108 Exemples de parties génératrices de groupe.

Introduction pour G un groupe et $A \in \mathcal{P}(G)$ on note $<A>$ l'intersection de tous les sous-groupes de G contenant A. C'est le plus petit sous-groupe de G qui contient A et on dit que c'est le sous-groupe engendré par A. On dit que A est une partie génératrice de G lorsque $<A> = G$

I] Groupes abéliens

1) Groupes monogènes et cycliques

Déf 1 Si A est réduit à un élément et $G = <A>$ alors on dit que G est monogène

Déf 2 Un groupe monogène et fini est dit cyclique

Exemple 3 $\mathbb{Z} = <1>$ est monogène non cyclique
$\mathbb{Z}/p\mathbb{Z} = <\bar{1}>$ est cyclique.

Proposition 4 Pour $a \in G$, $<a>$ est isomorphe à $\mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$ pour $n \in \mathbb{N}$

Corollaire 5 Si $|G|$ est fini premier alors G est cyclique.

Corollaire 6 Si $G \cong \mathbb{Z}/n\mathbb{Z}$ alors G admet $\varphi(n)$ générateurs

2) Groupes abéliens de type fini

Théorème 7 Soit G un groupe abélien fini. Alors il existe des entiers $a_1, \dots, a_n$ uniques tels que $a_n \geq 2$ et $a_n | a_{n-1} | \dots | a_1$ et
$$G \cong (\mathbb{Z}/a_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/a_n\mathbb{Z})$$

Application 8 : Critère d'isomorphie de deux groupes abéliens finis.

Théorème 9 : Soit G un groupe abélien de type fini. Alors il existe des entiers $a_1, \dots, a_n, r$ uniques tels que $a_n \geq 2$; $a_n | a_{n-1} | \dots | a_1$ et
$$G \cong \mathbb{Z}^r \times (\mathbb{Z}/a_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/a_n\mathbb{Z})$$

II] Groupes symétriques et diédraux

1) Groupes symétriques

Déf 10 : pour $n \in \mathbb{N}^*$, on appelle le groupe symétrique de degré n et on note $\mathfrak{S}_n$ le groupe des permutations de $[\![1, n]\!]$.

Théorème 11 : pour $n \geq 2$, $\mathfrak{S}_n$ est engendré par les transpositions.

Proposition 12 : pour $n \geq 2$, $\mathfrak{S}_n$ est engendré par l'un quelconque des ensembles suivants :
- les transpositions $(1, i)$ avec $2 \leq i \leq n$,
- les transpositions $(i, i+1)$ avec $1 \leq i \leq n-1$,
- la transposition $(1, 2)$ et le n-cycle $(1, 2, \dots, n)$

Déf 13 : pour $\sigma \in \mathfrak{S}_n$ la signature de σ est $\varepsilon(\sigma) := (-1)^p$, où $p := \text{card}\{(i,j) \in [\![1,n]\!]^2 \mid i < j \text{ et } \sigma(j) > \sigma(i)\}$

Déf 14 : Le noyau de ε est appelé le groupe alterné et noté $\mathcal{A}_n$

Théorème 15 : pour $n \geq 3$, A_n est engendré par les 3-cycles de la forme $(1,2,i)$ avec $3 \leq i \leq n$

Application 16 : pour $n \geq 5$, A_n est simple.

2) Groupes diédraux

Déf 17 : Soit D_n l'ensemble des isométries du plan qui conservent un polygone régulier à n côtés, autrement dit, qui conservent globalement l'ensemble de ses n sommets.
On appelle D_n le groupe diédral de degré n. $(n \geq 2)$

Prop 18 : D_n est fini d'ordre $2n$.

Prop 19 : D_n est engendré par la rotation de centre le centre du polygone et d'angle $\frac{2\pi}{n}$ et par une symétrie axiale d'axe un axe de symétrie du polygone.
D_n admet la présentation : $\langle a, b \mid b^n, a^2, (ab)^2 \rangle$

III) Le groupe linéaire

1) $GL(E)$ et $SL(E)$

Pour $\mathbb{K}$ un corps commutatif, notons E un $\mathbb{K}$-espace vectoriel de dimension n.

Déf 20 Le groupe linéaire $GL(E)$ est le groupe des applications linéaires bijectives de E dans E.

