الجمهوريـــــــــــــــة الجزائريـــــــــة الديمقراطيـــــــة الشعبيـــــة
وزارة التعليـــــــم العـــــــالي و البحـــــــث العلـــــمي
جامعة وهران للعلوم والتكنولوجيا محمد بوضياف
THE PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
UNIVERSITY OF SCIENCE AND TECHNOLOGY OF
ORAN MOHAMED BOUDIAF
Faculty of Mathematics and Computer Science
Department of Mathematics


# Handout of Algebra 01

# Courses and Exercises for Algebra 01

Author: Dr. ANBER Ahmed

Academic Year: 2025 -2026

THE PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
UNIVERSITY OF SCIENCE AND TECHNOLOGY OF
ORAN MOHAMED BOUDIAF

**Faculty of Mathematics and Computer Science**

**Department of Mathematics**


**Handout of Algebra 01**

# Courses and Exercises for Algebra 01

Academic Year : **2025 -2026**

# Table des matières

# Introduction

This handout was intended for students enrolled in the first year of the LMD system, computer science, first semester of the academic year.

The content of this handout corresponds to the official program for the subject Algebra 1 taught in the first year.

The manuscript contains five chapters :

- Concept of logic
- Sets and applications
- Binary relation on a set
- Algebraic structures
- Polynomial rings

At the end of each chapter, solved exercises and equivalent terminologies in French are given.

**Chapitre 1**

# Concept of logic

In this first chapter, we present the concept of mathematical logic.

## 1.1 Statements (Proposition)

**Definition 1.1**

A **proposition** is any declarative sentence that is either true (**T**) or false (**F**), but not both. If the proposition is true, we refer it the value 1 **(or T),** if it false, we refer it the value 0 **(or F)**.

Statements are usually denoted by letters : **P, Q, R,** ...

**Example 1.1**

1. "$\sqrt{2}$ is an irrational number" is a true proposition.

2. "Oran is the capital of Algeria" is a false proposition.

3. "$1 + 3 \geq 5$" is a false proposition.

4. "33 is a multiple of 3" is a true proposition.

**Truth tables**

We can summarize the state of a proposition $P$ by a truth table as follows :

| $P$ |
|---|
| 1 |
| 0 |

Table 1 : Truth table of a proposition $P$ .

**Negation :** Let $P$ be a proposition.

We call the negation of $P$ the proposition $\overline{P}$ or "$Not\ P$", which is false when $P$ is true and which is true when $P$ is false.

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

Table 2 : Truth table of the proposition $\overline{P}$.

**Example 1.2**

1. The negation of $P : (\sqrt{2}$ is an irrational number) is $\overline{P} : (\sqrt{2}$ is an rational number).
2. The negation of $Q : (1 + 3 \geq 5)$ is $\overline{Q} : (1 + 3 < 5)$.
3. The negation of $R$ : (The number 9 is even) is $\overline{R}$ : (The number 9 is not even).

## 1.2 Equivalence

Let $P$ and $Q$ be two propositions.

We say that $P$ and $Q$ are equivalent if they have the same truth values. We denote $(P \Leftrightarrow Q)$ which is read as ($P$ is equivalent to $Q$).

The truth table of the logical equivalence "$P \Leftrightarrow Q$" is

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

Table 3 : Truth table of the equivalente.

**Property 1.1**

Let $P$ be a proposition, then the negation of the negation of proposition $P$ is equivalent to $P$.

$$\overline{\overline{P}} \Leftrightarrow P.$$

## 1.3 Logical connectors

**The conjunction $P \wedge Q$** Read **(P and Q)**

Let $P, Q$ be two propositions, the proposition (**P and Q**) or $(P \wedge Q)$ is the conjunction of the two propositions $P, Q$.

- $(P \wedge Q)$ is true if $P$ and $Q$ are both true.

- $(P \wedge Q)$ is false in all other cases.

This is summarized in the following truth table :

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

or

| $P$ | $Q$ | $P \wedge Q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | F |

Table 4 : Truth table of the proposition $P \wedge Q$.

**Example 1.3**

**1.** Let $P_1 : (1 + 5 = 8)$ and $P_2 : (2 + 6 \geq 7)$ .

The conjunction of these propositions is :

$$P_1 \wedge P_2 : (\,(1 + 5 = 8) \text{ and } (2 + 6 \geq 7)\,),$$

$P_1 \wedge P_2$ is a false proposition, because $P_1$ is false.

**2.** Let $Q_1 :$ (The number 10 is even) and $Q_2 :$ (20 is a multiple of 4) .

The conjunction of these propositions is :

$$Q_1 \wedge Q_2 : (\text{(The number 10 is even) and } (20 \text{ is a multiple of } 4)\,),$$

$Q_1 \wedge Q_2$ is a true proposition, because $Q_1, Q_2$ are true propositions.

**Property 1.2**

Let $P$ be a proposition, then $(P \wedge \overline{P})$ is a false proposition.

**Proof.**

It suffices to note that the truth table of $P \wedge \overline{P}$

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

Table 5 : Truth table of $P \wedge \overline{P}$

**The disjunction $P \vee Q$** Read **(P or Q)**

Let $P, Q$ be two propositions, the proposition (**P or Q**) (or $(P \vee Q)$) is the disjunction of the two propositions $P, Q$.

- $(P \vee Q)$ is true if $P$ and $Q$ are both false.

- $(P \vee Q)$ is true in all other cases.

This is summarized in the following truth table :

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

Table 6 : Truth table of the disjunction.

**Example 1.4**

**1.** Let $P_1 : (1 + 5 = 8)$ , $P_2 : (2 + 6 \geq 11)$ .

The disjunction of these propositions is :

$$P_1 \vee P_2 : (\,(1 + 5 = 8) \text{ or } (2 + 6 \geq 11)\,),$$

$P_1 \vee P_2$ is a false proposition, because $P_1, P_2$ are false propositions.

**2.** Let $Q_1 :$ (The number 11 is even), $Q_2 :$ (20 is a multiple of 4) .

The disjunction of these propositions is :

$$Q_1 \vee Q_2 : (\text{(The number 11 is even) or (20 is a multiple of 4)}\,),$$

$Q_1 \vee Q_2$ is a true proposition, because $Q_2$ is true.

**Property 1.3**

Let $P$ be a proposition, then $(P \vee \overline{P})$ is a true proposition.

**Proof**

It suffices to note that the truth table of $P \vee \overline{P}$

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

Table 7 : Truth table of $P \vee \overline{P}$

**Theorem 1.1 (Morgan's Rules)** Let $P$ and $Q$ be two propositions, then :

1. $\overline{P \wedge Q} \Leftrightarrow \overline{P} \vee \overline{Q}$

2. $\overline{P \vee Q} \Leftrightarrow \overline{P} \wedge \overline{Q}$

**Proof**

We establish the proof of these rules by giving the truth values of the corresponding logical propositions.

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

We see that the propositions $\overline{P \wedge Q}$ and $\overline{P} \vee \overline{Q}$ have the same truth values, so they are equivalent. Similarly for $\overline{P \vee Q}$ and $\overline{P} \wedge \overline{Q}$.

**Theorem 1.2**

Let $P, Q$ and $R$ be three propositions, then :

1. $P \wedge Q \Leftrightarrow Q \wedge P$ and $P \vee Q \Leftrightarrow Q \vee P$

2. $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$ and $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$

3. $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$ and $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$

(We say that (or) and (and) are commutative, associative and distributive over each other).

**Proof.**

Let us prove, for example, the second equivalence of 3 using a truth table (you will prove the rest in a similar way).

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

We actually read the same truth values in the fourth and eighth columns.

**The Implication**. Let $P$ and $Q$ be two statements.

A proposition of the form $(P \Rightarrow Q)$, (read as ($P$ implies $Q$)) is called an implication. It is equivalent to the proposition $(Not\,(P)\ or\ Q)$. Its truth table is given by :

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

Table 8 : Truth table of the proposition $(P \Rightarrow Q)$

**The reciprocal and contrapositive of an implication**

Let $P$ and $Q$ be two propositions.

- The reciproc of the implication $(P \Rightarrow Q)$ is $(Q \Rightarrow P)$.

- The contrapositive of the implication $(P \Rightarrow Q)$ is $(\overline{Q} \Rightarrow \overline{P})$.

**Property 1.4**

An implication and its contrapositive are equivalent.

$$(P \Rightarrow Q) \Leftrightarrow \left(\overline{Q} \Rightarrow \overline{P}\right).$$

**Proof.**

We can use two different methods.

1. Using the truth values of the implications $(P \Rightarrow Q)$ and $(\overline{Q} \Rightarrow \overline{P})$, we obtain :

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

Table 9 : Truth table of $P \Rightarrow\ Q$ and $NonQ \Rightarrow NonP$

We see that the propositions $(P \Rightarrow Q)$ and $(\overline{Q} \Rightarrow \overline{P})$ have the same truth values, so they are equivalent.

2. Using the definition of implication, we obtain :

$$\left(\overline{Q} \Rightarrow \overline{P}\right) \Leftrightarrow \overline{\left(\overline{Q}\right)} \vee \overline{P} \Leftrightarrow Q \vee \overline{P} \Leftrightarrow \overline{P} \vee Q \Leftrightarrow (P \Rightarrow Q).$$

**The negation of implication**

The negation of the implication $(P \Rightarrow Q)$ is $(P \wedge \overline{Q})$.

$$\overline{(P \Rightarrow Q)} \Leftrightarrow \left(P \wedge \overline{Q}\right).$$

**Property 1.5**

Let $P, Q$, and $R$ be three propositions, then :

$$((P \Rightarrow Q) \wedge (Q \Rightarrow R))) \Rightarrow (P \Rightarrow R).$$

**Proof.**

Let us demonstrate using a truth table.

| $P$ | $Q$ | $R$ | $\overbrace{P \Rightarrow Q}^{P_1}$ | $\overbrace{Q \Rightarrow R}^{P_2}$ | $\overbrace{P \Rightarrow R}^{P_3}$ | $\overbrace{P_1 \wedge P_2}^{P_4}$ | $P_4 \Rightarrow P_3$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |

**Equivalente**. Let $P$ and $Q$ be two propositions, then :

The proposition ($P \Rightarrow Q$ and $Q \Rightarrow P$) is the proposition denoted by $(P \Leftrightarrow Q)$, (read as ($P$ if and only if $Q$)).

## 1.4 Quantifiers

The two symbols $\forall$ and $\exists$, called quantifiers, are defined as follows :

### 1.4.1 The universal quatifier

A proposition $P$ can depend on a parameter $x$, for example $(x^2 - 3x + 2 \geq 0)$, the proposition $P(x)$ is true or false depending on the value of $x$.

We write (for all $x$ element of $E$, the proposition $P(x)$ is true) as $(\forall x \in E,\, P(x))$.

This proposition is true when the propositions $P(x)$ are true for all elements $x$ of the set $E$.

**Example 1.5**

- «$\forall x \in \mathbb{R}, x^2 + 2x - 5 \geq 0$» is a false proposition.
- «$\forall n \in \mathbb{N}, \frac{n(n+1)}{2} \in \mathbb{N}$» is a true proposition.

### 1.4.2 The existential quantifier

We write (there exists at least one element $x$ of $E$, the proposition $P(x)$ is true) as ($\exists x \in E$, $P(x)$)

This proposition is true when we can find at least one element $x$ of $E$ for which $P(x)$ is true.

**Example 1.6**

- « $\exists x \in \mathbb{R},\ \ x^2 + 2x \geq 0$ » is a true proposition.
- « $\exists z \in \mathbb{N},\ \ z^2 + 2 \neq 0$ » is a false proposition.

**Remark 1.1**

The proposition : «There exists one and only one element $x$ of $E$ such that the proposition $P(x)$ is true» is written in abbreviation «$\exists! x \in E,\ P\,(x)$».

### 1.4.3 Negation of quantifiers

The negation of «for every element $x$ in $E$, the statement $P(x)$ is true» is «there exists an element $x$ in $E$ for which the statement $P(x)$ is false»

$$\overline{\forall x \in E,\ P\,(x)} \Leftrightarrow \exists x \in E, \overline{P\,(x)}.$$

The negation of «there exists an element $x$ in $E$ such that the statement $P(x)$ is true» is «for every element $x$ in $E$, the statement $P(x)$ is false»

$$\overline{\exists x \in E,\ P\,(x)} \Leftrightarrow \forall x \in E, \overline{P\,(x)}.$$

**Example 1.7**

- The negation of « $\forall x \in \mathbb{R},\ \ x^2 + 2x \geq 0$ » is « $\exists x \in \mathbb{R},\ \ x^2 + 2x < 0$ ».
- The negation of « $\exists z \in \mathbb{N},\ \ z^2 + 2 \neq 0$ » is « $\forall z \in \mathbb{N},\ \ z^2 + 2 = 0$».

- The negation of « $\exists x \in \mathbb{R}, \forall y \in [1, +\infty[\,, \quad x + y \geq 2$ » is « $\forall x \in \mathbb{R}, \exists y \in [1, +\infty[\,, \; x + y < 2$».

**Remark 1.2**

We can distribute $\forall$ on "AND" and $\exists$ on "OR" but we cannot distribute $\forall$ on "or" and $\exists$ on "and".

- $(\forall x \in E, P(x) \wedge Q(x)) \Leftrightarrow (\forall x \in E, P(x)) \wedge (\forall x \in E, Q(x))$.
- $(\exists x \in E, P(x) \vee Q(x)) \Leftrightarrow (\exists x \in E, P(x)) \vee (\exists x \in E, Q(x))$.
- $(\forall x \in E, P(x) \vee Q(x)) \Leftarrow (\forall x \in E, P(x)) \vee (\forall x \in E, Q(x))$.
- $(\exists x \in E, P(x) \wedge Q(x)) \Rightarrow (\exists x \in E, P(x)) \wedge (\exists x \in E, Q(x))$.

We can swap quantifiers of the same nature but we cannot swap quantifiers of different natures.

- $(\forall x \in E, \forall y \in E, P(x, y)) \Leftrightarrow (\forall y \in E, \forall x \in E, P(x, y))$.
- $(\exists x \in E, \exists y \in E, P(x, y)) \Leftrightarrow (\exists y \in E, \exists x \in E, P(x, y))$.

**Example 1.8**

The two logical sentences

$$P(x, y) : \forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x - y \geq 1$$

$$Q(x, y) : \exists x \in \mathbb{R}, \forall x \in \mathbb{R}, x - y \geq 1,$$

are different. The first one is true (because for any real number $x$, we can find a real $y = x - 2$, such that $x - y = 2 \geq 1$), while the second one is false (because for a real number $x = -1$, the proposition $-1 - y \geq 1$, is not true for all real $y$).

## 1.5 Types of reasoning

**Direct reasoning**

To show that $(P \Rightarrow Q)$ is true, we assume that $P$ is true and demonstrate that $Q$ is also true.

**Example 1.9**

Let $n \in \mathbb{N}$, prove that «if $n$ is odd, then $n^2$ is odd».

Suppose that $n$ is odd, then there exists a natural integer $k$ such that $n = 2k + 1$, let us then calculate $n^2$.

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1,$$

so, there exists a natural integer $p = 2k^2 + 2k$ such that $n^2 = 2p + 1$,which shows that $n^2$ is odd.

**Counter-examples**

To show that a proposition of the form $(\forall x \in E,\ P(x))$ is false, we show that its negation $(\exists x \in E,\ \overline{P(x)}\ )$ is true. This is providing a counterexample.

**Example 1.10**

Prove that the proposition «$\forall x \in \mathbb{C},\ \ x^2 + 1 \neq 0$» is false.

A counterexample for $x = i$ or $x = -i$, we find $x^2 + 1 = 0$, which shows that the proposition is false.

**Proof by Cases**

In ordrer to prove that a certain proposition $P(x)$ is true for all $x$ in a set $E$, we show that $P(x)$ is true for $x \in A \subset E$ ; then for $x \notin A$.

**Example 1.11**

Prove that «For all $x \in \mathbb{R}, |x - 1| \leq x^2 - x + 1$».

Let $x \in \mathbb{R}$,

**First case :** $x \geq 1$

$$\begin{aligned} x^2 - x + 1 - |x - 1| &= x^2 - x + 1 - (x - 1) \\ &= x^2 - 2x + 2 \\ &= (x + 1)^2 + 1 \geq 0 \end{aligned}$$

so, $|x - 1| \leq x^2 - x + 1$.

**Second case :** $x < 1$

$$\begin{aligned} x^2 - x + 1 - |x - 1| &= x^2 - x + 1 - (-x + 1) \\ &= x^2 \geq 0 \end{aligned}$$

so, $|x - 1| \leq x^2 - x + 1$.

**Conclusion :** In any case $|x - 1| \leq x^2 - x + 1$.

**Reasoning by contraposition**

Contrapositive reasoning is based on the following equivalence : $(P \Rightarrow Q) \Leftrightarrow (\overline{Q} \Rightarrow \overline{P})$, So if we want to show the assertion "$P \Rightarrow Q$" it is sufficient to show that $\overline{Q} \Rightarrow \overline{P}$ is true.

**Exemple 1.12**

*Let* $a, b \in \mathbb{R}$. *Prove that*

$$(a \neq 2 \ \textit{and} \ b \neq 2) \Rightarrow (ab - 2a - 2b + 4 \neq 0)$$

We prove its contrapositive,

$$ab - 2a - 2b + 4 = 0 \Rightarrow (a = 2 \ \textit{or} \ b = 2)$$

Suppose that $ab - 2a - 2b + 4 = 0$, so

$$\begin{aligned} ab - 2a - 2b + 4 = 0 \quad &\Rightarrow a(b-2) - 2(b-2) = 0 \\ &\Rightarrow (b-2)(a-2) = 0 \\ &\Rightarrow (a = 2 \quad \textit{or} \quad b = 2) \end{aligned}$$

So, according to the principle of reasoning by contrapositive, we deduce that

$$(a \neq 2 \ \textit{and} \ b \neq 2) \Rightarrow (ab - 2a - 2b + 4 \neq 0).$$

**Proof by Contradiction (absurd)**

The raisoning by the absurd (proof by contradiction) involves demonstrating the truth of a proposition by showing that its opposite leads to a contradiction.

For example to show that $P \Rightarrow Q$ , we assume both that $P$ is true and that $Q$ is false, and look for a contradiction.

**Example 1.13**

Prove that : for all integers $n$, if $n^2$ is odd, then $n$ is odd.

Take an integer $n$ and let $n^2$ be odd. In order to obtain a contradiction, assume that $n$ is even. So, $n = 2k$ for some integer $k$. Substituting, we have $n^2 = (2k)^2 = 2 \times (2k^2)$ showing that $n^2$ is even. This is a contradiction. Therefore, $n$ is an odd integer.

**Exemple 1.14**

Prove that $\sqrt{2}$ is irrational.

Suppose that $\sqrt{2}$ is a rational number. Then we can write it

$$\sqrt{2} = \frac{p}{q}$$

with $p \in \mathbb{Z}, q \in \mathbb{Z}^*$ and $p$, $q$ are coprime ($\gcd(p,q) = 1$).

We have :

$$\sqrt{2} = \frac{p}{q} \Rightarrow 2 = \frac{p^2}{q^2} \Rightarrow p^2 = 2q^2.$$

Since $p^2 = 2q^2$ then $p^2$ is even, so $p$ is even.

Since $p$ is even, then $\exists p_0 \in \mathbb{Z}$ such that $p = 2p_0$.

So

$$p^2 = 2q^2 \Rightarrow (2p_0)^2 = 2q^2 \Rightarrow q^2 = 2p_0^2.$$

Since $q^2 = 2p_0^2$ then $q^2$ is even, so $q$ is even.

Since $q$ is even, so $\exists q_0 \in \mathbb{Z}^*$ such that $q = 2q_0$.

Which gives a contradiction, because $\gcd(p,q) = 1$.

According to the principle of reasoning by absurdity, we deduce that $\sqrt{2}$ is irrational.

**Proof by Induction (recurrence)**

The principle of proof by Induction allows us to show that a proposition $P(n)$, dependent on $n$, is true for all $n \geq n_0$ with $n; n_0 \in \mathbb{N}$.

So, to prove that the property $P(n)$ is true for all integers $n$ starting from a certain initial value $n_0$. We follow the following steps :

**(a) Base Case :** Verify that the property $P(n)$ is true for the initial value $n = n_0$.

**(b) Inductive Step :** We show that $P(n) \Rightarrow P(n+1)$, assume that the property $P(n)$ is true and then prove that the property $P(n+1)$ is true.

**Example 1.15**

Prove that : the sum of the first $n$ integers is given by the formula :

$$\forall n \in \mathbb{N}, \sum_{k=0}^{n} \left(2^k\right) = 1 + 2 + 4 + ... + 2^n = 2^{n+1} - 1.$$

In this case, we have : $n_0 = 0$ and the proposition $P(n)$ defined by

$$P\left(n\right) : \sum_{k=0}^{n} \left(2^k\right) = 2^{n+1} - 1$$

**Step 1 : Base Case**

First, we need to verify the property $P\left(n\right)$ is true for the initial value $n_0 = 0$.

When $n = n_0$ :

$$\sum_{k=0}^{n} \left(2^k\right) = 1 = 2^{0+1} - 1,$$

so, $P\left(n_0\right)$ is true.

**Step 2 : Inductive Step** We show that $P(n) \Rightarrow P(n+1)$,

We assume that the proposition $P\left(n\right)$ is true, that is, we assume :

$$\sum_{k=0}^{n} \left(2^k\right) = 2^{n+1} - 1,$$

This assumption is called the inductive hypothesis.

And show that the proposition $P(n+1)$ is true, that is to say

$$\sum_{k=0}^{n+1} \left(2^k\right) = 2^{n+2} - 1.$$

We have,

$$\sum_{k=0}^{n+1} \left(2^k\right) = 1 + 2 + 4 + ... + 2^n + 2^{n+1} = \left(\sum_{k=0}^{n} \left(2^k\right)\right) + \left(2^{n+1}\right),$$

Using the inductive hypothesis, we can write :

$$\sum_{k=0}^{n+1} \left(2^k\right) = \left(2^{n+1} - 1\right) + \left(2^{n+1}\right) = 2^{n+2} - 1,$$

so, we have shown that $P(n+1)$ is true.

**Conclusion**

By the principle of mathematical induction, the proposition $P\left(n\right)$ is true for all integers $n$.

## 1.6 Exercises

**Exercise 1.1**

*Show which of the following propositions are true or false.*

**1.** $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y > 0$
**2.** $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y > 0$
**3.** $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y > 0$
**4.** $\exists x \in \mathbb{R}, (x + 1 = 0 \text{ and } x - 3 = 0)$
**5.** $(\exists x \in \mathbb{R}, x + 1 = 0) \text{ and } (\exists x \in \mathbb{R}, x - 3 = 0)$
**6.** $\forall x \in \mathbb{R}, (x + 1 \neq 0 \text{ or } x - 3 \neq 0)$
**7.** $(\forall x \in \mathbb{R}, x + 1 \neq 0) \text{ or } (\forall x \in \mathbb{R}, x - 3 \neq 0)$
**8.** $(1 + 2 = 3) \Rightarrow (2 - 5 = 4)$

**Solution.**

1. $(\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y > 0)$ is a false proposition, because for a real number $x = 0$, the

proposition $y > 0$, is not true for all real $y$.

2. $(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y > 0)$ is a true proposition, because for a real number $x$, we can find a real $y = -x + 2$, such that $x + y > 0$.

3. $(\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y > 0)$ is a true proposition, because we can find a real number $x = 1$, and a real $y = 2$, such that $x + y > 0$.

4. $(\exists x \in \mathbb{R}, (x + 1 = 0 \ \textit{and} \ x - 3 = 0))$ is a false proposition, because we can't find a real number $x$ , which verifies both equations.

5. $((\exists x \in \mathbb{R}, x + 1 = 0) \ \textit{and} \ (\exists x \in \mathbb{R}, x - 3 = 0))$ is a true proposition, because it's conjunction of two true propositions.

6. $(\forall x \in \mathbb{R}, (x + 1 \neq 0 \ \textit{or} \ x - 3 \neq 0))$ is a true proposition, because it's the negation of the proposition 4.

7. $((\forall x \in \mathbb{R}, x + 1 \neq 0) \ \textit{or} \ (\forall x \in \mathbb{R}, x - 3 \neq 0))$ is a false proposition, because it's the negation of the proposition 5.

8. $((1 + 2 = 3) \Rightarrow (2 - 5 = 4))$ is a false proposition, because the first proposition is true and the second is false.

**Exercise 1.2**

*Let $P$, $Q$ and $R$ be three logical propositions.*

$$P : \forall x \in \mathbb{R}, 2x - 1 \geq x, \qquad Q : \forall x \in \mathbb{R}, x^2 - 4 \geq 0$$
$$R : \forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \ \textit{if} \ x \geq y \ \textit{then} \ x^2 + y^2 \geq 0$$

*Are these propositions true or false ? Give their negations.*

**Solution.**

1. $P$ is false proposition, because for $x = 0$ we have $2x - 1 < x$. Their negation is

$$\overline{P} : \exists x \in \mathbb{R}, 2x - 1 < x.$$

2. $Q$ is false proposition, because for $x = 1$ we have $x^2 - 4 < 0$. Their negation is

$$\overline{Q} : \exists x \in \mathbb{R}, x^2 - 4 < 0.$$

3. $R$ is true proposition, because for all reals $x, y$ such that $x \geq y$ we have $x^2 + y^2 \geq 0$. Their negation is

$$\overline{R} : \exists x \in \mathbb{R}, \exists y \in \mathbb{R}, (x \geq y) \ \textit{and} \ (x^2 + y^2 < 0).$$

**Exercise 1.3**

Write the contrapositive and the negation of the following implications :

**1.** $\forall n \in \mathbb{N}^*,\ n^2-1$ *is not divisible by* $8 \Rightarrow\ n$ *is even*
**2.** $(x=y)$ *or* $((x+1)(y-1) \neq (x-1)(y+1))$
**3.** $\forall n \in \mathbb{N},$ *if* $n$ *is prime number, then* $(n=2$ *or* $n$ *is odd)*

**Solution.**

1. The contrapositive

$$\forall n \in \mathbb{N}^*,\quad n \text{ is odd} \Rightarrow n^2-1 \text{ is divisible by } 8$$

- The negation

$$\exists n \in \mathbb{N}^*,\ (n^2-1 \text{ is not divisible by } 8) \text{ and } (n \text{ is odd})$$

2. The proposition 2 is equivalent to

$$(x \neq y) \Rightarrow ((x+1)(y-1) \neq (x-1)(y+1))$$

- The contrapositive

$$((x+1)(y-1) = (x-1)(y+1)) \Rightarrow (x=y)\,.$$

- The negation

$$(x \neq y) \wedge ((x+1)(y-1) = (x-1)(y+1))$$

3. The contrapositive

$$\forall n \in \mathbb{N},\ \text{if } (n \neq 2 \text{ and } n \text{ is even}), \text{ then } (n \text{ is note prime number}).$$

- The negation

$$\exists n \in \mathbb{N}, (n \text{ is prime number}) \text{ and } (n \neq 2 \text{ and } n \text{ is even}).$$

**Exercise 1.4**

1. Show that for all $n \in \mathbb{N}$, $\frac{n(n+1)}{2}$ is a natural integer.

2. Using the proof by contradiction, prove that :

$$\textit{If } ab \textit{ is odd, then } a \textit{ is odd and } b \textit{ is odd.}$$

3. Using the proof by contrapositive, prove that :

$$(a \neq 4 \textit{ and } b \neq 4) \Rightarrow (ab - 4a - 4b + 16 \neq 0)\,.$$

**Solution.**

**1. Show that for all $n \in \mathbb{N}$, $\frac{n(n+1)}{2}$ is a natural integer.**

Let $n \in \mathbb{N}$,

**First case :** $n = 2k$

$$\frac{n(n+1)}{2} = \frac{2k(2k+1)}{2} = k(2k+1) \in \mathbb{N},$$

so, $\frac{n(n+1)}{2}$ is a natural integer.

