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

Romboldi
Ulmer
Perrin
Gourdon (dev 1)

I - Générateurs d'un groupe

1. Définitions

Définition 1.1 Soient G un groupe et $A \subset G$ une partie de G. Il existe un plus petit sous-groupe H de G contenant A. On dit que H est le sous-groupe engendré par A, ou que les éléments de A sont des générateurs de H.

On note $H = \langle A \rangle$.

Définition 1.2 L'ordre d'un élément g de G groupe est défini comme l'ordre du sous-groupe $\langle g \rangle$.

2. Groupes monogènes et cycliques

Définition 1.3 On dit qu'un groupe G est monogène s'il existe un élément $g \in G$ tel que $G = \langle g \rangle$.

Si de plus G est fini, on dit alors que G est cyclique.

Exemples 1.4

- le groupe $(\mathbb{Z},+)$ est monogène engendré par 1
- le groupe $(\mathbb{U}_n,+)$ est cyclique engendré par $e^{2i\pi/n}$

Théorème 1.5 Soit G un groupe monogène. S'il est infini, il est alors isomorphe à $(\mathbb{Z},+)$, s'il est fini d'ordre n, il est alors isomorphe à $(\mathbb{Z}_n,+)$.

Exemple 1.6

Un groupe G d'ordre p premier est cyclique engendré par chacun de ses éléments non neutres.

3. Sous-groupes d'un groupe cyclique

Soient $n \geq 2$ et $G = \langle g \rangle$ un groupe cyclique d'ordre n.

Proposition 1.7 Les sous-groupes de G sont cycliques d'ordre divisant n.

Théorème 1.8 Pour tout diviseur positif d de n, il existe un unique sous-groupe d'ordre d de G. Ce sous-groupe est le groupe cyclique $H = \langle g^{n/d} \rangle$. C'est également l'ensemble de tous les éléments de G d'ordre divisant d et les générateurs de H sont tous les éléments d'ordre d de G.

Le résultat précédent est en fait caractéristique des groupes cycliques :

Théorème 1.9 Un groupe commutatif fini d'ordre $n \geq 1$ est cyclique si, et seulement si pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d.

Exemple 1.10

les sous-groupes de $\mathbb{U}_n = \langle e^{2i\pi/n} \rangle$ sont les $\langle (e^{2i\pi/n})^{n/d} \rangle = \langle e^{2i\pi/d} \rangle = \mathbb{U}_d$ où d est un diviseur de n

Corollaire 1.11 Pour tout $n \geq 2$, $n = \sum_{d|n} \varphi(d)$.

II - Le groupe symétrique

Théorème 2.1 Toute permutation $\sigma \in \mathfrak{S}_n \setminus \{id\}$ se décompose en produit de cycles deux à deux disjoints. Cette décomposition est unique à l'ordre près.

Lemme 2.2 Soit $r \in [\![2,n]\!]$. Tout r-cycle de $\mathfrak{S}_n$ s'écrit comme produit de $r-1$ transpositions.

Corollaire 2.3 Soit $n \geqslant 2$, le groupe S_n est engendré par :

(i) les transpositions

(ii) les $n-1$ transpositions $(1\ k)$ $k \in [\![2, n]\!]$

(iii) les $n-1$ transpositions $(k\ k+1)$ $k \in [\![1, n-1]\!]$

(iv) $(1\ 2)$ et $(1\ 2 \dots n)$

Exemple 2.4

soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} = (1\ 2\ 3\ 4\ 5)(6\ 7)$

On a alors :

$$\begin{aligned} \sigma &= (1\,2)(2\,3)(3\,4)(4\,5)(6\,7) \\ &= (1\,2)(1\,2)(1\,3)(1\,2)(1\,3)(1\,4)(1\,3)(1\,4)(1\,5)(1\,4)(1\,6)(1\,7)(1\,6) \\ &= (1\,3)(1\,2)(1\,3)(1\,4)(1\,3)(1\,4)(1\,5)(1\,4)(1\,6)(1\,7)(1\,6) \end{aligned}$$

Proposition 2.5 Il existe un unique morphisme $S_n \longrightarrow \mathbb{C}^*$ non trivial.

