# Cours : Théorie des groupes (THGR)

Emily Clement

Licence de Mathématiques
Semestre 1
2014-2015

# Table des matières

# Introduction

Ce cours portera sur la théorie des groupes et se basera quasi-exclusivement sur mes notes du cours de Monsieur Sebag, professeur de mathématiques à la faculté de Rennes 1, mais ne respecte pas la structure interne des chapitres, et se basera également sur le livre de Daniel Perrin, et de quelques démonstrations et résultats que j'aurai ajoutées (polycopié anonyme sur les groupes diédraux, Travaux dirigés d'Axel Rogue,, démonstrations non faites en cours et laissé au lecteur) notamment sur les groupes quotients, cycliques et symétriques.
En espérant que les lecteurs de ce polycopié trouveront ici une lecture intéressante et claire...Pour la moindre coquille, ou suggestion, n'hésitez pas a m'en faire part.

# Chapitre 1

# Groupes et rappels

## I Définitions et propositions

**Définition 1.1** (Loi de composition interne sur un ensemble)**.**

Soit $E$ un ensemble, on appelle loi de composition interne sur $E$ toute application : $* : \quad E \times E \quad \rightarrow \quad E$ On rappelle que $E \times E = \{(x, y), x \in E, y \in E\}$.

**Définition 1.2.**

Un groupe $(G, *)$ est la donnée d'un ensemble **non vide** $G$ et $*$ une loi de composition interne de $G$ telle que :

- $*$ est associative
- $*$ possède un élément neutre $e$ :

$$\exists e \in G, \forall x \in G, x * e = e * x = x$$

- Tout élément de $G$ possède un élément symétrique :

$$\forall x \in G, \exists y \in G, x * y = y * x = e$$

On dit que le groupe $(G, *)$ est commutatif, ou abélien, si $*$ est commutative. L'ensemble $G$ est appelé l'ensemble sous-jacent du groupe.

On pourra avoir un élément dans un ensemble qui est le neutre à droite mais pas à gauche et généralement la question de cours classique sera la suivante :

**Exemple 1.3.** *Soit $E$ un ensemble muni d'une loi $*$ associative telle que :*

- $\forall x \in E, e * x = x$

— *Tout élément possède un inverse/symétrique à gauche.*

*Montrer que* $(G, *)$ *est un groupe.*

**Propriétés 1.4** (Propriété d'un groupe)**.**

Soit $(G, *)$ un groupe, $e$ son élément neutre.
- $e$ est unique et est son propre symétrique.
- Tout élément possède un unique symétrique. (On parlera donc du symétrique...)
- Si $x'$ est le symétrique de $x$, alors $x$ est le symétrique de $x'$.

*Démonstration.*

1. Supposons qu'un tel élément $e'$ existe. Unicité :

$$\underbrace{e * e'}_{=e} = e'$$

Symétrique :

$$e * e = e$$

2. Soit $x \in G$, soient $y, z$ deux symétriques.

$$(y * x) * z = y * (x * z)$$
$$e * z = y * e$$
$$z = y$$

Le reste des démonstrations n'a que peu d'intérêt.

□

**Définition 1.5.**

Soit $(G, *)$ un groupe, on dit que le groupe est fini si $G$ l'est. On appelle Card $G$ l'ordre du groupe, on le note $\mathrm{o}(G)$ ou $|G|$.
On observera que $\mathrm{o}(G) \geq 1$ pour tout groupe $(G, *)$

**Définition 1.6** (Image homomorphisme)**.**

Un groupe $G'$ est dit image homomorphe du groupe $G$ s'il existe un morphisme de groupe surjectif $f : G \to G'$

On ne rappellera pas les propriétés connues sur les groupes en général, afin de mettre l'accent sur la notion de quotient.

# II Premiers exemples de groupes.

## 1 $\mathbb{Z}/n\mathbb{Z}$

**Définition 1.7.**

On note $\mathbb{Z}/n\mathbb{Z}$ le quotient de $\mathbb{Z}$ par la relation d'équivalence $\mathcal{R}$ suivante, définie sur $\mathbb{Z}$ par :

$$x\mathcal{R}y \Leftrightarrow x - y \in n\mathbb{Z}$$

$$\mathbb{Z}/n\mathbb{Z} \stackrel{\text{def}}{=} \left\{ \underbrace{\overline{x}}_{\text{classe d'équivalence de } x}, x \in \mathbb{Z} \right\}$$

$\mathbb{Z}/n\mathbb{Z}$ est muni de la loi de groupe, commutative :

$$* : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ \left(\overline{x}, \overline{y}\right) & \mapsto & x \stackrel{-}{+} y \end{array}$$

**Pour affirmer que c'est une application**, il faut penser à vérifier l'indépendance vis à vis des choix.

## 2 Groupe symétrique

**Définition 1.8.**

Pour tout ensemble $E$, on note $S_E$ l'ensemble des bijections de $E$ dans $E$. Un élément de $S_E$ est appelé permutation de $E$.

**Proposition 1.9.**

Pour tout ensemble $E$, $(S_E, \circ)$ est un groupe.

*Démonstration.* Tout ensemble admet une bijection qui envoie chaque élément sur lui-même, notée $Id$. Donc $S_E$ est non-vide.

La composition est bien une loi de composition interne, car la composée de applications bijections l'est également.

La composition est associative.

$Id$ st bien un élément neutre pour la loi $\circ$ : Soit $f \in S_E$. Pour tout $x \in E$, $f \circ Id(x) = Id \circ f(x) = f(x)$. Donc $f \circ Id = Id \circ f = f$.

Enfin, tout $f \in S_E$ admet une application réciproque $f^{-1}$, définie comme : Pour tout $x \in E$, on pose $f^{-1}(x)$ comme l'unique élément $y$ tel que $f(y) = x$. Donc $f \circ f^{-1} = f^{-1}/circf = Id$. □

# III Sous-groupes

## 1 Brefs rappels

On rappellera quelques outils, mais les démonstrations seront souvent laissées au lecteur :

**Propriétés 1.10** (Bref rappels)**.**

1. Un groupe $G \neq \{e\}$ possède au moins deux sous-groupes : $G, (e_G)$.
2. $H \leq G$ est sous-groupe propre de $G$ si $H \neq G$, on le notera $H < G$.
3. Soit $H$ une sous-partie non vide de $G$,
$$H \leq G \Leftrightarrow \forall x, y \in G, x, y \in H \Rightarrow x^{-1}y \in H.$$
4. (Notation additive)
$$H \leq G \Leftrightarrow \forall x, y \in G, x, y \in H \Rightarrow x - y \in H.$$
5. Soit $G$ un groupe et $(H_i)_{i \in I}$ une famille de sous-groupes ($I \neq \varnothing$), alors $\bigcap_{i \in I} H_i$ est un sous-groupe.
6. Cette propriété n'est pas vraie pour l'union : contre exemple facile avec $3\mathbb{Z}$ et $8\mathbb{Z}$

**Lemme 1.11** (Sous-groupes de $n\mathbb{Z}$.)**.**

Les sous-groupes de $(\mathbb{Z}, +)$ sont les sous-ensembles de la forme $n\mathbb{Z}$, $n \geq 0$

*Démonstration.*
Résumé de la démonstration : une inclusion triviale et une non-triviale, traitons celle-ci.
Soit $H$ un sous-groupe de $(\mathbb{Z}, +)$ Soit $H = (0) = 0\mathbb{Z}$, soit $H \neq (0)$. $\exists x \in H, x \neq 0$, donc $H$ contient un élément non nul de $\mathbb{N}$, $\Gamma = H \bigcap \mathbb{N} \neq 0$, partie de $\mathbb{N}$ donc contient un plus petit élément, non nul, qu'on note $n$.

Pour montrer que $H = n\mathbb{Z}$, alors, on a déjà $n\mathbb{Z} \subset H$ (stabilité par $+$ ).
Soit $x \in H$, [Division euclidienne] :

$$\exists\,(q,r) \in \mathbb{Z} \times [\![0, n-1]\!], x = qn + r$$

$r = x - nq \in H$ (stabilité), comme $n$ est minimal, on ne peut pas avoir $r$ non nul, donc $r = 0$. $x \in n\mathbb{Z}$. □

**Exemple 1.12** (Exemples de sous-groupes)**.**

1. $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$
2. $(\mathbb{Q}^*, \times) < (\mathbb{R}^*, \times) < (\mathbb{C}, \times)$
3. $(U, \times) \overset{def}{=} (\{z \in \mathbb{C}, |z| = 1\}, \times) < (\mathbb{C}^*, \times)$
4. $(U_n, \times) \overset{def}{=} (\{z \in \mathbb{C}, z^n = 1\}, \times) < (\mathbb{C}^*, \times)$
5. $(GL(E), \circ) < (S_E, \times)$
6. $(\mathcal{Z}(G), \times) \overset{def}{=} (\{x \in G, xa = ax, \forall a \in G\}, \times) < (G, \times)$ *est un sous-groupe abélien.*

## 2 Sous-groupes engendrés par une partie

**Définition 1.13.**

Soit $G$ un groupe, $S$ une sous partie, non vide, de $G$.
$\mathcal{H}_S$ est l'ensemble des sous-groupes de $G$ contenant $S$, et on appelle sous-groupe engendrée par $S$ le sous-groupe :

$$\langle S \rangle \overset{\text{def}}{=} \bigcap_{H \in \mathcal{H}_S} H$$

On a la propriété suivante (additive/mutiplicative) :

**Propriétés 1.14** (Propriétés et quelques définitions)**.**

Soit $S$ une partie non vide d'un groupe $G$.

1. (additive)
   $\langle S\rangle = \left\{\sum_{i=0}^{n} x_i, n \in \mathbb{N}, \forall i \in [\![1,n]\!], x_i \in S| \text{ ou } -x_i \in S\right\}$
2. (multiplicative)
   $\langle S\rangle = \{\prod_{i=0}^{n} x_1.\ldots.x_n, n \in \mathbb{N}, \forall i \in [\![1,n]\!], x_i \in S| \text{ ou } x_i^{-1} \in S\}$
3. $\langle x\rangle \overset{\text{def}}{=} \{x^n, n \in \mathbb{Z}\}$
4. Si $\langle S\rangle = G$, $S$ est une partie génératrice de $G$, c'est un ensemble de générateur de $G$ et engendre $G$.
5. Si de plus $S = \{x\}$, on dit que $\langle x\rangle$ est monogène.
6. Si il existe $S \neq \varnothing$ et finie telle que $S$ engendre $G$, on dira que $G$ est de type fini.
   Attention on peut être de type fini sans être fini !
   Exemple : $\mathbb{Z} =< 1 >$ n'est pas fini.

**Définition 1.15** (Groupe cyclique)**.**

On appelle groupe cyclique tout groupe monogène et fini.

**Définition 1.16** (Ordre d'un élément)**.**

Soit $G$ un groupe et $x \in G$.

1. Si l'ensemble sous-jacent au groupe $\langle x\rangle$ est infini, on dit que $x$ est d'ordre infini.
2. Sinon, on dit que $x$ est d'ordre fini, le cardinal de $\langle x\rangle$ est appelé ordre de $x$, $\mathrm{o}(x)$.

**Exemple 1.17.**

1. *Soit $G$ un groupe, le seul élément d'ordre 1 est l'élément neutre.*
2. *Cas : $(\mathbb{Z}, +)$, tout élément non nul est d'ordre infini.*
3. *Cas groupes et sous-groupes de $S_3$ :*
   $e = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ $\tau_1 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ $\tau_2 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$
   $\tau_3 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ $\sigma_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ $\sigma_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ $S_3 = \{e, \tau_1, \tau_2, \tau_3, \sigma_1, \sigma_2\}$
   *on a* $\langle\sigma_1\rangle = \{e, \sigma_1, \sigma_2\}$

**Remarque 1.18** (Notation)**.**
*Soient $X, Y$ deux sous-ensembles non vides d'un groupe $G$.*

$$XY \overset{def}{=} \{xy \in G, x \in X, y \in Y\}.$$

*Exemple :*

1. $X = \{x\}$ $Y = G$, $XY = G$
2. $X = G = Y$, *alors* $GG = G^2 = G$

*Dans le cas général, $XY$ n'est pas nécessairement un sous-groupe de $G$.*

**Proposition 1.19.**

Soient $H, K$ tels que $H \leq G$, $K \leq G$.
$HK$ est un sous-groupe de G $\Leftrightarrow$ $HK = KH$ dans $G$.

*Démonstration.*
Premier sens : Supposons que $HK \leq G$. Soit $x \in H, y \in K$, $yx \in KH$, montrons que $yx \in HK$. Or

$$yx = \left(x^{-1}y^{-1}\right)^{-1}$$

$H$ et $K$ sont des sous-groupes, donc $x^{-1} \in H, y^{-1} \in K$ , donc $x^{-1}y^{-1} \in HK$, comme $HK$ est un sous-groupe de $G$ donc $yx = \left(x^{-1}y^{-1}\right)^{-1} \in HK$.
Montrons que $KH \subset HK$.
Soit $z \in HK$, $z^{-1} \in HK$, $\exists x \in H, y \in K, z^{-1} = xy$, d'où $x = y^{-1}x^{-1} \in KH$ (propriété des sous-groupes).
Deuxième sens : $e \in H, K$, donc $e = ee \in HK \neq \varnothing$
Soient $s, t \in HK$, il faudra montrer que $st^{-1} \in HK$ (utiliser les définition et les inverses) . □

**Exemple 1.20** (Cas d'une famille libre de sous-groupes)**.** *À faire...*

**Proposition 1.21** (Rappels)**.**

Soit $f \in \mathrm{Hom}(G, G')$, où $G, G'$ sont deux groupes. $f$ vérifie les propriétés suivantes :

1. $f(e) = e'$
2. $\forall x \in G, f\left(x^{-1}\right) = f(x)^{-1}$
3. $f(x^n) = f(x)^n, \forall n \in \mathbb{Z}$.
4. $H \leq G \Rightarrow f(H) \leq G'$
5. $H' \leq G' \Rightarrow f^{-1}(H') \leq G$
6. L'ensemble $f(G)$ est un sous-groupe de $G'$ appelé image de $G$, $\mathrm{Im}f$, on la note $\mathrm{Im}f$.
7. $\mathrm{Ker}\, f \leq G$, $\ker f \overset{\text{def}}{=} f^{-1}(e')$

# IV Isomorphisme et théorème de Cayley

## 1 Quelques rappels et propositions sur les isomorphismes et propriétés universelles.

**Définition 1.22.**

S'il existe un isomorphisme du groupe $G$ dans le groupe $G'$, on dit que les groupes $G$ et $G'$ sont isomorphes. Notation $G \simeq G'$.

**Propriétés 1.23.**

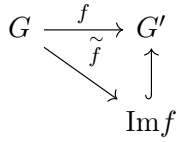
1. En général 2 groupes isomorphes ne sont pas rendus isomorphes par un unique isomorphisme de groupes.
2. $\simeq$ vérifie les axiomes d'une relations d'équivalence.
3. Les ensembles sous-jacents $G$ et $G'$ sont équipotents. En particulier deux groupes **finis** ont même cardinal.
4. 2 groupes sont isomorphes implique que les propriétés des deux structures sont les mêmes (corps, etc)
5. Toute bijection d'ensemble entre les ensembles sous-jacents à deux groupes isomorphes n'est pas nécessairement un isomorphisme.

**Exemple 1.24** (Exemple classique)**.** *$\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes.*

**Proposition 1.25** (Propriété universelle)**.**

Si $f \in \mathrm{Hom}\,(G, G')$ est injectif alors $G = \mathrm{Im} f$ et :




**Exemple 1.26.**

1. *Soit $G$ un groupe, $Aut\,(G) \leq S_G$*
   *En d'autres termes : le groupe des automorphismes de $G$ forme un sous-groupe du groupe des permutations de $G$.*
2. *Soit $E$ un $\mathbb{R}-$espace vectoriel, tel que $dim_{\mathbb{R}} E = n$, soit $\mathcal{B} = \{e_1, \ldots, e_n\}$ une base de $E$.*
   $$\begin{array}{ccc} GL\,(E) & \to & GL_n\,(\mathbb{R}) \\ f & \mapsto & Mat\,(f, \mathcal{B}) \end{array}$$
   *est un isomorphisme de groupes.*
3. *Automorphisme intérieur : Soit $G$ un groupe, $g \in G$,*
   $$\mathcal{O}_g : \begin{array}{ccc} G & \to & G \\ x & \mapsto & gxg^{-1} \end{array} \in Aut\,(G)$$
   *L'ensemble des automorphismes intérieur de $G$ :*
   $$Int\,(G) \overset{def}{=} \{f \in Aut\,(G)\,, \exists g \in G, f = \mathcal{O}_g\}$$
   *(l'ensemble des automorphisme de la forme $\mathcal{O}_g$)*
   $$Int\,(G) \leq Aut\,(G)$$

**Lemme 1.27.**

Soit $E, E'$ deux ensembles non vides, alors : Si $E, E'$ sont équipotents, alors $\mathrm{S}_E, \mathrm{S}_{E'}$ sont isomorphes.

Application : Si $|E| = n < +\infty$, alors $\mathrm{S}_E \simeq \mathrm{S}_n = \mathrm{S}_{\{1,\ldots,n\}}$ Et à présent on identifiera le groupe symétrique d'un ensemble fini $E$ et $\mathrm{S}_{|E|}$.

*Démonstration.*
Par hypothèse, il existe $f : E \to E'$ bijective.
Construisons un isomorphisme $\mathrm{S}_E \to \mathrm{S}_{E'}$ . Considérons : $\phi : \sigma \to f \circ \sigma \circ f^{-1}$ qui est un isomorphisme (le vérifier). Soit $\tau \in \mathrm{S}_E$, posons $\sigma \overset{\text{def}}{=} f^{-1} \circ \tau \circ f$, et on peut vérifier que $\phi(\sigma) = \tau$ □

## 2 Translation à gauche et théorème de Cayley.

**Définition 1.28** (Translation à gauche)**.**

Soit $G$ un groupe, et $g \in G$, on appelle translation à gauche par $g$ l'application d'ensemble définie par :

$$\mathrm{T}_g : \begin{array}{ccc} G & \to & G \\ x & \mapsto & gx \end{array}$$

On note $\mathrm{T}_G$ l'ensemble des translation à gauche de $G$. C'est un groupe comme le montre la propriété suivante.

**Propriétés 1.29.**

Cette application a les propriétés suivantes :

1. $\mathrm{T}_G \neq \varnothing$
2. Toute translation à gauche est une bijection : $\mathrm{T}_G \subseteq \mathrm{S}_G$, on a même $\mathrm{T}_G \leq \mathrm{S}_G$.
3. $G \simeq \mathrm{T}_G$.

*Démonstration.*

1. $\mathrm{T}_e = \mathrm{id}_G \in \mathrm{T}_G$
2. Montrons l'injectivité, puis la surjectivité et enfin le morphisme.
   Soient $x, y \in G$ tels que $\mathrm{T}_g(x) = \mathrm{T}_g(y)$. donc

   $$gx = gy$$

   Par composition à gauche par $g^{-1}$ ($G$ est un groupe) on en déduit que

   $$x = y.$$

   Soit $y \in G$, posons $x \overset{\text{def}}{=} g^{-1}g$, alors $\mathrm{T}_g(x) = y$.

Morphisme : soient $g_1, g_2 \in G$, soit $x \in G$,

$$\begin{aligned} \mathrm{T}_{g_1} \circ \mathrm{T}_{g_2}(x) &= g_1 g_2 x \\ &= (g_1 g_2)\, x \\ &= \mathrm{T}_{g_1 g_2}(x) \end{aligned}$$

On a donc que :

$$(\mathrm{T}_g)^{-1} = \mathrm{T}_{g^{-1}}$$

3. Il faut considérer l'application : $\phi : \begin{array}{ccc} G & \to & \mathrm{T}_G \\ g & \mapsto & \mathrm{T}_g \end{array} \in \mathrm{Hom}(G, \mathrm{T}_G)$. Il faut montrer que c'est un morphisme, et $\phi$ est bijective, le montrer en montrant que $\mathrm{Ker}\,\phi = e_G : g \in \mathrm{Ker}\,\phi$

$$\phi(g) = \mathrm{Id}_G = E_{\mathrm{S}_G}$$

Le surjectivité se déduit de la définition.

□

**Théorème 1.30** (Théorème de Cayley)**.**

Tout groupe $G$ est isomorphe à un sous-groupe de son groupe de permutations, $\mathrm{S}_G$.

*Démonstration.*
Soit $G$ un groupe et $g \in G$, on définit l'application suivante :

$$\mathrm{t}_g : \begin{array}{ccc} G & \to & G \\ \mathrm{t}_g(x) & \mapsto & gx \end{array}$$

On sait que cette application est une permutation, ce qui permet de définit une application t de $G$ dans $\mathrm{S}(G)$ par : $\forall g \in G, \mathrm{t}(g) = \mathrm{t}_g$.
t est un morphisme de groupe, son noyau est le groupe $\{e\}$. t est un isomorphisme de $G$ dans Imt qui est donc un sous groupe de $\mathrm{S}(G)$. □

# Chapitre 2

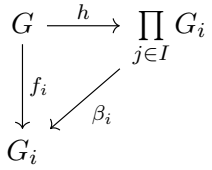
# Produit direct et semi-direct de groupes

## I Généralités et but

Soit $(G_i)_{i\in I}$ une famille de groupes, $I \neq \varnothing$. On va construire le groupe $\prod_{i\in I} G_i$ muni de la propriété universelle suivante :

1. $\forall i \in I$, il existe un morphisme de groupe $\beta_i : \prod_{j\in I} G_i \to G_i$ .
2. Soit $G$ un groupe quelconque, soit une famille $(f_i)_{i\in I}$ de morphisme de groupes, où $\forall i \in I, f_i \in \mathrm{Hom}\,(G, G_i)$.

   Alors il existe un unique morphisme de groupe $h \in \mathrm{Hom}\left(G, \prod_{j\in I} G_i\right)$ rendant commutatif (i.e tels que $f_i = \beta_i \circ h$ ) les diagrammes : $\forall i \in I$ :



# II Cas du produit direct de deux groupes

**Définition 2.1.**

Soit $G_1, G_2$ deux groupes, et on pose $G = G_1 \times G_2$. (produit cartésien), muni de la loi de compositions interne : $*$ : $\begin{array}{ccc} G \times G & \to & G \\ ((x_1, y_1), (x_2, y_2)) & \mapsto & (x_1 x_2, y_1 y_2) \end{array}$ $(G, *)$ forme un groupe. (la démonstration est facile.) On appelle le groupe $(G, *)$ produit direct des groupes $G_1$ et $G_2$.

**Remarque 2.2** (Notations)**.** *On associe à ce groupe les projections et injections canoniques suivantes :*

1. *Les projections :*

$$p_1 : \begin{array}{ccc} G_1 \times G_2 & \to & G_1 \\ (x_1, x_2) & \mapsto & x_1 \end{array}$$

$$p_2 : \begin{array}{ccc} G_1 \times G_2 & \to & G_2 \\ (x_1, x_2) & \mapsto & x_2 \end{array}$$

2. *Les injections :*

$$q_1 : \begin{array}{ccc} G_1 & \to & G_1 \times G_2 \\ x_1 & \mapsto & (x_1, e_2) \end{array}$$

$$q_2 : \begin{array}{ccc} G_2 & \to & G_1 \times G_2 \\ x_2 & \mapsto & (e_1, x_2) \end{array}$$

*On peut aisément vérifier que ces applications définissent des morphismes de groupes. Les projections sont surjectives et les injections injectives. Les applications induites par les morphismes d'injections canoniques :*

$$G_1 \longrightarrow G_1 \times (e_2)$$

*et*

$$G_1 \longrightarrow (e_1) \times G_2$$

*sont des isomorphismes de groupes. Par conséquent, le groupe $G_1 \times G_2$ contient au moins un sous-groupe isomorphe à $G_1$, et au moins un sous-groupe isomorphe à $G_2$.*

**Propriétés 2.3.**

On a les propriétés suivantes :

1. $p_1 \circ q_1 = \mathrm{Id}_{G_1}$, $p_2 \circ q_2 = \mathrm{Id}_{G_2}$
2. $\forall x = (x_1, x_2) \in G$, on a :

$$x = (p_1(x), p_2(x))$$

$$x = q_1(x_1)\, q_2(x_2) = q_2(x_2)\, q_1(x_1)$$

3. Si $G_1$, $G_2$ sont des groupes finis alors $G_2 \times G_2$ est aussi un groupe fini, avec

$$o(G_2 \times G_2) = o(G_1)\, o(G_2)$$

**Proposition 2.4.**

Soient $G_1, G_2$ deux groupes. Un groupe $G$ est isomorphe au groupe $G_1 \times G_2$ si et seulement si il existe $H_1$ et $H_2$ deux sous-groupes de $G$ tels que :

1. $\forall i \in [\![1, 2]\!]$, $H_i \simeq G_i$
2. $\forall (h_1, h_2) \in H_1 \times H_2, h_1 h_2 = h_2 h_1$ (tous les éléments de $H_1$ commutent avec les éléments de $H_2$)
3. $G = H_1 H_2$
4. $H_1 \bigcap H_2 = \{e_G\}$

Il est à noter la différence entre $H_1 H_2$ et $H_1 \times H_2$ :

$$H_1 H_2 \overset{\text{def}}{=} \{h_1 h_2 \in G, h_1 \in H_1, h_2 \in H_2\}$$

(cette définition nécessite que $H_1$ et $H_2$ soient deux sous-groupes d'un même groupe.)

$$H_1 \times H_2 \overset{\text{def}}{=} \{(h_1, h_2), h_1 \in H_1, h_2 \in H_2\}$$

Les deux définitions n'ont donc rien à voir.

*Démonstration.*
"⇒" : Supposons que $G$ est isomorphe à $G_1 \times G_2$, alors il existe un isomorphisme entre les deux, notons le $\phi$. Déterminons les sous-groupes vérifiant les conditions énoncées dans la réciproques, comme $G_1 \times G_2$ est isomorphe a $G$ on peut se ramener via l'isomorphisme (conservation des sous-groupes...) $\phi$ a étudier le problème pour le groupe $G_1 \times G_2$. On peut donc supposer

$G = G_1 \times G_2$ Dans ce cas on peut trouver les sous-groupes aisément, ils sont : $H_1 = \mathrm{Im}\,(q_1)\,, H_2 = \mathrm{Im}\,(q_2)$ On peut vérifier les quatre points aisément.
"$\Leftarrow$" : Si l'on suppose l'existence de deux tels sous-groupe de $G$. On cherche a construire un isomorphisme $\phi$ entre $G$ et $G_1 \times G_2$. Soit $g \in G$, $\exists\,(h_1, h_2) \in H_1 \times H_2$ telles que $g = h_1 h_2$, par les hypothèse 2) et 3).
Une telle écriture est unique, montrons le : si on suppose que il existe un autre couple $(h_1', h_2')$, $g = h_1' h_2'$, alors $h_1' h_2' = h_1 h_2$

$$e_G = h_1'^{-1} h_1 = h_2'^{-1} h_2$$

alors

$$h_1 = h_1', h_2 = h_2'$$

Considérer

$$\phi : \begin{array}{ccc} G & \to & G_1 \times G_2 \\ g = (h_1, h_2) & \mapsto & (q_1\,(h_1)\,, q_2\,(h_2)) \end{array}$$

$\phi$ induit un isomorphisme de groupes.

Autre manière de voir les choses : $\phi : \begin{array}{ccc} G & \to & G_1 \times G_2 \\ g = (h_1, h_2) & \mapsto & (\phi_1\,(h_1)\,, \phi_2\,(h_2)) \end{array}$
où $\phi_1$ et $\phi_2$ sont des isomorphismes respectivement entre $H_1$ et $G_1$, et entre $H_2$ et $G_2$. Et on a montré que $\forall y \in G, \exists!\,(h_1, h_2) \in H_1 \times H_2$ tels que $g = h_1 h_2$, donc l'application est bien définie. On peut vérifier que c'est un morphisme, injectif et surjectif. □

## III Cas d'une famille finie

On peut généraliser la notion de produit direct à une famille finie de groupes $G_1, \ldots, G_n$.

**Définition 2.5.**

Soit une famille finie de groupes $G_1, \ldots, G_n$. Si on pose $G = \underbrace{G_1 \times G_2 \times \cdots \times G_n}_{\text{Produit cartésien des ensembles sous-jacents}}$, muni de la loi :

$$* : \begin{array}{ccc} G \times G & \to & G \\ \left((x_i)_{i\in[\![1,n]\!]}\,, (y_i)_{i\in[\![1,n]\!]}\right) & \mapsto & (x_i y_i)_{i\in[\![1,n]\!]} \end{array}$$

$(G, *)$ forme un groupe, et on l'appelle produit direct des groupes $G_1, \ldots, G_n$

**Remarque 2.6** (Notations)**.** *On associe à ce groupe, comme pour le premier cas, les projections et injections canoniques suivantes :*

1. *Les projections canonique :* $\forall i \in [\![1,n]\!]$ *:*

$$p_i : \begin{array}{ccc} G & \to & G_i \\ (x_i)_{i\in[\![1,n]\!]} & \mapsto & x_i \end{array}$$

2. *Les injections canoniques :*

$$q_i : \begin{array}{ccc} G_i & \to & G \\ x & \mapsto & (e_1,\ldots,e_{i-1},x,e_{i+1},\ldots,e_n) \end{array}$$

*on a* $\forall i \in [\![1,n]\!], \forall x \in G, p_i \circ q_i(x) = x$,

$$G_i \xrightarrow{q_i} G \xrightarrow{p_i} G_i$$

**Proposition 2.7.**

Soient $G_1,\ldots,G_n$ une famille de $n \geq 2$ groupes. Un groupe $G$ est isomorphe au produit direct des $G_i$, si et seulement si il existe $H_1,\ldots,H_n$ $n$ sous-groupes de $G$ tels que :

1. $\forall i \in [\![1,n]\!], G_i \simeq H_i$
2. $\forall (i,j) \in [\![1,n]\!]$, $\forall h_i \in H_i, h_j \in H_j$,
$$h_j h_i = h_i h_j$$
3. $G = H_1 H_2 \ldots H_n$
4. $H_i \bigcap H_1 \ldots H_n = (e_G), \forall i [\![1,n]\!]$

# IV Cas d'une famille quelconque

**Définition 2.8.**

Considérons $I$ un ensemble non vide et $(G_i)_{i\in I}$ une famille de groupes indexés dans $I$.

L'ensemble $G$ muni de la loi $*$ : $\begin{array}{ccc} G\times G & \to & G \\ \left((x_i)_{i\in I},(y_i)_{i\in I}\right) & \mapsto & (x_i y_i)_{i\in I} \end{array}$,

où

$$G \overset{\text{def}}{=} \prod_{i\in I} G_i = \left\{(x_i)_{i\in I}, \forall i \in I, x_i \in G_i\right\}$$

forme un groupe, appelé produit direct des $G_i$.

**Lemme 2.9.**

On définit là encore les projections et injections, on peut munir le groupe $(G, *)$ définie comme précédemment, des applications :

1. Les projections canonique : $\forall i \in I$,

$$p_i : \begin{array}{ccc} G & \to & G_i \\ (x_i)_{i\in[\![1,n]\!]} & \mapsto & x_i \end{array}$$

2. Les injections canoniques : $\forall i \in I$,

$$q_i : \begin{array}{ccc} G_i & \to & G \\ x & \mapsto & (e_1, \ldots, e_{i-1}, x, e_{i+1}, \ldots, e_n) \end{array}$$

avec $\begin{cases} x_i = e_{G_j} \text{ si } i \neq j \\ x \text{ si } i = j \end{cases}$.

# V Preuve de la propriété universelle

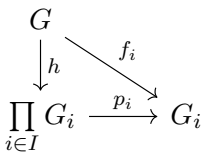
On a donc montré jusqu'au cas général d'une famille de groupe quelconque, l'existence d'un produit direct, muni des projections et injections. Il reste à montrer la propriété universelle.