**Second case :** $n = 2k + 1$

$$\frac{n(n+1)}{2} = \frac{(2k+1)(2k+2)}{2} = (2k+1)\,(k+1) \in \mathbb{N},$$

so, $\frac{n(n+1)}{2}$ is a natural integer.

**Conclusion :** In any case, $\frac{n(n+1)}{2}$ is a natural integer.

**2. Using the proof by contradiction, prove that :**

$$\text{If } ab \text{ is odd, then } a \text{ is odd and } b \text{ is odd.}$$

Suppose that $ab$ is odd and ($a$ is even or $b$ is even) . Then we can write

$$a = 2p \quad \text{or} \quad b = 2q,$$

so,

$$ab = 2k.$$

Which gives a contradiction, because $ab$ is odd.

According to the principle of reasoning by absurdity, we deduce that : If $ab$ is odd, then $a$ is odd and $b$ is odd.

**3. Using the proof by contrapositive, prove that :**

$$(a \neq 4 \ and \ b \neq 4) \Rightarrow (ab - 4a - 4b + 16 \neq 0).$$

We prove its contrapositive,

$$ab - 4a - 4b + 16 = 0 \Rightarrow (a = 4 \ or \ b = 4)$$

Suppose that $ab - 4a - 4b + 16 = 0$, so

$$\begin{aligned} ab - 4a - 4b + 16 = 0 \ &\Rightarrow a(b-4) - 4(b-4) = 0 \\ &\Rightarrow (b-4)(a-4) = 0 \\ &\Rightarrow (a = 4 \quad or \ \ b = 4) \end{aligned}$$

So, according to the principle of reasoning by contrapositive, we deduce that

$$(a \neq 4 \ and \ b \neq 4) \Rightarrow (ab - 4a - 4b + 16 \neq 0).$$

**Exercise 1.5**

*Using the proof by recurrence, prove that :*

*For any natural integer $n > 0$, we have :*

$$\textbf{(1).} \ \sum_{k=1}^{n} \left(3 + \tfrac{1}{3^k}\right) = \tfrac{1}{2}\left(1 + 6n - \tfrac{1}{3^n}\right) \qquad \textbf{(2).} \ \ n! \leq n^n$$

**Solution.**

**(1).** $\sum_{k=1}^{n} \left(3 + \tfrac{1}{3^k}\right) = \tfrac{1}{2}\left(1 + 6n - \tfrac{1}{3^n}\right)$ :

In this case, we have : $n_0 = 1$ and the proposition $P(n)$ defined by

$$P(n) : \sum_{k=1}^{n} \left(3 + \tfrac{1}{3^k}\right) = \tfrac{1}{2}\left(1 + 6n - \tfrac{1}{3^n}\right)$$

**Step 1 : Base Case**

First, we need to verify the property $P(n)$ is true for the initial value $n_0 = 1$.

When $n = n_0$ :

$$\sum_{k=0}^{n} \left(3 + \tfrac{1}{3^k}\right) = \left(3 + \tfrac{1}{3^1}\right) = \tfrac{10}{3} = \tfrac{1}{2}\left(1 + 6(1) - \tfrac{1}{3^1}\right),$$

so, $P(n_0)$ is true.

**Step 2 : Inductive Step** We show that $P(n) \Rightarrow P(n+1)$,

We assume that the proposition $P(n)$ is true, that is, we assume :

$$\sum_{k=1}^{n} \left(3 + \tfrac{1}{3^k}\right) = \tfrac{1}{2}\left(1 + 6n - \tfrac{1}{3^n}\right),$$

This assumption is called the inductive hypothesis.

and show that the proposition $P(n+1)$ is true, that is to say

$$\sum_{k=1}^{n+1} \left(3 + \tfrac{1}{3^k}\right) = \tfrac{1}{2}\left(7 + 6n - \tfrac{1}{3^{n+1}}\right).$$

We have,

$$\sum_{k=0}^{n+1} \left(3 + \tfrac{1}{3^k}\right) = \left(\sum_{k=0}^{n} \left(3 + \tfrac{1}{3^k}\right)\right) + \left(3 + \tfrac{1}{3^{n+1}}\right),$$

Using the inductive hypothesis, we can write :

$$\begin{aligned}\sum_{k=0}^{n+1} \left(3 + \tfrac{1}{3^k}\right) &= \tfrac{1}{2}\left(1 + 6n - \tfrac{1}{3^n}\right) + \left(3 + \tfrac{1}{3^{n+1}}\right) \\ &= \tfrac{1}{2}\left(1 + 6n - \tfrac{1}{3^n} + 6 + \tfrac{2}{3^{n+1}}\right) \\ &= \tfrac{1}{2}\left(7 + 6n - \tfrac{1}{3^{n+1}}\right),\end{aligned}$$

so, we have shown that $P(n+1)$ is true.

**Conclusion**

By the principle of mathematical induction, the proposition $P(n)$ is true for all integers $n > 0$.

**(2).** $n! \leq n^n$ :

In this case, we have : $n_0 = 1$ and the proposition $P(n)$ defined by

$$P(n) : n! \leq n^n$$

**Step 1 : Base Case**

First, we need to verify the property $P(n)$ is true for the initial value $n_0 = 1$.

When $n = n_0$ :

$$(n! = 1) \leq (n^n = 1),$$

so, $P(n_0)$ is true.

**Step 2 : Inductive Step** We show that $P(n) \Rightarrow P(n+1)$,

We assume that the proposition $P(n)$ is true, that is, we assume :

$$n! \leq n^n,$$

This assumption is called the inductive hypothesis.

and show that the proposition $P(n+1)$ is true, that is to say

$$(n+1)! \leq (n+1)^{n+1}.$$

We have,

$$\begin{aligned} n! \leq n^n &\Rightarrow (n!)(n+1) \leq (n^n)(n+1) \\ &\Rightarrow (n+1)! \leq (n^n)(n+1) \\ &\Rightarrow (n+1)! \leq (n+1)^n \times (n+1), \text{ because } n \leq n+1 \\ &\Rightarrow (n+1)! \leq (n+1)^{n+1}, \end{aligned}$$

so, we have shown that $P(n+1)$ is true.

**Conclusion**

By the principle of mathematical induction, the proposition $P(n)$ is true for all integers $n > 0$.

## 1.7 Terminology translation

| **English** | **Frensh** |
|---|---|
| True | Vraie |
| False | Fausse |
| Truth table | Table de vérité |
| Logical connectors | Connecteurs logiques |
| Conjunction | Conjonction |
| Disjunction | Disjonction |
| Quantifiers | Quantificateurs |
| Reasoning | Raisonnement |
| Prime number | Nombre premier |
| Odd | Impair |
| Even | Pair |
| Natural integer | Entier naturel |
| Hypothesis | Hypothèse |

Chapitre 2

# Sets and applications

In this second chapter, we will provide some definitions and properties associated with sets and applications. Solved exercises are included to help you practice and apply these techniques effectively

## 2.1 Sets

### 2.1.1 Definitions and examples

**Definition 2.1**

A set is a collection of objects, these objects are called elements of that set.

We use uppercase letters to label sets, and elements will usually be represented by lower case letters.

An element $x$ belongs to $E$ (written as $x \in E$) or does not belong to $E$ (written as $x \notin E$).

An empty set, denoted by $\varnothing$, is a set that does not contain any elements.

**Example 2.1**

- Let $E$ be the set of all integers between 1 and 8, then

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

**Definition 2.2**

The cardinality of a set $E$, denoted $card(E) = |E|$, is the number (finite or infinite) of elements in $E$.

If $card(E)$ is finite, theset $E$ is said to be finite. Otherwise, the set $E$ is said to be infinite.

**Example 2.2**

- $Card\left(\varnothing\right) = 0$.

- $Card\left(\{0, 1, 5, 7\}\right) = 4$.

- The set of prime numbers is infinite.

### 2.1.2 Parts of a set and complementary

**Definition 2.3 (Inclusion)**

- Let $A, E$ be two sets. We say that $A$ is included in $E$ (or $A$ is a subset of $E$), if every element of $A$ is also an element of $E$. This is denoted as : $A \subset E$.

$$A \subset E \Leftrightarrow (\text{every element of } A \text{ is also an element of } E)$$

$$\Leftrightarrow (\forall x \in A \Rightarrow x \in E)$$

- The set of parts of $E$ is denoted by $P(E)$ :

$$A \in P(E) \Leftrightarrow A \subset E.$$

- If $E$ has $n$ element, then $P(E)$ has $2^n$.

**Example 2.3**

- Let $E$ be the set defined by

$$E = \{1, 2, 3\}.$$

We have $Card\left(E\right) = 3$, so $Card\left(P\left(E\right)\right) = 2^3 = 8$.

$$P(E) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

**Definition 2.4 (Complement)**

The complement of the set $A$, written $C_{E}\left(A\right)$and read (the complement of $A$) is the set of all elements of $E$ that are not in $A$. Formally,

$$C_{E}\left(A\right) = \{a/a \in E \ and \ a \notin A\}.$$

Given two sets $A$ and $B$, We say that $A$ and $B$ are equal if and only if $A \subset B$ and $B \subset A$.

$$A = B \Leftrightarrow (A \subset B \text{ and } B \subset A)$$

$$\Leftrightarrow (\forall x, x \in A \Leftrightarrow x \in E).$$

**Proposition 2.1**

*Let $A, B$ two parts of a set $E$,*such that $A \subset B$. We always have

$$C_E\left(C_E^A\right) = A, \quad C_E(\varnothing) = E, \quad C_E(E) = \varnothing$$

$$A \subset B \Leftrightarrow C_E^B \subset C_E^A$$

**Proof.**

Let $A, B$ two parts of a set $E$ such that $A \subset B$, then

$$\begin{aligned} A \subset B &\Leftrightarrow (\forall a, a \in A \Rightarrow a \in B) \\ &\Leftrightarrow (\forall a, a \notin B \Rightarrow a \notin A) \\ &\Leftrightarrow (\forall a, a \in C_E B \Rightarrow a \in C_E A) \\ &\Leftrightarrow (C_E B \subset C_E A). \end{aligned}$$

### 2.1.3 Intersection and union

Let $A$ and $B$ be two sets.

**Definition 2.5 (Union)**

The union of $A$ and $B$, denoted as $A \cup B$ (read as : $A$ union $B$), is the set of elements $x$ that belong to either $A$ or $B$.

$$A \cup B = \{x / x \in A \text{ or } x \in B\}.$$

**Definition 2.6 (Intersection)**

The intersection of $A$ and $B$, denoted as $A \cap B$ (read as : $A$ intersect $B$), is the set of elements of elements $x$ that are in both $E$ and $F$.

$$A \cap B = \{x / x \in A \text{ and } x \in B\}.$$

We say that $A$ and $B$ are disjoint sets if $A \cap B = \emptyset$.

**Example 2.4**

Consider the following sets :

$$E = \{0, 1, 2, 3, 4, 5\}$$

$$F = \{1, 3, 5, 7, 9\},$$

Intersection $E \cap F$ :

$$E \cap F = \{1, 3, 5\}$$

Union $E \cup F$ :

$$E \cup F = \{0, 1, 2, 3, 4, 5, 7, 9\}.$$

**Proposition 2.2**

Let $A, B$ and $C$ three sets.

1. $A \cap B = B \cap A, \;\; A \cup B = B \cup A.$

2. $A \subset A \cup B, \;\; B \subset A \cup B.$

3. $A \cap B \subset A, \;\; A \cap B \subset B.$

4. $A \cap (B \cap C) = (A \cap B) \cap C, \;\; A \cup (B \cup C) = (A \cup B) \cup C.$

5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \;\; A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$

**Proof.** Let $A, B$ and $C$ three sets.

**1.** Let $x \in A \cap B$, we have :

$$\begin{aligned} x \in A \cap B &\Leftrightarrow (x \in A) \wedge (x \in B) \\ &\Leftrightarrow (x \in B) \wedge (x \in A) \\ &\Leftrightarrow x \in B \cap A, \end{aligned}$$

hence $A \cap B = B \cap A$.

Let $x \in A \cup B$, we have :

$$\begin{aligned} x \in A \cup B &\Leftrightarrow (x \in A) \vee (x \in B) \\ &\Leftrightarrow (x \in B) \vee (x \in A) \\ &\Leftrightarrow x \in B \cup A, \end{aligned}$$

hence $A \cup B = B \cup A$.

**2.3.** Trivial.

**4.** Let $x \in A \cap (B \cap C)$

$$\begin{aligned} x \in A \cap (B \cap C) &\Leftrightarrow (x \in A) \wedge (x \in B \cap C) \\ &\Leftrightarrow (x \in A) \wedge ((x \in B) \wedge (x \in C)) \\ &\Leftrightarrow (x \in A) \wedge (x \in B) \wedge (x \in C) \\ &\Leftrightarrow ((x \in A) \wedge (x \in B)) \wedge (x \in C) \\ &\Leftrightarrow (x \in A \cap B) \wedge (x \in C) \\ &\Leftrightarrow x \in (A \cap B) \cap C, \end{aligned}$$

hence $A \cap (B \cap C) = (A \cap B) \cap C$.

For the second equality, the same reasoning as the first equality.

**5.** Let $x \in A \cap (B \cup C)$

$$\begin{aligned} x \in A \cap (B \cup C) &\Leftrightarrow (x \in A) \wedge (x \in B \cup C) \\ &\Leftrightarrow (x \in A) \wedge ((x \in B) \vee (x \in C)) \\ &\Leftrightarrow ((x \in A) \vee (x \in B)) \wedge ((x \in A) \vee (x \in C)) \\ &\Leftrightarrow (x \in A \cup B) \wedge (x \in A \cup C) \\ &\Leftrightarrow (A \cup B) \cap (A \cup C), \end{aligned}$$

hence $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

For the second equality, the same reasoning as the first equality.

**Theorem 2.1**

*Let $A, B$ tow parts of a set $E$. Then we have*

1. $C_E(A \cap B) = C_E A \cup C_E B$.

2. $C_E(A \cup B) = C_E A \cap C_E B$.

**Proof.**

**1.** Let $x \in C_E(A \cap B)$. then $x \in E$ and $x \notin A \cap B$, so $x \notin A$ or $x \notin B$. Then $x \in C_E A$ or $x \in C_E B$. So $x \in C_E A \cup C_E B$, hence

$$C_E(A \cap B) \subset C_E A \cup C_E B.$$

Conversely, let $x \in C_E A \cup C_E B$. If $x \in C_E A$, then $x \notin A$, so $x \notin A \cap B$, and subsequently $x \in C_E(A \cap B)$.

In the same, if $x \in C_E B$, then $x \notin B$ , so $x \notin A \cap B$, and subsequently $x \in C_E (A \cap B)$.
In both cases $x \in C_E (A \cap B)$, hence

$$C_E A \cup C_E B \subset C_E (A \cap B).$$

The first equality is demonstrated.

**2.** For the second equality, we pose $A_1 = C_E A$, $B_1 = C_E B$ and using $C_E (C_E A) = A$.

### 2.1.4 Difference and symmetrical difference

Let $A, B$ be two subsets of $E$.

1. The difference of $A$ and $B$, denoted $A \setminus B$, consists of elements that are in $A$ but not in $B$,

$$A \setminus B = \{x / x \in A \text{ and } x \notin B\}.$$

2. The symmetric difference of $A$ and $B$, denoted $A \Delta B$, is the set

$$A \Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$$

**Example 2.5**. Consider the following sets :

$$E = \{0, 1, 2, 3, 4\}$$

$$F = \{1, 3, 5, 7\},$$

we have

$$E \setminus F = \{0, 2, 4\}, \quad F \setminus E = \{5, 7\},$$

and

$$E \Delta F = \{0, 2, 4, 5, 7\}.$$

### 2.1.5 Partition of a set

Let $E$ be a set. A partition of $E$ is a set $\{A_1, A_2, ..., A_n\}$ of subsets of $E$ that satisfies the following two conditions :

1. $\forall i, A_i \neq \varnothing$.

2. $A_i \cap A_j = \emptyset$ for all $i \neq j$.

3. $E = \cup A_i$

**Example 2.6**. Consider the following sets :

$$E = \{0, 1, 2, 3, 4\}$$

$$A = \left\{ \underbrace{\{0, 2\}}_{A_1}, \underbrace{\{1, 3\}}_{A_2}, \underbrace{\{4\}}_{A_3} \right\}.$$

We have :

(i). Non-empty subsets : $\forall i, A_i \neq \varnothing$.

$$A_1 \neq \varnothing, \quad A_2 \neq \varnothing, \quad A_3 \neq \varnothing$$

(ii). Disjoint subsets : $A_i \cap A_j = \emptyset$ for all $i \neq j$

$$A_1 \cap A_2 = \varnothing, \ A_1 \cap A_3 = \varnothing, \ A_2 \cap A_3 = \varnothing$$

(iii). Union of subsets equals the original set : $E = \cup A_i$

$$A_1 \cup A_2 \cup A_3 = E$$

Thus, $A = \left\{ \underbrace{\{0, 2\}}_{A_1}, \underbrace{\{1, 3\}}_{A_2}, \underbrace{\{4\}}_{A_3} \right\}$ is a partition of $E$.

### 2.1.6 Cartesian product

**Definition 2.7** Let $A, B$ be two sets. The Cartesian product, denoted $A \times B$, is the set of pairs $(x, y)$ where $x \in A$ and $y \in B$.

$$A \times B = \{(x, y)/x \in A \ and \ y \in B\}.$$

**Example 2.7**

1.

$$\mathbb{Z}^2 = \{(x, y)/x, y \in \mathbb{Z}\}.$$

2. Let $A = \{0, 1, 2\}$ and $B = \{2, 4\}$. Then

$$\begin{aligned} A \times B &= \{(x, y)/x \in A \text{ and } y \in B\} \\ &= \{(0,2), (0,4), (1,2), (1,4), (2,2), (2,4)\}. \end{aligned}$$

## 2.2 Applications

### 2.2.1 Definitions and examples

**Definition 2.8**

Let $E$ and $F$ be two sets.

An application from $E$ to $F$ is any correspondence $f$ associating each element $x$ of $E$ a unique element $y$ of $F$.

$$\begin{aligned} f : E &\to F \\ x &\mapsto y = f(x) \end{aligned}$$

– $E$ : the starting set.

– $F$ : the arrival set.

– $x$ : the antecedent of $y$ by $f$.

– $y = f(x)$ : the image of $x$ by $f$.

$$(f : E \to F \text{ is an application}) \Leftrightarrow (\forall x_1, x_2 \in E, (x_1 = x_2 \Rightarrow f(x_1) = f(x_2)))$$

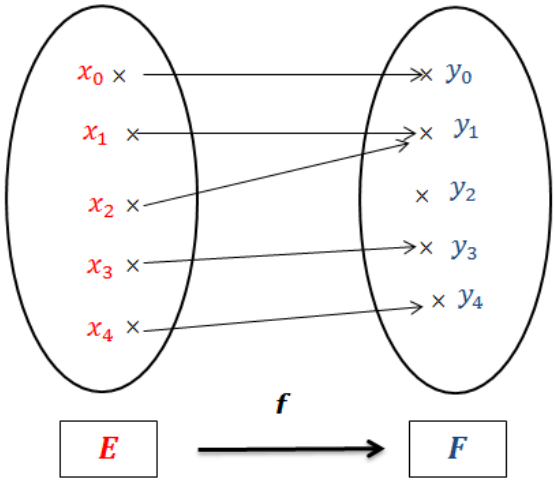


Fig 2.1 : Schema of an application $f$ from a set $E$ to a set $F$

**Example 2.9**

**1.**

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto \tfrac{2x}{x^2+1} \end{aligned}$$

$f$ is an application from $\mathbb{R}$ to $\mathbb{R}$.

**2.**

$$\begin{aligned} g : \mathbb{N} &\to \mathbb{N} \\ x &\mapsto \sqrt{x+1} \end{aligned}$$

$g$ is not an application. (For example, the element $x = 2$ does not have an image by $g$).

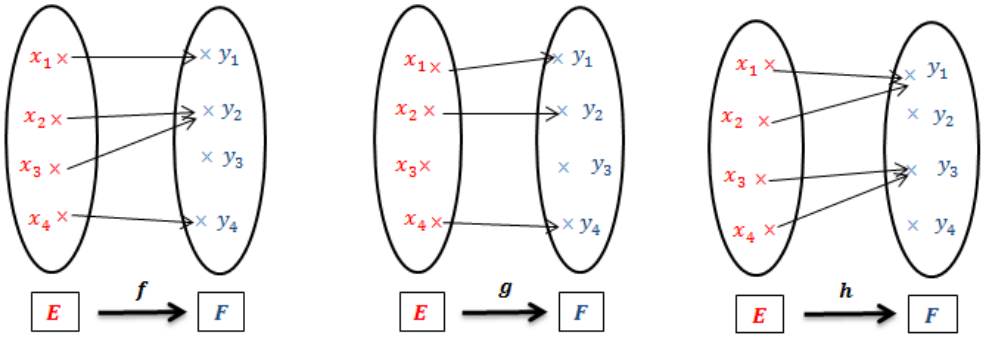
**3.** The application

$$\begin{aligned} h : E &\to E \\ x &\mapsto h(x) = x \end{aligned}$$

is called the identity application in $E$ and is denoted $Id_E$.

**Example 2.10**

Let be the following three applications :




- $f$ is note an application, because

$$\exists x_1, x_2 \in E / f(x_1) = f(x_2) = y_2.$$

- $g$ is note an application, because there is an element $x_3$ in $E$ does not have an image in $F$.

- $h$ is an application, because

$$\forall a, b \in E, (a = b \Rightarrow h(a) = h(b)).$$

### 2.2.2 Equality of two applications

We say that two applications $f, g$ are equal if

1. They have the same starting set $E$ and the same arrival set $F$.

2. For all $x \in E, f(x) = g(x)$.

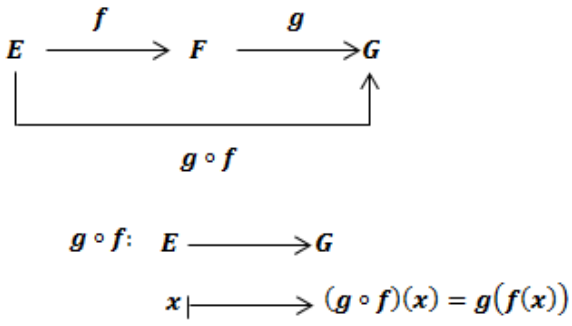
We denote $f = g$.

### 2.2.3 Compositions of applications

Let $f : E \to F$ and $g : F \to G$ be two applications. We denote by $g \circ f$ the application of $E$ in $G$ defined by :

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

This application is called a composite of the applications $f$ and $g$.




**Example 2.11**. Let be the following two applications :

$$\begin{array}{rccc} f: & \mathbb{R} & \to & ]0,1] \\ & x & \longmapsto & \frac{1}{\sqrt{1+x^2}} \end{array} \qquad \begin{array}{rccc} g: & ]0,1] & \to & ]-\infty,0] \\ & x & \longmapsto & \ln(x) \end{array}$$

then the composite application $g \circ f$ is defined as follows :

$$\begin{array}{rccc} g \circ f: & \mathbb{R} & \to & ]-\infty,0] \\ & x & \mapsto & (g \circ f)(x) = g(f(x)) = -\frac{1}{2}\ln(1+x^2) \end{array}$$

### 2.2.4 Restriction and extension

Let $f$ be an application from $E$ to $F$ and $A \subset E \subset G$.

The restriction of $f$ to $A$ is defined by :

$$\begin{array}{rccc} f_{/A}: & A & \to & F \\ & x & \longmapsto & y = f_{/A}(x) = f(x) \end{array}$$

We call an extension of $f$ to $G$ any application $g : G \to F$, such that for all $x \in G, g(x) = f(x)$. We also say that $f$ is an extension of $f_{/A}$.

### 2.2.5 Injection, surjection and bijection

#### Injection

**Definition 2.9**

Let $E, F$ be two sets and $f : E \to F$ be an application.

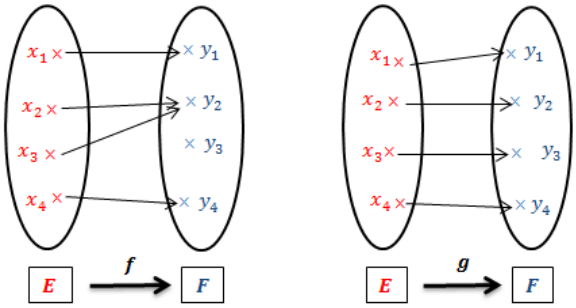
$f$ is injective if for each two (distinct) elements of $E$ there correspond, through $f$ , two distinct elements of $F$. then we have :

$$\forall x_1, x_2 \in E, f(x_1) = f(x_2) \Rightarrow x_1 = x_2,$$

or what amounts to the same thing :

$$\forall x_1, x_2 \in E, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

**Example 2.12**. Let be the following two applications :




- The application $f$ is note injective, because

$$\exists (a, b) = (x_2, x_3) \in E^2, (f(a) = f(b) = y_2) \wedge (a \neq b).$$

- The application $g$ is injective, because

$$\forall (a, b) \in E^2, (g(a) = g(b) \Rightarrow a = b).$$

**Example 2.13**. Let be the application $f : \mathbb{R} \to \mathbb{R}$, defined by $f(x) = \frac{2x}{1+x^2}$.

Let $a, b \in \mathbb{R}$, we have

$$\begin{aligned} f(a) = f(b) &\Rightarrow \tfrac{2a}{1+a^2} = \tfrac{2b}{1+b^2} \\ &\Rightarrow 2a(1+b^2) = 2b(1+a^2) \\ &\Rightarrow (a-b) + ab(b-a) = 0 \\ &\Rightarrow (a-b)(1-ab) = 0 \\ &\Rightarrow \begin{cases} a-b=0 \\ 1-ab=0 \end{cases} \end{aligned}$$

We can find two different elements have the same image. For example $a = \frac{1}{2}, b = 2$, we have $f(a) = f(b) = \frac{4}{5}$.

Then the application $f$ is note injective.

**Remark 2.1** Let $f : E \to F$ be an application. If $f$ is strictly monotonic on $E$ then it is injective.

### Surjection

#### Definition 2.10

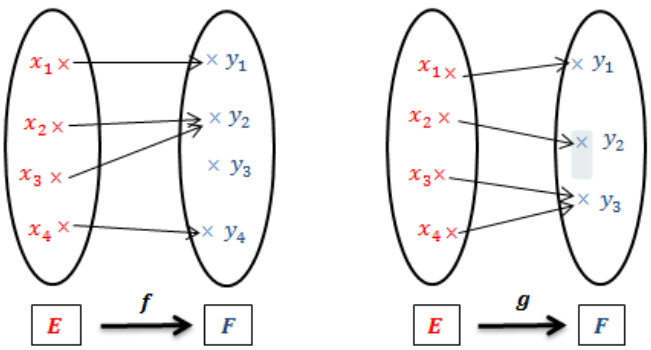
Let $E, F$ be two sets and $f : E \to F$ be an application.

$f$ is surjective if any element of $F$ is the image by the application $f$ of at least one element of $E$. then we have :

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

#### Example 2.14

Let be the following two applications :



- The application $f$ is note surjective, because the element $y_3$ has no antecedent.

- The application $g$ is surjective, because

$$\forall y \in F, \exists x \in E, y = g(x).$$

**Example 2.15**. Let be the application $f : \mathbb{R} \to \mathbb{R}$, defined by $f(x) = \frac{2x}{1+x^2}$.

Let $y \in \mathbb{R}$, we have

$$\begin{aligned} y = f(x) &\Leftrightarrow y = \tfrac{2x}{1+x^2} \\ &\Leftrightarrow yx^2 - 2x + y = 0 \\ \Delta = (-2)^2 - 4(y)(y) &= 4 - 4y^2. \end{aligned}$$

If $y \in ]-\infty, -1[ \cup ]1, +\infty[$, the equation has no solutions, that's to say the element $y$ has no antecedent. Then the application $f$ is note surjective.

