108. Exemples de parties génératrices. Applications.

Cadre : $(G,\cdot)$ désigne un groupe. $n \in \mathbb{N}^*$, K est un corps commutatif.

I. Sous-groupe engendré par une partie

[Bu] **Déf. (1) :** Soit A une partie de G. Le sous-groupe de G engendré par A est le plus petit sous-groupe de G contenant A. On
141 le note $\langle A \rangle$. On dit que A est une partie génératrice de G si $\langle A \rangle = G$.

Rq (2) : 1) $H \leq G$ et $A \subset H \Rightarrow \langle A \rangle \subset H$ 2) $\langle A \rangle = A \iff A \leq G$

Th. (3) : Soit $A \subset G$. On note $A^{-1} = \{x^{-1}, x \in A\}$.
Alors, on a $\langle A \rangle = \{x_1 \dots x_n \;/\; n \geq 0 \text{ et } x_i \in A \cup A^{-1}\}$

142 **Rq (4) :** si G est abélien et $A = \{a_1 \dots a_r\} \subset G$,
alors $\langle A \rangle = \langle a_1 \dots a_r \rangle = \{a_1^{m_1} \dots a_r^{m_r},\ m_1 \dots m_r \in \mathbb{Z}\}$

Prop (5) : Soient G, G' deux groupes, $\varphi : G \to G'$ un morphisme de
♡ groupes et $A \subset G$ une partie génératrice. Alors φ est entièrement déterminé par ses valeurs prises sur A.
De plus, si φ est un isomorphisme, alors $\varphi(A)$ est une partie génératrice de G'.

II. Groupes monogènes, groupes cycliques

1) Définitions, premières propriétés

[Bu] **Déf. (6) :** G est dit monogène s'il peut être engendré par un
154 seul élément, et cyclique s'il est monogène fini.

Ex. (7) : 1) $\mathbb{Z} = \langle 1 \rangle$ et ses sous-groupes $n\mathbb{Z}$, $n \in \mathbb{N}$ sont monogènes non cycliques (sauf si $n = 0$)
2) pour tout $n \geq 1$, $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$ est cyclique

Th. (8) : 1) Si G est monogène non cyclique, alors $G \simeq \mathbb{Z}$
2) si G est cyclique et $|G| = n$, alors $G \simeq \mathbb{Z}/n\mathbb{Z}$ $(n \geq 1)$

2) Générateurs de $\mathbb{Z}/n\mathbb{Z}$. Applications $n \in \mathbb{N}^*$

Prop. (9) : Soit $n \geq 2$ et $a \in \mathbb{N}$. Sont équivalentes : ♡
1) $a \wedge n = 1$
2) $\bar{a}$ est un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$
3) $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$

Ex. (10) : Les générateurs de $\mathbb{Z}/4\mathbb{Z}$ sont $\bar{1}$ et $\bar{3}$ [Bu]

Th. (11) : Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $\langle \overline{\tfrac{n}{d}} \rangle$ ~155
où $d \in \mathbb{N}$ et $d \mid n$.

Coro. (12) : Si $G = \langle x_0 \rangle$ est cyclique de cardinal n et H est un sous-groupe de G d'ordre d, alors $H = \langle x_0^{\frac{n}{d}} \rangle$.

Déf. (13) : La fonction indicatrice d'Euler est définie par
$\varphi(n) = |\{1 \leq a \leq n \;/\; a \wedge n = 1\}|$. 156

Coro. (14) : 1) $\mathbb{Z}/n\mathbb{Z}$ admet $\varphi(n)$ générateurs
2) Pour tout $d \mid n$, $\mathbb{Z}/n\mathbb{Z}$ contient $\varphi(d)$ éléments d'ordre d.

Prop. (15) : 1) si $p \in \mathbb{N}$ est premier et $\alpha \in \mathbb{N}^*$, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ 156
2) si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, alors $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$.

Ex. (16) : $\mathbb{Z}/12\mathbb{Z}$ admet $1 \times (3-1) \times 2 \times (2-1) = 4$ générateurs

Prop. (17) : $n = \sum_{d \mid n} \varphi(d)$

Appli. (18) : Soit K un corps commutatif. Tout sous-groupe fini de $(K^*, \cdot)$ [Per]
est cyclique. 74

Appli. (19) : (théorème de structure des groupes abéliens finis) [Bu]
Si G est abélien fini, $|G| \geq 2$, alors : 358
$\exists !\ d_1, \dots, d_s \geq 2,\ d_1 \mid d_2 \mid \dots \mid d_s \;/\; G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$.

Ex. (20) : Si G est abélien et $|G| = 60$, alors $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ ou $G \simeq \mathbb{Z}/60\mathbb{Z}$

Exercice (21) : Si G est abélien fini et $\hat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$, montrer que $|\hat{G}| = |G|$

II. Groupe symétrique, groupe alterné $n \geq 2$

[Ber] ### 1) Générateurs de S_n

Th. (22) : Toute permutation se décompose comme produit de
204 cycles à support disjoint. Cette décomposition est unique à l'ordre des facteurs près.

