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

1 Définition

Proposition 1. *Soit G un groupe et soit $(H_i)_{i\in I}$ une famille de sous-groupes de G. Alors $\bigcap H_i$ est un sous-groupe de G.*

Définition 2. Soit G un groupe et A une partie de G. On appelle sous-groupe engendré par A l'intersection de tous les sous-groupes de G qui contiennent A. On note ce sous-groupe $\langle A\rangle$.

Proposition 3. *Soit G un groupe et A une partie génératrice de G. Soient f et g des morphismes de G dans G'. Si $\forall a \in A$, $f(a) = g(a)$ alors $f = g$.*

2 Groupes monogènes

Définition 4. On appelle groupe monogène un groupe engendré par un seul élément. Si de plus il est fini, on dit qu'il est cyclique.

Proposition 5. *Soit G un groupe monogène. Si G est infini, alors G est isomorphe à $\mathbf{Z}$. Si G est fini de cardinal n, alors G est isomorphe à $\mathbf{Z}/n\mathbf{Z}$.*

Définition 6. On appelle fonction indicatrice d'Euler et on note $\varphi(n)$ le nombre d'entiers compris entre 1 et n qui sont premiers avec n.

Proposition 7. *Le groupe $\mathbf{Z}/n\mathbf{Z}$ est engendré par les $\overline{k}$ où k est premier avec n. Il possède donc $\varphi(n)$ générateurs.*

Proposition 8. *Pour tout d divisant n, le groupe $\mathbf{Z}/n\mathbf{Z}$ possède un unique sous-groupe d'ordre d, engendré par la classe de $\frac{n}{d}$.*

Proposition 9. *Pour tout $n \in \mathbf{N}^*$, on a $n = \sum_{d|n} \varphi(d)$.*

Application 10. Soit K un corps et G un sous-groupe fini du groupe multiplicatif K^*. Alors G est cyclique.

Proposition 11. *Soient $n, m \in \mathbf{N}^*$ et soit d leur PGCD. Alors il existe d morphismes entre les groupes $\mathbf{Z}/n\mathbf{Z}$ et $\mathbf{Z}/m\mathbf{Z}$. Ils sont de la forme $x[n] \mapsto ax[m]$ où a est un élément dont l'ordre dans $\mathbf{Z}/m\mathbf{Z}$ divise n et m.*

Corollaire 12. *Il y a $\varphi(n)$ automorphismes de $\mathbf{Z}/n\mathbf{Z}$. Ceux-ci sont de la forme $\overline{x} \mapsto \overline{kx}$ où k est premier avec n. Le groupe* $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$ *est isomorphe à $(\mathbf{Z}/n\mathbf{Z})^*$.*

3 Le groupe symétrique

Proposition 13. *Soit $\sigma \in \mathfrak{S}_n$. Alors l'action de $\mathfrak{S}_n$ sur $[\![1;n]\!]$ induit une action de $\langle\sigma\rangle$ sur $[\![1;n]\!]$. Notons $F_1, \dots, F_r$ les orbites pour cette action et définissons :*

$$\sigma_i(x) = \begin{cases} x & si\ x \notin F_i \\ \sigma(x) & si\ x \in F_i \end{cases}$$

Alors les σ_i sont des cycles d'ordre $|F_i|$, disjoints, et $\sigma = \sigma_1 \cdots \sigma_r$. Ainsi, toute permutation se décompose de façon unique en produit de cycles à supports disjoints.

Proposition 14 (générateurs de $\mathfrak{S}_n$)**.** *Le groupe $\mathfrak{S}_n$ est engendrés par les familles suivantes :*

1. *l'ensemble de tous les k–cycles pour $k \in \{1, \dots, n\}$;*
2. *l'ensemble de toutes les transpositions ;*
3. *l'ensemble des transpositions de la forme $(1\ i)$ pour i de 2 à n ;*
4. *l'ensemble des transpositions de la forme $(i\ i+1)$ pour i de 1 à n.*

Théorème 15. *Pour $n \geqslant 2$, il existe un unique morphisme non trivial de $\mathfrak{S}_n$ dans $\mathbf{C}^*$. On l'appelle la signature et on la note ε.*

Définition 16. Pour $n \geqslant 2$, on note $\mathfrak{A}_n$ le noyau de la signature.

