Université Bordeaux 1
Licence de Sciences, Technologies, Santé
Mentions Mathématiques et Informatique
N1MA4M11 Algèbre 3

# Algèbre 3

**Christine Bachoc**

# Table des matières


**1 Applications et relations d'équivalence** **7**
1.1 Rappels sur les applications . . . . . 7
1.2 Relations d'équivalence . . . . . 8

**2 Groupes, sous-groupes** **11**
2.1 Définition et exemples . . . . . 11
2.2 Sous-groupes . . . . . 13
2.3 Sous-groupe engendré par une partie . . . . . 14
2.4 Produit direct de groupes . . . . . 15

**3 Morphismes de groupes** **17**
3.1 Définitions . . . . . 17
3.2 Noyau, Image . . . . . 18
3.3 Le groupe des automorphismes . . . . . 18

**4 Ordres** **21**
4.1 Ordre d'un élément, ordre d'un groupe . . . . . 21
4.2 Groupes cycliques . . . . . 22
4.3 Classes modulo un sous-groupe, théorème de Lagrange . . . . . 22

**5 Sous-groupes distingués, quotients** **25**
5.1 Introduction . . . . . 25
5.2 Sous-groupes distingués et groupes quotients . . . . . 26
5.3 Sous-groupes distingués et morphismes . . . . . 26

**6 Groupes cycliques, groupes diédraux** **29**
6.1 Groupes cycliques . . . . . 29
6.2 La fonction d'Euler et le théorème chinois . . . . . 30
6.3 Groupes diédraux . . . . . 32

**7 Groupes opérant sur un ensemble** **33**
7.1 Introduction . . . . . 33
7.2 Actions de groupes . . . . . 33
7.3 Orbites et stabilisateurs . . . . . 34
7.4 Exemples d'actions de groupe . . . . . 35

**8 Le groupe symétrique $S_n$** **37**
8.1 Notations . . . 37
8.2 La décomposition canonique d'une permutation en produit de cycles . . . 38
8.3 Autres décompositions des permutations . . . 39
8.4 La signature . . . 40

**9 Anneaux** **43**
9.1 Définitions . . . 43
9.2 Exemples d'anneaux . . . 44
9.3 Sous-anneaux, produits directs et morphismes . . . 45

**10 Idéaux, anneaux quotients** **47**
10.1 Idéaux . . . 47
10.2 Idéaux principaux, anneaux principaux . . . 48
10.3 Quotient d'un anneau par un idéal . . . 49
10.4 Caractéristique d'un anneau . . . 50
10.5 Idéaux premiers et maximaux . . . 50
10.6 Anneaux non commutatifs . . . 51

**11 Introduction aux corps finis** **53**
11.1 Polynômes à une indéterminée . . . 53
11.2 Le quotient $K[X]/(P(X))$ . . . 54
11.3 Introduction aux corps finis . . . 55

# Introduction

# Chapitre 1

# Applications et relations d'équivalence

## 1.1 Rappels sur les applications

**Définition 1.1.1.** 1. Soit $A$ et $B$ des ensembles. Une *application* $f : A \to B$ associe à tout élément $x$ de $A$ un unique élément $f(x)$ de $B$.

2. Si $x \in A$ et $y \in B$ sont tels que $f(x) = y$, on dit que $y$ est *l'image* de $x$ par $f$ et que $x$ est un *antécédent* de $y$.
3. Si $A' \subset A$, *l'image directe* de $A'$ par $f$ est l'ensemble noté $f(A')$ des images des éléments de $A'$ par $f$.
$$f(A') = \{f(x) : x \in A'\} \subset B.$$
4. Si $B' \subset B$, *l'image réciproque* de $B'$ par $f$, est l'ensemble des antécédents des éléments de $B'$, et est notée $f^{-1}(B')$.
$$f^{-1}(B') = \{x \in A : f(x) \in B'\} \subset A.$$

Attention : $f^{-1}(B')$ est un ensemble et non pas un unique élément, même si $B' = \{y\}$. Ne pas confondre avec la notion de bijection inverse rappelée plus loin.

**Exemple 1.1.2.** Quelques exemples classiques :
- L'application identité $\mathrm{Id}_A : A \to A$ est définie par $\mathrm{Id}_A(x) = x$.
- Si $A$ est un *produit direct* $A = B \times C = \{(x, y) : x \in B, y \in C\}$, les projections $p_B : A \to B$ et $p_C : A \to C$ sont définies par $p_B((x, y)) = x$ et $p_C((x, y)) = y$.

**Exemple 1.1.3.** Prenons $f : \mathbb{Z} \to \mathbb{Z}$ définie par $f(x) = x^2$. On a $f(2) = 4$ et $f^{-1}(\{4\}) = \{2, -2\}$. Ainsi, 4 a deux antécédents. Par contre, $-1$ ou 3 n'ont pas d'antécédent. On a $f(\mathbb{Z}) = \mathbb{N}$.

**Définition 1.1.4.** Soit $f : A \to B$ une application.
1. On dit que $f$ est *injective* si tout élément $y$ de $B$ a au plus un antécédent.
2. On dit que $f$ est *surjective* si tout élément $y$ de $B$ possède au moins un antécédent.
3. On dit que $f$ est *bijective* si elle est à la fois injective et surjective. De façon équivalente, $f$ est bijective si et seulement si pour tout $y \in B$, il existe un unique élément de $A$ tel que $f(x) = y$.

**Théorème 1.1.5.** Supposons que $A$ et $B$ sont des ensembles finis. Les propriétés suivantes sont équivalentes :

1. $f : A \to B$ est une bijection
2. $f$ est injective et $|A| = |B|$
3. $f$ est surjective et $|A| = |B|$.

**Proposition 1.1.6.** (et définition)

1. Si $f : A \to B$ et $g : B \to C$, la *composée* $g \circ f$ est l'application $g \circ f : A \to C$ définie par $(g \circ f)(x) = g(f(x))$.
2. Si $f : A \to B$ est une bijection, on peut définir *l'application inverse* ou *réciproque* de $f$, que l'on note $f^{-1}$. C'est l'application de $B$ dans $A$ qui à tout $y$ dans $B$ associe son unique antécédent par $f$. On a alors $f \circ f^{-1} = \mathrm{Id}_B$ et $f^{-1} \circ f = \mathrm{Id}_A$.
3. Réciproquement, si $f : A \to B$ est telle qu'il existe une application $g : B \to A$ telle que $f \circ g = \mathrm{Id}_B$ et $g \circ f = \mathrm{Id}_A$, alors $f$ est une bijection et $g = f^{-1}$.
4. Une bijection de $A$ dans $A$ est appelée une *permutation* de $A$. L'ensemble des permutations de $A$ est noté $S(A)$. Si $f$ et $g$ appartiennent à $S(A)$, alors $f \circ g$ appartient aussi à $S(A)$, et $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

## 1.2 Relations d'équivalence

**Définition 1.2.1.** Soit $E$ un ensemble. Une *relation d'équivalence* $\mathcal{R}$ sur $E$ est une relation entre les éléments de $E$ qui vérifie les propriétés suivantes, pour tout $x \in E$, $y \in E$ :

1. $\mathcal{R}$ est réflexive : $x\mathcal{R}x$
2. $\mathcal{R}$ est symétrique : Si $x\mathcal{R}y$ alors $y\mathcal{R}x$
3. $\mathcal{R}$ est transitive : Si $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $x\mathcal{R}z$

**Exemple 1.2.2.** Soit $n$ un entier. On définit une relation sur $\mathbb{Z}$ par :

$$x\mathcal{R}y \text{ si } x - y \text{ est un multiple de } n.$$

On note traditionnellement $x \equiv y \bmod n$ (ou $x = y \bmod n$, ou $x = y(n)$) et on dit que $x$ *est congru à* $y$ *modulo* $n$. Remarquons que $x \equiv y \bmod n$ si et seulement si $x$ et $y$ ont le même reste dans la division euclidienne par $n$. On vérifie facilement que c'est une relation d'équivalence.

**Définition 1.2.3.** Soit $E$ un ensemble et soit $\mathcal{R}$ une relation d'équivalence sur $E$. Soit $x \in E$. La *classe d'équivalence* de $x$, notée $\mathrm{cl}(x)$, est l'ensemble des éléments de $E$ qui sont en relation avec $x$.

**Exemple 1.2.4.** La relation de congruence, avec $n = 2$. $\mathrm{cl}(0) = \{\dots, -2, 0, 2, 4, \dots\}$ est l'ensemble des entiers pairs. $\mathrm{cl}(1)$ est l'ensemble des entiers impairs. On a $\mathrm{cl}(0) = \mathrm{cl}(2) = \mathrm{cl}(4)$.

Pour un entier $n$ quelconque, et $a \in \mathbb{Z}$,

$$\mathrm{cl}(a) = \{\dots, a - n, a, a + n, a + 2n \dots\} = \{a + qn : q \in \mathbb{Z}\}.$$

**Proposition 1.2.5.** Soit $E$ un ensemble et soit $\mathcal{R}$ une relation d'équivalence sur $E$.

1. Soit $x$ et $y$ appartenant à $E$. Les classes d'équivalence de $x$ et $y$ sont soit égales soit disjointes. On a
$$\mathrm{cl}(x) = \mathrm{cl}(y) \Leftrightarrow x\mathcal{R}y \Leftrightarrow x \in \mathrm{cl}(y) \Leftrightarrow y \in \mathrm{cl}(x).$$
2. L'ensemble des classes d'équivalence de $E$ pour la relation $\mathcal{R}$ forme une partition de $E$. Cet ensemble est noté $E/\mathcal{R}$ et est appelé *ensemble quotient* de $E$ par $\mathcal{R}$.
3. On appelle *système de représentants* de $E$ pour la relation $\mathcal{R}$ un sous ensemble $\{x_i\}_{i\in I}$ d'éléments de $E$ tels que $\mathrm{cl}(x_i) \neq \mathrm{cl}(x_j)$ pour $i \neq j$ et $E = \cup_{i\in I} \mathrm{cl}(x_i)$.
4. L'application
$$\begin{aligned} s : E &\to E/\mathcal{R} \\ x &\mapsto \mathrm{cl}(x) \end{aligned}$$
est une surjection appelée "surjection canonique associée à la relation $\mathcal{R}$".

*Preuve.* 1. Montrons d'abord que $\mathrm{cl}(x) = \mathrm{cl}(y)$ si et seulement si $x\mathcal{R}y$. Si $\mathrm{cl}(x) = \mathrm{cl}(y)$ alors $x \in \mathrm{cl}(y)$ et donc $x\mathcal{R}y$. Dans l'autre sens, supposons $x\mathcal{R}y$. Montrons que $\mathrm{cl}(x) \subset \mathrm{cl}(y)$ : si $x' \in \mathrm{cl}(x)$, $x'\mathcal{R}x$ mais comme $x\mathcal{R}y$, on a $x'\mathcal{R}y$ par transitivité et donc $x' \in \mathrm{cl}(y)$. L'inclusion $\mathrm{cl}(y) \subset \mathrm{cl}(x)$ se montre de la même façon (ou se déduit de la propriété de symétrie de $\mathcal{R}$).

Supposons que $\mathrm{cl}(x)$ et $\mathrm{cl}(y)$ ne soient pas disjointes. Alors il existe $z \in \mathrm{cl}(x) \cap \mathrm{cl}(y)$. On a alors $z\mathcal{R}x$ et $z\mathcal{R}y$. D'après la propriété de transitivité, $x\mathcal{R}y$ et on a vu qu'alors $\mathrm{cl}(x) = \mathrm{cl}(y)$.

2. Tout élément de $E$ est dans sa propre classe d'équivalence, et on a vu que les classes d'équivalence sont égales ou disjointes donc elles forment bien une partition de $E$.

□

Attention : L'ensemble quotient $E/\mathcal{R}$ est un *ensemble d'ensembles*. Un élément de $E/\mathcal{R}$ est donc lui-même un ensemble.

**Exemple 1.2.6.** Toujours la relation de congruence modulo $n$. L'ensemble des classes d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$.
$$\mathbb{Z}/n\mathbb{Z} = \{\mathrm{cl}(0), \mathrm{cl}(1), \ldots, \mathrm{cl}(n-1)\}.$$
Il est en bijection avec l'ensemble des restes possibles dans la division par $n$, il est donc de cardinal $n$. L'ensemble $\{0, 1, \ldots, (n-1)\}$ est un système de représentants. Ce n'est pas le seul. Par exemple, pour $\mathbb{Z}/3\mathbb{Z}$, on peut prendre pour système de représentants $\{-1, 0, 1\}$.

**Notation.** On écrit plutôt $\mathrm{cl}(a) = a \bmod n$ et
$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, (n-1) \bmod n\}.$$

**Corollaire 1.2.7.** (L'équation aux classes) Si $E$ est un ensemble fini muni d'une relation d'équivalence $\mathcal{R}$,
$$|E| = \sum_{C\in E/\mathcal{R}} |C|.$$

*Preuve.* C'est une conséquence immédiate du fait que $E/\mathcal{R}$ forme une partition de $E$ (point 2. de la Proposition 1.2.5) □

**Théorème 1.2.8.** (Théorème de factorisation des applications) Soit $E$ un ensemble muni d'une relation d'équivalence $\mathcal{R}$ et soit $f : E \to F$ une application. Si, pour tout $x, y \in E$, l'implication suivante est vraie :

$$x\mathcal{R}y \Longrightarrow f(x) = f(y)$$

alors il existe une application $\tilde{f} : E/\mathcal{R} \to F$ unique telle que, pour tout $x \in E$, $\tilde{f}(\mathrm{cl}(x)) = f(x)$. On a le *diagramme commutatif* suivant, où $s$ est la surjection canonique :

$$\begin{tikzcd} E \arrow[r, "f"] \arrow[d, "s"'] & F \\ E/\mathcal{R} \arrow[ur, "\tilde{f}"'] & \end{tikzcd}$$

avec $\tilde{f} \circ s = f$. On dit alors que $\tilde{f}$ *factorise* $f$ *pour la relation* $\mathcal{R}$. De plus on a $\tilde{f}(E/\mathcal{R}) = f(E)$.

*Preuve.* Pour définir $\tilde{f} : E/\mathcal{R} \to F$, il faut définir un unique $\tilde{f}(C)$ pour tout $C \in E/\mathcal{R}$. Mais $C$ est un sous-ensemble de $E$. En fait, pour tout $x \in C$, $\mathrm{cl}(x) = C$ donc on voudrait que $\tilde{f}(C) = f(x)$ pour tout $x \in C$. Pour que cela définisse une application, il suffit que $f(x)$ ne dépende pas du choix de $x$ dans $C$. Autrement dit, il faut que $f(x) = f(y)$ lorsque $x$ et $y$ appartiennent tous les deux à $C$. C'est exactement l'hypothèse : $x$ et $y$ appartiennent à une même classe $C$ si et seulement si $x\mathcal{R}y$, et, dans ce cas, $f(x) = f(y)$.

Il est clair que $\tilde{f}$ est alors unique et que $\tilde{f}(E/\mathcal{R}) = f(E)$. $\square$

**Exemple 1.2.9.** On veut définir une application "naturelle" de $\mathbb{Z}/6\mathbb{Z}$ dans $\mathbb{Z}/3\mathbb{Z}$ en appliquant le théorème de factorisation. On note les surjections canoniques respectives $s_6$ et $s_3$. On a le diagramme :

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "f = s_3"] \arrow[d, "s_6"'] & \mathbb{Z}/3\mathbb{Z} \\ \mathbb{Z}/6\mathbb{Z} \arrow[ur, dashed, "\tilde{f}"'] & \end{tikzcd}$$

dans lequel on veut construire $\tilde{f}$. D'après le théorème de factorisation, l'existence de $\tilde{f}$ est assurée si on a l'implication :

$$x \equiv y \bmod 6 \Longrightarrow x \equiv y \bmod 3$$

ce qui se traduit par : si 6 divise $x - y$ alors 3 divise $x - y$. Comme 3 divise 6 c'est bien vrai !

On peut expliciter $\tilde{f}$ :

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 mod 6 |
|---|---|---|---|---|---|---|
| $\tilde{f}(x)$ | 0 | 1 | 2 | 0 | 1 | 2 mod 3 |

**Exercice.** généraliser l'exemple précédent à la construction d'une application de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ lorsque $n$ divise $m$.

# Chapitre 2

# Groupes, sous-groupes

## 2.1 Définition et exemples

**Définition 2.1.1.** Un groupe est un ensemble $G$ muni d'une loi de composition interne $*$, c'est-à-dire d'une application :

$$\begin{aligned} G \times G &\to G \\ (x, y) &\mapsto x * y \end{aligned}$$

vérifiant les propriétés suivantes :

1. La loi $*$ est *associative* : $x * (y * z) = (x * y) * z$ pour tout $x, y, z$ dans $G$.
2. $(G, *)$ possède un *élément neutre*, c'est-à-dire un élément $e \in G$ tel que $e * x = x * e = x$ pour tout $x$ dans $G$.
3. Tout élément de $G$ est *inversible* : pour tout $x \in G$, il existe $y \in G$ tel que $x*y = y*x = e$.

Si de plus, $x * y = y * x$ pour tout $x, y$ appartenant à $G$, on dit que $(G, *)$ est un groupe commutatif (ou abélien).

