

Licence 1/ MIAGE /2024-2025/Cours d'Algèbre  
**STRUCTURES ALGÈBRIQUES**

Enseignant: E. D. AKEKE

# Table des matières

<b>1</b>	<b>LOIS DE COMPOSITION</b>	<b>4</b>
1.1	Définitions et exemples . . . . .	4
1.2	Quelques propriétés . . . . .	7
1.3	Homomorphismes . . . . .	9
<b>2</b>	<b>STRUCTURES DE GROUPES</b>	<b>11</b>
2.1	Définition et exemples . . . . .	11
2.2	Produit cartésien de groupes . . . . .	12
2.3	Sous-groupes d'un groupe . . . . .	13
2.4	Homomorphismes de groupes . . . . .	18
2.5	Groupes quotients . . . . .	20
2.5.1	Congruences modulo un sous-groupe . . . . .	21
2.5.2	Théorème de Lagrange . . . . .	22
<b>3</b>	<b>STRUCTURES D'ANNEAUX ET CORPS</b>	<b>24</b>
3.1	Définition et exemples . . . . .	24
3.2	L'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ , $n \in \mathbb{N}$ . . . . .	24
3.3	Calculs dans un anneau . . . . .	28
3.4	Sous-anneaux . . . . .	31
3.5	Idéal d'un anneau commutatif . . . . .	31
3.6	Morphisme d'anneaux . . . . .	32
3.7	Corps . . . . .	33

<b>4</b>	<b>POLYNÔMES ET FRACTIONS RATIONNELLES</b>	<b>36</b>
4.1	Anneau des polynômes à coefficients dans un corps . . . . .	36
4.1.1	Définitions . . . . .	36
4.1.2	Opérations dans $\mathbb{K}[X]$ . . . . .	36
4.1.3	Notion de degré d'un polynôme . . . . .	37
4.2	Fonctions polynômiales . . . . .	37
4.3	Division euclidienne . . . . .	38
4.4	Division suivant les puissances croissantes . . . . .	39
4.5	Dérivée Formelle et racine multiple d'un polynôme . . . . .	39
4.6	Polynômes irréductibles . . . . .	42
4.7	Notions de pgcd et de ppcm . . . . .	42
4.8	Polynômes complexes . . . . .	45
4.9	Polynômes réels . . . . .	46
4.10	Relation entre racines et coefficients d'un polynôme scindé . . . . .	47
4.11	Fractions rationnelles . . . . .	48
4.11.1	Corps des fractions rationnelles à une indéterminée . . . . .	48
4.11.2	Décomposition en éléments simples des fractions rationnelles . . . . .	49

# 1 LOIS DE COMPOSITION

## 1.1 Définitions et exemples

**Définition 1.1** Soit  $E$  un ensemble non vide. On appelle **loi de composition interne** sur  $E$ , toute application de  $E \times E$  vers  $E$ .

Soit  $f : E \times E \longrightarrow E$  une loi de composition interne sur  $E$ . Si  $x \in E, y \in E$  et  $z = f(x, y)$ , on peut convenir d'écrire  $z = x \top y$  (ou  $x \perp y, x * y, x + y, x.y, \dots$ ). Les éléments  $x$  et  $y$  s'appellent les **termes** et  $z$  le résultat de **l'opération** de  $x$  par  $y$  pour la loi  $\top$ .

### Exemples

- i) Dans  $\mathbb{R}$  (ou  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ), les lois usuelles  $+$ ,  $\times$  sont des lois de composition internes.
- ii) Soit  $F$  un ensemble. Dans l'ensemble  $\mathcal{P}(F)$  des parties de  $F$ , les lois  $\cap, \cup, \Delta$  sont des lois de composition internes.
- iii) Soit  $F$  un ensemble non vide. Dans l'ensemble  $\mathcal{A}(F)$  des applications de  $F$  vers  $F$ , la composition des applications de  $F$  vers  $F$  est une loi de composition interne dans  $\mathcal{A}(F)$ . Cette loi est souvent notée "o".

**Définition 1.2** Soit  $(E, *)$  un ensemble non vide, muni d'une loi de composition interne.

- 1) Une partie non vide  $A$  de  $E$  est dite **stable** pour la loi  $*$  si :

$$\forall x, y \in A, \quad \text{on a } x * y \in A.$$

- 2) La loi  $*$  est **associative** dans  $E$  si la propriété suivante est satisfaite :

$$\forall x, y, z \in E, \quad (x * y) * z = x * (y * z).$$

- 3) Deux éléments  $x$  et  $y$  de  $E$  commutent dans  $E$  pour la loi  $*$  si

$$x * y = y * x$$

- 4) La loi  $*$  est **commutative** (dans  $E$ ) si :

$$\forall x, y \in E, \quad x * y = y * x$$

c'est à dire que deux éléments quelconque de  $E$  commutent pour la loi  $*$ .

- 5) L'élément  $e \in E$  est **élément neutre** pour la loi  $*$  si :

$$\forall x \in E, \quad x * e = x \quad \text{et} \quad e * x = x$$

6) L'élément  $a \in E$  est un **élément régulier** pour la loi  $*$  si :

$$\forall x, y \in E, \quad a * x = a * y \Rightarrow x = y \quad \text{et} \quad x * a = y * a \Rightarrow x = y.$$

7) Si  $(E, *)$  admet un élément neutre  $e$  et  $x, y \in E$ , on dit que  $y$  est le **symétrique** de  $x$  dans  $(E, *)$  si :

$$x * y = e \quad \text{et} \quad y * x = e.$$

8) L'élément  $a \in E$  est un **élément idempotent** pour la loi  $*$  si :

$$a * a = a$$

9) L'élément  $a \in E$  est dit **absorbant** si :

$$\forall x \in E, \quad a * x = a = x * a$$

(assez peu utilisé!).

**Remarque 1.1** Soit  $E$  un ensemble muni d'une loi de composition interne  $*$ .

Si la loi  $*$  admet un élément neutre dans  $E$  alors cet élément est l'**unique** élément neutre dans  $E$  (pour cette loi!).

Preuve (exercice facile)

### Exemples et contre-exemples

1) Les lois usuelles  $+$  et  $\times$  sont internes et associatives, commutatives dans  $\mathbb{R}$ . Dans  $(\mathbb{R}, +)$ , l'élément 0 est élément neutre. Dans  $(\mathbb{R}, \times)$  l'élément 1 est élément neutre.

La multiplication usuelle n'est pas une loi interne dans  $\mathbb{Z}_- = \{x \in \mathbb{Z} / x \leq 0\}$ .

2) Soit  $F$  un ensemble. Les lois  $\cap$  et  $\cup$  sont associatives et commutatives dans  $\mathcal{P}(F)$ .

3) Soit  $F$  un ensemble non vide. La loi " $\circ$ " de composition des applications de  $F$  vers  $F$  est associative, elle n'est pas commutative (en général  $g \circ f \neq f \circ g$ ).

4) Considérons la loi  $*$  définie sur  $\mathbb{R}$  par

$$\forall x, y \in \mathbb{R}, \quad x * y = x + y + xy.$$

C'est est une loi de composition interne dans  $\mathbb{R}$ .

(i) Pour tout  $x, y, z \in \mathbb{R}$ , on a

$$(x * y) * z = (x * y) + z + (x * y)z = (x + y + xy) + z + (x + y + xy)z$$

Donc  $(x * y) * z = x + y + z + xy + yz + xz + xyz$ . De même, on montre que

$$x * (y * z) = x + y + z + xy + yz + xz + xyz.$$

Ainsi,  $(x * y) * z = x * (y * z)$ . La loi  $*$  est donc associative dans  $\mathbb{R}$ .

(ii) Pour tout  $x, y \in \mathbb{R}$ , on a

$$x * y = x + y + xy = y + x + yx = y * x$$

Donc  $x * y = y * x$ . La loi  $*$  est donc commutative.

(iii) On vérifie sans difficulté que pour tout  $x \in \mathbb{R}$ , on a  $0 * x = x$  et  $x * 0 = x$ , donc 0 est l'élément neutre dans  $(\mathbb{R}, *)$ .

(iv) Pour tout  $x \in \mathbb{R}$ , existe-t-il un élément  $y \in \mathbb{R}$  tel que  $x * y = 0$ ?

on a  $x * y = 0 \Leftrightarrow x + y + xy = 0 \Rightarrow y = \frac{-x}{x+1}$  si  $x \neq -1$ . Donc tout élément  $x \in \mathbb{R} \setminus \{-1\}$

admet un symétrique dans  $\mathbb{R}$  pour la loi  $*$  et son symétrique est  $\frac{-x}{x+1}$ .

Remarquons  $-1$  n'admet pas de symétrique dans  $(\mathbb{R}, *)$ .

5) Soit  $F$  un ensemble. Dans  $(\mathcal{P}(F), \cup)$ , l'élément  $\emptyset$  est élément neutre. Dans  $(\mathcal{P}(E), \cap)$  l'élément  $F$  est l'élément neutre.

6) Dans  $(\mathcal{A}(F), \circ)$  l'élément  $id_E$  est élément neutre.

Les éléments de  $(\mathcal{A}(F), \circ)$  qui admettent un symétrique dans  $(\mathcal{A}(F), \circ)$  sont exactement les applications bijectives de  $F$  sur  $F$ .

7) La loi  $*$  définie sur  $\mathbb{R}$  par

$$\forall x, y \in \mathbb{R}, \quad x * y = x \times y + 3$$

est commutative. Elle n'est pas associative et n'admet pas d'élément neutre.

En effet, pour tout  $x, y \in \mathbb{R}$ , on a

$$x * y = x \times y + 3 = y \times x + 3 = y * x$$

d'où la commutativité.

On a  $(2 * 4) * 3 = 36$  et  $2 * (4 * 3) = 33$ , ainsi  $(2 * 4) * 3 \neq 2 * (4 * 3)$  et cette loi  $*$  n'est pas associative.

Supposons que cette loi  $*$  admette un élément neutre  $e \in \mathbb{R}$ . Alors  $\forall x \in \mathbb{R}$ , on a  $e * x = x$ . C'est à dire que pour tout  $x \in \mathbb{R}$ , on a

$$e x + 3 = x$$

On déduit alors que

$$\forall x \in \mathbb{R} \setminus \{0\}, e = \frac{x - 3}{x}$$

Ceci est absurde car l'élément, s'il existe, il est unique, indépendant de tout élément de  $\mathbb{R}$ .

### Exercice

1) On considère la loi  $*$  définie sur  $\mathbb{R}$  par

$$\forall x, y \in \mathbb{R}, \quad x * y = x^2 \times y.$$

Etudier les propriétés de cette loi (associativité, commutativité, élément neutre, éléments idempotents)

2) On considère la loi  $\top$  définie sur  $\mathbb{R}$  par

$$\forall x, y \in \mathbb{R}, \quad x \top y = x^2 \times y + 1.$$

Etudier les propriétés de cette loi (associativité, commutativité, élément neutre, éléments idempotents).

## 1.2 Quelques propriétés

**Proposition 1.1** *Soit  $E$  un ensemble muni d'une loi  $*$  **associative** et admettant un élément neutre  $e$ . Alors tout élément  $x \in E$  admet au plus un symétrique dans  $(E, *)$ .*

Preuve

Soit  $x \in E$ . Supposons que  $y$  et  $z$  soient deux symétriques de  $x$ . On a

$$y * x = e = x * z \tag{1}$$

La loi  $*$  étant associative, on a

$$(y * x) * z = y * (x * z) \tag{2}$$

Par conséquent  $e * z = y * e$ . D'où  $z = y$ .

**Notation 1.1** 1) *Soit  $E$  un ensemble muni d'une l.c.i noée " $\cdot$ ", **associative** et admettant un élément neutre.*

*Si  $x \in E$  admet un symétrique dans  $(E, \cdot)$ , l'unique symétrique de  $x$  dans  $E$  est noté  $x^{-1}$ .*

2) Soit  $E$  un ensemble muni de la loi  $+$  (loi additive) **associative** et admettant un élément neutre (souvent noté  $0$ ). Si  $x \in E$  admet un symétrique, l'unique symétrique de  $x$  dans  $E$  est noté  $-x$  (appelé **l'opposé** de  $x$  dans  $E$ ).

**Remarque 1.2** Soient  $E$  un ensemble muni d'une loi de composition interne notée  $\cdot$  et associative, admettant un élément neutre.

(1) Pour tout entier  $n \geq 1$  et pour tout  $x \in E$ , on pose :

$$x^n = \underbrace{x \cdot \dots \cdot x}_{n \text{ fois}}$$

Alors pour tout entier  $m, n \geq 1$  et pour tout  $x \in E$ , on a

$$(x^m)^n = x^{mn} \quad \text{et} \quad x^m \cdot x^n = x^{m+n}$$

(2) Soient  $x, y \in E$  et  $n \in \mathbb{N}^*$ . En général, on a  $(x \cdot y)^n \neq x^n \cdot y^n$  mais

$$\text{si} \quad x \cdot y = y \cdot x \quad \text{alors} \quad (x \cdot y)^n = x^n \cdot y^n$$

**Proposition 1.2** Soit  $E$  un ensemble muni d'une loi de composition interne notée " $\cdot$ ", associative et admettant un élément neutre et soit  $x, y \in E$ .

Si  $x$  admet un symétrique dans  $(E, \cdot)$  et  $y$  admet un symétrique dans  $(E, \cdot)$  alors  $x \cdot y$  admet un symétrique dans  $E$  et on a

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

(la notation additive est  $-(x + y) = -y - x$ ).

Preuve

En effet, on a

$$(x \cdot y) \cdot y^{-1} \cdot x^{-1} = (x \cdot y \cdot y^{-1}) \cdot x^{-1} = x \cdot e \cdot x^{-1} = x \cdot x^{-1} = e$$

et on a aussi

$$y^{-1} \cdot x^{-1} \cdot (x \cdot y) = e$$

où  $e$  est l'élément neutre dans  $(E, \cdot)$ . Donc  $x \cdot y$  admet un symétrique dans  $(E, \cdot)$  et son symétrique est  $y^{-1} \cdot x^{-1}$ , ainsi

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

**Corollaire 1.1** Soit  $E$  un ensemble muni d'une loi de composition interne notée " $\cdot$ ", **associative** et admettant un élément neutre. Si  $x \in E$  admet un symétrique dans  $(E, \cdot)$  alors  $\forall n \in \mathbb{N}^*$ , l'élément  $x^n$  admet un symétrique dans  $(E, \cdot)$  et on a

$$(x^n)^{-1} = (x^{-1})^n$$

(la notation additive est  $-(nx) = n(-x)$ ).

### 1.3 Homomorphismes

**Définition 1.3** Soient  $E$  et  $F$  deux ensembles non vides munis des lois  $*$  et  $\top$  respectivement.

On dit qu'une application  $f : (E, *) \longrightarrow (F, \top)$  est un **homomorphisme** si :

$$\forall x, y \in E, \quad f(x * y) = f(x) \top f(y)$$

Un homomorphisme bijectif est appelé un **isomorphisme**.

Si  $(E, *) = (F, \top)$  l'homomorphisme  $f$  est appelé un **endomorphisme**.

Un endomorphisme bijectif est appelé un **automorphisme**.

#### Exemples

1) L'application  $f : (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}, +)$  définie par  $f(x) = \ln(x)$  est un homomorphisme.

2) Soit  $a \in \mathbb{R}$ . L'application  $g_a : (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$  définie par  $g_a(x) = ax$  est un homomorphisme.

**Théorème 1.1** Si  $f : (E, *) \longrightarrow (F, \cdot)$  et  $g : (F, \cdot) \longrightarrow (G, \top)$  sont des homomorphismes alors  $g \circ f$  est un homomorphisme.

Preuve

$$g \circ f : (E, *) \longrightarrow (G, \top).$$

$\forall z \in E$ , on a

$$(g \circ f)(z) = g(f(z)).$$

$\forall x, y \in E$ , on a

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

$$(g \circ f)(x * y) = g(f(x)) \top g(f(y)).$$

$$(g \circ f)(x * y) = (g \circ f)(x) \top (g \circ f)(y).$$

Donc  $g \circ f$  est un homomorphisme de  $(E, *)$  vers  $(G, \top)$ .

**Théorème 1.2** Si  $f : (E, *) \longrightarrow (F, \cdot)$  est un isomorphisme alors  $f^{-1} : (F, \cdot) \longrightarrow (E, *)$  est un isomorphisme. On l'appelle **l'isomorphisme réciproque** de  $f$ .

Preuve (exercice!)

#### Exemple

L'application  $\text{Log} : \mathbb{R}_+^* \longrightarrow \mathbb{R}$  est un isomorphisme de  $(\mathbb{R}_+^*, \cdot)$  sur  $(\mathbb{R}, +)$ , l'isomorphisme réciproque se notant  $\exp$ .

**Remarque 1.3** a) Si  $f : (E, *) \longrightarrow (F, \cdot)$  est un homomorphisme et  $B$  une partie stable de  $E$  alors  $f(B)$  est une partie stable de  $F$ .

b) Soient  $(E, \top)$  et  $f$  une bijection de  $E$  sur un ensemble  $F$ . On peut définir une loi  $*$  sur  $F$  en posant :

$$\forall x, y \in F, \quad x * y = f(f^{-1}(x) \top f^{-1}(y)).$$

L'application  $f$  devient ainsi un isomorphisme de  $(E, \top)$  sur  $(F, *)$ . On dit qu'on a réalisé un **transport de structure**.

## 2 STRUCTURES DE GROUPE

### 2.1 Définition et exemples

**Définition 2.1** On appelle **groupe** un ensemble non vide  $G$ , muni d'une loi de composition interne  $*$ , vérifiant les propriétés suivantes :

- i) la loi  $*$  est associative,
- ii) la loi  $*$  admet un élément neutre dans  $G$ ,
- iii) tout élément de  $G$  admet un symétrique dans  $G$ .