**Théorème 2.10.**

Soit $I \neq \varnothing$ un ensemble. Soit $(G_i)_{i\in I}$ une famille quelconque de groupes indexée dans l'ensemble $I$. On a alors la propriété universelle suivante : Si $G$ est un groupe, et si $f_i \in \mathrm{Hom}\,(G, G_i)$, $\forall i \in I, \exists! h \in \mathrm{Hom}\left(G, \prod_{i\in I} G_i\right)$ tel que

$$p_i \circ h = g_i, \forall i \in I$$

En d'autres termes, $\exists h \in \mathrm{Hom}\left(G, \prod_{i\in I} G_i\right)$ rendant commutatif le diagramme de morphismes de groupes suivant pour tout $i$ dans $I$ :



*Démonstration.*
On fera la preuve dans le cas où $I = \{1,2\}$. Soient $G_1, G_2$ deux groupes, et $G$ un groupe muni de deux morphismes canoniques : $\forall i \in \{1,2\}, G \xrightarrow{f_i} G_i$.

1. Existence.
   Soit $h : \begin{array}{ccc} G & \to & G_1 \times G_2 \\ x & \mapsto & (f_1(x), f_2(x)) \end{array}$ On a donc

   $$p_i \circ h = f_i, \forall i \in \{1,2\}.$$

   On peut montrer que $H$ est un morphisme de groupes :

   $$\begin{aligned} h(xy) &= (f_1(xy), f_2(xy)) \\ &= (f_1(x) f_1(y), f_2(x) f_2(y)) \quad f_i \text{ morphisme de groupe} \\ &= (h(x) * h(y)) \end{aligned}$$

2. Unicité :
   Soit $h' \in \mathrm{Hom}(G, G_1 \times G_2)$ vérifiant $p_i \circ h' = f_i$, $\forall i \in \{1,2\}$.
   Montrons que $h' = h$, soit $x \in G$ :

   $$\begin{aligned} p_1 \circ h'(x) &= f_1(x) \\ p_2 \circ h'(x) &= f_2(x) \end{aligned}$$

   alors ces relations impliquent que :

   $$h'(x) = (f_1(x), f_2(x)) = h(x)$$

   donc les applications coïncident sur $G$ ,donc $h = h'$

□

# VI Produit semi-direct de groupes

Soient $G, H$ deux groupes et $\alpha : G \to \mathrm{Aut}(H)$ un morphisme de groupes.

**Définition 2.11.**

On définit l'application suivante :

$$\underset{\alpha}{\sim}: \begin{array}{ccc} G \times H & \to & H \\ (g,h) & \mapsto & \alpha(g)(h) \end{array}$$

**Propriétés 2.12.**

$\widetilde{\alpha}$ vérifie les propriétés suivantes :

1. $\forall g \in G, \quad : h \quad \mapsto \quad \widetilde{\alpha}\left(g_0, h\right) \in \mathrm{Aut}\left(H\right)$
2. $\forall g, g' \in G, \forall h \in H,$

$$\widetilde{\alpha}\left(gg', h\right) = \widetilde{\alpha}\left(g, \widetilde{\alpha}\left(g', h\right)\right)$$

3. $\forall h \in H, \widetilde{\alpha}\left(e_G, h\right) = h$, et $\forall g \in G, \widetilde{\alpha}\left(g, e_H\right) = e_H$

*Démonstration.*

1. On note $\phi_{g_0} = \quad : h \quad \mapsto \quad \widetilde{\alpha}\left(g_0, h\right) \in \mathrm{Aut}\left(H\right)$ . $\phi_{g_0}$ est une application de $H$ dans lui-même, c'est un morphisme car $\alpha : \quad G \quad \to \quad \mathrm{Aut}\left(H\right)$ .
2. $$\begin{aligned}\widetilde{\alpha}\left(gg', h\right) &= \alpha\left(gg'\right)\left(h\right) \\ &= \alpha\left(g\right)\left(\alpha\left(g'\right)\left(h\right)\right) \\ &= \alpha\left(g\right) \circ \widetilde{\alpha}\left(g', h\right) \\ &= \widetilde{\alpha}\left(g, \widetilde{\alpha}\left(g', h\right)\right)\end{aligned}$$
3. $$\begin{aligned}\widetilde{\alpha}\left(e_G, h\right) &= \alpha\left(e_G\right)\left(h\right) \\ &= \mathrm{Id}\left(h\right) \\ &= h\end{aligned}$$

   $$\begin{aligned}\widetilde{\alpha}\left(g, e_H\right) &= \alpha\left(g\right)\left(e_H\right) \\ &= e_H\end{aligned}$$

   Car car $\alpha\left(g\right)$ est un morphisme de groupe.

□

**Définition 2.13.**

$$*_{\widetilde{\alpha}} : \begin{array}{ccc} \left(H \times G\right)^2 & \to & H \times G \\ \left(h_1, g_1\right), \left(h_2, g_2\right) & \mapsto & \left(h_1 \tilde{\alpha}\left(g_1, h_2\right), g_1 g_2\right) \end{array}$$

définit une loi de composition interne au groupe $H \times G$. On a alors que $\left(H \times G, *_{\tilde{\alpha}}\right)$ est un groupe, on le note $H \rtimes_{\tilde{\alpha}} G$

*Démonstration.*

1. Associativité : Soient $(h_1, g_1), (h_2, g_2), (h_3, g_3) \in H \rtimes_{\tilde{\alpha}} G$

$$\begin{aligned}((h_1, g_1) *_{\tilde{\alpha}} (h_2, g_2)) *_{\tilde{\alpha}} (h_3, g_3) &= (h_1 \alpha (g_1, h_2), g_1 g_2) *_{\tilde{\alpha}} (h_3, g_3) \\ &= (h_1 \alpha (g_1, h_2) \alpha (g_1 g_2, h_3), g_1 g_2 g_3) \\ (h_1, g_1) *_{\tilde{\alpha}} ((h_2, g_2) *_{\tilde{\alpha}} (h_3, g_3)) &= (h_1, g_1) *_{\tilde{\alpha}} (h_2 \alpha (g_2, h_3), g_2 g_3) \\ &= (h_1 \alpha (g_1, h_2, \alpha (g_2, h_3)), g_1 g_2 g_3) \\ &= (h_1 \alpha (g_1, h_2) \alpha (g_1, \alpha((g_2, h_3), g_1 g_2 g_3))) \\ &= (h_1 \alpha (g_1, h_2) \alpha (g_1 g_2, h_3), g_1 g_2 g_3)\end{aligned}$$

2. Élément neutre :
   On va vérifier que $e = (e_H, e_G)$ est l'élément neutre de la loi $*_{\tilde{\alpha}}$, soit $(h, g) \in H \rtimes_{\tilde{\alpha}} G$, alors :

$$\begin{aligned}(e_H, e_G) *_{\tilde{\alpha}} (h, g) = e *_{\tilde{\alpha}} (h, g) &= (e_H, e_G) *_{\tilde{\alpha}} (h, g) \\ &= (e_H \alpha (e_G, h), e_G g) \\ &= (e_H h, e_G g) \\ &= (h, g)\end{aligned}$$

   Réciproquement, :

$$\begin{aligned}(h, g) *_{\tilde{\alpha}} e &= (h, g) *_{\tilde{\alpha}} (e_H, e_G) \\ &= (h \alpha (g, e_H), g e_G) \\ &= (h e_H, g) = (h, g)\end{aligned}$$

3. Existence du symétrique :
   Soit $(h, g) \in H \rtimes_{\tilde{\alpha}} H$, montrons que $\left(\alpha \left(g^{-1}, h\right)^{-1}, g^{-1}\right)$ est le symétrique de $(h, g)$

$$\begin{aligned}(h, g) *_{\tilde{\alpha}} \left(\alpha \left(g^{-1}, h\right)^{-1}, g^{-1}\right) &= \left(h \alpha \left(g, \alpha \left(g^{-1}, h\right)\right)^{-1}, e_G\right) \\ &\left(h \alpha (e_G, h)^{-1}, e_G\right) \\ &= (e_H, e_G)\end{aligned}$$

   Réciproquement :

$$\begin{aligned}\left(\alpha \left(g^{-1}, h\right)^{-1}, g^{-1}\right) *_{\tilde{\alpha}} (h, g) &= \left(\alpha \left(g^{-1}, h\right)^{-1} \alpha \left(g^{-1}, h\right), e_G\right) \\ &= (e_H, e_G)\end{aligned}$$

□

On a donc associé l'ensemble $H \times G$ au produit semi-direct $H \rtimes_{\tilde{\alpha}} G$ : On a construit une loi de composition interne qui permet de former un groupe. On a dans ce chapitre tenté de définir une structure de groupe pour les produit de groupes. on a :

1. Le produit direct de deux groupes formée naturellement par le produit cartésien, on a même définit une propriété universelle.
2. Une généralisation de cette notion : Le produit semi-direct. On aura une application de ceci dans les groupes diédraux. Comme dans le cas du produit direct : $G \times H$ est en bijection avec $G \rtimes_{\tilde{\alpha}} H$. Contrairement au produit direct, la multiplication n'est pas similaire, elle est plus compliqué et non naturelle, on opère par automorphisme de groupes. On prolongera cette notion avec les groupes quotient et les produits diédraux dans les chapitres suivants.
3. Le produit semi-direct est un premier exemple d'action de groupes. C'est à dire que chaque élément de $G$ est vu via $\alpha$, comme un automorphisme de $H$, c'est à dire une façon "d'agir" sur $H$. Le thème des actions de groupes sera abordé plus loin dans ce document.

# Chapitre 3

# Théorème de Lagrange

## I Relation d'équivalence modulo un sous-groupe.

Soit $G$ un groupe et $H \leq G$. On associe à cette dernière deux relations binaires sur $G$ :

$$x \,\mathcal{R}_H\, y \Leftrightarrow xy^{-1} \in H$$
$$x \,{}_H\mathcal{R}\, y \Leftrightarrow x^{-1}y \in H$$

On a la propriété suivantes :

**Propriétés 3.1.**

1. $\mathcal{R}_H$ et ${}_H\mathcal{R}$ sont des relations d'équivalence.
2. $$y\mathcal{R}_H x \Leftrightarrow y \in Hx \text{ et } y\,{}_H\mathcal{R} x \Leftrightarrow y \in xH$$
   où :
   $$Hx \overset{\text{def}}{=} \{hx,\ h \in H\} \subset G$$
   $$xH \overset{\text{def}}{=} \{xh,\ h \in H\} \subset G$$

*Démonstration.*
Montrons 1).
On effectuera les preuves pour $\mathcal{R}_H$, la preuve pour ${}_H\mathcal{R}$ étant similaire dans le raisonnement.

1. Réflexivité : $e_G = e_H = xx^{-1}$, $e_G \in H$ car $H \leq G$.
2. Symétrique : soit $x\mathcal{R}_H y$, $xy^{-1} \in H$, $\left(xy^{-1}\right)^{-1} = yx^{-1} \in H$ ($H$ est un groupe) donc $y\mathcal{R}_H x$.

3. Transitivité : Soient $x, y, z \in G$,

$$x\mathcal{R}_H y, xy^{-1} \in H \text{ et } y\mathcal{R}_H z, yz^{-1} \in H$$

On peut montrer que $x\mathcal{R}_H z$, i.e que $xz^{-1} \in H$, comme $H$ est un groupe, $\left(xy^{-1}\right)\left(yz^{-1}\right) \in H$.

Pour 2) $x\mathcal{R}_H x \Leftrightarrow yx^{-1} \in H$

$$\begin{aligned} y \in Hx &\Leftrightarrow \exists h \in H, y = hx \\ &\Leftrightarrow \exists h \in H, yx^{-1} = h \in H \Leftrightarrow y\mathcal{R}_H x \end{aligned}$$

□

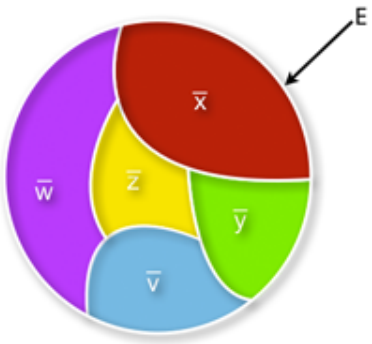
**Définition 3.2.**

Soit $H$ un sous-groupe de $G$. On appelle relation d'équivalence à droite (respectivement à gauche) la relation d'équivalence $\mathcal{R}_H$ (respectivement ${}_H\mathcal{R}$).
Les ensembles $Hx$ et $xH$ sont les classes d'équivalence à droite et à gauche , respectivement modulo ces relations d'équivalence.
On peut voir les relations d'équivalence comme une partition d'ensemble : Se donner une relation d'équivalence sur un ensemble $E$, cela revient a se donner une partition d'ensemble $E$. C'est en particulier vrai pour $\mathcal{R}_H$ et ${}_H\mathcal{R}$.

$$x \in Hx \text{ donc } G = \bigcup_{x \in G} Hx$$

$$\text{Si } Hx \neq hy \Rightarrow Hx \bigcap Hy \neq \varnothing$$

On peut le comprendre par un dessin :



L'ensemble $E$ est partitionné par la relation d'équivalence. $\overline{v}, \overline{y}, \overline{w}, \overline{x}, \overline{z}$ sont les classes d'équivalence (distinctes). $E/\mathcal{R} = \{\overline{v}, \overline{y}, \overline{w}, \overline{x}, \overline{z}\}$. On peut tout reprendre de manière additive :

$$x\mathcal{R}_H y \Leftrightarrow x - y \in H$$

$$Hx = \{h + x, h \in H\}$$

Si $H = G, Gx = xG = G$ et $\mathcal{R}_G =_G \mathcal{R}$ Si $H = \{e\}, {}_{\{e\}}\mathcal{R} = \mathcal{R}_{\{e\}}$
Si $G$ est un groupe abélien, ${}_H\mathcal{R} = \mathcal{R}_H$.

**Remarque 3.3.**
$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(n)$
*En général* ${}_H\mathcal{R} \neq \mathcal{R}_H$ *et* $Hx \neq xH$.
*On note :*

$$G/\mathcal{R}_H = (G/H)_d$$
$$G/{}_H\mathcal{R} = (G/H)_g$$

**Exemple 3.4.**
*On peut illustrer tout cela avec des groupes cycliques ; prenons* $S_3$, *groupe engendre par* $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *et* $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

$$S_3 = \left\{e, \sigma_3, \sigma_1, \sigma_1^2, \sigma_3 \circ \sigma_1, \sigma_1 \circ \sigma_3\right\}$$

$H \overset{def}{=} \{e, \sigma_3\}$ *et on peut montrer alors que :*

$$\begin{aligned} H &\overset{def}{=} \{e, \sigma_3\} \\ H\sigma_1 &= \{\sigma_1, \sigma_3 \circ \sigma_1\} \\ H\sigma_1^2 &= \left\{\sigma_1^2, \sigma_3 \circ \sigma_1^2 = \sigma_1 \circ \sigma_3\right\} \\ H &\overset{def}{=} \{e, \sigma_3\} \\ \sigma_1 H &= \{\sigma_1, \sigma_1 \circ \sigma_3\} \\ \sigma_1^2 H &= \left\{\sigma_1^2, \sigma_3 \circ \sigma_1\right\} \end{aligned}$$

*On a* $H\sigma_1 \neq \sigma_1 H$ *et* $\mathcal{R}_H \neq {}_H\mathcal{R}$

# II Théorème de Lagrange et formule des indices.

**Proposition 3.5.**

Soit $G$ un groupe, et $x \in G$, soit $H$ un sous-groupe de $G$.
Alors toute classe à droite $Hx$ (respectivement à gauche $xH$ ) est équipotente à $H$.

*Démonstration.*
Utiliser la fonction :

$$\gamma : \begin{array}{ccc} H & \to & Hx \\ h & \mapsto & hx \end{array}$$

et montrer que c'est une bijection ($h^{-1}$ existe car $H$ est un groupe.) □

**Corollaire 3.6.**

Une conséquence de cette proposition est l'équipotence des ensembles suivants, dans un groupe $G$ quelconque :

1. deux classes à droite
2. deux classes à gauche
3. une classe à droite et une classe à gauche.

i.e, si $x, y \in H \leq G$, on a :

$$|Hx| = |xH| = |yH| = |Hy|$$

**Corollaire 3.7.**

Si $G$ est un groupe et $H$ un sous-groupe de $G$, fini. Alors toute classe à droite $Hx$ et toute classe à gauche $xH$ est un ensemble fini et a même cardinal.

**Théorème 3.8** (Théorème de Lagrange)**.**

Si $G$ est un groupe fini, si $H$ est un sous-groupe de $G$, alors :

$$\mathrm{o}(h) \,|\, \mathrm{o}(g).$$

En d'autres termes, l'ordre de tout sous-groupe $H$ divise l'ordre de $G$.

*Démonstration.*
Les classes a droite modulo $H$ forment une partition finie de $G$. Si on note $S$ un système des représentants des classes a droites, alors :

$$\begin{aligned} \text{Card } G &= \sum_{s \in S} |Hs| = |Hx| \times \text{ Nombre de classes a droite} \\ &\qquad \text{Par le corollaire qui montre l'equipotence des classes a droite} \\ &= |Hx| \times k \end{aligned}$$

où $k$ est le nombre de classes à droite. □

**Corollaire 3.9.**

On a deux conséquences de ce théorème :

1. On a alors un lien avec l'ordre des éléments si $G$ est un groupe fini. Si $G$ est un groupe fini, alors $\forall x \in G$,
$$\mathrm{o}(x) \,|\, \mathrm{o}(G).$$
2. Si $G$ est un groupe fini, le nombre de classes à droite, modulo $H$, où $H$ est un sous-groupe de $G$, dans $G$ est égal au nombre de classes à gauche modulo $H$ dans $G$, ce nombre est égal à $\frac{\mathrm{o}(g)}{\mathrm{o}(H)}$ (par axiome : $\mathrm{o}(H) \geq 1$)

**Théorème 3.10.**

Soit $G$ un groupe, et $H$ un sous-groupe de $G$. Les ensembles $(G/H)_d$ et $(G/H)_g$ sont équipotents.

*Démonstration.* $\theta : \begin{array}{ccc} (G/H)_d & \to & (G/H)_g \\ Hx & \mapsto & x^{-1}H \end{array}$ Il faut montrer que cette application est définie et a un sens. i.e que l'on a $Hx = Hy \Rightarrow x^{-1}H = y^{-1}H$ (indépendance du choix du représentant).

$$Hx = Hy \Leftrightarrow xy^{-1} \in H \Leftrightarrow \exists h \in H, xy^{-1} = h, x = hy.$$

C'est donc équivalent à $xy^{-1} = h \in H$.

Donc, si $Hx = Hy$, on a $y^{-1} \in x^{-1}H$. Multiplier à droite par un élément de $h$ ne change pas la classe d'équivalence, donc $y^{-1}H \subset x^{-1}H$. Par un raisonnement symétrique, on a que $x^{-1}H \subset y^{-1}H$. Et on a bien que $Hx = Hy \Rightarrow x^{-1}H = y^{-1}H$. Il faut également montrer que $\theta$ est une bijection.

1. Surjectivité :
   Soit $xH \in (G/H)_g$, on a alors $\theta\left(Hx^{-1}\right) = xH$
2. Injectivité :
   Soient $x, y \in G$ telle que $x^{-1}H = y^{-1}H$, donc $xy^{-1} \in H$, $\exists h \in H, xy^{-1} = h$, donc $x = hy$. D'où $Hx = Hy$.

□

**Définition 3.11** (Indice)**.**

Soit $H$ un sous-groupe d'un groupe $G$, si l'ensemble $(G/H)_d$ est un ensemble fini. On dit que $H$ est un sous-groupe d'indice fini dans $G$, et on note $[G : H] = \text{Card } ((G/H)_d)$.

**Corollaire 3.12.**

Si $(G/H)_d$ est un ensemble fini, alors $(G/H)_g$ est un ensemble fini.

**Proposition 3.13** (Première formule d'indice)**.**

Si $G$ est un groupe fini, on a la formule : $\mathrm{o}(G) = \mathrm{o}(H)[G : H]$

*Démonstration.*
ici $[G : H] = \frac{\mathrm{o}(G)}{\mathrm{o}(H)}$ □

Attention, $[H : G]$ peut être fini sans que ni $G$ ni $H$ le soit. Exemple : $(\mathbb{Z}, +)$ et $n\mathbb{Z}$, alors $G/H$ est de cardinal $n$.

**Théorème 3.14** (Théorème de Poincaré)**.**

Soit $G$ un groupe, soit $(H_i)_{i\in[\![1,n]\!]}$, $n \geq 2$ une famille finie de sous-groupe d'indice fini. Alors $\bigcap_{i=1}^{n} H_i$ est d'indice fini et $\left[G : \bigcap_{i=1}^{n} H_i\right] \leq \prod_{i=1}^{n} [G : H_i]$

*Démonstration.*
On effectue une récurrence sur $n$, donc on traitera là le cas $n = 2$, qui correspond à l'hérédité, l'initialisation à $n = 1$ étant triviale.

Soient $H_1, H_2$ deux groupes d'indices finis dans $G$.
$\forall x \in G, (H_1 \bigcap H_2)\, x = H_1 x \bigcap H_2 x$ Soit $y \in (H_1 \bigcap H_2)\, x$, alors $yx^{-1} \in H_1$ et $yx^{-1} \in H_2$ d'où $y \in H_1 x$ et $y \in H_2 x$. Donc $y \in H_1 x \bigcap H_2 x$.
Réciproquement : $\forall y \in H_1 x \bigcap H_2 x$, alors $yx^{-1} \in H_1 \bigcap H_2$ d'où $y \in (H_1 \bigcap H_2)\, x$.
Par conséquent :

Soit $x \in G$. On a $\begin{cases} H_1 \bigcap H_2 \subseteq H_1 \\ H_1 \bigcap H_2 \subseteq H_2 \end{cases}$ donc $\begin{cases} (H_1 \bigcap H_2)\, x \subseteq H_1 x \\ (H_1 \bigcap H_2)\, x \subseteq H_2 x \end{cases}$.

Comme les classes à droite modulo $H_1$ et les classes à gauche modulo $H_2$ sont finies, on a que les classes modulo $H_1 \bigcap H_2$ sont également finies par les inclusions que l'on vient de démontrer (elles sont incluses dans les classes à gauche modulo $H_1$ et $H_2$). $H_1 \bigcap H_2$ est d'indice fini et

$$\left[G : H_1 \bigcap H_2\right] \leq [G : H_1] \times [G : H_2] .$$

□

**Théorème 3.15** (Formule des indices)**.**

Soit $G$ un groupe, et $H$ un sous-groupe de $G$ d'indice fini. Si $K$ est un sous-groupe de $G$ tel que $H \subseteq K$, alors $K$ est d'indice fini dans $G$ et on a la formule

$$[G : H] = [G : K] \times [K : H] .$$

*Démonstration.*
Soit $(x_i)_{i\in I}$ une famille de représentants des classes à droite de $K$ dans $G$. Alors $G = \bigsqcup_{i\in I} Kx_i$
Soit $(y_i)_{j\in J}$ une famille de représentants des classes à droite de $H$ dans $K$.

$$K = \bigsqcup_{j\in J} Hy_j$$

Montrons que $(x_i y_j)_{i,j}$ forme une famille de représentants des classes à droite de $H$ dans $G$. On va montrer pour cela que $G = \bigsqcup_{i,j} Hy_j x_i$. Soit $g \in G$, alors $\exists i \in I, \exists a \in K$ tels que $g = ax_i$. donc $\exists i \in J, \exists b \in H$ tels que $g = (by_j)\, x_i$. Donc $g \in Hy_i x_i$.
L'autre inclusion se déduit de la qualité de groupe de $G$, avec la stabilité par la loi $\cdot$

$$G = \bigcup_{i,j} Hy_j x_i.$$

Soient $(\lambda, i), (\mu, j)$, alors :

$$Hy_\lambda x_i = Hy_\mu x_j \Rightarrow (x_i = x_j \text{ et } y_\lambda = y_\mu)$$

Montrons pour cela que

$$H \subseteq K \Rightarrow K = KH.$$

En effet : $KH \subseteq K$ car $H \subseteq K$ et $K$ et $H$ sont des groupes. Si $x \in K$, $x = xe \in KH$.

$$\begin{aligned} Hy_\lambda x_i = Hy_\mu x_j &\Rightarrow KHy_\lambda x_i = KHy_\mu x_j \\ &\Rightarrow Ky_\lambda x_i = Ky_\mu x_j \\ &\Rightarrow Kx_i = Kx_j \Rightarrow x_i = x_j \end{aligned}$$

car $y_\lambda, y_\mu \in K$

$$\begin{aligned} Hy_\lambda x_i = Hy_\mu x_j &\Rightarrow Hy_\lambda = Hy_\mu \\ &\Rightarrow y_\lambda = y_\mu \end{aligned}$$

Donc $(x_i y_j)_{i,j}$ forme un système de représentants des classes à droite de $H$ dans $G$. Par hypothèse, cet ensemble est fini donc $I$ et $J$ sont finis.

$$[G : H] = \text{Card } \left( \{x_i y_j\}_{i,j} \right) = [G : K]\,[K : H]$$

□

# Chapitre 4

# Sous-groupes normaux

## I Relations d'équivalence compatibles avec une loi de composition.

Soit $E$ un ensemble muni d'une loi de composition interne $*$.

**Définition 4.1.**

On dit que une relation $\mathcal{R}$ sur $E$ est :

1. compatible à droite (respectivement à gauche) avec la loi de composition si

$$\forall x, y, a \in E, x\mathcal{R}y \Rightarrow (x * a)\ \mathcal{R}\ (y * a)$$

(respectivement : $x\mathcal{R}y \Rightarrow (a * x)\ \mathcal{R}\ (a * y)$)

2. compatible avec la loi de composition $*$ si :

$$\forall x, y, x', y' \in E, \quad x\mathcal{R}x', y\mathcal{R}y' \Rightarrow (x * y)\ \mathcal{R}\ \left(x' * y'\right).$$

On dira qu'une relation est compatible si elle est compatible à gauche et à droite.
Si $E$ est un ensemble, et $\mathcal{R}$ une relation d'équivalence, on notera $\overline{E} = E/\mathcal{R}$ l'ensemble quotient.

$$\mathrm{cl}_{\mathcal{R}} \overset{\text{def}}{=} \bar{\cdot} : \begin{array}{ccc} E & \to & \overline{E} \\ x & \mapsto & \overline{x} \end{array}$$

est une application surjective (par construction)

**Proposition 4.2.**

$$*_{\overline{E}} : \begin{array}{ccc} \overline{E} \times \overline{E} & \to & \overline{E} \\ (\overline{x}, \overline{y}) & \mapsto & \overline{x.y} \end{array}$$

est une loi de composition interne de $\overline{E}$, si et seulement si $\mathcal{R}$ est compatible à la loi $*$. On a

$$x *_{\overline{E}} y \overset{\text{def}}{=} \overline{x * y}$$

*Démonstration.* Preuve longue mais non technique. Il suffit d'appliquer les définitions.
La définition proposée induit celle d'un loi de composition interne si et seulement si $*\overline{E}$ est une application d'ensemble, i.e qu'elle est bien définie, donc on doit montrer l'indépendance des choix, c'est-à-dire :

$$\left(x\mathcal{R}x', y\mathcal{R}y' \Rightarrow xy\mathcal{R}x'y'\right)$$

Or ceci correspond à la définition de compatibilité de $\mathcal{R}$. □

**Proposition 4.3.**

Soit $G$ un groupe.

1. Si $H$ est un sous-groupe de $G$, la relation d'équivalence $\mathcal{R}_H$ (respectivement ${}_H\mathcal{R}$ ) est compatible à droite (respectivement à gauche) avec la loi de composition de $G$.
2. Si $\mathcal{R}$ est une relation d'équivalence définie sur $G$, compatible à droite (respectivement à gauche) avec la loi de composition de $G$, alors :
   Il existe un unique sous-groupe $H$ de $G$ tel que $\mathcal{R} = \mathcal{R}_H$ (respectivement $\mathcal{R} = {}_H\mathcal{R}$)

*Démonstration.*
On montrera pour $\mathcal{R}_H$ et pas pour ${}_H\mathcal{R}$.

1. Soit $H$ un sous-groupe de $G$. On doit montrer que $\mathcal{R}_H$ est compatible à droite. Soient $x, y, a \in G$ tels que $x\mathcal{R}_H y$.
   L'hypothèse est équivalente à $xy^{-1} \in H$, on veut montrer que $(x \cdot a)\,\mathcal{R}_H\,(y \cdot x)$.

$$xy^{-1} \in H$$

$$\text{donc } xy^{-1} = (xa)\left(a^{-1}y^{-1}\right) = \underbrace{(xa)}_{\in G}\underbrace{(ya)}_{\in G}^{-1} \in H$$

2. Soit $\mathcal{R}$ une relation sur $G$, compatible à droite. On pose $H \overset{\text{def}}{=} \overline{e_g}$ modulo $\mathcal{R}$.
   $H$ est un sous-ensemble non vide, montrons que $H$ est un sous-groupe de $G$.
   Soit $x, y \in H$, $x\mathcal{R}e$ $y\mathcal{R}e$ donc $xy^{-1}\mathcal{R}y^{-1}$ et $e\mathcal{R}y^{-1}$, par transitivité de $\mathcal{R}$, $xy^{-1}\mathcal{R}e \Leftrightarrow xy^{-1} \in H$, donc $H$ est bien un sous-groupe de $G$.
   Soit $x\mathcal{R}y$, montrons que $x\mathcal{R}_H y$. Par compatibilité à droite : $xy^{-1}\mathcal{R}e$, ce qui équivaut à $xy^{-1} \in H$, ou encore $x\mathcal{R}_H y$.

   $$\mathcal{R} \subseteq \mathcal{R}_H.$$

   Soit $x\mathcal{R}_H y$, alors $xy^{-1} \in H$, donc $xy^{-1}\mathcal{R}e$ d'où $x\mathcal{R}y$, par compatibilité de $\mathcal{R}$. donc

   $$\mathcal{R}_H \subseteq \mathcal{R}.$$

□

**Exemple 4.4.**
*Soit $G$ un groupe abélien. Pour tout sous-groupe $H$ de $G$,*

$$\mathcal{R}_H = {}_H\mathcal{R} = \mathcal{R}.$$

*En particulier, $G/H = (G/H)_d = (G/H)_g$ et la loi de composition sur $G$ est compatible avec $\mathcal{R}$.*

# II Notion de sous-groupes normaux

Un sous-groupe normal sera aussi appelé sous-groupe distingué.

**Définition 4.5.**

Soit $G$ un groupe, un sous-groupe $H$ de $G$, est dit normal (ou distingué) si $\mathcal{R}_H = {}_H\mathcal{R}$.
On note alors $H \triangleleft G$

**Propriétés 4.6.**

Soit $G$ un groupe.

1. $G$ et $(e)$ sont des sous-groupes distingués (normaux) de $G$.
2. Si $G$ est abélien, tout sous groupe est distingué (normal).

**Définition 4.7** (Groupe simple)**.**

Soit $G$ un groupe, $G$ est un groupe simple, si $G \neq (e)$ et si $(e)$, $G$ sont les seuls sous-groupes normaux de $G$.

**Propriétés 4.8.**

Les seuls groupes abéliens finis simples sont les groupes d'ordre $p$ premiers.

**Proposition 4.9.**

Soit $G$ un groupe abélien, l'application canonique est $\pi : \begin{array}{ccc} G & \to & G/H \\ x & \mapsto & \overline{x} \end{array}$.
La loi de composition $*_G$ induit une loi de composition sur $G/H$ qui le munit d'une structure de groupe abélien.

