104

Groupes finis. Exemples et applications.

On suppose connues les notions de groupe, sous-groupes, morphisme de groupes, sous-groupes distingués et actions de groupe.

I. FINITUDE D'UN GROUPE

a) Ordre

[Per] 1

Def 1 : Un groupe G est dit fini si son cardinal est fini. On appelle alors ordre de G son cardinal.

Exemple 2 : $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe fini d'ordre n.

Def 3 : Soit g un élément de G.
L'ordre de g est le plus petit entier $n>0$ qui vérifie $g^n = 1$.
C'est aussi l'ordre du sous-groupe engendré par $\{g\}$.

Def 4 : Soit G/H l'ensemble des classes à gauche de G relativement à un sous-groupe H.
On note $(G:H)$ et on appelle indice de H dans G le cardinal de G/H.

Thm 5 : [Lagrange]
Soient G un groupe fini, H un sous-groupe de G.
Alors $|G| = |H|\,(G:H)$.
En particulier, l'ordre de H et l'indice de H dans G divisent l'ordre de G.

Corollaire 6 : L'ordre d'un élément de G divise l'ordre de G.

Rem 7 : En général, un groupe n'admet pas nécessairement de sous-groupe d'ordre tout diviseur de n. Par exemple, $|A_4| = 12$, mais A_4 n'a pas de sous-groupe d'ordre 6.

[Gou] 1

Application 8 : [Petit théorème de Fermat]
Soit p un nombre premier, a nombre premier à p. Alors $a^{p-1} \equiv 1 \bmod p$.

[Per] 1

Prop 9 : Soit $f : G \to G'$ un morphisme de groupes.
Si G est fini, alors $|G| = |\mathrm{Ker}\, f| \cdot |\mathrm{Im}\, f|$.

Application 10 : Il y a $\frac{p-1}{2}$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$, pour p premier impair.

[Ber] 1

Def 10.1 : On appelle exposant de G, noté $\exp(G)$, le plus petit entier $n>0$ tel que $\forall x \in G,\ x^n = 1$.

Prop 10.2 : L'exposant de G est égal au ppcm des ordres de ses éléments, pour G fini.

Prop 10.3 : Soit G de lien fini. Il existe un élément dont l'ordre est l'exposant de G.

b) Actions de groupes

On suppose que G agit sur un ensemble X. Pour tout $x \in X$, on note $\mathrm{Stab}(x)$ le stabilisateur de x, et $\mathrm{Orb}(x)$ son orbite.

[Per] [Gou] 1

Propᵗᴵᵒⁿ 11 : $\phi_x : G/\mathrm{Stab}(x) \longrightarrow \mathrm{Orb}(x)$ est une bijection.
En particulier, si G est fini, $|\mathrm{Orb}(x)| = \dfrac{|G|}{|\mathrm{Stab}(x)|}$, pour tout $x \in X$.

Thm 12 : [équation aux classes]
Si X est fini, alors $|X| = \sum_{x \in R} |\mathrm{Orb}(x)| = \sum_{x \in R} \dfrac{|G|}{|\mathrm{Stab}(x)|}$,
où R est un système de représentants des orbites.

Exemple 13 : Si G agit sur lui-même par conjugaison, on a
$|G| = |Z(G)| + \sum_{x \in R \setminus Z(G)} \dfrac{|G|}{|\mathrm{Stab}(x)|}$,
où $Z(G)$ est le centre de G, défini par $Z(G) = \{g \in G \mid \forall x \in G,\ gx = xg\}$.

Définition 14 : On appelle p-groupe tout groupe de cardinal p^α où $\alpha \in \mathbb{N}^*$.

Application 15 : Le centre d'un p-groupe n'est pas trivial.

Application 16 : [Cauchy]
Soient $n \in \mathbb{N}^*$, p diviseur premier de n.
Tout groupe fini d'ordre n contient un élément d'ordre p.

Thm 17 : [formule de Burnside]
Soit G un groupe fini agissant sur X un ensemble fini.
Pour tout $g \in G$, on note $\mathrm{Fix}_x(g) = \{x \in X \mid g.x = x\}$ l'ensemble des éléments de X fixés par g. Alors le nombre d'orbites de cette action est $\dfrac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_x(g)|$.

Application 18 : Soit G de cardinal n.
La probabilité pour que 2 éléments de G, tirés de manière équiprobable et indépendante, commutent vaut $\frac{k}{n}$,
où k est le nombre de classes de conjugaison de G.

