# 104 — Groupes abéliens et non abéliens finis. Exemples et applications.

Soit $G$ un groupe fini d'ordre $n \in \mathbb{N}^*$.

## I) Outils pratiques pour l'étude des groupes

### A] Ordre d'un élément

[1]

**Def 1 :** Soit $g \in G$. On appelle ordre de $g$ l'unique entier $p>0$, s'il existe, tel que $g^p = 1$ et $g^k \neq 1$ $\forall k \in [1;p[$

**Ex 2 :** Tout élément de $\mathbb{Z}/p\mathbb{Z}$, $p$ premier, distincts de $\bar{0}$ est d'ordre $p$.

**Prop 3 :** $\theta(g) = \mathrm{Card}(g^k \mid k \in \mathbb{N})$ est fini et est l'ordre de $g$. En particulier, tout élément de $G$ admet un ordre.

**Prop 4 :** Soit $k \in \mathbb{Z}$. $g^k = 1 \iff k \in \theta(g)\mathbb{Z}$.

**Def 5 :** Soit $H$ un sous-groupe de $G$. On définit la relation d'équivalence de congruence (à gauche) modulo $H$ par : $x R y \iff \exists h \in H,\ y = hx$. On note $G/H$ le quotient.

**Thm 6 :** (de Lagrange) $|H| \mid |G|$.

**Cor 7 :** L'ordre de tout élément de $G$ divise $n$.

**Thm 8 :** Soit $k \in \mathbb{Z}^*$, et soit $g \in G$. Alors $\theta(g^k) = \dfrac{\theta(g)}{\theta(g) \wedge k}$

### B] Action de groupe

[2]

**Def 9 :** Soit $X$ un ensemble. Une action de $G$ sur $X$ est la donnée d'un morphisme de groupe de $G$ dans les bijections de $X$. Elle est dite fidèle si ce morphisme est injectif.

**Rem 10 :** Cette notion est très utile pour avoir des informations sur $G$.

**Ex 11 :** $\begin{array}{l} G \times G \to G \\ (g,h) \mapsto gh \end{array}$ est une action dite par translation à gauche de $G$ sur lui-même.

**Thm 12 :** (de Cayley) $G \hookrightarrow S_n$ le groupe symétrique.

**Ex 13 :** $\begin{array}{l} G \times G \to G \\ (g,h) \mapsto ghg^{-1} \end{array}$ est une action de $G$ sur $G$ dite par automorphisme intérieur.

Si $\varphi$ est une action sur $X$, on notera $\varphi(g)(x) = g \cdot x$

[2]

**Def 14 :** On appelle orbite de $x \in X$ : $Gx = \{g \cdot x \mid g \in G\}$. L'action est dite transitive s'il n'y a qu'une seule orbite. On appelle stabilisateur de $x$ : $\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = g\}$.

**Thm 15 :** $Gx$ et $G/\mathrm{Stab}(x)$ sont en bijection pour tout $x \in X$. On suppose maintenant $X$ fini.

**Cor 16 :** (Formule des classes) Soit $R$ une famille de représentants des orbites de $X$ sous l'action de $G$. Alors $\mathrm{Card}(X) = \sum_{x \in R} \dfrac{|G|}{|\mathrm{Stab}(x)|}$

### C] Applications aux p-groupes et aux théorèmes de Sylow

[2]

**Def 17 :** Soit $p$ un nombre premier. $G$ est un $p$-groupe si $n$ est une puissance de $p$.

**Prop 18 :** Posons $X^G = \{x \in X \mid g \cdot x = x\ \forall g \in G\}$ et supposons que $G$ soit un $p$-groupe. Alors $\mathrm{Card}\, X^G \equiv \mathrm{Card}\, X\ [p]$

**App 19 :** Le centre d'un $p$-groupe non trivial est non trivial.

**Cor 20 :** Tout groupe d'ordre $p^2$ est abélien.

**Def 21 :** Si $n = p^\alpha m$, $\alpha \neq 0$, avec $p \nmid m$. On appelle $p$-Sylow de $G$ tout sous-groupe $H$ d'ordre $p^\alpha$.

**Thm 22 :** (de Sylow) Si $p \mid n$, $G$ admet au moins un $p$-Sylow. De plus, tous les $p$-Sylow de $G$ sont conjugués et si on note $n_p$ leur nombre, on a $n_p \mid m$ et $n_p \equiv 1\ [p]$

[2] **Cor 23 :** Si $p | n$, $G$ admet des sous-groupes d'ordre $p^i$ pour $0 \leq i \leq \alpha$ où $n = p^\alpha m$ avec $p \nmid m$.

