P. Maurer
ENS Rennes

Leçon 104. Groupes abéliens et non abéliens finis. Exemples et applications

Devs :

- Théorèmes de Sylow
- Structure des groupes abéliens finis

Références :

1. Ulmer, Théorie des groupes
2. Comez, Elements d'algèbre et d'analyse
3. Perrin, Cours d'algèbre
4. Gourdon, Algèbre

L'étude des groupes finis et en particulier leur classification, a joué un rôle important dans le développement de nombreux outils mathématiques. Si le théorème de structure des groupes abéliens finis a été démontré depuis 1870, la classification des groupes non abéliens, elle, est beaucoup plus récente et difficile. Elle a conduit a introduire, par exemple, la notion de simplicité, l'étude des p-groupes via les théorèmes de Sylow, et (un peu) plus récemment la théorie des représentations.

Dans tout ce qui suit, G désigne un groupe fini et on note $|G|$ le cardinal de G. On se donne également $n \in \mathbb{N}$ un entier supérieur ou égal à 1.

1 Généralités sur les groupes finis

1.1 Ordre d'un groupe fini, ordre d'un élément

Définition 1.
Le cardinal $|G|$ du groupe fini G est appelé l'ordre de G. Si g est un élément de G, on appelle ordre de g le plus petit entier $n > 0$ (s'il en existe) qui vérifie $g^n = 1$. C'est aussi l'ordre du sous-groupe engendré par G.

Exemple 2. Pour tout $n \in \mathbb{N}$, le groupe $\mathbb{Z}/n\mathbb{Z}$ est fini d'ordre n. Une transpotion $\tau \in \mathcal{S}_n$ est un élément d'ordre deux dans l'ensemble des permutations d'ordre n.

Proposition 3.
Soit G un groupe abélien fini.

1. *Si $x \in G$ est d'ordre a et si $y \in G$ est d'ordre b, et si $a \wedge b = 1$, alors xy est d'ordre ab.*
2. *Si $a, b \in \mathbb{N}^*$ et si G contient des éléments d'ordre a et b, alors il contient un élément d'ordre $\mathrm{ppcm}(a, b)$.*
3. *Soit N le maximum des ordres des éléments de G. Alors on a $x^N = 1$ pour tout $x \in G$. On dit que N est l'exposant du groupe G.*

Proposition 4. *La relation $\sim_H$ donnée sur G par $x \sim_H y \iff \exists h \in H \quad x = hy$ est une relation d'équivalence, dont les classes d'équivalence sont notées gH et appelées les classes à gauche modulo G. On a $gH = \{gh : h \in H\}$.*

Définition 5. *On appelle ensemble quotient de G par la relation d'équivalence $\sim_H$, et on note G/H, l'ensemble $\{gH : g \in G\}$.*
On appelle indice de H dans G le cardinal de G/H, et on le note $[G : H]$.

Théorème 6. *(Lagrange)*
On a $|G/H| = \dfrac{|G|}{|H|}$. En particulier, l'ordre (et l'indice) de H dans G divise le cardinal de G.

Exemple 7. Tout groupe d'ordre p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, et ses seuls sous-groupes sont les sous-groupes triviaux G et $\{e\}$.

1.2 Actions de groupe

Définition 8. *Soit X un ensemble. On dit que G agit (ou opère) sur X s'il existe une application :*

$$\cdot : \begin{cases} G \times X & \to & X \\ (g, x) & \mapsto & g.x \end{cases}$$

vérifiant les propriétés suivantes :
i) $\forall g, g' \in G \quad \forall x \in X \; g.(g'.x) = g'.(g.x)$
ii) $\forall x \in X \quad 1.x = x$

Dans ce qui suit, on suppose que G agit sur l'ensemble X.

Remarque 9. Se donner une action de G sur X revient à se donner un morphisme $T : G \to \mathcal{S}(X)$ où $\mathcal{S}(X)$ désigne les bijections de X dans lui-même, via $g.x = T(g)(x)$.

Exemple 10. Le groupe $\mathcal{S}_n$ agit sur $\{1, \dots, n\}$, via $\sigma.i = \sigma(i)$.
Le groupe $\mathrm{GL}_n(\mathbb{K})$ agit sur $\mathbb{K}^n$ via $P.X = PX$.
Le groupe diédral D_n agit sur le polynôme régulier à n côtés.

Définition 11. *Soit $x \in X$.*
On définit le stabilisateur de x par $G_x = \{g \in G : g.x = x\}$, aussi noté $\mathrm{Stab}(x)$.
On définit l'orbite de x par $O(x) = \{y \in X : \exists g \in G, \; y = g.x\}$.

