104. Groupes finis. Exemples et applications.

Introduction : La classification des groupes finis est aujourd'hui considérée comme achevée, mais la démonstration complète comporte des milliers de pages. On présente ici quelques grandes idées de la théorie des groupes finis.

1 Généralités

Soit G un groupe de cardinal fini.

1.1 Définitions et premières propriétés

Définition 1. Le cardinal de G est appelé *ordre* de G.

Définition 2. Si $g \in G$, on appelle *ordre* de g l'entier $n = \min\{k \in \mathbb{N}^*, g^k = e_G\}$. On note $n = \text{ord}(g)$.

Théorème 3 (Lagrange)**.** Soit H sous-groupe de G. Alors $|G| = |H| \cdot |G/H|$.

Corollaire 4. L'ordre d'un élément de G divise l'ordre de G.

Définition 5. G est dit d'exposant fini s'il existe $N \in \mathbb{N}$ tel que pour tout $g \in G, g^N = e$.

Proposition 6. Tout groupe fini est d'exposant fini.

***Contre-exemple* 7.** *$(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ est d'exposant fini mais non fini.*

Théorème 8 (Burnside)**.** Tout sous-groupe de $GL_n(\mathbb{C})$ d'exposant fini est fini.

1.2 Actions de groupes finis

On suppose que G agit sur un ensemble X fini. Pour $x \in X$, on notera $\text{Orb}(x)$ son orbite et $\text{Stab}(x)$ son stabilisateur.

Théorème 9 (Formule des classes)**.** Pour tout $x \in X$, $|\text{Orb}(x)| = \dfrac{|G|}{|\text{Stab}(x)|}$.
En particulier, si $\Omega \subseteq X$ contient un unique représentant de chaque orbite, alors $|X| = \displaystyle\sum_{x \in \Omega} \frac{|G|}{|\text{Stab}(x)|}$.

***Application* 10.** *Si G est un p-groupe, son centre n'est pas trivial.*

Définition 11. On appelle fixateur de $g \in G$ l'ensemble $\text{Fix}(g) = \{x \in X, g \cdot x = x\}$.

Théorème 12 (Formule de Burnside)**.** Si G, X sont finis, le nombre d'orbites de l'action de G sur X est donné par $N = \dfrac{1}{|G|} \displaystyle\sum_{g \in G} |\text{Fix}(g)|$.

***Application* 13.** *Si une roue de loterie est découpée en n secteurs, et qu'on dispose de p couleurs, le nombre de coloriages possibles est $\dfrac{1}{n} \displaystyle\sum_{d|n} \varphi\left(\frac{n}{d}\right) p^d$.*

1.3 Exemples de groupes finis

Groupes cycliques

Définition 14. G est dit *cyclique* s'il est engendré par un élément.

***Exemple* 15.** *Pour tout $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{U}_n$ sont cycliques.*

Proposition 16. Les groupes cycliques et leurs produits directs sont abéliens.

Proposition 17. Tout groupe d'ordre premier est cyclique.

Groupes symétriques et alternés

Définition 18. Pour $n \in \mathbb{N}$, on appelle n-ème groupe symétrique le groupe $\mathcal{S}_n$ des permutations de $[\![1, n]\!]$.

Théorème 19 (Cayley)**.** Si $n = |G|$, alors G est isomorphe à un sous-groupe de $\mathcal{S}_n$.

Définition 20. On appelle *k-cycle* $(2 \leq k \leq n)$ une permutation c pour laquelle il existe $i_1, \cdots, i_k \in [\![1, n]\!]$ tels que $c(i_1) = i_2, \cdots, c(i_{k-1}) = i_k, c(i_k) = i_1$. Un tel cycle est noté $(i_1, i_2, \cdots, i_k)$, les autres éléments de $[\![1, n]\!]$ étant fixés. Le *support* d'un cycle c est l'ensemble $\{i \in [\![1, n]\!], c(i) \neq i\}$. Un 2-cycle est appelé *transposition*.

Théorème 21. Tout $\sigma \in \mathcal{S}_n$ peut s'écrire de façon unique comme produit de cycles à supports disjoints, ou comme produits de transpositions (non unique).

Définition 22. Si $\sigma \in \mathcal{S}_n$, on définit sa signature par $\varepsilon(\sigma) = \displaystyle\prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$.

Proposition 23. ε est un morphisme de groupes de $(\mathcal{S}_n, \circ)$ dans $(\{-1, 1\}, \times)$.

Définition 24. Le noyau de ε est appelé groupe alterné, et noté $\mathcal{A}_n$.

Groupes diédraux

Définition 25. Soit $n \in \mathbb{N}^*$. On appelle n-ème groupe diédral le groupe D_n des isométries conservant le polygone régulier à n sommets.

Proposition 26. D_n est constitué des n rotations de centre O et d'angle $\frac{2k\pi}{n}, k \in [\![0, n-1]\!]$ et des n réflexions par rapport aux droites passant par O et d'angle $\frac{k\pi}{n}, k \in [\![0, n-1]\!]$ avec l'axe horizontal.

Groupe quaternionique

Définition 27. On appelle groupe quaternionique le groupe $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ dont la loi est donnée par $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j$.

2 Classification des groupes finis

2.1 Groupes abéliens finis

Proposition 28. Pour $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ est l'unique groupe cyclique d'ordre n à isomorphisme près.