Proposition 17 (générateurs de $\mathfrak{A}_n$)**.**

1. *$\mathfrak{A}_n$ est engendré par les produits d'un nombre pair de transpositions.*
2. *Pour $n \geqslant 3$, $\mathfrak{A}_n$ est engendré par les 3–cycles.*
3. *Pour $n \geqslant 4$, $\mathfrak{A}_n$ est engendré par les doubles transpositions.*
4. *$\mathfrak{A}_n$ est engendré par les $(1\ 2\ i)$ pour i de 3 à n.*

Lemme 18. *Soient $a_1, \dots, a_{n-2}$ et $b_1, \dots, b_{n-2}$ deux listes d'éléments distincts de $\{1, \dots n\}$. Alors il existe $\sigma \in \mathfrak{A}_n$ tel que $\sigma(a_i) = b_i$.*

Théorème 19. *Pour $n \geqslant 5$, $\mathfrak{A}_n$ est un groupe simple.*

Corollaire 20. *Pour $n \geqslant 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.*

Lemme 21. *Si un automorphisme de $\mathfrak{S}_n$ transforme toute transposition en transposition, alors il est intérieur.*

Théorème 22. *Pour $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont tous intérieurs.*

4 Le groupe linéaire

On considère E un espace vectoriel de dimension finie n sur un corps $\mathbf{K}$.

Définition 23. On appelle matrices élémentaires les trois types de matrices suivants :

1. On appelle matrices de dilatation les matrices $D_{i,\alpha}^{(k)} = \begin{bmatrix} I_{i-1} & & \\ & \alpha & \\ & & I_{k-i-1} \end{bmatrix}$ avec $\alpha \in \mathbf{K}^*$.
2. On appelle matrices de transvection les matrices $T_{i,j,\beta}^{(k)} = I_k + \beta E_{i,j}$ avec $\beta \in \mathbf{K}^*$ et $i \neq j$.
3. On appelle matrices de permutation les matrices $P_{i,j}^{(k)} = P_{j,i}^{(k)}$ de la forme :
$$\begin{bmatrix} I_{i-1} & & & & \\ & 0 & \cdots & 1 & \\ & & I_{j-i-1} & & \\ & 1 & \cdots & 0 & \\ & & & & I_{k-j-1} \end{bmatrix}$$

Proposition 24. *Soit $M \in \mathcal{M}_{n,p}(\mathbf{K})$. Les opérations élémentaires sur les lignes de M sont obtenues par multiplication à gauche par des matrices élémentaires :*

Matrice	$D_{i,\alpha}^{(n)} M$	$T_{i,j,\beta}^{(n)} M$	$P_{i,j}^{(n)} M$
Opération	$L_i \leftarrow \alpha L_i$	$L_i \leftarrow L_i + \beta L_j$	$L_i \leftrightarrow L_j$

De même, les opérations élémentaires sur les colonnes de M sont obtenues par multiplication à droite par des matrices élémentaires :

Matrice	$M D_{i,\alpha}^{(p)}$	$M T_{i,j,\beta}^{(p)}$	$M P_{i,j}^{(p)}$
Opération	$C_i \leftarrow \alpha C_i$	$C_i \leftarrow C_j + \beta C_i$	$C_i \leftrightarrow C_j$

Lemme 25. *Les matrices $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ et $\left[\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right]$ sont des produits de matrices de transvection.*

