108

Exemples de parties génératrices d'un groupe. Applications.

Soit $(G,\cdot)$ un groupe

0 - Introduction

[Rb] 10 **Lemme 1** : Une intersection (quelconque) de sous-groupes de G reste un sous-groupe de G.

[Rb] 11 **Def 2** : Soit $X \subseteq G$. On appelle *sous-groupe engendré par X*, et on note $\langle X \rangle$, le plus petit sous-groupe de G contenant X. C'est l'intersection des sous-groupes de G contenant X.
Lorsque $X = \{x_1, \dots, x_n\}$, on note plus simplement $\langle X \rangle = \langle x_1, \dots, x_n \rangle$.

[Rb] 11 **Prop 3** : Soit $X \subseteq G$, posons $X^{-1} = \{x^{-1} : x \in X\}$. Alors :
$$\langle X \rangle = \{x_1 \cdots x_n : n \in \mathbb{N}^*, (x_1, \dots, x_n) \in (X \cup X^{-1})^n\}$$

[Rb] 11 **Def 4** : Une *partie génératrice* de G est un sous-ensemble $X \subseteq G$ tel que $G = \langle X \rangle$.

[Rb] 12 **Ex 5** : On pose $D(G) := \langle \{[a,b] = aba^{-1}b^{-1} : (a,b) \in G^2\} \rangle$. On l'appelle *groupe dérivé* de G, c'est le plus grand sous-groupe de G tel que $G/D(G)$ est abélien.

I - Groupes monogènes, groupes cycliques

[Rb] 13 **Def 6** :
- On dit que G est *monogène* s'il existe $g \in G$ tel que $G = \langle g \rangle$.
- On dit que G est *cyclique* si G est monogène et fini.

[Rb] 14 **Thm 7** :
- Si G est monogène infini, alors $G \simeq \mathbb{Z}$.
- Si G est cyclique, alors il existe $n \in \mathbb{N}^*$ tel que $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Prop 8 :
- L'ensemble des générateurs de $\mathbb{Z}$ est $\mathbb{Z}^\times = \{\pm 1\}$.
- L'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$ est $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{k} \in \mathbb{Z}/n\mathbb{Z} \mid \exists \bar{\ell} \in \mathbb{Z}/n\mathbb{Z} : \bar{k}\bar{\ell} = \bar{1}\} = \{\bar{k} \in \mathbb{Z}/n\mathbb{Z} \mid k \wedge n = 1\}$.

[Rb] 14 **Cor 9** : Si $G = \langle g \rangle$, alors l'ensemble des générateurs de G est $\{g^k : k \wedge \#G = 1\}$.

Def/Prop 10 : L'ordre d'un élément $g \in G$ est le plus petit entier k (ou $+\infty$) tel que $g^k = 1$. C'est aussi l'ordre de $\langle g \rangle$.

Prop 11 : G est cyclique si et seulement si G admet un élément d'ordre $\#G$.

Cor 12 : Tout groupe d'ordre premier est cyclique, tous ses éléments sauf 1_G en sont les générateurs. [Rb] 14

Thm 13 : Pour tous $p \geq 3$ et $\alpha \geq 1$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique. **DEV 1** [Rb] 292

Thm 14 [admis] : $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si, et seulement si $n \in \{2, 4, p^\alpha, 2p^\alpha : p \geq 3 \text{ premier}, \alpha \geq 1\}$. [Rb] 294

II - Groupes symétriques

Soit $n \geq 3$.

Def 15 : Le n^e *groupe symétrique* $\mathfrak{S}_n$ est l'ensemble des bijections de $[\![1,n]\!]$ dans $[\![1,n]\!]$ (les permutations de $[\![1,n]\!]$). [U] 43

Def/Prop 16 : Soit $\sigma \in \mathfrak{S}_n$. Le sous-groupe $\langle \sigma \rangle$ agit sur $[\![1,n]\!]$ par restriction de l'action de $\mathfrak{S}_n$. Les orbites de cette action sont appelées σ-orbites.

