. En ce qui concerne $SO(3, \mathbb{R})$ citons le résultat suivant.

Proposition 2.3. — *Une rotation de $SO(3)$ sera notée par $r = (k, \theta)$ où k est le vecteur unitaire de l'axe de la rotation et θ son angle. Soient alors $r = (OA, 2\alpha)$ et $s = (OB, 2\beta)$ deux rotations telles que $\frac{\alpha}{\pi}$ et $\frac{\beta}{\pi}$ soient irrationnels. Excepté une infinité dénombrable de valeurs pour la mesure c de l'angle entre les axes OA et OB, le groupe engendré par r et s est dense dans $SO(3)$.*

Preuve : Si P_3 est le plan OAB et $P_2 = (OA, -\alpha)(P_3)$ alors r s'écrit comme le produit des réflexions par rapport aux plans P_2 et P_3. De même s est le produit de P_1 et P_2 où $P_1 = (OB, \beta)(P_3)$.

Afin d'approcher une rotation $(k, 2\theta)$, on approche son axe puis son angle. Pour approcher $\mathbb{R}.k$, on approche les plans qu'il détermine avec OA, et OB. D'après le théorème de Jacobi-Kronecker, ils sont respectivement approchés par $P_2' = (OA, -p\alpha)(P_3)$ et $P_1' = (OB, q\beta)(P_3)$ si p et q sont des entiers adéquats. Ainsi $\mathbb{R}k' = P_1' \cap P_2'$ approche $\mathbb{R}k$.

Puisque $r^p = (OA, 2p\alpha)) = (P_3)(P_2')$ et $s^q = (OB, 2q\beta) = (P_1')(P_3)$, on a $s^q r^p = (P_1')(P_2')$ dont la mesure $2\gamma'$ de l'angle est donnée par la formule fondamentale de la trigonométrie sphérique

$$\cos \gamma' = \sin(p\alpha) \sin(q\beta) \cos c - \cos(p\alpha) \cos(q\beta)$$

On cherche $\frac{\gamma'}{\pi}$ irrationnel ; la formule précédente montre que si p et q décrivent les entiers et si $\frac{\gamma'}{\pi}$ décrit les rationnels, $\cos c$ ne prend qu'une infinité dénombrable de valeurs. On choisit alors c pour que $\cos c$ n'appartienne pas à cet ensemble de valeurs. Il en résulte alors que $\frac{\gamma'}{\pi}$

est irrationnel pour tout p, q. Le théorème de Jacobi-Kronecker montre alors que l'on peut choisir n pour que $2n\gamma'$ approche 2θ de sorte que $(s^q r^p)^n$ approche $(k, 2\theta)$. □

2.4. Le groupe unitaire. — Les matrices de Householder qui sont hermitiennes et unitaires (cf. M-T p.186) avec en application :
- ce sont exactement les matrices de $U(n)$ qui sont hermitiennes de signature $(n-1, 1)$;
- toute matrice de $SU(n)$ est un produit pair de matrices de Householder ;
- le sous-groupe de $U(n)$ engendré par les matrices hermitiennes de $U(n)$ est le sous-groupe de $U(n)$ constitué des matrices de déterminant ± 1 ;

Une matrice $M = [m_{i,j}] \in \mathbb{M}_n(K)$ est dite de Hessenberg si $m_{j,k} = 0$ pour tout (j, k) tel que $j - k \geq 2$. Le premier résultat est alors

Proposition 2.4. — *(cf.* [**?**] *10.1.1) Pour tout $M \in \mathbb{M}_n(\mathbb{C})$, il existe une matrice unitaire $U \in GL_n(\mathbb{C})$ telle que $U^{-1}MU$ est de Hessenberg ; si M est réelle on peut alors prendre $U \in O_n$.*

Preuve : On va construite une suite $M_1 = M, M_2, \cdots, M_{n-1}$ de matrices unitairement semblables telles que M_{n-r} est de la forme $\begin{pmatrix} H & Z' & B \\ O_{r,n-r-1} & Z & N \end{pmatrix}$ avec $(HZ') \in \mathbb{M}_{n-r}(\mathbb{C})$ de Hessenberg et $Z \in \mathbb{C}^r$. On passe de M_{n-r} à M_{n-r+1} de la façon suivante : si Z est colinéaire au premier vecteur e^1 de la base canonique de $\mathbb{C}^r$ alors il n'y a rien à faire, sinon soit $X \in \mathbb{C}^r$ unitaire tel que SZ est colinéaire à e^1 où $S = I_m - 2XX^*$ est la matrice unitaire de la symétrie par rapport à l'hyperplan $X^\perp$: $SX = -X$ et pour $Y \in X^\perp$ i.e. $X^*Y = 0$, $SY = Y$. On considère alors la matrice de Householder, cf. §**??**, $V = \begin{pmatrix} I_{n-r} & 0_{n-r,r} \\ 0_{r,n-r} & S \end{pmatrix}$ et on pose

