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
DÉPARTEMENT DE MATHÉMATIQUE
وزارة التعليم العالي والبحث العلمي
جامعة وهران للعلوم والتكنولوجيا محمد بوضياف
كلية الرياضيات و الاعلام الالي
قسم الرياضيات

POLYCOPIÉ

Algebra 1

2023/2024

PRÉPARER PAR

NAZIHA BELMAHI

Table des matières

Introduction

This Algebra 1 course is specifically designed for first-year mathematics students in the Department of Mathematics. The course aims to provide a strong foundation in fundamental algebraic concepts that are essential for further study in mathematics.

We will begin with Chapter 1: Logical Reasoning, where the focus will be on understanding logical propositions, mathematical quantifiers, and constructing rigorous proofs. These foundational skills are crucial for approaching more advanced topics.

In Chapter 2: Sets and Applications, we will cover the basic concepts of sets and their we provide some examples for a better understanding. This chapter will introduce essential definitions and provide examples to illustrate these concepts in a broader mathematical context.

Chapter 3: Relations will explore meaning and properties of relations, with a particular focus on equivalence and order relations. Understanding these relations is key to grasping how different mathematical ideas are interconnected.

Chapter 4: Algebraic Structures will cover important algebraic structures such as groups, rings, and fields. This chapter will delve into the abstract properties of these structures and their role in algebraic reasoning.

Finally, Chapter 5: Polynomials will address polynomial rings and polynomial arithmetic.

By the end of this course, students will have a comprehensive understanding of Algebra 1, preparing them for more advanced topics in mathematics.

Chapter 1

Logic Concepts

In this foundational chapter, we deal with the fundamental principles of mathematical logic and proof reasoning. This chapter lays the groundwork essential for the structured and logical exploration of mathematical concepts.

This chapter delves into the intricacies of logical connectors, truth tables, and quantifiers, understanding their role as the bedrock of rigorous mathematical reasoning. Through the exploration of proof methods like direct proofs and proof by contradiction, it will equip the students with the tools necessary to establish the validity of mathematical statements.

1.1 Assertions (Propositions)

Definition 1.1.1. *An assertion (or a logical statement) is a sentence that is either true or false, but not both at the same time.*

Example 1.1.2. *1. "$\sqrt{2}$ is an irrational number" is a true assertion.*

2. "16 is a multiple of 2" is a true assertion.

3. "19 is a multiple of 2" is a false assertion.

4. "Good morning" is not a logical statement.

Assertions are represented by uppercase letters $P, Q, R, \ldots$ If an assertion is true, we assign it the value 1 (or T); if it is false, we assign it the logical value 0 (or F).

Truth Table for Assertion P

P
1
0

Logical Connectors

Logical connectors allow us to create compound statements, called composite assertions, from assertions P, Q, R, ... We can determine the truth value of these compound assertions based on the truth values of P, Q, R, ... The most common logical connectors are "not," "and," "or," "implies," and "if and only if."

Negation

The negation of the assertion P is denoted as $\overline{P}$ (or sometimes $\neg P$), and it is true when P is false. For the logical connector not, we have the following truth table:

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

Example 1.1.3. *"12 is a multiple of 2" is a true statement. Its negation is "12 is not a multiple of 2," which is a false statement.*
"14 is a multiple of 3" is a false statement. Its negation is "14 is not a multiple of 3," which is a true statement. In this example:

It is important to note that the truth value of an assertion and its negation can be evaluated independently.

Conjunction

The conjunction logical connector is represented by the symbol $\wedge$. It allows us to combine two propositions into a single proposition that is true only if both original propositions are true. For example, if P and Q are true propositions, then $P \wedge Q$ (P and Q) is also true.
Let P, Q be two logical statement, we have the following truth table:

P	Q	$P \wedge Q$
1	1	1
1	0	0
0	1	0
0	0	0

Disjunction

The disjunction logical connector is represented by the symbol $\vee$. It allows us to combine two propositions into a single proposition that is true if at least one of the original propositions

is true. For example, if P is a true proposition and Q is a false proposition, then $P \vee Q$ (P or Q) is true.
Let P, Q be two logical statement, we have the following truth table:

P	Q	$P \vee Q$
1	1	1
1	0	1
0	1	1
0	0	0

Remark 1.1.4. *In general, the proposition $P \wedge Q$ is true if both P and Q are true, and false otherwise. The proposition $P \vee Q$ is true if at least one of the propositions P and Q is true, and false otherwise.*

Note that if both P and Q are true, then $P \vee Q$ is true. This is called an "inclusive or."

Remark 1.1.5.

1. *For any proposition P, one of the two propositions P or $\overline{P}$ is true, and the other is false. It follows that the proposition $P \wedge \overline{P}$ is always false, and the proposition $P \vee \overline{P}$ is always true.*

2. *The negation of $P \wedge Q$ is $\overline{P} \vee \overline{Q}$, and the negation of $P \vee Q$ is $\overline{P} \wedge \overline{Q}$*

3. *The proposition "$Q \vee P$" means the same thing as the proposition "$P \vee Q$". Similarly, the proposition "$Q \wedge P$" means the same thing as the proposition "$P \wedge Q$". We say that $\wedge$ and $\vee$ are commutative.*

4. *We can combine $\wedge$, $\vee$, and $\neg$ to form new propositions. It is important to pay attention to the placement of parentheses because the meaning depends on it. For example, let's assume that proposition P is false and proposition Q is true. In this case, $P \wedge (\overline{P} \vee Q)$ is false (because P is false, so P and (any proposition) is always false, regardless of that (proposition)). However, $(P \wedge \overline{P}) \vee Q$ is true (because Q is true, so (any proposition) OR Q is true, regardless of that (proposition)).*

Implication

The implication logical connector is represented by the symbol $\Rightarrow$ (or $\rightarrow$). It establishes a relationship between two propositions, where the first proposition (called the antecedent) implies the second proposition (called the consequent). If the antecedent is true, then the consequent must be true, but if the antecedent is false, we cannot draw any conclusions about the consequent.

Let P, Q be two logical statement, we have the following truth table:

P	Q	$P \Rightarrow Q$
1	1	1
1	0	0
0	1	1
0	0	1

Remark 1.1.6. *1. In practice, if P, Q, and R are three assertions, then the composite assertion $(P \Rightarrow Q) \wedge (Q \Rightarrow R)$ is written as $(P \Rightarrow Q \Rightarrow R)$.*

2. The implication $Q \Rightarrow P$ is called the reciprocal implication of $P \Rightarrow Q$.

3. The implication $\overline{Q} \Rightarrow \overline{P}$ is called the contrapositive implication of $P \Rightarrow Q$.

Examples 1.1.7.

- *Let the following assertions*

  1. *Antecedent P: It is raining.*
  2. *Consequent Q: The ground is wet.*

  In logical notation, this can be written as $P \Rightarrow Q$. If P is true (it is raining), then Q must also be true (the ground is wet). However, if P is false (it is not raining), the implication $P \Rightarrow Q$ is still considered true regardless of whether Q is true or false.

- *Let the following assertions*

  1. *Antecedent P: A number is divisible by 4.*
  2. *Consequent Q: The number is divisible by 2.*

  In logical terms, this is $P \Rightarrow Q$. If a number is divisible by 4, it must be divisible by 2. This implication is always true because divisibility by 4 guarantees divisibility by 2.
  Its contrapositive is " If a number is not divisible by 2, then it is not divisible by 4."
  The contrapositive of this statement is logically equivalent to the original implication. In formal notation, the contrapositive is $\overline{Q} \Rightarrow \overline{P}$. If a number is not divisible by 4, then it is not divisible by 2.

Equivalence

An assertion called the equivalence of P and Q and written as $P \Leftrightarrow Q$, is a statement that is true when P and Q are both true or both false, and false in all other cases. In other words,

if P is true, then Q is true, and if P is false, then Q is false.

Vocabulary: To say that P is equivalent to Q, we also say that P is true if and only if Q is true. We also say that P is a necessary and sufficient condition for Q.

The table below shows that proposition P is equivalent to proposition Q if and only if they are both true or both false.

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
1	1	1	1	1
1	0	0	1	0
0	1	1	0	0
0	0	1	1	1

Properties of Equivalence:

1. P is equivalent to P (equivalence is reflexive).
2. If P is equivalent to Q, then Q is equivalent to P (equivalence is symmetric).
3. If P is equivalent to Q and Q is equivalent to R, then P is equivalent to R (equivalence is transitive).
4. P is equivalent to Q if and only if "not P" is equivalent to "not Q."

Example of Transitivity of Equivalence:
Let a and b be real numbers. Let P, Q, and R be the following propositions:

$P : a + 1 > b + 1$

$Q : a > b$

$R : a - b > 0$

Since P is equivalent to Q and Q is equivalent to R, we can conclude that P is equivalent to R.

1.2 Mathematical Quantifiers

Definition 1.2.1. *Let E be a set. A predicate on E is a statement containing variables, such that when each of these variables is replaced by an element of E, we obtain a proposition (statement). A predicate containing the variable x will be denoted as $P(x)$.*

Example 1.2.2. *The statement $P(n)$ defined as "n is a multiple of 2" is a predicate on $\mathbb{N}$. It becomes a proposition when we assign an integer value to n. For example:*

1. *The proposition $P(10)$ defined as "10 is a multiple of 2" is true when n is replaced by 10.*
2. *The proposition $P(11)$ defined as "11 is a multiple of 2" is false when n is replaced by 11.*

Starting from a predicate $P(\cdot)$ defined on a set E, we can construct new statements called quantified statements using the quantifiers "there exists ($\exists$)" and "for all ($\forall$)".

Definition 1.2.3. *Let $P(\cdot)$ be a predicate defined on a set E.*

1. *The quantifier "for all" (also called "for every") denoted as $\forall$, enables the formulation of the quantified statement "$\forall x \in E, P(\cdot)$" which is true when all elements x of E satisfy $P(\cdot)$.*
2. *The quantifier "there exists" denoted as $\exists$, allows defining the quantified statement "$\exists x \in E, P(x)$" which is true when at least one element x_0 belonging to E satisfies the statement $P(x)$.*

Remark 1.2.4. *There exists a unique $x \in E$, $P(x)$, is noted "$\exists! x \in E, P(x)$".*

Example 1.2.5. 1. *The statement "$x^2+2x-3 < 0$" is a predicate defined on $\mathbb{R}$. It can be true or false depending on the value of x. The quantified statement "$\forall x \in]-3,1[, x^2+2x-3 < 0$" is a true statement because the quantity $x + 2x - 3$ is strictly negative for all x belonging to the open interval $]-3,1[$.*

2. *The quantified statement "$\exists x \in \mathbb{R}, x^2 = 4$" is true because there exists (at least) one element x in $\mathbb{R}$ that satisfies $x^2 = 4$. This is the case for the two real numbers -2 and 2.*

Negation Rules for Quantified Statements

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 for which the statement $P(x)$ is true" is "for every element x in E, the statement $P(x)$ is false."

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

Examples 1.2.6. 1. *The negation of $(\exists x \in (0,+\infty), x > 1)$ is $(\forall x \in (0,+\infty), x \leq 1)$.*

2. The negation of $(\forall x \in \mathbb{R}, 2x+2=0)$ *is* $(\exists x \in \mathbb{R}, 2x+2 \neq 0)$.

Remark 1.2.7. *It is not more difficult to write the negation of complex sentences. For the assertion*

$(\forall x \in E, P(x) \Rightarrow Q(x))$, *its negation is* $(\exists x \in E, P(x) \wedge \overline{Q(x)})$. *Since*

$$\Big(\forall x \in E, P(x) \Rightarrow Q(x)) \Leftrightarrow (\forall x \in E, \overline{P(x)} \vee Q(x)\Big).$$

1.3 Logical reasoning for proofs

There are many ways to prove mathematical statements. Here we will outline some usual techniques.

Direct reasoning

To show that the logical implication $P \Rightarrow Q$ is true, we need to assume that P is true and demonstrate that Q is true as a result. Which means, suppose that P is true (assumption). Use logical laws and reasoning to deduce Q from P.

Example 1.3.1. *Prove that, if* $a, b \in \mathbb{Q},\ a+b \in \mathbb{Q}$.
We have $a,\ b \in \mathbb{Q}$, *means* $a = \frac{p}{q}$ *and* $b = \frac{p'}{q'}$, *with* $p, p' \in \mathbb{Z}$ *and* $q, q' \in \mathbb{Z}^*$ *then*

$$a+b = \frac{pq'+p'q}{qq'} \in \mathbb{Q},\ (pq'+p'q \in \mathbb{Z} \text{ and } qq' \in \mathbb{Z}^*).$$

Case by case reasoning

To verify an assertion $P(x)$ for all $x \in E$, we prove the assertion for x belonging to a set A of E, then for the x that doesn't belong to A and belong to E. This is the disjunction method or case by case.

Example 1.3.2. *Prove that* $\forall n \in \mathbb{N}$, $\frac{n(n+1)}{2}$ *is an integer.*
We distinct two cases

(a) *If* n *is even, then* $n = 2k$, *and* $n+1 = 2k+1$ *with* $k \in \mathbb{N}$, *thus*

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

which is clearly an integer number.

(b) *If* n *is odd, then* $n = 2k+1$, *and* $n+1 = 2k+2 = 2(k+1)$ *with* $k \in \mathbb{N}$, *thus*

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

which is also an integer number.

Contrapositive reasoning

Contrapositive reasoning is a logical method based on the principle that if a logical implication is true, then its contrapositive is also true. Consider a logical implication of the form "If P, then Q" (P implies Q). The contrapositive of this implication is "If not Q, then not P" ($\overline{Q}$ implies $\overline{P}$). To demonstrate the validity of the initial implication, we can prove that its contrapositive is true. Contrapositive reasoning is useful when a direct proof of the initial implication is difficult. By proving the contrapositive, we can obtain a simpler or more direct proof.

Example 1.3.3. *Let $a, b > 0$. Prove that, if $a \neq b$ then $\frac{a}{b+1} \neq \frac{b}{a+1}$.*
The contrapositive of this proposition is "if $\frac{a}{b+1} = \frac{b}{a+1}$ then $a = b$"

$$\begin{aligned} \frac{a}{b+1} = \frac{b}{a+1} &\Rightarrow a(a+1) = b(b+1) \\ &\Rightarrow (a-b)(a+b+1) = 0. \end{aligned}$$

This implies $a - b = 0$ or $a + b + 1 = 0$. Since $a,\ b > 0$, then $a = b$.

Contradiction reasoning

Proof by contradiction is a logical method used to prove a proposition by initially assuming its negation and then demonstrating that it leads to a contradiction or an absurdity.

Example 1.3.4. *Proof that $\sqrt{2}$ is not a rational number.*
Suppose that $\sqrt{2} = \frac{m}{n}$, with $pgcd(m, n) = 1$, so that $2n^2 = m^2$. Which means that m^2 is even, this implies that m is even. Which means $m = 2k$, $k \in \mathbb{Z}$. Then $2n^2 = 4k^2$, which implies that $n^2 = 2k^2$. Hence, m^2 is even, this implies that n is even. Therefore, 2 is a common divisors for n and m, which is a contradiction with $pgcd(m, n) = 1$.

Reasoning by counter-example

The reasoning by counterexample is a logical method used to refute a proposition or statement by presenting a concrete example that contradicts it. If we need to prove an assertion of the form $\forall x \in E,\ P(x)$ is true, we need to prove $P(x)$ true for all $x \in E$. However, if we want to prove that this assertion is false, then we need to find $x \in E$ such that $P(x)$ is false.

Example 1.3.5. *Prove that the following assertion is false "Every positif integer is the sum of three squares."*
Let $a = 7$ an integer number. However, the squares less than 7 are just 1 and 4, which means 7 can't be the sum of three squares. Hence, the propositions is false.