Si de plus la loi  $*$  est commutative, le groupe  $(G, *)$  est appelé **groupe commutatif** ou plus souvent **groupe abélien**.

#### Exemples

- 1)  $(\mathbb{Z}, +)$  est un groupe abélien. Mais  $(\mathbb{Z}, \times)$  n'est pas un groupe.
- 2)  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$  sont des groupes abéliens.
- 3)  $(\mathbb{Q}, \times)$ ,  $(\mathbb{R}, \times)$ ,  $(\mathbb{C}, \times)$  ne sont pas des groupes.

En revanche,  $(\mathbb{Q}^*, \times)$ ,  $(\mathbb{R}^*, \times)$ ,  $(\mathbb{C}^*, \times)$  sont des groupes abéliens.

4) Soient  $E$  un ensemble non vide et  $\mathcal{A}(E)$  l'ensemble des applications de  $E$  vers  $E$ . On pose

$$S(E) = \{ f \in \mathcal{A}(E) / f \text{ bijective} \}$$

Alors l'ensemble  $(S(E), \circ)$  (où  $\circ$  est la loi de composition des applications) est un groupe.

Si  $n \in \mathbb{N}^*$  et  $E = \{1, 2, \dots, n\}$ , le groupe  $(S(E), \circ)$  se note  $S_n$ , appelé le **groupe des permutations** de  $E$  ou plus souvent **groupe symétrique** de rang  $n$ .

Notons que

$$\text{Card}(S_n) = n!$$

5) Si  $(G, \cdot)$  est un groupe et  $E$  un ensemble non vide quelconque, l'ensemble  $\mathcal{A}(E, G)$  des applications de  $E$  dans  $G$  est muni naturellement d'une structure de groupe, en définissant la loi notée encore  $\cdot$  sur  $\mathcal{A}(E, G)$  par  $f.g : E \rightarrow G$  avec  $(f.g)(x) = f(x).g(x)$ .

#### Exercice

- 1) Déterminer les éléments des groupes symétriques  $S_2$  et  $S_3$ . Etablir les tables de ces groupes.
- 2) Montrer que le groupe  $(S_3, \circ)$  n'est pas commutatif.
- 3) En déduire que, si  $n \geq 3$  alors le groupe  $(S_n, \circ)$  n'est pas commutatif.

### Exercice

Dire dans les cas suivants si on définit une loi de groupe :

1)  $G = ]-1, 1[$ ,  $x * y = \frac{x+y}{1+xy}$

2)  $G = \mathbb{R}$ ,  $x * y = x + y + xy$

3)  $G = \mathbb{R}$ ,  $x \top y = \max(x, y)$

4)  $G = \mathbb{R}_+$ ,  $x \top y = \max(x, y)$

5)  $G = \mathbb{R}$ ,  $x \triangle y = \sqrt[3]{x^3 + y^3}$ .

### Exercice

Dans  $\mathbb{R}^* \times \mathbb{R}$ , on définit la loi  $\top$  par

$$\forall (x, y), (x', y') \in \mathbb{R}^* \times \mathbb{R}, \quad (x, y) \top (x', y') = (x \cdot x', \frac{y}{x'} + x y').$$

Montrer que  $(\mathbb{R}^* \times \mathbb{R}, \top)$  est un groupe. Est-il abélien ?

## 2.2 Produit cartésien de groupes

Soient  $(G, *)$  et  $(F, \cdot)$  deux groupes. Le produit cartésien  $G \times F$  est muni de la loi de composition interne naturel  $\top$  définie par

$$\forall (x, y) \in G \times F, \forall (x', y') \in G \times F, \quad (x, y) \top (x', y') = (x * x', y \cdot y').$$

**Proposition 2.1**  $(G \times F, \top)$  est un groupe.

### Preuve

Il est clair que la loi  $\top$  est une loi de composition interne dans  $G \times F$ .

#### Associativité de la loi $\top$

Soient  $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in G \times F$ . on a

$$\begin{aligned} [(x_1, y_1) \top (x_2, y_2)] \top (x_3, y_3) &= (x_1 * x_2, y_1 \cdot y_2) \top (x_3, y_3) = ((x_1 * x_2) * x_3, (y_1 \cdot y_2) \cdot y_3) \\ (x_1, y_1) \top [(x_2, y_2) \top (x_3, y_3)] &= (x_1, y_1) \top (x_2 * x_3, y_2 \cdot y_3) = (x_1 * (x_2 * x_3), y_1 \cdot (y_2 \cdot y_3)) \end{aligned}$$

Les lois  $*$  et  $\top$  étant associatives, on a  $(x_1 * x_2) * x_3 = x_1 * (x_2 * x_3)$  et  $(y_1 \cdot y_2) \cdot y_3 = y_1 \cdot (y_2 \cdot y_3)$  d'où

$$[(x_1, y_1) \top (x_2, y_2)] \top (x_3, y_3) = (x_1, y_1) \top [(x_2, y_2) \top (x_3, y_3)].$$

La loi  $*$  est donc associative.

### Élément neutre

Soient  $e$  l'élément neutre de  $(G, *)$  et  $e'$  l'élément neutre de  $(F, \cdot)$ .

Pour tout  $(x, y) \in G \times F$  on a

$$\begin{aligned}(x, y) \top (e, e') &= (x * e, y \cdot e') = (x, y) \\ (e, e') \top (x, y) &= (e * x, e' \cdot y) = (x, y)\end{aligned}$$

Par conséquent  $(e, e')$  est l'élément neutre de  $G \times F$ .

### Éléments symétriques

Soit  $(x, y) \in G \times F$ . Soient  $x^{-1}$  le symétrique de  $x$  dans  $G$  et  $y^{-1}$  le symétrique de  $y$  dans  $F$ . On a

$$\begin{aligned}(x, y) \top (x^{-1}, y^{-1}) &= (x * x^{-1}, y \cdot y^{-1}) = (e, e') \\ (x^{-1}, y^{-1}) \top (x, y) &= (x^{-1} * x, y^{-1} \cdot y) = (e, e')\end{aligned}$$

Par conséquent  $(x, y)$  admet un symétrique dans  $G \times F$  et son symétrique est  $(x^{-1}, y^{-1})$ .

En somme,  $(G \times F, \top)$  est un groupe.

### **Exemples**

- 1)  $G = (\mathbb{R}, +)$ ,  $F = (\mathbb{R}, +)$ .
- 2)  $(\mathbb{R} \times \mathbb{R}, +)$  est un groupe :  $\forall (a, b), (c, d) \in \mathbb{R}^2$ ,  $(a, b) + (c, d) = (a + c, b + d)$ .
- 3)  $(\mathbb{R}^3, +)$  est un groupe, la loi  $+$  étant définie par

$$\forall (a_1, b_1, c_1), (a_2, b_2, c_2) \in \mathbb{R}^3, \quad (a_1, b_1, c_1) + (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2)$$

## **2.3 Sous-groupes d'un groupe**

**Définition 2.2** Soient  $(G, \cdot)$  un groupe d'élément neutre  $e$  et  $H$  un sous-ensemble de  $G$ . On dit que  $H$  est un **sous-groupe** du groupe  $(G, \cdot)$  si les conditions suivantes sont satisfaites :

- i)  $e \in H$ ,
- ii)  $\forall x, y \in H, \quad x \cdot y \in H$ ,
- iii)  $\forall x \in H, \quad x^{-1} \in H$ .

On note alors  $H < G$ .

Exprimer cette définition avec la notation additive  $+$ .

**Proposition 2.2** Soient  $(G, \cdot)$  un groupe d'élément neutre  $e$  et  $H$  une partie de  $G$ .

$H$  est un sous-groupe de  $G$  si et seulement si les conditions suivantes sont satisfaites :

- 1)  $e \in H$ ,
- 2)  $\forall x, y \in H, \quad x \cdot y^{-1} \in H$ .

### Preuve

Supposons que  $H$  soit un sous-groupe de  $G$ .

Alors  $e \in H$  d'après la définition 2.2. Soient  $x, y \in H$ . Alors  $y^{-1} \in H$  d'après la définition 2.2, iii) et  $x y^{-1} \in H$  d'après la définition 2.2, ii), d'où la proposition.

Réciproquement, supposons 1) et 2) vraies.

Il est clair que  $e \in H$ .

Soit  $x \in H$ . D'après 2) on a  $e x^{-1} \in H$  donc  $x^{-1} \in H$ , ce qui prouve iii) de la définition 2.2. Soient  $x, y \in H$ . Alors  $x \in H$  et  $y^{-1} \in H$ , donc  $x (y^{-1})^{-1} \in H$ , ainsi  $x y \in H$ . Ce qui prouve ii) de la définition 2.2. En somme,  $H$  est un sous-groupe de  $G$ .

### Exemples

1)  $\mathbb{Q}$  est un sous-groupe du groupe  $(\mathbb{R}, +)$ .

2)  $\mathbb{Z}$  est un sous-groupe du groupe  $(\mathbb{Q}, +)$ , donc du groupe  $(\mathbb{R}, +)$ .

3) Soit  $p \in \mathbb{Z}$ . On pose

$$p\mathbb{Z} = \{x \in \mathbb{Z} / \exists k \in \mathbb{Z}, x = p k\}.$$

Le lecteur remarquera que  $p\mathbb{Z}$  est exactement l'ensemble des éléments de  $\mathbb{Z}$  qui sont multiples de  $p$  dans  $\mathbb{Z}$ .

Pour tout  $p \in \mathbb{Z}$  l'ensemble  $p\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$  (exercice facile!).

### Remarque 2.1 (important !)

1) Une partie stable d'un groupe n'est pas nécessairement un sous-groupe. Par exemple  $\mathbb{N}$  est une partie stable de  $\mathbb{Z}$  pour l'addition usuelle, mais ce n'est pas un sous-groupe de  $(\mathbb{Z}, +)$ .

2) Tout sous-groupe d'un groupe a une structure de groupe (relativement à la loi induite) et tout sous-groupe d'un groupe commutatif est un groupe commutatif.

3) Si  $G$  est un groupe d'élément neutre  $e$  alors  $\{e\}$  et  $G$  sont des sous-groupes de  $G$  appelés **sous-groupes triviaux** de  $G$ .

**Proposition 2.3** Soient  $(G, *)$  un groupe et  $(H_i)_{i \in I}$  une famille de sous-groupes du groupe  $(G, *)$ .

Alors l'intersection  $\bigcap_{i \in I} H_i$  est un sous-groupe de  $G$ . En particulier, l'intersection de 2 sous-groupes de  $(G, *)$  est un sous-groupe de  $G$ .

**Preuve**

1)  $\forall i \in I, e \in H_i$  donc  $e \in \bigcap_{i \in I} H_i$

2) Soient  $x, y \in \bigcap_{i \in I} H_i$ .

$\forall i \in I$  on a  $x \in H_i$  et  $y^{-1} \in H_i$ , donc  $xy^{-1} \in H_i$  car  $H_i$  est un sous-groupe de  $G$ . Ainsi  $xy^{-1} \in \bigcap_{i \in I} H_i$ .

En somme  $\bigcap_{i \in I} H_i$  est un sous-groupe de  $G$ .

**Remarque 2.2** La réunion de 2 sous-groupes d'un groupe  $G$  n'est pas en général un sous-groupe de  $G$ .

Par exemple,  $3\mathbb{Z}$  et  $5\mathbb{Z}$  sont des sous groupes de  $\mathbb{Z}$ , mais  $3\mathbb{Z} \cup 5\mathbb{Z}$  n'est pas un sous-groupe de  $\mathbb{Z}$ .

En effet,  $3 \in 3\mathbb{Z}$  et  $5 \in 5\mathbb{Z}$  mais  $3 + 5 = 8 \notin 3\mathbb{Z} \cup 5\mathbb{Z}$

**Exercice**

Soient  $(G, .)$  un groupe,  $H$  et  $K$  deux sous-groupes de  $G$ .

Montrer que  $H \cup K$  est un sous-groupe de  $G$  si et seulement si  $H \subseteq K$  ou  $K \subseteq H$ .

**Proposition 2.4** Soit  $H$  une partie de  $\mathbb{Z}$ .

$$H \text{ est un sous-groupe de } (\mathbb{Z}, +) \iff \exists n \in \mathbb{N} \text{ tel que } H = n\mathbb{Z}$$

(Noter que si  $H \neq 0$  alors  $n = \min\{k \in \mathbb{N}^* / k \in H\}$ )

Preuve

Il est facile de vérifier que pour tous entier  $n$ ,  $n\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$ . Si  $H = \{0\}$ , alors on peut prendre  $n = 0$  et c'est le seul entier qui convienne. Si  $H \neq \{0\}$ , posons,  $n = \min(H \cap \mathbb{N}^*)$ , ( $n$  existe dans  $\mathbb{N}$ , c'est la propriété fondamentale de  $\mathbb{N}$ ), on a  $n \in H$ , comme  $H$  est un sous-groupe de  $(\mathbb{Z}, +)$ , tout multiple de  $n$  est dans  $H$ , i.e.  $n\mathbb{Z} \subset H$ . Soit  $k \in H$ , effectuons la division euclidienne de  $k$  par  $n$  ( $n \neq 0$ ) :  $k = nq + r$  avec  $0 \leq r < n$ .

On a donc  $r = k - nq \in H \cap \mathbb{N}^*$ , si  $r \neq 0$  alors  $r \geq n$ , ce qui est absurde, donc  $r = 0$  ce qui donne  $k = nq \in n\mathbb{Z}$ , finalement  $H = n\mathbb{Z}$ .

**Corollaire 2.1** Soient  $m, n \in \mathbb{Z}$ . On a

$$m\mathbb{Z} \cap n\mathbb{Z} = p\mathbb{Z}$$

où  $p = PPCM(m, n)$

Preuve (exercice!)

Soient  $m, n \in \mathbb{Z}$ . On pose

$$m\mathbb{Z} + n\mathbb{Z} = \{x \in \mathbb{Z} / \exists a, b \in \mathbb{Z}, x = ma + nb\}.$$

Il n'est pas difficile de prouver que  $m\mathbb{Z} + n\mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}$  (exercice!).

**Corollaire 2.2** Soient  $m, n \in \mathbb{Z}$ . On a

$$m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$$

où  $d = \text{PGCD}(m, n)$ .

Preuve (exercice cf. TD)

### Égalité de Bézout

Soient  $m, n \in \mathbb{Z}$  et  $d \in \mathbb{N}$ . D'après le corollaire 2.2 on a

$$d = \text{pgcd}(m, n) \Rightarrow \exists u, v \in \mathbb{Z} \text{ tel que } mu + nv = d.$$

En particulier,

$$m \text{ et } n \text{ sont premiers entre eux} \Leftrightarrow \exists u, v \in \mathbb{Z} \text{ tels que } mu + nv = 1$$

### **Exercice**

Déterminer l'entier naturel  $n$  tel que  $6\mathbb{Z} + 4\mathbb{Z} = n\mathbb{Z}$ .

1) Déterminer l'entier naturel  $m$  tel que  $6\mathbb{Z} \cap 14\mathbb{Z} = m\mathbb{Z}$ .

Expliciter les groupes suivants :

a)  $6\mathbb{Z} + 4\mathbb{Z} + 15\mathbb{Z}$

b)  $6\mathbb{Z} \cap 4\mathbb{Z} \cap 15\mathbb{Z}$ .

## **Sous-groupe engendré par une partie**

**Définition 2.3** Soient  $(G, *)$  un groupe et  $A$  une partie de  $G$ . Par définition le sous-groupe de  $G$  engendré par  $A$  est l'intersection de tous les sous-groupes de  $(G, *)$  contenant  $A$ . On le note  $\langle A \rangle$ .

On convient que le sous-groupe de  $G$  engendré par l'ensemble vide  $\emptyset$  est le singleton  $\{e_G\}$  où  $e_G$  est l'élément neutre du groupe  $G$ .

**Remarque 2.3** *Le sous-groupe  $\langle A \rangle$  est le plus petit sous-groupe (au sens de l'inclusion) de  $G$  contenant  $A$ .*

**Exercice**

Montrer que le sous-groupe de  $(\mathbb{R}, +)$  engendré par le sous-ensemble  $H = \{\frac{1}{n} / n \in \mathbb{N}^*\}$  est  $\mathbb{Q}$ .

**Théorème 2.1** *Soient  $(G, .)$  un groupe et  $A$  une partie non vide de  $G$ . Le sous-groupe  $\langle A \rangle$  de  $G$  engendré par  $A$  est*

$$\langle A \rangle = \{ x \in G / \exists k \in \mathbb{N}^*, \exists a_1, \dots, a_k \in A, \quad x = a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k} \text{ avec } \varepsilon_i = 1 \text{ ou } \varepsilon_i = -1 \}.$$

**Corollaire 2.3** *Soient  $(G, .)$  un groupe d'élément neutre  $e$  et  $x \in G$ . Alors le sous-groupe  $\langle x \rangle$  de  $G$  engendré par  $x$  est*

$$\langle x \rangle = \{ y \in G / \exists k \in \mathbb{Z}, \quad y = x^k \}.$$

**Exercice**

Soient  $(G, .)$  un groupe **fini** d'élément neutre  $e$  et  $x \in G, \quad x \neq e$ .

- 1) Montrer qu'il existe un entier  $k \in \mathbb{N}^*$  tel que  $x^k = e$ .
- 2) On pose  $H = \{ y \in G / \exists k \in \mathbb{Z}, \quad y = x^k \}$  et  $H' = \{ y \in G / \exists k \in \mathbb{N}, \quad y = x^k \}$ .  
Montrer que  $H = H'$
- 3) On pose  $n = \min\{p \in \mathbb{N}^* / x^p = e\}$ 
  - i) Prouver l'existence de l'entier  $n$ .
  - ii) Montrer que

$$\langle x \rangle = \{ e, x, \dots, x^{n-1} \}$$

En déduire que  $H = \langle x \rangle = H'$ .