**Remark 2.2** Let $f : E \to F$ be an application. $f$ is surjective if and only if $f(E) = F$.

### Bijection

**Definition 2.11**

Let $E, F$ be two sets and $f : E \to F$ be an application.

$f$ is bijective if $f$ is both injective and surjective. In other words,

$$\forall y \in F, \exists! x \in E, y = f(x)$$

**Example 2.16** Let be the following application

$$\begin{array}{rccc} f: & \mathbb{R} - \{1\} & \to & \mathbb{R} - \{2\} \\ & x & \longmapsto & \frac{2x+1}{x-1} \end{array}$$

Let $y \neq 2$, we have

$$\begin{aligned} y = f(x) &\Leftrightarrow y = \tfrac{2x+1}{x-1} \\ &\Leftrightarrow yx - y = 2x + 1 \\ &\Leftrightarrow x(y-2) = y + 1 \\ &\Leftrightarrow x = \tfrac{y+1}{y-2}, \ (y \neq 2). \end{aligned}$$

$x \in E = \mathbb{R} - \{1\}$?

Suppose that $x = 1$, so,

$$x = 1 \Leftrightarrow \tfrac{y+1}{y-2} = 1 \Leftrightarrow 1 = -1, \quad \text{which is impossible,}$$

so, from the reasoning by contradiction, we deduce that $x \neq 1$and moreover $x$ is unique.
Then, for every real $y \neq 2$ there exists an unique real $x \neq 1$ such that $y = f(x)$, so the application f is bijective.

**Bijection Theorem**

If $f$ is continuous and strictly increasing (or strictly decreasing) on an interval $[a, b]$, then $f$ performs a bijection from $[a, b]$ to $[f(a), f(b)]$ (or $[f(b), f(a)]$). (This also applies to an open interval).

**Example 2.17**. Let be the following application

$$\begin{array}{rccc} f: & [-1,1] & \to & [-1,1] \\ & x & \longmapsto & \frac{2x}{1+x^2} \end{array}$$

- $f$ is continuous on $[-1, 1]$.
- For any real $x \in [-1, 1]$, we have

$$f'(x) = \frac{2\left(1-x^2\right)}{(1+x^2)^2} \geq 0,$$

so, $f$ is strictly increasing. Then the application $f$ is bijective.

### 2.2.6 The reciprocal application

If $f : E \to F$ is a bijective application, then there exists a unique application $g : F \to E$, such that

$$g \circ f = Id_E \quad \text{and} \quad f \circ g = Id_F$$

The application $g$ is called the inverse or reciprocal of $f$ and we denote :

$$g = f^{-1}.$$

**Example 2.18**. Let be $f : [-1, 1] \to [-1, 1]$ an application defined by

$$f(x) = \frac{2x}{1+x^2}.$$

$f$ is a bijective application (see example 2.15), then it is invertible.
Let $y, x \in [-1, 1]$, such that $y = f(x)$.

$$y = f(x) \Leftrightarrow y = \frac{2x}{1+x^2} \Leftrightarrow yx^2 - 2x + y = 0,$$

$$\Delta = (-2)^2 - 4(y)(y) = 4 - 4y^2.$$

If $y \in ]-1,0[ \cup ]0,1[$, then

$$x = \frac{1-\sqrt{1-y^2}}{y} \in [-1,1]$$

$$x = \frac{1+\sqrt{1-y^2}}{y} \notin [-1,1].$$

If $y = 0$, then

$$x = 0.$$

If $y = \pm 1$, then

$$x = \pm 1.$$

So, the inverse of $f$ is defined by

$$\begin{array}{rccl} f^{-1}: & [-1,1] & \to & [-1,1] \\ & x & \longmapsto & \begin{cases} 0, & if \quad x = 0 \\ \frac{1-\sqrt{1-y^2}}{y}, & if \quad x \in ]-1,0[ \cup ]0,1[ \end{cases} \end{array}$$

**Proposition 2.3**

Let $f : E \to F$ and $g : F \to G$ be two applications, then :

1. $((f$ is injective$) \wedge (g$ is injective$)) \Rightarrow (g \circ f$ is injective).

2. $((f$ is surjective$) \wedge (g$ is surjective$)) \Rightarrow (g \circ f$ is surjective).

3. $((f$ is bijective$) \wedge (g$ is bijective$)) \Rightarrow (g \circ f$ is bijective and $(g \circ f)^{-1} = f^{-1} \circ g^{-1})$.

**Proof.**

**1.** Suppose that $(f$ is injective$) \wedge (g$ is injective) and show that $g \circ f$ is injective.

Let $a, b \in E$, we have :

$$\begin{aligned} (g \circ f)(a) = (g \circ f)(b) &\Rightarrow g(f(a)) = g(f(b)) \\ &\Rightarrow f(a) = f(b) \quad \text{(because } g \text{ is injective)} \\ &\Rightarrow a = b \quad \text{(because } f \text{ is injective),} \end{aligned}$$

which shows that $g \circ f$ is an injective application.

**2.** Suppose that $(f$ is surjective$) \wedge (g$ is surjective) and show that $g \circ f$ is surjective.

Let $z \in G$, since $g$ is surjective, then there exists $y \in F$ such that $z = g(y)$.

since $y \in F$ and $f$ is surjective, then there exists $x \in E$ such that $y = f(x)$, so $z = g(y) =$

$g(f(x))$.

We deduce that for any element $z \in G$ there exists $x \in E$ such that $z = g(f(x))$.

which shows that $g \circ f$ is a surjective application.

**3.** Suppoe that ($f$ is bijective) $\wedge$ ($g$ is bijective) and show that

$\left(g \circ f \text{ is bijective and } (g \circ f)^{-1} = f^{-1} \circ g^{-1}\right)$.

From 1 and 2 we deduce that $g \circ f$ is a bijective application.

Let $z \in G$, then there exists $y \in F$ and $x \in E$ such that $z = g(y), y = f(x)$ and $z = g(f(x))$.

So,

$$y = g^{-1}(z)$$

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

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

Then,

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

Hence

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

**Proposition 2.4**

Let Let $f : E \to F$ and $g : F' \to G$ be two applications such that $F' \subset F$, then :

1. ($g \circ f$ is injective) ) $\Rightarrow$ ($f$ is injective).

2. ($g \circ f$ is surjective) ) $\Rightarrow$ ($g$ is surjective).

**Proof.**

**1.** Suppose that ($g \circ f$ is injective) and show that ($f$ is injective)

Let $a, b \in E$, we have :

$$\begin{aligned} f(a) = f(b) &\Rightarrow g(f(a)) = g(f(b)) \quad \text{(because } g \text{ is an application)} \\ &\Rightarrow (g \circ f)(a) = (g \circ f)(b) \\ &\Rightarrow a = b \quad \text{(because } g \circ f \text{ is injective),} \end{aligned}$$

which shows that $f$ is an injective application.

**2.** Suppose that ($g \circ f$ is surjective) and show that ($g$ is surjective).

Let $z \in G$, then there exists $x \in E$ such that $z = (g \circ f)(x) = g(f(x))$.

So, there exists $y = f(x) \in F$ such that $z = g(f(x)) = g(y)$.

We deduce that for all $z \in G$ there exists $y \in F$ such that $z = g(y)$.

Which shows that $g$ is a surjective application.

### 2.2.7 Direct image - reciprocal image

Let $E, F$ be two sets and $f$ be an application of $E$ to $F$.

**Definition 2.12**

We call the direct image of a set $A \subset E$, the set

$$f(A) = \{f(x) / x \in A\}.$$

**Definition 2.13**

We call the inverse image of a set $B \subset F$, the set

$$f^{-1}(B) = \{x \in E / f(x) \in B\}.$$

**Example 2.19**. Let $f$ be the application from $\mathbb{R}$ to $\mathbb{R}$ defined by : $f(x) = 2x^2 + 5x - 3$

**Calculate** $f^{-1}(\{-3\})$

The set $f^{-1}(\{-3\})$ is the set of all $x \in \mathbb{R}$ such that $f(x) = -3$.

$$f^{-1}(\{-3\}) = \{x \in \mathbb{R} / f(x) = -3\}.$$

Solving the equation $f(x) = -3$ :

$$\begin{aligned} f(x) = -3 &\Leftrightarrow 2x^2 + 5x - 3 = -3 \\ &\Leftrightarrow 2x^2 + 5x = 0 \\ &\Leftrightarrow x(2x + 5) = 0 \\ &\Leftrightarrow (x = 0) \vee \left(x = -\tfrac{5}{2}\right), \end{aligned}$$

therefore,

$$f^{-1}(\{-3\}) = \left\{-\tfrac{5}{2}, 0\right\}.$$

**Calculate** $f([-2, 0])$ .

The set $f([-2, 0])$ is the set of all values $f(x)$ for $x \in [-2, 0]$.

$$f([-2, 0]) = \{f(x) / x \in [-2, 0]\}.$$

We can write $f(x)$ in the form

$$f(x) = 2x^2 + 5x - 3 = 2\left(x + \tfrac{5}{4}\right)^2 - \tfrac{49}{8}$$

$$\begin{aligned} x \in [-2, 0] \quad &\Leftrightarrow -\tfrac{3}{4} \leq x + \tfrac{5}{4} \leq \tfrac{5}{4} \\ &\Leftrightarrow 0 \leq \left(x + \tfrac{5}{4}\right)^2 \leq \tfrac{25}{16} \\ &\Leftrightarrow -\tfrac{49}{8} \leq f(x) \leq -\tfrac{24}{8}, \end{aligned}$$

so,

$$f([-2, 0]) = \left[-\tfrac{49}{8}, -\tfrac{24}{8}\right].$$

**Calculate** $f^{-1}([0, 1])$.

The set $f^{-1}([0, 1])$ is the set of all $x \in \mathbb{R}$ such that $f(x) \in [0, 1]$.

$$f^{-1}([0, 1]) = \{x \in E / f(x) \in [0, 1]\}.$$

$$\begin{aligned} f(x) \in [0, 1] \quad &\Leftrightarrow 0 \leq f(x) \leq 1 \\ &\Leftrightarrow 0 \leq 2\left(x + \tfrac{5}{4}\right)^2 - \tfrac{49}{8} \leq 1 \\ &\Leftrightarrow \tfrac{49}{16} \leq \left(x + \tfrac{5}{4}\right)^2 \leq \tfrac{57}{16} \\ &\Leftrightarrow x \in \left(]-\infty, -3] \cup \left[\tfrac{1}{2}, +\infty\right[\right) \cap \left(\left[-\sqrt{\tfrac{57}{16}} - \tfrac{5}{4}, \sqrt{\tfrac{57}{16}} - \tfrac{5}{4}\right]\right) \\ &\Leftrightarrow x \in \left[-\sqrt{\tfrac{57}{16}} - \tfrac{5}{4}, -3\right] \cup \left[\tfrac{1}{2}, \sqrt{\tfrac{57}{16}} - \tfrac{5}{4}\right], \end{aligned}$$

so,

$$f^{-1}([0, 1]) = \left[-\sqrt{\tfrac{57}{16}} - \tfrac{5}{4}, -3\right] \cup \left[\tfrac{1}{2}, \sqrt{\tfrac{57}{16}} - \tfrac{5}{4}\right].$$

**Proposition 2.5**

Let $A, B \subset E$ and $M, N \subset F$, Then :

1. $f(A \cup B) = f(A) \cup f(B)$.
2. $f(A \cap B) \subset f(A) \cup f(B)$.
3. $f^{-1}(M \cup N) = f^{-1}(M) \cup f^{-1}(N)$.
4. $f^{-1}(M \cap N) = f^{-1}(M) \cap f^{-1}(N)$.
5. $f^{-1}(C_F M) = C_E(f^{-1}(M))$.

**Proof.**

**1.** Let $y \in F$, then

$$\begin{aligned} y \in f(A \cup B) &\Leftrightarrow \exists x \in A \cup B, y = f(x) \\ &\Leftrightarrow \exists x ((x \in A \vee x \in B) \wedge (y = f(x))) \\ &\Leftrightarrow \exists x ((x \in A \wedge y = f(x)) \vee (x \in B \wedge y = f(x))) \\ &\Leftrightarrow (\exists x, (x \in A \wedge y = f(x))) \vee (\exists x, (x \in B \wedge y = f(x))) \\ &\Leftrightarrow (y \in f(A)) \vee (y \in f(B)) \\ &\Leftrightarrow y \in f(A) \cup f(B), \end{aligned}$$

so, $f(A \cup B) = f(A) \cup f(B)$.

**2.** Let $y \in F$, then

$$\begin{aligned} y \in f(A \cap B) &\Leftrightarrow \exists x \in A \cap B, y = f(x) \\ &\Leftrightarrow \exists x ((x \in A \wedge x \in B) \wedge (y = f(x))) \\ &\Leftrightarrow \exists x ((x \in A \wedge y = f(x)) \wedge (x \in B \wedge y = f(x))) \\ &\Rightarrow (\exists x, (x \in A \wedge y = f(x))) \wedge (\exists x, (x \in B \wedge y = f(x))) \\ &\Rightarrow (y \in f(A)) \wedge (y \in f(B)) \\ &\Rightarrow y \in f(A) \cap f(B), \end{aligned}$$

so, $f(A \cap B) \subset f(A) \cap f(B)$.

**3.** Let $x \in E$, then

$$\begin{aligned} x \in f^{-1}(M \cup N) &\Leftrightarrow f(x) \in M \cup N \\ &\Leftrightarrow (f(x) \in M) \vee (f(x) \in N) \\ &\Leftrightarrow (x \in f^{-1}(M)) \vee (x \in f^{-1}(N)) \\ &\Leftrightarrow x \in f^{-1}(M) \cup f^{-1}(N), \end{aligned}$$

so, $f^{-1}(M \cup N) = f^{-1}(M) \cup f^{-1}(N)$.

**4.** Let $x \in E$, then

$$\begin{aligned} x \in f^{-1}(M \cap N) &\Leftrightarrow f(x) \in M \cap N \\ &\Leftrightarrow (f(x) \in M) \wedge (f(x) \in N) \\ &\Leftrightarrow (x \in f^{-1}(M)) \wedge (x \in f^{-1}(N)) \\ &\Leftrightarrow x \in f^{-1}(M) \cap f^{-1}(N), \end{aligned}$$

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

**5.** Let $x \in E$, then

$$\begin{aligned} x \in f^{-1}(C_F M) &\Leftrightarrow f(x) \in C_F M \\ &\Leftrightarrow (f(x) \in F) \wedge (f(x) \notin M) \\ &\Leftrightarrow (x \in E) \wedge (x \notin f^{-1}(M)) \\ &\Leftrightarrow x \in C_E f^{-1}(M) \end{aligned}$$

so, $f^{-1}(C_F M) = C_E f^{-1}(M)$.

## 2.3 Exercises

**Exercise 2.1**

Let $A = \{n \in \mathbb{N} / n^2 - 3n \leq 2\}$ and $B = \{0, 1, 3, 5, 7\}$. Describe the sets $A \cap B$, $A \cup B$ and $A \times B$.

**Solution**

Describe the sets $A \cap B$, $A \cup B$ *and* $A \times B$

We have $A = \{n \in \mathbb{N} / n^2 - 3n \leq 2\} = \{0, 1, 2, 3\}$

**1.** $A \cap B$

$$\begin{aligned} A \cap B &= \{x / x \in A \text{ and } x \in B\} \\ &= \{0, 1, 3\} \end{aligned}$$

**2.** $A \cup B$

$$\begin{aligned} A \cup B &= \{x / x \in A \text{ or } x \in B\} \\ &= \{0, 1, 2, 3, 5, 7\} \end{aligned}$$

**3.** $A \times B$

$$\begin{aligned} A \times B &= \{(x,y)\,/x \in A \text{ and } y \in B\} \\ &= \{(0,0),(0,1),(0,3),(0,5),(0,7),(1,0),(1,1),(1,3),(1,5),(1,7), \\ &(2,0),(2,1),(2,3),(2,5),(2,7),(3,0),(3,1),(3,3),(3,5),(3,7)\} \end{aligned}$$

**Exercise 2.2**

Let $A, B$ tow parts of a set $E$. We suppose that

$$A \cap B \neq \varnothing, A \cup B \neq E, A \nsubseteq B, B \nsubseteq A$$

and

$$A_1 = A \cap B, A_2 = A \cap C_E^B, A_3 = B \cap C_E^A, A_4 = C_E^{A \cup B}.$$

Show that :

1. $A_1, A_2, A_3, A_4$ are non-empty.

2. $A_1, A_2, A_3, A_4$ are two by two disjoint.

3. $A_1 \cup A_2 \cup A_3 \cup A_4 = E$.

**Solution**

**1.** $A_1, A_2, A_3, A_4$ are non-empty. We have

$$A_1 = A \cap B \neq \varnothing, \quad \text{From the hypothesis}$$

$$A_2 = A \cap C_E^B = A \setminus B \neq \varnothing, \qquad \textit{because} \quad A \nsubseteq B.$$

$$A_3 = A \cap C_E^A = B \setminus A \neq \varnothing, \qquad \textit{because} \quad B \nsubseteq A.$$

$$A_4 = C_E^{A \cup B} = E \setminus (A \cup B) \neq \varnothing, \qquad \textit{because} \quad A \cup B \neq E.$$

**2.** $A_1, A_2, A_3, A_4$ are two by two disjoint.

We show that

$$A_i \cap A_j = \varnothing \quad \textit{with} \quad i \neq j \quad \textit{and} \quad i,j \in \{1,2,3,4\}$$

$$\begin{aligned} A_1 \cap A_2 &= (A \cap B) \cap \left(A \cap C_E^B\right) \\ &= A \cap B \cap A \cap C_E^B \\ &= (A \cap A) \cap \left(B \cap C_E^B\right) \\ &= A \cap \varnothing \\ &= \varnothing \end{aligned}$$

$$
\begin{aligned}
A_1 \cap A_3 &= (A \cap B) \cap \left(B \cap C_E^A\right) \\
&= A \cap B \cap B \cap C_E^A \\
&= (B \cap B) \cap \left(A \cap C_E^A\right) \\
&= B \cap \varnothing \\
&= \varnothing \\
A_1 \cap A_4 &= (A \cap B) \cap \left(C_E^{A \cup B}\right) \\
&= (A \cap B) \cap \left(C_E^A \cap C_E^B\right) \\
&= A \cap B \cap C_E^A \cap C_E^B \\
&= \left(A \cap C_E^A\right) \cap \left(B \cap C_E^B\right) \\
&= \varnothing \cap \varnothing \\
&= \varnothing \\
A_2 \cap A_3 &= \left(A \cap C_E^B\right) \cap \left(B \cap C_E^A\right) \\
&= A \cap C_E^B \cap B \cap C_E^A \\
&= \left(A \cap C_E^A\right) \cap \left(B \cap C_E^B\right) \\
&= \varnothing \cap \varnothing \\
&= \varnothing \\
A_2 \cap A_4 &= \left(A \cap C_E^B\right) \cap \left(C_E^{A \cup B}\right) \\
&= \left(A \cap C_E^B\right) \cap \left(C_E^A \cap C_E^B\right) \\
&= A \cap C_E^B \cap C_E^A \cap C_E^B \\
&= \left(A \cap C_E^A\right) \cap \left(C_E^B \cap C_E^B\right) \\
&= \varnothing \cap C_E^B \\
&= \varnothing
\end{aligned}
$$

$$\begin{aligned} A_3 \cap A_4 &= \left(B \cap C_E^A\right) \cap \left(C_E^{A\cup B}\right) \\ &= \left(B \cap C_E^A\right) \cap \left(C_E^A \cap C_E^B\right) \\ &= B \cap C_E^A \cap C_E^A \cap C_E^B \\ &= \left(B \cap C_E^B\right) \cap \left(C_E^A \cap C_E^A\right) \\ &= \varnothing \cap C_E^A \\ &= \varnothing \end{aligned}$$

**3.** $A_1 \cup A_2 \cup A_3 \cup A_4 = E$.

$$\begin{aligned} A_1 \cup A_2 \cup A_3 \cup A_4 &= (A \cap B) \cup \left(A \cap C_E^B\right) \cup \left(B \cap C_E^A\right) \cup \left(C_E^{A\cup B}\right) \\ &= (A \cap B) \cup \left(A \cap C_E^B\right) \cup \left(B \cap C_E^A\right) \cup \left(C_E^A \cap C_E^B\right) \\ &= \left[(A \cap B) \cup \left(A \cap C_E^B\right)\right] \cup \left[\left(B \cap C_E^A\right) \cup \left(C_E^A \cap C_E^B\right)\right] \\ &= \left[(A \cup A) \cap \left(A \cup C_E^B\right) \cap (B \cup A) \cap \left(B \cup C_E^B\right)\right] \\ &\quad \cup \left[\left(B \cup C_E^A\right) \cap \left(B \cup C_E^B\right) \cap \left(C_E^A \cup C_E^A\right) \cap \left(C_E^A \cup C_E^B\right)\right] \\ &= \left[A \cap \left(A \cup C_E^B\right) \cap (B \cup A) \cap E\right] \cup \left[\left(B \cup C_E^A\right) \cap E \cap C_E^A \cap \left(C_E^A \cup C_E^B\right)\right] \\ &= \left[A \cap \left(\left(A \cup C_E^B\right) \cap (B \cup A)\right)\right] \cup \left[C_E^A \cap \left(\left(B \cup C_E^A\right) \cap \left(C_E^A \cup C_E^B\right)\right)\right] \\ &= \left[A \cap \left(A \cup \left(B \cap C_E^B\right)\right)\right] \cup \left[C_E^A \cap \left(C_E^A \cup \left(B \cup C_E^B\right)\right)\right] \\ &= [A \cap (A \cup \varnothing)] \cup \left[C_E^A \cap \left(C_E^A \cup E\right)\right] \\ &= A \cup C_E^A \\ &= E \end{aligned}$$

**Exercice 2.3**

Let be the application $f : \mathbb{R} \to \mathbb{R}$, defined by

$$f(x) = x^2 + 3x + 2.$$

1. $f$ is-it injective ? surjective ?

2. Show that $f(\mathbb{R}) = \left[-\frac{1}{4}, +\infty\right[$.

3. Show that the restriction $g : \left[-\frac{3}{2}, +\infty\right[ \to \left[-\frac{1}{4}, +\infty\right[$, $g(x) = f(x)$ is bijective.

**Solution.**

**1.** $f$ **is-it injective ?** Let $a, b \in \mathbb{R}$, we have

$$\begin{aligned} f(a) = f(b) &\Rightarrow a^2 + 3a + 2 = b^2 + 3b + 2 \\ &\Rightarrow (a-b)(a+b) + 3(a-b) = 0 \\ &\Rightarrow (a-b)(a+b+3) = 0 \\ &\Rightarrow \begin{cases} a - b = 0 \\ a + b + 3 = 0 \end{cases} \end{aligned}$$

We can find two different elements have the same image. For example $a = -2, b = -1$, we have $f(a) = f(b) = 0$.

Then the application $f$ is note injective.

$f$ **is-it surjective ?** Let $y \in \mathbb{R}$, we have

$$\begin{aligned} y = f(x) &\Leftrightarrow y = x^2 + 3x + 2 \\ &\Leftrightarrow x^2 + 3x + 2 - y = 0 \end{aligned}$$

$$\Delta = (3)^2 - 4(1)(2 - y) = 1 + 4y.$$

If $y \in \left]-\infty, -\frac{1}{4}\right[$, the equation has no solutions, that's to say the element $y$ has no antecedent.

Then the application $f$ is note surjective.

**2. Show that** $f(\mathbb{R}) = \left[-\frac{1}{4}, +\infty\right[$.

We have,

$$f(\mathbb{R}) = \{f(x) / x \in \mathbb{R}\}.$$

The equation $y = f(x)$ has real solutions if and only if $\Delta = 1 + 4y \geq 0$, so there are solutions if and only if $y \in \left[-\frac{1}{4}, +\infty\right[$.

Thus,

$$f(\mathbb{R}) = \left[-\frac{1}{4}, +\infty\right[.$$

**3. Show that the restriction** $g : \left[-\frac{3}{2}, +\infty\right[ \to \left[-\frac{1}{4}, +\infty\right[$, $g(x) = f(x)$ **is bijective.**

Let $y \in [-1, 1]$, we are looking for a unique element $x \in \mathbb{R}$ such that $y = g(x)$.

If $y \in \left[-\frac{1}{4}, +\infty\right[$, so the possible solutions are

$$x = \frac{-3-\sqrt{1+4y}}{y} \notin \left[-\frac{3}{2}, +\infty\right[$$

or

$$x = \frac{-3+\sqrt{1+4y}}{y} \in \left[-\frac{3}{2}, +\infty\right[.$$

Then, for every real $y \geq -\frac{1}{4}$ there exists an unique real $x = \frac{-3+\sqrt{1+4y}}{y} \in \left[-\frac{3}{2}, +\infty\right[$ such that $y = g(x)$, so the application $g$ is bijective.

**Exercise 2.4**

Let $f$ be the application from $\mathbb{R}$ to $\mathbb{R}$ defined by : $f(x) = x^2 + 4x - 1$

1. Calculate $f^{-1}(\{-1\})$. Is the application $f$ bijective ?

2. Calculate $f([-1, 1])$ and $f^{-1}([0, 2])$.

**Solution**

**1. Calculate** $f^{-1}(\{-1\})$

The set $f^{-1}(\{-1\})$ is the set of all $x \in \mathbb{R}$ such that $f(x) = -1$.

$$f^{-1}(\{-1\}) = \{x \in \mathbb{R} / f(x) = -1\}.$$

Solving the equation $f(x) = -1$ :

$$\begin{aligned} f(x) = -1 &\Leftrightarrow x^2 + 4x - 1 = -1 \\ &\Leftrightarrow x^2 + 4x = 0 \\ &\Leftrightarrow x(x+4) = 0 \\ &\Leftrightarrow (x = 0) \vee (x = -4), \end{aligned}$$

Therefore,

$$f^{-1}(\{-1\}) = \{-4, 0\}.$$

**Is the application $f$ bijective ?**

We have $f(-4) = f(0) = -1$. Then there existe two different elements have the same image.

So, the application $f$ is note injective, which implies that $f$ is note bijective.

**2. Calculate** $f([-1, 1])$ .

The set $f([-1, 1])$ is the set of all values $f(x)$ for $x \in [-1, 1]$.

$$f([-1, 1]) = \{f(x) / x \in [-1, 1]\}.$$

We can write $f(x)$ in the form

$$f(x) = x^2 + 4x - 1 = (x+2)^2 - 5$$

$$\begin{aligned} x \in [-1,1] &\Leftrightarrow 1 \leq x+2 \leq 3 \\ &\Leftrightarrow 1 \leq (x+2)^2 \leq 9 \\ &\Leftrightarrow -4 \leq f(x) \leq 4, \end{aligned}$$

so,

$$f([-1,1]) = [-4,4].$$

**Calculate** $f^{-1}([0,2])$.

The set $f^{-1}([0,2])$ is the set of all $x \in \mathbb{R}$ such that $f(x) \in [0,2]$.

$$f^{-1}([0,2]) = \{x \in E / f(x) \in [0,2]\}.$$

$$\begin{aligned} f(x) \in [0,2] &\Leftrightarrow 0 \leq f(x) \leq 2 \\ &\Leftrightarrow 0 \leq (x+2)^2 - 5 \leq 2 \\ &\Leftrightarrow 5 \leq (x+2)^2 \leq 7 \\ &\Leftrightarrow x \in \left]-\infty, -\sqrt{5}-2\right] \cup \left[\sqrt{5}-2, +\infty\right[ \cap \left(\left[-\sqrt{7}-2, \sqrt{7}-2\right]\right) \\ &\Leftrightarrow x \in \left[-\sqrt{7}-2, -\sqrt{5}-2\right] \cup \left[\sqrt{5}-2, \sqrt{7}-2\right], \end{aligned}$$

so,

$$f^{-1}([0,2]) = \left[-\sqrt{7}-2, -\sqrt{5}-2\right] \cup \left[\sqrt{5}-2, \sqrt{7}-2\right].$$

## 2.4 Terminology translation

| **English** | **Frensh** |
|---|---|
| Set | Ensemble |
| Empty set | Ensemble vide |
| Element | Elément |
| Part | Partie |
| Complementary | Coplémentaire |
| Subset | Sous-ensemble |
| Cartesian product | Produit cartésien |
| Starting set | Enemble de départ |
| Arrival set | Ensemble d'arrivée |
| Strictly monotonic | Stéctement monotome |
| Strictly increasing | Strictement croissante |
| Strictly decreasing | Strictement décroissante |
| Direct image | Image directe |
| Reciprocal image | Image réciproque |

Chapitre 3

# Binary relation on a set

In this chapter, we present the binary relation on a set.

