108

Exemples de parties génératrices d'un groupe. Applications

Déf : Soient $(G,\times)$ un groupe et A une partie de G ($\neq \emptyset$)
Le sous-groupe de G engendré par A est le plus petit sous-groupe contenant A, on le note $\langle A \rangle$

Pté : $\langle A \rangle = \bigcap_{\substack{H \leq G \\ A \subset H}} H$ (définition extérieure)

ou $\langle A \rangle = \{ x_1 \cdots x_n \mid n \in \mathbb{N}, x_i \in A$ ou $x_i^{-1} \in A, \forall i \leq n \}$ (définition intérieure)

En particulier, si $x \in G$, $\langle x \rangle = \{ x^n \mid n \in \mathbb{Z} \}$

Déf : Si $\langle A \rangle = G$, on dit que A est une partie génératrice du groupe G ou que A engendre G.
S'il existe $x_0 \in G$ tel que $\langle x_0 \rangle = G$, le groupe (A)
G est dit monogène si G est infini et cyclique si G fini

Ex : Un groupe d'ordre p premier est toujours cyclique.

I Exemples en théorie des groupes

1) Les groupes cycliques et monogènes

Th : Soit G un groupe tel qu'il existe $x \in G$ vérifiant $\langle x \rangle = G$. On définit le morphisme de groupes $\varphi \begin{pmatrix} \mathbb{Z} \to G \\ k \mapsto x^k \end{pmatrix}$. Alors :

- si $G \simeq \mathbb{Z}$, alors G est monogène
- s'il existe $n \in \mathbb{N}^*$ tel que $G \simeq \mathbb{Z}/n\mathbb{Z}$, alors G est cyclique d'ordre n.

Rq : À isomorphisme près, il y a un seul groupe monogène ($\mathbb{Z}$) et un seul groupe cyclique d'ordre n ($\mathbb{Z}/n\mathbb{Z}$)
Les pptés des groupes monogènes découle de celles de $\mathbb{Z}$ (resp des groupes cycliques de celle de $\mathbb{Z}/n\mathbb{Z}$).

(x) et x_0 est dit générateur de G

Propo : Tout sous-groupe d'un groupe monogène est monogène.

Propo : Soit G un groupe cyclique d'ordre n tq $G = \langle x \rangle$
Alors pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d qui est $\langle x^{\frac{n}{d}} \rangle$ donc cyclique
Réciproquement, ces sous-groupes sont les seuls sous-groupes de G.

Propo : Soit G un groupe monogène tel que $G = \langle x \rangle$
Les seuls générateurs de G sont x et x^{-1}.

Propo : Soit G un groupe cyclique d'ordre n tq $\langle x \rangle = G$
Les seuls générateurs de G sont les x^k où k est un entier premier avec n.

Appli : L'ensemble des racines n-ièmes de l'unité (complexes) forment un groupe noté $\mathbb{U}_n$.
$\mathbb{U}_n$ est engendré par le générateur $e^{\frac{2\pi i}{n}}$ et donc aussi engendré par $e^{\frac{2\pi i k}{n}}$ où $k \wedge n = 1$.
Ces racines n-ièmes sont primitives et forment l'ensemble μ_n.

Déf : On définit $\varphi \begin{pmatrix} \mathbb{Z} \to \mathbb{N} \\ n \mapsto \varphi(n) \end{pmatrix}$ la fonction indicatrice d'Euler par $\varphi(n) = | \{ k \in [\![1, n-1]\!] \mid k \wedge n = 1 \} |$
$\varphi(n)$ désigne donc le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$ et donc le nombre de générateurs de tout groupe cyclique d'ordre n.

Pté : Si $n = \prod p_i^{\alpha_i}$, $\varphi(n) = \prod p_i^{\alpha_i - 1}(p_i - 1)$

Ex : $|\mu_{20}| = 8$

Pptés : Les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ pour la loi $\times$ et ils forment un groupe pour la loi $\times$ qu'on note $(\mathbb{Z}/n\mathbb{Z}^*, \times)$.

Propo : Un produit direct de groupes cycliques est cyclique si les ordres sont premiers entre eux.

Th de structure des groupes abéliens finis :
Soit G un groupe abélien fini.
Alors il existe une unique liste $(d_1, \dots, d_n)$ telle que $d_i \geq 2$, $d_i \mid d_{i+1}$ $\forall i \leq n-1$ et vérifiant
$G \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/d_n\mathbb{Z})$
$(d_1, \dots, d_n)$ est appelé la suite des invariants de G.

2) Le groupe symétrique

Def : Soit $n \in \mathbb{N}$. On appelle $(S_n, \circ)$ le groupe des bijections de $[\![1,n]\!]$.

Prop : Tout élément de S_n est produit de cycles disjoints de manière unique.

Prop : • Les transpositions engendrent S_n
• $\{(i\ i{+}1) \mid i \in [\![1,n-1]\!]\}$ est une partie génératrice de S_n
- $\{(1\ i) \mid i \leq n\}$ est une partie génératrice de S_n
- $\{(1\ 2), (1\ 2 \dots n)\}$ est une partie génératrice de S_n

Appli : Le calcul de la signature d'un élément est facilité sachant que $\varepsilon((i_1 \dots i_p)) = (-1)^{p-1}$
En particulier, la parité de toute décomposition en transposition de $\sigma \in S_n$ est conservée.

Prop : Soit A_n le groupe alterné ($A_n = \mathrm{Ker}(\varepsilon)$) alors les 3-cycles engendrent A_n.