$$M_{n-r+1} = V^{-1} M_{n-r} V = \begin{pmatrix} H & Z' & BS \\ 0_{n,n-r-1} & SZ & SNS \end{pmatrix}$$

qui est bien de la forme demandée. □

Remarques :
- la détermination de U est algorithmique et nécessite $5n^3/3 + O(n^2)$ multiplications et $4n^3/3 + O(n^2)$ additions.
- Si M est hermitienne alors $A = U^{-1}MU$ es tridiagonale avec $a_{j,j+1} = \overline{a_{j+1,j}}$ et $a_{j,j} \in \mathbb{R}$. La complexité est alors de $2n^3/3 + O(n^2)$ multiplications. Écrivons

$$A = \begin{pmatrix} m & \bar{a} & 0 & \cdots & 0 \\ a & & & & \\ 0 & A_1 & & & \\ \vdots & & & & \\ 0 & & & & \end{pmatrix}$$

et notons χ_{A_0}, χ_{A_1} les polynômes caractéristiques respectifs de A et A_1 : ce sont bien sûr des éléments de $\mathbb{R}[X]$ car les racines d'une matrice hermitienne sont réelles. En développant par rapport à la première colonne, on obtient alors

$$\chi_A(X) = m\chi_{A_1}(X) - |a|^2 \chi_{A_2}(X)$$

où A_2 est la matrice extraite de A_1 constituée de ses $n-2$ dernières lignes et colonnes. On remarque alors que la suite $(\chi_{A_j}(X))_{0 \leq j \leq n-1}$ est une suite de Sturm ce qui permet de calculer le nombre de racines de $\chi_{A_0}(X)$ dans un intervalle $[a, b] \subset \mathbb{R}$ quelconque. Il est

ainsi possible de calculer de manière approchée les valeurs propres de A par dichotomie en calculant $V(a)$, $V(b)$, $V(\frac{a+b}{2}), \cdots$.
– Soit M de Hessenberg et T triangulaire supérieure alors TM et MT sont de Hessenberg. Ainsi si $M = QR$ est sa factorisation QR, $Q = MR^{-1}$ est aussi de Hessenberg. Cette remarque est utilisée dans la méthode QR de localisation des valeurs propres, cf. §**??**.

2.5. Le groupe circulaire. — Dans le plan compactifié (sphère de Riemann) : groupe qui conserve les droite-cercles : il est engendré par les inversions : c'est soit une homographie (conserve le bi-rapport) soit homographie de la conjugaison complexe

3. Présentation d'un groupe par générateurs et relations

3.1. Définition. — Soit $S = \{a_i;\ i \in I\}$ un ensemble et $T = S \times \{-1, 1\}$: pour $a \in S$, on note $a^1 \in T$ pour $(a, 1) \in T$ et $a^{-1} = (a, -1)$. Un mot d'alphabet S est alors un élément de $E = \bigcup_{n\in\mathbb{N}} T^n$ que l'on note sous la forme $M = a_1^{\epsilon_1} \cdots a_n^{\epsilon_n}$ avec $a_i \in S$ et $\epsilon_i = \pm 1$; il sera dit réduit si pour tout $i = 1, \cdots, n-1$, $(a_i^{\epsilon_i}, a_{i+1}^{\epsilon_{i+1}})$ n'est pas de la forme (a^1, a^{-1}) ou (a^{-1}, a^1). On munit E d'une structure de monoïde par concaténation. Soit alors $F(S)$ l'ensemble des mots réduits d'alphabet S ; en supprimant les occurences a^1a^{-1} et $a^{-1}a^1$ dans la concaténation des mots, on munit $F(S)$ d'une structure de groupe d'élément neutre est le mot vide : c'est *le groupe libre construit sur* S.

Pour $R = (r_j)_{j\in J}$ un ensemble de mots réduits de $F(S)$, on note $N(R)$ le plus petit sous-groupe distingué de $F(S)$ contenant les r_j. Le groupe $F(S)/N(R)$ est alors appelé *le groupe présenté par les générateurs* S *et soumis aux relations* R. On le note aussi sous la forme $< (a_i)_{i\in I} \mid (r_j)_{j\in J} >$.
Exemples simples : $< a_1 > \simeq \mathbb{Z}$, $< a_1 \mid a_1^n > \simeq \mathbb{Z}/n\mathbb{Z}$, $< r, s \mid r^n,\ s^2,\ (sr)^2 > \simeq D_n$.

