**REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE**

Ministère de l'Enseignement Supérieur et de la recherche Scientifique

Ecole Supérieure en Génie Electrique et Energétique d'Oran


Département du cycle préparatoire

# Cours d'algèbre I destiné aux étudiants de la première année des classes préparatoires en Sciences et Technologies

Rédigé par

**Dr. Mountassir Hamdi Cherif**

Octobre 2018

# Table des matières

## 0.1 INTRODUCTION

Ce polycopié est issu du cours d'Algèbre 1 destiné à des étudiants de première année des classes préparatoires en Sciences et Technologies. Il regroupe l'essentiel du programme de mathématiques du semestre impair sous l'appellation Algèbre 1. Ce polycopié se veut avant tout un outil complémentaire aux cours et travaux dirigés qui sont dispensés dans les programmes du cursus officiel du Juillet 2015. Dans ce polycopie, nous avons voulu dégager les points essentiels permettant à l'étudiant de combler sa compréhension de certaines parties du cours magistral pour aborder efficacement les exercices proposés au cours des séances de travaux dirigés.

Le polycopié s'articule autour de quatre chapitres. A la fin de chaque chapitre on pourra trouver une série d'exercices. La plupart de ces exercices étaient proposés lors des séances de travaux dirigés ou des épreuves (DS et ES).

Le premier chapitre est consacré aux définitions et notions générales sur éléments de logique, la théorie des ensembles et les applications avec quelques exemples illustratifs. Dans le deuxième chapitre, on donne des définitions de structure du groupe, sous-groupe, anneau et sous anneau et structure de corps, ce chapitre est aussi illustré par des exemples. Le troisième chapitre traite les sujets suivants : anneau des polynômes ; définitions, opérations sur les polynômes, arithmétique des polynômes, racines d'un polynôme, polynômes irréductibles et factorisation des polynômes. Le dernier chapitre est consacré à la décompositions les fractions rationnelles dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

Pour une bonne et bénéfique utilisation de ce polycopié, nous recommandons à nos étudiants d'avoir avant tout une bonne compréhension du cours magistral pour la résolution des exercices proposés. Un cours ne peut être considéré comme compris qu'une fois que l'on arrive à essayer de solutionner la plupart des exercices proposés qui suivent.

A la fin de ce manuscrit, nous avons donné quelques références de base classiques et récentes et que le lecteur ou l'étudiant intéressé pourra aisément consulter.

**Chapitre 1**

# Eléments de logique, ensembles et applications

## 1.1 Eléments de logique

Dans cette section nous présentons des définitions et quelques propriétés pour les propositions mathématiques.

### 1.1.1 Propositions mathématiques

**Définition 1.1.1** *Une propositions mathématiques (assertion) est tout énoncé mathématiques qui possède l'une des valeurs de vérité suivante : Vraie, notée V ou (1) ou Fausse notée F ou (0).*

***Exemple 1.1.1*** *Les énonés suivants sont des assertions :*

***1***. $2 > 3$

***2***. $\cos(2\pi n) = 1, \;\; n \in \mathbb{N}$

***3***. *Elle travaille*

***4***. $1 + 3 = 4$

***5***. $\sqrt{2} \in \mathbb{N}$

***6***. *Pour tout* $x \in \mathbb{R}, \;\; x \geq 1$

**Les connecteurs logiques :**

Soient $P$ et $Q$ deux assertions (propostions logiques), nous allons définir de nouvelles assertions construites à partir de $P$ et de $Q$.

**La négation (—, non) :** On appelle la négation de $P$ l'assertion $\overline{P}$ (non$P$), qui est fausse si $P$ est vraie et qui est vraie si $P$ est fausse.

| $P$ | 1 | 0 |
|---|---|---|
| $\overline{P}$ | 0 | 1 |

Table de vérité de *non*$P$

**Exemple 1.1.2** *1. La négation de* $\sqrt{2} \in \mathbb{N}$ *est* $\sqrt{2} \notin \mathbb{N}$.

*2. La négation de* $2 > 3$ *est* $2 \leq 3$.

*3. La négation de* $''1 + 3 = 4\,''$ *est* $''1 + 3 \neq 4\,''$.

**La conjonction ‹∧, et› :** $P \wedge Q$ est l'assertion qui est vraie lorsque $P$ et $Q$ sont toutes les deux vraies.

| $P$ | 1 | 1 | 0 | 0 |
|---|---|---|---|---|
| $Q$ | 1 | 0 | 1 | 0 |
| $P \wedge Q$ | 1 | 0 | 0 | 0 |

Table de vérité de $\langle P \wedge Q \rangle$

**Exemple 1.1.3** *1.* $(\cos(2\pi n) = 1) \wedge (2 - 1 = 1)$ *est vraie.*

*2.* $P \wedge \overline{P}$ *est toujours fausse.*

**La disjonction ‹∨, ou› :** $P \vee Q$ est l'assertion qui est vraie sauf si $P$ et $Q$ sont toutes les deux fausses.

| $P$ | 1 | 1 | 0 | 0 |
|---|---|---|---|---|
| $Q$ | 1 | 0 | 1 | 0 |
| $P \vee Q$ | 1 | 1 | 1 | 0 |

Table de vérité de $\langle P \vee Q \rangle$

**Exemple 1.1.4** *1.* $(\sqrt{3} \in \mathbb{Q}) \vee (2 + 1 = 1)$ *est fausse.*

*2.* $P \vee \overline{P}$ *est toujours vraie.*

**L'implication ‹$\Longrightarrow$› ‹si ..., alors› :** $P \Longrightarrow Q$ est l'assertion qui est fausse uniquement si $P$ est vraie et $Q$ est fausse.

| $P$ | 1 | 1 | 0 | 0 |
|---|---|---|---|---|
| $Q$ | 1 | 0 | 1 | 0 |
| $P \Longrightarrow Q$ | 1 | 0 | 1 | 1 |

Table de vérité de ‹$P \Longrightarrow Q$›

**Exemple 1.1.5** *1.* $(\sqrt{3} \in \mathbb{Q}) \Longrightarrow (2+1=1)$ *est vraie.*

*2.* $-3 \in \mathbb{Z} \Longrightarrow \ 1 > 2$ *est fausse.*

**L'équivalence ‹$\Longleftrightarrow$› ‹si et seulement si› :** $P \Longleftrightarrow Q$ est l'assertion qui est vraie si $P$ et $Q$ sont vraies ou fausses.

| $P$ | 1 | 1 | 0 | 0 |
|---|---|---|---|---|
| $Q$ | 1 | 0 | 1 | 0 |
| $P \Longleftrightarrow Q$ | 1 | 0 | 0 | 1 |

Table de vérité de ‹$P \Longleftrightarrow Q$›

**Exemple 1.1.6** *1.* $(\sqrt{3} \in \mathbb{R}) \Longleftrightarrow (1+1=2)$ *est vraie.*

*2.* $P \Longleftrightarrow \overline{P}$ *est toujours fausse.*

**La contraposition :** Les deux propositions suivantes $P \Longrightarrow Q$ et $\overline{Q} \Longrightarrow \overline{P}$ sont équivalentes.

$\overline{Q} \Longrightarrow \overline{P}$ est la contraposée de $P \Longrightarrow Q$.

| $P$ | $Q$ | $P \Longrightarrow Q$ | $\overline{Q}$ | $\overline{P}$ | $\overline{Q} \Longrightarrow \overline{P}$ | $(P \Longrightarrow Q) \Longleftrightarrow \overline{Q} \Longrightarrow \overline{P}$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 |

Table de vérité de ‹$(P \Longrightarrow Q) \Longleftrightarrow (\overline{Q} \Longrightarrow \overline{P})$›

**L'implication réciproque :** On appelle la réciproque de $P \Longrightarrow Q$ est la proposition $Q \Longrightarrow P$.

**Théorème 1.1.1** *Soient $P$, $Q$ et $R$ trois assertions*

*1.* $P \wedge Q \Longleftrightarrow Q \wedge P$ *et* $P \vee Q \Longleftrightarrow Q \vee P$ *($\wedge$ et $\wedge$ sont commutatives)*

*2.* $P \wedge (Q \wedge R) \Longleftrightarrow (P \wedge Q) \wedge R$ *et* $P \vee (Q \vee R) \Longleftrightarrow (P \vee Q) \vee R$ *($\wedge$ et $\wedge$ sont associatives)*

*3.* $P \wedge (Q \vee R) \Longleftrightarrow (P \wedge Q) \vee (P \wedge R)$ *et* $P \vee (Q \wedge R) \Longleftrightarrow (P \vee Q) \wedge (P \vee R)$

*4.* $\overline{\overline{P}} \Longleftrightarrow P$

*5.* $\overline{P \wedge Q} \Longleftrightarrow \overline{P} \vee \overline{Q}$ *et* $\overline{P \vee Q} \Longleftrightarrow \overline{P} \wedge \overline{Q}$ *(lois de Morgan)*

*6.* $(P \Longrightarrow Q) \Longleftrightarrow (\overline{P} \vee Q)$

*7.* $\overline{P \Longrightarrow Q} \Longleftrightarrow P \wedge \overline{Q}$

*8.* $(P \Longleftrightarrow Q) \Longleftrightarrow [(P \Longrightarrow Q) \wedge (Q \Longrightarrow P)]$

*9.* $\overline{P \Longleftrightarrow Q} \Longleftrightarrow (P \wedge \overline{Q}) \vee (Q \wedge \overline{P})$

*10.* $[(P \Longrightarrow Q) \wedge (Q \Longrightarrow R)] \Longrightarrow (P \Longrightarrow R)$

**Preuve.** En utilisant la table de vérité, nous montrons quelques-uns et en laissons les autres aux lecteurs

2.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $P$ | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| $Q$ | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| $R$ | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| $P \wedge Q$ | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| $(P \wedge Q) \wedge R$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $Q \wedge R$ | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| $P \wedge (Q \wedge R)$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $P \wedge (Q \wedge R) \Longleftrightarrow (P \wedge Q) \wedge R$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

3.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $P$ | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| $Q$ | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| $R$ | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| $Q \wedge R$ | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| $P \vee (Q \wedge R)$ | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| $P \vee Q$ | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 |
| $P \vee R$ | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 |
| $(P \vee Q) \wedge (P \vee R)$ | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| $P \vee (Q \wedge R) \Longleftrightarrow (P \vee Q) \wedge (P \vee R)$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

5.

| $P$ | $Q$ | $P \wedge Q$ | $\overline{P \wedge Q}$ | $\overline{P}$ | $\overline{Q}$ | $\overline{P} \vee \overline{Q}$ | $\overline{P \wedge Q} \Longleftrightarrow \overline{P} \vee \overline{Q}$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |

10.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $P$ | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| $Q$ | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| $R$ | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| $P \Longrightarrow Q$ | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |
| $Q \Longrightarrow R$ | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 |
| $(P \Longrightarrow Q) \wedge (Q \Longrightarrow R)$ | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| $P \Longrightarrow R$ | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| $[(P \Longrightarrow Q) \wedge (Q \Longrightarrow R)] \Longrightarrow (P \Longrightarrow R)$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

□

### 1.1.2 Quantifications

‹ $x^2 \geq 6$› est vraie ou fausse selon les valeurs de $x$.

- L'assertion ‹$\forall x \in E$ ; $p(x)$› est vraie si les assertions $p(x)$ sont vraies pour tous les éléments $x$ de l'ensemble $E$.

On lit ‹Pour tout $x$ appartenant à $E$, $p(x)$ ›.

- L'assertion ‹$\exists x \in E$ ; $p(x)$› est vraie s'il existe au moins un $x$ de l'ensemble $E$ pour lequel $p(x)$ est vraie.

On lit ‹il existe $x$ appartenant à $E$, $p(x)$ ›.

- L'assertion ‹$\exists! x \in E$ ; $p(x)$› est vraie s'il existe un seul $x$ de l'ensemble $E$ pour lequel $p(x)$ est vraie.

**Exemple 1.1.7** *1.* $\forall x \in \mathbb{R}$ ; $x^2 \geq 1$ *Fausse.*

*2.* $\exists x \in \mathbb{R}$ ; $x(x-1) < 0$ *Vraie pour* $x = \frac{1}{2}$.

*3.* $\exists x \in \mathbb{R}$ ; $x^2 = -1$ *Fausse.*

*4.* $\forall x \in \mathbb{R}$ ; $x^2 \geq 0$ *Vraie.*

*5.* $\exists! x = 1 \in \mathbb{N}$ ; $\frac{1}{2} \leq x \leq \frac{3}{2}$ *Vraie.*

**La négation des quantifications**

- La négation de l'assertion ‹$\forall x \in E$ ; $p(x)$› est l'assertions ‹$\exists x \in E$ ; *non* $p(x)$›.

- La négation de l'assertion $\langle \exists x \in E \ ; \ p(x) \rangle$ est l'assertions $\langle \forall x \in E \ ; \ non \ p(x) \rangle$.

**Exemple 1.1.8** *1. La négation de* $\langle \forall x \in \mathbb{R} \ ; \ x^2 \geq 1 \rangle$ *est* $\langle \exists x \in \mathbb{R} \ ; \ x^2 < 1 \rangle$.

2. La négation de $\langle \exists x \in \mathbb{N} \ ; \ x(x+1) \notin \mathbb{R} \rangle$ est $\langle \forall x \in \mathbb{N} \ ; \ x(x+1) \in \mathbb{R} \rangle$.
3. La négation de $\langle \exists x \in \mathbb{R} \ ; \forall y \in \mathbb{R} : \quad x+y=0 \rangle$ est $\langle \forall x \in \mathbb{R} \ ; \exists y \in \mathbb{R} : \quad x+y \neq 0 \rangle$.

**Remarque 1.1.1** *L'ordre des quantificateurs différents dans une assertion est très important.*

**Exemple 1.1.9** *1. L'assertion* $\langle \exists x \in \mathbb{R} \ ; \forall y \in \mathbb{R} : \quad x \geq y \rangle$ *est fausse.*
*2. L'assertion* $\langle \forall y \in \mathbb{R} \ ; \exists x \in \mathbb{R} : \quad x \geq y \rangle$ *est vraie.*

### 1.1.3 Types de raisonnements mathématiques

**Raisonnement direct**

On veut montrer que l'assertion $\langle P \Longrightarrow Q \rangle$ est vraie. On suppose que $P$ est vraie et on montre qu'alors $Q$ est vraie.

