P. Maurer
ENS Rennes

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

Devs :

- Décomposition de Bruhat. Application aux générateurs de $\mathrm{GL}_n(\mathbb{K})$.
- Le groupe $\mathrm{SO}_3(\mathbb{R})$ est simple.

Références :

1. Ulmer, Théorie des groupes
2. Perrin, Cours d'algèbre
3. Gourdon, Algèbre
4. Dos Santos, Groupes finis et leurs représentations (Poly M1 Jussieu)

Dans tout le plan, G désigne un groupe.

1 Parties génératrices, générateurs, relations.

1.1 Partie génératrice d'un groupe

Définition 1. *Soit A une partie de G. Il existe un plus petit sous-groupe de G contenant A. On le note $\langle A\rangle$ et on l'appelle sous-groupe de G engendré par A.*

Remarque 2. L'existence de $\langle A\rangle$ peut se voir de deux manières :

- De l'extérieur : $\langle A\rangle = \bigcap_{\substack{H<G\\ A\subset H}} H$.
- De l'intérieur : $\langle A\rangle = \{a_1\cdots a_n : a_i\in A\cup A^{-1} \text{ et } n\in\mathbb{N}\}$, où $A^{-1}=\{x\in G : x^{-1}\in A\}$.

Définition 3. *On dit que $A\subset G$ engendre G si $G=\langle A\rangle$. On dit que G est de type fini si il admet une partie génératrice finie.*

Exemple 4. $\langle 1\rangle=\mathbb{Z}$, $\langle \overline{1}^{[n]}\rangle = \mathbb{Z}/n\mathbb{Z}$.

Exemple 5. On définit le groupe dérivé $D(G)$ comme le sous-groupe de G engendré par les commutateurs de G, i.e les éléments de la forme $xyx^{-1}y^{-1}$ avec $x,y\in G$.

Exemple 6. $D(G)$ est le plus petit sous-groupe de G tel que $G/D(G)$ soit ablien.

Si G est abélien, on a $D(G)=\{e\}$.

1.2 Groupes libres et présentations

Définition 7. *Soit $\mathcal{A}$ un ensemble fini, appelé alphabet. On considère l'ensemble $\mathcal{M}(\mathcal{A})$ des « mots » sur $\mathcal{A}$ de longueur finis, constitués des produits des éléments a_i de $\mathcal{A}$ et de leurs inverses a_i^{-1}. On dit que deux mots m et m' sont équivalents, et on note $m\sim m'$, si l'on peut aller de l'un à l'autre en ajoutant ou en enlevant des termes de la forme $a_i a_i^{-1}$ ou $a_i^{-1}a_i$. Ceci définit une relation d'équivalence sur $\mathcal{M}(A)$.*

Définition 8. *On appelle groupe libre l'alphabet $\mathcal{A}$, et on note $F(\mathcal{A})$, le groupe dont l'ensemble sous-jacent est $\mathcal{M}(\mathcal{A})/\sim$ et la loi est la concaténation des représentants des classes de mots.*

Exemple 9. $\mathbb{Z}$ est un groupe libre sur l'alphabet $\{1\}$. $\mathbb{Z}/n\mathbb{Z}$ n'est pas un groupe libre sur l'alphabet $\{\overline{1}\}$.

Remarque 10. Un groupe libre est soit d'ordre 1, soit infini.

Proposition 11. *Soit $\mathcal{A}$ un ensemble et G un groupe. Toute application $f:\mathcal{A}\to G$ peut être étendue de manière unique en un morphisme $\varphi_f: F(\mathcal{A})\to G$.*

Définition 12. *Soit $\mathcal{A}$ un ensemble, G un groupe, et $\varphi_f: F(\mathcal{A})\to G$ un morphisme surjectif. Un élément de $\mathrm{Ker}(\varphi_f)$ est appelé une relation entre les générateurs $\{f(a) : a\in\mathcal{A}\}$ de G.*

Si un sous-ensemble R de $\mathrm{Ker}(\varphi_f)$ engendre $\mathrm{Ker}(\varphi_f)$, alors on appelle $\mathcal{A}$ et R une présentation par générateurs et relations de G (i.e G est isomorphe au quotient $F(\mathcal{A})/\langle R\rangle$), et on note :

$$G=\langle \mathcal{A}|R\rangle$$

Exemple 13. Le groupe cyclique à n éléments a pour présentation $\langle a \mid a^n\rangle$.
Le groupe diédral D_n a pour présentation $\langle r,\tau \mid r^n,\tau^2,\tau r\tau^{-1}r\rangle$.
Le groupe des quaternions $\mathbb{H}_8$ a pour présentation $\langle i,j \mid i^4, i^2j^{-2}, jij^{-1}i\rangle$.

