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

Francinou - Gianella | Bouvier - Richard.
Algèbre 1. | Groupe

Contexte : P une partie d'un groupe

Prop $\{\prod_{i=1}^{k} a_i^{\varepsilon_i} \mid a_i \in P, k \in \mathbb{N}, \varepsilon_i \in \{\pm 1\}\}$ est le plus petit sous groupe de G contenant P.

Def : On le notera $\langle P \rangle$ et nommera sous groupe engendré par P.

I) Exemples dans les groupes abéliens

a) Groupes monogènes

Def : groupe monogène, groupe cyclique, ordre

Prop : G groupe monogène alors soit $G \simeq \mathbb{Z}/n\mathbb{Z}, n \neq 0$ soit $G \simeq \mathbb{Z}$

Prop : Les sous groupes de $\mathbb{Z}$ sont monogènes.

appli : $n, m \in \mathbb{Z}$, $\langle n, m \rangle = (n \wedge m)\mathbb{Z}$

Props :
- si $k \in \mathbb{Z}/n\mathbb{Z}$ alors $\operatorname{ord}(k) = n/_{n \wedge k}$
- $\{\bar{k} \mid k \wedge n = 1\}$ est l'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$
- Ce sont les inversibles de $\mathbb{Z}/n\mathbb{Z}$: $(\mathbb{Z}/n\mathbb{Z})^\times$
- Les morphismes de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/m\mathbb{Z}$ sont déterminés par :

$$\bar{1} \longmapsto \frac{\alpha m}{n \wedge m} \quad \alpha \in [\![0, n\wedge m - 1]\!]$$

Cor : $\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

Thm : Tout sous groupe fini du groupe des inversibles d'un corps est cyclique.

exemples : $\mathbb{F}_p^\times \simeq (\mathbb{Z}/p-1\mathbb{Z})$ $\quad \mathbb{F}_4^\times = \langle j \rangle$

contre exemples : $\mathbb{U} < \mathbb{C}^\times$ n'est pas monogène
$Q_8 < \mathbb{H}^\times$ n'est pas commutatif.

b) Exemples de groupes abéliens non monogènes

On s'intéresse alors à ceux de type fini.

exemples : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}^3$ sont de type fini mais $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ ou $\mathbb{Q}/\mathbb{Z}$ ne le sont pas.

Thm : Tout sous groupe de $\mathbb{Z}^N$ est engendré par au plus N éléments.

Application : déplacements dans $\mathbb{Z}^N$

La démonstration du théorème fournit une réponse à la question :

Soit $\begin{cases} X \subset \mathbb{Z}^N \\ \#X < +\infty \end{cases}$ si $y \in \mathbb{Z}^N$, $y \in \langle X \rangle$? Si oui, trouver $\lambda_x \in \mathbb{Z}$, $y = \sum_{x \in X} \lambda_x x$.

algo (grossier)
Soit $(x^i)_i \in \mathbb{Z}^n$. Poser $d = \bigwedge_i x^i_n$
Par Bézout $d = \sum a_i x^i_n$. Poser $z^n = \sum_i a_i x^i$
Réitérer sur $(x^i - x^i_n/_d \, z^n)_i \in \mathbb{Z}^{n-1}$.
Alors (z^i) est une famille génératrice échelonnée.

ex : $N=2$ $\quad X = \{\binom{3}{1}, \binom{2}{2}, \binom{6}{3}\} = "(e_1, e_2, e_3)"$

alors $z_2 = e_1$ $\quad z_1 = (e_3 - 3e_1) - (e_2 - 2e_1) = e_3 - e_2 - e_1 = \binom{1}{0}$.

donc $\langle X \rangle = \mathbb{Z}^2$

si $y = \binom{a}{b}$ alors $y = be_1 + (a-3b)(e_3 - e_2 - e_1)$
$= (4b-a)e_1 + (a-3b)e_3 - (a-3b)e_2$

Thm (admis) Si G abélien de type fini alors $G \simeq \mathbb{Z}^m \times \prod_{i=1}^{k} \mathbb{Z}/d_i\mathbb{Z}$ où $d_1 \mid \dots \mid d_k$

Une telle décomposition est unique.

Pourrait faire un dvpt ici (Bouvier-Richard)

II) Générateurs en algèbre linéaire

k un corps, $n \in \mathbb{N}^*$, (E_{ij}) la base canonique de $M_n(k)$

A) $GL_n(k)$ et $SL_n(k)$

Def - si $\alpha \neq 0$ et $i \neq j$ alors $I + \alpha E_{ij}$ est une matrice de transvection.
- une transvection est une matrice semblable à une matrice de transvection.
- si $\alpha \neq 1$ alors $I + (\alpha - 1)E_{ii}$ est une matrice de dilatation.
- une dilatation est une matrice semblable à une matrice de dilatation.

