

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

I - Généralités

Soit G un groupe.

1. Définitions

Lemme 1. Une intersection (quelconque) de sous-groupes de G est un sous-groupe de G .

[ROM21]
p. 10

Définition 2. Soit $X \subseteq G$. On appelle **sous-groupe engendré** par X , le plus petit sous-groupe (pour l'inclusion) de G contenant X . C'est l'intersection des sous-groupes de G contenant X . On le note $\langle X \rangle$ ou $\langle x_1, \dots, x_n \rangle$ si $X = \{x_1, \dots, x_n\}$.

Proposition 3. Soit $X \subseteq G$. On pose $X^{-1} = \{x^{-1} \mid x \in X\}$. Alors,

$$\langle X \rangle = \{x_1 \dots x_n \mid (x_1 \dots x_n) \in X \cup X^{-1}, n \in \mathbb{N}^*\}$$

Définition 4. Une **partie génératrice** de G est un sous-ensemble $X \subseteq G$ tel que $G = \langle X \rangle$.

Exemple 5. Soit D_G l'ensemble des commutateurs de G (ie. éléments de la forme ghg^{-1} pour $g, h \in G$). On pose $D(G) = \langle D_G \rangle$: $D(G)$ est le groupe dérivé de G , c'est le plus grand sous-groupe tel que $G/D(G)$ est abélien.

2. Groupes monogènes

Définition 6. On dit que G est **monogène** s'il existe $g \in G$ tel que $G = \langle g \rangle$, et on dit que G est cyclique s'il est monogène et fini.

Exemple 7. (i) \mathbb{Z} est monogène, l'ensemble de ses générateurs est $\mathbb{Z}^\times = \{\pm 1\}$.

(ii) $\mathbb{Z}/n\mathbb{Z}$, l'ensemble de ses générateurs est $(\mathbb{Z}/n\mathbb{Z})^\times = \{k \in \mathbb{Z}/n\mathbb{Z} \mid \text{pgcd}(k, n) = 1\}$.

Théorème 8. (i) Si G est monogène infini, alors $G \cong \mathbb{Z}$.

(ii) Si G est cyclique d'ordre n , alors $G \cong \mathbb{Z}/n\mathbb{Z}$.

Corollaire 9. Si $G = \langle g \rangle$ est cyclique d'ordre n , alors l'ensemble de ses générateurs est $\{g^k \mid \text{pgcd}(k, n) = 1\}$.

Définition 10. L'ordre d'un élément $g \in G$ est le cardinal de l'ensemble $\langle g \rangle$.

p. 6

Remarque 11. $g \in G$ est d'ordre n si et seulement si $g^n = e_G$ et $g^k \neq e_G$ pour tout $k \in \llbracket 1, n-1 \rrbracket$.

Proposition 12. Un groupe de cardinal premier est cyclique.

p. 14

Théorème 13. On suppose $G = \langle g \rangle$ cyclique d'ordre n .

- (i) Les sous-groupes de G sont cycliques d'ordre divisant n .
- (ii) Pour tout diviseur d de n , il existe un unique sous-groupe d'ordre d : $\langle g^{\frac{n}{d}} \rangle$.

Remarque 14. Le résultat précédent est en fait caractéristique des groupes cycliques.

3. Structure des groupes abéliens de type fini

On suppose dans cette sous-section que G est abélien.

[ULM21]

Définition 15. G est dit de **type fini** s'il existe une partie génératrice finie de G .

p. 105

Théorème 16 (Kronecker). Soit G un groupe abélien d'ordre $n \geq 2$. Il existe $r \in \mathbb{N}$ et une suite d'entiers $n_1 \geq 2$, n_2 multiple de n_1 , ..., n_k multiple de n_{k-1} telle que G est isomorphe au groupe produit

p. 112

$$\prod_{i=1}^k \mathbb{Z}/n_i\mathbb{Z} \times \mathbb{Z}^r$$

Exemple 17. Si $G = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$. Alors,

$$\begin{aligned} G &\cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \\ &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \end{aligned}$$

II - Exemples de parties génératrices

1. Groupe symétrique

Définition 18. Soit E un ensemble. On appelle **groupe des permutations** de E le groupe des bijections de E dans lui-même. On le note $S(E)$.

[ROM21]

p. 37

Notation 19. Si $E = \llbracket 1, n \rrbracket$, on note $S(E) = S_n$, le groupe symétrique à n éléments.