2 Groupes cycliques

Définition 14. *On dit que G est abélien si $hg=gh$ pour tout $g,h\in G$.*

Définition 15. *On dit que G est monogène s'il existe $a\in G$ tel que l'on ait $G=\langle a\rangle$. Si de plus G est fini, on dit que G est cyclique.*

Remarque 16. Tout groupe monogène est abélien.

Proposition 17. *Tout groupe cyclique G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ avec $n=|G|$.*

Exemple 18. Le groupe $\mathbb{U}_n$ des racines $n^{\text{èmes}}$ de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Définition 19. *Un élément $a \in G$ est dit d'ordre $p \in \mathbb{N}^*$ si $\langle a \rangle$ est fini d'ordre p. L'ordre est aussi le plus petit entier p non nul tel que $a^p = e$, et on a $\langle a \rangle = \{e, a, \dots, a^{p-1}\}$.*

Proposition 20. *Si G est fini d'ordre n, alors l'ordre de tout élément de G divise n. En particulier, tout élément $a \in G$ vérifie $a^n = e$.*

Proposition 21. *Soit $a \in G$ un élément d'ordre p. On a l'équivalence $a^q = e \iff q | e$.*

Proposition 22. *Si $|G|$ est premier, alors G est cyclique, engendré par tout élément différent du neutre.*

Proposition 23. *Si G est cyclique d'ordre n ($G = \langle a \rangle$), alors :*

$$\langle a^k \rangle = G \iff k \wedge n = 1$$

De manière générale, l'ordre de a^k est $\frac{n}{k \wedge n}$.

Définition 24. *Pour $n \geq 2$, on note $\varphi(n) := |\{k \leq n \ : \ k \wedge n = 1\}|$, et on convient que $\varphi(1) = 1$.*

$\varphi : \mathbb{N}^* \to \mathbb{N}^*$ est appelée la fonction d'Euler.

Proposition 25. *Il y a $\varphi(n)$ générateurs dans $\mathbb{Z}/n\mathbb{Z}$.*

Théorème 26. *On suppose que G est cyclique d'ordre n.*

Alors tout sous-groupe de G est cyclique, et pour tout $d | n$, il existe un unique sous-groupe H_d de G d'ordre d.

Théorème 27. *Pour tout $n \in \mathbb{N}^*$, on a $\varphi(n) = \sum_{d|n} \varphi(d)$.*

3 Groupe symétrique et diédral

3.1 Groupe symétrique

Définition 28. *On appelle groupe symétrique, et on note $\mathcal{S}_n$, le groupe des bijections de l'ensemble $\{1, \dots, n\}$.*

Définition 29. *Soit $\ell \geq 1$ et $i_1, \dots, i_\ell$ des éléments distincts de $\{1, \dots, n\}$. La permutation γ définie par :*

$$\begin{cases} \gamma(k) = k \text{ si } k \notin \{i_1, \dots, i_\ell\} \\ \gamma(i_j) = i_{j+1} \text{ si } i \leq \ell - 1 \\ \gamma(i_\ell) = i_1 \end{cases}$$

Est notée $(i_1 \cdots i_\ell)$ et est appelée cycle de longueur ℓ. Un cycle de longueur 2 est appelé une transposition. On appelle support de $(i_1 \cdots i_\ell)$ l'ensemble $\{i_1, \dots, i_\ell\}$.

Théorème 30. *Toute permutation $\sigma \in \mathcal{S}_n$ s'écrit de manière unique comme produit de cycles à support disjoints. En particulier, les cycles engendrent $\mathcal{S}_n$.*

Proposition 31. *Tout cycle $(i_1 \cdots i_\ell)$ s'écrit comme produit de transpositions $(i_1 i_2)(i_2 i_3) \cdots (i_{\ell-1} i_\ell)$. Au vu du théorème 30, on en déduit que $\mathcal{S}_n$ est engendré par les transpositions.*

En fait, les transpositions $(1, i)$ avec $i \leq n$ suffisent pour engendrer $\mathcal{S}_n$.