206 Ex. (23) : $n = 6$. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix} = (1\,5)(2\,6\,3)$

Coro (24) : S_n est engendré par les cycles.

207 Coro (25) : S_n est engendré par les transpositions

~209 Prop. (26) : Soit $k \leq n$. Deux k-cycles sont conjugués dans S_n.

Prop. (27) : Les parties suivantes sont génératrices de S_n

212 213 1) $\{(1\,i),\ 2 \leq i \leq n\}$ 2) $\{(i, i+1),\ 1 \leq i \leq n-1\}$ 3) $\{(1\,2), (1\,2 \dots n)\}$

Appli. (28) : voir Lemme (40).

2) Rappels sur A_n. Générateurs et applications

Th. (29) : Il existe un unique morphisme surjectif $\varepsilon : S_n \to \{\pm 1\}$.
213 De plus, ε vaut -1 sur les transpositions. ε est appelé morphisme
214 signature.

215 Déf. (30) : Le groupe alterné d'ordre n est $A_n = \ker \varepsilon$.

Prop. (31) : $A_n \lhd S_n$ et $[S_n : A_n] = 2$

Ex. (32) : $A_2 = \{id\}$; $A_3 = \{1, \sigma, \sigma^2\}$ où $\sigma = (1\,2\,3)$ est cyclique.

Prop. (33) : Si $n \geq 3$, alors A_n est engendré par les familles suivantes :

216 1) les produits de deux transpositions

2) les 3-cycles

Lemme (34) : Si $n \geq 5$, les 3-cycles sont conjugués dans A_n 217

[Per]

Prop. (35) : Si $n \geq 2$, le sous-groupe dérivé de S_n est $D(S_n) = A_n$.
Si $n \geq 5$, $D(A_n) = A_n$. 28

Th. (36) : Si $n \geq 3$ et $n \neq 4$, alors A_n est simple. DVP 1 28

Rq (37) : Faux si $n = 4$. $D(A_4) \cong V_4 = \{id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ 30

Lemme (38) : Si $n \geq 3$, $Z(S_n) = \{id\}$ 13

Notation (39) : $\mathrm{Aut}(G)$ est l'ensemble des automorphismes de G et $\mathrm{Int}(G)$ l'ensemble des automorphismes intérieurs de G.

Lemme (40) : Soit $\varphi \in \mathrm{Aut}\, S_n$. Si φ transforme transposition 31
en transposition, alors $\varphi \in \mathrm{Int}\, S_n$.

Th. (41) : Si $n \neq 6$, $\mathrm{Aut}\, S_n = \mathrm{Int}\, S_n$. 30

Rq (42) : Faux si $n = 6$: $\mathrm{Aut}\, S_n / \mathrm{Int}\, S_n \cong \mathbb{Z}/2\mathbb{Z}$ 33

III. Groupe linéaire, groupe spécial linéaire $n \geq 1$.

Déf. (43) : $GL_n(K) = \{M \in \mathcal{M}_n(K) \,/\, M \text{ est inversible}\} = \{M \in \mathcal{M}_n(K) \,/\, \det M \neq 0\}$
$SL_n(K) = \{M \in \mathcal{M}_n(K) \,/\, \det M = 1\}$.

Prop. (44) : $(GL_n(K), \cdot)$ est un groupe et $SL_n(K) \leq GL_n(K)$.

1) Matrices de transvection, de dilatation et de permutation [Ber]

Déf. (45). Une matrice de transvection (resp. dilatation) est une matrice de la forme 76

$T_{ij}(\lambda) = \begin{pmatrix} 1 & & \\ & \ddots & \lambda \cdots \\ & & 1 \end{pmatrix} i$ (resp. $D_i(\lambda) = \begin{pmatrix} 1 & & \\ & \lambda & \cdots \\ & & 1 \end{pmatrix} i$ 79

où $1 \leq i \neq j \leq n$ et $\lambda \in K \setminus \{0\}$; où $1 \leq i \leq n$ et $\lambda \in K \setminus \{0, 1\}$)

Prop (46) : $D_i(\lambda) \in GL_n(K)$, $T_{ij}(\mu) \in SL_n(K)$ $\forall 1 \leq i \neq j \leq n$,
$D_i(\lambda)^{-1} = D_i\left(\frac{1}{\lambda}\right)$ $T_{ij}(\mu)^{-1} = T_{ij}(-\mu)$ $\forall \lambda \in K^*$, $\forall \mu \in K \setminus \{0, 1\}$

[BMP] 187 **Déf. 47** : Soit $\sigma \in S_n$ et $(e_1 \dots e_n)$ la base canonique de K^n. La matrice de permutation associée à σ est $P_\sigma \in \mathcal{M}_n(K)$ telle que $P_\sigma e_i = e_{\sigma(i)}$ pour tout $1 \leq i \leq n$. Si $\sigma = (ij)$, on notera $P_{ij} = P_{(ij)}$.

