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

Principales applications :
1) Reformation sur la structure du groupe
2) Etude des morphismes
3) Montrer qu'un groupe est simple
4) Montrer une propriété d'un groupe.

(I) Parties génératrices d'un groupe [P], [H]

Prop-Déf 1 : Soit G un groupe et X un ensemble de G. Il existe un plus petit sous-groupe de G contenant X, qu'on appelle le sous-groupe engendré par X et qu'on note $\langle X \rangle$.

Exemple 1 : $(\mathbb{Z}/n\mathbb{Z}, +)$ est engendré par $\{\bar{1}\}$.

Proposition 1 : $\langle X \rangle$ est l'ensemble des mots de longueur finie en les $x_i \in X$ et les x_i^{-1}.

$$\langle X \rangle = \{ x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} \ ; \ x_i \in X, \ \varepsilon_i \in \{\pm 1\}, \ n \in \mathbb{N} \}$$

Exemple 2 : $(\mathbb{R}, +)$ est engendré par $\{\frac{1}{p} ; p \text{ premier}\}$

Définition 2 : Un groupe G est dit de type fini s'il contient une partie génératrice finie. [FGN]

Exemple 3 : $SL(2,\mathbb{Z})$ est engendré par $\{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\}$.

Proposition 2 : Un groupe fini de cardinal n possède une partie génératrice de cardinal au plus $\log_2(n)$. Cette borne est optimale (ex : $(\mathbb{Z}/2\mathbb{Z})^n$).

(II) Groupes abéliens :

1) Groupes cycliques

Définition 3 : Un groupe G engendré par $\{a\}$ est dit monogène. On le note $G = \langle a \rangle$.

Proposition 3 : Un groupe monogène est isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$.
Dans le second cas, G est dit cyclique.

Proposition 4 : Soit $a \in \mathbb{Z}$. Les propriétés suivantes sont équivalentes : [P]
(i) $a \wedge n = 1$
(ii) $\bar{a}$ génère $(\mathbb{Z}/n\mathbb{Z}, +)$
(iii) $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$

On a donc $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$.

Application 1 : [P] Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.

Application 2 : [Ort] Le symbole de Legendre est l'unique morphisme non trivial de $(\mathbb{Z}/p\mathbb{Z})^*$ dans $\{\pm 1\}$.

Application 3 : Les sous-groupes de $(\mathbb{R}, +)$ sont denses, soit monogènes. [G]

Application 4 : [C, Ptu] Soit G et G' deux groupes cycliques d'ordre n et m. Il existe $d = n \wedge m$ morphismes de G dans G'.
Exemple avec $G = \mathbb{Z}/12\mathbb{Z}$ et $G' = \mathbb{Z}/6\mathbb{Z}$.

2) Groupes abéliens finis [C]

Théorème 1 : Soit G un groupe abélien d'ordre $n \geq 2$. Il existe une suite $q_1 | q_2 | \dots | q_k$ d'entiers ≥ 2 tels que $G \simeq \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_k\mathbb{Z}$. Cette suite caractérise G à isomorphisme près et est appelée la suite des invariants de G.

Application 5 : Structure des groupes abéliens d'ordre $600 = 2^3 \times 3 \times 5^2$.

Application 6: Soit $n \geq 1$, $k \geq 2$. $d = n \wedge k$ et $m = ppcm(n,k)$. $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Application 7: $\hat{G}$, l'ensemble des caractères d'un groupe abélien fini G (caractère = homomorphisme de G dans $\mathbb{C}^*$) est isomorphe à G.

III Groupes diédraux et groupes symétriques : [P]

1) Groupe symétrique :

Théorème 2: Le groupe symétrique $\mathfrak{S}_n$ est engendré par les transpositions.

Remarque 1: On peut se limiter aux transpositions $(1\,2), (1\,3), \dots, (1\,n)$ ou encore $(1\,2), (2\,3), \dots (n-1\,n)$.

Corollaire 1: Le groupe alterné est engendré par les 3-cycles.

Application 8: Le groupe alterné A_n est simple pour $n \geq 5$.

Application 9: Le groupe des isométries conservant le tétraèdre est isomorphe à $\mathfrak{S}_4$.

2) Les groupes diédraux :

Définition 4: Pour $n \geq 2$, D_n est l'ensemble des isométries du plan affine euclidien qui conservent un polygone régulier à n côtés.

Proposition 5: D_n est un groupe fini d'ordre $2n$. Il est engendré par la rotation d'angle $2\pi/n$ et une symétrie axiale d'axe un axe de symétrie du polygone.

Application 10: D_n n'est pas un produit direct.

IV Autour du groupe linéaire :

1) $GL(E)$ et $SL(E)$: [P]

On note E un K-espace vectoriel de dimension finie.

Définition 5: $GL(E)$ est l'ensemble des K-automorphismes de E. $SL(E) = \ker \det$ où $\det : GL(E) \to K^*$ est l'application déterminant.

Prop-Déf 6: Soit H un hyperplan de E et $u \in GL(E)$ tel que $u|_H = id_H$. LCSSE :

(i) $\det u = \lambda \neq 1$

(ii) u est diagonalisable et admet un vp $\lambda \neq 1$.

(iii) $\dim(u - id) \notin H$

(iv) Dans une base convenable, $u \sim \begin{pmatrix} 1 & (0) \\ (0) & \lambda \end{pmatrix}$ avec $\lambda \in K^* \setminus \{1\}$.