## 3.1 Definitions

**Definition 3.1**

Let $E$ and $F$ be two sets. A binary relation from $E$ to $F$ is a subset $\Re$ of $E \times F$ (or correspondence $\Re$ that links elements of $E$ to elements of $F$).

If $(x, y) \in \Re$ then we say that $x$ is related to $y$ and we denote it $x\Re y$.

In the case where $E = F$ we say that $\Re$ is defined on $E$.

We say that $A$ is the domain and $B$ is the codomain of the relation $\Re$.

**Example 3.1**

- The equality «=» is a relation on a set $E$.
- The inequality «$\leq$» is a relation on $\mathbb{N}, \mathbb{Z}$ or $\mathbb{R}$.
- The inclusion «$\subset$» is a relation on $P(X)$, where $X$ is any set.
- Let $E = \mathbb{Z}$. We define a relation $\Re$ on $\mathbb{Z}$ by :

$$\forall\, (x, y) \in \mathbb{Z}^2, x\Re y \Leftrightarrow x - y \textit{ is a multiple of } 5$$

Thus, $9\Re 4$ since 5 divides $9 - 4 = 5$. Note that 9 is not related to 3 since 5 does not divide $9 - 3 = 6$.

**Definition 3.2** (Graph of a Relation)

Let $\Re$ be a relation from a set $E$ to a set $F$. The graph of $\Re$ (denoted $\Gamma_{\Re}$) is the set defined

by :

$$\Gamma_{\Re} = \{(x, y) \in E \times F / x \Re y\}.$$

**Example 3.2**

We consider the relation «$\leq$» on the set $E = \{0, 1, 2, 3, 4\}$.

So, we have

$$\begin{aligned} \Gamma_{\Re} &= \{(x, y) \in E^2 / x \Re y\} \\ &= \{(0,0), (0,1), (0,2), (0,3), (0,4), \\ &\quad (1,1), (1,2), (1,3), (1,4), (2,2), \\ &\quad (2,3), (2,4), (3,3), (3,4), (4,4)\} \end{aligned}$$

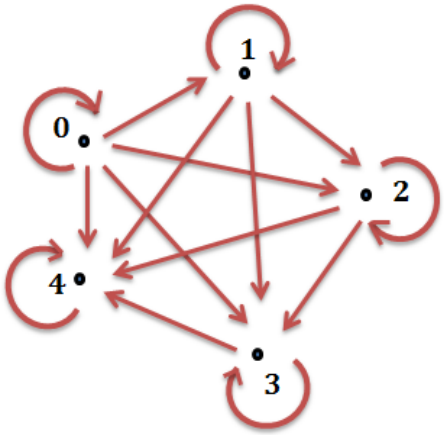



Fig 3.1 : Graph of the relation « $\leq$ »
on the set $E = \{0, 1, 2, 3, 4\}$

## 3.2 Properties of a binary relation on a set

### 3.2.1 Reflexive relation

**Definition 3.3.**

Let $\Re$ be a relation on a set $E$. $\Re$ is called reflexive if every element is related to itself.

$$\forall x \in E, x \Re x.$$

**Example 3.3**

- The inequality «$\leq$» on $\mathbb{N}, \mathbb{Z}$, or $\mathbb{R}$ is reflexive.

- The inequality «$<$» on $\mathbb{N}$ is not reflexive. Because we can find a natural number $x$ that is not related to itself.

### 3.2.2 Symmetric relation

**Definition 3.4**

Let $\Re$ be a relation on a set $E$. $\Re$ is called symmetric if

$$\forall x, y \in E, x\Re y \Rightarrow y\Re x.$$

**Example 3.4**

**-** The equality «=» on the set of integers $\mathbb{Z}$ is symmetric.

- The inequality «<» on $\mathbb{N}$ is not symmetric. Because we can find two natural integers $x, y$ such that $x$ is related to $y$ and $y$ is not related to $x$.

$$\exists\,(x, y) = (2, 3) \in \mathbb{N}^2, (2 < 3) \wedge (3 \not< 2)$$

### 3.2.3 Antisymmetric relation

**Definition 3.5**

Let $\Re$ be a relation on a set $E$. $\Re$ is called antisymmetric if

$$\forall x, y \in E, (x\Re y) \wedge (y\Re x) \Rightarrow x = y.$$

**Example 3.5**

**-** The inequality «$\leq$» on $\mathbb{N}, \mathbb{Z}$, or $\mathbb{R}$ is symmetric.

- We consider the binary relation $\Re$ defined on $\mathbb{Z}$ by :

$$\forall\,(a, b) \in \mathbb{Z}^2, a\Re b \Leftrightarrow |a| = |b|$$

$\Re$ is not antisymmetric. Because we can find two integers $a, b$ such that $a$ is related to $b$ and $b$ is related to $a$ but $a \neq b$.

$$\exists\,(a, b) = (2, -2) \in \mathbb{Z}^2, ((|2| = |-2|) \wedge (|-2| = |2|)) \wedge (2 \neq -2)\,.$$

### 3.2.4 Transitive relation

**Definition 3.6**

Let $\Re$ be a relation on a set $E$. $\Re$ is called transitve if

$$\forall x, y, z \in E, (x\Re y) \wedge (y\Re z) \Rightarrow x\Re z.$$

**Example 3.6**

- The equality «=» on the set of integers $\mathbb{Z}$ is transitive.

- The inequality «$\leq$» on $\mathbb{N}, \mathbb{Z}$, or $\mathbb{R}$ is transitive.

**Example 3.7**

We consider the relation «$\Re$» on the set $E = \{a, b, c\}$, such that

$$\Gamma_{\Re} = \{(a,a), (a,b), (a,c), (b,b), (b,a), (c,c), (c,a)\},$$

- $\Re$ is reflexive, because every element is related to itself.

$$\forall x \in E, x \Re x.$$

- $\Re$ is symmetric, because

$$\forall (x,y) \in E^2, (x \Re y) \Rightarrow (y \Re x).$$

- $\Re$ is not antisymmetric, because we can find two elements $x, y$ such that $x$ is related to $y$ and $y$ is related to $x$ but $x \neq y$.

$$\exists (x,y) = (a,b) \in E^2, ((a \Re b) \wedge (b \Re a)) \wedge (a \neq b)$$

- $\Re$ is not transitive, because we can find three elements $x, y, z$ such that $x$ is related to $y$ and $y$ is related to $z$ but $x$ is not related to $z$.

$$\exists (x,y,z) = (c,a,b) \in E^3, ((c \Re a) \wedge (a \Re b)) \wedge (c \textit{ is not related to } b).$$

## 3.3 Order relation

**Definition 3.7**

Let $\Re$ be a relation on a set $E$.

$\Re$ is called an order relation if $\Re$ is reflexive, antisymmetric and transitive.

**Example 3.8**

The inequality «$\leq$» on $\mathbb{N}, \mathbb{Z}$, or $\mathbb{R}$ is an order relation.

### 3.3.1 Total and partial order

**Definition 3.8**

Let $\Re$ be a relation on a set $E$.

1. Two elements $x$ and $y$ are said to be comparable by $\Re$, if $x\Re y$ or $y\Re x$.

2. We say that $\Re$ is a total order relation if all the elements of $E$ are pairwise comparable. Otherwise, we say that the relation is a partial order relation.

$\Re$ is called a total order relation if $\forall\,(x,y) \in E^2, x\Re y$ or $y\Re x$.

$\Re$ is called a partial order relation if $\exists\,(x,y) \in E^2$,($x$ is note related to $y$) and ( $y$ is note related to $x$).

**Example 3.9**. Let $E$ be a set and $X = \rho(E)$. We consider the following binary relation on $X$

$$\forall A, B \in X, A\Re B \Leftrightarrow A \subset B.$$

So, $\Re$ **is an order relation.**

(i). $\Re$ is reflexive, because for any set $A \in X$, we have

$$A \subset A \Rightarrow A\Re A.$$

(ii). $\Re$ is antisymmetric, because for all $A, B \in X$, we have

$$\begin{cases} A\Re B \\ \\ B\Re A \end{cases} \Leftrightarrow \begin{cases} A \subset B \\ \\ B \subset A \end{cases},$$

then, $A = B$.

(iii). $\Re$ is transitive, because for all $A, B, C \in X$, we have

$$\begin{cases} A\Re B \\ \\ B\Re C \end{cases} \Rightarrow \begin{cases} A \subset B \\ \\ B \subset C \end{cases}$$

$$\Rightarrow A \subset C$$

$$\Rightarrow A\Re C.$$

**Is the order total ?**

- If $E = \varnothing$, then $X = \{\varnothing\}$ and we have : $\forall A, B \in X, A = B = \varnothing$, so

$$\forall A, B \in X, A \subset B,$$

which shows that the order is total.

- If $E$ is a signgleton, then $E = \{a\}$ and $X = \{\varnothing, \{a\}\}$, for all $A, B \subset X$, we have

$$A = \varnothing \wedge A = \{a\} \quad \text{et} \quad B = \varnothing \wedge B = \{a\},$$

so,

$$\forall A, B \in X, A \subset B \vee B \subset A,$$

which shows that the order is total.

- If $E$ contains at least two distinct elements $a$ and $b$, then

$$\exists A = \{a\} \in X, B = \{b\} \in X, (A \subsetneq B) \text{ and } (B \subsetneq A),$$

which shows that the order is partial.

## 3.4 Equivalence relation

**Definition 3.9**

Let $\Re$ be a relation on a set $E$.

$\Re$ is called an equivalence relation if $\Re$ is reflexive, symmetric and transitive.

**Example 3.10**. Let $\delta$ be a binary relation defined on $\mathbb{R}$ by

$$\forall a, b \in \mathbb{R}, a\delta b \Leftrightarrow \cos^2(a) + \sin^2(b) = 1.$$

Show that $\delta$ is an equivalence relation.

(i). $\delta$ is reflexive, because for any real $a$, we have

$$\cos^2(a) + \sin^2(a) = 1 \Rightarrow a\delta a.$$

(ii). $\delta$ is symmetric, because for all $a, b \in \mathbb{R}$, we have

$$\begin{aligned} a\delta b &\Rightarrow \cos^2(a) + \sin^2(b) = 1 \\ &\Rightarrow \left(1 - \sin^2(a)\right) + \left(1 - \cos^2(b)\right) = 1 \\ &\Rightarrow -\sin^2(a) - \cos^2(b) + 2 = 1 \\ &\Rightarrow \cos^2(b) + \sin^2(a) = 1 \\ &\Rightarrow b\delta a. \end{aligned}$$

(iii). $\delta$ is transitive, because for all $a, b, c \in \mathbb{R}$, we have

$$\begin{cases} a\delta b \\ \\ b\delta c \end{cases} \Rightarrow \begin{cases} \cos^2(a) + \sin^2(b) = 1 \\ \\ \cos^2(b) + \sin^2(c) = 1 \end{cases}$$

$$\Rightarrow \left(\cos^2(a) + \sin^2(b)\right) + \left(\cos^2(b) + \sin^2(c)\right)) = 2$$

$$\Rightarrow \cos^2(a) + + \sin^2(c) + \left(\sin^2(b) + \cos^2(b)\right) = 2$$

$$\Rightarrow \cos^2(a) + + \sin^2(c) = 1$$

$$\Rightarrow a\delta c.$$

From (i), (ii) and (iii) we deduce that $\delta$ is an equivalence relation.

### 3.4.1 Equivalence class

**Definition 3.10**

- Let $\Re$ be an equivalence relation on a set $E$. Let $x \in E$, the equivalence class of $x$ is

$$Cl(x) = \dot{x} = \{y \in E / y\Re x\}.$$

- $Cl(x)$ is a subset of $E$.

- We call the quotient set of $E$ by the equivalence relation $\Re$, the set of equivalence classes of all the elements of $E$. This set is denoted $E/\Re$.

**Example 3.11**. In $\mathbb{R}$, we define the binary relation $\Re$ by :

$$\forall (x, y) \in E^2, x\Re y \Leftrightarrow x^2 - y^2 = x - y$$

Determine the equivalence class of $x \in \mathbb{R}$.

we can easily verify that $\Re$ is an equivalence relation.

Let $x \in \Re$, by definition of equivalence class, we have

$$\dot{x} = \{y \in \mathbb{R} / y\Re x\}$$

$$= \{y \in \mathbb{R} / y^2 - x^2 = y - x\}$$

$$= \{y \in \mathbb{R} / (y - x)(y + x - 1) = 0\}$$

- if $x = \frac{1}{2}$, then $\dot{x} = \left\{\frac{1}{2}\right\}$.

- if $x \neq \frac{1}{2}$, then $\dot{x} = \{x, 1-x\}$.

**Proposition 3.1**

Let $\Re$ be an equivalence relation on a set $E$. We have the following properties :

1. $\forall x \in E$

$$Cl\,(x) \neq \varnothing.$$

2.

$$Cl\,(x) = Cl\,(y) \Leftrightarrow x\Re y.$$

3. $\forall x, y \in E$

$$Cl\,(x) = Cl\,(y) \quad \text{ou} \quad Cl\,(x) \cap Cl\,(y) = \varnothing.$$

4. Let $F$ be a set of representatives of all classes then $\{Cl(x); x \in F\}$ constitutes a partition of $E$.

**Proof.**

**1.** Since $\Re$ is an equivalence relation, then $x\Re x$ ($\Re$ is reflexive). So, $x \in Cl(x)$, hence $Cl\,(x) \neq \varnothing$.

**2.**

($\Rightarrow$) Suppose that $Cl(x) = Cl(y)$

Let $z \in Cl(x)$, then $z \in Cl(y)$ and therefore $z\Re x$ and $z\Re y$, from the reflexivity and transitivity of $\Re$, we deduce that, $x\Re y$.

($\Leftarrow$) Suppose that $x\Re y$

We demonstrate that $Cl(x) \subset Cl(y)$

Let $z \in Cl\,(x)$, then $z\Re x$, by hypothesis we have $x\Re y$, and from the transitivity of $\Re$, we deduce that, $z\Re y$, so, $z \in Cl(y)$.

Then $Cl(x) \subset Cl(y)$.

In the same way we demonstrate that $Cl(y) \subset Cl(x)$.

**3.** Let $x, y \in E$, Suppose that $Cl\,(x) \cap Cl\,(y) \neq \varnothing$, then there exists $z \in Cl\,(x) \cap Cl\,(y)$, so $z\Re x$ and $z\Re y$.

Let's show that $Cl\,(x) = Cl\,(y)$

Let $t \in Cl\,(x)$, then

$$(t\Re x) \wedge (z\Re x) \wedge (z\Re y)\,,$$

from the reflexivity and transitivity of $\Re$, we deduce that,

$$(t\Re z) \wedge (z\Re y)\,,$$

and from the transitivity of $\Re$, we deduce that,

$$t\Re y,$$

so,

$$t \in Cl\,(y)\,,$$

then,

$$Cl\,(x) \subset Cl\,(y)\,.$$

In the same way we demonstrate that $Cl(y) \subset Cl(x)$.

**4.** Is a direct consequence of (1) and (3) : It must be shown that

(a) -

$$E = \underset{\dot{a_i} \in E/\Re}{\cup} \dot{a_i}$$

(b) -

$$\dot{a_i} \cap \dot{a_j} \;=\; \varnothing, \quad \forall i \neq j.$$

(a) is a consequence of (1). The equivalence classes of $E$ are all non-empty (every element of $E$ belongs to an equivalence class).

(b) is a consequence of (3). Two equivalence classes are either the same or disjoint.

## 3.5 Congruences

**Definition 3.11**

Let $n$ be a non-zero natural number. We say that two relative integers $a$ and $b$ are congruent modulo $n$, or that $a$ is congruent to $b$ modulo $n$ if $n$ divides $a - b$. We denote by $a \equiv b\ mod\ n$ or $a \equiv b[n]$.

**Example 3.12**

- $2025 \equiv 87[17]$. $2025 - 87 = 1938 = 17 \times 14$.

- $421 \equiv 16[5]$. $421 - 16 = 405 = 5 \times 81$.

**Proposition 3.2**

The congruence relation modulo $n$ is an equivalence relation.

**Proof.**

Let $n$ be a non-zero natural integer and $a, b, c \in \mathbb{Z}$. We have :

(i).

$$a - a = 0 = 0 \times n \Rightarrow a \Re a,$$

so, $\Re$ is reflexive.

(ii).

$$\begin{aligned} a \Re b &\Rightarrow a \equiv b[n] \\ &\Rightarrow a - b = nk, \ with \ k \in \mathbb{Z} \\ &\Rightarrow b - a = nk', \ with \ k' = -k \in \mathbb{Z} \\ &\Rightarrow b \equiv a[n] \Rightarrow b \Re a, \end{aligned}$$

so, $\Re$ is symmetric.

(iii).

$$\begin{aligned} \begin{cases} a \Re b \\ b \Re c \end{cases} &\Rightarrow \begin{cases} a \equiv b[n] \\ b \equiv c[n] \end{cases} \\ &\Rightarrow \begin{cases} a - b = nk_1 \\ b - c = nk_2 \end{cases} , with \ k_1, k_2 \in \mathbb{Z} \\ &\Rightarrow (a - b) + (b - c) = (nk_1) + (nk_1) \\ &\Rightarrow a - c = n(k_1 + k_2) \\ &\Rightarrow a - c = nk_3, with \ k_3 = k_1 + k_2 \in \mathbb{Z} \\ &\Rightarrow a \equiv c[n] \Rightarrow a \Re c, \end{aligned}$$

so, $\Re$ is transitive.

From (i), (ii) and (iii) we deduce that $\Re$ is an equivalence relation.

**Proposition 3.3**

$a \equiv b[n]$ if and only if $a$ and $b$ have the same rest in Euclidean division by $n$.

**Proof**

Let $(q_1, r_1)$ and $(q_2, r_2)$ be the two unique elements of $\mathbb{Z} \times \mathbb{N}$, such that

$$a = nq_1 + r_1 \text{ and } b = nq_2 + r_2 \ ,$$

with $0 \leq r_1, r_2 < n$.

Then,

$$a - b = n \times (q_1 - q_2) + (r_1 - r_2) \, ,$$

$$a - b \in n\mathbb{Z} \Leftrightarrow r_1 - r_2 \in n\mathbb{Z}$$

we have

$$-n < r_1 - r_2 < n \quad \text{and} \quad ]-n, n[ \cap n\mathbb{Z} = \{0\} \, ,$$

so,

$$r_1 = r_2.$$

**Proposition 3.4**

Let $n$ be a non-zero natural integer and $a, b, c, d \in \mathbb{Z}$.

1. If $a \equiv b[n]$ and $c \equiv d[n]$, then

$$a + c \equiv b + d[n], \ a - c \equiv b - d[n], \ a \times c \equiv b \times d[n]$$

$$a^k \equiv b^k[n], \ \text{with } k \in \mathbb{N}^*.$$

2. If $a \equiv b[n]$, then for all $p \in \mathbb{Z}$

$$a + p \equiv b + p[n], \quad a - p \equiv b - p[n], \ a \times p \equiv b \times p[n]$$

## 3.6 The set $\mathbb{Z}/n\mathbb{Z}$

For any integer $n \geq 2$ ; $\mathbb{Z}/n\mathbb{Z}$ is the quotient set of $\mathbb{Z}$ by the congruence relation modulo $n$.

We have :

$$\mathbb{Z}/n\mathbb{Z} = \left\{ \dot{0}, \dot{1}, \dot{2}, ..., \widehat{\dot{n-1}} \right\},$$

where $\dot{x}$ is the class of $x$, that is, the set of numbers whose Euclidean division by $n$ has the rest $x$.

**Example 3.13**

- For $n = 2$, we have

$$\mathbb{Z}/2\mathbb{Z} = \left\{\dot{0}, \dot{1}\right\},$$

with $\dot{0} = \{\text{even number}\}$ and $\dot{1} = \{\text{odd number}\}$.

- For $n = 4$, we have

$$\mathbb{Z}/4\mathbb{Z} = \left\{\dot{0}, \dot{1}, \dot{2}, \dot{3}\right\}.$$

**Operations**

We will define a sum operation denoted by $\dot{+}$ and a multiplication operation denoted by $\dot{\times}$ on $\mathbb{Z}/n\mathbb{Z}$ as follows :

$$\dot{a} \ \dot{+} \ \dot{b} \ = \ \widehat{a + b}$$

$$\dot{a} \ \dot{\times} \ \dot{b} \ = \ \widehat{a \times b}$$

**Example 3.14**

Some calculations in $\mathbb{Z}/12\mathbb{Z}$

-

$$\dot{10} \ \dot{+} \ \dot{8} \ = \ \widehat{10 + 8} \ = \ \dot{18} \ = \ \dot{6}, \ \ \dot{5} \ \dot{\times} \ \dot{7} \ = \ \widehat{5 \times 7} \ = \ \dot{35} \ = \ \dot{11},$$

-

$$\dot{10} \ \dot{+} \ \dot{2} \ = \ \widehat{10 + 2} \ = \ \dot{12} \ = \ \dot{0},$$

we say that $\dot{10}$ is the opposite of $\dot{2}$ and that $\dot{2}$ is the opposite of $\dot{10}$.

-

$$\dot{5} \ \dot{\times} \ \dot{5} \ = \ \widehat{5 \times 5} \ = \ \dot{25} \ = \ \dot{1},$$

we say that $\dot{5}$ is the inverse of itself.

-

$$\dot{4} \ \dot{\times} \ \dot{3} \ = \ \dot{12} \ = \ \dot{0},$$

we say that $\dot{4}$ and $\dot{3}$ are divisors of zeros.

**Example 3.15**

The sum operation $\dot{+}$ and the multiplication operation $\dot{\times}$ on $\mathbb{Z}/7\mathbb{Z}$

| $\dot{+}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ | $\dot{6}$ |
|---|---|---|---|---|---|---|---|
| $\dot{0}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ | $\dot{6}$ |
| $\dot{1}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ | $\dot{6}$ | $\dot{0}$ |
| $\dot{2}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ | $\dot{6}$ | $\dot{0}$ | $\dot{1}$ |
| $\dot{3}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ | $\dot{6}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ |
| $\dot{4}$ | $\dot{4}$ | $\dot{5}$ | $\dot{6}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ |
| $\dot{5}$ | $\dot{5}$ | $\dot{6}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ |
| $\dot{6}$ | $\dot{6}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ |

Tab 3.1 : Sum operation on $\mathbb{Z}/7\mathbb{Z}$

| $\dot{\times}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ | $\dot{6}$ |
|---|---|---|---|---|---|---|---|
| $\dot{0}$ | $\dot{0}$ | $\dot{0}$ | $\dot{0}$ | $\dot{0}$ | $\dot{0}$ | $\dot{0}$ | $\dot{0}$ |
| $\dot{1}$ | $\dot{0}$ | $\dot{1}$ | $\dot{2}$ | $\dot{3}$ | $\dot{4}$ | $\dot{5}$ | $\dot{6}$ |
| $\dot{2}$ | $\dot{0}$ | $\dot{2}$ | $\dot{4}$ | $\dot{6}$ | $\dot{1}$ | $\dot{3}$ | $\dot{5}$ |
| $\dot{3}$ | $\dot{0}$ | $\dot{3}$ | $\dot{6}$ | $\dot{2}$ | $\dot{5}$ | $\dot{1}$ | $\dot{2}$ |
| $\dot{4}$ | $\dot{0}$ | $\dot{4}$ | $\dot{1}$ | $\dot{5}$ | $\dot{2}$ | $\dot{6}$ | $\dot{3}$ |
| $\dot{5}$ | $\dot{0}$ | $\dot{5}$ | $\dot{3}$ | $\dot{1}$ | $\dot{6}$ | $\dot{4}$ | $\dot{2}$ |
| $\dot{6}$ | $\dot{0}$ | $\dot{6}$ | $\dot{5}$ | $\dot{4}$ | $\dot{3}$ | $\dot{2}$ | $\dot{1}$ |

Tab 3.2 : Multiplication operation on $\mathbb{Z}/7\mathbb{Z}$

## 3.7 Exercises

**Exercise 3.1**

Let $\Re$ be the binary relation on $E = \{0, 1, 2, 3, 4\}$ defined by

$$x \Re y \Leftrightarrow 2x - y \in \mathbb{N}$$

1. Determine $\Gamma_{\Re}$ graph of $\Re$.

2. Is $\Re$ reflexive ? symmetric ? Antisymmetric ? Transitive ?

**Solution**

**1. Determine $\Gamma_{\Re}$ graph of $\Re$.**

$$\begin{aligned}
\Gamma_{\Re} &= \{(x, y) \in E^2 / x \Re y\} \\
&= \left\{(x, y) \in E^2 / \tfrac{x+5y}{6} \in \mathbb{N}\right\} \\
&= \begin{array}{l} \{(0,0), (1,0), (1,1), (1,2), (2,0), (2,1), \\ (2,2), (2,3), (2,4), (3,0), (3,1), (3,2) \\ , (3,3), (3,4), (4,0), (4,1), (4,2), (4,3), (4,4)\} \end{array}
\end{aligned}$$

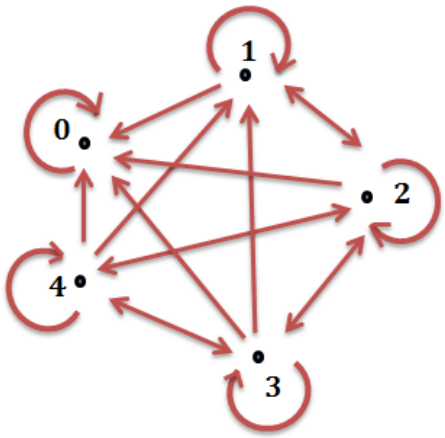



Fig 3.2 : Graph of the relation «$\Re$»
on the set $E$.

**2. Is $\Re$ reflexive ? symmetric ? Antisymmetric ? Transitive ?**

- $\Re$ is reflexive, because every element is related to itself.

$$\forall x \in E, 2x - x = x \in \mathbb{N}, \text{ so } x\Re x.$$

- $\Re$ is note symmetric, because we can find two elements $x, y$ such that $x$ is related to $y$ and $y$ is note related to $x$

$$\exists\,(x, y) = (1, 0) \in E^2, (1\Re 0) \text{ but } 0 \text{ is note related to } 1.$$

- $\Re$ is not antisymmetric, because we can find two elements $x, y$ such that $x$ is related to $y$ and $y$ is related to $x$ but $x \neq y$.

$$\exists\,(x, y) = (2, 3) \in E^2, ((2\Re 3) \wedge (3\Re 2)) \wedge (2 \neq 3)$$

- $\Re$ is not transitive, because we can find three elements $x, y, z$ such that $x$ is related to $y$ and $y$ is related to $z$ but $x$ is not related to $z$.

$$\exists\,(x, y, z) = (1, 2, 3) \in E^3, ((1\Re 2) \wedge (2\Re 3)) \wedge (1 \text{ is not related to } 3)\,.$$

**Exercise 3.2**

In $\mathbb{R}$, we define the binary relation $\Re$ by :

$$\forall\,(x,y)\in E^2, x\Re y \Leftrightarrow x^3-y^3=x^2-y^2$$

Show that $\Re$ is an equivalence relation and determine the equivalence class of $x\in\mathbb{R}$.