Par définition, l'entier naturel  $n$  est appelé **l'ordre** de  $x$  et noté  $o(x)$ .

**Exercice**

Soit  $p \in \mathbb{N}^*$ .

On pose  $H_p = \{ z \in \mathbb{C} / z^p = 1 \}$ .

- 1) Montrer que  $H_p$  est un sous-groupe du groupe multiplicatif  $(\mathbb{C}^*, .)$ .
- 2) Déterminer les éléments de  $H_p$ . Quel est le cardinal de  $H_p$ ?
- 3) Expliciter  $H_8$  et déterminer l'ordre de chacun de ces éléments.

## 2.4 Homomorphismes de groupes

**Définition 2.4** Soient  $(G, *)$ ,  $(H, \top)$  deux groupes et  $f : G \longrightarrow H$  un homomorphisme. L'homomorphisme  $f$  est appelé **homomorphisme** (ou **morphisme**) de groupes.

On appelle **noyau** de  $f$  et on note  $\ker(f)$ , le sous-ensemble de  $G$  défini par

$$\ker(f) = \{x \in G / f(x) = e_H\}$$

où  $e_H$  est l'élément neutre du groupe  $H$ .

**L'image** de  $f$ , notée  $\text{Im}(f)$  ou  $f(G)$ , est le sous-ensemble de  $H$  défini par

$$\text{Im}(f) = \{h \in H / \exists x \in G, y = f(x)\}.$$

### Exemples

L'application  $g : (\mathbb{R}_+, \times) \longrightarrow (\mathbb{R}, +)$  définie par  $x \longmapsto \ln(x)$  est un morphisme de groupes. Soit  $n \in \mathbb{N}^*$ . L'application  $f : (\mathbb{C}^*, \times) \longrightarrow (\mathbb{C}^*, \times)$  définie par  $z \longmapsto z^n$  est un morphisme de groupes.

**Remarque 2.4** L'homomorphisme  $f$  satisfait les propriétés suivantes :

1)  $f(e_G) = e_H$

2)  $\forall x \in G \quad f(x^{-1}) = (f(x))^{-1}.$

**Théorème 2.2** Soit  $f : (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$  un morphisme de groupes continu en 0, alors :

$$\forall x \in \mathbb{R}, f(x) = ax$$

où  $a = f(1)$ .

Preuve

On pose  $a = f(1)$ , on montre que  $\forall n \in \mathbb{N}, f(n) = an$  (récurrence), on en déduit que  $f(-n) = a(-n)$  car  $f(-n) = -f(n)$ , d'où :  $\forall n \in \mathbb{Z}, f(n) = an$ .

Soit  $r = \frac{p}{q}$  un rationnel avec  $q \in \mathbb{N}^*$ , alors  $f(qr) = f(p) = ap = qf(r)$  d'où  $f(r) = ar$ .

Soit  $x \in \mathbb{R}$  et  $(r_n)$  une suite de rationnels qui converge vers  $x$ , alors  $(x - r_n)$  converge vers 0 et donc  $f(x - r_n)$  tend vers  $f(0) = 0$ , or  $f(x - r_n) = f(x) - f(r_n)$  donc  $(f(r_n))$  converge vers  $f(x)$ . Or  $f(r_n) = ar_n \longrightarrow ax$ , par conséquent  $f(x) = ax$ .

**Proposition 2.5** Soit  $f : G \longrightarrow H$  un morphisme de groupes.

L'image directe par  $f$  de tout sous-groupe de  $G$  est un sous-groupe de  $H$ . En particulier,  $\text{Im}(f)$  est un sous-groupe de  $H$ .

Preuve

Soit  $K$  un sous-groupe de  $G$ . Montrons que  $f(K)$  est un sous-groupe de  $H$ .

1) Comme  $e_G \in K$  alors  $f(e_G) \in f(K)$ .

2) Soient  $a, b \in f(K)$ . Alors, il existe  $x, y \in K$  tel que  $a = f(x)$  et  $b = f(y)$ . Ainsi

$$ab^{-1} = f(x) f(y^{-1}) = f(xy^{-1})$$

or  $xy^{-1} \in K$  donc  $ab^{-1} \in f(K)$ .

En somme,  $f(K)$  est un sous-groupe de  $H$ .

On déduit aussi que  $\text{Im}(f) = f(G)$  est un sous-groupe de  $H$ .

**Proposition 2.6** Soit  $f : G \longrightarrow H$  un morphisme de groupes.

L'image réciproque par  $f$  de tout sous-groupe de  $H$  est un sous-groupe de  $G$  contenant  $\ker f$ . En particulier,  $\ker(f)$  est un sous-groupe de  $G$ .

Preuve (Exercice!)

**Proposition 2.7** Soit  $f : G \longrightarrow H$  un morphisme de groupes.

$$f \text{ injective} \Leftrightarrow \ker f = \{e_G\}.$$

Preuve

Supposons  $f$  injective. Pour tout  $x \in \ker f$  on a  $f(x) = f(e_G)$ . Le caractère injectif de  $f$  implique que  $x = e_G$ , donc  $\ker f = \{e_G\}$ .

Supposons  $\ker f = \{e_G\}$ .

Soient  $x, y \in G$  tels que  $f(x) = f(y)$ . On a  $f(x).(f(y))^{-1} = e_H$ . Comme  $(f(y))^{-1} = f(y^{-1})$  on a  $f(x).f(y^{-1}) = e_H$ . Ainsi  $f(xy^{-1}) = e_H$ , d'où  $xy^{-1} \in \ker f$  et comme  $\ker f = \{e_G\}$ , on a  $xy^{-1} = e_G$ , c'est à dire que  $x = y$ . Donc  $f$  est injective.

**Exercice**

1) Caractériser les homomorphismes de groupes de  $(\mathbb{Z}, +)$  vers  $(\mathbb{Z}, +)$ .

En déduire les isomorphismes de groupes de  $(\mathbb{Z}, +)$  sur  $(\mathbb{Z}, +)$ .

2) Caractériser les homomorphismes de groupes  $(\mathbb{Q}, +)$  vers  $(\mathbb{Q}, +)$ .

## 2.5 Groupes quotients

Soient  $(G, \cdot)$  un groupe et  $H$  un sous-groupe de  $G$ .

On définit sur  $G$  la relation  $\mathcal{R}_g$  par

$$\forall x, y \in G, \quad x \mathcal{R}_g y \iff x^{-1}y \in H.$$

La relation  $\mathcal{R}_g$  est une relation d'équivalence sur  $G$ .

La classe d'équivalence de  $x \in G$ , notée  $xH$  est

$$xH = \{ y \in G / \exists h \in H, \quad y = xh \}.$$

L'ensemble  $G/\mathcal{R}_g$  des classes d'équivalence est appelé *ensemble des classes à gauche modulo  $H$* .

De même la relation  $\mathcal{R}_d$  définie par

$$\forall x, y \in G, \quad x \mathcal{R}_d y \iff yx^{-1} \in H$$

est une relation d'équivalence sur  $G$ .

La classe de  $x \in G$  pour cette relation est le sous-ensemble

$$Hx = \{ y \in G / \exists h \in H, \quad y = hx \}.$$

L'ensemble quotient  $G/\mathcal{R}_d$  est *l'ensemble des classes à droite modulo  $H$* .

**Définition 2.5** *Le sous-groupe  $H$  du groupe  $(G, \cdot)$  est un **sous-groupe distingué** du groupe  $(G, \cdot)$  si*

$$\forall x \in G, \quad xH = Hx.$$

*Si  $H$  est un sous-groupe distingué de  $G$ , on écrit  $H \triangleleft G$ .*

### Exemple

Les sous-groupes d'un groupe commutatif sont distingués.

Les sous-groupes de  $(\mathbb{Z}, +)$  sont donc des sous-groupes distingués.

**Proposition 2.8** *Soit  $H$  un sous-groupe du groupe  $(G, \cdot)$ . Les assertions suivantes sont équivalentes.*

- i)  $H$  est un sous-groupe distingué du groupe  $(G, \cdot)$ ,*
- ii)  $\forall x \in G, \quad xHx^{-1} = H,$*
- iii)  $\forall x \in G, \forall h \in H, \quad xhx^{-1} \in H,$*
- iv)  $\forall x \in G, \quad xH \subset Hx,$*

$$v) \forall x \in G, \quad Hx \subset xH.$$

**Preuve** (exercice!).

**Proposition 2.9** Soit  $f : (G_1, *) \longrightarrow (G_2, \top)$  un morphisme de groupes. Alors le noyau  $\ker f$  est un sous-groupe distingué de  $G_1$ .

**Preuve**

$\forall x \in G, \forall h \in \ker f$  on a

$$f(x*h*x^{-1}) = f(x)\top f(h)\top f(x^{-1}) = f(x)\top_{e_{G_2}}\top f(x^{-1}) = f(x)\top f(x^{-1}) = f(x*x^{-1}) = f(e_{G_1})$$

Comme  $f(e_{G_1}) = e_{G_2}$  on a  $x * h * x^{-1} \in \ker f$

### 2.5.1 Congruences modulo un sous-groupe

**Définition 2.6** Soit  $(G, .)$  un groupe.

On dit qu'une relation d'équivalence  $\mathcal{R}$  sur  $G$  est une **congruence** si elle est compatible avec la loi du groupe, c'est à dire

$$\forall a, a', b, b' \in G \quad a \mathcal{R} a' \quad \text{et} \quad b \mathcal{R} b' \quad \Rightarrow \quad a.b \mathcal{R} a'.b'$$

**Exemple**

Soit  $n \in \mathbb{N}$ . On considère le groupe additif  $(\mathbb{Z}, +)$ .

La relation  $\mathcal{R}_n$  d'équivalence modulo  $n$  est une congruence.

**Proposition 2.10** Soient  $\mathcal{R}$  une congruence sur le groupe  $G$  et  $H = \bar{1}_G$  la classe de l'élément neutre  $1_G$  de  $G$ . Alors  $H$  est un sous-groupe de  $G$ .

**Preuve**

1) il est évident que  $1_G \in H = \bar{1}_G$ .

2)  $\forall x, y \in H$  on a  $x \mathcal{R} 1_G$  et  $y \mathcal{R} 1_G$ .

Les relations  $1_G \mathcal{R} y$  et  $y^{-1} \mathcal{R} y^{-1}$  entraînent par compatibilité

$$y^{-1} \mathcal{R} 1_G.$$

Les relations  $x \mathcal{R} 1_G$  et  $y^{-1} \mathcal{R} 1_G$  entraînent par compatibilité que

$$xy^{-1} \mathcal{R} \bar{1}_G,$$

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

On conclut que  $H$  est un sous-groupe de  $G$ .

**Théorème 2.3** Soient  $(G, \cdot)$  un groupe,  $H$  un sous-groupe distingué de  $(G, \cdot)$ . La relation binaire sur  $(G, \cdot)$  définie par  $\forall x, y \in G, \quad x \mathcal{R} y \Leftrightarrow x^{-1}y \in H$  est une congruence sur  $G$ , l'ensemble quotient  $G/\mathcal{R}$  muni de la loi quotient est un groupe, on le note  $G/H$ . On l'appelle le groupe quotient de  $G$  par  $H$ . L'application surjective  $j : G \longrightarrow G/H$  définie par  $j(x) = \bar{x}$  est un morphisme de groupes.

Notons que la loi quotient est définie par  $\forall \bar{x}, \bar{y} \in G/\mathcal{R}, \quad \bar{x} \cdot \bar{y} = \overline{x \cdot y}$

**Exemple** (cf. page 24)

Soit  $n \in \mathbb{N}$ . La relation d'équivalence  $\mathcal{R}_n$  sur  $\mathbb{Z}$  définie par

$$\forall x, y \in \mathbb{Z}, \quad x \mathcal{R}_n y \Leftrightarrow x - y \in n\mathbb{Z}$$

est une congruence sur  $\mathbb{Z}$ . L'ensemble  $(\mathbb{Z}/n\mathbb{Z}, +)$  est un groupe abélien ayant  $n$  éléments. (rappelons que  $\forall \bar{x}, \bar{y} \in \mathbb{Z}/n\mathbb{Z}, \quad \bar{x} + \bar{y} = \overline{x + y}$ ).

**Exercice**

Montrer que les sous-groupes de  $(\mathbb{Z}/n\mathbb{Z}, +)$  sont de la forme  $(p\mathbb{Z}/n\mathbb{Z})$  où  $p$  est un entier naturel divisant  $n$ .

(indication : on pourra utiliser la surjection canonique  $s : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ ).

## 2.5.2 Théorème de Lagrange

**Théorème 2.4** (de **LAGRANGE**)

Soient  $G$  un groupe **fini** et  $H$  est un sous-groupe de  $G$ .

Alors  $\text{card}(H)$  divise  $\text{card}(G)$ . En particulier l'ordre de tout élément de  $G$  divise  $\text{card}(G)$ .

Preuve

Le groupe  $G$  étant fini, le nombre de classes d'équivalence à gauche modulo  $H$  est fini. Posons  $n = \text{card}(G/\mathcal{R}_g)$ . Il existe donc des éléments  $x_1, \dots, x_n$  dans  $G$  tels que

$$G/\mathcal{R}_g = \{x_1H, \dots, x_nH\}$$

Rappelons que pour tout  $x \in G$ , l'application  $H \longrightarrow xH, h \longmapsto xh$  est bijective, donc  $\text{card}(xH) = \text{card}(H)$ .

Puisque  $G = \bigcup_{i=1}^n x_iH$  et les classes d'équivalence sont deux à deux disjointes, on a

$$\text{card}(G) = \text{card}(x_1H) + \dots + \text{card}(x_nH).$$

Et comme  $\forall i = 1, \dots, n, \quad \text{card}(x_iH) = \text{card}(H)$ , on déduit que

$$\text{card}(G) = n \text{card}(H)$$

d'où  $\text{card}(H)$  divise  $\text{card}(G)$ .

**Théorème 2.5** Soient  $n \in \mathbb{N}$  et  $p \in \mathbb{N}$ . Alors  $p$  divise  $n$  si et seulement si le groupe  $(\mathbb{Z}/n\mathbb{Z}, +)$  admet un (unique) sous-groupe de cardinal  $p$ . Précisément, les sous-groupes du groupe  $(\mathbb{Z}/n\mathbb{Z}, +)$  sont de la forme  $k\mathbb{Z}/n\mathbb{Z}$  où  $k \in \mathbb{N}$  divise  $n$ .

**Remarque 2.5** Soit  $n \in \mathbb{N}$ . D'après le théorème précédent, le nombre de sous-groupes du groupe  $(\mathbb{Z}/n\mathbb{Z}, +)$  est égal au nombre d'entiers naturels qui divisent  $n$ .

### Exercice

- 1) Déterminer tous les sous-groupes du groupe  $(\mathbb{Z}/24\mathbb{Z}, +)$ .
- 2) Déterminer tous les sous-groupes du groupe  $(\mathbb{Z}/29\mathbb{Z}, +)$ .

## 3 STRUCTURES D'ANNEAUX ET CORPS

### 3.1 Définition et exemples

**Définition 3.1** Soit  $(A, +, \cdot)$  un ensemble muni de deux lois de composition internes. On dit que  $(A, +, \cdot)$  est un **anneau** si les conditions suivantes sont satisfaites :

- i)  $(A, +)$  est un groupe abélien,
- ii) la seconde loi " $\cdot$ " est associative, c'est à dire

$$\forall a, b, c \in A, \quad a(bc) = (ab)c$$

- iii) la seconde loi est distributive par rapport à la première, c'est à dire :

$$\forall a, b, c \in A, \quad a(b+c) = ab+ac \quad \text{et} \quad (a+b)c = ac+bc.$$

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

Si la loi  $\cdot$  possède un élément neutre, on dit que  $A$  est un **anneau unitaire**, cet élément neutre se note  $1$  ou  $1_A$  et s'appelle **élément unité**.

#### Exemples

1)  $(\mathbb{R}, +, \times)$ ,  $(\mathbb{Z}, +, \times)$  sont des anneaux commutatifs unitaires.

2) Si  $(G, +)$  est un groupe abélien,  $(\text{End}(G), +, \circ)$  est un anneau en posant :

$$\forall f, g \in \text{End}(G), \quad f+g : x \mapsto f(x) + g(x) \quad \text{et} \quad f \circ g : x \mapsto f(g(x))$$

3) Si  $(A, +, \times)$  est un anneau unitaire et  $E$  un ensemble non vide alors l'ensemble  $\mathcal{A}(E, A)$  des applications de  $E$  vers  $A$ , est un anneau unitaire pour les lois définies par :

$$\forall f, g \in \mathcal{A}(E, A), \quad f+g : x \mapsto f(x) + g(x) \quad \text{et} \quad f.g : x \mapsto f(x).g(x).$$

Ainsi, par exemple  $\mathcal{A}(\mathbb{N}, \mathbb{R})$  est un anneau pour les lois usuelles (c'est l'anneau des suites réelles).

#### Exercice

Soit  $E$  un ensemble. Montrer que  $(\mathcal{P}(E), \Delta, \cap)$  est un anneau commutatif unitaire.