**Exemple 1.1.10** *Montrer que : si* $a, b \in \mathbb{Q}$, *alors* $a+b \in \mathbb{Q}$.
*Prenons* $a \in \mathbb{Q}$, $b \in \mathbb{Q}$. *Rappelons que les rationnels* $\mathbb{Q}$ *sont l'ensemble des réels s'écrivant* $\frac{p}{q}$, *avec* $p \in \mathbb{Z}$ *et* $q \in \mathbb{N}^*$.
*Alors* $a = \frac{p}{q}$ , *avec* $p \in \mathbb{Z}$ *et* $q \in \mathbb{N}^*$. *De même* $b = \frac{p'}{q'}$ , *avec* $p' \in \mathbb{Z}$ *et* $q' \in \mathbb{N}^*$.
*Donc* $a+b = \frac{p}{q} + \frac{p'}{q'} = \frac{pq'+p'q}{qq'} \in \mathbb{Q}$, *avec* $pq' + p'q \in \mathbb{Z}$ *et* $qq' \in \mathbb{N}^*$.

**Raisonnement par la contraposition**

Le raisonnement par contraposition est basé sur l'équivalence : $(P \Longrightarrow Q) \Longleftrightarrow (\overline{Q} \Longrightarrow \overline{P})$. Donc si l'on souhaite montrer l'assertion « $P \Longrightarrow Q$ », on montre en fait que si $\overline{Q}$ est vraie alors $\overline{P}$ est vraie.

**Exemple 1.1.11** *Soit* $n \in \mathbb{N}$. *Montrer que : si* $n^2$ *est pair alors* $n$ *est pair.*
*On veut monter que :* « $\forall n \in \mathbb{N}$, $n^2$ *est pair* $\Longrightarrow$ $n$ *est pair* ».

*On suppose que $n$ n'est pas pair, et on montre qu'alors $n^2$ n'est pas pair.*
*Comme $n$ n'est pas pair, il est impair et donc il existe $k \in \mathbb{N}$ tel que : $n = 2k + 1$. Alors $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2k' + 1$ avec $k' \in \mathbb{N}$. Donc $n^2$ est impair, nous avons montré que si $n$ est impair alors $n^2$ est impair. Par contraposition ceci est équivalent à : si $n^2$ est pair alors $n$ est pair.*

**Raisonnement par l'absurde**

Pour montrer que : « $P \Longrightarrow Q$ », on suppose à la fois que $P$ est vraie et que $Q$ est fausse et on cherche une contradiction. Ainsi si $P$ est vraie alors $Q$ doit être vraie.

**Exemple 1.1.12** *Soient $a, b \geq 0$. Montrer que : si $\frac{a}{1+b} = \frac{b}{1+a}$, alors $a = b$ c'est-à-dire : $\frac{a}{1+b} = \frac{b}{1+a} \Longrightarrow a = b$.*
*Par l'absurde en supposant que : $\frac{a}{1+b} = \frac{b}{1+a}$ et $a \neq b$.*
*Comme $\frac{a}{1+b} = \frac{b}{1+a}$ alors $a(1 + a) = b(1 + b)$ donc $a + a^2 = b + b^2$ d'où $a^2 - b^2 = b - a$. Cela conduit à $(a - b)(a + b) = -(a - b)$.*
*Comme $a \neq b$ alors, en divisant par $a-b$ on obtient $a+b = -1$. On obtient une contradiction car la somme de deux nombres positifs ne peut être négative.*
*On conclut que : si $\frac{a}{1+b} = \frac{b}{1+a}$, alors $a = b$ .*

**Raisonnement par contre exemple**

Si l'on veut montrer qu'une assertion du type $\langle[\forall x \in E \ ; \ p(x)] \Longleftrightarrow [\forall x(x \in E \Longrightarrow \ p(x)]\rangle$ est vraie alors pour chaque $x$ de $E$ il faut montrer que $p(x)$ est vraie. Par contre pour montrer que cette assertion est fausse, alors il suffit de trouver $x \in E$ tel que $p(x)$ soit fausse.

**Exemple 1.1.13** *La propriété suivante est-elle vraie : "deux rectangles de même aire ont même périmètre".*
*Preuve : Les rectangles de longueurs respectives $4m$ et $2m$ et de largeurs respectives $0,5$ et $1$ constituent un contre-exemple.*

**Exemple 1.1.14** *L'assertion $\langle[\forall x \in \mathbb{R} \ ; \ x^2 \leq 3] \Longleftrightarrow [\forall x(x \in \mathbb{R} \Longrightarrow x^2 \leq 3]\rangle$ est-elle vraie ?*
*Cette assertion est fausse car : $\exists x = 3 \in \mathbb{R}$ (vraie) mais $x^2 = 9 > 3$ (fausse).*

# 1.2 Ensembles

## 1.2.1 Définitions

**Définition 1.2.1** *(ensemble)*

*un ensemble est un groupement d'objet distincts.*

*- si $x$ est un élément de $E$, on écrit $x \in E$.*

*- si $x$ n'est pas un élément de $E$, on écrit $x \notin E$.*

**Définition 1.2.2** *(cardinal)*

*Le nombre d'élément de $E$ est appelé le cardinal et on le note $card(E)$, un ensemble qui n'ést pas fini est dit infini.*

**Exemple 1.2.1** *1)- Les ensembles usuels :*

- *l'ensemble des entiers naturels* $\mathbb{N} = \{0, 1, 2, 3, ...\}$.
- *l'ensemble des entiers relatifs* $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$.
- *l'ensemble des rationnels* $\mathbb{Q} = \{\frac{p}{q}, \text{ avec } p \in \mathbb{Z} \text{ et } q \in \mathbb{N}^*\}$.
- *l'ensemble des réels* $\mathbb{R}$.
- *l'ensemble des nombres complexes* $\mathbb{C}$.

*2)-* $A = \{x \in \mathbb{N};\ 0 \leq x \leq 5\} = \{0, 1, 2, 3, 4, 5\}$.

$card(A) = 6$.

- Un ensemble particulier est l'ensemble vide, noté $\emptyset$ qui est l'ensemble ne contenant aucun élément. $card(\emptyset) = 0$

- Un ensemble **Singleton** contient un seul élément, son cardinal vaut 1.

## 1.2.2 Produit cartésien

**Définition 1.2.3** *On appelle produit de deux ensembles $E$ et $F$, noté $E \times F$, l'ensemble des couples $(x, y)$ tels que $x \in E$ et $y \in F$ c'est-'a-dire :* $E \times F = \{(x, y);\ x \in E \text{ et } y \in F\}$.

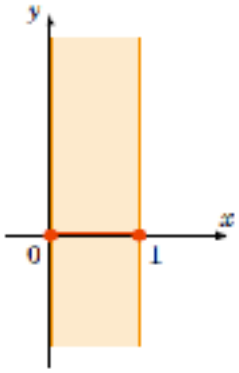
*Plus généralement, on définit le produit cartésien de $n$ ensembles $E_1, E_2, \cdots, E_n$ par*

$$\prod_{i=1}^{n} E_i = \{(x_1, \cdots, x_n);\ \forall i = 1, \cdots, n,\ x_i \in E_i\}.$$

***Exemple 1.2.2*** *1)-* $\mathbb{R}^n = \underbrace{\mathbb{R} \times \mathbb{R} \times ... \times \mathbb{R}}_{n\ fois}$

*2)-* $\mathbb{R}^2 = \{(x, y);\ \ x \in \mathbb{R}\ \ et\ \ y \in \mathbb{R}\}$.

*3)-* $A \times \mathbb{R} = \{(x, y);\ \ x \in A = [0, 1]\ \ et\ \ y \in \mathbb{R}\}$.




**Proposition 1.2.1** *Soient E, F deux ensembles finis, alors*

$$card(E \times F) = card(E) \times card(F)$$

**Exemple 1.2.3** *Soient* $E = \{a, b, c\}$ *et* $F = \{1, 2, 3, 4\}$.

$card(E) = 3$ *et* $card(F) = 4$ *, alors* $card(E \times F) = 12$.

$E \times F = \{(x, y);\ \ x \in E\ \ et\ \ y \in F\}$

$= \{(a, 1), (a, 2), (a, 3), (a, 4), (b, 1), (b, 2), (b, 3), (b, 4), (c, 1), (c, 2), (c, 3), (c, 4)\}$.

*En génal,* $E \times F \neq F \times E$.

### 1.2.3 Ensemble des parties

**Définition 1.2.4** *Soit E un ensemble, les sous ensembles de E forment un ensemble appelé ensemble des parties de E noté par :* $p(E)$.

$$A \in p(E) \Longleftrightarrow A \subseteq E$$

**Proposition 1.2.2** *Soit E un ensembles fini, alors*

$$card(p(E)) = 2^{card(E)}$$

Soit $E = \{a, b, c\}$, alors $card(E) = 3$ et $card(p(E)) = 8$.

En effet, $p(E) = \{\emptyset, E, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}\}$.

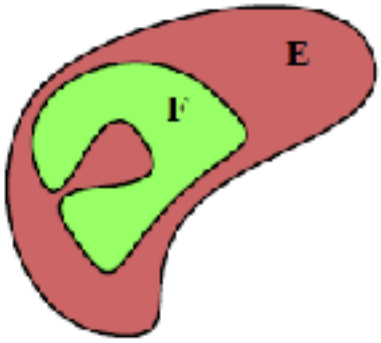
### 1.2.4 Opérations sur les ensembles

**Inclusion**

Soient $E, F$ deux ensembles

- On dit que $F$ est inclus dans $E$, ou que $E$ contient $F$, ou que $F$ est une partie de $E$ si tout élément de $F$ est élément de $E$.

Autrement dit, $F \subset E \Longleftrightarrow [\forall x(x \in F \Longrightarrow x \in E)]$




- L'ensemble vide $\emptyset$ est inclus dans tout ensemble.

**Egalité**

- $E = F$ si et seulement si $E \subset F$ et $F \subset E$.

Autrement dit, $E = F \Longleftrightarrow [\forall x(x \in E \Longleftrightarrow x \in F)]$

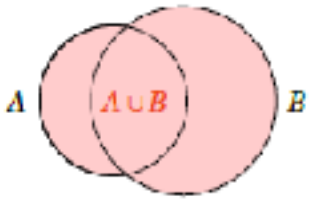
**Exemple 1.2.4** $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

**Union**

Soient $A$, $B$ et $C$ trois parties d'un ensemble $E$.

- On applelle réunion de $A$ et $B$, notée $A \cup B$ l'ensemble des $x$ tels que $x \in A$ ou $x \in B$ (Le «ou» n'est pas exclusif : $x$ peut appartenir à $A$ et à $B$ en même temps).

Autrement dit, $A \cup B = \{x, \quad x \in A \vee x \in B\}$, $x \in A \cup B \Longleftrightarrow x \in A \vee x \in B$




**Proposition 1.2.3** *1.* $A \cup B = B \cup A \quad et \quad (A \cup B) \cup C = A \cup (B \cup C)$

*2.* $A \subset (A \cup B) \Longrightarrow A \cup B = B$

*3.* $A \cup \emptyset = A \quad , \quad A \cup A = A \quad , \quad A \cup E = E$

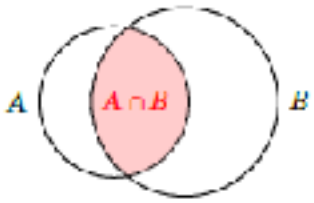
*4.* $A \subset (A \cup B) \quad et \quad B \subset (A \cup B).$

**Intersection**

Soient $A$, $B$ et $C \in p(E)$.

- On applelle l'intersection de $A$ et $B$, notée $A \cap B$ l'ensemble des $x$ tels que $x \in A$ et $x \in B$.

Autrement dit, $A \cap B = \{x, \quad x \in A \wedge x \in B\}$, $x \in A \cap B \Longleftrightarrow x \in A \wedge x \in B$




**Proposition 1.2.4** *1.* $A \cap B = B \cap A \quad et \quad (A \cap B) \cap C = A \cap (B \cap C)$

*2.* $A \subset B \Longleftrightarrow A \cap B = A$

*3.* $A \cap \emptyset = \emptyset \quad , \quad A \cap A = A \quad , \quad A \cap E = A$

*4.* $A \cap B \subset A \quad et \quad A \cap B \subset B.$

*5.* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad et \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

*6. Si $A$ et $B$ sont finis, alors*

*a)* $card(A \cup B) = card(A) + card(B) - card(A \cap B)$

*b)* $card(A \cap B) \leq \min(card(A), card(B))$

**Lemme 1.2.1** *Soient $A$ et $B$ deux ensembles finis.*

*Si* $A \subset B$ *et* $card(A) = card(B)$ *, alors* $A = B.$

**Complémentaire**

Soit $A \in p(E)$.

- On applelle complémentaire de $A$ dans $E$, notée $C_E(A)$, $E \setminus A$ (et parfois $\overline{A}$, $A^c$ ) l'ensemble des $x$ tels que $x \in E$ et $x \notin A$ .

Autrement dit,

$C_E(A) = \{x, \quad x \in E \wedge x \notin A\}$ , $x \in C_E(A) \Longleftrightarrow x \in E \wedge x \notin A \Longleftrightarrow x \in E \wedge x \in \overline{A}$

**Proposition 1.2.5** *1.* $A \cap C_E(A) = \emptyset \quad$ *et* $\quad A \cup C_E(A) = E$

*2.* $C_E(C_E(A)) = A$ , $\quad C_E(E) = \emptyset$ , $\quad C_E(\emptyset) = E$

*3.* $C_E(A \cap B) = C_E(A) \cup C_E(B) \quad$ *et* $\quad C_E(A \cup B) = C_E(A) \cap C_E(B)$.

*4. Si* $A \subset E$ *, avec* $E$ *est fini, alors* $card(C_E(A)) = card(E) - card(A)$

**Preuve.** 3.

$x \in C_E(A \cap B) \Longleftrightarrow x \in E \wedge x \notin A \cap B \Longleftrightarrow x \in E \wedge \overline{x \in A \cap B} \Longleftrightarrow x \in E \wedge (x \notin A \vee x \notin B)$ $\Longleftrightarrow (x \in E \wedge x \notin A) \vee (x \in E \wedge x \notin B) \Longleftrightarrow x \in C_E(A) \vee x \in x \in C_E(B) \Longleftrightarrow x \in C_E(A) \cup C_E(B)$ □

**Différence et différence symétrique**

Soient $A$, $B \in p(E)$.

