Cadre : G est un groupe.

I Génération d'un groupe

1) Sous-groupe engendré

Définition 1. Soit X une partie de G. L'intersection des sous-groupes de G qui contiennent X est un sous-groupe de G, qu'on appelle sous-groupe engendré par X et qu'on note $\langle X \rangle$. Si $G = \langle X \rangle$, alors on dit que X est une partie génératrice de G.

Exemple 2. *(i)* $\forall\, a \in G,\ \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$

(ii) Si a et b commutent dans G, $\langle a, b \rangle = \{a^m b^n \mid m, n \in \mathbb{Z}\}$. On peut généraliser pour tout nombre fini d'élément.

Définition 3. (i) G est monogène s'il est engendré par un élément.

(ii) G est cyclique s'il est monogène et fini.

(iii) G est de type fini s'il est engendré par une partie finie.

Exemple 4. $(n\mathbb{Z}, +)$ *est monogène car engendré par n.*

Définition 5. On appelle groupe dérivé de G le sous-groupe de G engendré par ses commutateurs.

Remarque 6. *Si G est abélien, son groupe dérivé est trivial.*

2) Ordre d'un élément

Définition 7. Un élément a de G est dit d'ordre $p \in \mathbb{N}^\star$ si $\langle a \rangle$ est fini de cardinal p. On a alors $\langle a \rangle = \{e, a, a^2, \ldots, a^{p-1}\}$. Si cet ensemble n'est pas fini, a est dit d'ordre infini.

Exemple 8. *(i) e est d'ordre 1 dans G.*

(ii) 1 est d'ordre infini dans $\mathbb{Z}$.

(iii) Dans $\mathfrak{S}_n$, un cycle de longueur ℓ est d'ordre ℓ.

Théorème 9. *Si G est fini d'ordre n, l'ordre de tout élément divise n.*

Proposition 10. *Soit $a \in G$ d'ordre p. Alors $a^q = e \Leftrightarrow p \mid q$.*

Proposition 11. *Soit G d'ordre fini. Soient $g, h \in G$ qui commutent d'ordre p et q.*

(i) gh est d'ordre fini qui divise $\mathrm{ppcm}(p, q)$.

(ii) Si $\langle g \rangle \cap \langle h \rangle = \{e\}$, alors gh est d'ordre $\mathrm{ppcm}(p, q)$.

(iii) Si p et q sont premiers entre eux, alors gh est d'ordre pq.

Théorème 12. *Soit G un groupe abélien fini. Il existe un élément d'ordre le* ppcm *de tous ses éléments. Cet entier est l'exposant de G.*

II Cas des groupes abéliens

1) Groupes cycliques

Exemple 13. *Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ et le groupe des racines n-ièmes de l'unité sont cycliques d'ordre n.*

Théorème 14. *Un groupe cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Proposition 15. *Soit $G = \langle a \rangle$ cyclique à n éléments. Alors $G = \langle g \rangle$ si, et seulement si, k et n sont premiers entre eux.*

Corollaire 16. *Un groupe cyclique d'ordre n possède $\varphi(n)$ générateurs.*

Corollaire 17. *Un groupe de cardinal premier est cyclique et tout élément non trivial est générateur.*

Théorème 18. *Soit $G = \langle a \rangle$ cyclique à n éléments.*

(i) Les sous-groupes de G sont cycliques d'ordre divisant n.

(ii) Soit d un diviseur de n. Il existe un unique sous-groupe de G d'ordre d qui est $\left\langle a^{\frac{n}{d}} \right\rangle$. Ces générateurs sont les éléments d'ordre d.

Application 19. *Soit $n \in \mathbb{N}^\star$, alors $n = \sum_{d \mid n} \varphi(d)$.*

Application 20. *Soit $\mathbb{K}$ un corps. Tout sous-groupe du groupe multiplicatif est cyclique.*

2) Groupes abéliens finis

Théorème 21. *Soit G un groupe abélien fini, alors :*

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z} \quad \text{où} \quad \forall\, i \in [\![1, n-1]\!],\ d_i \mid d_{i+1}$$

De plus, les d_i sont uniques. Ce sont les facteurs invariants.

Corollaire 22. *Si $d \mid |G|$, G admet un sous-groupe cyclique d'ordre d.*

III Groupe symétrique

1) Générateurs

Proposition 23. *Toute permutation se décompose en produit de cycles à supports disjoints. Cette décomposition est unique à l'ordre près.*

Exemple 24. $\left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9&10\\3&10&2&4&7&9&8&5&6&1\end{smallmatrix}\right) = (1\ 3\ 2\ 10)(4)(5\ 7\ 8)(6\ 9)$

Proposition 25. *Toute permutation de $\mathfrak{S}_n$ se décompose en produit de (au plus $n-1$) transpositions.*

Exemple 26. $\left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9&10\\3&10&2&4&7&9&8&5&6&1\end{smallmatrix}\right) = (1\ 10)(1\ 2)(1\ 3)(5\ 8)(5\ 7)(6\ 9)$

Corollaire 27. *La signature d'une permutation est déterminée par la parité du nombre de transpositions la composant.*

Proposition 28. *Les familles suivantes engendrent $\mathfrak{S}_n$:*

(i) $\{(1\ i)\,|\,1 < i \leqslant n\}$

(ii) $\{(i\ i+1)\,|\,1 \leqslant i < n\}$

(iii) $\{(1\ 2), (1\ 2\ \ldots\ n)\}$

Remarque 29. *Quel que soit n, deux éléments suffisent à engendrer $\mathfrak{S}_n$.*

