Leçon 108 Exemples de parties génératrices d'un groupe, applications

Dorian Cacitti-Holland

2020-2021

Références.

1. Algèbre et géométrie de Jean-Etienne Rombaldi
2. Eléments d'analyse et d'algèbre de Pierre Colmez
3. Théorie des groupes de Félix Ulmer
4. Cours d'algèbre de Daniel Perrin
5. Analyse matricielle de Jean-Etienne Rombaldi
6. Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni

Développements.

1. Simplicté du groupe alterné A_n
2. Générateurs de $SL(E)$ et $GL(E)$
3. Simplicité de $SO_3(\mathbb{R})$

Table des matières

1. Définition : Soit G un groupe et $S \subset G$, alors on dit que S engendre G si tout élément de G s'écrit comme produit fini d'éléments de S et d'inverse d'éléments de S, on le note $G = \langle S \rangle$, et si $S = \{x_1, ..., x_r\}$ alors on le note $G = \langle x_1, ..., x_r \rangle$

1 Cas des groupes abéliens

1.1 Les groupes monogènes et cycliques

(Chapitres 1.4 et 1.5 d'Algèbre et géométrie de Jean-Etienne Rombaldi et 0.3.1 de Eléments d'analyse et d'algèbre de Pierre Colmez)

On considère G un groupe.

1. Définition : On dit que G est monogène s'il existe $g \in G$ tel que $G = \langle g \rangle$, si de plus G est fini alors on dit que G est cyclique
2. Exemple : $\mathbb{Z} = \langle 1 \rangle$ n'est pas cyclique
3. Exemple : Le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité est cyclique
4. Proposition : Si G est cyclique alors G est abélien
5. Théorème : Si $G = \langle g \rangle$ est cyclique d'ordre n alors ses générateurs sont les g^k avec $k \in [\![1, n-1]\!]$ premier avec n
6. Corollaire : Le nombre de générateurs de G est égal à $\varphi(n)$
7. Exemple : Si n premier alors le nombre de générateurs de Γ_n est $n-1$
8. Théorème : Un groupe de cardinal premier est cyclique, et un groupe de cardinal pq avec p, q premiers entre eux est cyclique
9. Remarque : Si p, q ne sont pas premiers entre eux alors G n'est pas nécessairement cyclique
10. Exemple : $|S_3| = 6 = 3 \times 2$ n'est pas cyclique, $(\mathbb{Z}/\mathbb{Z})^2$ n'est pas cyclique
11. Théorème : Si $G = \langle g \rangle$ cyclique alors les sous-groupes de G sont cycliques d'ordre divisant n et pour tout diviseur d de n il existe un unique sous-groupe de G d'ordre d, il s'agit de $\langle a^{\frac{n}{d}} \rangle$
12. Exemple : Si n pair alors $\mathbb{U}_{\frac{n}{2}}$ est un sous-groupe cyclique de $\mathbb{U}_n$ et est engendré par $e^{\frac{4i\pi}{n}}$

1.2 Groupes abéliens finis

(Chapitres 1.5 et 1.9 d'Algèbre et géométrie de Jean-Etienne Rombaldi et 0.3.2 et I.2.5 de Eléments d'analyse et d'algèbre de Pierre Colmez)

On considère un groupe abélien fini G.

1. Théorème de Cauchy : Soit p diviseur premier de n, alors il existe $g \in G$ d'ordre p
2. Remarque : Si G non cyclique et d diviseur quelconque de n alors il n'existe pas nécessairement d'élément d'ordre d dans G
3. Exemple : Dans $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ il n'existe pas d'élément d'ordre 4

4. Définition : L'exposant de G est l'entier $N(G) = PPCM(o(g), g \in G)$
5. Exemple : Si $G = \mathbb{Z}/9\mathbb{Z}$ alors $N(G) = 3$
6. Définition : Un caractère de G est un morphisme de groupe de G dans $\mathbb{C}^*$, et on note $\hat{G}$ l'ensemble des caractères sur G
7. Exemple : Le morphisme $g \in G \longmapsto 1 \in \mathbb{C}^*$ est la caractère trivial
8. Proposition : Soit H sous-groupe de G et χ caractère de H, alors χ peut se prolonger en un caractère sur G
9. Lemme : $\hat{G}$ est un groupe et G et $\hat{\hat{G}}$ sont isomorphes
10. Proposition : G et $\hat{G}$ ont le même exposant
11. Théorème : Il existe $g \in G$ d'ordre $N(G)$
12. Théorème de structure des groupes abéliens finis : $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times ...\mathbb{Z}/d_r\mathbb{Z}$ avec $d_{i+1} \mid d_i$
13. Application : Dans ce cas, si on détermine $\chi_1 \in \hat{G}$ d'ordre $N(G)$ et $x_1 \in G$ tel que $\chi_1(x_1) = e^{\frac{2i\pi}{N}}$, alors on recommence ce procédé avec $ker(\chi_1)$, pour obtenir à la fin $x_1, ..., x_r$ engendrant G

