الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of Higher Education and Scientific Research

ABDELHAFID BOUSSOUF UNIVERSITY NI CENTER MILA
Institute of Mathematics and Computer Science, Department of Mathematics

AlgebrA 1

BOUOUDEN RABAH

(First-Year Mathematics Bachelor's Course)

Année Universitaire : 2024/2025

Table of Contents

Introduction

This booklet is specifically designed for first-year LMD students in Mathematics and Computer Science, with the goal of providing a solid foundation in fundamental mathematical concepts. It covers several key topics that are essential for understanding mathematical structures and their applications across various branches of the exact sciences.

Chapter 1 introduces the basic concepts of mathematical logic, a fundamental area that helps in formulating precise statements and developing rigorous proofs. This chapter equips students with the logical reasoning skills necessary for their future studies in mathematics.

Chapter 2 is entirely dedicated to the study of sets, relations, and functions. These are foundational concepts in mathematics, and the chapter emphasizes set theory, the notion of relations, and how functions and mappings are defined and analyzed. It provides practical tools for solving complex problems in mathematics.

In Chapter 3, we delve into algebraic structures, focusing particularly on groups, rings, and fields. These concepts are at the heart of modern algebra and are essential for understanding the various ways in which elements can be combined or manipulated within a given system.

Finally, Chapter 4 is devoted to the study of polynomial rings, a key area of algebra. Polynomial rings are fundamental objects in many areas of mathematics and computer science, and this chapter provides a detailed analysis of their properties, operations, and applications.

We hope that this booklet will meet the expectations of the students, providing them with a clear and thorough understanding of the topics covered. It is designed not only to provide the necessary knowledge but also to stimulate critical thinking and the application of concepts to real-world situations.

At the end of the booklet, we have included a selection of bibliographic references for students who wish to further explore the topics and deepen their understanding of the material presented in this document.

Chapter 1

Logic concepts

In this chapter, we will limit ourselves to the introduction of the first elements of classical logic, laying the groundwork for further exploration into this foundational discipline. Logic, as we define it, is the study of arguments, a process of reasoning in which we draw conclusions from premises. At its core, logic seeks to provide a structured framework for distinguishing valid from invalid reasoning. In other words, logic attempts to codify what counts as legitimate means by which to draw conclusions from given information. It establishes rules and principles that help us evaluate the soundness of an argument, ensuring that conclusions follow logically from their premises. By doing so, logic serves as a critical tool in various fields, from philosophy and mathematics to everyday decision-making, offering a method to assess the strength and validity of different forms of reasoning.

This expanded version adds more context to what logic is, why it is important, and its application in different areas.

1.1 Propositions (Statements)

To study arguments, one must first study sentences, as they are the essential components of arguments

Definition 1.1.1.
A sentence that is either true or false is called a proposition.

P
1
0

TABLE 1.1: Truth table of a proposition P

However, not all sentences are propositions. Questions, exclamations, commands, and self-contradictory sentences, like the following examples, cannot be asserted or denied.

Example 1.1.1.

1. *Is mathematics logic?*
2. *Hey there!*
3. *Do not panic.*
4. *This sentence is false.*

Statements are denoted by capital letters P, Q, R,....

If the proposition is true, we assign it the value 1 (or T); if it is false, we assign it the value 0 (or F).

There are two types of propositions.
♦ An atom is a proposition that is not comprised of other propositions.

Example 1.1.2.

1. *"Algiers is the capital of Algeria" is a true proposition.*
2. *"16 is a multiple of 2" is a true proposition.*
3. *"19 is a multiple of 2" is a false proposition.*

♦ A proposition that is not atomic but is constructed using other propositions is called a compound proposition.

1.2 The Propositional Calculus

Propositions may be combined in various ways to form more complicated proposition. There are five types.

Definition 1.2.1. ***(A negation)***
A negation of a given proposition P is a proposition $\bar{P}$ $(NotP)$ such that when P is true, $\bar{P}$ is false; when P is false, $\bar{P}$ is true.

Example 1.2.1.

