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

I. Définition

[P] p10

Def ① : soit $A \subset G$ (groupe). Le sous-groupe engendré par A est l'intersection de tous les sous-groupes de G qui contiennent A (noté $\langle A \rangle$). Une partie génératrice de G est alors une partie $A \subset G$ telle que $\langle A \rangle = G$.

prop ② : Un morphisme de groupes entre G et G' est entièrement déterminé par ses valeurs sur une partie génératrice de G.

II. Groupes monogènes

[R] p13

Def ③ : On dit que G est monogène s'il existe $g \in G$ tel que $G = \langle g \rangle$. G est dit cyclique s'il est de plus fini.

Ex ④ : $(\mathbb{Z}, +)$ et ses sous-groupes $n\mathbb{Z}$. $\mathbb{Z}/n\mathbb{Z}$.

Thm ⑤ : Soit G groupe monogène, alors il est isomorphe à $(\mathbb{Z}, +)$ s'il est infini, et s'il est cyclique d'ordre n, il est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.
en particulier, si $G = \langle g \rangle$ est cyclique, les générateurs de G sont alors les g^k où $k \in \{1, \dots, n-1\}$ est premier avec n.

[P] p24

Def ⑥ : On appelle fonction d'Euler et on note $\varphi(n)$ le nombre d'entiers x tq $1 \leq x \leq n$ et $x \wedge n = 1$
en particulier, un groupe cyclique a $\varphi(n)$ générateurs.

Thm ⑦ : Soit G un groupe cyclique de cardinal n ($G = \langle a \rangle$). $\forall d | n$, il existe un unique sous-groupe d'ordre d de G et c'est $H_d = \langle a^{\frac{n}{d}} \rangle$.

[P] p74

Lemme ⑧ : $\forall n \in \mathbb{N}^*$, on a $n = \sum_{d|n} \varphi(d)$

application ⑨ : soit K un corps et G sous-groupe fini de K^*. Alors G est cyclique.

p24

prop ⑩ : $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.

III. Groupe Symétrique

prop ⑪ : Soit $\sigma \in S_n$. $\langle \sigma \rangle$ agit sur $[\![1, n]\!]$ par

$$\begin{array}{ccc} \langle \sigma \rangle \times [\![1,n]\!] & \longrightarrow & [\![1,n]\!] \\ (\sigma^k, i) & \longmapsto & \sigma^k(i) \end{array}$$

Notant $O_1 \dots O_r$ les orbites pour cette action et notant $\sigma_j(x) = \begin{cases} x & \text{si } x \notin O_j \\ \sigma(x) & \text{si } x \in O_j \end{cases}$ alors $\sigma = \sigma_1 \dots \sigma_r$ est une décomposition de σ en cycles à support disjoints.

[R] p47

cor ⑫ : (i) les transpositions engendrent S_n.
(ii) les transposition $((1k))_{2 \leq k \leq n}$ engendrent S_n
(iii) les transposition $(k, k+1)_{1 \leq k \leq n}$ engendrent S_n
(iv) (12) et $(12 \dots n)$ engendrent S_n

application ⑬ : Il existe un unique morphisme non trivial $\varepsilon : S_n \to \mathbb{C}^*$ appelé morphisme signature.

Def ⑬ : On appelle groupe alterné noté $A_n = \ker(\varepsilon)$

PEG

prop ⑭ : (i) A_n est engendré par les produits d'un nombre pair de transposition
(ii) pour $n \geq 3$, A_n est engendré par les 3-cycles / les $(12i)$ $i \geq 3$
(iii) pour $n \geq 5$, A_n est engendré par les double-transpositions

Thm 15 : pour $n \geq 5$, A_n est simple,

cor 16 : les groupes distingués de S_n pour $n \geq 5$ sont $\{id\}$, A_n et S_n.

FGN 1 p69

Lemme 17 : Si un automorphisme de S_n transforme toute transposition en transposition, alors il est intérieur.

Thm 18 : pour $n \neq 6$, les automorphismes de S_n sont tous intérieurs.

IV. Le Groupe linéaire

ici, E désigne un ev de dimension finie n sur un corps $\mathbb{K}$.