- On applelle la différence de $A$ et $B$, notée $A \setminus B$ l'ensemble des $x$ tels que $x \in A$ et $x \notin B$

Autrement dit, $A \setminus B = \{x, \quad x \in A \wedge x \notin B\} = A \cap C_E(B)$.

$x \in A \setminus B \Longleftrightarrow x \in A \wedge x \notin B \Longleftrightarrow x \in A \wedge x \in C_E(B) \Longleftrightarrow x \in A \cap C_E(B)$.

- La différence symétrique $A$ et $B$, notée $A \triangle B$ est définie par :

$A \triangle B = \{x, \quad x \in A \cup B \wedge x \notin A \cap B\}$ .

$A \triangle B = (A \cup B) \setminus (A \cap B) = A \setminus B \cup B \setminus A = A \cap C_E(B) \cup B \cap C_E(A)$

# 1.3 Applications

## 1.3.1 Définitions

**Définition 1.3.1** *Soient* $E$ *et* $F$ *deux ensembles. On appelle application de* $E$ *dans* $F$*, toute correspondance* $f$ *entre les éléments de* $E$ *et ceux de* $F$ *qui à tout élément* $x \in E$ *fait corres-*

*pondre un unique élément $y \in F$ noté $f(x)$.*

*– $y = f(x)$ est appelé image de $x$ et $x$ est un antécédant de $y$.*

– On représente l'application $f$ de $E$ dans $F$ par $f : E \longrightarrow F$.

– L'enemble $E$ est appelé ensemble de départ et $F$ l'ensemble d'arrivée de l'application $f$.

– Le graphe de $f$ est l'ensemble des couples $(x; f(x))$.

– Notons que tout élément de $F$ n'est pas nécessairement l'image d'un élément de $E$.

Formellement, une correspondance $f$ entre deux ensembles non vides est une application si et seulement si :

$$\forall x, x' \in E; \quad (x = x') \Longrightarrow (f(x) = f(x'))$$

Autrement dit :

$$\forall x \in E;\ \exists! y \in F \quad \text{tel que :} \quad y = f(x)$$

– On notera $F(E; F)$ l'ensemble des applications de $E$ dans $F$. (On trouve egalement la notation $F^E$).

**Exemple 1.3.1** • *Soit $E$ un ensemble. L'application qui à chaque élément $x$ de $E$ associe lui-même est appelée application identique ou identité de $E$. On la note $Id_E$.*

$$Id_E : E \longrightarrow E, \qquad \forall x \in E; \qquad Id_E(x) = x.$$

• *Soient $E$, $F$ deux ensembles et $a \in F$. Si tout élément $x$ de $E$ a pour image $f(x) = a$, l'application est dite constante et égale à $a$.*

$$f : E \longrightarrow F, \qquad \forall x \in E; \qquad f(x) = a.$$

• *Soient $E$ un ensemble et $A$ une partie de $E$. On appelle fonction caractéristique de $A$ dans $E$ ou fonction indicatrice de $A$ dans $E$ la fonction de $E$ dans $\{0; 1\}$ telle que :*
*$f(x) = 1$ si $x \in A$ et $f(x) = 0$ si $x \notin A$.*

• *L'application qui à chaque nombre réel $x$ associe $0$ est appelée application nulle.*
$f : E \longrightarrow F, \qquad \forall x \in E; \qquad f(x) = 0.$

• *Soient $n$ un entier positif et $a_0$, $a_1$,..., $a_n$ des réels, la fonction $p : \mathbb{R} \longrightarrow \mathbb{R}$ qui à chaque réel $x$, associe : $p(x) = a_0 + a_1x + ... + a_nx^n$ est appelée une application (fonction) polynôme.*

**Définition 1.3.2** *( Egalité de deux applications)*

*On dit que deux applications $f$ et $g$ sont égales si :*

*1. Elles ont un même ensemble de départ $E$ et un même ensemble d'arrivée $F$.*

*2.* $\forall x \in E,\ \ f(x) = g(x)$.

**Définition 1.3.3** *( Somme de deux applications et multiplication une application par un scalaire)*

*Soient* $f, g : E \longrightarrow F$ *deux applications et* $\lambda \in \Bbbk$ $(\Bbbk = \mathbb{R} \vee \mathbb{C})$*, alors*

*1.* $f + g$ *est une application telle que :* $\forall x \in E; \quad (f+g)(x) = f(x) + g(x)$.

*2.* $\lambda f$ *est une application telle que :* $\forall x \in E; \quad (\lambda f)(x) = \lambda f(x)$.

**Définition 1.3.4** *(Composition des applications)*

*Soient* $f : E \longrightarrow F$ *et* $g : F \longrightarrow G$*, on note* $g \circ f$ *l'application de* $E$ *dans* $G$ *définie par :*

$$\forall x \in E, \quad (g \circ f)(x) = g(f(x)).$$

*Cette application est appelée composée des applications $f$ et $g$.*

***Exemple 1.3.2*** *Etant données les applications*

$f : \mathbb{R}_+^* \longrightarrow \mathbb{R}_+^*\ ,\ \ \forall x \in \mathbb{R}_+^*\ ;\quad f(x) = \frac{1}{x}$ *et* $g : \mathbb{R}_+^* \longrightarrow \mathbb{R},\ \ \forall x \in \mathbb{R}_+^*\ ;\quad g(x) = \frac{x}{x+1}$

*alors*

$g \circ f : \mathbb{R}_+^* \longrightarrow \mathbb{R},\ \ \forall x \in \mathbb{R}_+^*;\quad (g \circ f)(x) = g(f(x)) = g(\frac{1}{x}) = \frac{\frac{1}{x}}{\frac{1}{x}+1} = \frac{1}{x+1}$ *et* $f \circ g$ *n'est pas bien définie.*

**Proposition 1.3.1** *1. Soient $E$, $F$, $G$ et $H$ quatre ensembles.*

*Pour toutes applications* $f : E \longrightarrow F$, $g : F \longrightarrow G$ *et* $h : G \longrightarrow H$*, on a*

$$(h \circ g) \circ f = h \circ (g \circ f)$$

*2. Si* $f : E \longrightarrow F$, *on a*

$$f \circ Id_E = f \qquad et \qquad Id_F \circ f = f$$

### 1.3.2 Image directe, image réciproque

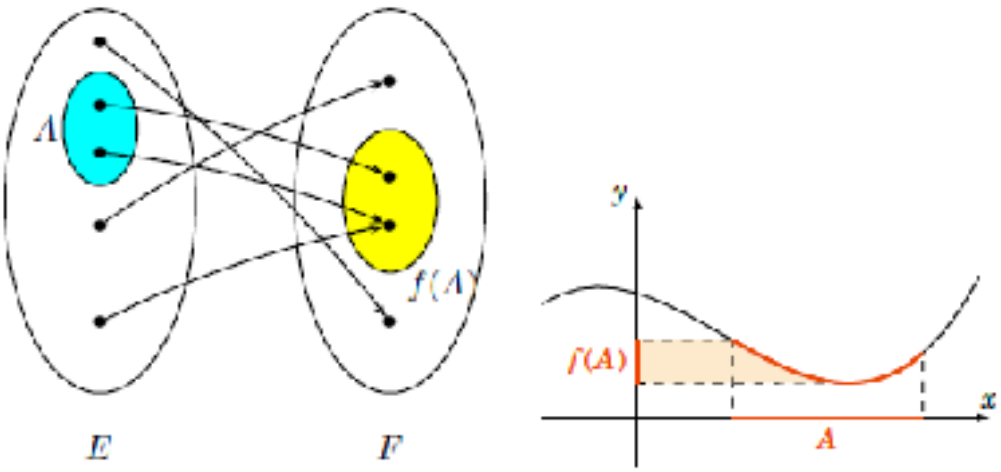
**Définition 1.3.5** *Soient* $f : E \longrightarrow F$ *et* $A \subset E$ .

*On appelle image de* $A$ *par* $f$*, l'ensemble des images des éléments de* $A$ *noté :*

$$f(A) = \{f(x), \qquad x \in A\} \subset F$$

Formellement on a :

$$\forall y \in F,\ y \in f(A) \Longleftrightarrow \exists x \in A,\ y = f(x)$$



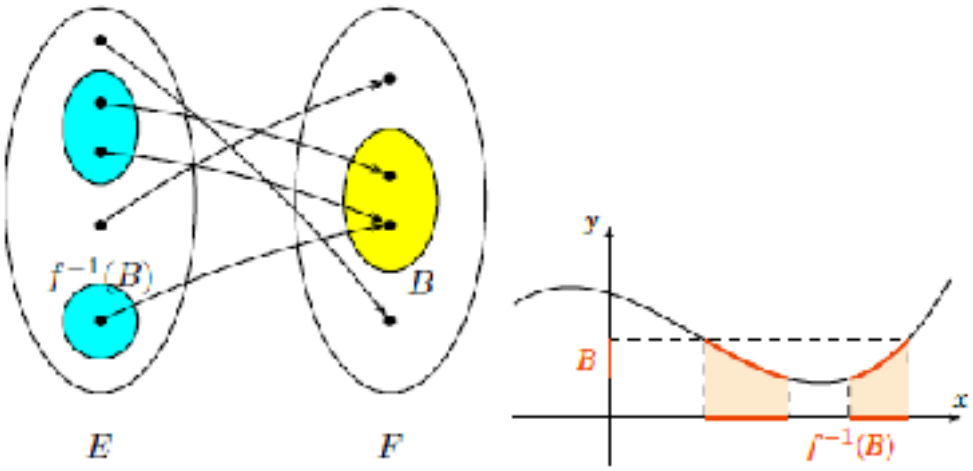

**Définition 1.3.6** *Soient* $f : E \longrightarrow F$ *et* $B \subset F$.

*On appelle image réciproque de* $B$ *par* $f$*, l'ensemble des antécédents des éléments de* $B$*, noté*

$$f^{-1}(B) = \{x \in E, \qquad f(x) \in B\} \subset E$$

*Formellement on a :*

$$\forall x \in E,\ x \in f^{-1}(B) \Longleftrightarrow f(x) \in B$$




**Exemple 1.3.3** *Soit l'application $f$ définie de $\mathbb{R}$ dans $\mathbb{R}$ par : $f(x) = 2x + 1$, $\forall x \in \mathbb{R}$. Soient $A = \{1, 2, 4\}$ et $B = \{1, 7\}$, alors $f(A) = \{3, 5, 9\}$ et $f^{-1}(B) = \{0, 3\}$.*

**Proposition 1.3.2** *Soient $f : E \longrightarrow F$, $A, A' \subset E$ et $B, B' \subset F$, alors*

1. $A \subset A' \Longrightarrow f(A) \subset f(A')$ et $B \subset B' \Longrightarrow f^{-1}(B) \subset f^{-1}(B')$
2. $f(A \cup A') = f(A) \cup f(A')$
3. $f(A \cap A') \subset f(A) \cap f(A')$
4. $f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B')$
5. $f^{-1}(B \cap B') = f^{-1}(B) \cap f^{-1}(B')$
6. $f^{-1}(\complement_F B) = \complement_E f^{-1}(B)$.

**Remarque 1.3.1** *Les ensembles $\complement_F f(A)$ et $f(\complement_E A)$ ne sont pas toujours comparables.*

### 1.3.3 Injection, surjection, bijection

Soit $f : E \longrightarrow F$ une application.

**Définition 1.3.7** *(Injectivité)*

*On dit que $f$ est injective si tout élément de $F$ possède au plus un antécédant. C'est-à-dire que deux éléments distincts de $E$ ne peuvent pas être des antécédents d'un même élément de $F$, ce qui revient formellement a :*

$$f \text{ est injective } \Longleftrightarrow \forall x, x' \in E,\ (x \neq x' \Longrightarrow f(x) \neq f(x'))$$

*ou*

$$f \text{ est injective } \iff \forall x, x' \in E,\ (f(x) = f(x') \Longrightarrow x = x')$$

**Exemple 1.3.4** *1. Soit l'application $f$ définie de $\mathbb{R}$ dans $\mathbb{R}$ par : $f(x) = x^2$.*
*Pour $x = -2$ et $x = 2$, on a : $f(x) = f(x') = 4$, donc $f$ n'est pas injective.*
*2. Soit l'application $f$ définie de $\mathbb{R}$ dans $\mathbb{R}$ par : $f(x) = 2x + 1$.*
*On a : $\forall x, x' \in \mathbb{R},\ f(x) = f(x') \Longrightarrow x = x'$.*
*Donc $f$ est injective.*

***Remarque 1.3.2*** *Toute application monotone injective.*

**Définition 1.3.8** *(Surjectivité)*

*On dit que $f$ est surjective si tout élément de $F$ possède au moins un antécédant. Ce qui revient formellement a :*

$$f \text{ est surjective} \iff \forall y \in F,\ \exists x \in E;\ y = f(x)$$

**Exemple 1.3.5** *1. Soit l'application $f$ définie de $\mathbb{R}$ dans $\mathbb{R}$ par : $f(x) = x^2$.*
*$f$ n'est pas surjective car pour $y = -1$, $\nexists x \in \mathbb{R}$ tel que : $x^2 = -1$.*
*2. Si $f$ est définie de $\mathbb{R}$ dans $\mathbb{R}_+$ par : $f(x) = x^2$,*
*$f$ est surjective car : $\forall y \in \mathbb{R}_+$, $\exists x = \sqrt{y} \in \mathbb{R}$ tel que : $f(x) = f(\sqrt{y}) = y$.*

**Définition 1.3.9** *(Bijectivité)*

*On dit que $f$ est bijective si elle est injective et surjective. Formellement on a :*

$$f \text{ est bijective} \iff \forall y \in F,\ \exists! x \in E;\ y = f(x)$$

*L'existence du $x$ vient de la surjectivité et l'unicité de l'injectivité.*
*Autrement dit, tout élément de $F$ a un unique antécédent par $f$ .*

### L'application réciproque

**Proposition 1.3.3** *Une application $f : E \longrightarrow F$ est bijective si et seulement si il existe une unique application $g : F \longrightarrow E$ telle que :*

$$f \circ g = Id_F \quad et \quad g \circ f = Id_E \ .$$

*Si $f$ est bijective alors l'application $g$ est unique et elle est aussi bijective. L'application $g$ s'appelle la bijection réciproque de $f$ et elle est notée $f^{-1}$.*
*De plus*

$$(f^{-1})^{-1} = f.$$

**Exemple 1.3.6** *1. On considère l'application $f : \mathbb{R} \longrightarrow \mathbb{R}$ telle que : $f(x) = 2x + 1$.*
*Pour montrer que $f$ est bijective, on revient à examiner l'existence de solution de l'équation $y = f(x)$, pour tout $y \in \mathbb{R}$.*
*Soit $y \in \mathbb{R}$, alors*

$$\begin{aligned} y &= f(x) \Longleftrightarrow y = 2x + 1 \\ &\Longleftrightarrow 2x = y - 1 \\ &\Longleftrightarrow x = \frac{y-1}{2} \end{aligned}$$

*Donc $f^{-1}$ existe, elle est définie par : $f^{-1} : \mathbb{R} \longrightarrow \mathbb{R}$ telle que :*

$$f(y) = \frac{y-1}{2}.$$

*De plus $f \circ f^{-1} = Id$ et $f^{-1} \circ f = Id$ .*
*2. $f : \mathbb{R} \longrightarrow \mathbb{R}_+^*$ définie par $f(x) = \exp(x)$ est bijective, sa bijection réciproque est $g : \mathbb{R}_+^* \longrightarrow \mathbb{R}$ définie par $g(y) = \ln(y)$.*
*Nous avons bien : $\exp(\ln(y)) = y$, pour tout $y \in \mathbb{R}_+^*$ et $\ln(\exp(x)) = x$, pour tout $x \in \mathbb{R}$.*

**Proposition 1.3.4** *Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$, alors*
*1. ($f$ injective ) $\wedge$ ($g$ injective ) $\Longrightarrow$ ($g \circ f$ injective ).*
*2. ($f$ surjective ) $\wedge$ ($g$ surjective ) $\Longrightarrow$ ($g \circ f$ surjective ).*
*3. ($f$ bijective ) $\wedge$ ($g$ bijective ) $\Longrightarrow$ ($g \circ f$ bijective) et sa bijection réciproque est*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

## 1.4 Série d'exercices

**Exercice 1 :**

Soient $P, Q$ et $R$ trois assertions logiques.