Induction reasoning

Induction is a method of mathematical proof used to establish that a statement $P(n)$ holds true for all natural numbers.
The process of mathematical induction consists of three main steps:

1. We prove that the statement is true for the first value, n_0. This serves as the base case for the induction.

2. We assume that the statement is true for an arbitrary value k, which is known as the inductive hypothesis.

3. We prove that if the statement is true for k, it is also true for $k+1$. This completes the induction step.

Example 1.3.6. *Prove that* $1+2+3+...+n = \frac{1}{2}n(n+1)$.

Note the proposition $1+2+3+...+n = \frac{1}{2}n(n+1)$ by (P_n). Let $n=1$, P_1 is true $(1 = \frac{1}{2}(1)(2))$. Suppose that (P_n) is true and prove that (P_{n+1}) is true.

$$(P_{n+1}):\ 1+2+3+...+n+(n+1) = \frac{1}{2}(n+1)(n+2).$$

We have

$$\begin{aligned} 1+2+3+...+n+(n+1) &= \frac{1}{2}n(n+1)+(n+1) \\ &= (n+1)(\frac{1}{2}n+1) \\ &= \frac{1}{2}(n+1)(n+2). \end{aligned}$$

Which means (P_{n+1}) is true. Then the proposition (P_n) is true.

1.4 Some exercises with solutions

Exercise 1.4.1. *Let P, Q and R three propositions, prove that* $(P \Rightarrow Q) \Leftrightarrow (\overline{P} \vee Q)$; $(P \Rightarrow Q) \Leftrightarrow (\overline{Q} \Rightarrow \overline{P})$.

Solution

Let P, Q and R three propositions

- $(P \Rightarrow Q) \Leftrightarrow (\overline{P} \vee Q)$

P	Q	$\overline{P}$	$P \Rightarrow Q$	$\overline{P} \vee Q$	$\Leftrightarrow$
1	1	0	1	1	1
1	0	0	0	0	1
0	1	1	1	1	1
0	0	1	1	1	1

- $(P \Rightarrow Q) \Leftrightarrow (\overline{Q} \Rightarrow \overline{P})$

P	Q	$\overline{P}$	$\overline{Q}$	$P \Rightarrow Q$	$\overline{Q} \Rightarrow \overline{P}$	$\Leftrightarrow$
1	1	0	0	1	1	1
1	0	0	1	0	0	1
0	1	1	0	1	1	1
0	0	1	1	1	1	1

Exercise 1.4.2. *Let A, B two sets in $\mathbb{R}$, write using $\forall$, $\exists$ the following assertions:*

$$A = \emptyset,\ A \subset B,\ A \nsubseteq B.$$

Solution

Let A, B two sets in $\mathbb{R}$

- $A = \emptyset \Leftrightarrow \forall x \in \mathbb{R},\ x \notin A.$
- $A \subset B \Leftrightarrow \forall x \in A,\ x \in B.$
- $A \nsubseteq B \Leftrightarrow \exists x \in A,\ x \notin B.$

Exercise 1.4.3. *Give the negation of the following assertions, Are these assertions true or false?*

a) $\exists x \in \mathbb{R},\ \forall y \in \mathbb{R},\ x + y > 0.$

b) $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ x + y > 0.$

Solution :

a) The negation of the proposition (a) is $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ x + y \leq 0.$

The proposition $\exists x \in \mathbb{R},\ \forall y \in \mathbb{R},\ x + y > 0$ is false

(Since, it is sufficient to choose $x = -y - 1$, then $x + y < 0$).

b) The negation of the proposition (b) is $\exists x \in \mathbb{R},\ \forall y \in \mathbb{R},\ x + y \leq 0$.
The proposition $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ x + y > 0$ is true
(Let $x \in \mathbb{R}$, consider $y = -x + 1$).

Exercise 1.4.4. *Let $A = \{2, 3, 6, 8\}$, determine the truth value of each of the following propositions*

1. *$\exists x \in A$, such that $x + 2 = 4$.*
2. *$\forall x \in A$, $x + 3 < 9$.*
3. *$\forall x \in A$, $x + 4 \geq 11$.*
4. *$\exists x \in A$, such that x is even.*
5. *$\exists x \in A$, such that $x - 5$ is a natural number.*

Solution :
Let $A = \{2, 3, 6, 8\}$. We evaluate the truth value of each proposition:

1. $\exists x \in A$, such that $x + 2 = 4$.
   Solution: Solving $x + 2 = 4$, we find $x = 2$. Since $2 \in A$, this proposition is **true**.
2. $\forall x \in A$, $x + 3 < 9$.
   Solution: Evaluate $x + 3$ for each $x \in A$:
   $$2 + 3 = 5, \quad 3 + 3 = 6, \quad 6 + 3 = 9, \quad 8 + 3 = 11.$$
   Since $8 + 3 = 11 \geq 9$, this proposition is **false**.
3. $\forall x \in A$, $x + 4 \geq 11$.
   Solution: Evaluate $x + 4$ for each $x \in A$:
   $$2 + 4 = 6, \quad 3 + 4 = 7, \quad 6 + 4 = 10, \quad 8 + 4 = 12.$$
   Since $6, 7, 10 < 11$, this proposition is **false**.
4. $\exists x \in A$, such that x is even.
   Solution: The even numbers in A are $2, 6, 8$. Since these exist, the proposition is **true**.
5. $\exists x \in A$, such that $x - 5$ is a natural number.
   Solution: Solve $x - 5 \geq 0$, which gives $x \geq 5$. The numbers $6, 8 \in A$ satisfy this condition. Hence, the proposition is **true**.

Exercise 1.4.5. (I) *Using the quantifiers $\forall$ and $\exists$, write the following*

1. *For all real number x, its square is positif.*
2. *For any natural number n, there exists a real number x, such that the exponential of x is equal to n.*
3. *Let f be a function defined from $\mathbb{R}$ to $\mathbb{R}$ such that*
   - *f is the zero function.*
   - *f is constant.*
   - *f is an even function.*

(II) *Write the negation of the previous propositions.*

Solution :

(I) Writing with quantifiers:

1. For all real numbers x, its square is positive:

   $$\forall x \in \mathbb{R},\ x^2 \geq 0.$$

2. For any natural number n, there exists a real number x, such that the exponential of x equals n:

   $$\forall n \in \mathbb{N},\ \exists x \in \mathbb{R},\ e^x = n.$$

3. Let f be a function $f : \mathbb{R} \to \mathbb{R}$:

   - f is the zero function:

     $$\forall x \in \mathbb{R},\ f(x) = 0.$$

   - f is constant:

     $$\exists c \in \mathbb{R},\ \forall x \in \mathbb{R},\ f(x) = c.$$

   - f is an even function:

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

(II) Negations:

1. $\exists x \in \mathbb{R},\ x^2 < 0.$

2. $\exists n \in \mathbb{N},\ \forall x \in \mathbb{R},\ e^x \neq n.$

3. For $f : \mathbb{R} \to \mathbb{R}$:

   - f is not the zero function:

     $$\exists x \in \mathbb{R},\ f(x) \neq 0.$$

   - f is not constant:

     $$\forall c \in \mathbb{R},\ \exists x \in \mathbb{R},\ f(x) \neq c.$$

   - f is not an even function:

     $$\exists x \in \mathbb{R},\ f(-x) \neq f(x).$$

Exercise 1.4.6. *Prove that*

1. $\forall n \in \mathbb{N}$, *if* n^2 *is even then* n *is even.*

2. $\forall x, y \in \mathbb{R}$, *if* $x \neq 2$ *and* $y \neq 2$ *then* $xy - 2x - 2y + 4 \neq 0$.

3. $\forall x, y \in \mathbb{R},\ xy \leq \frac{1}{2}(x^2 + y^2)$.

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

Solution :

1. Prove: $\forall n \in \mathbb{N}$, n^2 is even $\implies$ n is even.
   Using contrapositive, $\big(\forall n \in \mathbb{N}$, n is odd $\implies$ n^2 is even.$\big)$ If n is odd, then $n = 2k + 1$ for some $k \in \mathbb{N}$. This implies $n^2 = (2k+1)^2 = 4k^2+2k+1 = 2(2k^2+k)+1$, where $2k^2+k \in \mathbb{N}$. Hence, n^2 is odd.

2. Prove: $\forall x, y \in \mathbb{R}$, $x \neq 2$ and $y \neq 2$ $\implies$ $xy - 2x - 2y + 4 \neq 0$.
   Using contrapositive, $\forall x, y \in \mathbb{R},\ xy - 2x - 2y + 4 = 0 \implies x = 2$ or $y = 2$.
   We have $xy - 2x - 2y + 4 = (x - 2)(y - 2) = 0$. Then, $(x - 2) = 0$ or $(y - 2) = 0$.
   Which implies, $x = 2$ or $y = 2$.

3. Prove: $\forall x, y \in \mathbb{R},\ xy \leq \frac{1}{2}(x^2 + y^2)$.
   We have $(x - y)^2 \geq 0$

   $$x^2 + y^2 \geq 2xy \implies \frac{1}{2}(x^2 + y^2) \geq xy.$$

4. Prove: $\forall n \in \mathbb{N}, \sum_{k=0}^{n} 2^k = 2^{n+1} - 1$.

   Use induction:

   - Base case ($n = 0$): $\sum_{k=0}^{0} 2^k = 2^0 = 1$, and $2^{0+1} - 1 = 1$. True.
   - Inductive step: Assume true for n, prove for $n + 1$:

     $$\sum_{k=0}^{n+1} 2^k = \sum_{k=0}^{n} 2^k + 2^{n+1}.$$

     By the inductive hypothesis:

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

     Thus, the result holds.

Chapter 2

Sets and applications

This chapter introduces fundamental concepts of sets, elements, subsets, and set operations (union, intersection, complement) that are frequently used in linear algebra, it focuses also on functions and mappings, including injective, surjective, and bijective functions. It explores the composition of functions and the concept of reciprocal functions, which are crucial for understanding transformations and operations. Additionally, it discusses the direct and inverse images of sets under a function, providing students with the essential tools to represent and analyze mathematical relationships and functions.

2.1 Sets

Definition 2.1.1. *(Sets in Extension and Comprehension) A set $E = \{a, b, ...\}$ defined by listing its elements $a, b, ...$ is called a set defined in extension. If $E = \{x, P(x)\}$ is the set of elements x that satisfy the proposition P, then E is called a set defined in comprehension.*

Example 2.1.2.

- *$\{1, 2\}$ is a set defined in extension.*
- *$\{x \in \mathbb{R},\ x^2 - 2 = 0\}$ is a set defined in comprehension.*

Definition 2.1.3. *(Special Sets)*

- *The empty set, denoted by $\emptyset$, is a set that does not contain any elements.*
- *A set with only one element is called a singleton.*
- *A set with exactly two distinct elements is called a pair.*
- *The cardinality of a set E, denoted as $card(E)$, is the number of elements in a finite set.*

Definition 2.1.4. *(Set Inclusion) A set F is said to be contained in, a subset of, or included in set E, denoted as $F \subseteq E$, if every element of F is also an element of E. If there exists at least one element in F that is not in E, it is denoted as $F \nsubseteq E$.*

Remark 2.1.5. *(Properties of Set Inclusion)*

- *Every set E is a subset of itself (reflexivity). $E \subseteq E$.*
- *If set F is a subset of set E and set G is a subset of set F, then G is also a subset of E (transitivity). If $F \subseteq E$ and $G \subseteq F$, then $G \subseteq E$.*
- *If E and F are sets such that $E \subseteq F$ and $F \subseteq E$, then E and F have the same elements, and they are equal $E = F$ (Antisymmetry).*
- *If $F \subset E$, then $Card(F) \leq Card(E)$.*

Definition 2.1.6. *(Power set) Let E be a set, the subsets of E form a set called set of parts of E (Power set) and noted $\mathcal{P}(E)$(The set of all subsets of E). In other words, $A \in \mathcal{P}(E)$ means $A \subset E$.*

Remark 2.1.7. *The elements of $\mathcal{P}(E)$ are subsets of E and not elements in E. Moreover, unlike the set E that can be empty, the set of $\mathcal{P}(E)$ can't be empty, because it contains at least E, $\emptyset$.*

Example 2.1.8. *If $E = \{a, b, c\}$ then*

$$\mathcal{P}(E) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, E\}.$$

Proposition 2.1.9. *If E is a finite set of cardinal n, the $\mathcal{P}(E)$ is also finite with $Card(\mathcal{P}(E)) = 2^n$.*

Definition 2.1.10. *(Complement) If $F \subseteq E$, the complement of F in E is the set $C_E F$, also denoted as F^c or F_E^c, defined by*

$$F^c = \{x \in E,\ x \notin F\}.$$

Example 2.1.11. *Let $F = \{x \in \mathbb{N},\ 0 \leq x \leq 6\}$ be a set, it's complement in $\mathbb{N}$ is*

$$F_{\mathbb{N}}^c = \{x \in \mathbb{N},\ x > 6\}.$$

However, it's complement in $\mathbb{Z}$ is

$$F_Z^c = \{x \in \mathbb{Z},\ x < 0 \text{ or } x > 6\} \neq F_{\mathbb{N}}^c.$$

Definition 2.1.12. *(Intersection) The intersection of two sets E and F is the set $E \cap F$ consisting of elements x that are both in E and in F. Two sets E and F are said to be disjoint if $E \cap F = \emptyset$.*

$$E \cap F = \{x \mid x \in E \text{ and } x \in F\}.$$

Proposition 2.1.13. *1. $E \cap F = F \cap E$ (commutativity).*

2. $E \cap (F \cap G) = (E \cap F) \cap G$ (associativity).

3. $(E \subset (F \cap G)) \Leftrightarrow [(E \subset F) \text{ and } (E \subset G)]$.

Definition 2.1.14. *(Union) The union of two sets E and F is the set $E \cup F$ consisting of elements x that are in E.*

$$E \cup F = \{x \mid x \in E \text{ or } x \in F\}.$$

Proposition 2.1.15. *Let F, G two subsets of E we have the following relations, called Morgan's laws*

- $(F \cap G)^c = F^c \cup G^c$.
- $(F \cup G)^c = F^c \cap G^c$.

Proposition 2.1.16. *Let F and G two subsets of E, then*

1. $(F^c)^c = F$.

2. $F \cap F^c = \emptyset, \quad F \cup F^c = E$.

3. $F \subseteq G \iff G^c \subseteq F^c$.

Proposition 2.1.17. *Let F, G two finite parts of a set E, then*

$$Card(F \cup G) = Card(F) + Card(G) - Card(F \cap G).$$

Definition 2.1.18. *(Cartesian Product) The Cartesian product of two sets E and F is the set*

$$E \times F = \{(x, y) \mid x \in E, y \in F\}.$$

The diagonal of a set E is given by

$$\Delta_E = \{(x, x) \mid x \in E\} \subseteq E \times E.$$

Proposition 2.1.19. *Let E, F two finite non empty sets, we have $Card(E \times F) = Card(E) \times Card(F)$.*

Definition 2.1.20. *(Difference) If E and F are two sets, the difference $E \setminus F$ between E and F is the set of elements of E that are not in F.*

$$E \setminus F = \{x \mid \ x \in E,\ x \notin F\}$$

The symmetric difference $E\Delta F$ of E and F is given by

$$E\Delta F = (E \setminus F) \cup (F \setminus E).$$

Remark 2.1.21. *If $F \subset G$, then $F \setminus G = \emptyset$.*

Definition 2.1.22. *(Partition of a set)*

1. *For a non-empty set E, a partition $A = \{A_1, A_2, \ldots, A_n\}$ of E is a set of non-empty subsets of E such that $E = \bigcup_{i=1}^{n} A_i = A_1 \cup A_2 ... \cup A_n$ and $A_i \cap A_j = \emptyset$ for $i \neq j$.*
2. *For a partition $A = \{A_1, A_2, \ldots, A_n\}$ of a set E, each set A_i is called a cell of the partition.*

2.2 Functions and Applications

2.2.1 Functions

Definition 2.2.1. *A correspondence f from E to F is called a function if every element x in E has at most one corresponding element y in F.*

- *We say that E is the domain or (the source set), and F is called the codomain or (the target set).*
- *The element associated to x by f, is called the image of x and it is noted $f(x)$ (means $y = f(x)$).*
- *The domain of definition of a function f (denoted by D_f) is the set of elements x of E for which $f(x)$ exists.*

Examples 2.2.2. 1. *The following correspondence is a function*

$$\{(1, 2), (-1, 1), (3, 3)\}.$$

Where, the first component is the input, and the second one is output.