1. *The negation of $3+8=5$ is $3+8\neq 5$. In this case, we say that $3+8=5$ has been negated.*
2. *Negating the proposition the sine function is periodic yields the sine function is not periodic.*
3. *The negation of "The number 5 is even" is "The number 5 is not even".*

For the proposition $\bar{P}$, we obtain the following truth table (1.2)

P	$\bar{P}$
1	0
0	1

TABLE 1.2: Truth table of the proposition $\bar{P}$

Definition 1.2.2. ***(A conjunction)***
A conjunction is a proposition formed by combining two propositions (called conjuncts) using the word 'and.' The conjunction of sentences A and B will be designated by A and B $(A \wedge B)$ and has the following truth table:
$A \wedge B$ is true if and only if both A and B are true.
$A \wedge B$ are called the conjuncts of A and B.

Example 1.2.2.

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

TABLE 1.3: Truth table of the statement $P \wedge Q$

1. Let:

$$P_1 : \textit{It is sunny today.}$$
$$P_2 : \textit{The temperature is warm.}$$

The conjunction of these propositions is:

$$P_1 \wedge P_2 : \textit{It is sunny today and the temperature is warm.}$$

2. Let:

$$Q_1 : \textit{The car is red.}$$
$$Q_2 : \textit{The car has alloy wheels.}$$

The conjunction of these propositions is:

$$Q_1 \wedge Q_2 : \textit{The car is red and it has alloy wheels.}$$

In natural languages, there are two distinct uses of "or": the inclusive and the exclusive. According to the inclusive usage, A **or** B means "either A, or B, or both". In contrast, according to the exclusive usage, the meaning is "either A or B, but not both". To represent the inclusive connective, we will introduce a special symbol, $\vee$.

Definition 1.2.3. *(A disjunction)*
A disjunction is a proposition formed by combining two propositions (called disjuncts) using the word or. $A \vee B$ is false if and only if both A and B are false. $A \vee B$ called a disjunction, with the disjuncts A and B. The truth table of $A \vee B$ is as follows:

Example 1.2.3.

A	B	$A \vee B$
1	1	1
0	1	1
1	0	1
0	0	0

TABLE 1.4: Truth table of the proposition $A \vee B$

1. *Let:*

$$P_1 : \textit{It is raining.}$$
$$P_2 : \textit{It is windy.}$$

The disjunction of these propositions is:

$$P_1 \vee P_2 : \textit{It is raining or it is windy.}$$

2. *Let:*

$$Q_1 : \textit{The temperature is above 25 C.}$$
$$Q_2 : \textit{The humidity level is high.}$$

The disjunction of these propositions is:

$$Q_1 \vee Q_2 : \textit{The temperature is above 25 C or the humidity level is high.}$$

3. *« 10 is divisible by 2» is a true statement. « 10 is divisible by 3 » is a false statement. So, $P \wedge Q$ is a false statement. On the other hand, $P \vee Q$ is true.*

A statement of the form "If P, then Q" is called a conditional statement. The statement "P" is called the antecedent or the hypothesis, and "Q" is called the consequent or the conclusion. If P, then Q is also expressed by saying that Q is a necessary condition for P. An other way to express it is to say that P is a sufficient condition for Q.

Definition 1.2.4. *(Implication, Equivalence)*
Let P and Q be two statements.

1. *A statement of the form $P \Rightarrow Q$ (read as "P implies Q") is called an implication. The statement $P \Rightarrow Q$ is logically equivalent to the statement "If*

P, then Q". The statement "P" is called the antecedent or hypothesis, and "Q" is called the consequent or conclusion. Mathematically, the truth table for $P \Rightarrow Q$ is as in table 1.5.

P	Q	$P \Longrightarrow Q$
1	1	1
1	0	0
0	1	1
0	0	1

TABLE 1.5: Truth table of the statement $P \Longrightarrow Q$

2. *A statement of the form P if and only if Q (abbreviated as $P \iff Q$) is called an equivalence. The statement $P \iff Q$ is logically equivalent to the conjunction of $P \Rightarrow Q$ and $Q \Rightarrow P$, which means that P implies Q and Q implies P. The statement $P \iff Q$ is true when both P and Q are either both true or both false, and false in all other cases. Mathematically, the truth table for $P \iff Q$ is as in table 1.6.*

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

TABLE 1.6: Truth table of the statement $P \Leftrightarrow Q$

Remark 1.2.1.

