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

1. Générateurs d'un groupe, premiers exemples

1.1. Parties génératrices et groupes libres

1. Définition-proposition. Soient G un groupe et $S \subseteq G$ une partie. Alors il existe un plus petit sous-groupe de G contenant le partie S. Il s'agit du groupe

$$\langle S \rangle \coloneqq \bigcap_{H \in \mathscr{H}_S} H$$

où l'ensemble $\mathscr{H}_S \subset \mathscr{P}(G)$ est constitué des sous-groupes de G contenant la partie S. Le sous-groupe $\langle S \rangle$ est le *sous-groupe de G engendré par la partie S*.

2. Exemple. Le groupe additif $\mathbf{Z}$ est engendré par l'entier 1, c'est-à-dire $\mathbf{Z} = \langle 1 \rangle$. L'égalité $G = \langle G \rangle$ est toujours vraie.

3. Notation. Si l'ensemble $S = \{x_1, \dots, x_n\}$ est fini, on notera $\langle S \rangle = \langle x_1, \dots, x_n \rangle$.

4. Proposition. Soient G un groupe et $S \subseteq G$ une partie. Soient $x \in G$ un élément. Alors $x \in \langle S \rangle$ si et seulement s'il existe des éléments $x_1, \dots, x_k \in S$ tels que

- $x = x_1 \cdots x_k$;
- $x_i \in S$ ou $x_i^{-1} \in S$ pour tout indice $i \in [\![1, k]\!]$.

5. Exemple. Pour tout élément $x \in G$, on a $\langle x \rangle = \{x^k \mid n \in \mathbf{N}\}$.

6. Définition. Une partie $S \subseteq G$ *génère* un groupe G si $G = \langle S \rangle$. On dit que c'est une partie génératrice du groupe G.

7. Exemple. Pour tout entier $n \geqslant 1$, la partie $\{1\}$ génère le groupe $\mathbf{Z}/n\mathbf{Z}$.

8. Définition. Le *groupe dérivé* d'un groupe G est le sous-groupe $\mathrm{D}(G)$ engendré par les *commutateurs* $[x, y] \coloneqq xyx^{-1}y^{-1}$ avec $x, y \in G$.

9. Exemple. Le groupe dérivé d'un groupe abélien est trivial. On a $\mathrm{D}(\mathfrak{A}_n) = \mathfrak{A}_n$.

10. Proposition. Le groupe quotient $G^{\mathrm{ab}} \coloneqq G/\mathrm{D}(G)$ est abélien. Soit A un groupe abélien. Alors tout morphisme $G \longrightarrow A$ se factorise en un morphisme $G^{\mathrm{ab}} \longrightarrow A$.

11. Définition. Soient A et A^{-1} deux ensembles de même cardinal. On les notes

$$A = \{x_i\}_{i \in I} \qquad \text{et} \qquad A^{-1} = \{x_i^{-1}\}_{i \in I}.$$

Soit $\mathrm{M}(A)$ l'ensemble des suites finies de l'ensemble $A \cup A^{-1}$. On le munit de l'opération $\cdot$ définie par

$$(a_1, \dots, a_m) \cdot (b_1, \dots, b_m) = (a_1, \dots, a_n, b_1, \dots, b_m).$$

Alors le couple $(\mathrm{M}(A), \cdot)$ est un monoïde. Deux éléments de l'ensemble $\mathrm{M}(A)$ sont *équivalents* si l'un se transforme en l'entre en enlevant ou ajoutant des termes de la forme $x_i^{-1}x_i^{-1}$ avec $i \in I$. Alors l'opération $\cdot$ induit une structure de groupe sur l'ensemble quotient $\mathrm{F}(A) \coloneqq \mathrm{M}(A)/\!\sim$, appelé le *groupe libre sur l'alphabet A*, et le neutre est le mot vide $\varepsilon \coloneqq ()$.

12. Exemple. Dans l'ensemble $\mathrm{F}(\{x, y, z\})$, les mots $xyy^{-1}x$ et xx sont équivalents.

13. Proposition. Soient A un ensemble et G un groupe. Alors toute application $A \longrightarrow G$ s'étend en un unique morphisme $\mathrm{F}(A) \longrightarrow G$.

14. Définition. Soit $R \subseteq A$ un sous-ensemble. La *présentation par générateur de l'ensemble A et relation de l'ensemble R* est le groupe quotient $\langle A \mid R \rangle \coloneqq \mathrm{F}(A)/\langle R \rangle$.

15. Exemple. Le groupe $\langle 1 \mid n \cdot 1 \rangle$ est isomorphe au groupe $\mathbf{Z}/n\mathbf{Z}$. Le groupe diédral $\mathbf{D}_n$ est isomorphe au groupe $\langle s, r \mid s^2, r^n, srsr \rangle$

1.2. Groupes cycliques et de type fini

16. Définition. Un groupe est *monogène* s'il admet une partie génératrice à un élément. Un *groupe cyclique* est un groupe fini monogène.