2. *The following correspondence is not a function*

$$\{(1, 2), (1, 4), (3, 3)\}.$$

Since, there is an input has two different outputs.

3. *The correspondence g that associates each integer with its square is indeed a function, and we can write it as $g : \mathbb{N} \longrightarrow \mathbb{N}$, for $g(n) = n^2$, the domain of g is $D_g = \mathbb{N}$.*

Definition 2.2.3. *Let*

$$\begin{aligned} f :& E \longrightarrow F \\ & x \longmapsto f(x) \end{aligned}$$

be a function, A is a subset of E and B is a subset of F.

1. *The image of A by f is*
$$f(A) = \{f(x),\ x \in A \cap D_f\}.$$

2. *The preimage (or inverse image) of B by f is*
$$f^{-1}(B) = \{x \in E,\ f(x) \in B\}.$$

3. *Let $f : E \longrightarrow F$, if $A \subset E$, we call graph of A, and we note it $G_f(A)$, the subset of $E \times F$ formed by the couples $(x, f(x))$ such that $x \in A \cap D_f$. Which means*
$$G_f(A) = \{(x, f(x)) \in E \times F \mid x \in A \cap D_f\}.$$

Examples 2.2.4. 1. *Let $g : \mathbb{Z} \longrightarrow \mathbb{N}$ be a function such that $g(n) = n^2$. $G_g = \{(n, n^2) \mid n \in \mathbb{Z}\}$, $g(\{-1, 1, 0, 2, 3\}) = \{0, 1, 4, 9\}$, $g^{-1}(\{9\}) = \{-3, 3\}$.*

2. *Let $h : \mathbb{R}^* \longrightarrow \mathbb{R}$ defined by $h(x) = \frac{1}{x}$.*
$G_h = \{(x, \frac{1}{x}) \mid x \in \mathbb{R}^*\}$, $h([-1, 2]) =]-\infty, -1] \cup [\frac{1}{2}, +\infty[$, and
$$h^{-1}([2, 3]) = \left[\frac{1}{3}, \frac{1}{2}\right].$$

2.2.2 Representations of Functions

The representation of a function $f : E \longrightarrow F$ depends on the nature of the sets E and F. The most commonly used representations are as follows

1. **Representation using a formula**.
Example: Let's consider the function $g : \mathbb{Z} \longrightarrow \mathbb{N}$ such that $g(n) = n^2$.

2. **Representation using a table of values** (useful when A is finite).
Example: Let's consider the function $h : \{-2, -1, 0, 1, 2\} \longrightarrow \mathbb{N}$ such that:

n	-2	-1	0	1	2
h(n)	4	1	3	1	0

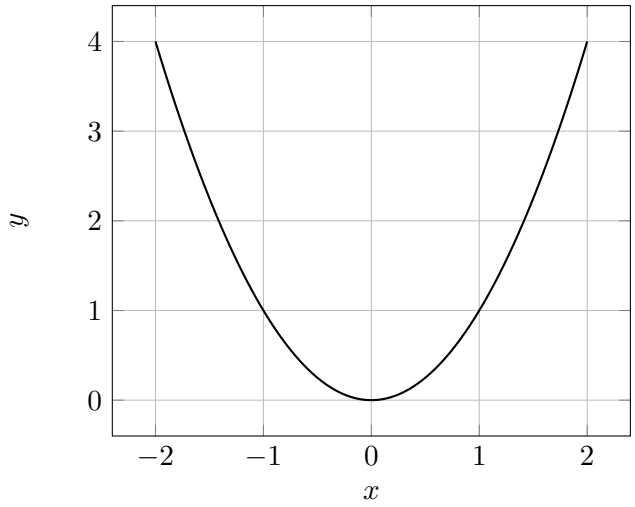


Figure 2.1: The graph of $k(x) = x^2$.

3. **Representation using a graph**. Example: Let's consider the function $k : \mathbb{R} \longrightarrow \mathbb{R}$ such that $k(x) = x^2$. See the graph below:

Definition 2.2.5. *(Composition of functions) The composition of the function $f : E \longrightarrow F$ and the function $g : F \longrightarrow G$ is the function*

$$\begin{aligned} g \circ f :& E \longrightarrow G \\ & x \longmapsto g(f(x)). \end{aligned}$$

Example 2.2.6. *Let the functions f, g defined from $\mathbb{R}$ to $\mathbb{R}$ given by $f(x) = 3x - 2$ and $g(x) = x^2$. The composition of f followed by g is the function $g \circ f : \mathbb{R} \longrightarrow \mathbb{R}$, such that $g \circ f(x) = g(f(x)) = (3x - 2)^2$.*

2.2.3 Applications

Definition 2.2.7. *A function f is an application (mapping) if every element of E has (exactly) one image in F. We denote by $\mathcal{F}(E, F)$ the set of all applications from E to F. A function f is an application if and only if its domain of definition is all of E.*

Examples 2.2.8.

1. *The function $g : \mathbb{Z} \longrightarrow \mathbb{N}$, defined by $g(n) = n^2$, is a mapping from $\mathbb{Z}$ to $\mathbb{N}$.*
2. *The function $f : \mathbb{R} \longrightarrow \mathbb{R}$, defined by $f(x) = \frac{1}{x}$ is not a mapping, because $D_f = \mathbb{R}^* \neq \mathbb{R}$.*
3. *The function $Id_E : E \longrightarrow E$, defined by $Id_E(x) = x$, is a specific mapping called the identity mapping of E.*

2.2.4 Restriction and Extension

Let $f : E \longrightarrow F$ be a mapping.

1. The restriction of f to a subset E_0 of E is the mapping $g : E_0 \longrightarrow F$ defined by $g(x) = f(x)$ for all $x \in E_0$ (g is often denoted as $f_{|E_0}$).

2. The extension of f to a set $\tilde{E}$ containing E is the function $h : \tilde{E} \longrightarrow F$ defined by $h(x) = f(x)$ for all $x \in E$.

Example 2.2.9. *Let the mapping $f : \mathbb{Z} \longrightarrow \mathbb{N}$ be defined by $f(n) = |n|$. The restriction of f to $\mathbb{N}$ is the identity mapping $Id_{\mathbb{N}}$. We can also say that the mapping f is an extension of $Id_{\mathbb{N}}$.*

Remark 2.2.10. *The restriction is always unique, but an extension is not unique.*

2.2.5 Equality of mappings

Two mappings $f : E \longrightarrow F$ and $g : E' \longrightarrow F'$ are equal if $E = E'$, $F = F'$, and for all $x \in E$, we have $f(x) = g(x)$. In this case, we write $f = g$.

Example 2.2.11. *The mappings f and g defined from $\mathbb{N}$ to $\mathbb{Z}$ by $f(n) = cos(\pi n)$ and $g(n) = (-1)^n$ are equal, and we can write $f = g$.*

Proposition 2.2.12. *Let $f : E \longrightarrow F$ be an application.*

1. *Let A and B be two subsets of F. Then*

   (a) *If $A \subset B$, then $f^{-1}(A) \subset f^{-1}(B)$.*

   (b) *We always have $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.*

   (c) *We always have $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.*

2. *Let A and B be two subsets of E. Then*

   (a) *If $A \subset B$, then $f(A) \subset f(B)$.*

   (b) *We always have $f(A \cup B) = f(A) \cup f(B)$.*

   (c) *We always have $f(A \cap B) \subset f(A) \cap f(B)$.*

3. **(a)** *If A is a subset of E, then $A \subseteq f^{-1}(f(A))$.*

   (b) *If B is a subset of F, then $f(f^{-1}(B)) \subseteq B$.*

2.2.6 Injection, Surjection, Bijection

Definition 2.2.13. *(injection"one to one") Let E and F be two sets, and let $f : E \longrightarrow F$ be a function.*
f is injective if every element of F has at most one pre-image in E. In other words:

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

Also, it can be written using the contrapositive as follow

$$\forall x, y \in E,\ x \neq y \Rightarrow f(x) \neq f(y).$$

Examples 2.2.14.

1. *The function $f : \mathbb{R} \longrightarrow \mathbb{R}$ such that $f(x) = 3x + 1$ is one to one, since $f(x) = f(y)$ implies $3x + 1 = 3y + 1$. Hence $x = y$.*
2. *The function $f : \mathbb{R}^* \longrightarrow \mathbb{R}$ such that $f(x) = \frac{1}{x}$ is one to one, since $f(x) = f(y)$ implies $\frac{1}{x} = \frac{1}{y}$. Hence $x = y$.*
3. *The function $f : \mathbb{R} \longrightarrow \mathbb{R}^+$ such that $f(x) = x^2$ is not one to one, since $f(-1) = f(1)$.*

Theorem 2.2.15. *Let $f : E \longrightarrow F$ be a function. The following assertions are equivalents*

1. *f is injective.*
2. *For all $(x, y) \in E^2$, $x \neq y$ implies $f(x) \neq f(y)$.*
3. *For all $b \in F$, the equation $f(x) = b$ has at most one solution x.*

Proof : To prove this theorem, it is sufficient to prove 1) $\Rightarrow$ 2) $\Rightarrow$ 3) $\Rightarrow$ 1).

- 1) $\Rightarrow$ 2), this implication can be obtained easily by using the contrapositive of the injectivity definition.
- 2) $\Rightarrow$ 3), suppose that the equation $f(x) = b$ has two solutions x, y or more, which means $x \neq y$, using 2), we get $f(x) \neq f(y)$,i.e., $b \neq b$ which is a contradiction. Hence, the equation $f(x) = b$ has at most one solution.
- 3) $\Rightarrow$ 1), Let $x, y \in E$ such that $f(x) = f(y)$, then x is a solution of $f(x) = b$, $b \in F$, and also y is a solution of $f(y) = b$. Using 3), x can't be different of y, which means $x = y$. Hence, f is injective.

□

Definition 2.2.16. *(Surjection"Onto") f is surjective if every element of F has at least one pre-image in E. In other words:*

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

Examples 2.2.17.

1. *The function $f : \mathbb{R} \longrightarrow \mathbb{R}$ such that $f(x) = 3x + 1$ is surjective, since*

$$\forall y \in \mathbb{R},\ \exists x = \frac{y-1}{3} \in \mathbb{R}, f(x) = y.$$

2. *The function $f : \mathbb{R}^* \longrightarrow \mathbb{R}$ such that $f(x) = \frac{1}{x}$ is not surjective, since $y = 0$ has no antecedent.*

3. *The function $f : \mathbb{R} \longrightarrow \mathbb{R}^+$ such that $f(x) = x^2$ is surjective, since*

$$\forall y \in \mathbb{R}^+,\ \exists x = \pm\sqrt{y} \in \mathbb{R}, f(x) = y.$$

Theorem 2.2.18. *Let $f : E \longrightarrow F$ be a function. The following assertions are equivalents*

1. *f is surjective.*

2. *$f(E) = F$.*

3. *For all $b \in F$, the equation $f(x) = b$ has at least one solution x.*

Proof :

- Show that 1) implies 2). If f is surjective, then for every y in F, there exists x in E such that $y = f(x)$. Thus, y is in $f(E)$, and since $f(E)$ is a subset of F, it follows that 2) holds.

- Show that 2) implies 3). If 2) holds, then for every $b \in F$, there exists at least one x in E such that $b = f(x)$, which means x is a solution to the equation.

- Show that 3) implies 1). If 3) holds, then for every y in F, there is at least one solution x to the equation $f(x) = y$, which means x is a pre-image of y.

□

Definition 2.2.19. *(Bijection) f is bijective if it is both injective and surjective (every element of F has exactly one pre-image in E).*

Examples 2.2.20.

1. *The function $f : \mathbb{R} \longrightarrow \mathbb{R}$ such that $f(x) = 3x + 1$ is bijective, since it is injective and surjective.*

2. *The function $f : \mathbb{R}^* \longrightarrow \mathbb{R}$ such that $f(x) = \frac{1}{x}$ is not bijective, since it is not surjective.*

3. *The function $f : \mathbb{R} \longrightarrow \mathbb{R}^+$ such that $f(x) = x^2$ is not bijective, since it is not injective.*

Theorem 2.2.21. *Let $f : E \longrightarrow F$ be a function. The following assertions are equivalents*

1. *f is bijective.*

2. *For all $b \in F$, the equation $f(x) = b$ has a unique solution x.*

Proof : A function is bijective if and only if the equation $y = f(x)$ has at least (see Theorem 2.2.15) and at most (see Theorem 2.2.18) one solution, hence a unique solution. □

2.2.6.1 Reciprocal application of a bijective function

Definition 2.2.22. *Let $f : E \longrightarrow F$ be a bijective function. The reciprocal application of f, denoted by f^{-1}, is defined as $f^{-1} : F \longrightarrow E$, where $f^{-1}(y) = x$, and x is the antecedent of y by f (i.e., $f(x) = y$).*

Example 2.2.23. *The bijection f defined from $\mathbb{R}$ to $\mathbb{R}$ by $f(x) = 3x+1$, its reciprocal application is defined from $\mathbb{R}$ to $\mathbb{R}$ by $f^{-1}(x) = \frac{x-1}{3}$.*

Theorem 2.2.24. *Let $f : E \longrightarrow F$ be a bijective function. Then*

(a) *The reciprocal application f^{-1} is bijective and $(f^{-1})^{-1} = f$.*

(b) *$f \circ f^{-1} = Id_F$ and $f^{-1} \circ f = Id_E$.*

Proof : (a) For each $x \in E$, the equation $f^{-1}(y) = x$ has a unique solution $y = f(x)$ and it is unique because another solution y' can only be $f(x)$. Then, according to Theorem 2.2.21, f^{-1} is bijective. Moreover, $(f^{-1})^{-1} : E \longrightarrow F$ and $(f^{-1})^{-1}(x) = y$ since $f^{-1}(y) = x$. Therefore, $(f^{-1})^{-1} = f$.

(b) We have $f : E \longrightarrow F$ and $f^{-1} : F \longrightarrow E$, then $f \circ f^{-1} : F \longrightarrow F$. Also, $f \circ f^{-1}(y) = f(x) = y = Id_F(y)$, hence the equality $f \circ f^{-1} = Id_F$. Similarly, it can be shown that $f^{-1} \circ f = Id_E$.

□

Theorem 2.2.25. *(Bijection Theorem) Let I be an interval in $\mathbb{R}$. Let $f : I \to \mathbb{R}$. We assume that f is continuous and strictly monotonic on I. Then*

- *f establishes a bijection from I to the interval $J = f(I)$.*

- *f^{-1} is strictly monotonic on J, with the same direction of variation as f, and $f^{-1} : J \to I$ with $f^{-1}(y) = x$ (x is the antecedent of y by f).*

2.3 Some exercises with solutions

Exercise 2.3.1. *Let $E = \{a, b, c, d\}$ be a set, can we write the following*
(1) $a \in E$, (2) $a \subset E$, (3) $\{a\} \subset E$, (4) $\emptyset \in E$, (5) $\emptyset \subset E$.
Give the power set of E.

Solution:
Let $E = \{a, b, c, d\}$ be a set, can we write the following

(1) $a \in E$ true, since a is an element in E.

(2) $a \subset E$ has no sense, since a is not a set.

(3) $\{a\} \subset E$ true, since $\{a\}$ is a subset of E.

(4) $\emptyset \in E$ false, since the EmptySet is not an element of E.