1. Donner la table de vérité de $P \Longrightarrow Q$.

2. Montrer que $(P \Longrightarrow Q) \Longleftrightarrow (\overline{P} \vee Q)$. Déduire $\overline{P \Longrightarrow Q}$.

3. Montrer que $[(P \Longrightarrow Q) \wedge (Q \Longrightarrow R)] \Longrightarrow (P \Longrightarrow R)$.

**Exercice 2 :**

Indiquer parmi les propositions suivantes celles qui sont vraies et celles qui sont fausses :

(1) $\forall x \in \mathbb{R}; \quad x^2 > -1.$

(2) $\exists x \in \mathbb{R}; \quad x^2 \leq -1.$

(3) $\exists x \in \mathbb{R}; \quad x^2 - 4x + 3 = 0.$

(4) $\exists! x \in \mathbb{R}; \quad x^2 - 3x + 2 = 0.$

(5) $\forall x \in \mathbb{R}, \quad \forall y \in \mathbb{R} : \quad x + y = 0.$

(6) $\exists x \in \mathbb{R}, \quad \forall y \in \mathbb{R} : \quad x + y = 0.$

(7) $\forall x \in \mathbb{R}, \quad \exists y \in \mathbb{R} : \quad x + y = 0.$

(8) $\exists x \in \mathbb{R}, \quad \exists y \in \mathbb{R} : \quad x + y = 0.$

- Nier les propositions 5, 6, 7, 8.

**Exercice 3 :**

Soient $f$ une fonction de $\mathbb{R} \longrightarrow \mathbb{R}$.

Traduire en termes de quantificateurs les expressions suivantes, ainsi que leurs négations :

1. $f$ est bornée.
2. $f$ est paire.
3. $f$ est croissante.
4. $f$ n'a jamais les mêmes valeurs en deux points distincts.

**Exercice 4 :** (Types de raisonnements)

1) Montrer que $\forall n \in N*$, $8\frac{n(n+1)}{2} + 1$ est un carré.

2) Soit $n$ un entier. Enoncer et démontrer la contraposée de la proposition suivante :

Si $n^2$ est impair, alors $n$ est impair.

3) On rappelle que $\sqrt{2}$ est un nombre irrationnel.

Démontrer que si $a$ et $b$ sont deux entiers relatifs tels que $a + b\sqrt{2} = 0$, alors $a = b = 0$.

**Exercice 5 :**

Soit $A = \{\{1, 2, 3\}, \{4, 5\}, \{6, 7, 8\}\}$.

Parmi les propositions suivantes déterminer celles qui sont vraies :

1) $2 \in A$; 2) $\{1, 2, 3\} \in A$; 3) $\{4, 5\} \subset A$; 4) $\{\{6, 7, 8\}\} \subset A$; 5) $\emptyset \in A$; 6) $\emptyset \subset A$.

**Exercice 6 :**

Soient $A, B, C$ trois parties d'un ensemble $E$.

Montrer que :

1. $A \subset B \Longrightarrow B^c \subset A^c$.
2. $(A \cap B)^c = A^c \cup B^c$ et $(A \cup B)^c = A^c \cap B^c$ .
3. $A \setminus (A \setminus B) = A \cap B$.
4. $B \cup (A \setminus B) = A \cup B$.

**Exercice 7 :**

Soient $A, B, C$ trois parties d'un ensemble $E$.

On appelle différence symétrique de $A$ et $B$, le sous ensemble $A \triangle B$ défini par :

$A \triangle B = (A \cup B) \setminus (A \cap B)$.

1. Calculer $A \triangle A$, $A \triangle E$, $A \triangle A^c$, $A \triangle \emptyset$ .
2. Montrer que :
   a. $A \triangle B = (A \setminus B) \cup (B \setminus A)$.
   b. $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$.

**Exercice 8 :**

On considère les ensembles des parties $P(G)$ et $P(H)$ où $G$ et $H$ sont deux parties de $E$.

1. Montrer que $P(G \cap H) = P(G) \cap P(H)$ .
2. A-t-on $P(G \cup H) = P(G) \cup P(H)$ ?
3. On considère un autre ensemble F. Etablir que :
   a. $(G \cup H) \times F = (G \times F) \cup (H \times F)$.
   b. $(G \cap H) \times F = (G \times F) \cap (H \times F)$.

**Exercice 9 :**

Pour chacun des cas suivants, dire si l'application $f$ est bien définie, si oui, $f$ est-elle injective ? surjective ? bijective ?

1) $f : \{0, 1, 2\} \to \{1, 8, -1, 24\}$ ,telle que $f(0) = -1, f(1) = 24, f(2) = 1$.

2) $f : \mathbb{N} \to \mathbb{N}$ définie par : $\forall n \in \mathbb{N},\ f(n) = n + 1$.

3) $f : \mathbb{Z} \to \mathbb{Z}$ définie par : $\forall n \in \mathbb{Z},\ f(n) = -n$.

**Exercice 10 :**

Soient $E$ et $F$ deux ensembles. Soient $A, B$ deux parties de $E$ et $M, N$ deux parties de $F$. $f : E \longrightarrow F$ une application.

Montrer que :

1) $A \subset B \Rightarrow f(A) \subset f(B)$ et $M \subset N \Rightarrow f^{-1}(M) \subset f^{-1}(N)$.

2) $f(A \cup B) = f(A) \cup f(B)$.

3) $f(A \cap B) \subset f(A) \cap f(B)$, donner un exemple montrant que $f(A \cap B) \neq f(A) \cap f(B)$.

4) $f^{-1}(M \cap N) = f^{-1}(M) \cap f^{-1}(N)$.

5) $f^{-1}(C_F N) = C_E f^{-1}(N)$.

**Exercice 11 :**

Soient $f$ et $g$ deux applications de $\mathbb{R} \longrightarrow \mathbb{R}$ définies par : $f(x) = x^2 + x$ et $g(x) = 2 - x$.

1) Trouver $g(1)$, $g(\{1\})$, $f^{-1}(\{0\})$, $f([-1, 1])$, $f^{-1}(]0, +\infty[)$.

2) Montrer que $g$ admet une application réciproque que l'on calculera.

3) A-t-on $g \circ f = f \circ g$ ?

**Exercice 12 :**

Soient les deux applications suivantes $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ et $g : \mathbb{R} \longrightarrow \mathbb{R}^2$ définies par :

$$f(x, y) = xy \quad \text{et} \quad g(x) = (x, x^2)$$

1) Etudier l'injectivité, la surjectivité et la bijectivité de $g$ et de $f$ .

2) Trouver $g \circ f$ et $f \circ g$.

3) Etudier l'injectivité, la surjectivité et la bijectivité de $g \circ f$ et de $f \circ g$.

Chapitre 2

# Structures algébriques

## 2.1 Loi de composition interne

**Définition 2.1.1** *On appelle loi de composition interne (l.c.i) sur un ensemble $E$, toute application $* : E \times E \longrightarrow E$. L'ensemble $E$ est dit stable par rapport à la loi $*$ si*

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

**Exemple 2.1.1** *1. La multiplication et l'addition sont des lci sur* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *et* $\mathbb{C}$.
*2. Soit $A$ un ensemble et $E = p(A)$, alors l'intersection et la réunion d'ensembles sont deux lois de compositions internes dans $E$ car :* $\forall X, Y \in p(A), \ (X \cap Y) \subset A \ \text{ et } \ (X \cup Y) \subset A$.

*3. Si $G$ est un ensemble, sur $E = F(G; G)$, la composition des applications définit une lci.*
*4. La soustraction " $-$ " n'est pas une loi de composition interne dans* $\mathbb{N}$ *car : si* $2, 3 \in \mathbb{N}$, $2 - 3 \notin \mathbb{N}$.

**Définition 2.1.2** *(Propriétés d'une lci)*
*Soit $*$ une lci sur un ensemble $E$. On dit que $*$est :*
*commutative si et seulement si* $\forall x, y \in E, \ x * y = y * x$.
*associative si et seulement si* $\forall x, y, z \in E, \ x * (y * z) = (x * y) * z$.

**Exemple 2.1.2** *1. Les loies usuelles " $+$ " et " $\times$ " sont commutatives et associatives sur* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *et* $\mathbb{C}$.

*2. Soit $A$ un ensemble et $E = p(A)$, alors " $\cap$ " et " $\cup$ " sont commutatives et associatives sur $E$.*

*3. Soit $G$ est un ensemble, sur $E = F(G;G)$, " $\circ$ " n'est pas commutative $(g \circ f \neq f \circ g)$.*

**Définition 2.1.3** *(Elément neutre)*

*Soit $E$ un ensemble muni d'une une lci $*$. Soit $e \in E$.*

*"$e$" est un élément neutre à gauche (respectivement à droite) de la loi $*$ si $\forall x \in E, e * x = x$ (respectivement $x * e = x$)*

*Si $e$ est un élément neutre à droite et à gauche de $*$ on dit que $e$ est un élément neutre de $*$.*

**Définition 2.1.4** *(Elément symétrique)*

*Soit $*$ une lci sur un ensemble $E$ admettant un élément neutre $e$. On dit qu'un élément $x \in E$ est inversible, ou symétrisable, à droite (respectivement à gauche ) de $*$ si*

*$\exists x\prime \in E,\ x * x' = e$ (respectivement $x' * x = e$) et $x'$ est dit un inverse (ou un symétrique) à droite (respectivement à gauche ) de $x$.*

*S'il existe $x' \in E$ tel que : $x' * x = x * x' = e$ , on dit que $x$ est inversible (ou symétrisable) et $x'$est dit un inverse (ou un symétrique) de $x$ par rapport à $*$.*

**Exemple 2.1.3** *1. "0" (resp "1") est l'élément neutre de $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ par rapport à " $+$ " (resp " $\times$ ").*

*2. Soit $A$ un ensemble et $E = p(A)$, alors $\emptyset$ est l'élément neutre de " $\cup$ " et $A$ est l'élément neutre de " $\cap$ ".*

*3. " $-x$" est l'élément symétrique de $x$ sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ par rapport à " $+$ ".*

*4. "$\frac{1}{x}$" est l'élément symétrique de $x$ sur $\mathbb{R}^*$ et $\mathbb{C}^*$ par rapport à " $\times$ ".*

**Remarque 2.1.1** *1. Si $*$ possède un élément neutre, alors il est unique.*

*2. Soit $*$ une lci dans $E$, associative et admettant un élément neutre $e$. Si un élément $x \in E$ admet $x_1$ un inverse (ou symétrique) à droite et $x_2$ un inverse (ou symétrique) à gauche, alors $x_1$ et $x_2$ sont identiques. On déduit que l'associativité de la loi assure l'unicité du symétrique d'un élément s'il existe.*

## 2.2 Structure de groupe

### 2.2.1 Définitions

**Définition 2.2.1** *On appelle groupe, tout ensemble non vide $G$ muni d'une loi de composition interne $*$ telle que :*

*1. $*$ est associative ;*

*2. $*$ possède un élément neutre $e$ ;*

*3. Tout élément de $E$ est symétrisable.*

*Si de plus $*$ est commutative, on dit que $(G, *)$ est un groupe commutatif, ou groupe Abélien.*

**Exemple 2.2.1** *1. $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs.*

*2. $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes commutatifs.*

*3. $(\mathbb{N}, +)$ n'est pas un groupe.*

*4. On définit la loi * sur $\mathbb{R} - \{1\}$ par :*

$$\forall x, y \in \mathbb{R} - \{1\}, \quad x * y = x + y - xy$$

*$(\mathbb{R} - \{1\}, *)$ est un groupe commutatif car :*

*a). Loi de composition interne :*

*$*$ est une loi de composition interne dans $\mathbb{R} - \{1\}$ ssi $\forall x, y \in \mathbb{R} - \{1\}, \ x * y \in -\{1\}$ ie :*

$(x \neq 1 \wedge y \neq 1) \Longrightarrow x * y = x + y - xy \neq 1$.