**Cor 24 :** (Théorème de Cauchy) Si $p | n$, $G$ admet un élément d'ordre $p$.

**App 25 :** Un groupe d'ordre 63 n'est jamais simple.

## II) Cas des groupes abéliens

### A] Groupes cycliques

**Def 26 :** $G$ est dit cyclique si $\exists g \in G \,/\, G = \langle g \rangle = \{g^k \mid k \in \mathbb{N}\}$

**Rem 27 :** Un groupe cyclique est en particulier abélien.

**Thm 28 :** Les groupes $\mathbb{Z}/n\mathbb{Z}$ sont les seuls groupes cycliques à isomorphisme près.

[1] **Prop 29 :** Si $G = \langle g \rangle$, les générateurs de $G$ sont les $g^k$ tels que $k \wedge n = 1$

**Thm 30 :** Si $n$ est premier, $G$ est cyclique.

**Thm 31 :** Si $G$ est cyclique, tout sous-groupe de $G$ est cyclique d'ordre divisant $n$. Réciproquement, si $d | n$, si $G = \langle g \rangle$, $H = \langle g^{\frac{n}{d}} \rangle$ est l'unique sous-groupe d'ordre $d$.

### B] Structure des groupes abéliens finis

On supposera ici que $G$ est abélien avec $n \geq 2$.

**Lem 32 :** Soit $a \in G$ d'ordre maximal $O(a)$. Pour tout $y \in G/\langle a \rangle$, il existe $x \in G$ tel que $O(x) = O(y)$ et $\bar{x} = y$

[3] **Thm 33 :** Il existe des uniques entiers $q_1 | q_2 | \dots | q_k$ tels que $G \simeq \prod_{i=1}^{k} \mathbb{Z}/q_i\mathbb{Z}$. Ces entiers sont appelés les invariants de $G$.

**Cor 34 :** Il existe un élément de $G$ d'ordre le PPCM de tous les ordres de $G$. [3]

**Cor 35 :** Pour tout diviseur $d | n$, il existe un sous-groupe de $G$ d'ordre $d$.

## III) Exemples remarquables de groupes

### A] Groupes symétriques, groupes alternés

**Def 36 :** On appelle $n$-ème groupe symétrique le groupe des bijections de $[\![1;n]\!]$ dans lui-même, noté $S_n$.

**Rem 37 :** Ce groupe n'est pas abélien dès que $n \geq 3$.

**Rem 38 :** $S_n$ agit naturellement sur $[\![1;n]\!]$.

**Thm 39 :** $|S_n| = n!$ [4]

**Def 40 :** Soit $\sigma \in S_n$. On appelle support de $\sigma$ : $\mathrm{Supp}(\sigma) = \{x \in [\![1;n]\!] \mid \sigma(x) \neq x\}$.
$\sigma$ est un $p$-cycle, $p \in [\![1;n]\!]$, si il existe $a_1, \dots, a_p$ 2 à 2 distincts dans $[\![1;n]\!]$ tels que $\mathrm{supp}(\sigma) = \{a_i \mid i \in [\![1;p]\!]\}$, $\sigma(a_i) = a_{i+1}$ $\forall i \in [\![1;p-1]\!]$ et $\sigma(a_p) = \sigma(a_1)$. On le note $\sigma = (a_1 \dots a_p)$. Si $p = 2$, on parle de transposition.

**Thm 41 :** Toute permutation de $S_n$ se décompose de façon unique en produit de cycles à support disjoints.

**Def 42 :** Le type d'une permutation est le vecteur de coordonnées les longueurs des cycles dans sa décomposition du Thm 41 classés par ordre croissant. [3]

**Cor 43 :** Deux permutations sont conjuguées si et seulement si elles ont même type.

**App 44 :** (Théorème de Brauer) Pour $\sigma \in S_n$, soit $P_\sigma \in GL_n(\mathbb{R})$ définie par : $\forall i \in [\![1;n]\!]$, $P_\sigma e_i = e_{\sigma(i)}$. Alors $\sigma$ et $\sigma' \in S_n$ sont conjuguées si et seulement si $P_\sigma$ et $P_{\sigma'}$ sont semblables.