1. *In practice, if P, Q, and R denote three statements, then the composite statement ($P \Rightarrow Q$ and $Q \Rightarrow R$) is written as: ($P \Rightarrow Q \Rightarrow R$).*

   Similarly, the composite statement ($P \Leftrightarrow Q$ and $Q \Leftrightarrow R$) is written as: ($P \Leftrightarrow Q \Leftrightarrow R$).

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

1.2.1 Properties

Definition 1.2.5.

Let P and Q be two propositions (either composite or simple).

1. *If P is true when Q is true, and if P is false when Q is false, then we say that P and Q have the same truth table or that they are logically equivalent, and we denote this by $P \Leftrightarrow Q$.*

2. *In the opposite case, we denote this by $P \not\Leftrightarrow Q$.*

Example 1.2.4.
Let P, Q, and R be three statements, then:

1. $\bar{\bar{P}} \Leftrightarrow P$.

2. $(P \wedge P) \Leftrightarrow P$. *Similarly,* $(P \vee P) \Leftrightarrow P$.

3. $(P \wedge Q) \Leftrightarrow (Q \wedge P), \qquad (P \vee Q) \Leftrightarrow (Q \vee P)$.

4. $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R), \qquad (P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$.

5. $(P \wedge (Q \vee P) \Leftrightarrow P$.

6. $(P \Leftrightarrow Q \Leftrightarrow (Q \Leftrightarrow P)$.

7. $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R), \qquad P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$.

8. $\overline{P \wedge Q} \Leftrightarrow \overline{P} \vee \overline{Q}, \qquad \overline{P \vee Q} \Leftrightarrow \overline{P} \wedge \overline{Q}$.

9. *The compound proposition* $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$ *is true regardless of the truth values of P, Q and R.*

10. *The compound proposition* $((P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R)) \Rightarrow (P \Leftrightarrow R)$ *is true regardless of the truth values of P, Q and R.*

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

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

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

14. $(P \Leftrightarrow Q) \Leftrightarrow ((P \Rightarrow Q) \wedge (Q \Rightarrow P))$.

1.3 Mathematical quantifiers

Definition 1.3.1.
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.

A predicate containing the variable x will be denoted by $P(x)$.

Example 1.3.1.
The statement $P(n)$ defined by " n is a multiple of 2" is a predicate on $\mathbb{N}$. It becomes a proposition when an integer value is assigned to n. For example,

1. *The proposition $P(10)$ defined by "10 is a multiple of 2" obtained by replacing n with 10, is true;*
2. *The proposition $P(11)$ defined by "11 is a multiple of 2" obtained by replacing n with 11, is false.*

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

Definition 1.3.2.
Let $P(x)$ be a predicate defined on a set E.

1. *(**Universal quantifier**)The quantifier "for all" (also called "for every"), denoted by $\forall$, allows us to define the quantified proposition "$\forall x \in E,\ P(x)$" which is true when all elements x of E satisfy $P(x)$.*
2. *(**Existential quantifier**) The quantifier "there exists," denoted by $\exists$, allows us to define the quantified proposition "$\exists x \in E,\ P(x)$" which is true when there exists (at least) one element x belonging to E that satisfies the statement $P(x)$.*

Example 1.3.2.

1. *The statement "$x^2 + 2x - 3 \leq 0$" is a predicate defined on $\mathbb{R}$. It can be true or false depending on the value of x.*

   The statement "$\forall x \in [-3, 1],\ x^2 + 2x - 3 \leq 0$" is a quantified proposition. It is true because the quantity $x^2 + 2x - 3$ is negative or zero for every x belonging to the closed interval $[-3, 1]$.

2. *The quantified proposition "$\forall x \in \mathbb{N},\ (n-3)n > 0$" is false because there exists an element n in $\mathbb{N}$ (taking $n = 0$, $n = 1$, $n = 2$, or $n = 3$) for which the statement "$(n-3)n > 0$" is false.*

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

1.3.1 The rules of negation for a quantified proposition

1. 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.»

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

.

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

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

.

Here are some examples:

Example 1.3.3.