**Solution**

**1. Show that $\Re$ is an equivalence relation :**

Let $x,y,z\in\mathbb{R}$, we have

(i).

$$x^3-x^3=0=x^2-x^2\Rightarrow x\Re x,$$

so, $\Re$ is reflexive.

(ii).

$$\begin{aligned} x\Re y &\Rightarrow x^3-y^3=x^2-y^2\\ &\Rightarrow (x^3-y^3)\times(-1)=(x^2-y^2)\times(-1)\\ &\Rightarrow y^3-x^3=y^2-x^2\\ &\Rightarrow y\Re x, \end{aligned}$$

so, $\Re$ is symmetric.

(iii).

$$\begin{aligned} \left\{\begin{array}{l} x\Re y\\ y\Re z \end{array}\right. &\Rightarrow \left\{\begin{array}{l} x^3-y^3=x^2-y^2\\ y^3-z^3=y^2-z^2 \end{array}\right.\\ &\Rightarrow (x^3-y^3)+(y^3-z^3)=(x^2-y^2)+(y^2-z^2)\\ &\Rightarrow x^3-z^3=x^2-z^2\\ &\Rightarrow x\Re z, \end{aligned}$$

so, $\Re$ is transitive.

From (i), (ii) and (iii) we deduce that $\Re$ is an equivalence relation.

**2. Determine the equivalence class of $x\in\mathbb{R}$**

Let $x\in\mathbb{R}$, we have

$$\dot{x} \;=\; \{y\in\mathbb{R}/y\Re x\} \;=\; \{y\in\mathbb{R}/y^3-x^3=y^2-x^2\}$$

$$\begin{aligned} y^3 - x^3 = y^2 - x^2 &\Leftrightarrow (y^3 - x^3) - (y^2 - x^2) = 0 \\ &\Leftrightarrow (y-x)(y^2 + yx + x^2) - (x-y)(x+y) = 0 \\ &\Leftrightarrow (y-x)(y^2 + yx + x^2 - x - y) = 0 \\ &\Leftrightarrow \begin{cases} y - x = 0 \\ y^2 + (x-1)y + x^2 - x = 0 \end{cases} \end{aligned}$$

We solve the second equation.

If $x \in ]-\frac{1}{3}, 1[$, the equation has two solutions

$$y = \frac{1-x-\sqrt{1+2x-3x^2}}{2} \quad \text{or} \quad y = \frac{1-x+\sqrt{1+2x-3x^2}}{2}$$

If $x = 1$, the equation has one solution

$$y = 0.$$

If $x = -\frac{1}{3}$, the equation has one solution

$$y = \frac{4}{3}.$$

If $x \in ]-\infty, -\frac{1}{3}[\cup]1, +\infty[$, the equation has no solutions.

So,

$$\dot{x} = \begin{cases} \left\{x, \frac{1-x-\sqrt{1+2x-3x^2}}{2}, \frac{1-x+\sqrt{1+2x-3x^2}}{2}\right\} \ \textit{if} \quad x \in ]-\frac{1}{3}, 1[ \\ \{0, 1\} \ \textit{if} \quad x = 1 \\ \left\{-\frac{1}{3}, \frac{4}{3}\right\} \ \textit{if} \quad x = -\frac{1}{3} \\ \{x\} \ \textit{if} \quad x \in ]-\infty, -\frac{1}{3}[\cup]1, +\infty[ \end{cases}$$

**Exercise 3.3**

In $\mathbb{Z}$, we define the binary relation $\Re$ by :

$$\forall (x, y) \in \mathbb{Z}^2, x \Re y \Leftrightarrow x - y \textit{ is multiple of } 6$$

1. Show that $\Re$ is an equivalence relation.

2. Determine the quotient set $\mathbb{Z}/\Re$.

3. Show that $\dot{\widehat{49}} = \dot{\widehat{25}}$ and $\dot{\widehat{57}} \cap \dot{\widehat{17}} = \varnothing$.

**Solution**

**1. Show that $\Re$ is an equivalence relation.**

Let $x, y, z \in \mathbb{Z}$, we have

(i).

$$x - x = 0 = 0 \times 6 \Rightarrow x \Re x,$$

so, $\Re$ is reflexive.

(ii).

$$\begin{aligned} x \Re y &\Rightarrow x - y = 6k, \textit{ with } k \in \mathbb{Z} \\ &\Rightarrow y - x = 6k', \textit{ with } k' = -k \in \mathbb{Z} \\ &\Rightarrow y \Re x, \end{aligned}$$

so, $\Re$ is symmetric.

(iii).

$$\begin{aligned} \begin{cases} x \Re y \\ y \Re z \end{cases} &\Rightarrow \begin{cases} x - y = 6k_1 \\ y - z = 6k_2 \end{cases} \\ &\Rightarrow (x - y) + (y - z) = 6k_1 + 6k_2 \\ &\Rightarrow x - z = 6k_3, \ \ \textit{with } k_3 = k_1 + k_2 \in \mathbb{Z} \\ &\Rightarrow x \Re z, \end{aligned}$$

so, $\Re$ is transitive.

From (i), (ii) and (iii) we deduce that $\Re$ is an equivalence relation.

**2. Determine the quotient set $\mathbb{Z}/\Re$.**

We know that $\mathbb{Z}/\Re$ is the set of equivalence classes of all elements of $\mathbb{Z}$. And since $\Re$ is the congruence relation, then

$$\mathbb{Z}/6\mathbb{Z} = \left\{ \dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5} \right\}.$$

**3. Show that $\dot{\widehat{49}} = \dot{\widehat{25}}$ and $\dot{\widehat{57}} \cap \dot{\widehat{17}} = \varnothing$.**

We know that two equivalence classes are either the same or disjoint. We have

$$49 - 25 = 24 = 6 \times 4,$$

which implies

$$49 \Re 25,$$

so,

$$\dot{\widehat{49}} \ = \ \dot{\widehat{25}}$$

And

$$57 - 17 = 40 = 6 \times 6 + 4,$$

which implies

$$57 \textit{ is note related to } 17,$$

so,

$$\dot{\widehat{57}} \cap \dot{\widehat{17}} = \varnothing.$$

**Exercise 3.4**

In $\mathbb{R}^2$, we define the binary relation $\Re$ by :

$$\forall (x,y), \left(x^{'}, y^{'}\right) \in \mathbb{R}^2, (x,y) \Re \left(x^{'}, y^{'}\right) \Leftrightarrow \left(x \leq x^{'}\right) \textit{ and } \left(y \leq y^{'}\right)$$

1. Show that $\Re$ is an order relation.

2. Is the order total ?

**Solution**

**1. Show that $\Re$ is an order relation.**

Let $(x,y), \left(x^{'}, y^{'}\right), \left(x^{"}, y^{"}\right) \in \mathbb{R}^2$, we have

(i).

$$(x \leq x) \textit{ and } (y \leq y) \Rightarrow (x,y) \Re (x,y),$$

so, $\Re$ is reflexive.

(ii).

$$\begin{cases} (x,y) \Re \left(x^{'}, y^{'}\right) \\ \left(x^{'}, y^{'}\right) \Re (x,y) \end{cases} \Rightarrow \begin{cases} \left(x \leq x^{'}\right) \textit{ and } \left(y \leq y^{'}\right) \\ \left(x^{'} \leq x\right) \textit{ and } \left(y^{'} \leq y\right) \end{cases}$$

$$\Rightarrow \left(x = x^{'}\right) \textit{ and } \left(y = y^{'}\right)$$

$$\Rightarrow (x,y) = \left(x^{'}, y^{'}\right),$$

so, $\Re$ is antisymmetric.

(iii).

$$\begin{cases} (x,y)\,\Re\left(x^{'},y^{'}\right) \\ \left(x^{'},y^{'}\right)\Re\left(x^{"},y^{"}\right) \end{cases} \Rightarrow \begin{cases} \left(x \leq x^{'}\right) \ \textit{and} \ \left(y \leq y^{'}\right) \\ \left(x^{'} \leq x^{"}\right) \ \textit{and} \ \left(y^{'} \leq y^{"}\right) \end{cases}$$

$$\Rightarrow \left(x \leq x^{"}\right) \ \textit{and} \ \left(y \leq y^{"}\right)$$

$$\Rightarrow (x,y)\,\Re\left(x^{"},y^{"}\right)$$

so, $\Re$ is transitive.

From (i), (ii) and (iii) we deduce that $\Re$ is an equivalence relation.

**2. Is the order total ?**

Let $(x,y)=(3,5)\,,\left(x^{'},y^{'}\right)=(1,7)\in\mathbb{R}^2$. We have

$$(3,5) \ \textit{is note related to} \ (1,7)\,,$$

and

$$(1,7) \ \textit{is note related to} \ (3,5)\,,$$

we deduce that the order is partial.

**Exercise 3.5**

In $\mathbb{R}_{+}^{*}$, we define the binary relation $T$ by :

$$\forall x,y\in\mathbb{R}_{+}^{*}, x\Re y \Leftrightarrow \exists n\in\mathbb{N}, y=x^{n},$$

1. Show that $T$ is an order relation.

2. Is the order total ?

**Solution**

**1. Show that $T$ is an order relation.**

Let $x,y,z\in\mathbb{R}_{+}^{*}$, we have

(i).

$$x=x^{1}\Rightarrow\exists n=1\in\mathbb{N}, x=x^{n}\Rightarrow xTx,$$

so, $T$ is reflexive.

(ii).

$$\begin{cases} xTy \\ \\ yTx \end{cases} \Rightarrow \begin{cases} \exists n_1 \in \mathbb{N}, y = x^{n_1} \\ \\ \exists n_2 \in \mathbb{N}, x = y^{n_2} \end{cases}$$

$$\Rightarrow y = x^{n_1} = (y^{n_2})^{n_1}$$

$$\Rightarrow y = y^{n_2 \times n_1} \Rightarrow n_2 \times n_1 = 1 \Rightarrow n_2 = n_1 = 1$$

$$\Rightarrow x = y,$$

so, $T$ is antisymmetric.

(iii).

$$\begin{cases} xTy \\ \\ yTz \end{cases} \Rightarrow \begin{cases} \exists n_1 \in \mathbb{N}, y = x^{n_1} \\ \\ \exists n_2 \in \mathbb{N}, z = y^{n_2} \end{cases}$$

$$\Rightarrow z = y^{n_2} = \left(x^{n_1}\right)^{n_2} = x^{n_1 \times n_2}$$

$$\Rightarrow \exists n_3 = n_1 \times n_2 \in \mathbb{N}, z = x^{n_3}$$

$$\Rightarrow xTz,$$

so, $\Re$ is transitive.

From (i), (ii) and (iii) we deduce that $\Re$ is an equivalence relation.

**2. Is the order total ?**

Let $(x, y) = (7, 4) \in \mathbb{R}_+^* \times \mathbb{R}_+^*$. We have

$$7 \textit{ is note related to } 4,$$

and

$$4 \textit{ is note related to } 7,$$

we deduce that the order is partial.

## 3.8 Terminology translation

| **English** | **Frensh** |
|---|---|
| Binary relation | Relation binaire |
| Order relation | Relation d'ordre |
| Inequality | Inégalité |
| Partial order | Ordre partiel |
| Total order | Ordre total |
| Pairwise comparable | Comparables deux à deux |
| Equivalence class | Classe d'équivalence |
| Quotient set | Ensemble quotient |
| Euclidean division | Division euclidienne |

Chapitre 4

# Algebraic structures

In this chapter, we present the algebraic structures.

## 4.1 Law of internal composition

**Definition 4.1**

Let $E$ be a non-empty set.

- A law of internal composition on $E$ is an application $*$ from $E \times E$ to $E$.

$$\begin{array}{rccc} * : & E \times E & \to & E \\ & (x, y) & \mapsto & x * y \end{array}$$

- The internal composition law can be noted by $*, \Delta, \oplus, ...$, or other symbols.

**Example 4.1**

- The composition laws defined by addition $(+)$ and multiplication $(\times)$ on the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are internal laws.

- Let $E$ be any set. Let $X, Y \in P(E)$, the composition law $(X, Y) \to X \cup Y$ is an internal law on $P(E)$.

- Let $*$ be defined on $\mathbb{R}$ :

$$x * y = \frac{1}{x+y+1},$$

Then $*$ is not an internal composition law, because $(0, -1) \in \mathbb{R} \times \mathbb{R}$ does not have a defined image.

### 4.1.1 Stability

**Definition 4.2**

Let be $*$ an internal composition law in a set $E$.

A subset $F$ of $E$ is said to be stable for this internal law if and only if

$$\forall x, y \in F, x * y \in F.$$

### 4.1.2 Properties of an internal composition law

### 4.1.3 Associativity

**Definition 4.3**

Let $*$ be an internal composition laws in a set $E$. We say that $*$ is associative if and only if

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

**Example 4.2**. Let $*$ be an internal composition law defined on $\mathbb{R}$ by

$$x * y = x + y - xy.$$

Let $x, y, z \in \mathbb{R}$, we have

$$\begin{aligned} x * \underbrace{(y * z)}_{a} &= x + a - xa \\ &= x + (y + z - yz) - x(y + z - yz) \\ &= x + y + z - yz - xy - xz + xyz \quad .....(1), \end{aligned}$$

and

$$\begin{aligned} \underbrace{(x * y)}_{b} * z &= b + z - bz \\ &= (x + y - xy) + z - (x + y - xy)\, z \\ &= x + y + z - xy - xz - yz + xyz \quad .....(2), \end{aligned}$$

when (1) = (2), then $*$ is associative.

### 4.1.4 Commutativity

**Definition 4.4**

Let $*$ be an internal composition laws in a set $E$. We say that $*$ is commutative if and only if

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

**Example 4.3**. Let $*$ be an internal composition law defined on $\mathbb{R}$ by

$$x * y = x + y - xy.$$

Let $x, y \in \mathbb{R}$, we have

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

so, $*$ is commutative.

### 4.1.5 Neutral element

**Definition 4.5**

Let $*$ be an internal composition laws in a set $E$.

The law $*$ admits a neutral element (noted $e$) on $E$, if and only if

$$\exists e \in E, \forall x \in E, x * e = e * x = e.$$

**Remark 4.1**

The neutral element, when it exists, is unique.

Indeed, suppose that $e^{'}$ is another neutral element for the law $*$, then $e^{'} = e^{'} * e = e * e^{'} = e$.

**Example 4.4**

Let $*$ be an internal composition law defined on $\mathbb{R} - \{1\}$ by

$$x * y = x + y - xy.$$

Let $x \in \mathbb{R} - \{1\}$, we have

$$\begin{aligned} x * e = x &\Leftrightarrow x + e - xe = x \\ &\Leftrightarrow e\,(1 - x) = 0, \\ &\Leftrightarrow e = 0, \ \textit{because } x \neq 1, \end{aligned}$$

and

$$\begin{aligned} e * x = x &\Leftrightarrow e + x - ex = x \\ &\Leftrightarrow e\,(1 - x) = 0, \\ &\Leftrightarrow e = 0, \ \textit{because } x \neq 1, \end{aligned}$$

then, $e = 1$ is a neutral element.

### 4.1.6 Symmetric element

**Definition 4.6**

Let $*$ be an internal composition laws in a set $E$.

The element $x$ of $E$ is said to be invertible (or symmetrizable) for the law $*$ if the law $*$ admits a neutral element $e$ and if there exists an element $x^{'}$ in $E$ such that

$$x * x^{'} = x^{'} * x = e.$$

**Remark 4.2**

The symmetric $x^{'}$ of $x \in E$ is unique for the law $*$ .

Indeed, let $x^{"}$ be a second symmetric element of $x$. Using the associativity of the law $*$, we obtain

$$x^{'} = e * x^{'} = \left(x^{"} * x\right) * x^{'} = x^{"} * \left(x * x^{'}\right) = x^{"} * e = x^{"}.$$

**Example 4.5**

Let $*$ be an internal composition law defined on $\mathbb{R} - \{1\}$ by

$$x * y = x + y - xy.$$

Let $x \in \mathbb{R} - \{1\}$ , we have

$$\begin{aligned} x * x^{'} = e &\Leftrightarrow x + x^{'} - xx^{'} = 0 \\ &\Leftrightarrow x^{'}\,(1 - x) = -x, \\ &\Leftrightarrow x^{'} = -\tfrac{x}{1-x}, \ \textit{because } x \neq 1, \end{aligned}$$

and

$$x^{'} * x = x \Leftrightarrow x^{'} + x - x^{'}x = 0$$

$$\Leftrightarrow x^{'}(1-x) = -x,$$

$$\Leftrightarrow x^{'} = -\frac{x}{1-x},\ \textit{because}\ x \neq 1.$$

$x^{'} = -\frac{x}{1-x} \in \mathbb{R} - \{1\}$?

Suppose that, $x^{'} = -\frac{x}{1-x} = 1$

$$x^{'} = -\frac{x}{1-x} = 1 \Leftrightarrow -x = 1 - x \Leftrightarrow 0 = -1,$$

This is a contradiction. Therefore, $x^{'} \neq 1$.

Then $x^{'} = -\frac{x}{1-x}$ is a symmertic element.

### 4.1.7 Distributivity

**Definition 4.7**

Let $*$ and $\Delta$ be two internal composition laws in a set $E$.

We say that the law $*$ is distributive with respect to the law $\Delta$ if

$$\forall x, y, z \in E, x * (y \Delta z) = (x * y) \Delta (x * z)\ \ \textit{and}\ \ (y \Delta z) * x = (y * x) \Delta (z * x).$$

## 4.2 Groups

**Definition 4.8**

Let $*$ bean internal composition laws in a set $G$.

We say that $(G, *)$ is a group if

(a) The law $*$ is associative on $G$.

(b) There exists a neutral element $e \in G$.

(c) Every element of $G$ is symmetrizable for the law $*$.

We also say that the set $G$ has a group structure for the operation $*$.

And if in addition $*$ is commutative, we say that $(G, *)$ is an abelian (or commutative) group.

**Exemple 4.6**

*Let* $E = ]-1, 1[$. We define on $E$ the law $*$ by

$$\forall a, b \in E,\ a * b = \tfrac{a+b}{1+ab}.$$

Show that $(E, *)$ is an abelian group.

**(a).** Show that $*$ is internal

$$\forall a, b \in E,\ a * b \in E.$$

Let $a, b \in E$, we have :

$$\begin{aligned} a, b \in E &\Rightarrow |ab| < 1 \\ &\Rightarrow 1 + ab > 0, \end{aligned}$$

so,

$$\begin{aligned} a * b \in E &\Leftrightarrow -1 < \tfrac{a+b}{1+ab} < 1 \\ &\Leftrightarrow \left|\tfrac{a+b}{1+ab}\right| < 1 \\ &\Leftrightarrow |a + b| < |1 + ab| = 1 + ab \\ &\Leftrightarrow |a + b| - 1 - ab < 0 \end{aligned}$$

First case : if $a + b \leq 0$, then

$$\begin{aligned} |a + b| - 1 - ab &= -a - b - 1 - ab \\ &= -a\,(1 + b) - (1 + b) \\ &= -\,(1 + a)\,(1 + b) < 0. \end{aligned}$$

Second case : if $a + b \geq 0$, then

$$\begin{aligned} |a + b| - 1 - ab &= a + b - 1 - ab \\ &= a\,(1 - b) - (1 - b) \\ &= -\,(1 - a)\,(1 - b) < 0. \end{aligned}$$

In both cases, we deduce that the law $*$ is internal in $E$.

**(b).** The law $*$ is commutative

$$\forall a, b \in E,\ a * b = b * a.$$

Let $a, b \in E$, we have :

$$a * b = \tfrac{a+b}{1+ab} = \tfrac{b+a}{1+ba} = b * a,$$

so, $*$ is commutative.

**(c).** The law $*$ is associative

$$\forall a, b, c \in E,\ a * (b * c) = (a * b) * c.$$

Let $a, b, c \in E$, we have :

$$\begin{aligned} a * (b * c) &= a * \tfrac{b+c}{1+bc} \\ &= \tfrac{a+\frac{b+c}{1+bc}}{1+a\frac{b+c}{1+bc}} \\ &= \left(\tfrac{a+abc+b+c}{1+bc}\right) \times \left(\tfrac{1+bc}{1+bc+ab+ac}\right) \\ &= \tfrac{a+b+c+abc}{1+bc+ab+ac}, \end{aligned}$$

and

$$\begin{aligned} (a * b) * c &= \tfrac{a+b}{1+ab} * c \\ &= \tfrac{\frac{a+b}{1+ab}+c}{1+\frac{a+b}{1+ab}c} \\ &= \left(\tfrac{a+b+c+abc}{1+ab}\right) \times \left(\tfrac{1+ab}{1+ab+ac+bc}\right) \\ &= \tfrac{a+b+c+abc}{1+ab+ac+bc}. \end{aligned}$$

**(e).** The law $*$ admits a neutral element, that is to say

$$\exists e \in E, \forall a \in E,\ a * e = e * a = a.$$

Let $a \in E$, we have :

$$\begin{aligned} a * e = a &\Leftrightarrow \tfrac{a+e}{1+ae} = a \\ &\Leftrightarrow a + e = a + a^2 e \\ &\Leftrightarrow e\,(1 - a^2) = 0 \\ &\Rightarrow e = 0, \qquad car\ \ |a| < 1. \end{aligned}$$

Since the law $*$ is commutative, then

$$0 * a = a * 0 = a,$$

so, $*$admits a neutral element $e = 0$.

**(f).** Each element of $E$ admits a symmetric in $E$, that is to say

$$\forall a \in E,\ \exists a' \in E,\ a * a' = a' * a = e.$$

Let $a \in E$, we have :

$$\begin{aligned} a * a' = e \quad &\Leftrightarrow \tfrac{a+a'}{1+aa'} = 0 \\ &\Leftrightarrow a + a' = 0, \\ &\Leftrightarrow a' = -a \in E. \end{aligned}$$

Since the law $*$ is commutative, then

$$a' * a = a * a' = 0,$$

therefore, each element $a$ of $E$ admits a symmetric $a^{'} = -a$ in $E$.

Finally, $(E, *)$ is an abelian group.

### 4.2.1 Sub-group

**Definition 4.9**

A subgroup of a group $(G, *)$ is a non-empty subset $G^{'}$ of $G$ such that :

1. $*$ induces an internal composition law on $G^{'}$.

2. With this law, $G^{'}$ forms a group. We denote this as $G^{'} < G$.

**Proposition 4.3**

The subset $G^{'} \subset G$ is a subgroup of a group $(G, *)$ if and only if

1. $G^{'} \neq \varnothing$ $(e \in G^{'})$.

2. $\forall x, y \in G^{'}, x * y \in G^{'}$.

3.$\forall x \in G^{'}, x^{-1} \in G^{'}$.

**Proposition 4.4**

The subset $G^{'} \subset G$ is a subgroup of a group $(G, *)$ if and only if

1. $G^{'} \neq \varnothing$ $(e \in G^{'})$.

2. $\forall x, y \in G^{'}, x * y^{-1} \in G^{'}$.

**Exemple 4.7**

Let $(\mathbb{Z}, +)$ be a group, then $5\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

We have :

$$5\mathbb{Z} = \{5 \times k / k \in \mathbb{Z}\} = \{..., -10, -5, 0, 5, 10, ...\}$$

(i). $e = 0 \in 5\mathbb{Z}$.

(ii). Let $x, y \in 5\mathbb{Z}$, then $\exists k_1, k_2 \in \mathbb{Z}$, such that $x = 5k_1$ and $y = 5k_2$, so

$$x + y = 5k_1 + 5k_2 = 5k_3, \text{ with } k_3 = k_1 + k_2 \in \mathbb{Z},$$

then, $x + y \in 5\mathbb{Z}$.

(iii). Let $x \in 5\mathbb{Z}$, then $\exists k \in \mathbb{Z}$, such that $x = 5k$, so

$$-x = -5k = 5k', \text{ with } k' = -k \in \mathbb{Z},$$

then, $-x \in 5\mathbb{Z}$.

For (i), (ii) and (iii), then $5\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

**Proposition 4.5**

The intersection of any family of subgroups of a group $(G, *)$ is a subgroup of $(G, *)$.

**Proof.**

Let $(H_i)_{i \in I}$ be a family of subgroups of a group $(G, *)$. Let $H = \cap_{i \in I} (H_i)$ be the intersection of all $H_i$.

(a). The set $H$ is non-empty, because $e \in H_i$, then $e \in \cap_{i \in I} (H_i) = H$.

(b). Let $x, y \in H$, then $x, y \in H_i$, so we have $x * y^{-1} \in H_i$ (because $H_i$ is a subgroup), then $x * y^{-1} \in \cap_{i \in I} (H_i) = H$.

For (a) and (b), then $H$ is a subgroup of $(G, *)$.

**Remark 4.1**

The arbitrary union of subgroups of a group $(G, *)$ is not necessarily a subgroup of $(G, *)$.

**Exemple 4.8**. Let $(\mathbb{Z}, +)$ be a group, then $2\mathbb{Z}$ and $3\mathbb{Z}$ are two subgroups of $\mathbb{Z}$.

We have :

$$2\mathbb{Z} \cup 3\mathbb{Z} = \{..., -6, -4, -3, -2, 0, 2, 3, 4, 6, ...\}.$$

For $a = 2$ and $b = 3$, we have

$$a + b = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z},$$

then $\exists a, b \in 2\mathbb{Z} \cup 3\mathbb{Z}$, such that $a + b \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. Therefore, $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subgroup of $(\mathbb{Z}, +)$.

### 4.2.2 Quotient group

Let $(E, *)$ be a group and $F$ a subgroup of $E$. We define a binary relation $\Re$ on $E$ by :

$$\forall a, b \in E, \quad a \ \Re \ b \Leftrightarrow a * b^{-1} \in F.$$

$\Re$ is an equivalence relation on $E$.

Indeed, for $a, b, c \in E$ we have :

(i) $\Re$ is reflexive, because

$$a * a^{-1} = e \in F \ , \quad \textit{because } F \ \textit{ is a subgroup of } E,$$

so, $a \ \Re \ a$.

(ii) $\Re$ is symmetrical, because

$$\begin{aligned} a \ \Re \ b \ &\Rightarrow a * b^{-1} \in F \\ &\Rightarrow (a * b^{-1})^{-1} \in F \\ &\Rightarrow b * a^{-1} \in F \\ &\Rightarrow b \ \Re \ a \end{aligned}$$

(iii) $\Re$ is transitive, because

$$\begin{aligned} (a \ \Re \ b) \textit{ and } (b \ \Re \ c) \ &\Rightarrow (a * b^{-1} \in F) \textit{ and } (b * c^{-1} \in F) \\ &\Rightarrow (a * b^{-1}) * (b * c^{-1}) \in F \ , \ \textit{because } F \ \textit{ is a subgroup of } E \\ &\Rightarrow a * (b^{-1} * b) * c^{-1} \in F \ , \quad \textit{because} * \ \textit{ is associative}, \\ &\Rightarrow a * c^{-1} \in F \\ &\Rightarrow a \ \Re \ c \end{aligned}$$

We denote by $E/F$ the quotient set $E/\Re$. We define on $E/F \times E/F$ the operation $\oplus$ by :

$$\forall \left(\dot{a}, \dot{b}\right) \in E/F \times E/F, \ \dot{a} \oplus \dot{b} \ = \ \dot{\overline{a * b}}$$

**Proposition 4.5**

*If $(E, *)$ is an abelian group, then $(E/F, \oplus)$ is an abelian group, called the quotient group of $E$ by $F$.*

**Proof**

(1) $\oplus$ is a law of internal composition,

We prove that, $*$ is an application from $E/F \times E/F$ to $E/F$.

