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

Pandou

18 mai 2022

1 Généralités

Définition 1. *Soit G un groupe et A une partie de G. Le plus petit sous-groupe de G contenant A est le sous-groupe engendré par A, noté $\langle A\rangle$. On dit que A engendre G si $\langle A\rangle = G$.*

Remarque 2 : On a $\langle A\rangle = \bigcap_{A\subset H} H$. Quand A est fini, on dit que G est de type fini.

Exemples 3 :
- Dans $\mathbb{Z}$, $\langle n\rangle = n\mathbb{Z}$.
- Soit G un groupe, son groupe dérivé est le groupe engendré par les commutateurs $[x,y] = xyx^{-1}y^{-1}$.

Théorème 4. *On a*

$$\langle A\rangle = \left\{a_1...a_n, n\in\mathbb{N}, a_i \in A\cup A^{-1}\right\}$$

Proposition 5. *Soit $\varphi : G \longrightarrow G'$ un morphisme de groupes et $A \subset G$, alors $\varphi(G) = \langle\varphi(A)\rangle$. En particulier, si φ est un isomorphisme, alors $\varphi(A)$ engendre G'.*

Remarque 6 : Pour connaître les morphismes de G dans G', il suffit de connaître l'image des générateurs de G dans G'.

2 Groupes finis et groupes de type fini

2.1 Groupes abéliens

Définition 7. *On dit que G est monogène s'il est engendré par un élément. S'il est fini, on dit qu'il y est cyclique.*

Proposition 8. *Un groupe est monogène est isomorphe à $\mathbb{Z}$ s'il est infini, et à $\mathbb{Z}/n\mathbb{Z}$ s'il est d'ordre $n\in\mathbb{N}$.*

Proposition 9. *Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $\mathbb{Z}/d\mathbb{Z}$ où d divise n.*

Proposition 10. *Soit $n\geqslant 2$ et $a\in\mathbb{N}$. Alors,*
1. *$a\wedge n = 1$.*
2. *$\overline{a}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$.*
3. *$\overline{a}$ est un inversible de $\mathbb{Z}/n\mathbb{Z}$.*

Exemple 11 : Si p est premier, alors $\mathbb{Z}/p\mathbb{Z}$ est engendré par tout élément non nul.

Définition 12. *On note $\varphi(n)$ le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$.*

Exemple 13 : Si p est premier, $\varphi(p) = p-1$. Plus généralement, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Théorème 14 (Reste chinois)**.** *Si n et m sont premiers entre eux, alors*

$$\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$$

En particulier, $\varphi(nm) = \varphi(n)\varphi(m)$.

Corollaire 15. *Soit G et H deux groupes cycliques d'ordres m et n. Alors, $G\times H$ est cyclique si, et seulement si, m et n sont premiers entre eux.*

Corollaire 16. *Si $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, on a*

$$\varphi(n) = \prod_{i=1}^{k}(p_i-1)p_i^{\alpha_i-1} = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

Proposition 17. *Pour d divisant n, $\mathbb{Z}/n\mathbb{Z}$ admet $\varphi(d)$ éléments d'ordre d. En particulier, on a*

$$n = \sum_{d|n} \varphi(d)$$

Application 18 : Soit K un corps commutatif. Tout sous-groupe fini de K^* est cyclique.

Théorème 19 (Structure des groupes abéliens finis)**.** *Soit G un groupe abélien fini, alors il existe un unique $d_1, ..., d_r$ tel que $d_1|...|d_r$ et*

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_r\mathbb{Z}$$

Exemple 19 : Il y a 3 groupes abéliens d'ordre 8.

Proposition 20. *Un sous-groupe d'un groupe abélien de type fini est de type fini.*

Théorème 21 (Structure des groupes abéliens de type fini)**.** *Soit G un groupe abélien de type fini, il existe $m, d_1, ..., d_r$ tel que $d_1|...|d_r$ et*

$$G \simeq \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_r\mathbb{Z}$$

2.2 Groupe symétrique

Proposition 22. *$\mathfrak{S}_n$ est engendré par les transpositions.*

Application 23 : Il existe un unique morphisme non trivial $\mathfrak{S}_n \longrightarrow \mathbb{C}^*$.

Proposition 24. *$\mathfrak{S}_n$ est engendré par les familles suivantes :*
- *$(i, i+1)$ pour $0 \leqslant i \leqslant n-1$.*
- *$(1, 2)$ et $(1, ..., n)$.*

Remarque 25 : Si $n \geqslant 3$, $\mathfrak{S}_n$ n'est pas monogène car n'est pas abélien. Donc, le nombre minimum de permutations pour engendrer $\mathfrak{S}_n$ est 2.

Proposition 26. *Toute permutation est produit d'au plus n transpositions.*

Théorème 27. *Tout permutation $\sigma \in \mathfrak{S}_n$ se décompose en un produit unique (à l'ordre près) de cycles à support disjoint.*

Application 28 : Deux permutations sont conjuguées si, et seulement si, ils ont même nombre de cycles de même longueur.

DEVELOPPEMENT 1

Théorème 29. *Si $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont tous intérieurs.*

Remarque 30 : Si $n = 6$, $\mathrm{Int}(\mathfrak{S}_6)$ est un sous-groupe d'indice 2 de $\mathrm{Aut}(\mathfrak{S}_6)$.