**Exemple 4.10.**
*Soit $H$ le noyau d'un morphisme de groupes définie sur le groupe $G$. soit $f : \begin{array}{ccc} G & \to & G' \end{array}$ un morphisme de groupe, $H = \operatorname{Ker} f$ , c'est un sous-groupe de $G$.*
$\forall x, y \in G$,

$$\begin{aligned} x\mathcal{R}_H x &\Leftrightarrow xy^{-1} \in \operatorname{Ker} f \\ &\Leftrightarrow f(x)\left(f(y)\right)^{-1} = e_G \\ &\Leftrightarrow f(x) = f(y) \end{aligned}$$

*de même $x\mathcal{R}_h y \Leftrightarrow f(x) = f(y)$*
*Donc on a $\mathcal{R}_H = {}_H\mathcal{R} = \mathcal{R}$ et $\mathcal{R}$ est compatible avec $*_G$.*

**Proposition 4.11.**

$\forall f \in \operatorname{Hom}(G, G')$, et $\pi : \begin{array}{ccc} G & \to & G/\operatorname{Ker} f \end{array}$ .
La loi de composition $*_G$ induit sur $G/\operatorname{Ker} f$ une loi de composition qui le munit d'une structure de groupe.

**Proposition 4.12** (Noyau d'un morphisme de groupe)**.**

Soit $f : G \to G'$ un morphisme de groupes.
Alors le noyau $\operatorname{Ker} f$ est un sous-groupe distingué de $G$.

*Démonstration.*
Soit $h \in \ker f$, $g \in G$, montrons que $ghg^{-1} \in \ker f$.
$f\left(ghg^{-1}\right) = f(g) f(h) f(g)^{-1} = f(g) f(g)^{-1} = e$, d'où le résultat. □

## III Structure de sous-groupe sur l'ensemble $(G/H)$

Soit $H$ un sous-groupe de $G$, muni de la loi $+$. On veut munir l'ensemble $G/H$ d'une structure de groupe, or d'emblée ce n'est pas nécessairement un groupe. On peut essayer de définir une loi de groupe, et pour cela il est nécessaire d'utiliser la notion de groupe abélien ou de sous-groupe distingué (notion plus faible). On se place dans le cas des sous-groupes distingués donc on note $G/H$ sans distinguer gauche et droite car $\forall x \in G, xH = Hx$. On a le résultat suivant :

**Théorème 4.13.**

Soit $H$ un sous-groupe de $G$, la loi quotient

$$\dot{+} : \begin{array}{ccc} G/H \times G/H & \to & \dfrac{G/H}{x+y} \\ (\overline{x}, \overline{y}) & \mapsto & \end{array}$$

sur $G/H$ est bien définie si et seulement si $H$ est dinstingué dans $G$. Dans ce cas, on a la projection canonique :

$$\pi : \begin{array}{ccc} G & \to & G/H \\ g & \mapsto & \overline{g} \end{array}$$

qui définit alors un morphisme de groupes. Cette projection est surjective par construction.

*Démonstration.*
Il faut définir une multiplication sur $G/H$ qui le munisse d'une structure de groupe. $\pi$ est surjective donc

$$\forall x \in G/H, \exists g \in G, x = \pi(g)$$

On veut que *pi* soit un morphisme de groupe donc on cherche a avoir, $\forall x, x' \in G/H$,

$$xx' = \pi(g)\pi\left(g'\right) = \pi\left(gg'\right)$$

Le produit à définir doit être indépendant des choix de $g$ et $g$ comme antécédents de $x$ et $x'$ (indépendance du choix)
On prend $g_1, g_1' \in G$ tels que $\pi(g_1) = x$ et $\pi(g_1') = x'$,donc $\exists h, h' \in H$ tels que $g_1 = gh$ et $g_1' = h'g'$. Or, parce que $H$ est un sous-groupe distingué de $G$ :

$$g'^{-1}hg' \in H, g^{-1}h'g \in H$$

donc

$$\begin{aligned}\pi\left(g_1 g_1'\right) &= \pi\left(ghg'h'\right) \\ &= \pi\left(gg'g'^{-1}hg'h'\right) \\ &= \pi\left(gg'\right)\end{aligned}$$

On a donc l'indépendance du choix. Par construction, $\pi$ est donc un morphisme de groupe. □

**Propriétés 4.14** (Propriété universelle du groupe quotient)**.**

Soit $f \in \mathrm{Hom}(G, G')$, tel que $H \subset \ker f$. Alors il existe un unique morphisme $\tilde{f} : G/H \to G'$ tel que

$$f = \tilde{f} \circ \pi.$$

Le noyau de $\tilde{f}$ est l'image de $\ker f$ dans $G/H$ qui s'identifie à $\ker(f)/H$.
De plus $\tilde{f}$ est injectif si et seulement si $H = \ker f$.

*Démonstration.*
Soit $x \in G/H$. $\exists g \in G, x = \pi(g)$ donc $\tilde{f}(x) = f(g)$. On le définit ainsi car $\pi$ est surjective donc tout élément de $G/H$ peut être écrit comme image d'un élément par $\pi$.
On peut montrer que $\tilde{f}$ est un morphisme de groupes : Soient $x = \pi(g), x' = \pi(g') \in G/H$, alors l'antécédent de $xx'$ dans $G$ est $gg'$.

$$\begin{aligned}\tilde{f}\left(xx'\right) &= f\left(gg'\right) \\ &= f(g) f\left(g'\right) \text{ car } f \text{ est un morphisme} \\ &= \tilde{f}(x) \tilde{f}\left(x'\right)\end{aligned}$$

Donc $\tilde{f}$ est un morphisme de groupe.

$$\begin{aligned}x \in \ker \tilde{f} &\Leftrightarrow \tilde{f}(x) = f(g) = e' \\ &\Leftrightarrow g \in \ker f\end{aligned}$$

donc $x$ est dans l'image dans $\ker f$ dans $G/H$. (l'inclusion inverse est triviale)
□

# IV Propriétés des sous-groupes distingués

**Théorème 4.15.**

Soit $G$ un groupe, soit $H$ un sous-groupe de $G$, alors les propriétés suivantes sont équivalentes :

1. $H$ est normal.
2. $\forall x \in G, Hx = xH$
3. $\forall x \in G, xHx^{-1} = H$
4. $\forall x \in G, x^{-1}Hx = H$
5. $\forall x \in G, \forall h \in H, xhx^{-1} \in H$
6. $\forall x \in G, \forall h \in H, x^{-1}hx \in H$

*Démonstration.*

(1) $\Leftrightarrow$ (2) par définition.

(2) $\Leftrightarrow$ (3) :
"$\Rightarrow$" : Soit $x \in G$, $\forall h \in H$, $\exists h' \in H, xh = h'x$, donc $xhx^{-1} \in H$.
Soit $z \in xHx^{-1}$, $\exists h \in H, z = xhx^{-1}$, $hx \in Hx = xH$, alors $\exists h' \in H, hx = xh^{-1}$, donc $h = xh'x^{-1} \in xHx^{-1}$.
"$\Leftarrow$" : Soit $x \in G$, soit $z \in H$, $\exists h \in H, z = xh$. D'où $\underbrace{xhx^{-1}}_{\in H} = zX^{-1}$, donc $z \in HX$ donc

$$xH \subseteq Hx.$$

Soit $z \in Hx$, $\exists h \in H$, $z = hx$, donc $x^{-1}z = x^{-1}hx \in H$.

(3) $\Leftrightarrow$ (4) : Utiliser la bijection $x \mapsto x^{-1}$ .

(5) $\Leftrightarrow$ (6) : idem.

(5) $\Leftrightarrow$ (2) :
"$\Leftarrow$" : Soit $x \in G$, soit $h \in H$, $xh \in xH = Hx$, $\exists! h' \in H, xh = h'x$.
"$\Rightarrow$" : Soit $z \in Hx$, alors par hypothèse, $\exists h \in H, z = hx$, d'où $z \in xH$, d'où $Hx \subset Hx$. De même on montre que $xH \subset Hx$.

□

**Propriétés 4.16.**

Soient $G$ un groupe et $H$ et $K$ deux sous-groupe de $G$. On a alors :

$$H \triangleleft G \Rightarrow H \triangleleft K.$$

**Exemple 4.17.**

1. *Soit $G$ un groupe. On sait que $Int(G) \leq Aut(G)$, on a en fait $Int(G) \triangleleft Aut(G)$, en effet :*
   *Soit $\theta_g \in Int(G)$, $\alpha \in Aut(G)$. On doit montrer que : $\alpha \circ \theta_g \circ \alpha^{-1} \in Int(G)$, donc :*
   *Soit $x \in G$ :*

$$\begin{aligned} \alpha \circ \theta_g \circ \alpha^{-1}(x) &= \alpha\left(\theta_g\left(\alpha^{-1}(x)\right)\right) \\ &= \alpha\left(g\alpha^{-1}(x)\, g^{-1}\right) \\ &\text{or } \alpha \text{ est un morphisme} \\ &= \alpha(g)\,\alpha\left(\alpha^{-1}(x)\right)\alpha(g) \\ &= \alpha(g)\, x \alpha(g)^{-1} \\ \alpha \circ \theta_g \circ \alpha^{-1} &= \theta_{\alpha(g)} \end{aligned}$$

2. *Cas des groupes cycliques : $S_3$.*
   $S_3 = \langle \sigma, \tau \rangle$ *où* $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
   *soit $N = \langle \sigma \rangle = \left\{e, \sigma, \sigma^2\right\}$. Alors $N \triangleleft S_3$*
3. *Soit $G$ un groupe, alors $\mathcal{Z}(G) = \{a \in G, ax = xa, \forall x \in G\} \leq G$*
   *Montrons que $\mathcal{Z}(G) \triangleleft G$ :*
   *Soit $a \in \mathcal{Z}(G), x \in G$. Alors $xax^{-1} = axx^{-1} = a \in \mathcal{Z}(G)$. Donc $\mathcal{Z}(G) \triangleleft G$.*

**Proposition 4.18.**

Soit $G$ un groupe : Si $G/\mathcal{Z}(G)$ est monogène, alors $G$ est abélien.

*Démonstration.*
On sait d'emblée que $\mathcal{Z}(G)$ est distingué donc on peut parler de $G/\mathcal{Z}(G)$ comme d'un groupe.
Si $G$ est abélien, alors $\mathcal{Z}(G) = G$ donc

$$G/\mathcal{Z}(G) = G/G = (0)$$

donc le groupe est monogène.
Réciproquement, supposons $G/\mathcal{Z}(G)$ monogène. On pose $\pi : \begin{array}{ccc} G & \to & G/\mathcal{Z}(G) \\ x & \mapsto & \overline{x} \end{array}$ le morphisme quotient, supposons le groupe $G/\mathcal{Z}(G)$ monogène, alors $\exists a \in G, \forall x \in G, \exists n \in \mathcal{Z}, \overline{x} = \overline{a}^n$

Soient $x, y \in G$ on veut montrer que $xy = yx$. $\exists m, n \in ZZ$ tels que $\overline{x} = \overline{a}^m$,$\overline{y} = \overline{a}^n$ donc $\exists z_1, z_2 \in \mathcal{Z}(G)$ tel que $x = a^m z_1$ te $y = a^n z_2$. donc :

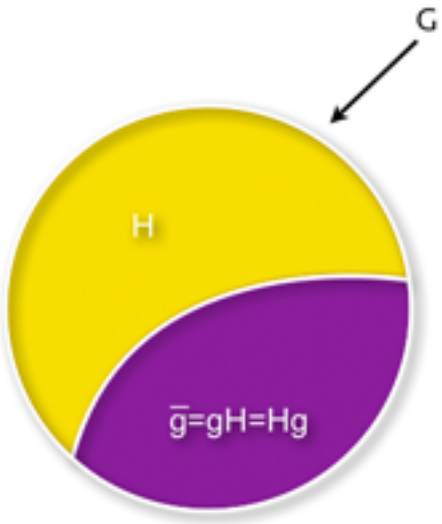
$$\begin{aligned} xy &= (a^m z_1)(a^n z_2) \\ &= a^m z_1 a^n z_2 \\ &= a^{m+n} z_1 z_2 \text{ car } z_i \in \mathcal{Z}(G) \\ &= a^{n+m} z_1 z_2 \\ xy &= yx \end{aligned}$$

□

**Proposition 4.19.**

Soit $G$ un groupe, soit $H$ un sous-groupe de $G$ d'indice 2.
alors $H \triangleleft G$.

*Démonstration.*
$H$ est d'indice 2 donc possède seulement deux classes d'équivalence dans le quotient. $H$ est déjà une classe d'équivalence.
$\forall g \in G$, soit :
$g \in H$, alors $gH = Hg = H$
$g \notin H$ alors $gH = H^c$ et $Hg = H^c$ car ce sont deux classes d'équivalence, et les deux classes d'équivalence partitionnent l'ensemble $G$, dans ce cas $gH = Hg$.
Dans tous les cas $gH = Hg$, donc $H \triangleleft G$. On peut expliquer cette démonstration par un dessin :




□

**Proposition 4.20.**

Soit $G$ un groupe, et $(H_i)_{i\in I}$ une famille de sous-groupes de $G$.
Si $\forall i \in I, H_i \triangleleft G$, alors $\bigcap_{i\in I} H_i \triangleleft G$.

*Démonstration.*
Soit $h \in \bigcap_{i\in I} H_i$, soit $x \in G$, alors $\forall i \in I$, $xH_ix^{-1} = H_i$. donc

$$x\left(\bigcap_{i\in I} H_i\right)x^{-1} = \bigcap_{i\in I} H_i.$$

□

**Propriétés 4.21** (Stabilité du caractère distingué d'un groupe)**.**

Soient $G, G'$ deux groupes, soit $f \in \mathrm{Hom}(G, G')$, alors on a les propriétés suivantes :

1. Si $H \triangleleft G$, alors $f(H) \triangleleft f(G)$.
   De plus si $f$ est surjective, $f(H) \triangleleft G'$
2. Si $H' \triangleleft G'$ alors $f^{-1}(H') \triangleleft G$.

*Démonstration.*

1. Soit $f(x) \in f(G)$, et $f(h) \in f(H)$. alors :
$$f(x) f(h) f(x)^{-1} = f\left(xhx^{-1}\right) \in f(H)$$
2. Soit $x \in G$, $h \in f^{-1}(H')$, montrons que $xhx^{-1} \in f^{-1}(H')$. on a :
$$\underbrace{f(x) f(h) f(x)^{-1}}_{\in H'} = f\left(xhx^{-1}\right) \in H'$$
$$xhx^{-1} \in f^{-1}\left(H'\right).$$

□

**Proposition 4.22.**

Soit $G$ un groupe et $H$ et $K$ des sous-groupes de $G$.

1. Si $H \triangleleft G$, alors $H \bigcap K \triangleleft K$.
2. Si $H \triangleleft G$, alors $HK$ est un sous-groupe de $G$ et $H \triangleleft HK$.

*Démonstration.*

1. soit $h \in H \bigcap K$, $k \in K$ alors a-t-on $khk^{-1} \in H \bigcap K$ ?
   $khk^{-1} \in H$ car $H \triangleleft G$
   $khk^{-1} \in K$ car $h, k, k^{-1} \in K$ donc
   $$khk^{-1} \in H \cap K.$$
2. On sait que $(HK \leq G) \Leftrightarrow (HK = KH)$
   Soit $h \in H$, et $k \in K$, alors $kh \in KH$. Comme $H \triangleleft G$, alors $khk^{-1} \in H$, donc $\exists h' \in H$ tel que $khk^{-1} = h'$. d'où $kh = h'k \in HK$ donc $KH \subseteq HK$. On pourrait de même montrer que $HK \subseteq KH$. On sait donc que $HK$ est un sous-groupe de $G$.
   $$H \triangleleft G, H \subset HK \Rightarrow H \triangleleft HK.$$

□

# V Classes de conjugaison et normalisateur

Soit $E$ un ensemble, on notera $\mathcal{P}(E)$ l'ensemble des parties de $E$.

**Définition 4.23** (Conjugaison par un élément d'un groupe)**.**

Soit $G$ un groupe, et $g \in G$ l'application :

$$\begin{array}{ccc} G & \to & G \\ x & \mapsto & gxg^{-1} \end{array}$$

est appelée la conjugaison par $g$ dans $G$.
Elle est noté $\text{Int}(g)$. On a déjà montre qu'il s'agissait d'un automorphisme de $G$, admettant une application inverse : $x \mapsto g^{-1}xg$
On définit la relation d'équivalence sur $G$ : "$y$ est est conjugué de "$x$" par : $\exists g \in G, x = gyg^{-1}$.
Les classes selon cette relation d'équivalence sont appelées les classes de conjugaison dans $G$.

*Démonstration.*

1. Réflexivité : $x = 1_G x 1_G^{-1}$
2. Symétrie : Si $\exists g \in G, x = gyg^{-1}$, alors $y = g^{-1}yg = \left(g^{-1}\right) x \left(g^{-1}\right)^{-1}$.
3. Transitivité : Soient $x, y, z \in G$, Si $\exists g, h \in G$ tels que $y = gxg^{-1}$ et $z = hyh^{-1}$, alors $z = hgxg^{-1}h^{-1} = (hg)\, x\, (hg)^{-1}$.

□

**Définition 4.24.**

Soit $G$ un groupe et $S$ un ensemble non vide dans $\mathcal{P}(E)$. On pose

$$S' \overset{\text{def}}{=} \left\{g \in G, \exists s \in S, g = xsx^{-1}\right\}$$

$$S' \in \mathcal{P}(E) \text{ est conjugé à } S \Leftrightarrow \exists x \in G, S' = xSx^{-1}$$

**Propriétés 4.25.**

La relation de conjugaison est une relation d'équivalence sur $\mathcal{P}(G)$ et par convention le conjugué de $\varnothing$ est $\varnothing$. La classe de conjugaison de $S \neq \varnothing$ modulo la relation de conjugaison est appelé classe de conjugaison de $S$, c'est l'ensemble $\left\{xSx^{-1}, x \in G\right\}$.

**Définition 4.26.**

Si $S \neq \varnothing$ et $S' \neq \varnothing$ telle que $S' = xSx^{-1}$ alors $S'$ est l'image ensemble de $S$ par l'automorphisme intérieur de $G$ associée à l'élément $x$.

**Propriétés 4.27.**

1. Deux parties conjuguées sont équipotentes. Évidement : si $G$ est une sous-partie finie, elles ont alors même cardinal.
2. Si $S = \{g\}$, on appellera la classe de conjugaison de $S$ classe de conjugaison de $g$.
3. Si $H$ est un sous-groupe de $G$. Tout conjugué de $H$ est un sous-groupe de $G$, isomorphe à $H$.

**Définition 4.28.**

Soit $G$ un groupe, soit $S \neq \varnothing$ une partie non vide de $G$. On appelle :

1. Normalisateur de $S$ dans $G$ l'ensemble :
$$N_G(S) \overset{\text{def}}{=} \left\{x \in G, xSx^{-1} = S\right\}$$
2. Centralisateur de $S$ dans $G$ :
$$C_G(S) \overset{\text{def}}{=} \left\{x \in G, \forall s \in S,\ xsx^{-1} = s\right\}.$$

**Remarque 4.29.**
*Cas du singleton : Si* $S = \{g\}$, $C_G(\{g\}) = N_G(\{g\})$.

**Propriétés 4.30.**

Soit $G$ un groupe et $S \neq \varnothing$ une partie non vide de $G$. On a les trois propriétés suivantes :

1. $N_G(\{S\}) \leq G$
2. $C_G(\{S\}) \leq G$
3. $C_G(\{S\}) \triangleleft N_G(\{S\})$.

*Démonstration.*
1) et 2) étant faciles à montrer, cela sera laissé au lecteur.
Montrons 3) , montrons déjà que $C_G(\{S\}) \triangleleft N_G(\{S\})$.
Soit $h \in C_G(\{S\}), x \in N_G(\{S\})$.
Il faut montrer que $xhx^{-1} \in C_G(S)$.
Soit $s \in S$, comme $h \in C_G(S)$, donc $\forall s \in S$, $hsh^{-1} = s$. Il faut montrer que $xhx^{-1}s\left(xhx^{-1}\right)^{-1} = s$. il est à noter que $N_G(S)$ étant un groupe, $x^{-1} \in N_G(S)$.

$$\begin{aligned}
xhx^{-1}s\left(xhx^{-1}\right)^{-1} &= xhx^{-1}sx(xh)^{-1} \\
&= xhx^{-1}sxh^{-1}x^{-1} \text{ Or } x^{-1}sx \in S \text{ car } x^{-1} \in N_G(X) \\
&= xh\left(x^{-1}sx\right)h^{-1}x^{-1} \\
&= x\left(x^{-1}sx\right)x^{-1} \text{ car } h \in N_G(S) \text{ et } x^{-1}sx \in S \\
&= xx^{-1}sxx^{-1} \\
&= s
\end{aligned}$$

D'où $C_G(\{S\}) \triangleleft N_G(\{S\})$. □

**Théorème 4.31.**

Soit $G$ un groupe, et $H$ un sous-groupe de $G$. On a alors l'équivalence :

$$H \triangleleft G \Leftrightarrow G = N_G(H).$$

*Démonstration.*
Ce'st un jeu de définition :

$$H \triangleleft G \Leftrightarrow \forall x \in G, xH = Hx$$

donc si $H \triangleleft G$, $N_G(H) = \left\{x \in G, xHx^{-1} = H\right\} = \{x \in G, xH = Hx\} = H$
De même si $N_G(H) = \left\{x \in G, xHx^{-1} = H\right\} = \{x \in G, xH = Hx\} = G$, alors $\forall x \in G$ on a $xH = Hx$, donc $H \triangleleft G$. □

**Proposition 4.32.**

Soit $G$ un groupe.

1. Si $H$ un sous-groupe de $G$ alors $H \triangleleft N_G(H)$
2. Si $H, K$ sont deux sous-groupes de $G$ tels que $H$ est un sous-groupe de $K$. Alors :

   $$H \triangleleft K \Rightarrow K \text{ est un sous-groupe de } N_G(H)$$

3. Si $H, K$ sont deux sous-groupes de $G$, si $K$ est un sous-groupe de $N_G(H)$, alors $HK$ est un sous-groupe de $G$ et $H \triangleleft HK$.

On sait donc que $N_G(H)$ est le plus grand sous-groupe de $G$ (au sens de l'inclusion) dans lequel $H$ est normal (distingué par rapport à $G$).

*Démonstration.*

1. On sait par définition du normalisateur que $H \subseteq N_G(H)$.
   Pour l'autre inclusion : soit $x \in N_G(H)$, alors $xHx^{-1} = H$, donc on a immédiatement que $H \triangleleft N_G(H)$.
2. Supposons que $H \leq K$.
   $H \triangleleft K$, $\forall k \in K$, $kHk^{-1} = H$, donc $\forall k \in K$, $k \in N_G(H)$
3. On sait que si $KH = HK$, alors $HK$ est un sous-groupe de $G$. Montrons ici que $KH = HK$. Soit $h \in H$ et $k \in K$, comme par hypothèse $K$ est un sous-groupe de $N_G(H)$, alors $k, h^{-1} \in N_G(H)$, donc $k^{-1}Hk = H$, donc $\exists h' \in H$ tel que $k^{-1}hk = k'$.

Donc $hk = kk' \in KH$ d'où $HK \subseteq KH$. De même on montre que $KH \subseteq HK$. Donc $HK$ est un sous-groupe de $G$.
Montrons a présent que $H \triangleleft HK$. Comme $H \triangleleft N_G(H)$, et $H \leq HK \leq N_G(H)$ on a $H \triangleleft HK$.

□

# VI Produit semi-direct d'un sous-groupe normal, pour un autre sous-groupe.

**Définition 4.33.**

Soit $G$ un groupe, $H$ et $N$ deux sous-groupes de $G$. On dit que $G$ est le produit semi-direct de $N$ par $H$ si :
- $N \triangleleft G$
- $G = NH$
- $N \bigcap H = (e)$

**Remarque 4.34.**
*Traduisons certains hypothèses :*
- *2) signifie que tout élément de $G$ s'écrit comme produit d'un élément de $N$ et de $H$ (dans l'ordre) :* $\forall g \in G, \exists x \in N, \exists y \in H, g = xy$.
- *3) traduit l'unicité de cette écriture : Soit* $g \in G, x, x' \in N, y, y' \in H$ *tels que* $xy = x'y' = g$, *alors :*

$$\underbrace{x^{-1}x}_{\in N} = \underbrace{y'y^{-1}}_{\in H} \in N \bigcap H$$

*donc*

$$x^{-1}x = y'y^{-1} = e$$

*d'où*

$$x = x' \text{ et } y = y'.$$

*Démonstration.*
Montrons que cette définition a un sens, c'est-a-dire que $G \simeq N \rtimes_\alpha H$, où :

$$\alpha : \begin{array}{ccc} H & \to & \mathrm{Aut}(N) \\ h & \mapsto & \left(g \mapsto hgh^{-1}\right) \end{array}.$$

$hgh^{-1} \in N$ car $N \triangleleft G$, et donc $g \mapsto hgh^{-1}$ est bien un automorphisme de $N$.
On rappelle que l'ensemble sous-jacent à $N \rtimes_\alpha H$ est $N \times H$, muni de la loi :

$$(g_1, h_1) * (g_2, h_2) = (g_1 \alpha(h_1, g_2), h_1 h_2)$$

Le but ici est donc de construire un isomorphisme entre $G$ et $N \rtimes_\alpha H$. Posons :

$$\varphi : \begin{array}{ccc} G & \to & N \rtimes_\alpha H \\ gh = x & \mapsto & (g,h) \end{array}$$

$$\psi : \begin{array}{ccc} N \rtimes_\alpha H & \to & G \\ (g,h) & \mapsto & gh \end{array}$$

Montrons a présent que $\varphi \in \mathrm{Hom}\,(G, N \rtimes_\alpha H)$.
Soient $g, g' \in N, h, h' \in H$, alors :

$$\begin{aligned} ghg'h' &= \left(ghg'h^{-1}\right) hh' \\ \varphi\left(ghg'h'\right) &= \left(ghg'h^{-1}, hh'\right) \\ \varphi(gh)\,\varphi\left(g'h'\right) &= (g,h) *_\alpha \left(g', h'\right) \\ &= \left(g\alpha\left(h, g'\right), hh'\right) \\ &= \left(ghg'h^{-1}, hh'\right) \end{aligned}$$

□

Voyons à présent quelques propriétés et propositions à propos des produits semi-direct des groupes.

**Proposition 4.35.**

Soit $G$ un groupe, supposons qu'il existe $N, H$ deux groupes tels que $G = N \rtimes_{\tilde{\alpha}} H$. Alors les applications :

$$\varphi : \begin{array}{ccc} H & \to & G \\ h & \mapsto & (e,h) \end{array}$$

$$\psi : \begin{array}{ccc} N & \to & G \\ x & \mapsto & (x,e) \end{array}$$

sont des morphisme de groupes injectifs.
De plus si $H' = \mathrm{Im}\varphi$ et $N' = \mathrm{Im}\psi$, alors :

$$G = N' \rtimes_{\tilde{\alpha}} H' = \mathrm{Im}\varphi \rtimes_{\tilde{\alpha}} \mathrm{Im}\psi.$$

*Démonstration.*
Il s'agit de vérifier que les sous-groupes $N'$ et $H'$ vérifient la définition suivante :

1. $N' \lhd G$, soit $(y,k) \in G$, $(x,e) \in N'$, on va montrer ainsi que

$$(y,k) *_\alpha (x,e) * (y,k)^{-1} \in N'$$

Or $(y,k)^{-1} = \left(\alpha\left(k^{-1},y\right)^{-1}, k^{-1}\right)$, donc :

$$\begin{aligned}(y,k) *_\alpha (x,e) * (y,k)^{-1} &= (y\ \alpha(k,x), k) *_\alpha \left(\alpha\left(k^{-1},y\right)^{-1}, k^{-1}\right)\\ &= \left(y\ \alpha(k,x)\,\alpha\left(k, \alpha\left(k^{-1},y\right)^{-1}\right), e\right)\\ &= \left(y\ \alpha(k,x)\,\alpha\left(k, \alpha\left(k^{-1},y^{-1}\right)\right), e\right)\\ &= \left(y\ \alpha(k,x)\,\alpha\left(k, \alpha\left(e,y^{-1}\right)\right), e\right)\\ &= \left(y\ \alpha(k,x)\,y^{-1}, e\right) \in \mathrm{Im}\psi = N'\end{aligned}$$

2. $G = N'H'$ : Comme $N' \triangleleft G$, on a $N'H' \leq G$, soit $(x,h) \in G$, donc :

$$\begin{aligned}\underbrace{(x,e)}_{\in N'} *_\alpha \underbrace{(e,h)}_{\in H'} &= (x\alpha(e,e), h)\\ &= (x,h)\end{aligned}$$

3. $N' \bigcap H' = (e)$ :

$$(x,h) \in N' \Leftrightarrow h = e$$
$$(x,h) \in H' \Leftrightarrow x = e$$

D'où le résultat.

On va à présent identifier tout élément $(x,h) \in G$ au produit $(x,e) * (e,h)$, que l'on notera plus simplement, par abus, $xh$.
Soit $x, y \in N$, et $h, k \in H$, alors :

$$\begin{aligned}xhyk &= (x,h) *_\alpha (y,k)\\ &= (x\alpha(h,k), hk)\\ x\alpha(h,y)\,hk\end{aligned}$$

Si on applique cette égalité à :

$$ehxh^{-1} = hxh^{-1} = e\alpha(h,x)\,hh' = \alpha(h,x).$$

□

# Chapitre 5

# Groupe quotient

## I Introduction et buts

On a vu précédemment que $G/H$ est muni d'une structure de groupe si $H$ est distingué. Développons ici cette notion. On a les outils nécessaires pour construire un groupe $Q$ qui vérifie la propriété universelle suivante :

- Il existe un morphisme de groupe surjectif : $\pi : G \to Q$
- Pour tout groupe $G'$ et tout morphisme $f \in \mathrm{Hom}(G, G')$ tel que $H \subset \ker f$, il existe un unique morphisme de groupe $\tilde{f} : G \to G'$ rendant commutatif le diagramme suivant :

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \tilde{f}} & \\ Q & & \end{array}$$

i.e

$$\tilde{f} \circ \pi = f.$$

**Théorème 5.1.**

Soit $G$ un groupe, et $H$ un groupe distingué de $G$. Alors l'ensemble quotient $G/H$ peut être muni d'une loi de groupe induite par celle de $G$, via la formule :

$$\forall x, y \in G, \overline{x} \cdot_{G/H} \overline{y} = \overline{x \cdot_G y}$$

En outre l'application canonique $\pi : \begin{array}{ccc} G & \to G/H \\ x & \mapsto & \overline{x} \end{array}$ est un morphisme de groupes surjectif.

*Démonstration.*

La preuve a été faite précédemment, ceci n'est en fait qu'un rappel. □

## II Définitions et construction

**Définition 5.2.**

Le quotient $G/H$ muni de la structure de groupe précédente est appelé groupe quotient.

**Théorème 5.3.**

Soit $G$ un groupe, et $H$ un sous-groupe de $G$. Alors :

$$(H \triangleleft G) \Leftrightarrow \left(\exists f \in \operatorname{Hom}\left(G, G'\right), H = \ker f\right)$$

*Démonstration.*
Le sens $\Leftarrow$ a déjà été montré.
Le sens $\Rightarrow$ : On cherche le noyau de $\pi$.

$$\pi^{-1}\left(\overline{e}\right) = \{x \in G, \pi\left(x\right) = \overline{x} = \overline{e}\}$$

$$\overline{x} = \overline{e} \Leftrightarrow x \in He = H$$

□

**Proposition 5.4.**

Soit $G$ un groupe, et $H$ un groupe distingue de $G$. Soit $G'$ un groupe et $f \in \operatorname{Hom}\left(G, G'\right)$.

1. $f$ surjectif $\Leftrightarrow$ $\tilde{f}$ surjectif
2. $\tilde{f}$ injectif $\Leftrightarrow$ $H = \ker f$
3. $\tilde{f}$ bijectif $\Leftrightarrow$ $H = \ker f$ et $f$ est surjectif.

*Démonstration.*

1. Si $\tilde{f}$ est surjectif, alors $f = \tilde{f} \circ \pi$ l'est comme composition d'applications surjectives.
   Si $f$ est surjectif, soit $y \in G'$, $\exists x \in G$ telle que $f\left(x\right) = y$ donc $\tilde{f}\left(\tilde{x}\right) = y$.