Notation 20. Soit $\sigma \in S_n$. On note :

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

pour signifier que σ est la bijection $\sigma : k \mapsto \sigma(k)$.

Définition 21. Soient $l \leq n$ et $i_1, \dots, i_l \in \llbracket 1, n \rrbracket$ des éléments distincts. La permutation $\gamma \in S_n$ définie par

$$\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1, \dots, i_l\} \\ i_{k+1} & \text{si } j = i_k \text{ avec } k < l \\ i_1 & \text{si } j = i_l \end{cases}$$

et notée $(i_1 \dots i_l)$ est appelée **cycle** de longueur l et de **support** $\{i_1, \dots, i_l\}$. Un cycle de longueur 2 est une **transposition**.

Proposition 22. (i) S_n est engendré par les transpositions. On peut même se limiter aux transpositions de la forme $(1 \ k)$ ou encore $(k \ k+1)$ (pour $k \leq n$).

p. 44

(ii) S_n est engendré par $(1 \ 2)$ et $(1 \dots n)$.

Définition 23. — Soit $\sigma \in S_n$. On appelle **signature** de σ , notée $\epsilon(\sigma)$ l'entier $\epsilon(\sigma) =$

$$\prod_{i \neq j} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

— $\sigma \mapsto \epsilon(\sigma)$ est un morphisme de S_n dans $\{\pm 1\}$, on note A_n son noyau.

p. 48

Lemme 24. Les 3-cycles sont conjugués dans A_n pour $n \geq 5$.

[PER]

p. 15

Lemme 25. Le produit de deux transpositions est un produit de 3-cycles.

[ROM21]

p. 49

Proposition 26. A_n est engendré par les 3-cycles pour $n \geq 3$.

[DEV]

Théorème 27. A_n est simple pour $n \geq 5$.

[PER]
p. 28

Corollaire 28. Le groupe dérivé de A_n est A_n pour $n \geq 5$, et le groupe dérivé de S_n est A_n pour $n \geq 2$.

2. Groupe diédral

Définition 29. Pour un entier $n \geq 1$, le **groupe diédral** D_n est le sous-groupe, de $GL_2(\mathbb{R})$ engendré par la symétrie axiale s et la rotation d'angle $\theta = \frac{2\pi}{n}$ définies respectivement par les matrices

[ULM21]
p. 8

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ et } R = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

Exemple 30. $D_1 = \{\text{id}, s\}$.

Proposition 31. (i) D_n est un groupe d'ordre $2n$.

(ii) $r^n = s^2 = \text{id}$ et $sr = r^{-1}s$.

Proposition 32. Un groupe non cyclique d'ordre 4 est isomorphe à D_2 .

p. 28

Exemple 33. S_2 est isomorphe à D_2 .

p. 65

Proposition 34. Un groupe fini d'ordre $2p$ avec p premier est soit cyclique, soit isomorphe à D_p .

p. 28

Exemple 35. S_3 est isomorphe à D_3 .

Proposition 36. Les sous-groupes de D_n sont soit cyclique, soit isomorphes à un D_m où $m \mid n$.

p. 47

III - Applications en algèbre linéaire

1. Groupe linéaire

[PER]
p. 97

Proposition 37. Soit $u \in GL(E) \setminus \{\text{id}_E\}$. Soit H un hyperplan de E tel que $u|_H = \text{id}_H$. Les assertions suivantes sont équivalentes :

- (i) $\det(u) = 1$.
- (ii) u n'est pas diagonalisable.
- (iii) $\text{Im}(u - \text{id}_E) \subseteq H$.
- (iv) Le morphisme induit $\bar{u} : E/H \rightarrow E/H$ est l'identité de E/H .
- (v) En notant $H = \text{Ker}(f)$ (où f désigne une forme linéaire sur E), il existe $a \in H \setminus \{0\}$ tel que

$$u = \text{id}_E + f \cdot a$$

- (vi) Dans une base adaptée, la matrice de u s'écrit

$$\begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Définition 38. En reprenant les notations précédentes, on dit que u est une **transvection** d'hyperplan H et de droite $\text{Vect}(a)$.

Proposition 39. Soient $u \in GL(E)$ et τ une transvection d'hyperplan H et de droite D . Alors, $u\tau u^{-1}$ est une transvection d'hyperplan $u(H)$ et de droite $u(D)$.