1. *The negation of* $(\forall x \in [0, +\infty[,\ \ (x^2 \geq 1))$ *is* $(\exists x \in [0, +\infty[,\ \ (x^2 < 1))$.
2. *The negation of* $(\exists z \in \mathbb{C},\ \ z^2 + z + 1 = 0)$ *is* $(\forall z \in \mathbb{C},\ \ z^2 + z + 1 \neq 0)$.
3. *It is not more difficult to write the negation of complex sentences. For the proposition:*

$$\forall x \in \mathbb{R}, \quad \exists y > 0 \quad (x + y > 10),$$

its negation

$$\exists x \in \mathbb{R}, \quad \forall y > 0 \quad (x + y \leq 10).$$

Remark 1.3.1.
The order of quantifiers is very important. For example, the two logical sentences

$$\forall x \in \mathbb{R} \ \ \exists y > 0 \ \ (x + y > 10) \text{ and } \exists y > 0 \ \ \forall x \in \mathbb{R} \ \ (x + y > 10)$$

are different. The first one is true, while the second one is false.

1.4 Proof methods

The purpose of the propositional logic of Chapter 1 is to model the basic reasoning that one does in mathematics. Here are some classical methods of reasoning.

1.4.1 Universal Proofs

Our first paragraph proofs will be for propositions with universal quantifiers. To prove $\forall x \in E,\ P(x)$ (interpreted to mean that $P(x)$ holds for all x from a given universe E) from a given set of premises, we show that every object x satisfies $P(x)$ assuming those premises. For this we follow the following diagram

$$\text{Let a be an object in the universe } E \longrightarrow \text{Prove } P(a).$$

Example 1.4.1. *To prove that for all real numbers x,*

$$(x-1)^3 = x^3 - 3x^2 + 3x - 1$$

we introduce a real number and then check the equation.

Proof 1.4.1. *Let a be a real number. Then,*

$$(a-1)^3 = (a-1)(a-1)^2 = (a-1)(a^2 - 2a + 1) = a^3 - 3a^2 + 3a - 1.$$

1.4.2 Existential Proofs

Suppose that we want to write a paragraph proof for $\exists x \in E,\ P(x)$. This means that we must show that there exists at least one object of the universe E that satisfies the formula $P(x)$. It will be our job to find that object. To do this directly, we pick an object that we think will satisfy $P(x)$. This object is called a candidate. We then check that it does satisfy $P(x)$. This type of a proof is called a direct existential proof, and its structure is illustrated as follows:

Choose a candidate from the universe. $\longrightarrow$ Check that the candidate satisfies $P(x)$.

1.4.3 Direct reasoning

We want to show that the proposition ' $P \Rightarrow Q$ ' is true. We assume that P is true and then demonstrate that Q is true as well by following these steps:

1. **assume the antecedent,**
2. **translate the antecedent,**
3. **translate the consequent so that the goal of the proof is known,**
4. **deduce the consequent.**

Example 1.4.2.
We use Direct Proof to write a paragraph proof of the proposition

for all integers x, if 4 divides x, then x is even.

Proof 1.4.2.
Assume that 4 divides the integer a. This means $a = 4k$ for some integer k. We must show that $a = 2l$ for some integer l, but we know that $a = 4k = 2.(2k)$. Hence, let $l = 2k$.

1.4.4 Reasoning by contraposition

Sometimes it is difficult to prove a conditional directly. An alternative is to prove the contrapositive. This is sometimes easier or simply requires fewer lines.

Contrapositive reasoning is based on the following equivalence :

$$(P \Rightarrow Q) \Leftrightarrow (\overline{Q} \Rightarrow \overline{P}). \tag{1.1}$$

Therefore, if we want to show the proposition $P \Rightarrow Q$, we actually demonstrate that if $\overline{Q}$ is true, then $\overline{P}$ is true.

Example 1.4.3.
Let us show that

for all integers n, if n^2 is odd, then n is odd.

A direct proof of this is a problem. Instead, we prove its contrapositive,

$$\text{if } n \text{ is even, then } n^2 \text{ is even.}$$

Proof 1.4.3.
Let n be an even integer. This means that $n = 2k$ for some integer k. To see that n^2 is even, calculate to find $n^2 = (2k)^2 = 4k^2 = 2.(2k^2)$.