**Proposition 2.1.2.** Dans un groupe $(G, *)$, on a les propriétés suivantes :

1. L'élément neutre est unique.
2. L'inverse d'un élément est unique. On note $x^{-1}$ l'(unique) inverse de $x \in G$.
3. On a : $e^{-1} = e$, $(x^{-1})^{-1} = x$, $(x * y)^{-1} = y^{-1} * x^{-1}$.

*Démonstration.* Si $G$ possède deux neutres $e$ et $e'$ alors $e * e' = e$ mais aussi $e * e' = e'$ donc $e = e'$.

Supposons que $x$ ait deux inverses $y$ et $y'$. Alors $x*y = e$ et $x*y' = e$ par définition. On en déduit que $x*y = x*y'$. On multiplie cette identité à gauche par $y$ et on utilise l'associativité : $y * (x * y) = y * (x * y')$ donc $(y * x) * y = (y * x) * y'$. Mais $y * x = e$ donc $e * y = e * y'$ donc $y = y'$.

Pour démontrer ces assertions, on utilise crucialement la propriété d'unicité de l'inverse : puisque $e$ est neutre, en particulier, $e * e = e$. Mais $e$ a un unique inverse donc cet inverse est bien $e$. De même, la propriété $x * x^{-1} = x^{-1} * x = e$ montre que $x$ est l'inverse de $x^{-1}$. On vérifie, par associativité de la loi, que $(x * y) * (y^{-1} * x^{-1}) = (y^{-1} * x^{-1}) * (x * x) = e$ et on en conclut que l'inverse de $x * y$ est $y^{-1} * x^{-1}$. □

**Exemple 2.1.3.** Quelques exemples standards :

- $(\mathbb{Z}, +)$ pour lequel $e = 0$, l'inverse de $x$ est $-x$. Il est commutatif.
- $(\mathbb{Q}^*, \times)$ pour lequel $e = 1$, l'inverse de $x$ est $1/x$. Il est commutatif.
- $(S(A), \circ)$ où $A$ est un ensemble quelconque. Le neutre est $e = \mathrm{Id}_A$, l'inverse de $f$ est l'application inverse $f^{-1}$.
- L'ensemble $GL(n, \mathbb{R})$ des matrices carrées de taille $n$ à coefficients dans $\mathbb{R}$ de déterminant non nul, muni du produit des matrices. Le neutre est la matrice identité, l'inverse est la matrice inverse.

**Exemple 2.1.4. Le groupe symétrique $S_n$.** C'est un exemple très important sur lequel on reviendra en détails. Le groupe symétrique d'ordre $n$, noté $S_n$, est le groupe $S(\{1, 2, \dots, n\})$. L'opération est la composition, mais on la note plus simplement $\sigma_1\sigma_2 = \sigma_1 \circ \sigma_2$. Une permutation est notée de la façon suivante :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}.$$

Un *cycle* est une permutation particulière qui permute circulairement un sous-ensemble de $\{1, \dots, n\}$ et laisse les autres éléments inchangés. On note $\sigma = (a_1, \dots, a_p)$ si $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3, \dots, \sigma(a_p) = a_1$. On dit que $p$ est *la longueur* du cycle. Exemple : un cycle de longueur 3 dans $S_5$.

$$\sigma = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,1\,2\,4\,5 \end{pmatrix} = (1, 3, 2).$$

Un cycle de longueur 2 s'appelle *une transposition*.

**Exercice.** Montrez que $S_n$ n'est pas commutatif si $n \geq 3$. Montrez que $|S_n| = n!$.

La *table de Cayley* d'un groupe $(G, *)$ fini est la table d'opération de $(G, *)$. Par exemple, la table de Cayley de $G = (\{1, -1\}, \times)$ est :

| $\times$ | $1$ | $-1$ |
|---|---|---|
| $1$ | $1$ | $-1$ |
| $-1$ | $-1$ | $1$ |

**Exercice.** Construire la table de Cayley de $S_2$ et de $S_3$.

**Exemple 2.1.5. Le groupe $(\mathbb{Z}/nZ, +)$.** C'est aussi un exemple très important sur lequel on reviendra souvent. On définit une opération d'addition dans $\mathbb{Z}/n\mathbb{Z}$ en posant :

$$(a \bmod n) + (b \bmod n) = (a + b) \bmod n.$$

Pour avoir un sens, il faut montrer que cette définition ne dépend pas du choix d'un représentant d'une classe de congruence modulo $n$. Autrement dit, si $a = a' \bmod n$ et $b = b' \bmod n$, il faut montrer que $(a+b) = (a'+b') \bmod n$. Pour cela, on traduit les congruences par des égalités dans $\mathbb{Z}$ : il existe $u$ tel que $a = a'+un$ et il existe $v$ tel que $b = b'+vn$. Alors $(a+b) = (a'+b')+(u+v)n$ ce qui conduit à : $(a + b) = (a' + b') \bmod n$.

On vérifie aisément que le neutre pour cette opération est $0 \bmod n$ et que tout élément $x \bmod n$ est inversible, d'inverse $-x \bmod n$.

**Exercice.** Construire la table de Cayley de $(\mathbb{Z}/n\mathbb{Z}, +)$ pour $n = 2, 3, 4, \dots$.

**Exemple 2.1.6. Le groupe multiplicatif** $(\mathbb{Z}/n\mathbb{Z})^*$**.** De la même façon que pour l'addition, on peut définir une multiplication dans $\mathbb{Z}/n\mathbb{Z}$ en posant :

$$(a \bmod n)(b \bmod n) = (ab) \bmod n.$$

Cette loi est associative, commutative, et possède un élément neutre qui est $1 \bmod n$. Par contre, tout élément n'est pas inversible, en particulier $0 \bmod n$ n'est *jamais* inversible. Par exemple, on vérifie facilement que les inversibles modulo 4 sont 1 et 3. On note $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ qui sont inversibles pour la multiplication. On a donc :

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a \bmod n : \text{ il existe } b \in \mathbb{Z} \text{ tel que } ab = 1 \bmod n\}.$$

Alors $(\mathbb{Z}/n\mathbb{Z})^*$ muni de la multiplication est un groupe commutatif. Par exemple :

$$(\mathbb{Z}/4\mathbb{Z})^* = \{1, 3\} \quad (\mathbb{Z}/5\mathbb{Z})^* = \{1, 2, 3, 4\} \quad (\mathbb{Z}/6\mathbb{Z})^* = \{1, 5\}$$

**Exercice.** Démontrez en détail que la multiplication définie ci-dessus a bien un sens, et que $(\mathbb{Z}/n\mathbb{Z})^*$ muni de cette multiplication est un groupe commutatif.

**Notation.** Pour alléger les notations, on va souvent utiliser la *notation multiplicative* pour un groupe général : $x * y = xy$, et $e = 1$. On dit que $xy$ est le *produit* de $x$ et $y$. On utilise aussi les raccourcis $x^n = x * \cdots * x$ ($n$ termes), $x^0 = e$, pour $n \in \mathbb{N}$ et $x^{-n} = x^{-1} * \cdots * x^{-1}$.

Lorsque le groupe est commutatif, en particulier lorsque la loi est issue de l'addition usuelle, on emploie la *notation additive* $x * y = x + y$ et $e = 0$. Alors on parle d'opposé plutôt que d'inverse d'un élément, et on note $nx = x + \cdots + x$.

## 2.2 Sous-groupes

**Définition 2.2.1.** Soit $(G, *)$ un groupe. Un sous-groupe de $G$ est un sous-ensemble $H \subset G$ tel que $(H, *)$ soit un groupe.

Examinons les propriétés que doit vérifier $H \subset G$ pour être un groupe pour $*$. Tout d'abord il est nécessaire que la loi $*$ soit interne dans $H$, c'est-à-dire que $x * y \in H$ pour tout $x \in H$, $y \in H$. Remarquons que la loi $*$ étant associative dans $G$, elle l'est forcément dans $H$. Il y a une petite subtilité avec le neutre : en fait, le neutre de $H$ ne peut être que le neutre de $G$. En effet, si $e'$ est le neutre de $H$, on a comme $e' \in G$, $e' * e = e'$. Mais aussi $e' * e' = e'$ en raisonnant dans $H$. Donc $e' * e = e' * e'$. Comme $e' \in G$, il a un inverse $e'^{-1}$ dans $G$. On multiplie la précédente égalité à gauche par celui-ci, pour obtenir : $(e'^{-1} * e') * e = (e'^{-1} * e') * e'$ soit $e * e = e * e'$ soit $e = e'$.

Donc si $(H, *)$ est un groupe, son neutre est $e$ le neutre de $G$. Pour ce qui est de l'inverse, un élément de $H$ a bien toujours un inverse (unique) dans $G$. Il faut donc que cet inverse appartienne à $H$.

En résumé, si $H$ est un sous-groupe de $G$, alors :

$$\begin{array}{rl} (i) & \text{Pour tout } x \in H, y \in H, x * y \in H. \\ (ii) & e \in H \\ (iii) & \text{Pour tout } x \in H, x^{-1} \in H. \end{array}$$

Réciproquement, si les propriétés (i), (ii), (iii), sont vérifiées, alors $(H, *)$ est bien un groupe. En effet, l'associativité et la propriété $e * x = x$ sont automatiquement vraies dans $H$ puisqu'elles sont vraies dans $G$.

La proposition suivante énonce la propriété minimale suffisante à vérifier pour qu'un sous-ensemble de $G$ soit un sous-groupe de $G$ :

**Proposition 2.2.2.** Soit $(G, *)$ un groupe et soit $H \subset G$. Alors $H$ est un sous-groupe de $G$ si et seulement si, $H$ est non vide, et vérifie :

$$\text{Pour tout } x \in H, y \in H, x * y^{-1} \in H. \tag{2.1}$$

*Démonstration.* Supposons que $H$ soit un sous-groupe de $G$. Alors on a vu que $H$ vérifie (i), (ii), (iii). En particulier (ii) indique que le neutre $e$ de $G$ appartient à $H$ donc $H$ est non vide. Si $x$ et $y$ sont dans $H$, d'après (iii), $y^{-1} \in H$ et, d'après (i), $x * y^{-1} \in H$.

Réciproquement, supposons que $H$ est non vide et vérifie (2.1). Il contient donc un élément $x$. Donc, par (2.1), $x * x^{-1} = e \in H$. En appliquant encore (2.1), on obtient $e * x^{-1} = x^{-1} \in H$. Si $x$ et $y$ sont dans $H$, on a vu que $y^{-1} \in H$, donc encore avec (2.1), $x * y = x * (y^{-1})^{-1} \in H$. Donc (i), (ii), (iii) sont vérifiées donc $H$ est bien un sous-groupe de $G$. □

**Exemple 2.2.3.**
- $\{e\}$ et $G$ sont des sous-groupes de $G$.
- $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. En effet, il est non vide puisque $0 \in n\mathbb{Z}$ et si $x = nk \in n\mathbb{Z}$, $y = n\ell \in \mathbb{Z}$, $x - y = n(k - \ell) \in n\mathbb{Z}$.
- Dans $S_n$, $H = \{\sigma \in S_n : \sigma(1) = 1\}$ est un sous-groupe de $S_n$.

**Proposition 2.2.4.** Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$.

*Démonstration.* On vient de voir que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Réciproquement, soit $H$ un sous-groupe de $\mathbb{Z}$. Soit $n$ son plus petit élément strictement positif. Soit $x \in \mathbb{Z}$, par division euclidienne il existe $q$ et $r \in \{0, 1, \ldots, n-1\}$ tels que $x = qn + r$. Alors $qn$, et donc $r = x - qn$ appartient à $H$. Comme $r \in \{0, 1, \ldots, n-1\} \cap H$ et que $n$ est le plus petit élément strictement positif de $H$, il n'y a qu'une possibilité c'est $r = 0$. Donc $x \in n\mathbb{Z}$ et $H = n\mathbb{Z}$. □

**Proposition 2.2.5.** Soit $H_1$ et $H_2$ deux sous-groupes de $(G, *)$. L'intersection $H_1 \cap H_2$ de $H_1$ et $H_2$ est un sous-groupe de $G$.

**Remarque 2.2.6.** Attention, la réunion de deux sous-groupes n'est pas un sous-groupe. Par exemple $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de $(\mathbb{Z}, +)$ car $2 + 3 = 5$ n'est pas dans cet ensemble.

## 2.3 Sous-groupe engendré par une partie

**Définition 2.3.1.** Soit $S \subset G$. On appelle *sous-groupe engendré par* $S$ et on note $\langle S \rangle$ l'intersection de tous les sous-groupes de $G$ contenant $S$. C'est un sous-groupe de $G$, et c'est le plus petit contenant $S$ (au sens où, si $H$ est un sous-groupe de $G$ contenant $S$, alors $\langle S \rangle \subset H$).

Si $S = \{x\}$ avec $x \in G$, on note $\langle x \rangle = \langle \{x\} \rangle$.

**Exemple 2.3.2.**
1. Si $S = \{e\}$, $\langle e \rangle = \{e\}$
2. Si $S = \{2, 3\} \subset \mathbb{Z}$, $\langle S \rangle = \mathbb{Z}$. En effet, $1 = 3 - 2 \in \langle S \rangle$.

**Proposition 2.3.3.** Soit $G$ un groupe noté multiplicativement.
1. $\langle x \rangle = \{x^k : k \in \mathbb{Z}\}$.
2. Si $x$ et $y$ commutent, i.e. $xy = yx$, alors $\langle x, y \rangle = \{x^k y^\ell : k, \ell \in \mathbb{Z}\}$.
3. Si $H_1$ et $H_2$ sont des sous-groupes de $G$, et que $h_1 h_2 = h_2 h_1$ pour tout $h_1 \in H_1$, $h_2 \in H_2$, alors $\langle H_1 \cup H_2 \rangle = \{h_1 h_2 : h_1 \in H_1, h_2 \in H_2\}$.

## 2.4 Produit direct de groupes

**Proposition 2.4.1.** Soit $(G, *)$ et $(G', \circ)$ deux groupes. Le *produit direct* $G \times G'$ de ces deux groupes est l'ensemble

$$G \times G' = \{(x, y) : x \in G, y \in G'\}.$$

Muni de l'opération : $(x, y) \cdot (x', y') = (x * x', y \circ y')$, c'est un groupe dont le neutre est $(e_G, e_{G'})$ et l'inverse de $(x, y)$ est $(x^{-1}, y^{-1})$.

*Démonstration.* C'est facile. □

**Remarque 2.4.2.** Bien souvent, on note de la même façon les lois de $G$, $G'$ et $G \times G'$. Attention de ne pas les confondre ! Par exemple, dans $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $(2, 2) + (2, 2) = (0, 4)$.

# Chapitre 3

# Morphismes de groupes

## 3.1 Définitions

**Définition 3.1.1.** Un *morphisme (ou homomorphisme)* d'un groupe $(G, *)$ dans un groupe $(H, \circ)$ est une application $f : G \to H$ qui est compatible avec les lois des groupes, c'est-à-dire qui vérifie :

$$\text{pour tout } x \in G, y \in G, f(x * y) = f(x) \circ f(y).$$

Si, en outre, $f$ est une bijection, on dit que $f$ est un *isomorphisme*. Un isomorphisme d'un groupe $G$ sur lui-même est appelé un *automorphisme*.

**Exemple 3.1.2.** Soit $G$ un groupe noté multiplicativement et soit $x \in G$. L'application $f : \mathbb{Z} \to G$ définie par : $f(k) = x^k$ est un morphisme de groupes. En effet, $f(k + k') = x^{k+k'} = x^k x^{k'} = f(k)f(k')$.

**Proposition 3.1.3.** Avec les notations précédentes, si $f$ est un morphisme de $G$ sur $H$, alors $f(e_G) = e_H$, et, pour tout $x \in G$, $f(x^{-1}) = f(x)^{-1}$.

*Démonstration.* On a : $f(e_G) = f(e_G * e_G) = f(e_G) \circ f(e_G)$. En multipliant par $f(e_G)^{-1}$, on obtient $e_H = f(e_G)$.

On a d'une part $f(x * x^{-1}) = f(e_G) = e_H$ et d'autre part $f(x * x^{-1}) = f(x) \circ f(x^{-1})$ donc $f(x) \circ f(x^{-1}) = e_H$ ce qui montre bien que $f(x^{-1}) = f(x)^{-1}$. □

**Proposition 3.1.4.** Si $f : G \to H$ et $g : H \to K$ sont des morphismes de groupes, alors $g \circ f : G \to K$ est aussi un morphisme de groupes.

*Démonstration.* On note $*$ la loi de $G$, $\cdot$ la loi de $H$, $\star$ la loi de $K$. Alors,

$$(g \circ f)(x * y) = g(f(x * y)) = g(f(x) \cdot f(y)) = g(f(x)) \star g(f(y)) = (g \circ f)(x) \star (g \circ f)(y)$$

donc $g \circ f$ est bien un homomorphisme de $(G, *)$ dans $K, \star)$. □

**Proposition 3.1.5.** Si $f : G \to H$ est un morphisme de groupe bijectif, alors son application réciproque $f^{-1} : H \to G$ est aussi un morphisme de groupe.

