

Exemples de parties génératrices d'un groupe. Applications.

Mohamed NASSIRI

Intro

Références

- [GOUal] Les maths en tête : Algèbre, Xavier Gourdon
[ML3al] Mathématiques L3 Algèbre, Aviva Szpirglas
[TAU] Algèbre pour l'agrégation interne, Patrice Tauvel
[MER] Cours de géométrie, Dany-Jack Mercier
[WAR] Mathématiques tout-en-un MPSI-PCSI, Claude Deschamps et André Warusfel
[CAL] Éléments de théorie des groupes, Josette Calais
[COL] Éléments d'analyse et d'algèbre (et de théorie des nombres), Pierre Colmez
[DEL] Théorie des groupes 2e édition, Jean Delcourt

Développements

Générateurs de S_n
 $SO_3(\mathbb{R})$ et les quaternions

1 Groupes monogènes, Groupes abéliens de type fini

1.1 Groupes monogènes, groupes cycliques [ML3ag] p.233-234

Définition 1 Un groupe G est dit monogène s'il est engendré par un seul élément (i.e.) s'il existe $g \in G$ tel que

$$G = \{g^n ; n \in \mathbb{Z}\}$$

Si G est de cardinal fini, il est dit cyclique.

Proposition 2 Si le groupe G est monogène, alors il est abélien.

Proposition 3 Un groupe monogène de cardinal infini est isomorphe à \mathbb{Z} .

Les groupes cycliques sont les $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{Z}^*$.

Théorème 4 Soit $k \in \mathbb{Z}$. k est premier avec $n \Leftrightarrow \bar{k}$ est générateur du groupe $\mathbb{Z}/n\mathbb{Z}$. [PER] p.24

Définition 5 Soit $E(n) = \{k \in \mathbb{N} \mid 1 \leq k \leq n-1 \text{ et } (k, n) = 1\}$. On appelle fonction indicatrice d'Euler l'application $\varphi : \mathbb{N}^* \mapsto \mathbb{N}^*$ telle que :

$$\varphi(1) = 1, \text{ et } \varphi(n) = \text{card}(E(n)), \forall n > 1.$$

[CAL] p.104

Proposition 6 Le nombre de générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$ est $\varphi(n)$. [CAL] p.104

Exemple 7 $\varphi(p) = p-1$, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, $\alpha \in \mathbb{N}^*$. [PER] p.24

1.2 Groupes abéliens de type fini

Définition 8 Un groupe G est dit de type fini s'il existe un nombre fini d'éléments g_1, \dots, g_n de G tels que $G = \langle g_1, \dots, g_n \rangle$.

Un tel n -uplet (g_1, \dots, g_n) est appelé système de générateurs de G . [GOUal] p.19

Théorème 9 (admis) Soit G est un groupe abélien de type fini. Alors il existe un unique entier $n \in \mathbb{N}$, un unique ensemble de nombres premiers (p_1, \dots, p_k) , et pour tout $1 \leq i \leq k$ une unique suite d'entiers $n_{i,1} \geq \dots \geq n_{i,r_i} \geq 1$ telle que

$$G \cong \mathbb{Z}^n \times \prod_{i=1}^k (\mathbb{Z}/p_i^{n_{i,1}}\mathbb{Z}) \times \dots \times (\mathbb{Z}/p_i^{n_{i,r_i}}\mathbb{Z})$$

p.255

Corollaire 10 (admis) Théorème de structure des groupes abéliens finis

Si G est un groupe abélien fini, il existe un entier $r \in \mathbb{N}$, et des entiers N_1, \dots, N_r , où N_1 est l'exposant de G et $N_{i+1} \mid N_i$ si $i \leq r-1$, tels que

$$G \cong \bigoplus_{i=1}^r \mathbb{Z}/N_i\mathbb{Z}$$

[COL] p.251-252

Exemple 11 Soit G le groupe

$$G = \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$$

Alors

$$G \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$$

[DEL] p.111-112

2 Groupe des permutations

2.1 Groupes symétriques p.45→47

Définition 12 Soit E un ensemble. Une bijection de E sur lui-même est appelée permutation de E . On note l'ensemble des permutations de E $\mathcal{S}(E)$. Lorsque $E = [1, \dots, n]$, on note $\mathcal{S}_n = \mathcal{S}(E)$. Une permutation σ sera notée :

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

Remarque 13 On se place dans le cadre \mathcal{S}_n .

Proposition 14 Muni de la composition des applications, \mathcal{S}_n est un groupe, appelé groupe symétrique, et on a $|\mathcal{S}_n| = n!$.

Proposition 15 Théorème de Cayley : Tout groupe fini G de cardinal n est isomorphe à un sous-groupe de \mathcal{S}_n .

Proposition 16 Principe de conjugaison : Si $\sigma = (a_1 \dots a_p) \in \mathcal{S}_n$ est un cycle d'ordre p et $\tau \in \mathcal{S}_n$, on a

$$\tau \sigma \tau^{-1} = (\tau(a_1) \dots \tau(a_p))$$

[PER] p.15

Théorème 17 ♠ Générateurs de \mathcal{S}_n ♠

Soit $n \geq 2$.

- (i) Les transpositions engendrent \mathcal{S}_n .
- (ii) L'ensemble $\{(1 \ i), 2 \leq i \leq n\}$ engendrent \mathcal{S}_n .
- (iii) Le nombre minimal de transpositions engendrant \mathcal{S}_n est $n-1$.

Corollaire 18 (i) L'ensemble $\{(i \ i+1), 1 \leq i \leq n-1\}$ engendrent \mathcal{S}_n .

(ii) La transposition $(1 \ 2)$ et le n -cycle $(1 \ 2 \dots n)$ engendrent \mathcal{S}_n .