Prop. 48 : Pour tout $\sigma \in S_n$, $P_\sigma \in GL_n(K)$ et $\det P_\sigma = \varepsilon(\sigma)$

Prop. 49 : Soit $M \in \mathcal{M}_n(K)$. L'opération de multiplication à gauche ou à droite par une matrice de transvection (resp. dilatation, transposition) a un effet donné dans le tableau en ANNEXE.

Méthode 50 : L'algorithme du pivot de Gauss permet de transformer $M \in \mathcal{M}_{n,p}(K)$ en une matrice échelonnée.

Appli. 51 : Calcul de rang, de déterminant, résolution de système d'équation linéaire.

Ex. 52 : $M = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 2 & 0 \end{pmatrix} \xrightarrow{P_{12} \cdot M} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 2 & 0 \end{pmatrix} \xrightarrow{T_{32}(-2) \cdot} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & -2 \end{pmatrix}$ ⚠ $\det M = 2$

2) Générateurs de $GL_n(K)$ et de $SL_n(K)$

[Bu] **Th. 53** : 1) Toute matrice $M \in SL_n(K)$ est produit de matrices de transvection
79 2) Toute matrice $M \in GL_n(K)$ est produit de matrices de transvection et d'au plus une matrice de dilatation

[NAZU2] **Appli. 54** : 1) $SL_n(\mathbb{R})$, $SL_n(\mathbb{C})$ et $GL_n(\mathbb{C})$ sont connexes
116 2) $GL_n(\mathbb{R})$ admet deux composantes connexes : $GL_n^+(\mathbb{R})$ et $GL_n^-(\mathbb{R})$

IV. Groupe orthogonal et groupe spécial orthogonal

Cadre : $(E, \langle , \rangle)$ est un espace euclidien de dimension $n \geq 1$. Pour $u \in \mathcal{L}(E)$, on notera u^* son adjoint.

1) Définitions, propriétés fondamentales.

[Bu] **Déf. 55** : $O(E) = \{u \in \mathcal{L}(E) \,/\, u^* u = id\}$ est l'ensemble des isométries
99 de E. $SO(E) = \{u \in O(E) \,/\, \det u = 1\}$.

Prop. 56 : $(O(E), \circ)$ est un groupe appelé groupe orthogonal. $SO(E) \leq O(E)$ est appelé groupe spécial orthogonal.

Th. 57 : Soit $u \in \mathcal{L}(E)$ et F un sev de E. Si u est normal (resp. une isométrie) alors F et $F^\perp$ sont stables par u et u^*, et $u_{|F}$ est normal (resp. une isométrie). 96

2) Générateurs de $O(E)$ et de $SO(E)$

Rappel : $s \in \mathcal{L}(E)$ est une symétrie si $s^2 = id$. On a alors $E = \mathrm{Ker}(s - id) \oplus \mathrm{Ker}(s + id)$

Prop. 59 : Soit $s \in \mathcal{L}(E)$ une symétrie. Alors $s \in O(E)$ ssi $\mathrm{Ker}(s-id)^\perp = \mathrm{Ker}(s+id)$ 97

Déf. 60 : Une symétrie orthogonale par rapport à un hyperplan est appelée une réflexion orthogonale. 101
Si $n \geq 2$, une symétrie orthogonale par rapport à un sev de dimension $n-2$ est appelée un renversement. 104

Th. 61 : (générateurs de $O(E)$)
Soit $u \in O(E)$. On pose $r_u = rg(u - id)$. 102
i) u est le produit de r_u réflexions orthogonales.
ii) si u est produit de p réflexions orthogonales, alors $p \geq r_u$ DVP 2

Th. 62 : (générateurs de $SO(E)$)
Soit $u \in SO(E)$. Si $n \geq 3$, alors u est le produit d'au plus n renversements. 104

Rq 63 : Faux si $n = 2$. 105

Appli. 64 : $SO_3(\mathbb{R})$ est simple [Per] 148

ANNEXE

Prop. 49 :

$T_{ij}(\lambda)\Pi$	$D_i(\lambda)\Pi$	$P_{ij}\Pi$	$\Pi T_{ij}(\lambda)$	$\Pi D_i(\lambda)$	ΠP_{ij}
$L_i \leftarrow L_i + \lambda L_j$	$L_i \leftarrow \lambda L_i$	$L_i \leftrightarrow L_j$	$C_j \leftarrow C_j + \lambda C_i$	$C_i \leftarrow \lambda C_i$	$C_i \leftrightarrow C_j$

Références :

- [Be] Berhuy, *Algèbre : le grand combat* (2e éd.)
- [Per] Perrin, *Cours d'algèbre*
- [BMP] Beck, *Objectif agrégation* (2e éd.)
- [NH2G2] Caldero, *Nouvelles...* Tome 1