*Démonstration.* On note $*$ la loi de $G$, $\cdot$ la loi de $H$. Soit $x, y \in H$, on veut montrer que $f^{-1}(x \cdot y) = f^{-1}(x) * f^{-1}(y)$. Comme $f$ est bijective, il existe $x'$ et $y'$ dans $G$ tels que $x = f(x')$ et $y = f(y')$. Comme $f$ est un morphisme de groupe, on a

$$f(x' * y') = f(x') \cdot f(y')$$

soit

$$x' * y' = f^{-1}(f(x') \cdot f(y'))$$

ou encore

$$f^{-1}(x) * f^{-1}(y) = f^{-1}(x \cdot y).$$

□

## 3.2 Noyau, Image

On associe à un morphisme de groupes deux sous-groupes, appelés noyau et image de $f$ :

**Définition 3.2.1.** Si $f : G \to H$ est un homomorphisme, on note $\mathrm{Ker}(f)$ et on appelle *noyau de* $f$ :

$$\mathrm{Ker}(f) = f^{-1}(\{e_H\}) = \{x \in G : f(x) = e_H\} \subset G.$$

On note $\mathrm{Im}(f)$ et on appelle *image de* $f$ :

$$\mathrm{Im}(f) = f(G) = \{f(x) : x \in G\} \subset H.$$

**Proposition 3.2.2.** Le noyau de $f$ est un sous-groupe de $G$ et l'image de $f$ est un sous-groupe de $H$.

*Démonstration.* Montrons que $\mathrm{Ker}(f)$ est un sous-groupe de $G$. D'abord, $e_G \in \mathrm{Ker}(f)$ puisqu'on a démontré que $f(e_G) = e_H$, donc $\mathrm{Ker}(f)$ est non vide. Si $x \in \mathrm{Ker}(f)$ et $y \in \mathrm{Ker}(f)$, on doit montrer que $x * y^{-1} \in \mathrm{Ker}(f)$. On calcule $f(x * y^{-1})$ :

$$f(x * y^{-1}) = f(x) \circ f(y^{-1}) = f(x) \circ f(y)^{-1} = e_H * e_H^{-1} = e_H$$

donc $x * y^{-1} \in \mathrm{Ker}(f)$.

Montrons que $\mathrm{Im}(f)$ est un sous-groupe de $H$. Comme $e_H = f(e_G)$, $e_H \in \mathrm{Im}(f)$ et $\mathrm{Im}(f)$ est non vide. Soit $u = f(x)$ et $v = f(y)$ appartenant à $\mathrm{Im}(f)$. Alors $u \circ v^{-1} = f(x) \circ f(y)^{-1} = f(x * y^{-1}) \in \mathrm{Im}(f)$. Donc $\mathrm{Im}(f)$ est bien un sous-groupe de $H$. □

**Théorème 3.2.3.** Soit $f : G \to H$ un morphisme de groupes. Pour que $f$ soit injective, il suffit que $\mathrm{Ker}(f) = \{e_G\}$.

*Démonstration.* Supposons que $\mathrm{Ker}(f) = \{e_G\}$ et montrons que $f$ est injective. Supposons que $f(x) = f(y)$. Alors, $f(x) \circ f(y)^{-1} = e_H$ soit $f(x * y^{-1}) = e_H$. Donc $x * y^{-1} \in \mathrm{Ker}(f) = \{e_G\}$ donc $x * y^{-1} = e_G$ donc $x = y$.

On a montré que, si $f(x) = f(y)$, alors $x = y$, donc $f$ est bien injective. □

## 3.3 Le groupe des automorphismes

**Théorème 3.3.1.** Soit $G$ un groupe noté multiplicativement et soit $y \in G$.

1. L'application $\phi_y : G \to G$ définie par $\phi_y(x) = yxy^{-1}$ est un automorphisme de $G$. On dit que $\phi_y$ est un *automorphisme intérieur* de $G$.
2. L'ensemble $\mathrm{Aut}(G)$ des automorphismes de $G$ est un groupe pour la composition des applications.

3. L'application :

$$\begin{aligned}\phi : G &\to \mathrm{Aut}(G)\\ y &\mapsto \phi_y\end{aligned}$$

est un homomorphisme de groupes, dont le noyau est l'ensemble $Z(G)$ des $y$ commutant avec tous les éléments de $G$, et est appelé le *centre de* $G$ :

$$Z(G) := \{y \in G : xy = yx \text{ pour tout } x \in G\}$$

et dont l'image est l'ensemble $\mathrm{Int}(G)$ des automorphismes intérieurs de $G$.

4. $Z(G)$ est un sous-groupe distingué de $G$ et $\mathrm{Int}(G)$ est un sous-groupe de $\mathrm{Aut}(G)$.

*Démonstration.* Montrons que $\phi_y$ est un morphisme : en effet,

$$\phi_y(xz) = y(xz)y^{-1} = (yxy^{-1})(yzy^{-1}) = \phi_y(x)\phi_y(z).$$

On vérifie que $\phi_e = \mathrm{Id}_G$ et que $\phi_y \circ \phi_{y'} = \phi_{yy'}$. En particulier, $\phi_y \circ \phi_{y^{-1}} = \phi_{y^{-1}} \circ \phi_y = \mathrm{Id}_G$ donc $\phi_y$ est une bijection. De plus, on vient de montrer que $\phi$ est un homomorphisme de groupes.

Pour montrer que $\mathrm{Aut}(G)$ est un groupe pour la composition, on montre que c'est un sous-groupe de $S(G)$. En effet, $\mathrm{Id}_G \in \mathrm{Aut}(G)$ qui est non vide. Si $f$ et $g$ appartiennent à $\mathrm{Aut}(G)$, on vérifie que $f \circ g$ et $f^{-1}$ sont bien des homomorphismes de groupes.

Un élément $y$ appartient au noyau de $\phi$ si et seulement si $\phi_y = \mathrm{Id}_G$, ce qui équivaut à $\phi_y(x) = yxy^{-1} = x$ pour tout $x \in G$, soit $yx = xy$ pour tout $x \in G$. Donc $\mathrm{Ker}(\phi)$ est égal à $Z(G)$ qui est donc un sous-goupe distingué de $G$.

Il est clair que l'image de $\phi$ est l'ensemble des automorphismes intérieurs, c'est donc un sous-groupe de $G$. $\square$

# Chapitre 4

# Ordres

À partir de maintenant, on utilise systématiquement la notation multiplicative $x * y = xy$ et $e = 1_G$ pour un groupe général $G$. Un peu plus tard on simplifiera encore $1_G$ en 1.

## 4.1 Ordre d'un élément, ordre d'un groupe

**Définition 4.1.1.** L'ordre d'un groupe est le nombre de ses éléments. On note $|G|$ l'ordre de $G$.

**Définition 4.1.2.** Soit $G$ un groupe et soit $x \in G$. L'ordre de $x$ est le plus petit entier $k \geq 1$, s'il existe, tel que $x^k = 1_G$.

Si pour tout $k$, $x^k \neq 1_G$, on dit que $x$ est d'ordre infini.

**Exemple 4.1.3.**
- Le neutre $1_G$ est toujours d'ordre 1.
- Dans $(\mathbb{Z}, +)$, tout élément non nul est d'ordre infini.
- Dans $(\mathbb{Z}/n\mathbb{Z}, +)$, tout élément $a$ vérifie $na = 0$. Mais $a$ n'est pas forcément d'ordre $n$ ! Exemple : dans $\mathbb{Z}/6\mathbb{Z}$, 2 est d'ordre 3.
- Dans $(\mathbb{Z}/n\mathbb{Z}, +)$, 1 est d'ordre $n$.
- Dans $S_n$, un cycle de longueur $p$ est d'ordre $p$. En particulier, les transpositions sont d'ordre 2.

**Proposition 4.1.4.** Soit $G$ un groupe et soit $x \in G$, un élément d'ordre $k$. Si $n \in \mathbb{Z}$ et si $n = kq + r$, $0 \leq r < k$ est la division euclidienne de $n$ par $k$, alors

$$x^n = x^r.$$

On a l'équivalence :

$$x^n = 1_G \iff k \text{ divise } n$$

*Démonstration.* Si $n = kq + r$ alors $x^n = x^{kq+r} = (x^k)^q.x^r$. Donc, si $x^k = 1$ alors $x^n = x^r$.

En particulier, si $k$ divise $n$ alors $r = 0$ et $x^n = x^r = 1$. Réciproquement, si $x^n = 1$, alors $x^r = 1$ avec $0 \leq r < k$ mais comme $k$ est le plus petit entier positif avec cette propriété, c'est que $r = 0$ et donc que $k$ divise $n$. □

**Remarque 4.1.5.** On peut interpréter la notion d'ordre d'un élément en termes de morphisme : soit l'application

$$\begin{aligned} f : \mathbb{Z} &\to G \\ n &\mapsto x^n. \end{aligned}$$

Alors f est un homomorphisme de groupes et son noyau $\mathrm{Ker}(f)$ est un sous-groupe de $\mathbb{Z}$, donc il est de la forme $k\mathbb{Z}$. L'entier positif $k$ est précisément le plus petit entier $n > 0$ tel que $n \in \mathrm{Ker}(f)$, c'est-à-dire tel que $x^n = 1$. C'est donc l'ordre de $x$.

**Remarque 4.1.6.**
1. Si $x^n = 1_G$, il ne faut pas conclure trop rapidement que $n$ est l'ordre de $x$. Par contre, on sait que l'ordre de $x$ est un diviseur de $n$, ça limite les possibilités. En fait, on peut alors calculer l'ordre de $x$ en descendant *l'arbre des diviseurs de n*.
2. Si $G$ est un groupe fini, alors tout élément est d'ordre fini. En effet, $\{1_G, x, x^2, \ldots, x^n, \ldots\}$ ne peut être infini donc il existe $k < \ell$ tels que $x^k = x^\ell$ d'où on tire $x^{\ell-k} = 1_G$.

## 4.2 Groupes cycliques

On a déjà vu la notion de sous-groupe engendré par un élément $x \in G$.

**Définition 4.2.1.** Un groupe $G$ est dit *monogène* s'il existe $x \in G$ tel que $G = \langle x \rangle$. Un groupe monogène fini est dit *cyclique*. Un élément $x$ tel que $G = \langle x \rangle$ est appelé *un générateur* de $G$.

**Exemple 4.2.2.** $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre $n$. $(\mathbb{Z}/5\mathbb{Z})^*$ est cyclique d'ordre 4. Listez leurs générateurs.

**Proposition 4.2.3.** Soit $G$ un groupe et $x \in G$.
1. Si $x$ est d'ordre $k$, $\langle x \rangle = \{1, x, x^2, \ldots, x^{k-1}\}$ et $|\langle x \rangle| = k$.
2. $G$ est cyclique si et seulement si $G$ contient un élément d'ordre $|G|$.

*Démonstration.* On a déjà vu que $\langle x \rangle = \{x^n : n \in \mathbb{Z}\}$ donc $\{1, x, x^2, \ldots, x^{k-1}\} \subset \langle x \rangle$. Si $x$ est d'ordre $k$, $x^n = x^r$ où $r$ est le reste de $n$ dans la division euclidienne par $k$, $0 \leq r < k$, donc l'inclusion inverse est vérifiée. Il reste à montrer que l'ensemble $\{1, x, x^2, \ldots, x^{k-1}\}$ a exactement $k$ éléments, c'est-à-dire que les $x^i$, $0 \leq i \leq k-1$ sont distincts. En effet, supposons que, pour $0 \leq i < j \leq k-1$, on ait $x^i = x^j$. Alors, $x^{j-i} = 1$. Mais $1 \leq j - i \leq k-1$, donc c'est en contradiction avec la propriété que $k$ est le plus petit entier positif tel que $x^k = 1$.

Supposons $G$ cyclique. Alors, il existe $x \in G$ tel que $G = \langle x \rangle$, et, d'après la discussion qui précède, $|G|$ est égal à l'ordre de $x$. Donc $G$ contient bien un élément dont l'ordre vaut $|G|$. Réciproquement, supposons que $G$ contienne un élément $x$ d'ordre $k = |G|$. Alors $\langle x \rangle \subset G$ et $|\langle x \rangle| = k = |G|$ donc on peut conclure que $\langle x \rangle = G$ □

**Remarque 4.2.4.** Attention : Un groupe cyclique n'a pas un unique générateur. En fait, il a autant de générateurs qu'il y a d'éléments d'ordre égal à l'ordre de ce groupe. Exemples : générateurs de $(\mathbb{Z}/5\mathbb{Z}, +)$ et générateurs de $((\mathbb{Z}/5\mathbb{Z})^*, \times)$.

## 4.3 Classes modulo un sous-groupe, théorème de Lagrange

**Proposition 4.3.1.** Soit $G$ un groupe, et soit $H$ un sous-groupe de $G$, les relations suivantes sont des relations d'équivalence sur $G$ :

$$x\mathcal{R}_g y \text{ si } x^{-1}y \in H$$
$$x\mathcal{R}_d y \text{ si } yx^{-1} \in H.$$

Les classes d'équivalence pour $\mathcal{R}_g$ sont les ensembles $xH = \{xh : h \in H\}$, pour $x \in G$, et sont appelées les *classes à gauche de G modulo H*. Les classes d'équivalence pour $\mathcal{R}_d$ sont les ensembles $Hx = \{hx : h \in H\}$, pour $x \in G$, et sont appelées les *classes à droite de $G$ modulo $H$*.

*Démonstration.* Montrons que $\mathcal{R}_g$ est une relation d'équivalence : $x^{-1}x = 1 \in H$ donc $\mathcal{R}_g$ est réflexive. Si $x^{-1}y \in H$ alors son inverse qui est $y^{-1}x$ est aussi dans $H$ ce qui signifie que $y\mathcal{R}_g x$, donc $\mathcal{R}_g$ est symétrique. Montrons la transitivité : si $x^{-1}y \in H$ et $y^{-1}z \in H$ alors le produit $(x^{-1}y)(y^{-1}z) = z^{-1}z \in H$.

On a $y\mathcal{R}_g x$ si et seulement si $x^{-1}y \in H$ ce qui équivaut, en multipliant à gauche par $x$, à $y \in xH$.

La relation $\mathcal{R}_d$ se traite de la même façon. $\square$

On va utiliser la relation $\mathcal{R}_g$ pour démontrer le théorème de Lagrange. On reviendra sur ces relations d'équivalence au moment de l'étude des groupes quotient.

**Théorème 4.3.2** (Théorème de Lagrange)**.** Soit $G$ un groupe fini. L'ordre d'un sous-groupe de $G$ divise l'ordre de $G$.

*Démonstration.* Soit $H$ un sous-groupe de $G$. On a vu que la relation à gauche sur $G$ associée à $\mathcal{R}_g$ est une relation d'équivalence. Soit $\{x_1, \dots x_s\}$ un système de représentants des classes à gauche $G/\mathcal{R}_g$. Alors $\{x_1H, \dots, x_sH\}$ forme une partition de $G$ : $G$ est la réunion disjointe des classes $x_iH$ pour $1 \leq i \leq s$. Mais le cardinal de $xH$ est égal à l'ordre de $H$ car l'application $h \to xh$ est une bijection de $H$ sur $xH$ d'inverse $h \to x^{-1}h$. Donc on a $|G| = s|H|$ et $|H|$ divise $|G|$. $\square$

**Corollaire 4.3.3.** Soit $G$ un groupe fini. L'ordre d'un élément $x$ de $G$ divise l'ordre de $G$.

*Démonstration.* On applique le théorème de Lagrange à $H = \langle x \rangle$, en se rappelant que l'ordre de $x$ est égal à l'ordre de $\langle x \rangle$. $\square$

**Corollaire 4.3.4.** Soit $G$ un groupe fini. Pour tout $x \in G$, $x^{|G|} = 1$.

*Démonstration.* On a vu que l'ordre de $x$ divise $|G|$ donc c'est évident. $\square$

**Exemple 4.3.5.**
1. $G = \mathbb{Z}$, $H = n\mathbb{Z}$. Les relations $\mathcal{R}_g$ et $\mathcal{R}_d$ sont identiques et sont égales à la relation de congruence modulo $n$.
2. $G = S_3$, $H = \{\mathrm{Id}, (1,2)\}$. On a :

$$G/\mathcal{R}_g = \{\{\mathrm{Id}, (1,2)\}, \{(1,2,3), (1,3)\}, \{1,3,2), (2,3)\}\}$$
$$G/\mathcal{R}_d = \{\{\mathrm{Id}, (1,2)\}, \{(1,2,3), (2,3)\}, \{1,3,2), (1,3)\}\}$$

**Exercice.** Explicitez les classes à gauche et à droite de $G = S_4$ modulo $H = \langle (1,2), (3,4) \rangle$ puis modulo $H = \langle (1,2,3,4) \rangle$.

**Notation.** On note $G/H$ l'ensemble des classes à gauche de $G$ modulo $H$ et $H \setminus G$ l'ensemble des classes à droite. D'après ce qui précède, $|G/H| = |H \setminus G| = |G|/|H|$. On note cet entier $[G : H]$ et on l'appelle *l'indice de $H$ dans $G$*.

# Chapitre 5

# Sous-groupes distingués, quotients

## 5.1 Introduction

Au cours du chapitre 4, on a associé à un groupe $G$ et à un sous-groupe $H$ de $G$, deux ensembles : l'ensemble $G/H$ des classes à gauche et celui $H \setminus G$ des classes à droite modulo $H$. On aimerait bien pouvoir munir ces ensembles d'une structure de groupe.

En fait on a déjà vu cela dans le cas particulier $G = \mathbb{Z}$, $H = n\mathbb{Z}$, lorsqu'on a muni $\mathbb{Z}/n\mathbb{Z}$ de sa structure de groupe.

On va voir que le raisonnement qu'on a suivi pour $\mathbb{Z}$ se généralise facilement au cas d'un groupe $G$ commutatif, mais que, lorsque $G$ n'est pas commutatif, il faut que le sous-groupe $H$ ait une propriété supplémentaire.

