

Références

- [Cours d'Algèbre - Daniel Perrin](#)
- [Mathématiques pour l'Agrégation \(Algèbre\) - J.E. Rombaldi](#)
- [M. Alessandri - Thèmes de géométrie](#)
- [Modules sur les anneaux commutatifs - Diaz Toca, Lombardi et Quitté](#)
- [Théorie de Galois - Escofier](#)
-

Développements

- [Automorphismes de \$S_n\$](#)
- [Générateurs de \$O\(q\)\$](#)

Méta-plan

1. Philosophie de la méthode
 1. Notion de partie génératrice
 2. Extensions de groupes
 3. La méthode en action : le groupe dérivé
2. Deux études de groupes et de leurs générateurs
 1. Groupe symétrique, groupe alterné
 2. Groupes de matrices
3. Le cas des groupes abéliens

Plan détaillé

Petite introduction : l'objectif est de pouvoir étudier des groupes compliqués en se ramenant à des parties plus simples, comme on étudie un espace vectoriel en étudiant une base. Dans les groupes, le problème est plus compliqué. Dans une première partie, on introduira plusieurs outils permettant de décomposer un groupe en parties plus simples, puis on étudiera des cas concrets d'applications. Enfin, on s'intéressera aux groupes abéliens de type fini dans leur ensemble.

I - Philosophie de la méthode

1 - Utilisation de parties génératrices [Perrin]

1. Définition : soit G un groupe et $S \subset G$. Il existe un unique sous-groupe de G , minimal pour l'inclusion et contenant S , noté $\langle S \rangle$. On l'appelle sous-groupe engendré par S . Si $\langle S \rangle = G$, on dit que S est une partie génératrice de G . Si une telle partie finie existe, on dit que G est de type fini.
2. Exemples :
 1. 1 engendre $\mathbb{Z}/n\mathbb{Z}$.
 2. La rotation d'angle $2\pi/n$ et la symétrie du plan par rapport à l'axe des abscisses engendrent le groupe diédral.
3. Proposition : description en extension
4. Théorème : Soient $\Phi, \Psi : G \rightarrow H$ des morphismes de groupes et $S \subset G$ une partie génératrice de G . Alors $\Phi|_S = \Psi|_S \implies \Phi = \Psi$.
5. Remarque : il est difficile de généraliser au cas des groupes la notion de famille libre et de base. Par exemple, quelque soit la partie génératrice de S considérée dans $\mathbb{Z}/n\mathbb{Z}$, il n'est pas toujours possible d'étendre une fonction de S dans $\mathbb{Z}/(n+1)\mathbb{Z}$ en un morphisme de groupes sur $\mathbb{Z}/n\mathbb{Z}$.

2 - Extensions de groupes [Perrin, Alessandri]

1. Définition : suite exacte courte. Suite exacte scindée. Extension.
2. Exemple : Soit $\mathcal{E}$ un $\mathbb{R}$ -espace affine de dimension finie. On dispose de deux suites exactes courtes scindées

$$1 \rightarrow \text{Trans}(\mathcal{E}) \rightarrow \text{Aff}(\mathcal{E}) \rightarrow GL(\vec{\mathcal{E}}) \rightarrow 1$$

(et la même avec le groupe orthogonal)

3. Proposition : Si $1 \rightarrow N \rightarrow G \rightarrow H \rightarrow 1$ est exacte, scindée à droite, et si S_N et S_H sont des parties génératrices de G , on peut trouver une partie génératrice de G en concaténant les images de S_N et S_H dans G .
4. Définition : produit direct
5. Théorème : soient G, N, H trois groupes. Les assertions suivantes sont équivalentes :
 1. $G \cong N \times H$
 2. G admet deux sous-groupes distingués $\bar{N}$ et $\bar{H}$ isomorphes à N et H respectivement, tels que $\bar{N} \cap \bar{H} = 1$ et $\bar{N}\bar{H} = G$.