Déf 21 : Le groupe spécial linéaire est
$$SL(E) := \{u \in GL(E) \mid \det u = 1\}.$$

Déf-Prop 22 : Soient H un hyperplan de E et $u \in GL(E)$ tel que $u_{|H} = id_{|H}$. Alors il y a équivalence entre :
1) $\det u \neq 1$
2) u admet une valeur propre différente de 1 et u est diagonalisable
3) $Im(u - id) \not\subset H$.

Si u vérifie une de ces propriétés alors on dit que u est une dilatation.

Déf-Prop 23 : Soient H un hyperplan de E et $f \in E^*$ tel que $H = Ker f$ et $u \in GL(E)$ tel que $u \neq id$ et $u_{|H} = id_{|H}$. Alors il y a équivalence entre
1) $\det u = 1$
2) u n'est pas diagonalisable
3) $Im(u - id) \subset H$
4) $\exists a \in H \setminus \{0\}, \forall x \in E \quad u(x) = x + f(x).a$
5) dans une certaine base, u a pour matrice $\begin{pmatrix} 1 & & (0) \\ & \ddots & 1 \\ (0) & & 1 \end{pmatrix}$

Si u vérifie une de ces propriétés alors on dit que u est une transvection.

Théorème 24 : $SL(E)$ est engendré par les transvections.

Théorème 25 : $GL(E)$ est engendré par les transvections et les dilatations [DVLPT]

Application 26 calcul des centres :
centre de $GL(E) = \mathbb{K}^*.I_n$,
centre de $SL(E) = \{\lambda I_n \mid \lambda^n = 1_{\mathbb{K}}\}$

Application 27 : groupes dérivés
$D(GL_2(\mathbb{F}_2)) = D(SL_2(\mathbb{F}_2)) \simeq A_3$,
$D(SL_2(\mathbb{F}_3)) \simeq H_8$ (groupe des quaternions),
pour les autres cas : $D(GL(E)) = D(SL(E)) = SL(E)$

2) Le groupe orthogonal

Ici $\mathbb{K} = \mathbb{R}$. Notons q une forme quadratique non dégénérée sur E.

Déf 28 : Le groupe orthogonal est
$$O(q) := \{u \in GL(E) \mid \forall x \in E.\ q(u(x)) = q(x)\}$$
et $O^+(q) := O(q) \cap SL(E)$

Déf 29 : Soit $u \in GL(E)$ tel que $u^2 = id$
Si $\dim(\ker(u+id)) = 1$ (resp 2) alors on dit que u est une réflexion (resp renversement)

Prop 30 : Soit $u \in GL(E)$ tel que $u^2 = id$ Alors
$$u \in O(q) \iff \ker(u-id) \perp \ker(u+id)$$

Théorème 31 : $O(q)$ est engendré par les réflexions orthogonales. Plus précisément si $u \in O(q)$ alors u est produit d'au plus n réflexions.

Théorème 32 : Tout élément de $O^+(q)$ est produit d'au plus n renversements.

Application 33 : $\forall n \geq 2$ $D(O(q)) = O^+(q)$
$\forall n \geq 3$: $D(O^+(q)) = O^+(q)$
Pour $n = 2$: $D(O^+(q)) = \{id\}$.

IV] Homographies et groupe modulaire

Pour E un espace vectoriel notons $P(E)$ l'espace projectif associé à E et $p : E \to P(E)$ la projection

1) Homographies

Déf 34 : Une homographie $g : P(E) \to P(E)$ est une application telle qu'il existe un isomorphisme linéaire $f : E \to E$ tel que $p \circ f = g \circ p$.

Prop 35 Les homographies forment un groupe noté $PGL(E)$ isomorphe à $GL(E)/\{\text{homothéties}\}$.

Cas de $PGL_2(\mathbb{C})$:
$$PGL_2(\mathbb{C}) = \{z \mapsto \frac{az+b}{cz+d} \mid ab - bc \neq 0\}.$$

Prop 36 : $PGL_2(\mathbb{C})$ est engendré par les similitudes directes ($z \mapsto az+b$ avec $a \neq 0$) et $z \mapsto 1/z$

2) Le groupe modulaire

Déf 37 : On appelle groupe modulaire le groupe
$$PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm id\}$$

Application 38 Action de $PSL_2(\mathbb{Z})$ sur le demi-plan de Poincaré $\{z \in \mathbb{C} \mid Im(z) > 0\}$ [DVLPT]

Réf : Cours d'algèbre, Perrin

Géométrie, Audin

Algèbre, Tauvel

Éléments de théorie des groupes Calais

Algèbre et géométrie, Combes.