2. $H = \ker f$ soit $x \in G$, $\tilde{f}(\tilde{x}) = f(x) = e_G$ donc $x \in \ker f = H$ donc $\overline{x} = e_{G/H}$.
   Réciproquement, supposons que $\tilde{f}$ soit injectif, alors :

$$\tilde{f} \circ \pi = f$$

$$\ker f = \pi^{-1}\left(\tilde{f}\left(e_{G/H}\right)\right) = \pi^{-1}(e_G) = H$$

□

# III Application nilpotente de ces résultats

**Théorème 5.5.**

Soit $f \in \mathrm{Hom}(G, G')$, on sait que $\ker f \triangleleft G$, on peut factoriser $f : G \to G'$ par l'inclusion $\mathrm{Im} f \subset G'$, i.e on a un diagramme commutatif :

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ & \searrow^{\tilde{f}} & \uparrow \\ & & \mathrm{Im} f \end{array}$$

La restriction $f : G \to \mathrm{Im} f$ est un morphisme de groupe qui est surjectif. On a $\mathrm{Im} f \simeq G/\mathrm{Ker}\, f$.

# IV Sous-groupes quotient

**Théorème 5.6** (Théorème de correspondance des sous-groupes)**.**

Soit $G$ un groupe, soit $H$ un sous-groupe distingué $G$, soit $\pi : G \to G/H$ le morphisme canonique.
Alors les applications, $\pi_*, \pi^{-1}$ définissant par restrictions des bijections réciproques :

$$\pi_* : \{K \leq G, H \subset K\} \to \{J \leq G/H\}$$

$$\pi^{-1} : \{J \leq G/H\} \to \{K \leq G, H \subset K\}$$

*Démonstration.*
Si $K$ est un sous-groupe $G$, $\pi(K) \leq G/H$ on note $\overline{K}$ le représentant de $K$, alors $\pi^{-1}\left(\overline{K}\right) \leq G$

1. Restriction :
   Soit $\overline{K} \leq G/H$, $\overline{e} \in \overline{K}$ donc $\underbrace{\pi^{-1}(e)}_{=H} \subset \pi^{-1}\left(\overline{K}\right)$
2. Bijection :
   Soit $\overline{K} \leq G/H$, $\pi_* \circ \pi^{-1}\left(\overline{K}\right) = \pi\left(\pi^{-1}\left(\overline{K}\right)\right) = \overline{K}$ Soit $K$ un sous groupe de $G$ contenant $H$, montrons que $\pi^{-1}(\pi(K)) = K$.
3. $K \subset \pi^{-1}\pi(K)$
4. Soit $x \in \pi^{-1}\pi(K)$, alors $\exists k \in K$, $\underbrace{\pi(x)}_{=\overline{x}} = \pi(k) = \overline{k}$. $x \in HK$ mais $H \subseteq K$ donc $x \in K$.

□

**Remarque 5.7.**
*Soit $K$ un sous-groupe de $G$, contenant $H$, avec $H \triangleleft G$. On peut considérer :* $\pi_K : K \to K/H$ *donc* $\pi(K) = K/H$.

**Proposition 5.8.**

Soit $G$ un groupe, soit $H \triangleleft G$.
Soit $\pi : G \to G/H$ le morphisme canonique.
Soit $K$ un sous-groupe de $G$ tel que $H \nsubseteq HK$.
Alors $\overline{HK}$ est un sous-groupe de $G$ tel que $H \subset HK$ et $\pi(K) = HK/H$

*Démonstration.*
Comme $H$ est distingué ($H \triangleleft G$ ) alors $HK$ est un sous-groupe de $G$ et $H \triangleleft HK$.
Comme $H \subseteq HK$, $\pi(HK) = HK/K$, on va montrer que $\pi(K) = \pi(HK)$.
Soit $x \in G$, on a les équivalences suivantes :

$$\begin{aligned}
\overline{x} \in \pi(K) &\Leftrightarrow (\exists k \in K, x \in Hk) \\
\overline{x} \in \pi(K) &\Leftrightarrow (\exists k \in K, x \in HKk) \\
&\Leftrightarrow (\exists k \in K, x \in Hk) \text{ car } k \in K
\end{aligned}$$

□

**Corollaire 5.9.**

Soit $G = (\mathbb{Z}, +)$, soit $n \in \mathbb{N}$, $n \geq 2$. les sous-groupes de $\mathbb{Z}/(n)$ sont les ensembles de la forme $k\mathbb{Z}/n\mathbb{Z}$ avec $k|n$.

**Proposition 5.10.**

Soit $G$ un groupe et $H \triangleleft G$.

1. Si $K, K'$ sont deux sous-groupes de $G$ contenant $H$, alors :
$$K \leq K' \Rightarrow K/H \leq K'/H$$
2. $(H \leq K, K \triangleleft G) \Rightarrow (K/H \triangleleft G/H)$

*Démonstration.*

1. Soit $y \in K/H$. Alors il existe $k \in K$ tel que $y = kH$. Par hypothèse, $k \in K \subset K'$. Donc $kH \in K'/H$.
2. On note $\pi$ le morphisme de projection de $G$ sur $G/H$. $\pi$ est un morphisme surjectif donc l'image d'un groupe distingué est distinguée (Voir propriété 4.21). D'où $K/H = \pi(K) \triangleleft G/H$.

□

# Chapitre 6

# Premier exemple de groupes : Groupes monogènes

## I Généralités

**Définition 6.1.**

Un groupe $G$ est dit monogène s'il existe $x \in G$ tel que $G = \langle x \rangle$
Un groupe $G$ est dit cyclique s'il est monogène et fini.
Selon les notations :

- $\langle x \rangle = \left\{x^k, k \in \mathbb{Z}\right\}$
- $\langle x \rangle = \{kx, k \in \mathbb{Z}\}$.

**Lemme 6.2.**

Soient $G, G'$ deux groupes.
Soit $f : G \to G'$ un morphisme de groupes.
Si $G$ est monogène, alors $\mathrm{Im} f$ est monogène.

*Démonstration.*
$\exists x \in G$, $G = \langle x \rangle = \left\{x^k, k \in \mathbb{Z}\right\}$ donc

$$F(G) = \left\{f(x)^k, k \in \mathbb{Z}\right\} = \langle f(x) \rangle$$

donc $\mathrm{Im} f$ est un groupe monogène. □

**Corollaire 6.3.**

$\forall n \in \mathbb{N}, \mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique.

*Démonstration.*
$\langle 1 \rangle = \mathbb{Z} \quad \to \quad Z/(n)$ est surjectif. on peut donc appliquer le lemme et comme $\mathbb{Z}/(n)$ est un ensemble fini, la groupe associé est cyclique. □

**Théorème 6.4.**

Soit $G$ un groupe monogène, alors on a deux possibilités :
- Soit $G \simeq \mathbb{Z}$ ($G$ est alors infini)
- $\exists n \in \mathbb{N}^*$, $G \simeq \mathbb{Z}/n\mathbb{Z}$

*Démonstration.*
Par hypothèse, il existe $x \in G$ tel que $G = \langle x \rangle$.
On construit $\varphi : \begin{array}{ccc} \mathbb{Z} & \to & G \\ x & \mapsto & x^k \end{array} \in \mathrm{Hom}(\mathbb{Z}, G)$ est qui surjectif.
Soit $\ker \varphi = (0)$ et alors $\varphi$ injectif.

$$G \simeq \mathbb{Z}$$

Soit $\ker \varphi \neq (0)$, alors $\ker \varphi \leq \mathbb{Z}$, donc $\exists n \in \mathbb{Z}, \ker \varphi = n\mathbb{Z}$, et donc $\phi$ se factorise par un $\tilde{\varphi} : \mathbb{Z}/n\mathbb{Z} \to G$ bijectif. □

**Corollaire 6.5.**

On a les deux propriétés suivantes :

1. Deux groupes monogènes infinis sont isomorphes.
2. Deux groupes cycliques de même ordre sont isomorphes.

Par consequent, a isomorphisme près, les seuls groupes monogènes sont :

$$\mathbb{Z}, (\mathbb{Z}/n\mathbb{Z})_{n \in N^*}$$

**Remarque 6.6.**
*Soit $G$ un groupe cyclique, d'ordre $n$, alors :*

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \ldots, \overline{n-1}\right\}$$

$$G = \left\{e, x, \ldots, x^{n-1}\right\}$$

$$1 \leq k \leq n-1 \Leftrightarrow 1 \leq n-k \leq n-1$$

*On peut montrer que $x^{n-k}$ symétrique de $x^k$ $\forall k \in [\![1, n]\!]$*

**Proposition 6.7.**

Soit $G = \langle x \rangle$ un groupe cyclique d'ordre $n$, alors :

$$\left(\exists k \in \mathbb{Z}, \text{ et } x^k = e\right) \Leftrightarrow k \in n\mathbb{Z}$$

et $n$ est le plus petit entier strictement positif tel que $x^n = e$.

*Démonstration.*
On a le morphisme surjectif $\varphi_x : \begin{array}{ccc} \mathbb{Z} & \to & G \\ k & \mapsto & x^k \end{array}$

$$x^k = e \Leftrightarrow k \in \ker \varphi \Rightarrow k \in n\mathbb{Z}.$$

□

**Exemple 6.8.**

1. *$\mathcal{U}_n$ l'ensemble des racines $n-$ème de l'unité est un groupe cyclique d'ordre $n$.*
2. *Soit $G$ un groupe fini d'ordre $p$, $p$ premier. Donc $p \geq 2$, $\exists x \in G \setminus \{e\}$ telle que $\langle x \rangle$ est un sous-groupe de $G$. Par le théorème de Lagrange, on a :*
$$o(x) \,|\, o(G) = p$$

# II Sous-groupes d'un groupe monogène

**Théorème 6.9** (Sous groupe d'un groupe monogène infini ou cyclique)**.**

1. Soit $G$ un groupe monogène infini.
Si $H$ un sous-groupe de $G$ non réduit à $(e_G)$, alors $H$ est un groupe monogène infini.
2. Soit $G$ un groupe cyclique, alors si $H$ est un sous-groupe de $G$, $H$ est un groupe cyclique.

*Démonstration.*
On se ramène à l'étude de $\mathbb{Z}$ ou de $\mathbb{Z}/n\mathbb{Z}$, via l'isomorphisme $\varphi$ énoncé précédemment.

1. Pour $\mathbb{Z}$, les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, $n \in \mathbb{N}^*$, donc sont infini pour $n \geq 1$.

2. Si $n \neq 0$, $\mathbb{Z}/n\mathbb{Z}$ est cyclique. Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ correspondent aux images des sous-groupes de $\mathbb{Z}$ contenant $n\mathbb{Z}$ ( $k\mathbb{Z}$ avec $k|n$ ).
Si $\overline{K}$ est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$, $\exists k \in \mathbb{Z}$ tel que $k|n$ tels que $\overline{K} = \pi(k\mathbb{Z})$. $\overline{K}$ est l'image d'un groupe monogène par un morphisme surjectif, donc il est monogène.
De plus il est fini, donc $\overline{K}$ est cyclique.

□

**Proposition 6.10** (Caractérisation des sous-groupes d'ordre divisant l'ordre du groupe)**.**

Soit $G = \langle x \rangle$ un un groupe cyclique, d'ordre $n \geq 1$. Alors pour tout diviseur $d$ de $n$ dans $\mathbb{N}$, il existe un unique sous-groupe $H_d$ d'ordre $d$ de $G$.
En outre : $H_d = \left\langle x^{\frac{n}{d}} \right\rangle$
En d'autres termes, il existe une bijection :

$$\varphi : \begin{array}{ccc} \{d, d \in \mathbb{N} \text{ et } d|n\} & \to & \{H, H \text{ sous-groupe de } G\} \\ k & \mapsto & \langle x^k \rangle \end{array}$$

*Démonstration.*

1. Réduction du problème à $\mathbb{Z}/n\mathbb{Z}$ :
Considérons l'isomorphisme de groupes suivant :

$$\overline{\psi} : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & G \\ \overline{k} & \mapsto & x^k \end{array}$$

Pour cet isomorphisme, on observe que les sous-groupes de $G$ sont images de sous-groupes de $\mathbb{Z}/n\mathbb{Z}$. On est donc réduits à étudier la validité de l'énoncé dans le cas $\mathbb{Z}/n\mathbb{Z}$

2. Cas $\mathbb{Z}/n\mathbb{Z}$. On considère l'application

$$\varphi : \begin{array}{ccc} \{\text{diviseurs de } n\} & \to & \{\text{sous-groupes de } \mathbb{Z}/n\mathbb{Z}\} \\ k & \mapsto & \langle \overline{k} \rangle \end{array}$$

Montrons que $\varphi$ est surjective. Soit $\overline{K}$ un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. On pose $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ le morphisme quotient.

$$n\mathbb{Z} = \pi^{-1}\left(\overline{0}\right) \subset \pi^{-1}\left(\overline{K}\right) = k\mathbb{Z}$$

Par surjectivité de $\pi$ : $\overline{K} = \pi(k\mathbb{Z}) = \langle \overline{k} \rangle$ et $k|n$.

3. Quel est l'ordre de $\overrightarrow{K} = \langle \overline{k} \rangle$
   C'est le plus petit entier $m$ tel que $m\overline{k} = \overline{0} \Leftrightarrow \pi(\overline{m}k) = \pi(n) \Leftrightarrow n|mk$. Mais $k|n$ donc
   $$\mathrm{o}\left(\overline{K}\right) = \frac{n}{k}$$
   Montrons l'injectivité de $\varphi$, soient $k, k'$ deux diviseurs de $n$, distincts.
   $$\varphi(k) = \langle \overline{k} \rangle, \varphi\left(k'\right) = \langle \overline{k'} \rangle$$
   Ces deux groupes sont bien distincts puisque :
   $$\mathrm{o}\langle k \rangle = \frac{n}{k} \neq \frac{n}{k'} = \mathrm{o}\langle k' \rangle$$

□

**Exemple 6.11.**
*On peut lister les sous-groupes de* $\langle \overline{6} \rangle$*, car ses diviseurs positifs sont* $1, 2, 3, 6$*. Donc par l'énoncé précédent, les sous groupes sont :*
- $\langle \overline{1} \rangle = \mathbb{Z}/(6)$
- $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}\}$
- $\langle \overline{3} \rangle = \{\overline{0}, \overline{3}\}$

*Il est à noter que* $\langle \overline{4} \rangle$ *et* $\langle \overline{5} \rangle$ *sont déjà dans la liste de ces trois groupes.*

**Corollaire 6.12** (Nombre de sous-groupes d'un groupe cyclique)**.**

Si $G$ est un groupe cyclique d'ordre $n \geq 1$, alors le nombre de sous-groupes de $G$ est égal au nombre de diviseurs de $n$ dans $\mathbb{N}$. En d'autre terme : Si $G$ est un groupe cyclique,

$$\text{Card } \{H, H \leq G\} = \text{Card } \{m \in \mathbb{N}, m \mid \mathrm{o}(G)\}$$

**Proposition 6.13.**

Soit $G \neq (e)$ un groupe. On a l'équivalence suivante :
Les sous-groupes de $G$ sont exactement $(e)$ et $G$ si et seulement si $G$ est un groupe cyclique d'ordre premier.

*Démonstration.*
2) $\Rightarrow$ 1) : Lagrange.
1) $\Rightarrow$ 2) : $\exists x \in G$ tel que $x \neq e$. On a donc $\langle x \rangle \neq ()$, et $\langle x \rangle = G$ par hypothèse. On a trois choix :
- $G$ est infini, donc $G \simeq \mathbb{Z}$
- $G$ possède une infinité de sous-groupes propres, ce qui est impossible.
- $G$ est cyclique donc $\mathrm{o}(G)$ est premier, par le théorème précédent.

□

# III Générateur d'un groupe cyclique

## 1 Généralités

**Théorème 6.14.**

Soit $G = \langle x \rangle$ un groupe monogène alors on a deux possibilités :
- Si $G$ est infini, les seuls générateurs de $G$ sont $x$ et $x^{-1}$
- Si $G$ est cyclique, d'ordre $n \geq 2$, alors : l'ensemble des générateurs de $G$ est formé des éléments $x^k$, où $k$ est premier avec $n$

Pour rappel, on sait par Bezout que :

$$\begin{aligned}(k,n) = 1 &\Leftrightarrow \exists u, v \in \mathbb{Z}, uk + nv = 1 \\ &\Leftrightarrow \exists u \in \mathbb{Z}, \overline{u}\overline{k} = \overline{1} \text{ dans } \mathbb{Z}/n\mathbb{Z} \\ &\Leftrightarrow \overline{k} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z}\end{aligned}$$

*Démonstration.*

1. Pour trouver les générateurs d'un espace particulier, on peut tenter de construire un isomorphisme entre un espace de départ simple, dont les générateurs sont connus, et cet espace. Les générateurs seront alors les images par l'isomorphisme des générateurs de l'espace de départs.
   $\psi : \begin{array}{ccc} \mathbb{Z} & \to & G \\ k & \mapsto & x^k \end{array}$ est un isomorphisme. Les générateurs de $G$ sont donc les images des générateurs de $\mathbb{Z}$ qui sont 1 et $-1$. Cela conclut la preuve.
2. Supposons $G$ cyclique. On veut les entiers $k \in \mathbb{Z}$ tels que $\langle x^k \rangle = G$. Montrons au préalable le lemme suivant :

   **Lemme 6.15.**

   Soit $G = \langle x \rangle$ un groupe monogène. On a alors l'équivalence suivante : $\langle x^k \rangle = G$ si et seulement si $\exists m \in \mathbb{Z}, x = x^{km}$

   *Démonstration.*
   Supposons $\langle x^k \rangle = G$, alors soit $y \in G$, $\exists m \in \mathbb{Z}$ tel que $y = \left(x^k\right)^m = x^{km}$.
   Supposons qu'il existe $m \in \mathbb{Z}$ tel que $x = x^{km}$, alors comme $\forall g \in G$, $\exists t \in \mathbb{Z}, g = x^t$, d'où $g = x^{kmt}$ □

alors :

$$\begin{aligned}\left\langle x^k \right\rangle = G &\Leftrightarrow \exists m \in \mathbb{Z}, x = x^{km} \\ &\Leftrightarrow \exists m \in \mathbb{Z}, 1 = x^{km-1} \\ &\Leftrightarrow \exists m \in \mathbb{Z}, n | km - 1 \\ &\Leftrightarrow \exists m, q \in \mathbb{Z}, km = 1 + qn \\ &\Leftrightarrow (k, n) = 1 \text{ par Bezout}\end{aligned}$$

□

**Définition 6.16** (Indicatrice d'Euler)**.**

On appelle indicatrice d'Euler l'application : $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ définit par :

- $\varphi(1) = 1$
- $\varphi(n) =$ le nombre de sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Soit le nombre d'entiers $1 \leq k \leq n-1$ tels que $(k, n) = 1$, si $n \geq 2$.

**Lemme 6.17.**

Soient $a, b \in \mathbb{N}^*$, tels que $a$ et $b$ soient premier entre eux, alors

$$\varphi(ab) = \varphi(a)\varphi(b)$$

*Démonstration.* C'est une conséquence du théorème des restes chinois, démontré un peu plus loin. □

Calcul de $\phi(n)$ :

- Cas $n^k$ avec $n$ premier. Parmi les $n^k$ entiers de 1 à $n^k$, ceux qui ne sont pas premiers avec $n^k$ sont ceux divisibles par $n$, et il y en a $n^{k-1}$. $\varphi\left(n^k\right) = n^k - n^{k-1}$.
- Sinon, décomposition en facteurs premiers : Si $n = \prod_{i=1}^{r} p_i^{k_i}$ où les $p_i$ sont premiers, on a :

$$\varphi\left(\prod_{i=1}^{r} p_i^{k_i}\right) = \prod_{i=1}^{r} \varphi\left(p_i^{k_i}\right)$$

D'où :

$$\varphi(n) = \prod_{i=1}^{r} p_i^k - p_i^{k_i}$$

**Proposition 6.18.**

Soit $n \in \mathbb{N}^*, n \geq 2$, les générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les éléments inversibles (pour la multiplication) de $\mathbb{Z}/n\mathbb{Z}$ et leur ensemble forme un groupe multiplicatif abélien de cardinal $\varphi(n)$.

*Démonstration.*
$(k, n) = 1 \Leftrightarrow k \in \mathbb{Z}/n\mathbb{Z}^\times$ dans $\mathbb{Z}$. Soit $U_n \overset{\text{def}}{=} \{k \in \mathbb{Z}, (k, n) = 1\}$, $\varphi(n) =$ Card $U_n$. On a une loi de composition de $U_n$ :

$$\begin{array}{ccc} U_n \times U_n & \to & U_n \\ \left(\overline{k}, \overline{k'}\right) & \mapsto & \overline{kk'} \end{array}$$

Cela définit une application qui satisfait aux conditions de loi de composition interne, commutative. □

Montrer en exercice :
Si $n$ est un nombre premier, montrer que $U_n = (\mathbb{Z}/n\mathbb{Z})/\left\{\overline{0}\right\}$

## 2 Théorème des restes chinois

On veut savoir si le produit direct de groupes cycliques est un groupe cyclique.

**Proposition 6.19.**

Si $G$ et $G'$ sont deux groupes, si $G \times G'$ est cyclique alors $G$ et $G'$ le sont.

*Démonstration.*
$G$ est isomorphe à un sous-groupe de $G \times G'$ , en particulier au groupe $G \times \{e'_G\}$, qui est cyclique comme sous-groupe d'un groupe cyclique. Donc $G$ est cyclique. On applique le même raisonnement pour $G'$. □

Cependant, la réciproque est fausse, on peut prendre en contre-exemple : $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$ sont cycliques, mais $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ est d'ordre 8 et non cyclique : aucun élément de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ n'est d'ordre 8 : Énumérons les éléments de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

1. $(0, 0)$ d'ordre 1
2. $(0, 1)$ d'ordre 4
3. $(0, 2)$ d'ordre 2
4. $(0, 3)$ d'ordre 4

5. $(1,0)$ d'ordre 2
6. $(1,1)$ d'ordre 4
7. $(1,2)$ d'ordre 2
8. $(1,3)$ d'ordre 4.

Le grand résultat de ce chapitre est :

**Théorème 6.20** (Produit direct de groupe cyclique)**.**

Soient $G$ et $G'$ deux groupes cycliques, d'ordres respectifs $n$ et $m$. $G \times G'$ est cyclique $\Leftrightarrow (n,m) = 1$.

Comment va-t-on le montrer ? On va se ramener au cas $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
En effet : ($G \times G'$ est cyclique ) $\Leftrightarrow$ ($G \times G'$ est isomorphe à un groupe cyclique d'ordre $mn$)
On a le diagramme suivant :

$$\begin{array}{ccc} G \times G' & \xrightarrow{\sim} & G'' \\ \downarrow{\scriptstyle \overline{\psi}\times\overline{\psi}} & & \downarrow{\scriptstyle \psi} \\ \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\sim} & \mathbb{Z}/mn\mathbb{Z} \end{array}$$

**Théorème 6.21** (Théorème des restes chinois)**.**

Soient $m, n \in \mathbb{N}$, où $m, n \geq 2$.
Les groupes $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/mn\mathbb{Z}$ sont isomorphes si et seulement si $(m,n) = 1$.

*Démonstration.*
Posons $f : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ z & \mapsto & (\overline{x}, \overline{x}) \end{array}$ On peut montrer que $f$ est un morphisme de groupe.
Montrons tout d'abord le lemme suivant :

**Lemme 6.22.**

Soit $m, n \in \mathbb{N}$, $m, n \geq 2$, alors :

$$n\mathbb{Z} \bigcap m\mathbb{Z} = \text{ppcm}\,(m,n)\,\mathbb{Z}$$

De plus c'est un groupe.

*Démonstration du lemme.*

$$\begin{aligned} n' \in n\mathbb{Z} \bigcap m\mathbb{Z} &\Leftrightarrow n|n' \text{ et } m|n' \\ &\Leftrightarrow \text{ppcm}\,(n,m)\,|n' \\ &\Leftrightarrow n' \in \text{ppcm}\,(n,m)\,\mathbb{Z} \end{aligned}$$

□

**Retour à la démonstration**
Noyau de $f$ : Soit $x \in \mathbb{Z}$,

$$f(x) = \left(\overline{0}, \overline{0}\right) \Leftrightarrow m|x \text{ et } n|x$$

$\ker f = n\mathbb{Z} \bigcap m\mathbb{Z} = \text{ppcm}\,(m,n)\,\mathbb{Z}$ donc : $(m,n) = 1 \Rightarrow \text{pccm}\,(m,n) = mn$.
Le lemme de factorisation des morphismes de groupes donne :

$$\text{Im}f \simeq (\mathbb{Z}/mn\mathbb{Z}) \text{ si } (m,n) = 1$$

$f$ est un morphisme de groupes à valeurs dans un groupe d'ordre $mn$, donc $f$ surjectif $\Leftrightarrow (m,n) = 1$.
Donc $f$ induit un isomorphisme $\Leftrightarrow (m,n) = 1$ □

**Corollaire 6.23.**

Soit $k \in \mathbb{N}$, $k \geq 2$ , soient $m_1, \ldots, m_k \in \mathbb{N}$, avec $\forall i \in [\![1,k]\!], m_i \geq 2$ alors :

$(\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$ est isomorphe a $\mathbb{Z}/m_1 \ldots m_k\mathbb{Z}) \Leftrightarrow$
(les entiers $m_i$ sont premiers entre deux 2 à 2)

# Chapitre 7

# Deuxième exemple de groupes : Groupes symétriques

**Définition 7.1** (Permutation)**.**

Soit $X$ un ensemble, une permutation d'un ensemble $X$ est une bijection de $X$ sur lui-même.
En particulier une permutation de $n$ éléments, $n \in \mathbb{N}$ est une bijection d'un ensemble fini de cardinal $n$ sur lui-même.

**Définition 7.2** (Groupe symétrique)**.**

Soit $n \geq 1$, le groupe symétrique $\mathrm{S}_n$ est l'ensemble des permutations de $\{1, \ldots, n\}$.
La loi de composition des applications munit cet ensemble d'une structure de groupes, ce groupe est d'ordre $n!$ et non abélien dès que $n \geq 3$

On rappelle le théorème de Cayley, énoncé en 2

**Théorème 7.3** (Rappel : Théorème de Caley)**.**

Tout groupe $G$ est isomorphe à un sous-groupe de son groupe de permutations, $\mathrm{S}_G$.

**Définition 7.4.**

Soit $\sigma \in \mathrm{S}_n$, on appelle support de $\sigma$ l'ensemble $\mathrm{Supp}(\sigma)$ :

$$\mathrm{Supp}(\sigma) \overset{\text{def}}{=} \{i \in [\![1, n]\!], \sigma(i) \neq i\}$$

Le support de $\sigma$ est l'ensemble des indices qui sont changés par $\sigma$

**Exemple 7.5.**
*Soit $\sigma \in S_n$,*

$$Supp(\sigma) = \varnothing \Leftrightarrow \sigma = Id$$

**Lemme 7.6.**

Soit $n \in \mathbb{N}^*$, $\sigma \in \mathrm{S}_n$, alors

$$\sigma(\mathrm{Supp}(\sigma)) = \mathrm{Supp}(\sigma)$$

*Démonstration.*
Soit $i \in \mathrm{Supp}(\sigma)$ posons $j \overset{\text{def}}{=} \sigma(i)$
Supposons que $j \notin \mathrm{Supp}(\sigma)$,

$$\sigma(j) = j = \sigma(i)$$

donc $i = j = \sigma(i)$ : ce qui est une contradiction.
Donc $j \in \mathrm{Supp}(\sigma)$. □

**Proposition 7.7.**

Soit $n \in \mathbb{N}^*$, alors deux permutations $\sigma, \sigma' \in \mathrm{S}_n$ de supports disjoints commutent.

*Démonstration.*
Si $n = 1$ l'énoncé est évident.
Si $\sigma$ ou $\sigma' = \mathrm{Id}$, le résultat est encore évident.
Sinon, soit $i \in \mathrm{Supp}(\sigma)$, alors $i \notin \mathrm{Supp}(\sigma')$ et $\sigma(i) \notin \mathrm{Supp}(\sigma')$ par le lemme.

$$\begin{aligned} \sigma \circ \sigma'(i) &= \sigma(i) \\ &= \sigma' \circ \sigma(i) \\ &= \sigma(i) \end{aligned}$$

Si $i \notin \text{Supp}(\sigma)$, c'est le même raisonnement.
Si $i \notin \text{Supp}(\sigma) \cup \text{Supp}(\sigma')$, alors :

$$\sigma \circ \sigma'(i) = \sigma(i) = \sigma' \circ \sigma(i).$$

□

À toute permutation $\sigma \in \mathrm{S}_n$, on peut associer la relation binaire $\mathcal{R}_\sigma$ définie sur $[\![1, n]\!]$ par

$$i \mathcal{R}_\sigma j \Leftrightarrow \exists r \in \mathbb{Z}, j = \sigma^r(i)$$

**Propriétés 7.8.**

$\mathcal{R}_\sigma$ est une relation d'équivalence.

**Définition 7.9** (Classe d'équivalence)**.**

Soit $\sigma \in \mathrm{S}_n$, $\forall i \in [\![1, n]\!]$, on note $\Omega_\sigma(i)$ la classe d'équivalence de $i$ pour la relation $\mathcal{R}_\sigma$ :

$$\Omega_\sigma(i) \overset{\text{def}}{=} \{\sigma^r(i), r \in \mathbb{Z}\}$$

On appelle cet ensemble la $\sigma-$orbite de $i$.

**Exemple 7.10.**

1. *Soit $i \notin Supp(\sigma)$, alors $\Omega_\sigma(i) = \{i\}$*
2. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$ *on a les $\sigma-$ orbites :*
   $\Omega_\sigma(1) = \{1, 3, 5\}$ $\Omega_\sigma(2) = \{2\}$, $\Omega_\sigma(4) = \{4, 6\}$

**Définition 7.11.**

Une permutation $\gamma \in \mathrm{S}_n$ est appelé **cycle de longueur** $r$, ou $r$-cycle, avec $r \in [\![1, n]\!]$ si il existe une suite ordonnée de $r$ entiers $j_1, \ldots, j_r \in [\![1, r]\!]$ telle que

$$\gamma(j_1) = j_2, \gamma(j_2) = j_3, \ldots \gamma(j_r) = j_1$$

et

$$\forall k \in [\![1, n]\!] \setminus \{j_1, \ldots, j_r\}, \gamma(k) = k$$

Un tel cycle est noté $\gamma = (j_1, j_2 \ldots, j_r)$

**Définition 7.12** (Ordre d'une permutation)**.**

Soit $\gamma \in \mathrm{S}_n$ un cycle. On appelle longueur de $\gamma$ l'ordre de $\gamma$ comme élément de $\mathrm{S}_n$, ou, de manière équivalente, le cardinal du support de $\gamma$.

$$\mathrm{o}(\gamma) = \mathrm{Card}\ \mathrm{Supp}\gamma$$

**Propriétés 7.13.**

1. $\mathrm{Supp}\gamma = \{j_1, \ldots, j_r\}$
2. Tout cycle de longueur 1 est égal à l'identité :

$$\gamma = (j) \Leftrightarrow \gamma(j) = j \text{ et } \forall k \in [\![1, n]\!] \setminus \{j\},\ \gamma(k) = k$$

**Exemple 7.14.**
$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix}$ *alors on a* $\mathrm{Supp}\gamma = \{2, 4, 5, 6\}$*, c'est un cycle de longueur 4.*

**Définition 7.15.**

Sot $n \geq 2$, un cycle de longueur 2 dans $\mathrm{S}_n$ est appelé transposition.

**Proposition 7.16.**

Soit $n \geq 1$, tout $r-$cycle dans $\mathrm{S}_n$ est d'ordre $r$.