### 3.2 L'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ , $n \in \mathbb{N}$

Soit  $n \in \mathbb{N}$ . Étant donnés  $x, y \in \mathbb{Z}$ , on dit que  $x$  est **congru** à  $y$  **modulo**  $n$  si et seulement si  $n$  divise  $y - x$ . On écrit alors

$$x \equiv y \pmod{n}$$

**Proposition 3.1** *La relation de congruence modulo  $n$  est une relation d'équivalence sur  $\mathbb{Z}$ .*

Preuve

Réflexivité :

pour tout  $x \in \mathbb{Z}$ , on a  $x - x = 0$  et on sait que  $n$  divise 0, d'où  $n$  divise  $x - x$  et

$$x \equiv x \pmod{n}$$

Symétrie :

Soient  $x, y \in \mathbb{Z}$  tels que  $x \equiv y \pmod{n}$ . Alors il existe  $k \in \mathbb{N}$  tel que  $y - x = nk$ . Ainsi, on a  $x - y = n(-k)$  avec  $-k \in \mathbb{Z}$ , donc  $y \equiv x \pmod{n}$ . En somme,

$$x \equiv y \pmod{n} \Leftrightarrow y \equiv x \pmod{n}$$

Transitivité :

Soient  $x, y, z \in \mathbb{Z}$  tels que  $x \equiv y \pmod{n}$  et  $y \equiv z \pmod{n}$ . Alors il existe des entiers  $k, q \in \mathbb{Z}$  tels que  $y - x = nk$  et  $z - y = nq$ . On déduit que  $z - x = n(k + q)$  avec  $k + q \in \mathbb{Z}$ , donc  $x \equiv z \pmod{n}$ . En somme

$$x \equiv y \pmod{n} \text{ et } y \equiv z \pmod{n} \Rightarrow x \equiv z \pmod{n}$$

La relation de congruence modulo  $n$  étant à la fois réflexive, symétrique et transitive sur  $\mathbb{Z}$ , c'est donc une relation d'équivalence sur  $\mathbb{Z}$ .  $\square$

Pour tout  $x \in \mathbb{Z}$ , on note  $\bar{x}$  la **classe d'équivalence** de  $x$  modulo  $n$ , c'est à dire l'ensemble  $\{y \in \mathbb{Z} / x \equiv y \pmod{n}\}$  (dans certains ouvrages, cet ensemble est noté  $x + n\mathbb{Z}$ )

**Propriétés 1** *Compatibilité avec l'addition et la multiplication*

Soient  $a, b, c, d$  des entiers relatifs.

- (1) Si  $a \equiv b \pmod{n}$  et  $c \equiv d \pmod{n}$  alors  $a + c \equiv b + d \pmod{n}$
- (2) Si  $a \equiv b \pmod{n}$  et  $c \equiv d \pmod{n}$  alors  $ac \equiv bd \pmod{n}$

Preuve

Supposons  $a \equiv b \pmod{n}$  et  $c \equiv d \pmod{n}$ . Il existe  $k, q \in \mathbb{Z}$  tels que  $b - a = nk$  et  $d - c = nq$ .

(1) Alors  $(b + d) - (a + c) = n(k + q)$  avec  $k + q \in \mathbb{Z}$ , donc  $a + c \equiv b + d \pmod{n}$ .

(2) On a  $b = a + nk$  et  $d = c + nq$ . Par conséquent,  $bd = (a + nk)(c + nq)$ , autrement dit  $bd = ac + anq + nkc + n^2kq$ . Ainsi  $bd - ac = n(aq + kc + nkq)$  avec  $aq + kc + nkq \in \mathbb{Z}$ , d'où  $ac \equiv bd \pmod{n}$ .  $\square$

**Corollaire 3.1** *Soient  $x, y \in \mathbb{Z}$*

- (i)  $\forall k \in \mathbb{N}, x \equiv y \pmod{n} \Rightarrow kx \equiv ky \pmod{n}$   
(ii)  $\forall k \in \mathbb{N}^*, x \equiv y \pmod{n} \Rightarrow x^k \equiv y^k \pmod{n}$

Preuve (exercice facile!)

Notons par  $\mathbb{Z}_n$  l'ensemble des classes d'équivalence modulo  $n$ . Cet ensemble est par définition l'**ensemble quotient modulo  $n$** .

**Proposition 3.2** Soit  $n \in \mathbb{N}, n \neq 0$ .

L'ensemble quotient  $\mathbb{Z}_n$  est fini, précisément cet ensemble contient exactement  $n$  éléments.

$$\mathbb{Z}_n = \{\bar{0}, \dots, \overline{n-1}\}$$

Preuve

Soit  $x \in \mathbb{Z}$ . D'après la division euclidienne de  $x$  par  $n$ , il existe  $q, r \in \mathbb{Z}$  tels que

$$x = nq + r$$

avec  $0 \leq r < n$ . Ainsi, l'entier  $n$  divise  $x - r$ , donc  $\bar{x} = \bar{r}$ . Aussi, il n'est pas difficile de prouver que les éléments  $\bar{y}, y = 0, \dots, n-1$  sont deux à deux distincts. On déduit que  $\mathbb{Z}_n = \{\bar{0}, \dots, \overline{n-1}\}$  et  $\text{card}(\mathbb{Z}_n) = n$ .  $\square$

On définit sur l'ensemble  $\mathbb{Z}_n$  deux lois de composition interne : Pour tout  $x, y \in \mathbb{Z}$ , on pose

$$\bar{x} + \bar{y} = \overline{x + y} \quad \text{et} \quad \bar{x} \times \bar{y} = \overline{x \times y} \quad (*)$$

Ces deux lois sont bien définies d'après les propriétés de compatibilité avec l'addition et la multiplication (cf. Propriété 1)

**Théorème 3.1** Pour tout entier  $n \in \mathbb{N}$ ,  $(\mathbb{Z}_n, +, \times)$  est un anneau commutatif unitaire.

Cet anneau est souvent noté  $\mathbb{Z}/n\mathbb{Z}$ , appelé l'**anneau quotient modulo  $n$** . Le groupe  $(\mathbb{Z}_n, +)$  est aussi noté  $\mathbb{Z}/n\mathbb{Z}$  et appelé le groupe quotient modulo  $n$ .

Preuve

Montrons que  $(\mathbb{Z}_n, +)$  est un groupe commutatif.

Associativité :

Soient  $x, y, z \in \mathbb{Z}$ . On a

$$\bar{x} + (\bar{y} + \bar{z}) = \bar{x} + \overline{y + z} = \overline{x + (y + z)} = \overline{(x + y) + z} = \overline{x + y} + \bar{z} = (\bar{x} + \bar{y}) + \bar{z}$$

Donc  $\bar{x} + (\bar{y} + \bar{z}) = (\bar{x} + \bar{y}) + \bar{z}$ .

Commutativité :

Pour tout  $x, y \in \mathbb{Z}$ , on a

$$\bar{x} + \bar{y} = \overline{x + y} = \overline{y + x} = \bar{y} + \bar{x}$$

Donc  $\bar{x} + \bar{y} = \bar{y} + \bar{x}$ .

Élément neutre :

Pour tout  $x \in \mathbb{Z}$ , on a

$$\bar{x} + \bar{0} = \overline{x + 0} = \bar{x}$$

et

$$\bar{0} + \bar{x} = \overline{0 + x} = \bar{x}$$

Donc  $\bar{0}$  est l'élément neutre dans  $(\mathbb{Z}_n, +)$ .

Éléments symétriques :

Pour tout  $x \in \mathbb{Z}$ , on a

$$\bar{x} + \overline{-x} = \overline{x + (-x)} = \bar{0}$$

et

$$\overline{-x} + \bar{x} = \overline{(-x) + x} = \bar{0}$$

Donc  $\overline{-x}$  est le symétrique de  $\bar{x}$  dans  $(\mathbb{Z}_n, +)$ . Ainsi  $-\bar{x} = \overline{-x}$ .

En somme,  $(\mathbb{Z}_n, +)$  est un groupe commutatif.

D'autre part, pour tout  $x, y, z \in \mathbb{Z}$ , on a

$$(\bar{x} \bar{y}) \bar{z} = \overline{xy} \bar{z} = \overline{(xy)z} = \overline{x(yz)} = \bar{x} \bar{y} \bar{z} = \bar{x} (\bar{y} \bar{z})$$

Donc  $(\bar{x} \bar{y}) \bar{z} = \bar{x} (\bar{y} \bar{z})$  d'où l'associativité de la deuxième loi.

On a aussi

$$\bar{x} \bar{y} = \overline{xy} = \overline{yx} = \bar{y} \bar{x}$$

Donc  $\bar{x} \bar{y} = \bar{y} \bar{x}$  et la deuxième loi est commutative.

Il n'est pas difficile de prouver que

$$\bar{x} (\bar{y} + \bar{z}) = \bar{x} \bar{y} + \bar{x} \bar{z}$$

et

$$(\bar{y} + \bar{z}) \bar{x} = \bar{y} \bar{x} + \bar{z} \bar{x}$$

D'où la distributivité de la loi quotient  $\times$  par rapport à la loi quotient  $+$ .

De plus  $\bar{1}$  est l'élément neutre dans  $(\mathbb{Z}_n, \times)$ .

De tout ce qui précède, on déduit que  $(\mathbb{Z}_n, +, \times)$  est un anneau commutatif unitaire.

### Exercice

1) Établir la table de  $\mathbb{Z}/2\mathbb{Z}$  la loi  $+$ , puis la loi  $\times$ .

2) Mêmes questions avec les anneaux  $\mathbb{Z}/3\mathbb{Z}$ ,  $\mathbb{Z}/6\mathbb{Z}$ .

## 3.3 Calculs dans un anneau

Soit  $(A, +, \cdot)$  un anneau unitaire. On a les propriétés suivantes

1)  $\forall x \in A \quad x \cdot 0 = 0 = 0 \cdot x$

2)  $\forall x, y \in A \quad x(-y) = -(xy) = (-x)y$

3)  $\forall x, y, z \in A \quad x(y - z) = xy - xz$  et  $(x - y)z = xz - yz$

4)  $\forall x, y, z, t \in A \quad (x + y)(z + t) = xz + xt + yz + yt$

5)  $\forall x, y \in A \quad (x + y)^2 = x^2 + xy + yx + y^2$

Preuve

1) Pour tout  $x \in A$ , on a  $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$  donc  $x \cdot 0 = x \cdot 0 + x \cdot 0$ , par conséquent,  $x \cdot 0 = 0$ . De même, on montre que  $0 \cdot x = 0$ .

2) Pour tout  $x, y \in A$ , on a

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

donc  $x(-y) + xy = 0$ . Ainsi,  $x(-y) = -(xy)$ . De même, on montre que  $(-xy) = -(xy)$ .

3) Pour tout  $x, y, z \in A$ , on

$$x(y - z) = x(y + (-z)) = xy + x(-z) = xy + (-(xz)) = xy - (xz)$$

Donc  $x(y - z) = xy - xz$ . On montre de même que  $(x - y)z = xz - yz$ .

4) Pour tout  $x, y, z, t \in A$ , on a  $(x + y)(z + t) = x(z + t) + y(z + t) = xz + xt + yz + yt$ .

5) C'est une conséquence immédiate de 4).

Insistons sur le fait que l'on peut avoir  $xy = 0$  sans que  $x$  ou  $y$  soit nul, et même  $x^n = 0$  sans que  $x$  soit nul. Par exemple, dans l'anneau  $\mathbb{Z}/6\mathbb{Z}$ , on a  $\bar{2} \cdot \bar{3} = \bar{0}$ , mais  $\bar{2} \neq 0$  et  $\bar{3} \neq 0$ . Dans l'anneau  $\mathbb{Z}/4\mathbb{Z}$ , on a  $\bar{2} \neq 0$  mais  $\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$ .

### Formule du binôme de Newton

Soient  $A$  un anneau,  $n \in \mathbb{N}$  et  $a, b \in A$ . Alors

$$\text{Si } ab = ba \text{ alors } (a + b)^n = \sum_{k=0}^n C_n^k a^k b^{n-k}$$

**Définition 3.2** Soit  $A$  un anneau, on dit que  $a \in A$  est un **diviseur** de zéro dans  $A$  si  $a \neq 0$  et s'il existe  $b \in A$ ,  $b \neq 0$  tel que

$$ab = 0 \quad \text{ou} \quad ba = 0.$$

### Exemples

Dans l'anneau  $\mathbb{Z}/6\mathbb{Z}$ , l'élément  $\bar{3}$  est un diviseur de  $\bar{0}$ .

### Exercice

Déterminer tous les diviseurs de  $\bar{0}$  de l'anneau  $\mathbb{Z}/24\mathbb{Z}$ .

**Définition 3.3** On dit que l'anneau  $A$  est **intègre** si l'anneau  $A$  est commutatif, non réduit à zéro et dépourvu de diviseurs de zéro, c'est à dire que

$$\forall a, b \in A, \quad ab = 0 \quad \Rightarrow \quad a = 0 \quad \text{ou} \quad b = 0.$$

### Exemples

$\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  sont des anneaux intègres.

**Proposition 3.3** Soit  $m \in \mathbb{N}$ .

L'anneau  $\mathbb{Z}/m\mathbb{Z}$  est intègre si et seulement si  $m = 0$  ou  $m$  est un nombre premier.

Preuve (exercice)

**Théorème-Définition 3.1** Soit  $A$  un anneau unitaire, si  $x \in A$  admet un symétrique pour la multiplication, on dit que  $x$  est une **unité** de  $A$ . On dit aussi que  $x$  est un élément **inversible** de  $A$ . L'ensemble des éléments inversibles de  $A$  se note  $U(A)$ .

L'ensemble  $U(A)$  est stable pour la multiplication, et muni de la multiplication induite  $U(A)$  est un groupe dont  $1_A$  est l'élément neutre.

Preuve (facile) laissée au lecteur.

### Exemples

- 1)  $U(\mathbb{Z}) = \{-1, 1\}$
- 2)  $U(\mathbb{R}) = \mathbb{R} \setminus \{0\}$ .

**Proposition 3.4** Soient  $m \in \mathbb{N}$  et  $x \in \mathbb{Z}$ .

L'élément  $\bar{x}$  est un élément inversible de l'anneau  $\mathbb{Z}/m\mathbb{Z}$  si et seulement si  $\text{PGCD}(m, x) = 1$ .

Preuve

$\bar{x}$  inversible dans l'anneau  $\mathbb{Z}/m\mathbb{Z}$  si et seulement si il existe  $u \in \mathbb{Z}$  tel que  $\bar{x}\bar{u} = \bar{1}$ . Ceci équivaut à dire que l'entier  $m$  divise  $xu - 1$ , c'est à dire qu'il existe  $v \in \mathbb{Z}$  tel que  $ux + mv = 1$ , autrement dit  $\text{PGCD}(m, x) = 1$  d'après le théorème de Bézout.

**Exercice**

(1) Pour chacun des anneaux suivants, déterminer les éléments inversibles :

$\mathbb{Z}/12\mathbb{Z}$ ,  $\mathbb{Z}/24\mathbb{Z}$ ,  $\mathbb{Z}/32\mathbb{Z}$ ,  $\mathbb{Z}/13\mathbb{Z}$ .

(2) Pour chacun des éléments inversibles de l'anneau  $\mathbb{Z}/24\mathbb{Z}$  déterminer son inverse.

**Théorème 3.2** Soit  $n_1, n_2, \dots, n_r$  une suites d'entiers positifs, premiers entre eux deux à deux. Alors le système de congruences

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

a une unique solution  $x$  modulo  $N = n_1 n_2 \dots n_r$ .

$$x = a_1 N_1 y_1 + a_2 N_2 y_2 + \dots + a_r N_r y_r$$

avec  $N_i = \frac{N}{n_i}$  et  $y_i N_i \equiv 1 \pmod{n_i}$  pour  $i = 1, \dots, r$ .

**Exercice**

1) Résoudre le système de congruence suivant :

$$\begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 5 \pmod{11} \end{cases}$$

2) Résoudre le système de congruence suivant :

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

### 3.4 Sous-anneaux

**Définition 3.4** Soient  $A$  un anneau unitaire et  $B \subseteq A$ . On dit que  $B$  est un sous-anneau de  $A$  si :

- i)  $B$  est stable pour les deux lois,
- ii)  $1_A \in B$ ,
- iii)  $B$  muni des deux lois induites a une structure d'anneau.

**Proposition 3.5** Soient  $A$  un anneau unitaire et  $B \subseteq A$ . Alors  $B$  est un sous-anneau de  $A$  si et seulement si :

- i)  $\forall a, b \in B, \quad a - b \in B$ ,
- ii)  $1_A \in B$ ,
- iii)  $\forall a, b \in B, \quad ab \in B$ .

### 3.5 Idéal d'un anneau commutatif

**Définition 3.5** Soient  $A$  un anneau commutatif,  $I$  une partie de  $A$ .

On dit que  $I$  est **un idéal** de  $A$  si :

- i)  $(I, +)$  est un sous-groupe de  $(A, +)$
- ii)  $\forall a \in A, \quad \forall x \in I, \quad ax \in I$

#### Exemples

- 1)  $\mathbb{Z}$  est un sous-anneau de  $\mathbb{Q}$  mais n'est pas un idéal de  $\mathbb{Q}$ .
- 2) Les idéaux de  $\mathbb{Z}$  sont exactement les sous-ensembles  $n\mathbb{Z}$  où  $n \in \mathbb{N}$ .

**Proposition 3.6** Soient  $A$  un anneau commutatif et  $I$  un sous-ensemble de  $A$ .

Alors  $I$  est un idéal de  $A$  si et seulement si les trois propriétés suivantes sont satisfaites :

- 1)  $0 \in I$
- 2)  $\forall x, y \in I, \quad x - y \in I$
- 3)  $\forall a \in A, \quad \forall x \in I, \quad ax \in I$ .

#### Exercice

Soient  $I$  et  $J$  deux idéaux de l'anneau  $A$ .

On pose  $I + J = \{x \in A / \exists a \in I, b \in J, \quad x = a + b\}$ .

Montrer que  $I + J$  est un idéal de  $A$ .

**Définition 3.6** Soit  $A$  un anneau commutatif. Un idéal  $I$  de  $A$  est dit **principal** s'il existe  $a \in A$  tel que  $I = aA = \{x \in A / \exists b \in A, x = ab\}$ .

On dit que  $A$  est un **anneau principal** s'il est commutatif, intègre et si tout idéal de  $A$  est principal.

Par exemple, l'anneau  $\mathbb{Z}$  est un anneau principal.

Nous verrons par la suite que l'anneau  $K[X]$  des polynômes en une indéterminée, à coefficients dans le corps commutatif  $K$  est un anneau principal.

