104. Groupes finis : Exemples et applications.

Refs : [Ulm] Ulmer, Théorie des groupes. [Cal1] Calais, Éléments de théorie des groupes
[Perr] Perrin, Cours d'Algèbre

Devts : Théorème de Sylow
Table de G_4
Groupes des isométries du tétraèdre.

I. Généralités sur les groupes finis

1) Ordre d'un groupe fini

Def 1 : On appelle ordre d'un groupe G le cardinal de l'ensemble sous-jacent, on le note $|G|$. Un groupe est dit fini quand son ordre est fini.

Ex 2 : Le groupe $\mathbb{Z}/n\mathbb{Z}$ est fini d'ordre n

Def 3 : On appelle ordre d'un élément d'un groupe l'ordre de son sous groupe engendré.

Ex 4 : $\bar{3} \in \mathbb{Z}/6\mathbb{Z}$ est d'ordre 2.

Def 5 : Si tous les éléments de G sont d'ordre fini, on définit l'exposant de G comme le ppcm des l'ordres de ses éléments.

Ex 6 : Un groupe fini d'exposant 2 est abélien, $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ est un groupe infini d'exposant 2.

[FGA1] Théo 7 (Burnside). Tout sous groupe d'exposant fini de $Gl_n(\mathbb{C})$ est lui même fini.

Expl $Gl_n(\mathbb{F}_p)$ + ordre

[Ulm] 24.25 Def 8 : Soit G un groupe et $H \subseteq G$ un sous groupe. On appelle Indice de H dans G, noté $[G:H]$, le cardinal de l'ensemble quotient G/H.

Théo 9 (Formule de Lagrange) Soit G un groupe fini et $H \subseteq G$ un sous groupe. On a $|G| = |H|[G:H]$.

Cor 10 : (Lagrange) Avec les notations précédentes, $|H| \mid |G|$

Ex 11 : Tout groupe d'ordre premier est abélien et cyclique.

2) Action de groupe

[Ulm] 27.29 Def 12 : Soit G un groupe et X un ensemble non vide, une action de G sur X est la donnée d'un morphisme de groupes $G \to \mathfrak{S}(X)$ où $\mathfrak{S}(X)$ désigne le groupes des bijections $X \to X$.

On fixe G un groupe fini et X un ensemble non vide

[Ulm] 27.30 Prop 13 : La donnée d'une action de G sur X équivaut à la donnée d'une application $A : G \times X \to X$ respectant

$$A(g, A(g', x)) = A(gg', x) \quad \forall g, g' \in G, x \in X$$
$$A(1, x) = x \quad \forall x \in X.$$

On notera $g.x = A(g, x)$.

Ex 14 : G agit sur lui même par translation : $g.g' := gg'$ et par conjugaison $g.g' = gg'g^{-1}$.

On fixe à présent une action de G sur X.

Def 15 : Soit $x \in X$, on appelle orbite de x sous l'action de G l'ensemble $O_G(x) = \{g.x \mid g \in G\}$. On appelle stabilisateur de x, sous l'action de G l'ensemble $G_x = \{g \in G \mid g.x = x\}$. L'action de G sur X est dite transitive si elle admet une seule orbite.

[Cal1] 183 Prop 16 : Les orbites sous l'action de G forment une partition de X, quand celui-ci est fini, on a

$$|X| = \sum_{x \in C} |O_G(x)|$$

où C est un ensemble de représentants des orbites.

Théo 17 : Pour X fini et $x \in X$, on a $[G:G_x] = |O_G(x)|$, d'où

$$|X| = \sum_{x \in C} [G:G_x]$$

avec les notation de la proposition précédente.

Théo 18 : (Formule de Burnside) En posant, pour $g \in G$, $X_g := \{x \in X \mid g.x = x\}$ on obtient que le nombre d'orbites sous l'action de G est donnée par

$$\frac{1}{|G|} \sum_{g \in G} |X_g|$$

3) Cas des p-groupes, Théorèmes de Sylow

[Perr] 16.17 Lemme 19 : Soit G un p-groupe opérant sur un ensemble X et soit X^G l'ensemble des points fixes sous l'action de G :

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

on a alors $|X| \equiv |X^G| \, [p]$

Théo 20 : Le centre d'un p-groupe est non trivial.

Cor 21 (Cauchy) Si $|G|$ est divisible par p, alors G admet un élément d'ordre p.

[Per] 18-19

Def 22 : Soit p premier divisant $|G|$, on pose $|G| = p^\alpha m$ avec $p \nmid m$. On appelle p-sous groupe de Sylow (ou p-Sylow) de G un sous groupe d'ordre p^α. On note $Syl_p(G)$ l'ensemble des p-Sylow de G.