Exemple 12.

Dans l'action de $\mathcal{S}_n$ sur $\{1,\dots,n\}$, le stabilisateur d'un point est isomorphe à $\mathcal{S}_{n-1}$.

Proposition 13. *(Cayley)*
Si G est fini de cardinal n, alors G est isomorphme à un sous-groupe de $\mathcal{S}_n$.

Proposition 14.
Soit $x\in X$. L'application $f:\begin{cases} G/G_x\to O(x)\\ gG_x\mapsto gx\end{cases}$ est une bijection entre l'ensemble des classes à gauche du stabilisateur G_x dans G et l'orbite $O(x)$ de x dans G.

Corollaire 15. *(relation orbite-stabilisateurs)*
Soit $x\in X$. Alors on a :
1. $|O(x)|=[G:G_x]$,
2. $|O(x)|=\dfrac{|G|}{|G_x|}$.

Proposition 16. *(formule des classes)*
Soit $O(x_1)$,...,$O(x_q)$ les orbites distinctes des éléments de X sous l'action de G. Alors :

$$|X|=\sum_{i=1}^{q}|O(x_i)|=\sum_{i=1}^{q}\frac{|G|}{|G_{x_i}|}.$$

1.3 Groupes symétriques et diédraux

Définition 17. *On appelle groupe symétrique d'ordre n le groupe $\mathcal{S}_n$ des bijections entre $[\![1,n]\!]$ et lui-même. Le groupe $\mathcal{S}_n$ est d'ordre $|\mathcal{S}_n|=n!$.*

Définition 18. *Soit $\sigma\in\mathcal{S}_n$. Les éléments $i\in\{1,\dots,n\}$ qui vérifient $\sigma(i)=i$ sont appelés points fixes de σ, et on note $\mathrm{Fix}(\sigma)$ l'ensemble de ses points fixes.*
On appelle support de σ, et on le note $\mathrm{Supp}(\sigma)$, l'ensemble $\{1,\dots,n\}\setminus\mathrm{Fix}(\sigma)$.

Proposition 19. *Soit $\sigma,\rho\in\mathcal{S}_n$. On a toujours $\mathrm{Supp}(\sigma\rho)\subset\mathrm{Supp}(\sigma)\cup\mathrm{Supp}(\rho)$.*
Si $\mathrm{Supp}(\sigma)\cap\mathrm{Supp}(\rho)=\varnothing$, on dit que σ et ρ sont des permutations à support disjoint, et dans ce cas, on a $\mathrm{Supp}(\sigma\rho)=\mathrm{Supp}(\sigma)\sqcup\mathrm{Supp}(\rho)$ et
- *$\sigma\rho(i)$ est égal à $\sigma(i)$ si $i\in\mathrm{Supp}(\sigma)$ et à $\rho(i)$ si $i\in\mathrm{Supp}(\rho)$,*
- *$\sigma\rho=\rho\sigma$,*
- *$\sigma\rho=\mathrm{Id}_n\iff\sigma=\rho=\mathrm{Id}_n$.*

Définition 20. *Soit $\ell\geq1$ un entier et $i_1,\dots,i_\ell$ des éléments distincts de $[\![1,n]\!]$. La permutation γ définie par $\gamma(j)=\begin{cases} j & \text{si } j\notin\{i_1,\dots,i_\ell\}\\ j+1 & \text{si } j\in\{i_1,\dots,i_{\ell-1}\}\\ i_1 & \text{si } j=i_{\ell-1}\end{cases}$ est notée $(i_1,\dots,i_\ell)$ et est appelée cycle de longueur ℓ.*
Un cycle de longueur deux est appelé une transposition.

Théorème 21.
Toute permutation $\sigma\in\mathcal{S}_n$ s'écrit comme produit $\sigma=\gamma_1\cdots\gamma_m$ de cycles γ_i de longueur $\ell\geq2$ dont les supports sont deux à deux disjoints. Cette décomposition est unique à l'ordre des facteurs près.

Corollaire 22. *Toute permutation $\sigma\in\mathcal{S}_n$ se décompose en un produit de transpositions. Il n'y a pas, a priori, unicité dans cette décomposition.*

Exemple 23. La permutation $\sigma=\begin{pmatrix}1&2&3&4&5&6\\2&4&5&1&3&6\end{pmatrix}\in\mathcal{S}_6$ se décompose en $\sigma=(1,2,4)(3,5)$.