(5) $\emptyset \subset E$ true, the EmptySet is included in all the sets.

The power set of E is

$$\mathcal{P}(E) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c.d\},$$

$$\{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, E\}\,.$$

Exercise 2.3.2. *Let $A =]-\infty, 2[$, $B =]-2, 6[$, and $C =]-4, +\infty[$ three sets of $\mathbb{R}$.*
Determine $A \cap B$, $A \cup B$, $B \cap C$, A^c, $A^c \cap B^c$, $A \backslash B$.

Solution:
Let $A =]-\infty, 2[$, $B =]-2, 6[$, and $C =]-4, +\infty[$ three sets of $\mathbb{R}$.
Determine $A \cap B$, $A \cup B$, $B \cap C$, A^c, $A^c \cap B^c$, $A \backslash B$ and $(B \cup C)^c$.

- $A \cap B =]-2, 2[$.
- $A \cup B =]-\infty, 6[$.
- $B \cap C =]-2, 6[$
- $A^c = [2, +\infty[$.
- $A^c \cap B^c = [6, +\infty[$.
- $A \backslash B =]-\infty, -2]$.
- $(B \cup C)^c =]-\infty, -4]$.

Exercise 2.3.3. *Let A and B be two non empty sets, using different approaches, prove that*

$$(A\backslash B) \cup (A \cap B) = A.$$

Solution :

Proof using element-chasing:

Let $x \in (A \setminus B) \cup (A \cap B)$. Then:

$$x \in A \setminus B \quad \text{or} \quad x \in A \cap B.$$

In both cases, $x \in A$, so $(A \setminus B) \cup (A \cap B) \subseteq A$.

Conversely, if $x \in A$, then either $x \notin B$ (so $x \in A \setminus B$) or $x \in B$ (so $x \in A \cap B$). Thus, $x \in (A \setminus B) \cup (A \cap B)$, proving $A \subseteq (A \setminus B) \cup (A \cap B)$.

Therefore, $(A \setminus B) \cup (A \cap B) = A$.

Proof using set identities:

$$A \setminus B = \{x \in A \mid x \notin B\}, \quad A \cap B = \{x \in A \mid x \in B\}.$$

Taking the union:

$$(A \setminus B) \cup (A \cap B) = \{x \in A \mid x \notin B\} \cup \{x \in A \mid x \in B\} = \{x \in A\}.$$

Thus, $(A \setminus B) \cup (A \cap B) = A$.

Exercise 2.3.4. *Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $f(x) = \frac{2x}{1+x^2}$*

1. *Is f injective? surjective?*
2. *Prove that $f(\mathbb{R}) = [-1, 1]$.*
3. *Prove that the restriction $g : [-1, 1] \longrightarrow [-1, 1]$ such that $g(x) = f(x)$ is a bijection.*
4. *Prove the previous results using the study of variations of f.*

Solution :

Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $f(x) = \frac{2x}{1+x^2}$

1. f is not injective because $f(2) = f(\frac{1}{2}) = \frac{4}{5}$. f is not surjective, because $y = 2$ has no pre-image: indeed, the equation $f(x) = 2$ becomes $2x = 2(1 + x^2)$, which simplifies to $x^2 - x + 1 = 0$, and this has no solutions in $\mathbb{R}$.

2. The equation $f(x) = y$ is equivalent to the equation $yx^2 - 2x + y = 0$. This equation has real solutions if and only if $\Delta = 4 - 4y^2 \geq 0$, so there are solutions if and only if $-1 \leq y \leq 1$. Thus, we have $f(\mathbb{R}) = [-1, 1]$.

3. Let $y \in (-1,1)/\{0\}$. The possible solutions of the equation $g(x) = y$ are $x = \frac{1-\sqrt{1-y^2}}{y}$ and $x = \frac{1+\sqrt{1-y^2}}{y}$. The second solution does not belongs to $[-1,1]$ (solution is strictly greater than 1 if $y > 0$, and strictly less than -1 if $y < 0$). On the other hand, $x = \frac{1-\sqrt{1-y^2}}{y} = \frac{y}{1+\sqrt{1-y^2}} \in [-1,1]$. Since

$$1 \leq 1 + \sqrt{1-y^2} \;\Rightarrow\; 0 < \frac{1}{1+\sqrt{1-y^2}} \leq 1,$$

and, since $-1 < y < 1$, then

$$-1 \leq \frac{-1}{1+\sqrt{1-y^2}} \leq x \leq \frac{1}{1+\sqrt{1-y^2}} \leq 1.$$

In other way, if $y = 1$, the equation $g(x) = 1$ has the unique solution $x = 1$, while if $y = -1$, the equation $g(x) = -1$ has the unique solution $x = -1$. Finally, if $y = 0$, the equation $g(x) = 0$ has the unique solution $x = 0$. In all cases, we have proven that for all y in $[-1,1]$, the equation $g(x) = y$ has a unique solution with x in $[-1,1]$. We have indeed proven that g is a bijection.

4. Variations of f:

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

x	$-\infty$		-1		1		$+\infty$
Sign of $f'(x)$		$-$		$+$		$-$	
Variations of $f(x)$	0	$\searrow$	-1	$\nearrow$	1	$\searrow$	0

On the interval $[-1,1]$, $f'(x) \geq 0$, then f is increasing and continuous with $f(-1) = -1$ and $f(1) = 1$. Hence, via mean value theorem, each $y \in [-1,1]$ has a unique antecedent $x \in [-1,1]$. So, the restriction of f which is called g is a bijection.
An analysis method, using the continuity and strict monotonicity of g, would be easier!

Exercise 2.3.5. *Determine $f(I)$, then verify that f realise a bijection from I to $J = f(I)$, then precise f^{-1}, where*

$$f(x) = \sqrt{2x+3} - 2,\ I =]\frac{-3}{2}, +\infty[$$

Solution :
$f(x) = \sqrt{2x+3}$-2, $I = \left]\frac{-3}{2}, +\infty\right[$

- For $x \in \left]\frac{-3}{2}, +\infty\right[$, we have $x > \frac{-3}{2}$, which implies that $f(x) > -1$. Hence

$$f(I) =]-2, +\infty[.$$

Since the function f is continuous on the interval $\left]\frac{-3}{2}, +\infty\right[$ and strictly increasing (because $f'(x) = \frac{1}{\sqrt{2x+3}} > 0$), then f realizes a bijection from I to $J = f(I)$.

- **Precise f^{-1}.**

  Let $y \in J = [-2, +\infty[$ and $x \in \left]\frac{-3}{2}, +\infty\right[$ such that $y = f(x)$

$$\begin{aligned} y = f(x) &\Leftrightarrow y = \sqrt{2x+3} - 2 \\ &\Leftrightarrow (y+2)^2 = 2x + 1 \\ &\Leftrightarrow x = \frac{1}{2}(y+2)^2 - \frac{3}{2} \in]\frac{-3}{2}, +\infty[. \end{aligned}$$

  So, the function f^{-1} is defined by

$$\begin{aligned} f^{-1} :]-2, +\infty[&\longrightarrow \left]\frac{-3}{2}, +\infty\right[\\ x &\longmapsto \frac{1}{2}(x+2)^2 - \frac{3}{2}. \end{aligned}$$

Exercise 2.3.6. *Let $x \in \mathbb{R}_+$, $f(x) = \frac{x}{x+1}$, compute $f \circ f \circ f \circ ... \circ f$ (n times) in term of $n \in \mathbb{N}^*$ and $x \in \mathbb{R}_+$.*

Solution :

Given $f(x) = \frac{x}{x+1}$, we want to compute $f^n(x)$.
Let $f^1(x) = f(x) = \frac{x}{x+1}$. For $n = 2$:

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

For $n = 3$:

$$f^3(x) = f\left(f^2(x)\right) = f\left(\frac{x}{2x+1}\right) = \frac{\frac{x}{2x+1}}{\frac{x}{2x+1}+1} = \frac{x}{3x+1}.$$

By induction:

$$f^n(x) = \frac{x}{nx+1}, \quad \forall n \in \mathbb{N}^*.$$

Now, we prove this last using recurrence:
For $n = 1$, it's evident.
Suppose the formula is true for n, and prove that it remains true for $n+1$.

$$f^{n+1}(x) = f\left(f^n(x)\right) = f\left(\frac{x}{nx+1}\right) = \frac{\frac{x}{nx+1}}{1+\frac{x}{nx+1}} = \frac{x}{(n+1)x+1}$$

Exercise 2.3.7. *Let f and g be applications from $\mathbb{N}$ to $\mathbb{N}$ defined by $f(x) = 2x$ and*

$$g(x) = \begin{cases} \frac{x}{2}, & if\ x\ is\ even, \\ 0, & if\ x\ is\ odd. \end{cases}$$

Determine $f \circ g$ and $g \circ f$. The functions f and g are one to one? onto? bijections?

Solution :

Given functions:

$$f(x) = 2x, \quad g(x) = \begin{cases} \frac{x}{2}, & \text{if } x \text{ is even}, \\ 0, & \text{if } x \text{ is odd}. \end{cases}$$

1. **Compute $f \circ g(x)$:**

$$f(g(x)) = \begin{cases} f\left(\frac{x}{2}\right) = x, & \text{if } x \text{ is even}, \\ f(0) = 0, & \text{if } x \text{ is odd}. \end{cases}$$

2. **Compute $g \circ f(x)$:**

$$g(f(x)) = g(2x) = \frac{2x}{2} = x, \quad \forall x \in \mathbb{N}.$$

3. **Injectivity and surjectivity:**

- $f(x) = 2x$ is injective (let $x, y \in \mathbb{N}, f(x) = f(y)$ implies $x = y$). However, f is not surjective ($\exists y \in \mathbb{N}, \forall x \in \mathbb{N},\ f(x) \neq y$), consider $y = 1$.
- $g(x)$ is not injective (e.g., $g(1) = g(3) = 0$) and not surjective (e.g., $3 \notin Im(g)$).

Exercise 2.3.8. *Let*

$$\begin{aligned} f :& [1, +\infty[\longrightarrow [1, +\infty[\\ & x \longmapsto e^{ln^2(x)}. \end{aligned}$$

Prove that f is a bijection, and determine its reciprocal application.

Solution :

Given $f(x) = e^{(\ln x)^2}$.

Injectivity:

Let $x_1, x_2 \in [1, +\infty[$, suppose $f(x_1) = f(x_2)$. Then:

$$e^{(\ln x_1)^2} = e^{(\ln x_2)^2} \implies (\ln x_1)^2 = (\ln x_2)^2.$$

Since $x_1, x_2 \in [1, +\infty[$, then $\ln x_1$ and $\ln x_2$ are positif. Hence $x_1 = x_2$. Thus, f is injective.

Surjectivity:

Let $y \in [1, +\infty[$. Solve $y = e^{(\ln x)^2}$:

$$\ln y = (\ln x)^2 \implies \ln x = \pm\sqrt{\ln y}.$$

Since $x \in [1, +\infty[$, only $\ln x = \sqrt{\ln y}$ is valid, so f is surjective.

Inverse:

For $y \in [1, +\infty[$,

$$f^{-1}(y) = e^{\sqrt{\ln y}}.$$

Chapter 3

Relations

This chapter introduces the fundamental concept of relations, exploring how elements in sets relate to one another. We'll focus on two types of relations: equivalence relations and order relations.

Equivalence relations provide insights into the concept of equality and equivalence classes, allowing us to group elements based on shared properties. Order relations, on the other hand, establish hierarchies among elements, defining relationships like partial and total orders.

3.1 Generalities of relations

Definition 3.1.1. *A relation from a set A to a set B is any correspondence $\mathcal{R}$ that links elements of A to elements of B in a certain way.*

1. *We call A the domain and B the codomain of the relation $\mathcal{R}$.*
2. *If x is linked to y by relation $\mathcal{R}$, we say that x is in relation $\mathcal{R}$ with y, and we write $x\mathcal{R}y$ or $\mathcal{R}(x, y)$. Otherwise, we write $x \not\mathcal{R} y$ or $\not\mathcal{R}(x, y)$.*
3. *A relation from A to A is called a relation on A.*

Examples 3.1.2.
1. *Let A be the set of university professors in Usto M-B, and B the set of students in Usto M-B university. We can determine a relation $\mathcal{R}$ from A to B by defining that $(x, y) \in A \times B$ satisfies $x\mathcal{R}y$ if and only if x teaches y.*
2. *Let $A = B = \mathbb{Z}$. We can determine a relation $\mathcal{R}$ on $\mathbb{Z}$ by defining that $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ satisfies $\mathcal{R}(x, y)$ if and only if $x - y$ is even. We have, for example, $1\mathcal{R}5$ but $12 \not\mathcal{R}3$.*

Definition 3.1.3. *(Graph of a relation) The graph of $\mathcal{R}$ (denoted $G_{\mathcal{R}}$) is the set defined by*

$$G_{\mathcal{R}} = \{(x, y) \in A \times B \mid x\mathcal{R}y\}.$$

For example, considering the relation $\mathcal{R}$ from the previous example, we have $(1,7) \in G_{\mathcal{R}}$ and $(18,5) \notin G_{\mathcal{R}}$.

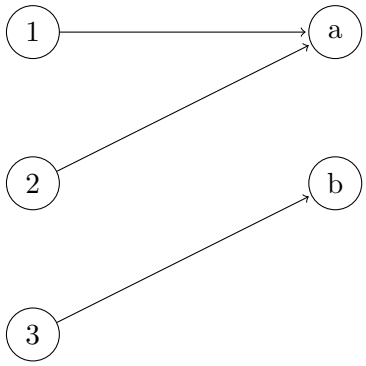
Remark 3.1.4. *Given two relations $\mathcal{R} = (A, B, G_{\mathcal{R}})$ and $\mathcal{R}' = (A', B', G_{\mathcal{R}'})$, the statement "the relations $\mathcal{R}$ and $\mathcal{R}'$ are equal" means that $A = A'$, $B = B'$, and $G_{\mathcal{R}} = G_{\mathcal{R}'}$ same source, same target, and same graph.*

3.2 Representation of a binary relation

We are once again interested in binary relations on two given sets A and B.

1. Set representation: Simply list the pairs satisfying the relation.

2. Representation using a sagittal diagram: A diagram with two curves for arbitrary A and B (one curve for the source A and the other for the target B). When $A = B$, you can either keep the two-curve representation or bring everything together in a single curve representing A. This latter view is often very instructive.
   Let A and B two sets, where A has elements $\{1, 2, 3\}$, and B has elements $\{a, b\}$. Below is an illustrative diagram that represent the relation $\mathcal{R} = \{(1, a), (2, a), (3, b)\}$



3. Representation using a formula: For example, the relation $\mathcal{R}$ on $\mathbb{R}$ such that $x\mathcal{R}y$ if and only if $x^2 = y^2$.

3.3 Properties of a Binary Relation on a Set

We now focus on a binary relation where the source coincides with the target. Thus, we have a relation on a given set A. Here, we explore the main properties that such a binary relation may or may not possess.