On dit que u est une dilatation d'hyperplan $H = \ker(u - id)$, de droite $D = \mathrm{Im}(u - id)$, de rapport λ.

Prop-Déf 7: Soit H un hyperplan de E, d'équation $f \in E^*$. Soit $u \in GL(E)$ tel que $u \neq id$, $u|_H = id_H$. LCSSE : (i) $\det u = 1$

(ii) u n'est pas diagonalisable

(iii) $D = \mathrm{Im}(u - id) \subset H$.

(iv) $\exists a \in H$, $a \neq 0$ tq $\forall x \in E$ $u(x) = x + f(x)a$

(v) Dans une base convenable, $u \sim \begin{pmatrix} 1 & (0) \\ (0) & 1 \end{pmatrix}$

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

Théorème 3 : • Les transvections engendrent $SL(E)$.
• Les transvections et les dilatations engendrent $GL(E)$.

Application 11 : $SL_n(\mathbb{R})$ et $GL_n(\mathbb{C})$ sont connexes par arcs. $GL_n(\mathbb{R})$ a deux composantes connexes par arcs. [FGN]

Application 12 : [P] . $\mathcal{D}(GL_n(K)) = SL_n(K)$, sauf pour $n=2$, $K=\mathbb{F}_2$.
. $\mathcal{D}(SL_n(K)) = SL_n(K)$, sauf pour $\begin{cases} n=2, K=\mathbb{F}_2 \\ n=2, K=\mathbb{F}_3 \end{cases}$.

Théorème de Frobenius-Zolotarev : Soit p un nombre premier impair et $K = \mathbb{F}_p$.
Alors, $\forall u \in GL(E)$ $\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$ [GA]
où $\left(\frac{\cdot}{p}\right)$ est le symbole de Legendre.

Application 13 : les matrices inversibles diagonalisables engendrent $GL_n(\mathbb{R})$ [FGN].

2) Groupe orthogonal euclidien :

Définition 8 : $O_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : {}^tAA = I_n\}$
$SO_n(\mathbb{R}) = O_n(\mathbb{R}) \cap SL_n(\mathbb{R})$

Théorème 4 : • $O_n(\mathbb{R})$ est engendré par les réflexions orthogonales.
• $SO_n(\mathbb{R})$ est engendré par les renversements.
Plus précisément, si $u \in O_n(\mathbb{R})$ est le produit d'au plus n réflexions. si $u \in SO_n(\mathbb{R})$ est le produit d'au plus n renversements.

Application 15 : $SO_3(\mathbb{R})$ est simple.

3) Groupe circulaire [A] - [CG]

Définition 9 : On pose sur $\mathbb{C}^2 \setminus \{(0,0)\}$ la relation d'équivalence : $x \mathcal{R} y \Leftrightarrow \exists \lambda \in \mathbb{C}^* : x = \lambda y$.
La droite projective complexe $P_1(\mathbb{C})$ est alors définie par $P_1(\mathbb{C}) = \mathbb{C}^2 \setminus \{(0,0)\} / \mathcal{R}$.

Prop-Définition 10 : L'action de $GL_2(\mathbb{C})$ sur $\mathbb{C}^2$ préserve les droites. Cela induit une action de $GL_2(\mathbb{C})$ sur $P_1(\mathbb{C})$. Deux matrices sont équivalentes si elles définissent la même action. Le quotient de $GL_2(\mathbb{C})$ par cette relation est noté $PGL_2(\mathbb{C})$.
$PGL_2(\mathbb{C})$ est appelé le groupe projectif linéaire complexe.
Ses éléments sont les homographies de $P_1(\mathbb{C})$.

Théorème 5 : L'action de $PGL_2(\mathbb{C})$ dans $P_1(\mathbb{C})$ est 3-simplement transitive : pour deux triplets (de points distincts) (a_1, a_2, a_3) et (b_1, b_2, b_3) de $P_1(\mathbb{C})^3$, il existe une unique homographie h telle que $h(a_1) = b_1$, $h(a_2) = b_2$, $h(a_3) = b_3$.

Définition 11 : Soit z_1, z_2, z_3, z_4 quatre points distincts de $P_1(\mathbb{C})$ et h telle que $h(z_1) = \infty$, $h(z_2) = 0$, $h(z_3) = 1$. Alors le birapport est défini par $[z_1, z_2, z_3, z_4] = h(z_4)$.

Proposition 6 : $[z_1, z_2, z_3, z_4] = \frac{z_3 - z_1}{z_3 - z_2} \times \frac{z_4 - z_2}{z_4 - z_1}$

Théorème 6 : Le groupe circulaire (engendré par les homographies et la conjugaison complexe) est exactement l'ensemble des applications conservant droites et cercles de $\mathbb{C}$.

[U] = Felix Ulmer, "Théorie des groupes"
[P] = Daniel Perrin, "Cours d'algèbre".
[FGN] = Francinou - Gianella - Nicolas,
"Exo de mathématiques, oraux x-ens
algèbre 2".
[C] = François Combes, "Algèbre et géométrie"
[G] = Gourdon, "Analyse".
[A] = Nicole Audin, "Géométrie"
[CG] = Caldero - Germoni, "Histoires
hédonistes de groupes et de géométries, Tome 1".