Rappelons que $H \setminus G = \{Hx : x \in G\}$. On voudrait donc donner un sens au produit $(Hx)(Hy)$ de deux classes. Le plus raisonnable serait d'avoir :

$$(Hx)(Hy) = Hxy. \tag{5.1}$$

Mais deux classes peuvent coincider : plus précisément, on a $Hx = Hx'$ si et seulement si $x'x^{-1} \in H$. Il faut donc, pour que l'opération (5.1) soit bien définie, que :

$$Hx = Hx',\ Hy = Hy' \Longrightarrow Hxy = Hx'y'.$$

soit, en traduisant :

$$x'x^{-1} \in H,\ y'y^{-1} \in H \Longrightarrow (x'y')(xy)^{-1} \in H. \tag{5.2}$$

Mais $(x'y')(xy)^{-1} = x'y'y^{-1}x^{-1} = (x'x^{-1})x(y'y^{-1})x^{-1}$. Sous les hypothèses de (5.2), $x'x^{-1} \in H$, donc la condition $(x'y')(xy)^{-1} \in H$ équivaut à demander que $x(y'y^{-1})x^{-1} \in H$. On voit tout de suite que, si $G$ est commutatif, $x(y'y^{-1})x^{-1} = y'y^{-1}$ est bien dans $H$, mais ce n'est pas toujours le cas si $G$ est non commutatif. En fait, la propriété qu'il nous faudrait pour que (5.2) soit vérifiée est la suivante :

$$\text{Pour tout } x \in G, \text{ pour tout } h \in H, xhx^{-1} \in H. \tag{5.3}$$

En effet, si cela était vrai, on pourrait l'appliquer à $h = y'y^{-1}$, et obtenir l'implication (5.2). Si (5.4) est vraie, on dit que $H$ *est un sous-groupe distingué de* $G$.

## 5.2 Sous-groupes distingués et groupes quotients

**Définition 5.2.1.** Soit $G$ un groupe et $H$ un sous-groupe de $G$. On dit que $H$ est un *sous-groupe distingué ou normal de $G$* , et on note $H \lhd G$ si :

$$\text{Pour tout } x \in G, \text{ pour tout } h \in H, xhx^{-1} \in H. \tag{5.4}$$

**Exemple 5.2.2.** - Si $G$ est commutatif, tous ses sous-groupes sont distingués puisque $xhx^{-1} = hxx^{-1} = h \in H$.

- $\{e\}$ et $G$ sont des sous-groupes distingués de $G$.
- $G = S_3$. Le sous-groupe $H = \{\mathrm{Id}, (1,2)\}$ n'est pas distingué dans $G$. Le sous-groupe $H = \langle(1,2,3)\rangle$ est distingué dans $S_3$.

**Théorème 5.2.3.** Soit $G$ un groupe et soit $H$ un sous-groupe distingué de $G$.

1. Pour tout $x \in G$, $xH = Hx$. En particulier, $G/H = H \setminus G$.
2. $G/H$ est un groupe pour la loi :
$$(xH)(yH) = xyH$$
appelé *groupe quotient de $G$ par $H$*.
3. La surjection canonique $s : G \to G/H$ est un homomorphisme de groupes.

*Démonstration.* 1. Il est clair que $H \lhd G$ si et seulement si $xHx^{-1} = H$ pour tout $x \in G$, ce qui équivaut à $xH = Hx$ pour tout $x \in G$.

2. Voir l'introduction du chapitre

3. On a $s(x) = xH$ et la loi sur $G/H$ est telle que $(xH)(yH) = xyH$ soit exactement telle que $s(x)s(y) = s(xy)$. □

**Remarque 5.2.4.** Si $H$ est distingué dans $G$, on vient de voir que l'ensemble $G/H$ est un groupe. Bien sûr, son ordre est $|G/H| = |G|/|H|$.

## 5.3 Sous-groupes distingués et morphismes

**Proposition 5.3.1.** Soit $f : G \to K$ un homomorphisme de groupes. Le noyau $\mathrm{Ker}(f)$ de $f$ est un sous-groupe distingué de $G$.

Réciproquement, tout sous-groupe distingué $H$ de $G$ est le noyau d'un homomorphisme de groupe : $H = \mathrm{Ker}(s)$ où $s : G \to G/H$ est la surjection canonique.

*Démonstration.* Soit $H = \mathrm{Ker}(f)$. Soit $x \in G$ et $h \in H$ ; on veut montrer que $xhx^{-1} \in H$. On calcule $f(xhx^{-1})$.

$$f(xhx^{-1}) = f(x)f(h)f(x)^{-1} = f(x)f(x)^{-1} = e_K$$

donc $xhx^{-1} \in H$ et $H \lhd G$.

Il est clair que $\mathrm{Ker}(s) = H$. □

**Théorème 5.3.2.** Soit $f : G \to K$ un homomorphisme de groupes. Il existe un homomorphisme de groupes unique $\tilde{f} : G/\mathrm{Ker}(f) \to K$ tel que, pour tout $x \in G$, $\tilde{f}(s(x)) = f(x)$, c'est-à-dire rendant le diagramme suivant commutatif :

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, "s"'] & K \\
G/\operatorname{Ker}(f) \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}$$

De plus, $\tilde{f}$ est injective et définit un isomorphisme de $G/\operatorname{Ker}(f)$ sur $\operatorname{Im}(f)$.

*Démonstration.* On applique le théorème 1.2.8 pour construire l'application $\tilde{f}$. Il faut donc montrer l'implication :

$$x^{-1}y \in \operatorname{Ker}(f) \Longrightarrow f(x) = f(y).$$

En effet, si $x^{-1}y \in \operatorname{Ker}(f)$, alors $f(xy^{-1}) = 1$ soit $f(x)f(y)^{-1} = 1$ donc $f(x) = f(y)$.

Montrons que $\tilde{f}$ est un morphisme : soit $a = s(x)$ et $b = s(y)$ deux éléments de $G/\operatorname{Ker}(f)$. On a

$$\tilde{f}(ab) = \tilde{f}(s(x)s(y)) = \tilde{f}(s(xy)) = f(xy) = f(x)f(y) = \tilde{f}(a)\tilde{f}(b).$$

Montrons que $\tilde{f}$ est injective : pour cela il suffit de montrer que $\operatorname{Ker}(\tilde{f}) = \{1_{G/\operatorname{Ker}(f)}\}$. Soit $a = s(x)$ tel que $\tilde{f}(a) = 1_K$. Alors $f(x) = 1_K$, donc $x \in \operatorname{Ker}(f)$, ce qui signifie exactement que $a = s(x) = 1_{G/\operatorname{Ker}(f)}$. □

# Chapitre 6

# Groupes cycliques, groupes diédraux

## 6.1 Groupes cycliques

Tout d'abord, on va voir que, à isomorphisme près, il y a un seul groupe cyclique d'ordre donné.

**Théorème 6.1.1.** Soit $G$ un groupe cyclique. Alors, soit $G$ est d'ordre infini et $G$ est isomorphes à $(\mathbb{Z},+)$, soit $G$ est d'ordre fini $n$ et $G$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$.

*Démonstration.* Si $G$ est cyclique alors il est engendré par un générateur $x : G = \langle x \rangle$. On a déjà introduit l'homomorphisme surjectif

$$\begin{aligned} f : \mathbb{Z} &\to G \\ k &\mapsto x^k \end{aligned}$$

Le noyau de $f$ est $\{0\}$ si $x$ est d'ordre infini, et est $n\mathbb{Z}$ où $n$ est l'ordre de $x$ sinon. Par le théorème de factorisation 1.2.8 le morphisme induit $\tilde{f} : \mathbb{Z}/\operatorname{Ker}(f) \to G$ est un isomorphisme. On obtient donc un isomorphisme de $\mathbb{Z}$ sur $G$ dans le cas où $G$ est infini et un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur $G$ dans le cas où $G$ est fini d'ordre $n$. $\square$

On considère maintenant uniquement le cas cyclique fini. Examinons d'abord les ordres des éléments de $G$ et les sous-groupes de $G$ :

**Proposition 6.1.2.** Soit $G = \langle x \rangle$ un groupe cyclique d'ordre $n$.

1. L'ordre de $x^k$ est $n/\operatorname{pgcd}(n,k)$. En particulier, les générateurs de $G$ sont les $x^k$ avec $\operatorname{pgcd}(n,k) = 1$.
2. Soit $H$ un sous-groupe de $G$. Alors $H$ est cyclique et son ordre $d$ divise $n$.
3. Réciproquement, si $d$ divise $n$, $G$ contient un unique sous-groupe d'ordre $d$ qui est $H = \langle x^{n/d} \rangle = \{y \in G : y^d = 1\}$.

*Démonstration.* (1) Soit $d = \operatorname{pgcd}(n,k)$. On pose $n = dn'$ et $k = dk'$, avec $\operatorname{pgcd}(n',k') = 1$. On a :

$$(x^k)^{n'} = x^{kn'} = x^{dk'n'} = (x^{dn'})^{k'} = (x^n)^{k'} = 1$$

donc l'ordre $a$ de $x^k$ divise $n'$. D'autre part, on a

$$1 = (x^k)^a = x^{ka} = x^{dk'a}$$

donc $n$, l'ordre de $x$, divise $dk'a$. Mais $n = dn'$ donc $n'$ divise $k'a$. Par le lemme de Gauss, comme $\mathrm{pgcd}(n', k') = 1$, on peut conclure que $n'$ divise $a$. Conclusion : $a = n'$.

(2) Soit $H$ un sous-groupe de $G$ d'ordre $d$. D'après le théorème de Lagrange, $d$ divise $n$. Soit $\ell$ le plus petit entier positif tel que $x^\ell \in H$. Par division euclidienne, on montre que, si $x^k \in H$, alors $k$ est un multiple de $\ell$ donc $H = \langle x^\ell \rangle$ est cyclique.

(3) Soit $d$ un diviseur de $n$ et soit $q = n/d$. D'après (1), $x^q$ est d'ordre $d$ donc engendre un sous-groupe $H = \langle x^q \rangle$ de $G$ d'ordre $d$. Remarquons que $H$ est contenu dans $K := \{y \in G : y^d = 1\}$. En effet, $(x^{q\ell})^d = x^{q\ell d} = (x^n)^\ell = 1$. Réciproquement, soit $y = x^a \in K$. Alors $x^{ad} = 1$ donc $n$ divise $ad$ donc $q$ divise $a$ donc $y \in H$. On a montré l'égalité $H = K$ et en particulier cela montre qu'il n'y a pas d'autre sous-groupe d'ordre $d$. □

Maintenant les images et les quotients d'un groupe cyclique :

**Proposition 6.1.3.** Soit $G$ un groupe cyclique.

1. Soit $f : G \to K$ un morphisme de groupes. Alors $\mathrm{Im}(f)$ est un sous-groupe cyclique de $K$.
2. Soit $H$ un sous-groupe de $G$. Alors le quotient $G/H$ est un groupe cyclique.

*Démonstration.* (1) Montrons que, si $G$ est engendré par $x$, alors $\mathrm{Im}(f)$ est engendré par $f(x)$. En effet, soit $y \in \mathrm{Im}(f)$. Par définition, il existe $z \in G$ tel que $y = f(z)$. Puisque $G$ est cyclique, il existe $k \in \mathbb{Z}$ tel que $z = x^k$ soit $y = f(x^k) = f(x)^k \in \langle f(x) \rangle$. Donc $\mathrm{Im}(f) = \langle f(x) \rangle$.

(2) Soit $H$ un sous-groupe de $G$. Puisque $G$ est commutatif, $H$ est distingué dans $G$ et le quotient $G/H$ est un groupe. Par construction, $G/H$ est l'image de $G$ par la surjection canonique $s : G \to G/H$ qui est un morphisme de groupe donc d'après ce qui précède $G/H$ est cyclique. □

## 6.2 La fonction d'Euler et le théorème chinois

**Définition 6.2.1.** La fonction $\varphi$ d'Euler est définie pour $n \geq 1$, $n$ entier par :

$$\varphi(n) = |\{a, 1 \leq a \leq n : \mathrm{pgcd}(a, n) = 1\}|.$$

**Proposition 6.2.2.** On a :

1. Si $d$ divise $n$, $\varphi(d)$ est le nombre d'éléments d'ordre $d$ dans un groupe cyclique d'ordre $n$. En particulier, $\varphi(n)$ est le nombre de générateurs d'un groupe cyclique d'ordre $n$.
2. $\varphi(n)$ est le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$, autrement dit $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$.

*Démonstration.* On a vu (1) dans la proposition 6.1.2 et (2) au chapitre 1. □

**Proposition 6.2.3.** La fonction $\varphi$ vérifie :

1. $\varphi(1) = 1$.
2. Pour tout $k \geq 1$, $\varphi(p^k) = p^k - p^{k-1}$.
3. Si $\mathrm{pgcd}(m, n) = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$.
4. $\sum_{d \text{ divise } n} \varphi(d) = n$.

Remarquons que, avec les propriétés 2. et 3., on peut calculer $\varphi(n)$ pour tout $n$.

**Exemple 6.2.4.** Calculons $\varphi(1728)$. Comme $1728 = 12^3 = 2^6 * 3^3$, $\varphi(1728) = \varphi(2^6)\varphi(3^3) = (2^6 - 2^5)(3^3 - 3^2) = 576$.

*Démonstration.* (1) Les entiers $a \in [1 \dots p^k]$ qui sont premiers avec $p^k$ sont ceux qui ne sont pas multiples de $p$. Comme il y a $p^{k-1}$ multiples de $p$ entre 1 et $p^k$, on obtient le résultat.

(2) C'est une conséquence du *théorème chinois* qui suit.

(3) Soit $G$ un groupe cyclique d'ordre $n$ ; $G$ est la réunion disjointe des ensembles $O_d = \{y \in G : \text{ordre}(y) = d\}$ pour $d$ divisant $n$ (th de Lagrange : l'ordre d'un élément divise l'ordre du groupe). Comme $|O_d| = \varphi(d)$, on en déduit que $n = |G| = \sum_{d \text{ divise } n} \varphi(d)$. □

**Théorème 6.2.5** (Le théorème chinois)**.** Si $\text{pgcd}(m, n) = 1$, l'homomorphisme de groupes :

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x &\mapsto (x \bmod m, x \bmod n) \end{aligned}$$

induit un isomorphisme :

$$\tilde{f} : \mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

L'isomorphisme réciproque est défini par :

$$\begin{aligned} g : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/mn\mathbb{Z} \\ (a \bmod m, b \bmod n) &\mapsto anv + bmu \bmod mn \end{aligned}$$

où $1 = mu + nv$ est une relation de Bezout entre $m$ et $n$.

*Démonstration.* On applique le théorème de factorisation des morphismes de groupes (Théorme 1.2.8) à $f$. Le noyau de $f$ est $\text{Ker}(f) = m\mathbb{Z} \cap n\mathbb{Z} = \text{ppcm}(m, n)\mathbb{Z} = mn\mathbb{Z}$ donc $f$ induit un morphisme injectif $\tilde{f} : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Comme $|\mathbb{Z}/mn\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = mn$, $\tilde{f}$ est un isomorphisme.

On a : $mu = 1 - nv = 1 \bmod n$ et $nv = 1 - mu = 1 \bmod m$ donc $anv + bmu = a \bmod m$ et $anv + bmu = b \bmod n$ donc $\tilde{f} \circ g = \text{Id}$. □

**Corollaire 6.2.6.** Si $\text{pgcd}(m, n) = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$.

*Démonstration.* On utilise le lemme suivant, laissé en exercice :

**Lemme 6.2.7.** Si $G = H \times K$ est un produit direct de groupes alors l'ordre de $(x, y) \in G$ est le ppcm des ordres de $x$ et $y$.

On applique ce lemme au produit direct $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ dans lequel on veut compter les éléments d'ordre $mn$. Donc un élément $(a, b)$ est d'ordre le ppcm des ordres respectifs de $a$ et $b$. Comme $\text{pgcd}(m, n) = 1$, et que l'ordre de $a$ divise $m$ et l'ordre de $b$ divise $n$, ces ordres sont aussi premiers entre eux donc l'ordre du couple $(a, b)$ est le produit des ordres de $a$ et $b$. Donc $(a, b)$ est d'ordre $mn$ si et seulement si $a$ est d'ordre $m$ dans $\mathbb{Z}/m\mathbb{Z}$ et $b$ d'ordre $n$ dans $\mathbb{Z}/n\mathbb{Z}$. On peut donc conclure que $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ contient $\varphi(m)\varphi(n)$ éléments d'ordre $mn$. Par le théorème chinois, $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}$ donc il contient $\varphi(mn)$ éléments d'ordre $mn$. Finalement, on a bien démontré que $\varphi(mn) = \varphi(m)\varphi(n)$. □

**Corollaire 6.2.8.** Le produit direct de deux groupes cycliques d'ordres premiers entre eux est cyclique.

*Démonstration.* Puisque un groupe cyclique d'ordre $m$ est isomorphe à $\mathbb{Z}/m\mathbb{Z}$, cela découle immédiatement du théorème chinois. $\square$

**Remarque 6.2.9.** Bien, sûr, si $m$ et $n$ ne sont pas premiers entre eux, le produit direct de deux groupes cycliques d'ordre $m$ et $n$ n'est pas en général cyclique. Par exemple, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2Z$ n'est pas cyclique car il ne contient pas d'éléments d'ordre 4.