Corollaire 32. *Pour $\sigma \in \mathcal{S}_n$ une permutation, on appelle type de σ la liste des longueurs des cycles apparaissant dans la décomposition de σ en produit de cycles à support disjoints classées par ordre croissants.*

Alors deux permutations sont conjuguées si et seulement si elles ont le même type. Ceci détermine entièrement les classes de conjugaisons de $\mathcal{S}_n$.

Proposition 33. *Il existe un unique morphisme $\varepsilon : \mathcal{S}_n \to \{-1, 1\}$ non trivial. Il est appelé la signature. On note $\mathcal{A}_n = \mathrm{Ker}(\varepsilon)$, et on a $|\mathcal{A}_n| = \frac{n!}{2}$.*

Proposition 34. *$\mathcal{A}_n$ est engendré par les cycles de la forme $(1, i, j)$ avec i et j distincts dans $\{2, \dots, n\}$. En particulier, $\mathcal{A}_n$ est engendré par les 3-cycles de $\mathcal{S}_n$.*

Théorème 35. *Pour $n \geq 5$, $\mathcal{A}_n$ est simple.*

Corollaire 36. *Pour $n \geq 5$, $D(\mathcal{S}_n) = \mathcal{A}_n$.*

3.2 Groupe diédral

Définition 37. *Pour $n \in \mathbb{N}^*$, on appelle groupe diédral D_n le groupe des isométries affines préservant le n-gône régulier.*

Proposition 38. *D_n est engendré par r et s, où r est une rotation d'angle $\frac{2\pi}{n}$ et s une symétrie axiale. On a en fait la présentation :*

$$D_n = \langle r, s \mid s^2, r^n, srsr^2 \rangle$$

Proposition 39. *On a également $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.*

Proposition 40. *On a $D(D_{2m}) = \langle r^2 \rangle$ et $D(D_{2m+1}) = \langle r \rangle$.*

4 Autour du groupe linéaire

4.1 Générateurs du groupe linéaire et décomposition de Bruhat

Dans cette partie, k désigne un corps quelconque et n désigne un entier plus grand que 1.

Définition 41. *On appelle drapeau de k^n toute suite $\{0\}=F_0\subset\cdots\subset F_n$ de sous-espaces vectoriels de k^n tels que les inclusions soient strictes. Si de plus $\dim(F_i)=i$ pour tout i, on dit que le drapeau $(F_0,\dots,F_n)$ est complet.*

Exemple 42. Soit $(e_1,\dots,e_n)$ la base canonique de k^n. On définit $F_i=\mathrm{Vect}(e_1,\dots,e_i)$ pour $i\geq 1$ et $F_0=\{0\}$. Alors $\mathcal{C}=(F_0,\dots,F_n)$ est un drapeau complet, appelé le drapeau complet canonique.

Définition 43. *On note $B_n(k)$ l'ensemble des matrices triangulaires inversibles de $\mathrm{GL}_n(k)$.*

Proposition 44. *$B_n(k)$ est le stabilisateur du drapeau complet canonique $\mathcal{C}$ pour l'action naturelle de $\mathrm{GL}_n(k)$ sur les drapeaux. En particulier, $B_n(k)$ est un sous-groupe de $\mathrm{GL}_n(k)$.*

Définition 45. *Soit $\lambda,\alpha\in k$ et $(E_{ij})_{1\leq i,j\leq n}$ la base canonique de $\mathcal{M}_n(k)$.*
On appelle transvection toute matrice de la forme $T_{ij}(\lambda)=I_n+\lambda E_{ij}$ avec $i\neq j$.
On appelle dilatation toute matrice de la forme $D_i(\alpha)=I_n+(\alpha-1)E_{ii}$.

Proposition 46. *Pour $i<j$, $T_{ij}(\lambda)\in B_n(k)$ et pour $\alpha\neq 0$, $D_i(\alpha)\in B_n(k)$.*

Remarque 47. Multiplier à gauche par une transvection $T_{ij}(\lambda)$ (respectivement multiplier à droite par $T_{ij}(\lambda)$) revient à faire l'opération sur les lignes $L_i\leftarrow L_i+\lambda L_j$ (respectivement l'opération sur les colones $C_j\leftarrow C_j+\lambda C_i$).