Théorème 29 (Lemme chinois)**.** Soient $m, n \in \mathbb{N}^*$. Alors $\mathbb{Z}/mn\mathbb{Z}$ est isomorphe à $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, si et seulement si, m et n sont premiers entre eux.

***Application* 30.** *L'ensemble des solutions de* $\begin{cases} x \equiv 2[3] \\ x \equiv 4[5] \end{cases}$ *est* $\{14 + 15k, k \in \mathbb{Z}\}$.

Lemme 31. Si H sous-groupe distingué d'un groupe fini G, alors tout morphisme $H \to \mathbb{C}^*$ se prolonge en un morphisme $G \to \mathbb{C}^*$.

Théorème 32. Soit G un groupe abélien fini.
Alors il existe une unique suite d'entiers naturels $d_1, \cdots, d_k$ tels que G soit isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$ et $\forall i \in [\![1, k-1]\!], d_i | d_{i+1}$.

***Exemple* 33.** $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ *est isomorphe à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$.

***Application* 34.** *À isomorphisme près, il existe 5 groupes abéliens d'ordre 48.*

2.2 Groupes non abéliens

Définition 35. Si G est un groupe d'ordre $p^k m$ avec p premier et $p \wedge m = 1$, on appelle p-Sylow de G tout sous-groupe d'ordre p^k.

Théorème 36 (Sylow)**.** Soit p un nombre premier, soit G un groupe d'ordre multiple de p.

1. G possède un p-Sylow.
2. Tous les p-Sylow sont conjugués. En particulier, s'il n'existe qu'un seul p-Sylow, il est distingué dans G.
3. Si on note n_p le nombre de p-Sylow, $n_p \equiv 1[p]$ et $p | m$.

***Application* 37.** *Il n'existe pas de groupe simple d'ordre 30 ou 105.*

***Application* 38.** *Pour* $n \geq 5, \mathcal{A}_n$ *est simple.*

3 Représentations linéaires des groupes finis

3.1 Définitions et propriétés

Définition 39. Soit G un groupe. On appelle représentation linéaire de G la donnée d'un couple (ρ, V) où V est un $\mathbb{C}$-espace vectoriel et $\rho : G \to GL(V)$ morphisme de groupes. Si V est de dimension finie, sa dimension est appelée degré de la représentation.

***Exemple* 40.**
- *Le morphisme constant* $\mathbf{1} : G \to \mathbb{C}^*$ *est une représentation de degré 1.*
- *Le groupe diédral s'identifie à un sous-groupe de* $GL(\mathbb{R}^2)$ *: c'est la représentation standard, de degré 2.*

Définition 41. On dit qu'un sous-espace W de V est stable par la représentation s'il est stable par tous les $\rho(g), g \in G$. La représentation est dite irréductible si ses seuls sous-espaces stables sont $\{0\}$ et V.

Définition 42. (ρ_1, V_1) et (ρ_2, V_2) sont dites équivalentes s'il existe $f : V_1 \to V_2$ isomorphisme tel que $\forall g \in G, \rho_2(g) = f \circ \rho_1(g) \circ f^{-1}$.

3.2 Caractères

Définition 43. On appelle caractère d'une représentation (ρ, V) l'application $\chi_\rho : g \mapsto \mathrm{tr}(\rho(g))$.

On munit l'ensemble $\mathcal{F}(G)$ des fonctions de G dans $\mathbb{C}$ du produit scalaire hermitien $\langle \varphi, \psi \rangle = \dfrac{1}{|G|} \displaystyle\sum_{g \in G} \varphi(g)\overline{\psi(g)}$.

Théorème 44.
- Il y a autant de classes d'équivalence de représentations irréductibles que de classes de conjugaison de G.
- Les caractères irréductibles forment une base orthonormée de l'espace des fonctions $G \to \mathbb{C}$ constantes sur les classes de conjugaison.

Définition 45. On appelle table de caractères le tableau donnant la valeur de chaque caractère irréductible sur chaque classe de conjugaison.

***Exemple* 46.** *Table de caractères de* $\mathcal{S}_4$.

Annexe

Classification des groupes de petit cardinal

Ordre	Classes d'isomorphisme	Nb classes
2	$\mathbb{Z}/2\mathbb{Z}$	1
3	$\mathbb{Z}/3\mathbb{Z}$	1
4	$\mathbb{Z}/4\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^2$	2
5	$\mathbb{Z}/5\mathbb{Z}$	1
6	$\mathbb{Z}/6\mathbb{Z}, \mathcal{S}_3 \simeq D_3$	2
7	$\mathbb{Z}/7\mathbb{Z}$	1
8	$\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^3, D_4, \mathbb{H}_8$	5
9	$\mathbb{Z}/9\mathbb{Z}, (\mathbb{Z}/3\mathbb{Z})^2$	2
10	$\mathbb{Z}/10\mathbb{Z}, D_5$	2

Développements

— Théorème de Burnside.
— Théorème de structure des groupes abéliens finis.
— Table de caractères de $\mathcal{S}_4$.

Références

[1] F. Combes, Algèbre et géométrie, Bréal.

[2] J. Delcourt, Théorie des groupes, Dunod.

[3] G. Rauch, Les groupes finis et leurs représentations, Ellipses.

[4] A. Szpirglas et al., Algèbre L3, Pearson.