3. Il existe une suite exacte $1 \rightarrow N \rightarrow G \rightarrow H \rightarrow 1$ scindée.
6. Exemple : Si $\mathcal{E}$ est un espace affine euclidien de direction E , on a un isomorphisme :

$$(E, +) \times O(E) \cong Iso(\mathcal{E})$$

3 - La méthode en action : le groupe dérivé [Perrin]

1. Définition : commutateur, groupe dérivé
2. Exemple : soit n un entier impair. On considère le groupe diédral d'ordre $2n$, c'est-à-dire le groupe d'isométries du plan engendré par la symétrie orthogonale d'axe des abscisses et la rotation d'angle $2\pi/n$. Le groupe dérivé de D_{2n} est son sous-groupe engendré par les rotations. Il est isomorphe à $\mathbb{U}_n$ le groupe des racines n -ièmes de l'unité.
3. Remarque : G est abélien ssi $D(G) = 1$.
4. Proposition : $D(G)$ est distingué dans G .
5. Proposition : soient G et H deux groupes et $\phi : G \rightarrow H$ un morphisme. Alors $\phi(D(G)) \subset D(H)$.
6. Application : Soit H un groupe abélien. Un morphisme de groupes de D_{2n} dans H ne peut prendre qu'une ou deux valeurs. En particulier, si H est fini d'ordre impair, $Hom(D_{2n}, H) = 1$.

II - Deux études de parties génératrices de groupes

1 - Groupe symétrique [Rombaldi, Perrin]

1. Théorème (Cayley) : tout groupe fini G s'injecte dans $\mathfrak{S}_{[G]}$.
2. Définition : on appelle cycle de $\mathfrak{S}_n$ toute permutation σ telle que $[[1, n]]$ contient une unique orbite non triviale sous l'action naturelle de $\langle \sigma \rangle$. On appelle longueur du cycle le cardinal de cette orbite. Dans le cas particulier d'un cycle de longueur 2, on parle de transposition.
3. Théorème (parties génératrices de $\mathfrak{S}_n$) :
 1. Les transposition de la forme $(1, i)$ engendrent $\mathfrak{S}_n$.
 2. La transposition $(1, 2)$ et le cycle $(1, 2, \dots, n)$ engendrent $\mathfrak{S}_n$.
 3. Toute permutation de $\mathfrak{S}_n$ s'écrit de façon unique à ordre des termes près comme un produit de cycles à supports disjoints

4. Application (définition du morphisme signature) : L'application ϵ qui à σ associe $(-1)^{n - p(\sigma) - \phi(\sigma)}$, avec p le nombre de cycles dans sa décomposition en cycles et ϕ le nombre de points fixes est un morphisme de groupes bien défini. On note $\mathfrak{A}_n$ son noyau.
5. Proposition (générateurs de $\mathfrak{A}_n$) : pour $n \geq 3$, les 3-cycles engendrent $\mathfrak{A}_n$. Ils sont de plus tous conjugués dans $\mathfrak{A}_n$.
6. Application : $\mathfrak{A}_n$ est le groupe dérivé de $\mathfrak{S}_n$ pour $n \geq 2$. En particulier, la signature est l'unique morphisme non trivial de $\mathfrak{S}_n$ dans $\mathbb{C}^\times$.
7. Théorème : $\mathfrak{A}_n$ est simple pour $n \geq 5$.
8. Corollaire : pour $n \geq 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont lui-même, 1 et $\mathfrak{A}_n$.
9. Application : pour $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont tous intérieurs. (DVT 1)

2 - Groupes de matrices [Rombaldi]

Fixons K un corps et n un entier.