Définition 24. *Soit $\sigma\in\mathcal{S}_n$. On appelle signature de σ, et on note $\varepsilon(\sigma)$, le nombre*

$$\varepsilon(\sigma)=\prod_{1\leq i<j\leq n}\frac{\sigma(i)-\sigma(j)}{i-j}.$$

Proposition 25. *L'application $\varepsilon:\mathcal{S}_n\to\{-1,1\}$ est un morphisme de groupes. Son noyau est appelé le groupe alterné, noté $\mathcal{A}_n$. C'est un sous-groupe distingué de $\mathcal{S}_n$.*
La parité du nombre de transpositions dans la décomposition en produit de transpositions $\sigma\in\mathcal{S}_n$ ne dépend pas de la décomposition, et $\varepsilon(\sigma)$ vaut 1 ou -1 selon que ce nombre est pair ou impair.

Définition 26. *On appelle $n^{\text{ème}}$ groupe diédral, et on note D_n, le groupe des isométries affines qui laissent stable le polygône régulier à n côtés.*

Proposition 27. *Le groupe D_n a pour cardinal $2n$. Ses générateurs sont donnés par*

$$s=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\text{ et }r=\begin{pmatrix}\cos(\theta)&-\sin(\theta)\\\sin(\theta)&\cos(\theta)\end{pmatrix}\text{ avec }\theta=\frac{2\pi}{n}.$$

Ils vérifient les relations $s^2=\mathrm{Id}$, $srs=r^{-1}$, et les éléments de D_n sont donnés par

$$\{\mathrm{Id},r,r^2,\dots,r^{n-1},s,rs,\dots,r^{n-1}s\}.$$

2 Groupes abéliens et leur classification

2.1 Groupes cycliques

Définition 28. *On dit qu'un groupe G est cyclique s'il est engendré par un de ses éléments.*

Proposition 29. *Un groupe cyclique fini G d'ordre $n\in\mathbb{N}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Théorème 30. *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 31. *(restes chinois)*
Soit $n, m \in \mathbb{N}$ premiers entre eux. Alors $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

2.2 Caractères des représentations irréductibles et groupe dual

Lemme 32. *Soit G un groupe abélien et (V, ρ) une représentation irréductible de G. Alors $\dim(V) = 1$.*

Définition 33.
On appelle caractère d'une représentation (V, ρ) de G l'application $\chi_V : G \to \mathbb{C}$ définie par $\chi_V(g) := \mathrm{Tr}(\rho(g))$.
Si V est de dimension 1, $\mathrm{GL}(V)$ est isomorphe à $\mathbb{C}^*$, donc la représentation V s'identifie à un morphisme de groupes $\chi : G \to \mathbb{C}^*$. On appelle caractère linéaire de G un tel morphisme, et on note $\hat{G}$ l'ensemble des caractères linéaires de G.

Proposition 34. *Si V est une représentation de dimension 1 de G et χ le caractère linéaire associé, on a $\chi_V = \chi$: le caractère du caractère linéaire est le caractère linéaire lui-même.*
Muni du produit $(\chi_1 \chi_2)(g) := \chi_1(g)\,\chi_2(g)$, l'ensemble $\hat{G}$ des caractères linéaires de G est un groupe commutatif. On l'appelle le groupe dual de G.

Remarque 35. Dans le cas où G est abélien, on déduit du lemme 1 que $\mathrm{Irr}(G)$ coïncide avec $\hat{G}$.

Théorème 36. *(Frobenius)*
Les caractères irréductibles forment une base des fonctions centrales, i.e des fonctions $\phi : G \to \mathbb{C}$ qui sont constantes sur les classes de conjugaison de G.

Corollaire 37. *Le nombre de représentations irréductibles de G est égal au nombre $|\mathrm{Conj}(G)|$ de classes de conjugaison dans G. En particulier, il est fini.*

Corollaire 38. *Si G est abélien, toute fonction $\phi : G \to \mathbb{C}$ est centrale, et l'ensemble des caractères linéaires $\hat{G}$ forme une base orthonormale des fonctions de G sur $\mathbb{C}$.*

Définition 39. *Soit G un groupe qui agit sur lui même à gauche. On définit la représentation régulière V_G de G comme l'espace vectoriel V_G de dimension $|G|$, de base $(e_h)_{h \in G}$, muni de l'action linéaire de G donnée par $g \cdot e_h = e_{g \cdot h}$.*

Remarque 40. Dans la base $(e_h)_{h \in G}$, la matrice de $g \in G$ est une matrice de permutation, dont le terme diagonal vaut 1 si et seulement si $gh = h$, et zéro sinon.