Definition 3.3.1. *Let $\mathcal{R}$ be a (binary) relation on a set A. We say that $\mathcal{R}$ is:*

1. *Reflexive, for every $a \in A$, we have $a\mathcal{R}a$.*

2. *Symmetric, for every pair $(a, b) \in A^2$, if $a\mathcal{R}b$, then $b\mathcal{R}a$.*

3. *Transitive, for every triplet of elements $a, b, c \in A$, if ($a\mathcal{R}b$ and $b\mathcal{R}c$), then ($a\mathcal{R}c$).*

4. *Antisymmetric, for every $(a, b) \in A^2$, if ($a\mathcal{R}b$ and $b\mathcal{R}a$), then ($a = b$).*

Examples 3.3.2. *1. Let the relation $\mathcal{R}$ be defined on $\mathbb{Z}$ as follows: $x\mathcal{R}y \Leftrightarrow x$ divides y.*

   (a) *For any $x \in \mathbb{Z}$, we have x divides x. So, for all $x \in \mathbb{Z}$, $x\mathcal{R}x$ holds, which means $\mathcal{R}$ is reflexive.*

   (b) *For $x, y \in \mathbb{Z}$, $x\mathcal{R}y$ implies (x divides y) $\nRightarrow$ (y divides x). For example, 1 divides 4, but 4 does not divide 1, hence $\mathcal{R}$ is not symmetric.*

   (c) *Let $x, y \in \mathbb{Z}$, we have $(x\mathcal{R}y)$ and $(y\mathcal{R}x) \Rightarrow$ ((x divides y) and (y divides x)) $\nRightarrow$ $x = y$, for example, (1 divides -1) and (-1 divides 1), but $-1 \neq 1$, hence $\mathcal{R}$ is not antisymmetric.*

   (d) *For $x, y, z \in \mathbb{Z}$, if $(x\mathcal{R}y)$ and $(y\mathcal{R}z) \Rightarrow$ ((x divides y) and (y divides z)) $\Rightarrow$ (x divides z), then $x\mathcal{R}z$. Thus, $\mathcal{R}$ is transitive.*

2. *Let $A = B = \mathbb{Z}$, and $\mathcal{R} = (a, b) \in \mathbb{Z}^2,\ 2|(a - b)$. Then $\mathcal{R}$ is reflexive, symmetric, transitive, but not antisymmetric.*

3. *Given the set $\mathcal{U}$, the inclusion relation, which relates subsets of $\mathcal{U}$ as follows $(X \subseteq Y)$, is reflexive, transitive, and antisymmetric, but not symmetric.*

Remark 3.3.3. *Symmetric and antisymmetric relations are fundamentally different properties, but it is possible for a relation to satisfy both simultaneously. For instance, the identity relation $\mathcal{R} = \{(x, x),\ x \in A\}$ on any set A, is an example of a relation that is both symmetric and antisymmetric.*

3.4 Equivalence Relation

Definition 3.4.1. *Let $\mathcal{R}$ be a relation on a set A.*

1. *$\mathcal{R}$ is called an equivalence relation if $\mathcal{R}$ is reflexive, symmetric, and transitive.*

2. *If $\mathcal{R}$ is an equivalence relation, then*

   (a) *For each $a \in A$, the set $\dot{a} = \{x \in A | x\mathcal{R}a\}$ is called the equivalence class of a modulo $\mathcal{R}$.*

(b) *The set $A_{|\mathcal{R}} = \{\dot{a} | a \in A\}$ is called the quotient set of A by $\mathcal{R}$.*

Examples 3.4.2. *1. The relation $\mathcal{R}$ given over $\mathbb{R}$ by the following formula $x\mathcal{R}y$ if and only if $x^2 = y^2$ is an equivalence relation, and $\dot{0} = \{0\}$, and for $a \neq 0$, $\dot{a} = \{a, -a\}$.*
$\mathbb{R}_{|\mathcal{R}} = \{\{0\},\ \{a, -a\},\ a > 0\}$.

2. Let $\mathcal{R}_n$ be a relation of congruence modulo n defined on $\mathbb{Z}$ by $x\mathcal{R}_n y$ if and only if n divides $y - x$, is indeed an equivalence relation.
For this relation, we have

$$\begin{aligned}\dot{a} &= \{x \in \mathbb{Z}/n \text{ divides } x - a\} \\ &= \{x \in \mathbb{Z}/x = nq + a,\ q \in \mathbb{Z}\}\end{aligned}$$

noted $n\mathbb{Z} + a$.
In this case $\mathbb{Z}_{|\mathcal{R}_n} = \{n\mathbb{Z} + a, a \in \mathbb{Z}\}$ which is identified by $\mathbb{Z}_{|n\mathbb{Z}}$.

Remark 3.4.3. *The class $\dot{a}$ is also denoted as $\bar{a}$, $[a]$, and $Cl(a)$.*
If x is in an equivalence relation with y, we say that x and y are equivalent.

Theorem 3.4.4. *Let $\mathcal{R}$ be an equivalence relation on a non-empty set A, then*

1. *Every element of A is in an equivalence class. That is, $A = \cup\dot{a}$, where $a \in A$.*
2. *Two elements are equivalent if and only if they belong to the same class. That is, for all $a, x \in A$, $a\mathcal{R}x$ if and only if $\dot{a} = \dot{x}$.*
3. *Any equivalence classes are disjoint or coincide. That is, for all $a, x \in A$, $\dot{a} \cap \dot{x} = \emptyset$ or $\dot{a} = \dot{x}$.*
4. *The equivalence classes form a partition of A. That is, every element in A belongs to exactly one equivalence class, and the union of all equivalence classes covers A entirely.*

Proof :

1. Every element $a \in A$ verifies $a\mathcal{R}a$, which means $a \in \dot{a}$.
2. Suppose that $a\mathcal{R}x$ and let $y \in \dot{a}$, then $y\mathcal{R}a$. Thus, by transitivity $y\mathcal{R}x$, so $y \in \dot{x}$. Then $\dot{a} \subset \dot{x}$. Similarly, $\dot{x} \subset \dot{a}$.
   Inversely, if $\dot{a} = \dot{x}$, we take an element $y \in \dot{a} = \dot{x}$, satisfies $a\mathcal{R}y$ and $y\mathcal{R}x$. Thus, by transitivity, we get $a\mathcal{R}x$.

3. Suppose the opposite, means $\dot{a} \cap \dot{x} \neq \emptyset$ and $\dot{a} \neq \dot{x}$. Thus, $\exists y \in A$ satisfies $a\mathcal{R}y$ and $y\mathcal{R}x$.Thus, by transitivity, we get $a\mathcal{R}x$ and using (2), we conclude that $\dot{a} = \dot{x}$, which is a contradiction with $\dot{a} \neq \dot{x}$.

4. Due to (1), we have $\dot{a} \neq \emptyset$ and $A = \cup\dot{a}$, where $a \in A$, and using (3) $\dot{a} \cap \dot{b} = \emptyset$ if $\dot{a} \neq \dot{b}$. Consequently, the equivalence classes form a partition of A.

□

Example 3.4.5. *If $n = 3$, we have $\mathbb{Z}_{|3\mathbb{Z}} = \{\dot{0}, \dot{1}, \dot{3}\} = \{\dot{3}, \dot{1}, \dot{2}\} = \{\dot{-3}, \dot{4}, \dot{5}\}$.*

3.5 Order Relation

Definition 3.5.1. *Let $\mathcal{R}$ be a relation on a set A.*
$\mathcal{R}$ is called an order relation if $\mathcal{R}$ is reflexive, antisymmetric, and transitive.

(a) *If $\mathcal{R}$ is an order relation, we often write $\leq_{\mathcal{R}}$ instead of $\mathcal{R}$.*

(b) *$\leq_{\mathcal{R}}$ is called a total order relation if*

$$\forall x, y \in A,\ ((x \leq_{\mathcal{R}} y) \vee (y \leq_{\mathcal{R}} x)).$$

(c) *$\leq_{\mathcal{R}}$ is called a partial order relation if*

$$\exists x, y \in A,\ ((x \not\leq_{\mathcal{R}} y) \wedge (y \not\leq_{\mathcal{R}} x)).$$

Remark 3.5.2. *Two elements x and y are said to be comparable by $\leq_{\mathcal{R}}$ if $x \leq_{\mathcal{R}} y$ or $y \leq_{\mathcal{R}} x$.*

Examples 3.5.3. *1. The inclusion relation $\mathcal{R}$ on $\mathcal{P}(\mathbb{N})$ is a partial order. (For X, Y, and Z in $\mathcal{P}(\mathbb{N})$*

- *Reflexivity $X \subseteq X$*
- *Antisymmetry $X \subset Y$ and $Y \subseteq X$ implies $X = Y$.*
- *Transitivity $X \subseteq Y$ and $Y \subseteq Z$ implies $X \subseteq Z$. Moreover, the subsets $\{1, 2\}$ and $\{1, 3\}$ are incomparable.*

2. The way words are arranged in a dictionary defines a total order relation called lexicographic order, denoted by $\leq_{lex}$. For example, algebra $\leq_{lex}$ analysis.

Definition 3.5.4. *(Special Elements)Let $\mathcal{R}$ be an order relation on a set E, and let A be a subset of E, then*

1. *An element $m \in E$ is called a minimum of A if*

   (a) $m \in A$.

   (b) *for every $x \in A$, we have $m \leq_{\mathcal{R}} x$. (We also say that m is a smallest (least) element of A.)*

2. *An element $M \in E$ is called a maximum of A if*

   (a) $M \in A$.

   (b) *for every $x \in A$, we have $x \leq_{\mathcal{R}} M$. (We also say that M is a greatest element of A.)*

3. *An extremum is an element that is either a minimum or a maximum.*

4. *An element u in the set E is called a lower bound of A if for every $x \in A$, $u \leq_{\mathcal{R}} x$. (It is also said that A is bounded below by u.)*

5. *An element U in the set E is called an upper bound of A if for every $x \in A$, $x \leq_{\mathcal{R}} U$. (It is also said that A is bounded above by U.)*

6. *The set A is said to be bounded below in E if A has a lower bound in E; A is said to be bounded above in E if A has an upper bound in E; and A is said to be bounded in E if A is both bounded below and above.*

7. *An element v in the set E is called a infimum of A if*

   (a) *v is a lower bound of A,*

   (b) *for every lower bound v' of A, we have $v' \leq_{\mathcal{R}} v$. Notation: $v = inf(A)$.*

8. *An element V in the set E is called a supremum of A if*

   (a) *V is an upper bound of A,*

   (b) *for every upper bound $'V$ of A, we have $V \leq_{\mathcal{R}} V'$. Notation: $V = sup(A)$.*

Examples 3.5.5. *For the usual order $\leq$ on the set of real numbers $\mathbb{R}$, let $B =]-4, 0[\cup [\frac{1}{2}, +\infty[$.*
We have the following
There is no $min(B)$ (4 is a good candidate, but 4 is not in B).
There is no $max(B)$ (There are no candidates for the maximum element in B).
The set of lower bounds of B is $]-\infty, -4]$, so $inf(B) = -4$.
There are no upper bounds of B, so $sup(B)$ does not exist.

3.6 Some Exercises with solutions

Exercise 3.6.1. *Are the following relations, reflexive? symmetric? antisymmetric? transitive?*

(a) $E = \mathbb{Z}$, *and* $x\mathcal{R}y \Leftrightarrow x = -y$;

(b) $E = \mathbb{R}$, *and* $x\mathcal{R}y \Leftrightarrow cos^2(x) + sin^2(y) = 1$;

Solution :

(a) $E = \mathbb{Z}$, and $x\mathcal{R}y \Leftrightarrow x = -y$;

The relation is not reflexive because 1 is not in a relation with itself. In fact, $1 \not\mathcal{R}1$. The relation is symmetric because $x = -y$ then, $y = -x$. It is not antisymmetric because $1\mathcal{R}-1$ and $-1\mathcal{R}1$, while $1 \neq -1$. It is not transitive either. In fact, we have $1\mathcal{R}-1$, $-1\mathcal{R}1$, and $1 \not\mathcal{R}1$.

(b) $E = \mathbb{R}$, and $x\mathcal{R}y \Leftrightarrow cos^2(x) + sin^2(x) = 1$;

From the formula $cos^2x + sin^2x = 1$, we can deduce that the relation is reflexive. It is also symmetric, since, if $x\mathcal{R}y$, i.e., $cos^2x + sin^2y = 1$, then, we have

$$sin^2x + cos^2x + cos^2y + sin^2y = (cos^2x + sin^2y) + (cos^2y + sin^2x) = 1 + (cos^2y + sin^2x),$$

and on the other hand, we have

$$sin^2x + cos^2x + cos^2y + sin^2y = 1 + 1 = 2,$$

which implies

$$cos^2y + sin^2x = 1,$$

and therefore, the relation is symmetric. It is not antisymmetric because $0\mathcal{R}2\pi$ and $2\pi\mathcal{R}0$ while $0 \neq 2\pi$. It is transitive. If $x\mathcal{R}y$ and $y\mathcal{R}z$, we have $cos^2x + sin^2y = 1$ and $cos^2y + sin^2z = 1$ which implies $cos^2x + (sin^2y + cos^2y) + sin^2z = 2$ and thus, $cos^2x + sin^2z = 1$.

Exercise 3.6.2. *Let* $\mathcal{R}$ *a relation defined on* $\mathbb{Z}$ *by*

$$x\mathcal{R}y \Leftrightarrow x^2 - y^2 = x - y.$$

1. *Prove that* $\mathcal{R}$ *is an equivalence relation.*
2. *Determine the equivalence class of any element* $x \in \mathbb{R}$. *Precise the equivalence class of* 1.

Solution :

Let $\mathcal{R}$ a relation defined on $\mathbb{Z}$ by

$$x\mathcal{R}y \Leftrightarrow x^2 - y^2 = x - y.$$

1. It suffices to notice that $x\mathcal{R}y \Leftrightarrow x^2 - x = y^2 - y \Leftrightarrow f(x) = f(y)$, with $f : x \longmapsto x^2 - x$. It is then easy to verify by applying the definition that $\mathcal{R}$ is an equivalence relation, $\mathcal{R}$ is reflexive, since $\forall x \in \mathbb{R}$, $f(x) = f(x)$. $\mathcal{R}$ is symmetric, since $\forall x, y \in \mathbb{R}$, $f(x) = f(y)$ implies that $f(y) = f(x)$. And $\mathcal{R}$ is transitive, since $\forall x, y, z \in \mathbb{R}$, $f(x) = f(y)$ and $f(y) = f(z)$, then $f(x) = f(z)$.

2. Let $x \in \mathbb{R}$. We are looking for elements y in R such that $x\mathcal{R}y$. Therefore, we need to solve the equation in y
$$x^2 - y^2 = x - y.$$
It factors as
$$(x - y)(x + y - 1) = 0$$
Its solutions are $y = x$ and $y = 1 - x$. The class of x is thus equal to $\{x, 1 - x\}$. It consists of two elements unless $x = \frac{1}{2}$. In that case, it equals $\left\{\frac{1}{2}\right\}$. Hence, the equivalence class of 1 is $\{0, 1\}$.

Exercise 3.6.3. *Let $\mathcal{R}$ a relation defined on $\mathbb{R}$ by*
$$x\mathcal{R}y \Leftrightarrow x^3 - y^3 \geq 0.$$
Prove that $\mathcal{R}$ is an order relation. Is the order total?

Solution :
Let $\mathcal{R}$ a relation defined on $\mathbb{R}$ by
$$x\mathcal{R}y \Leftrightarrow x^3 - y^3 \geq 0.$$
$\mathcal{R}$ is an order relation

1. The relation is reflexive: for any $x \in \mathbb{R}$, $x^3 - x^3 \geq 0$, and therefore $x\mathcal{R}x$.

2. The relation is antisymmetric: let $x, y \in \mathbb{R}$ such that $x\mathcal{R}y$ and $x\mathcal{R}y$, means
$$\begin{cases} x^3 - y^3 \geq 0 \\ y^3 - x^3 \geq 0 \end{cases} \Rightarrow x^3 - y^3 = 0.$$
Which means $x = y$.

3. The relation is transitive: let $x, y, z \in \mathbb{R}$ such that $x\mathcal{R}y$ and $y\mathcal{R}z$, means
$$\begin{cases} x^3 - y^3 \geq 0 \\ y^3 - z^3 \geq 0 \end{cases} \Rightarrow x^3 - z^3 \geq 0.$$
Which means $x\mathcal{R}z$.

The order is total, since $\forall x, y \in \mathbb{R}$, either $x^3 - y^3 \geq 0$ or $y^3 - x^3 \geq 0$.