*Démonstration.*
Soit $\gamma$ un $r-$cycle dans $\mathrm{S}_n$. Alors $\langle\gamma\rangle$ est de cardinal $r$ et donc $\gamma$ est d'ordre $r$. □

**Corollaire 7.17.**

Soit $n \geq 2$ soit $\gamma$ une transposition de $\mathrm{S}_k$ alors $\gamma = \gamma^{-1}$.

**Théorème 7.18** (Décomposition unique en cycles disjoints)**.**

Soit $n \in \mathbb{N}^*$, toute permutation $\sigma \neq \mathrm{Id}$ dans $\mathrm{S}_n$ s'écrit sous la forme

$$\sigma = \gamma_1 \circ \gamma_2 \circ, \ldots, \circ \gamma_s$$

où $s \in \mathbb{N}^*$ et $\gamma_1, \ldots, \gamma_s$ sont des cycles disjoints tous différents de $Id$. En outre cette décomposition est unique a l'ordre des facteurs près, on appelle cette décomposition **la décomposition canonique** de $\sigma$.

La démonstration sera admise pour le moment.

**Corollaire 7.19.**

Soit $n \in \mathbb{N}^*$, et $\sigma \in \mathrm{S}_n, \sigma \neq \mathrm{Id}$, en reprenant les notations du théorème, si on note

$$\sigma = \gamma_1 \circ \gamma_2 \circ, \ldots, \circ \gamma_s$$

la décomposition canonique de $\sigma$, l'ordre de $\sigma$ est $\mathrm{o}(\sigma)$ et vaut :

$$\mathrm{o}(\sigma) = \mathrm{ppcm}\left(\mathrm{o}(\gamma_1), \ldots, \mathrm{o}(\gamma_s)\right)$$

de plus, un résultat utile est que $\forall t \in \mathbb{N}^*$,

$$\sigma^t = \gamma_1^t \ldots \gamma_n^t$$

*Démonstration.*
On pose $m \overset{\text{def}}{=} \mathrm{ppcm}\left(\mathrm{o}(\gamma_1), \ldots, \mathrm{o}(\gamma_s)\right)$
Soit $t \in \mathbb{N}*$, on a $\mathrm{Supp}\gamma_i^t \subset \mathrm{Supp}\gamma_i$ donc les permutations $\gamma_1^t, \ldots, \gamma_s^t$ restent disjointes, donc commutent. d'où :

$$\sigma^t = \gamma_1^t \ldots \gamma_n^t.$$

Pour $m = t$ on a $\sigma^m = \gamma_1^m \ldots \gamma_n^m = \mathrm{Id}_E$ par définition du ppcm.
et pour $l \overset{\text{def}}{=} \mathrm{o}(\sigma)$ on a $\sigma^l = \mathrm{Id}_E$ donc

$$\gamma_1^l \ldots \gamma_n^l = \mathrm{Id}_E$$

Comme $\mathrm{Supp}\,\mathrm{Id}_E = \varnothing$, $\mathrm{Supp}\,\mathrm{Id}_E = \bigcup_{i=1}^{s} \mathrm{Supp}\,\gamma_i^l$ donc $\mathrm{Supp}\,\gamma_i^l = \varnothing \ \forall i \in [\![1, s]\!]$,
donc : $l$ est multiple de $m$ d'où $\mathrm{o}(\sigma) = m$ □

**Exemple 7.20.**
*Si* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix}$ *alors* $\sigma = (1,5,3)\,(4,6)$

Voici un autre théorème de décomposition, mais où les supports n'ont pas à être disjoints et où la décomposition n'est pas unique, l'avantage est ici de décomposer en produit de transpositions.

**Théorème 7.21** (Décomposition des permutation en produit de transpositions)**.**

Soit $n \geq 2$
Tout permutation $\sigma \neq \mathrm{Id}$ de $\mathrm{S}_n$ se décompose de manière **non unique** en un produit de transpositions.

*Démonstration.*
On raisonnera par récurrence sur $n$.

**Initialisation :** Pour $n = 2$, $\mathrm{S}_2 = \{\mathrm{Id}, (1,2)\}$, $(1,2)$ est le produit d'une seule transposition.

**Hérédité :** soit $n \in \mathbb{N}^*$, supposons que toute permutation de $[\![1, n]\!]$ peut se décomposer comme produit de transpositions dans $\mathrm{S}_n$. Soit $\sigma \in S_{k+1}$. On a deux cas :
Premier cas : La permutation laisse $n+1$ inchangée. On note alors $\sigma'$ sa restriction sur $[\![1, n]\!]$. On peut alors la décomposer en produits de transpositions $\gamma_i$ dans $[\![1, n]\!]$, $\sigma'_k = \gamma_1 \dots \gamma_p$, $p \in \mathbb{N}$. et on a même $\sigma = \gamma_1 \dots \gamma_p$
Second cas : $\sigma(n+1) \neq n+1$ On note $\tau_0$ la transposition $((n+1), \sigma(n+1))$, on a alors :

$$\tau_0 \sigma (n+1) = n+1$$

et on se ramène au cas précédent : $\tau_0\sigma$ est un produit de transpositions $\gamma_1 \dots \gamma_p$, et comme $\tau_0^2 = \mathrm{Id}$, on a $\sigma = \tau_0\gamma_1 \dots \gamma_p$ qui est un produit de transpositions.

□

**Exemple 7.22.**

1. $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix}$ $\gamma = (2,4,6,5)$, *donc* $\gamma = (2,4)(4,6)(6,5)$
2. $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$ $\gamma = (1,5,3)(4,6)$, *donc* $\gamma = (1,5)(5,3)(4,6)$

**Définition 7.23.**

Soit $n \geq 1$, soit $\sigma \in \mathrm{S}_n$ et $t$ le nombre de $\sigma-$orbites distinctes dans $[\![1, n]\!]$
On appelle signature de $\sigma$ l'entier $\varepsilon(\sigma) = (-1)^{n-t}$ En fait on a plus précisément, si on note $\mathcal{P}$ l'ensemble des paires d'éléments distincts de $[\![1, n]\!]$.
On dit que la paire $\{i, j\}$ (avec $i < j$) est en inversion pour $\sigma$ quand $\sigma(i) > \sigma(j)$.
Une permutation est paire si elle possède un nombre pair d'inversions, et impaire sinon.
La signature d'une permutation paire est 1, -1 celle d'une impaire.

$$\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i} = \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma(j) - \sigma(i)}{j - i}$$

**Théorème 7.24.**

Soit $n \geq 2$. L'application $\varepsilon : \begin{array}{ccc} \mathrm{S}_n & \to & \{-1, 1\} \\ \sigma & \mapsto & \varepsilon(\sigma) \end{array}$ est un morphisme surjectif.

*Démonstration.* Remarquons que la signature de (12) est $-1$. (Car elle possède une inversion). Donc $\varepsilon$ est surjective.

Soient $\sigma$ et $\gamma$ deux permutations de $S_n$. Alors :

$$\begin{aligned}
\varepsilon(\sigma \circ \gamma) &= \prod_{\{i,j\}\in\mathcal{P}} \frac{\gamma\circ\sigma(j) - \gamma\circ\sigma(i)}{j - i} \\
&= \prod_{\{i,j\}\in\mathcal{P}} \frac{\gamma\circ\sigma(j) - \gamma\circ\sigma(i)}{\sigma(j) - \sigma(i)} \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma(j) - \sigma(i)}{j - i} \\
&= \prod_{\{i,j\}\in\mathcal{P}} \frac{\gamma(j) - \gamma(i)}{j - i} \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma(j) - \sigma(i)}{j - i} = \varepsilon(\gamma)\varepsilon(\sigma)
\end{aligned}$$

□

**Proposition 7.25** (Conséquences)**.**

Pour une permutation $\sigma$ donnée, toutes ses décompositions en transpositions ont la même parité de nombre de transpositions, qui est aussi la parité de $\sigma$.

# Chapitre 8

# Notion de groupe opérant sur un ensemble

## I Généralités

**Définition 8.1.**

Soit $G$ un groupe, et $E$ un ensemble non vide.
On dit que $G$ opère à gauche sur $E$ s'il existe une application :

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

vérifiant les propriétés suivantes :

- $\forall g_1, g_2 \in G, \forall x \in E,\ (g_1.g_2) * x = g_1.(g_2 * x)$ où $\cdot$ est la loi de composition interne et $*$ la loi de composition externe.
- $\forall x \in E,\ e * x = x$

On appelle cette application loi de composition externe. On définit de manière analogue l'action à droite d'un groupe $G$ sur un ensemble non vide.
On appelle un tel ensemble $E$ un $G$-ensemble.

On ne parlera ici que des actions à gauche quand on dira que $G$ agit sur $E$ et on notera de la même manière $*$ et $\cdot$ par $\cdot$ sans faire de différence (de notation) entre la loi interne et externe.

**Proposition 8.2.**

Soit $G$ un groupe opérant sur un ensemble $E$. On a les propriétés suivantes :

1. $\forall g \in G$, l'application :

$$\gamma_g : \begin{array}{ccc} E & \to & E \\ x & \mapsto & g * x \end{array}$$

est une permutation de $E$.

2. L'application

$$\gamma : \begin{array}{ccc} G & \to & \mathrm{S}_E \\ g & \mapsto & \gamma_g \end{array}$$

est un morphisme de groupes. Son noyau $\ker(\gamma)$ est alors appelé noyau de l'action de $G$ sur $E$.

*Démonstration.*

1. Montrons que c'est une application bijective :
Surjectivité : Soit $y \in E$, posons $x = g^{-1}y$, alors :

$$\begin{aligned} \gamma_g(x) &= g.\left(g^{-1}.y\right) \\ &= \left(gg^{-1}\right).y \\ &= y \end{aligned}$$

Injectivité : Soient $x, y \in E$,

$$\begin{aligned} \text{Si } \gamma_g(x) &= \gamma_g(y) \\ g.y &= g.x \\ \left(g^{-1}g\right).x &= \left(g^{-1}g\right).y \\ x &= y \end{aligned}$$

2. $\forall g_1, g_2 \in G$, alors $\forall x \in E$ :

$$\begin{aligned} \gamma(g_1g_2) &= \gamma(g_1).\gamma(g_2). \text{ En effet,} \\ \gamma(g_1g_2).x &= (g_1g_2).x \\ &= g_1.(g_2.x) \\ &= \gamma(g_1).(g_2).x \end{aligned}$$

D'où le résultat.

□

**Corollaire 8.3.**

On peut donc associer à toute action de groupe $G$ sur $E$ un morphisme $\gamma \in \mathrm{Hom}(G, \mathrm{S}_E)$.

$$\gamma : \begin{array}{ccc} G & \to & \mathrm{S}_E \\ g & \mapsto & \gamma_g \end{array}$$

Le noyau de l'action est le noyau du morphisme de groupe $\gamma$.

On va montrer la réciproque :

**Proposition 8.4.**

Soit $\lambda \in \mathrm{Hom}(G, \mathrm{S}_E)$, on peut lui associer une loi de composition externe sur $E$ :

$$\begin{array}{ccc} G \times E & \to & E \\ (g, x) & \mapsto & \underbrace{\lambda(g)}_{\in \mathrm{S}_E}(x) \end{array}$$

qui vérifie les deux propriétés axiomatiques suivantes :

- $\lambda(e) = \mathrm{Id}_E$ et si $x \in E, e.x = \lambda(e)(x) = x$
- Soient $g_1, g_2 \in G$, alors :

$$\lambda(g_1 g_2) = \lambda(g_1)\lambda(g_2)$$

Soit $x \in E$,

$$\begin{aligned} (g_1 g_2).x &= \lambda(g_1).\lambda(g_2)(x) \\ &= \lambda(g_1).(\lambda(g_2)(x)) \\ &= g_1.(g_2.x) \end{aligned}$$

# II Exemples

On va énoncer ici plusieurs exemples d'actions de groupes.

1. $G$ opère sur $G$ par translation a gauche :

$$\begin{array}{ccc} G \times G & \to & G \\ (g, x) & \mapsto & g.x \overset{\text{def}}{=} gx \end{array}$$

La loi interne ici est la même que la loi externe.
Cette action est en fait celle avec laquelle on a démontré le théorème de Caley (2).
On trouve une illustration aussi en géométrie affine linéaire.

2. $G$ opère sur $\mathcal{P}(G)$ par translation a gauche :

$$\begin{array}{ccc} G \times \mathcal{P}(G) & \to & \mathcal{P}(G) \\ (g, S) & \mapsto & \begin{cases} g.S = \{gx, x \in S\} \text{ si } S \neq \varnothing \\ \varnothing \text{ si } S = \varnothing \end{cases} \end{array}$$

3. Soit $H$ un sous-groupe de $G$, alors $G$ opère par translation à gauche sur l'ensemble $(G/H)_g$ : les classes d'équivalence à gauche modulo $H$.

$$\begin{array}{ccc} G \times (G/H)_g & \to & (G/H)_g \\ (g, xH) & \mapsto & gxH \end{array}$$

Cette définition a un sens car, si on vérifie l'indépendance des choix : soient $x, y \in G$ tels que $xH = yH$ Alors $xH = yH \Rightarrow y^{-1}x \in H$ Montrons que $gxH = gyH$.

$$\begin{aligned} (gy)^{-1} gxH &= y^{-1}g^{-1}yxH \\ &= y^{-1}xH = H \end{aligned}$$

Donc $gxH = gyH$.

4. $G$ opère $G$ par conjugaison :

$$\begin{array}{ccc} G \times G & \to & G \\ (g, x) & \mapsto & gxg^{-1} \end{array}$$

5. $G$ opère également sur $\mathcal{P}(G)$ par conjugaison :

$$\begin{array}{ccc} G \times \mathcal{P}(G) & \to & \mathcal{P}(G) \\ (g, S) & \mapsto & \begin{cases} g.Sg^{-1} = \{gx, x \in S\} \text{ si } S \neq \varnothing \\ \varnothing \text{ si } S = \varnothing \end{cases} \end{array}$$

6. Soit $E$ un ensemble non vide, $\mathrm{S}_E$ opère sur $E$.

$$\begin{array}{ccc} \mathrm{S}_E \times E & \to & E \\ (\sigma, x) & \mapsto & \sigma(x) \end{array}$$

# Chapitre 9

# Stabilisateur et orbite

## I Définitions et exemples

Soit $G$ un groupe opérant sur $E$ un ensemble non vide. On note

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

la loi de composition externe.

**Définition 9.1** (Stabilisateur)**.**

Soit $x \in E$, on définit un stabilisateur de $x$ par l'ensemble des éléments de G laissant $x$ inchangé par l'action considérée (cela peut être toute action de groupe.) :

$$G_x \overset{\text{def}}{=} \{g \in G, g.x = x\}$$

On appellera parfois également cet ensemble sous-groupe d'isotropie.

**Proposition 9.2.**

Soit $x \in E$,$G_x$ est un sous-groupe de $G$.

On pourra donc maintenant définir l'orbite sur $E$ :

**Proposition 9.3.**

Soit $E$ un ensemble non vide, on peut considérer la relation binaire $\mathcal{R}_G$ définie par la formule : $\forall x, y \in E$,

$$x\mathcal{R}_G y \Leftrightarrow \exists g \in G, y = g.x$$

$\mathcal{R}_G$ définit une relation d'équivalence.

**Définition 9.4** (Orbite de $x$ sous l'action de $G$.)**.**

On appelle l'orbite de $x$ sous l'action de $G$ (ou $G-$orbite) la classe d'équivalence de $x$ par $\mathcal{R}_G$, on la note $\Omega_x$.

$$\begin{aligned}\Omega_x &= \{y \in E, \exists g \in G, y = g.x\} \\ &= \{g.x, g \in G\}\end{aligned}$$

1. On peut voir l'orbite de $x$ comme l'image de $G$ par $\begin{array}{ccc} G & \to & E \\ g & \mapsto & g * x \end{array}$.
2. Les $G-$orbites forment une partition de l'ensemble $E$, c'est-à-dire que : $\forall x, y \in E$
$$\Omega_x \cap \Omega_y = \varnothing \text{ ou } \Omega_x = \Omega_y$$
et
$$E = \bigcup_{x \in E} \Omega_x$$
En effet l'orbite de $x$ est la classe d'équivalence de $x$, or les classes d'équivalence forment une partition de $E$.

1. Soit $\sigma \in \mathrm{S}_n$ une permutation de l'ensemble $[\![1, n]\!]$, soit $i \in [\![1, n]\!]$ :
$$\begin{aligned}\Omega_i &= \left\{\sigma^k(i), k \in \mathbb{N}\right\} \\ &= \sigma - \text{orbite de } i\end{aligned}$$

2. $G$ opère sur $G$ pour la translation a gauche : soit $\mathbf{x} \in \mathbf{G}$.
$$\begin{aligned}G_x &= \{g \in G, g.x = gx = x\} = (e) \\ \Omega_x &= \{gx, g \in G\} = G\end{aligned}$$

3. Supposons que $G$ opère par conjugaison sur $G$, soit $x \in G$.

$$\begin{aligned} G_x &= \left\{g \in G, gxg^{-1} = x\right\} \\ &= C_G(x) \\ \Omega_x &= \{g.x, g \in G\} \\ &= \left\{gxg^{-1}, g \in G\right\} \end{aligned}$$

   $\Omega_x$ correspond à la classe de conjugaison de $x$ dans $G$.

4. Supposons que $G$ opère par conjugaison sur $\mathcal{P}(G)$, $S \neq \varnothing$.

$$\begin{aligned} G_S &= \left\{g \in G, gSg^{-1} = S\right\} \\ &= N_G(S) \\ \Omega_S &= \left\{gSg^{-1}, g \in G\right\} \end{aligned}$$

   $\Omega_S$ correspond au classe de conjugaison de $S$, et $G_\varnothing = G$ et $\Omega_\varnothing = \{\varnothing\}$

5. Soit $H$ un sous-groupe de $G$, supposons que $G$ agit par translation à gauche sur $(G/H)_g$, alors :

$$G_x = xHx^{-1}$$

   Soit $g \in G$,

$$\begin{aligned} g \in G_x &\Leftrightarrow gxH = xH \\ &\Leftrightarrow gx \in xH \\ &\Leftrightarrow g \in xHx^{-1} \end{aligned}$$

   En particulier, on a la proposition suivante :

**Proposition 9.5.**

Soit $G$ un groupe et $H$ un sous-groupe de $G$. Le noyau de l'action de $G$ sur $(G/H)_g$ est $\bigcap_{x \in G} xHx^{-1}$.
En outre c'est le plus grand sous-groupe de $G$, normal dans $G$ et contenu dans $H$.

**Remarque 9.6.** *On notera que de plus, si $H \triangleleft G$ alors* $\ker\gamma = H$
*Si $G$ est un sous-groupe simple (voir 4.7), alors pour tout sous-groupe propre $H$ de $G$, $G$ est isomorphe à un sous-groupe de $S_{(G/H)_g}$*
$\ker\gamma \neq G$ *signifie que si $\gamma$ est injectif, alors par le lemme de factorisation : $G \simeq Im\gamma$*

*Démonstration.*
Le noyau de l'action de groupe est le noyau du morphisme de groupe :

$$\begin{array}{rccc} & G & \to & \mathrm{S}_{(G/H)_g} \\ \gamma : & g & \mapsto & \left(\gamma_g : \begin{array}{ccc} (G/H)_g & \to & (G/H)_g \\ xH & \mapsto & gxH \end{array}\right) \end{array}$$

Soit $x \in G$,

$$\begin{aligned} g \in \ker\gamma &\Leftrightarrow \gamma(g) \overset{\text{def}}{=} \gamma_g = \mathrm{Id} \\ &\Leftrightarrow \forall x \in G, gxH = xH \\ &\Leftrightarrow g \in \bigcap_{x\in G} xHx^{-1} \end{aligned}$$

$\ker\gamma$ est normal, contenu dans $H$, normal car c'est un noyau contenu dans $H$ (le noyau d'un morphisme de groupe est normal).
Si $g \in \ker\gamma$ ,alors $g \in H = gH = H$ donc $g \in H$.
C'est le plus grand sous-groupe de $G$, normal dans $G$ et contenu dans $H$ : Soit $N$ un sous-groupe normal de $G$ tel que $N$ est contenu dans $H$. alors $\forall x \in G$, $\underbrace{xNx^{-1}}_{=N} \subset x \subset xHx^{-1}$ donc $N \subseteq \ker(\gamma)$. □

**Corollaire 9.7.**

Soit $G$ un groupe fini d'ordre $n \geq 2$ contenant un sous-groupe propre $H$ tel que $[G : H] = k \geq 1$. Supposons que $n$ ne divise pas $k!$, alors $G$ n'est pas simple.

En effet si $G$ était simple, la remarque et le théorème de Lagrange impliqueraient que $n$ diviserait $k!$

# II Propriétés des stabilisateurs et orbites.

**Théorème 9.8.**

Soit $G$ un groupe et $E$ un $G-$ensemble (ou $G-$ens), alors $\forall x \in E$, $\forall y \in E$,

$$x\mathcal{R}_G y \Rightarrow G_x \text{ et } G_y \text{ sont conjugués dans } \mathcal{P}(G)$$

*Démonstration.*
Soient $x, y \in E$, alors

$$x \mathcal{R}_G y \Rightarrow \exists g \in G, y = g.x$$

On veut montrer que $G_y = gG_xg^{-1}$. Soit $g' \in G_y$ alors $g'.y = y$ donc :

$$\begin{aligned} \left(g'g\right).x &= g'g.x \\ &= g.x \\ \left(g^{-1}g'g\right).x &= x \end{aligned}$$

Donc $g^{-1}g'g \in G_x$, d'où $g' \in gG_xg^{-1}$.

$$G_y \subseteq gG_xg^{-1}$$

Soit $g_1 \in gG_xg^{-1}$, $\exists g' \in G_x$ tel que $g_1 = gg'g^{-1}$ ce qui équivaut à $g^{-1}g_1g \in G_x$. i.e $g^{-1}g_1g.x = x$ d'où :

$$g_1.\left(g_1.x\right) = g.x = y$$

d'où $g_1 \in G_y$. Donc

$$gG_xg^{-1} \subseteq G_y$$

D'où l'égalité par double inclusion. □

**Théorème 9.9** (Formule des classes)**.**

Soit $G$ un groupe et $E$ un $G-$ens.
$\forall x \in E$, on a la propriété suivante : $\Omega_x$ et $\left(G/G_x\right)_g$ sont équipotents.

**Corollaire 9.10.**

Soit $G$ un groupe **fini** et $E$ un $G-$ens.

$$|\Omega_x| = [G : G_x] .$$

*Démonstration.*
On va construire explicitement une bijection entre les deux ensembles :

$$\lambda : \ \Omega_x \ \rightarrow \ \left(G/G_x\right)_g$$

Les éléments de $(G/G_x)_g$ sont les ensembles de la forme $gG_x$ pour $g \in G$. On pose donc la fonction $\lambda$ définie par :

$$\lambda(g.x) = gG_x$$

La définition a un sens si on vérifie l'indépendance des choix : soit $g' \in G$ tel que

$$g.x = g'.x$$

alors $\left(g^{-1}g'\right).x = x$ donc $g^{-1}g' \in G_x$, d'où $gG_x = g'G_x$.
Pour la surjectivité, elle est donnée par construction.
Pour l'injectivité, soient $g_1, g_2 \in G$ tels que

$$g_1G_x = g_2G_x$$

donc :

$$\begin{aligned} \left(g_1^{-1}g_2\right).x &= x \\ \text{i.e } g_1^{-1}g_2 &\in G_1 \\ g_2.x &= g_1.x \end{aligned}$$

□

**Corollaire 9.11.**

Soit $E$ un ensemble fini et $G$ un groupe opérant sur $E$. Soit $(x_i)_{i\in[\![1,q]\!]}$ une famille de représentants des $G-$orbites distinctes, alors :

$$|E| = \sum_{i=1}^{q} |\Omega_{x_i}|$$

$$|E| = \sum_{i=1}^{q} [G : G_{x_i}]$$

**Remarque 9.12.** *Par ailleurs, $\Omega_x$ est fini car $E$ l'est, et ce pour tout $x \in E$, par le théorème $(G/G_x)_g$ est fini donc $G_x$ est d'indice fini dans $G$.*

*Démonstration.*
Les $G-$orbites définissent une partition de l'ensemble $E$, puisque ce sont les classes d'une relation d'équivalence. On a choisit les $x_i$ formant une famille des représentants des $g-$orbites distinctes.)

$$|E| = \sum_{i=1}^{r} |\Omega_{x_i}|$$

$$|\Omega_{x_i}| = [G : G_{x_i}]$$

$$|E| = \sum_{i=1}^{r} [G : G_{x_i}]$$

□

**Dans le cas particulier de l'action par conjugaison :**

**Corollaire 9.13** (Cas de l'action par conjugaison)**.**

Soit $G$ un groupe fini agissant sur lui-même par conjugaison.
Si $(x_i)_{i\in[\![1,r]\!]}$ est une famille de représentants des classes de conjugaisons distinctes dans $G$. alors :

$$\mathrm{o}(G) = \sum_{i=1}^{r} [G : C_G(x_i)]$$

ou $C_G(x_i)$ est le centralisateur de $x_i$ dans $G$.

On a quelques propriétés intéressantes sur cette action particulière :

**Propriétés 9.14.**

Soit $G$ opérant sur lui-même par conjugaison.

1. $x \in \mathcal{Z}(G) \Leftrightarrow C_G(x) = G$
   Le centre de G est $\mathcal{Z}(G) = \{a \in G,\ \forall y \in G ay = ya,\}$
2. $z \in \mathcal{Z}(G) \Leftrightarrow [G : C_G(x)] = 1$
3. $x \in \mathcal{Z}(G) \Leftrightarrow \left\{gxg^{-1}, g \in G\right\} = \Omega_x = \{x\}$

Revenons au cadre plus général :

**Définition 9.15** (Orbite ponctuelle)**.**

Soit $G$ un groupe et $E$ un $G-$ens.
On appelle orbite ponctuelle toute $G-$orbite réduite à un unique élément. On dit aussi que $x$ est point fixe de l'action.

**Théorème 9.16.**

Soit $G$ un groupe fini, agissant sur lui-même par conjugaison, soit $\mathcal{Z}(G)$ le centre de $G$.
Soit $(x_i)_{i\in[\![1,k]\!]}$ une famille des représentants des classes de conjugaisons distinctes et non ponctuelles, alors :

$$\mathrm{o}(G) = \mathrm{o}(\mathcal{Z}(G)) + \sum_{i=1}^{k} [G : C_G(x_i)].$$

*Démonstration.*
Supposons $G$ abélien, alors $G = \mathcal{Z}(G)$, il n'y a donc pas d'orbite non ponctuelle, donc $k = 0$ et $\mathrm{o}(G) = \mathrm{o}(\mathcal{Z}(G))$
Supposons à présent $G$ non abélien, on a nécessairement $k \geq 1$ et quitte à réordonner les $(x_i)$, supposons $\forall i \in [\![1,k]\!]$, les orbites $\Omega_i$ ne sont pas ponctuelles, et $\forall i \in [\![k+1,r]\!]$ elles le sont.
Par la remarque, on sait que $\forall i \in [\![k+1,r]\!], x_i \in \mathcal{Z}(G)$, d'où $\mathcal{Z}(G) = \{x_{k+1},\dots,x_r\}$ On a la formule :

$$\begin{aligned}\mathrm{o}(G) &= \sum_{i=k+1}^{r} |\Omega_{x_i}| + \sum_{i=1}^{k} |\Omega_{x_i}| \\ &= \mathrm{o}(\mathcal{Z}(G)) + \sum_{i=1}^{k} [G : C_G(x_i)]\end{aligned}$$

□

On a une conséquence de ce théorème :

**Corollaire 9.17** (Centre d'un $p$-groupe)**.**

Si $G$ est un groupe fini, d'ordre $p^k$, où $p$ est premier, alors le centre de $G$ n'est pas réduit à un élément.
En d'autres termes, le centre des groupes finis dont l'ordre est une puissance de nombre premier n'est pas un singleton.

*Démonstration.* Soit $(x_i)_{[\![1,k]\!]}$ une famille de représentants des orbites non-ponctuelles.
$\mathrm{o}(\mathcal{Z}(G)) = \mathrm{o}(G) - \sum_{i=1}^{k} [G : C_G(x_i)]$

$\forall i \in [\![1,k]\!], [G, C_G(x_i)] \,|p^k$, on sait que $[G, C_G(x_i)] > 1$, donc

$$p|\,[G, C_G(x_i)]\,, \forall i \in [\![1,k]\!]$$

Comme $p|o(G)$, on en déduit que $p|o(\mathcal{Z}(G))$. □

**Corollaire 9.18.**

Soit $p$ un nombre premier, et $G$ un groupe.
Alors tout sous-groupe fini de $G$, d'ordre $p^2$ est abélien.

*Démonstration.*
Soit $H$ un sous-groupe de $G$ d'ordre $p^2$. On veut montrer que $\mathcal{Z}(H) = H$.
Par le corollaire précédent, $p|o(\mathcal{Z}(H))$, donc $H/\mathcal{Z}(H)$ est un groupe d'ordre 1 ou $p$, donc est cyclique, donc $H$ est abélien. □

**Définition 9.19** (Opérer transitivement)**.**

1. On dit qu'un groupe $G$ opère transitivement sur un ensemble $E$ si $E$ n'a qu'une seule orbite sous l'action de $G$. i.e que $\forall x, y \in G, \exists g \in G, y = g.x$
2. On dit que $G$ opère simplement transitivement si $\forall x, y \in E, \exists! g \in G, y = g.x$

On remarque que $G$ opère transitivement sur $E \Leftrightarrow \exists x \in E, \Omega_x = E$

# III Illustration : Structure affine linéaire sur un ensemble $E$

On va illustrer cette définition : on va comparer cette structure a l'action de groupe additif sous-jacent a un espace vectoriel sur un ensemble (par translation).

**Exemple 9.20** (Groupes opérant transitivement)**.**

1. *$G$ opère transitivement sur $G$ par translation a gauche :*
   *Soient $x, y \in G$,*
   $$y = \left(yx^{-1}\right) x$$
2. *Si $E$ est un $G-$ens, $\forall x \in E$, $G$ opère transitivement sur la $G-$orbite $\Omega_x$.*

3. *Si $G = (e)$, $G$ opère transitivement sur $G$ par conjugaison.*

**Définition 9.21** (Opérer fidèlement)**.**

Soit $G$ un groupe operant sur un ensemble $E$, on dit que $G$ opère fidèlement sur $E$ si :

$$\gamma : \begin{array}{ccc} G & \to & \mathrm{S}_E \\ g & \mapsto & \left(\gamma_g : \begin{array}{ccc} E & \to & E \\ x & \mapsto & g.x \end{array}\right) \end{array}$$

est injectif.
En d'autres termes : $G$ opère fidèlement sur $E$ si et seulement si $\forall g \in G, \gamma_g = \mathrm{Id} \Rightarrow g = e$.
Par ailleurs : $\gamma_g = \mathrm{Id} \Leftrightarrow \forall x \in E, g.x = x$.

# IV Sous-ensemble des points fixes des $G-$ensembles

**Définition 9.22.**

Soit $G$ un groupe opérant sur un ensemble $E$, on définit :

$$E_G = \mathrm{Fix}_E(G) \overset{\text{def}}{=} \{x \in E, \forall g \in G, g.x = x\}$$

Cet ensemble est appelé sous-ensemble des points fixes de $E$ sous l'action de $G$.
On a aussi que $E_G = \{x \in E, G_x = G\} = \{x \in E, \Omega_x = \{x\}\}$.

**Exemple 9.23.**

1. *Supposons que $G$ opère sur $G$ par conjugaison, alors :*

$$\Omega_x = \{x\} \Leftrightarrow x \in \mathcal{Z}(G)$$

2. *Soit $G$ un sous-groupe de $S_4$, opérant sur $E = \{1,2,3,4\}$ de manière canonique. Alors :*
*Si $G = \langle (1,2,3) \rangle$, $E_G = \{4\}$*
*Si $G = \langle (1,2)(3,4) \rangle$, alors $E_G = \varnothing$.*

**Proposition 9.24** (Sous-groupe et action de groupe)**.**

Soit $G$ un groupe opérant sur un ensemble, et $K$ un sous-groupe de $G$. Alors $K$ opère sur l'ensemble $E$ et

$$\cdot : \begin{array}{ccc} K \times E & \to & E \\ (k, x) & \mapsto & k.x \end{array}$$

est encore une loi de composition externe.