II - GROUPES ABÉLIENS FINIS

a) Groupes cycliques

[Rom] **Def 19 :** 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.

Exemple 20 : Le groupe des racines n^e de l'unité $U_n = \{\exp(2ik\pi/n) : 0 \leq k < n\}$.

Thm 21 : Tout groupe cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Prop 22 : Si $G = \langle g \rangle$ est cyclique d'ordre n, ses générateurs sont les $\{g^k\}$, où k est un entier compris entre 1 et $n-1$, premier avec n.

Def 23 : On appelle fonction indicatrice d'Euler la fonction $\varphi : n \in \mathbb{N}^* \mapsto |(\mathbb{Z}/n\mathbb{Z})^\times|$.

Exemple 24 : Si p est premier, $\varphi(p) = p-1$.

Prop 25 : $\varphi(n)$ est le nombre de générateurs d'un groupe cyclique d'ordre n.

Exemple 26 : Les générateurs de $\mathbb{Z}/6\mathbb{Z}$ sont $\bar{1}$ et $\bar{5}$.

Proposition 27 : On a $n = \sum_{d|n} \varphi(d)$.

Prop 28 : Soit G cyclique d'ordre n, engendré par g.
Pour tout diviseur positif d de n, il existe un unique sous-groupe H de G, d'ordre d. De plus, il est cyclique et engendré par $g^{\frac{n}{d}}$.

Rem 29 : C'est une condition nécessaire et suffisante pour être cyclique.

Thm 30 : Un groupe de cardinal premier est cyclique.

Thm 31 : Si $n \geq 2$ est premier avec $\varphi(n)$, alors tout groupe abélien d'ordre n est cyclique.

Exemple 32 : Tout groupe abélien d'ordre 15 est cyclique.

[Ben] **Thm 33 :** Le groupe multiplicatif d'un corps fini est cyclique.

b) Décomposition des groupes abéliens finis

[Rom] **Thm 34 :** [Lester chinois]
Soient $n, m \in \mathbb{N}^*$, premiers entre eux. Alors $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

[IP] **Def 35 :** Un caractère d'un groupe G est un morphisme de groupes de G dans $\mathbb{C}^\times$.

Lemme 36 : Soient G un groupe abélien fini, H un sous-groupe de G.
Tout caractère $\chi : H \to \mathbb{C}^\times$ peut se prolonger en un caractère de G.

Théorème 37 : [de structure des groupes abéliens finis]
Soit G un groupe abélien fini non trivial,
Il existe un unique $r \geq 1$ et des uniques entiers $n_1, \dots, n_r \geq 2$ tels que $n_i | n_{i-1}$ $\forall i \geq 2$, et tels que $G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$.

Exemple 38 : Tout groupe abélien d'ordre 60 est isomorphe à $\mathbb{Z}/60\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$.

Application 39 : Tout groupe d'ordre p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou $(\mathbb{Z}/p\mathbb{Z})^2$.

c) Dualité

[SS] [Rey] **Lemme 40 :** L'ensemble des caractères de G forme un groupe $\hat{G}$, le groupe dual de G.

Exemple 41 : Sur $\mathbb{Z}/n\mathbb{Z}$, les caractères sont $e_\ell : k \mapsto e^{\frac{2i\pi k\ell}{n}}$, pour $0 \leq \ell \leq n-1$.
On a un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et $\hat{\mathbb{Z}/n\mathbb{Z}}$.

Prop 42 : Soit G un groupe abélien fini. Alors $G \simeq \hat{G}$.

Def 43 : On note $\mathbb{C}[G]$ l'ensemble des fonctions de G dans $\mathbb{C}$. C'est un $\mathbb{C}$-espace vectoriel de dimension $|G|$. On le munit du produit hermitien :
$\forall (f, g) \in \mathbb{C}[G]^2$, $\langle f, g \rangle := \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}$.

Prop 44 : Soit G un groupe abélien fini. $\hat{G}$ est une famille orthonormale d'éléments

Prop 45 : Soit G un groupe abélien fini. $\hat{G}$ est une base orthonormale de $\mathbb{C}[G]$.

Def 46 : Pour $f \in \mathbb{C}[G]$, on définit pour $\chi \in \hat{G}$ le coefficient de Fourier de f par rapport à χ par $c_f(\chi) = \langle f, \chi \rangle$.

