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

1 Généralités

Définition 1. Soit G un groupe et une partie S de G. On définit le *sous-groupe de G engendré par S*, noté $\langle S \rangle$, comme le plus petit sous-groupe de G (au sens de l'inclusion) contenant S. On dit que S est une *partie génératrice* de G si $\langle S \rangle = G$, et que G est de *type fini* s'il est engendré par une partie génératrice finie.

Proposition 1. *$\langle S \rangle$ est l'intersection des sous-groupes de G contenant S (ce qui justifie l'existence et l'unicité dans la définition précédente). On a de plus $\langle S \rangle = \{s_1^{\varepsilon_1} \dots s_n^{\varepsilon_n} \mid n \in \mathbf{N}, s_i \in S, \varepsilon_i \in \{-1, 1\}\}$.*

Corollaire 1. *Un groupe de type fini est dénombrable.*

Proposition 2. *Un groupe fini de cardinal n a une partie génératrice de cardinal au plus $\log_2 n$. Cette borne est optimale (cf $(\mathbf{Z}/2\mathbf{Z})^n$).*

2 Groupes abéliens

2.1 Groupes monogènes

Définition 2. Un groupe G engendré par un seul élément est dit *monogène*.

Proposition 3. *Un groupe monogène est isomorphe à $\mathbf{Z}$ ou $\mathbf{Z}/n\mathbf{Z}$ pour un $n \in \mathbf{N}^*$ via le passage au quotient de l'application $\mathbf{Z} \to G$, $i \mapsto a^i$, avec a un générateur de G.*

Proposition 4. *Les générateurs de $\mathbf{Z}/n\mathbf{Z}$ sont les classes des entiers premiers à n, donc $\mathbf{Z}/n\mathbf{Z}$ admet exactement $\varphi(n)$ générateurs distincts.*

Proposition 5. *Tout groupe tel que G/Z soit cyclique est abélien.*

Application. Structure des groupes d'ordre p^2.

Théorème 1. *L'ensemble des générateurs de $\mathbf{Z}/n\mathbf{Z}$ est égal à l'ensemble des inversibles de $\mathbf{Z}/n\mathbf{Z}$, groupe isomorphe à $Aut(\mathbf{Z}/n\mathbf{Z})$.*

Théorème 2. *Structure des automorphismes.*

Application. Caractérisation des $\mathbf{Z}/n\mathbf{Z}$ dont le groupe des automorphismes est cyclique.

Application. Il existe exactement $n \wedge m$ morphismes de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{Z}/m\mathbf{Z}$.

Proposition 6. *Les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont monogènes. Plus exactement, il existe un sous-groupe d'ordre d de $\mathbf{Z}/n\mathbf{Z}$ ssi $d|n$, auquel cas un tel sous-groupe est unique.*

Proposition 7. *Les générateurs de $\mathbf{Z}$ sont exactement 1 et -1. Les sous-groupes de $\mathbf{Z}$ sont les $n\mathbf{Z}$, avec $n \in \mathbf{N}$.*

Exemple. Pour $m, n \in \mathbf{Z}$, le sous-groupe de $\mathbf{Z}$ $\langle m, n\rangle$ est $\langle m \wedge n\rangle$.

Exemple. Les sous-groupes additifs de $\mathbf{R}$ sont :
– les sous-groupes denses de $\mathbf{R}$ ou
– les groupes monogènes du type $x\mathbf{Z}$, avec $x \in \mathbf{R}$.

2.2 Groupes abéliens de type fini

Théorème 3. *Soit G un groupe abélien fini. Alors $\exists! a_n|a_{n-1}|\dots|a_1$, $a_n > 1 : g \approx \mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_n\mathbf{Z}$.*

Application. Critère d'isomorphie de deux groupes abéliens finis.

Théorème 4. *Soit G un groupe abélien de type fini. Alors $\exists! r \in \mathbf{N}$, $\exists! a_n|a_{n-1}|\dots|a_1$, $a_n > 1 : g \approx \mathbf{Z}^r \times \mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_n\mathbf{Z}$.*

3 Exemples classiques

3.1 Groupes symétrique et alterné

Proposition 8. *Les transpositions engendrent $\mathfrak{S}_n$. On a de plus les systèmes générateurs minimaux suivants :*
– $(1,2),(1,3),\dots,(1,n)$.
– $(1,2),(2,3),\dots,(n-1,n)$.
De plus, une partie génératrice de $\mathfrak{S}_n$ formée uniquement de transpositions ent de cardinal au moins $n-1$.