Let $\dot{a}, \dot{b}, \dot{c}, \dot{d} \in E/F$, show that

$$\left(\dot{a}, \dot{b}\right) = \left(\dot{c}, \dot{d}\right) \Rightarrow \ \dot{a} \oplus \dot{b} \ = \ \dot{c} \oplus \dot{d}$$

Suppose that $\left(\dot{a}, \dot{b}\right) = \left(\dot{c}, \dot{d}\right)$, then : $\forall x \in E$,

$$\begin{aligned}
x \in \ \dot{a} \oplus \dot{b} \quad & \Leftrightarrow x \in \ \overline{\dot{a} * \dot{b}} \\
& \Leftrightarrow x \Re (a * b) \\
& \Leftrightarrow x * (a * b)^{-1} \in F \\
& \Leftrightarrow x * b^{-1} * a^{-1} \in F \\
& \Rightarrow (x * b^{-1} * a^{-1}) * (a * c^{-1}) \in F, \textit{ because } F \textit{ is a subgroup} \\
& \Rightarrow (x * b^{-1}) * (a^{-1} * a) * c^{-1} \in F, \textit{ because } * \textit{ is associative} \\
& \Rightarrow (x * b^{-1}) * c^{-1} \in F \\
& \Rightarrow ((x * b^{-1}) * c^{-1}) * (b * d^{-1}) \in F, \textit{ because } F \textit{ is a subgroup} \\
& \Rightarrow x * (b^{-1} * b) * c^{-1} * d^{-1} \in F, \textit{ because } * \textit{ is associative and commutative} \\
& \Rightarrow x * c^{-1} * d^{-1} \in F \\
& \Rightarrow x * (d * c)^{-1} \in F \\
& \Rightarrow x \Re (d * c) \\
& \Rightarrow x \Re (c * d), \textit{ because } * \textit{ is commutative} \\
& \Rightarrow x \in \ \overline{\dot{c} * \dot{d}} \\
& \Rightarrow x \in \ \dot{c} \oplus \dot{d}
\end{aligned}$$

so,

$$\dot{a} \oplus \dot{b} \ \subset \ \dot{c} \oplus \dot{d},$$

and in the same way we show that

$$\dot{c} \oplus \dot{d} \ \subset \ \dot{a} \oplus \dot{b},$$

consequently,

$$\dot{a} \oplus \dot{b} \ = \ \dot{c} \oplus \dot{d},$$

which shows that the law $\oplus$ is internal in $E/F$.

(2) $\oplus$ is associative, because $\forall \dot{a}, \dot{b}, \dot{c} \in E/F$, we have

$$\begin{aligned}
\dot{a} \oplus \left(\dot{b} \oplus \dot{c}\right) &= \dot{a} \oplus \left(\dot{\overline{b * c}}\right) \\
&= \dot{\overline{a * (b * c)}} \\
&= \dot{\overline{(a * b) * c}} \quad , \textit{because} * \textit{is associative} \\
&= \left(\dot{\overline{a * b}}\right) \oplus \dot{c} \\
&= \left(\dot{a} \oplus \dot{b}\right) \oplus \dot{c}
\end{aligned}$$

(3) $\oplus$ admits a neutral element,

If $e$ is the neutral element of $*$, then $\dot{e}$ is the neutral element of $\oplus$, because $\forall \dot{a} \in E/F$, we have

$$\dot{a} \oplus \dot{e} = \dot{\overline{a * e}} = \dot{a}$$

*and*

$$\dot{e} \oplus \dot{a} = \dot{\overline{e * a}} = \dot{a}$$

(4) Every element is inversible,

Let $\dot{a} \in E/F$, then $(\dot{a})^{-1} = \dot{\overline{a^{-1}}}$

$$\dot{a} \oplus (\dot{a})^{-1} = \dot{\overline{a * a^{-1}}} = \dot{e}$$

*and*

$$(\dot{a})^{-1} \oplus \dot{a} = \dot{\overline{a^{-1} * a}} = \dot{e}$$

(5) $\oplus$ is commutative, because $\forall \dot{a}, \dot{b} \in E/F$, we have

$$\begin{aligned}
\dot{a} \oplus \dot{b} &= \dot{\overline{a * b}} \\
&= \dot{\overline{b * a}}, \quad \textit{because} * \textit{is commutative} \\
&= \dot{b} \oplus \dot{a}
\end{aligned}$$

For (1), (2), (3), (4) and (5) we deduce that $(E/F, \oplus)$ is an abelian group.

**Example 4.5**

We know that $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z},+)$ with $n \in \mathbb{N}$. Therefore $(\mathbb{Z}/n\mathbb{Z},\oplus)$ is a quotient group.

### 4.2.3 Group of permutations

**Definition 4.10**

Let $E$ be a set. A permutation of $E$ is a bijection from $E$ to itself. We denote by $S_E$ the set of permutations of $E$. If $E=\{1,2,...,n\}$, we simply denote it by $S_n$. The set $S_E$, equipped with the composition of applications, forms a group with identity $e=id$, called the symmetric group on the set $E$.

**Example 4.10**

Let's assume $E=\{1,2,3,4\}$. A permutation $\sigma \in S_4$ is represented as follows :

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

where $\sigma : E \to E$ is an application bijective.

Let $\sigma_1, \sigma_2$ two permutations defined by

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

we have $\sigma_1(1)=3, \sigma_1(2)=1, \sigma_1(3)=4, \sigma_1(4)=2$, and

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma_1 \circ \sigma_2(1) & \sigma_1 \circ \sigma_2(2) & \sigma_1 \circ \sigma_2(3) & \sigma_1 \circ \sigma_2(4) \end{pmatrix},$$

with,

$$\begin{array}{l} \sigma_1 \circ \sigma_2(1) = \sigma_1 (\sigma_2(1)) = \sigma_1 (2) = 1 \\ \sigma_1 \circ \sigma_2(2) = \sigma_1 (\sigma_2(2)) = \sigma_1 (3) = 4 \\ \sigma_1 \circ \sigma_2(3) = \sigma_1 (\sigma_2(3)) = \sigma_1 (4) = 2 \\ \sigma_1 \circ \sigma_2(4) = \sigma_1 (\sigma_2(4)) = \sigma_1 (1) = 3, \end{array}$$

then

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}.$$

With the same method, we find

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}.$$

### 4.2.4 Group homomorphism

**Definition 4.11**

Let $(E,*)$ and $(F,\Delta)$ be two groups. An application $f$ from $E$ to $F$ is a group homomorphism if :

$$\forall x,y\in E, f\left(x*y\right)=f\left(x\right)\Delta f\left(y\right).$$

Moreover :

1. If $E=F$ and $*=\Delta$, it is called an endomorphism.

2. If $f$ is bijective, it is an isomorphism.

3. If $f$ is a bijective endomorphism, it is an automorphism.

**Exemple 4.8**

Let $f$ and $g$ be two applications, such that :

$$\begin{array}{rccc} f: & (\mathbb{R},+) & \rightarrow & (\mathbb{R}^*,\times) \\ & x & \longmapsto & e^x \end{array}$$

and

$$\begin{array}{rccc} g: & (\mathbb{R}^*,\times) & \rightarrow & (\mathbb{R},+) \\ & x & \longmapsto & \ln|x| \end{array}$$

For $x,y\in\mathbb{R}$ and $a,b\in\mathbb{R}^*$ , we have

$$f\left(x+y\right)=e^{x+y}=e^x\times e^y=f\left(x\right)\times f\left(y\right),$$

and

$$g\left(a\times b\right)=\ln|a\times b|=\ln|a|+\ln|b|=g\left(a\right)+g\left(b\right),$$

then, $f$ is a group homomorphisme of $(\mathbb{R},+)$ to $(\mathbb{R}^*,\times)$ and $g$ is a group homomorphisme of $(\mathbb{R}^*,\times)$ to $(\mathbb{R},+)$.

**Proposition 4.7** (Properties of Group Homomorphisms)

Let $f$ be a homomorphism from $(E,*)$ to $(F,\Delta)$.

1. $f(e_E)=e_F$.

2. $\forall x\in E, f\left(x^{-1}\right)=\left(f\left(x\right)\right)^{-1}$.

3. If $f$ is an isomorphism, then its inverse $f^{-1}$ is also an isomorphism from $(F,\Delta)$ to $(E,*)$.

4. If $E^{'}<E$ (subgroup of E), then $f(E^{'})<F$.

5. If $F^{'}<F$ (subgroup of F), then $f^{-1}(F^{'})<E$.

**Proof.**

**1.** We have

$$f\left(e_E * e_E\right) = f\left(e_E\right) = e_F \ \Delta \ f\left(e_E\right),$$

since $f$ is a homomorphism, we deduce that

$$f\left(e_E\right) \ \Delta \ f\left(e_E\right) = e_F \ \Delta \ f\left(e_E\right),$$

since, all the elements of the group $(F, \Delta)$ are regular, we deduce that

$$f\left(e_E\right) = e_F$$

**2.** Let $x \in E$, we have

$$f\left(x\right) \ \Delta \ f\left(x^{-1}\right) = f\left(x * x^{-1}\right) = f\left(e_E\right) = e_F,$$

and

$$f\left(x^{-1}\right) \ \Delta \ f\left(x\right) \ = f\left(x^{-1} * x\right) = f\left(e_E\right) = e_F,$$

we deduce that

$$\left(f\left(x\right)\right)^{-1} = f\left(x^{-1}\right).$$

**Proposition 4.8**

Let $f$ be a homomorphism from $(E, *)$ to $(F, \Delta)$.

1. If $E^{'} < E$ (subgroup of E), then $f(E^{'}) < F$.

2. If $F^{'} < F$ (subgroup of F), then $f^{-1}(F^{'}) < E$.

**Proof.**

**1.** Let $E'$ a subgroup of $E$ .

(i) We have $e \in E'$, because $E'$ is a subgroup of $E$, then

$$f\left(e\right) \in f\left(E'\right),$$

so,

$$f\left(E'\right) \neq \emptyset.$$

(ii) Let $a, b \in f(E')$, then there exists $x, y \in E'$ such that $a = f(x)$ and $b = f(y)$, then

$$a \ \Delta \ b^{-1} = f(x) \ \Delta \ (f(y))^{-1} = f(x) \ \Delta \ f(y^{-1}) = f(x * y^{-1})$$

since $E'$ is a subgroup of $E$ then $x * y^{-1} \in E'$ , so

$$a \ \Delta \ b^{-1} = f(x * y^{-1}) \in f(E'),$$

for (i) and (ii) we deduce that $f(E')$ is a subgroup of $F$.

**2.** Let $F'$ a subgroup of $F$, then

(i) $f(e) = h$, since $F'$ is a subgroup of $F$, then

$$h \in F',$$

so, $e \in f^{-1}(F')$.

(ii) Let $x, y \in f^{-1}(F')$, then

$$f(x), f(y) \in F',$$

since $F'$ is a subgroup of $F$, then

$$f(x)\Delta(f(y))^{-1} \in F' \Leftrightarrow f(x)\Delta f(y^{-1}) \in F' \Leftrightarrow f\left(x * y^{-1}\right) \in F',$$

so,

$$x * y^{-1} \in f^{-1}(F').$$

for (i) an (ii) we deduce that $f^{-1}(F')$ is a subgroup of $E$.

### 4.2.5 Kernel and image

**Definition 4.12**

Let $f$ be a homomorphism from $E$ to $F$.

1. The kernel of $f$, denoted $\ker(f)$, is the set of pre-images of $e_F$ :

$$\ker f = f^{-1}\left(\{e_F\}\right) = \{x \in E / f\left(x\right) = e_F\}.$$

2. The image of $f$, denoted $\mathrm{Im}(f)$, is $f(E)$ (set of images by $f$ of elements of E)

$$\mathrm{Im}\, f = f\left(E\right) = \{f\left(x\right) / x \in E\}.$$

**Proposition 4.8**

Let $f$ be a homomorphism from $(E, *)$ to $(F, \Delta)$.

1. $f$ is injective if and only if $\ker(f) = \{e_E\}$.

2. $f$ is surjective if and only if $\mathrm{Im}(f) = F$.

**Proof.**

1. ($\Rightarrow$) Suppose that $f$ is injective.

we have $f(e_E) = e_F$, then $e_E \in \ker f$, so $\{e_E\} \subset \ker f$.

Let $x \in \ker(f)$. Then $f(x) = e_F$,

$$\begin{aligned} f(x) = e_F \quad &\Rightarrow f(x) = f(e_E), \ \textit{because } f(e_E) = e_F \\ &\Rightarrow x = e_E, \textit{ because } f \textit{ is injective.} \\ &\Rightarrow x \in \{e_E\}, \end{aligned}$$

so, $\ker f \subset \{e_E\}$. Thus, $\ker(f) = \{e_E\}$.

($\Leftarrow$)Conversely, suppose $\ker(f) = \{e_E\}$ and show that $f$ is injective.

Consider $x, y \in E$, such that $f(x) = f(y)$.

$$\begin{aligned} f(x) = f(y) \Rightarrow \quad & f(x)\Delta\left(f(y)\right)^{-1} = e_F, \ \textit{because } f(y)\Delta\left(f(y)\right)^{-1} = e_F \\ &\Rightarrow f(x)\Delta f^{-1}(y) = e_F, \quad \textit{because } \left(f(y)\right)^{-1} = f\left(y^{-1}\right) \\ &\Rightarrow f\left(x * y^{-1}\right) = e_F, \quad \textit{because } f \textit{ is homomorphism} \\ &\Rightarrow x * y^{-1} \in \ker\left(f\right) \\ &\Rightarrow x * y^{-1} = e_E, \ \textit{because } \ker(f) = \{e_E\} \\ &\Rightarrow x = y, \end{aligned}$$

then, $f$ is injective.

2. We use the definition of surjectivity.

$$\begin{aligned} f \textit{ is surjective} \quad &\Leftrightarrow \forall y \in F, \exists x \in E, y = f(x) \\ &\Leftrightarrow \mathrm{Im}\left(f\right) = f\left(E\right). \end{aligned}$$

## 4.3 Rings

**Definition 4.13**

We call a ring any set $A$ equipped with two internal composition laws $+$ and $\bullet$ such that :

**1.** $(A, +)$ is a commutative group with identity element denoted by $0_A$.

**2.** The operation $\bullet$ is associative and distributive on the left and right with respect to $*$ :

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

**3.** The operation $\bullet$ is distributive on the left and right with respect to $+$ :

$$\forall x, y, z \in A, x \bullet (y + z) = (x \bullet y) + (x \bullet z) \quad \text{and} \quad (y + z) \bullet x = (y \bullet x) + (z \bullet x) \, .$$

If $\bullet$ is commutative, we say that $(A, +, \bullet)$ is a commutative ring.

If $\bullet$ has a neutral element, the ring is said to be unitary.

We denote by $0_A$ the neutral element of $+$ and by $1_A$ the neutral element of $\bullet$.

We denote by $-x$ the symmetric of $x$ by the law $+$ (called opposite of $x$) and $x^{-1}$ the symmetric of $x$ by the law $\bullet$ (called inverse of $x$).

**Example 4.13**

$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, and $(\mathbb{C}, +, \times)$ are unitary commutative rings.

### 4.3.1 Calculation rules in a ring

Let $(A, +, \bullet)$ be a ring, then we have the following calculation rules :

For any $x, y$ and $z \in A$,

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. $(y - z) \bullet x = (y \bullet x) - (z \bullet x)$.

**Proof**

1. Let $x \in A$, then

$$0_A \bullet x = (0_A + 0_A) \bullet x = (0_A \bullet x) + (0_A \bullet x)$$

because $\bullet$ is is distributive with respect to $+$, since all the elements of $A$ are symmetrizable, we deduce that

$$0_A \bullet x = 0_A.$$

In the same way we show that

$$x \bullet 0_A = 0_A.$$

2. Let $x, y \in A$ and show that $x \bullet (-y)$ is the symmetry of $(x \bullet y)$. We have :

$$(x \bullet (-y)) + (x \bullet y) = x \bullet (-y + y) = x \bullet 0_A = 0_A$$

as $+$ is commutative we deduce that

$$(x \bullet (-y)) = -(x \bullet y).$$

In the same way we show that

$$(-x) \bullet y = -(x \bullet y).$$

The proof of properties 3 and 4 essentially uses the distributivity of the law $\bullet$ with respect to $+$.

### 4.3.2 Integral rings

**Definition 4.14**

Let $(A, +, \times)$ be a commutative ring.

- We say that $y \in A^* = A - \{0_A\}$ divides $x \in A$, or that $y$ is a divisor of $x$ or that $x$ is divisible by $y$, if

$$\exists z \in A^*, x = y \bullet z.$$

- If $0_A$ does not have a divisor in $A$, we say that $(A, +, \times)$ is an integral ring or an integrity ring.

- $(A, +, \times)$ is an integral domain if

$$\forall x, y \in A, x \times y = 0_A \Rightarrow (x = 0_A) \vee (y = 0_A).$$

- Or, by contraposition, if

$$\forall x, y \in A, (x \neq 0_A) \wedge (y \neq 0_A) \Rightarrow x \times y \neq 0_A.$$

**Example 4.14**

1. $(\mathbb{Z}, +, \times)$ of integers is integral, it has no zero divisors.

2. The ring $\mathbb{Z}/8\mathbb{Z}$ of residue classes modulo 8 is not integral because

$$\overset{\bullet}{2} \times \overset{\bullet}{4} = \overset{\bullet}{0}.$$

### 4.3.3 Sub-rings

**Definition 4.15**

Let $(A, +, \bullet)$ be a ring. A non-empty subset $A^{'}$ of $A$ is a subring of $A$ if :

The operations $+$ and $\bullet$ induce binary operations on $A^{'}$, and with these operations, $(A^{'}, +, \bullet)$ is a ring.

**Proposition 4.12**

A subset $A^{'}$ of $A$ is a subring if and only if

1. $(A^{'}, *)$ is a subgroup of $(A, *)$.

2.$\forall x, y \in A^{'}, x \Delta y \in A^{'}$.

**Example 4.14**

$(\mathbb{Z}, +, \times)$ is a subring of $(\mathbb{Q}, +, \times)$, which is a subring of $(\mathbb{R}, +, \times)$, which is a subring of $(\mathbb{C}, +, \times)$.

### 4.3.4 Ring homomorphisms

Let $(A, +, \bullet)$ and $(B, \oplus, \otimes)$ be two rings. A ring homomorphism from $A$ to $B$ is a application $f$ from $A$ to $B$ such that :

$$\forall x, y \in A, f(x + y) = f(x) \oplus f(y) \ \ and \ \ f(x \times y) = f(x) \otimes f(y).$$

### 4.3.5 Ideals

Let $(A, +, \times)$ be a commutative ring.

**Definition 4.16**

A subset $I$ of $A$ is an ideal on the right (respectively on the left) of a ring $(A, +, \times)$ if

1. $(I,+)$ is a subgroup of $(A,+)$.

2. $\forall x \in A$, *(*$\forall y \in I$*)*, $x \bullet y \in I$ *(respectively* $y \bullet x \in I$*).*

If $I$ is a right and left ideal of $A$, we say that $I$ is a two-sided ideal of $A$.

If the ring $A$ is commutative, every ideal of $A$ is two-sided, and in this case we only speak of an ideal without specifying whether it is right, left, or two-sided.

**Example 4.11**

Let $(A,+,\bullet)$ be a ring, then $I = \{O_A\}$ is a two-sided ideal of $A$.

In the commutative ring $(\mathbb{Z},+,\times)$, $n\mathbb{Z}$ is an ideal.

### 4.3.6 Quotient rings

Let $(A,+,\bullet)$ be a commutative ring and $I$ is an ideal of $A$. We consider the quotient group $(A/I,\oplus)$, and we define the application $\otimes$ from $A/I \times A/I$ to $A/I$ by

$$\forall \left(\dot{a},\dot{b}\right) \in A/I \times A/I,\ \dot{a} \otimes \dot{b} \ = \ \dot{\overline{a \bullet b}}$$

$(A/I,\oplus,\otimes)$ is commutative ring. If furthermore $A$ is an unitary ring, then $(A/I,\oplus,\otimes)$ is an unitary ring and $\dot{\overline{1_A}}$ is its unit element.

## 4.4 Field

**Definition 4.17**

Let $(\Bbbk,+,\bullet)$ be a unit ring.

We say that $(\Bbbk,+,\bullet)$ is a field if every non-zero element of $\Bbbk$ is invertible. If $\bullet$ is commutative, we say that $(\Bbbk,+,\bullet)$ is a commutative field.

**Example 4.1**

- $(\mathbb{Q},+,\times)$ and $(\mathbb{R},+,\times)$ are commutative fields.

- $(\mathbb{Z},+,\times)$ is not a field because the elements of $\mathbb{Z}^* - \{-1,1\}$ have no inverses for the law $\times$.

**Proposition 4.10**

Every field is an integral ring.

**Proposition 4.11**

$\mathbb{Z}/n\mathbb{Z}$ is a field if $n$ is prime.

### 4.4.1 Sub-field

**Definition 4.18**

Let $(\mathbb{k}, +, \bullet)$ be a field and let $\mathbb{k}'$ be a non-empty subset of $\mathbb{k}$.

We say that $\mathbb{k}'$ is a subfield of $\mathbb{k}$ if $\mathbb{k}'$ is stable under $+$ and $\times$ in $\mathbb{k}$, and $\mathbb{k}'$ equipped with the induced operations from $\mathbb{k}$ forms a field itself.

**Example 4.2**

$(\mathbb{Q}, +, \times)$ is a subfield of $(\mathbb{R}, +, \times)$.

**Proposition 4.12**

Let $(\mathbb{k}, +, \bullet)$ be a field. A subset $\mathbb{k}'$ of $\mathbb{k}$ is a subfield if and only if :

1. $\left(\mathbb{k}', +\right)$ is a subgroup of $(\mathbb{k}, +)$.

2. For all $x; y \in \mathbb{k}'$, $x; y \in \mathbb{k}'$ (stability of $\mathbb{k}'$ under $\times$)

3. $\mathbb{k}'$ contains the identity element of $\mathbb{k}$, and the inverse of every $x \in \mathbb{k}'$ in $(\mathbb{k}, \times)$ is also an element of $\mathbb{k}'$.

## 4.5 Exercises

**Exercise 4.1**

We define on $\mathbb{R} - \left\{\frac{1}{2}\right\}$, the composition law $*$ by :

$$\forall x, y \in \mathbb{R} - \left\{\tfrac{1}{2}\right\}, x * y = x + y - 2xy.$$

1. Prove that $\left(\mathbb{R} - \left\{\frac{1}{2}\right\}, *\right)$ is an abelian group.

2. Let $H$ be the subset of $\mathbb{R} - \left\{\frac{1}{2}\right\}$ defined by $H = ]-\infty, 0]$. Is $(H, *)$ a subgroup of $\left(\mathbb{R} - \left\{\frac{1}{2}\right\}, *\right)$ ? Justify your answer.

3. Let $f$ be the map defined by :

$$\begin{array}{rcl} f : \mathbb{R}^* & \to & \mathbb{R} - \left\{\frac{1}{2}\right\} \\ x & \mapsto & \frac{x+1}{2} \end{array}$$

Is $f$ a group morphism ? Justify your answer.

**Solution.**

**1. Prove that $\left(\mathbb{R} - \left\{\frac{1}{2}\right\}, *\right)$ is an abelian group.**

a. Internal composition law : we need to verify if

$$\forall x, y \in \mathbb{R} - \left\{\tfrac{1}{2}\right\}, x * y \in \mathbb{R} - \left\{\tfrac{1}{2}\right\}.$$

Let $x, y \in \mathbb{R} - \left\{\frac{1}{2}\right\}$ ($x \neq \frac{1}{2}$ and $y \neq \frac{1}{2}$),

Suppose that $x * y = \frac{1}{2}$

$$\begin{aligned} x * y = \tfrac{1}{2} &\Leftrightarrow x + y - 2xy = \tfrac{1}{2} \\ &\Leftrightarrow 2x + 2y - 4xy - 1 = 0 \\ &\Leftrightarrow 2x\,(1 - 2y) + (2y - 1) = 0 \\ &\Leftrightarrow (1 - 2y)\,(2x - 1) = 0 \\ &\Leftrightarrow x \neq \tfrac{1}{2} \text{ or } \ y \neq \tfrac{1}{2}, \end{aligned}$$

This is a contradiction. Therefore, $x * y \neq \frac{1}{2}$. Then $*$ is a internal composition law.

b. Commutativity : we need to verify if

$$\forall x, y \in \mathbb{R} - \left\{\tfrac{1}{2}\right\}, x * y = y * x.$$

Let $x, y \in \mathbb{R} - \left\{\frac{1}{2}\right\}$, we have

$$x * y = x + y - 2xy = y + x - 2yx = y * x,$$

so, $*$ is commutative.

c. Associativity : we need to verify if

$$\forall x, y, z \in \mathbb{R} - \left\{\tfrac{1}{2}\right\}, x * (y * z) = (x * y) * z.$$

Let $x, y, z \in \mathbb{R} - \left\{\frac{1}{2}\right\}$, we have

$$\begin{aligned} x * \underbrace{(y * z)}_{a} &= x + a - 2xa \\ &= x + (y + z - 2yz) - 2x\,(y + z - 2yz) \\ &= x + y + z - 2yz - 2xy - 2xz + 4xyz \ \ldots.(1) \end{aligned}$$

and

$$\begin{aligned} \underbrace{(x * y)}_{b} * z &= b + z - 2bz \\ &= (x + y - 2xy) + z - 2\,(x + y - 2xy)\,z \\ &= x + y - 2xy + z - 2xz - 2yz + 4xyz \ \ldots.(2) \end{aligned}$$

since (1) = (2), Thus, $*$ is associative.

d. Neutral Element : To find a neutral element $e \in \mathbb{R} - \left\{\frac{1}{2}\right\}$, we need to solve the equation

$$x * e = e * x = x, \text{ with } x \in \mathbb{R} - \left\{\frac{1}{2}\right\},$$

Let $x \in \mathbb{R} - \left\{\frac{1}{2}\right\}$, we have

$$x * e = x \Leftrightarrow x + e - 2xe = x \Leftrightarrow e\,(1 - 2x) = 0 \Leftrightarrow e = 0, \text{ because } x \neq \tfrac{1}{2},$$

since $*$ is commutative, then $e * x = x * e = x$, so, $e = 1$ is a neutral element.

e. Inverse Elements : For all $x \in \mathbb{R} - \left\{\frac{1}{2}\right\}$ we need find an inverse $x^{-1} \in \mathbb{R} - \left\{\frac{1}{2}\right\}$, such that

$$x * x^{-1} = x^{-1} * x = e.$$

Let $x \in \mathbb{R} - \left\{\frac{1}{2}\right\}$, we have

$$\begin{aligned} x * x^{'} = e \quad &\Leftrightarrow x + x^{'} - 2xx^{'} = 0 \\ &\Leftrightarrow x^{'}\,(1 - 2x) = -x, \\ &\Leftrightarrow x^{'} = -\tfrac{x}{1-2x}, \text{ because } x \neq 2, \end{aligned}$$

$x^{'} = -\frac{x}{1-2x} \in \mathbb{R} - \left\{\frac{1}{2}\right\}$?

Suppose that, $x^{'} = -\frac{x}{1-2x} = \frac{1}{2}$

$$x^{'} = -\tfrac{x}{1-2x} = \tfrac{1}{2} \Leftrightarrow -2x = 1 - 2x \Leftrightarrow 0 = 1,$$

This is a contradiction. Therefore, $x^{'} \neq \frac{1}{2}$.

Since $*$ is commutative, then $x^{'} * x = x + x^{'} = e$, so, $x^{'} = -\frac{x}{1-2x}$ is a symmertic element.