**Proposition 3.7** Soit  $A$  un anneau commutatif.

Une intersection quelconque d'idéaux de  $A$  est un idéal de  $A$ . En particulier, si  $I$  et  $J$  sont des idéaux de  $A$  alors  $I \cap J$  est un idéal de  $A$ .

**Preuve** (exercice!)

**Théorème 3.3** Soit  $A$  un anneau commutatif. Si  $I$  est un idéal de  $A$  alors la relation binaire définie sur  $A$  par :

$$\forall x, y \in A, \quad x \mathcal{R} y \iff x - y \in I$$

est une relation d'équivalence, compatible avec les deux lois de l'anneau  $A$ .

L'ensemble quotient, noté  $A/I$ , muni des deux lois quotients est un anneau commutatif appelé **anneau quotient** de  $A$  par l'idéal  $I$ .

Rappelons que les deux lois quotients sont définies de la façon suivante :

$$\forall x, y \quad \overline{x \cdot y} = \overline{x} \overline{y} \quad \text{et} \quad \overline{x + y} = \overline{x} + \overline{y}$$

Par exemple  $\mathbb{Z}/n\mathbb{Z}$  est un anneau commutatif unitaire.

## 3.6 Morphisme d'anneaux

**Définition 3.7** Soient  $A, B$  deux anneaux unitaires, et  $f : A \rightarrow B$  une application. On dit que  $f$  est un **morphisme d'anneaux** (ou un homomorphisme) de  $A$  dans  $B$  si

- i)  $f(1_A) = 1_B$ ,
- ii)  $\forall a, b \in A \quad f(a + b) = f(a) + f(b)$ ,
- iii)  $\forall a, b \in A \quad f(ab) = f(a)f(b)$ .

On définit de façon évidente les notions d'endomorphisme, d'isomorphisme et d'automorphisme d'anneaux.

**Théorème 3.4** Soit  $f : A \longrightarrow B$  un morphisme d'anneaux.

- (i) Si  $A'$  est un sous-anneau de  $A$  alors  $f(A')$  est un sous-anneau de  $B$ .
- (ii) Si  $B'$  est un sous-anneau de  $B$  alors  $f^{-1}(B')$  est un sous-anneau de  $A$ .
- (iii) Si  $A$  et  $B$  sont commutatifs, et si  $I'$  est un idéal de  $B$  alors  $f^{-1}(I')$  est un idéal de  $A$ .

En particulier,  $\ker f = \{x \in A / f(x) = 0\}$  est un idéal de  $A$ .

**Proposition 3.8** Soit  $f : A \longrightarrow B$  un morphisme d'anneaux. On a l'équivalence

$$f \text{ injectif} \Leftrightarrow \ker f = \{0\}.$$

**Preuve**

Le morphisme d'anneaux est un morphisme de groupes. D'après la proposition 2.7, on a le résultat.

**Théorème 3.5** Soient  $A, B, C$  trois anneaux.

- (i) Si  $f : A \longrightarrow B$  et  $g : B \longrightarrow C$  sont des morphismes d'anneaux alors  $g \circ f : A \longrightarrow C$  est un morphisme d'anneaux.
- (ii) Si  $f : A \longrightarrow B$  est un isomorphisme d'anneaux alors  $f^{-1}$  est un isomorphisme de  $B$  sur  $A$ .
- (iii)  $(\text{End}(A), +, \circ)$  est un anneau, dont le groupe des unités est  $(\text{Aut}(A), \circ)$ .

**Théorème 3.6 (Transport de structure)**

Si  $A$  est un anneau et  $f$  une bijection de  $A$  sur un ensemble  $E$ , alors on peut définir deux lois sur  $E$ , de sorte que  $f$  devienne un isomorphisme d'anneaux.

Les démonstrations de ces deux théorèmes sont tout à fait évidentes et laissées au lecteur.

## 3.7 Corps

**Définition 3.8** Soit  $\mathbb{K}$  un ensemble non vide muni de deux lois  $+$  et  $\times$  de composition interne. On dit que  $(\mathbb{K}, +, \times)$  est un **corps** si

- i)  $(\mathbb{K}, +, \times)$  est un anneau unitaire, et  $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$ ,
- ii)  $\forall x \in \mathbb{K} \setminus \{0_{\mathbb{K}}\}, \exists x' \in \mathbb{K}, x x' = 1_{\mathbb{K}} = x' x$ .

Si de plus la multiplication est commutative, on dit que  $\mathbb{K}$  est un **corps commutatif**.

**Remarque 3.1** 1) Si  $(\mathbb{K}, +, \times)$  est un corps alors  $\mathbb{K} \setminus \{0\}$  est un groupe pour la loi  $\times$ , qui est abélien si et seulement si le corps  $\mathbb{K}$  est commutatif.

2) Tout corps est un anneau intègre (la réciproque est fautive, par exemple, l'anneau  $\mathbb{Z}$  est intègre mais n'est pas un corps). Un corps est donc en particulier un anneau sans diviseurs de zéro.

3) Si  $I$  est un idéal du corps  $\mathbb{K}$  alors  $I = \{0\}$  ou  $I = \mathbb{K}$ .

### Exemples

1)  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  sont des corps commutatifs pour les lois usuelles.

2)  $\mathbb{Q}[\sqrt{2}] = \{x \in \mathbb{R} / \exists a, b \in \mathbb{Q}, x = a + b\sqrt{2}\}$  est un corps commutatif (le démontrer!).

**Proposition 3.9** Soit  $m \in \mathbb{N}$ .

L'anneau  $\mathbb{Z}/m\mathbb{Z}$  est un corps si et seulement si  $m$  est un nombre premier.

Preuve

Supposons que l'anneau  $\mathbb{Z}/m\mathbb{Z}$  soit un corps. Alors l'anneau  $\mathbb{Z}/m\mathbb{Z}$  est intègre et d'après la proposition 3.3,  $m = 0$  ou bien  $m$  est un nombre premier. On sait que si  $m = 0$ , on a  $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/0\mathbb{Z}$  qui est isomorphe à  $\mathbb{Z}$  et on sait que l'anneau  $\mathbb{Z}$  n'est pas intègre. Forcément  $m$  est un nombre premier. Réciproquement, si  $m$  est un nombre premier alors pour tout entier  $x$  tel que  $1 \leq x \leq m - 1$ , on a  $PGCD(x, m) = 1$  et d'après la proposition 3.4,  $\bar{x}$  est un élément inversible de l'anneau  $\mathbb{Z}/m\mathbb{Z}$ . Donc l'anneau  $\mathbb{Z}/m\mathbb{Z}$  est un corps.

**Définition 3.9** Soient  $\mathbb{K}$  un corps et  $K$  une partie de  $\mathbb{K}$ . On dit que  $K$  est un **sous-corps** de  $\mathbb{K}$  ou que  $\mathbb{K}$  est un **sur-corps** de  $K$  si :

- i)  $K$  est un sous-anneau de  $\mathbb{K}$ ,
- ii)  $\forall x \in K \setminus \{0\}, x^{-1} \in K \setminus \{0\}$ .

1) Par exemple  $\mathbb{Q}$  est un sous-corps du corps  $\mathbb{Q}[\sqrt{2}]$  qui est lui-même un sous-corps du corps  $\mathbb{R}$ .

2) Le corps  $\mathbb{Q}$  n'a pas de sous-corps propres. En effet, si  $K$  est un sous-corps de  $\mathbb{Q}$ , montrer que l'on a nécessairement  $K = \mathbb{Q}$ .

3)  $\mathbb{Z}/p\mathbb{Z}$  ( $p$  premier) n'a pas de sous-corps propres.

**Proposition 3.10** Soient  $\mathbb{K}$  un corps et  $K$  une partie de  $\mathbb{K}$ . Alors  $K$  est un sous-corps de  $\mathbb{K}$  si et seulement si les quatre propriétés suivantes sont satisfaites :

- i)  $1_{\mathbb{K}} \in K$ ,
- ii)  $\forall x, y \in K, x - y \in K$ ,

- iii)*  $\forall x, y \in K, \quad xy \in K,$
- iv)*  $\forall x \in K \setminus \{0\}, \quad x^{-1} \in K \setminus \{0\}.$

**Preuve**

Les assertions *i*), *ii*) et *iii*) expriment que  $K$  est un sous-anneau de  $\mathbb{K}$ .

## 4 POLYNÔMES ET FRACTIONS RATIONNELLES

### 4.1 Anneau des polynômes à coefficients dans un corps

#### 4.1.1 Définitions

Par la suite,  $\mathbb{K}$  désigne un corps commutatif.

**Définition 4.1** On appelle **polynôme** à coefficients dans le corps  $\mathbb{K}$  en l'indéterminée  $X$  tout objet noté

$$P = a_0 + a_1 X + \dots + a_n X^n + \dots$$

(on écrit aussi  $P = \sum_{n=0}^{+\infty} a_n X^n$ ) où  $(a_n)_{n \in \mathbb{N}}$  est une suite d'éléments de  $\mathbb{K}$  nulle à partir d'un certain rang, appelée suite des coefficients de  $P$ . On note  $\mathbb{K}[X]$  l'ensemble de ces polynômes.

**Définition 4.2** Deux polynômes  $P = \sum_{n=0}^{+\infty} a_n X^n$  et  $Q = \sum_{n=0}^{+\infty} b_n X^n$  de  $\mathbb{K}[X]$  sont dits égaux si et, seulement si, ils ont les mêmes coefficients, c'est à dire,

$$P = Q \quad \Leftrightarrow \quad \forall n \in \mathbb{N} \quad a_n = b_n.$$

**Définition 4.3** 1) On appelle **monôme**, tout polynôme de la forme  $P = a X^n$  avec  $a \in \mathbb{K}$ ,  $n \in \mathbb{N}$ .

2) Soit  $P = \sum_{n=0}^{+\infty} a_n X^n \in \mathbb{K}[X]$ . On dit que  $P$  est un **polynôme pair** (resp. **impair**) si et seulement si  $\forall p \in \mathbb{N}$ ,  $a_{2p+1} = 0$  (resp.  $a_{2p} = 0$ ).

#### 4.1.2 Opérations dans $\mathbb{K}[X]$

**Définition 4.4** Soient  $P = \sum_{n=0}^{+\infty} a_n X^n \in \mathbb{K}[X]$  et  $Q = \sum_{n=0}^{+\infty} b_n X^n \in \mathbb{K}[X]$ .

1) On définit le polynôme  $P + Q$  par  $P + Q = \sum_{n=0}^{+\infty} (a_n + b_n) X^n$ . On l'appelle la somme des polynômes  $P$  et  $Q$ .

2) On définit le polynôme  $P \times Q$  par  $P \times Q = \sum_{n=0}^{+\infty} c_n X^n$  avec  $c_n = \sum_{k=0}^n a_k b_{n-k}$ . On l'appelle produit des polynômes  $P$  et  $Q$ .

**Théorème 4.1**  $(\mathbb{K}[X], +, \times)$  est un anneau commutatif unitaire, d'élément nul le polynôme nul et d'élément unité le polynôme constant égal à 1.

**Définition 4.5 (Opération externe)**

Si  $\lambda \in \mathbb{K}$  et  $P = \sum_{n=0}^{+\infty} a_n X^n \in \mathbb{K}[X]$ , on définit le polynôme  $\lambda P$  par  $\lambda P = \sum_{n=0}^{+\infty} (\lambda a_n) X^n$ .

**Exercice**

Soit  $P(X) \in \mathbb{K}$ . Montrer que

- 1)  $P(X)$  pair si et seulement si  $P(-X) = P(X)$
- 2)  $P(X)$  impair si et seulement si  $P(-X) = -P(X)$ .

**4.1.3 Notion de degré d'un polynôme**

**Définition 4.6** Soit  $P = \sum_{n=0}^{+\infty} a_n X^n$  un polynôme non nul. On appelle degré de  $P$  le plus grand entier  $k \in \mathbb{N}$  tel  $a_k \neq 0$ . On le note  $k = \deg P$ . Le coefficient  $a_k$  est alors appelé **coefficient dominant** de  $P$ .

Le polynôme  $P$  est dit **unitaire** si son coefficient dominant égale 1.

Si  $P = 0$  on convient que  $\deg P = -\infty$ .

**Proposition 4.1** On a les propriétés suivantes

- 1)  $\forall P, Q \in \mathbb{K}[X] \quad \deg(PQ) = \deg(P) + \deg(Q)$ ,
- 2)  $\forall \lambda \in \mathbb{K}, \forall P \in \mathbb{K}[X] \quad \deg(\lambda P) = \begin{cases} \deg P & \text{si } \lambda \neq 0 \\ -\infty & \text{si } \lambda = 0, \end{cases}$
- 3)  $\forall P, Q \in \mathbb{K}[X]$ , on a

$$\deg(P + Q) \leq \max(\deg(P), \deg(Q)),$$

avec égalité lorsque  $\deg P \neq \deg Q$ .

**Corollaire 4.1** 1) Les éléments inversibles de l'anneau  $\mathbb{K}[X]$  sont les polynômes constants non nuls.

2)  $\forall P, Q \in \mathbb{K}[X], \quad PQ = 0 \Rightarrow P = 0 \quad \text{ou} \quad Q = 0$  (l'anneau  $\mathbb{K}[X]$  est intègre).

**Théorème 4.2** L'anneau  $K[X]$  est un anneau principal.

**4.2 Fonctions polynômiales**

**Définition 4.7** Soit  $P = a_0 + a_1 X + \dots + a_n X^n \in \mathbb{K}[X]$  et  $x \in \mathbb{K}$ .

- i) Le scalaire  $P(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{K}$  est appelé **valeur** de  $P$  en  $x$ , on le note  $P(x)$ .

ii) On appelle **racine** (ou **zéro**) d'un polynôme  $P \in \mathbb{K}[X]$  tout scalaire  $x \in \mathbb{K}$  tel que  $P(x) = 0$ .

**Définition 4.8** Soit  $P \in \mathbb{K}[X]$ . On appelle **fonction polynômiale** associée à  $P$  l'application  $\tilde{P} : \mathbb{K} \rightarrow \mathbb{K}$  définie par  $\tilde{P}(x) = P(x)$  pour tout  $x \in \mathbb{K}$ .

**Propriétés 2** On a les propriétés suivantes ( $x \in \mathbb{K}$ )

i)  $\forall P, Q \in \mathbb{K}[X], \quad (P + Q)(x) = P(x) + Q(x),$

ii)  $\forall \lambda \in \mathbb{K}, \forall P \in \mathbb{K}[X] \quad (\lambda P)(x) = \lambda P(x),$

iii)  $\forall P, Q \in \mathbb{K}[X], \quad (PQ)(x) = P(x)Q(x).$

### 4.3 Division euclidienne

**Théorème 4.3** Soit  $P \in \mathbb{K}[X]$ . Pour tout polynôme  $A \in \mathbb{K}[X]$ , il existe un **unique** couple  $(Q, R) \in \mathbb{K}[X]^2$  tel que

$$P = AQ + R \quad \text{avec} \quad \deg R < \deg A.$$

Le polynôme  $Q$  est appelé **quotient** de la **division euclidienne** de  $P$  par  $A$  et le polynôme  $R$  est appelé le **reste** de la division euclidienne de  $P$  par  $A$ .

Exemple! (cf. Cours Magistral)

**Définition 4.9** On dit que le polynôme  $A \in \mathbb{K}[X]$  **divise** le polynôme  $P \in \mathbb{K}[X]$  dans  $\mathbb{K}[X]$  si le reste de la division euclidienne de  $P$  par  $A$  est nul, on écrit  $A/P$ , on dit aussi que  $P$  est un **multiple** de  $A$ .

**Proposition 4.2** Soient  $P \in \mathbb{K}[X]$ ,  $a \in \mathbb{K}$ . Alors

$$a \text{ est une racine de } P \Leftrightarrow (X - a)/P.$$

#### Preuve

Il est évident que si  $(X - a)/P$  alors  $a$  est une racine de  $P$ . Réciproquement supposons que  $a$  est une racine de  $P$ . D'après la division euclidienne de  $P$  par  $X - a$ , il existe un couple (unique)  $(Q, R) \in \mathbb{K}[X]^2$  tel que

$$P = (X - a)Q + R \quad \text{avec} \quad \deg R < \deg (X - a).$$

Comme  $\deg(X - a) = 1$  alors  $\deg R = 0$  ou  $\deg R = -\infty$ . On a nécessairement  $\deg R = -\infty$  c'est à dire  $R = 0$ , sinon  $P(a) \neq 0$ . Ainsi  $P = (X - a)Q$ , c'est à dire  $X - a$  divise  $P$ .

## 4.4 Division suivant les puissances croissantes

**Théorème-Définition 4.1** Soient  $A, B$  deux polynômes de  $\mathbb{K}[X]$  tels que  $v(B) = 0$ . Soit  $h \in \mathbb{N}$ , il existe un couple unique de polynômes  $Q_h, R_h$  tels que :

$$A = B Q_h + R_h, \quad \deg Q_h \leq h, \quad v(R_h) > h.$$

Les polynômes  $Q_h$  et  $R_h$  s'appellent respectivement **quotient** et **reste** dans la division **sui-**  
**vant les puissances croissantes** de  $A$  par  $B$  à l'ordre  $h$ .

Notons qu'il existe une infinité de divisions suivant les puissances croissantes, une pour chaque valeur de l'entier  $h$ . Le lecteur est invité à noter que la division suivant les puissances croissantes de  $A$  par  $B$  n'est définie que si la valuation de  $B$  est nulle.

La **valuation** d'un polynôme  $B = b_0 + b_1 X + \dots + b_n X^n$  est par définition

$$val(B) = \min\{k \in [[0, n]] / b_k \neq 0\}.$$

**Exemple** (cf. cours magistral).

## 4.5 Dérivée Formelle et racine multiple d'un polynôme

Dans cette sous-section, le corps  $\mathbb{K}$  est supposé de caractéristique zéro, c'est à dire que  $\forall n \in \mathbb{N}^*, \underbrace{1_{\mathbb{K}} + \dots + 1_{\mathbb{K}}}_{n \text{ fois}} \neq 0_{\mathbb{K}}$ .