Corollaire 2. *Il existe un seul morphisme non trivial de $\mathfrak{S}_n$ dans $\mathbf{C}^*$, appelé signature. Ainsi, $\mathfrak{A}_n$ est le seul sous-groupe d'indice 2 de $\mathfrak{S}_n$.*

Proposition 9. *La transposition $(1,2)$ et le cycle $(1,2\dots n)$ engendrent $\mathfrak{S}_n$.*

Proposition 10. *Pour tout $n \geq 3$, le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles.*

Corollaire 3. *Pour tout n, $\mathfrak{A}_n$ est engendré par les carrés des éléments de $\mathfrak{S}_n$.*

Théorème 5. *$\mathfrak{A}_n$ est simple pour tout $n \geq 5$.*

Proposition 11 ([Per p. 31])**.** *Soit $\varphi \in Aut(\mathfrak{S}_n)$; si φ transforme toute transposition en une transposition, alors φ est intérieur.*

Théorème 6. *Pour tout $n \neq 6$, tout automorphisme de $\mathfrak{S}_n$ est intérieur.*

3.2 Groupe linéaire

Soit k un corps et E un k-e.v. de dimension finie n.

Définition 3. On appelle *dilatation* de E tout endomorphisme ayant pour matrice dans une base convenable : $\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \lambda \end{pmatrix}$, avec $\lambda \in k^*$, $\lambda \neq 1$.

On appelle *transvection* de E tout endomorphisme ayant pour matrice dans une base convenable : $\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & 1 \\ & & & 1 \end{pmatrix}$, avec $\lambda \in k^*$, $\lambda \neq 1$.

Proposition 12. *Soit H un hyperplan de E d'équation donnée par $f \in E^*$. Soit $u \in Gl(E)$, $u \neq Id$ tq $u_{|H} = Id$. Lpsse :*

(i) *u est une transvection d'hyperplan H et de droite D*

(ii) *$det(u) = 1$*

(iii) *u n'est pas diagonalisable*

(iv) *on a $D = Im(u - Id) \subset H$*

(v) *l'homomorphisme induit $E/H \to E/H$ est l'identité sur E/H*

(vi) *il existe $a \in H \setminus \{0\}$ tq $\forall x \in E,\ u(x) = x + f(x)a$*

Proposition 13. *Soit τ une transvection de droite D et d'hyperplan H. Soit $u \in Gl(E)$. Alors $u\tau u^{-1}$ est une transvection de droite $u(D)$ et d'hyperplan $u(H)$.*

Corollaire 4. *Le centre de $Gl(E)$ est formé exactement des homotéties de E, il est donc isomorphe à k^*. Le centre de $Sl(E)$ est la trace du centre de $Gl(E)$ sur $Sl(E)$, il est donc isomorphe au groupe des racines n-ièmes de k.*

Théorème 7. *Les transvections engendrent $Sl(E)$.*

Corollaire 5. *Les transvections et les dilatations engendrent $Gl(E)$.*

Applications

Proposition 14. *$Sl_n(\mathbf{R})$ est connexe.*

Application ([FGN2 p. 179]). Pour $n \geq 2$, toute matrice de $Gl_n(K)$ s'écrit comme un produit de matrices de trace nulle.

Théorème 8. *On a $D(Gl(E)) = Sl(E)$ sauf si $n = 2$ et $k = \mathbf{F}_2$.*
On a $D(Sl(E)) = Sl(E)$ sauf si $n = 2$ et $k = \mathbf{F}_2$ ou $n = 2$ et $k = \mathbf{F}_3$.

Théorème 9 (Frobenius-Zolotarev)**.** *Soit p un nompbre premier impair et E un $\mathbf{F}_p$-espace vectoriel de dimension finie. Alors pour tout $u \in Gl(E)$, on a $\varepsilon(u) = \left(\frac{det(u)}{p}\right)$.*

3.3 Groupe orthogonal

Soit E un espace vectoriel réel de dimension finie n muni d'une forme quadratique définie positive q.

Théorème 10. *Forme canonique des éléments de O_n [Per p.147].*

Théorème 11. *Le groupe orthogonal associé à q, noté $O(q)$ est engendré par les réflexions orthogonales. Plus précisément, tout élément de $O(q)$ est le produit d'au plus n réflexions.*

Application. Cf Perrin p. 199 !

3.4 Groupe Diédral

Définition, générateurs et relations.

3.5 Groupe modulaire

Définition 4. On appelle *groupe modulaire* le groupe $\Gamma = PSl_2(\mathbf{R})$. On le fait agir sur le demi-plan de Poincaré $\mathbf{H}$ par homographies : $\begin{pmatrix} a & b \\ c & d \end{pmatrix} * z = \frac{az+b}{cz+d}$.

Proposition 15. *Un domaine fondamental pour l'action de Γ sur le demi-plan de Poincaré est l'ensemble $D = \{z \in \mathbf{H} \mid |z| \geq 1, -1/2 \leq Re(z) \leq 1/2\}$.*

Théorème 12. *Le groupe Γ est engendré par les matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.*

Décompositions classiques (polaire, choleski, Cartan, Iwasawa, LU) .

4 Groupes libres

Référence groupes libres ? Marshall ?