**Conclusion :** $\left(\mathbb{R} - \left\{\frac{1}{2}\right\}, *\right)$ is an abelian group.

**2. Is** $(H, *)$ **a subgroup of** $\left(\mathbb{R} - \left\{\frac{1}{2}\right\}, *\right)$ **?**

For $x = -2$ and $y = -3$, we have

$$x * y^{-1} = (-2) + \left(-\tfrac{-3}{1-2(-3)}\right) - 2\,(-2)\left(-\tfrac{-3}{1-2(-3)}\right) = -2 + \tfrac{3}{7} + \tfrac{12}{7} = \tfrac{1}{7} \notin H,$$

then $(H, *)$ is not a subgroup of $\left(\mathbb{R} - \left\{\frac{1}{2}\right\}, *\right)$.

**3.** Let $f$ be the map defined by :

$$\begin{aligned} f : \mathbb{R}^* &\to \mathbb{R} - \left\{\tfrac{1}{2}\right\} \\ x &\mapsto \tfrac{x+1}{2} \end{aligned}$$

**Is $f$ a group morphism ?**

Let $x, y \in \mathbb{R} - \left\{\frac{1}{2}\right\}$, we have

$$\begin{aligned} f(x) * f(y) &= f(x) + f(y) - 2f(x) f(y) \\ &= \tfrac{x+1}{2} + \tfrac{y+1}{2} - 2\tfrac{x+1}{2}\tfrac{y+1}{2} \\ &= \tfrac{x+1+y+1-xy-x-y-1}{2} = \tfrac{1+xy}{2} = f(x \times y), \end{aligned}$$

then, $f$ is a group morphism.

**Exercise 4.2**

We consider the following permutations

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 3 & 1 & 2 \end{pmatrix}$$

1. Calculate $\sigma_1 \circ \sigma_2$, $\sigma_1 \circ \sigma_3$, $\sigma_2 \circ \sigma_3$, $\sigma_3 \circ \sigma_2$, $\sigma_4 \circ \sigma_4$.

2. $(S_3, \circ)$ is it a commutative group ?

**Solution.**

**1.** $\sigma_1 \circ \sigma_2$

$$\begin{aligned} \sigma_1 \circ \sigma_2 &= \begin{pmatrix} 1 & 2 & 3 \\ & & \\ \sigma_1 \circ \sigma_2(1) & \sigma_1 \circ \sigma_2(1) & \sigma_1 \circ \sigma_2(3) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 \\ & & \\ \sigma_1(\sigma_2(1)) & \sigma_1(\sigma_2(1)) & \sigma_1(\sigma_2(3)) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 \\ & & \\ \sigma_1(2) & \sigma_1(1) & \sigma_1(3) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 3 & 1 & 2 \end{pmatrix} = \sigma_4 \end{aligned}$$

De la même manière, on trouve

$$\sigma_1 \circ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_2 \circ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 1 & 3 & 2 \end{pmatrix} = \sigma_1$$

$$\sigma_3 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 3 & 2 & 1 \end{pmatrix}, \qquad \sigma_4 \circ \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 2 & 3 & 1 \end{pmatrix} = \sigma_3$$

**2.** $(S_3, \circ)$ is not a commutative group, because

$$\sigma_2 \circ \sigma_3 \neq \sigma_3 \circ \sigma_2.$$

**Exercice 4.3**

Let $+$ and $\bullet$ two internal composition laws in $\mathbb{R}^2$ defined by :

$$\forall (a,b),(c,d) \in \mathbb{R}^2, \quad (a,b) + (c,d) = (a+c, b+d)$$

$$\forall (a,b),(c,d) \in \mathbb{R}^2, \quad (a,b) \bullet (c,d) = (ac - bd, ad + cb)$$

Show that $(\mathbb{R}^2, +, \bullet)$ is a commutative field.

**Solution**

**1.** $(\mathbb{R}^2, +)$ **is an abelian group**

(a). $+$ is commutative

$$\forall (a,b),(c,d) \in \mathbb{R}^2, (a,b) + (c,d) = (c,d) + (a,b)$$

Let $(a,b),(c,d) \in \mathbb{R}^2$, we have

$$\begin{aligned} (a,b) + (c,d) &= (a+c, b+d) \\ &= (c+a, d+b) \\ &= (c,d) + (a,b) \end{aligned}$$

(b). $+$ is associative,

$$\forall (a,b),(c,d),(e,f) \in \mathbb{R}^2, \quad (a,b) + ((c,d) + (e,f)) = ((a,b) + (c,d)) + (e,f)$$

Let $(a,b),(c,d),(e,f) \in \mathbb{R}^2$, we have

$$\begin{aligned} (a,b) + ((c,d) + (e,f)) &= (a,b) + (c+e, d+f) \\ &= (a+c+e, b+d+f) \\ &= (a+c, b+d) + (e,f) \\ &= ((a,b) + (c,d)) + (e,f) \end{aligned}$$

(c). Neutral element

$$\exists\,(e_1,e_2)\in\mathbb{R}^2,\forall\,(a,b)\in\mathbb{R}^2,\quad (a,b)+(e_1,e_2)=(e_1,e_2)+(a,b)=(a,b)$$

Let $(a,b)\in\mathbb{R}^2$, we have

$$\begin{aligned}(a,b)+(e_1,e_2)=(a,b) &\Leftrightarrow (a+e_1,b+e_2)=(a,b)\\ &\Leftrightarrow \begin{cases} a+e_1=a\\ \\ b+e_2=b\end{cases}\\ &\Leftrightarrow \begin{cases} e_1=0\\ \\ e_2=0\end{cases},\end{aligned}$$

as the law $+$ is commtative, then

$$(e_1,e_2)+(a,b)=(a,b)+(e_1,e_2)=(a,b)\,,$$

hence $+$ has a neutral element $0_{\mathbb{R}^2}=(0,0)$.

(d). Symmetrical element

$$\forall\,(a,b)\in\mathbb{R}^2,\exists\,(a',b')\in\mathbb{R}^2,\quad (a,b)+(a',b')=(a',b')+(a,b)=(e_1,e_2)$$

Let $(a,b)\in\mathbb{R}^2$,

$$\begin{aligned}(a,b)+(a',b') &=(0,0)\Leftrightarrow (a+a',b+b')=(0,0)\\ &\Leftrightarrow \begin{cases} a+a'=0\\ \\ b+b'=0\end{cases}\\ &\Leftrightarrow \begin{cases} a'=-a\\ \\ b'=-b\end{cases}\end{aligned}$$

as the law $+$ is commtative, then

$$(a',b')+(a,b)=(a,b)+(a',b')=(0,0)\,,$$

hence all element $(a,b)\in\mathbb{R}^2$ is symmetrizable and its symmetrical is $(a',b')=(-a,-b)$.

**2. $\bullet$ is associative,**

$$\forall\,(a,b)\,,(c,d)\,,(e,f)\in\mathbb{R}^2,\quad (a,b)\bullet((c,d)\bullet(e,f))=((a,b)\bullet(c,d))\bullet(e,f)$$

Let $(a,b),(c,d),(e,f) \in \mathbb{R}^2$, we have :

$$\begin{aligned}(a,b) \bullet ((c,d) \bullet (e,f)) &= (a,b) \bullet (ce-df, cf+ed) \\ &= (a(ce-df) - b(cf+ed), a(cf+ed) + (ce-df)b) \\ &= (ace - adf - bcf - bed, acf + aed + ceb - dfb),\end{aligned}$$

and

$$\begin{aligned}((a,b) \bullet (c,d)) \bullet (e,f) &= (ac-bd, ad+cb) \bullet (e,f) \\ &= ((ac-bd)e - (ad+cb)f, (ac-bd)f + e(ad+cb)) \\ &= (ace - bde - adf - cbf, acf - bdf + ade + cbe),\end{aligned}$$

so,

$$(a,b) \bullet ((c,d) \bullet (e,f)) = ((a,b) \bullet (c,d)) \bullet (e,f)$$

**3. $\bullet$ is commtative,**

$$\begin{aligned}\forall (a,b),(c,d) \in \mathbb{R}^2, \quad (a,b) \bullet (c,d) &= (c,d) \bullet (a,b) \\ (a,b) \bullet (c,d) &= (ac-bd, ad+cb) \\ &= (ca-db, cb+ad) \\ &= (c,d) \bullet (a,b)\end{aligned}$$

**4. $\bullet$ is distributive with respect to $+$ ,** $\forall (a,b),(c,d),(e,f) \in \mathbb{R}^2$,

$$(a,b) \bullet ((c,d) + (e,f)) = ((a,b) \bullet (c,d)) + ((a,b) \bullet (e,f))$$

*and*

$$((c,d) + (e,f)) \bullet (a,b) = ((c,d) \bullet (a,b)) + ((e,f) \bullet (a,b))$$

Let $(a,b),(c,d),(e,f) \in \mathbb{R}^2$, we have

$$\begin{aligned}(a,b) \bullet ((c,d) + (e,f)) &= (a,b) \bullet (c+e, d+f) \\ &= (a(c+e) - b(d+f), a(d+f) + (c+e)b) \\ &= (ac + ae - bd - bf, ad + af + cb + eb),\end{aligned}$$

and

$$\begin{aligned}((a,b) \bullet (c,d)) + ((a,b) \bullet (e,f)) &= (ac-bd, ad+cb) + (ae-bf, af+eb) \\ &= (ac - bd + ae - bf, ad + cb + af + eb),\end{aligned}$$

so,

$$(a,b)\bullet((c,d)+(e,f))=((a,b)\bullet(c,d))+((a,b)\bullet(e,f))$$

as the law $\bullet$ is commtative, then

$$\begin{aligned}((c,d)+(e,f))\bullet(a,b) &= (a,b)\bullet((c,d)+(e,f))\\ &= ((a,b)\bullet(c,d))+((a,b)\bullet(e,f))\\ &= ((c,d)\bullet(a,b))+((e,f)\bullet(a,b))\end{aligned}$$

hence $\bullet$ is distributive with respect to $+$.

**5. Neutral element with respect to $\bullet$**

$$\exists\,(a_1,a_2)\in\mathbb{R}^2,\forall\,(a,b)\in\mathbb{R}^2,\quad (a,b)\bullet(a_1,a_2)=(a_1,a_2)\bullet(a,b)=(a,b)$$

Let $(a,b)\in\mathbb{R}^2$

$$\begin{aligned}(a,b)\bullet(a_1,a_2)=(a,b) &\Leftrightarrow (aa_1-ba_2,aa_2+a_1b)=(a,b)\\ &\Leftrightarrow \begin{cases} aa_1-ba_2=a\\ aa_2+a_1b=b\end{cases}\\ &\Leftrightarrow \begin{cases} a_1=1\\ a_2=0\end{cases},\end{aligned}$$

as the law $\bullet$ is commtative, then

$$(a_1,a_2)+(a,b)=(a,b)+(a_1,a_2)=(a,b)\,,$$

hence $\bullet$ has a neutral element $1_{\mathbb{R}^2}=(1,0)$

**6. Element symmetrical with respect to $\bullet$**

$$\forall\,(a,b)\in\mathbb{R}^2-\{(0,0)\}\,,\exists\,(a',b')\in\mathbb{R}^2-\{(0,0)\}\,,\quad (a,b)\bullet(a',b')=(a',b')\bullet(a,b)=(1,0)$$

Let $(a,b) \in \mathbb{R}^2 - \{(0,0)\}$, w have :

$$(a,b) \bullet (a',b') = (1,0) \quad \Leftrightarrow (aa' - bb', ab' + a'b) = (1,0)$$

$$\Leftrightarrow \begin{cases} aa' - bb' = 1 \\ ab' + a'b = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} a' = \frac{a}{a^2+b^2} \in \mathbb{R}^* \\ b' = \frac{-b}{a^2+b^2} \in \mathbb{R}^* \end{cases},$$

as the law $\bullet$ is commtative, then

$$(a',b') + (a,b) = (a,b) + (a',b') = (1,0),$$

so, all element $(a,b) \in \mathbb{R}^2 - \{(0,0)\}$ admits an inverse $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$ in $\mathbb{R}^2 - \{(0,0)\}$.

**Exercice 4.4**

1. Prove that $\mathbb{Z}/_6\mathbb{Z}$ admits divisors of zero. $\mathbb{Z}/_6\mathbb{Z}$ is it a field ?

2. Prove that $\mathbb{Z}/_5\mathbb{Z}$ is a field.

**Solution.**

**1. Prove that $\mathbb{Z}/_6\mathbb{Z}$ admits divisors of zero. $\mathbb{Z}/_6\mathbb{Z}$ is it a field ?**

We know that

$$\mathbb{Z}/_6\mathbb{Z} = \left\{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}\right\},$$

we have

$$\dot{2} \times \dot{3} = \dot{0},$$

and

$$\dot{4} \times \dot{3} = \dot{0},$$

so, $\mathbb{Z}/_6\mathbb{Z}$ admits divisors of zero. Then $\mathbb{Z}/_6\mathbb{Z}$ is not a field.

**2. Prove that $\mathbb{Z}/_5\mathbb{Z}$ is a field.**

$\mathbb{Z}/_5\mathbb{Z}$ is a field, because 5 is prime.

**Exercice 4.5**

Let $n \in \mathbb{N}, n \geq 2$. we consider the ring $\mathbb{Z}/n\mathbb{Z}$

1. Prove that $\overline{n-1}$ is an inversible element of $\mathbb{Z}/n\mathbb{Z}$.

2. Determine the set of all investible elements of $\mathbb{Z}/n\mathbb{Z}$.

**Solution.**

Let $n \in \mathbb{N}, n \geq 2$. we consider the ring $\mathbb{Z}/n\mathbb{Z}$

**1.** Prove that $\overline{n-1}$ is an inversible element of $\mathbb{Z}/n\mathbb{Z}$

$\dot{\overline{n-1}}$ is inversible if there exists $\dot{\overline{p}} \in \mathbb{Z}/_n\mathbb{Z}$ such that

$$\dot{\overline{n-1}} \ \dot{\times} \ \dot{\overline{p}} \ = \ \dot{\overline{1}},$$

then,

$$\begin{aligned}(n-1)\,p \equiv 1\,[n] \ &\Leftrightarrow -p \equiv 1\,[n] \\ &\Leftrightarrow \exists k \in \mathbb{Z}, -p = 1 + kn \\ &\Leftrightarrow \exists k' \in \mathbb{Z}, p = k'n - 1,\end{aligned}$$

so, we can take $p = n - 1$

$$\begin{aligned}\dot{\overline{n-1}} \ \dot{\times} \ \dot{\overline{n-1}} \ &= \dot{\overline{(n-1)\,(n-1)}} \\ &= \dot{\overline{n^2 - 2n + 1}} \\ &= \dot{\overline{1}}.\end{aligned}$$

**2.** Determine the set of all investible elements of $\mathbb{Z}/n\mathbb{Z}$.

Let $\dot{\overline{a}} \in \mathbb{Z}/_n\mathbb{Z}$, We say that $\dot{\overline{a}}$ is inversible element if there exists $\dot{\overline{b}} \in \mathbb{Z}/_n\mathbb{Z}$ such that

$$\dot{\overline{a}} \ \dot{\times} \ \dot{\overline{b}} \ = \ \dot{\overline{1}},$$

then,

$$\begin{aligned}ab \equiv 1\,[n] \ &\Leftrightarrow \exists k \in \mathbb{Z}, ab = 1 + kn \\ &\Leftrightarrow a \textit{ is prime with } n\end{aligned}$$

## 4.6 Terminology translation

| **English** | **Frensh** |
|---|---|
| Algebraic structures | Structures algébriques |
| Law of internal composition | Loi de composition interne |
| Non-empty set | Ensemble non vide |
| Associativity | Assiciativité |
| Commutativity | Commutativité |
| Neutral element | Elémént neutre |
| Symmetric element | Elémént symétrique |
| Distributivity | Distributivité |
| Sub-group | Sous groupe |
| Kernel | Noyau |
| Rings | Anneaux |
| Integral ring | Anneau intégré |
| Sub-ring | Sous-anneau |
| Field | Corps |
| Sub-field | Sous-corps |
| Prime | Premier |

Chapitre 5

# Polynomial rings

Throughout this chapter we shall assume that $\mathbb{k}$ is a commutative ring ($\mathbb{k} = \mathbb{R}$ or $\mathbb{C}$).

## 5.1 Definitions

**Definition 5.1**

We call a polynomial with coefficients in $\mathbb{k}$ any expression of the form :

$$P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n = \sum_{i=0}^{n} a_iX^i,$$

where $n \in \mathbb{N}$ and the coefficients $a_0, a_1, a_2, ..., a_n$ are elements of $\mathbb{k}$. The symbol $X$ is called the indeterminate (we set $X^0 = 1$).

- The set of polynomials with coefficients in $\mathbb{k}$ is denoted by $\mathbb{k}[X]$.

- The $a_i$ are called the coefficients of the polynomial.

- If all the coefficients $a_i$ are zero, $P$ is called the zero polynomial and is denoted by 0.

- Polynomials with only one non-zero term (of the type $a_kX^k$) are called monomials.

- Let $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$ be a polynomial with $a_n \neq 0$. The monomial $a_nX^n$ is called the leading term. The coefficient $a_n$ is called the leading coefficient of $P$.

- If the leading coefficient is 1, $P$ is called monic.

**Example 5.1**

- $P(X) = 1 + X^7$ and $Q(X) = -2 + 3X - X^4$ are two polynomials.

- $R(X) = \frac{1+X^7}{2+X^2}$ is not a polynomial.

**Definition 5.2**

If $n$ is the largest nonnegative number for which $a_n \neq 0$, we say that the degree of $P$ is $n$ and write $deg(P) = n$.

- If $P = 0$ is the zero polynomial, then the degree of $P$ is defined to be $-\infty$.

- A polynomial of the form $P(X) = a_0$ is called a constant polynomial. If $a_0 \neq 0$, its degree is 0.

We note :

$$\mathbb{k}_n[X] = \{P \in \mathbb{k}[X] / deg(P) \leq n\}.$$

**Example 5.2**

- $P(X) = 1 + X^7$ is a polynomial of degree 7.

- $Q(X) = -2 + 3X - X^4$ is a polynomial of degree 4.

- $R(X) = 5$ is a polynomial of degree 0.

## 5.2 Polynomial operations

### 5.2.1 Equality

Two polynomials are equal exactly when their corresponding coefficients are equal.

That is, if we let

$$P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n,$$

and

$$Q(X) = b_0 + b_1X + b_2X^2 + ... + b_nX^n,$$

then $P(X) = Q(X)$ if and only if $a_i = b_i$ for all $i = 1, 2, ..., n$.

### 5.2.2 Addition

Let $P, Q \in \mathbb{k}_n[X]$, such as

$$P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n,$$

and

$$Q(X) = b_0 + b_1X + b_2X^2 + ... + b_nX^n.$$

Then the sum of $P(X)$ and $Q(X)$ is

$$\begin{aligned}(P+Q)(X) &= (a_0+b_0)+(a_1+b_1)X+(a_2+b_2)X^2+...+(a_n+b_n)X^n \\ &= \sum_{i=0}^{n}(a_i+b_i)X^i\end{aligned}$$

### 5.2.3 Multiplication

Let $P \in \mathbb{k}_n[X]$ and $Q \in \mathbb{k}_m[X]$, such as

$$P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n,$$

and

$$Q(X) = b_0 + b_1X + b_2X^2 + ... + b_mX^m.$$

We define the product of $P(X)$ and $Q(X)$ by :

$$\begin{aligned}(P\times Q)(X) &= c_0 + c_1X + c_2X^2 + ... + c_rX^r \\ &= \sum_{i=0}^{r} c_iX^i,\end{aligned}$$

with $r = n+m$ and $c_k = \sum_{i+j=k} a_ib_j$ for $k \in \{0,1,...,r\}$.

### 5.2.4 Multiplication by a scalar

Let $P \in \mathbb{k}_n[X]$, such as

$$P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n,$$

We define the product of $P(X)$ and $\lambda \in \mathbb{k}$ by :

$$\begin{aligned}(\lambda P)(X) &= \lambda a_0 + \lambda a_1X + \lambda a_2X^2 + ... + \lambda a_nX^n \\ &= \sum_{i=0}^{n}\lambda a_iX^i.\end{aligned}$$

**Example 5.3**

Suppose that

$$P(X) = 1 + X + 3X^3,$$

and

$$Q(X) = 2X + 3X^2 - X^4.$$

The sum of these two polynomials is

$$(P+Q)(X) = 1 + 3X + 3X^2 + 3X^3 - X^4$$

The product,

$$(P \times Q)(X) = \sum_{i=0}^{7} c_i X^i,$$

with $c_k = \sum_{i+j=k} a_i b_j$ for $k \in \{0, 1, ..., 7\}$

$$c_0 = \sum_{i+j=0} a_i b_j = a_0 b_0 = 0 \quad c_1 = \sum_{i+j=1} a_i b_j = a_0 b_1 + a_1 b_0 = 2 \quad c_2 = \sum_{i+j=2} a_i b_j = a_0 b_2 + a_2 b_0 + a_1 b_1 = 5$$
$$c_3 = \sum_{i+j=3} a_i b_j = 3 \qquad c_4 = \sum_{i+j=4} a_i b_j = 5 \qquad c_5 = \sum_{i+j=5} a_i b_j = 8$$
$$c_6 = \sum_{i+j=6} a_i b_j = 0 \qquad c_7 = \sum_{i+j=7} a_i b_j = -3,$$

then,

$$(P \times Q)(X) = 2X + 5X^2 + 3X^3 - 5X^4 + 8X^5 - 3X^7.$$

**Theorem 5.1**

Let $\Bbbk$ be a commutative ring with identity. Then $\Bbbk[X]$ is a commutative ring with identity.

**Proof**

It is clear that $(+)$ and $(\times)$ are two laws of internal composition.

We have :

**(1) $\Bbbk[X]$ is an abelian group**

Let $P_1, P_2, P_3 \in \Bbbk[X]$ , such as

$$P_1(X) = \sum_{i=0}^{n} a_i X^i, \quad P_2(X) = \sum_{i=0}^{n} a_i^{'} X^i, \quad P_3(X) = \sum_{i=0}^{n} a_i^{"} X^i,$$

(a) Associativity

We verify

$$P_1 + (P_2 + P_3) = (P_1 + P_2) + P_3,$$

we have

$$(P_1 + (P_2 + P_3))(X) = P_1(X) + (P_2 + P_3)(X) = P_1(X) + P_2(X) + P_3(X),$$

and

$$((P_1 + P_2) + P_3)(X) = (P_1 + P_2)(X) + P_3(X) = P_1(X) + P_2(X) + P_3(X),$$

then

$$(P_1 + (P_2 + P_3))(X) = ((P_1 + P_2) + P_3)(X),$$

Hence, + is associative.

(b) Commutativity :

We verify

$$P_1 + P_2 = P_2 + P_1,$$

we have

$$(P_1 + P_2)(X) = \sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{n} a_i' X^i = \sum_{i=0}^{n} \left(a_i + a_i'\right) X^i$$

$$\sum_{i=0}^{n} \left(a_i' + a_i\right) X^i = \sum_{i=0}^{n} a_i' X^i + \sum_{i=0}^{n} a_i X^i = (P_2 + P_1)(X),$$

Therefore, + is commutative.

(c) Neutral Element :

We seek a polynomial $e = \sum_{i=0}^{n} e_i X^i$ such that $P_1 + e = e + P_1 = P_1$ .

Setting $P_1 + e = P_1$ gives :

$$\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{n} e_i X^i = \sum_{i=0}^{n} a_i X^i \Leftrightarrow \sum_{i=0}^{n} (a_i + e_i) X^i = \sum_{i=0}^{n} a_i X^i \Leftrightarrow e_i = 0 \text{ for all } i \in \{0, 1, ..., n\}.$$

Therefore, the zero polynomial, $e(X) = 0$, is the additive identity.

(d) every element of $\mathbb{k}[X]$ is symmetrizable for the operation +.

We look for a polynomial $Q = \sum_{i=0}^{n} b_i X^i$ such that $P_1 + Q = Q + P_1 = e$, where $e$ is the neutral element.

Solving $P_1 + Q = e$ gives :

$$P_1 + Q = e \Leftrightarrow \sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{n} b_i X^i = 0 \Leftrightarrow \sum_{i=0}^{n} (a_i + b_i) X^i = 0 \Leftrightarrow a_i + b_i = 0 \Leftrightarrow b_i = -a_i,$$

Hence, the inverse of $P_1$ is $-P_1$.

**(2) The operation $\times$ is associative :**

We verify

$$P_1 \times (P_2 \times P_3) = (P_1 \times P_2) \times P_3,$$

**(3) The operation $\times$ is distributive on the left and right with respect to $+$ :**

We verify

$$P_1 \times (P_2 + P_3) = (P_1 \times P_2) + (P_1 \times P_3),$$

and

$$(P_2 + P_3) \times P_1 = (P_2 \times P_1) + (P_3 \times P_1),$$

**(4) The operation $\times$ has a neutral element different from $0_{\Bbbk[X]}$, denoted by $1_{\Bbbk[X]} = 1$.**

It is easy to verify that

$$P_1 \times 1_{\Bbbk[X]} = 1_{\Bbbk[X]} \times P_1 = P_1.$$

**Conclusion :** From (1), (2), (3), and (4), we deduce that $(\Bbbk[X], +, \times)$ is a commutative ring with identity.

**Proposition 5.1**

Let $P, Q \in \Bbbk[X]$, we have :

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

$$\deg(P \times Q) = \deg(P) + \deg(Q)$$

$$\deg(\lambda P) = \deg(P), \ \textit{with } \lambda \in \Bbbk$$

# 5.3 Polynomial arithmetic

## 5.3.1 Division

**Definition 5.3**

Let $P, Q \in \Bbbk[X]$. We say that $P$ divides $Q$, denoted as $P \setminus Q$, if there exists $R \in \Bbbk[X]$ such

that $Q = PR$.

**Example 5.4**

- The polynomial $X^2 + 2X$ divides $-X^4 - X^3 + 3X^2 + 2X$

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

- The polynomial $X^2 + 2X$ does not divide $X^3 + 3X^2 + 2X$.

**Proposition 5.2**

Let $P, Q, R, S \in \mathbb{k}[X]$.

1. If $P \setminus Q$ and $Q \setminus R$, then $P \setminus R$.

2. If $P \setminus Q$ and $P \setminus R$, then $P \setminus (Q + R)$.

3. If $P \setminus Q$ and $R \setminus S$, then $PR \setminus QS$.

### 5.3.2 Euclidean division

**Theorem 5.2.** (Euclidean Division)

Let $A, B \in \mathbb{k}[X]$ be two polynomials with coefficients in a field $\mathbb{k}$ such that $B \neq 0$. Then there exists a unique pair $(Q, R)$ of $\mathbb{k}[X]$ such that $A = BQ + R$ and $deg(R) < deg(B)$.

- $Q$ is called the quotient and $R$ the rest, and $A = BQ + R$ is the Euclidean division of $A$ by $B$.

- The condition $deg(R) < deg(B)$ means that $R = 0$ or $0 \leq deg(R) < deg(B)$.

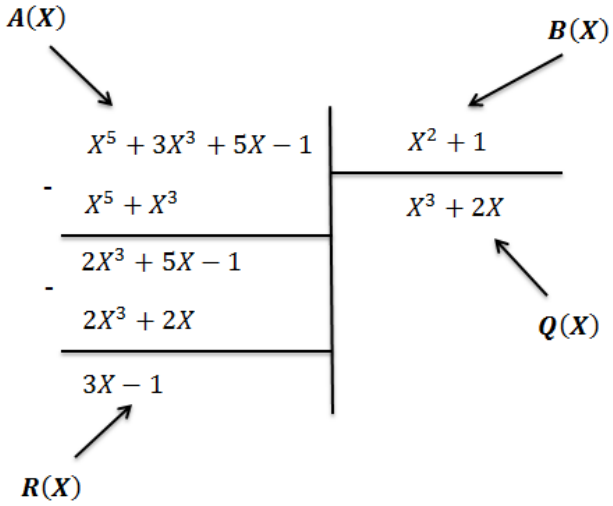
- $R = 0$ if and only if $B \setminus A$.