Prop: $M \in M_n(k)$ de colonnes (C_j) et de lignes (L_i)
les opérations et manipulations suivantes sont équivalentes :
- $M(I + \alpha E_{ij})$ et $C_j \leftarrow C_j + \alpha C_i$
- $(I + \alpha E_{ij})M$ et $L_i \leftarrow L_i + \alpha L_j$

Thm $SL_n(k)$ est engendré par les matrices de transvections.

Rq : Une telle décomposition est effective.

Cor : - $GL_n(k)$ est engendré par les matrices de transvection et de dilatation
- Si $k \neq \mathbb{F}_2$, $GL_n(k)$ est engendré par les dilatations.
- $SL_2(k)$ est engendré par $\begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$ et $\begin{pmatrix} 1 & \alpha \\ & 1 \end{pmatrix}$, $\alpha \in k$

applications :

i) Connexité :
- $SL_n(\mathbb{R})$ et $GL_n(\mathbb{C})$ sont connexes par arcs.
- $GL_n(\mathbb{R})$ admet deux composantes connexes.

ii) $Z(SL_n(k)) = \mathbb{U}_n \, Id$

iii) si $n \neq 2, k \neq \mathbb{F}_2$, $D(GL_n(k)) = SL_n(k)$
si $n \neq 2, k \neq \mathbb{F}_2, \mathbb{F}_3$, $D(SL_n(k)) = SL_n(k)$

B) Homographies sur la droite projective.

Prop : - $PSL_2(k)$ est engendré par $z \mapsto z + a$, $a \in k$ et $z \mapsto -1/z$.
- Pour engendré $PGL_2(k)$ on adjoint $z \mapsto az$, $a \in k^\times$.

ex: $PGL(2,4) = PSL(2,4)$ est engendré par $z \mapsto z+1$, $z \mapsto zj$, $z \mapsto 1/z$

Cor : - $PGL_2(\mathbb{C})$ préserve les angles orientés
- $PGL_2(\mathbb{C})$ préserve l'ensemble constitué des cercles et des droites.

Def: $\mathcal{C} := \langle PGL_2(\mathbb{C}), z \mapsto \bar{z} \rangle$ le groupe circulaire.

Thm : $\mathcal{C}$ est le groupe des transformations qui préserve l'ensemble constitué des cercles et des droites.

C) Groupe orthogonal

Prop: $O_n(\mathbb{R})$ est engendré par les réflexions orthogonales
$SO_n(\mathbb{R})$ est engendré par les retournements orthogonaux.

Rq Une telle décomposition est effective.

application : - $O_n(\mathbb{R})$ a deux composantes connexes dont l'une est $SO_n(\mathbb{R})$.
- $SO_3(\mathbb{R})$ est simple) DVP
- Si $n > 2$, $D(SO_n(\mathbb{R})) = SO_n(\mathbb{R})$
si $n = 2$, $D(SO_2(\mathbb{R})) = \{Id\}$
- Si $n > 2$ impair $Z(SO_n(\mathbb{R})) = Id$, pair $Z(SO_n(\mathbb{R})) = \{\pm Id\}$

- Les opérateurs différentiels d'ordre 2, invariant par changement de repère orthonormé sont :
$$a\Delta + b, \quad a \in \mathbb{R}^*, b \in \mathbb{R}.$$

Bonne idée d'application.

Parler de birapport « les homographies préservent le birapport ».
Surjectivité de $SL(2,\mathbb{Z}) \twoheadrightarrow SL(2,\mathbb{Z}/p\mathbb{Z})$ (XENS)

III) Exemples dans les groupes finis

A) Quelques propriétés générales

Prop $|G| < +\infty$ alors il existe $P \subset G$ telle que $\langle P \rangle = G$ et $\# P \leq \log_2 |G|$

Rq Cette estimation est optimale : $G = (\mathbb{Z}/2\mathbb{Z})^n$

appli : $|\mathrm{Aut}(G)| \leq |G|^{\log_2 |G|}$

B) Groupe diédral

Def $D_n := \mathrm{Stab}_{O_2(\mathbb{R})}(\mathbb{U}_n)$ pour l'action canonique de $O_2(\mathbb{R})$ sur $\mathcal{P}(\mathbb{C}) = \mathcal{P}(\mathbb{R}^2)$

Prop: Si r est la rotation d'angle $2\pi/n$ et s la symétrie d'axe réel alors :

- $D_n = \langle r, s \rangle$
- $r^n = s^2 = id = (rs)^2$
- $|D_n| = 2n$

Thm : Représentations irréductibles de D_n :

- Pour $k = 1, \ldots, \lfloor \frac{n-1}{2} \rfloor$, $\begin{cases} r \longmapsto r^k \\ s \longmapsto s \end{cases}$ définit une représentation irréductible de degré 2. Ce sont les seules.
- Les représentations irréductibles de degré 1 sont le morphisme trivial et le déterminant avec : de plus si n est pair
$\chi(r^k) = (-1)^k \quad \chi(s) = \pm 1$

Prop: $D(D_n) = \langle r^2 \rangle$

C) Groupe symétrique

Prop: Toute permutation se décompose de manière unique en produit de cycles à support disjoints.