En particulier, on en déduit que $\chi_{V_G}(1) = |G|$ et $\chi_{V_G}(g) = 0$ si $g \neq 1$.

Proposition 41. *(formule de Burnside)*
Si W est une représentation irréductible de G, alors W apparaît dans la représentation régulière avec la multiplicité $\dim W$, et on a

$$\sum_{W \in \mathrm{Irr}(G)} (\dim W)^2 = |G|.$$

2.3 Théorèmes de structure

Développement 1 :

Lemme 42. *Soit G un groupe abélien fini. Alors G est isomorphe à $\hat{\hat{G}}$.*

Lemme 43. *Soit G un groupe abélien fini. Alors G et $\hat{G}$ ont le même exposant.*

Théorème 44. *(Théorème de structure des groupes abéliens finis, existence)*
Soit G un groupe abélien fini. Alors il existe $r \in \mathbb{N}$ et des entiers $N_1, \ldots, N_r$, où N_1 est l'exposant de G et qui vérifient $N_{i+1} | N_i$ pour tout $i \leq r-1$, et qui sont tels que

$$G \simeq \prod_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}.$$

Remarque 45. Les facteurs $N_1, \ldots, N_r$ sont en fait uniques, et on les appelle les invariants de G.

3 Groupes non abéliens et simplicité

3.1 Notion de groupes simples

Définition 46. *On dit que G est simple si ses seuls sous-groupes distingués sont $\{e\}$ et lui-même.*

Proposition 47. *Les seuls groupes abéliens simples sont les $\mathbb{Z}/p\mathbb{Z}$ avec p premier.*

Théorème 48. *$\mathcal{A}_n$ est simple pour $n \geq 5$.*

Corollaire 49. *Pour $n \geq 5$, le seul groupe distingué non trivial de $\mathcal{S}_n$ est $\mathcal{A}_n$.*

Remarque 50. Le résultat est faux pour $n = 4$: $\mathcal{A}_4$ admet un sous-groupe distingué non trivial qui est V_4.

3.2 Etude des p-groupes et théorèmes de Sylow

Définition 51. *Soit p un nombre premier. On appelle p-groupe un groupe fini d'ordre une puissance de p.*

Définition 52. *On appelle ensemble des points fixes d'un ensemble X pour l'action de G l'ensemble :*

$$X^G = \{x \in X \,:\, \forall g \in G \quad g.x = x\}$$

Proposition 53. *On suppose que G est un p-groupe et que X est fini. Alors on a :*

$$|X| \equiv |X^G| \pmod{p}$$

Corollaire 54. *Le centre d'un p-groupe distinct de $\{1\}$ n'est pas réduit à $\{1\}$.*

Corollaire 55. *Soit p un nombre premier. Alors tout groupe fini G de cardinal p^2 est abélien, et plus précisément isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$ ou bien à $\mathbb{Z}/p^2\mathbb{Z}$.*

Exemple 56. Le corollaire devient faux pour les groupes d'ordre p^k avec $k \geq 3$. On peut donner en exemple le sous-groupe $T_3(\mathbb{F}_p)$ de $\mathrm{GL}_3(\mathbb{F}_p)$ constitué des matrices triangulaires supérieures avec des 1 sur la diagonale.

Définition 57. *Soit G un groupe de cardinal $n = p^\alpha m$ avec p premier avec $p \nmid n$. On appelle p-Sylow de G tout sous-groupe de cardinal p^α.*

Exemple 58. Soit $n = p^\alpha m$ avec $p \nmid m$. Alors $\mathbb{Z}/n\mathbb{Z}$ a un unique p-Sylow donné par $\langle m \rangle$.

L'ensemble $T_n(\mathbb{F}_p)$ des matrices triangulaires supérieures de taille n avec des 1 sur la diagonale est un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$.

Développement 2 :

Théorème 59. *(Sylow)*
Soit G un groupe d'ordre $p^\alpha m$ avec $p \nmid m$. Alors :

1. *G possède au moins un p-Sylow.*
2. *Les p-Sylow sont tous conjugués entre eux.*
3. *En notant k le nombre de p-Sylow, on a $k \equiv 1 \pmod{p}$ et k divise m.*

Exemple 60. Tout groupe d'ordre 15 est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Exemple 61. Il n'existe pas de groupe simple d'ordre 63 et 255.