Par conséquent :

1. Si $K_x$ est le stabilisateur de l'élément $x \in E$ pour cette action, on peut montrer que $K_x = K \cap G_x$
2. Si $E_K = \{x \in E, \forall k \in K, k.x = x\}$ (c'est l'ensemble des points fixes du $K-$ens $E$).
   On peut montrer que $E_K = \{x \in E, K_x = K\}$ donc $x \in E_K \Rightarrow K \leq G_x$.
3. Si $G$ opère fidèlement sur $E$, $K$ opère fidèlement sur $E$.
4. Mais si $G$ opère transitivement sur $E$ alors un sous-groupe de $G$ peut ne pas opérer transitivement sur $E$ par restriction.
   On prend comme exemple $H \leq G$, et l'action de groupe de $G$ par translation sur $(G/H)_g$, on peut chercher une CNS pour qu'un sous-groupe $K$ de $G$ opère transitivement sur $(G/H)_g$ par restriction.

**Lemme 9.25** (Action d'un $p$-groupe)**.**

Soit $p$ un nombre premier, soit $n \in \mathbb{N}^*$, soit $G$ un groupe fini d'ordre $p^k$, alors :

$$(G \text{ opère sur un ensemble fini } E) \Rightarrow |E_G| \equiv |E| \mod p$$

*Démonstration.*
On veut montrer que $p$ divise $|E_G| - |E|$
Par ce qui précède, on a $x \in E_G \Leftrightarrow \Omega_x = \{x\}$. $|E_G|$ correspond au nombre d'orbites ponctuelles.

$$|E| = |E_G| + \sum_{i=1}^{k} |\Omega_{x_i}|$$

où la famille $(x_i)_{i \in [\![1,k]\!]}$ est un système de représentants des orbites non ponctuelles distinctes. On a :

— $|\Omega_{x_i}| > 1, \forall i \in [\![1, k]\!]$.

— $|\Omega_{x_i}| = [G : G_{x_i}]$ or $\forall i \in [\![1, k]\!]$, $[G : G_{x_i}] \,|\mathrm{o}\,(G)$.

$$\forall i \in [\![1, k]\!], \exists m_i \in \mathbb{N}, 1 \leq m_i \leq m, p^{m_i} |\, [G : G_{x_i}]$$

En particulier, $\forall i \in [\![1, k]\!], p |\, [G : G_{x_i}]$, d'où $p |\, |E| - |E_G|$.

□

**Lemme 9.26.**

Soit $p$ un nombre premier, soit $n \in \mathbb{N}^*$, soit $G$ un groupe et $H$ et $K$ deux sous-groupes de $G$.
Supposons que $[G : H] = r \geq 1$, $p$ ne divise pas $r$ et $\mathrm{o}\,(K) = p^n$.
En d'autres termes supposons que $p$ ne divise pas l'indice de $G/H$ et que $K$ soit d'ordre d'une puissance non nulle de $p$.
Alors le sous-groupe $K$ est contenu dans un conjugué de $H$.

*Démonstration.*
Soit $E \overset{\text{def}}{=} (G/H)_q$, $E$ est un ensemble fini de cardinal $r$. $K$ étant un sous-groupe de $G$, $K$ opère par translation a gauche sur $E$.
Par le lemme précédent on sait que :

$$|E_K| \equiv r\,[p]$$

Si $r \geq 1$, alors $E_K \neq \varnothing$, $\exists x \in G, xH \in E_k \Leftrightarrow K \leq E_K$.
Par ailleurs on sait que $G_{xH} = xHx^{-1}$, donc $K \leq xHx^{-1}$, et est donc dans un conjugué de $H$. □

# Chapitre 10

# Formule de Burnside

## I Théorème et démonstration.

Soit $G$ un groupe opérant sur un ensemble $E$, soit $X \neq \varnothing$, $X \subseteq E$. $\forall g \in G$, on pose : $\mathrm{Fix}_X(g) \overset{\text{def}}{=} \{x \in X, g.x = x\}$

**Théorème 10.1** (Formule de Burnside)**.**

Soit $E$ un ensemble fini, et $G$ un groupe fini agissant sur $E$. Soit $t$ le nombre des $G-$orbites, alors on a la formule suivante :

$$t.|G| = \sum_{g \in G} |\mathrm{Fix}_E(g)|$$

*Démonstration.*
Posons $S \overset{\text{def}}{=} \{(x, g) \in E \times G, g.x = x\}$. On rappelle que :

$$\mathrm{Fix}_X(g) \overset{\text{def}}{=} \{x \in X, g.x = x\}$$

$$G_x \overset{\text{def}}{=} \{g \in G, g.x = x\}$$

donc

$$S = \bigsqcup_{x \in E} \{x\} \times G_x$$

$$|S| = \sum_{x \in E} |G_x|$$

$$S = \bigsqcup_{g \in G} \mathrm{Fix}_E(g) \times \{g\}$$

$$|S| = \sum_{g \in G} |\mathrm{Fix}_E(g)|$$

Pour tout $x \in E$,

$$|E| = |\Omega_x| = [G : G_x] = \frac{|G|}{|G_x|}$$

On prend $(x_i)_{i\in[\![1,t]\!]}$ une famille de représentants des $g-$orbites distinctes, alors :

$$\begin{aligned}
\sum_{g\in G} |\mathrm{Fix}_E(g)| &= \sum_{x\in E} |G_x| \\
&= \sum_{i\in[\![1,t]\!]} \sum_{x\in\Omega_{x_i}} \frac{|G|}{|\Omega_x|} \\
&= |G| \sum_{i\in[\![1,t]\!]} \sum_{x\in\Omega_{x_i}} \frac{1}{|\Omega_{x_i}|} \\
&= |G| \sum_{i\in[\![1,t]\!]} 1 \\
\sum_{g\in G} |\mathrm{Fix}_E(g)| &= |G|\,.t
\end{aligned}$$

□

# II Applications

## 1 Développement classique : Une application en combinatoire - Coloriage de cube.

De combien de manières différentes peut-on colorier un cube avec les couleurs rouge, blanc ou bleu ?
Un cube contient 6 faces et on a 3 couleurs : $3^6$ manières de colorier un cube, mais certains coloriages sont les mêmes : par rotations. Les coloriages sont les mêmes s'ils sont dans la même orbite du groupe de rotation de $G$ du cube, agissant sur $X$ l'ensemble des $3^6$ coloriages possibles. On doit donc compter le nombre d'orbites de $G$ sur $X$.

On peut montrer que $G \cong S_4$ et que les 24 rotations du cube sont exactement celles détaillées dans le tableau ci-dessous.
Première interrogation : Pour chaque rotation $g$ du cube, combien de coloriages laisse-t-elle fixe ? On va détailler chaque rotation :

| Rotation | Nombre de rotations | Nombre de coloriages fixés par une rotations | Contribution à $\sum \lvert\mathrm{Fix}\,(g)\rvert$ |
|---|---|---|---|
| Id | 1 | $3^6$ | 729 |
| Axes par sommets diagonalement opposés, d'angle $\pm\frac{2\pi}{3}$ | 8 | $3^2$ | 72 |
| Axes par milieux des cotes opposés, d'angle $\pi$ | 6 | $3^3$ | 162 |
| Axes par centres des faces opposés, d'angle $\pi$ | 3 | $3^4$ | 243 |
| Axes par centres des faces opposés, d'angle $\frac{\pm\pi}{2}$ | 6 | $3^3$ | 162 |
| Total : | 24 | | 1368 |

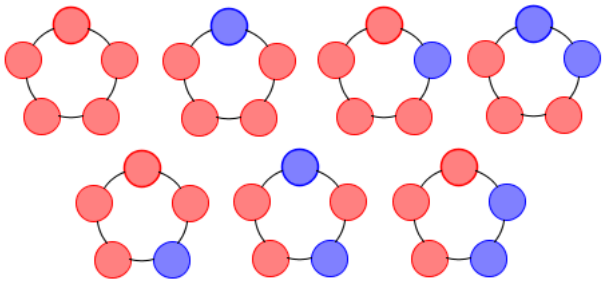
D'où

$$\lvert\mathrm{Orb}_X\,(G)\rvert = \frac{1}{\lvert G\rvert}\sum_{g\in G}\lvert\mathrm{Fix}_X\,(g)\rvert = \frac{1368}{24} = 57$$

On a donc 57 manières différentes de colorier un cube en rouge, blanc et/ou bleu, par Burnside ! (L'exemple se trouve dans Groups and Geometry, de Neumann-Stay-Thompson)

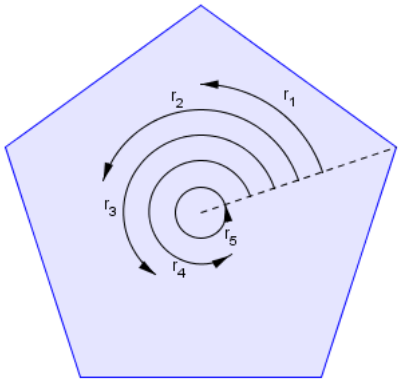
## 2 Développement classique à nouveau : Encore une application en combinatoire - Colliers de perles.

On trouve les mêmes raisonnements pour fabriquer des colliers bicolores :



En effet quand on fabrique un colleir avec des perles rouges et bleues, certains sont les mêmes à une rotations près :




(Développer si le temps)

# Chapitre 11

# Groupes finis et théorèmes de Sylow

## I Groupes finis

Soit $G$ un groupe fini d'ordre $m$, on a vu que le théorème de Lagrange assurait que tout sous-groupe de $G$ était d'ordre divisant $m$.
On va étudier ici si une réciproque est possible, c'est-a-dire si tout diviseur de $m$ est associé à un sous-groupe de $G$ : Est-ce vrai dans le cas des groupes cyclique ou en général ?

**Définition 11.1** (Groupe alterné)**.**

Le groupe alterné de degré $n$, noté $\mathrm{A}_n$ est un sous-groupe de permutations paires de degré $n$. C'est un sous groupe distingué de $\mathrm{S}_n$. On peut voir $\mathrm{A}_n$ comme le noyau du morphisme signature : $\mathrm{A}_n = \ker \varepsilon = \varepsilon^{-1}(1)$

**Propriétés 11.2.**

Soit $n \in \mathbb{N}^*$

$$\text{Card } \mathrm{A}_n = \frac{\text{Card } \mathrm{S}_n}{2}$$

*Démonstration.* Considérer $\varepsilon_{|G}$, le morphisme est surjectif et son noyau est $\mathrm{A}_n$, donc

$$G/\ker \varepsilon \simeq \{\pm 1\}$$

□

$\mathrm{A}_n \triangleleft \mathrm{S}_n$ :
$\mathrm{A}_n \neq \varnothing$ car il contient l'élément neutre, qui se décompose en 0 transpositions.
Si $\phi$ est un éléments de $\mathrm{A}_n$, si $\sigma \in \mathrm{S}_n$, alors $\sigma\phi\sigma^{-1} \in \mathrm{A}_n$.
Or $\sigma$ se décompose en autant de transpositions que $\sigma$ (cela se montre) et $\phi$ est le produit d'un nombre pair de transpositions. La somme du nombre de toutes ces transpositions est donc paire.

On peut aussi voir que $A_n$ est d'indice 2 dans $S_n$ donc distingué.

**Définition 11.3** ($p-$groupes)**.**

Pour $p$ un entier premier, on appelle $p-$groupes finis les groupes finis dont le cardinal est une puissance non nulle de $p$.

## II Premier théorème de Sylow

Soit $p$ un nombre premier et $n \in \mathbb{N}^*$.

**Théorème 11.4** (Théorème de Sylow)**.**

Soit $G$ un groupe fini, si on suppose que $\mathrm{o}(G) = sp^n$ avec $p$ ne divisant **pas** $s$, alors $\forall r \in [\![1, n]\!]$ il existe un sous-groupe $H$ de $G$ d'ordre $\mathrm{o}(H) = p^r$.
Les sous-groupes d'ordre $p^n$ sont appelés $p$-sous-groupes de Sylow.

Pour démontrer ce théorème, on montrera le lemme suivant :

**Lemme 11.5.**

Soit $G$ un groupe fini, si on suppose que $\mathrm{o}(G) = sp^n$ avec $p$ ne divisant **pas** $s$, alors $\exists \lambda \in \mathbb{N}^*$ non divisible par $p$ tel que :

$$\binom{sp^n}{p^r} = \lambda p^{n-r}$$

*Démonstration.*

$$\begin{aligned}\binom{sp^n}{p^r} &= \frac{sp^n}{p^r}\frac{sp^n-1}{1}\cdots\frac{sp^n-(p^r-1)}{p^r-1} \\ &= sp^{n-r}\frac{sp^n-1}{1}\frac{sp^n-2}{2}\cdots\frac{sp^n-(p^r-1)}{p^r-1}\end{aligned}$$

On peut écrire un entier de 1 à $p^r - 1$ sous la forme $qp^a$ où $0 \geq a < r$ et $q$ non divisible par $p$. d'où :

$$\frac{sp^n - k}{k} = \frac{sp^{n-a} - q}{q}$$

$p$ ne divise pas $q$, donc $p$ ne divise pas $sp^{n-a} - q$, comme $p$ est premier, $p$ ne divise pas $\lambda = \frac{sp^n-1}{1} \dots \frac{sp^n-(p^r-1)}{p^r-1}$
D'où le résultat. □

*Démonstration du théorème.*
Soit $r \in [\![1, n]\!]$, on pose $\mathcal{F}$ l'ensemble des parties de $G$ de cardinal $p^r$. On veut extraire de cet ensemble un sous-groupe de $G$.
Par le lemme précédent, $\exists \lambda \in \mathbb{N}$ tel que $p$ ne divise pas $\lambda$, et que $\binom{sp^n}{p^r} = \text{Card } \mathcal{F} = \lambda p^{n-r}$
On va construire une action de $G$ sur cet ensemble $\mathcal{F}$ (la translation par $G$ est une permutation) : $\forall A \in \mathcal{F}$, $\forall g \in G$, $|gA| = |A|$

$$\begin{array}{ccc} G \times \mathcal{F} & \to & \mathcal{F} \\ (g, A) & \mapsto & gA \end{array}$$

Soit $\{A_i\}_{i \in [\![1,k]\!]}$ une famille de représentants des $G$-orbites disjointes de $\mathcal{F}$, on a alors, par la formule des classes (voir 9.9 ) :

$$|\mathcal{F}| = \sum_{i=1}^{k} [G : G_{A_i}]$$

$$\lambda p^{n-r} = \sum_{i=1}^{k} [G : G_{A_i}]$$

Si $p^{n-r+1}$ divise $\frac{|G|}{|G_{A_i}|}$ pour tout $i \in [\![1, n]\!]$ alors $p^{n-r+1}$ divise $\sum_{i=1}^{k} [G : G_{A_i}]$, c'est-à-dire $\lambda p^{n-r}$, et donc on aura $p$ divisant $\lambda$, ce qui est exclu.
Donc il existe au moins un entier $i \in [\![1, k]\!]$ tel que $p^{n-r+1}$ ne divise pas $[G : G_{A_i}]$. Posons $H = G_{A_i}$, montrons que $H$ est d'ordre $p^r$. On a :

$$\begin{aligned} sp^n &= |G| \\ &= |H| \frac{|G|}{|G_{A_i}|} \end{aligned}$$

$p^{n-r+1}$ ne divise pas $\frac{|G|}{|G_{A_i}|}$, donc $\frac{|G|}{|G_{A_i}|} = s'p^\alpha$ où $\alpha \in [\![0, n-r]\!]$ et $s'$ premier avec $p$, donc comme $s'$ divise $sp^n$ et en premier avec $p$, $s'$ divise $s$ (Gauss). En posant $s'' = \frac{s}{s'}$, on a $|H| = s''p^{n-\alpha}$. Or $0 \leq \alpha \leq n - r \Leftrightarrow n \geq n - \alpha \geq r$, d'où

$$\text{o}(H) = s''p^{n-\alpha} \geq p^r$$

Montrons à présent que $\mathrm{o}(H) \leq p^r$. Soit $a \in A_i$, $g \mapsto g.a$ est une application injective : $|H| \leq \mathrm{Card}\ A_i = p^r$. Comme $H$ est un sous-groupe de $G$, $H$ est le sous-groupe d'ordre $p^r$ de $G$ que l'on cherchait. □

Si on applique ce théorème à $n = 1$ et $r = 1$ on obtient le théorème suivant :

**Corollaire 11.6** (Théorème de Cauchy)**.**

Soit $G$ un groupe fini, et $p$ un nombre premier, divisant $\mathrm{o}(G)$. Alors $G$ possède au moins un élément d'ordre $p$.

**Corollaire 11.7.**

Soit $p$ un nombre premier, $n \in \mathbb{N}^*$, $s \in \mathbb{N}$ tel que $p$ ne divise pas $s$. Soit un groupe $G$ fini, d'ordre $sp^h$. $G$ contient alors au moins un sous-groupe d'ordre $p^h$.

**Définition 11.8** ($p-$groupe, $p-$sous-groupe et $p-$sous-groupe de Sylow.)**.**

1. Si $G$ un groupe fini, alors $G$ est un $p-$groupe si $\mathrm{o}(G) = p^r$ avec $p$ premier $r \in \mathbb{N}$.
2. Si $G$ est un groupe d'ordre fini, avec $p$ un nombre premier tel que $p|\mathrm{o}(G)$, alors tout sous-groupe de $G$ d'ordre une puissance non nulle de $p$ est appelé $p-$sous-groupe de $G$.
3. Si $G$ est un groupe fini d'ordre $\mathbf{sp^r}$, $p$ premier tel que $p$ ne divise pas $s$ alors un sous-groupe $H$ de $G$ est appelé $p-$sous groupe de Sylow de $G$ (ou $p-$Sylow) si $\mathrm{o}(H) = p^r$, $r \in \mathbb{N}$.
   On remarquera qu'un $p-$Sylow est un $p-$groupe.
   On notera $\mathbf{Syl}_p(G)$ l'ensemble des $p-$Sylow de $G$.

La définition de $p-$Sylow a un sens et ils existent par le corollaire précédent.

## III Second théorème de Sylow

**Théorème 11.9** (Second théorème de Sylow)**.**

Soit $G$ un groupe fini, $p$ un nombre premier divisant $\mathrm{o}(G)$. Alors :

1. Tout sous-groupe de $G$ est contenu dans un $p-$Sylow de $G$. Autrement dit, les $p$-Sylow sont les éléments maximaux pour l'inclusion de l'ensemble des $p$-sous-groupes de $G$.
2. Les $p-$Sylow de $G$ sont tous conjugués 2 à 2.
3. Le nombre $t$ des $p-$Sylow de $G$ vérifie :

$$t \equiv 1\,[p]$$

$$t | \mathrm{o}(G)$$

**Lemme 11.10.**

Soit $G$ un groupe fini. Si $S$ est un $p-$Sylow de $G$, alors $S$ est l'unique $p-$Sylow de $N_G(S) = \left\{g \in G | gSg^{-1} = S\right\}$

*Démonstration du lemme.*
$N_G(S)$ est un sous-groupe de $G$, donc son ordre est de la forme $s'p^a$, où $0 \leq a \leq n$ et $p$ ne divise pas $s'$
$S$ est un sous-groupe de $N_G(S)$ donc $|S| = p^n$ divise $|N_G(S)| = s'p^a$, comme $p$ ne divise pas $s'$, $p^n$ divise $p^a$, comme $a \leq n$, on a nécessairement $a = n$.
$|N_G(S)| = s'p^n$ Comme $|S| = p^n$, $S$ est un $p-$sous-groupe de Sylow de $N_G(S)$.
Soit $K$ un $p-$sous-groupe de Sylow de $N_G(S)$, on applique le premier théorème de Sylow au cas $H = S$. $[N_G(S) : S] = s'$ est premier avec $p$. Donc par le lemme 9.26, $K$ est contenu dans un conjugué de $H$, donc $\exists x \in N_G(S)$ tel que $K$ est un sous-groupe de $xSx^{-1} = S$, car $x \in N_G(S)$. donc $K$ est un sous-groupe de $S$, or $|K| = |S| = p^n$ donc $K = S$. □

*Démonstration du théorème.*

1. Soit $H$ un $p-$groupe de $G$. Si $S$ est un $p-$Sylow de $G$, on a : $[G : S] = s$ et le lemme 9.26 assure que :

$$\exists x \in G, H \subseteq xSx^{-1}$$

en particulier, $xSx^{-1}$ est un sous-groupe de $G$, et $\left|xSx^{-1}\right| = |S|$ donc $xSx^{-1}$ est un $p-$Sylow de $G$ contenant $H$.

2. Soient $S, S'$ deux $p-$Sylow, d'après le premier point, $\exists x \in G$, tel que$S'$ est un sous-groupe de $xSx^{-1}$.

$$\left|S'\right| = p^n = \left|xSx^{-1}\right|$$

donc $S' = xSx^{-1}$.

3. Soit $\mathcal{S}$ l'ensemble des $p-$Sylow de $G$, par le deuxième point, on sait que $G$ opère par conjugaison transitivement sur $\mathcal{S}$, donc si $S$ est un $p-$Sylow, par le corollaire 9.10 :

$$|\mathcal{S}| = [G : N_G(S)]$$

$S \subset N_G(S)$ donc $[G : N_G(S)]$ divise $[G : S] = s$. En particulier $|\mathcal{S}|$ divise l'ordre de $G$.
$S$ est un sous-groupe de $G$ donc agit sur $\mathcal{S}$ par conjugaison.
Soit $\mathcal{S}_S$ l'ensemble des points fixes du $S-$ens $\mathcal{S}$, on a prouvé la formule (9.25) :

$$|\mathcal{S}| \equiv |\mathcal{S}_S| \ [p]$$

Il s'agit de déduire le résultat de cette formule : Soit $S' \in \mathcal{S}_S$, $\forall g \in S, gS'g^{-1} = S'$, ce qui équivaut à dire que $S$ est un sous-groupe de $N_G(S')$, par le lemme précédent, le sous-groupe $N_G(S')$ ne contient qu'un seul $p-$Sylow, i.e $S'$. Par conséquent $|\mathcal{S}_S| = 1$. D'où le résultat.

□

Pour l'usage pratique de ce théorème, il faut retenir que :

**Corollaire 11.11** ("Troisième" théorème de Sylow)**.**

Soit $G$ un groupe d'ordre $sp^n$ avec $p$ ne divisant pas $s$. Si $n_p$ est le nombre de $p-$Sylow de $G$ alors :

1. $n_p | s$
2. $n_p \equiv 1 \ [p]$

**Corollaire 11.12.**

1. Un groupe $G$ a un unique $p-$Sylow si et seulement si $S$ est normal dans $G$.
2. Dans un groupe abélien fini $G$, pour tout $p$ premier divisant $o(G)$, il existe un unique $p-$Sylow, qui est donc distingué.

# IV Application des théorèmes de Sylow

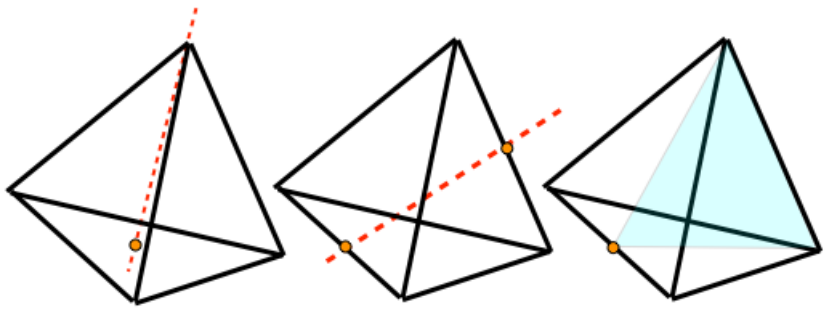
Les résultats seront tirés ici du cours de Monsieur Sebag et de développement d'agrégation.

## 1 Dans $A_4$, il n'existe pas de sous-groupe d'ordre 6

On peut tout d'abord remarquer que $S_4$ est le groupe de symétrie du tétraèdre, qui présente 24 cas de symétrie :

1. l'identité
2. 8 rotations selon les 4 axes passant par chacun des sommets et le centre de la face opposée. Ce sont des rotations de 1/3 ou 2/3 tours.
3. 3 rotations d'un demi-tour autour de la droite passant par les milieux des côtés opposés
4. 12 réflexions (par rapport à un plan passant par une arête et coupant le tétraèdre en deux.) et compositions avec les 12 précédentes.

Ce groupe est isomorphe à $S_4$, et d'ordre 24, non commutatif. $A_4$ est constitué des 12 premiers éléments de cette liste, et est le groupe de rotation du tétraèdre.



Si $A_4$ avait un sous-groupe $H$ de cardinal 6, $H$ serait distingué. Si ce groupe contenait un 3−cycle, il contiendrait un 3−sous-groupe de Sylow de $A_4$ donc, par hypothèse, il contiendrait tous les 3−sous-groupes de Sylow de $A_4$ et a fortiori tous les 3−cycles. Comme il y a 8 3−cycles dans $A_4$ cela n'est pas possible. $H$ ne contient donc aucun 3−cycle et il ne peut être alors de cardinal 6.

## 2 Générateurs et sous-groupes de Sylow

**Proposition 11.13.**

Soit $G$ un groupe fini. Soient $p_1, \dots, p_r$ les diviseurs premiers de son ordre. (i.e la décomposition en facteur premiers de $n \overset{\text{def}}{=} \mathrm{o}(G) = \prod_{i=0}^{r} p_i^{\alpha_i}$).
$\forall i \in [\![1, r]\!]$, notion $H$ un $p_i-$Sylow de $G$. Les sous-groupes $H_1, \dots, H_r$ engendrent alors le groupe $G$.

*Démonstration.*
$n \overset{\text{def}}{=} \mathrm{o}(G) = \prod_{i=0}^{r} p_i^{\alpha_i}$. On pose :

$$K = \langle H_1, \dots, H_r \rangle$$

on a $\forall i \in [\![1, r]\!], H_i < K$ et par le théorème de Lagrange, $p_i^{e_i} \overset{\text{def}}{=} |H_i|$ divise $\mathrm{o}(K)$, par le lemme de Gauss, $n$ divise $|K|$. Comme $K$ est un sous-groupe de $G$, par égalité de leur ordre

$$K = G$$

□

**Corollaire 11.14.**

Tout groupe abélien fini $G$ est isomorphe au produit **direct** de ses sous-groupes de Sylow.

*Démonstration.*
On conservera les mêmes notations que celle de la proposition précédente. Comme les sous-groupes $H_i$ sont distingués ($G$ groupe abélien), et que l'application :

$$\begin{array}{ccc} \prod_{i=1}^{r} H_i & \to & G \\ (h_1, \dots, h_r) & \mapsto & h_1 \dots h_r \end{array}$$

est un homomorphisme surjectif, il est injectif car $G$ et $\prod_{i=1}^{r} H_i$ ont même cardinal (même ordre). D'où l'isomorphisme entre les deux groupes. □

## 3 L'argument de Frattini

**Théorème 11.15** (Argument de Frattini)**.**

Soit $G$ un groupe, soit $H$ un sous-groupe normal et fini de $G$. Soit $S$ un $p-$Sylow de $H$ alors :

$$G = HN_G(S).$$

*Démonstration.*
Pour tout $g \in G$, le sous groupe $gSg^{-1}$ est contenu dans $H$ ($H$ est distingué), et c'est même un sous-groupe de Sylow de $H$. Par le théorème de Sylow, $\exists h \in H$ tel que $gSg^{-1} = hSh^{-1}$, ce qui équivaut à $h^{-1}g \in N_G(S)$, $g \in hN_G(S)$. □

**Corollaire 11.16** (Premier Corollaire)**.**

Soit $G$ un groupe fini, et $S$ un $p-$Sylow de $G$. Soit $H$ un sous-groupe de $G$ alors on a la propriété suivante :

$$N_G(S) \text{ est un sous-groupe de } H \Rightarrow N_G(H) = H$$

*Démonstration.*
Comme $S \subset N_G(S)$ et $S \leq G$,et que $N_G(S) \leq H$, alors $S$ est un sous-groupe de $H$, qui est un sous-groupe de $G$. Comme $S$ est un $p-$Sylow de $G$, c'est un $p-$Sylow de $H$. On applique l'argument de Frattini a $(H, N_G(S))$ dans $N_G(H)$, car $H \triangleleft N_G(H)$, on obtient que $H \subseteq N_G(H) = HN_{N_G(S)}(S) \subseteq HN_G(S) \subseteq H$ D'où :

$$H \subseteq N_G(H) \subseteq H$$

□

**Corollaire 11.17** (Deuxième corollaire)**.**

Pour tout sous-groupe de Sylow $S$ d'un groupe fini $G$, on a la relation suivante :

$$N_G(N_G(S)) = N_G(S)$$

*Démonstration.*
Ceci est une conséquence directe du premier corolaire, en posant $H = N_G(S)$
□

## 4 Unicité des $p-$Sylow

**Théorème 11.18.**

Soit $p, q$ deux nombres premiers distincts et $G$ un groupe fini tel que $\mathrm{o}(G) = pq$. Si $q \not\equiv 1\,[p]$, alors $G$ a un unique $p-$Sylow.

*Démonstration.*
Soit $n_p$ le nombre de $p-$Sylow de $G$. Montrons que $n_p = 1$. Par le second théorème de Sylow, on a que $n_p$ divise $q$ et $n_p \equiv 1\,[p]$, alors $n_p = 1$ ou $q$. Comme $q \not\equiv 1\,[p]$,

$$n_p = 1.$$

□

## 5 Quelques critères de simplicité et de non-simplicité.

Pour la définition de groupe simple, voir 4.7.

**Lemme 11.19.**

Soit $p$ un nombre premier, $G$ un groupe fini, d'ordre $p^n$, où $n \geq 1$. Si $G$ est non abélien, alors $G$ n'est pas simple.

*Démonstration.*
$G$ est non abélien, on a directement que $\mathcal{Z}(G) \neq G$, donc $\mathcal{Z}(G) \triangleleft G$ et $\mathcal{Z}(G) \neq (e)$. C'est donc un sous-groupe normal et non trivial de $G$. Donc $G$ n'est pas simple. □

**Proposition 11.20.**

Soit $p$ un nombre premier, et $G$ un groupe fini non abélien, simple tel que $p$ divise $\mathrm{o}(G)$, alors $G$ a au moins plus d'un $p-$Sylow. (i.e $n_p > 1$)

*Démonstration.*
Si $S$ est un $p-$Sylow de $G$, par hypothèse $S \neq (e)$ et $S < G$. En effet si $S = G$, en particulier $\mathrm{o}(G) = p^n$.
Le lemme précédent contredit alors la simplicité de $G$.
Supposons que $S$ soit l'unique $p-$Sylow de $G$, il est alors nécessairement normal dans $G$. Donc $S$ est un sous-groupe normal propre et non trivial de $G$. Ce qui est absurde donc $n_p > 1$ □

**Proposition 11.21.**

Soit $p, q$ deux nombres premiers, soit $G$ un groupe fini d'ordre $pq$. Alors $G$ n'est pas simple.

*Démonstration.*
Par hypothèse $p > q$ et $p$ ne divise pas $q - 1$.
Par le théorème 11.18, $G$ a un unique $p-$Sylow $S$, donc par la proposition précédente $G$ n'est pas simple.

$$S \triangleleft G, (e) < S < G$$

□

**Proposition 11.22** (Critère de cyclicité)**.**

Soient $p, q$ deux nombres premiers, on suppose que $p \not\equiv 1\,[q]$ et $q \not\equiv 1\,[p]$.
Alors tout groupe d'ordre $pq$ est cyclique.