Théo 23) (Sylow) Soit G un groupe fini et p divisant $|G|$:
(a) $Syl_p G$ est non vide.
(b) Si $H \leq G$ est un p-groupe et $S \in Syl_p(G)$, alors il existe $a \in G$ tel que $H \subseteq aSa^{-1}$. En particulier deux p-Sylow de G sont conjugués.
(c) On a $|Syl_p(G)| \equiv 1 [p]$, ...

Cor 24 : Un p-Sylow de G est unique si et seulement si il est distingué.

Ex 25 : Un groupe d'ordre 35 est cyclique.
Un groupe d'ordre 200 n'est pas simple

II. Groupes abéliens finis

1) Groupes cycliques.

[Cal1]

Def 26 : Un groupe fini G est dit cyclique si il est engendré par un de ses éléments.

Prop 27 : Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$: Deux groupes cycliques sont isomorphes si et seulement si ils ont même ordre.

Prop 28 : Si G est cyclique d'ordre n, alors tous sous groupe de G est cyclique. et G admet un unique sous groupe d'ordre d si et seulement si $d \mid n$.

Cor 29 : Un groupe cyclique est simple si et seulement si il est d'ordre premier.

Cor 30 : Pour p premier, tout groupe d'ordre p^2 est abélien

Théo 31. (Restes chinois) Soient $n, m \in \mathbb{N}$, on a
$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z}$$
si et seulement si n et m sont premiers entre eux.

2) Théorème de structure.

[Ulm] 106

Def 32 : Soit G abélien, on définit G_{tors} comme l'ensemble des éléments d'ordre fini de G, il s'agit d'un sous groupe de G.

Lem 33 : Soit G abélien de type fini, on a G fini si et seulement si $G = G_{tors}$

[Ulm] 106, 110

Théo 34 : Tout groupe abélien fini est isomorphe à un produit de groupes cycliques
$$\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z}$$
où k est un entier naturel et m_i des entiers non nuls tels que $m_i \mid m_{i+1}$ pour $i<k$. Ceux-ci sont uniques et appelés les invariants du groupe.

Théo 35 : Soit G un p-groupe abélien. Il existe une unique suite $r_1 \leq \dots \leq r_k$ avec $k \in \mathbb{N}^*$ telle que
$$G \simeq \mathbb{Z}/p^{r_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_k}\mathbb{Z}.$$

Cor 36 : Un groupe abélien fini G d'ordre n, alors G admet un sous groupe d'ordre d pour tout d divisant n.

III. Groupes finis remarquables.

1) Groupe symétrique, groupe alterné.

Def 37 : Soit X un ensemble fini, la classe d'isomorphie du groupe $\mathfrak{S}(X)$ dépend uniquement du cardinal de X, on note donc $\mathfrak{S}_n$ le groupe des bijections d'un ensemble de cardinal $n \in \mathbb{N}$.

[Ulm] 41-46

Théo 38 (Cayley) Tout groupe fini d'ordre n est isomorphe à un sous groupe de $\mathfrak{S}_n$

Def : Soient $1 \leq l \in \mathbb{N}$ et $i_1, \dots, i_l$ des éléments distincts de $[\![1, n]\!]$, la permutation $\gamma \in \mathfrak{S}_n$ définie par
$$\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1, \dots, i_l\} \\ i_{k+1} & \text{si } j = i_k \text{ avec } k<l \\ i_1 & \text{si } j = i_l \end{cases}$$
est notée $(i_1, \dots, i_l)$ et est appelée cycle de longueur l. Un cycle de longueur 2 sera appelé une transposition.

Théo 39 : Tout élément de $\mathfrak{S}_n$ se décompose comme produit de cycles à support disjoint, cette décomposition est unique à permutation des facteurs près.

Prop 40 : Deux éléments de $\mathfrak{S}_n$ sont conjugués si et seulement si les cycles disjoints apparaissant dans leur décomposition sont de même longueur.

[Ulm] 49-53

Def 41 Soit $\sigma \in \mathfrak{S}_n$, on appelle signature de $\sigma \in \mathfrak{S}_n$, notée $\varepsilon(\sigma)$, le nombre
$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Prop 42 : L'application $\varepsilon : \mathfrak{S}_n \longrightarrow \{\pm 1\}$ est un morphisme de groupes, on note $\mathfrak{A}_n$ son noyau, le groupe alterné, distingué et d'indice 2 dans $\mathfrak{S}_n$.

Prop 43 : Soit $n \geq 3$
- Le groupe symétrique $\mathfrak{S}_n$ est engendré par les transpositions $(1, i)$ avec $i \in [\![2, n]\!]$
- Le groupe alterné $\mathfrak{A}_n$ est engendré par les 3-cycles $(1, i, j)$ avec $i \neq j \in [\![2, n]\!]$. (en particulier, $\mathfrak{A}_n$ est engendré par les 3-cycles de $\mathfrak{S}_n$).