Appli : A_n est un groupe simple si $n \geq 5$

3) Le groupe diédral

Def : Soit $n \in \mathbb{N}$. Le groupe diédral d'ordre n noté D_n est le groupe formé par les isométries du plan qui préservent le polygone régulier à n côtés centré en O.

Prop : Le groupe diédral D_n est formé :
- des n rotations d'angle $\frac{2\pi k}{n}$, $k \in [\![1,n]\!]$ et de centre O qu'on note r_k (et $r_1 = r$)
- si $n \equiv 1\ [2]$, des n symétries orthogonales de droites (OA_k) où A_k désigne les sommets du polygone
- si $n \equiv 0\ [2]$, des n symétries orthogonales de droites (OB_k) où B_k milieu d'un côté du polygone

Ainsi, $\forall n \in \mathbb{N}$, D_n est fini d'ordre $2n$.

Prop : Soit r la rotation d'angle $\frac{2\pi}{n}$ et de centre O et soit s une symétrie de D_n.
Alors $\langle r, s \rangle = D_n$

Rq : En fait $\{r_k, s\}$ où $k \wedge n$ est une partie génératrice de D_n

Prop : $D_n = \langle r \rangle \rtimes \langle s \rangle \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

DEV 1 — Table des caractères des D_n
La donnée $\langle r, s \rangle = D_n$ permet de dresser les tables de caractères de D_n.

Ex : La table de D_4 est donnée en annexe

II Exemples en algèbre linéaire et géométrie

1) Le groupe linéaire et spécial linéaire

Per

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n ($\mathbb{K}$ corps qq.)

Def : On note $(GL(E), \circ)$ le groupe des endomorphismes bijectifs de E.
On appelle groupe spécial linéaire noté $SL(E)$ le sous-groupe de $GL(E)$ $\{f \in GL(E) \mid \det(f) = 1\}$

Def : Soit H un hyperplan de E et $f \in GL(E)$ telle que $f_{|H} = Id$. Soit $D = \mathrm{Im}(f - Id)$
• f est une dilatation d'hyperplan H, de droite D de rapport λ si l'une des conditions suivantes équivalentes est vérifiée avec $H = \mathrm{Ker}(f - Id)$

- $\det(f) \neq 1$
- f admet 1 comme vp et est diagonalisable
- $\exists B$ tel que $\mathrm{Mat}_B(f) = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix}$

• f est une transvection d'hyperplan H et de droite D si l'une des conditions équivalentes est vérifiée : (avec $H = \mathrm{Ker}(f)$)

- $\det(f) = 1$
- f n'est pas diagonalisable
- $\exists B$ tq $\mathrm{Mat}_B(f) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & \\ & & 1 \end{pmatrix}$

<u>Prop</u> : • Les transvections engendrent $SL(E)$
• Les dilatations et les transvections engendrent $GL(E)$. — K(*)

<u>Appli</u> : $Z(GL(E))$ est l'ensemble des homothéties de E.

2) Le groupe orthogonal

Soit E euclidien muni du produit scalaire $<\cdot|\cdot>$

<u>Def</u> : On appelle groupe orthogonal de E noté $O(E)$ l'ensemble des applications f vérifiant $\forall (x,y) \in E,\ <f(x)|f(y)> = <x|y>$.

On appelle groupe spécial orthogonal de E le sous-groupe de $O(E)$ des éléments de déterminant 1.

<u>Lemme</u> : Soit $f \in O(E)$ et F un sev de E.
Si F est f-stable, alors $F^\perp$ est f-stable.

<u>Def</u> : On appelle réflexion toute symétrie orthogonale par rapport à un hyperplan.
On appelle retournement toute symétrie orthogonale par rapport à F où $\dim(F) = n-2$ (donc dans E de dim ≥ 2)

REV 2 — Générateurs de $O(E)$ et $SO(E)$

Tout élément de $O(E)$ est produit d'au plus n réflexions.
Tout élément de $SO(E)$ est produit de retournements si $n \geq 3$.

<u>Appli</u> : Soit $G(E)$ l'ensemble des isométries affines de $\mathbb{R}^n$ muni de sa structure d'espace affine euclidien.
Tout élément de $G(E)$ est produit d'au plus $n+1$ réflexions affines.

<u>Appli</u> : Classification des isométries affines et vectorielles du plan. Soit $f \in G(E)$, $\vec{f} \in G(E)$

f produit de 0 SM $\to \vec{f} = Id$	f produit de 1 SM $\to \vec{f}$ symétrie orthogonale	f produit de 2 SM $\to \vec{f}$ rotation
$\to f$ est une translation	Si f a un pt fixe $\to f$ réflexion affine	$\to f$ est une rotation affine.
	Si f sans pt fixe $\to f$ réflexion glissée	

3) Le groupe des homographies et circulaire

<u>Def</u> : On note $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$
Le groupe des homographies noté $\mathbb{P}GL_2(\mathbb{C})$ est l'ensemble des applications $z \mapsto \frac{az+b}{cz+d}$ avec $ad - bc \neq 0$, $(a,b,c,d) \in \mathbb{C}^4$

<u>Prop</u> : Les similitudes directes et l'application $z \mapsto \frac{1}{z}$ forment une partie génératrice de $\mathbb{P}GL_2(\mathbb{C})$

(*) L'écrire en termes de matrices !!!
Application à la convexité.

1) Pratique pour étudier G
Par ex., cyclique si $e_G = |G|$

2) Car $(ij)(ik) = 3$-cycle

Références : CALAIS (Groupe)
COMBES
PERRIN
AUDIN