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

I Cas des groupes abéliens

A Les groupes monogènes et cycliques Rom 1.4 1.5

On considère G un groupe.

Définition 1 : On dit que G est monogène s'il existe $g \in G$ tel que $G = \langle g \rangle$. Si de plus G est fini, on dit qu'il est cyclique.

Exemple 2 : Le groupe $(\mathbb{Z}, +)$ est monogène engendré par 1.
Le groupe μ_n des racines n-ièmes de l'unité est cyclique.

Proposition 3 : Soit G un groupe monogène. S'il est infini, il est isomorphe à $(\mathbb{Z}, +)$. S'il est cyclique d'ordre n, il est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Théorème 4 : Si $G = \langle g \rangle$ est un groupe cyclique d'ordre n, ses générateurs sont alors les g^k, où $k \in [\![1, n-1]\!]$ et $n \wedge k = 1$.

Corollaire 5 : Le nombre de générateurs de G est égal à $\varphi(n)$.

Exemple 6 : pour $p \in \mathcal{P}$, $\mathbb{Z}/p\mathbb{Z}$ admet $p-1$ générateurs.

Théorème 7 : Un groupe de cardinal premier est cyclique.

Théorème 8 : Un groupe commutatif d'ordre pq où p et q sont deux nombres premiers distincts est cyclique.

Remarque 9 : C'est faux si $p = q$, par exemple $(\mathbb{Z}_p)^2$ qui est d'ordre p^2 est non cyclique puisque tous ses éléments distincts de neutre sont d'ordre p.
$|S_3| = 2 \times 3 = 6$ n'est pas cyclique (car pas commutatif).

Théorème 10 : Si $G = \langle g \rangle$ cyclique alors les sous-groupes de G sont tous cycliques d'ordre diviseur l'ordre de $G = n$. De plus pour tout diviseur positif d de n il existe un unique sous-groupe d'ordre d de G, c'est le groupe cyclique $H = \langle g^{\frac{n}{d}} \rangle$.

Exemple 11 : Les sous-groupes de $\mathbb{Z}_p$, $p \in \mathcal{P}$ sont $\{e\}$ et lui même.

B Structure des groupes abéliens finis. Rom 1.5 1.9 Ulm 12.2

Théorème 12 (Cauchy) : Soit G un groupe commutatif d'ordre $n \geq 2$. Pour tout diviseur premier p de n il existe dans G un élément d'ordre p.

Remarque 13 : Pour G commutatif non cyclique et d diviseur quelconque de n, il n'existe pas nécessairement d'élément d'ordre d dans G. Par exemple pour G non cyclique et $d = n$ il n'existe pas d'élément d'ordre n.

Définition 14 : G est dit de type fini s'il existe une partie finie de G qui engendre G.

Exemple 15 : $\mathbb{Z}$ est de type fini car $\mathbb{Z} = \langle 1 \rangle$.

Théorème 16 : Tout groupe abélien G de type fini est isomorphe à un produit direct de groupes cycliques de la forme :
$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k} \times \mathbb{Z}^n \qquad (n, k) \in \mathbb{N}$$
et pour tout $i \in [\![1, k-1]\!]$, m_i divise m_{i+1}.

Exemple 16 bis : Les groupes abéliens d'ordre 8 sont $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

II Groupe symétrique

A Générateurs Rom 2.1 2.3 2.4 2.5

Définition 17 : Un k-cycle est une permutation circulaire ie de la forme $\sigma = (i_1 \cdots i_k)$, si $k = 2$ on parle de transposition.

Proposition 18 : Les transpositions engendrent les k-cycles.

Théorème 19 : Toute permutation peut s'écrire comme produit de cycles deux à deux disjoints, de plus cette décomposition est unique à l'ordre près.

Remarque 20 : Si $\sigma = \gamma_1 \cdots \gamma_p$ est une telle décomposition on a alors la partition
$\mathrm{Supp}\,\sigma = \bigsqcup_{k=1}^{p} \mathrm{Supp}(\gamma_k)$ et $\mathrm{ord}(\sigma) = \mathrm{ppcm}(\mathrm{ord}(\gamma_k))$.

Corollaire 21 : Le groupe $S(E)$ est engendré par les transpositions.

Exemple 22 : Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 7 & 4 & 6 \end{pmatrix} = (1\,2\,3\,4\,5)(6\,7) = (1\,2)(1\,3)(3\,4)(4\,5)(6\,7)$

Lemme 23 : S_m est engendré par les $m-1$ transpositions $(1,k)$ où $2 \leq k \leq m$.

Exemple 24 : $(i\,j) = (1\,i)(1\,j)(1\,i)$

Proposition 25 : S_m est engendré par les $m-1$ transpositions $(k, k+1)$ où $k \in [\![1, m-1]\!]$.

Exemple 26 : $(1,k) = (k-1,k)(1,k-1)(k-1,k) = (k-2,k-1)(1,k-2)(k-2,k-1)$

Proposition 27 : S_m est engendré par $(1\,2)$ et $(1\,2 \cdots m)$

Exemple 28 : $(k, k+1) = (1\,2 \cdots m)^{k-1}(1\,2)\left((1\,2 \cdots m)^{k-1}\right)^{-1}$

B Sous groupe alterné X.G 1.2 Rom 2.7

Définition 29 : Soit $\sigma \in S_m$. On appelle signature de σ le produit
$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq m} \frac{\sigma(j) - \sigma(i)}{j - i}$$

On a $\varepsilon(\sigma) \in \{-1, 1\}$. Si $\varepsilon(\sigma) = 1$ (resp $\varepsilon(\sigma) = -1$), σ est dite paire (resp impaire).