1. Proposition : le morphisme déterminant $GL_n(K) \rightarrow K^\times$ admet une rétraction explicite et donne naissance à une suite exacte scindée à droite

$$1 \rightarrow SL_n(K) \rightarrow GL_n(K) \rightarrow K^\times \rightarrow 1$$

2. Définition (transvections, dilatations) : on appelle matrice de transvection toute matrice de la forme $I_n + \lambda E_{i,j}$, $i \neq j$, $\lambda \neq 0$. On appelle dilatation toute matrice diagonale inversible dont tous les termes sauf 1 sont égaux à 1.
3. Théorème : Les matrices de transvection engendrent $SL_n(K)$.
4. Corollaire : les transvections et les dilatations engendrent $GL_n(K)$
5. Application : On considère un système linéaire de la forme $Ax = 0$. Quelques soient les matrices inversibles P et Q , il est possible à l'aide des opérations élémentaires du pivot de Gauss de mettre ce système sous la forme $(P \cdot A \cdot Q)x = 0$.
6. Corollaire : si $n \geq 3$, $D(GL_n(K)) = D(SL_n(K)) = SL_n(K)$.
On suppose dans la suite que K est de caractéristique différente de 2 et on fixe (E, q) un K -espace quadratique anisotrope de dimension finie n .
7. Définition (réflexion, renversement) : on appelle réflexion (resp. renversement) tout endomorphisme u de E tel qu'il existe un sous-espace vectoriel H de

dimension $n - 1$ (resp $n - 2$) tel que u soit la symétrie par rapport à H parallèlement à $H^\perp$.

8. Proposition : les réflexions sont des isométries de déterminant -1 . Les renversements sont des isométries de déterminant 1 .
9. Théorème : soit u une q -isométrie. Notons $p(u) := n - \dim(\ker(I_d - u))$. Alors u est produit de $p(u)$ réflexions, et pas moins. Si de plus u est de déterminant 1 , u est produit d'au plus $p(u)$ renversements. (DVT 2)
10. Application : Soit $\mathcal{E}$ un espace affine euclidien de dimension finie. Le groupe des isométries de $\mathcal{E}$ est engendré par les réflexions et les translations.

III - Le cas des groupes abéliens [Rombaldi, Diaz-Toca Lombardi Quitté, Escofier]

1. Définition (groupe cyclique) : on appelle groupe cyclique un groupe fini engendré par un seul élément.
2. Exemples :
 1. Le groupe des racines n -ièmes de l'unité de $\mathbb{C}$ est cyclique d'ordre n .
 2. Si K est un corps fini de cardinal q , $K^\times$ est cyclique de cardinal $q - 1$.
3. Théorème (structure des groupes cycliques) : tout groupe cyclique G d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Pour tout diviseur d de n , G admet un unique sous-groupe d'ordre d et ce groupe est cyclique.
4. Proposition : soit $\mathbb{F}_q$ un corps fini à q -éléments et $L/\mathbb{F}_q$ une extension de corps de degré n . Le groupe d'automorphisme $\text{Aut}(L/\mathbb{F}_q)$ est cyclique, engendré par l'application $x \mapsto x^q$.
5. Application : soit $\mathbb{F}_q$ un corps fini de cardinal q et n une entier premier avec la caractéristique de $\mathbb{F}_q$. Les facteurs irréductibles dans $\mathbb{F}_q[X]$ du n -ième polynôme cyclotomique Φ_n ont tous pour degré l'ordre de q dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$.
6. Théorème (structure des groupes abéliens de type fini) : soit G un groupe abélien de type fini. Alors il existe un unique couple d'entiers (r, s) et une unique famille d'entiers positifs $d_s \mid \cdots \mid d_1$ tels que G soit isomorphe au produit direct

$$G \cong \mathbb{Z}^r \times \prod_{i=1}^s \mathbb{Z}/d_i\mathbb{Z}$$

En particulier, G admet une famille génératrice de cardinal $r + s$.

7. Exemple :

8. Application : soit G un groupe abélien fini de cardinal n . Pour tout $d \mid n$, G admet un sous-groupe d'ordre d .