Exercise 3.6.4. *Let $\mathcal{R}$ be a relation defined on $\mathbb{Z} \times \mathbb{N}^*$ by*

$$(n, m)\mathcal{R}(n', m') \Leftrightarrow nm' = n'm.$$

1. *Prove that $\mathcal{R}$ is an equivalence relation.*
2. *Let $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$, with $p \wedge q = 1$, write the equivalence class of (p, q).*

Solution :

Let $\mathcal{R}$ be a relation on $\mathbb{Z} \times \mathbb{N}^*$ defined by

$$(n, m)\mathcal{R}(n', m') \iff nm' = n'm.$$

1. **$\mathcal{R}$ is an equivalence relation:**
   - **Reflexivity:** For $(n, m) \in \mathbb{Z} \times \mathbb{N}^*$,
     $$nm = nm,$$
     so $(n, m)\mathcal{R}(n, m)$. Thus, $\mathcal{R}$ is reflexive.
   - **Symmetry:** If $(n, m)\mathcal{R}(n', m')$, then $nm' = n'm$. Switching sides, $n'm = nm'$, so $(n', m')\mathcal{R}(n, m)$. Thus, $\mathcal{R}$ is symmetric.
   - **Transitivity:** If $(n, m)\mathcal{R}(n', m')$ and $(n', m')\mathcal{R}(n'', m'')$, then
     $$nm' = n'm \quad \text{and} \quad n'm'' = n''m'.$$
     Multiplying the 1st equation by m", $nm'm'' = n''m'm$, so $nm'' = n''m$. Thus, $(n, m)\mathcal{R}(n'', m'')$, and $\mathcal{R}$ is transitive.

   Since $\mathcal{R}$ is reflexive, symmetric, and transitive, it is an equivalence relation.

2. **Equivalence class of (p, q):** For $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$, the equivalence class is:
   $$cl(p, q) = \{(n, m) \in \mathbb{Z} \times \mathbb{N}^* \mid nq = pm\}.$$

Exercise 3.6.5. *Let E, F be two sets, and $f : E \longrightarrow F$ be an application. We define the relation $\mathcal{R}$ on E, such that for all $x, x' \in E$,*

$$x\mathcal{R}x' \Leftrightarrow f(x) = f(x').$$

1. *Prove that $\mathcal{R}$ is an equivalence relation.*

2. Write the equivalence class of an element $x \in E$.

Solution :

Let E, F be sets, and let $f : E \to F$. Define $\mathcal{R}$ on E by

$$x\mathcal{R}x' \iff f(x) = f(x').$$

1. **Prove that $\mathcal{R}$ is an equivalence relation:**

   - **Reflexivity:** For all $x \in E$,

     $$f(x) = f(x),$$

     so $x\mathcal{R}x$. Thus, $\mathcal{R}$ is reflexive.
   - **Symmetry:** If $x\mathcal{R}x'$, then $f(x) = f(x')$. By symmetry of equality, $f(x') = f(x)$, so $x'\mathcal{R}x$. Thus, $\mathcal{R}$ is symmetric.
   - **Transitivity:** If $x\mathcal{R}x'$ and $x'\mathcal{R}x''$, then $f(x) = f(x')$ and $f(x') = f(x'')$. By transitivity of equality, $f(x) = f(x'')$, so $x\mathcal{R}x''$. Thus, $\mathcal{R}$ is transitive.

   Since $\mathcal{R}$ is reflexive, symmetric, and transitive, it is an equivalence relation.

2. **Equivalence class of $x \in E$:** The equivalence class of $x \in E$ is:

   $$\dot{x} = \{x' \in E \mid f(x') = f(x)\} = f^{-1}\{f(x)\}.$$

Exercise 3.6.6. *Prove that the following binary relation $\mathcal{R}$ defined on $]1, +\infty[$ by*

$$x\mathcal{R}y \;\Leftrightarrow\; \frac{x}{1+x^2} \geq \frac{y}{1+y^2}$$

is a total order relation.

Solution :

Let $\mathcal{R}$ be defined on $]1, +\infty[$ by

$$x\mathcal{R}y \iff \frac{x}{1+x^2} \geq \frac{y}{1+y^2}.$$

Prove that $\mathcal{R}$ is a total order relation:

- **Reflexivity:** For all $x \in]1, +\infty[$,

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

  Thus, $\mathcal{R}$ is reflexive.

- **Antisymmetry:** If $x\mathcal{R}y$ and $y\mathcal{R}x$, then

$$\frac{x}{1+x^2} = \frac{y}{1+y^2}.$$

This implies $x = y$. Thus, $\mathcal{R}$ is antisymmetric.

- **Transitivity:** If $x\mathcal{R}y$ and $y\mathcal{R}z$, then

$$\frac{x}{1+x^2} \geq \frac{y}{1+y^2} \quad \text{and} \quad \frac{y}{1+y^2} \geq \frac{z}{1+z^2}.$$

Combining these, $\frac{x}{1+x^2} \geq \frac{z}{1+z^2}$. Thus, $\mathcal{R}$ is transitive.

- **Totality:** For all $x, y \in]1, +\infty[$,

$$\frac{x}{1+x^2} \geq \frac{y}{1+y^2} \quad \text{or} \quad \frac{y}{1+y^2} \geq \frac{x}{1+x^2}.$$

Thus, $\mathcal{R}$ is total order relation.

Chapter 4

Algebraic structures

This chapter serves as a gateway to understanding abstract algebraic concepts in the study of linear algebra. We'll explore fundamental algebraic structures such as groups, rings, and fields.

Groups provide a framework for studying symmetry and transformations, while rings and fields extend these concepts, encompassing properties related to addition and multiplication.

4.1 Binary operations

Definition 4.1.1. *A binary operation (or Internal composition laws) on a non-empty set E is an application $*$ from $E \times E$ to E. For any elements x and y in E, the result of the operation $*$ applied to (x, y) is denoted by $x * y$, $x * y$ is an element of E.*

Examples 4.1.2.

1. *Ordinary addition $+$ is an internal composition law on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.*

   Ordinary multiplication $\times$ is an internal composition law on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

   Subtraction is an internal composition law on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, but not on $\mathbb{N}$.

2. *The composition $\circ$ is an internal composition law on set $\mathcal{A}(E)$, the set of applications from E to E. If $f : E \longrightarrow E$ and $g : E \longrightarrow E$ are two applications, then $f \circ g : E \longrightarrow E$ is also an application.*

3. *The intersection $\cap$ is an internal composition law on set $\mathcal{P}(E)$, the set of subsets of E.*

Definition 4.1.3. *A non-empty set E equipped with one or more binary operations is called an algebraic structure. If the operations are denoted as $*_1, *_2, ..., *_n$, then the algebraic structure is noted as $(E, *_1, *_2, ..., *_n)$.*

Example 4.1.4. *$(\mathbb{N}, +)$, $(\mathbb{Z}, +, -)$, $(\mathbb{R}, +, \times)$, $(\mathcal{A}(E, E), \circ)$, and $(\mathcal{P}(E), \cap)$ are algebraic structures.*

Definition 4.1.5. *Let $*$ be an binary operation on a non-empty set E. Then*

1. *We say that the law $*$ is associative if, for all x, y, z in E, we have $(x * y) * z = x * (y * z)$.*

2. *An element e of E is called the neutral element (or unit element) of $*$, if for every x in E, we have $e * x = x * e = x$.*

3. *If e is the neutral element of $*$, we say that an element x in E is invertible (or symmetrizable) if there exists an element y in E such that $x * y = y * x = e$, and y is called the inverse (or symmetrical) of x and is denoted as x^{-1}.*

4. *We say that the law $*$ is commutative if, for all x, y in E, we have $x * y = y * x$.*

Remark 4.1.6. *If the law $*$ is associative, parentheses can be omitted, and we can write $x*y*z$ instead of $(x * y) * z$ and $x * (y * z)$.*

Examples 4.1.7.

1. *The usual addition $+$ on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ is an associative and commutative law, and it has 0 as the neutral element.*
   In $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, every element x has its symmetrical (inverse) x^{-1}. In $\mathbb{N}$, the only element with a symmetrical property for the usual addition is 0.
   The usual multiplication $\times$ on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ is an associative and commutative law, with 1 as the identity element.
   In $\mathbb{Q}^*$, $\mathbb{R}^*$ and $\mathbb{C}^*$, every non-zero element x has its inverse (symmetrical) $\frac{1}{x}$. The element 0 does not have an inverse for the usual multiplication $\times$.
   In $\mathbb{Z}$, the only invertible elements for the usual multiplication are ± 1.

2. *The composition $\circ$ on $\mathcal{A}(E, E)$ is an associative law, with the identity function Id_E as the neutral element. The only invertible elements are the bijective functions. $((f \circ g) \circ h = f \circ (g \circ h)$, $f \circ Id_E = f = Id_E \circ f$, where Id_E is the identity function and f has a reciprocal function f^{-1} as its inverse for the composition, as $f \circ f^{-1} = Id_E = f^{-1} \circ f)$. The composition, in general, is not commutative.*

Theorem 4.1.8. *Let E be a set with an internal composition law $*$. Then*

1. *The neutral element e, if it exists, is unique.*

2. *If $*$ is associative and there exists a neutral element e, then the inverse element x^{-1} of an element x (if it exists) is unique. Additionally, if y also has an inverse, then $(x * y)^{-1} = y^{-1} * x^{-1}$.*

Proof : Let's assume e' is another neutral element of $*$. Then, we have $e' * e = e * e' = e$, and since e is also a neutral element, we get $e' * e = e * e' = e'$. Hence, $e' = e$, and the neutral element is unique.
Let's assume x' is another inverse of x. Then, we have $x * x' = x' * x = e$, and consequently, $x^{-1} = (x' * x) * x^{-1} = x' * (x * x^{-1}) = x'$. So, the inverse is unique
We have $x * x^{-1} = e = x^{-1} * x$, since the inverse is unique, then x is the inverse of x^{-1}. Which means $(x^{-1})^{-1} = x$.
We also have $(y^{-1} * x^{-1}) * (x * y) = y^{-1} * x^{-1} * x * y = e$ and $(x * y) * (y^{-1} * x^{-1}) = x * y * y^{-1} * x^{-1} = e$, since the inverse is unique. Then, $y^{-1} * x^{-1}$ is the inverse of $x * y$. Which means $(x * y)^{-1} = y^{-1} * x^{-1}$. □

4.2 Groups

4.2.1 Definitions

Definition 4.2.1. *Let $(G, *)$ be a structured set. We say that $(G, *)$ is a group if*

(a) *the law $*$ is associative on G,*

(b) *there exists a neutral element for the law $*$ 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 law $*$.
We say that the group $(G, *)$ is commutative (or abelian) if the law $*$ is commutative on G.

Example 4.2.2. *We provide examples of groups*

1. *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ equipped with addition.*
2. *$\mathbb{Q}^*$, $\mathbb{R}^*$ and $\mathbb{C}^*$, equipped with multiplication.*

4.2.2 Subgroups

Definition 4.2.3. *(Subgroups) A subgroup of a group $(G, *)$ is a non-empty subset H of G such that*

1. *$*$ induces an internal composition law on H.*
2. *Equipped with this law, H is a group. We denote it as $H < G$.*

Proposition 4.2.4. *The set $H \subseteq G$ is a subgroup of a group $(G, *)$ if and only if*

1. *H is non-empty.*
2. *For all $(x, y) \in H^2$, $x * y \in H$.*
3. *For all $x \in H$, $x^{-1} \in H$.*

Proposition 4.2.5. *The set H is a subgroup of a group $(G, *)$ if and only if*

1. *H is non-empty.*
2. *For all $(x, y) \in H^2$, $x * y^{-1} \in H$.*

Example 4.2.6.
- *Let $(G, *)$ be a group. Then G and $\{e_G\}$ are subgroups of G.*
- *$(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.*

Proposition 4.2.7. *The arbitrary intersection 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 $K = \bigcap_{i \in I} H_i$ be the intersection of all the H_i's. The set K is non-empty since it contains the identity element e, which belongs to each of the subgroups H_i. Let x and y be two elements of K. For all $i \in I$, we have $x * y^{-1} \in H_i$, since H_i is a subgroup. Thus, $x * y^{-1} \in K$, which proves that K is a subgroup of G. □

Remark 4.2.8. *The arbitrary union of subgroups of a group $(G, *)$ is not necessarily a subgroup of $(G, *)$.*

Example 4.2.9. *Let $*$ be the internal composition law defined on $\mathbb{R}^2$ as follows. For any $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$, $(x_1, y_1) * (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$. We have that $(\mathbb{R}^2, *)$ is a group. Also, $\mathbb{R} \times \{0\}$ and $\{0\} \times \mathbb{R}$ are two subgroups of $(\mathbb{R}^2, *)$. However, $\mathbb{R} \times \{0\} \cup \{0\} \times \mathbb{R}$ is not a subgroup of $(\mathbb{R}^2, *)$.*

4.2.3 Examples of groups

4.2.3.1 The group $\mathbb{Z}/n\mathbb{Z}$

First, it is clear that if n is a positive integer, the set $n\mathbb{Z}$ of integers of the form nk, where k varies in $\mathbb{Z}$ (the set of multiples of n), forms an additive subgroup of $(\mathbb{Z}, +)$.

Proposition 4.2.10. *Every subgroup of $(\mathbb{Z}, +)$ is of the form $(n\mathbb{Z}, +)$.*

Remark 4.2.11. *The congruence relation modulo n, where $n \in \mathbb{N}$ and denoted by $\Leftrightarrow$, is defined as follows*

$$\forall x, y \in \mathbb{Z},\ x \Leftrightarrow y[n] \Leftrightarrow (x - y) \in n\mathbb{Z} \ \Leftrightarrow\ \exists k \in \mathbb{N} / y = x - nk.$$

Read as "x is congruent to y modulo n," it defines an equivalence relation in $(\mathbb{Z}, +)$.
The quotient set is finite and can be written as

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

For example $\mathbb{Z}/2\mathbb{Z} = \{\dot{0}, \dot{1}\}$, $\mathbb{Z}/3\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\}$, $\mathbb{Z}/4\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}\}$, *and* $\mathbb{Z}/6\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}\}$.

- *The quotient addition on* $\mathbb{Z}/n\mathbb{Z}$ *induced by that of* $\mathbb{Z}$ *is given by*

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z},\ \dot{x}\dot{+}\dot{y} = \widehat{x+y}.$$

- *The quotient multiplication on* $\mathbb{Z}/n\mathbb{Z}$ *induced by that of* $\mathbb{Z}$ *is given by*

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z}, \dot{x}\dot{\times}\dot{y} = \widehat{x \times y}.$$

For example, writing the addition and multiplication tables in the quotient set $\mathbb{Z}/n\mathbb{Z}$.

$\dot{+}$	$\dot{0}$	$\dot{1}$
$\dot{0}$	$\dot{0}$	$\dot{1}$
$\dot{1}$	$\dot{1}$	$\dot{0}$

$\dot{\times}$	$\dot{0}$	$\dot{1}$
$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$

Proposition 4.2.12. *The set* $(\mathbb{Z}/n\mathbb{Z}, +)$ *forms a commutative group (quotient group of* $\mathbb{Z}$ *by the congruence relation) with neutral elements* $\dot{0}$ *for addition operation.*

4.2.3.2 Permutation Group

Definition 4.2.13. *Let* E *be a set. A permutation of* E *is a bijection from* E *to itself. We denote the set of permutations of* E *as* S_E. *If* $E = \{1, ..., n\}$, *we simply write* S_n. *The set* S_E *equipped with the composition law of applications forms a group with identity* $e = Id$, *called the symmetric group on the set* E.

Example 4.2.14. *Let's assume* $E = \{1, 2, 3, 4, 5\}$, *and we denote a permutation* $\sigma \in S_5$ *as follows*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$$

Which means $\sigma(1) = 2$, $\sigma(2) = 4$, *etc.*
If we consider

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix} \text{ and } \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix}$$

Then, $\sigma_1 \circ \sigma_2(3) = \sigma_1(2) = 2$.