On peut montrer que, pour tout $m, n$, on a :

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\operatorname{pgcd}(m,n)\mathbb{Z} \times \mathbb{Z}/\operatorname{ppcm}(m,n)\mathbb{Z}.$$

## 6.3 Groupes diédraux

Considérons le groupe $\mathrm{Is}(\mathcal{P}_n)$ des isométries planes d'un polygone régulier $\mathcal{P}_n$ à $n$ sommets. On suppose que $\mathcal{P}_n$ est centré en $(0,0)$ et que $(1,0)$ est un sommet. Alors, les éléments de $\mathrm{Is}(\mathcal{P}_n)$ fixent le centre $(0,0)$ donc ce sont des transformations linéaires.

Ce groupe contient $n$ rotations $r_k$, d'angle $2k\pi/n$ pour $k = 0, 1, \ldots, n-1$, ainsi que $n$ symétries $s_1, \ldots, s_n$ d'axes $D_1, \ldots, D_n$. On note $D_1$ l'axe horizontal ; on obtient $D_2, \ldots, D_n$ en tournant successivement $D_1$ d'un angle $\pi/n$. On a

$$\mathrm{Is}(\mathcal{P}_n) = \{r_0, r_1, \ldots, r_{n-1}, s_1, \ldots, s_n\}.$$

$\mathrm{Is}(\mathcal{P}_n)$ est un groupe d'ordre $2n$ qui est non commutatif pour $n \geq 3$.

Notons $r = r_1$ la rotation d'angle $2\pi/n$. On a $r_k = r^k$ et $r$ est d'ordre $n$. Cet élément engendre un sous-groupe cyclique d'ordre $n$.

En général, si $r_\theta$ est la rotation d'angle $\theta$ et $s_D$ la symétrie d'axe $D$, on a :

$$s_D r_\theta = s_{D'}, \text{ où } D' = r_{-\theta/2}(D).$$

En posant $s = s_1$, on a donc $\{s_1, \ldots, s_n\} = \{s, sr, sr^2, \ldots, sr^{n-1}\}$. Donc,

$$\mathrm{Is}(\mathcal{P}_n) = \{\mathrm{Id}, r, r^2, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$$

et $\mathrm{Is}(\mathcal{P}_n)$ est engendré par les deux éléments $s$ et $r$. Pour connaitre entièrement la multiplication dans $\mathrm{Is}(\mathcal{P}_n)$, il suffit de calculer le produit $rs$. Or, on a vu que $sr$ est une symétrie donc $srsr = 1$ donc $rs = s^{-1}r^{-1} = sr^{n-1}$.

Les relations $s^2 = 1$, $r^n = 1$, $rs = sr^{n-1}$ déterminent la table de multiplication de $\mathrm{Is}(\mathcal{P}_n)$ de façon unique (exercice). Le groupe abstrait défini ainsi *par générateurs et relations* s'appelle le groupe diédral, et noté $D_{2n}$ :

$$D_{2n} = \langle s, r \mid s^2 = 1, r^n = 1, rs = sr^{n-1}\rangle.$$

Le sous-groupe cyclique $C = \langle r\rangle$ est un sous-groupe distingué dans $D_{2n}$. En effet, $sr^k s = r^{-k}$. Le groupe quotient $G/C$ est d'ordre 2.

**Exercice 6.1.** Montrez que les sous-groupes du groupe diédral $D_{2n}$ sont soit cycliques soit diédraux.

# Chapitre 7

# Groupes opérant sur un ensemble

## 7.1 Introduction

Revenons sur le groupe $\mathrm{Is}(\mathcal{P}_n)$ des isométries du polygone régulier à $n$ sommets $\mathcal{P}_n$. Notons $\{P_1, P_2, \ldots, P_n\}$ les sommets de $\mathcal{P}_n$. Alors, pour tout $g \in \mathrm{Is}(\mathcal{P}_n)$ et pour tout $P_i$, $g(P_i)$ est un autre sommet $P_j$. Notons :

$$g \cdot i = j \quad \text{lorsque} \quad g(P_i) = P_j.$$

On dit que *le groupe* $\mathrm{Is}(\mathcal{P}_n)$ *opère sur l'ensemble* $\{1, 2, \ldots, n\}$. Prenons le cas $n = 5$, et les notations du chapitre précédent : $r$ est la rotation d'angle $2\pi/5$ et $s$ est la symétrie d'axe horizontal. On a :

$$\begin{aligned} r \cdot 1 = 2,\ r \cdot 2 = 3,\ r \cdot 3 = 4,\ r \cdot 4 = 5,\ r \cdot 5 = 1 \\ s \cdot 1 = 1,\ s \cdot 2 = 5,\ s \cdot 3 = 4,\ s \cdot 4 = 3,\ s \cdot 5 = 2 \end{aligned}$$

On voit que l'action de $r$ induit une permutation de l'ensemble $\{1, 2, 3, 4, 5\}$ qui est le cycle $(1, 2, 3, 4, 5)$ tandis que $s$ induit la permutation $(2, 5)(3, 4)$. Plus généralement, chaque élément $g$ de $\mathrm{Is}(\mathcal{P}_5)$ définit une permutation de $\{1, 2, 3, 4, 5\}$, notée $\sigma(g)$. On a donc une application :

$$\begin{aligned} \sigma : \mathrm{Is}(\mathcal{P}_5) &\to S_5 \\ g &\mapsto \sigma(g). \end{aligned}$$

On va voir que $\sigma$ est un morphisme de groupes.

## 7.2 Actions de groupes

**Définition 7.2.1.** Soit $G$ un groupe et $X$ un ensemble. Une opération (action) de $G$ sur $X$ est une application :

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

vérifiant les propriétés suivantes :

1. Pour tout $x \in X$, $1 \cdot x = x$
2. Pour tout $g, g' \in G$ et $x \in X$, $g \cdot (g' \cdot x) = (gg') \cdot x$

**Exemple 7.2.2.** Voici quelques exemples :

- L'action du groupe $\mathrm{Is}(\mathcal{P}_n)$ sur $X = \{1, \ldots, n\}$, voir la section d'introduction.
- Le groupe $\mathrm{GL}(n, \mathbb{R})$ opère sur $X = \mathbb{R}^n$ par : $A \cdot x = Ax^t$.
- Le groupe symétrique $S_n$ opère sur $\{1, 2, \ldots, n\}$ par $\sigma \cdot i = \sigma(i)$.

**Proposition 7.2.3.** Soit $G$ un groupe opérant sur un ensemble $X$. L'application $\sigma$ définie par :

$$\begin{aligned} \sigma : G &\to S(X) \\ g &\mapsto \sigma(g) : \begin{aligned} X &\to X \\ x &\mapsto g \cdot x \end{aligned} \end{aligned}$$

est un morphisme de groupes de $G$ dans $S(X)$.

*Démonstration.* Tout d'abord, il faut justifier que $\sigma(g) \in S(X)$, c'est-à-dire que $\sigma(g)$ est une bijection de $X$. En effet, on a $(\sigma(g) \circ \sigma(g^{-1}))(x) = \sigma(g)(g^{-1} \cdot x) = g \cdot (g^{-1} \cdot x)$. En vertu des propriétés d'action de groupe, $g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = 1 \cdot x = x$. Donc $\sigma(g) \circ \sigma(g^{-1}) = \mathrm{Id}_X$ donc $\sigma(g)$ est bien une permutation de $X$.

Montrons que $\sigma$ est un morphisme de groupe, soit que $\sigma(gg') = \sigma(g)\sigma(g')$. Pour cela, on calcule $(\sigma(g)\sigma(g'))(x)$ pour $x \in X$ :

$$(\sigma(g)\sigma(g'))(x) = \sigma(g)(\sigma(g')(x)) = \sigma(g)(g' \cdot x) = g \cdot (g' \cdot x) = (gg') \cdot x = \sigma(gg')(x).$$

Donc on a bien $\sigma(gg') = \sigma(g)\sigma(g')$ et $\sigma$ est un morphisme de groupes. □

## 7.3 Orbites et stabilisateurs

**Définition 7.3.1.** Soit $G$ un groupe opérant sur un ensemble $X$.

1. Le *stabilisateur* ou *groupe d'isotropie* $G_x$ de $x \in X$ est le sous-groupe de $G$ défini par :

$$G_x = \{g \in G : g \cdot x = x\}.$$

2. L'*orbite* $O_x$ de $x \in X$ est le sous-ensemble de $X$ défini par :

$$O_x = \{g \cdot x : g \in G\}.$$

**Exemple 7.3.2.** Pour l'action de $G = \mathrm{Is}(\mathcal{P}_n)$ sur $\{1, 2, \ldots, n\}$, et pour $x = 1$, $G_1 = \{\mathrm{Id}, s\}$ et $O_1 = \{1, \ldots, n\}$. On remarque que $|O_1| = n$ et $|\mathrm{Is}(\mathcal{P}_n)|/|G_1| = 2n/n = n$ sont égaux.

**Théorème 7.3.3.** Soit $G$ un groupe opérant sur un ensemble $X$.

1. La relation $\mathcal{R}$ sur $X$ définie par :

$$x \mathcal{R}\, y \Longleftrightarrow \text{il existe } g \in G \text{ tel que } y = g \cdot x.$$

   est une relation d'équivalence, dont les classes d'équivalence sont les orbites de $G$ sur $X$ : $\mathrm{cl}(x) = O_x$. On note $X/G$ l'ensemble $X/\mathcal{R}$ de ces classes d'équivalence, $X/G$ est donc l'ensemble des orbites de $X$ sous l'action de $G$.

2. Pour tout $x \in G$, $O_x$ est en bijection avec l'ensemble $G/G_x$ des classes à gauche de $G$ modulo $G_x$. En particulier, si $G$ est fini,

$$|O_x| = |G|/|G_x|.$$

3. Soit $\{x_i\}_{i\in I}$ un *système de représentants* des classes d'équivalence pour la relation $\mathcal{R}$ (c'est-à-dire des orbites). On a : $X = \sqcup_{i\in I} O_{x_i}$ (réunion disjointe), d'où, si $X$ et $G$ sont finis, *l'équation aux classes* :

$$|X| = \sum_{i\in I} |O_{x_i}| = \sum_{i\in I} |G|/|G_{x_i}|.$$

*Démonstration.* On laisse au lecteur le soin de vérifier que $\mathcal{R}$ est bien une relation d'équivalence, dont les classes d'équivalence sont les orbites. Celles-ci forment une partition de $X$, d'après la Proposition 1.2.5, et l'équation aux classes en découle (revoir le point 3. de Proposition 1.2.5 et la définition d'un système de représentants des classes d'équivalence).

Il reste à mettre en évidence une bijection entre $G/G_x$ et $O_x$. Pour cela, on se rappelle que $G/G_x = \{gG_x : g \in G\}$. Soit l'application

$$\begin{aligned} f : G &\to O_x \\ g &\mapsto g\cdot x. \end{aligned}$$

Comme, si $h \in G_x$, $(gh)\cdot x = g\cdot(h\cdot x) = g\cdot x$, $f$ induit (par le théorème de factorisation 1.2.8) une application $\tilde{f}$ :

$$\begin{aligned} \tilde{f} : G/G_x &\to O_x \\ gG_x &\mapsto g\cdot x. \end{aligned}$$

De plus, $f$ est clairement surjective donc l'application induite $\tilde{f}$ l'est aussi.

Il reste à montrer que $\tilde{f}$ est injective : pour cela, supposons que $\tilde{f}(gG_x) = \tilde{f}(g'G_x)$, soit que $g\cdot x = g'\cdot x$. Alors, $(g^{-1}g')\cdot x = x$, ce qui signifie que $g^{-1}g' \in G_x$, soit $g'G_x = gG_x$. Donc, $\tilde{f}$ est bien injective. □

**Définition 7.3.4.** Soit $G$ un groupe opérant sur un ensemble $X$.

1. On dit que $G$ opère *transitivement* sur $X$ si, pour tout $x, y \in X$, il existe $g \in G$ tel que $y = g\cdot x$. De façon équivalente, $O_x = X$ pour tout $x \in X$.
2. On dit que $G$ opère *fidèlement* sur $X$ si le seul élément $g \in G$ tel que $g\cdot x = x$ pour tout $x \in X$ est $g = 1$. De façon équivalente, $G$ opère fidèlement sur $X$ si $\mathrm{Ker}(\sigma) = \cap_{x\in X} G_x = \{1\}$ ($\sigma$ est un morphisme injectif).
3. On dit que $G$ opère *librement* sur $X$ si le seul élément $g \in G$ tel qu'il existe $x \in X$ tel que $g\cdot x = x$, est $g = 1$. De façon équivalente, $G$ opère fidèlement sur $X$ si $G_x = \{1\}$ pour tout $x \in X$.

**Exemple 7.3.5.** Le groupe $\mathrm{Is}(\mathcal{P}_n)$ opère transitivement et fidèlement sur $\{1, 2, \ldots, n\}$. Il n'opère pas librement : en effet, $s\cdot 1 = 1$. Par contre, le sous-groupe cyclique d'ordre $n$ opère sur $\{1, \ldots, n\}$ librement et transitivement.

## 7.4 Exemples d'actions de groupe

Voici quelques exemples classiques d'actions de groupe :

1. Un groupe $G$ opère sur lui-même par translation à gauche : $g\cdot x = gx$ pour tout $g, x \in G$.

2. $G$ opère sur lui-même par conjugaison : $g \cdot x = gxg^{-1}$. On dit que $y = gxg^{-1}$ et $x$ sont *conjugués dans* $G$. Les orbites pour cette action s'appellent *les classes de conjugaison de* $G$.
3. Si $H$ est un sous-groupe de $G$, $G$ opère sur l'ensemble des classes à gauche $G/H$ par : $g \cdot xH = (gx)H$.
4. Le groupe $\mathrm{GL}(\mathbb{R}^n)$ opère sur $\mathbb{R}^n$, mais également sur l'ensemble des droites de $\mathbb{R}^n$, et plus généralement sur l'ensemble des sous-espaces vectoriels de dimension $k$ de $\mathbb{R}^n$.
5. Le groupe symétrique $S_n$ opère sur $X = \{1, \dots, n\}$, mais aussi sur l'ensemble des parties de $X$ qui sont de cardinal $k$.

**Exercice 7.1.** Vérifiez que ce sont bien des actions de groupe. Pour chacune de ces actions que pouvez-vous dire des stabilisateurs et des orbites des éléments de $X$ ?
**Exercice 7.2.** En utilisant l'action de $G$ sur lui-même par translation à gauche, et le morphisme $\sigma$ associé, montrez que tout groupe fini est isomorphe à un sous-groupe d'un groupe de permutations (c'est le *théorème de Cayley*)

**Remarque 7.4.1.** Dans ce chapitre, nous avons défini et étudié l'*action à gauche* d'un groupe sur un ensemble. Si on remplace la condition : $g \cdot (g' \cdot x) = (gg') \cdot x$ par : $g \cdot (g' \cdot x) = (g'g) \cdot x$, on dit que l'action est à droite et on préfère la noter $x \cdot g$ de sorte que : $(x \cdot g) \cdot g' = x \cdot (gg')$. On peut transformer facilement une action à droite en action à gauche en posant : $g \cdot x := x \cdot g^{-1}$.

# Chapitre 8

# Le groupe symétrique $S_n$

## 8.1 Notations

On rappelle quelques notations, introduites précédemment. Le groupe symétrique $S_n$ est le groupe des permutations de l'ensemble $\{1, 2, \ldots, n\}$, muni de la loi de composition. Il est d'ordre $n!$.

Une permutation quelconque est notée :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}.$$

Un *cycle* est une permutation particulière qui permute circulairement un sous-ensemble de $\{1, \ldots, n\}$ et laisse les autres éléments inchangés. On note le cycle $\sigma = (a_1, \ldots, a_p)$, $p \geq 2$, si $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3, \ldots, \sigma(a_p) = a_1$. On dit que $p \geq 2$ est *la longueur* du cycle $\sigma$ et on la note $\ell(\sigma)$. Une *transposition* est un cycle de longueur 2.

**Définition 8.1.1.** Le *support* d'une permutation $\sigma$ est l'ensemble :

$$\mathrm{Sup}(\sigma) := \{i \in \{1, \ldots, n\} : \sigma(i) \neq i\}.$$

**Proposition 8.1.2.** On a les propriétés suivantes :

1. Si $\sigma = (a_1, \ldots, a_p)$, $\mathrm{Sup}(\sigma) = \{a_1, \ldots, a_p\}$.
2. Si $S$ est le support de $\sigma$, $\sigma(S) = S$.
3. Deux permutations de supports disjoints commutent.

*Démonstration.* 1. et 2. sont faciles. Montrons 3. Soit $\sigma_1$ une permutation de support $S_1$ et $\sigma_2$ une permutation de support $S_2$, telles que $S_1 \cap S_2 = \emptyset$. Montrons que $\sigma_1\sigma_2 = \sigma_2\sigma_1$. On peut distinguer trois cas :

- $i \notin S_1 \cup S_2$. Alors, $\sigma_1\sigma_2(i) = \sigma_1(\sigma_2(i)) = \sigma_1(i) = i$, et de même, $\sigma_2\sigma_1(i) = \sigma_2(\sigma_1(i)) = \sigma_2(i) = i$.
- $i \in S_1$. Alors, $i \notin S_2$ donc $\sigma_1\sigma_2(i) = \sigma_1(i)$. De plus, $\sigma_1(i) \in S_1$ d'après 2. donc $\sigma_1(i) \notin S_2$ et $\sigma_2(\sigma_1(i)) = \sigma_1(i)$.
- $i \in S_2$. Ce cas est analogue au précédent.

