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

I/ Généralités et définitions

1) Partie génératrice d'un groupe

Def 1: Pour A une partie d'un groupe G, on note $\langle A\rangle$ le plus petit sous groupe de G contenant A. Il est appelé sous groupe engendré par A.

Ex 2: On appelle groupe dérivé de G (noté $D(G)$) le groupe engendré par les commutateurs, i.e. les éléments de la forme $[x,y]=xyx^{-1}y^{-1}$

Prop 3: Une intersection de sous groupes est un groupe et pour $A\subset G$,
$$\langle A\rangle = \bigcap_{H_i<G \text{ avec } A\subset H_i} H_i$$

Prop 4: On a $\langle A\rangle = \{x_1^{m_1}\dots x_p^{m_p} \mid p\in\mathbb{N},\ (x_1,\dots x_p)\in A^p,\ (m_1,\dots m_p)\in\mathbb{Z}^p\}$

Def 5: On dit que A est une partie génératrice de G si $\langle A\rangle = G$.

Thm 6: Soit P un prédicat sur G. Si P est vérifié sur une partie génératrice de G et P vérifie $\forall a,b\in G, [P(a)\wedge P(b)] \Rightarrow P(ab)$, alors P est vérifié sur G.

Thm 7: Soient f et g deux morphismes de groupes de G dans H. Soit $A\subset G$ t.q $\langle A\rangle = G$. Si $\forall a\in A, f(a)=g(a)$, alors $f=g$.

2) Rang d'un groupe et éléments superflus:

Def 8: Le rang d'un groupe est le cardinal de la plus petite famille génératrice.

Ex 9: $(\mathbb{Z}/n\mathbb{Z},+)$ est de rang 1.

Def 10: Un élément $x\in G$ est dit superflu (ou mou) si pour toute partie $S\subset G$, $\langle S,x\rangle = G \Rightarrow \langle S\rangle = G$

Ex 11: L'élément neutre est superflu

Def 12: L'ensemble des éléments superflus est un groupe noté $\Phi(G)$ et appelé groupe de Frattini.

Thm 13: $\Phi(G)$ est l'intersection des sous groupes maximaux de G.

Thm 14: Soit G un p-groupe fini. Alors $G/\Phi(G)$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$ pour un certain n, et peut donc être vu comme un $\mathbb{F}_p$ espace vectoriel. (admis)

3) Groupe libre et présentation par générateurs et relations

Def 15: Soit Σ un ensemble et Σ^{-1} en bijection avec Σ. On note x^{-1} l'image de $x\in\Sigma$ par cette bijection. On pose $\mathcal{L}(\Sigma) = (\Sigma\cup\Sigma^{-1})^{(\mathbb{N})}$. Les séquences sont appelées mots. Deux mots sont équivalents si l'on peut passer de l'un à l'autre en supprimant les sous séquences de la forme xx^{-1} ou $x^{-1}x$. On pose $L(\Sigma) = \mathcal{L}(\Sigma)/\sim$. C'est un groupe muni de la concaténation, appelé groupe libre sur Σ.

Rem 16: Intuitivement, le groupe libre est le plus grand groupe engendré par Σ.

Def 17: Soit Σ un ensemble et R un sous ensemble de $L(\Sigma)$. Soit H le sous groupe distingué de $L(\Sigma)$ engendré par R. On note $\langle\Sigma|R\rangle$ le groupe G/H. On dit que $\langle\Sigma|R\rangle$ est une présentation de G/H.

Ex 18: Le groupe diédral D_n des isométries conservant un polygone régulier à n côtés a pour présentation $\langle r,s \mid r^n, s^2, (rs)^2\rangle$.

II/ Groupes abéliens

1) Groupes monogènes et groupes cycliques.

Def 19: Un groupe G est dit monogène s'il est engendré par un singleton. Si de plus G est fini, il est dit cyclique.

Ex 20: $(\mathbb{Z}/n\mathbb{Z},+)$ et $(\mathbb{Z},+)$ sont engendrés par 1 et donc respectivement cyclique et monogène.

Rem 21: Tout groupe monogène est abélien. De plus, G monogène $\Longleftrightarrow$ G est de rang 1.

Prop 22: Tout groupe monogène est isomorphe à $(\mathbb{Z},+)$ ou à un $(\mathbb{Z}/n\mathbb{Z},+)$

Def 23: On appelle ordre de a (potentiellement infini), le cardinal de $\langle a\rangle$.

