# 104 - Groupes finis. Exemples et applications.

## 1 Généralités

### 1.1 Sous-groupes

**Théorème 1** (Lagrange)**.** *Si $H$ est un sous-groupe fini du groupe fini $G$, alors l'ordre de $H$ divise l'ordre de $G$. Plus précisément, on a : $|G| = |H|(G : H)$.*

*Application.* L'ordre d'un élément d'un groupe divise l'ordre du groupe. En particulier, un groupe d'ordre permier $p$ est cyclique.
Petit théorème de Fermat : Soit $p$ un nombre premier. Si $a \wedge p = 1$, alors $p|a^{p-1}$.

**Proposition 1.** *Exposant d'un groupe abélien fini.*

### 1.2 Actions de groupe et produit semi-direct

**Définition 1.**
- Un sous-groupe $H$ d'un groupe $G$ est dit *distingué* si pour tout $h \in H$ et $g \in G$, on a $ghg^{-1} \in H$. On note alors $H \triangleleft G$.
- $G/H$ est alors muni d'une structure de groupe, appelé *groupe quotient*. La surjection canonique $\pi : G \to G/H$ est de noyau $H$.
- Un groupe $G \neq \{1\}$ est dit *simple* si ses seuls sous-groupes distingués sont $\{1\}$ et $G$.
- On appelle *centre* de $G$ le sous-groupe $Z(G) = \{a \in G \mid \forall g \in G, ga = ag\}$. C'est un sous-groupe distingué (et même caractéristique) de $G$.
- On appelle *groupe dérivé* de $G$ le groupe $D(G)$ engendré par les commutateurs d'éléments de $G$. Il est distingué, et le quotient $G/D(G)$ est abélien.
- On dit qu'un groupe $G$ agit sur un ensemble $X$ si on s'est donné une application $G \times X \to X,\ (g, x) \mapsto g.x$ telle que :

  (i) $\forall g, g' \in G,\ \forall x \in X,\ g.(g'.x) = (gg').x$.

  (ii) $\forall x \in X,\ 1.x = x$.

  Il revient au même de se donner un morphisme $\varphi : G \to \mathfrak{S}(X)$.
- L'*orbite* de $x$ est $G.x = \{g.x \mid g \in G\}$, le *stabilisateur* de $x$ est $G_x = \{g \in G \mid g.x = x\}$.

*Exemple.* Exemples d'actions de groupes (cf leçon correspondante).

**Théorème 2** (Formule des classes)**.** *Soit $X$ un ensemble fini sur lequel $G$ agit. Pour tout $x \in X$, l'application $\overline{g} \mapsto g.x$ de $G/H.x$ dans $G.x$ est une bijection. On a alors pour $O$ un système de représentants d'orbites,*

$$|X| = \sum_{\overline{x} \in O} \frac{|G|}{|H_x|}$$

*Application.* Le centre d'un $p$-groupe non trivial est non trivial. Ainsi, un groupe d'ordre $p^2$, avec $p$ premier, est soit isomorphe à $\mathbf{Z}/p\mathbf{Z}$, soit isomorphe à $(\mathbf{Z}/p\mathbf{Z})^2$.

**Théorème 3** (Formule de Burnside)**.** *Soit $X$ un ensemble fini sur lequel $G$ agit. On note pour $g \in G$ $Fix(g) = \{x \in X \mid g.x = x\}$. Alors le nombre d'orbites de $X$ sous $G$ vaut $\frac{1}{|G|} \sum_{g \in G} |Fix(g)|$*

*Application.* Le colier de perles [Alessandri, Combes].

**Définition 2.** Si $G$ agit sur $H$ par automorphismes (i.e. $\varphi : G \to Aut(X)$), on définit le *produit semi-direct* $H \rtimes G$ comme l'ensemble $H \times G$ muni de la loi $(h, g)(h', g') = (h(g.h'), gg')$.