Les corps  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  sont de caractéristique 0. Le corps  $\mathbb{Z}/5\mathbb{Z}$  n'est pas de caractéristique zéro puisque  $\bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{5} = \bar{0}$  n'est pas de caractéristique zéro.

**Définition 4.10** Soit  $P = \sum_{k=0}^n a_k X^k = a_0 + a_1 X + \dots + a_n X^n \in \mathbb{K}[X]$  un polynôme de degré  $n$ . On appelle **polynôme dérivé** de  $P$  le polynôme noté  $P'$  défini par :

$$P' = a_1 + 2 a_2 X + \dots + n a_n X^{n-1} = \sum_{k=1}^n k a_k X^{k-1}.$$

Exemple

Dans  $\mathbb{R}[X]$ , si  $P(X) = 4 X^5 - 7 X^3 + 10 X + 5$  alors  $P'(X) = 20 X^4 - 21 X^2 + 10$ .

**Remarque 4.1** Soit  $P \in \mathbb{K}[X]$ .

i)  $P' = 0 \Leftrightarrow P$  est un polynôme constant

ii) Si  $P$  est non constant alors  $\deg P' = \deg P - 1$ .

**Proposition 4.3** On a les propriétés suivantes

- i)  $\forall \lambda, \mu \in \mathbb{K}, P, Q \in \mathbb{K}[X], (\lambda P + \mu Q)' = \lambda P' + \mu Q'$
- ii)  $\forall \lambda, \mu \in \mathbb{K}, P, Q \in \mathbb{K}[X], (PQ)' = P'Q + P Q'$ .
- iii)  $\forall n \in \mathbb{N}^*, \forall P \in \mathbb{K}[X], (P^n)' = n P' P^{n-1}$ .

## Dérivées d'ordre supérieur

Soit  $P = \sum_{k=0}^n a_k X^k = a_0 + a_1 X + \dots + a_n X^n \in \mathbb{K}[X]$  un polynôme de degré  $n$  et  $k \in \mathbb{N}$ .

Le polynôme dérivé de  $P'$  noté  $P''$  ou  $P^{(2)}$  est appelé la **dérivée seconde** de  $P$  ou la dérivée d'ordre 2 de  $P$ . Le polynôme dérivé de  $P''$  noté  $P^{(3)}$  est appelé le **polynôme dérivé d'ordre 3** de  $P$ . Par itération on obtient le polynôme dérivé de  $P^{(k-1)}$  noté  $P^{(k)}$  et appelé le **polynôme dérivé d'ordre  $k$**  de  $P$ .

**NB** : on convient que  $P^{(0)} = P$ .

**Proposition 4.4** Soit  $P \in \mathbb{K}[X]$  et  $k \in \mathbb{N}$ .

- i) Si  $\deg P < k$  alors  $\deg P^{(k)} = -\infty$ , c'est à dire que  $P^{(k)} = 0$ ,
- ii) Si  $\deg P \geq k$  alors  $\deg P^{(k)} = \deg P - k$ ,
- iii)  $\forall \lambda, \mu \in \mathbb{K}, \forall P, Q \in \mathbb{K}[X], (\lambda P + \mu Q)^{(k)} = \lambda P^{(k)} + \mu Q^{(k)}$
- iv)  $\forall P, Q \in \mathbb{K}[X]$  on a la **formule de Leibniz**

$$(PQ)^{(k)} = \sum_{i=0}^k C_k^i P^{(i)} Q^{(k-i)}.$$

$$\text{avec } C_k^i = \frac{k!}{i!(k-i)!}.$$

**Théorème 4.4 (Formule de Taylor)**

Pour tout  $P \in \mathbb{K}[X]$  avec  $n = \deg P$  et tout scalaire  $a \in \mathbb{K}$  on a

$$P = \sum_{i=0}^n \frac{P^{(i)}(a)}{i!} (X - a)^i.$$

**Définition 4.11** Soient  $P \in \mathbb{K}[X]$  tel que  $P \neq 0$  et  $a \in \mathbb{K}$ . L'**ordre de multiplicité** de  $a$  en tant que racine de  $P$  est par définition le plus grand entier  $k \in \mathbb{N}$  tel que  $(X - a)^k / P$ .

Si  $k = 0$  alors  $a$  n'est pas racine de  $P$ .

Si  $k = 1$  on dit que  $a$  est **racine simple**.

Si  $k \geq 2$  on parle de racine multiple (double, triple,...).

On convient que si  $P = 0$  alors tout  $a \in \mathbb{K}$  est racine de multiplicité  $+\infty$  de  $P$ .

**Proposition 4.5** Soient  $P \in \mathbb{K}[X]$ ,  $P \neq 0$ ,  $a \in \mathbb{K}$  et  $k \in \mathbb{N}$ . Les assertions suivantes sont équivalentes :

- i)  $a$  est une racine de multiplicité  $k$  de  $P$ ,
- ii)  $(X - a)^k / P$  et  $(X - a)^{k+1}$  ne divise pas  $P$ ,
- iii)  $\exists Q \in \mathbb{K}[X]$  tel que  $P = (X - a)^k Q$  avec  $Q(a) \neq 0$ .

**Remarque 4.2** (très important!) Soit  $P \in \mathbb{K}[X]$ .

- 1) Si  $P$  est un polynôme non nul alors la somme des multiplicités de ces racines est inférieure ou égale au degré de  $P$ .
- 2) Un polynôme de degré  $n$  admet au plus  $n$  racines comptées avec leur multiplicité.
- 3) Si  $P$  est un polynôme de degré  $n$  admettant  $n$  racines distinctes alors il n'y en n'a pas d'autres et celles-ci sont simples.
- 4) Si  $P$  est un polynôme de degré  $n$  admettant au moins  $n + 1$  racines alors  $P = 0$ .
- 5) Si  $P$  admet une infinité de racines alors  $P = 0$ .
- 6) Si  $a$  est racine de multiplicité  $k \in \mathbb{N}^*$  de  $P$  alors  $a$  est une racine de multiplicité  $k - 1$  du polynôme dérivé  $P'$ .
- 7) Les racines de  $P$  sont simples si et seulement si  $P$  et  $P'$  n'ont pas de racines communes.

**NB** : le lecteur est vivement prié de se convaincre de ces assertions.

**Théorème 4.5** Soient  $P \in \mathbb{K}[X]$ ,  $P \neq 0$ ,  $a \in \mathbb{N}$  et  $k \in \mathbb{N}^*$ . Les assertions suivantes sont équivalentes.

- i)  $a$  est racine d'ordre de multiplicité  $k$  de  $P$ ,
- ii)  $P(a) = P'(a) = \dots = P^{(k-1)}(a) = 0$  et  $P^{(k)}(a) \neq 0$ .

Preuve (utiliser la formule de Taylor).

## 4.6 Polynômes irréductibles

**Définition 4.12** 1) Deux polynômes  $P$  et  $Q$  de  $\mathbb{K}[X]$  sont dits **associés** si et seulement si il existe  $\lambda \in \mathbb{K}$ ,  $\lambda \neq 0$ ,  $P = \lambda Q$ .

2) Un polynôme  $P$  est dit **unitaire** si son coefficient dominant est égal à 1. Tout polynôme  $P \in \mathbb{K}[X]$ , non nul, est associé à un unique polynôme unitaire.

Le lecteur remarquera que deux polynômes  $P$  et  $Q$  associés ont le même degré.

**Définition 4.13** Un polynôme  $P \in \mathbb{K}[X]$  est dit **irréductible** dans  $\mathbb{K}[X]$  si tout polynôme de  $\mathbb{K}[X]$  diviseur de  $P$  dans  $\mathbb{K}[X]$  est un polynôme constant non nul ou un polynôme associé à  $P$ . Autrement dit  $P$  est un polynôme irréductible si  $P$  n'a pas de diviseur non trivial.

1) Dans  $\mathbb{K}[X]$  les polynômes de la forme  $aX + b$  avec  $a, b \in \mathbb{K}$ ,  $b \neq 0$ , sont irréductibles dans  $\mathbb{K}[X]$ .

2) Dans  $\mathbb{R}[X]$  les polynômes de degré 2 irréductibles sont exactement ceux qui sont à discriminant strictement inférieur à 0.

3) Le polynôme  $X^2 + 1$  est irréductible dans  $\mathbb{R}[X]$ , mais il est réductible dans  $\mathbb{C}[X]$ , puisque  $X^2 + 1 = (X + i)(X - i)$ .

**Proposition 4.6** Soient  $A, B \in \mathbb{K}[X]$  et  $P$  un polynôme irréductible dans  $\mathbb{K}[X]$ . Alors

$$P / AB \Rightarrow P/A \text{ ou } P/B.$$

**Théorème 4.6** Soit  $P$  un polynôme non constant de  $\mathbb{K}[X]$ . Alors

$\exists n \in \mathbb{N}^*$  et  $\exists P_1, \dots, P_n$  des polynômes irréductibles deux à deux distincts et  $\exists \alpha_1, \dots, \alpha_n \in \mathbb{N}^*$  tels que

$$P = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}.$$

De plus cette décomposition est unique à l'ordre près des facteurs, on l'appelle décomposition en **produit de facteurs irréductibles** de  $P$ .

## 4.7 Notions de pgcd et de ppcm

**Définition 4.14** Soient  $A, B \in \mathbb{K}[X]$ .

1) On note  $Div(A, B) = Div(A) \cap Div(B)$  l'ensemble des polynômes de  $\mathbb{K}[X]$ , diviseurs

communs à  $A$  et  $B$  dans  $\mathbb{K}[X]$ .

2) On note  $Mul(A, B) = Mul(A) \cap Mul(B)$  l'ensemble des polynômes de  $\mathbb{K}[X]$ , multiples communs à  $A$  et  $B$  dans  $\mathbb{K}[X]$ .

**Proposition 4.7** Soient  $A, B, R \in \mathbb{K}[X]$ .  
Si  $A = BQ + R$  alors  $Div(A, B) = Div(B, R)$ .

Le résultat suivant est une conséquence de la proposition précédente.

**Théorème 4.7** Soient  $A, B \in \mathbb{K}[X]$ , il existe un unique polynôme  $D \in \mathbb{K}[X]$ , unitaire ou nul, tel que  $Div(A, B) = Div(D)$ . Ce polynôme  $D$  est appelé le **pgcd** des polynômes  $A$  et  $B$ . On note  $D = \text{pgcd}(A, B)$  ou  $A \wedge B$ .

L'**algorithme d'Euclide** permet de calculer le pgcd de deux polynômes (cf. cours magistral).

**Théorème 4.8 (Egalité de Bézout)**

Si  $D = \text{pgcd}(A, B)$  alors  $\exists U, V \in \mathbb{K}[X]$  tels que  $D = AU + BV$ .

**Définition 4.15** Deux polynômes  $A$  et  $B$  sont dits **premiers entre eux** dans  $\mathbb{K}[X]$  si leurs diviseurs communs dans  $\mathbb{K}[X]$  sont exactement les polynômes constants non nuls. Ceci signifie encore  $\text{pgcd}(A, B) = 1$ .

**Théorème 4.9 (Théorème de Bezout)**

Soient  $A, B \in \mathbb{K}[X]$ .

$A$  et  $B$  sont premiers entre eux  $\Leftrightarrow \exists U, V \in \mathbb{K}[X]$  tels que  $AU + BV = 1$ .

Preuve

Supposons que les polynômes  $A$  et  $B$  soient premiers entre eux dans  $\mathbb{K}[X]$ . D'après l'égalité de Bézout,  $\exists U, V \in \mathbb{K}[X]$  tels que  $AU + BV = 1$ . Réciproquement, supposons qu'il existe  $U, V \in \mathbb{K}[X]$  tels que

$$AU + BV = 1 \quad (*)$$

Soit  $H \in \mathbb{K}[X]$  un commun diviseur de  $A$  et  $B$  dans  $\mathbb{K}[X]$ . Alors  $H$  divise  $AU + BV$  dans  $\mathbb{K}[X]$  et d'après l'égalité (\*),  $H$  divise le polynôme constant 1, forcément  $H$  est un polynôme constant non nul. Donc  $\text{pgcd}(A, B) = 1$ .

**Corollaire 4.2** *On a les propriétés suivantes*

- i)  $\text{pgcd}(A, B) = 1$  et  $\text{pgcd}(A, C) = 1 \Rightarrow \text{pgcd}(A, BC) = 1$ ,
- ii)  $\text{pgcd}(A, B_1) = 1, \dots, \text{pgcd}(A, B_n) = 1 \Rightarrow \text{pgcd}(A, B_1 \dots B_n) = 1$ ,
- iii)  $\text{pgcd}(A, B) = 1 \Rightarrow \forall n, m \in \mathbb{N}, \text{pgcd}(A^n, B^m) = 1$ .

**Théorème 4.10 (Théorème de Gauss)**

Soient  $A, B, C \in \mathbb{K}[X]$ .

Si  $A/B/C$  et  $\text{pgcd}(A, B) = 1$  alors  $A/C$ .

Preuve

Supposons que  $A/B/C$  et  $\text{pgcd}(A, B) = 1$ . Alors il existe  $D \in \mathbb{K}[X]$  tel que  $BC = AD$  et il existe  $U, V \in \mathbb{K}[X]$  tels que

$$UA + VB = 1 \quad (*)$$

D'après la relation (\*), on obtient  $UAC + VBC = C$ . Par conséquent, on obtient

$$UAC + VAD = C$$

c'est à dire que  $A(UC + VD) = C$  et  $A$  divise  $C$ .

**Théorème 4.11** *Si  $A/C$  et  $B/C$  et  $\text{pgcd}(A, B) = 1$  alors  $AB/C$ .*

Preuve

Supposons que  $A/C$  et  $B/C$  et  $\text{pgcd}(A, B) = 1$ . Alors il existe  $D, H \in \mathbb{K}[X]$  tel que  $C = DA$  et  $C = HB$  et il existe  $U, V \in \mathbb{K}[X]$  tels que

$$UA + VB = 1 \quad (*)$$

Ainsi, d'après la relation (\*), on a  $UAC + VBC = C$ . Par suite, on obtient que

$$UAHB + VBDA = C$$

c'est à dire que  $AB(UH + VD) = C$ . Donc  $AB$  divise  $C$ .

**Corollaire 4.3** *Si  $A_1, \dots, A_n$  sont des diviseurs de  $P$  deux à deux premiers entre eux alors  $A_1 \dots A_n/P$ .*

**Théorème 4.12**  $\forall A, B \in \mathbb{K}[X]$ , il existe un scalaire  $\lambda \in \mathbb{K}$  tel que

$$\text{pgcd}(A, B) \text{ppcm}(A, B) = \lambda AB.$$

Preuve (exercice!)

## Polynômes scindés

**Définition 4.16** Un polynôme  $P \in \mathbb{K}[X]$  est dit **scindé** dans  $\mathbb{K}[X]$  si et seulement si il existe  $\lambda \in \mathbb{K}^*$ ,  $\exists n \in \mathbb{N}^*$ ,  $\exists a_1, \dots, a_n \in \mathbb{K}$  tels que

$$P = \lambda (X - a_1) \dots (X - a_n).$$

**Proposition 4.8** Un polynôme  $P \in \mathbb{K}[X]$  est scindé dans  $\mathbb{K}$  si et seulement si la somme des multiplicités de ses racines (dans  $\mathbb{K}$ ) est égale à son degré.

## 4.8 Polynômes complexes

Tout élément de  $\mathbb{C}[X]$  est appelé un polynôme complexe.

**Théorème 4.13 (Théorème de Alembert-Gauss)**

Tout polynôme non constant de  $\mathbb{C}[X]$  admet au moins une racine dans  $\mathbb{C}$ .

(On dit que le corps  $\mathbb{C}$  est **algébriquement clos**.)

**Corollaire 4.4** Les polynômes irréductibles de  $\mathbb{C}[X]$  sont exactement les polynômes de degré égal à 1.

**Corollaire 4.5** Soit  $P \in \mathbb{C}[X]$  non constant. Alors  $P$  est scindé dans  $\mathbb{C}[X]$ . Plus précisément  $\exists \lambda \in \mathbb{C}^*$ ,  $\exists n \in \mathbb{N}^*$  et  $\exists a_1, \dots, a_n \in \mathbb{C}$  des scalaires deux à deux distincts et  $\exists \alpha_1, \dots, \alpha_n \in \mathbb{N}^*$  tels que

$$P = \lambda (X - a_1)^{\alpha_1} (X - a_2)^{\alpha_2} \dots (X - a_n)^{\alpha_n}.$$

De plus cette décomposition est unique à l'ordre près des facteurs.

**Proposition 4.9** Soient  $A, B \in \mathbb{C}[X]$ .

$$\text{pgcd}(A, B) = 1 \quad \Leftrightarrow \quad A \quad \text{et} \quad B \quad \text{n'ont pas de racines en commun.}$$

Soit  $P = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{C}[X]$ . On appelle **conjugué** de  $P$  le polynôme

$$\bar{P} = \bar{a}_n X^n + \dots + \bar{a}_1 X + \bar{a}_0 \in \mathbb{C}[X].$$

**Propriétés 3** Soient  $P, Q \in \mathbb{C}[X]$ .

$$1) \text{ On a } \overline{\overline{P}} = P, \quad \overline{P+Q} = \overline{P} + \overline{Q}, \quad \overline{PQ} = \overline{P} \overline{Q},$$

$$2) P/Q \Leftrightarrow \overline{P}/\overline{Q},$$

$$3) \forall a \in \mathbb{C}, \overline{P(a)} = \overline{P}(\overline{a}).$$

**Proposition 4.10** Soient  $P \in \mathbb{C}[X]$ ,  $a \in \mathbb{C}$  et  $\alpha \in \mathbb{N}$ . Les assertions suivantes sont équivalentes.

