

[Rom]
[Ber]

108: Exemples de parties génératrices d'un groupe Applications

I- Parties génératrices d'un groupe

1) Généralités [Rom] 11-12

- def sous groupe engendré $\langle X \rangle$
- def groupe de type fini + ex
- def groupe dérivée

2) Groupes monogènes et cyclique [Rom] 13 [Ber] 155

- def monogène et cyclique + ex

↳ morphisme surjectif $\pi: \mathbb{Z} \rightarrow G$
 $k \mapsto a^k$

→ Th G monogène infini $\simeq \mathbb{Z}$

G monogène cyclique $\simeq \mathbb{Z}/n\mathbb{Z}$

- Th groupe d'ordre premier est cyclique
- Th ss groupe d'un groupe monogène est monogène

3) Groupes abéliens de type fini [Ber] 358-361

- Th structure des groupes abélien finis

II- Applications

1) Le groupe symétrique [Ber] 199 215

- Rappel S_n + th décompositions en cycles à supp disjoints
- générateurs de S_n

DEV 1

- Applications groupe des isométries du cube et tétraèdre + dessins

DEV 1

- def signature et A_n

- A_n simple

DEV 2

- cas A_4

- def $\text{Aut}(G)$ $\text{Aut}(S_n) = \text{Inn}(S_n)$

2) Algèbre linéaire [Rom] 139-141

- $GL_n(K)$
- def matrices de translation et dilatation.
- $GL_n(K)$ engendré par les translation et dilatation
- $SL_n(K)$ — dilatation

3) le groupe des quaternions [Per] 160-164

- def $\mathbb{H}$
- def quaternions de norme 1 : G
- Th $G_{\{1, \pm 1\}} \cong SO_3(\mathbb{R})$

DEV3

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

Soit $(G, \cdot)$ un groupe

I- Parties génératrices d'un groupe

1) Généralités

Lemme 1: L'intersection (quelconque) de sous-groupes de G est un sous groupe de G

Définition 2: Soit $X \subseteq G$, le sous groupe engendré par X est l'intersection de tous les sous-groupes de G qui contiennent X . On le note $\langle X \rangle$.

Lorsque $X = \{x_1, \dots, x_n\}$, $\langle X \rangle = \langle x_1, \dots, x_n \rangle$

Définition 3: Soit $X \subseteq G$. On dit que X engendre G si $G = \langle X \rangle$. On dit que G est de type fini s'il admet une partie génératrice finie

Exemple 4: On pose $D(G) = \langle [a, b] = aba^{-1}b^{-1} : (a, b) \in G^2 \rangle$

On l'appelle groupe dérivé de G

2) Groupes monogènes et cycliques

Définition 5: On dit que G est monogène s'il existe un élément $g \in G$ tel que $G = \langle g \rangle$. Si de plus G est fini, on dit alors qu'il est cyclique.

Exemple 6: $(\mathbb{Z}, +)$ est monogène engendré par 1.

Ses sous groupes sont de la forme $n\mathbb{Z}$ avec $n \geq 0$ sont monogènes

$\cdot$ $\mathbb{Z}_n$ est cyclique d'ordre n et isomorphe à $\mathbb{Z}/n\mathbb{Z}$ par l'application $\bar{k} \mapsto e^{\frac{2ik\pi}{n}}$

Théorème 7: Soit G un groupe monogène. s'il est infini, il est isomorphe à $(\mathbb{Z}, +)$, si est cyclique d'ordre n , il est alors isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$

Théorème 8: Un groupe de cardinal premier est cyclique

Corollaire 9: Si $G = \langle g \rangle$ est un groupe cyclique d'ordre n , ses générateurs sont les g^k où $1 \leq k \leq n-1$ premier avec n

Proposition 10: Tout sous-groupe d'un groupe monogène est monogène

Théorème 11: Soit G un groupe cyclique d'ordre n . Pour tout diviseur positif d de n , il existe un unique sous groupe H_d d'ordre d , cyclique.

Si x_0 est un générateur de G , $H_d = \langle x_0^{\frac{n}{d}} \rangle$.

3) Groupes abéliens de type fini

Théorème 12: Soit G un groupe abélien fini.

Alors il existe des entiers $d_1, \dots, d_s \geq 2$ vérifiant $d_1 | d_2 | \dots | d_s$ tels que $G \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$

De plus, la suite d'entiers $(d_1, \dots, d_s)$ est unique et ne dépend que de la classe d'isomorphisme de G .

Définition 13: Les entiers $d_1, \dots, d_r$ sont dits facteurs invariants de G précédant sont appelés facteurs invariants de G .

Corollaire 14: Deux groupes abéliens finis sont isomorphes si, et seulement si, ils ont les mêmes facteurs invariants.