3.2. Cas des groupes symétriques et alternés. — Soit G_n le groupe engendré $x_1, \cdots, x_{n-1}$ et soumis aux relations :

$$\begin{aligned} x_i^2 &= 1 \qquad 1 \le i \le n-1 \\ (x_i x_{i+1})^3 &= 1 \qquad 2 \le i \le n-2 \\ (x_i x_j)^2 &= 1 \qquad |i-j| > 1. \end{aligned}$$

Pour $n = 2$ on a déjà vu que $G_2 \simeq \mathbb{Z}/2\mathbb{Z} \simeq \mathfrak{S}_2$. On suppose donc $n \ge 3$ et soit H le sous-groupe de G engendré par $x_1, \cdots, x_{n-2}$.

Lemme 3.1. — *On a* $G = H \cup Hx_{n-1} \cup \cdots \cup Hx_{n-1}. \cdots .x_2.x_1$.

Preuve : Notons $K = H \cup Hx_{n-1} \cup \cdots \cup Hx_{n-1}. \cdots .x_2.x_1$. Il suffit alors de montrer que K est un sous-groupe de G.

□

Proposition 3.2. — *Pour tout* $1 \le i \le n-1$, *soit* $a_i = (i, i+1)$ *la transposition de* $\mathfrak{S}_n$. *Alors l'application* $< x_1, \cdots, x_{n-1} > \to \mathfrak{S}_n$ *qui à* x_i *associe* a_i, *induit une bijection de* G *sur* $\mathfrak{S}_n$.

Preuve : Comme $\mathfrak{S}_n$ est engendré par les transpositions a_i pour $1 \le i \le n-1$, l'application de l'énoncé est surjective. En outre comme les $a_i \in \mathfrak{S}_n$ vérifient les relations suivantes :

$$\begin{aligned} a_i^2 &= 1 \qquad 1 \le i \le n-1 \\ (a_i a_{i+1})^3 &= 1 \qquad 2 \le i \le n-2 \end{aligned}$$

$$(a_i a_j)^2 = 1 \qquad |i-j| > 1$$

l'application de l'énoncé se factorise par G. On va alors raisonner par récurrence sur n.

□

Soit G'_n le groupe engendré par les générateurs $x_1, \cdots x_{n-2}$ soumis aux relations :

$$x_1^3 = x_i^2 = 1 \qquad 2 \leq i \leq n-2$$
$$(x_i x_{i+1})^3 = 1 \qquad 1 \leq i \leq n-3$$
$$(x_i x_j)^2 = 1 \qquad |i-j| > 1.$$

Pour $n = 3$, on a déjà vu que $G'_3 \simeq \mathbb{Z}/3\mathbb{Z} \simeq \mathcal{A}_3$. Supposons donc $n \geq 4$. Soit H le sous-groupe de G engendré par $x_1, \cdots x_{n-3}$.

Lemme 3.3. — *On a*

$$G'_n = H \cup Hx_{n-2} \cup \cdots \cup Hx_{n-2}.\cdots x_2.x_1 \cup Hx_{n-2}.\cdots .x_2.x_1^2$$

Preuve : Notons $K = H \cup Hx_{n-2} \cup \cdots \cup Hx_{n-2}.\cdots x_2.x_1 \cup Hx_{n-2}.\cdots .x_2.x_1^2$. Il suffit donc de montrer que K est un sous-groupe de G'_n.

□

Proposition 3.4. — *Soient $a_1 = (1,2,3)$ et $a_i = (1,2)(i+1, i+2)$ pour $2 \leq i \leq n-2$ les permutations de $\mathcal{A}_n$. L'application $< x_1, \cdots, x_{n-2} > \rightarrow \mathcal{A}_n$ qui à x_i associe a_i, induit un isomorphisme $G'_n \simeq \mathcal{A}_n$.*

Preuve : Comme $\mathcal{A}_n$ est engendré par $a_1, \cdots, a_{n-2}$, l'application de l'énoncé est surjective. Par ailleurs comme les a_i vérifient les relations suivantes :

$$a_1^3 = a_i^2 = 1 \qquad 2 \leq i \leq n-2$$
$$(a_i a_{i+1})^3 = 1 \qquad 1 \leq i \leq n-3$$
$$(a_i a_j)^2 = 1 \qquad |i-j| > 1$$

l'application se factorise par G'_n. On raisonne alors par récurrence sur n.

□

3.3. Groupes de Coxeter. — C'est un groupe ayant une présentation du type $< r_1, \cdots, r_n \mid (r_i r_j)^{m_{i,j}} >$ où $(m_{i,j})_{1 \leq i,j \leq n}$ est une matrice symétrique à valeurs dans $\mathbb{N} \cup \{\infty\}$ avec $m_{i,i} = 1$ (i.e. les générateurs sont d'ordre 2) et $m_{i,j} \geq 2$ pour $i \neq j$: la condition $(rir_j)^\infty$ signifie par convention qu'aucune relation n'est imposée entre r_i et r_j.

