# 104 Groupes finis. Exemples et applications.

## I - Outils d'étude de groupes finis

Soit $G$ un groupe.

### 1. Ordre d'un groupe, ordre d'un élément

**Définition 1. L'ordre** du groupe $G$, noté $|G|$ est le cardinal de l'ensemble sous-jacent $G$. Si $G$ est fini de cardinal $n$, on dit que $G$ est **d'ordre** $n$. Sinon, on dit que $G$ est **d'ordre infini**. [ULM21] p. 1

**Exemple 2.** Les multiplicatifs des corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont d'ordre infini.

**Définition 3.** On appelle **ordre** d'un élément $g \in G$, l'ordre du sous-groupe $\langle g \rangle$ qu'il engendre. p. 6

**Exemple 4.** L'élément $i$ est d'ordre 4 dans $\mathbb{C}^*$.

**Proposition 5.** Soit $g \in G$ d'ordre $n$. Alors,

(i) $n$ est le plus petit entier strictement positif ayant la propriété $g^n = e_G$.

(ii) $\langle g \rangle = \{e_G, g, \dots, g^{n-1}\}$.

(iii) Pour $k \in \mathbb{Z}$, $g^k = e_G$ si et seulement si $n \mid k$.

**Exemple 6.** Pour $n \in \mathbb{Z}$, on a $\langle n \rangle = \{nk \mid k \in \mathbb{Z}\}$ et on note ce groupe $n\mathbb{Z}$.

**Théorème 7.** Soit $g \in G$. Alors, p. 18

(i) $g$ est d'ordre infini si et seulement si $\langle g \rangle$ est isomorphe à $(\mathbb{Z}, +)$. Dans ce cas $g^i \neq g^j$ dès que $i \neq j$ et $\langle g \rangle = \{\dots, g^{-1}, e_G, g, \dots\}$.

(ii) $g$ est d'ordre fini si et seulement si $g, \dots, g^{n-1}$ sont tous distincts et si $g^n = e_G$.

**Théorème 8** (Lagrange)**.** On suppose $G$ fini. Soit $H < G$. Alors, p. 25

$$|H| \mid |G|$$

En particulier, l'ordre d'un élément de $G$ divise toujours l'ordre de $G$.

## 2. Groupes cycliques

**Définition 9.** On dit que $G$ est **cyclique** s'il est engendré par un seul élément. p. 6

**Proposition 10.** Un groupe fini d'ordre premier est cyclique. p. 26

**Théorème 11.** On suppose $G$ fini d'ordre $n$. Alors,

(i) Si $G$ est abélien et s'il existe au plus un sous-groupe d'ordre $d$ pour tout diviseur $d$ de $n$, alors $G$ est cyclique.

(ii) Si $G$ est cyclique, tous ses sous-groupes le sont aussi.

(iii) $G$ est cyclique si et seulement si pour tout diviseur $d$ de $n$, $G$ admet exactement un sous-groupe d'ordre $d$.

**Théorème 12.** Tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique. **[ROM21]** p. 25

**Corollaire 13.** L'ensemble des racines $n$-ièmes de l'unité d'un corps est un sous-groupe cyclique de son groupe multiplicatif.

## 3. Actions de groupes

Soit $X$ un ensemble.

**[ULM21]** p. 29

**Définition 14.** On appelle **action** (à gauche) de $G$ sur $X$ toute application

$$\begin{array}{ccc} G \times X & \to & X \\ (g,x) & \mapsto & g \cdot x \end{array}$$

satisfaisant les conditions suivantes :

(i) $\forall g,h \in G, \forall x \in X, g \cdot (h \cdot x) = (gh) \cdot x$.

(ii) $\forall x \in X, e_G \cdot x = x$.

*Remarque* 15. On peut de même définir une action à droite de $G$ sur $X$.

**Définition 16.** On définit pour tout $x \in X$ :

— $G \cdot x = \{g \cdot x \mid g \in G\} \subseteq X$ l'**orbite de** $x$.

— $\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\} < G$ le **stabilisateur de** $x$.

On suppose ici que $G$ et $X$ sont finis.