Proposition 30. *$\mathfrak{A}_n$ est engendré par les 3-cycles. Si $n \geqslant 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.*

Théorème 31 (Simplicité de $\mathfrak{A}_n$)**.** *Soit $n \geqslant 3$, $\mathfrak{A}_n$ est simple si, et seulement si, $n \neq 4$.*

2.3 Groupe diédral

Définition 32. *On note D_{2n} le groupe des isométries préservant un n-gone régulier.*

Proposition 33. *D_{2n} est d'ordre $2n$ est engendré par une symétrie axiale s et par une rotation r d'angle $\frac{2\pi}{n}$.*

Remarque 35 : $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

3 Groupes matriciels

3.1 Groupe (spécial) linéaire

Définition 36. *On définit :*
1. *les matrices de transvection : $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$ pour $i \neq j$ et $\lambda \in K^*$.*
2. *les matrices de dilatation : $D_i(\alpha) = \mathrm{diag}(1, ..., \alpha, ..., 1)$ où α est en position i et $\alpha \in K \setminus \{0, 1\}$.*

Remarque 37 : Soit $A \in M_n(K)$, on note $L_1, ..., L_n$ les lignes de A et $C_1, ..., C_n$ les colonnes de A. Alors,
1. $T_{i,j}(\lambda)A$ revient à l'opération élémentaire $L_i \leftarrow L_i + \lambda L_j$.
2. $AT_{i,j}(\lambda)$ revient à l'opération élémentaire $C_j \leftarrow C_j + \lambda C_i$.

Proposition 38.
- *$\lambda \mapsto T_{i,j}(\lambda)$ est un morphisme de groupes de $\mathbb{R}$ vers $SL_n(\mathbb{R})$.*

- $\alpha \mapsto D_i(\alpha)$ *est un morphisme de groupes de* $\mathbb{R}^*$ *vers* $GL_n(\mathbb{R})$.

Théorème 39. *$SL_n(K)$ est engendré par les transvections.*

Corollaire 40. *$GL_n(K)$ est engendré par les transvections et les dilatations.*

Application 41 : $GL_n(\mathbb{R})$ a deux composantes connexes homéomorphes : $GL_n^+(\mathbb{R})$ et $GL_n^-(\mathbb{R})$ et $SL_n(\mathbb{R})$ est connexe.

Proposition 42 (Conjugaison dans $SL_n(K)$)**.** *Soit $n \in \mathbb{N}$.*

1. *Les transvections sont toujours conjuguées dans $GL_n(K)$.*
2. *Si $n \geqslant 3$, les transvections sont conjuguées dans $SL_n(K)$.*
3. *Dans $SL_2(K)$, toute transvection est conjugué à $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$.*
4. *Dans $SL_2(K)$, $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ sont conjugués dans $SL_2(K)$ si, et seulement si, $\dfrac{\lambda}{\mu}$ est un carré dans K.*

DEVELOPPEMENT 2

Lemme 43. *Si $n \geqslant 3$, le groupe dérivé de $SL_n(\mathbb{Z}/2\mathbb{Z})$ est lui-même.*

Théorème 44. *Soit G un groupe abélien fini d'ordre p. On s'intéresse aux morphismes de $GL_n(K) \longrightarrow G$.*

- *Si $K = \mathbb{C}$, le seul morphisme de $GL_n(\mathbb{C})$ dans G est trivial.*
- *Si $K = \mathbb{R}$ et G est d'ordre impair, le seul morphisme de $GL_n(\mathbb{R})$ dans G est trivial.*
- *Si $K = \mathbb{R}$ et G est d'ordre pair, alors Il existe des morphismes non triviaux de $GL_n(\mathbb{R})$ dans G. Ils sont définis par $f_a : M \longmapsto \begin{cases} 1 & si\ \det(M) > 0 \\ a & si\ \det(M) < 0 \end{cases}$ où a est un élément d'ordre 2 de G.*
- *Si $K = \mathbb{Z}/q\mathbb{Z}$, avec q premier impair, alors il existe des morphismes non triviaux si, et seulement si, $q-1$ et p ne sont pas premiers entre eux.*
- *Si $K = \mathbb{Z}/2\mathbb{Z}$, il existe des morphismes non triviaux si, et seulement si, p est pair et $n = 2$.*

Théorème 45 (Simplicité de PSL_n)**.** *$PSL_n(K)$ est simple, sauf $PSL_2(\mathbb{F}_2)$ et $PSL_2(\mathbb{F}_3)$.*

Remarque 46 : $PSL_2(\mathbb{F}_2)$ et $PSL_2(\mathbb{F}_3)$ ne sont effectivement pas simples.

3.2 Groupe (spécial) orthogonal

Définition 47. *Une symétrie orthogonale par rapport à un hyperplan est appelée une réflexion orthogonale.*
Une symétrie orthogonale par rapport à un sous-espace de codimension 2 est appelée un renversement.

Théorème 48. *Les réflexions engendrent $O_n(\mathbb{R})$.*

Corollaire 49. *Les renversements engendrent $SO_n(\mathbb{R})$ et, si $n \geqslant 3$, ils sont conjugués dans $SO(n)$.*

DEVELOPPEMENT 3

Théorème 50. *$SO(3)$ est simple.*

Remarque 51 : Plus généralement, $SO(2n+1)$ est simple et $PSO(2n)$ est simple sauf $PSO(4)$.

Théorème 52 (Isomorphismes exceptionnels)**.** *On a les isomorphismes exceptionnels suivants :*

$$PSU(2) \simeq SO(3) \qquad et \qquad PSO(4) \simeq SO(3) \times SO(3)$$

Références :

- Arnaudiès, Fraysse, Cours de mathématiques Tome 1, Algèbre.
- Calais, Éléments de théorie des groupes.
- Perrin, Cours d'algèbre.