3.4. Lemme du ping-pong. — Soit G un groupe opérant sur un ensemble X et soient H, H' deux sous-groupes de G. On suppose qu'il existe deux parties non vides X, X' de X telles que

$$hX' \subset X \text{ si } h \in H \backslash 1 \text{ et } h'X \subset X' \text{ si } h' \in H' \backslash 1$$

Alors si H' n'est pas réduit à 2 éléments et $X' \nsubseteq X$ alors le morphisme canonique $H * H' \rightarrow < H, H' >$ est un isomorphisme. (applications à $PSL_2(\mathbb{R}) = \mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$

Preuve : On suppose $H \neq 1$, considérons d'abord un produit impair $p = h_0 h'_1 h_1 \cdots h'_k h_k$ avec $h_i \in H - \{1\}$ et $h'_i \in H' - \{1\}$. Si $p = 1$ on a

$$X' = h_0 h'_1 h_1 \cdots h'_k h_k X' \subset h_0 h'_1 h_1 \cdots h'_k X \subset \cdots \subset h_0 X' \subset X$$

ce qui n'est pas. Pour un produit impair du style $h'_0 h_1 h'_1 \cdots h_k h'_k$ le raisonnement est similaire.

Pour un produit pair $p = h_1 h'_1 \cdots h_k h'_k$, choisissons $h' \in H' - \{1, h'_k\}$ de sorte que

$$h'p(h')^{-1} = h'h_1 h'_1 \cdots h_k(h(_k(h()^{-1})$$

est un produit impair comme plus haut et donc $p \neq 1$. Le cas $p = h'_1 h_1 \cdots h'_k h_k$ se traite de la même façon. □

Applications : dans $SL_2(\mathbb{Z})$ on note

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

– considérons l'application de $\mathbb{Z}/2\ Zm * \mathbb{Z}/3\mathbb{Z}$ qui à $(1,0)$ associe S et à $(0,1)$ $T^{-1}S$: comme $S^2 = (ST)^3$ ce morphisme est bien défini, pour montrer qu'il s'agit d'un isomorphisme il suffit de montrer que tout mot en $X = S$ et $Y = T^{-1}S$ de la forme $X^{e_1}Y^{f_1}X^{e_2}Y^{f_2}\cdots X^{e_r}Y^{f_r}$ avec $e_1 = 0, 1$, $e_i = 1$, $0 < f_i < 3$ et $0 \leq f_r \leq 2$. Il suffit de vérifier que l'image de i est distincte de i ce qui permet de se ramener au cas où le mot est un produit de XY et XY^2. Or on vérifie aisément que XY et XY^2 conserve le deuxième cadran et font baisser l'ordonnée, d'où le résultat.
Remarque : on peut aussi joueur au ping pong avec $X = \mathbb{R}_{>0} \coprod \infty$ et $X' = \mathbb{R}_{\leq 0}$.

– on note $\Gamma(2)$ le noyau de $SL_2(\mathbb{Z}) \twoheadrightarrow SL_2(\mathbb{Z}/2\mathbb{Z})$ et soit $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$. En considérant l'action de $SL_2(\mathbb{Z})$ sur $\mathbb{P}^1(\mathbb{R})$ et en jouant au "ping-pong" avec les parties $P_A =]-1, 1[$ et $P_B = P_A^c$, on montre que $\Gamma(2)$ est le groupe libre engendré par A et B.

4. Applications

4.1. Sous-groupes paradoxaux et paradoxe de Banach-Tarski. — On considère les deux rotations vectorielles de $\mathbb{R}^3$, u, v dont les matrices dans la base canonique sont

$$U = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \text{ et } V = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1/2 & \sqrt{3}/2 \\ 0 & -\sqrt{3}/2 & -1/2 \end{pmatrix}$$

Soit G le groupe engendré par u et v.

Proposition 4.1. — *Tout élément $r \in G\backslash\{Id, u\}$ s'écrit de manière unique sous la forme $r = u^{\epsilon_1}v^{n_1}uv^{n_2}u\cdots uv^{n_k}u^{\epsilon_2}$ avec $\epsilon_1, \epsilon_2 \in \{0, 1\}$ et les $n_i \in \{1, 2\}$.*

Preuve :

□

On définit une partition (I, J, K) de G de la manière suivante
– pour tout n, $(v^2u)^n \in I$;
– pour tout n, $u(v^2u)^n \in J$;
– pour tout n, $vu(v^2u)^n \in K$;
– les éléments de G qui ne sont pas de cette forme appartiennent à I, J, K respectivement suivant que leur écriture commence à gauche par u, v, v^2 respectivement.