Def 17 : [U] 43
- Un k-cycle ($2 \leq k \leq n$) est une permutation σ n'ayant qu'une seule σ-orbite non ponctuelle $\{i_1, \dots, i_k\}$. On la note $\sigma = (i_1, \dots, i_k)$ pour signifier que $\forall j \notin \{i_1, \dots, i_k\}, \sigma(j) = j$, et $\sigma(i_j) = i_{j+1}$ en regardant les indices modulo k.
- Un 2-cycle est appelé transposition.

Thm 18 : Toute permutation se décompose de manière unique (à l'ordre des facteurs près) comme produit de cycles à supports disjoints. [U] 43

Prop 19 : $(i_1, \dots, i_k) = (i_1, i_2)(i_2, i_3) \cdots (i_{k-1}, i_k)$ [Rb] 44

Cor 20 : Les transpositions engendrent $\mathfrak{S}_n$. [Rb] 44

[Rb] 44-45 **Prop 21** : $\mathfrak{S}_n = \langle (i,i+1),\ 1\leq i<n\rangle = \langle (1,i),\ 2\leq i\leq n\rangle = \langle (1,2),(1,2,\dots,n)\rangle$

[Rb] 47 **Def/Prop 22** : Il existe un unique morphisme $\varepsilon : \mathfrak{S}_n \longrightarrow \{\pm 1\}$ qui envoie les transpositions sur -1. On appelle *signature* de σ la quantité $\varepsilon(\sigma)$.

[Rb] 49 **Def 23** : On appelle n^e *groupe alterné* le sous-groupe $A_n = \mathrm{Ker}(\varepsilon)$. C'est l'ensemble des permutations dites *paires*.

[Rb] 49 **Thm 24** : Pour $n\geq 3$, les 3-cycles engendrent A_n, et y sont conjugués.

[R] 50 **Thm 25** : Pour $n\geq 5$, A_n est simple.

III - Groupes linéaires, groupes orthogonaux

Soient K un corps et $n\geq 2$.

A - Groupes linéaires et pivot de Gauss

[Rb] 139 **Def 26** : L'ensemble $\mathcal{M}_n(K)$ des matrices carrées de taille $n\times n$ est un anneau pour $+$ et $\times$, dont le groupe des inversibles est noté $GL_n(K)$, appelé *groupe linéaire d'ordre n sur K*.

[Rb] 141 **Def 27** : On note $SL_n(K)$ le noyau du morphisme $\det$ de $GL_n(K)$ dans $K^\times$. On l'appelle *groupe spécial linéaire d'ordre n sur K*.

Soit $A\in\mathcal{M}_n(K)$. On note $L_1,\dots,L_p$ les lignes de A, et $C_1,\dots,C_n$ ses colonnes.

[B] 315-318 **Def 28** : Soient $\alpha\in K^\times$, $(i,j)\in[\![1,n]\!]^2$ tel que $i\neq j$ et $\sigma\in\mathfrak{S}_n$.

- On définit une *matrice de dilatation* $D_i(\alpha) = \begin{array}{c} i \\ \begin{pmatrix} 1 & & \\ & \ddots & \\ & & \alpha & \\ & & & \ddots \\ & & & & 1\end{pmatrix} i \end{array} \in GL_n(K)$.
- On définit une *matrice de transvection* $T_{i,j}(\alpha) = I_n + \alpha E_{i,j} \in GL_n(K)$.
- On définit une *matrice de permutation* $P_\sigma = (\delta_{i,\sigma(j)})_{1\leq i,j\leq n} \in GL_n(K)$.

[B] 315-318 **Def 29** : On définit les opérations élémentaires sur les colonnes :

- $C_i \longleftarrow \alpha C_i$: on remplace C_i par αC_i
- $C_i \longleftarrow C_i + \alpha C_j$: on remplace C_i par $C_i+\alpha C_j$
- $C_i \longleftrightarrow C_j$: on échange C_i et C_j

[B] 315-318 **Thm 30** : On a les correspondances suivantes entre opérations élémentaires et multiplication matricielle :