*On suppose que $x \neq 1$ et $y \neq 1$ mais $x + y - xy = 1$.*

$x + y - xy = 1 \Longleftrightarrow x - 1 + y - xy = 0 \Longleftrightarrow (x - 1)(1 - y) = 0 \Longrightarrow (x = 1) \vee (y = 1)$

*contradiction, donc si $\forall x, y \in \mathbb{R} - \{1\}$, alors $x * y \in \mathbb{R} - \{1\}$.*

*b). Commutativité :*

*$*$ est commutative car : $\forall x, y \in \mathbb{R} - \{1\}, \ x * y = x + y - xy = y + x - yx = y * x$.*

*c). Associativité :*

$*$ *est associative ssi :* $\forall x, y, z \in \mathbb{R} - \{1\}\,,\ \ (x * y) * z = x * (y * z)$.

$$\begin{aligned}(x * y) * z &= (x + y - xy) * z \\ &= (x + y - xy) + z - (x + y - xy)z \\ &= x + y - xy + z - xz - yz + xyz \\ &= x + (y + z - yz) - x(y + z - yz) \\ &= x * (y + z - yz) \\ &= x * (y * z).\end{aligned}$$

*d) . L'élément neutre :*

$\overset{?}{\exists} e \in \mathbb{R} - \{1\}\,, \forall x \in \mathbb{R} - \{1\}\,;\ \ x * e = x$

$$\begin{aligned}x * e &= x \Longleftrightarrow x + e - xe = x \\ &\Longleftrightarrow e(1 - x) = 0 \\ &\Longrightarrow e = 0 \ \ (x \neq 1)\end{aligned}$$

*e). L'élément symétrique :*

$\forall x \in \mathbb{R} - \{1\}\,, \overset{?}{\exists} x' \in \mathbb{R} - \{1\}\,;\ \ x * x' = 0$

$$\begin{aligned}x * x' &= 0 \Longleftrightarrow x + x' - xx\prime = 0 \\ &\Longrightarrow x' = \frac{-x}{1 - x} \in \mathbb{R} - \{1\}\end{aligned}$$

### 2.2.2 Sous groupes

**Définition 2.2.2** *Soient $(G, *)$ un groupe et $H$ une partie de $G$. On dit que $H$ est un sous groupe de $G$ ssi*

*1.* $e \in H \quad (H \neq \emptyset)$.

*2.* $\forall x, y \in H$, $x * y \in H$ .

*3.* $\forall x \in H$, $x^{-1} \in H$ .

**Remarque 2.2.1** *Un critère pratique et plus rapide pour prouver que $H$ est un sous-groupe de $G$ est :*

– *$H$ contient au moins un élément (élément neutre).*

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

**Exemple 2.2.2** *1). $(\mathbb{Z},+)$ et $(\mathbb{Q},+)$ sont des sous groupes de $(\mathbb{R},+)$ .*

*2). $(\mathbb{R}_+^*,\times)$ est un sous groupe de $(\mathbb{R}^*,\times)$.*

*3). Soit $(G,*)$ un groupe non commutatif.*

*Soit $C(G)=\{a\in G;\quad x*a=a*x,\ \ \forall x\in G\}$(centre d'un groupe) .*

*Le centre $C(G)$ est un sous groupe de $(G,*)$.*

*4). Soient $a\in\mathbb{C}^*$ et $H=\{a^n,\ \ n\in\mathbb{Z}\}$ est un sous groupe de $(\mathbb{C}^*,\times)$.*

*a). $1\in H$ car $\exists n=1\in\mathbb{Z};\ 1=a^1$.*

*b). Soient $z_1,z_2\in H$; est-ce que $z_1,z_2\in H$?*

*Comme $z_1,z_2\in H$, alors $\exists n_1\in\mathbb{Z}$ tel que : $z_1=a^{n_1}$ et $\exists n_2\in\mathbb{Z}$ tel que : $z_2=a^{n_2}$*

$$z_1\times z_2=a^{n_1}\times a^{n_2}=a^{n_1+n_2}$$

*Donc, $z_1\times z_2\in H$ car $\exists n_1+n_2\in\mathbb{Z}$ tel que : $z_1\times z_2=a^{n_1+n_2}$.*

*c). Soit $z\in H$; $\exists n\in\mathbb{Z}$ tel que : $z=a^n$, alors $z^{-1}=a^{-n}$*

*Donc, $z^{-1}\in H$ car $\exists -n\in\mathbb{Z}$ tel que : $z^{-1}=a^{-n}$.*

**Opérations sur les sous groupes**

**Proposition 2.2.1** *Soient $H$ et $K$ deux sous groupes de $(G,*)$, alors*

*1. $H\cap K$ est un sous groupe de $(G,*)$.*

*2. En général, $H\cup K$ n'est pas forcément un sous groupe de $(G,*)$.*

***Preuve.***

*1. $H\cap K$ est un sous groupe de $(G,*)$ ssi :* $\begin{cases} e\in H\cap K \\ \forall x,y\in H\cap K;\quad x*y^{-1}\in H\cap K \end{cases}$.

*a) $e\in H\cap K$ car : $e\in H\wedge e\in K$ ($H$ et $K$ deux sous groupes de $(G,*)$).*

*b) On a : $x,y\in H\cap K$, c'est-à-dire :* $\begin{cases} x\in H\wedge x\in K \\ y\in H\wedge y\in K \end{cases}$.

*Comme $H$ et $K$ sont deux sous groupes de $(G,*)$, on obtient : $x*y^{-1}\in H\wedge x*y^{-1}\in K$.*

*Donc, $x*y^{-1}\in H\cap K$.*

*2. Soit le contre exemple suivant :*

*Soient $(\mathbb{Z},+)$ un groupe et $(n\mathbb{Z},+)$ les sous groupes de $(\mathbb{Z},+)$, avec $n\in\mathbb{N}$.*

*$n\mathbb{Z}=\{na,\ \ a\in\mathbb{Z}\}$ et soient $H=2\mathbb{Z}=\{2a,\ \ a\in\mathbb{Z}\}$ et $K=3\mathbb{Z}=\{3a,\ \ a\in\mathbb{Z}\}$.*

*Alors $H\cup K=\{2a,\ 3a\ ;\ \ a\in\mathbb{Z}\}$.*

*Si, on prend par exemple :*

*$2\in H$ et $3\in K$, alors $2\in H\cup K$ et $3\in H\cup K$ mais $2+3\notin H\cup K$.*

*Donc* $2\mathbb{Z} \cup 3\mathbb{Z}$ *n'est pas un sous groupe de* $(\mathbb{Z}, +)$. □

## 2.3 Structure d'anneaux et sous anneaux

### 2.3.1 Anneaux

**Définition 2.3.1** *On appelle anneau, tout ensemble* $A$ *muni de deux lois de composition internes* $+$ *et* $\bullet$ *telles que :*

*1.* $(A, +)$ *est un groupe abélien (on notera* $0$ *ou* $0_A$ *l'élément neutre de* $+$*),*

*2.* $\bullet$ *est associative ;*

$$\forall x, y, z \in A,\ (x \bullet y) \bullet z = x \bullet (y \bullet z).$$

*3.* $\bullet$ *distributive à droite et à gauche par rapport à* $+$ *;*

$$\forall x, y, z \in A,\ x \bullet (y + z) = x \bullet y + x \bullet z \quad et \quad (y + z) \bullet x = y \bullet x + z \bullet x$$

*4.* " $\bullet$ " *admet un élément neutre noté* $1_A$

$$\exists 1_A, \forall x \in A;\ x \bullet 1_A = 1_A \bullet x = x$$

*Si de plus* $\bullet$ *est commutative, on dit que* $(A, +, \bullet)$ *est un anneau commutatif.*

**Remarque 2.3.1** *1).* $(A, +)$ *étant un groupe, alors tous les éléments de* $A$ *sont symétrisables et on convient de noter* $-x$ *le symétrique d'un élément* $x \in A$*.*
*2). Dans un tel anneau, on dit qu'un élément est inversible s'il l'est par rapport à la deuxième loi* $\bullet$*. L'inverse d'un élément* $x \in A$ *est noté* $x^{-1}$*.*

**Exemple 2.3.1** $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$ , $(\mathbb{R}, +, \times)$ *et* $(\mathbb{C}, +, \times)$ *sont des anneaux commutatifs.*

**Régles de Calcul dans un Anneau**

Soit $(A, +, \bullet)$ un anneau, alors on a les règles de calculs suivantes :
Pour tous $x, y$ et $z \in A$,
1. $0_A \bullet x = x \bullet 0_A = 0_A$
2. $x \bullet (-y) = (-x) \bullet y = -(x \bullet y)$
3. $x \bullet (y - z) = (x \bullet y) - (x \bullet z)$
4. $(y - z) \bullet x = (y \bullet x) - (z \bullet x)$

### 2.3.2 Sous anneaux

**Définition 2.3.2** *Soient $(A,+,\bullet)$ un anneau et $H$ sous ensemble de $A$ ($H \subset A$), on dit que $(H,+,\bullet)$ est un sous anneau de $(A,+,\bullet)$ si et seulement si :*

*1). $(A,+)$ est un sous groupe de $(A,+)$.*

*2). $\bullet$ est stable dans $H$ ; $\forall x,y \in H,\ x \bullet y \in H$ .*

*3). $1_A \in H$.*

**Exemple 2.3.2** *$(\mathbb{Z},+,\times)$ est un sous anneau de $(\mathbb{R},+,\times)$.*

## 2.4 Corps

**Définition 2.4.1** *On dit $(K,+,\bullet)$ est un corps si et seulement si :*

*1). $(K,+,\bullet)$ est un anneau.*

*2). Tout élément non nul de $K$ est inversible ;*

$$\forall x \in K-\{0\}\,, \exists x \in K-\{0\}\,;\ x \bullet x^{-1} = x^{-1} \bullet x = 1_A$$

*Si de plus $\bullet$ est commutative, on dit que $K$ est un corps commutatif.*

**Remarque 2.4.1** *Tout corps est un anneau.*

**Exemple 2.4.1** *1). $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des corps commutatifs.*

*2). $(\mathbb{Z},+,\times)$ n'est pas un corps car : il existe des éléments non nuls de $\mathbb{Z}$ qui ne sont pas inversibles comme par exemple 3.*

*3). $(\Bbbk[X],+,\times)$ est un anneau commutatif mais il n'est pas un corps.*

**Exercise 1** *Soient $\oplus$ et $\otimes$ deux lois de composition internes dans $\mathbb{R}^2$ définies par :*

$$\forall (x_1,y_1),(x_2,y_2) \in \mathbb{R}^2;\ (x_1,y_1) \oplus (x_2,y_2) = (x_1+x_2, y_1+y_2),$$

$$(x_1,y_1) \otimes (x_2,y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$$

*Montrer que $(\mathbb{R}^2,\oplus,\otimes)$ est un corps commutatif.*

***Solution :***

*1.* $(\mathbb{R}^2, \oplus)$ *est un groupe abélien*

*a).* $\oplus$ *est commutative*

$$\forall (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2;\ (x_1, y_1) \oplus (x_2, y_2) = (x_2 + x_1, y_2 + y_1) = (x_2, y_2) \oplus (x_1, y_1)$$

*b).* $\oplus$ *est associaive,* $\forall (x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R}^2$;

$$\begin{aligned}
(x_1, y_1) \oplus [(x_2, y_2) \oplus (x_3, y_3)] &= (x_1, y_1) \oplus [(x_2 + x_3, y_2 + y_3)] \\
&= (x_1 + (x_2 + x_{3)}, y_1 + (y_2 + y_3)) \\
&= ((x_1 + x_2) + x_{3)}, (y_1 + y_2) + y_3) \\
&= (x_1 + x_2, y_1 + y_2) \oplus (x_3, y_3) \\
&= [(x_1, y_1) \oplus (x_2, y_2)] \oplus (x_3, y_3)
\end{aligned}$$

*c). Elément neutre*

$$\exists e = (0, 0) \in \mathbb{R}^2, \forall (x_1, y_1) \in \mathbb{R}^2;\ (x_1, y_1) \oplus (0, 0) = (x_1 + 0, y_1 + 0) = (x_1, y_1)$$

*d). Elément symétrique*

$$\forall (x_1, y_1) \in \mathbb{R}^2, \exists e = -(x_1, y_1) = (-x_1, -y_1) \in \mathbb{R}^2;\ (x_1, y_1) \oplus (-x_1, -y_1) = (x_1 + (-x_1), y_1 + (-y_1)) = (0, 0)$$

*2).* $\otimes$ *est associative ;* $\forall (x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R}^2$;

$$\begin{aligned}
(x_1, y_1) \otimes [(x_2, y_2) \otimes (x_3, y_3)] &= (x_1, y_1) \otimes (x_2 x_3 - y_2 y_3, x_2 y_3 + x_3 y_2) \\
&= (x_1(x_2 x_3 - y_2 y_3) - y_1(x_2 y_3 + x_3 y_2), x_1(x_2 y_3 + x_3 y_2) + y_1(x_2 x_3 - y_2 y_3)) \\
[(x_1, y_1) \oplus (x_2, y_2)] \otimes (x_3, y_3) &= (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1) \otimes (x_3, y_3) \\
&= ((x_1 x_2 - y_1 y_2)\, x_3 - (x_1 y_2 + x_2 y_1) y_3, (x_1 x_2 - y_1 y_2) y_3 + (x_1 y_2 + x_2 y_1) x_3) \\
&= (x_1, y_1) \otimes [(x_2, y_2) \otimes (x_3, y_3)]
\end{aligned}$$

*De plus* $\otimes$ *est commutative ;* $\forall (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$;

$$(x_1, y_1) \otimes (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1) = (x_2 x_1 - y_2 y_1, y_1 x_2 + y_2 x_1) = (x_2, y_2) \otimes (x_1, y_1)$$

*3). $\otimes$ distributive à droite ou à gauche ($\otimes$ commutative) par rapport à $\oplus$ ;* $\forall(x_1,y_1),(x_2,y_2),(x_3,y_3) \in \mathbb{R}^2$;

$$\begin{aligned}
(x_1,y_1)\otimes[(x_2,y_2)\oplus(x_3,y_3)] &= (x_1,y_1)\otimes(x_2+x_3,y_2+y_3)\\
&= (x_1(x_2+x_3)-y_1(y_2+y_3),x_1(y_2+y_3)+y_1(x_2+x_3))\\
[\,(x_1,y_1)\otimes(x_2,y_2)]\oplus[\,x_1,y_1)\otimes(x_3,y_3)] &= (x_1x_2-y_1y_2,x_1y_2+x_2y_1)\oplus(x_1x_3-y_1y_3,x_1y_3+x_3y_1)\\
&= ((x_1x_2-y_1y_2)+(x_1x_3-y_1y_3)\,,(x_1y_2+x_2y_1)+(x_1y_3+x_3y_1\\
&= (x_1,y_1)\otimes[(x_2,y_2)\oplus(x_3,y_3)]
\end{aligned}$$

*4) Elément neutre par rapport à $\otimes$*

$$\exists e'=(1,0)\in\mathbb{R}^2,\forall(x_1,y_1)\in\mathbb{R}^2;\ (x_1,y_1)\otimes(1,0)=(x_1.1-y_1.0,x_1.0+y_1.1)=(x_1,y_1)$$

*5). Elément symétrique par rapport à $\otimes$*

$$\forall(x_1,y_1)\in\mathbb{R}^2-\{(0,0)\}\,,\exists(x_1^{-1},y_1^{-1})\in\mathbb{R}^2-\{(0,0)\}\,;\ (x_1,y_1)\otimes(x_1^{-1},y_1^{-1})=(1,0)$$

$$\begin{aligned}
(x_1,y_1)\otimes(x_1^{-1},y_1^{-1}) &= (1,0)\Longleftrightarrow(x_1x_1^{-1}-y_1y_1^{-1},x_1y_1^{-1}+x_1^{-1}y_1)=(0,0)\\
&\Longrightarrow \begin{cases} x_1x_1^{-1}-y_1y_1^{-1}=1\\ x_1y_1^{-1}+x_1^{-1}y_1=0\end{cases}\\
&\Longrightarrow \begin{cases} x_1^{-1}=\frac{x_1}{x_1^2+y_1^2}\in\mathbb{R}-\{0\}\\ y_1^{-1}=\frac{-y_1}{x_1^2+y_1^2}\in\mathbb{R}-\{0\}\end{cases}
\end{aligned}$$

*Donc, $(\mathbb{R}^2,\oplus,\otimes)$ est un corps commutatif.*

## 2.5 Série d'exercices

**Exercice 1 :**

On munit $]-1,1[$ de la loi $*$ définie par :

$$\forall x, y \in ]-1,1[\,;\ x * y = \frac{x+y}{1+xy}$$

Montrer que $(]-1,1[\,, *)$ est un groupe commutatif.