Proposition 30 : Soient $\sigma, \tau \in S_m$ alors $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\,\varepsilon(\tau)$.

Exemple 31 : Une transposition est de signature -1.
La signature d'un cycle de longueur p est $(-1)^{p-1}$.

Remarque 32 : La proposition précédente exprime le fait que $\varepsilon : S_m \to \{-1,1\}$ est un morphisme de groupe.

Définition 33 : On définit $A(E) = \{\sigma \in S(E),\ \varepsilon(\sigma) = 1\} = \ker \varepsilon$ le sous groupe alterné.

Proposition 34 : $A(E)$ est distingué dans $S(E)$ et $[S(E) : A(E)] = 2$

Proposition 35 : Pour $m \geq 3$, $A(E)$ est engendré par les 3 cycles.

Développement Pour tout $m \geq 5$, A_m est simple.

Application 36 : A_5 est l'unique groupe simple d'ordre 60 (à isomorphisme près).

III Groupe linéaire

A Générateurs de $GL(E)$ et de $SL(E)$ Per 4.2 4.3

Soit E un $\mathbb{K}$ espace vectoriel de dimension n.

Lemme 37 : Soient $x, y \in E \setminus \{0\}$. Il existe une transvection u ou un produit de deux transvections $u\sigma$, tel que $u(x) = y$ ou $u\sigma(x) = y$.

Théorème 38 : Les transvections engendrent $SL(E)$ Per 4.2 4.3

Corollaire 39 : Les transvections et les dilatations engendrent $GL(E)$.

Remarque 40 : Matriciellement pour tout $A \in GL_n(\mathbb{K})$ il existe $P_1, \dots, P_r, Q_1, \dots, Q_s$ matrices de transvections telles que
$$A = P_1 \cdots P_r \det(A) I_n Q_1 \cdots Q_s$$

Application 41 : La méthode du pivot de Gauss est similaire à la démonstration du résultat précédent.

Définition 42 : Soit $u, v \in GL(E)$ on appelle commutateur de u et de v
$$[u, v] = uvu^{-1}v^{-1}$$

Exemple 43 : Si $u = id$, pour tout $v \in GL(E)$, $[u, v] = id_E$.

Définition 44 : On note $D(GL(E))$ le sous espace de $GL(E)$ engendré par les commutateurs et $D(SL(E))$ celui engendré par les commutateurs de $SL(E)$.

Théorème 45 : On a $D(GL_n(\mathbb{K})) = SL_n(\mathbb{K})$ sauf si $n = 2$ et $\mathbb{K} = \mathbb{F}_2$.
On a $D(SL_n(\mathbb{K})) = SL_n(\mathbb{K})$ sauf si $(n = 2, \mathbb{K} = \mathbb{F}_2)$ ou $(n = 2, \mathbb{K} = \mathbb{F}_3)$.

Théorème 46 : Le centre Z de $GL(E)$ est formé des homothéties $x \mapsto \lambda x$, $\lambda \in \mathbb{K}^*$
Il est donc isomorphe à $\mathbb{K}^*$.
Le centre de $SL(E)$ est $Z \cap SL(E)$, il est isomorphe à $\mu_n(\mathbb{K})$.

B Le groupe orthogonal Rom 22.5 Pey 8.5

On considère E un espace euclidien de dimension finie n.

Définition 47 : Si F est un sev de E, la symétrie orthogonale par rapport à F est l'application définie sur E par :

$$\forall x \in E, \quad s_F(x) = p_F(x) - p_{F^\perp}(x).$$

Remarque 48 : De $p_F + p_{F^\perp} = id$ on déduit que s_F est aussi définie par

$$\forall x \in E, \quad s_F(x) = 2p_F(x) - x = x - 2p_{F^\perp}(x).$$

Exemple 49 : Si $D = \mathbb{R}a$ est une droite vectorielle on a :

$$s_D(x) = 2p_D(x) - x = 2\left\langle \frac{x|a\rangle}{\|a\|^2} a - x \right.$$

Si $H = D^\perp$ est un hyperplan on a alors :

$$s_H(x) = 2p_H(x) - x = x - 2\frac{\langle x, a\rangle}{\|a\|^2} a$$

Définition 50 : On appelle réflexion une symétrie orthogonale par rapport à un hyperplan et demi-tour ou retournement une symétrie orthogonale par rapport à une droite.

Développement Pour $n = \dim E \geq 2$ le groupe $O(E)$ est engendré par l'ensemble des réflexions. Précisément, toute isométrie de E peut s'écrire comme le produit d'au plus n réflexions.

Théorème 51 : Pour $n \geq 3$, le groupe $O^+(E)$ est engendré par les renversements.

Lemme 52 : Si $n \geq 3$, pour τ_1, τ_2 réflexions il existe σ_1, σ_2 retournements tels que $\tau_1\tau_2 = \sigma_1\sigma_2$.

Références

Rombaldi Mathématiques pour l'agrégation Rom

Daniel Perrin Cours d'Algèbre Per

Xavier Gourdon Algèbre X.G