DÉVELOPPEMENT 1

[SS] [Rey]
Def 47 : On définit la transformée de Fourier par $\mathcal{F} : \begin{cases} \mathbb{C}[G] \to \mathbb{C}[\hat{G}] \\ f \mapsto \hat{f} \end{cases}$ où $\forall \chi \in \hat{G}$, $\hat{f}(\chi) := |G| \, c_f(\bar{\chi}) = \sum_{x \in G} f(x) \chi(x)$.

Prop 48 : [Formule d'inversion]
Pour $f \in \mathbb{C}[G]$, on a $f = \sum_{\chi \in \hat{G}} c_f(\chi) \chi = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi) \bar{\chi}$.

Prop 49 : [Formule de Parseval-Plancherel]
Pour $f \in \mathbb{C}[G]$, $\|f\|^2 = \sum_{\chi \in \hat{G}} |c_f(\chi)|^2$.

[IP] **Application 50 :** Transformée de Fourier rapide pour la multiplication d'entiers.

III - GROUPES NON ABÉLIENS FINIS

a) Groupes symétriques

[Rom]

Def 51 : Le groupe des bijections de $\{1, \dots, n\}$ sur lui-même est appelé groupe des permutations d'ordre n, noté S_n.

Def 52 : Soit $r \in [\![2, n]\!]$. On appelle cycle de longueur r toute permutation $\sigma \in S_n$ telle que $\begin{cases} \forall k \in \{1, \dots, r-1\}, \ \sigma(x_k) = x_{k+1} \\ \sigma(x_r) = x_1 \\ \forall k > r, \ \sigma(x_k) = x_k \end{cases}$.
Un 2-cycle est appelé une transposition.

Rem 53 : S_n est de cardinal $n!$. Il est non-abélien pour $n \geq 2$.

Thm 54 : Toute permutation $\sigma \in S_n \setminus \{Id\}$ se décompose en produit de cycles à support disjoint. Cette décomposition est unique à l'ordre près.

Thm 55 : S_n est engendré par :
- les transpositions ;
- les transpositions $(1, k)$ où $k \in \{2, \dots, n\}$;
- les transpositions $(k, k+1)$ où $k \in \{1, \dots, n-1\}$;
- $(1, 2)$ et $(1, 2, \dots, n)$.

Def 56 : On appelle signature de $\sigma \in S_n$, noté $\varepsilon(\sigma)$, le nombre
$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Prop 57 : L'application signature $\varepsilon : S_n \to \{\pm 1\}$ est un morphisme de groupes, surjectif pour $n \geq 2$. $\sigma \mapsto \varepsilon(\sigma)$

Def 58 : Le noyau du morphisme signature est distingué, d'indice 2 pour $n \geq 2$. [Ulm]
Il est appelé groupe alterné, noté A_n.

Prop 59 : A_n est engendré par les 3-cycles, pour $n \geq 3$.

Thm 60 : A_n est un groupe simple (sans sous-groupe distingué strict) pour $n \geq 5$. DEV 2

b) Groupe des isométries

Def 61 : On appelle n^e groupe diédral le groupe D_{2n} des isométries du plan laissant invariant l'ensemble des sommets du polygone régulier à n côtés, défini par $P_n = \{(\cos\frac{2k\pi}{n}, \sin\frac{2k\pi}{n}) \mid 0 \leq k \leq n-1\}$. [Gou]

Prop 62 : D_{2n} est un groupe d'ordre $2n$, non abélien pour $n \geq 2$.

Prop 63 : D_{2n} est engendré par une symétrie axiale s et la rotation r d'angle $\theta = \frac{2\pi}{n}$. [Ulm]

Prop 64 : D_{2n} est caractérisé comme étant engendré par un élément r d'ordre n, et un élément s d'ordre 2, tels que $rsrs = Id$.

Exemple 65 : S_3 est isomorphe à D_6. [Rom]

RÉFÉRENCES

[Ber] Berhuy, Algèbre : le grand combat
[Gou] Gourdon, Algèbre (Les maths en tête)
[IP] Isenmann, Pecatte, L'oral de l'agrégation de mathématiques
[Per] Perrin, Cours d'algèbre
[Rey] Peyré, L'algèbre discrète de la transformée de Fourier
[Rom] Romboldi, Mathématiques pour l'agrégation : algèbre et géométrie
[SS] Stein, Shakarchi, Fourier analysis : an introduction
[Ulm] Ulmer, Théorie des groupes