NH2G2 p230

H2G2 p144

Def 19 : Les matrices élémentaires sont de la forme :

(i) dilatation $D_{i,\alpha}^{(p)} = \begin{pmatrix} I_{i-1} & & 0 \\ & \alpha & \\ 0 & & I_{p-i-1} \end{pmatrix}$ $\forall \alpha \in \mathbb{K}^*$, $1 \leq i \leq p$

(ii) transvection $T_{i,j,\beta}^{(p)} = \begin{pmatrix} 1 & & \beta \\ & \ddots & \\ & & 1 \end{pmatrix}$ β en (i,j), $\beta \in \mathbb{K}$, $1 \leq i \neq j \leq p$

(iii) permutation $1 \leq i < j \leq p$ $P_{ij}^{(p)} = P_{ji}^{(p)} = \begin{pmatrix} I_{j-1} & & & \\ & 0 & \cdots & 1 \\ & \vdots & I_{j-i-1} & \vdots \\ & 1 & \cdots & 0 \\ & & & I_{p-j-1} \end{pmatrix}$

prop 20 : On a les correspondances suivantes avec les opérations élémentaires : soit $A \in \mathcal{M}_{m,n}(\mathbb{K})$

opération	$D_{i,\alpha}^{(m)} A$	$T_{i,j,\beta}^{(m)} A$	$P_{i,j}^{(m)} A$
résultat	$L_i \leftarrow \alpha L_i$	$L_i \leftarrow L_i + \beta L_j$	$L_i \leftrightarrow L_j$

(on a le résultat analogue sur les colonnes en multipliant à droite)

NH2G2 p234

lemme 21 : on a $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -\lambda^{-1} & 1 \end{pmatrix}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ sont produits de transvections

FGN 2 p165

ou NH2G2 p245

Thm 22 : le groupe $SL_n(\mathbb{K})$ est engendré par les matrices de transvections. $GL_n(\mathbb{K})$ est engendré par les transvections et les dilatations.

app 23 : si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $SL_n(\mathbb{K})$ est connexe par arc

si $\mathbb{K} = \mathbb{R}$, $GL(\mathbb{R})_+ = \{M \in GL_n(\mathbb{R}),\ \det(M) > 0\}$ est connexe par arcs.

[O] p96

Def-prop 24 : Soit H un hyperplan de E et $u \in GL(E)$ tel que $u_{|H} = id_H$. Les conditions suivantes sont équivalentes :

1) $\det(u) = \lambda \neq 1$
2) u admet une valeur propre $\lambda \neq 1$ (donc une droite propre) et u est diagonalisable
3) $Im(u - Id) \not\subset H$
4) dans une base $Mat(u) = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix}$ $\lambda \in \mathbb{K}^*$ $\lambda \neq 1$

dans ce cas, u est une dilatation d'hyperplan H, de droite D, de rapport λ.

Def-prop 25 : Soit H un hyperplan de E, d'équation $f \in E^*$ ($H = \ker(f)$). Soit $u \in GL(E)$, $u \neq Id$ tel que $u_{|H} = Id_H$. Les conditions suivantes sont équivalentes :

1) $\det(u) = 1$
2) u non diagonalisable
3) $D = Im(u - Id) \subset H$
4) $\bar{u} : E/H \to E/H$ est l'identité ($\bar{u}(\bar{x}) = \overline{u(x)}$)
5) $\exists a \in H$, $a \neq 0$ et $\forall x \in E$ $u(x) = x + f(x)a$.

6) Dans une base. $\mathrm{Mat}(u) = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

On dit alors que u est une transvection d'hyperplan H et de droite D.

p 13 Thm (26) : Les transvections engendrent $SL(E)$.
Les transvections et les dilatations engendrent $GL(E)$.

V. Le groupe orthogonal

Def (27) : une réflexion est une symétrie orthogonale par rapport à un hyperplan. Un retournement est une symétrie orthogonale par rapport à un sev de dimension $n-2$.

FGN 3 p61 Thm (28) : $u \in O(E)$ s'écrit comme produit de r réflexions où $r = \mathrm{rg}(u - Id_E)$.

cor (29) : si $n \geq 3$, $SO(E)$ est engendré par les retournements

Thm (30) : (réduction des matrices orthogonales)
$\forall A \in O_n(\mathbb{R})$, $\exists\, Q \in O_n(\mathbb{R})$ tel que

$$A = Q \begin{pmatrix} R_{\theta_1} & & & & \\ & \ddots & & & 0 \\ & & R_{\theta_n} & & \\ 0 & & & -I_p & \\ & & & & I_q \end{pmatrix} \quad \text{où } R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

app (31) : $SO_n(\mathbb{R})$ est connexe par arcs.

Références :

FGN 1 : Francinou Algèbre 1 (17 18)
FGN 2 : ——————— 2 (22)
FGN 3 : ——————— 3 (V)
NH2G2 : Caldero Germoni (IV)
[P] : Perrin (Cours d'Algèbre)
[R] : Rombaldi (Maths pour l'agreg)