Lemme 4.2. — *On a $K = vJ$, $I = vK$ et $I = u(J \cup K)$.*

Preuve :

□

Deux parties A et B de l'espace euclidien $\mathbb{R}^3$ sont dites superposables et on notera $A\mathcal{D}B$, s'il existe un déplacement r de $\mathbb{R}^3$ tel que $B = r(A)$; on définit ainsi une relation d'équivalence. Soit S la sphère unité de $\mathbb{R}^3$; on pose

$$D = \{x \in S \ / \ \exists r \in G\backslash\{Id\},\ r(x) = x\}$$

Lemme 4.3. — *L'ensemble D est dénombrable et est stable par G.*

Les orbites de $S\backslash D$ sous l'action de G, constituent une partition de $S\backslash D$. En utilisant l'axiome du choix, on construit un ensemble T contenant un élément de chaque orbite.

Lemme 4.4. — *En posant $A = I(T)$, $B = J(T)$ et $C = K(T)$, on obtient une partition finie (A, B, C, D) de S avec D dénombrable, A, B, C superposables et $A\mathcal{D}(B \cup C)$.*

Remarque : en quelque sorte, A est à la fois la moitié et le tiers de la sphère.

On appelle découpage d'une partie A de $\mathbb{R}^3$, une partition finie $(A_i)_{1\leq i\leq n}$ de A. On dira que deux parties A, B de $\mathbb{R}^3$ sont puzzle-équivalentes s'il existe une entier n et des découpages $(A_i)_{1\leq i\leq n}$ et $(B_i)_{1\leq i\leq n}$ tels que pour tout $1 \leq i \leq n$, A_i et B_i sont superposables ; on définit ainsi une relation d'équivalence que l'on notera $\mathcal{P}$. Soient S_1 et S_2 deux sphères disjointes de rayon 1, de centres respectifs O_1, O_2 et soient (A_1, B_1, C_1, D_1) et (A_2, B_2, C_2, D_2) les découpages obtenus en translatant (A, B, C, D).

Lemme 4.5. — *On a $(S\backslash D)\mathcal{P}((S_1\backslash D_1) \cup (S_2\backslash D_2))$.*

On cherche à éliminer les ensembles dénombrables dans la duplication de la sphère ci-dessus. On veut prouver le résultat suivant : si Σ est une sphère et Δ est un sous-ensemble dénombrable de Σ, alors

$$\Sigma\mathcal{P}(\Sigma\backslash\Delta)$$

Pour cela on peut choisir $\delta \in \Sigma$ tel que $\pm\delta \notin \Delta$ de sorte que l'ensemble des rotations d'axe (O, δ) vérifiant qu'il existe $n \in \mathbb{N}\backslash\{0\}$, $x, y \in \Delta$ tels que $r^n(x) = y$ est dénombrable. Soit alors ρ une rotation n'appartenant pas à cet ensemble, de sorte que les ensembles $\rho^n(\Delta)$ sont deux à deux disjoints. En considérant $U = \bigcup_{n\geq 0} \rho^n(\Delta)$, on obtient le résultat.

On veut désormais dupliquer les boules fermées ; on a

$$(K\backslash\{O\})\mathcal{P}((K_1\backslash\{O_1\}) \cup (K_2\backslash\{O_2\}))$$

de sorte qu'en considérant $\Delta = \{(\cos n, \sin n, 0),\ n \in \mathbb{N}\}$, la rotation d'axe z et d'angle 1 radian envoie Δ sur $\Delta\backslash\{(1, 0, 0)\}$ et ainsi

$$K\mathcal{P}K\backslash\{(1, 0, 0)\}$$

ce qui permet la duplication des boules.

Remarque : De manière plus générale, on peut montrer le théorème suivant

Théorème 4.6. — *(Banach-Tarski) Si A et B sont deux parties de $\mathbb{R}^3$ bornées et d'intérieurs non vides, alors A et B sont puzzle-équivalentes.*

4.2. Séries thêta et formes modulaires. — Dans la preuve de l'équation fonctionnelle de la fonction zéta de Riemann, on utilise la fonction thêta usuelle

$$\theta(z) = \sum_{n\in\mathbb{Z}} e^{i\pi n^2 z}$$

pour $z = iy$, $y > 0$. Celle-ci définit une fonction holomorphe sur le demi-plan de Poincaré ; la formule sommatoire de Poisson donne par prolongement analytique l'équation fonctionnelle

$$\theta(-\frac{1}{z}) = (-iz)^{1/2}\theta(z)$$

où $(-iz)^{1/2}$ est donné par la branche de la fonction sur $\mathcal{H}$ qui envoie iy sur $\sqrt{y}$. Cette relation jointe à la relation évidente $\theta(z+2) = \theta(z)$ donne une règle de transformation pour $f(\gamma z)$ pour tout $\gamma \in < T^2, S > \subset PSL_2(\mathbb{Z})$ agissant sur $\mathcal{H}$ par homographies. De même pour tout $k \geq 1$, $\theta(z)^k$ satisfait à des formules de transformation analogues. Par ailleurs les égalités