□

**Proposition 8.1.3.** Propriétés des cycles :

1. Un cycle de longueur $p$ est d'ordre $p$ dans $S_n$.
2. Si $c = (a_1, \dots, a_p)$, et $\sigma \in S_n$, alors $\sigma c \sigma^{-1}$ est encore un cycle, de même longueur que $c$ :
$$\sigma c \sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_p)).$$
3. Deux cycles de même longueur sont conjugués dans $S_n$.

*Démonstration.* 1. Si $c = (a_1, \dots, a_p)$, $c^k(a_1) = a_{k+1}$ donc, si $c^k = 1$, alors $k \geq p$. Il est clair que $c^p = 1$.

2. Posons $\tau = \sigma c \sigma^{-1}$. Alors, $\tau(\sigma(a_i)) = \sigma c \sigma^{-1} \sigma(a_i) = \sigma c(a_i) = \sigma(a_{i+1})$. D'autre part, si $k \notin \mathrm{Sup}(c)$, $\tau(\sigma(k)) = \sigma c \sigma^{-1} \sigma(k) = \sigma c(k) = \sigma(k)$. Donc $\tau$ est bien le cycle $(\sigma(a_1), \dots, \sigma(a_p))$.

3. Si $c = (a_1, \dots, a_p)$, et $c' = (b_1, \dots, b_p)$, il existe une permutation $\sigma$ de $\{1, 2, \dots, n\}$ telle que $\sigma(a_i) = b_i$ pour $i = 1, \dots, p$. D'après 2., $c' = \sigma c \sigma^{-1}$. □

## 8.2 La décomposition canonique d'une permutation en produit de cycles

**Théorème 8.2.1.** Une permutation $\sigma$ se décompose en un produit de cycles à supports disjoints, de façon unique à l'ordre près.

Soit $O_{a_1}, \dots, O_{a_s}$ les orbites de l'ensemble $\{1, 2, \dots, n\}$ sous l'action du groupe $\langle \sigma \rangle$, telles que $|O_{a_i}| \geq 2$. Si $O_{a_i} = \{a_i, \sigma(a_i), \dots, \sigma^{k_i - 1}(a_i)\}$ pour $k_i \geq 2$ et $1 \leq i \leq s$, alors
$$\sigma = \prod_{i=1}^{s} c_i, \quad \text{où } c_i = (a_i, \sigma(a_i), \dots, \sigma^{k_i - 1}(a_i)) \tag{8.1}$$

*Démonstration.* Le groupe $H := \langle \sigma \rangle$ opère sur $\{1, \dots, n\}$. Ses orbites forment donc une partition de l'ensemble $\{1, \dots, n\}$. Si $O_x = \{x\}$ est une orbite à un élément, c'est que $\sigma(x) = x$. Soit $\{a_1, \dots, a_s\}$ un système de représentants des orbites de cardinal au moins 2 ; alors $O_{a_i} = \{a_i, \sigma(a_i), \dots, \sigma^{k_i - 1}(a_i)\}$ pour un certain $k_i \geq 2$, tel que $\sigma^{k_i}(a_i) = a_i$. On pose $c_i = (a_i, \sigma(a_i), \dots, \sigma^{k_i - 1}(a_i))$ et $\tau := \prod_{i=1}^{s} c_i$. Montrons que $\tau = \sigma$ : Soit $k \in \{1, \dots, n\}$. Puisque les $O_{a_i}$ forment une partition de $\{1, \dots, n\}$, il existe $i$ tel que $k \in O_{a_i}$, donc un entier $u$, $0 \leq u \leq k_i - 1$, tels que $k = \sigma^u(a_i)$. Puisque les supports des cycles $c_i$ sont disjoints, $\tau(k) = c_i(k) = c_i(\sigma^u(a_i)) = \sigma^{u+1}(a_i) = \sigma(k)$. Donc, $\tau(k) = \sigma(k)$ pour tout $k$, donc $\sigma = \tau$.

Il reste à démontrer l'unicité de la décomposition. Supposons donc que $\sigma$ admette deux décompositions en produit de cycles disjoints : $\sigma = \prod_{i=1}^{s} c_i = \prod_{i=1}^{s'} c'_i$. Les réunions des supports de chacune de ces deux familles de cycles forment le support $S$ de $\sigma$. Plus précisément, les supports des $c_i$ (et donc aussi des $c'_i$) sont les orbites de $H$ agissant sur $S$, qui forment une partition de $S$. Donc $s = s'$, et, quitte à réordonner les $c'_i$, on peut supposer que $\mathrm{Sup}(c_i) = \mathrm{Sup}(c'_i)$. Soit $a_i \in \mathrm{Sup}(c_i) = \mathrm{Sup}(c'_i)$ ; alors $c_i = c'_i = (a_i, \sigma(a_i), \dots, \sigma^{k_i - 1}(a_i))$. □

**Remarque 8.2.2.** Le théorème 8.2.1 donne une méthode algorithmique pour effectuer cette décomposition. Voyons cela sur un exemple :
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 3 & 1 & 7 & 6 & 5 & 2 & 8 & 10 & 9 \end{pmatrix}$$
On part de 1 et on applique successivement $\sigma$ pour obtenir $O_1$ et donc le premier cycle $c_1$ : $1 \to 4 \to 7 \to 2 \to 3 \to 1$, donc $c_1 = (1, 4, 7, 2, 3)$. On recommence en partant d'un élément qui n'a pas été visité : $5 \to 6 \to 5$ ; puis $8 \to 8$ et $9 \to 10 \to 9$ qui donnent :
$$\sigma = (1, 4, 7, 2, 3)(5, 6)(9, 10).$$

**Exemple 8.2.3.** Une application de la décomposition en cycles disjoints du théorème 8.2.1 : calcul de $\sigma^N$. Prenons la permutation $\sigma$ de l'exmple précédent, avec $N = 1145$. Parce que les cycles à supports disjoints commutent,

$$\sigma^{1145} = (1, 4, 7, 2, 3)^{1145}(5, 6)^{1145}(9, 10)^{1145}.$$

Il suffit maintenant de réduire les exposants modulo les longueurs respectives des cycles, ce qui donne

$$\sigma^{1145} = (1, 4, 7, 2, 3)^0(5, 6)^1(9, 10)^1 = (5, 6)(9, 10).$$

**Corollaire 8.2.4.** Soit $\sigma = c_1 \dots c_s$ la décomposition en produits de cycles disjoints de $\sigma$, avec $\ell_i := \ell(c_i)$ ordonnés par ordre décroissant.

1. L'ordre de $\sigma$ est le ppcm de $\ell_1, \dots, \ell_s$.
2. Deux permutations sont conjuguées dans $S_n$ si et seulement si elles ont le même $(\ell_1, \dots, \ell_s)$.

*Démonstration.* On a déjà vu que $\sigma^k = c_1^k \dots c_s^k$. Comme les supports des $c_i$ sont disjoints, $\sigma^k = 1$ si et seulement si $c_i^k = 1$ pour tout $i = 1, \dots, s$. Comme l'ordre de $c_i$ vaut $\ell_i$, $c_i^k = 1$ si et seulement si $\ell_i$ divise $k$. Finalement, on a démontré que $\sigma^k = 1$ si et seulement si $\mathrm{ppcm}(\ell_1, \dots, \ell_s)$ divise $k$ donc l'ordre de $\sigma$ est bien $\mathrm{ppcm}(\ell_1, \dots, \ell_s)$.

Soit $\sigma$ et $\sigma'$ deux permutations conjuguées dans $S_n$. Il existe donc $\tau \in S_n$ tel que $\sigma' = \tau\sigma\tau^{-1}$. Avec les notations du théorème, on en déduit que

$$\begin{aligned}\sigma' = \tau\sigma\tau^{-1} &= \tau c_1 \dots c_s \tau^{-1} \\ &= (\tau c_1 \tau^{-1})(\tau c_2 \tau^{-1}) \dots (\tau c_s \tau^{-1}).\end{aligned}$$

D'après la proposition 8.1.3, $c_i' := \tau c_i \tau^{-1}$ est un cycle de même longueur que $c_i$ et de support $\tau(\mathrm{Sup}(c_i))$. Donc $\sigma' = c_1' \dots c_s'$ est son unique décomposition en produit de cycles disjoints. Si $\ell_i' := \ell(c_i')$, on a donc $(\ell_1, \dots, \ell_s) = (\ell_1', \dots, \ell_s')$.

Réciproquement, supposons que $\sigma$ et $\sigma'$ soient deux permutations dont les decómpositions en produit de cycles disjoints $\sigma = \prod_{i-1}^{s} c_i$ et $\sigma' = \prod_{i=1}^{s} c_i'$ vérifient $\ell(c_i) = \ell(c_i') =: \ell_i$. Alors, on peut construire une permutation $\tau$ telle que $c_i = (a_{i,1}, \dots, a_{i,\ell_i})$, $c_i' = (b_{i,1}, \dots, b_{i,ell_i})$, et $\tau(a_{i,j}) = b_{i,j}$. On vérifie que $\sigma' = \tau\sigma\tau^{-1}$. Donc $\sigma$ et $\sigma'$ sont conjuguées. □

## 8.3 Autres décompositions des permutations

**Théorème 8.3.1.** On a :

1. $c = (a_1, \dots, a_p) = (a_1, a_2)(a_2, a_3) \dots (a_{p-1}, a_p)$.
2. Toute permutation est un produit de transpositions.

*Démonstration.* 1. se vérifie directement, et 2. se démontre avec le théorème 8.2.1. □

**Théorème 8.3.2.** Les ensembles suivants sont générateurs de $S_n$ :

1. L'ensemble des transpositions
2. $\{(1, 2), (1, 3), \dots, (1, k), \dots, (1, n)\}$
3. $\{(1, 2), (2, 3), \dots, (k - 1, k), \dots, (n - 1, n)\}$
4. $\{(1, 2), (1, 2, 3, \dots, n)\}$

*Démonstration.* 1. C'est le théorème 8.3.1.

2. On a $(i,j) = (1,i)(1,j)(1,i)$.
3. On a $(1,i+1) = (1,i)(i,i+1)(1,i)$.
4. Soit $c = (1,2,\dots)$ ; $c(1,2)c^{-1} = (2,3)$, etc..

$\square$

## 8.4 La signature

**Définition 8.4.1.** Soit $\sigma \in S_n$. Le *nombre d'inversions de* $\sigma$, est le nombre

$$i(\sigma) := |\{(i,j) : 1 \leq i < j \leq n \text{ et } \sigma(i) > \sigma(j)\}$$

La *signature de sigma* est définie par :

$$\epsilon(\sigma) = (-1)^{i(\sigma)}.$$

**Proposition 8.4.2.**

$$\epsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

**Théorème 8.4.3.** Pour toutes permutations $\sigma, \sigma' \in S_n$,

$$\epsilon(\sigma\sigma') = \epsilon(\sigma)\epsilon(\sigma').$$

Autrement dit, l'application :

$$\begin{aligned} \epsilon : S_n &\to \{-1, 1\} \\ \sigma &\mapsto \epsilon(\sigma) \end{aligned}$$

est un homomorphisme de groupes.

*Démonstration.* On calcule $\epsilon(\sigma\sigma')$ avec la formule de la proposition 8.4.2 :

$$\begin{aligned} \epsilon(\sigma\sigma') &= \prod_{1 \leq i < j \leq n} \frac{\sigma\sigma'(i) - \sigma\sigma'(j)}{i - j} \\ &= \prod_{1 \leq i < j \leq n} \Big(\frac{\sigma\sigma'(i) - \sigma\sigma'(j)}{\sigma'(i) - \sigma'(j)}\Big)\Big(\frac{\sigma'(i) - \sigma'(j)}{i - j}\Big) \\ &= \prod_{1 \leq i < j \leq n} \frac{\sigma\sigma'(i) - \sigma\sigma'(j)}{\sigma'(i) - \sigma'(j)} \prod_{1 \leq i < j \leq n} \frac{\sigma'(i) - \sigma'(j)}{i - j}. \end{aligned}$$

On remarque que, en posant $i' = \sigma'(i)$ et $j' = \sigma'(j)$, on a

$$\frac{\sigma\sigma'(i) - \sigma\sigma'(j)}{\sigma'(i) - \sigma'(j)} = \frac{\sigma(i') - \sigma(j')}{i' - j'} = \frac{\sigma(j') - \sigma(i')}{j' - i'}$$

donc

$$\epsilon(\sigma\sigma') = \prod_{1 \leq i' < j' \leq n} \frac{\sigma(i') - \sigma(j')}{i' - j'} \prod_{1 \leq i < j \leq n} \frac{\sigma'(i) - \sigma'(j)}{i - j} = \epsilon(\sigma)\epsilon(\sigma').$$

$\square$

**Corollaire 8.4.4.** Si $c$ est un cycle de longueur $\ell$,

$$\epsilon(c) = (-1)^{\ell-1}.$$

*Démonstration.* On vérifie que $\epsilon((i,j)) = -1$ et on utilise le théorème 8.3.1 1. $\square$

**Corollaire 8.4.5.** L'ensemble des permutations de signature $+1$ est un sous-groupe distingué de $S_n$, d'indice 2 dans $S_n$, appelé *le groupe alterné* et noté $A_n$.

*Démonstration.* Par définition, $A_n = \mathrm{Ker}(\epsilon)$ donc $A_n$ est un sous-groupe distingué de $S_n$. De plus, le théorème de factorisation des groupes montre que $S_n/A_n \simeq \{-1,1\}$ qui est d'ordre 2. $\square$

# Chapitre 9

# Anneaux

## 9.1 Définitions

**Définition 9.1.1.** Un *anneau* $(A, +, \cdot)$ est un ensemble muni de deux lois de composition interne $+$ et $\cdot$ telles que :

1. $(A, +)$ est un groupe commutatif de neutre noté 0 et appelé *zéro*.
2. La loi $\cdot$ vérifie :
   (a) Elle est associative : $(x \cdot y) \cdot x = x \cdot (y \cdot z)$ pour tout $x, y, z \in A$.
   (b) Elle possède un élément neutre noté 1 et appelé *un* ou *unité* : $1 \cdot x = x \cdot 1 = x$ pour tout $x \in A$.
3. La loi $\cdot$ est distributive sur l'addition $+$ : pour tout $x, y, z \in A$, $x \cdot (y + z) = x \cdot y + x \cdot z$ et $(x + y) \cdot z = x \cdot z + y \cdot z$.

Si en outre la loi $\cdot$ est commutative, on dit que $A$ est un *anneau commutatif.*

**Remarque 9.1.2.** On a : $0 \cdot x = x \cdot 0 = 0$ pour tout $x \in A$. En effet,

$$0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x \Longrightarrow 0 \cdot x = 0.$$

Également, on montre que $(-x) \cdot y = -(x \cdot y)$ car :

$$x \cdot y + (-x) \cdot y = (x + (-x)) \cdot y = 0 \cdot y = 0.$$

**Notation.** L'opposé de $x$ pour $+$ est noté $-x$. Désormais on note $x \cdot y = xy$.

**Définition 9.1.3.** Soit $(A, +, \cdot)$ un anneau. Un élément $x \in A$ est appelé *un inversible* (ou une unité) de $A$ s'il est inversible pour $\cdot$, c'est-à-dire s'il existe $y \in A$ tel que $xy = yx = 1$. On note $y = x^{-1}$. L'ensemble des inversibles de $A$ est noté $A^*$.

**Proposition 9.1.4.** $(A^*, \cdot)$ est un groupe appelé le groupe des inversibles (ou le groupe des unités) de $A$. On a $A^* \subset A \setminus \{0\}$. Si $A$ est commutatif et si $A^* = A \setminus \{0\}$, c'est-à-dire si tout élément non nul de $A$ est inversible, on dit que $A$ *est un corps.*

*Démonstration.* La loi $\cdot$ est bien interne dans $A^*$ : si $x, y \in A^*$ alors $xy$ est inversible d'inverse $y^{-1}x^{-1}$. On a $1 \in A^*$ car 1 est inversible : $1 \cdot 1 = 1$. Par définition, tout élément $x \in A^*$ est inversible, et son inverse $x^{-1}$ est aussi dans $A^*$ puisque il est inversible d'inverse $x$.

On a vu que $0x = 0$ donc 0 n'est jamais inversible, d'où l'inclusion $A^* \subset A \setminus \{0\}$. $\square$

**Définition 9.1.5.** Un *diviseur de zéro* d'un anneau $A$ est un élément $x \in A$ tel que : $x \neq 0$ et il existe $y \neq 0$, $y \in A$, avec $xy = 0$ ou $yx = 0$. Un anneau $A$ sans diviseur de zéro s'appelle un *anneau intègre.*

**Remarque 9.1.6.** Si $x \in A^*$ alors $x$ n'est pas un diviseur de zéro de $A$. En effet, si $xy = 0$, en multipliant à gauche par $x^{-1}$, on obtient $y = 0$.

## 9.2 Exemples d'anneaux

**Exemple 9.2.1.** Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux commutatifs et intègres, pour les opérations d'addition et de multiplication usuelles. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps.

