108. Exemples de parties génératrices de groupes. Applications.

Introduction : On peut souvent étendre des propriétés à un groupe entier en raisonnant sur des parties génératrices.

1 Généralités

Soit G un groupe.

Définition 1. Si A est une partie de G, on appelle sous-groupe engendré par A et on note $\langle A\rangle$ l'intersection de tous les sous-groupes de G contenant A.

Proposition 2. C'est le plus petit sous-groupe de G contenant A.

***Exemple* 3.** *Si $G=\mathbb{Z}, A=\{4,14\}$, alors $\langle A\rangle = 2\mathbb{Z}$.*

Définition 4. Pour $g,h\in G$, on définit leur commutateur $[g,h]=ghg^{-1}h^{-1}$. On définit alors $D(G)$, appelé le groupe dérivé de G, comme le sous-groupe engendré par les commutateurs.

2 Groupes abéliens de type fini

2.1 Groupes cycliques

Définition 5. G est dit monogène s'il existe $g\in G$ tel que $G=\langle g\rangle$, et cyclique s'il est de plus fini.

***Exemple* 6.** *Pour tout $n\in\mathbb{N}^*, \mathbb{Z}/n\mathbb{Z}$ et $\mathbb{U}_n$ sont cycliques d'ordre n. Tout groupe d'ordre premier est cyclique.*

Proposition 7. Tout groupe monogène est abélien.

Théorème 8. Tout groupe monogène infini est isomorphe à $\mathbb{Z}$. Tout groupe cyclique d'ordre $n\in\mathbb{N}^*$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Remarque 9. Si G est cyclique, tout morphisme de G dans un groupe est entièrement déterminé par l'image d'un générateur de G.

***Application* 10.** *Si G est un groupe, on appelle dual de G l'ensemble $\widehat{G}$ des morphismes de G dans $\mathbb{C}^*$. Si G est cyclique, on a la table de caractères de G, et G est isomorphe à $\widehat{G}$.*

Proposition 11. Soit $\overline{k}\in\mathbb{Z}/n\mathbb{Z}$. $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ ssi $k\wedge n=1$.

Définition 12. On définit l'indicatrice d'Euler $\varphi(n)=\#\{k\in[\![1,n-1]\!], k\wedge n=1\}$.

Proposition 13. On a $\varphi(n)=\#(\mathbb{Z}/n\mathbb{Z})^*$, et $\varphi(n)=\sum_{d|n}\varphi(d)$.

***Exemple* 14.** *Les générateurs de $\mathbb{Z}/12\mathbb{Z}$ sont $1,5,7,11$ et $\varphi(12)=4$.*

Proposition 15. Si $d|n$, $\mathbb{Z}/n\mathbb{Z}$ possède un unique sous-groupe d'ordre d, il est engendré par $\frac{\overline{n}}{d}$.

Proposition 16. Pour tout $n\in\mathbb{N}^*$, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})\simeq(\mathbb{Z}/n\mathbb{Z})^*$.

Théorème 17. Si q est un entier primaire, $\mathbb{F}_q^*$ est cyclique d'ordre $q-1$.

2.2 Cas général

Théorème 18 (chinois)**.** Soient $n_1,\cdots,n_k\in\mathbb{N}^*$. Alors $\mathbb{Z}/(n_1\cdots n_k)\mathbb{Z}$ est cyclique ssi les $(n_i)_i$ sont deux à deux premiers entre eux.

Corollaire 19. Si $m\wedge n=1$, alors $\varphi(mn)=\varphi(m)\varphi(n)$, et si n a pour décomposition en nombres premiers $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, on a $\varphi(n)=n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$.

***Application* 20.** *L'ensemble des $x\in\mathbb{Z}$ vérifiant $x\equiv 2 \mod 4, x\equiv 3 \mod 5, x\equiv 1 \mod 9$ est $\{118+180k, k\in\mathbb{Z}\}$.*

Théorème 21. Si G groupe abélien fini, il existe une unique suite d'entiers non nuls $d_1|\cdots|d_k$ tels que $G\simeq\mathbb{Z}/d_1\mathbb{Z}\times\cdots\times\mathbb{Z}/d_k\mathbb{Z}$.

***Application* 22.** *À isomorphisme près, il existe 6 groupes abéliens d'ordre 600.*

Définition 23. G est dit de type fini s'il possède une partie génératrice finie.

Théorème 24. Si G groupe abélien de type fini, il existe un unique $n\in\mathbb{N}$ et une unique suite d'entiers non nuls $d_1|\cdots|d_k$ tels que $G\simeq\mathbb{Z}^n\times\mathbb{Z}/d_1\mathbb{Z}\times\cdots\times\mathbb{Z}/d_k\mathbb{Z}$.

3 Exemples pour des groupes non abéliens

3.1 Groupes symétriques et alternés

Proposition 25. Pour $n\in\mathbb{N}^*$, le groupe symétrique $\mathcal{S}_n$ est engendré par les transpositions.