**Proposition 17.** Soit $x \in X$. Alors :
- $|G \cdot x| = (G : \mathrm{Stab}_G(x))$.
- $|G| = |\mathrm{Stab}_G(x)||G \cdot x|$.
- $|G \cdot x| = \frac{|G|}{|\mathrm{Stab}_G(x)|}$

p. 71

**Théorème 18** (Formule des classes)**.** Soit $\Omega$ un système de représentants des orbites de l'action de $G$ sur $X$. Alors,

$$|X| = \sum_{\omega \in \Omega} |G \cdot \omega| = \sum_{\omega \in \Omega} (G : \mathrm{Stab}_G(\omega)) = \sum_{\omega \in \Omega} \frac{|G|}{|\mathrm{Stab}_G(\omega)|}$$

**Définition 19.** On définit :
- $X^G = \{x \in X \mid \forall g \in G, g \cdot x = x\}$ l'ensemble des points de $X$ laissés fixes par tous les éléments de $G$.
- $X^g = \{x \in X \mid g \cdot x = x\}$ l'ensemble des points de $X$ laissés fixes par $g \in G$.

**Corollaire 20** (Formule de Burnside)**.** Le nombre $r$ d'orbites de $X$ sous l'action de $G$ est donné par

$$r = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

**Corollaire 21.** Soit $p$ un nombre premier. Si $G$ est un $p$-groupe (ie. l'ordre de $G$ est une puissance de $p$), alors,

$$|X^G| \equiv |X| \mod p$$

où $X^G$ désigne l'ensemble des points fixes de $X$ sous l'action de $G$.

**Corollaire 22.** Soit $p$ un nombre premier. Le centre d'un $p$-groupe non trivial est non trivial.

**Corollaire 23.** Soit $p$ un nombre premier. Un groupe d'ordre $p^2$ est toujours abélien.

**Application 24** (Théorème de Cauchy)**.** On suppose $G$ non trivial et fini. Soit $p$ un premier divisant l'ordre de $G$. Alors il existe un élément d'ordre $p$ dans $G$.

[DEV]

**Application 25** (Premier théorème de Sylow)**.** On suppose $G$ fini d'ordre $np^\alpha$ avec $n, \alpha \in \mathbb{N}$ et $p$ premier tel que $p \nmid n$. Alors, il existe un sous-groupe de $G$ d'ordre $p^\alpha$.

[GOU21] p. 44

# II - Groupes abéliens finis

## 1. Un exemple fondamental : $\mathbb{Z}/n\mathbb{Z}$

**Proposition 26.** $n\mathbb{Z}$ est un sous-groupe distingué de $(\mathbb{Z},+)$, si bien que l'on peut définir le quotient $\mathbb{Z}/n\mathbb{Z}$. [ULM21] p. 45

**Proposition 27.** $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre $n$.

**Proposition 28.** On peut définir une structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$. Le groupe multiplicatif de cet anneau est alors d'ordre $\varphi(n)$.

**Corollaire 29.** $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si $p$ est premier.

**Proposition 30.** Dans le cas du Théorème 7 Point (ii), $\langle g\rangle$ est alors isomorphe à $\mathbb{Z}/n\mathbb{Z}$. [ROM21] p. 14

**Exemple 31.**

$$\mu_n \cong \mathbb{Z}/n\mathbb{Z}$$

où $\mu_n$ désigne le groupe cyclique des racines de l'unité de $\mathbb{C}^*$.

## 2. Décomposition cyclique

**Théorème 32** (Chinois)**.** Soient $n$ et $m$ deux entiers premiers entre eux. Alors, [ULM21] p. 81

$$\mathbb{Z}/nm\mathbb{Z} \equiv \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

**Théorème 33** (Kronecker)**.** Soit $G$ un groupe abélien d'ordre $n \geq 2$. Il existe une suite d'entiers $n_1 \geq 2$, $n_2$ multiple de $n_1$, …, $n_k$ multiple de $n_{k-1}$ telle que $G$ est isomorphe au groupe produit p. 112

$$\prod_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}$$

**Exemple 34.** Soit $G = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$. Alors,

$$\begin{aligned} G &\cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \\ &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \end{aligned}$$

# III - Groupes non abéliens finis

Les groupes qui suivent sont, sauf cas particuliers, des groupes non abéliens.

## 1. Groupes symétrique et alterné

**Définition 35.** L'ensemble des permutations de $[\![1,n]\!]$ est un groupe pour la composition des applications : c'est le **groupe symétrique**, noté $S_n$.

p. 55

*Remarque* 36. $S_n$ est fini, d'ordre $n!$.