Prop : $\mathfrak{S}_n = \langle (i, i+1), i = 1 \ldots n-1 \rangle$
$= \langle (1,2), (1\,2 \ldots n) \rangle$
$= \langle (1,i), i = 1, \ldots, n \rangle$.

Thm: Les nombres d'éléments de deux décompositions d'une même permutation, en transposition, ont même parité.

Csq : La signature est bien définie.

Prop : A_n est engendré par les 3-cycles. (pour $n \geq 3$).

applications: A_4 est le groupe des rotations du tétraèdre
S_4 est le groupe des rotations du cube.

Thm : Pour $n \geq 5$, A_n est simple.

Thm: Pour $n \neq 6$, $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$) DVP
Simon $\mathrm{Aut}(\mathfrak{S}_6) / \mathrm{Int}(\mathfrak{S}_6) \simeq \mathbb{Z}/2\mathbb{Z}$

Les familles génératrices proposées ne sont pas minimales

ex : A_5 :

On a $PGL(2,4) \simeq A_5$.

Donc A_5 est engendré par 3 doubles transpositions :
$(0\,1)(j\,j^2)$; $(0\,j)(1\,j^2)$; $(0\,\infty)(j\,j^2)$ [où $[\![1,5]\!] \simeq \mathbb{P}_1(\mathbb{F}_4)$]

On peut faire mieux encore :
$(1\,2\,3)$ et $(1\,4)(2\,5)$ suffisent.

Refs: Perrin Cours d'algèbre
Caldero Germoni : H_2G_2

Automorphismes de $\mathfrak{S}_n$

Soit $n \neq 6$.

Théorème : $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$

Lemme : Soit $\sigma \in \mathfrak{S}_n$ un produit de p transpositions à supports deux à deux disjoints.

Alors le cardinal du centralisateur de σ est $2^p p!(n-2p)!$

Démonstration : σ s'écrit sous la forme $\prod_{i=1}^{p} (a_1^i\ a_2^i)$.

Soit $w \in \mathfrak{S}_n$ commutant avec σ. Alors $w\sigma w^{-1} = \sigma$

Donc $\prod_{i=1}^{p} (a_1^i\ a_2^i) = \prod_{i=1}^{p} (w(a_1^i)\ w(a_2^i))$

Donc w laisse stable $[\![1;n]\!] \setminus \{a_1^i ; a_2^i \ / \ i \in [\![1;p]\!]\}$

Et $\forall i \in [\![1;p]\!]\ \exists! j \in [\![1;p]\!]$ $\begin{cases} w(a_1^i) = w(a_2^j) & \text{et alors } w(a_2^i) = w(a_1^j) \\ \text{ou} & \\ w(a_1^i) = w(a_1^j) & w(a_2^i) = w(a_2^j) \end{cases}$

w envoie $\{a_1^i ; a_2^i\}$ sur $\{a_2^j ; a_1^j\}$ (permutation des p ensembles $\{a_1^k ; a_2^k\}$)

D'où le cardinal du centralisateur ($2^p p!(n-2p)!$)

Lemme : Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$ tel que φ envoie une transposition sur une transposition.

Alors $\varphi \in \mathrm{Int}(\mathfrak{S}_n)$

Démonstration : On pose $\varphi((12)) = (\alpha_1\ \alpha_2)$

Comme (12) et (13) ne sont pas disjoints et ne sont pas à supports disjoints, $\varphi((13))$ est de la forme (α_1, α_3), $\alpha_3 \neq \alpha_2$.

De la même façon, $\varphi((1m)) = (\alpha_1, \alpha_m)$ ou (α_2, α_m) pour $m \geq 3$

Or $(13)(12)(13) = (23)$ donc $\varphi((23)) = (\alpha_2\ \alpha_3)$ et (23) et $(1m)$ sont à supports disjoints donc $\varphi((1m))$ et $(\alpha_2\ \alpha_3)$ aussi.

D'où $\varphi((1m)) = (\alpha_1, \alpha_m)$. et $\alpha : i \mapsto \alpha_i$ est une permutation de $[\![1;n]\!]$.

On considère l'automorphisme de $\mathfrak{S}_n$ (intérieur) suivant $\psi : \sigma \mapsto \alpha\sigma\alpha^{-1}$. ψ et φ sont égales sur les transpositions, qui engendrent $\mathfrak{S}_n$. Donc $\varphi = \psi$ et φ est intérieur.

Démonstration : Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$.

