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

1 Généralités

On désignera dans cette partie par $(G,.)$ un groupe.

1.1 Partie génératrice d'un sous-groupe

Proposition 1 (ROM 10/ BER 141)**.** L'intersection d'une famille non vide de sous-groupe de G est un sous-groupe de G.

Définition 2 (ROM 11, BER 141)**.** Si X est une partie de $(G,.)$, le sous groupe de G engendré par X est l'intersection de tous les sous-groupes de G qui contiennent X. On le note $< X >$.

Proposition 3 (ROM 11, BER 141)**.** $< X >$ est le plus petit sous-groupe de G, au sens de l'inclusion, contenant X.

Notation 4 (ROM 11)**.** Si $X = x_1, ..., x_n$ on sera amené à noter $< x_1, ..., x_n >$ à la place de $< X >$.

Proposition 5 (ROM 11)**.** Soit X une partie de G. Notons $X^{-1} = \{x^{-1} | x \in X\}$. Les éléments de $< X >$ sont de la forme $x_1...x_r$ où $r \in \mathbb{N}^*$ et $x_k \in X \cup X^{-1}$ pour tout $1 \leq k \leq r$.

Exemple 6 (No ref)**.** Le sous-groupe des éléments pairs de $(\mathbb{Z}, +)$ est engendré par 2. En effet tous ces éléments s'écrivent sous la forme $2k$ avec $k \in \mathbb{Z}$.

1.2 Partie génératrice d'un groupe

Définition 7 (ROM 11, BER 142)**.** Si X est une partie de $(G,.)$, on dit que X engendre G si $G =< X >$.

Définition 8 (ROM 13)**.** On dit que G est monogène si il existe un élément g de G tel que $G =< g >$.
Si G est monogène et fini, on dit lors qu'il est cyclique.

Proposition 9 (ROM 13)**.** Un groupe monogène $(G,.)$ est commutatif et on a : $< g >= \{\prod_{k=1}^{r} g^{\varepsilon_k} | r \in \mathbb{N}^*, \varepsilon_k = \pm 1 \text{ pour } 1 \leq k \leq r\} = \{g^n | n \in \mathbb{Z}\}$
Si (G,+) est un groupe additif on a $< g >= \{ng | n \in \mathbb{Z}\}$.

Exemple 10 (ROM 13)**.** Le groupe additif $(\mathbb{Z}, +)$ est monogène engendré par 1. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique et est engendré par $\bar{1}$.

1.3 Notion d'ordre

Définition 11 (Ber 130)**.** Si G est un groupe fini, son nombre d'éléments $|G|$ est appelé l'ordre de G.

Théorème 12 (ROM 14, BER 156)**.** Soit G un groupe monogène.
Si il est infini, G est isomoprhe à $(\mathbb{Z}, +)$.
Si il est cyclique d'ordre n, il est alors isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Proposition 13 (ROM 14)**.** Si $G =< g >$ est un groupe cyclique d'ordre n, alors ses générateurs sont les g^k, où $1 \leq k \leq n-1$ est premier avec n.

Exemple 14 (No ref, ROM 14)**.**
1. Les générateur de $\mathbb{Z}/n\mathbb{Z}$ sont les $k \in \mathbb{Z}$ qui sont premiers avec n.
2. Soit $n \in \mathbb{N}^*$. L'ensemble des racines complexes n-ième de l'unité $\mathbb{U}_n$ est cyclique engendré par $e^{\frac{2i\pi}{n}}$. Il est donc d'ordre n et ainsi on a $\mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$.

Définition 15 (ROM 6, BER 149)**.** L'ordre d'un élément $g \in G$ est $o(g) = card(< g >)$.
Si $o(g) \in \mathbb{N}$, on dit que g est d'ordre fini, et sinon on dit qu'il est d'ordre infini.

Proposition 16 (ROM 7)**.** Soit $g \in G$ et $n \in \mathbb{N}^*$.LASSE :
1. g est d'ordre n
2. $g^n = 1$ et $g^k \neq 1$ pour tout $k \in [\![1, n-1]\!]$
3. Pour tout $k \in \mathbb{Z}$, $g^k = 1 \iff n|k$

Proposition 17 (ROM 17)**.** G cyclique si et seulement si, pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d de G.

Avoir en tête contre exemple A_4 pas de ssgp ordre 6

Corollaire 18 (ROM p14)**.** Un groupe de cardinal premier est cyclique.

Application 19 (un peu ROM p 292)**.** $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si n est premier.

2 Exemple du groupe symétrique

2.1 Introduction

Définition 20 (BER 201)**.** Le groupe symétrique $\mathfrak{S}(E)$ est l'ensemble des bijections (appelées permutations) de $1, ...n$ dans lui même.

Définition 21 (BER 200, 202)**.** Le support d'une permutation σ est l'ensemble $Supp(\sigma) = \{a \in E | \sigma(a) \neq a\}$.
Pour $x \in E$ et σ, on définit la σ-orbite de x l'ensemble $\mathcal{O}_\sigma(x) = \{\sigma^k(x) | k \in \mathbb{Z}\}$.