1)  $a$  est racine de multiplicité  $\alpha$  de  $P$ ,

2)  $\overline{a}$  est racine de multiplicité  $\alpha$  de  $\overline{P}$ .

## 4.9 Polynômes réels

Tout élément  $P \in \mathbb{R}[X]$  est appelé un polynôme réel. On appelle racine complexe de  $P \in \mathbb{R}[X]$  toute racine de  $P$  vue comme polynôme complexe.

**Proposition 4.11** Soit  $P \in \mathbb{R}[X]$  un polynôme de degré  $n \in \mathbb{N}$ . Alors  $P$  admet exactement  $n$  racines complexes comptées avec leur multiplicité.

**Proposition 4.12** Les racines complexes de  $P \in \mathbb{R}[X]$  sont deux à deux conjuguées. Si  $z$  est une racine complexe non réel d'ordre  $k$  du polynôme  $P \in \mathbb{R}[X]$  alors  $\overline{z}$  est aussi racine d'ordre  $k$  de  $P$ .

**Corollaire 4.6** Tout polynôme réel de **degré impair** possède au moins une racine réelle.

**Corollaire 4.7** Les polynômes irréductibles de  $\mathbb{R}[X]$  sont exactement les polynômes de degré 1 et les polynômes de degré 2 de discriminant  $< 0$ .

**Théorème 4.14** Soit  $P \in \mathbb{R}[X]$  non constant. Alors  $\exists \lambda \in \mathbb{R}^*$ ,  $\exists n, m \in \mathbb{N}$ ,  $\exists a_1, \dots, a_n \in \mathbb{R}$ ,  $\exists (b_1, c_1), \dots, (b_m, c_m) \in \mathbb{R}^2$  deux à deux distincts, tels que  $\Delta_j = b_j^2 - 4c_j < 0$ ,  $\exists \alpha_1, \dots, \alpha_n \in \mathbb{N}^*$  et  $\exists \beta_1, \dots, \beta_m \in \mathbb{N}^*$  tels que

$$P = \lambda \prod_{i=1}^n (X - a_i)^{\alpha_i} \prod_{j=1}^m (X^2 + b_j X + c_j)^{\beta_j}.$$

De plus cette décomposition est unique à l'ordre près des facteurs.

## 4.10 Relation entre racines et coefficients d'un polynôme scindé

Soit  $P = a_n X^n + \dots + a_1 X + a_0$  un polynôme scindé de degré  $n \in \mathbb{N}^*$ , réel ou complexe. Soient  $x_1, \dots, x_n$  les racines de  $P$  comptées avec leur multiplicité. Alors on a

$$P = a_n X^n + \dots + a_1 X + a_0 = a_n (X - x_1) \cdots (X - x_n).$$

En développant le second membre, on peut exprimer les coefficients de  $P$  en fonction de ses racines.

**Définition 4.17** Soient  $n \in \mathbb{N}^*$  et  $x_1, \dots, x_n \in \mathbb{K}$ . On appelle expressions symétriques élémentaires des  $x_1, \dots, x_n$  les quantités suivantes :

$$\begin{aligned} \sigma_1 &= \sum_1^n x_i, & \sigma_2 &= \sum_{1 \leq i < j \leq n} x_i x_j, & \sigma_3 &= \sum_{1 \leq i < j < k \leq n} x_i x_j x_k, & \text{et} \\ \sigma_p &= \sum_{1 \leq i_1 < i_2 < \dots < i_p \leq n} x_{i_1} x_{i_2} \dots x_{i_p} & (\text{pour } 1 \leq p \leq n). \end{aligned}$$

Ainsi  $\sigma_p$  apparaît comme la somme de tous les produits possibles de  $p$  éléments d'indices distincts choisis dans  $x_1, \dots, x_n$ .

**Théorème 4.15** Soient  $n \in \mathbb{N}^*$ ,  $x_1, \dots, x_n \in \mathbb{K}$  et  $\sigma_1, \dots, \sigma_n$  les expressions symétriques élémentaires en les  $x_1, \dots, x_n$ . On a alors

$$(X - x_1) \cdots (X - x_n) = X^n - \sigma_1 X^{n-1} + \dots + (-1)^k \sigma_k X^{n-k} + \dots + (-1)^n \sigma_n.$$

**Théorème 4.16** Soient  $P = a_n X^n + \dots + a_1 X + a_0$  un polynôme de degré  $n \in \mathbb{N}^*$  et  $x_1, \dots, x_n \in \mathbb{K}$ . Les assertions suivantes sont équivalentes :

(i)  $x_1, \dots, x_n$  sont les racines de  $P$  comptées avec multiplicité,

(ii)  $\forall 1 \leq k \leq n$  on a  $\sigma_k = \frac{(-1)^k a_{n-k}}{a_n}$ .

En particulier :

Soit  $P = a X^2 + b X + c$  avec  $a \neq 0$ .

$x_1, x_2$  sont les racines de  $P$  comptées avec multiplicité ssi  $\begin{cases} x_1 + x_2 = \frac{-b}{a} \\ x_1 x_2 = \frac{c}{a} \end{cases}$

En particulier :

Soit  $P = aX^3 + bX^2 + cX + d$  avec  $a \neq 0$ .

$x_1, x_2, x_3$  sont les racines de  $P$  comptées avec multiplicité ssi

$$\begin{cases} x_1 + x_2 + x_3 = -\frac{b}{a} \\ x_1 x_2 + x_2 x_3 + x_1 x_3 = \frac{c}{a} \\ x_1 x_2 x_3 = -\frac{d}{a} \end{cases}$$

## 4.11 Fractions rationnelles

### 4.11.1 Corps des fractions rationnelles à une indéterminée

Une fraction rationnelle  $F$  est une classe de couples de polynômes  $(P, Q)$  avec  $Q \neq 0$ . Si  $(P, Q)$  est un représentant quelconque de  $F$  on convient d'écrire  $F = \frac{P}{Q}$ . La relation d'équivalence s'écrit

$$(P, Q) \mathcal{R} (P_1, Q_1) \Leftrightarrow PQ_1 = QP_1$$

Soit  $D = \text{pgcd}(P, Q)$ . On peut écrire  $P = DP_1$  et on a  $\frac{P}{Q} = \frac{P_1}{Q_1}$  avec  $P_1$  et  $Q_1$  premiers entre eux, d'où

**Définition 4.18** Soit  $F$  une fraction rationnelle de  $\mathbb{K}(X)$ . Tout représentant de  $F$ , écrit  $\frac{P_1}{Q_1}$ , tel que  $P_1$  et  $Q_1$  soient premiers entre eux s'appelle **forme irréductible** de  $F$ . Si de plus  $Q_1$  est normalisé cette représentation est unique et s'appelle la **forme réduite** de  $F$ . Le polynôme  $P_1$  est appelé **numérateur** et le polynôme  $Q_1$  est appelé **dénominateur** de  $F$ .

**Théorème-Définition 4.2** Soient  $F$  une fraction rationnelle non nulle de  $\mathbb{K}[X]$  et  $\frac{P}{Q}$  une représentant quelconque de  $F$ . L'entier relatif  $\deg P - \deg Q$  est indépendant du représentant choisi de  $F$ . On l'appelle le **degré** de la fraction rationnelle  $F$ .

**Preuve** En effet, si  $F = \frac{P}{Q} = \frac{P_1}{Q_1}$ , on a  $PQ_1 = QP_1$ . Par conséquent on a

$$\deg P + \deg Q_1 = \deg P_1 + \deg Q$$

d'où  $\deg P - \deg Q = \deg P_1 - \deg Q_1$ . On convient, comme pour les polynômes, de poser  $\deg 0 = -\infty$ .

On définit sur  $\mathbb{K}(X)$  l'addition et la multiplication de la façon suivante :

$$\forall \frac{P}{Q}, \frac{S}{R} \in \mathbb{K}(X), \quad \frac{P}{Q} + \frac{S}{R} = \frac{PR + QS}{QR}, \quad \frac{P}{Q} \frac{S}{R} = \frac{PS}{QR}$$

**Théorème 4.17**  $(\mathbb{K}(X), +, \cdot)$  est un corps commutatif unitaire.

#### 4.11.2 Décomposition en éléments simples des fractions rationnelles

**Proposition 4.13** Soit  $F = \frac{P}{Q}$ , il existe un unique polynôme  $E$  tel que  $F = \frac{P}{Q} = E + \frac{R}{Q}$  avec  $\deg R < \deg Q$ .

##### Preuve

D'après la division euclidienne de  $P$  par  $Q$  on a  $F = PE + \frac{R}{Q}$  avec  $\deg R < \deg Q$  soit  $\frac{P}{Q} = E + \frac{R}{Q}$ . Ce qui montre l'existence de  $E$  ainsi que son unicité.

**Théorème 4.18** Soit  $F$  une fraction rationnelle quelconque écrite sous-forme irréductible et normalisée de  $\mathbb{K}[X]$ . Supposons également son dénominateur écrit sous forme de produit de polynômes irréductibles, c-à-d

$$F = \frac{P}{Q} = \frac{P}{Q_1^{n_1} \dots Q_l^{n_l}}$$

Il existe une famille unique de polynômes  $(E, N_{1,1}, \dots, N_{1,n_1}, N_{2,1}, \dots, N_{2,n_2}, \dots, N_{l,1}, \dots, N_{l,n_l})$  telle que

$$F = E + \left( \frac{N_{1,1}}{Q_1} + \dots + \frac{N_{1,n_1}}{Q_1^{n_1}} \right) + \left( \frac{N_{2,1}}{Q_2} + \dots + \frac{N_{2,n_2}}{Q_2^{n_2}} \right) + \dots + \left( \frac{N_{l,1}}{Q_l} + \dots + \frac{N_{l,n_l}}{Q_l^{n_l}} \right)$$

avec  $\forall i \in [[1, l]], \forall j \in [[1, n_i]], \deg N_{ij} < \deg Q_i$ .

#### Décomposition dans $\mathbb{C}(X)$

**Théorème 4.19** Soit  $F \in \mathbb{C}[X]$  une fraction rationnelle complexe écrite sous-forme irréductible et normalisée. Supposons également son dénominateur écrit sous forme de produit de polynômes irréductibles, c-à-d

$$F = \frac{P}{Q} = \frac{P}{(X - a_1)^{\alpha_1} \dots (X - a_n)^{\alpha_n}}$$

Il existe un unique polynôme  $E$  et une unique famille de scalaires

$$(\lambda_{1,1}, \dots, \lambda_{1,\alpha_1}, \lambda_{2,1}, \dots, \lambda_{2,\alpha_2}, \dots, \lambda_{n,1}, \dots, \lambda_{n,\alpha_n})$$

tels que

$$F = E + \left( \frac{\lambda_{1,1}}{X - a_1} + \dots + \frac{\lambda_{1,\alpha_1}}{(X - a_1)^{\alpha_1}} \right) + \left( \frac{\lambda_{2,1}}{X - a_2} + \dots + \frac{\lambda_{2,\alpha_2}}{(X - a_2)^{\alpha_2}} \right) + \dots + \left( \frac{\lambda_{n,1}}{X - a_n} + \dots + \frac{\lambda_{n,\alpha_n}}{(X - a_n)^{\alpha_n}} \right)$$

$E$  s'appelle la **partie entière** de  $F$  et  $\frac{\lambda_{i,1}}{X - a_i} + \dots + \frac{\lambda_{i,\alpha_i}}{(X - a_i)^{\alpha_i}}$  la **partie polaire** relative au pôle  $a_i$ .

### Décomposition dans $\mathbb{R}(X)$

**Théorème 4.20** Soit  $F = \frac{P}{Q} \in \mathbb{R}[X]$  une fraction rationnelle réelle. Soit

$$Q(X) = (X - a_1)^{\alpha_1} \dots (X - a_m)^{\alpha_m} (X^2 + p_1 X + q_1)^{\beta_1} \dots (X^2 + p_n X + q_n)^{\beta_n}$$

l'écriture de  $Q$  en produit de polynômes irréductibles. Alors il existe un polynôme unique  $E$  de  $\mathbb{R}[X]$  et des familles uniques de **réels**  $(A_{ij}), i \in [[1, m]], j \in [[1, \alpha_i]], (B_{kl}), C_{kl}, k \in [[1, n]], l \in [[1, \beta_k]]$  tels que

$$\frac{P(X)}{Q(X)} = E(X) + \sum_{i=1}^m \left( \sum_{j=1}^{\alpha_i} \frac{A_{ij}}{(X - a_i)^j} \right) + \sum_k \left( \sum_{l=1}^{\beta_k} \frac{B_{kl} X + C_{kl}}{(X^2 + p_k X + q_k)^l} \right)$$

Les éléments de la première sommation s'appellent éléments **simples de première espèce** et ceux de la seconde **éléments simples de deuxième espèce**.

Des exemples pratiques de décompositions seront donnés au cours et aux séances de TD!

# EXERCICES

## I - PLANCHE D'EXERCICES (Lois de compositions)

### **Exercice 1**

1) On considère la loi  $*$  définie sur  $\mathbb{R}$  par :

$$\forall x, y \in \mathbb{R}, \quad x * y = x \times y + 3.$$

Vérifier que la loi  $*$  est interne dans  $\mathbb{R}$  et étudier les propriétés de cette loi (associativité, élément neutre, commutativité, éléments symétriques, éléments idempotents...etc...)

2) Étudier les propriétés des lois suivantes (définies sur  $\mathbb{R}$ )

a)  $\forall x, y \in \mathbb{R}, \quad x * y = x^2 \times y.$

b)  $\forall x, y \in \mathbb{R}, \quad x \top y = x^2 \times y + 1.$

### **Exercice 2**

Soit  $E$  un ensemble muni d'une loi  $\top$  associative, commutative et idempotente ( $\forall x \in E, x \top x = x$ ). On définit sur  $E$  la relation  $\mathcal{R}$  par :

$$\forall x, y \in E, \quad x \mathcal{R} y \iff x \top y = y.$$

Montrer que  $\mathcal{R}$  est une relation d'ordre et que  $\forall x, y \in E, \quad x \top y = \sup\{x, y\}.$

### **Exercice 3**

Soit  $E$  un ensemble muni d'une loi de composition interne notée multiplicativement, et d'une relation d'ordre  $\leq$ , vérifiant :

i)  $\forall x, a, b \in E \quad (x \leq a \text{ et } x \leq b) \Rightarrow x \leq ab.$

ii)  $\forall a, b \in E, \quad ab \leq a \text{ et } ab \leq b$

1) Montrer que  $ab \leq ba$  et en déduire que la loi est commutative.

2) Montrer que la loi est associative.

### **Exercice 4**

Soit  $E$  un ensemble muni de deux lois internes notées  $\cdot$  et  $*$ , la première admettant un élément neutre  $e$ , et la seconde admettant un élément neutre  $f$ . On suppose de plus que :

$$\forall x, y, u, v \in E, \quad (x * y) \cdot (u * v) = (x \cdot u) * (y \cdot v)$$

1) Montrer que  $e = f$ .

2) Montrer que  $\forall x, y \in E, \quad x * y = x \cdot y.$

3) Montrer que la loi  $*$  (qui est donc la même que la loi  $\cdot$ ) est commutative et associative.

### **Exercice 5**

Sur l'ensemble  $G = ]-1, 1[$ , on considère la loi  $*$  définie par

$$a * b = \frac{a + b}{1 + ab}$$

- 1) Vérifier que la loi  $*$  est une loi de composition interne sur  $] - 1, 1[$ .
- 2) Montrer que  $G$  muni de cette loi  $*$  est un groupe commutatif.

### Exercice 6

On pose  $E = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ . On munit  $E$  de la loi  $*$  par :

$$(x, y), (a, b) \in E, \quad (x, y) * (a, b) = (x + y a, y b)$$

- i) Montrer que la loi  $*$  est associative ;
- ii) Est-elle commutative ?
- iii) A-t-elle un élément neutre ? Quels sont alors les éléments inversibles de  $E$  ?

## II - PLANCHE D'EXERCICES (Groupes, Anneaux, Corps)

### Exercice 1

On considère les quatre fonctions de  $\mathbb{R}^*$  dans  $\mathbb{R}^*$  :

$$f_1(x) = x, \quad f_2(x) = \frac{1}{x}, \quad f_3(x) = -x, \quad f_4(x) = -\frac{1}{x}.$$

Montrer que  $G = \{f_1, f_2, f_3, f_4\}$  est un groupe pour la loi  $\circ$  de composition des applications. Est-il abélien ?

### Exercice 2

On pose  $D = \{x \in \mathbb{Q} / \exists a \in \mathbb{Z}, \exists n \in \mathbb{N}, x = \frac{a}{10^n}\}$ .

Montrer que  $D$  est un sous-groupe de  $(\mathbb{Q}, +)$ .

### Exercice 3

Étudier les lois de compositions internes  $*$  et  $\top$  définies sur  $\mathbb{R}$  par

$$\forall a, b \in \mathbb{R}, \quad a * b = \frac{a + b}{2}, \quad a \top b = (a - 1)(b - 1) + 1$$

### Exercice 4

Soit  $E = \{\circ, \triangle, \heartsuit\}$

- 1) Dire combien de lois de composition internes il y a sur  $E$ .
- 2) Écrire la table d'une loi de composition interne commutative sur  $E$ .
- 3) Écrire la table d'une loi commutative de composition interne sur  $E$  admettant  $\heartsuit$  pour élément neutre.

### Exercice 5

Soient  $(G, \cdot)$  un groupe et  $H$  une partie non vide, **finie** et stable de  $G$ . Montrer que  $H$  est un sous-groupe de  $G$ .

(indication : on pourra considérer les éléments  $x, x^2, \dots, x^n, x^{n+1}, \dots$  où  $x \in H$  et  $n = \text{card}(H)$ )

(On peut aussi considérer les applications  $\delta_a : H \rightarrow G$ ,  $\delta_a(x) = ax$  où  $a \in H$ .)