**Proposition 2.** *Soit $G$ un groupe et $H, K$ des sous-groupes de $G$ tq $H$ distingué dans $G$, $H \cap K = \{1\}$ et $HK = G$. Alors $G$ est isomorphe au produit semi-direct $H \rtimes K$, avec l'action $k.h = khk^{-1}$. De plus, lpsse :*

*(i)* $G \approx H \times K$

*(ii)* $K \lhd G$

*(iii)* *l'action $\varphi$ est triviale.*

### 1.3 $p$-groupes

**Définition 3.**

- Si $p$ est premier, on appelle *$p$-groupe* tout groupe de cardinal $p^n$, avec $n \in \mathbf{N}^*$.
- Si $G$ est un groupe fini, un *$p$ sous-groupe de Sylow* de $G$ est un sous-groupe $S$ de $G$ qui est un $p$-groupe tel que $(g : S) \wedge p = 1$.

**Théorème 4** (Sylow)**.** *Soit $G$ un groupe fini de cardinal $p^\alpha m$, avec $p$ premier et $m \wedge p = 1$. On note $N_p$ le nombre de $p$-Sylow de $G$. Alors :*

- *deux $p$-Sylow sont conjugués*
- *Tout sous $p$-groupe de $G$ est contenu dans un $p$-Sylow*
- *$N_p \equiv 1$ $[p]$ et $N_p | m$*
- *si $N_p = 1$, alors le $p$-Sylow de $G$ est distingué.*

**Proposition 3.** *Le centre d'un $p$-groupe est non-trivial, ainsi un $p$-groupe n'est pas simple. Un $p$-groupe possède des sous-groupes de tous les ordres possibles.*

*Application.* Applications à la simplicité.

## 2 Groupes abéliens

### Les groupes cycliques

**Proposition 4.** *Un groupe monogène fini est isomorphe à* $\mathbf{Z}/n\mathbf{Z}$*, avec* $n$ *l'ordre du groupe.*

**Théorème 5** (lemme chinois)**.** *Si* $m \wedge n = 1$*, alors on a un isomorphisme d'anneaux :* $\mathbf{Z}/mn\mathbf{Z} \simeq \mathbf{Z}/m\mathbf{R} \times \mathbf{Z}/n\mathbf{Z}$*.*

*Application.* Résolutions de systèmes d'équations de congruences.

**Théorème 6.** *Soit* $s \in \mathbf{Z}$*. Lpsse :*

*(i)* $s \wedge n = 1$

*(ii)* $s$ *est un générateur du groupe* $(\mathbf{Z}/n\mathbf{Z}, +)$

*(iii)* $s \in (\mathbf{Z}/n\mathbf{Z})^*$

**Proposition 5.** *On a l'isomorphisme :* $\begin{array}{rcl} \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) & \to & (\mathbf{Z}/n\mathbf{Z})^* \\ \phi & \mapsto & \phi(1) \end{array}$

**Théorème 7** (Structure de $(\mathbf{Z}/n\mathbf{Z})^*$)**.** *On décompose* $n$ *en facteurs premiers :* $n = \prod_i p_i^{\alpha_i}$*. Alors, par le lemme chinois,* $(\mathbf{Z}/n\mathbf{Z})^* \simeq \prod_i (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^*$*. De plus pour tout nombre premier impair* $p$ *et tout entier* $\alpha$ *on a :* $(\mathbf{Z}/p^\alpha\mathbf{Z})^* \simeq \mathbf{Z}/p^{\alpha-1}(p-1)\mathbf{Z}$*,* $(\mathbf{Z}/2\mathbf{Z})^* \simeq \{1\}$*,* $(\mathbf{Z}/4Z)^* \simeq \mathbf{Z}/2Z$ *et pour tout entier* $\alpha > 2$*,* $(\mathbf{Z}/2^\alpha\mathbf{Z})^* \simeq \mathbf{Z}/2^{\alpha-2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$

*Application.* Soit $G$ un groupe d'ordre $pq$, avec $p$ et $q$ premiers, $p < q$. Alors
- si $p \not| q-1$, alors $G \approx \mathbf{Z}/pq\mathbf{Z}$,
- si $p | q-1$, alors $G \approx \mathbf{Z}/pq\mathbf{Z}$ ou $G \approx \mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$.