Définition 22 (BER 202)**.** Une permutation σ est un cycle s'il n'existe qu'une seule σ-orbite non réduite à un singleton.
Si $p \geq 2$ est le nombre d'éléments de $Supp(\sigma)$, on dit que σ est un p-cycle. Un 2-cycle est appelée une transposition.

Notation 23. Dans la suite, Ω^* représentera l'ensemble des σ-orbites non réduites à un seul élément.

Proposition 24 (BER 200 1) 4) + BER 201)**.** Soient $\sigma, \rho \in \mathfrak{S}(E)$.

1. $\sigma(Supp(\sigma)) = Supp(\sigma)$
2. $Supp(\sigma\rho) \subset Supp(\sigma) \cup Supp(\rho)$
3. Si $Supp(\sigma) \cap Supp(\rho) = \emptyset$ alors σ et ρ commutent.

Proposition 25 (ROM 38)**.** Soit σ, $p \geq 2$ et soit $(a_1, ..., a_p)$ un p-cycle. On a : $\sigma(a_1, ..., a_p)\sigma^{-1} = (\sigma(a_1), ..., \sigma(a_p))$.

Proposition 26. Soit $p \geq 2$. Un p-cycle est d'ordre p.

2.2 Générateurs

Lemme 27 (BER 202, ROM 41)**.** Soit ω une σ-orbite à p éléments et soit $a \in \omega$. Alors, p est le plus petit entier positif tel que $\sigma^p(a) = a$ et on a $w = \{a, \sigma(a), ..., \sigma^{p-1}(a)\}$.

Lemme 28 (BER 203)**.** Soit $\omega \in \Omega^*$. On définit $\sigma_\omega \in \mathfrak{S}(E)$ par $\sigma_\omega(a) = \sigma(a)$ si $a \in \omega$ et $\sigma_\omega(a) = a$ si $a \notin \omega$. Alors σ_ω est un cycle de support ω, et pour tout $a \in \omega$, on a $\sigma_\omega = (a \quad \sigma(a) \ ... \ \sigma^{p-1}(a))$, où p est le nombre d'éléments dans ω.
De plus, tout p-cycle est de cette forme.

Théorème 29 (BER 204, ROM42 DEV 1)**.** Soit $\sigma \in \mathfrak{S}(E)$. Alors σ se décompose en produit de cycles à support disjoints, et cette décomposition est unique à l'ordre des facteurs près. Cette décomposition est donnée par : $\sigma = \prod_{\omega \in \Omega^*} \sigma_\omega$ où Ω^* représente l'ensemble des σ-orbites non réduite à un singleton.

Corollaire 30 (BER 206, DEV 1)**.** $\mathfrak{S}(E)$ est engendré par

1. les cycles.
2. les transpositions.

Corollaire 31 (BER 207)**.** $\mathfrak{S}_n$ est engendré par

1. les transpositions $(k \ k+1)$ pour $1 \leq k \leq n-1$
2. les transpositions $(1 \ k+1)$ pour $1 \leq k \leq n-1$
3. (12) et (1 2 ... n)

Exemple 32. (12345678)(43265871) a pour décomposition en cycle (1468)(23) et pour décomposition en transposition (14)(46)(68)(23)

2.3 Groupe alterné

Définition 33 (No ref, appuyé sur BER 214, ROM 47)**.** On définit la signature de σ par l'élément $\epsilon(\sigma) = (-1)^r$, où r est le nombre de transposition dans la décomposistion en transposition de σ.

Proposition 34 (No ref, appuyé sur BER 214, ROM 47)**.** La signature est un morphisme.

Définition 35 (BER 215)**.** Le groupe alterné, noté $\mathfrak{A}_n$, est l'ensemble des permutations de $\mathfrak{S}_n$ de signature 1.

Proposition 36 (BER 215)**.** $\mathfrak{A}_n$ est un sous groupe distingué de $\mathfrak{S}_n$ de cardinal $\frac{n!}{2}$.

Exemple 37 (BER 214)**.** La signature d'un p-cycle σ est $(-1)^{p-1}$.

Proposition 38 (BER 216)**.** Si $n \geq 3$, le groupe alterné $\mathfrak{A}_n$ est engendré par chacune des familles suivantes :

1. les produits de deux transpositions
2. les 3-cycles.

Théorème 39 (BER 217)**.** [DVP bonus] Soit $n \geq 3$. Le groupe alterné $\mathfrak{A}_n$ est simple si et seulement si $n \neq 4$.

3 Groupe linéaire

Dans cette partie, E désignera un $\mathbb{K}$-espace vectoriel de dimension finie n.

3.1 Introduction

Définition 40 (BER 39)**.** L'ensemble des automorphismes de E est un groupe pour la composition des applications, noté $GL(E)$ et appelé groupe linéaire.