4.2.4 Group homomorphism

Definition 4.2.15. *Let $(G, *)$ and $(H, \star)$ be two groups. An application f from G to H is a group homomorphism when*

$$\forall x, y \in G,\ f(x * y) = f(x) \star f(y).$$

Moreover,

1. *If $G = H$ and $* = \star$, it is called an endomorphism.*
2. *If f is bijective, it is called an isomorphism.*
3. *If f is a bijective endomorphism, it is called an automorphism.*

Examples 4.2.16.

- *The application $x \longmapsto 2x$ realizes an automorphism of $(\mathbb{R}, +)$.*
- *The application $f : \mathbb{R} \longrightarrow \mathbb{R}_+^*$ that associates each real number with its exponential is a group morphism of $\mathbb{R}$ under addition, to $\mathbb{R}_+^*$ under multiplication, since $f(x + y) = f(x) \cdot f(y)$, for all $x, y \in \mathbb{R}$.*

Proposition 4.2.17. *(Some Elementary Properties of Group Homomorphisms) Let f be a homomorphism from $(G, *)$ to $(H, \star)$*

1. *$f(e_G) = e_H$.*
2. *For all $x \in G$, $f(x') = (f(x))'$ (where x' is the symmetric of x in G, and $(f(x))'$ is the symmetric of $f(x)$ in H).*
3. *If f is an isomorphism, then its reciprocal application f^{-1} is an isomorphism from $(H, \star)$ to $(G, *)$.*
4. *If $G' < G$ then $f(G') < H$.*
5. *If $H' < H$ then $f^{-1}(H') < G$.*

Proof :

1. $f(e_G * e_G) = f(e_G)$ then $f(e_G) \star f(e_G) = f(e_G)$, which shows that by composing on the right with $f(e_G)'$, that $f(e_G) = e_H$.

2. Let $x \in G$
$$f(x') \star f(x) = f(x' * x) = f(e_G) = e_H.$$
On the other hand,
$$f(x) \star f(x') = f(x * x') = f(e_G) = e_H.$$
Hence, $f(x') = (f(x))'$.

3. Let y_1 and y_2 be two arbitrary elements of H. Set $x_1 = f^{-1}(y_1)$, $x_2 = f^{-1}(y_2)$. Since f is a group homomorphism, we have $f(x_1 * x_2) = f(x_1) \star f(x_2)$, so $f(x_1 * x_2) = y_1 \star y_2$, which implies $x_1 * x_2 = f^{-1}(y_1 \star y_2)$, i.e., $f^{-1}(y_1) * f^{-1}(y_2) = f^{-1}(y_1 \star y_2)$. This proves that f^{-1} is a group morphism from H to G, which completes the proof.

4. and 5. Left for the reader.

□

Definition 4.2.18. *Let f be a homomorphism from G to H*

1. *The kernel of f, denoted $Ker(f)$, is the set of antecedents of e_H under f*
$$Ker(f) = \{x \in G \mid f(x) = e_H\}.$$

2. *The image of f, denoted $Im(f)$, is $f(G)$ (the set of images of elements in G under f), i.e.,*
$$Im(f) = \{f(x), x \in G\}.$$

Remark 4.2.19. *According to the last two points of proposition (5.4.1), the kernel and image of f are respective subgroups of G and H.*

Proposition 4.2.20. *Let f be a homomorphism from $(G, *)$ to $(H, \star)$*

1. *f is surjective if and only if $Im(f) = H$.*

2. *f is injective if and only if $Ker(f) = \{e_G\}$.*

Proof : (1) is immediate by the definition of onto mapping. To prove (2), first assume that f is injective. Let x be an element of $Ker(f)$. We have $f(x) = e_H$, and since $f(e_G) = e_H$, we deduce that $f(x) = f(e_G)$, which implies $x = e_G$ due to the injectivity of f. Thus, $Ker(f) = \{e_G\}$. Conversely, suppose that $Ker(f) = \{e_G\}$, and let's show that f is injective. Consider $x, y \in G$ such that $f(x) = f(y)$. Then, $f(x) \star (f(y))' = e_H$, so $f(x * y') = e_H$, which means $x * y' \in Ker(f)$. Since $Ker(f) = \{e_G\}$, we get $x * y' = e_G$, and consequently, $x = y$. This demonstrates the injectivity of f, this completes the proof. □

4.3 Ring Structure

4.3.1 Definitions

Definition 4.3.1. *A ring is a set equipped with two binary operations $(A, *, \star)$ such that*

1. *$(A, *)$ forms a commutative group with the identity denoted as 0_A.*
2. *The operation $\star$ is an associative and distributive binary operation on A with respect to $*$*

$$\forall x, y \in A,\ x \star (y * z) = x \star y * x \star z,\ \text{and}\ (x * y) \star z = x \star z * y \star z.$$

Example 4.3.2. *The sets $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, and $(\mathbb{C}, +, \times)$ are well-known rings.*

Definition 4.3.3. *(Types of rings)*

1. *A ring $(A, *, \star)$ is said **Ring with unity** if its multiplicative identity exists i.e.,*

$$\exists 1_A \in A,\ 1_A \star x = x \star 1_A = x,\ \forall x \in A.$$

2. *A ring $(A, *, \star)$ is said **Commutative ring** (or abelian ring) if the operation $\star$ is commutative.*

Remark 4.3.4.
1. *If the operation $\star$ is commutative, the ring is called a commutative or abelian ring.*
2. *The set $A - \{0_A\}$ is denoted A^*.*

Notations and Conventions. Let $(A, *, \star)$ be a ring. Let n be a non-zero natural number, and let x be an element of A.

1. We denote the element nx in A, which is equal to the composition by the first law $*$ of n terms equal to x. In other words, for all $n \in \mathbb{N}^*$ and $x \in A$,

$$nx = \underbrace{x * x * x * ... * x}_{n\ terms}$$

   In particular, taking $n = 1$, we have $1x = x$ for all $x \in A$.

2. Similarly, we denote the element x^n in A, which is equal to the composition by the second law $\star$ of n terms equal to x. In other words, for all $n \in \mathbb{N}^*$ and $x \in A$,

$$x^n = \underbrace{x \star x \star x \star ... \star x}_{n\ terms}$$

   In particular, taking $n = 1$, we have: $x^1 = x$ for all $x \in A$.

3. And for $n = 0$? Let's denote by 0_A the zero element and by 1_A the unit element of $(A, *, \star)$ (this notation is a bit unfortunate here as it reminds us of the additive notation and the multiplicative notation that we are trying to avoid). Then, by convention, for all $x \in A$, $0x = 0_A$ and $x^0 = 1_A$.

For simplicity, we temporarily omit the notations $\star$ and $*$ defined on A in favor of the notations additive $(+)$ and multiplicative $(\times)$. So, we refer to the ring $(A, +, \times)$ instead of $(A, *, \star)$.

Definition 4.3.5. *1. A commutative ring $(A, +, \times)$ is called integral if it is*

(a) *Different from the zero ring (i.e., if $A \neq \{0_A\}$),*

(b) $\forall a, b \in A$, $(a \times b = 0) \Rightarrow (a = 0 \vee b = 0)$.

2. When a product $a \times b$ is zero but neither a nor b is zero, we say that a and b are zero divisors.

Example 4.3.6.

- $(\mathbb{Z}, +, \times)$ *of integers is integral, it has no zero divisors.*
- *The ring $\mathbb{Z}/6\mathbb{Z}$ of residue classes modulo 6 is not integral since $\dot{2}\dot{\times}\dot{3} = \dot{6}$, so $\dot{2}\dot{\times}\dot{3} = \dot{0}$. The same applies to $\mathbb{Z}/4\mathbb{Z}$.*

Definition 4.3.7. *Let $(A, +, \times)$ be a ring (not necessarily commutative) and 0_A be the zero of the ring. An element $a \in A$ is said nilpotent if*

$$\exists n \in \mathbb{N}^*,\ a^n = 0_A.$$

Remark 4.3.8. *1. $(A, +, \times)$ be a ring, (not necessarily commutative), then it is clear that a nilpotent element of A is a zero divisor.*

2. Every ring has at least a nilpotent element which is 0_A.

Proposition 4.3.9. *Let $(A, +, \times)$ be a ring. The computation rules in rings are as follows*

1. $\forall x \in A$, $x \times 0_A = 0_A \times x = 0_A$ *(The element 0_A is then called an absorbing element for the law $\times$.)*
2. $\forall x, y \in A$, $(-x) \times y = x \times (-y) = -(x \times y)$.
3. $\forall x \in A$, $(-1_A) \times x = -x$.
4. $\forall x, y \in A$, $(-x) \times (-y) = x \times y$.
5. $\forall x, y, z \in A$, $x \times (y - z) = x \times y - x \times z$ *and* $(y - z) \times x = y \times x - z \times x$.

4.3.2 Sub-rings

Definition 4.3.10. *Let $(A, *, \star)$ be a ring. A non-empty subset A_1 of A is a sub-ring of A if the laws $*$ and $\star$ induce binary operations on A_1, and equipped with these laws, $(A_1, *, \star)$ is a ring.*

Proposition 4.3.11. *A non-empty subset A_1 of A is a sub-ring of A if and only if*

1. $0_A \in A_1$;
2. *For all $x, y \in A_1$, $x * y^{-1} \in A_1$;*
3. $\forall x, y \in A_1,\ x \star y \in A_1$.

Example 4.3.12. *$(\mathbb{Z}, +, \times)$ is a sub-ring of $(\mathbb{Q}, +, \times)$, which is a sub-ring of $(\mathbb{R}, +, \times)$, and that is a sub-ring of $(\mathbb{C}, +, \times)$.*

4.3.3 Ring Homomorphisms

Definition 4.3.13. *Let $(A, +_A, \times_A)$ and $(B, +_B, \times_B)$ be two rings with unites 1_A and 1_B (respectively). A ring homomorphism from A to B is a function from A to B such that*

1. $f(1_A) = 1_B$;
2. *For all $x, y \in A$, $f(x +_A y) = f(x) +_B f(y)$, and $f(x \times_A y) = f(x) \times_B f(y)$.*

4.3.4 Ideals of a Commutative Ring

Let $(A, +, \times)$ be a commutative ring

Definition 4.3.14. *(Ideal) A subset I of A is an ideal of the ring $(A, +, \times)$ if*

1. *$(I, +)$ is a subgroup of $(A, +)$;*
2. *For every $a \in A$, we have $aI \subset I$, in other words $\forall a \in A$, $\forall x \in I$: $ax \in I$.*

Proposition 4.3.15. *A subset I of A is an ideal of the ring $(A, +, \times)$ if and only if*

1. $0_A \in I$;
2. *For all $x, y \in I$, $x - y \in I$.*
3. $\forall a \in A$, $\forall x \in I$, $a \times x \in I$.

Examples 4.3.16. 1. *Every non-trivial ring has at least two ideals: the trivial ideal $\{0\}$ and A itself. The ideals of A, distinct from A, are called proper ideals.*

2. *Every element x of A defines a principal ideal*

$$< x >= xA = \{ax/a \in A\}.$$

It is the smallest ideal that contains a, and we say it is generated by a.

3. *More generally, if $x_1, x_2, ..., x_n$ belong to A, the smallest ideal containing $x_1, x_2, ..., x_n$ is*

$$< x_1, x_2, ..., x_n >= x_1A + x_2A + ... + x_nA = \{a_1x_1 + ... + a_nx_n/a_1, ..., a_n \in A\}.$$

Indeed, it is immediately verified that $I = x_1A + x_2A + ... + x_nA$ is non-empty and stable under linear combinations, therefore it is an ideal.

4.4 Field Structure

Definition 4.4.1. *A field is a commutative ring in which every non-zero element is invertible. If, in addition, the second operation $\times$ is commutative on $\mathbb{K}$, then we say that the field $(\mathbb{K}, +, \times)$ is commutative.*

Example 4.4.2. *$(\mathbb{Q}, +, \times)$ and $(\mathbb{R}, +, \times)$ are commutative fields.*
$(\mathbb{Z}, +, \times)$ is not a field.

4.5 Some exercises with solutions

Exercise 4.5.1. *Show that the given laws equip the set G with a group structure and determine if it's abelian*

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

Solution :

$(G, *)$ is a group since,

- $*$ is a binary operation on G, let $x, y \in G$
  To prove that, fix $y \in]-1, 1[$ and studying the function defined on $]-1, 1[$ by:

$$f(t) = \frac{t + y}{1 + ty}$$

this function is derivable on $]-1, 1[$, and

$$f'(t) = \frac{1 - y^2}{(1 + ty)^2} > 0, \text{ on }]-1, 1[$$

which means that f is strictly increasing on $]-1, 1[$ and

$$f(-1) < x * y = f(x) < f(1),$$

since $f(-1) = -1$ and $f(1) = 1$, then $x * y \in]-1, 1[$.

- $*$ is associative, $\forall (x,y,z) \in G^*$

$$\begin{aligned} x*(y*z) &= \frac{x+(y*z)}{1+x(y*z)} \\ &= \frac{x+\frac{y+z}{1+yz}}{1+x\frac{y+z}{1+yz}} \\ &= \frac{x+y+z+xyz}{1+xy+xz+yz}. \end{aligned}$$

  Similarly,

$$(x*y)*z = \frac{x+y+z+xyz}{1+xy+xz+yz}.$$

- 0 is a neutral element for the operation $*$, since

$$\forall x \in G,\ x*0 = 0*x = \frac{x+0}{1+x(0)} = x.$$

- Each element of G has a symmetrical element in G, since

$$\forall x \in G,\ x*y = y*x = 0,$$

  which means

$$\frac{x+y}{1+xy} = 0.$$

  Hence, $y = -x$.
  Then $(G,*)$ is a group. Additionally, it is abelian, since

$$\forall x,y \in G,\ x*y = y*x.$$

Exercise 4.5.2. *In the following cases, determine if H is a subgroup of group G*

1. $G = (\mathbb{Z},+)$; $H =$ {*even numbers*}.

2. $G = (\mathbb{R},+)$; $H = [1,+\infty[$.

Solution :

1. H is a subgroup of G, since $0 \in H$, and

$$\forall x,y \in H,\ \ -x \in H \text{ and } x+y \in H.$$

2. H i a not a subgroup of G, since $0 \notin H$.

Exercise 4.5.3. *Let $(G,+)$ be a commutative group. We denote by $End(G)$ the set of endomorphisms of G, on which we define the operation $+$ as follows*

$$\forall f,\ g \in End(G),\ (f+g)(x) = f(x) + g(x),\ \forall x \in G.$$

Prove that $(End(G),+,\circ)$ forms a ring.

Solution :

We remark that $+$ and $\circ$ is an internal composition law on $End(G)$, we need to check the properties:

1. $(End(G),+,\circ)$ is a commutative group, since $+$ is associative, commutative, and the application $0_G : G \to G$ is an identity element for the operation $+$, and each element $f \in End(G)$ has an inverse $-f : G \to G$ that associates to each element $x \in G$, $-f(x)$.

2. The operation $\circ$ is associative.

3. The operation $\circ$ has an identity element, which is the identity application.

4. The operation $\circ$ is distributive, since $\forall f,g,h \in End(G)$ and for all $x \in G$,

$$\begin{aligned}((f+g)\circ h)(x) &= (f+g)(h(x)) \\ &= f(h(x)) + g(h(x)) \\ &= (f\circ h + g\circ h)(x),\end{aligned}$$

and

$$\begin{aligned}(f\circ(g+h))(x) &= f((g+h)(x)) \\ &= f(g(x)+h(x)) \\ &= f(g(x)) + f(h(x)) \\ &= (f\circ g + f\circ h)(x).\end{aligned}$$

Hence, $(End(G),+,\circ)$ is a ring.