*Démonstration.*
Soit $G$ un groupe d'ordre $pq$. Par le théorème précédent, on sait que $G$ possède un unique $p-$Sylow, $S$ et un unique $q-$Sylow $T$. Comme $S$ et $T$ sont d'ordres premiers, ils sont cycliques, et il existe $x, y \in G$, tels que $S = \langle x \rangle, T = \langle y \rangle$. Montrons alors que $x$ et $y$ commutent. Soit $z \overset{\text{def}}{=} x^{-1}y^{-1}xy \in G$. Montrons que $z = e$. L'unicité de $S$ et $T$ implique que $S \triangleleft G$ et $T \triangleleft G$.

$$z = \left(x^{-1}y^{-1}xy\right) = x^{-1}\left(y^{-1}xy\right) = x^{-1}x = e.$$

Le chapitre sur le produit permet alors de conclure que $G = \langle x \rangle \langle y \rangle$ est cyclique, d'ordre $pq$. □

**Proposition 11.23.**

Soient $G$ un groupe d'ordre composé $n$ et $p$ un nombre premier divisant $n$, i.e $\exists m, r \in \mathbb{N}$, $n = mp^r$ avec $p$ ne divisant pas $m$, Si le seul diviseur $d$ de $n$ congru à 1 modulo $p$ est $d = 1$ alors $G$ n'est pas simple.

*Démonstration.*
Posons $n = mp^r$, $p$ ne divisant pas $m$.

Pour $m = 1$, on obtient $r > 1$ et $G$ est un $p-$groupe d'ordre non premier. On peut montrer que un sous-groupe maximal de $G$ est d'ordre $p^{r-1} > 1$ et est distingué. En particulier $G$ n'est pas simple.
Pour $m > 1$, le nombre de $p-$Sylow divisant $m$ et étant congru a 1 modulo $p$, on a $n_p = 1$ et l'unique $p-$Sylow est distingué. Ce qui achève la preuve. □

**Pour terminer sur les groupes simples : Exemples de groupes simples**

**Théorème 11.24** (Caractérisation des groupes simple d'ordre $< 60$)**.**

Un groupe d'ordre strictement inférieur à 60 est simple si et seulement s'il est trivial ou d'ordre premier.

*Démonstration.*
Par la dernière proposition, les seuls ordres composées qui ne rentrent pas dans les hypothèses sont : $12, 24, 30, 36, 38$ et $56$.
Pour $n = 12$ la conséquences des théorèmes de Sylow nous donne que $n_2 \in \{1, 3\}$.
Dans le premier cas, le $2-$Sylow est distingué et $G$ n'est donc pas simple.
Dans le second cas, l'action de conjugaison de $G$ sur $\mathrm{Syl}_2(G)$ induit un homomorphisme , non trivial car le deuxième théorème de Sylow nous dit que l'action est transitive. Card $\mathrm{S}_3 < 12$, donc $\varphi$ n'est pas injectif et son noyau est donc non trivial, donc $G$ n'est pas simple car le noyau est un sous-groupe de $G$.
On traite également par cette méthode les cas $n = 24, 48, 36$
Cas $n = 30 = 2.3.5$, la conséquence du théorème de Sylow nous montrer que $n_3 \in \{1, 10\}, n_5 \in \{1, 6\}$, si $n_3$ et $n_6$ sont strictement supérieurs à 1, $G$ possède 20 éléments d'ordre 3 et 24 d'ordre 5, donc au moins 45 éléments, ce qui est absurde.
On procède de la même manière pour $n = 56 = 2^3.6$, on obtient $n_7 \in \{1, 8\}$ et si $n_7 = 8$, l'union $X$ des éléments d'ordre 7 est de cardinal 48. En particulier le complémentaire de $X$ est de cardinal 8 et contient les $2-$Sylow (qui sont de cardinal 8) d'où l'égalité $n_2 = 1$. □

**Théorème 11.25** ($\mathrm{A}_5$)**.**

$\mathrm{A}_5$ est simple.

*Démonstration.* Soit $H$ un sous-groupe distingue de $\mathrm{A}_5$, non réduit a l'élément neutre. Par la décomposition d'une permutation en cycles disjoints, les éléments de $\mathrm{A}_5$ sont d'ordre $1, 2, 3$ ou $5$.

Si $H$ ne contient que des éléments d'ordre 1 ou 2, $H$ est un 2−groupe et son ordre est 2 ou 4. Dans le cas où c'est 2, $H$ serait un sous-groupe du centre de $\mathrm{A}_5$ et serait engendré par le produit $x = (ab)(cd)$ de deux transpositions. Mais on peut montrer que $x$ ne commute pas avec le 3−cycle $(abc)$, donc c'est absurde.
Finalement il reste la possibilité que $H$ soit d'ordre 4 ce qui en fait un 2−Sylow de $\mathrm{A}_5$, et alors il n'est pas distingué car il existe plus que 3 éléments d'ordre 2 et donc plusieurs 2-Sylow. Donc $H$ ne peut pas être un 2-groupe, et contient donc forcément un élément d'ordre 3 ou d'ordre 5.
Si les $p$−Sylow d'un groupe sont d'ordre $p$, l'intersection de deux d'entre eux est réduite a $(e)$ et leur union est de cardinal $(p-1)\,n_p + 1$.
Il existe $(p-1)\,n_p$ éléments d'ordre $p$. Si on applique ce raisonnement ici on a $20 = 2n_3$ (resp $24 = 4n_5$) éléments d'ordre 3 (resp 5). Donc $n_3 = 10$ et $n_5 = 6$.
Si $H$ possède un élément d'ordre 3 (resp 5), il contient un 3−Sylow (resp un 5−Sylow) et les contient même tous. Donc $\mathrm{o}(H) \geq 21$ (resp $\mathrm{o}(H) \geq 25$). Par le théorème de Lagrange, son ordre est donc égal a 30 ou 60. Dans le cas où l'ordre de $H$ est 30, les théorèmes de Sylow nous assurent que $H$ contient un élément d'ordre 3 et un d'ordre 5. Donc il contient tous les 3−Sylow et les 5−Sylow, donc $\mathrm{o}(H) > 20 + 24 + 1 = 45$ ce qui est absurde. Donc

$$H = \mathrm{A}_5$$

$\mathrm{A}_5$ est donc simple. □

**Théorème 11.26.**

Un groupe simple d'ordre 60 est isomorphe à $\mathrm{A}_5$.

*Démonstration.*
Il suffit de montrer qu'il possède un sous-groupe $H$ d'ordre 12, car l'action par translation sur les classes à gauche sous $H$ induit un homomorphisme non trivial, donc injectif, de $G$ dans $\mathrm{S}_5$. On identifie $G$ avec son image par cet homomorphisme, l'intersection de $G$ avec $\mathrm{A}_5$ est un sous groupe distingué de $G$ et n'est pas réduit à l'élément neutre. Sinon l'ordre de $G$ divisera 2 car la restriction à $G$ de l'homomorphisme de signature de $\mathrm{S}_5$ dans $\{\pm 1\}$ serait injectif. Par simplicité on en déduit que $G$ est contenu et coïncide, avec $\mathrm{A}_5$.
Montrons donc que $G$ contient un groupe d'ordre 12. La conséquence du théorème de Sylow implique que $n_2 \in \{1, 3, 5, 15\}$. Comme $G$ est simple on n'a pas $n_2 = 1$, de meme pour $n_2 = 3$.
L'action de conjugaison sur les 2−Sylow induirait un homomorphisme injectif de $G$ dans $\mathrm{S}_3$, ce qui est exclu.
Pour $n_2 = 5$ le normalisateur d'un 2−Sylow est d'ordre 12 par la formule

des classes.
Pour $n_2 = 15 : G$ ne peut avoir un seul 5-Sylow, sinon celui-ci serait distingué et contredirait la simplicité de $G$. Donc $G$ possède 6 $5-$Sylow, ce qui donne 24 élément d'ordre 5. Si tous les 2-Sylow sont d'intersections 2 à 2 triviales, il y alors 45 éléments d'ordre 1,2 ou 4, ce qui est absurde.
Il existe donc deux $2-$Sylow $S$ et $T$ tels que $S \bigcap T = \{1, x\}$ est d'ordre 2. En particulier le centralisateur $H$ de $x$ dans $G$ contient l'union $S \bigcup T$, son ordre, divisible par 4, est strictement supérieur à 6, donc vaut $12, 20$, ou 60. Le cas où $H$ est d'ordre 20 est a exclure, en effet si tel était le cas la conséquence des théorèmes de Sylow impliquerait que le sous-groupe $H$ contiendrait un unique $5-$Sylow $S$ de G. Le normalisateur de $S$ dans $G$ serait alors d'ordre au moins 20 (car contiendrait au moins $H$), ce qui donnerai au plus 3 $5-$Sylow. Comme $n_5$ peut être 1 ou 6, on aurait alors un unique 5-Sylow distingué. De même le sous-groupe $H$ ne peut pas coïncider avec $G$, sinon $S \cap T$ serait distingué, contredisant la simplicité de $G$. On en déduit donc que $H$ est d'ordre 12, ce qui conclut la démonstration. □

# Chapitre 12

# Groupes abéliens de type fini

On utilisera dans ces deux chapitres **la notation additive.**

## I Somme directe de groupes abéliens

### 1 Somme directe de sous-groupes (d'un groupe abélien)

On s'intéressera d'abord à la somme de deux sous-groupes. Soient $H$ et $K$ deux sous-groupes d'un groupe abélien $G$. On rappelle que la somme de $H$ et $K$ est le sous-groupe engendre par $H \cup K$, et on le note $H + K \overset{\text{def}}{=} \{x + y \mid x \in H, y \in K\}$.

**Définition 12.1** (Somme directe)**.**

Le sous-groupe $H+K$ est dit somme directe de $H$ et $K$ si $H \bigcap K = \varnothing$.

**Proposition 12.2** (Rappel)**.**

Soit $G$ un groupe abélien, soient $H$ et $K$ des sous-groupe de $G$. La somme $H + K$ est directe si et seulement si $\forall z \in H + K, \exists!\ (x, y) \in H \times K, z = x + y$. (la décomposition est donc unique)

*Démonstration.*
Laissée en exercice au lecteur. □

Maintenant, traitons le cas d'une somme directe d'une famille quelconque de sous-groupes. Soit $I$ un ensemble non vide, et $(H_i)_{i\in I}$ une famille de sous-groupes d'un groupe abélien $G$. Le sous-groupe de $G$ engendré par $\bigcup_{i\in I} H_i$ est

noté $\sum_{i\in I} H_i$.
Si $I$ est fini, notons $I = [\![1, n]\!]$, alors

$$\sum_{i\in I} H_i = \{x_1 + \cdots + x_n \mid \forall i \in I, x_i \in H_i\}$$

Si $I$ est infini, alors

$$\sum_{i\in I} H_i = \left\{x_{i_1} + \cdots + x_{i_n} \mid n \in \mathbb{N}, \forall j \in I, x_{i_j} \in H_j\right\}$$

La notation est admise car :

$$x \in \sum_{i\in I} H_i \Leftrightarrow x = \underbrace{\sum_{i\in I} x_i}_{\text{Somme à support fini}}$$

**Définition 12.3** (Somme directe d'une famille quelconque de sous-groupes)**.**

Soit $G$ un groupe abélien, $(H_i)_{i\in I}$ une famille arbitraire de sous-groupes de $G$. Alors le sous-groupe $\sum_{i\in I} H_i$ est appelé somme directe des $H_i$ si $\forall j \in I, H_j \bigcap \left(\sum_{i\in I, i\neq j} H_i\right) = (0)$.
Dans ce cas on peut écrire : $\bigoplus_{i\in I} H_i$

**Proposition 12.4.**

Soit $G$ un groupe abélien, et $\{H_i\}_{i\in I}$ une famille de sous-groupes de $G$. Alors $\left(\sum_{i\in I} H_i\right)$ est en somme directe si et seulement si $\forall x \in \sum_{i\in I} H_i$, $x$ s'écrit de manière unique sous la forme $x = \sum_{1\leq k\leq n} x_k$, avec $n \in \mathbb{N}, x_{i_k} \in H_k, \forall k \in [\![1, n]\!]$.

## 2 Définition de la somme directe de groupes

Soit $(G_i)_{i\in I}$ une famille de groupes abéliens, $I$ un ensemble non vide. Le but de ce paragraphe est de construire un groupe $\bigoplus_{i\in I} G_i$ vérifiant la propriété universelle suivante :

1. $\forall i \in I$, il existe un morphisme de groupe injectif :
$$q_i : \ G_i \ \to \ \bigoplus_{i\in I} G_i.$$
2. $\forall g \in G$, pour toute famille de morphismes $(f_i)_{i\in I}$, $f_i \in \mathrm{Hom}\,(G_i, G)$, il existe un unique morphisme $\varphi \in \mathrm{Hom}\left(\bigoplus_{i\in I} G_i, G\right)$ rendant commutatif le diagramme suivant :
$$\begin{array}{ccc} G_i & \xrightarrow{f_i} & G \\ \downarrow{\scriptstyle q_i} & \nearrow{\scriptstyle \varphi} & \\ \bigoplus_{i\in I} G_i & & \end{array} \quad , \forall i \in I, f_i = \varphi \circ q_i.$$

Attention, la propriété universelle du produit et celle de la somme direct sont différentes !
Construisons à présent ce groupe : On note
$$P \overset{\text{def}}{=} \prod_{i\in I} G_i$$
$$\forall i \in I, q_i : \begin{array}{ccc} G_i & \to & \prod_{j\in I} G_j = P \\ x & \mapsto & (x_j)_{j\in I} = \begin{cases} x \text{ si } j = i \\ 0_{G_j} \text{ sinon.} \end{cases} \end{array}$$
Pour tout $i \in I$, on associe à $q_i$ son image dans $P$. On pose alors $\bigoplus_{i\in I} G_i$ le sous groupe de $P$ engendré par la famille de $(\mathrm{Im}\,(q_i))_{i\in I}$ :
$$\bigoplus_{i\in I} G_i \overset{\text{def}}{=} \sum_{i\in I} \mathrm{Im}\,(q_i)$$

**Remarque 12.5.**

*Soit $j \in I$, calculons $Im\,(q_j) \bigcap \left( \sum_{i\in I, i\neq j} (Im\,(q_i)) \right)$, on a :*
$$\forall i \in I, x \in Im\,(q_i) \Leftrightarrow x = \left( \underbrace{0, \ldots, 0, x, 0, \ldots, 0}_{x \text{ à la position } j} \right)$$
*De cette description on déduit : $Im\,(q_j) \bigcap \sum_{i\neq j} Imq_i = (0)$, finalement on a prouvé que :*
$$\bigoplus_{i\in I} G_i = \bigoplus_{i\in I} Im\,(q_i)$$

**Définition 12.6.**

Soit $I$ un ensemble non vide, et $(G_i)_{i\in I}$ une famille de groupes abéliens et le sous-groupe $P = \bigoplus_{i\in I} G_i$ du produit direct.
$\prod_{i\in I} G_i$ construit ci-dessus est appelé somme directe des $G_i$.

Décrivons le en terme d'éléments :

L'élément $x$ s'écrit de manière unique $x = y_{i_1} + \cdots + y_{i_n}$, avec $n \in \mathbb{N}, \forall i \in [\![1, n]\!], y_{i_j} \in \mathrm{Im}\left(q_{i_j}\right)$.

$$x = q_{i_1}\left(x_{i_1}\right) + \cdots + q_{i_n}\left(x_{i_n}\right).$$

**Remarque 12.7.**

1. $\bigoplus_{i\in I} G_i$ *est un sous-groupe de* $\prod_{i\in I} G_i$.
2. $\bigoplus_{i\in I} G_i = \prod_{i\in I} G_i \Leftrightarrow I$ *fini.*
   *Si* $\forall i \in I, G_i = G$, *alors* $\bigoplus_{i\in I} G_i \overset{def}{=} G^{(I)}$ *et* $\prod_{i\in I} G_i = G^I$.
   *Vérifions que l'objet défini ci-dessus est solution du problème universel énoncé en début de chapitre.*

*Démonstration.*

**Cas où $I$ est fini** : Par induction, on se convaincra qu'il suffit de traiter le cas $|I| = 2$. Prenons donc $I = \{1, 2\}$. Par construction :

$$\mathrm{Im}\left(q_i\right) \subset G_1 \oplus G_2$$

Par factorisation :

$$q_i : \begin{array}{ccc} G_i & \to & \mathrm{Im}\left(q_i\right) \subset G_1 \oplus G_2 \end{array}$$

$$\begin{array}{ccccc} G_1 & \xrightarrow{q_1} & G_1 \oplus G_2 & \xleftarrow{q_2} & G_2 \\ & {\scriptstyle f_1}\searrow & \downarrow{\scriptstyle \exists!\varphi} & \swarrow{\scriptstyle f_2} & \\ & & G & & \end{array}$$

Existence de $\varphi$ : $\begin{array}{ccc} G_1 \oplus G_2 & \to & G \\ x & \mapsto & f_1\left(x_1\right) + f_2\left(x_2\right) \end{array}$. Soit $x \in G_1 \oplus G_2$, alors $\exists!\left(x_1, x_2\right) \in G_1 \times G_2$, $x = q_1\left(x_1\right) + q_2\left(x_2\right)$. On vérifie la commutativité, i.e que $\forall i \in \{1, 2\}$, $\varphi\left(q_i\left(x_i\right)\right) = f_i\left(x_i\right)$. On a alors $\varphi$

morphisme de groupes.
Unicité de $\varphi \in \mathrm{Hom}(G_1 \oplus G_2, G)$ faisant commuter le diagramme :

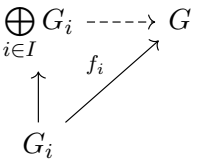
$$\begin{aligned}\varphi(x_1, x_2) &= \varphi(q_1(x) + q_2(x)) \\ &= f_1(x_1) + f_2(x_2)\end{aligned}$$

C'est donc la seule possibilité pour $\phi$.

**Cas où $I$ est infini.**
$(x_i)_{i\in I} \in \bigoplus_{i\in I} G_i$, $\bigoplus_{i\in I} G_i$ opère sur lui-même. On veut construire :

$$\varphi : \begin{array}{ccc} \bigoplus_{i\in I} G_i & \to & G \\ \underbrace{(x_i)_{i\in I}}_{\text{à support fini}} & \mapsto & \sum_{i\in I} f_i(x_i) \end{array}$$

avec $\forall i \in I, f_i(x_i) \in G$.




Cela donne l'existence de $\varphi$ par construction et comme dans le cas $I$ fini, l'unicité se déduit par commutativité.

□

La proposition qui suit est une proposition formelle.

**Proposition 12.8.**

Soit $(G_i)_{i\in I}$, $I \neq \varnothing$ famille de groupes abéliens. Soit $G$ un groupe abélien.
Alors $G$ est isomorphe a $\bigoplus_{i\in I} G_i$ si et seulement si il existe une famille de sous-groupes $(H_i)_{i\in I}$ de G tels que :
- $\forall i \in I, H_i \simeq G_i$
- $G = \bigoplus_{i\in I} H_i$

*Démonstration.*
Démonstration laissée en exercice. □

**Corollaire 12.9.**

Soit $(G_i)_{i\in I}, (G'_i)_{i\in I}$, $I \neq \varnothing$, alors :

$$\left(\forall i \in I, G_i \simeq G'_i\right) \Rightarrow \bigoplus_{i\in I} G_i \simeq \bigoplus_{i\in I} G'_i.$$

*Démonstration.*
On pose $N \overset{\text{def}}{=} \bigoplus_{i\in I} G_i, T \overset{\text{def}}{=} \bigoplus_{i\in I} \operatorname{Im}(q_i), G = \prod_{i\in I} G_i$
$q_i : G_i \to G$ est un morphisme canonique (injectivité). On pose $H_i \overset{\text{def}}{=} \operatorname{Im}(q_i)$ $\forall i \in I$, c'est un sous-groupe de $T$. Par hypothèse, pour tout $i$ dans $I$, $H_i \simeq G_i \simeq G'_i$ et donc

$$T \simeq \bigoplus_{i\in I} G_i$$

□

**Définition 12.10.**

Soit $G$ un groupe abélien, $H$ un sous-groupe de $G$. On dit que $H$ est un facteur direct de $G$ s'il existe un sous-groupe $K$ de $G$ tel que $G = H \oplus K$.
(On notera que $K$ est aussi un facteur direct de $G$)

**Proposition 12.11.**

Soit $G$ un groupe, soit $H$ un sous-groupe de $G$ tel que $H$ s'injecte dans $G$ par $q$. On a l'équivalence suivante :

$$(H \text{ est un facteur direct de } G) \Leftrightarrow (\exists p \in \operatorname{Hom}(G, H), p \circ q = \mathrm{Id})$$

*Démonstration.*
Si $H$ est un facteur direct de $G$ : $H \overset{q}{\hookrightarrow} G = H \oplus K \simeq H \times K$ et $p \circ q = \mathrm{Id}$
Réciproquement, supposons qu'il existe $p \in \operatorname{Hom}(G, H)$ tel que $p \circ q = \mathrm{Id}$, soit $g \in G, h = p(g) \in H$ donc $p(q(h)) = h$ d'où $p(q(h) - g) = 0$ donc

$$g - p(h) \in \operatorname{Ker} p$$

donc

$$g \in H + \ker p, G = H + \operatorname{Ker} p$$

Prouvons que $\ker(p) \bigcap H = \{0\}$ : Soit $h \in H \bigcap \operatorname{Ker}(p)$, alors $h = p \circ q(h) = p(h)$, i.e $h = 0$. □

# II Groupes abéliens, libres de types finis

## 1 Caractérisation des groupes abéliens libres

**Définition 12.12.**

On dit que $G$ un groupe abélien est libre s'il est somme directe de groupe monogènes infinis.
i.e il existe $I \neq \varnothing$ un ensemble tel que : $\forall i \in I, G_i = \langle x_i \rangle$, où $x_i \in G_i$. ($G_i \simeq \mathbb{Z}$) En effet $x_i$ est d'ordre infini donc $G_i \simeq \mathbb{Z}$ sinon on aurait $G_i \simeq \mathbb{Z}/n\mathbb{Z}$ où $n = \mathrm{o}(x_i)$.

$$G = \bigoplus_{i \in I} \langle x_i \rangle \simeq \bigoplus_{i \in I} \mathbb{Z} \simeq \mathbb{Z}^{(I)}$$

$$\forall i \in I, \exists x_i' \in G, G = \bigoplus_{i \in I} \langle x_i' \rangle$$

En fait on doit comprendre cela de cette manière : Un groupe abélien libre est un groupe abélien qui possède une base, i.e une partie $B$ telle que tout élément du groupe s'écrive de manière unique comme combinaison linéaire à coefficients entiers d'éléments de $B$
Par convention, le groupe trivial $\{0\}$ est libre, de base $\varnothing$.

**Définition 12.13** (Base de groupes libres)**.**

La famille des $(x_i')_{i \in I}$ est appelée base

**Proposition 12.14.**

Soit $F$ un groupe abélien, $X = (x_i)_{i \in I}$ une famille d'éléments de $F$.
On a alors l'équivalence entre :

- $F$ est un groupe abélien libre de base $X$.
- $\forall x \in F, \exists! k \in \mathbb{N}^*, \forall j \in [\![1, k]\!],\ \exists! i_j \in X,\ \exists n_j \in \mathbb{Z}$, tels que

$$x = \sum_{j=1}^{k} n_j x_{i_j}.$$

- $X$ est une partie génératrice de $F$ et
  $\forall (i_1, \ldots, i_k) \in I, \left[ \sum_{i=1}^{k} n_j x_{i_j} = 0 \Rightarrow \forall i \in [\![1, k]\!], n_j = 0 \right]$.

*Démonstration.*
Montrons la première implication : Soit $X$ une base de $F$, d'où $F = \bigoplus_{i \in I} \langle x_i \rangle$,

alors $\forall x \in F, x = \sum_{j=1}^{k} y_{i_j}$, avec $y_{i_j} \in \langle x_{i_j} \rangle, \forall j \in [\![1, j]\!]$

$$\forall j \in [\![1, k]\!], y_{i_j} = n_j x_{i_j}, \text{ où } x_{i_j} \in \mathbb{Z}$$

□

**Définition 12.15.**

Si $G$ est un groupe abélien et $(u_i)$ une famille d'éléments de $G$.
Les $u_i \in G$ sont linéairement indépendants sur $\mathbb{Z}$ si et seulement si Pour tout famille finie non vide $(i_1, \ldots, i_k)$, on a l'implication $\left( \sum_{j=1}^{k} n_j u_{i_j} = 0 \right) \Rightarrow (\forall j \in [\![1, k]\!], n_j = 0)$

**Propriétés 12.16.**

1. Dans un groupe abélien, une sous-famille d'une famille libre est libre.
2. Tout élément d'une famille libre est non nul

**Théorème 12.17** (Admis)**.**

Soit $G$ un groupe abélien de type fini, alors il existe un groupe abélien libre $G'$ ayant une base de cardinal fini et un morphisme de groupe injectif

$$f : \ G' \ \to \ G$$

On notera que $G'/\ker f \simeq G$

## 2 Rang d'un groupe abélien libre de type fini

**Théorème 12.18.**

Soit $F$ un groupe abélien non réduit à l'élément neutre. On a l'équivalence suivante :

$$(F \text{ est libre et de type fini}) \Leftrightarrow (F \text{ a une base finie})$$

Dans ce cas, toutes les bases sont finies et ont le même nombre d'éléments. Ce nombre est appelé **rang** de $F$.
Si $F$ est libre de type fini et possède une base finie, on dira qu'il est de rang fini.

On classera les groupes abélien libres comme les espaces vectoriel : à isomorphismes près.

*Démonstration.*
L'inclusion de droite se fait par définition.
Montrons l'inclusion à gauche : Soit $X = (x_i)_{i\in I}$ une base de $F$. Soit $Y = \{y_1, \dots, y_k\}$ un système de générateurs de $F$. Pour tout $m \in [\![1, k]\!]$, il existe $J_m \subset I$ tel que $y_m \in \sum\limits_{J\subset J_m} \langle x_j \rangle$.

Soit $x \in F$, alors $\exists a_m \in \mathbb{Z}$ tel que $x = \sum\limits_{i=1}^{s} a_i y_i$. En d'autres termes, $x \in \sum\limits_{j\in J} \langle x_i \rangle$ si $J = \bigcup\limits_{m=1}^{s} J_m$.
Donc $(x_i)_{i\in J}$ est une famille libre (comme sous-famille de famille libre).
Montrons que $I = J$, supposons que $\exists k \in I$ tel que $k \notin J$. alors :

$$\begin{cases} x_k = \sum\limits_{j\in J} n_j x_j \\ x_k \neq 0 \end{cases}$$

donc

$$\langle x_k \rangle \bigcap \sum_{i\in I, i\neq k} \langle x_i \rangle \neq \langle 0 \rangle$$

car qui est impossible car $(x_i)_{i\in I}$ est une base de $F$. Donc $(x_j)_{j\in J}$ est une famille génératrice de $F$ donc $F = \bigoplus\limits_{j\in J} \langle x_j \rangle$ et tout base de $F$ est finie.
Montrons que toutes les bases ont le même cardinal :
Soit $\{x_1, \dots, x_n\}$ une base de $F$, on introduit le sous-groupe $2F = \{2x, x \in F\}$, qui ne dépend donc que de la donnée de $x \in F$, or $x$ s'écrit de manière unique.
$x = \sum\limits_{i-1}^{k} \alpha_i x_i$. Si on prend $x \in F$ écrit de telle manière.

$$x \in 2F \Leftrightarrow \forall i \in I, \alpha_i = 2\beta_i$$

Par conséquent $2F = \bigoplus_{i=1}^{k} \langle 2x_i \rangle$ et donc : $F/2F = \left(\bigoplus_{j]1}^{n} \langle x_i \rangle\right) / \left(\bigoplus_{j]1}^{n} \langle 2x_i \rangle\right)$
On en déduit un isomorphisme de groupe : $F/2F \simeq \bigoplus_{i=1}^{n} \mathbb{Z}/2\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z})^n$.
Ce quotient ne dépend que de $F$, donc $n$ est constant indépendamment de la base. □

**Proposition 12.19** (Admise)**.**

Soit $G$ un groupe abélien et $H$ un sous-groupe de $G$. On a alors l'équivalence suivante :

$$(G/H \text{ est libre}) \Leftrightarrow (H \text{ est facteur direct de } G)$$

## III Groupes abéliens de torsion

**Définition 12.20.**

Soit $G$ un groupe, on dit que :
- $G$ est de torsion si tout élément de $G$ est d'ordre fini.
- $G$ est sans torsion si tout élément de $G \setminus \{e_G\}$ est d'ordre infini.

**Exemple 12.21.**
1. *Tout groupe fini est de torsion.*
2. *Un groupe abélien libre est de torsion.*
3. *$\mathbb{Q}$ est sans torsion.*
4. *$\mathbb{Q}/\mathbb{Z}$ est de torsion.*
5. *$(C^*, *)$ est ni de torsion, ni sans torsion.*

On pourra s'interroger sur : On sait qu'un groupe fini et de type fini est de torsion, mais la réciproque est-elle vraie ? La réciproque est vraie par le théorème de structure suivant :

**Théorème 12.22.**

Soit $G$ un groupe abélien, alors :
- $\mathrm{T}(G)$ l'ensemble formé des éléments de $G$ d'ordre fini est un sous-groupe de $G$.
- $G/\mathrm{T}(G)$ est un groupe sans torsion

**Exemple 12.23.** *Si $G$ est de torsion, alors $T(G) = G$*

*Démonstration.*
$\forall x, y \in \mathrm{T}(G), \exists n, m \in \mathbb{Z}$ tel que $\mathrm{o}(x) = n, \mathrm{o}(y) = m$

$$mn(x-y) = mnx - mny = 0$$

donc $x - y \in T(G)$ et

$$\mathrm{T}(G) \leq G$$

Soit $\overline{x} \in G/\mathrm{T}(G)$, tel que $m\overline{x} = \overline{0}$, $n > 1$.
Alors $mx \in \mathrm{T}(G)$, donc $\exists n \in \mathbb{Z}, mnx = 0$ d'où $x \in \mathrm{T}(G)$ et $\overline{x} = \overline{0}$ □

# IV Théorème de structure des groupes abéliens de type fini

**Proposition 12.24.**

Soit $G$ un groupe abélien de type fini alors :
- $G$ est de torsion $\Leftrightarrow$ $G$ est fini.
- $G$ est sans torsion $\Leftrightarrow$ $G$ est libre.

*Démonstration.*
Le sens réciproque est trivial, faisons le sens direct :
Premier point : Supposons $G$ de torsion. Alors il existe une famille génératrice $\lambda = (x_1, \ldots, x_k)$, soit $\alpha_i \overset{\text{def}}{=} \mathrm{o}(x_i) \in \mathbb{N}$. Soit $y \in G$, alors $\exists (x_i)_{i \in [\![1,k]\!]} \in \mathbb{Z}^k$, $y = \sum_{i-1}^{k} n_i x_i$.
Pour $i \in [\![1,k]\!], n_i = \alpha_i q_i + r_i$ (division euclidienne) où $r_i$ est bornée par hypothèse. Donc l'ensemble des éléments est paramétrée par $\sum_{i=1}^{n} \beta_i x_i$ où $|\beta_i| \leq \alpha_i$.
Donc $G$ est fini.
Deuxième point : supposons $G$ sans torsion, alors $X = \{x_1, \ldots, x_r\}$ est un système de générateurs de $G$, c'est à dire $G = \sum_{i=1}^{r} \langle x_i \rangle$. On raisonne par récurrence sur $r$.
Si $r = 1$, $G = \langle x_1 \rangle \simeq \mathbb{Z}$, et $G$ est libre.
Soit $r \geq 2$, tel que ce soit vrai pour $k \in [\![1, r-1]\!]$,
Si on a $\sum_{i=1}^{r} n_i x_i = 0$, on pose $d \overset{\text{def}}{=} \underset{i \in [\![1,r]\!]}{\mathrm{pgcd}}(n_i)$.
Alors on peut supposer $d = 1$. En effet, si $1 < d$, alors

$$d\left(\sum_{i=1}^{r} n_i' x_i\right) = 0$$

d'où $\sum_{i=1}^{r} n_i x_i = 0$ car $G$ est sans torsion.