**Exercice 2 :**

Soit $(G, *)$ un groupe abélien (on note $e$ le neutre et $a^{'}$ le symétrique de $a$).

Soit $\alpha$ un élément de $G$, différent de $e$.

On définit une loi $\top$ en posant :

$$\forall a, b \in G,\ a \top b = a * b * \alpha.$$

Montrer que $(G, \top)$ est un groupe abélien.

**Exercice 3 :**

On appelle centre d'un groupe $(G, *)$ non commutatif, la partie $C$ de $G$ définie par

$$C = \{x \in G :\ \forall y \in G, x * y = y * x\}$$

1) Montrer que $C$ est un sous-groupe de $(G, *)$.

2) Que devient $C$ si $(G, *)$ est commutatif ?

**Exercice 4 :**

Soient $v \in \mathbb{C}$ et $H = \{a + vb :\quad a, b \in \mathbb{Z}\}$.

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

**Exercice 5 :**

On définit sur $\mathbb{Z}^2$ deux lois de compositions internes notées $+$ et $*$ par:

$$(a,b) + (c,d) = (a+c, b+d) \qquad \text{et} \qquad (a,b) * (c,d) = (ac, ad+bc)$$

1) Montrer que $(\mathbb{Z}^2, +, *)$ est un anneau commutatif.

1) Montrer que $A = \{(a, 0);\ \ a \in \mathbb{Z}\}$ est un sous-anneau de $(\mathbb{Z}^2, +, *)$.

**Exercice 6 :**

On considère sur $\mathbb{R}$ les deux lois de compositions internes suivantes :

$$x \oplus y = x + y - 1 \qquad \text{et} \qquad x \otimes y = x + y - xy.$$

Avec la loi $\oplus$ est associative et commutative.

$(\mathbb{R}, \oplus, \otimes)$ est-il un anneau commutatif ?

**Exercice 7 :**

Pour $a, b \in \mathbb{R}$, on pose

$$a \top b = a + b - 1 \qquad \text{et} \qquad a * b = ab - a - b + 2$$

-Montrer que $(\mathbb{R}, \top, *)$ est un corps.

Chapitre 3

# Anneau des polynômes

## 3.1 Définitions

Dans tout ce chapitre $\mathbb{k}$ désignera l'un des corps $\mathbb{R}$ ou $\mathbb{C}$.

**Définition 3.1.1** *Un polynôme à coefficients dans* $\mathbb{k}$ *est une expression de la forme*

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_2 X^2 + a_1 X + a_0,$$

*avec* $n \in \mathbb{N}$ *et* $a_0, a_1, ..., a_n \in \mathbb{k}$.

*L'ensemble des polynômes est noté* $\mathbb{k}[X]$.

– *Les* $a_i$ *sont appelés les coefficients du polynôme.*

– *Si tous les coefficients* $a_i$ *sont nuls,* $P$ *est appelé le polynôme nul, il est noté* $0$.

– *On appelle le degré de* $P$ *le plus grand entier* $i$ *tel que* $a_i \neq 0$, *on le note* $\deg P$.

*Pour le degré du polynôme nul on pose par convention* $\deg(0) = -\infty$.

– *Un polynôme de la forme* $P = a_0$ *avec* $a_0 \in \mathbb{k}$ *est appelé un polynôme constant. Si* $a_0 \neq 0$, *son degré est* $0$.

**Exemple 3.1.1** *1)* $X^4 + 2X^2 - 1$ *est un polynôme de degré* $4$.

*2)* $X^n + X$ *est un polynôme de degré* $n$.

*3)* $-2$ *est un polynôme constant, de degré* $0$.

**Définition 3.1.2** – *Les polynômes comportant un seul terme non nul (du type* $a_k X^k$*) sont appelés monômes.*

– *Soit* $P = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$, *un polynôme avec* $a_n \neq 0$.

*On appelle terme dominant le monôme* $a_nX^n$.

*Le coefficient* $a_n$ *est appelé le coefficient dominant de* $P$.

– *Si le coefficient dominant est* 1, *on dit que* $P$ *est un polynôme unitaire.*

**Exemple 3.1.2**

$$P(X) = (X-1)(X^n + X^{n-1} + ... + X + 1).$$

*On développe cette expression :*

$$P(X) = (X^{n+1} + X^n + ... + X^2 + X) - (X^n + X^{n-1} + ... + X + 1) = X^{n+1} - 1.$$

$P(X)$ *est donc un polynôme de degré* $n+1$, *il est unitaire et est somme de deux monômes :* $X^{n+1}$ *et* $-1$.

## 3.2 Opérations sur les polynômes :

– **Égalité :**

Soient $P = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ et $Q = b_nX^n + b_{n-1}X^{n-1} + ... + b_1X + b_0$ deux polynômes à coefficients dans $\mathbb{k}$.

$P = Q$ ssi $a_i = b_i$ pour tout $i$, et on dit que $P$ et $Q$ sont égaux.

– **Addition :**

Soient $P = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ et $Q = b_nX^n + b_{n-1}X^{n-1} + ... + b_1X + b_0$. On définit : $P + Q = (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1} + (a_1 + b_1)X + (a_0 + b_0)$.

– **Multiplication :**

Soient $P = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ et $Q = b_mX^m + b_{m-1}X^{m-1} + ... + b_1X + b_0$.

On définit : $P \times Q = c_rX^r + c_{r-1}X^{r-1} + ... + c_1X + c_0$,

avec $r = n + m$, $c_k = \sum_{i+j=k} a_ib_j$ pour $k \in \{0, ..., r\}$.

– **Multiplication par un scalaire :**

Si $\lambda \in \mathbb{k}$ alors $\lambda P$ est le polynôme dont le $i$-ème coefficient est $\lambda a_i$.

**Exemple 3.2.1** – *Soient* $P = aX^3 + bX^2 + cX + d$ *et* $Q = \alpha X^2 + \beta X + \gamma$.

*Alors* $P+Q = aX^3 + (b+\alpha)X^2 + (c+\beta)X + (d+\gamma)$, $P \times Q = (a\alpha)X^5 + (a\beta + b\alpha)X^4 + (a\gamma + b\beta + c\alpha)X^3 + (b\gamma + c\beta + d\alpha)X^2 + (c\gamma + d\beta)X + d\gamma$ *. Enfin* $P = Q$ *si et seulement si* $a = 0$, $b = \alpha$, $c = \beta$ *et* $d = \gamma$.

– *La multiplication par un scalaire* $\lambda.P$ *équivaut à multiplier le polynôme constant* $\lambda$ *par le polynôme* $P$*. L'addition et la multiplication se comportent sans problème.*

**Proposition 3.2.1** *Pour* $P, Q, R \in \Bbbk[X]$ *alors*

- $0 + P = P$, $P + Q = Q + P$, $(P + Q) + R = P + (Q + R)$.
- $1.P = P$, $P \times Q = Q \times P$, $(P \times Q) \times R = P \times (Q \times R)$.
- $P \times (Q + R) = P \times Q + P \times R$.

*Donc,* $(\Bbbk[X], +, \times)$ *est un anneau commutatif.*

**Proposition 3.2.2** *Soient* $P$ *et* $Q$ *deux polynômes à coefficients dans* $\Bbbk$.

- $\deg(P \times Q) = \deg P + \deg Q$.
- $\deg(P + Q) \leq max(\deg P, \deg Q)$.

*On note* $\mathbb{R}_n[X] = \{P \in \mathbb{R}[X]; \quad \deg P \leq n\}$ *. Si* $P, Q \in \mathbb{R}_n[X]$ *alors* $P + Q \in \mathbb{R}_n[X]$.

## 3.3 Arithmétique des polynômes :

### 3.3.1 Division euclidienne (ou suivant les puissances décroissantes)

**Définition 3.3.1** *Soient* $A, B \in \Bbbk[X]$*, on dit que* $B$ *divise* $A$ *s'il existe* $Q \in \Bbbk[X]$ *tel que* $A = BQ$*. On note alors* $B \mid A$.

*On dit aussi que* $A$ *est multiple de* $B$ *ou que* $A$ *est divisible par* $B$.

**Proposition 3.3.1** *Soient* $A, B, C \in \Bbbk[X]$

*1. Si* $A \mid B$ *et* $B \mid A$*, alors il existe* $\lambda \in \Bbbk^*$ *tel que* $A = \lambda B$.

*2. Si* $A \mid B$ *et* $B \mid C$ *alors* $A \mid C$.

*3. Si* $C \mid A$ *et* $C \mid B$ *alors* $C \mid \mathrm{pgcd}(A, B)$.

**Théorème 3.3.1** ***(Division euclidienne des polynômes)***.

*Soient* $A, B \in \Bbbk[X]$*, avec* $B \neq 0$*, alors il existe un unique polynôme* $Q$ *et il existe un unique polynôme* $R$ *tels que :*

$A = BQ + R$ *et* $\deg R < \deg B$.

*$Q$ est appelé le quotient et $R$ le reste et cette écriture est la division euclidienne de $A$ par $B$. Notez que la condition* $\deg R < \deg B$ *signifie $R = 0$ ou bien* $0 \leq \deg R < \deg B$.

*Enfin $R = 0$ si et seulement si $B \mid A$.*

**Exemple 3.3.1** *On pose une division de polynômes comme on pose une division euclidienne de deux entiers. Par exemple si $A = 2X^4 - X^3 - 2X^2 + 3X - 1$ et $B = X^2 - X + 1$.*
*Alors on trouve $Q = 2X^2 + X - 3$ et $R = -X + 2$. On n'oublie pas de vérifier qu'effectivement $A = BQ + R$.*

**Exemple 3.3.2** *Pour $X^4 - 3X^3 + X + 1$ divisé par $X^2 + 2$ on trouve un quotient égal à $X^2 - 3X - 2$ et un reste égale à $7X + 5$.*

### 3.3.2 Division suivant les puissances croissantes

**Théorème 3.3.2** *Soient $A, B$ deux polynômes de degrés respectivement $n$ et $p$ sur $\mathbb{k}$ et soit $h \in \mathbb{N}^*$. Il existe un couple unique de polynômes $(Q, R) \in \mathbb{k}[X]^2$, tel que :*
$A(X) = B(X)Q(X) + X^{h+1}R(X)$ *avec* $\deg Q \leq h$, *si* $Q \neq 0$.