Proposition 41 (ROM 139)**.** Pour une base B de E choisie, l'application qui à un automorphisme de E associe sa matrice représentative dans la base B est un isomorphisme de $GL(E)$ dans $\mathcal{M}_n(\mathbb{K})$

Proposition 42 (PER 96)**.** Le déterminant est un morphisme de $Gl(E)$ dans $\mathbb{K}^*$.

Définition 43 (un peu BER 69)**.** On définit $SL(E)$ comme le noyau du déterminant. C'est donc un sous groupe de $GL(E)$ que l'on appelle le groupe spécial linéaire.

3.2 Générateurs

On désignera par H un hyperplan de E et f une forme linéaire de noyau H.

Définition 44 (TL2 336)**.** Une transvection d'hyperplan H est un endomorphisme de E de la forme $x \mapsto x + f(x)u$ où $u \in H$.

Une dilatation d'hyperplan H est un automorphisme de E de la fomre $x \mapsto x + f(x)u$ où $u \notin H$.

Définition 45 (TL1 228)**.** Une matrice de transvection est une matrice de la forme

$$T_{i,j}(\lambda) = I_n + \lambda E_{i,j} = \begin{pmatrix} 1 & & & & \\ & . & & \lambda & \\ & & . & & \\ & & & . & \\ & & & & 1 \end{pmatrix} \text{ avec } \lambda \in \mathbb{K}^*$$

Une matrice de dilatation est une matrice de la forme

$$D_i(\lambda) = I_n + (\lambda - 1)E_{i,i} = \begin{pmatrix} 1 & & & & \\ & ... & & & \\ & & \lambda & & \\ & & & ... & \\ & & & & 1 \end{pmatrix} \text{ avec } \lambda \in \mathbb{K}^*$$

Proposition 46 (ROM 336)**.** Soit $\varphi \in \mathcal{L}(E)$.

1. Si il existe une base $\mathcal{B}$ de E telle que $Mat_{\mathcal{B}}(\varphi)$ est une matrice de transvection, alors φ est une transvection.
2. Réciproquement si φ est une transvection autre que l'identité, il existe une base $\mathcal{B}$ de E telle que $Mat_{\mathcal{B}}(\varphi) = T_{n-1,1}(1)$.
3. Si il existe une base $\mathcal{B}$ de E telle que $Mat_{\mathcal{B}}(\varphi)$ est une matrice de dilatation $D_i(\lambda) \neq I_n$, alors φ est une dilatation de rapport λ.
4. Réciproquement si φ est une dilatation de rapport $\lambda \in \mathbb{K} \setminus \{0, 1\}$, il existe une base $\mathcal{B}$ de E telle que $Mat_{\mathcal{B}}(\varphi) = D_n(\lambda)$.

Proposition 47 (TL1 229)**.** Tableau correspondance opérations matrices/ opérations sur lignes/ colonnes

Lemme 48 (TL2)**.** 337 Pour toutes matrices de $GL(E)$ on peut alors se ramener à un produit de tranvections et d'une matrice de la forme $diag(1, ..., 1, \lambda)$ avec $\lambda \in k^*$.

Théorème 49 (ROM153)**.** SL(E) est engendré par l'ensemble des transvection et GL(E) est engendré par l'ensemble des dilatations et transvections.

Application 50 (CAL p80)**.** $SL_n(\mathbb{K})$ est connexe par arc pour $\mathbb{K} = \mathbb{C}$.

3.3 Sous groupe orthogonal

Dans cette partie, on considèrera $(E, < ., . >)$ un espace euclidien réel, toujours de dimension finie n.

Définition 51 (ROMp720)**.** Une isométrie de E est une application $u : E \to E$ qui conserve le produit scalaire, c'est-à-dire telle que $< u(x), u(y) >=< x, y >$ pour tous x, y dans E.

Définition 52. On appelle groupe orthogonal, et on note $O(E)$, l'ensemble des isométrie de E.

Proposition 53 (ROMp720)**.** $u \in \mathcal{L}(E)$ est une isométrie si et seulement si elle est linéaire et conserve la norme.

Proposition 54 (ROMp162,721)**.** Une isométrie est un automorphisme de E et $O(E)$ est un sous-groupe compact de $GL(E)$.

Définition 55 (par coeur par trop ref, un peu PER p125 et un peu ROM p730)**.** Soit $u \in GL(E)$ tel que $u^2 = id$.
On dit que u est une réflexion si $dim(ker(u - id)) = n - 1$, c'est à dire si c'est une symétrie par rapport à un hyperplan.

Théorème 56 (DEV2)**.** [Oraux XENS] Le groupe O(E) est engendré par les réflexions. Plus précisément, si u est dans O(E), u est produit d'au plus $r = rg(u - id)$réflexions.

A avoir en tête : On peut définir pgcd grace partie génératrices (BER 143)

Proposition 57 (Ber 156)**.** Deux groupes cycliques sont isomorphes si ils ont même ordre.