**Exemple 9.2.2.** $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau. Son groupe des unités est $(\mathbb{Z}/n\mathbb{Z})^*$, d'ordre $\varphi(n)$. $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n$ est premier. Si $n$ n'est pas premier, les éléments non nuls et non inversibles, c'est-à-dire les $a \bmod n$ tels que $\mathrm{pgcd}(a, n) > 1$, sont tous diviseurs de zéro.

**Exemple 9.2.3.** Si $A$ est un anneau commutatif, l'ensemble $M_n(A)$ des matrices carrées de taille $n$ est un anneau de zéro la matrice dont tous les coefficients font 0 et de 1 la matrice identité $\mathrm{Id}_n$. Si $n \geq 2$ il n'est pas commutatif et possède des diviseurs de zéros. Les inversibles sont les matrices $M$ dont le déterminant est un inversible dans $A$. Leur ensemble est noté $\mathrm{GL}_n(A)$.

$$\mathrm{GL}_n(A) = \{M \in M_n(A) : \det(M) \in A^*\}.$$

**Exemple 9.2.4.** Si $A$ est un anneau commutatif, l'ensemble $A[X]$ des polynômes à coefficients dans $A$ est un anneau commutatif.

$$A[X] = \{P(X) = \sum_{k=0}^{n} a_k X^k : n \geq 0, (a_0, \dots, a_n) \in A^{n+1}\}.$$

Les opérations d'addition et de multiplication sont définies, pour $P(X) = \sum_{k=0}^{n} a_k X^k$ et $Q(X) = \sum_{k=0}^{n} b_k X^k$, par :

$$(P + Q)(X) = \sum_{k=0}^{n} (a_k + b_k) X^k$$

et

$$PQ(X) = \sum_{k=0}^{2n} c_k X^k, \quad c_k = \sum_{\substack{0 \leq i \leq n \\ 0 \leq j \leq n \\ i+j=k}} a_i b_j.$$

Le zéro de $A[X]$ est $P = 0_A$, le neutre pour la multiplication est $P = 1_A$.

**Exemple 9.2.5.** L'anneau des polynômes à $n$ indéterminées $A[X_1, \dots, X_n]$ et à coefficients dans un anneau commutatif $A$ généralise l'exemple précédent. Il peut être construit récursivement : $A[x_1, \dots, X_n] = (A[X_1, \dots, X_{n-1}])[X_n]$.

On résume les propriétés de ces anneaux dans le tableau suivant :

| $A$ | $A^*$ | diviseurs de zéro | commutatif | intègre | corps |
|---|---|---|---|---|---|
| $\mathbb{Z}$ | $\{-1,1\}$ | $\emptyset$ | oui | oui | non |
| $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ | $K \setminus \{0\}$ | $\emptyset$ | oui | oui | oui |
| $\mathbb{Z}/n\mathbb{Z}$ | $\{a \bmod n :$ $\mathrm{pgcd}(a,n) = 1\}$ | $\{a \neq 0 \bmod n :$ $\mathrm{pgcd}(a,n) > 1\}$ | oui | ssi $n$ premier | ssi $n$ premier |
| $M_n(K), n \geq 2$ $K$ corps | $\mathrm{GL}_n(K) =$ $\{M : \det(M) \neq 0\}$ | $\{M \neq 0 :$ $\det(M) = 0\}$ | non | non | non |
| $K[X_1, \ldots, X_n]$ $K$ corps | $K^*$ | $\emptyset$ | oui | oui | non |

## 9.3 Sous-anneaux, produits directs et morphismes

Désormais, on suppose tous les anneaux commutatifs. On introduit les notions classiques de sous-structures, produit et morphismes.

**Définition 9.3.1.** Un sous-anneau $B$ d'un anneau commutatif $(A, +, \cdot)$ est un sous-ensemble de $A$ qui est un anneau pour les mêmes lois, et qui contient $1_A$.

**Proposition 9.3.2.** $B \subset A$ est un sous-anneau de $A$ s'il vérifie les conditions suivantes :

1. $1_A \in B$
2. Pour tout $x, y \in B$, $x - y \in B$
3. Pour tout $x, y \in B$, $xy \in B$

*Démonstration.* Les conditions 1. et 2. garantissent que $(B, +)$ est un sous-groupe de $(A, +)$ d'après la proposition 2.2.2, et la condition 3. que la mutiplication est une loi de composition interne pour $B$. Comme $1_A \in B$, la multiplication possède bien un élément neutre dans $B$. Les autres propriétés définissant un anneau sont vraies pour $A$ donc aussi pour $B$. □

**Proposition 9.3.3.** Si $(A, +, \cdot)$ et $(B, \star, *)$ sont des anneaux, le produit direct $A \times B$ est un anneau pour les lois :

$$(x, y) \oplus (x', y') = (x + x', y \star y')$$
$$(x, y) \odot (x', y') = (x \cdot x', y * y').$$

Son zéro est $(0_A, 0_B)$ et son élément unité est $(1_A, 1_B)$.

*Démonstration.* Laissée au lecteur. □

**Remarque 9.3.4.** Pour simplifier les notations, on garde le plus souvent les mêmes notations $+$ et $\cdot$ pour les lois de tous les anneaux.

**Définition 9.3.5.** Un morphisme de l'anneau $(A, +, \cdot)$ sur l'anneau $(B, +, \cdot)$ est une application $f : A \to B$ vérifiant :

1. $f(1_A) = 1_B$,
2. Pour tout $x, y \in A$, $f(x + y) = f(x) + f(y)$,
3. Pour tout $x, y \in A$, $f(xy) = f(x)f(y)$.

Son noyau $\mathrm{Ker}(f)$ et son image $\mathrm{Im}(f)$ sont définis respectivement par :

$$\mathrm{Ker}(f) = \{x \in A : f(x) = 0_B\} \qquad \mathrm{Im}(f) = \{f(x) : x \in A\} \subset B.$$

**Remarque 9.3.6.** Un morphisme d'anneaux $f : A \to B$ est en particulier un morphisme des groupes additifs. Il vérifie donc $f(0_A) = 0_B$ et $f(-x) = -f(x)$. Si $x$ est inversible dans $A$, $f(x)$ l'est aussi : en effet, de la relation $xy = 1_A$ on déduit $f(x)f(y) = f(1_A) = 1_B$. En outre, $f(x^{-1}) = f(x)^{-1}$.

**Exemple 9.3.7.** L'application $f : A \times B \to A$ définie par $f(x, y) = x$ est un morphisme d'anneaux surjectif et de noyau $\{0\} \times B$.

**Proposition 9.3.8.** Si $f : A \to B$ est un morphisme d'anneaux, l'image $\mathrm{Im}(f)$ de $f$ est un sous-anneau de $B$.

*Démonstration.* C'est immédiat en appliquant la proposition 9.3.2. □

**Remarque 9.3.9.** Le noyau $\mathrm{Ker}(f)$ n'est pas un sous-anneau de $A$ car il ne contient pas $1_A$. En effet, cela signifierait que $f(1_A) = 0_B$. On verra au prochain chapitre que c'est un *idéal* de $A$.

# Chapitre 10

# Idéaux, anneaux quotients

Dans ce chapitre, **tous les anneaux sont commutatifs**.

## 10.1 Idéaux

**Définition 10.1.1.** Un sous-ensemble $I \subset A$ est un *idéal* de $A$ si :

1. $(I, +)$ est un sous-groupe de $(A, +)$.
2. Pour tout $x \in I$, et tout $a \in A$, $ax \in I$.

**Exemple 10.1.2.** $\{0\}$ et $A$ sont des idéaux de $A$.

**Proposition 10.1.3.** Soit $I$ un idéal de $A$. Alors $I$ contient un élément inversible de $A$ si et seulement si $I = A$. En particulier, si $A$ est un corps, ses seuls idéaux sont $\{0\}$ et $A$.

*Démonstration.* La condition est clairement nécessaire puisque, si $I = A$, $1 \in I$. Réciproquement, si $x \in I \cap A^*$, alors, en prenant $a = x^{-1}$ dans la définition d'un idéal, $I$ contient $x^{-1}x = 1$ donc $y \cdot 1 = y$ pour tout $y \in A$. □

**Exemple 10.1.4.** Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$. En effet, on a déjà vu que les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$. Si $x \in n\mathbb{Z}$, c'est-à-dire $x = nq$ pour un $q \in \mathbb{Z}$, et si $a \in \mathbb{Z}$, alors $ax = naq \in n\mathbb{Z}$.

**Exemple 10.1.5.** Si $A$ est un anneau, et si $x \in A$, l'ensemble

$$I = Ax = \{ax : a \in A\}$$

est un idéal de $A$. En effet :

- $0 \in I$ et, si $y = ax \in I$ et $y' = a'x \in I$, $y - y' = ax - a'x = (a - a')x \in I$. Donc $(I, +)$ est bien un sous-groupe de $(A, +)$.
- Si $y = ax \in I$ et si $b \in A$, $by = bax = (ba)x \in I$.

On dit que $I$ *est un idéal principal.*

**Proposition 10.1.6.** Si $f : A \to B$ est un morphisme d'anneaux, alors

$$\mathrm{Ker}(f) = \{x \in A : f(x) = 0\}$$

est un idéal de $A$.

*Démonstration.* Comme $f$ est un homomorphisme d'anneaux, c'est en particulier un homomorphisme des groupes additifs. Donc on sait que $\mathrm{Ker}(f)$ est un sous-groupe de $A$. Soit $x \in \mathrm{Ker}(f)$ et $a \in A$ ; montrons que $ax \in \mathrm{Ker}(f)$. En effet, $f(ax) = f(a)f(x) = f(a) \cdot 0 = 0$ donc $ax \in \mathrm{Ker}(f)$. □

**Définition et Proposition 10.1.7.** Soit $A$ un anneau et $I$ et $J$ deux idéaux de $A$.

1. La somme $I + J$ de $I$ et $J$ est définie par :
$$I + J = \{x + y : x \in I, y \in J\}$$
2. Le produit $IJ$ de $I$ et $J$ est défini par :
$$IJ = \{\sum_{finie} xy : x \in I, y \in J\}$$
3. L'intersection $I \cap J$ est l'intersection usuelle des ensembles.

Alors $I + J$, $IJ$ et $I \cap J$ sont des idéaux de $A$. En outre $IJ \subset I \cap J$, $I \cap J$ est le plus grand idéal de $A$ contenu dans $I$ et $J$, et $I + J$ est le plus petit idéal de $A$ contenant $I$ et $J$.

4. Si $S$ est une partie de $A$, on note $(S)$ le plus petit idéal de $A$ contenant $S$. On l'appelle *l'idéal engendré par* $S$. Si $S = \{x_1, \dots, x_s\}$,
$$(S) = (x_1, \dots, x_s) = Ax_1 + \cdots + Ax_s.$$

*Démonstration.* Immédiat à partir de la définition d'un idéal. □

## 10.2 Idéaux principaux, anneaux principaux

**Définition 10.2.1.** Un *idéal principal* d'un anneau $A$ est un idéal de la forme :
$$I = Ax = \{ax : a \in A\}.$$
On dit que $x$ est *un générateur* de $I$. On note aussi $I = (x)$.

Un anneau commutatif et intègre dont tous les idéaux sont principaux est appelé un *anneau principal*.

**Exemple 10.2.2.** $\mathbb{Z}$ est un anneau principal.

**Exercice 10.1.** Montrez que, si $I = Ax$ est principal, les générateurs de $I$ sont les $ux$ avec $u \in A^*$.

**Remarque 10.2.3.** Les propriétés arithmétiques de $\mathbb{Z}$ s'étendent à un anneau $A$ principal, et donc en particulier à $K[X]$, où $K$ est un corps :

- Si $x, y \in A$, le pgcd de $x$ et $y$ est par définition un générateur de l'idéal $Ax + Ay$. Il est défini à la multiplication près par une unité de $A$. Dans le cas $A = K[X]$, on le choisit unitaire, c'est-à-dire de coefficient dominant 1, il est ainsi uniquement défini.
- On obtient par construction le théorème de Bezout : il existe $u$ et $v$ tels que $\mathrm{pgcd}(x, y) = xu + yv$.
- Le ppcm de $x$ et $y$ est par définition un générateur de $Ax \cap Ay$. Dans le cas $A = K[X]$, on le choisit unitaire.

– On a $\operatorname{pgcd}(x, y) \operatorname{ppcm}(x, y) = xy$.
– La relation de divisibilité : $x \mid y$ s'il existe $q$ tel que $y = qx$, est équivalente à la condition : $Ay \subset Ax$.
– La notion de nombre premier s'étend aussi : on parle d'irréductible d'un anneau pour un élément non inversible dont les seuls diviseurs sont 1 et lui-même, aux inversibles près. Alors, tout élément est le produit de façon essentiellement unique d'irréductibles de $A$.

**Exercice 10.2.** Faire la liste des polynômes irréductibles de $\mathbb{Z}/2\mathbb{Z}[X]$ de degrés $1, 2, 3, 4$. Même question pour $\mathbb{Z}/3\mathbb{Z}[X]$.

## 10.3 Quotient d'un anneau par un idéal

Soit $A$ un anneau et $I$ un idéal de $A$. Comme $(A, +)$ est un groupe commutatif, et que $I$ est un sous-groupe de ce groupe, le quotient $A/I$ est muni d'une structure de groupe d'après le chapitre 5. Nous allons voir que $A/I$ est aussi un anneau.

**Théorème 10.3.1.** Soit $A$ un anneau (commutatif) et $I$ un idéal de $A$. La multiplication dans $A/I$ donnée par :

$$(x + I) \cdot (y + I) = xy + I$$

est bien définie et munit le groupe quotient $A/I$ d'une structure d'anneau pour laquelle le zéro est la classe $I$ de $0_A$ et l'unité est la classe $1_A + I$ de l'unité de $A$.

*Démonstration.* Pour montrer que la multiplication est bien définie, il faut montrer qu'elle ne dépend pas du choix des représentants des classes, soit :

$$\text{si} \quad \begin{cases} x + I = x' + I \\ y + I = y' + I \end{cases} \qquad \text{alors} \quad xy + I = x'y' + I.$$

En effet, si $x' = x + a$, $y' = y + b$ avec $a, b \in I$, $x'y' = (x + a)(y + b) = xy + xb + ay + ab$. On remarque que $xb + ay + ab \in I$ grâce à la propriété d'idéal.

On vérifie que $(1_A + I)(x + I) = 1_A \cdot x + I = x + I$ donc $1_A + I$ est bien l'unité de $A/I$. L'associativité et la distributivité se vérifient facilement. □

**Exemple 10.3.2.** Bien sûr, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est le quotient de l'anneau $\mathbb{Z}$ par son idéal $n\mathbb{Z}$.

Sans surprise, on obtient la version "anneaux" du théorème de factorisation :

**Théorème 10.3.3.** Soit $f : A \to B$ un homomorphisme d'anneaux. Il existe un homomorphisme d'anneaux unique $\tilde{f} : A/\operatorname{Ker}(f) \to B$ tel que, pour tout $x \in A$, $\tilde{f}(s(x)) = f(x)$, c'est-à-dire rendant le diagramme suivant commutatif :

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "s"'] & B \\ E/\operatorname{Ker}(f) \arrow[ur, "\tilde{f}"'] & \end{tikzcd}$$

De plus, $\tilde{f}$ est injective et définit un isomorphisme de $A/\operatorname{Ker}(f)$ sur $\operatorname{Im}(f)$.

*Démonstration.* Laissée en exercice. □

## 10.4 Caractéristique d'un anneau

**Définition 10.4.1.** Soit $A$ un anneau (commutatif). La caractéristique de $A$ est le plus petit entier $k \geq 1$, s'il existe, tel que $k \cdot 1 = 0$. Si $k \cdot 1 \neq 0$ pour tout $k \geq 1$, on dit que $A$ est de caractéristique 0. On note $\operatorname{car}(A)$ la caractéristique de $A$.

**Exemple 10.4.2.** Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont de caractéristique 0. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique $n$.

**Proposition 10.4.3.** L'application

$$\begin{aligned} f : \mathbb{Z} &\to A \\ k &\mapsto k \cdot 1 \end{aligned}$$

est un homomorphisme d'anneaux, a pour noyau $\operatorname{car}(A)\mathbb{Z}$, et induit un homomorphisme injectif

$$\tilde{f} : \mathbb{Z}/\operatorname{car}(A)\mathbb{Z} \to A.$$

*Démonstration.* Il est clair que $f$ est un homomorphisme d'anneaux de noyau $\operatorname{car}(A)\mathbb{Z}$. Pour le reste on applique le théorème de factorisation des anneaux. □

**Corollaire 10.4.4.** Si $K$ est un corps, alors soit $\operatorname{car}(K) = 0$ et dans ce cas $K$ est infini, et contient un sous corps isomorphe à $\mathbb{Q}$, soit $\operatorname{car}(K)$ est un nombre premier $p$, et $K$ contient un sous corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

*Démonstration.* Si $K$ est un corps de caractéristique 0, alors d'après la proposition précédente, $K$ contient un sous-anneau isomorphe à $Z$ (l'image de $\tilde{f}$). Mais alors les éléments non nuls de cet anneau sont inversibles dans $K$ ce qui signifie qu'ils sont contenus dans un sous corps isomorphe à $\mathbb{Q}$.