- $D_i(\alpha)A \iff L_i \longleftarrow \alpha L_i$ • $A D_i(\alpha) \iff C_i \longleftarrow \alpha C_i$
- $T_{i,j}(\alpha)A \iff L_i \longleftarrow L_i + \alpha L_j$ • $A T_{i,j}(\alpha) \iff C_j \longleftarrow C_j + \alpha C_i$
- $P_{(i,j)}A \iff L_i \leftrightarrow L_j$ • $A P_{(i,j)} \iff C_i \leftrightarrow C_j$

Thm 31 (pivot de Gauss) : Pour toute matrice de rang r, il existe une suite d'opérations élémentaires qui transforme cette matrice en la matrice $J_{n,r} = \mathrm{Diag}(I_r, O_{n-r})$.
Plus précisément, si $\mathrm{rg}(A)=n$, alors il existe $\sigma\in\mathfrak{S}_n$ et des matrices de transvection $T_1,\dots,T_p$ telles que $A = P_\sigma T_1\cdots T_p D_\alpha$ où D_α est la matrice de dilatation D_α de rapport $\alpha = \det(A)$.

Cor 32 : • Les matrices de transvection et de dilatation engendrent $GL_n(K)$. [Rb] 151-153
• Les matrices de transvection engendrent $SL_n(K)$.

B - Groupe orthogonal d'un espace quadratique

Soit (E,q) un espace quadratique sur K, de forme polaire φ. Supposons $\mathrm{car}(K)\neq 2$.

[P] 123-124 **Def 33** : • Le *groupe orthogonal* de (E,q) est $O(q) = \{u\in\mathcal{L}(E) \mid q\circ u = q\}$

- Le *groupe spécial orthogonal* de (E,q) est $SO(q) = \{u\in O(q) \mid \det(u)=1\}$
- Lorsque q est le produit scalaire canonique relativement à une base donnée, on note $O(E) = O(q) = \{u\in\mathcal{L}(E) \mid {}^t u\circ u = id_E\}$ et $SO(E) = SO(q) = \{u\in O(E) \mid \det(u)=1\}$.
- On note également $O_n(K) = \{M\in\mathcal{M}_n(K) \mid {}^t MM = I_n\}$ et $SO_n(K) = \{M\in O_n(K) \mid \det(M)=1\}$

[Rb] 1723 Prop 34 : Si $\mathcal{B}$ est une base orthonormale de E, alors $u \in O(E) \iff \mathrm{Mat}_{\mathcal{B}}(u) \in O_n(\mathbb{K})$

[Rb] 746 Thm 35 (de réduction des isométries) : Soit $u \in O(\mathbb{R}^n)$. Il existe une base orthonormale $\mathcal{B}$ de $\mathbb{R}^n$ telle que $\mathrm{Mat}_{\mathcal{B}}(u) = \mathrm{Diag}(R(\theta_1), \dots, R(\theta_r), \varepsilon_1, \dots, \varepsilon_p)$ où $R(\theta_i) = \begin{pmatrix} \cos(\theta_i) & -\sin(\theta_i) \\ \sin(\theta_i) & \cos(\theta_i) \end{pmatrix}$ et $\varepsilon_i = \pm 1$.

[P] 125 Def 36 : Soit $u \in O(q)$ telle que $u^2 = id_E$.

- On dit que u est une réflexion si $\dim(\mathrm{Ker}(u + id_E)) = 1$, autrement dit si u est une symétrie par rapport à un hyperplan.
- On dit que u est un renversement si $\dim(\mathrm{Ker}(u + id_E)) = 2$, autrement dit si u est une symétrie par rapport à un plan.

On suppose désormais que E est un $\mathbb{R}$-espace vectoriel de dimension finie $n \geq 1$, et que q est définie positive.

DEV2

[P] 143 Thm 37 : Tout élément de $O(q)$ est produit d'au plus n réflexions.

[P] 143 Lemme 38 : Si $n \geq 3$, alors pour toutes réflexions τ_1 et τ_2, il existe deux renversements σ_1 et σ_2 tels que $\tau_1 \tau_2 = \sigma_1 \sigma_2$.

[P] 143 Thm 39 : Pour $n \geq 3$, tout élément de $SO(q)$ est produit d'au plus n renversements.

Références

[Rb] Rombaldi

[U] Ulmer, Théorie des groupes

[P] Perrin

[B] Burg