1.4.5 Proof by Cases

Suppose that we want to prove $P \Rightarrow Q$ and this is difficult for some reason. We notice, however, that P can be broken into cases. Namely, there exist $P_1, P_2, ..P_n$ such that $P \Leftrightarrow P_1 \bigvee P_2 \bigvee ... \bigvee P_n$.
If we can prove $P_i \Rightarrow Q$ for each i, we have proved $P \Rightarrow Q$.

Example 1.4.4.
Prove that for any integer n, the number $n^3 - n$ is even.

Proof 1.4.4.
We will prove this statement by considering two cases: one where n is even and one where n is odd.

Case 1:** n **is even

If n is even, then by definition, $n = 2k$ for some integer k. Therefore:

$$n^3 - n = (2k)^3 - 2k = 8k^3 - 2k = 2(4k^3 - k).$$

Since $2(4k^3 - k)$ is divisible by 2, $n^3 - n$ is an even number in this case.

Case 2:** n **is odd

If n is odd, then by definition, $n = 2k + 1$ for some integer k. Therefore:

$$n^3 - n = (2k + 1)^3 - (2k + 1).$$

First, expand $(2k + 1)^3$:

$$(2k + 1)^3 = 8k^3 + 12k^2 + 6k + 1.$$

Now calculate:

$$n^3 - n = 8k^3 + 12k^2 + 6k + 1 - (2k + 1) = 8k^3 + 12k^2 + 4k.$$

We notice that $8k^3 + 12k^2 + 4k$ *is divisible by 2, and hence it is even. Therefore, in this case,* $n^3 - n$ *is also even.*

Since we have shown that $n^3 - n$ *is even in both cases, we conclude that* $n^3 - n$ *is always even for any integer* n*.*

1.4.6 Counterexamples

To show that an proposition of the type $\forall x \in E \;\; P(x)$ is true, one must demonstrate that $P(x)$ is true for each x in E.
On the other hand, to show that this proposition is false, it is enough to find an $a \in E$ such that $P(a)$ is false (i.e., $\overline{P(a)}$ is true). (Remember, the negation of $\forall x \in E, \;\; P(x)$ is $\exists x \in E, \;\; \overline{P(x)}$).
To find such an a is to find a counterexample to the proposition $\forall x \in E \;\; P(x)$.

Example 1.4.5.
Prove that the statement "All prime numbers are odd" is false.

Proof 1.4.5. *The statement "All prime numbers are odd" is false. A counterexample to this statement is the number 2, which is both a prime number and an even number.*

- The number 2 is prime because it is only divisible by 1 and itself. - Since 2 is even, it contradicts the statement that all prime numbers are odd.

Thus, the statement "All prime numbers are odd" is false, as the number 2 serves as a counterexample.

1.4.7 Proof by Contradiction:

Proof by contradiction, also known as reasoning by the absurd, involves demonstrating the truth of a proposition by showing that its opposite leads to a contradiction. To use this type of reasoning, follow these steps:

1. **Assume the negation:** Suppose that the proposition you want to prove is false.
2. **Develop the consequences:** Develop the logical consequences of this assumption.
3. **Identify the contradiction:** Show that these consequences lead to a contradiction.
4. **Conclusion:** Conclude that the initial assumption must be false, which means that the proposition you want to prove is true.

Example 1.4.6.

Prove that :

$$\textit{for all integers } n, \textit{ if } n^2 \textit{ is odd, then } n \textit{ is odd.}$$

Proof 1.4.6.

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

1.4.8 Proof by Induction

Proof by induction is a method used in mathematics to prove that a property $P(n)$ holds for all integers n starting from a certain initial value n_0. It consists of two steps:

1. **Base Case:** Verify that the property $P(n)$ is true for the initial value $n = n_0$.
2. **Inductive Step:** Assume that the property is true for a certain integer k (inductive hypothesis), and then prove that the property is true for $k + 1$.

Example 1.4.7.

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

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

1. ***Step 1**: Base Case*

   First, we need to verify the formula for the initial value $n = 1$.

   When $n = 1$:

   $$1 = \frac{1(1+1)}{2} = \frac{1 \cdot 2}{2} = 1$$

   So, the formula holds for $n = 1$.