Considérons $\sum_{i=1}^{r} n_i x_i = 0$ tel que $\underset{i\in[\![1,r]\!]}{\text{pgcd}}\,(n_i) = 1$ montrons que $n_i = 0$ pour tout $i$.

**1er cas :** $\exists j \in [\![1,r]\!], n_j = 1$ On peut supposer $j = 1$, alors

$$\sum_{i=1}^{r} n_i x_i = 0 \Leftrightarrow -\sum_{i=2}^{r} n_i x_i = x_1$$

Donc $\{x_2, \ldots, x_r\}$ est une famille génératrice de $G$, par hypothèse de récurrence, on obtient le résultat.

**2ème cas :** $\forall j \in [\![1,r]\!]\ n_j \neq 0$ Il existe en particulier $n_i, n_j$ distincts et différents de 0 tels que $|n_i| \neq |n_j|$. On suppose $|n_1| > |n_2| > 0$, $\exists \lambda \in \mathbb{Z}$ tel que

$$0 \leq |n_1 - \lambda n_2| \leq n_2$$

$n_1 = qn_2, \lambda = q - 1$. Par division euclidienne, et si on prend le reste, on introduit $x_2' \overset{\text{def}}{=} x_2 + \lambda x_1$ alors $\{x_1, x_2', x_3, \ldots, x_r\}$ reste génératrice. Par suite $\sum_{i=1}^{r} n_i x_i = 0$ devient

$$0 = (n_1 - \lambda n_2)\, x_1 + n_2 x_2 + \cdots + \ldots$$

On a $\text{pgcd}\,(n_1 - \lambda n_2, \ldots, n_r) = 1$

On a donc deux cas :

- Si $|n_1 - \lambda n_2| = 1$, on est ramené au cas précédent.
- Si $|n_1 - \lambda n_2| > 1$ on rapplique ce processus jusqu'à avoir un coefficient 1. On est assuré que ce processus termine car la somme des modules des coefficients décroit strictement à chaque passage.

□

**Théorème 12.25.**

Tout groupe abélien de type fini est somme directe d'un groupe abélien libre de type fini et d'un groupe fini.
De plus, cette décomposition est unique à isomorphisme près.

*Démonstration.*
$G/\mathrm{T}(G)$ est un groupe abélien de type fini, donc $G/\mathrm{T}(G)$ est libre de type fini, donc $\mathrm{T}(G)$ est facteur direct de $G$ par 12.19. $\exists F \leq G$ tel que

$$G = \mathrm{T}(G) \oplus F$$

$\mathrm{T}(G)$ est abélien de torsion, donc $\mathrm{T}(G) \simeq G/F$ et $F$ est donc de type fini, de plus il est libre.

$\mathrm{T}(G)$ est abélien de type fini et de torsion donc est fini par 12.24. □

**Théorème 12.26.**

Soit $G$ abélien de type fini.
Alors :

1. $\exists x_1, \dots, x_r, y_1, \dots, y_l \in G$ tel que :
   — $G = \langle x_1 \rangle \oplus \cdots \oplus \langle x_r \rangle \oplus \langle y_1 \rangle \oplus \cdots \oplus \langle y_l \rangle$
   — Si $r \neq 0$, $\langle x_i \rangle \simeq \mathbb{Z}, \forall i \in [\![1, r]\!]$
   — Si $r \neq 0$, $\langle y_i \rangle$ est cyclique, d'ordre $d_j$, $\forall j \in [\![1, l]\!]$ tel que $\forall j \in [\![1, l-1]\!], d_{j+1} | d_j$
2. Si $G = \langle v_1 \rangle \oplus \cdots \oplus \langle v_q \rangle \oplus \langle w_1 \rangle \oplus \cdots \oplus \langle w_t \rangle$ avec : $\langle v_i \rangle \simeq \mathbb{Z}$ et $\langle w_i \rangle$ cyclique d'ordre $e_i$ avec $\forall i \in [\![1, t-1]\!], e_{i+1} | e_i$ alors :
$$\begin{cases} r = q \\ s = t \\ e_j = \alpha_j \forall j \in [\![1, l]\!] \end{cases}$$

Dans la pratique, on utilisera souvent ce théorème sous cette forme équivalente :

**Théorème 12.27.**

Soit $G$ abélien de type fini. Alors $\exists!(r, m) \in \mathbb{N}^2$, $\exists!(d_1, \dots, d_m) \in \mathbb{N}^m$ tels que :

$$d_1 \mid \cdots \mid d_m$$

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z}$$

# Chapitre 13

# Troisième exemple de groupes : les groupes Diédraux

## I Définitions

Soit $n \in \mathbb{N}$ tel que $n \geq 3$. On se place dans le plan complexe, et on considère le polygone régulier à $n$ côtés $\mathrm{P}_n$ formé par les racines $n^{\text{ièmes}}$ de l'unité $\exp^{\frac{2ik\pi}{n}}$ où $k \in [\![0, n-1]\!]$.

**Proposition 13.1.**

L'ensemble des isométries affines de $\mathbb{C} \cong \mathbb{R}^2$ opère sur $\mathbb{C}^n$ via l'opération :

$$f \cdot (x_1, \ldots, x_n) = (f(x_1), \ldots, f(x_n)).$$

*Démonstration.*
Immédiate. □

**Définition 13.2** (Groupe diédral)**.**

On appelle groupe diédral de degré $n$ et on dote $\mathrm{D}_n$ le stabilisateur de $\left\{\exp^{\frac{2ik\pi}{n}}, k \in [\![0, n-1]\!]\right\}$ pour l'opération définie dans la proposition précédente.

On peut donc en conclure que le groupe Diédral de degré $n$ est l'ensemble des isométries affines telle que l'image de $\mathrm{P}_n$ est $\mathrm{P}_n$. Tout isométrie conservant $\mathrm{P}_n$ fixe le point $O$ par conservation des distances, il suffit donc de considérer les isométries vectorielles, autrement dit $O_2(\mathbb{R})$

**Rappel : Isométries vectorielles.**

**Définition 13.3.**

L'ensemble des isométries vectorielles de $\mathbb{R}^2$ est l'ensemble des applications linéaires inversibles préservant les distances.

**Proposition 13.4.**

Une isométrie vectorielle de $\mathbb{R}^2$ est de déterminant 1 ou -1 et envoie toute base orthonormée sur une base orthonormée. Elle est entièrement déterminée par l'image de deux point non-colinéaires.

## II Caractérisation de $D_n$.

Soit $n \in \mathbb{N}$, tel que $n \geq 3$.

**Proposition 13.5.**

$D_n$ contient un sous-groupe cyclique d'ordre 2.

*Démonstration.*
La réflexion $s$ d'axe $(OI)$, avec $I$ d'affixe 1 appartient a $D_n$. Or $s$ est d'ordre 2 donc $\langle s \rangle$ est un sous-groupe cyclique, d'ordre 2 de $D_n$. En effet la réflexion d'axe renvoie un point $A$ à un symétrique par cette réflexion, notons le $A'$, mais le symétrique de $A'$ par la réflexion est lui même $A$. □

De manière plus générale encore :

**Proposition 13.6.**

$D_n$ contient un sous-groupe cyclique d'ordre $n$.

*Démonstration.*
Les rotations $r\left(O, \frac{2k\pi}{n}\right)$ de centre O et d'angle $\frac{2k\pi}{n}$, où $k \in [\![0, n-1]\!]$ appartiennent à $D_n$. Ces rotations auxquelles on ajoute l'identité Id forment un sous-groupe cyclique de $D_n$, d'ordre $n$, engendré par la rotation $r\left(O, \frac{2\pi}{n}\right)$ (qui est d'ordre $n$ ). On pose ensuite $s \overset{\text{def}}{=} s\,(OI)$ la réflexion d'axe $(OI)$ avec $I$ d'affixe 1 et $r = r\left(O, \frac{2\pi}{n}\right)$ la rotation de centre $O$ et d'angle $\frac{2\pi}{n}$.
On a montre que $s$ et $r$ appartiennent a $D_n$. □

**Proposition 13.7.**

On a, en conservant les notations précédentes :

$$s \circ r \circ s \circ r = \mathrm{Id}$$

*Démonstration.*
Montrons que $s \circ r \circ = r^{-1}$, $r^{-1}$ est la rotation de centre $O$, et d'angle $\frac{-2\pi}{n}$, or :

$$\det(s \circ r \circ s) = \det r = 1$$

donc $s \circ r \circ s$ est une isométrie directe de $\mathbb{R}^2$, i.e une rotation. De plus $s \circ r \circ s(\mathrm{O}) = O$ donc $s \circ r \circ s$ est de centre $O$. $s \circ r \circ s(I) = s(r(I))$ est le point d'affixe $\exp^{-2\pi n}$ donc $s \circ r \circ s$ est une rotation de centre $O$ et d'angle $\frac{-2\pi}{n}$, i.e $s \circ r \circ s = r^{-1}$. □

**Proposition 13.8.**

$\mathrm{D}_n$ est engendré par $s$ et $r$.

*Démonstration.*
Posons $A_0 = I$, pour $k \in [\![1, n-1]\!]$, on définit $A_k$ comme le point d'affixe $\exp \frac{2k\pi}{n}$.
Soit $f \in \mathrm{D}_n$, alors $f$ étant une isométrie de $\mathbb{R}^2$, ayant au moins un point fixe, $O$, $f$ est soit une rotation, soit une réflexion. Si il existe $k \in [\![0, n-1]\!]$ tel que $f(A_k) = A_k$, alors $O$ et $A_k$ sont des points fixes pour $f$ donc $f$ est la réflexion d'axe $(OA_k)$.
$s \circ r^{n-2k}(A_k) = s(A_{n-k}) = A_k$ donc $O$ et $A_k$ sont des points fixes pour $s \circ r^{n-2k}$. D'où $s \circ r^{n-2k} = f$ et $f \in \langle \{s, r\} \rangle$.
Supposons que $f(A_k) \neq A_k$, pour tout $k \in [\![0, n-1]\!]$, supposons que $f$ soit une rotation.
Soient $k, m \in [\![0, n-1]\!]$ tels que $f(A_k) = A_m$, alors l'angle de $f$ est égal a $\left(\overrightarrow{OA_k}, \overrightarrow{OA_m}\right) = \arg \frac{e^{\frac{2ik\pi}{n}}}{e^{\frac{2im\pi}{n}}} = \frac{2(k-m)\pi}{n}$
D'où $f = r^{k-m} \in \langle \{s, r\} \rangle$ Supposons maintenant que $f$ est une réflexion d'angle $\Delta$, $O$ appartient a $\Delta$. $f \in \mathrm{D}_n$, il existe $k \in [\![0, n-1]\!]$ tel que $\Delta$ coupe $[A_k, A_{k+1}]$ en son milieu (où on pose $A_n = A_0$ si $k = n$ ).
Montrons alors que $f = s \circ r^{n-2k-1}$ :

$$\det\left(s \circ r^{n-2k-1}\right) = \det(s) \det\left(r^{n-2k-1}\right) = -1.1 = -1$$

donc $s \circ r^{n-2k-1}$ est une réflexion. Comme $s \circ r^{n-2k-1}(A_k) = s(A_{n-k-1}) = A_{k+1}$, l'axe de $s \circ r^{n-2k-1}$ passe par le milieu de $[A_k, A_{k+1}]$. Comme $s \circ$

$r^{n-2k-1} \in \mathrm{D}_n$, $O$ appartient a l'axe de $s \circ r^{n-2k-1}$. D'où l'axe de $s \circ r^{n-2k-1}$ est $\Delta$ et $fs \circ r^{n-2k-1} \in \langle\{s, r\}\rangle$.
Tout élément de $\mathrm{D}_n$ appartient a $\langle\{s, r\}\rangle$ donc $\mathrm{D}_n \subseteq \langle\{s, r\}\rangle$. Comme $s, r \in \mathrm{D}_n$, on a également : $\langle\{s, r\}\rangle \subseteq \mathrm{D}_n$. D'où :

$$\langle\{s, r\}\rangle = \mathrm{D}_n$$

□

**Proposition 13.9** (Pour résumer)**.**

$\mathrm{D}_n$ est donc un sous-groupe engendre par deux éléments $s$ et $r$ verifiant :

- $s$ est d'ordre 2
- $r$ est d'ordre $n$
- $s \circ r \circ s \circ r = \mathrm{Id}$. (Ou encore, $sr$ est d'ordre 2)

# III Étude de $\mathrm{D}_n$.

Par les résultats des sections précédentes on a donc les propositions :

**Proposition 13.10.**

Tout groupe engendré par deux éléments $a$ et $b$ tels que :

1. $a$ est d'ordre 2
2. $b$ est d'ordre $n$
3. $abab = 1$

est isomorphe à $\mathrm{D}_n$.

Pour étudier $\mathrm{D}_n$, on va donc se placer dans le cadre définie par la proposition précédente.

## 1 Éléments de $\mathrm{D}_n$.

**Proposition 13.11.**

$\mathrm{D}_n$ n'est pas abélien.

*Démonstration.*
Puisque $abab = 1$, on a $abab^{-1} = b^{-2}$. Or $b^{-2}$ est différent de 1 car $b$ est

d'ordre $n > 2$, donc $abab^{-1} \neq 1$. D'où, $a$ étant d'ordre 2, $(ab)(ba)^{-1} = abab^{-1} \neq 1$ et par conséquent, $ab \neq ba$.
$\mathrm{D}_n$ n'est donc pas abélien. □

**Proposition 13.12.**

Pour tout nombre entier $k \in [\![0, n-1]\!]$, on a

$$ab^k a = b^{-k}$$

*Démonstration.*
Nous allons procéder par récurrence sur $k$, $1 \leq k \leq n$.

$k = 1$ **:** $abab = 1$ donc $aba = b^{-1}$

**Héridité :** Supposons que la propriété est vrai jusqu'à l'entier $k-1$, alors :

$$\begin{aligned} ab^k a &= ab^{k-1}ba \\ &= ab^{k-1}aaba \text{ car } a \text{ est d'ordre2} \\ &= b^{1-k}b^{-1} \text{ par hypothèse de récurrence} \\ &= b^{-k} \end{aligned}$$

□

**Proposition 13.13.**

$a$ n'est pas une puissance de $b$.

*Démonstration.*
Supposons qu'il existe un entier $k$ compris entre 1 et $n-1$ tel que : $a = b^k$ alors $abab = b^{2k+2} = b^{2k}b^2$, comme $a = b^k$ est d'ordre 2, alors $b^{2k} = 1$ d'où $abab = b^2$ et comme $abab = 1$,on obtient $b^2 = 1$.
Par conséquent, $k$ est d'ordre au plus 2, ce qui est impossible puisque $b$ est d'ordre $n > 2$. □

**Proposition 13.14.**

$\mathrm{D}_n = \{1, a, b, \ldots, b^{n-1}, ab, \ldots, ab^{n-1}\}$.

*Démonstration.*
Comme $a$ n'est pas une puissance de $b$, $D_n$ contient les éléments distincts : $1, a, b, \ldots, b^{n-1}$. Si $k, m$ sont deux entiers distincts compris entre 1 et $n-1$, alors $ab^k \neq ab^m$. D'où, puisque $b$ est d'ordre $n$, et comme $a$ n'est pas une puissance de $b$, $D_n$ contient les éléments $1, a, b, \ldots, b^{n-1}, ab, \ldots, ab^{n-1}$.
Soit $x \in D_n$, comme $D_n$ est engendre par $a$ et $b$, $x$ s'écrit sous la forme $a^{m_1}b^{k_1}\ldots a^{m_r}b^{k_r}$ avec $\forall i \in [\![1, r]\!], m_i = 0$ ou 1 et $k_i \in [\![0, n-1]\!]$, par la propriété 13.12, et puisque $a = a^{-1}$, $b^k a = ab^{-k}$, et ce pour tout entier $k$ compris entre 1 et $n-1$.
D'où on peut se ramener à l'écriture de $x$ à une écriture de la forme $a^k b^m$ avec $k = 0$ ou 1 et $m$ compris entre 0 et $n-1$.
Par suite, $D_n = \{1, a, b, \ldots, b^{n-1}, ab, \ldots, ab^{n-1}\}$ □

**Corollaire 13.15.**

$D_n$ est d'ordre $2n$

## 2 Sous-groupe normaux de $D_n$.

**Proposition 13.16.**

$\langle b \rangle$ est un sous-groupe normal de $D_n$.

*Démonstration.*
L'ordre de $\langle b \rangle$ est $n$, donc l'indice de $\langle b \rangle$ dans $D_n$ est $[D_n : \langle b \rangle] = \frac{|textD_n|}{|\langle b \rangle|} = 2$.
On en déduit que $\langle b \rangle$ est normal dans $D_n$. □

**Proposition 13.17.**

$D_n$ est le produit semi-direct de $\langle b \rangle$ par $\langle a \rangle$

*Démonstration.*
Par la proposition précédente, on a $\langle b \rangle$ normal dans $D_n$, et $a$ n'est pas une puissance de $b$ (cf proposition 13.13), donc $\langle b \rangle \bigcap \langle a \rangle = \{1\}$. Comme l'ordre de $\langle b \rangle \langle a \rangle$ est $\frac{|\langle b \rangle \langle a \rangle|}{|\langle b \rangle \bigcap \langle a \rangle|}$ (cf le cours sur le produit semi-direct). On a donc :

$$|\langle b \rangle \langle a \rangle| = \frac{2n}{1} = 2n = |D_n|$$

et par conséquent $\langle b \rangle \langle a \rangle = D_n$ D'où $D_n$ est le produit semi-direct de $\langle b \rangle$ par $\langle a \rangle$. □

Par la propriété 13.12, on définit un homomorphisme $\alpha$ du groupe $\langle a\rangle$ dans le groupe $\mathrm{Aut}(\langle b\rangle)$ en posant :

$$\begin{cases}\alpha(1) = \mathrm{Id} \\ \alpha(a)\left(b^k\right) = ab^ka^{-1} = ab^ka = b^{-k}\end{cases}$$

**Proposition 13.18.**

$\mathrm{D}_n$ est isomorphe au produit semi-direct $\langle b\rangle \rtimes_\alpha \langle a\rangle$.

*Démonstration.*
Si on pose $N = \langle b\rangle \times \{1\}$ et $H = \{1\} \times \langle a\rangle$ alors $\langle b\rangle \rtimes_\alpha \langle a\rangle$ est le produit semi-direct de $N$ par $H$.
Montrons que le produit semi-direct de $\langle b\rangle$ par $\langle a\rangle$ dans $\mathrm{D}_n$ est isomorphe au produit semi direct de $N$ par $H$ dans $\langle b\rangle \rtimes_\alpha \langle a\rangle$.
$\forall k \in [\![0, n-1]\!]$, on pose $f\left(b^ka^m\right) = \left(b^k, 1\right)(1, a^m)$. $f$ est clairement bijective.
Soient $0 \leq k, r \leq n-1, m, s \in \{0, 1\}$. $\langle b\rangle$ étant normal dans $\mathrm{D}_n$, on a $a^mb^ra^{-m} \in \langle b\rangle$ donc :

$$\begin{aligned} f\left(b^ma^kb^ra^s\right) &= f\left(b^ma^kb^ra^{-m}\right) f\left(a^ma^s\right) \\ &= \left(b^ma^kb^ra^{-m}, 1\right)\left(1, a^ma^s\right)\end{aligned}$$

Puisque l'on utilise la loi du produit semi-direct, on a :

$$\begin{aligned} f(b^ka^m)f(b^ra^s) &= \left(b^k, 1\right)(1, a^m)\left(b^r, 1\right)(1, a^s) \\ &= \left(b^k\alpha(1)(1), 1a^m\right)\left(b^r\alpha(1)(1), 1a^s\right) \\ &= \left(b^k, a^m\right)\left(b^r, a^s\right) \\ &= \left(b^k\alpha\left(a^m\right)\left(b^r\right), a^ma^s\right) \\ &= \left(b^ka^mb^ra^{-m}, a^ma^s\right)\end{aligned}$$

D'où $f$ est un isomorphisme entre les produits directs de sous-groupes : $\langle b\rangle \rtimes_\alpha \langle a\rangle$ et $H \rtimes_\alpha K$.
Or par la proposition précédente, le produit semi-direct $\langle b\rangle \rtimes \langle a\rangle$ est égal à $\mathrm{D}_n$, donc $\mathrm{D}_n$ est isomorphe à $\langle b\rangle \rtimes_\alpha \langle a\rangle$. □

**Corollaire 13.19.**

$\mathrm{D}_n$ est isomorphe au produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes_\gamma \mathbb{Z}/2\mathbb{Z}$.

*Démonstration.*
$\langle b\rangle$ est un groupe cyclique d'ordre $n$, donc $\langle b\rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, de même $\langle a\rangle$ est isomorphe a $\mathbb{Z}/2\mathbb{Z}$.
D'où le produit semi-direct $\langle b\rangle \rtimes_\alpha \langle a\rangle$ est isomorphe au produit semi direct $\mathbb{Z}/n\mathbb{Z} \rtimes_\gamma \mathbb{Z}/2\mathbb{Z}$, où $\gamma$ est défini de $\mathbb{Z}/2\mathbb{Z}$ dans Aut $(\mathbb{Z}/n\mathbb{Z})$ par :

$$\begin{cases} \gamma\left(\overline{0}\right) = \mathrm{Id} \\ \gamma\left(\overline{1}\right)(\tilde{m}) = -\tilde{m} \end{cases}$$

(cf cours du produit semi-direct)
Puisque $\mathrm{D}_n$ est isomorphe au produit semi-direct $\langle b\rangle \rtimes_\alpha \langle a\rangle$, $\mathrm{D}_n$ est isomorphe au produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes_\gamma \mathbb{Z}/2\mathbb{Z}$. □

**Proposition 13.20.**

$\forall k \in [\![0, n-1]\!]$, $bab^k b^{-1} = ab^{k-2}$.

*Démonstration.*
Puisque $abab = 1$, et $a$ est d'ordre 2, on a $ba = ab^{-1}$. D'où

$$bab^k b^{-1} = ab^{-1}b^{k-1} = ab^{k-2}.$$

□

**Proposition 13.21.**

1. Si $n$ est impair, alors les sous-groupe normaux de $\mathrm{D}_n$ sont $\mathrm{D}_n$ et les sous-groupes de $\langle b\rangle$.
2. Si $n$ est pair, alors les sous-groupes normaux de $\mathrm{D}_n$ sont $\mathrm{D}_n$, les sous-groupes de $\langle b\rangle$, le sous-groupe engendré par $b^2$ et $a$, et le sous-groupe engendré par $b^2$ et $ab$.

*Démonstration.*
$\langle b\rangle$ étant cyclique, les sous-groupes de $\langle b\rangle$ sont les groupes cycliques. Soit $k \in [\![1, n-1]\!]$, alors montrons que $\left\langle b^k\right\rangle$ est un sous-groupe normal de $\mathrm{D}_n$.
$\left\langle b^k\right\rangle$ est un sous-groupe normal de $\langle b\rangle$. Soit $i \in [\![0, n-1]\!]$, par la propriété 13.12, $ab^i b^k \left(ab^i\right)^{-1} = ab^k a = b^{-k} \in \left\langle b^k\right\rangle$.
Donc $\left\langle b^k\right\rangle$ est un sous-groupe normal de $\mathrm{D}_n$, $\forall k \in [\![1, n-1]\!]$.
Soit $N$ un sous-groupe normal de $\mathrm{D}_n$ non inclus dans $\langle b\rangle$. Il existe alors, par la proposition 13.14 un entier $k \in [\![0, n-1]\!]$ tel que $ab^k \in N$, alors par la propriété précédente, $N$ contient $ab^{k-2}$ élément différent de 1. Par la proposition 13.13, $N$ contient l'élément $ab^{k-2}ab^k = b^2$, et par conséquent $N$ contient le groupe $\left\langle b^2\right\rangle$.

1. Si $n$ est impair, alors $\text{pgcd}(2,n) = 1$ et par conséquent, $\langle b^2 \rangle = \langle b \rangle$, $N$ est ainsi d'ordre au moins égal à $n+1$, Or $|N|$ divise $|\mathrm{D}_n|$, i.e $2n$, donc $|N| = 2n$ et par suite, $N = \mathrm{D}_n$.
2. Si $n$ pair : $\forall i \in [\![1, \frac{n}{2} - 1]\!]$, $ab^k b^{2i} = ab^{k+2i}$ et par la proposition 13.12, $b^{2i}ab^k = aab^{2i}ab^k = ab^{k+n-2i} = ab^{k+2\left(\frac{n}{2}-i\right)}$ donc $\left\langle \left\{ b^2, ab^k \right\} \right\rangle$ est constitué des éléments $b^{2i}$ et $ab^{k+2i}$, $\forall i \in [\![0, \frac{n}{2} - 1]\!]$. Ainsi $\left\langle \left\{ b^2, ab^k \right\} \right\rangle$ est d'ordre $n$ donc $\left\langle \left\{ b^2, ab^k \right\} \right\rangle$ est d'indice 2 dans $\mathrm{D}_n$, cf cours normaux. Comme $ab^k$ et $b^2$ appartiennent a $N$, $N$ contient $\left\langle \left\{ b^2, ab^k \right\} \right\rangle$. D'où $N$ a au moins $n$ éléments. Or $|N|$ divise $|\mathrm{D}_n| = 2n$ donc $|N| = n$, i.e $N = \left\langle \left\{ b^2, ab^k \right\} \right\rangle$ ou $|N| = 2n$. i.e $N = \mathrm{D}_n$
   Maintenant, déterminons l'ensemble des groupes de la forme $\left\langle \left\{ b^2, ab^k \right\} \right\rangle$. Comme $\left\langle \left\{ b^2, ab^k \right\} \right\rangle$ est constitué des éléments $b^{2i}$ et $ab^{k+2i}$ avec $i \in [\![0, \frac{n}{2} - 1]\!]$, on a $\left\langle \left\{ b^2, ab^k \right\} \right\rangle = \left\langle \left\{ b^2, ab^m \right\} \right\rangle$ si $m - k$ est pair.
   Il y a donc deux sous-groupes de la forme $\left\langle \left\{ b^2, ab^k \right\} \right\rangle$ : $\left\langle \left\{ b^2, ab \right\} \right\rangle$ et $\left\langle \left\{ b^2, a \right\} \right\rangle$.
   Les sous-groupes normaux de $\mathrm{D}_n$ lorsque $n$ est pair, sont $\mathrm{D}_n$, les sous-groupes de $\langle b \rangle$, le sous-groupe $\left\langle \left\{ b^2, ab \right\} \right\rangle$ et le sous-groupe $\left\langle \left\{ b^2, a \right\} \right\rangle$.

□

## 3 Centre et groupe dérivé de $\mathrm{D}_n$.

**Proposition 13.22.**

1. Si $n$ est impair, avec $\mathcal{Z}(\mathrm{D}_n) = \{\mathrm{Id}\}$
2. Si $n$ est pair, alors $\mathcal{Z}(\mathrm{D}_n) = \left\{ \mathrm{Id}, b^{\frac{n}{2}} \right\}$

*Démonstration.* Soit $k \in [\![1, n-1]\!]$, par la proposition 13.12,

$$ab^k \left(b^k a\right)^{-1} = ab^k ab^{-k} = b^{-2k}.$$

Si $n$ est impair, ou si $n$ est pair et $k \neq \frac{n}{2}$, alors $b^{-2k} \neq 1$. On a alors $ab^k \neq b^k a$, donc $b^k \notin \mathcal{Z}(\mathrm{D}_n)$

1. Si $n$ est impair, alors puisque $\mathcal{Z}(\mathrm{D}_n)$ est un sous-groupe normal de $\mathrm{D}_n$, $\mathcal{Z}(\mathrm{D}_n)$ est un sous-groupe de $\langle b \rangle$, d'après la proposition 13.21.
   Or chacun de ces sous-groupes, hormis $\{1\}$ possède une puissance non nulle de $b$ donc il ne peut être inclus dans $\mathcal{Z}(\mathrm{D}_n)$, d'après ce qui précède. D'où $\mathcal{Z}(\mathrm{D}_n) = \{\mathrm{Id}\}$.
2. Il est clair que $b^{\frac{n}{2}}$ commute avec toute puissance de $b$. De plus, $\left(b^{\frac{n}{2}}\right)^2 = b^n = 1$ donc $b^{\frac{n}{2}} = b^{-\frac{n}{2}}$

$\forall k \in [\![0, n-1]\!]$, $ab^k b^{\frac{n}{2}} = ab^{\frac{n}{2}+k}$ et d'apres la proposition 13.12, on a :

$$\begin{aligned} b^{\frac{n}{2}} ab^k &= aab^{\frac{n}{2}} ab^k \\ &= ab^{-\frac{n}{2}} b^k \\ &= ab^{\frac{n}{2}} b^k \\ &= ab^{\frac{n}{2}+k} \end{aligned}$$

D'où $b^{\frac{n}{2}} \in \mathcal{Z}(\mathrm{D}_n)$.
On a vu que, si $k \neq \frac{n}{2}$, alors $b^k \notin \mathcal{Z}(\mathrm{D}_n)$.
Comme $abab = 1$, on a $ab = b^{-1}a \neq ba$, donc $a \notin \mathcal{Z}(\mathrm{D}_n)$
De plus $aab = b$ et $aba = b^{-1} \neq b$ donc $ab \notin \mathcal{Z}(\mathrm{D}_n)$
D'où, puisque $\mathcal{Z}(\mathrm{D}_n)$ est un sous-groupe normal de $\mathrm{D}_n$, $\mathcal{Z}(\mathrm{D}_n) = \left\{1, b^{\frac{n}{2}}\right\}$ d'après la proposition 13.21.

□

**Proposition 13.23.**

1. Si $n$ est impair, alors : $\mathrm{D}(\mathrm{D}_n) = \langle b \rangle$
2. Si $n$ est pair, alors : $\mathrm{D}(\mathrm{D}_n) = \langle b^2 \rangle$

*Démonstration.*
Pour tout couple $(i, j) \in [\![0, n-1]\!] \times [\![0, n-1]\!]$, on a en utilisant la proposition 13.12 :

$$\begin{aligned} \left[b^i, b^j\right] &= b^i b^j b^{-i} b^{-j} = 1 \\ \left[ab^i, b^j\right] &= ab^i b^j b^{-i} ab^{-j} \\ &= ab^j ab^{-j} \\ &= b^{-2j} \\ \left[b^j, ab^i\right] &= \left(\left[ab^i, b^j\right]\right)^{-1} \\ &= b^{-2j} \\ \left[ab^i, ab^j\right] &= ab^i ab^j b^{-i} ab^{-j} a \\ &= b^{-i} b^j b^{-i} b^j = 1 \end{aligned}$$

D'où, puisque $\mathrm{D}(\mathrm{D}_n)$ est engendré par les commutateurs, $\mathrm{D}(\mathrm{D}_n)$ est inclus dans $\langle b^2 \rangle$.
Comme $\left[a, b^{-1}\right] = ab^{-1}ab = b^2$, $\langle b^2 \rangle$ est inclus dans $\mathrm{D}(\mathrm{D}_n)$. D'où $\mathrm{D}(\mathrm{D}_n) = \langle b^2 \rangle$
Lorsque $n$ est impair, $\mathrm{pgcd}(2, n) = 1$, donc $\langle b^2 \rangle = \langle b \rangle$. □

**Corollaire 13.24.**

Le groupe $\mathrm{D}_n$ est résoluble,

*Démonstration.*
$\left\langle b^2 \right\rangle$ et $\langle b \rangle$ étant cycliques, donc abéliens, on a $\mathrm{D}\left(\langle b \rangle\right) = \mathrm{D}\left(\left\langle b^2 \right\rangle\right) = \{1\}$
D'où :

$$\mathrm{D}^2\left(\mathrm{D}_n\right) = \mathrm{D}\left(\mathrm{D}\left(\mathrm{D}_n\right)\right) = \{1\}$$

et $\mathrm{D}_n$ est donc résoluble. □

F I N