***Application* 26.** *La signature est l'unique morphisme de groupes non trivial de $\mathcal{S}_n$ dans $\mathbb{C}^*$.*

***Application* 27.** *$\mathcal{S}_4$ est isomorphe au groupe des isométries préservant le tétraèdre régulier. On peut en déduire la table de caractères de $\mathcal{S}_4$.*

Proposition 28. $\mathcal{S}_n$ possède également les parties génératrices suivantes :
- L'ensemble des transpositions de la forme $(1, i), 2 \leq i \leq n$.
- L'ensemble des transpositions de la forme $(i, i+1), 1 \leq i \leq n-1$.
- La transposition $(1, 2)$ et le cycle $(1, 2, \cdots, n)$.

Proposition 29. Pour $n \geq 3$, les 3-cycles engendrent $\mathcal{A}_n$. De plus, pour $n \geq 5$, ils sont conjugués dans $\mathcal{A}_n$.

Théorème 30. Pour $n \geq 5$, $\mathcal{A}_n$ est simple.

Corollaire 31. Pour $n \geq 5, D(\mathcal{S}_n) = D(\mathcal{A}_n) = \mathcal{A}_n$.

3.2 Groupes diédraux

Définition 32. Pour $n \in \mathbb{N}^*$, on définit le groupe diédral D_n comme le groupe des isométries du plan conservant le polygone régulier à n côtés.

Proposition 33. Si on note r la rotation d'angle $\frac{2\pi}{n}$ et s une symétrie appartenant à $\mathcal{D}_n$, alors $D_n = \langle r, s \rangle$ et on a $r^n = 1, s^2 = 1$ et $(sr)^2 = 1$.

***Application* 34.** *Table de caractères de D_4.*

4 Parties génératrices en algèbre linéaire

4.1 Groupe linéaire

Soient K un corps, E un K-espace vectoriel de dimension n.

Définition 35. Soient H un hyperplan de E, D un supplémentaire de H, $\lambda \neq 1$. On appelle dilatation d'hyperplan H, de droite D et de rapport λ un automorphisme $u \in GL(E)$ tel que $H = \ker(u - \mathrm{Id}), D = \ker(u - \lambda \mathrm{Id})$.

Proposition 36. Soit $u \in GL(E)$ fixant un hyperplan H. On a équivalence entre : (i). u dilatation, (ii). $\lambda := \det(u) \neq 1$, (iii). u possède une valeur propre distincte de 1 et u diagonalisable, (iv). $\mathrm{Im}(u - \mathrm{Id}) \not\subset H$, (v). u a pour matrice $diag(1, \cdots, 1, \lambda)$ dans une certaine base.

Corollaire 37. Deux dilatations sont conjuguées ssi elles ont même rapport.

Définition 38. On appelle transvection un élément de $SL(E)$ distinct de Id_E fixant un hyperplan.

Proposition 39. Soit $u \in GL(E)$ fixant un hyperplan $H = \ker(\varphi)$. On a équivalence entre : (i). u transvection, (ii). $\exists a \in H, \forall x \in E, u(x) = x + \varphi(x)a$, (iii). u non diagonalisable, (iv). $\mathrm{Im}(u - \mathrm{Id}) \neq \{0\}$ et $\mathrm{Im}(u - \mathrm{Id}) \subset H$, (v). u a pour matrice $I_n + E_{n-1,n}$ dans une certaine base.

Proposition 40. Soit $u \in GL(E)$. C'est une transvection ssi $(u - \mathrm{Id}_E)$ est de rang 1 et $(u - \mathrm{Id}_E)^2 = 0$.

Proposition 41. Deux transvections sont conjuguées dans $GL(E)$, et dans $SL(E)$ si $n \geq 3$.

Théorème 42. $SL(E)$ est engendré par les transvections, et $GL(E)$ par les transvections et les dilatations.

Corollaire 43. Si $\mathrm{car}(K) > 2$ ou $n \geq 3$, on a $D(GL_n(K)) = D(SL_n(K)) = SL_n(K)$.

***Application* 44** (Frobenius-Zolotarev)**.** *Soit $p \geq 3$ premier, soit $u \in GL_n(\mathbb{F}_p)$. Alors $\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$.*

4.2 Groupe orthogonal

On suppose ici que E est un espace euclidien.

Lemme 45. Soit $u \in GL(E)$ vérifiant $u^2 = \mathrm{Id}_E$. Alors il existe deux sous-espaces E^+, E^- de E stables par u vérifiant $E = E^+ \oplus E^-$ et $u_{E^+} = \mathrm{Id}_{E^+}, u_{E^-} = -\mathrm{Id}_{E^-}$.

Définition 46. Si $\dim(E^-) = 1$, on dit que u est une réflexion. Si $\dim(E^-) = 2$, on dit que u est un renversement.

Remarque 47. Les réflexions sont donc les symétries orthogonales par rapport à un hyperplan.

***Exemple* 48.** *Si $\dim(E) = 3$, les renversements sont les rotations d'angle π.*

Théorème 49. Tout élément de $O(E)$ s'écrit comme le produit d'au plus n réflexions.

Théorème 50. Si $\dim(E) \geq 3$, tout élément de $SO(E)$ s'écrit comme le produit d'au plus n renversements.

***Application* 51.** *$SO_3(\mathbb{R})$ est un groupe simple.*

Développements

— Théorème de Frobenius-Zolotarev.
— Simplicité de $SO_3(\mathbb{R})$.

Références

[1] F. Combes, Algèbre et géométrie, Bréal.

[2] D. Perrin, Cours d'algèbre, Ellipses.

[3] A. Szpirglas et al., Algèbre L3, Pearson.