Définition 2.6 On appelle ce morphisme la signature et on le note ε.
On définit le groupe alterné $\mathcal{A}_n$ comme le noyau de ε.

Proposition 2.7 Le groupe $\mathcal{A}_n$ est engendré par les 3-cycles.

Proposition 2.8 Pour $n = 3$ ou $n \geqslant 5$, le groupe $\mathcal{A}_n$ est simple.

Application 2.9 $\mathcal{A}_5$ est l'unique groupe simple d'ordre 60 à isomorphisme près.

III - En algèbre linéaire

1. Le groupe linéaire

On considère $\mathbb{K}$ un corps (commutatif) et E un $\mathbb{K}$-espace vectoriel de dimension n.

Définition 3.1 On désigne par matrices élémentaires de $\mathcal{M}_n(\mathbb{K})$ les matrices suivantes :

(i) les matrices de dilatation $D_i(\lambda) = I_n + (\lambda - 1)E_{i,i}$ avec $i \in [\![1, n]\!]$, $\lambda \in \mathbb{K}^*$

(ii) les matrices de transvection $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$, $i \neq j \in [\![1, n]\!]$, $\lambda \in \mathbb{K}^*$

(iii) les matrices de permutation $P_{ij} = I_n - (E_{ii} + E_{jj}) + (E_{ij} + E_{ji})$, $i \neq j \in [\![1, n]\!]$

Proposition 3.2 On a les correspondances suivantes avec les opérations élémentaires :

opération	$D_i(\lambda)A$	$T_{ij}(\lambda)A$	$P_{ij}A$	$AD_i(\lambda)$	$AT_{ij}(\lambda)$	AP_{ij}
résultat	$L_i \leftarrow \lambda L_i$	$L_i \leftarrow L_i + \lambda L_j$	$L_i \leftrightarrow L_j$	$C_i \leftarrow \lambda C_i$	$C_i \leftarrow C_i + \lambda C_j$	$C_i \leftrightarrow C_j$

Théorème 3.3 Le groupe $GL_n(\mathbb{K})$ est engendré par les transvections et les dilatations, tandis que le groupe $SL_n(\mathbb{K})$ est engendré par les transvections.

développement 1

Corollaire 3.4 Les espaces $GL_n(\mathbb{K})$ et $SL_n(\mathbb{K})$ sont connexes par arcs.

Définition 3.5 Soit φ une forme linéaire non nulle de E. On appelle :

- transvection d'hyperplan $\operatorname{Ker}\varphi$, $u : x \in E \longmapsto x + \varphi(x)a$ où $a \in \operatorname{Ker}\varphi$
- dilatation d'hyperplan $\operatorname{Ker}\varphi$, $v : x \in E \longmapsto x + \varphi(x)b$ où $b \in E \setminus \operatorname{Ker}\varphi$

Théorème 3.6 Le groupe $GL(E)$ est engendré par les transvections et les dilatations, tandis que $SL(E)$ est engendré par les transvections.

2. Le groupe orthogonal

On considère E un espace euclidien de dimension finie n.

Définition 3.7 On appelle réflexion une symétrie orthogonale par rapport à un hyperplan, et retournement une symétrie orthogonale par rapport à une droite.

Théorème 3.8 Le groupe $O(E)$ est engendré par les réflexions. Plus précisément, pour $u \in O(E)$, u est le produit de $p_u := \operatorname{rg}(u - id_E)$ réflexions.

Théorème 3.9 Le groupe $SO(E)$, pour $n \geqslant 3$, est engendré par les retournements. Plus précisément, $u \in SO(E)$ est produit d'au plus n retournements.

développement 2

Lemme 3.10 Si $n \geqslant 3$, pour τ_1, τ_2 réflexions, il existe σ_1, σ_2 retournements tels que $\tau_1 \tau_2 = \sigma_1 \sigma_2$.