2. ***Step 2:** Inductive Step*

   Next, we assume that the formula holds for some integer k. That is, we assume:

   $$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$$

   This assumption is called the inductive hypothesis.

   We need to show that if the formula holds for $n = k$, then it also holds for $n = k + 1$.

   Consider the sum of the first $k + 1$ positive integers:

   $$1 + 2 + 3 + \cdots + k + (k+1)$$

   Using the inductive hypothesis, we can write:

   $$1 + 2 + 3 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1)$$

   We need to simplify the right-hand side:

   $$\frac{k(k+1)}{2} + (k+1)$$

   Factor $k + 1$ out of the terms on the right:

   $$\frac{k(k+1)}{2} + (k+1)$$

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

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

So we have shown that if the formula holds for $n = k$, it also holds for $n = k + 1$.

3. ***Conclusion***
   By the principle of mathematical induction, the formula $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ is true for all positive integers n.

1.5 Exercices

Exercice 1.1.
Which of the following sentences are propositions? What are the truth values of those that are propositions?

1. *Paris is in France or Madrid is in China.*
2. *Open the door.*
3. *The moon is a satellite of the Earth.*
4. $x + 5 = 7$.
5. $x + 5 > 9$ *for every real number* x.

Exercice 1.2.
Determine whether each of the following implications is true or false.

1. *If* 0.5 *is an integer, then* $1 + 0.5 = 3$.
2. *If* $5 > 2$, *then cats can fly.*
3. *If* $3 \times 5 = 15$, *then* $1 + 2 = 3$.
4. *For any real* $x \in \mathbb{R}$, *if* $x \leq 0$, *then* $(x - 1) < 0$.

Exercice 1.3.
Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ be a function. Negate the following propositions:

1. $\exists x \in \mathbb{R}$ *such that* $f(x) = 0$.
2. $\exists M > 0$, $\forall A > 0$, $\exists x \geq A : f(x) \leq M$.
3. $\exists x \in \mathbb{R}$, $f(x) > 0$.

4. $\forall \epsilon > 0,\ \exists \eta > 0$ *such that* $\forall (x, y) \in I^2,\ |x - y| \leq \eta \Rightarrow |f(x) - f(y)| > \epsilon$.

Exercice 1.4.
Consider the statement "for all integers a and b, if $a + b$ is even, then a and b are even":

1. *Write the contrapositive of the statement.*
2. *Write the converse of the statement.*
3. *Write the negation of the statement.*
4. *Is the original statement true or false? Prove your answer.*
5. *Is the contrapositive of the original statement true or false? Prove your answer.*
6. *Is the converse of the original statement true or false? Prove your answer.*
7. *Is the negation of the original statement true or false? Prove your answer.*

Exercice 1.5. *(Direct Proof)*
Prove that if n is an even integer, then n^2 is also an even integer.

Exercice 1.6. *(Proof by Contradiction)*
Prove that $\sqrt{2}$ is irrational.

Exercice 1.7. *(Proof by Contrapositive)*

1. *Prove that if n^2 is an even integer, then n is also an even integer.*
2. *Prove that if a and b are integers and ab is odd, then both a and b are odd.*

Exercice 1.8. *(Proof by Mathematical Induction)*

1. *Prove that for all positive integers n, $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.*
2. *Prove that for all positive integers n, $2^n > n$.*

Exercice 1.9. *(Proof by Cases)*
Show that for all $x \in \mathbb{R}$, the following inequality holds:

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

Exercice 1.10. *(Counterexample)*
Prove that the following statement is false: "Every positive integer is the sum of three squares."

1.6 Exercise Solutions

Solution 1.1.

1. *The sentence "Paris is in France or Madrid is in China" is a true proposition.*
2. *The sentence "Open the door" is not a proposition because it is a command.*
3. *The sentence "The moon is a satellite of the Earth" is a true proposition.*
4. *The equation* $x + 5 = 7$ *is not a proposition.*
5. *The inequality* $x + 5 > 9$ *for every real number* x *is a false proposition.*

Solution 1.2.
Determine whether each of the following implications is true or false.