$$\theta(z)^k = \sum_{n\geq 0} r_k(n) e^{i\pi n z}$$

où $r_k(n)$ désigne le nombre de représentations de n comme somme de k carrés d'entiers, justifient à elles seules, l'acharnement qu'ont subies ces séries. En particulier, on peut montrer les identités suivantes :

$$\begin{aligned} r_2(n) &= 4\textstyle\sum_{d|n} \chi_4(d) \\ r_4(n) &= 8(3+(-1)^n)\textstyle\sum_{d|n} d \\ r_6(n) &= 16\textstyle\sum_{d|n} d^2\chi_4(\frac{n}{d}) - 4\sum_{d|n} d^2\chi_4(d) \end{aligned}$$

avec $\chi_4(n) = d_1(n) - d_3(n)$ où $d_1(m)$ (resp. $d_3(m)$) est le nombre de diviseur $d \equiv 1 \mod 4$ (resp. $d \equiv 3 \mod 4$) de n. Plus généralement une fonction f est dite **elliptique** par rapport à un réseau Λ si c'est une fonction méromorphe sur $\mathbb{C}$ qui est Λ-périodique, i.e.

$$f(z+\omega) = f(z)$$

pour tout $z \in \mathbb{C}$ et tout $\omega \in \Lambda$.
Remarque : f est Λ-périodique si et seulement si $f(z+\omega_1) = f(z) = f(z+\omega_2)$ pour tout $z \in \mathbb{C}$ avec $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. Par ailleurs si f n'a pas de poles, montrer que f est constante.

Soit F une fonction sur l'ensemble $\mathcal{R}$ des réseaux de $\mathbb{C}$ à valeurs complexes de poids $k \in \mathbb{Z}$, i.e. telle que $F(\lambda\Gamma) = \lambda^{-2k}F(\Gamma)$ pour tout réseau $\Gamma \in \mathcal{R}$ et tout $\lambda \in \mathbb{C}^\times$. La formule

$$F(\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2) = \omega_2^{-2k} f(\frac{\omega_1}{\omega_2})$$

définit une fonction modulaire f de poids $2k$ et de niveau 1, i.e. $f_{|2kA} = f$ pour tout $A \in SL_2(\mathbb{Z})$, où

$$f_{|2k\ A} = (cz+d)^{-k} f(\frac{az+b}{cz+d}) \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Remarque : l'étude des formes modulaires et plus généralement des formes automorphes est intimement liée à l'étude des courbes elliptiques, à la géométrie des variétés de Shimura et aux représentations galoisiennes via la philosophie de Langlands sur les fonctions L qui leurs sont associées.

4.3. Analyse harmonique. —

5. Développements

- génération du SL_n par les transvections [**1**]
- simplicité de SO_3 [**1**]
- génération du groupe circulaire ou $PSL_2(\mathbb{Z})$
- génération du groupe alterné ou symétrique [**1**]
- groupes libres un exemple

6. Questions

Exercice 6.1. — *Soit $u \in O(q)$ et $F_u = \{x \in E \ / \ u(x) = x\}$ et on note $p_u = n - \dim F_u$. Montrez par récurrence sur p_u, que u est le produit d'au plus p_u réflexions. Montrez ensuite que u est le produit d'au moins p_u réflexions.*

Exercice 6.2. — *Montrez que pour $n \geq 3$, tout élément de $O^+(q)$ est produit d'au plus n renversements.*

Exercice 6.3. — *Soient u_1 et u_2 deux symétries orthogonales de même nature (i.e. tels que $\dim \mathrm{Ker}(u_1 - Id) = \dim \mathrm{Ker}(u_2 - Id)$). Montrez que u_1 et u_2 sont conjuguées par $O^+(q)$. En déduire alors que $D(O(q)) = D(O^+(q)) = O^+(q)$.*

Exercice 6.4. — *Montrez que pour tout $u \in O(q)$, il existe une décomposition orthogonale*

$$E = \mathrm{Ker}(u - Id) \oplus \mathrm{Ker}(u + Id) \oplus P_1 \oplus \cdots \oplus P_r$$

où les P_i sont des plans stables par u, tels que la restriction de u y soit une rotation.

Exercice 6.5. — *(M-T p.187) Les matrices de Householder sont exactement les matrices de $U(n)$ qui sont hermitiennes de signature $(n-1, 1)$.*

Exercice 6.6. — *(a) Montrer que le sous-espace vectoriel engendré par le cône nilpotent est l'hyperplan des matrices de trace nulle.*

(b) Montrer que le sous-espace vectoriel engendré par les matrices nilpotentes de rang 1 est le même hyperplan.

(c) En déduire que le sous-espace vectoriel engendré par les matrices d'une classe de similitude quelconque de matrices nilpotentes est l'hyperplan des matrices de trace nulle.