[3] **Cor 45 :** Il y a autant de classes de conjugaisons dans $S_n$ que de façon d'écrire $n$ comme somme d'entiers naturels.

**Def 46 :** On définit la signature de $\sigma \in S_n$ par $\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j}$

[1] **Thm 47 :** C'est un morphisme de groupe. On note $A_n = \ker \varepsilon$ le groupe alterné. On a alors $|A_n| = \frac{n!}{2}$

**Thm 48 :** (DEV2) $A_n$ est simple pour $n \geq 5$.

## B] Groupes diédraux

**Def 49 :** Soit $P_n$ le polygone régulier à $n$ côtés. On appelle groupe diédral le groupe $D_n$ des isométries affines préservant $P_n$.

[4] **Rem 50 :** Une isométrie affine préserve $P_n$ si et seulement si elle préserve ses sommets.

**Thm 51 :** $D_n$ est un groupe fini d'ordre $2n$ engendré par un élément $r$ d'ordre $n$ et un élément $s$ d'ordre 2 tels que $rsr = s$

**App 52 :** $D_3 \simeq S_3$

# IV) Représentation d'un groupe fini

**Def 53 :** On appelle représentation de $G$ tout couple $(\rho, V)$ où $V$ est un $\mathbb{C}$-espace vectoriel et $\rho$ une action de $G$ sur $V$. Le caractère de cette représentation

[1] est $\chi_\rho : \begin{array}{l} G \to \mathbb{C} \\ g \mapsto \mathrm{Tr}(\rho(g)) \end{array}$

**Ex 54 :** Soit $V$ de base $(e_1, \dots, e_n)$ avec $n = |G|$. Alors $\rho : \begin{array}{l} G \to GL(V) \\ g \mapsto (e_h \mapsto e_{gh}) \end{array}$ est une représentation appelée représentation régulière de $G$.

**Def 55 :** Soient $(\rho, V)$ une représentation et $W$ un sous-espace de $V$. $W$ est dit $G$-invariant si $\forall g \in G$, $\rho(g)(W) \subset W$. $(\rho, V)$, ou $\chi_\rho$, est dit irréductible si $V$ n'admet pas de sous-espaces $G$-invariants autres que $\{1\}$ et $V$.

**Rem 56 :** Un sous-espace $G$-invariant $W$ induit une sous-représentation $(\rho, W)$.

**Thm 57 :** (de Maschke) $(\rho, V)$ se décompose en somme directe de sous-représentations irréductibles.

**Def 58 :** Soient $\chi_1$ et $\chi_2$ deux caractères. On définit $\langle \chi_1, \chi_2 \rangle = \frac{1}{n} \sum_{g \in G} \overline{\chi_1(g)} \chi_2(g)$

**Thm 59 :** Il y a exactement autant de caractères irréductibles de $G$ que de classes de conjugaisons. De plus, si $g_1, \dots, g_p$ sont des représentants des classes de conjugaison et $\chi_1, \dots, \chi_p$ les caractères irréductibles : [1]

$$\frac{1}{|G|} \sum_{k=1}^{p} \overline{\chi_k(g_i)} \chi_k(g_j) = \begin{cases} \frac{1}{\mathrm{Card}(g_i)} & \text{si } i = j \\ 0 & \text{sinon} \end{cases}$$

**Cor 60 :** Si $\chi$ est un caractère de $G$, il est irréductible si et seulement si $\langle \chi | \chi \rangle = 1$.

**Cor 61 :** (Formule de Burnside) Si $n_1, \dots, n_p$ sont les dimensions des caractères irréductibles, $n = \sum_{i=1}^{p} n_i^2$

**App 62 :** $G$ est abélien si et seulement si ses seuls caractères irréductibles sont de dimension 1.

**App 63 :** (DEV3) Compte tenu de ces formules, on peut construire la table de caractère de $S_4$ (Fig 1)

Fig 1 : Table de caractères de $S_4$

| | id | (1 2) | (1 2 3) | (1 2)(3 4) | (1 2 3 4) |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | -1 | 1 | 1 | -1 |
| $\chi_3$ | 3 | 1 | 0 | -1 | -1 |
| $\chi_4$ | 3 | -1 | 0 | -1 | 1 |
| $\chi_5$ | 2 | 0 | -1 | 2 | 0 |

Références :


- Algèbre et géométrie, Rombaldi [1]
- Cours d'algèbre, Perrin [2]
- Algèbre et géométrie, Combes [3]
- Cours de géométrie, Mercier [4]