### Exercice 6

Soit  $H = \{f(x, y, z) \in \mathbb{R}^3 / x + 2y - z = 0\}$ .

a) Montrer que  $(H, +)$  est un groupe abélien.

b) Soit  $f : H \rightarrow H$  définie par  $\forall (x, y, z) \in H$ ,  $f(x, y, z) = (x - 2z, z - y, x - 2y)$ .

i) Montrer que  $f$  est un morphisme de groupes,

ii) Déterminer son noyau et son image

iii) Le morphisme  $f$  est-il injectif? Est-il surjectif?

### Exercice 7

Soit  $G$  un groupe,  $A$  et  $B$  deux sous-groupes de  $G$ .

On pose

$$AB = \{x \in G / \exists a \in A, \exists b \in B, x = ab\}$$

Montrer que :

$AB$  est un sous-groupe de  $G$  si et seulement si  $AB = BA$ .

### Exercice 8

Soit  $(G, +)$  un groupe additif abélien.

(On rappelle que  $m \cdot a = \underbrace{a + a + \dots + a}_m$  pour tout  $m \in \mathbb{N}^*$  et  $a \in G$ )

On suppose qu'il existe un entier naturel non nul  $n$  tel que  $n \cdot a = 0$  pour tout  $a \in G$ . Soit  $p$  le plus petit entier naturel non nul ayant cette propriété. On suppose que l'on peut écrire  $p = r \cdot s$ , avec  $\text{PGCD}(r, s) = 1$ . On pose

$$G_r = \{x \in G / r \cdot x = 0\}, \quad G_s = \{x \in G / s \cdot x = 0\}$$

1) Prouver que  $G_r$  et  $G_s$  sont des sous-groupes de  $G$ .

2) Montrer que  $G_r \cap G_s = \{0\}$ . (On pourra utiliser l'identité de Bezout).

3) Vérifier que  $\forall x \in G$  on a  $r \cdot x \in G_s$ .

4) Montrer que  $G = G_r + G_s$  où  $G_r + G_s = \{x \in G / \exists a \in G_r, \exists b \in G_s \text{ tel que } x = a + b\}$ .

### Exercice 9

On considère le groupe additif  $(\mathbb{Z}, +)$  et  $H \subset \mathbb{Z}$ .

a) Montrer que

$$H \text{ est un sous-groupe de } \mathbb{Z} \Leftrightarrow \exists n \in \mathbb{N} \text{ tel que } H = n\mathbb{Z}$$

b) Montrer que les sous-groupes du groupe additif  $\mathbb{Z}/n\mathbb{Z}$  sont de la forme  $p\mathbb{Z}/n\mathbb{Z}$  où  $p$  divise  $n$ . (on pourra utiliser la surjection canonique  $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ ).

Application : déterminer les sous-groupes des groupes  $\mathbb{Z}/30\mathbb{Z}$ ,  $\mathbb{Z}/13\mathbb{Z}$ .

### Exercice 10

Soient  $G$  un groupe **fini** d'élément neutre  $e$  et  $x \in G$ ,  $x \neq e$ .

- 1) Montrer qu'il existe un entier  $k \in \mathbb{N}^*$  tel que  $x^k = e$ .
- 2) On pose  $H = \{y \in G / \exists k \in \mathbb{Z}, y = x^k\}$  et  $H' = \{y \in G / \exists k \in \mathbb{N}, y = x^k\}$ .  
Montrer que  $H = H'$
- 3) On pose  $n = \min\{p \in \mathbb{N}^* / x^p = e\}$ 
  - i) Justifier l'existence de l'entier  $n$ .
  - ii) Montrer que

$$\langle x \rangle = \{e, x, \dots, x^{n-1}\}$$

En déduire que  $H = \langle x \rangle = H'$ .

Par définition l'entier naturel  $n$  est appelé **l'ordre** de  $x$  et noté  $o(x)$ .

### Exercice 11

Soit  $p \in \mathbb{N}^*$ .

On pose  $H_p = \{z \in \mathbb{C} / z^p = 1\}$ .

- 1) Montrer que  $H_p$  est un sous-groupe du groupe multiplicatif  $(\mathbb{C}^*, \cdot)$ .
- 2) Déterminer les éléments de  $H_p$ . Quel est le cardinal de  $H_p$ ?
- 3) Expliciter  $H_8$  et déterminer l'ordre de chacun de ces éléments.

### Exercice 12

Soit  $E$  un ensemble et  $\mathcal{P}(E)$  l'ensemble des parties de  $E$ . On note  $\bar{X}$  le complémentaire de  $X \in \mathcal{P}(E)$  dans  $E$ . On définit sur  $\mathcal{P}(E)$  les lois suivantes

$$\forall A, B \in \mathcal{P}(E), \quad A \oplus B = (\bar{A} \cap B) \cup (\bar{B} \cap A) \quad \text{et} \quad A \bullet B = A \cap B$$

Montrer que  $(\mathcal{P}(E), \oplus, \bullet)$  est un anneau. Est-il intègre?

### Exercice 13

On note par  $\bar{z}$  le conjugué de  $z$  dans  $\mathbb{C}$ .

I- On pose  $\mathbb{Z}[i] = \{z \in \mathbb{C} / \exists a, b \in \mathbb{Z} \quad z = a + ib\}$ .

Montrer  $(\mathbb{Z}[i], +, \times)$  est un anneau. Quels sont les éléments inversibles de  $\mathbb{Z}[i]$ ?

II- On considère l'ensemble

$$A = \{z \in \mathbb{C} / \exists a, b \in \mathbb{Z} \quad z = a + ib\sqrt{5}\}$$

1) Montrer que  $(A, +, \times)$  est un anneau.

Pour  $u, v \in A$ , on dit que  $u$  divise  $v$  si il existe  $w \in A$  tel que  $v = wu$ .

2) Montrer que si  $u$  divise  $v$  alors  $u\bar{u}$  divise  $v\bar{v}$  dans  $\mathbb{Z}$ .

3) Quels sont les éléments inversibles de  $A$ .

4) Quels sont les diviseurs de 9?

### **Exercice 14**

Soit  $A$  un anneau commutatif,  $I$  un idéal de  $A$ . On pose

$$\sqrt{I} = \{x \in A / \exists n \in \mathbb{N}^*, x^n \in I\}$$

1) Montrer que  $\sqrt{I}$  est un idéal de  $A$  contenant  $I$ .

2) Montrer que  $\sqrt{\sqrt{I}} = \sqrt{I}$ .

3) Montrer que  $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$  où  $J$  est un idéal de  $A$ .

4) Quels sont les idéaux  $I$  de  $\mathbb{Z}$  tels que  $I = \sqrt{I}$ ?

5) Montrer que si  $x \in \sqrt{\{0\}}$  alors  $1 - x$  est inversible dans l'anneau  $A$ .

### **Exercice 15**

Soit  $n \in \mathbb{N}^*$ . Montrer que l'anneau  $\mathbb{Z}/n\mathbb{Z}$  est un corps si et seulement si  $n$  est un nombre premier.

### **Exercice 13**

On pose  $\mathbb{Q}(\sqrt{2}) = \{x \in \mathbb{R} / \exists a, b \in \mathbb{Q}, x = a + b\sqrt{2}\}$ .

Montrer que  $(\mathbb{Q}(\sqrt{2}), \times, +)$  est un corps commutatif.

### **Exercice 14**

Soit  $(A, +, \times)$  un anneau intègre fini. Montrer que  $A$  est un corps.

### **Exercice 15**

Soit  $\mathbb{R}$  muni de la loi de composition "  $*$  " définie par

$$\forall (x, y) \in \mathbb{R}^2, x * y = x + y - xy.$$

1)  $(\mathbb{R}, *)$  est-il un groupe commutatif? En déduire la structure de  $(\mathbb{R} \setminus \{1\}, *)$ .

2) Montrer que  $a = 1$  n'est pas un élément régulier de  $(\mathbb{R}, *)$ .

3) Calculer

$$x^{*n} = \underbrace{x * x * \dots * x}_{n \text{ fois}}$$

pour  $n \in \mathbb{N}^*$ . En déduire que

$$x^{*n} = \sum_{k=1}^n (-1)^{k-1} C_n^k x^k$$

4) Résoudre dans  $\mathbb{R}$ , les équations suivantes

$$(i) \quad x^{2014} = 1, \quad (ii) \quad x^4 = -15$$

### Exercice 16

On définit dans  $E = \mathbb{R}^* \times \mathbb{R}$  une loi de composition "  $\top$  " par :

$$\forall (a, b), (a', b') \in E, \quad (a, b) \top (a', b') = (aa', a'b + b')$$

1)  $(E, \top)$  est-il un groupe commutatif?

2) Résoudre les équations suivantes dans  $E$ .

i)  $(a, b) \top (1, 3) = (a^2, 0)$ ,

ii)  $(a, b) \top (a, b) = (a^3, b^2)$ .

## III - PLANCHE D'EXERCICES (Polynômes et fractions rationnelles)

### Exercice 1

Soient  $P(X) \in \mathbb{K}[X]$  un polynôme de degré  $n \geq 2$  à coefficients dans le corps  $\mathbb{K}$  et  $a, b \in \mathbb{K}$ ,  $a \neq b$ .

i) Montrer que  $(X - a)(X - b)$  divise  $P(X)$  si et seulement si  $(X - a)$  et  $(X - b)$  divisent  $P(X)$ .

ii) Montrer que pour tout entier  $k$ ,  $1 \leq k \leq n$  le polynôme

$$(X - a)^k \text{ divise } P(X) \iff P^{(i)}(a) = 0, \quad \forall i = 0, 1, \dots, k - 1$$

iii) En déduire que  $a$  est une racine d'ordre  $k$  de  $P(X)$  si et seulement si  $P^{(i)}(a) = 0$ ,  $\forall i = 0, 1, \dots, k - 1$  et  $P^{(k)}(a) \neq 0$ .

### Exercice 2

a) Montrer que pour tout entier naturel non nul  $n$ , le polynôme  $A_n = nX^{n+1} - (n+1)X^n + 1$  est divisible par  $(X - 1)^2$ . Calculer le quotient.

- b) Montrer que pour tout entier  $n \geq 1$ , le polynôme réel  $(X - 2)^{2n} + (X - 1)^n - 1$  est divisible par  $X^2 - 3X + 2$ . Quel est le quotient ?
- c) Soit  $n \geq 2$ ,  $n \in \mathbb{N}$ . Quel est le reste de la division euclidienne du polynôme réel  $(\cos \theta + X \sin \theta)^n$  par le polynôme  $X^2 + 1$  ?
- d) Démontrer que le polynôme  $P(X) = \sum_{k=0}^n \frac{X^k}{k!}$  n'a que des racines simples.

### Exercice 3

Soit  $P$  un polynôme de degré  $n$  à coefficient réels, possédant  $n$  racines réelles distinctes.

- 1) Montrer que son polynôme dérivé  $P'$  possède  $(n - 1)$  racines réelles distinctes.
- 2) En déduire que le polynôme  $P^2 + 1$  n'a que des racines simples dans  $\mathbb{C}$ .

Donner un contre exemple dans  $\mathbb{C}[X]$ , c'est à dire un polynôme de degré  $n$  ayant  $n$  racines distinctes dans  $\mathbb{C}$ , alors que  $P^2 + 1$  possède des racines multiples.

### Exercice 4

Déterminer un polynôme  $P(X)$  à coefficients dans  $\mathbb{R}$ , de degré 5 tel que

- i)  $P(X) + 10$  soit divisible par  $(X + 2)^3$ ,
- ii)  $P(X) - 10$  soit divisible par  $(X - 2)^3$ .

### Exercice 5

Décomposer dans  $\mathbb{R}(X)$  les fractions rationnelles suivantes :

$$F_1 = \frac{2}{X^4 - 1}, F_2 = \frac{2}{(X^3 + 1)(X^2 + X + 1)}, F_3 = \frac{X}{(X - 2)^5(X - 1)}, F_4 = \frac{X^6}{(X^2 + 1)(X - 1)^3},$$

$$F_5 = \frac{X^4 + 1}{(X^2 - 1)^3}, F_6 = \frac{1}{X(X^2 + X + 1)^2}, F_7 = \frac{1}{X^6 - 1}.$$

### Exercice 6

Calculer le pgcd des polynômes réels  $P$  et  $Q$  suivants

- 1)  $P = X^4 + 2X^3 - 11X^2 - 12X + 36$  et  $Q = 4X^3 + 6X^2 - 22X - 12$
- 2)  $P = (2X + 3)^3(x - 5)^4(X^2 + 2X + 3)^3(X^2 - 9)^7$  et  $Q = (2X + 3)^7(x - 5)(X^2 + 2X + 1)(X - 3)^4$

### Exercice 7

Décomposer dans  $\mathbb{C}(X)$  les fractions rationnelles suivantes :

$$A(X) = \frac{n!}{X(X + 1) \dots (X + n)}; \quad B(X) = \frac{1}{X^n - 1}.$$

### Exercice 8

Décomposer dans  $\mathbb{R}(X)$  la fraction rationnelle :

$$\frac{3X^2 - 1}{(X - 1)X^2(X + 1)^2}$$

En déduire, pour  $N \in \mathbb{N} \setminus \{0, 1\}$ , la valeur de la somme

$$S_N = \sum_{n=2}^N \frac{3n^2 - 1}{(n - 1)^2 n^2 (n + 1)^2}$$

et  $\lim_{N \rightarrow \infty} S_N$ .

### **Exercice 9**

Soit  $P$  un polynôme de  $\mathbb{R}$  de degré  $n \geq 1$ , possédant  $n$  racines distinctes et non nulles  $(x_k)_{1 \leq k \leq n}$ .

- 1) Décomposer en éléments simples la fraction rationnelle  $\frac{1}{X P(X)}$ .
- 2) En déduire valeur de la somme  $\sum_{k=1}^n \frac{1}{x_k P'(x_k)}$ .

### **Exercice 10**

On considère l'anneau  $K = \mathbb{Z}/5\mathbb{Z}$ . On notera par  $\bar{a}$  la classe de  $a \in \mathbb{Z}$  dans  $K$ .

- 1) Écrire les tables de l'addition et de la multiplication de  $K$ . Vérifier que  $K$  est un corps fini.
- 2) Soit  $\mathcal{A}(K, K)$  l'ensemble des applications de  $K$  dans  $K$ .  
On considère l'application  $\psi : K[X] \rightarrow \mathcal{A}(K, K)$  telle que  $\psi(P(X)) = \hat{P}$  où  $\hat{P}$  est la fonction polynôme associée à  $P(X)$ .

Montrer que  $\psi$  est un morphisme d'anneaux. Est-il injectif? Déterminer  $\ker \psi$ .

- 3) Montrer que si  $\mathbb{K}$  est un corps infini le morphisme d'anneaux  $\phi : \mathbb{K}[X] \rightarrow \mathcal{A}(\mathbb{K}, \mathbb{K})$ ,  $\phi(P(X)) = \hat{P}$  est injectif. (l'égalité des polynômes équivaut donc à l'égalité des fonctions polynômes associées).
- 4) Dans  $K(X)$  le corps des fractions rationnelles en  $X$  à coefficients dans  $K$ , on considère la fraction
 
$$F(X) = \frac{X^5 + \bar{2}X^4 + \bar{2}X^2 + \bar{2}X}{(X + \bar{1})^2(X + \bar{3})}.$$
  - a) Écrire l'équation de la division euclidienne de  $X^5 + \bar{2}X^4 + \bar{2}X^2 + \bar{2}X$  par  $(X + \bar{1})^2(X + \bar{3})$ .
  - b) Décomposer  $F(X)$  en éléments simples.

### Exercice 11

Soit  $\mathbb{R}[X]$  l'anneau des polynômes réels et  $P \in \mathbb{R}[X]$ .

1) Montrer que si  $z$  est une racine complexe non réelle de  $P$  (considéré comme élément de  $\mathbb{C}[X]$ ) alors  $\bar{z}$  est aussi une racine de  $P$  (où  $\bar{z}$  est le conjugué de  $z$ ).

2) En déduire que si  $n$  est impair alors  $P$  admet au moins une racine réelle.

3) Soient  $\theta \in \mathbb{R}$  et  $m \in \mathbb{N}^*$ . Déterminer tous les nombres complexes  $z$  tels que  $z^m = e^{im\theta}$  (on rappelle que  $e^{ix} = \cos x + i \sin x$  pour tout  $x \in \mathbb{R}$ )

4) On considère le polynôme réel

$$P = (1 + X)^{2n} + (1 - X)^{2n} \quad \text{où } n \text{ est un entier strictement positif.}$$

a) Déterminer le coefficient du monôme du plus haut degré de  $P$ .

b) Vérifier que  $-1$  et  $1$  ne sont pas racines de  $P$  et déterminer les racines complexes du polynôme  $P$ .

c) Décomposer  $P$  en produit de facteurs irréductibles dans  $\mathbb{C}[X]$ .

d) Décomposer  $P$  en produit de facteurs irréductibles dans  $\mathbb{R}[X]$ .

e) En déduire que

$$\prod_{k=0}^{n-1} \tan^2 \frac{(2k+1)\pi}{4n} = 1$$

### Bibliographie

1) **Claude Deschamp - André Warusfel**

Mathématiques (Tout-En-Un) première année (Cours et Exercices corrigés), *édition Dunod* 2003.

2) **Jean-louis Roque, Christian Leboeuf, Gérard Chassard, Jean Gueguand**, Cours d'algèbre, classes préparatoires aux Grandes Écoles Commerciales, Ellipses, 1987.

3) **Josette Calais**, Éléments de théorie de groupes, Presse Universitaire de France (PUF), 3-ème édition, 1998.

4) **Josette Calais**, Éléments de théorie des anneaux, Ellipses, 2006.