**Exemple 3.3.3** *La division suivant les puissances croissantes de $A(X) = 2 - 3X + 4X^2 - 5X^3$ par $B(X) = 1 - X - X^2$ pour $h = 3$ s'écrit* $A(X) = B(X)\underbrace{(2 - X + 5X^2 - X^3)}_{Q(X) \text{ à l'ordre } 3} + X^4 \underbrace{(4 - X)}_{Reste}$

### 3.3.3 PGCD, Algorithme d'Euclide

**Proposition 3.3.2** *Soient $A, B \in \mathbb{k}[X]$, avec $A \neq 0$ ou $B \neq 0$. Il existe un unique polynôme unitaire de plus grand degré qui divise à la fois $A$ et $B$.*
*Cet unique polynôme est appelé le* pgcd *(plus grand commun diviseur) de $A$ et $B$ que l'on note* $\operatorname{pgcd}(A, B)$.
*Soient $A$ et $B$ des polynômes, $B \neq 0$.*

*On calcule les divisions euclidiennes successives,*

$$\begin{aligned} A &= BQ_1 + R_1 \quad et \quad \deg R_1 < \deg B \\ B &= R_1Q_2 + R_2 \ et \quad \deg R_2 < \deg R_1 \\ R_1 &= R_2Q_3 + R_3 \ et \quad \deg R_3 < \deg R_2 \\ &\vdots \end{aligned}$$

$$\begin{aligned} R_{k-2} &= R_{k-1}Q_k + R_k \ et \quad \deg R_k < \deg R_{k-1} \\ R_{k-1} &= R_kQ_{k+1} \end{aligned}$$

*Le degré du reste diminue à chaque division.*
*On arrête l'algorithme lorsque le reste est nul. Le* pgcd *est le dernier reste non nul* $R_k$ *.*

**Exemple 3.3.4** *Calculons le* pgcd *de* $A = X^4 - 1$ *et* $B = X^3 - 1$*. On applique l'algorithme d'Euclide :*

$$X^4 - 1 = (X^3 - 1) \times X + X - 1$$

$$X^3 - 1 = (X - 1) \times (X^2 + X + 1) + 0$$

*Le* pgcd *est le dernier reste non nul, donc* $\text{pgcd}(X^4 - 1, X^3 - 1) = X - 1$*.*

**Exemple 3.3.5** *Calculons le* pgcd *de* $A = X^5 + X^4 + 2X^3 + X^2 + X + 2$ *et* $B = X^4 + 2X^3 + X^2 - 4$*.*

$$X^5 + X^4 + 2X^3 + X^2 + X + 2 = (X^4 + 2X^3 + X^2 - 4) \times (X - 1) + 3X^3 + 2X^2 + 5X - 2$$

$$X^4 + 2X^3 + X^2 - 4 = (3X^3 + 2X^2 + 5X - 2) \times \frac{1}{9}(3X + 4) - \frac{14}{9}(X^2 + X + 2)$$

$$3X^3 + 2X^2 + 5X - 2 = (X^2 + X + 2) \times (3X - 1) + 0$$

*Ainsi* $\text{pgcd}(A, B) = X^2 + X + 2$*.*

**Définition 3.3.2** *Soient* $A, B \in \mathbb{k}[X]$*. On dit que* $A$ *et* $B$ *sont premiers entre eux si* $\text{pgcd}(A, B) = 1$*.*

### 3.3.4 Théorème de Bézout et théorème de Gauss

**Théorème 3.3.3** ***(Théorème de Bézout)***
*Soient $A, B \in \Bbbk[X]$ des polynômes avec $A \neq 0$ ou $B \neq 0$. On note $D = \mathrm{pgcd}(A, B)$. Il existe deux polynômes $U, V \in \Bbbk[X]$ tels que : $AU + BV = D$.*

**Exemple 3.3.6** *Nous avons calculé* $\mathrm{pgcd}(X^4 - 1, X^3 - 1) = X - 1$.
*Nous remontons l'algorithme d'Euclide, ici il n'y avait qu'une ligne :*

$$X^4 - 1 = (X^3 - 1) \times \ X + \ X - 1,$$

*pour en déduire $X-1 = (X^4-1)\times 1+(X^3-1)\times(-X)$. Donc $U = 1$ et $V = -X$ conviennent.*

**Exemple 3.3.7** *Pour $A = X^5 + X^4 + 2X^3 + X^2 + \ X + 2$ et $B = X^4 + 2X^3 + \ X^2 - 4$ nous avons trouvé $D = \mathrm{pgcd}(A, B) = \ X^2 + X + 2$. En partant de l'avant dernière ligne de l'algorithme d'Euclide on a :*

$$B = (3X^3 + 2X^2 + 5X - 2) \times \frac{1}{9}(3X + 4) - \frac{14}{9}D,$$

*donc*

$$-\frac{14}{9}D = B - (3X^3 + 2X^2 + 5X - 2) \times \frac{1}{9}(3X + 4).$$

*La ligne au-dessus dans l'algorithme d'Euclide était :*

$$A = B \times (X - 1) + 3X^3 + 2X^2 + 5X - 2.$$

*On substitue le reste pour obtenir :*

$$-\frac{14}{9}D = B - (A - B \times (X - 1)) \times \frac{1}{9}(3X + 4).$$

*On en déduit*

$$-\frac{14}{9}D = -A \times \frac{1}{9}(3X + 4) + B(1 + (X - 1) \times \frac{1}{9}(3X + 4))$$

*En posant $U = \frac{1}{14}(3X+4)$ et $V = -\frac{1}{14}(9+(X-1)(3X+4)) = -\frac{1}{14}(3X^2+X+5)$, on trouve : $AU + BV = D$.*
*Le corollaire suivant s'appelle aussi le théorème de Bézout.*

**Corollaire 3.3.1** *Soient $A$ et $B$ deux polynômes. $A$ et $B$ sont premiers entre eux si et seulement s'il existe deux polynômes $U$ et $V$ tels que : $AU + BV = 1$.*
*Comme conséquence, on obtient le* ***théorème de Gauss*** *qui affirme que*
*Soient $A, B \in \Bbbk[X]$. Si $A \mid BC$ et $\text{pgcd}(A, B) = 1$ alors $A \mid C$.*

## 3.4 Racines d'un polynôme

**Définition 3.4.1** *Soit $P = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0 \in \Bbbk[X]$. Pour un élément $x \in \Bbbk$, on note $P(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$. On associe ainsi au polynôme $P$ une fonction polynôme (que l'on note encore $P$)*

$$P : K \to K, x \to P(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0.$$

**Définition 3.4.2** *Soit $P \in \Bbbk[X]$ et $\alpha \in \Bbbk$. On dit que $\alpha$ est une racine (ou un zéro) de $P$ si $P(\alpha) = 0$.*

$$P(\alpha) = 0 \Leftrightarrow X - \alpha \quad \textit{divise} \quad P$$

**Preuve.**
Lorsque l'on écrit la division euclidienne de $P$ par $X - \alpha$ on obtient $P = Q.(X - \alpha) + R$ où $R$ est une constante car $\deg R < \deg(X - \alpha) = 1$.
Donc $P(\alpha) = 0 \Leftrightarrow R(\alpha) \Leftrightarrow R = 0 \Leftrightarrow X - \alpha \mid P$. □

**Définition 3.4.3** *Soit $k \in \mathbb{N}^*$. On dit que $\alpha$ est une racine de multiplicité $k$ de $P$ si $(X-\alpha)^k$ divise $P$ alors que $(X - \alpha)^{k+1}$ ne divise pas $P$. Lorsque $k = 1$ on parle d'une racine simple, lorsque $k = 2$ d'une racine double, etc. On dit aussi que $\alpha$ est une racine d'ordre $k$.*

**Proposition 3.4.1** *Il y a équivalence entre :*
*(i) $\alpha$ est une racine de multiplicité $k$ de $P$.*
*(ii) Il existe $Q \in \Bbbk[X]$ tel que $P = (X - \alpha)^kQ$, avec $Q(\alpha) \neq 0$.*
*(iii) $P(\alpha) = P'(\alpha) = ... = P^{(k-1)}(\alpha) = 0$ et $P^{(k)}(\alpha) \neq 0$.*

### 3.4.1 Théorème de d'Alembert-Gauss

**Théorème 3.4.1** *(Théorème de d'Alembert-Gauss).*
*Tout polynôme à coefficients complexes de degré $n \geq 1$ a au moins une racine dans $\mathbb{C}$. Il admet exactement $n$ racines si on compte chaque racine avec multiplicité.*

**Exemple 3.4.1** *Soit $P(X) = aX^2 + bX + c$ un polynôme de degré 2 à coefficients réels : $a, b, c \in \mathbb{R}$ et $a \neq 0$.*
*– Si $\triangle = b^2 - 4ac > 0$ alors $P$ admet 2 racines réelles distinctes $\frac{-b-\sqrt{\triangle}}{2a}$ et $\frac{-b+\sqrt{\triangle}}{2a}$.*
*– Si $\triangle < 0$ alors $P$ admet 2 racines complexes distinctes $\frac{-b-\mathrm{i}\sqrt{\triangle}}{2a}$ et $\frac{-b+\mathrm{i}\sqrt{\triangle}}{2a}$.*
*– Si $\triangle = 0$ alors $P$ admet une racine réelle double $\frac{-b}{2a}$.*
*En tenant compte des multiplicités on a donc toujours exactement 2 racines.*
*Pour les autres corps que les nombres complexes nous avons le résultat plus faible suivant :*

**Théorème 3.4.2** *Soit $P \in \mathbb{k}[X]$ de degré $n \geq 1$. Alors $P$ admet au plus $n$ racines dans $\mathbb{k}$.*

**Exemple 3.4.2** *$P(X) = 3X^3 - 2X^2 + 6X - 4$. Considéré comme un polynôme à coefficients dans $\mathbb{Q}$ ou $\mathbb{R}$, $P$ n'a qu'une seule racine (qui est simple) $\alpha = \frac{2}{3}$ et il se décompose en $P(X) = 3(X - \frac{2}{3})(X^2 + 2)$. Si on considère maintenant $P$ comme un polynôme à coefficients dans $\mathbb{C}$ alors $P(X) = 3(X - \frac{2}{3})(X - \mathrm{i}\sqrt{2})(X + \mathrm{i}\sqrt{2})$ et admet 3 racines simples.*

## 3.5 Polynômes irréductibles

**Définition 3.5.1** *Soit $P \in \mathbb{k}[X]$ un polynôme de degré $\geq 1$, on dit que $P$ est irréductible si pour tout $Q \in \mathbb{k}[X]$ divisant $P$, alors, soit $Q \in \mathbb{k}^*$, il existe $\lambda \in \mathbb{k}^*$ tel que $Q = \lambda P$.*

**Remarque 3.5.1** *– Un polynôme irréductible $P$ est donc un polynôme non constant dont les seuls diviseurs de $P$ sont les constantes ou $P$ lui-même (à une constante multiplicative près).*
*– La notion de polynôme irréductible pour l'arithmétique de $\mathbb{k}[X]$ correspond à la notion de nombre premier pour l'arithmétique de $\mathbb{Z}$.*
*– Dans le cas contraire, on dit que $P$ est réductible ; il existe alors des polynômes $A, B$ de $\mathbb{k}[X]$ tels que $P = AB$, avec $\deg A \geq 1$ et $\deg B \geq 1$.*

**Exemple 3.5.1** *1) Tous les polynômes de degré* 1 *sont irréductibles. Par conséquent il y a une infinité de polynômes irréductibles.*
*2)* $X^2-1=(X-1)(X+1)\in\mathbb{R}[X]$ *est réductible.*
*3)* $X^2+1=(X-\mathrm{i})(X+\mathrm{i})$ *est réductible dans* $\mathbb{C}[X]$ *mais est irréductible dans* $\mathbb{R}[X]$.
*4)* $X^2-2=(X-\sqrt{2})(X+\sqrt{2})$ *est réductible dans* $\mathbb{R}[X]$ *mais est irréductible dans* $\mathbb{Q}[X]$.

**Proposition 3.5.1** *(Lemme d'Euclide)*
*Soit* $P\in\Bbbk[X]$ *un polynôme irréductible et soient* $A,B\in\Bbbk[X]$. *Si* $P\mid AB$ *alors* $P\mid A$ *ou* $P\mid B$.

**Preuve.** Si $P$ ne divise pas $A$ alors $\mathrm{pgcd}(P,A)=1$ car $P$ est irréductible. Donc, par le lemme de Gauss, $P$ divise $B$. □

## 3.6 Factorisation dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$

**Théorème 3.6.1** *Tout polynôme non constant* $A\in\Bbbk[X]$ *s'écrit comme un produit de polynômes irréductibles unitaires :*

$$A=\lambda P_1^{k_1}P_2^{k_2}...P_r^{k_r}$$

*où* $\lambda\in\Bbbk^*$, $r\in\mathbb{N}^*$, $k_i\in\mathbb{N}^*$ *et les* $P_i$ *sont des polynômes irréductibles distincts. De plus cette décomposition est unique à l'ordre près des facteurs.*

**Théorème 3.6.2** *Les polynômes irréductibles de* $\mathbb{C}[X]$ *sont les polynômes de degré* 1.
*Donc pour* $P\in\mathbb{C}[X]$ *de degré* $n\geq 1$ *la factorisation s'écrit*

$$P=\lambda(X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}...(X-\alpha_r)^{k_r},$$

*où* $\alpha_1,\alpha_2,...\alpha_r$ *sont les racines distinctes de* $P$ *et* $k_1,k_2,...k_r$ *sont leurs multiplicités.*

**Théorème 3.6.3** *Les polynômes irréductibles de* $\mathbb{R}[X]$ *sont les polynômes de degré* 1 *ainsi que les polynômes de degré* 2 *ayant un discriminant* $\triangle<0$.
*Soit* $P\in\mathbb{C}[X]$ *de degré* $n\geq 1$. *Alors la factorisation s'écrit*

$$P=\lambda(X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}...(X-\alpha_r)^{k_r}Q_1^{l_1}...Q_s^{l_s},$$

*où les* $\alpha_i$ *sont exactement les racines réelles distinctes de multiplicité* $k_i$ *et les* $Q_i$ *sont des polynômes irréductibles de degré* 2 *:* $Q_i=X^2+\beta_iX+\gamma_i$ *avec* $\triangle=\beta_i^2-4\gamma_i<0$.

**Exemple 3.6.1** *$P(X) = 2X^4(X-1)^3(X^2+1)^2(X^2+X+1)$ est déjà décomposé en facteurs irréductibles dans $\mathbb{R}[X]$ alors que sa décomposition dans $\mathbb{C}[X]$ est*
$P(X) = 2X^4(X-1)^3(X-\mathrm{i})^2(X+\mathrm{i})^2(X-j)(X-j^2)$ *où* $j = e^{\frac{2\,\mathrm{i}\,\pi}{3}} = \frac{-1+\mathrm{i}\sqrt{3}}{2}$.

**Exemple 3.6.2** *Soit $P(X) = X^4 + 1$.*
*– Sur $\mathbb{C}$. On peut d'abord décomposer $P(X) = (X^2+\mathrm{i})(X^2-\mathrm{i})$. Les racines de $P$ sont donc les racines carrées complexes de $\mathrm{i}$ et $-\mathrm{i}$. Ainsi $P$ se factorise dans $\mathbb{C}[X]$ :*

$$P(X) = (X - \frac{\sqrt{2}}{2}(1+\mathrm{i}))(X + \frac{\sqrt{2}}{2}(1+\mathrm{i}))(X - \frac{\sqrt{2}}{2}(1-\mathrm{i}))(X + \frac{\sqrt{2}}{2}(1-\mathrm{i})).$$

*– Sur $\mathbb{R}$. Pour un polynôme à coefficient réels, si $\alpha$ est une racine alors $\overline{\alpha}$ aussi. Dans la décomposition ci-dessus on regroupe les facteurs ayant des racines conjuguées, cela doit conduire à un polynôme réel :*

$$P(X) = \left[(X - \frac{\sqrt{2}}{2}(1+\mathrm{i}))(X - \frac{\sqrt{2}}{2}(1-\mathrm{i}))\right]\left[(X + \frac{\sqrt{2}}{2}(1+\mathrm{i}))(X + \frac{\sqrt{2}}{2}(1-\mathrm{i}))\right],$$

*qui est la factorisation dans $\mathbb{R}[X]$.*

## 3.7 Série d'exercices

**Exercice 1 :**

Effectuer les divisions euclidiennes de

$$X^4 - X^3 + X - 2 \quad \text{par} \quad X^2 - 2X + 4$$

$$3X^5 + 2X^4 - X^2 + 1 \quad \text{par} \quad X^3 + X + 2$$

$$3X^5 + 4X^2 + 1 \quad \text{par} \quad X^2 + 2X + 3$$

**Exercice 2 :**

Effectuer la division selon les puissances croissantes de :

$$X^4 + X^3 - 2X + 1 \quad \text{par} \quad X^2 + X + 1 \quad \text{à l'ordre } 2$$

$$X^6 - 2X^4 + X^3 + 1 \quad \text{par} \quad X^3 + X^2 + 1 \quad \text{à l'ordre 4}$$

**Exercice 3 :**

Pour $n \in \mathbb{N}$, montrer que le pôlynome

$$nX^{n+1} - (n+1)X^n + 1$$

est divisible par $(X-1)^2$.