Thm 24 (Cauchy): Soit G un groupe fini et p un diviseur premier de $\#G$. Alors il existe un élément d'ordre p dans G.

Def 25: L'indicatrice d'Euler φ est la fonction qui à chaque entier naturel n associe le nombre d'entiers entre 1 et n, premiers avec n.

Ex 26: Pour tout entier premier p, $\varphi(p) = p-1$

Prop 27: Dans $\mathbb{Z}/n\mathbb{Z}$, l'ordre de $\bar{k}$ est égal à $\frac{n}{n \wedge k}$. Par conséquent, $\mathbb{Z}/n\mathbb{Z}$ est cyclique et engendré par les $\bar{k}$ avec k premiers avec n. Le groupe $\mathbb{Z}/n\mathbb{Z}$ possède donc $\varphi(n)$ générateurs.

Prop 28: Le produit $G_1 \times \dots G_n$ de groupes cycliques d'ordre $m_1, \dots m_n$ est cyclique, si et seulement si les m_i sont premiers entre eux 2 à 2.

2) Groupe abéliens de type fini:

Def 29: Un groupe est dit de type fini si il admet une partie génératrice finie

Rem 30: Tout groupe fini est de type fini car $\langle G \rangle = G$.

Thm 31: Soit G abélien fini. Il existe une unique séquence d'entiers $q_1, \dots q_n$ telle que $\forall i, q_i | q_{i+1}$ et G soit isomorphe à $\left(\mathbb{Z}/_{q_1\mathbb{Z}} \times \dots \mathbb{Z}/_{q_n\mathbb{Z}}\right)$.

Def 32: Cette suite d'entiers est appelée suite des invariants de G.

App 33: Énumération des groupes finis abéliens d'ordre $600 = 2^3 \times 5^2 \times 3$.

Thm 34: Soit G abélien de type fini. Il existe une unique séquence d'entiers r, $q_1 \dots q_n$ telle que $\forall i, q_i | q_{i+1}$ et G soit isomorphe à

$$\mathbb{Z}^r \times \mathbb{Z}/_{q_1\mathbb{Z}} \times \dots \times \mathbb{Z}/_{q_n\mathbb{Z}}.$$

III/ Groupes de permutations

1) Le groupe symétrique.

Def 35: On note $\mathfrak{S}_n$ le groupe des permutations d'un ensemble à n éléments, muni de la composition.

Prop 36: Générateurs classiques de $\mathfrak{S}_n$:
- L'ensemble des cycles
- L'ensemble des transpositions
- L'ensemble des transpositions de la forme $(1\ i)$
- L'ensemble des transpositions de la forme $(i\ i{+}1)$
- $\{(1\ 2), (1\ 2 \dots n)\}$

Rem 37: $\mathfrak{S}_n$ est de rang 2 car non cyclique.

2) Le groupe alterné

Def 38: On note $\mathfrak{A}_n := \ker(\varepsilon)$ le sous groupe distingué de $\mathfrak{S}_n$ des permutations de signature 1.

Prop 39: Générateurs de $\mathfrak{A}_n$:
- L'ensemble des 3-cycles si $n \geq 3$.
- $\{(1\ 2\ 3), (1\ 2 \dots n)\}$ si n impair
- $\{(1\ 2\ 3), (2\ 3 \dots n)\}$ si n pair.

Prop 40: Les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

Thm 41: Pour $n \neq 4$, le groupe $\mathfrak{A}_n$ est simple (i.e. il ne possède pas de sous groupes normaux non triviaux.) DEV 1

Cor 42: On a $D(\mathfrak{A}_n) = \mathfrak{A}_n$ pour $n \geq 5$ et $D(\mathfrak{S}_n) = \mathfrak{A}_n$ pour $n \geq 2$.

Thm 43: Pour $n \neq 6$, tout automorphisme de $\mathfrak{S}_n$ est intérieur

IV/ Groupe linéaire

Soient $\mathbb{K}$ un corps commutatif et E un $\mathbb{K}$-espace vectoriel de dimension fini n.

Def 44: L'ensemble des automorphismes muni de la composition est un groupe appelé groupe linéaire et noté $GL(E)$. Le sous groupe de $GL(E)$ composé des automorphismes de déterminant 1 est le groupe spécial linéaire (noté $SL(E)$)

On note encore $GL(n, \mathbb{K})$ et $SL(n, \mathbb{K})$ ces groupes vus comme groupes de matrices.