**Théorème 37** (Cayley)**.** Tout groupe fini d'ordre $n$ est isomorphe à un sous-groupe de $S_n$.

**Définition 38.** Soient $l \in \mathbb{N}^*$ et $i_1, \dots, i_l \in [\![1,n]\!]$ des éléments distincts. La permutation $\gamma \in S_n$ définie par

$$\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1, \dots, i_l\} \\ i_{k+1} & \text{si } j = i_k \text{ avec } k < l \\ i_1 & \text{si } j = i_l \end{cases}$$

et notée $\begin{pmatrix} i_1 & \dots & i_l \end{pmatrix}$ est appelée **cycle** de longueur $l$ et de **support** $\{i_1, \dots, i_l\}$. Un cycle de longueur 2 est une **transposition**.

**Exemple 39.** $\gamma = \begin{pmatrix} 1 & 4 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 4 & 2 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 5 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 1 & 4 & 2 \end{pmatrix}$ est un cycle de $S_5$ de longueur 4.

**Théorème 40.** Toute permutation de $S_n$ s'écrit de manière unique (à l'ordre près) comme produit de cycles dont les supports sont deux à deux disjoints.

**Exemple 41.**

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 3 & 5 \end{pmatrix}$$

**Définition 42.** On appelle **type** d'une permutation $\sigma \in S_n$ et on note $[l_1, \dots, l_m]$ la liste des cardinaux $l_i$ des orbites dans $[\![1,n]\!]$ de l'action du groupe $\langle \sigma \rangle$ sur $[\![1,n]\!]$, rangée dans l'ordre croissant.

**Proposition 43.** Une permutation de type $[l_1, \dots, l_m]$ a pour ordre $\text{ppcm}(l_1, \dots, l_m)$.

**Exemple 44.** La permutation de l'Exemple 41 est d'ordre 6.

**Définition 45.**
— Soit $\sigma \in S_n$. On appelle **signature** de $\sigma$, notée $\epsilon(\sigma)$ l'entier $\epsilon(\sigma) = \prod_{i\neq j} \frac{\sigma(i)-\sigma(j)}{i-j}$.
— $\sigma \mapsto \epsilon(\sigma)$ est un morphisme de $S_n$ dans $\{\pm 1\}$, on note $A_n$ son noyau.

**Lemme 46.** Les 3-cycles sont conjugués dans $A_n$ pour $n \geq 5$. **[PER]** p. 15

**Lemme 47.** Le produit de deux transpositions est un produit de 3-cycles. **[ROM21]** p. 49

**Proposition 48.** $A_n$ est engendré par les 3-cycles pour $n \geq 3$.

[DEV]

**Théorème 49.** $A_n$ est simple pour $n \geq 5$. **[PER]** p. 28

## 2. Groupe linéaire sur un corps fini

Soit $V$ un espace vectoriel de dimension finie $n$ sur un corps $\mathbb{K}$.

**[ULM21]** p. 119

**Définition 50.**
— Le **groupe linéaire** de $V$, $\mathrm{GL}(V)$ est le groupe des applications linéaires de $V$ dans lui-même qui sont inversibles.
— Le **groupe spécial linéaire** de $V$, $\mathrm{SL}(V)$ est le sous-groupe de $\mathrm{GL}(V)$ constitué des applications de déterminant 1.
— Les quotients de ces groupes par leur centre sont respectivement notés $\mathrm{PGL}(V)$ et $\mathrm{PSL}(V)$.

**Proposition 51.** On se place dans le cas où $\mathbb{K} = \mathbb{F}_q$. Alors, les groupes précédents sont finis, et : p. 124

(i) $|\mathrm{GL}(V)| = q^{\frac{n(n-1)}{2}}((q^n-1)\dots(q-1))$.
(ii) $|\mathrm{PGL}(V)| = |\mathrm{SL}(V)| = \frac{|\mathrm{GL}(V)|}{q-1}$.
(iii) $|\mathrm{PSL}(V)| = |\mathrm{SL}(V)| = \frac{|\mathrm{GL}(V)|}{(q-1)\,\mathrm{pgcd}(n,q-1)}$.