Multiplier à gauche par une dilatation $D_i(\alpha)$ (respetivement multiplier à droite par $D_i(\alpha)$) revient à faire l'opération sur les lignes $L_i\leftarrow\alpha L_i$ (respectivement l'opération sur les colones $C_i\leftarrow\alpha C_i$).

Proposition 48. *Soit $(e_1,\dots,e_n)$ la base canonique de k^n. Pour $\sigma\in\mathcal{S}_n$, on note w_σ l'application linéaire donnée par $w_\sigma(e_i)=e_{\sigma(i)}$.*
Alors $w:\mathcal{S}_n\to\mathrm{GL}_n(k)$ est un morphisme de groupes injectif.

Développement 1 :

Théorème 49. *(Décomposition de Bruhat)*
On a la décomposition suivante :

$$\mathrm{GL}_n(k)=\bigsqcup_{\sigma\in\mathcal{S}_n}B_n(k)\,w_\sigma\,B_n(k)$$

Corollaire 50. *$\mathrm{GL}_n(k)$ est engendré par les transvections et les matrices diagonales inversibles.*

Définition 51. *L'application déterminant $\det:\mathrm{GL}_n(k)\to k^*$ est un morphisme de groupes. Son noyau est noté $\mathrm{SL}_n(k)$ et est appelé groupe spécial linéaire d'ordre n.*

Théorème 52. *$\mathrm{SL}_n(k)$ est engendré par les transvections.*

4.2 Le groupe orthogonal

Ici, $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$ et $n\in\mathbb{N}^*$.

Définition 53. *L'ensemble des isométries linéaires de $\mathbb{K}^n$ est un groupe appelé groupe orthogonal et noté $O_n(\mathbb{K})$.*

Proposition 54. *Le sous-ensemble $\mathrm{SO}_n(\mathbb{K})$ des isométries de déterminant 1 est un sous-groupe distingué de $O_n(\mathbb{K})$, appelé groupe spécial orthogonal.*

Proposition 55. *Soit $u\in\mathrm{GL}_n(\mathbb{K})$ avec $u^2=\mathrm{Id}$. Il existe deux sous-espaces E^+ et E^- qui vérifient :*

1. *$\mathbb{K}^n=E^+\oplus E^-$.*
2. *$u_{|E^+}=\mathrm{Id}_{E^+}$ et $u_{|E^-}=-\mathrm{Id}_{E^-}$.*

Dans une base $(e_1,\dots,e_n)$, telle que $e_1,\dots,e_p\in E^+$ et $e_{p+1},\dots,e_n\in E^-$, la matrice de u est donnée par :

$$\begin{pmatrix}1&&&&&(0)\\&\ddots&&&&\\&&1&&&\\&&&-1&&\\&&&&\ddots&\\(0)&&&&&-1\end{pmatrix}$$

Si on a $u^2=\mathrm{Id}$ et $u\neq\mathrm{Id}$, on dit que u est une involution (ou encore une symétrie). Si $\dim(E^-)=1$ (resp. 2), on dit que u est une réflexion (resp. un renversement).

Proposition 56. *Soit $u\in\mathrm{GL}_n(\mathbb{K})$ avec $u^2=\mathrm{Id}$. Alors u est une isométrie si et seulement si E^+ et E^- sont orthogonaux.*

Théorème 57. *Le groupe $O_n(\mathbb{K})$ est engendré par les rélfexions orthogonales. Plus précisément, si $u\in O_n(\mathbb{K})$, u est produit d'au plus n réflexions.*

Théorème 58. *Pour $n\geq 3$, $\mathrm{SO}_n(\mathbb{K})$ est engendré par les renversements, plus précisément, tout élément $u\in\mathrm{SO}_n(\mathbb{K})$ est produit d'au plus n renversements.*

Lemme 59. *Soit $n\geq 3$ et τ_1,τ_2 des réflexions. Il existe des renversements σ_1 et σ_2 tels que $\tau_1\tau_2=\sigma_1\sigma_2$.*

Proposition 60. *Pour $n\geq 2$, $D(O_n(\mathbb{K}))=\mathrm{SO}_n(\mathbb{K})$.*
Pour $n\geq 3$, $D(\mathrm{SO}_n(\mathbb{K}))=\mathrm{SO}_n(\mathbb{K})$.

Développement 2 :

Théorème 61. *Le groupe $\mathrm{SO}_3(\mathbb{R})$ est simple.*