Exercice 6.7. — *Une rotation de $SO(3)$ sera notée par $r = (k, \theta)$ où k est le vecteur unitaire de l'axe de la rotation et θ son angle. Soient alors $r = (OA, 2\alpha)$ et $s = (OB, 2\beta)$ deux rotations telles que $\frac{\alpha}{\pi}$ et $\frac{\beta}{\pi}$ soient irrationnels. Montrez que si l'on excepté une infinité dénombrable de valeurs pour la mesure c de l'angle entre les axes OA et OB, le groupe engendré par r et s est dense dans $SO(3)$.*

7. Solutions

6.1 On raisonne par récurrence sur p_u, le cas $p_u = 0$ correspondant à $u = Id$. Supposons donc $p_u > 0$ et soit $x \in F_u^\perp$ non nul et soit $y = u(x) \neq x$ car $x \notin F_u$; on a $y \in F_u^\perp$ car F_u étant stable par u, $F_u^\perp$ l'est aussi. De plus comme x et y on même norme, on en déduit que $(x - y, x + y) = 0$ (triangle isocèle). On considère alors la réflexion τ définie par $x - y$ de sorte que $\tau(x - y) = y - x$ et $\tau(x + y) = x + y$ soit donc $\tau(y) = x$ avec $\tau_{|F_u} = Id$. Ainsi on a $F_u \subset F_{\tau \circ u}$ ce dernier contenant x de sorte que $p_{\tau \circ u} < p_u$ et on conclut par récurrence.

En outre si u est le produit de r réflexions alors F_u est clairement de dimension supérieure ou égale à $n-r$ (l'intersection de r hyperplans) soit donc $p_u \leq r$.

6.2 Le cas $n = 3$ est évident en remarquant que si τ est une réflexion, alors $-\tau$ est un renversement de sorte que le produit de deux réflexions (et donc tout produit d'un nombre pair) est un produit de deux renversements $\tau_1 \circ \tau_2 = (-\tau_1) \circ (-\tau_2)$.

Pour $n \geq 3$, soient τ_1 et τ_2 des réflexions par rapport aux hyperplans H_1 et H_2 et $u = \tau_1 \circ \tau_2$. Soit alors $V \subset H_1 \cap H_2$ un sous-espace de dimension $n-3$: $u_{|V} = Id$ et $V^\perp$ est stable sous u. D'après le cas $n = 3$, on a $u_{V^\perp} = \sigma_1 \circ \sigma_2$ où σ_1, σ_2 sont des renversements de $V^\perp$. On obtient le résultat en prolongeant les σ_i par l'identité sur V.

6.3 On décompose l'espace $E = E_1 \oplus E_1^\perp = E_2 \oplus E_2^\perp$ où $E_i = \mathrm{Ker}(u_i - Id)$. On choisit alors des bases orthonormées (e_i^1) et (e_i^2) de E adaptées à ces décompositions. Soit alors u tel que $u(e_i^1) = e_i^2$; u est une isométrie et quitte à changer ϵ_1 en $-\epsilon_1$, on peut supposer que u est positive. On vérifie alors immédiatement que $u \circ u_1 \circ u^{-1} = u_2$.

L'inclusion $D(O(q)) \subset O^+(q)$ est évidente ; réciproquement soient τ_1 et τ_2 deux réflexions et soit u tel que $u \circ \tau_1 \circ u^{-1} = \tau_2$ de sorte que $\tau_1 \circ \tau_2 = [\tau_1, u]$. Comme tout élément de $O^+(q)$ est le produit d'un nombre pair de réflexions, on obtient bien l'inclusion réciproque.

De même pour montrer que $O^+(q) \subset D(O^+(q))$ pour $n \geq 3$, il suffit de montrer que tout renversement est un commutateur. Soit V un sous-espace de dimension 3 et (e_1, e_2, e_3) une base orthonormée. Soient $\sigma_1, \sigma_2, \sigma_3$ les renversements définis par $(\sigma_i)_{|V^\perp} = Id$ et $\sigma_i(e_i) = e_i)$ et donc $\sigma_i(e_j) = -e_j$ pour $i \neq j$. On a alors $\sigma_3 = \sigma_1 \circ \sigma_2$. En outre il existe $u \in O^+(q)$ tel que $\sigma_2 = u \circ \sigma_1 \circ u^{-1}$ et donc $\sigma_3 = [\sigma_1, u]$.