Théo 44 : Pour $n \geq 5$, on a   Def simple
- $\mathfrak{A}_n$ est simple
- $\mathfrak{A}_n$ est le seul sous groupe normal de $\mathfrak{S}_n$.

2) Isométries et groupe diédraux.

[Cal1] 120 126 DVP

Def 45 : Soit E un $\mathbb{R}$-espace affine euclidien, et $X \neq \emptyset$ une partie de E. On appelle $Isom(X)$ le sous groupe du groupe affine préservant X : il s'agit du stabilisateur de X sous l'action du groupe affine.

Ex 46 : Si K est le cube unité de $\mathbb{R}^3$, alors $Isom(K) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$. Si T est le tétraèdre régulier, alors $Isom(T) \simeq \mathfrak{S}_4$.

Def 46 : Si $P_n \subseteq \mathbb{R}^2$ est un polygone régulier à n côtés, on note $D_n = Isom(P_n)$ le n-ème groupe diédral.

Prop 47 : Le groupe D_n est d'ordre $2n$, et agit sur les sommets de P_n.

Théo 48 : Le groupe D_n est isomorphe au produit semi direct non trivial $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

IV. Représentations des groupes finis.

[Ulm] 143 153.

On fixe G un groupe fini d'ordre n

Def 49 : On définit l'algèbre de groupe de G par
$$\mathbb{C}G := \left\{ \sum_{g \in G} a_g g \mid g \in G \right\}$$

Une représentation (linéaire) de G est un $\mathbb{C}G$-module.

Prop 50 : La donnée d'une représentation de G est équivalente à celle d'un $\mathbb{C}$-espace vectoriel V, muni d'un morphisme $G \rightarrow GL(V)$.

On étudiera seulement le cas où V est de dimension finie sur $\mathbb{C}$.

Ex 51 : Le morphisme trivial $G \rightarrow GL_1(\mathbb{C})$ est appelé représentation triviale

Par le théorème de Cayley, on peut plonger G dans $\mathfrak{S}_n$, et $\mathfrak{S}_n$ dans $GL_n(\mathbb{C})$ en faisant agir $\mathfrak{S}_n$ par permutations ; c'est la représentation par permutation $\mathbb{C}G$ vu comme $\mathbb{C}G$ module est la représentation régulière.

Prop 52 : Si V est un $\mathbb{C}G$-module et $f : V \rightarrow V$ une application $\mathbb{C}$-linéaire, f induit un morphisme de $\mathbb{C}G$-modules par
$$\tilde{f}(v) = \frac{1}{|G|} \sum_{g \in G} g f(g^{-1} \cdot v).$$

Théo 53 (Maschke) Soit V un $\mathbb{C}G$-module et $W \leq V$ un sous-$\mathbb{C}G$-module, alors W admet un supplémentaire dans V.

Def 54 : Soit V un $\mathbb{C}G$-module, la composition du morphisme $G \rightarrow GL(V)$ par la trace est une application constante sur les classes de conjugaisons de G, appelée caractère du $\mathbb{C}G$-module V, noté χ_V.

Théo 55 : On appelle caractère irréductible le caractère associé à un $\mathbb{C}G$-module simple :
- Il y a autant de caractères irréductibles que de classes de conjugaisons de G.
- La formule $\langle \phi, \psi \rangle = |G|^{-1} \sum_{g \in G} \overline{\phi(g)} \psi(g)$ définit un produit scalaire sur le $\mathbb{C}$-espace vectoriel des fonctions centrales, pour lequel les caractères irréductibles forment une base orthonormée
- χ est irréductible si et seulement si $\langle \chi, \chi \rangle = 1$ si l'un est de degré 1
- le produit de deux caractères irréductible est encore un caractère irréductible.
- Si $\{C_1 \dots C_s\}$ sont les classes de conjugaisons de G, et $Irr(G) = \{\chi_1 \dots \chi_s\}$ les caractères irréductibles de G, alors
$$\sum_{\chi \in Irr(G)} \chi(C_i) \overline{\chi(C_j)} = \delta_{ij} \frac{|G|}{|C_i|}$$

Appl 56 : Table de caractères de $\mathfrak{S}_4$ (cf Annexe).

DVP

Annexe :

	1	$(12)(34)$	(12)	(123)	(1234)
$\mathbb{1}$	1	1	1	1	1
χ_ε	1	1	-1	1	-1
χ_1	2	2	0	-1	0
χ_2	3	-1	1	0	-1
χ_3	3	-1	-1	0	1