2 Groupe symétrique

2.1 Générateurs

(Chapitres 2.1, 2.3, 2.4, 2.5 et 2.7 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Définition : Un k-cycle est une permutation circulaire ie de la forme $\sigma(i_1 i_2 ... i_k)$, si $k = 2$ alors on parle de transposition
2. Proposition : Les transpositions engendrent les k-cycles
3. Théorème : Toute permutation peut s'écrire comme produit de cycles à supports disjoints, de plus cette décomposition est unique à l'ordre près des facteurs
4. Remarque : Soit $\sigma \in S_n$ et $\sigma = \tau_1 ... \tau_r$ une telle décomposition, alors $Supp(\sigma) = \bigsqcup_{1 \leq i \leq r} Supp(\tau_i)$ et $o(\sigma) = PPCM(o(\tau_i), 1 \leq i \leq r)$
5. Corollaire : Les transpositions engendrent S_n, cette décomposition n'est pas unique mais la parité du nombre de transpositions ne varie pas
6. Exemple : $(1256)(234)(46) = (1234)(56) = (14)(13)(12)(56) \in S_6$ a pour pour ordre $ppcm(4, 2) = 4$
7. Proposition : S_n est engendré par les $n-1$ transpositions $(1k)$ pour $k \in [\![2, n]\!]$
8. Exemple : $(ij) = (1i)(1j)(1i)$
9. Proposition : S_n est engendré par $n-1$ transposition $(k, k+1)$ pour $k \in [\![1, n-1]\!]$
10. Exemple : $(1k) = (k-1, k)(1, k-1)(k-1, k) = (k-1, k)(k-2, k-1)(1, k-2)(k-2, k-1)(k-1, k)$
11. Proposition : S_n est engendré par (12) et $(1, 2, ..., n)$
12. Exemple : $(k, k+1) = (1, 2, ..., n)^{k-1}(12)((1, 2, ..., , n)^{k-1})^{-1}$

2.2 Sous-groupe alterné

(Chapitres 2.6 et 2.7 d'Algèbre et géométrie de Jean-Etienne Rombaldi, 5.3 de Théorie des groupes de Félix Ulmer et 1.8 du Cours d'algèbre de Daniel Perrin)

1. Théorème : ε est l'unique morphisme non trivial de S_n dans $\{-1, 1\}$
2. Définition : A_n est le noyau de ε, ie le sous-groupe des permutations parires (de signature 1)
3. Proposition : $A_n \triangleleft S_n$ et $|A_n| = \frac{n!}{2}$
4. Théorème : Les 3-cycles engendrent A_n
5. Exemple : $(12)(34) = (123)(234)$
6. Lemme : Si $n \geq 5$, soit $N \triangleleft A_n$ tel que N contienne un 3-cycle, alors $N = A$
7. Théorème : Si $n \geq 5$ alors A_n est simple, ie il n'admet de sous-groupes distingués non triviaux
8. Corollaire : Si $n \geq 5$, $D(A_n) = A_n$ et $D(S_n) = A_n$
9. Exemple : A_4 admet pour sous-groupes distingués $\{id\}, V_4, A_4$ avec V_4 le groupe des doubles transpositions de S_4
10. Corollaire : Si $n \geq 5$ alors les sous-groupe distingués de S_n sont $\{id\}, A_n, S_n$
11. Corollaire : $H < S_n$ d'indice n est isomorphe à S_{n-1}

3 Groupes d'isométries préservant une partie

3.1 Groupes diédraux

(Chapitres III.3 de Eléments de théorie des groupes et 3.4.3 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Définition : On dit que G est de type D_{2n} s'il est dicyclique engendré par un élément r d'ordre n et un élément s d'ordre 2 tel que $rsrs = 1$
2. Théorème : Si G de type D_{2n} alors $G = \{id, r, ..., r^{n-1}\} \cup \{s, sr, ..., sr^{n-1}\}$
3. Corollaire : Les groupes de type D_{2n} sont isomorphes
4. Exemple : Dans le plan la rotation d'angle $\frac{2\pi}{n}$ et la réflexion d'axe $\mathbb{R}e_1$ engendrent un groupe $\langle r, s\rangle$ de type D_{2n}
5. Définition : On note Γ_n l'ensemble des sommets d'un polygone régulier à n côtés et $Is(\Gamma_n)$ le groupe des isométries conservant Γ_n
6. Théorème : Avec les notations de l'exemple précédent, on a $Isom(\Gamma_n) = \langle r, s\rangle$, donc $Isom(\Gamma_n)$ est un groupe de type D_{2n}
7. Exemple : S_3 est isomorphe au groupe du triangle équilatéral, donc S_3 est de type D_6