Soit τ une transposition de $\mathfrak{S}_n$.

$\varphi(\tau)$ est d'ordre 2 donc est un produit de p transpositions.

Or le cardinaux des commutants de τ et de $\varphi(\tau)$ sont égaux.

i.e. $2^p p!(n-2p)! = 2(n-2)!$

Et donc, comme $n \neq 6$, on a $p=1$

Donc φ envoie toute transposition sur une transposition et $\varphi \in \mathrm{Int}(\mathfrak{S}_n)$

Développement : Simplicité de $SO_3(\mathbb{R})$
Binome : Léo Bigorgne et Joackim Bernier
Référence : Philippe Caldero et Jérôme Germoni, *Histoires hédonistes de groupes et de géométries* page 237
Prérequis :

— Réduction de $O_n(\mathbb{R})$: Si $M \in O_n(\mathbb{R})$ alors il existe $P \in O_n\mathbb{R}$ tel que $P^{-1}MP$ soit diagonale par blocs, chacun des blocs étant d'une des trois formes suivantes : $-1, 1, \begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix}$ pour $\theta \in \mathbb{R}$.
— corollaire : $SO_n(\mathbb{R})$ est connexe par arcs.
— $SO_n(\mathbb{R})$ est compact.
— Si $M \in O_n(\mathbb{R})$ stabilise un sous espace H alors il stabilise aussi son orthogonal.
— $O_n(\mathbb{R})$ est engendré par les reflexions.
— Le centre de $SO_n(\mathbb{R})$ ne contient que des matrices scalaires.

Idée des preuves :

— Par récurrence totale sur la dimension à initialiser pour $n = 2$. Puis montrer qu'il existe soit un plan soit une droite stable.
— Par récurrence sur la dimension. On prend $x \neq u(x)$ on compose à gauche par la réflexion d'hyperplan $(x - u(x))^{\perp}$.
— Un endomorphime qui commute avec un autre laisse stable ses sous espaces propres.

La démonstration :

— **Définition : Retournement orthogonal** élément de $SO_n(\mathbb{R})$ dont la réduction ne contient que des 1 et deux -1.
— **Étape 1 : Pour $n \geq 3$, $SO_n(\mathbb{R})$ est engendré par les retournements orthogononaux.** Si $u \in SO_n(\mathbb{R})$ alors $u = \prod_{i=1}^{2k} R_{H_i}$. On montre donc qu'un produit de deux réflexions R_H et $R_{H'}$ et un produit de deux retournements orthogononaux.
Soit F un sous espace de dimension 1 dans $H \cap H'$, on pose alors :

$$\begin{cases} r|F = -I_1, \\ r|F^{\perp} = R_H|F^{\perp}, \\ r'|F = -I_1, \\ r'|F^{\perp} = R_{H'}|F^{\perp}. \end{cases}$$

r est un retournement car $r|F^{\perp}$ est une réflexion.
Attention dans la référence il y a une erreur.
— Soit H un sous groupe distingué non trivial de $SO_3(\mathbb{R})$.
— **Étape 2 : Si H contient un retournement, il les contient tous.** Soit $r_D \in H$ un retournement d'axe D. Soit D' une autre droite. Alors il existe $s \in SO_3(\mathbb{R})$ envoyant D sur D'. Alors $r_{D'} = srs^{-1} \in H$.
— **Étape 3 : H contient au moins un retournement.**
Soit $h \in H$ non trivial. On pose alors : $\begin{array}{cccc} \phi & : & SO_3(\mathbb{R}) & \to & \mathbb{R} \\ & & g & \mapsto & tr(ghg^{-1}h^{-1}) \end{array}$ Si $g \in SO_3(\mathbb{R})$ alors $ghg^{-1}h^{-1} \in H$ puisque H est distingué. Si θ est l'angle associé au bloc de taille deux de $ghg^{-1}h^{-1}$ alors $\phi(g) = 1+2cos(\theta) \leq 3$ et il y a égalité pour $g = h$.
Puisque $SO_3(\mathbb{R})$ *est connexe* et ϕ est continue alors $\phi(SO_3(\mathbb{R})) := [a; 3]$.
Par l'absurde si a=3 alors, pour tout $g \in SO_3(\mathbb{R})$, $tr(ghg^{-1}h^{-1}) = 3$, donc $ghg^{-1}h^{-1} = I_3$ $(\theta = 0)$. Mais alors $h = I_3$ ce qui est exclu.
Donc $a < 3$, donc il existe $n \in \mathbb{N}$ tel que $a < 1 + 2cos(\frac{\pi}{n}) < 3$. Soit g l'antécédent d'un tel élément, alors $ghg^{-1}h^{-1}$ est une rotation d'angle $\frac{\pi}{n}$. Ainsi, $(ghg^{-1}h^{-1})^n$ est un retournement qui est dans H.