Théorème 40. Si $n \geq 2$, les transvections engendrent $SL(E)$.

Proposition 41. Soit $u \in GL(E)$. Soit H un hyperplan de E tel que $u|_H = \text{id}_H$. Les assertions suivantes sont équivalentes :

- (i) $\det(u) = \lambda \neq 1$.
- (ii) u admet une valeur propre $\lambda \neq 1$.
- (iii) $\text{Im}(u - \text{id}_E) \not\subseteq H$.
- (iv) Dans une base adaptée, la matrice de u s'écrit

$$\begin{pmatrix} I_{n-1} & 0 \\ 0 & \lambda \end{pmatrix}$$

avec $\lambda \neq 1$.

Théorème 42. Si $n \geq 2$, les transvections et les dilatations engendrent $GL(E)$.

Notation 43. Soit $a \in \mathbb{F}_p$. On note $\left(\frac{a}{p}\right)$ le symbole de Legendre de a modulo p .

Lemme 44. Soient $p \geq 3$ un nombre premier et V un espace vectoriel sur \mathbb{F}_p de dimension finie. Les dilatations engendrent $GL(V)$.

Application 45 (Théorème de Frobenius-Zolotarev). Soient $p \geq 3$ un nombre premier et V un espace vectoriel sur \mathbb{F}_p de dimension finie.

$$\forall u \in GL(V), \epsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où u est vu comme une permutation des éléments de V .

2. Groupe orthogonal

Soit E un espace vectoriel réel de dimension n . Soit φ une forme bilinéaire, symétrique, non dégénérée sur E . On note q la forme quadratique associée.

[PER]
p. 123

Définition 46. — On appelle **isométries** de E (relativement à q), les endomorphismes $u \in GL(E)$ qui vérifient :

$$\forall x, y \in E, q(x, y) = q(u(x), u(y))$$

- L'ensemble des isométries de E forme un groupe, appelé **groupe orthogonal** de E , et noté $\mathcal{O}_q(E)$.
- Le sous-groupe des isométries de E de déterminant 1 est appelé **groupe spécial orthogonal** de E , et est noté $SO_q(E)$.

Définition 47. Soit $u \in SO_q(E)$ tel que $u^2 = \text{id}_E$.

- On dit que u est une **réflexion** si $\dim(\text{Ker}(u + \text{id}_E)) = 1$ (ie. u est une symétrie par rapport à un hyperplan).
- On dit que u est un **retournement** si $\dim(\text{Ker}(u + \text{id}_E)) = 2$ (ie. u est une symétrie par rapport à un plan).

On suppose désormais de plus que φ est définie positive (ie. φ est un produit scalaire).

Théorème 48. On suppose $n \geq 3$. Alors :

- (i) $\mathcal{O}_q(E)$ est engendré par les réflexions.
- (ii) $SO_q(E)$ est engendré par les retournements.

Application 49. On suppose $n \geq 3$. Alors :

(i) $D(\mathcal{O}_q(E)) = \text{SO}_q(E)$.

(ii) $D(\text{SO}_q(E)) = \text{SO}_q(E)$.

Bibliographie

L'oral à l'agrégation de mathématiques

[I-P]

LUCAS ISENMANN et TIMOTHÉE PECATTE. *L'oral à l'agrégation de mathématiques. Une sélection de développements*. 2^e éd. Ellipses, 26 mars 2024.

<https://www.editions-ellipses.fr/accueil/15218-28346-loral-a-lagregation-de-mathematiques-une-selection-de-developpements-2e-edition-9782340086487.html>.

Cours d'algèbre

[PER]

DANIEL PERRIN. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.

<https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html>.

Mathématiques pour l'agrégation

[ROM21]

JEAN-ÉTIENNE ROMBALDI. *Mathématiques pour l'agrégation. Algèbre et géométrie*. 2^e éd. De Boeck Supérieur, 20 avr. 2021.

<https://www.deboecksuperieur.com/ouvrage/9782807332201-mathematiques-pour-l-agregation-algebre-et-geometrie>.

Théorie des groupes

[ULM21]

FELIX ULMER. *Théorie des groupes. Cours et exercices*. 2^e éd. Ellipses, 3 août 2021.

<https://www.editions-ellipses.fr/accueil/13760-25304-theorie-des-groupes-2e-edition-9782340057241.html>.