17. Exemple. Le groupe $\mathbf{Z}/4\mathbf{Z}$ est cyclique et il est engendré par l'élément 1 ou 3. Le groupe $\mathbf{Z}$ est monogène mais non cyclique.

18. Proposition. Soit $n \geqslant 1$ un entier. Alors le groupe $\mathbf{Z}/n\mathbf{Z}$ est cyclique. Plus précisément, un élément $k \in \mathbf{Z}/n\mathbf{Z}$ le génère si et seulement si $n \wedge k = 1$.

19. Théorème. Tout groupe cyclique d'ordre n est isomorphe au groupe $\mathbf{Z}/n\mathbf{Z}$.

20. Corollaire. On considère l'indicatrice d'Euler $\varphi \colon \mathbf{N}^* \longrightarrow \mathbf{N}^*$. Alors un groupe cyclique d'ordre n possède exactement $\varphi(n)$ générateurs.

21. Proposition. Pour deux entiers $m, n \in \mathbf{Z}$, le sous-groupe $\langle m, n \rangle \subset \mathbf{Z}$ est monogène de générateur $\mathrm{pgcd}(m, n)$.

22. Théorème. Soit k un corps. Alors tout sous-groupe fini du groupe multiplicatif $k^\times$ est cyclique.

23. Exemple. Pour une puissance q d'un nombre premier, on a $\mathbf{F}_q^\times \simeq \mathbf{Z}/(q-1)\mathbf{Z}$.

24. Définition. Un groupe est *de type fini* s'il admet une partie génératrice finie.

25. Remarque. Un groupe fini est de type fini, mais la réciproque est fausse puisque le groupe $\mathbf{Z} = \langle 1 \rangle$ est de type fini bien qu'il soit infini.

26. Théorème *(de structure des groupes abéliens de type fini)*. Soit G un groupe abélien de type fini. Alors il existe des uniques entiers $e_1, \dots, e_n, r \geqslant 1$ tels que

$$G \simeq \mathbf{Z}/e_1\mathbf{Z} \times \cdots \times \mathbf{Z}/e_n\mathbf{Z} \times \mathbf{Z}^r \qquad \text{et} \qquad d_1 \mid \cdots \mid d_n.$$

2. Le groupe symétrique

2.1. Générateurs du groupe symétrique

27. Théorème. Soit $n \geqslant 1$ un entier. Alors toute permutation du groupe $\mathfrak{S}_n$ s'écrit comme un produit de cycles à support disjoints. De plus, cette écriture est unique à l'ordre près des facteurs.

28. Exemple. Dans le groupe $\mathfrak{S}_5$, on peut écrire

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} = (1\ 4\ 5)(2\ 3).$$

29. Corollaire. Deux permutations du groupe $\mathfrak{S}_n$ sont conjuguées si et seulement si, dans leurs décomposition en cycles à supports disjoints, elles ont le même nombre de k-cycles pour tout entier $k \in [\![2, n]\!]$.

30. Lemme. Tout cycle $(a_1\ \cdots\ a_r) \in \mathfrak{S}_n$ est un produit de $r-1$-transpositions. Plus précisément, on a $(a_1\ \cdots\ a_r) = (a_1\ a_r)(a_1\ a_{r-1}) \cdots (a_1\ a_2)$.

31. Corollaire. Le groupe $\mathfrak{S}_n$ est engendré par les transpositions.

32. Corollaire. Il est engendré par

- ou bien les transpositions de la forme $(1\ i)$ avec $i \in [\![2, n]\!]$;

– ou bien les transpositions de la forme $(k\ k+1)$ avec $i \in [\![2, n]\!]$;
– ou bien la transposition $(1\ 2)$ et le cycle $(1\ 2\ \cdots\ n)$.

33. Application. Les groupes des isométries positives du cube est isomorphe au groupe $\mathfrak{S}_4$.

2.2. Le groupe alterné

34. Lemme. Le produit de deux transpositions est un produit de trois cycles. Plus précisément, pour tout entier $x, y, z, t \in [\![1, n]\!]$ deux à deux distincts, on a

$$(x\ y)(x\ z) = (x\ z\ y) \qquad \text{et} \qquad (x\ y)(z\ t) = (x\ y\ z)(y\ z\ t).$$

35. Théorème. Lorsque $n \geqslant 3$, le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles.
36. Corollaire. On a $\mathrm{D}(\mathfrak{A}_n) = \mathfrak{A}_n$ lorsque $n \geqslant 5$ et $\mathrm{D}(\mathfrak{S}_n) = \mathfrak{A}_n$ lorsque $n \geqslant 2$.
37. Lemme. Le groupe $\mathfrak{A}_5$ est simple.
38. Théorème. Lorsque $n \geqslant 5$, le groupe $\mathfrak{A}_n$ est simple.
39. Corollaire. Lorsque $n \geqslant 5$, les seuls sous-groupes distingués du groupe $\mathfrak{S}_n$ sont le groupe trivial, le groupe alterné $\mathfrak{A}_n$ et lui-même.