2.2 Le groupe alterné [GOUal] p.21

Définition 19 Soit $\sigma \in \mathcal{S}_n$. On appelle signature de σ le produit

$$\epsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Proposition 20 Soient $\sigma, \tau \in \mathcal{S}_n$. Alors

- (i) $\epsilon(\sigma) \in \{-1, 1\}$,
- (ii) $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$.
- (iii) ϵ est l'unique morphisme de groupe non trivial de \mathcal{S}_n dans \mathbb{R}^* .

Définition 21 On définit le groupe alterné $\mathcal{A}_n = \text{Kere}$.

Proposition 22 Pour $n \geq 3$,

- (i) $Z(\mathcal{S}_n) = \{Id\}$, et \mathcal{S}_n n'est pas abélien.
 - (ii) \mathcal{A}_n est engendré par les permutations $(1 \ i)(1 \ j)$, où $2 \leq i, j \leq n$.
 - (ii) \mathcal{A}_n est engendré par les 3-cycles de la forme $(1 \ 2 \ i)$, où $3 \leq i \leq n$.
- \mathcal{A}_n est engendré par les éléments σ^2 , $\sigma \in \mathcal{S}_n$.

[TAU] p.49

Théorème 23 \mathcal{A}_n est simple pour $n \geq 5$

3 Le groupe diédral [MER] p.304 → 311

Définition 24 On appelle groupe diédral D_n le groupe des isométries du plan qui conservent un polygone régulier P_n à n côtés.

Théorème 25 Le groupe diédral D_n est un groupe fini d'ordre $2n$ engendré par un élément r d'ordre n et un élément s d'ordre 2.

Il contient n rotations d'angle $\frac{k\pi}{n}$, $k = 0, \dots, n-1$ ainsi que n symétries. En notant r la rotation d'angle $\frac{2\pi}{n}$ et s une des symétries, on a

$$r^n = 1 \quad s^2 = 1 \quad (sr)^2 = 1$$

Exemple 26 Le groupe du triangle équilatéral est isomorphe au groupe \mathfrak{S}_3 des permutations d'un ensemble de trois éléments. On peut donc écrire

$$D_3 \approx \mathfrak{S}_3$$

Remarque 27 On peut identifier les isométries de $\text{Is}(P_n)$ à leurs parties linéaires et aux matrices de ces parties linéaires dans une base orthonormale directe. On a donc

$$\text{Is}^+(P_n) = \left\{ \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix} ; k = 0, \dots, n-1 \right\}$$

$$\text{Is}^-(P_n) = \left\{ \begin{pmatrix} \cos k\theta & \sin k\theta \\ \sin k\theta & -\cos k\theta \end{pmatrix} ; k = 0, \dots, n-1 \right\}$$

4 Groupe des quaternions de norme 1 [PER] p.160 → 164

Proposition-définition 28 Il existe une algèbre \mathbb{H} de dimension 4 sur \mathbb{R} , appelé algèbre des quaternions, muni d'une base $1, i, j, k$ telle que :

- (i) 1 est élément neutre pour la multiplication,
- (ii) on a les formules

$$jk = -kj = i, \quad ki = -ik = j, \quad ij = -ji = k$$

$$i^2 = j^2 = k^2 = -1$$

Un quaternion s'écrit alors

$$q = a + bi + cj + dk, \quad \text{avec } a, b, c, d \in \mathbb{R}$$

Définition 29 \mathbb{H} est muni de la norme algébrique N suivante : $\forall q = a + bi + cj + dk \in \mathbb{H}$

$$N(q) = a^2 + b^2 + c^2 + d^2$$

Proposition 30 Le groupe G des quaternions de norme 1 est le groupe

$$\{\pm 1, \pm i, \pm j, \pm k\}$$

Ce groupe est d'ordre 8 et non abélien.

Théorème 31 ♠ $SO_3(\mathbb{R})$ et les quaternions ♠
Soit G le groupe des quaternions de norme 1. On a l'isomorphisme suivant :

$$G/\{-1, 1\} \xrightarrow{\sim} SO_3(\mathbb{R})$$

5 Groupe linéaire et groupe spécial linéaire

Définition 32 On appelle groupe linéaire l'ensemble des K -automorphismes de E et on le note $GL(E)$. Cet ensemble a une structure de groupe pour la composition des endomorphismes. [ML3al] p.294

Définition 33 Pour $n \in \mathbb{N}^*$, on définit $GL_n(K)$ comme le groupe des automorphismes de K^n .

Lorsque E est de dimension $n \in \mathbb{N}^*$, on a un isomorphisme entre $GL(E)$ et $GL_n(K)$ en fixant une base de E . [ML3al] p.294

Définition 34 Le noyau de l'application \det est appelé groupe spécial linéaire et est noté $SL_n(K)$ (i.e.)

$$SL_n(K) = \{u \in GL_n(K) \mid \det(u) = 1\}$$

[ML3al] p.296

Définition 35 On appelle matrice de transvection toute matrice de la forme $T_{ij}(\lambda) = I_n + \lambda E_{i,j}$ avec $i \neq j$ et $\lambda \in \mathbb{K}$.

On appelle matrice de dilatation toute matrice diagonale $D_i(\lambda) = I_n + (\lambda - 1)E_{i,i}$ avec $\lambda \in \mathbb{K}^*$ [FGN-XXX] p.XXX

Remarque 36 On a un lien entre ces matrices et les opérations dites élémentaires.

Voir Tableau 1

Théorème 37 L'ensemble des matrices de transvection engendre le groupe $SL_n(\mathbb{K})$ et l'ensemble des matrices de transvection et de dilatation engendre le groupe $GL_n(\mathbb{K})$. [FGNXXX] p.XXX

Questions

Exercice :

Solution :

Exercice :

Solution :

Exercice :

Solution :