Exemples de parties génératrices de groupes. Applications

I- Généralités.

Th 1 : Soit G un groupe. Toute intersection non vide de sous-groupes de G est un sous-groupe de G.

Def 1 : Soit $S \subset G$, on définit le sous-groupe engendré par S : $\langle S \rangle = \bigcap_{\substack{H < G \\ S \subset H}} H$

C'est le plus petit sous-groupe de G contenant S.

- Soit $S \subset G$ et $H \subset G$ un sous-groupe tel que $\langle S \rangle = H$: on dit que S est une partie génératrice de H.

Rq 1 : $\langle S \rangle = \{ s_1 \dots s_n / n \in \mathbb{N}$ et $\forall i \in [\![1, n]\!], s_i \in S$ ou $s_i^{-1} \in S \}$ ce sont des mots de longueur finie en les éléments de S ou leurs inverses.

Cor 1 : Soit $S \subset G$ une partie génératrice. Alors G est commutatif si et seulement si les éléments de S commutent 2 à 2.

Ex 1 : $(\mathbb{Q}, +)$ est engendré par $\{ \frac{1}{p}, p$ premier $\}$. C'est un groupe commutatif.

Exemples de parties génératrices :

a) **Th 2 : Cartan-Dieudonné** : Dev 1

- Soit $u \in O(E)$, alors u peut s'écrire comme le produit de moins de n réflexions, où $r = \text{rg}(u - \text{id})$
- Soit $u \in SO(E)$, alors u peut s'écrire comme le produit de moins de n retournements, où $r = \text{rg}(u - \text{id})$

b) **Th 3** :
- $SL(E)$ est engendré par les transvections
- $GL(E)$ est engendré par les transvections et les dilatations.

Dev

Application : $\mathcal{D}(GL_n(\mathbb{K})) = SL_n(\mathbb{K})$ sauf pour $GL_2(\mathbb{F}_2)$ et $GL_2(\mathbb{F}_3)$

c) **Th 4 : Décomposition polaire**

Soit $A \in GL_n(\mathbb{R})$, alors il existe un unique couple $(O, S) \in O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R})$ tel que $A = OS$.

Th 5 : Décomposition QR

Soit $A \in GL_n(\mathbb{R})$, alors il existe un unique couple $(Q, R) \in O_n(\mathbb{R}) \times T_n^{++}(\mathbb{R})$ tel que $A = QR$

Prop: Si $\varphi, \psi : G \to H$ morphismes coïncident sur une partie génératrice de G, alors ils sont égaux

Rq: Même si il y a unicité dans les deux dernières décompositions, il n'y a pas unicité de l'écriture dans le système de générateurs !

II - Groupes de type fini

Def 2: G est de type fini si il existe $s_1, \dots, s_n \in G$ tels que $G = \langle s_1, \dots, s_n \rangle$

Ex: $SL_2(\mathbb{Z}) = \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$ donc $SL_2(\mathbb{Z})$ est de type fini.

Th: de structure des groupes abéliens de type fini: (6).

Tout groupe abélien G de type fini est isomorphe à un produit direct de groupe de la forme

$$\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z}^r$$

où $r, k \in \mathbb{N}$, et $\forall i \in \{1, \dots, k-1\}$, $m_i \mid m_{i+1}$.

Application: En notant ψ l'isomorphisme du théorème de structure, on a $G = \langle \{\varphi^{-1}(e_i), 1 \le i \le n+r\} \rangle$ où $e_i = (0, \dots, \underset{\text{i ème}}{\bar{1}}, 0, \dots, 0)$

2) Groupes monogènes

Def 3: Un groupe est monogène si il peut être engendré par un seul élément

Prop 1: un groupe monogène est abélien.

Prop 2: la donnée d'un générateur s d'un groupe G monogène, définit un morphisme surjectif de $\mathbb{Z}$ dans G : $n \mapsto s^n$.

3) Groupes cycliques

Def 4: Un groupe est cyclique si il est monogène fini.

Prop 3: Tout groupe cyclique est isomorphe à un $\mathbb{Z}/n\mathbb{Z}$ pour un certain $n \in \mathbb{N}^*$.

Prop 4: Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{k}$ tq $k \wedge n = 1$. Il y en a donc $\varphi(n)$.

Cor 2: $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Prop 5: Soit k un corps fini, alors tout sous-groupe fini de $(k^*, \times)$ est cyclique.

III - Le groupe symétrique et le groupe diédral.

Def: S_n est l'ensemble des bijections de $\{1,\dots,n\}$ dans lui-même, muni de la loi de composition.

Prop: S_n est engendré par l'un des ensembles suivants:
- les cycles.
- les transpositions
- $\{(1,i),\ 1\leq i\leq n\}$
- $\{(i,i+1),\ 1\leq i<n\}$
- $\{(1,2),(1,\dots,n)\}$

Cor: $Aut(S_n) = Int(S_n)$, $n\neq 6$

Def+Prop: Il existe un unique morphisme de groupe $\varepsilon : S_n \to \mathbb{Z}/2\mathbb{Z}$ surjectif; c'est la signature. On définit $A_n = \ker(\varepsilon)$ le groupe alterné.

Prop: A_n est engendré par l'un des ensembles suivants:
- Les cycles de longueur impaire
- Les 3-cycles
- $\{(1,i,j),\ 2\leq i,j\leq n\}$
- $\{(1,2,i),\ 3\leq i\leq n\}$

Cor: Soit $\varphi : S_n \to S_n$, $x \mapsto x^2$, alors $Im(\varphi) = A_n$

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

Références:
- Oraux X-ENS 1,2,3 Algèbre
- Th des groupes; Feta Ulmer
- Perrin
- Ccarlet (Décomposition)..

autre possibilité: groupes linéaires
réf: Caldero