3. Le groupe linéaire et ses sous-groupes

40. Cadre. On considère un corps k et un k-espace vectoriel E de dimension $n \geqslant 1$.

3.1. Générateurs du groupes linéaire et spécial linéaire

41. Proposition. Soient $H \subset E$ un hyperplan et $u \in \mathrm{GL}(E)$ un automorphisme tel que $u|_H = \mathrm{Id}_H$. Alors les points suivants sont équivalents :
– $\det u \neq 1$;
– l'automorphisme u admet une valeur propre $\lambda \neq 1$ et il est diagonalisable ;
– $\mathrm{Im}(u - \mathrm{Id}_E) \not\subset H$;
– dans une base convenable, la matrice de l'automorphisme u est $\mathrm{diag}(1, \ldots, 1, \lambda)$ avec $\lambda \in k^\times \setminus \{1\}$.

42. Définition. Un automorphisme $u \in \mathrm{GL}(E)$ vérifiant ces points est une *dilatation d'hyperplan H, de droite* $\mathrm{Im}(u - \mathrm{Id}_E)$ *et de rapport* λ.

43. Proposition. Soient $H \subset E$ un hyperplan et $u \in \mathrm{GL}(E) \setminus \{\mathrm{Id}_E\}$ un automorphisme tel que $u|_H = \mathrm{Id}_H$. Alors les points suivants sont équivalents :
– $\det u = 1$;
– l'automorphisme u n'est pas diagonalisable ;
– $\mathrm{Im}(u - \mathrm{Id}_E) \subset H$;
– l'automorphisme induit $\overline{u}\colon E/H \longrightarrow E/H$ est l'identité ;
– il existe un vecteur $a \in H \setminus \{0\}$ et une forme linéaire $f \in E^*$ tels que

$$\forall x \in E, \qquad u(x) = x + f(x)a\ ;$$

– dans une base convenable, la matrice de l'automorphisme u est

$$\begin{pmatrix} 1 & & & (0) \\ & \ddots & & \\ & & 1 & 1 \\ (0) & & & 1 \end{pmatrix}.$$

44. Définition. Un automorphisme $u \in \mathrm{GL}(E)$ vérifiant ces points est une *transvection d'hyperplan H et de droite* $\mathrm{Im}(u - \mathrm{Id}_E)$.
45. Lemme. Soient $u \in \mathrm{GL}(E) \setminus \{\mathrm{Id}_E\}$ un automorphisme et $D \subset E$ une droite. Alors les points suivants sont équivalents :
– l'automorphisme u est une transvection de droite D ;
– $u|_D = \mathrm{Id}_D$ et l'automorphisme induit $\overline{u}\colon E/D \longrightarrow E/D$ est l'identité.
46. Théorème. Le groupe $\mathrm{SL}(E)$ est engendré par les transvections.
47. Corollaire. Le groupe $\mathrm{GL}(E)$ est engendré par les transvections et dilatations.

3.2. Les groupes d'isométries

48. Cadre. On suppose que le corps k est celui des réels et que l'espace E est euclidien de dimension $n \geqslant 1$.
49. Définition. Dans un espace vectoriel ou affine euclidien, une *réflexion* est une symétrie orthogonale par rapport à un hyperplan.
50. Lemme. Soit $F \subseteq E$ un sous-espace vectoriel stable par une isométrie $f \in \mathrm{O}(E)$. Alors son orthogonal $F^\perp$ est également stable par l'isométrie u.
51. Théorème. Tout isométrie du groupe $\mathrm{O}(E)$ se décompose en un produit de p réflexions avec $p \leqslant n$.
52. Corollaire. Soit $\mathscr{E}$ un espace affine euclidien de dimension n. Alors toute isométrie de $\mathscr{E}$ se décompose en un produit de p réflexions avec $p \leqslant n + 1$.
53. Exemple. Le groupe des isométries positive du cube est engendré par les retournements d'axe $[MN]$ comme indiqué par une figure (mais lol je pe pa fer de figur).

[1] Michèle Audin. *Géométrie*. EDP Sciences, 2006.
[2] Josette Calais. *Éléments de théorie des groupes*. 3e édition. Presses Universitaires de France, 1998.
[3] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.
[4] Felix Ulmer. *Théorie des groupes*. 2e édition. Ellipses, 2021.