**Example 5.5**

Let $A, B \in \mathbb{R}[X]$, such as $A(X) = X^5 + 3X^3 + 5X - 1$ and $B(X) = X^2 + 1$.

We have

$$A(X) = B(X) \times \underbrace{(X^3 + 2X)}_{Q(X)} + \underbrace{(3X - 1)}_{R(X)}.$$




### 5.3.3 Irreducible polynomials

### 5.3.4 Greatest common divisor

**Definition 5.5**

Let $A, B \in \mathbb{k}[X]$ be two polynomials with coefficients in a field $\mathbb{k}$, with $A \neq 0$ or $B \neq 0$. There is a unique unit polynomial of higher degree that divides both $A$ and $B$.

This unique polynomial is called the *gcd* (greatest common divisor) of $A$ and $B$, which is noted as $gcd(A, B)$.

**Euclid's algorithm**

Let $A$ and $B$ be polynomials, $B \neq 0$.

We calculate the successive Euclidean divisions,

$$A = BQ_1 + R_1, \qquad deg(R_1) < deg(B)$$

$$B = R_1Q_2 + R_2, \qquad deg(R_2) < deg(R_1)$$

$$R_1 = R_2Q_3 + R_3, \qquad deg(R_3) < deg(R_2)$$

$$\vdots$$

$$R_{k-2} = R_{k-1}Q_k + R_k, \qquad deg(R_k) < deg(R_{k-1})$$

$$R_{k-1} = R_kQ_{k+1},$$

The degree of the rest decreases with each division. The algorithm stops when the rest equal to zero.

The gcd is the last non-zero rest $R_k$ (made unitary).

**Example 5.6**

Let $A, B \in \mathbb{R}[X]$, such as $A(X) = X^5 + X^3 + 2X^2 - 2X + 6$ and $B(X) = X^3 + 4X^2 + 2X + 8$.

We have

$$A(X) = B(X) \times \underbrace{\left(X^2 - 4X + 15\right)}_{Q_1(X)} + \underbrace{\left(-58X^2 - 62X - 114\right)}_{R_1(X)}$$

$$B(X) = R_1(X) \times \underbrace{\left(X^2 - 4X + 15\right)}_{Q_2(X)} + \underbrace{\left(-58X^2 - 62X - 114\right)}_{R_2(X)}$$

$$R_1(X) = R_2(X) \times \underbrace{\left(X^2 - 4X + 15\right)}_{Q_3(X)} + \underbrace{\left(-58X^2 - 62X - 114\right)}_{R_3(X)}$$

The gcd is the last non-zero rest (made unitary), so

$$\gcd(A, B) = X^2 + 2$$

**Proposition 5.3** Properties of gcd

Let $P, Q \in \Bbbk[X]$. Then

1. $\gcd(P, Q)$ is a common divisor of $P$ and $Q$.

2. If $D$ is another common divisor of $P$ and $Q$, then $D$ divides $\gcd(P, Q)$.

3. There exist polynomials $(U, V) \in \Bbbk[X]$ such that $PU + QV = \gcd(P, Q)$.

**Definition 5.6** Coprime polynomial

Let $A, B \in \Bbbk[X]$ be two polynomials with coefficients in a field $\Bbbk$.

We say that $A$ and $B$ are coprime if $\gcd(A, B) = 1$.

For any $A, B \in \Bbbk[X]$ we can reduce to coprime polynomials : if $\gcd(A, B) = D$, then $A$ and $B$ are written : $A = DA'$, $B = DB'$ with $gcd(A'; B') = 1$.

**Example 5.7**

Let $A, B \in \mathbb{R}[X]$, such as $A(X) = X^4 + 2X^3 - 2X^2 - 3X$ and $B(X) = X^3 + 3X^2 + X - 1$.

We have

$$\gcd(A, B) = 1 + X,$$

so,

$$A(X) = (1 + X)(X^3 + X^2 - 3X)$$

$$B(X) = (1 + X)(X^2 + 2X - 1)$$

$$\gcd\left(X^3+X^2-3X, X^2+2X-1\right)$$

**Bezout's Theorem**

Let $A, B \in \Bbbk[X]$, with A $\neq 0$ or B $\neq 0$. Denote by $D = \gcd(A, B)$.

There exist two polynomials $U, V \in \Bbbk[X]$ such that

$$AU + BV = D.$$

**Proposition 5.4**

Let $A, B \in \Bbbk[X]$, $A$ and $B$ are coprime if there exist two polynomials $U, V \in \Bbbk[X]$ such that

$$AU + BV = 1.$$

### 5.3.5 Factorization

**Definition 5.8**

A polynomial $A$ of $\Bbbk[X]$ is said to be irreducible if its degree is greater than or equal to 1 and if its only divisors are non-zero constant polynomials and polynomials of the form $cA$ ( $c \in \Bbbk^*$).

A polynomial $A$ is therefore irreducible if it has exactly two unit divisors (these two divisors are then 1 and $\frac{1}{d}A$ where $d$ is the leading coefficient).

**Theorem 5.3.**

Let $A \in \Bbbk[X]$ be a non-zero polynomial. Then $A$ decomposes uniquely up to the order of factors as :

$$A = c \times R_1^{\alpha_1} \times R_2^{\alpha 2} \times R_3^{\alpha_2} \times ... \times R_k^{\alpha_k}$$

where $k \in \mathbb{N}^*, R_i$ are distinct, unit, irreducible polynomials in $\Bbbk[X]$ and $c \in \Bbbk^*$ is the leading coefficient of $A$ and $\forall i \in \{1, ..., k\}, \alpha_i \in \mathbb{N}^*$.

**Example 5.5.**

Consider the polynomial $P = 2X^2 + 9$. Then $P$ exists in both $\mathbb{R}[X]$ and $\mathbb{C}[X]$.

However, care must be taken as its factorization differs in these two rings :

1. $P$ factors as $(\sqrt{2}X - 3i) \times (\sqrt{2}X + 3i)$ in $\mathbb{C}[X]$.

2. $P$ is irreducible in $\mathbb{R}[X]$.

## 5.4 Roots of a polynomial

**Definition 5.9**

Let $P \in \mathbb{k}[X]$ be such that

$$P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$$

Let $\alpha \in \mathbb{k}$. We say that $\alpha$ is a root (or a zero) of $P$ if

$$P(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n 0.$$

**Example 5.7**

Let $A \in \mathbb{R}_3[X]$ be such that

$$A(X) = 3 - X + 2X^2 - 4X^3$$

We have :

$$A(1) = 3 - (1) + 2(1)^2 - 4(1)^3 = 0,$$

therefore, $\alpha = 1$ is a root of $A$.

**Proposition 5.5**

Let $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in \mathbb{k}[X]$ and $\alpha \in \mathbb{k}$.

$$P(\alpha) = 0 \Leftrightarrow (X - \alpha) \ \textit{divides} \ P(X).$$

**Proof**

Let $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in \mathbb{k}[X]$ and $\alpha \in \mathbb{k}$.

The Euclidean division of $P(X)$ by $(X - \alpha)$ gives

$$P(X) = Q(X - \alpha) + R$$

with $degR < deg(X - \alpha) = 1$.

So, $degR = 0$ which gives $R$ is a constant.

So,

$$P(\alpha) = 0 \Leftrightarrow R(\alpha) = 0 \Leftrightarrow R = 0,$$

so, $(X - \alpha)$ divides $P(X)$.

### 5.4.1 Multiplicity of roots

**Definition 5.10**

Let $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in \Bbbk[X]$ and $\alpha \in \Bbbk$.

We say that $\alpha$ is a root of multiplicity $k \in \mathbb{N}^*$ (or root of order $k$) of $P$ if $(X-\alpha)^k$ divides $P$ while $(X-\alpha)^{k+1}$ does not divide $P$.

When $k = 1$ we speak of a simple root, when $k = 2$ of a double root, etc.

**Derived Polynomial**

We define the derived polynomial of $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in \Bbbk[X]$ as follows

$$P'(X) = a_1 + 2a_2X + ... + na_nX^{n-1}.$$

We can define successive derivatives in the same way.

**Proposition 5.6**

Let $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in \Bbbk[X]$ and $\alpha \in \Bbbk$.

We have the equivalence between

**1.** $\alpha$ is a root of multiplicity $k \in \mathbb{N}^*$.

**2.** There exists $Q(X) \in \Bbbk[X]$ such that

$$P(X) = (X-\alpha)^k Q(X);$$

with $Q(\alpha) \neq 0$.

**3.**

$$P(\alpha) = P'(\alpha) = ... = P^{(k-1)}(\alpha) = 0,$$

and

$$P^{(k)}(\alpha) \neq 0.$$

## 5.5 Exercises

**Exercise 5.1**

In the following cases, perform the Euclidean division of $A$ by $B$ :

**1.**

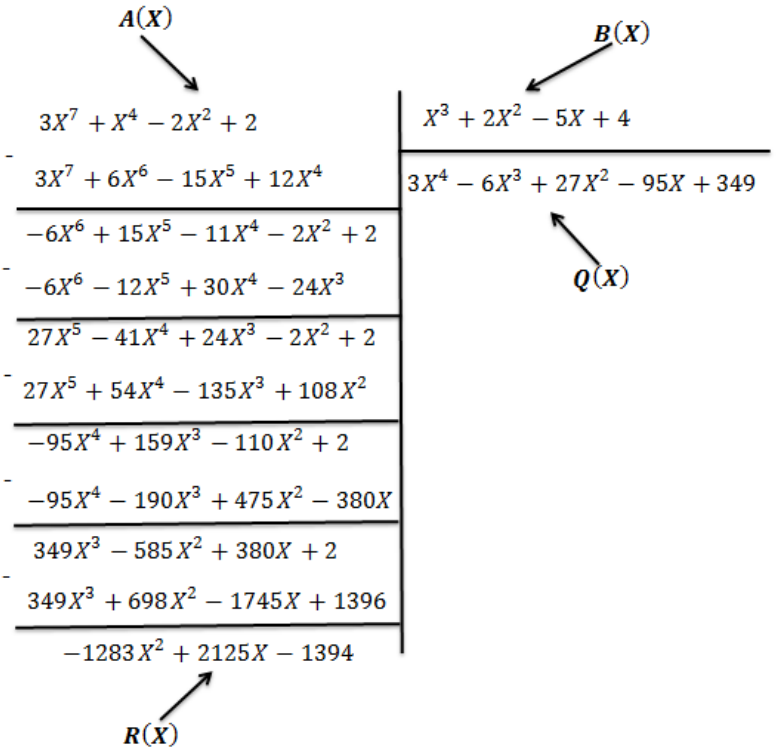
$$A(X) = 3X^7 + X^4 - 2X^2 + 2 \text{ and } B(X) = X^3 + 2X^2 - 5X + 4$$

**2.**

$$A(X) = X^5 + X^4 + 2X^3 - 3X + 2 \text{ and } B(X) = X^2 - 3X + 5$$

**Solution**

**1.**




$$A(X) = B(X)\underbrace{\left(3X^4 - 6X^3 + 27X^2 - 95X + 349\right)}_{Q(X)} + \underbrace{\left(-1283X^2 + 2125X - 1394\right)}_{R(X)},$$

so,

$$Q(X) = 3X^4 - 6X^3 + 27X^2 - 95X + 349$$

$$R(X) = -1283X^2 + 2125X - 1394$$

**2.** In the same method, we find

$$A(X) = B(X)\underbrace{\left(X^3 + 4X^2 + 9X + 7\right)}_{Q(X)} + \underbrace{\left(-27X - 33\right)}_{R(X)},$$

so,

$$Q(X) = X^3 + 4X^2 + 9X + 7$$

$$R(X) = -27X - 33$$

**Exercise 5.2**

Determine the *gcd* of the following polynomials :

**1.**

$$A(X) = X^6 + 7X^4 + 7X^2 - 15 \text{ and } B(X) = X^4 - 1$$

**2.**

$$A(X) = X^4 - 2X^3 - 2X^2 - 2X - 3 \text{ and } B(X) = X^3 + 4X^2 + 8X + 5$$

**Solution**

**1.** Apply the Euclidean algorithm :

$$\begin{aligned} A(X) &= B(X)\underbrace{\left(X^2+7\right)}_{Q_1(X)} + \underbrace{\left(8X^2-8\right)}_{R_1(X)}, \\ B(X) &= R_1(X)\underbrace{\left(\frac{1}{8}X^2+\frac{1}{8}\right)}_{Q_2(X)} + \underbrace{(0)}_{R_2(X)}, \end{aligned}$$

The *gcd* is the last non-zero rest (made unitary), so, we find :

$$gcd(A(X), B(X)) = X^2 - 1.$$

**2.** Apply the Euclidean algorithm :

$$\begin{aligned} A(X) &= B(X)\underbrace{(X-6)}_{Q_1(X)} + \underbrace{\left(14X^2+41X+27\right)}_{R_1(X)}, \\ B(X) &= R_1(X)\underbrace{\left(\frac{1}{14}X+\frac{15}{196}\right)}_{Q_2(X)} + \underbrace{\left(\frac{575}{196}X+\frac{575}{196}\right)}_{R_2(X)}, \\ R_1(X) &= R_2(X)\underbrace{\left(\frac{2744}{575}X+\frac{5292}{575}\right)}_{Q_3(X)} + \underbrace{(0)}_{R_3(X)}. \end{aligned}$$

Thus, we find :

$$gcd(A(X), B(X)) = X + 1$$

**Exercise 5.3**

Montrer que les polynômes $P$ et $Q$ suivants sont premiers entre eux. Trouver $U$ et $V \in \mathbb{R}[X]$ tel que $UP + VQ = 1$ :

**1.**

$$P(X) = X^5 + 2X^4 + 5X^3 + 10X^2 + 4X + 8 \text{ and } Q(X) = X^3 - 7X + 6$$

**2.**

$$P(X) = X^3 - 2X^2 + X - 2 \text{ and } Q(X) = X^2 + 4X + 3$$

**Solution**

**1.** We verify that $\gcd(P, Q) = 1$.

We calculate the successive Euclidean divisions,

$$P(X) = Q(X)\underbrace{\left(X^2 + 2X + 12\right)}_{Q_1(X)} + \underbrace{\left(18X^2 + 76X - 64\right)}_{R_1(X)}$$

$$Q(X) = R_1(X)\underbrace{\left(\frac{1}{18}X - \frac{19}{81}\right)}_{Q_2(X)} + \underbrace{\left(\frac{1165}{81}X - \frac{730}{81}\right)}_{R_2(X)}$$

$$R_1(X) = R_2(X)\underbrace{\left(\frac{1458}{1165}X + \frac{1647216}{271445}\right)}_{Q_3(X)} + \underbrace{\left(-\frac{505440}{54289}\right)}_{R_3(X)}$$

$$R_2(X) = R_3(X)\underbrace{\left(-\frac{12649337}{8188128}X + \frac{3963097}{4094064}\right)}_{Q_4(X)} + \underbrace{(0)}_{R_4(X)}$$

The gcd is the last non-zero rest (made unitary), so

$$\gcd(P, Q) = 1.$$

Find $U$ and $V \in \mathbb{R}[X]$ tel que $UP + VQ = 1$ :

We have

$$R_1(X) = R_2(X)\underbrace{\left(\frac{1458}{1165}X + \frac{1647216}{271445}\right)}_{Q_3(X)} + \underbrace{\left(-\frac{505440}{54289}\right)}_{R_3(X)} \ldots (Eq1).$$

Then

$$\begin{aligned}
(Eq1) \quad &\Leftrightarrow -\tfrac{505440}{54289} = R_1(X) - R_2(X)\left(\tfrac{1458}{1165}X + \tfrac{1647216}{271445}\right) \\
&\Leftrightarrow -\tfrac{505440}{54289} = R_1(X) - \left(Q(X) - R_1(X)\left(\tfrac{1}{18}X - \tfrac{19}{81}\right)\right)\left(\tfrac{1458}{1165}X + \tfrac{1647216}{271445}\right) \\
&\Leftrightarrow -\tfrac{505440}{54289} = R_1(X)\left(1 + \left(\tfrac{1}{18}X - \tfrac{19}{81}\right)\left(\tfrac{1458}{1165}X + \tfrac{1647216}{271445}\right)\right) Q(X)\left(\tfrac{1458}{1165}X + \tfrac{1647216}{271445}\right) \\
&\Leftrightarrow -\tfrac{505440}{54289} = (P(X) - Q(X)(X^2 + 2X + 12))\begin{pmatrix} 1 + \left(\tfrac{1}{18}X - \tfrac{19}{81}\right) \\ \left(\tfrac{1458}{1165}X + \tfrac{1647216}{271445}\right) \end{pmatrix} \\
&\times Q(X)\left(\tfrac{1458}{1165}X + \tfrac{1647216}{271445}\right) \\
&\Leftrightarrow -\tfrac{505440}{54289} = P(X)\left(1 + \left(\tfrac{1}{18}X - \tfrac{19}{81}\right)\left(\tfrac{1458}{1165}X + \tfrac{1647216}{271445}\right)\right) \times \\
&Q(X)\begin{bmatrix} (X^2 + 2X + 12)\left(1 + \left(\tfrac{1}{18}X - \tfrac{19}{81}\right)\left(\tfrac{1458}{1165}X + \tfrac{1647216}{271445}\right)\right) \\ + \left(\tfrac{1458}{1165}X + \tfrac{1647216}{271445}\right) \end{bmatrix}
\end{aligned}$$

so,

$$U(X) = -\left(1 + \left(\tfrac{1}{18}X - \tfrac{19}{81}\right)\left(\tfrac{1458}{1165}X + \tfrac{1647216}{271445}\right)\right) \times \tfrac{54289}{505440}$$

$$V(X) = -\begin{bmatrix} (X^2 + 2X + 12)\left(1 + \left(\tfrac{1}{18}X - \tfrac{19}{81}\right)\left(\tfrac{1458}{1165}X + \tfrac{1647216}{271445}\right)\right) \\ + \left(\tfrac{1458}{1165}X + \tfrac{1647216}{271445}\right) \end{bmatrix} \times \tfrac{54289}{505440}$$

**2.** We verify that $\gcd(P, Q) = 1$.

We calculate the successive Euclidean divisions,

$$P(X) = Q(X)\underbrace{(X - 6)}_{Q_1(X)} + \underbrace{(22X + 16)}_{R_1(X)}$$

$$Q(X) = R_1(X)\underbrace{\left(\frac{1}{22}X + \frac{18}{121}\right)}_{Q_2(X)} + \underbrace{\left(\frac{75}{121}\right)}_{R_2(X)}$$

$$R_1(X) = R_2(X)\underbrace{\left(\frac{2662}{75}X + \frac{1936}{75}\right)}_{Q_3(X)} + \underbrace{(0)}_{R_3(X)}$$

The gcd is the last non-zero rest (made unitary), so

$$\gcd(P, Q) = 1.$$

Find $U$ and $V \in \mathbb{R}[X]$ tel que $UP + VQ = 1$ :

We have

$$Q(X) = R_1(X)\underbrace{\left(\frac{1}{22}X + \frac{18}{121}\right)}_{Q_2(X)} + \underbrace{\left(\frac{75}{121}\right)}_{R_2(X)} \ldots (Eq2).$$

So

$$\begin{aligned}(Eq2) &\Leftrightarrow \tfrac{75}{121} = Q(X) - R_1(X)\left(\tfrac{1}{22}X + \tfrac{18}{121}\right)\\ &\Leftrightarrow \tfrac{75}{121} = Q(X) - (P(X) - Q(X)(X-6))\left(\tfrac{1}{22}X + \tfrac{18}{121}\right)\\ &\Leftrightarrow \tfrac{75}{121} = -\left(\tfrac{1}{22}X + \tfrac{18}{121}\right)P(X) + \left(1 + (X-6)\left(\tfrac{1}{22}X + \tfrac{18}{121}\right)\right)Q(X),\end{aligned}$$

so,

$$U(X) = \left(-\tfrac{1}{22}X - \tfrac{18}{121}\right) \times \tfrac{121}{75} = -\tfrac{11}{150}X - \tfrac{6}{25}$$

$$V(X) = \left(1 + (X-6)\left(\tfrac{1}{22}X + \tfrac{18}{121}\right)\right) \times \tfrac{121}{75} = \tfrac{11}{150}X^2 - \tfrac{1}{5}X + \tfrac{13}{75}.$$

**Exercise 5.4**

Let the polynomial

$$P(X) = X^5 - 7X^4 + 16X^3 - 16X^2 + 15X - 9$$

1. Show that 3 is a double root of the polynomial $P$.

2. Factor $P$ into $\mathbb{R}[X]$.

3. Deduce the roots of $P$ in $\mathbb{C}$.

**Solution**

**1. Show that 3 is a double root of the polynomial $P$.**

We have

$$P'(X) = 5X^4 - 28X^3 + 48X^2 - 32X + 15$$

$$P''(X) = 20X^3 - 84X^2 + 96X - 32$$

$$P(3) = 3^5 - 7 \times 3^4 + 16 \times 3^3 - 16 \times 3^2 + 15 \times 3 - 9 = 0$$

$$\begin{aligned}P'(3) &= 5 \times 3^4 - 28 \times 3^3 + 48 \times 3^2 - 32 \times 3 + 15\\ &= 5 \times 3^4 - 28 \times 3^3 + 48 \times 3^2 - 32 \times 3 + 15\\ &= 405 - 756 + 432 - 96 + 15 = 0\end{aligned}$$

$$\begin{aligned}P''(3) &= 20 \times 3^3 - 84 \times 3^2 + 96 \times 3 - 32\\ &= 540 - 756 + 288 - 32\\ &= 40 \neq 0\end{aligned}$$

So, $P(3) = P'(3) = 0$ and $P''(3) \neq 0$, which shows that 3 is a double root of the polynomial $P$.

**2. Factor $P$ into $\mathbb{R}[X]$.**

We perform the Euclidean division of $P(X)$ by $(X-3)^2$, we obtain :

$$P(X) = (X-3)^2 (X^3 - X^2 + X - 1)$$

We see that

$$\begin{aligned} X^3 - X^2 + X - 1 &= X^2 (X-1) + (X-1) \\ &= (X-1)(X^2+1), \end{aligned}$$

So, we have

$$P(X) = (X-3)^2 (X^2+1)(X-1).$$

**3. Deduce the roots of $P$ in $\mathbb{C}$.**

$$\begin{aligned} P(X) = 0 &\Leftrightarrow (X-3)^2 (X^2+1)(X-1) = 0 \\ &\Leftrightarrow \begin{cases} (X-3)^2 = 0 \\ X^2 + 1 = 0 \\ X - 1 = 0 \end{cases} \\ &\Leftrightarrow \begin{cases} X = 3 \\ X = \pm i \\ X = 1 \end{cases} \end{aligned}$$

So, the roots of $P$ in $\mathbb{C}$ are :

$X = 3$ (*double root* ), $X = i$ (*simple root* ), $X = -i$ (*simple root* ), $X = 1$ (*simple root*).

**Exercise 5.5**

Factorize the following polynomials in $\mathbb{C}[X]$ and then in $\mathbb{R}[X]$ :

$$\begin{aligned} &1 + X^4 \\ &1 - X^8 \\ &1 - (X^2 + 3X - 4)^2 \end{aligned}$$

**Solution**

**1.** We start by looking for the complex roots to factor in $\mathbb{C}[X]$, then we group the conjugate complex roots.

$$1 + X^4 = 0 \Leftrightarrow X^4 = -1 \Leftrightarrow X = e^{\frac{(2k+1)\pi}{4} i}, \text{ with } k \in \{0,1,2,3\},$$

so, the roots of $P$ in $\mathbb{C}$ are :

$$X_0 = e^{\frac{\pi}{4}i} \ , \ X_1 = e^{\frac{3\pi}{4}i} \ , \quad X_2 = e^{\frac{5\pi}{4}i} \ , \ X_3 = e^{\frac{7\pi}{4}i} \ .$$

$$\begin{aligned} 1+X^4 &= (X-X_0)(X-X_1)(X-X_2)(X-X_3) \\ &= [(X-X_0)(X-X_3)]\,[(X-X_1)(X-X_2)] \\ &= (X^2-(X_0+X_3)X+X_0X_3)\,(X^2-(X_1+X_2)X+X_1X_2) \\ &= \left(X^2-\sqrt{2}X+1\right)\left(X^2+\sqrt{2}X+1\right) \end{aligned}$$

The two polynomials $X^2-\sqrt{2}X+1$ and $X^2+\sqrt{2}X+1$ have no real roots, so they are irreducible in $\mathbb{R}[X]$.

**2.**

$$\begin{aligned} 1-X^8 &= (1-X^4)(1+X^4) \\ &= (1-X^2)(1+X^2)(1+X^4) \\ &= (1-X)(1+X)(X-i)(X+i)(1+X^4) \\ &= (1-X)(1+X)(X-i)(X+i)(X-X_0)(X-X_1)(X-X_2)(X-X_3) \\ &= (1-X)(1+X)(1+X^2)\left(X^2-\sqrt{2}X+1\right)\left(X^2+\sqrt{2}X+1\right). \end{aligned}$$

**3.**

$$\begin{aligned} 1-(X^2+3X-4)^2 &= [1-(X^2+3X-4)]\,[1+(X^2+3X-4)] \\ &= (-X^2-3X+5)(X^2+3X-3) \end{aligned}$$

Factorize the polynomial $-X^2-3X+5$

$$\Delta = (-3)^2-4(-1)(5) = 29,$$

then

$$X = \tfrac{-3+\sqrt{29}}{2} \quad \text{or} \quad X = \tfrac{-3-\sqrt{29}}{2}$$

thus

$$-X^2-3X+5 = -\left(X-\tfrac{-3+\sqrt{29}}{2}\right)\left(X-\tfrac{-3-\sqrt{29}}{2}\right)$$

Factorize the polynomial $X^2+3X-3$

$$\Delta = (3)^2-4(1)(-3) = 21,$$

then

$$X = \frac{3-\sqrt{21}}{2} \text{ or } X = \frac{3+\sqrt{21}}{2}$$

thus

$$-X^2 - 3X + 5 = \left(X - \frac{3-\sqrt{21}}{2}\right)\left(X - \frac{3+\sqrt{21}}{2}\right).$$

So,

$$1 - (X^2 + 3X - 4)^2 = \left(X - \frac{3-\sqrt{21}}{2}\right)\left(X - \frac{3+\sqrt{21}}{2}\right)\left(\frac{-3+\sqrt{29}}{2} - X\right)\left(X + \frac{3+\sqrt{29}}{2}\right)$$

## 5.6 Terminology translation

| **English** | **Frensh** |
|---|---|
| Polynomial rings | Anneaux de polynôme |
| Polynomial arithmetic | Arithmétique polynômiale |
| Irreducible polynomials | Polynômes irréductibles |
| Greatest common divisor | Plus grand diviseur commun |
| Factorization | Factorisation |
| Roots of a polynomial | Racines d'un polynôme |
| Multiplicity of roots | Multiplicité des racines |

# Bibliographie


[1] Cours de mathématiques première année : exo7.

[2] Djebbar Samir, Cours maths 1 et exercices avec solutions.

[3] M. Mechab : Cours d'algèbre-LMD sciences et techniques.

[4] M. Mignotte et J. Nervi, Algèbre : licences sciences 1ère année, Ellipses, Paris, 2004.

[5] J. Franchini et J. C. Jacquens, Algèbre : cours, exercices corrigés, travaux dirigés, Ellipses, Paris, 1996.

[6] C. Degrave et D. Degrave, Algèbre 1ère année : cours, méthodes, exercices résolus, Bréal, 2003.

[7] S. Balac et F. Sturm, Algèbre et analyse : cours de mathématiques de première année avec exercices corrigés, Presses polytechniques et universitaires romandes, 2003.