Théorème 26. *Le groupe $\mathrm{SL}_n(\mathbf{K})$ est engendré par les matrices de transvections. Le groupe $\mathrm{GL}_n(\mathbf{K})$ est engendré par les matrices de transvections et les matrices de dilatation.*

Corollaire 27. *Si K est $\mathbf{R}$ ou $\mathbf{C}$, alors $\mathrm{SL}_n(\mathbf{K})$ est connexe par arcs.*

Proposition 28. *Soit H un hyperplan de E et soit $u \in \mathrm{GL}(E)$ tel que $u_{|H} = \mathrm{id}_H$. Les assertions suivantes sont équivalentes :*

1. *$\det u = \lambda \neq 1$.*
2. *u admet une valeur propre $\lambda \neq 1$ et u est diagonalisable.*
3. *$D = \mathrm{Im}(u - \mathrm{id}) \not\subseteq H$.*

4. *Il existe une base dans laquelle u a pour matrice une matrice de dilatation.*

Dans ces conditions, on dit que u est une dilatation d'hyperplan $H = \ker(u - \mathrm{id})$, de droite D et de rapport λ.

Proposition 29. *Soit $H = \ker f$ un hyperplan de E et soit $u \in \mathrm{GL}(E)$ tel que $u_{|H} = \mathrm{id}_H$ et $u \neq \mathrm{id}$. Les assertions suivantes sont équivalentes :*

1. $\det u = 1$.
2. *u n'est pas diagonalisable.*
3. $D = \mathrm{Im}(u - \mathrm{id}) \subseteq H$.
4. *Il existe $a \in H$ non nul tel que $\forall x \in E$, $u(x) = x + f(x)a$.*
5. *Il existe une base dans laquelle u a pour matrice une matrice de transvection.*

Dans ces conditions, on dit que u est un transvection d'hyperplan H et de droite D.

Théorème 30. *Le groupe $\mathrm{SL}(E)$ est engendré par les transvections. Le groupe $\mathrm{GL}(E)$ est engendré par les transvections et les dilatations.*

5 Le groupe orthogonal

On considère maintenant E un espace euclidien de dimension n.

Définition 31. On appelle réflexion une symétrie orthogonale par rapport à un hyperplan. On appelle retournement une symétrie orthogonal par rapport à un s.e.v. de dimension $n-2$.

Théorème 32. *Soit $u \in \mathrm{O}(E)$, notons $r = \mathrm{rg}(u - \mathrm{id}_E)$. Alors u s'écrit comme le produit d'exactement r réflexions, et ce nombre est minimal.*

Corollaire 33. *Si $n \geqslant 3$, $\mathrm{SO}(E)$ est engendré par les retournements.*

Théorème 34 (réduction des isométries)**.** *Soit $A \in \mathrm{O}_n(\mathbf{R})$. Alors il existe $Q \in \mathrm{O}_n(\mathbf{R})$ tel que :*

$$A = Q \begin{bmatrix} R_{\theta_1} & & & & & & \\ & \ddots & & & & & \\ & & R_{\theta_p} & & & & \\ & & & \varepsilon_1 & & & \\ & & & & \ddots & & \\ & & & & & \varepsilon_q \end{bmatrix} {}^{\mathrm{t}}Q,\ R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix},\ \varepsilon_i \in \{\pm 1\}$$

Corollaire 35. *Le groupe $\mathrm{SO}_n(\mathbf{R})$ est connexe par arcs.*

Théorème 36. *Le groupe $\mathrm{SO}_3(\mathbf{R})$ est simple.*

Développements

1. Automorphismes de $\mathfrak{S}_n$. **[22]**
2. Générateurs de $\mathrm{O}(E)$. **[32]**

Références

— CALDERO et GERMONI, *Nouvelles histoires hédonistes de groupes et de géométries, tomes I et II.*
— COMBES, *Algèbre et géométrie.*
— GOURDON, *Les maths en tête, algèbre.*
— PERRIN, *Cours d'algèbre.*