Def 45: Soit H un hyperplan de E et $u \in GL(E)$ tel que $u_{|H} = id_H$. Les assertions suivantes sont équivalentes :
- $\det(u) = \lambda \neq 1$
- u admet une valeur propre $\lambda \neq 1$ et u est diagonalisable.
- $\operatorname{Im}(u - id) \not\subset H$
- dans une base adéquate $\mathcal{B}$, $[u]_{\mathcal{B}} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix}$ avec $\lambda \neq 1$.

On dit que u est une dilatation.

Def 46: Soit $f \in E^* \setminus 0$, $H := \ker(f)$ et $u \in GL(E) \setminus \{id\}$ tel que $u_{|H} = id_H$. Les assertions suivantes sont équivalentes :
- $\det(u) = 1$
- u n'est pas diagonalisable
- $D := \operatorname{Im}(u - id) \subseteq H$
- le morphisme induit $\bar{u} : E/_H \to E/_H$ est l'identité sur $E/_H$.

- il existe $a \in E \setminus \{0\}$ tel que $\forall x \in E$, $u(x) = x + f(x)a$
- dans une base convenable $\mathcal{B}$, $[u]_{\mathcal{B}} = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & 1 \\ 0 & & & 1 \end{pmatrix} = I + E_{n-1,n}$

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

DEV 2

Thm 47: $SL(E)$ est engendré par les transvections.

Prop 48: Les transvections sont conjuguées dans si $n \geqslant 3$.

Thm 49: $GL(E)$ est engendré par les transvections et les dilatations.

App 50: $PSL(n, \mathbb{K})$ est simple sauf si $n=2$ et ($\mathbb{K} = \mathbb{F}_2$ ou $\mathbb{F}_3$)

Prop 51: On a :
- $D(GL(n,\mathbb{K})) = SL(n,\mathbb{K})$ sauf si $n=2$ et $\mathbb{K} = \mathbb{F}_2$.
- $D(SL(n,\mathbb{K})) = SL(n,\mathbb{K})$ sauf si $n=2$ et ($\mathbb{K} = \mathbb{F}_2$ ou $\mathbb{F}_3$).

App 52: . Les sous groupes distingués de $GL(n,\mathbb{K})$ non triviaux sont les sous groupes du centre et les sous-groupes de $SL(n,\mathbb{K})$ (quand $n \geqslant 3$)
. Les sous groupes distingués non triviaux de $SL(n,\mathbb{K})$ sont les sous groupes du centre.

Prop 53: Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $SL(n,\mathbb{K})$ est connexe par arcs.

V/ Groupe orthogonal

Soit E un espace vectoriel euclidien réel de dimension finie n.

Def 54: L'ensemble des isométries muni de la composition est un groupe appelé groupe orthogonal et noté $O(E)$. L'ensemble des isométries de déterminant 1 est un sous groupe distingué de $O(E)$, noté $SO(E)$ et appelé groupe spécial orthogonal.

Notation 55: Soit $u \in GL(E)$ telle que $u^2 = id_E$. On pose $E^+(u) = \ker(u - id)$ et $E^-(u) = \ker(u + id)$. On a $E^+(u) \oplus E^-(u) = E$ et dans une base adaptée $\mathcal{B}$, $[u]_{\mathcal{B}} = \begin{pmatrix} \underbrace{\begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix}}_{p} & 0 \\ 0 & \underbrace{\begin{matrix} -1 & & \\ & \ddots & \\ & & -1 \end{matrix}}_{n-p} \end{pmatrix}$ où $p = \dim(E^+(u))$.

Si $u \neq id_E$, on dit que u est une symétrie. Si $\dim(E^-(u)) = 1$, on dit que u est une réflexion, si $\dim(E^-(u)) = 2$, c'est un renversement

Prop 56: Soit u une symétrie. u est une isométrie si et seulement si $E^-(u)$ et $E^+(u)$ sont orthogonaux.

Thm 57: Chaque isométrie est produit d'au plus n réflexions orthogonales. Par conséquent, les réflexions engendrent $O(E)$.

Prop 58: Les décompositions des isométries de $SO(E)$ en produit de réflexion orthogonales font intervenir un nombre pair de termes.

Thm 59: Pour $n \geqslant 3$, chaque isométrie $u \in SO(E)$ est produit d'au plus n renversements orthogonaux. Par conséquent les renversements engendrent $SO(E)$.

Références :

- Algèbre et Géométrie, Combes
- Théorie des groupes, Delcourt
- Cours d'Algèbre, Perrin
- Théorie des groupes, Ulmer