Exercise 4.5.4. *If $(G,*)$ is a group such that $(a*b)^2 = a^2 * b^2$, for all $(a,b) \in G^2$, prove that $(G,*)$ is an abelian group.*

Solution :

For any $a,b \in G$, by the given property:

$$(a*b)*(a*b) = (a*a)*(b*b).$$

Using associativity, expand both sides:

$$(a * b) * (a * b) = a * (b * a) * b.$$

Equating with the right-hand side:

$$a * (b * a) * b = (a * a) * (b * b).$$

Cancel a and b on both sides (using inverses):

$$b * a = a * b.$$

Thus, $(G, *)$ is abelian.

Exercise 4.5.5. *Determine whether the following maps are ring homomorphisms:*

1. $f_1 : \mathbb{Z} \longrightarrow \mathbb{Z}$, *with* $f_1(x) = x + 1$.
2. $f_2 : \mathbb{Z} \longrightarrow \mathbb{Z}$, *with* $f_2(x) = x^2 + 1$.
3. $f_3 : \mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$, *with* $f_3(x) = 4x$.

Solution :

1. $f_1 : (\mathbb{Z}, +, \times) \to (\mathbb{Z}, +, \times)$, with $f_1(x) = x + 1$:
   - Additivity: $f_1(x + y) = (x + y) + 1 \neq f_1(x) + f_1(y) = (x + 1) + (y + 1)$.
   - Multiplicativity: $f_1(xy) = xy + 1 \neq f_1(x)f_1(y) = (x + 1)(y + 1)$.

   Therefore, f_1 is **not** a ring homomorphism.

2. $f_2 : (\mathbb{Z}, +, \times) \to (\mathbb{Z}, +, \times)$, with $f_2(x) = x^2 + 1$:
   - Additivity: $f_2(x + y) = (x + y)^2 + 1 \neq f_2(x) + f_2(y) = (x^2 + 1) + (y^2 + 1)$.
   - Multiplicativity: $f_2(xy) = (xy)^2 + 1 \neq f_2(x)f_2(y) = (x^2 + 1)(y^2 + 1)$.

   Therefore, f_2 is **not** a ring homomorphism.

3. $f_3 : (\mathbb{Z}/15\mathbb{Z}, \dot{+}, \dot{\times}) \to (\mathbb{Z}/15\mathbb{Z}, \dot{+}, \dot{\times})$, with $f_3(x) = 4x$:
   - Additivity: $f_3(x + y) = 4(x + y) = 4x + 4y = f_3(x) + f_3(y)$.
   - Multiplicativity: $f_3(xy) = 4(xy)$ and $f_3(x)f_3(y) = (4x)(4y) = xy \neq f_3(xy)$.

   Therefore, f_3 is a **ring homomorphism**.

Chapter 5

Polynomials ring

This chapter is depicted to the field of polynomials, essential tools in various mathematical computations and applications. We'll explore the nature of polynomials, their degrees, roots, and properties within the context of polynomial rings.

5.1 Construction of polynomials ring

A polynomial with coefficients in $\mathbb{K}$ (ring) is defined as a finite sequence $(a_0, ..., a_n)$ of elements from $\mathbb{K}$. We denote this polynomial as $\sum_{n\geq 0} a_n X^n$, where X is referred to as the indeterminate. We denote $\mathbb{K}[X]$ as the set of polynomials with coefficients in $\mathbb{K}$.
We define the following operations on $\mathbb{K}[X]$: If $P(X) = \sum_{n\geq 0} a_n X^n$ and $Q(X) = \sum_{n\geq 0} b_n X^n$ (where the sequences (a_n) and (b_n) are zero from a certain rank), then we have:

$$(P+Q)(X) = \sum_{n\geq 0} (a_n + b_n) X^n,$$

and

$$(PQ)(X) = \sum_{n\geq 0} c_n X^n, \ where \ c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

These two operations make $\mathbb{K}[X]$ into a ring. Let A and B be in $\mathbb{K}[X]$, with $B = \sum_{n=0}^{N} b_n X^n$. Then, the composition of A by B in the polynomial ring $\mathbb{K}[X]$ is given as:

$$B \circ A = \sum_{n=0}^{N} b_n A^n.$$

5.2 Polynomial degree, roots and multiplicity

Polynomial degree

If $P = \sum_{n\geq 0} a_n X^n$ is not zero, there exists a larger index $n \in \mathbb{N}$ such that $a_n \neq 0$. This integer is called the degree of P, denoted $deg(P)$. The corresponding coefficient is called the leading coefficient of P. By convention, if P is zero, its degree is $-\infty$. A polynomial with a leading coefficient equal to 1 is called unitary (monic).
For all non-zero polynomials $P, Q \in \mathbb{K}[X]$, where $\mathbb{K}$ is an integral domain, we have

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

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

Example 5.2.1. *$P(x) = 3x^2 + 4x - 2$ is a degree two polynomial in the ring $\mathbb{Z}_4[x]$ (where $\mathbb{Z}_4$ the quotient group of the integers $\mathbb{Z}$ by the subgroup $4\mathbb{Z}$).*
$Q(x) = x^3 - 2x + 3$ is of a degree three polynomial in the ring $\mathbb{R}[x]$.

Example 5.2.2. *Consider $P(x) = 2x = 1$ and $Q(x) = 2x$, P and Q are of degree 1 polynomials in the ring $\mathbb{Z}_4[x]$,*
$deg(PQ) = deg(2x(2x+1)) = deg(2x) = 1$, and $deg(P) + deg(Q) = 2$.

Polynomial roots, multiplicity

Definition 5.2.3. *We say that a is a root of P if $P(a) = 0$. This is equivalent to saying that $(X - a)$ divides P.*

Remark 5.2.4. *In general, the rest of the Eucledian division of a polynomial $P(X)$ by $(X - a)$ is $P(a)$.*

Proposition 5.2.5. *If $a_1, ..., a_n$ are distinct roots of P, then $(X - a_1), ..., (X - a_n)$ divide P. A polynomial of degree n has at most n roots.*

Definition 5.2.6. *Let P be in $\mathbb{K}[X]$, let $a \in \mathbb{K}$, and let $m \in \mathbb{N}$. We say that a is a root of multiplicity m if $P(a) = P'(a) = ... = P^{(m-1)}(a) = 0$ and $P^{(m)}(a) \neq 0$.*

Theorem 5.2.7. *Let $P \in \mathbb{K}[X]$, let $a \in \mathbb{K}$, and let $m \in \mathbb{N}$. The following statements are equivalent:*

1. *a is a root of P with multiplicity m.*
2. *$(X - a), ..., (X - a)^m$ divide P, and $(X - a)^{m+1}$ does not divide P.*

Definition 5.2.8. *A polynomial $P(x)$ of degree N is said to be factored if it can be expressed as follows:*

$$P(x) = a_N \prod_{i=1}^{N} (x - z_i).$$

5.3 Arithmetics of polynomials

Let $\mathbb{K}$ represents the field $\mathbb{R}$ or $\mathbb{C}$.

Derivation: For$P = \sum_{n\geq 0} a_n X^n$, $P' = \sum_{n\geq 1} n a_n X^{n-1}$, called the derivative polynomial of P. If $deg(P) \geq 1$, then $deg(P') = deg(P) - 1$.

Leibniz's Formula: For$P, Q \in \mathbb{K}[X]$ and $n \in \mathbb{N}$, we have

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

Taylor's Formula: Let P be in $\mathbb{K}[X]$ and $a \in \mathbb{K}$. Then

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

Divisibility, Euclidean Division: Let $A, B \in \mathbb{K}[X]$ with B nonzero polynomial. We say that B divides A if there exists $Q \in \mathbb{K}[X]$ such that $A = BQ$. We also say that B is a divisor of A or that A is a multiple of B.

Two nonzero polynomials A and B in $\mathbb{K}[X]$ are said to be associated if A divides B and B divides A. This is equivalent to saying that there exists $\lambda \in \mathbb{K}^*$ such that $A = \lambda B$.

Theorem 5.3.1. *(Euclidean Division of Polynomials). Let A, B be in $\mathbb{K}[X]$ with B nonzero polynomial. There exists a unique pair $(Q, R) \in \mathbb{K}[X]$ such that*

$$A = BQ + R \text{ and } deg(R) < deg(B).$$

Example 5.3.2. *The quotient and remainder on dividing $f(X) = X^5 - X^2 + 2$ by $g(X) = X^2 + 1$ in the following case are:*

$Q(X) = X^3 - X - 1$ *and* $R(X) = X + 3$.

Remark 5.3.3. *A polynomial $P = \sum_{n=0}^{N} a_n X^n \in \mathbb{K}[X]$ defines a polynomial function $\widetilde{P} : K \to K$ as $\widetilde{P}(z) = \sum_{n=0}^{N} a_n z^n$. Often, we identify a polynomial with a polynomial function.*

In terms of polynomial arithmetic, if A and B are non-zero polynomials in $\mathbb{K}[X]$, each common divisor of A and B of maximal degree is called the GCD of A and B.
We say that A and B are coprime if $A \wedge B = 1$.

Theorem 5.3.4. *(Bezout theorem) Let $A, B \in \mathbb{K}[X]$ be non-zero. Then $A \wedge B = 1$ if and only if there exist $U, V \in \mathbb{K}[X]$ such that $AU + BV = 1$.*

Lemma 5.3.5. *(Gauss lemma) Let $A, B, C \in \mathbb{K}[X]$ be non-zero. We assume $A \wedge B = 1$. Then if $A|BC$, we have $A|C$.*

Remark 5.3.6. *Let A, B be non-zero elements in $\mathbb{K}[X]$. Any common multiple of A and B with minimal degree is called the least common multiple (LCM) of A and B. All LCMs of A and B are associated. In particular, only one is unitary, sometimes referred to as the LCM of A and B. It's denoted as $A \vee B$.*

Irreducible Polynomials

Theorem 5.3.7. *d'Alembert-Gauss's Theorem: Every non-constant polynomial in $\mathbb{C}[X]$ has a root in $\mathbb{C}$.*

Therefore, every non-constant polynomial in $\mathbb{C}[X]$ is factorable.
A polynomial $P \in \mathbb{K}[X]$ is irreducible if it's of degree greater than or equal to 1, and if all its divisors are constant polynomials or polynomials associated with P (meaning the polynomials of the form λP where $\lambda \in \mathbb{K}$).

Decomposition into irreducible factors over $\mathbb{C}[X]$

The irreducible polynomials of $\mathbb{C}[X]$ are polynomials of degree 1.
Every non-zero polynomial is a product of its leading coefficient and unitary irreducible polynomials. This decomposition is unique up to the order of terms.

Corollary 5.3.8. *Let $A, B \in \mathbb{K}[X]$ with B non-zero. Then B divides A if and only if all the roots of B are roots of A, and their multiplicity as roots of A is greater than or equal to their multiplicity as roots of B.*
In particular, two non-zero polynomials in $\mathbb{C}[X]$ are coprime if and only if they have no common roots.

Decomposition into irreducible factors over $\mathbb{R}[X]$

The irreducible polynomials of $\mathbb{R}[X]$ are polynomials of degree 1 and polynomials of degree 2 with strictly negative discriminants. Every non-zero polynomial is a product of its leading coefficient and unitary irreducible polynomials. This decomposition is unique up to the order of terms.

5.4 Some exercises with solutions

Exercise 5.4.1. *Determine the rest of the euclidian division of X^n over $(X-1)^2$.*

Solution:

There exists a unique couple of polynomials $(P, Q) \in \mathbb{R}[X]$ such that $X^n = (X-1)^2Q + R$, with $deg(R) < 2$. Hence, there exists $a, b \in \mathbb{R}$ such that $R = aX + b$, then

$$X^n = (X-1)^2Q + aX + b \tag{5.4.1}$$

For $X = 1$, we get $a + b = 1$.
We derivative the formula (5.4.1), and we replace $X = 1$, we get $a = n$. Hence

$$R = nX + 1 - n.$$

Exercise 5.4.2. *Let $P = X^5 + X^4 + 2X^3 + 2X^2 + X + 1$*

1. *Compute the GCD of P and P'.*
2. *Determine the common roots of P and P'. Then, determine the multiple roots of P in $\mathbb{C}$.*
3. *Prove that $(X^2+1)^2$ divides P.*
4. *Factorize P in $\mathbb{R}[X]$.*

Solution:

1. We have $P' = 5X^4 + 4X^3 + 6X^2 + 4X + 1$. Using Euclidian division, we obtain
$$P = P'(\frac{1}{5}X + \frac{1}{25}) + (\frac{16}{25}X^3 + \frac{24}{25}X^2 + \frac{16}{25}X + \frac{24}{25}).$$
Using the euclidian division of P' over the rest again, we get that the GCD of P and P' is $X^2 + 1$.
2. The common roots of P and P' are i and $-i$. The multiple roots of P are also i and $-i$.
3. P can be divided by $(X-i)^2(X+i)^2 = (X^2+1)^2$

4. Dividing P over $(X^2+1)^2$, we obtain $X+1$. Hence,

$$P = (X^2+1)^2(X+1).$$

Exercise 5.4.3. *For the following pairs of polynomials $f(X)$ and $g(X)$, find the quotient and remainder on dividing $g(X)$ by $f(X)$.*

1. $g(X) = X^7 - X^3 + 5$, $f(X) = X^3 + 7$ *over* $\mathbb{Q}$.
2. $g(X) = X^2 + 1$, $f(X) = X^2$ *over* $\mathbb{Q}$.

Solution:

1. $g(X) = X^7 - X^3 + 5$, $f(X) = X^3 + 7$ over $\mathbb{Q}$:

$$\frac{g(X)}{f(X)} = X^4 - 7X - 1 + \frac{49X + 12}{X^3 + 7}.$$

Quotient: $X^4 - 7X - 1$, **Remainder:** $49X + 12$.

2. $g(X) = X^2 + 1$, $f(X) = X^2$ over $\mathbb{Q}$:

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

Quotient: 1, **Remainder:** 1.

Exercise 5.4.4. *For which values of $\alpha \in \mathbb{R}$, the polynomial $P(X) = X^3 - 3X + \alpha$ has a root with multiplicity 2. What is the other root?*

Solution:

- Let r be a root with multiplicity 2. Then $P(r) = 0$ and $P'(r) = 0$.
- Compute the derivative:

$$P'(X) = 3X^2 - 3.$$

From $P'(r) = 0$:

$$3r^2 - 3 = 0 \quad \Rightarrow \quad r^2 = 1 \quad \Rightarrow \quad r = \pm 1.$$

- Case $r = 1$: Substitute $r = 1$ into $P(r) = 0$:

$$P(1) = 1^3 - 3(1) + \alpha = 0 \quad \Rightarrow \quad \alpha = 2.$$

- Case $r = -1$: Substitute $r = -1$ into $P(r) = 0$:

$$P(-1) = (-1)^3 - 3(-1) + \alpha = 0 \quad \Rightarrow \quad \alpha = -2.$$

- For $\alpha = 2$, the polynomial is $P(X) = X^3 - 3X + 2$. The roots are 1 (multiplicity 2) and -2.

- For $\alpha = -2$, the polynomial is $P(X) = X^3 - 3X - 2$. The roots are -1 (multiplicity 2) and 2.

Conclusion: The values of α are $\alpha = 2$ or $\alpha = -2$. The other roots are -2 and 2, respectively.

Conclusion

Throughout this course, we have concentrate on a captivating exploration into the foundational principles of algebra 1. From logic and mathematical reasoning to sets, functions, relations, algebraic structures, and polynomial rings, each section has unveiled crucial concepts pivotal in mathematical analysis and problem-solving.

Bibliography

[1] Colmez, P. (2008). Elemets d'analyse et d'algébre. Palaiseau Cedex, France

[2] Fraleigh, J. B. (2017). A First Course in Abstract Algebra, 7th Edition.

[3] Dummit, D. S., & Foote, R. M. (2003). Abstract Algebra. John Wiley & Sons.

These references offer detailed introduction to fundamental concepts of Linear algebra for first year undergraduate students of mathematics.