2) Groupe alterné

Proposition 30. *$\mathfrak{A}_n \trianglelefteq \mathfrak{S}_n$. De plus, $\mathfrak{S}_n/\mathfrak{A}_n \cong \{\pm 1\}$.*

Lemme 31. *$\mathfrak{A}_n$ est $n-2$ fois transitif sur $[\![1,n]\!]$: si on a $a_1,\ldots,a_{n-2} \in [\![1,n]\!]$ distincts et $b_1,\ldots,b_{n-2} \in [\![1,n]\!]$ distincts, il existe $\sigma \in \mathfrak{A}_n$ tel que $\sigma(a_i) = b_i$ pour tout $i \in [\![1,n-2]\!]$.*

Proposition 32. *Les cycles d'ordre 3 sont conjugués dans $\mathfrak{A}_n$ pour $n \geqslant 5$.*

Proposition 33. *$\mathfrak{A}_n$ est engendré par les 3-cycles de $\mathfrak{S}_n$.*

Théorème 34. *$\mathfrak{A}_n$ est simple pour $n \geqslant 5$.*

Corollaire 35. *Pour $n \geqslant 5$, le groupe dérivé de $\mathfrak{A}_n$ est $\mathfrak{A}_n$.*

Corollaire 36. *Pour $n \geqslant 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\mathfrak{S}_n$, $\mathfrak{A}_n$ et $\{Id\}$.*

IV Applications en algèbre linéaire

On considère E un $\mathbb{K}$-espace vectoriel de dimension finie n.

1) Groupe linéaire

Proposition 37. *Soient $H = \mathrm{Ker}(f)$ un hyperplan de E et $u \in GL(E)$ tel que $u \neq Id_E$ et $u|_H = Id_H$. On note $D = \mathrm{Im}(u - Id_E)$. Les assertions suivantes sont équivalentes.*

(i) $\det(u) = 1$

(ii) *u n'est pas diagonalisable.*

(iii) $D \subset H$

(iv) *$\overline{u} : E/H \to E/H$ définie par $\overline{u}(\overline{x}) = \overline{u(x)}$ est l'identité.*

(v) *Il existe $a \in H \setminus \{0\}$ tel que $u = Id_E + fa$.*

(vi) *La matrice de u dans une certaine base est $T_{i,j}(\lambda)$.*

u est alors une transvection d'hyperplan H de droite D.

Corollaire 38. *Soit $u \in GL(E)$ tel que $u \neq Id_E$. Les assertions suivantes sont équivalentes :*

(i) *u est une transvection de droite D.*

(ii) *$\overline{u} : E/D \to E/D$ définie par $\overline{u}(\overline{x}) = \overline{u(x)}$ est l'identité et $u|_D = Id_D$.*

Proposition 39. *Soient H un hyperplan de E et $u \in GL(E)$ tel que $u|_H = Id_H$. Les assertions suivantes sont équivalentes.*

(i) $\det(u) = \lambda \neq 1$

(ii) *λ est valeur propre de u et u est diagonalisable.*

(iii) $D = \mathrm{Im}(u - Id_E) \not\subset H$

(iv) *La matrice de u dans une certaine base est $D_i(\lambda)$.*

u est alors une dilatation d'hyperplan H de droite D et de rapport λ.

Lemme 40. *On suppose E de dimension $n \geqslant 2$. Soient $x, y \in E \setminus \{0\}$. Il existe une transvection u ou un produit de deux transvections uv, tel que $u(x) = y$ ou $uv(x) = y$.*

Théorème 41. *Les transvections engendrent $SL(E)$.*

Théorème 42. *Les transvections et les dilatations engendrent $GL(E)$.*

2) Groupe orthogonal

Définition 43. Soit F un sous-espace vectoriel de E. Pour tout $x \in E$, il existe une unique décomposition $x = x_1 + x_2$ avec $x_1 \in F$ et $x_2 \in F^\perp$. On appelle symétrie orthogonale par rapport à F l'application :

$$s : \left| \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & x_1 - x_2 \end{array} \right.$$

Définition 44. Une réflexion est une symétrie orthogonale par rapport à un hyperplan. Un retournement est une symétrie par rapport à un hyperplan de dimension $n-2$.

Théorème 45. *Tout élément de $O(E)$ s'écrit comme produit de r réflexions, où $r = \mathrm{rg}(u - Id_E)$.*

Corollaire 46. *Si $n \geqslant 3$, $SO(E)$ est engendré par les retournements.*

Théorème 47. *Soit $M \in O_n(\mathbb{R})$, alors M est semblable à :*

$$\begin{pmatrix} I_r & & & & 0 \\ & -I_m & & & \\ & & R_{\theta_1} & & \\ & & & \ddots & \\ 0 & & & & R_{\theta_s} \end{pmatrix} \quad \text{avec} \quad \left\{ \begin{array}{l} \theta_i \in]0; 2\pi[\setminus \{\pi\} \\ R_{\theta_i} = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix} \end{array} \right.$$

Application 48. *$SO_n(\mathbb{R})$ est connexe par arcs.*

Développements

— Simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$ (33,34) [Per96]
— Générateurs de $GL(E)$ et de $SL(E)$ (39,40,41) [Per96]

Références

[Per96] Daniel Perrin. *Cours d'Algèbre.* Ellipses, 1996
[Gou94] Xavier Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e edition, 1994
[Rom20] Jean-Étienne Rombaldi. *Algèbre et Géométrie.* DeBoeck, 2020