Exemple 15: $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/3\mathbb{Z}$

II- Applications

1) Le groupe symétrique

Définition 16: Le groupe symétrique S_n est l'ensemble des bijections de $[1, n]$ dans $[1, n]$.

Définition/Proposition 17: Soit $\sigma \in S_n$. Le groupe $\langle \sigma \rangle$ agit sur $[1, n]$ par restriction de l'action de S_n . Les orbites de cette action sont appelées orbites.

Définition 18: $\sigma \in S_n$ est un cycle s'il n'existe qu'une seule σ -orbite non réduite à un singleton.

Un 2-cycle est appelé transposition.

Théorème 19: Toute permutation de S_n se décompose en produit de cycles à supports disjoints et cette décomposition est unique à l'ordre près des facteurs.

Corollaire 20: S_n est engendré par les transpositions.

Corollaire 21: S_n est engendré par:

- les transpositions $(1, i)$, $i \in [2, n]$
- les transpositions $(i, i+1)$, $i \in [1, n-1]$
- (12) et $(12 \dots n)$

Application 22: Soit E l'espace euclidien de dimension 3. En notant $\mathcal{V}$ le cube régulier et $I_3(\mathcal{V})$ le groupe des isométries du cube. On a

$$I_3^+(\mathcal{V}) \cong S_4 \text{ et } I_3(\mathcal{V}) \cong S_4 \times \mathbb{Z}/2\mathbb{Z} \quad \boxed{\text{DEV 1}}$$

Définition/Proposition 23: Il existe un unique morphisme $\varepsilon: S_n \rightarrow \{\pm 1\}$ qui associe les transpositions sur -1 .

Définition 24: Le groupe alterné, noté A_n est l'ensemble des permutations de S_n de signature 1.

Proposition 25: Pour $n \geq 3$, les 3-cycles engendrent A_n .

Théorème 26: Pour $n = 3$ et $n \geq 5$ A_n est simple. $\boxed{\text{DEV 2}}$

2) Le groupe des quaternions

Proposition Définition 27: Il existe une algèbre H de dimension 4 sur $\mathbb{R}$, appelée algèbre des quaternions, munie d'une base $1, i, j, k$ telle que:

1) 1 est le neutre pour la multiplication

2) on a: $i^2 = j^2 = k^2 = -1$, $jk = -kj = i$, $ki = -ik = j$, $ij = -ji = k$

Un quaternion s'écrit alors: $q = a + bi + cj + dk$, $a, b, c, d \in \mathbb{R}$

Définition 28: Le groupe G des quaternions de norme 1 est le groupe $\{\pm 1, \pm i, \pm j, \pm k\}$ pour $N(q) = a^2 + b^2 + c^2 + d^2$

Théorème 29: $G_{\{\pm 1\}} \simeq SO_3(\mathbb{R})$ DEV 3

3) Le groupe linéaire

[Rom] Soit $\mathbb{K}$ un corps et $n \geq 2$

139 Définition 30: L'ensemble $M_n(\mathbb{K})$ désigne l'algèbre des matrices carrées d'ordre n . $GL_n(\mathbb{K})$ le groupe des matrices inversibles de $M_n(\mathbb{K})$, appelé groupe linéaire d'ordre n .

141 Définition 31: $SL_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) \mid \det(A) = 1\}$
le groupe spécial linéaire

Définition 32: Soit $\lambda \in \mathbb{K}^*$, $(i, j) \in \llbracket 1, n \rrbracket^2$ tel que $i \neq j$,

. On définit:

• matrice de transvection $T_{ij}(\lambda) = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \lambda & \\ & & & \ddots \\ & & & & 1 \end{pmatrix} \in GL_n(\mathbb{K})$

• matrice de dilatation $D(\lambda) = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \lambda & \\ & & & \ddots \end{pmatrix}$

Théorème 33: $SL_n(\mathbb{K})$ est engendré par les transvections
 $GL_n(\mathbb{K})$ est engendré par les transvections et dilatations

Notion utile pour
montrer des prop
sur des groupes

L> ex: HCH' ?

si on a une partie génératrice
de $H \cap P$, il suffit de
mq PCH'

L> mq H distingué

L> surjectivité d'un morphisme

L> simplicité

ex A_n simple
DEV 1

lien avec la
géométrie

isométries des cubes
DEV 2

→ utile pour réduire
l'étude des groupes
à ses générateurs

→ analogue aux
bases dans un EV

108: Exemples de parties
génératrices d'un groupe
Applications

Généralités

Ce que ça signifie

monogène

$\mathbb{Z}$

cyclique

$\mathbb{Z}/n\mathbb{Z}$

info sur leur ss groupe

nombreuses applications

groupe important
 S_n

plusieurs parties
génératrices

Algèbre linéaire

$GL_n(\mathbb{K})$

↳ translations et dilations

groupe quaternion

$G/\{\pm 1\} \cong SO_3(\mathbb{R})$

DEV 3