3.2 Groupes d'isométries du tétraèdre et du cube

(Chapitre 3.4.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi et Exercice 3.6.6 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Définition : On considère T est le tétraèdre régulier et C le cube de $\mathbb{R}^3$, et $Isom(T)$ et $Isom(C)$ les groupes d'isométries les conservant
2. Théorème : Comme les transposition engendrent S_4, $Isom(T) \simeq S_4$
3. Corollaire : $Isom^+(T) \simeq A_4$
4. Théorème : $Isom(C) = Isom(S)$ avec S l'ensemble des sommets du cube, de même $Isom^+(C) = Isom^+(S)$
5. Remarque : En vectorialisant $\mathbb{R}^3$ en fixant l'origine en l'isobarycentre du cube, on se ramène au cas vectoriel
6. Remarque : Une application affine qui conserve le cube est une isométrie
7. Théorème : Comme les transpositions engendrent S_4, $Isom^+(S) \simeq S_4$
8. Corollaire : $Isom(S) \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}$
9. Application : On obtient la table de caractères de S_4 en annexe

4 Groupe linéaire et sous-groupes

4.1 Générateurs de $GL(E)$ et de $SL(E)$

(Chapitres IV.2 et IV.3 du Cours d'algèbre de Daniel Perrin et 5.4 et 5.5 d'Analyse matricielle de Jean-Etienne Rombaldi)

1. Lemme : Soit $x, y \in E\backslash\{0\}$ alors il existe $u \in GL(E)$ une transvection ou un produit de deux transvections telle que $u(x) = y$
2. Théorème : $SL(E)$ est engendré par les transvections
3. Corollaire : $GL(E)$ est engendré par les transvections et les dilatations
4. Remarque : Matriciellement pour tout $A \in GL_n(K)$ il existe des matrices de transvections $P_1, ..., P_r, Q_1, ..., Q_s$ telles que $A = P_1...P_r D(det(A))Q_1...Q_r$
5. Application : La méthode du pivot de Gauss est similaire à la démonstration du résultat précédent
6. Définition : Soit $u, v \in GL(E)$, alors $[u, v] = uvu^{-1}v^{-1}$ est appelé commutateur de $GL(E)$
7. Exemple : Si $u = id_E$ alors $[u, v] = id_E$
8. Définition : On note $D(GL(E))$ le sous-espace de $GL(E)$ engendré par les commutateurs, et $D(SL(E))$ celui engendré par les commutateurs d'éléments de $SL(E)$
9. Théorème : $D(GL(E)) = SL(E)$ et $D(SL(E)) = SL(E)$ (sauf dans si $n = 2$ et $K = \mathbb{F}_2$ ou $K = \mathbb{F}_3$)
10. Remarque : Quant au centre on a $Z(GL(E))$ est formé des homothéties non nulles et $Z(SL(E))$ des homothéties de rapport λ racine n-ième de l'unité

4.2 Groupe orthogonal

(Chapitres 22.3 et 22.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi, II.3 et II.4 de Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni et VI.2 du Cours d'algèbre de Daniel Perrin)

On considère E un espace euclidien.

1. Définition : Soit $u \in End(E)$, alors on dit que u est orthogonal si $\langle u(x), u(y)\rangle = \langle x, y\rangle$, et on note $O(E)$ leur ensemble, de plus on note $SO(E) = O(E) \cap det^{-1}(\{1\})$
2. Proposition : $O(E)$ est un sous-groupe compact de $GL(E)$ et pour $u \in O(E)$, $u^{-1} = u^*$
3. Proposition : $Z(O(E)) = \{id_E, -id_E\}$, en particulier $O(E)$ n'est pas abélien, de plus $Z(SO(E)) = \{id_E\}$ si n impair et $Z(SO(E)) = \{id_E, -id_E\}$ si n pair
4. Définition : Soit $u \in O(E)$ diagonalisable $diag(-I_p, I_{n-p}$, si $p = 1$ alors on dit que u est une réflexion orthogonale, si $p = 2$ alors on dit que u est un renversement et si $p = n - 1$ alors on dit que u est un retournement
5. Théorème : $O(E)$ est engendré par les réflexions orthogonales, plus précisément pour $u \in O(E)$, alors u est produit d'au plus $n = dim(E)$ réflexions
6. Lemme : Soit τ_1, τ_2 deux réflexions de E, alors il existe σ_1, σ_2 deux renversements tels que $\tau_1\tau_2 = \sigma_1\sigma_2$
7. Théorème : $SO(E)$ est engendré par les renversements, plus précisément pour $u \in SO(E)$, alors u est produit d'au plus $n = dim(E)$ renversements
8. Proposition : $SO(E)$ est connexe
9. Corollaire : Les composantes connexes de $O(E)$ sont $SO(E)$ et $O^-(E) := O(E) \cap det^{-1}(\{-1\})$
10. Lemme : Soit $N \triangleleft SO_3(\mathbb{R})$ tel que N contienne un renversement, alors $N = SO_3(\mathbb{R})$
11. Application : $SO_3(\mathbb{R})$ est un groupe simple