Si la caractéristique de $K$ est un nombre $n > 0$, comme un corps n'a pas de diviseurs de zéro alors que $\mathbb{Z}/n\mathbb{Z}$ a des diviseurs de zéro si $n$ n'est pas premier ou nul, cela oblige $n$ à être premier. □

## 10.5 Idéaux premiers et maximaux

**Définition 10.5.1.** Soit $A$ un anneau (commutatif). Soit $I$ un idéal de $A$.

1. On dit que $I$ est un idéal *premier* si, pour tout $x, y \in A$,

$$xy \in I \Longrightarrow x \in I \text{ ou } y \in I.$$

2. On dit que $I$ est un idéal *maximal* si $I \neq A$ et si $I$ est maximal pour l'inclusion.

**Exemple 10.5.2.** Dans $\mathbb{Z}$, l'idéal $n\mathbb{Z}$ est premier si et seulement si $n = 0$ ou $n$ est premier. Il est maximal ssi $n$ est premier.

**Théorème 10.5.3.** Avec les notations précédentes,

1. $I$ est premier si et seulement si $A/I$ est un anneau intègre.
2. $I$ est maximal si et seulement si $A/I$ est un corps.

*Démonstration.* Soit $s : A \to A/I$ la surjection canonique. 1. La condition définissant un idéal premier peut se reformuler en :

$$s(xy) = 0 \Longrightarrow s(x) = 0 \text{ ou } s(y) = 0.$$

Comme $s(xy) = s(x)s(y)$, et que $s$ est surjective, cela équivaut bien à la propriété d'intégrité de $A/I$.

2. On remarque que les idéaux de $A/I$ sont les $J/I$, avec $J$ un idéal de $A$ contenant $I$. Alors, dire que $I$ est maximal équivaut à dire que $A/I$ ne contient pas d'idéaux non triviaux. On a déjà vu qu'un corps n'a que des idéaux triviaux. Réciproquement, si un anneau $B$ ne contient pas d'idéaux non triviaux, c'est un corps. En effet, si $x \in B$ est non nul, alors l'idéal $Bx = B$ ; en particulier, il existe $y \in B$ tel que $xy = 1$ donc $x$ est inversible. □

**Exemple 10.5.4.** Dans $K[X]$, les idéaux premiers sont $\{0\}$ et $(P(X))$ avec $P(X)$ irréductible. Ces derniers sont aussi maximaux.

## 10.6 Anneaux non commutatifs

On a supposé dans tout ce chapitre que les anneaux considérés sont commutatifs. Dans le cas non commutatif, quelques nuances s'imposent : on distingue *idéaux à gauche* et *idéaux à droite*, vérifiant respectivement $a \in A, x \in I \Longrightarrow ax \in I$ et $a \in A, x \in I \Longrightarrow xa \in I$. Un idéal à droite et à gauche est appelé un *idéal bilatère*. Le quotient $A/I$ est muni d'une structure d'anneau seulement si l'idéal est bilatère.

**Exemple 10.6.1.** Dans $M_n(K)$, les seuls idéaux bilatères sont $\{0\}$ et $M_n(K)$. Par contre, il existe des idéaux non triviaux : par exemple, si $V$ est un sous-espace vectoriel de $K^n$ non trivial,

$$I_V := \{M : xM = 0 \text{ pour tout } x \in V\},$$

est un idéal à droite.

# Chapitre 11

# Introduction aux corps finis

## 11.1 Polynômes à une indéterminée

Soit $K$ un corps, dans cette partie on rappelle les propriétés de l'anneau $(K[X], +, \cdot)$. Ces propriétés vous sont déjà connues lorsque $K = \mathbb{R}, \mathbb{C}$ et s'étendent à un corps quelconque. On a déjà rencontré d'autres corps que $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, avec les quotients $\mathbb{Z}/p\mathbb{Z}$ où $p$ est un nombre premier. On rencontrera encore de nouveaux corps dans ce chapitre.

On définit le *degré* de $P(X) \in K[X]$ par : $\deg(P) = -\infty$ si $P = 0$, et $\deg(P) = d$ si $P = \sum_{k=0}^{d} a_k X^k$ avec $a_d \neq 0$. Le coefficient $a_d$ est le *coefficient dominant* de $P$. Si $a_d = 1$, on dit que le polynôme $P$ est *unitaire*. On a les propriétés : $\deg(AB) = \deg(A) + \deg(B)$ et $\deg(A + B) \leq \max(\deg(A), \deg(B))$ (avec égalité si $\deg(A) \neq \deg(B)$).

**Proposition 11.1.1.** $K[X]^* = K^*$.

*Démonstration.* Clairement $K^* \subset K[X]^*$. Réciproquement, supposons $A(X)B(X) = 1$. Alors d'après les propriétés du degré rappelées ci-dessus, $\deg(A) + \deg(B) = 0$ ce qui implique $\deg(A) = \deg(B) = 0$. □

L'anneau $K[X]$ est muni d'une *division euclidienne* : pour tout polynômes $A(X)$, $B(X) \neq 0 \in K[X]$, il existe $Q(X)$ et $R(X)$ uniques tels que

$$A(X) = B(X)Q(X) + R(X)$$

avec $\deg(R) < \deg(B)$.

**Exemple 11.1.2.** Si $B(X) = X - b$ alors la division de $A$ par $B$ s'écrit :

$$A(X) = (X - b)Q(X) + A(b).$$

L'anneau $K[X]$ partage avec $\mathbb{Z}$ beaucoup de propriétés, du fait de cette division euclidienne. En particulier c'est un anneau principal :

**Théorème 11.1.3.** Si $K$ est un corps, $K[X]$ est un anneau principal.

*Démonstration.* Pour montrer qu'un idéal $I$ de $K[X]$ est principal, on exploite la division euclidienne, comme on l'a fait pour $\mathbb{Z}$. Soit $P \in I$, un polynôme non nul et de degré minimal. Soit $A \in I$. Effectuons la division euclidienne de $A$ par $P$ : il existe donc $Q$ et $R$ tels que $A = PQ + R$, avec $\deg(R) < \deg(P)$. Alors, $R = A - PQ \in I$ ; comme on a pris $P$ de degré minimal parmi les polynômes non nuls de $I$, nécessairement $R = 0$. □

**Notation.** Pour alléger les notations, on écrit $(P(X))$ pour l'idéal principal $K[X]P(X)$.

La notion de nombres premiers est remplacée dans $K[X]$ par celle de *polynôme irréductible* :

**Définition 11.1.4.** Un polynôme $P(X) \in K[X]$ de degré $\deg(P) \geq 1$ est dit *irréductible* s'il n'existe pas de polynômes $A(X)$ et $B(X)$ avec $\deg(A) \geq 1$ et $\deg(B) \geq 1$ tels que $P(X) = A(X)B(X)$.

**Remarque 11.1.5.**

1. Noter l'importance des conditions $\deg(A) \geq 1$ et $\deg(B) \geq 1$. En effet, on peut toujours factoriser un polynôme $P$ par un polynôme constant.
2. Il est important de préciser sur quel corps on se place. Par exemple, $X^2+1$ est irréductible dans $\mathbb{R}[X]$ mais $X^2 + 1 = (X + i)(X - i)$ n'est pas irréductible dans $\mathbb{C}[X]$.
3. Si $P$ est irréductible dans $K[X]$ alors il n'a pas de racines dans $K$. En effet, si $a$ est une racine de $P$ alors, d'après l'exemple 11.1.2, $P(X) = (X - a)Q(X)$. Mais attention, la réciproque est fausse, et en particulier il ne suffit pas, pour montrer qu'un polynôme est irréductible dans $K[X]$, de montrer qu'il n'a pas de racines dans $K$. Par exemple, $(X^2 + 1)^2$ n'a pas de racines dans $\mathbb{R}$ et pourtant il n'est pas irréductible.

**Exemple 11.1.6.** Les polynômes irréductibles de degré au plus 2 de $\mathbb{Z}/2\mathbb{Z}[X]$ sont : $X$, $X+1$, $X^2 + X + 1$.

De la même manière qu'un entier se factorise de façon unique comme produit de puissances de nombres premiers, on a :

**Théorème 11.1.7.** Tout polynôme $P(X) \in K[X]$, $P(X) \neq 0$, s'écrit de façon unique sous la forme :

$$P(X) = \lambda P_1(X)^{e_1} \dots P_r(X)^{e_r}$$

où $\lambda \in K^*$, $P_1, \dots, P_r$ sont des polynômes irréductibles et unitaires, et $e_1 \geq 1, \dots, e_r \geq 1$.

## 11.2 Le quotient $K[X]/(P(X))$

**Proposition 11.2.1.** Soit $P(X) \in K[X]$ un polynôme de degré $d$. Tout polynôme $A(X) \in K[X]$ a un représentant unique dans le quotient $K[X]/(P(X))$ de degré inférieur ou égal à $d - 1$, qui est son reste dans la division par $P(X)$.

*Démonstration.* Soit $A(X) = P(X)Q(X) + R(X)$, $\deg(R) < d$, la division euclidienne de $A$ par $P$. On a bien : $A(X) - R(X) = P(X)Q(X) \in (P(X))$. Réciproquement, si $A(X)$ a pour représentant $R'(X)$ avec $\deg(R') < d$ c'est bien qu'il existe $Q'$ tel que $A = PQ' + R'$ mais alors par unicité de la division euclidienne, $Q = Q'$ et $R = R'$. □

**Notation.** Dans la situation ci-dessus, on note : $A(X) = R(X) \bmod P(X)$.

D'après la proposition précédente, si $\deg(P) = d$,

$$K[X]/(P(X)) = \{a_0 + a_1X + \cdots + a_{d-1}X^{d-1} \bmod P(X),\ (a_0, \dots, a_{d-1}) \in K^d\}.$$

Précisons comment les opérations dans le quotient $K[X]/(P(X))$ se calculent dans cette représentation : soit $A(X) = a_0 + a_1X + \cdots + a_{d-1}X^{d-1} \bmod P(X)$ et $B(X) = b_0 + b_1X + \cdots + b_{d-1}X^{d-1} \bmod P(X)$. Alors la somme se calcule simplement :

$$A(X) + B(X) = (a_0 + b_0) + \cdots + (a_{d-1} + b_{d-1})X^{d-1} \bmod P(X).$$

Pour le produit, on calcule $A(X)B(X)$ dans $K[X]$, puis on calcule le reste de ce polynôme dans la division par $P(X)$. Prenons un exemple : dans $\mathbb{Z}/2\mathbb{Z}[X]/(X^2+X+1)$, soit $A(X)=X$ et $B(X) = X+1$. On a $A(X)B(X) = X(X+1) = X^2+X = (X^2+X+1)+1$ donc $A(X)B(X) = 1 \bmod (X^2+X+1)$.

Pour décider si un polynôme $A(X)$ est inversible dans $K[X]/(P(X))$, on fait comme dans $\mathbb{Z}/n\mathbb{Z}$ :

**Proposition 11.2.2.** *$A(X)$ est inversible dans $K[X]/(P(X))$ si et seulement si $A(X)$ est premier avec $P(X)$, et dans ce cas, son inverse est donné par une relation de Bezout : il existe $U(X)$ et $V(X)$ tels que $A(X)U(X) + P(X)V(X) = 1$ et l'inverse de $A(X) \bmod P(X)$ est $U(X) \bmod P(X)$.*

**Remarque 11.2.3.** Rappelons qu'on calcule algorithmiquement une relation de Bezout entre $A(X)$ et $B(X)$ à l'aide de *l'algorithme d'Euclide étendu*.

On en déduit le théorème :

**Théorème 11.2.4.** *L'anneau $K[X]/(P(X))$ est un corps si et seulement si $P(X)$ est un polynôme irréductible de $K[X]$.*

*Démonstration.* En effet, si $P$ est irréductible alors tout polynôme de degré compris entre 1 et $d-1$ est premier avec $P$. □

## 11.3 Introduction aux corps finis

On a vu avec le théorème 11.2.4 une façon de construire des corps finis : en effet, il suffit de prendre pour corps de base $\mathbb{Z}/p\mathbb{Z}$ avec $p$ premier, et $P(X)$ un polynôme irréductible de $\mathbb{Z}/p\mathbb{Z}[X]$. Alors le quotient $\mathbb{Z}/p\mathbb{Z}[X]/(P(X))$ est un corps fini, dont on résume les propriétés dans la proposition suivante :

**Proposition 11.3.1.** *Soit $p$ un nombre premier, et $P(X)$ un polynôme irréductible de $\mathbb{Z}/p\mathbb{Z}[X]$, de degré $d \geq 1$. Alors le quotient $\mathbb{Z}/p\mathbb{Z}[X]/(P(X))$ est un corps fini à $p^d$ éléments. Son groupe multiplicatif est un groupe fini d'ordre $p^d-1$.*

*Démonstration.* On a vu que

$$\mathbb{Z}/p\mathbb{Z}[X]/(P(X)) = \{a_0 + a_1X + \cdots + a_{d-1}X^{d-1} \bmod P(X),\ (a_0, \ldots, a_{d-1}) \in (\mathbb{Z}/p\mathbb{Z})^d\}.$$

Il y a donc exactement $p^d$ valeurs possibles pour le $d$-uplet $(a_0, \ldots, a_{d-1})$. □

**Exercice 11.1.** Construire un corps fini à 16 éléments en prenant $K = \mathbb{Z}/2\mathbb{Z}$ et $P = X^4+X+1$. Montrez que $\alpha = X \bmod P$ est d'ordre 15 dans son groupe multiplicatif. En déduire que celui-ci est cyclique.

Il y a maintenant deux questions naturelles à propos des corps finis : d'une part, peut-on construire des corps finis avec un nombre d'éléments qui ne soit pas égal à une puissance d'un nombre premier ? Nous allons répondre par la négative dans le prochain théorème. D'autre part, étant donnés $p$ et $d$, combien y a-t-il, à isomorphisme près, de corps fini à $p^d$ éléments ? La réponse est : il y en a un et un seul, et il est de la forme $\mathbb{Z}/p\mathbb{Z}[X]/(P(X))$ avec $P$ irréductible de degré $d$, mais nous ne le démontrerons pas ici.

**Théorème 11.3.2.** Si $K$ est un corps fini, alors il existe un nombre premier $p$ et un entier $d \geq 1$ tel que son cardinal soit égal à $p^d$.

*Démonstration.* Pour démontrer ce résultat, nous faisons appel aux outils de l'algébre linéaire. Tout d'abord, nous savons que la caractéristique de $K$ est un nombre premier $p$ et que $K$ contient un sous-corps $k$ isomorphe à $\mathbb{Z}/p\mathbb{Z}$ (Corollaire 10.4.4). Il est facile de voir que la multiplication dans $K$ induit une structure de $k$-espace vectoriel sur $K$. Comme $K$ est fini, il est à fortiori de dimension finie sur $k$. Soit $d$ sa dimension ; alors il existe une base $e_1, \ldots, e_d$ de $K$ sur $k$ et $K = \{\lambda_1 e_1 + \cdots + \lambda_d e_d \ : \ (\lambda_1, \ldots, \lambda_d) \in (\mathbb{Z}/p\mathbb{Z})^d\}$. Le $d$-uplet $(\lambda_1, \ldots, \lambda_d)$ peut prendre exactement $p^d$ valeurs et chaque valeur correspond à un unique élément de $K$ donc $K$ est de cardinal $p^d$. □

Nous concluons ce chapitre par un résultat décrivant la structure du groupe multiplicatif d'un corps fini.

**Théorème 11.3.3.** Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique. En particulier, le groupe multiplicatif d'un corps fini est cyclique.

*Démonstration.* Soit $K$ un corps et soit $G \subset K^*$ un sous-groupe fini, d'ordre $n$. On veut montrer que $G$ est cyclique, c'est-à-dire que $G$ contient un élément d'ordre $n$. D'après le théorème de Lagrange, l'ordre d'un élément de $G$ divise $n$. Soit donc, pour $d$ divisant $n$, $O_d := \{x \in G \ \ \text{ordre}(x) = d\}$. On a donc

$$n = \sum_{d|n} |O_d|.$$

On montre le lemme suivant :

**Lemme 11.3.4.** $|O_d| = 0$ ou $|O_d| = \varphi(d)$.

*Démonstration.* Supposons que $|O_d| \geq 1$, et soit $x \in O_d$. Alors, $x^d = 1$ donc $x$ est une racine du polynôme $X^d - 1 \in K[X]$. D'autre part, toutes les puissances de $x$ : $1, x, \ldots, x^{d-1}$, sont aussi des racines de ce polynôme, et, comme $x$ est d'ordre $d$, cela fait $d$ racines distinctes. Or on sait qu'un polynôme à coefficients dans un corps n'a pas plus de racines dans ce corps que son degré. Donc le polynôme $X^d - 1$ n'a pas d'autres racines dans $K$ que celles de l'ensemble $\{1, x, \ldots, x^{d-1}\}$. On peut en conclure que $O_d \subset \langle x \rangle$ puisqu'un élément $y \in O_d$ est aussi une racine de $X^d - 1$. Mais on connait le nombre d'éléments d'ordre $d$ dans $\langle x \rangle$ qui est un groupe cyclique d'ordre $d$ : c'est $\varphi(d)$ (Proposition 6.2.2). Donc $|O_d| = \varphi(d)$. □

On peut maintenant terminer la preuve du théorème : on a d'une part

$$n = \sum_{d|n} |O_d|, \quad |O_d| = 0 \text{ ou } \varphi(d)$$

et d'autre part (Proposition 6.2.3)

$$n = \sum_{d|n} \varphi(d)$$

donc on peut conclure que $|O_d| = \varphi(d)$ *pour tout* $d$, et en particulier $|O_n| = \varphi(n) > 0$. □