**Exercice 4 :**

1. Déterminer $a_n$ et $b_n$ pour que $A_n = a_n X_{n+1} + b_n X^n + 1$ soit divisible par $B = (X-1)^2$.

2. Former alors le quotient $Q_n$ dans la division de $A_n$ par $B$.

**Exercice 5 :**

Calculer le pgcd $D$ des polynômes $A$ et $B$ d e nis ci-dessous. Trouver des polynôomes $U$ et V tels que $D = AU + BV$ .

$$A = X^5 + 3X^4 + 2X^3 - X^2 - 3X - 2 \quad \text{et} \quad B = X^4 + 2X^3 + 2X^2 + 7X + 6.$$

$$A = X^5 + 3X^4 + X^3 + X^2 + 3X + 1 \quad \text{et} \quad B = X^4 + 2X^3 + X + 2.$$

$$A = X^6 - 2X^5 + 2X^4 - 3X^3 + 3X^2 - 2X \quad \text{et} \quad B = X^4 - 2X^3 + X^2 - X + 1.$$

**Exercice 6 :**

Quels sont, parmi les polynômes suivants, ceux qui sont irréductibles sur $\mathbb{R}$ et $\mathbb{C}$ :

1. $X + 2$.
2. $X^2 - 4X + 3$.
3. $X^2 + 1$.
4. $X^3 - 1$.
5. $X^{12} - 1$.

Chapitre 4

# Fractions rationnelles

## 4.1 Définitions

**Définition 4.1.1** *On appelle fraction rationnelle (à coefficients dans* $\Bbbk$ *) le quotient* $\frac{P}{Q}$ *où* $P, Q \in \Bbbk[X]$ *sont deux polynômes et* $Q \neq 0$.
*Toute fraction rationnelle se décompose comme une somme de fractions rationnelles élémentaires que l'on appelle des «éléments simples». Mais les éléments simples sont différents sur* $\mathbb{C}$ *où sur* $\mathbb{R}$.

**Définition 4.1.2** *Soit la fraction rationnelle* $F(X) = \frac{P(X)}{Q(X)}$ *. On dira que* $\alpha$ *est un pôle de* $F$ *si* $\alpha$ *est une racine du polynôme* $Q$.

**Exemple 4.1.1** *1). Soit*

$$F(X) = \frac{2X+1}{X^3+3X+X},$$

$0$ *est un pôle de* $F$.

*2). Soit le polynome suivant*

$$G(X) = \frac{X^2+x+1}{(X+1)^3}$$

$-1$ *est un pôle de* $G(X)$.

## 4.2 Décomposition en éléments simples dans $\mathbb{C}[X]$

**Théorème 4.2.1** *Soit $\frac{P}{Q}$ une fraction rationnelle avec $P, Q \in \mathbb{C}[X]$, $\text{pgcd}(P,Q) = 1$ «On doit rendre la fraction irréductible» et $Q(X) = (X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}...(X-\alpha_r)^{k_r}$. Alors il existe une et une seule écriture :*

$$\frac{P}{Q} = E + \frac{a_{1,1}}{(X-\alpha_1)^{k_1}} + \frac{a_{1,2}}{(X-\alpha_1)^{k_1-1}} + ... + \frac{a_{1,k_1}}{(X-\alpha_1)} + \frac{a_{2,1}}{(X-\alpha_2)^{k_2}} + ... + \frac{a_{2,k_2}}{(X-\alpha_2)} + ...$$

*Le polynôme $E$ s'appelle la partie polynomiale (où partie entière).*
*Les termes $\frac{a}{(X-\alpha)^i}$ sont les éléments simples sur $\mathbb{C}$.*

**Exemple 4.2.1** *Vérifier que*

$$\frac{1}{X^2+1} = \frac{a}{X+i} + \frac{b}{X-i} \qquad avec \qquad a = \frac{1}{2}i, \quad b = -\frac{1}{2}i$$

*Vérifier que*

$$\frac{X^4 - 8X^2 + 9X - 7}{(X-2)^2(X+3)} = X + 1 + \frac{-1}{(X-2)^2} + \frac{2}{X-2} + \frac{-1}{X+3}$$

*Comment se calcule cette décomposition ? En général on commence par déterminer la partie polynomiale.*
*Tout d'abord si $\deg Q > \deg P$ alors $E(X) = 0$. Si $\deg P \geq \deg Q$ alors effectuons la division euclidienne de $P$ par $Q$ :*

$$P = Q \cdot E + R$$

*donc*

$$\frac{P}{Q} = E + \frac{R}{Q} \quad où \quad \deg R < \deg Q.$$

*La partie polynomiale est donc le quotient de cette division. Et on s'est ramené au cas d'une fraction $\frac{R}{Q}$ avec $\deg R < \deg Q$.*

**Exemple 4.2.2** *Décomposons la fraction*

$$\frac{P}{Q} = \frac{X^5 - 2X^3 + 4X^2 - 8X + 11}{X^3 - 3X + 2}.$$

– ***Première étape : partie polynomiale :***

*On calcule la division euclidienne de $P$ par $Q$ :*

$$P(X) = (X^2+1)Q(X) + 2X^2 - 5X + 9.$$

*Donc la partie polynomiale est $E(X) = X^2 + 1$ et la fraction s'écrit*

$$\frac{P(X)}{Q(X)} = X^2 + 1 + \frac{2X^2 - 5X + 9}{Q(X)}.$$

*Notons que pour la fraction $\frac{2X^2-5X+9}{Q(X)}$ le degré du numérateur est strictement plus petit que le degré du dénominateur.*

– ***Deuxième étape : factorisation du dénominateur :***

*$Q$ a pour racine évidente $+1$ (racine double) et $-2$ (racine simple) et se factorise donc ainsi* $Q(X) = (X-1)^2(X+2)$.

– ***Troisième étape : décomposition théorique en éléments simples :***

*Le théorème de décomposition en éléments simples nous dit qu'il existe une unique décomposition :*

$$\frac{P(X)}{Q(X)} = E(X) + \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}.$$

*Nous savons déjà que $E(X) = X^2 + 1$, il reste à trouver les nombres $a, b, c$.*

– ***Quatrième étape : détermination des coefficients :***

*Voici une première façon de déterminer $a, b, c$.*

*On récrit la fraction $\frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}$ au même dénominateur et on l'identifie avec $\frac{2X^2-5X+9}{Q(X)}$ :*

*On en trouve*

$$b + c = 2,\ a + b - 2c = -5 \quad et \quad 2a - 2b + c = 9.$$

*Cela conduit à l'unique solution*

$$a = 2, b = -1, c = 3.$$

*Donc*

$$\frac{P}{Q} = \frac{X^5 - 2X^3 + 4X^2 - 8X + 11}{X^3 - 3X + 2} = X^2 + 1 + \frac{2}{(X-1)^2} + \frac{-1}{X-1} + \frac{3}{X+2}.$$

***Détermination des coefficients :*** *Voici une autre méthode plus efficace.*

*Notons* $\frac{R(X)}{Q(X)} = \frac{2X^2-5X+9}{(X-1)^2(X+2)}$ *dont la décomposition théorique est :*

$$\frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}$$

*Pour déterminer* $a$ *on multiplie la fraction* $\frac{R}{Q}$ *par* $(X-1)^2$ *et on évalue en* $x = 1$.

*Tout d'abord en partant de la décomposition théorique on a :*

$$F_1(X) = (X-1)^2\frac{R(X)}{Q(X)} = a + b(X-1) + \frac{c(X-1)^2}{(X+2)} = \frac{2X^2-5X+9}{(X+2)}$$

*Donc* $F_1(1) = a$.

*D'autre part*

$$F_1(X) = (X-1)^2\frac{R(X)}{Q(X)} = (X-1)^2\frac{2X^2-5X+9}{(X-1)^2(X+2)} = \frac{2X^2-5X+9}{(X+2)}$$

*donc* $F_1(1) = 2$,*on en déduit* $a = 2$.

*On fait le même processus pour déterminer* $c$ *: on multiplie par* $(X+2)$ *et on évalue en* $-2$.

*On calcule*

$$F_2(X) = (X+2)\frac{R(X)}{Q(X)} = \frac{2X^2-5X+9}{(X+2)} = a\frac{X+2}{(X-1)^2} + b\frac{X+2}{X-1} + c$$

*de deux façons et lorsque l'onévalue* $x = 2$ *on obtient d'une part* $F_2(2) = c$ *et d'autre part* $F_2(2) = 3$. *Ainsi* $c = 3$.

*Comme les coefficients sont uniques tous les moyens sont bons pour les déterminer. Par exemple lorsque l'on évalue la décomposition théorique*

$$\frac{R(X)}{Q(X)} = \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2} \quad en \quad x = 0,$$

*on obtient :*

$$\frac{R(0)}{Q(0)} = a - b + \frac{c}{2}.$$

*Donc* $\frac{9}{2} = a - b + \frac{c}{2}$, $b = -1$.

## 4.3 Décomposition en éléments simples dans $\mathbb{R}[X]$

**Théorème 4.3.1** *Soit* $\frac{P}{Q}$ *une fraction rationnelle avec* $P, Q \in \mathbb{R}[X]$, $\text{pgcd}(P, Q) = 1$. *Alors* $\frac{P}{Q}$ *s'écrit de manière unique comme somme :*

– *d'une partie polynomiale* $E(X)$,

– *d'éléments simples du type* $\frac{a}{(X-\alpha)^i}$,

– *d'éléments simples du type* $\frac{aX+b}{(X^2+\alpha X+\beta)^i}$

*Où les* $X-\alpha$ *et* $X^2+\alpha X+\beta$ *sont les facteurs irréductibles de* $Q(X)$ *et les exposants* $i$ *sont inférieurs ou égaux à la puissance correspondante dans cette factorisation.*

**Exemple 4.3.1** *On peut vérifier que*

$$F(X)=\frac{4}{(X-2)^2(X+1)}=\frac{a}{(X-2)^2}+\frac{b}{X-2}+\frac{c}{X+1}=\frac{4/5}{(X-2)^2}+\frac{-4/9}{X-2}+\frac{4/9}{X+1}.$$

*et on peut aussi vérifier que*

$$G(X)=\frac{1}{(X^2+1)(X-1)}=\frac{a}{X-1}+\frac{bX+c}{X^2+1}=\frac{1/2}{X-1}+\frac{-1/2X-1/2}{X^2+1}$$

**Exemple 4.3.2** *Décomposition en éléments simples de*

$$\frac{P(X)}{Q(X)}=\frac{3X^4+5X^3+8X^2+3}{(X^2+X+1)^2(X-1)}.$$

*Comme* $\deg P<\deg Q$ *alors* $E(X)=0$.

*Le dénominateur est déjà factorisé sur* $\mathbb{R}$ *car* $X^2+X+1$ *est irréductible.*

*La décomposition théorique est donc :*

$$\frac{P(X)}{Q(X)}=\frac{aX+b}{(X^2+X+1)^2}+\frac{cX+d}{X^2+X+1}+\frac{e}{X-1}.$$

*Il faut ensuite mener au mieux les calculs pour déterminer les coefficients afin d'obtenir :*

$$\frac{P(X)}{Q(X)}=\frac{2X+1}{(X^2+X+1)^2}+\frac{-1}{X^2+X+1}+\frac{3}{X-1}.$$

## 4.4 Série d'exercices

**Exercice 1 :**

1) Décomposer en éléments simples dans $\mathbb{R}[X]$ les fractions suivantes :

$$E(X)=\frac{X}{X^2-4}$$

$$F(X) = \frac{2X^3 + X^2 - X + 1}{X^2 - 3X + 2}$$

$$G(X) = \frac{2X^3 + X^2 - X + 1}{X^2 - 2X + 1}$$

$$H(X) = \frac{X^4 + 2X^2 + 1}{X^2 - 1}$$

**Exercice 2 :**

Décomposer en éléments simples dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$ les fractions suivantes :

$$E(X) = \frac{2X^3 + X^2 - X + 1}{X^2 - 4}$$

$$F(X) = \frac{3X^2 + 2X + 1}{X(X^2 + X + 1)}$$

$$G(X) = \frac{2X^4 + 1}{X(X-1)^3(X^2 + X + 1)}$$

$$H(X) = \frac{X^2 + 1}{X^4 + 1}$$

**Exercice 3 :**

Décomposer en élément simples dans $\mathbb{C}[X]$

$$E = \frac{X^2 + 1}{X(X + j)^3(X - 1)^4}$$

**Exercice 4 :**

Décomposer en élément simples dans $\mathbb{R}[X]$

$$F = \frac{n!}{X(X + 1)(X + 2)...(X + n)}$$

# Bibliographie


[1] Hitta, Amara, *Cours d'algèbre et exercices corrigés*. O.P.U., 1994.

[2] Jean-Pierre Escofier, *Toutes l'algèbre de la licence. Cours et exercices corrigés*, DUNOD.

[3] Arnaud Bodin, *Cours de mathématiques- Première année*, université Lille1, France.

[4] Baba-Hamed. C, Benhabib. K, *Algèbre 1. Rappel de cours et exercices avec solutions.* O.P.U., 1985.

[5] Mohammed Hichem Mortad, *Exercices corrigés d'Algèbre*, université d'Oran1, Algérie, Dar el Bassair, 2013.

[6] Alain Soyeur, *Cours de Mathématiques MPSI-2 Lycée Fermat*, université Lille1, France.