6.4 On procède par récurrence sur la dimension, les cas $n = 1$ et $n = 2$ étant bien connus. Si u admet une valeur propre réelle (forcément ± 1), c'est terminé (en particulier si n est impair). Sinon soit $\lambda \in \mathbb{C}$ une valeur propre du complexifié de $u_{\mathbb{C}}$, de sorte que $\bar{\lambda}$ est aussi valeur propre. Soit alors $x \in E \otimes_{\mathbb{R}} \mathbb{C}$ un vecteur propre du complexifié relativement à λ et soit $\bar{x}$ son conjugué qui est alors propre pour $\bar{\lambda}$ relativement à $u_{\mathbb{C}}$. Le plan complexe $P = \mathbb{C}x + \mathbb{C}\bar{x}$ est alors invariant par $u_{\mathbb{C}}$. On remarque alors que les vecteurs $\frac{x+\bar{x}}{2}$ et $\frac{x-\bar{x}}{2i}$ sont réels et forment une base de P de sorte que le plan réel qu'ils engendrent et stable sous u.

6.5 Rappelons qu'une matrice de Householder associée au vecteur colonne $v \in \mathbb{C}^n - \{0\}$ est $H(v) = I - 2\frac{vv^*}{v^*v}$. La matrice vv^* est hermitienne de rang 1 ; ses valeurs propres sont 0 à l'ordre $n-1$ et $\mathrm{tr}(vv^*) = v^*v$. Ainsi les valeurs propres de $H(v)$ qui est clairement hermitienne et unitaire sont 1 à l'ordre $n-1$ et -1 à l'ordre 1.

Réciproquement si H est une matrice hermitienne unitaire, ses valeurs propres sont réelles de module 1 ; vu l'hypothèse sur la signature et le fait que H est diagonalisable dans une base orthonormée $H = UDU^*$ avec $D = \mathrm{diag}(-1, 1, \cdots, 1)$, c'est à dire $H = UH(e_1)U^{-1} = H(U(e_1))$.

6.6 Dans les trois cas, l'inclusion est immédiate. On va montrer directement (b). Comme d'habitude cela repose sur un petit calcul en dimension 2, à savoir : $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ est semblable à $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ en considérant la nouvelle base $e_1 + e_2$ et $e_1 - e_2$.

Soit alors A une matrice de trace nulle ; en ajoutant une combinaison linéaire de matrice nilpotente de rang 1, on se ramène à A diagonale $\mathrm{diag}(a_1, \cdots, a_b)$ avec $\sum_i a_i = 0$ que l'on écrit sous la forme

$$\mathrm{diag}(a_1, -a_1, 0, \cdots, 0) + \mathrm{diag}(0, a_2 + a_1, a_3, \cdots, a_n).$$

D'après le calcul précédent la première matrice est semblable à une combinaison linéaire de matrice nilpotentes de rang 1 ; la deuxième aussi par hypothèse de récurrence.

(c) L'orbite d'une classe de similitude quelconque contient dans son adhérence la classe de similitude des matrices nilpotentes de rang 1. On conclut alors d'après (b).

6.7 Si P_3 est le plan OAB et $P_2 = (OA, -\alpha)(P_3)$ alors r s'écrit comme le produit des réflexions par rapport aux plans P_2 et P_3. De même s est le produit de P_1 et P_2 où $P_1 = (OB, \beta)(P_3)$.

Afin d'approcher une rotation $(k, 2\theta)$, on approche son axe puis son angle. Pour approcher $\mathbb{R}.k$, on approche les plans qu'il détermine avec OA, et OB. D'après le théorème de Jacobi-Kronecker, ils sont respectivement approchés par $P_2' = (OA, -p\alpha)(P_3)$ et $P_1' = (OB, q\beta)(P_3)$ si p et q sont des entiers adéquats. Ainsi $\mathbb{R}k' = P_1' \cap P_2'$ approche $\mathbb{R}k$.

Puisque $r^p = (OA, 2p\alpha)) = (P_3)(P_2')$ et $s^q = (OB, 2q\beta) = (P_1')(P_3)$, on a $s^q r^p = (P_1')(P_2')$ dont la mesure $2\gamma'$ de l'angle est donnée par la formule fondamentale de la trigonométrie sphérique

$$\cos\gamma' = \sin(p\alpha)\sin(q\beta)\cos c - \cos(p\alpha)\cos(q\beta)$$

On cherche $\frac{\gamma'}{\pi}$ irrationnel ; la formule précédente montre que si p et q décrivent les entiers et si $\frac{\gamma'}{\pi}$ décrit les rationnels, $\cos c$ ne prend qu'une infinité dénombrable de valeurs. On choisit alors c pour que $\cos c$ n'appartienne pas à cet ensemble de valeurs. Il en résulte alors que $\frac{\gamma'}{\pi}$ est irrationnel pour tout p, q. Le théorème de Jacobi-Kronecker montre alors que l'on peut choisir n pour que $2n\gamma'$ approche 2θ de sorte que $(s^q r^p)^n$ approche $(k, 2\theta)$.

Références

[1] D. Perrin. *Cours d'algèbre*. Ellipses, 1998.

Pascal Boyer