*Exemple.* $(\mathbf{Z}/n\mathbf{Z})^*$ est cyclique ssi $n = 4$ ou $n = p^\alpha$ ou $n = 2p^\alpha$, avec $p$ nombre premier impair.

### Application : l'algorithme RSA

On se donne deux grands nombres premiers $p$ et $q$ tels que $n = pq$, et un entier $d$ inversible modulo $\varphi(n)$, appelé *clef publique*. Le chiffrement d'un message $a \in \mathbf{Z}/n\mathbf{Z}$ est donné par la fonction $f : \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z},\ a \mapsto a^d$, et le déchiffrement par l'inverse de $f$ : $g : a \mapsto a^e$, avec $e$ un inverse de $d$ dans $\mathbf{Z}/\varphi(n)\mathbf{Z}$, appelé *clef privée*. La robustesse de cet algorithme réside dans le fait que le calcul de $g$, i.e. celui de $e$, nécessite la connaissance de $\varphi(n)$, et donc de $p$ et de $q$. Or la factorisation de nombres tels que $n$ est en pratique extrêmement longue : le calcul de l'inverse est impossible en temps raisonnable.

**Décomposition des groupes abéliens**

**Théorème 8.** *Soit $G$ un groupe abélien fini. Il existe une unique suite d'entiers $a_1|a_2|\dots|a_n$, avec $a_1 > 1$ telle que $G \approx \mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_k\mathbf{Z}$.*

*Application.* Soit $G$ un groupe. On appelle *caractère* de $G$ tout homomorphisme de $G$ dans $\mathbf{C}^*$. Ceux-ci forment le groupe $\hat{G}$. Si $G$ est abélien fini, alors $G \approx \hat{G}$.

# 3 Exemples de groupes non abéliens

## 3.1 Groupe symétrique

**Théorème 9** (Cayley)**.** *Tout groupe d'ordre $n$ est isomorphe à un sous-groupe de $\mathfrak{S}_n$*

**Proposition 6.** *Toute permutation se décompose de manière unique en produit de cycles à supports disjoints (à l'ordre près des cycles).*
*Toute permutation se décompose en produit de transpositions.*

**Proposition 7.** *Il existe un unique morphisme non trivial de $\mathfrak{S}_n$ dans $\mathbf{C}^*$, appelé* signature *et noté $\varepsilon$. Il est à valeurs dans $\{-1, 1\}$ et on a :*

$$\varepsilon\sigma = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

**Définition 4.** Le noyau de la signature est le *groupe alterné*, noté $\mathfrak{A}_n$.

**Proposition 8.** *Si $n \geq 2$, alors $\mathfrak{A}_n$ est le seul groupe d'indice 2 de $\mathfrak{S}_n$.*
*Si $n \geq 3$, alors $\mathfrak{A}_n$ est engendré par les 3-cycles.*

**Théorème 10.** *Pour $n \geq 5$, $\mathfrak{A}_n$ est simple.*

**Corollaire 1.** *Pour $n \geq 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{1\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.*

## 3.2 Groupe diédral

**Définition 5.** Le groupe diédral d'ordre $2n$, noté $D_n$, est le groupe des isométries du plan conservant un polygone régulier à $n$ côtés.

**Proposition 9.** *$D_n$ est isomorphe au produit semi-direct $\mathbf{R}/n\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$, où l'action est donnée par l'inversion, i.e. $\varphi(1)$ est l'inversion.*

# 4 Groupes de petits ordres

**Sylow, props sur les $p$-gpes, les gpes d'ordre $pq$...**
Classification jusqu'à 15 (FG) !
Groupes simples jusqu'à 100, groupe d'ordre 60.