### 3. Groupe diédral

**Définition 52.** Pour un entier $n \geq 1$, le **groupe diédral** $D_n$ est le sous-groupe, de $\mathrm{GL}_2(\mathbb{R})$ engendré par la symétrie axiale $s$ et la rotation d'angle $\theta = \frac{2\pi}{n}$ définies respectivement par les matrices

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ et } R = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

p. 8

**Exemple 53.** $D_1 = \{\mathrm{id}, s\}$.

**Proposition 54.** (i) $D_n$ est un groupe d'ordre $2n$.
(ii) $r^n = s^2 = \mathrm{id}$ et $sr = r^{-1}s$.

**Proposition 55.** Un groupe non cyclique d'ordre 4 est isomorphe à $D_2$.

p. 28

**Exemple 56.** $S_2$ est isomorphe à $D_2$.

p. 65

**Proposition 57.** Un groupe fini d'ordre $2p$ avec $p$ premier est soit cyclique, soit isomorphe à $D_p$.

p. 28

**Exemple 58.** $S_3$ est isomorphe à $D_3$.

**Proposition 59.** Les sous-groupes de $D_n$ sont soit cyclique, soit isomorphes à un $D_m$ où $m \mid n$.

p. 47

## IV - Représentations linéaires de groupes finis

Dans cette partie, $G$ désigne un groupe d'ordre fini.

p. 144

**Définition 60.** — Une **représentation linéaire** $\rho$ est un morphisme de $G$ dans $\mathrm{GL}(V)$ où $V$ désigne un espace-vectoriel de dimension finie $n$ sur $\mathbb{C}$.

— On dit que $n$ est le **degré** de $\rho$.

— On dit que $\rho$ est **irréductible** si $V \neq \{0\}$ et si aucun sous-espace vectoriel de $V$ n'est stable par $\rho(g)$ pour tout $g \in G$, hormis $\{0\}$ et $V$.

**Exemple 61.** Soit $\varphi : G \to S_n$ le morphisme structurel d'une action de $G$ sur un ensemble de cardinal $n$. On obtient une représentation de $G$ sur $\mathbb{C}^n = \{e_1, \dots, e_n\}$ en posant

$$\rho(g)(e_i) = e_{\varphi(g)(i)}$$

c'est la représentation par permutations de $G$ associé à l'action. Elle est de degré $n$.

**Définition 62.** La représentation par permutations de $G$ associée à l'action par translation à gauche de $G$ sur lui-même est la **représentation régulière** de $G$, on la note $\rho_G$.

**Définition 63.** On peut associer à toute représentation linéaire $\rho$, son **caractère** $\chi = \text{trace} \circ \rho$. On dit que $\chi$ est **irréductible** si $\rho$ est irréductible.

p. 150

**Proposition 64.** (i) Les caractères sont des fonctions constantes sur les classes de conjugaison.

(ii) Il y a autant de caractères irréductibles que de classes de conjugaisons.

**Définition 65.** Soit $\rho : G \to \text{GL}(V)$ une représentation linéaire de $G$. On suppose $V = W \oplus W_0$ avec $W$ et $W_0$ stables par $\rho(g)$ pour tout $g \in G$. On dit alors que $\rho$ est **somme directe** de $\rho_W$ et de $\rho_{W_0}$.

**Théorème 66** (Maschke)**.** Toute représentation linéaire de $G$ est somme directe de représentations irréductibles.

**Théorème 67.** Les sous-groupes distingués de $G$ sont exactement les

$$\bigcap_{i \in I} \text{Ker}(\rho_i) \text{ où } I \in \mathscr{P}(\llbracket 1, r \rrbracket)$$

**[PEY]** p. 231

**Corollaire 68.** $G$ est simple si et seulement si $\forall i \neq 1, \forall g \neq e_G, \chi_i(g) \neq \chi_i(e_G)$.

# Bibliographie


**Les maths en tête** **[GOU21]**

Xavier GOURDON. *Les maths en tête. Algèbre et probabilités*. 3e éd. Ellipses, 13 juill. 2021.
https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html.

**Cours d'algèbre** **[PER]**

Daniel PERRIN. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.
https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html.

**L'algèbre discrète de la transformée de Fourier** **[PEY]**

Gabriel PEYRÉ. *L'algèbre discrète de la transformée de Fourier. Niveau M1*. Ellipses, 15 jan. 2004.
https://adtf-livre.github.io.

**Mathématiques pour l'agrégation** **[ROM21]**

Jean-Étienne ROMBALDI. *Mathématiques pour l'agrégation. Algèbre et géométrie*. 2e éd. De Boeck Supérieur, 20 avr. 2021.
https://www.deboecksuperieur.com/ouvrage/9782807332201-mathematiques-pour-l-agregation-algebre-et-geometrie.

**Théorie des groupes** **[ULM21]**

Felix ULMER. *Théorie des groupes. Cours et exercices*. 2e éd. Ellipses, 3 août 2021.
https://www.editions-ellipses.fr/accueil/13760-25304-theorie-des-groupes-2e-edition-9782340057241.html.