1. *If* 0.5 *is an integer, then* $1 + 0.5 = 3$. *True.*
2. *If* $5 > 2$, *then cats can fly. False.*
3. *If* $3 \times 5 = 15$, *then* $1 + 2 = 3$. *True.*
4. *For any real* $x \in \mathbb{R}$, *if* $x \leq 0$, *then* $(x - 1) < 0$. *True.*

Solution 1.3.
Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ *be a function. Negate the following propositions:*

1. $\exists x \in \mathbb{R}$ *such that* $f(x) = 0$.
   Negation: $\forall x \in \mathbb{R},\ f(x) \neq 0$.
2. $\exists M > 0,\ \forall A > 0,\ \exists x \geq A\ :\ f(x) \leq M$.
   Negation: $\forall M > 0,\ \exists A > 0,\ \forall x \geq A : f(x) > M$.
3. $\exists x \in \mathbb{R},\ f(x) > 0$.
   Negation: $\forall x \in \mathbb{R},\ f(x) \leq 0$.

4. $\forall \epsilon > 0,\ \exists \eta > 0,\ \forall (x, y) \in I^2,\ (|x - y| \leq \eta \Rightarrow |f(x) - f(y)| > \epsilon)$.
   Negation: $\exists \epsilon > 0,\ \forall \eta > 0,\ \exists (x, y) \in I^2,\ |x - y| \leq \eta \wedge |f(x) - f(y)| \leq \epsilon$.

Solution 1.4.

Consider the statement "for all integers a and b, if $a + b$ is even, then a and b are even."

1. ***Contrapositive:*** *"For all integers a and b, if a or b is odd, then $a + b$ is odd."*
2. ***Converse:*** *"For all integers a and b, if a and b are even, then $a+b$ is even."*
3. ***Negation:*** *"There exist integers a and b such that $a + b$ is even and a is odd or b is odd."*
4. ***Original Statement:*** *False (Counterexample: $a = 1, b = 1$, $a + b = 2$, but both are odd.)*
5. ***Contrapositive:*** *False (The contrapositive is logically equivalent to the original statement.)*
6. ***Converse:*** *True (The sum of two even numbers is always even.)*
7. ***Negation:*** *True*

Solution 1.5.

Prove that if n is an even integer, then n^2 is also an even integer.

Suppose n is an even integer. By definition, this means $n = 2k$ for some integer k. Now, consider n^2:

$$n^2 = (2k)^2 = 4k^2$$

Since k is an integer, $4k^2$ is clearly divisible by 2 (specifically, $4k^2 = 2(2k^2)$). Therefore, n^2 is even. □

Solution 1.6.

Suppose, for the sake of contradiction, that $\sqrt{2}$ is rational. This means we can express $\sqrt{2}$ as $\frac{p}{q}$, where p and q are integers with no common factors (i.e., $\frac{p}{q}$ is in its simplest form).

Then,

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

Squaring both sides gives:

$$2 = \left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2}$$

Multiplying through by q^2 *gives:*

$$2q^2 = p^2$$

This implies that p^2 *is even (since* $2q^2$ *is even). From this, we conclude that* p *itself must be even (because the square of an odd number is odd, and the square of an even number is even).*

Let $p = 2k$ *for some integer* k*. Substituting in* $p^2 = (2k)^2 = 4k^2$*, we get:*

$$2q^2 = 4k^2 \implies q^2 = 2k^2$$

This shows that q^2 *is even, hence* q *must also be even (similar reasoning as for* p*). Now, both* p *and* q *are even. However, this contradicts our initial assumption that* $\frac{p}{q}$ *is in its simplest form (no common factors). If both* p *and* q *are even, then* $\frac{p}{q}$ *can be further reduced by dividing both numerator and denominator by 2, which contradicts the assumption that* $\frac{p}{q}$ *is already in its simplest form.*

Therefore, our initial assumption that $\sqrt{2}$ *is rational must be false. Hence,* $\sqrt{2}$ *is irrational.* □

Solution 1.7.

(1) Prove that if n^2 ***is an even integer, then*** n ***is also an even integer.***

We will prove this statement by contrapositive.

Contrapositive: *The contrapositive of "If* n^2 *is even, then* n *is even" is: "If* n *is odd, then* n^2 *is odd."*

Proof: *Let* n *be an odd integer. By the definition of odd integers,* $n = 2k + 1$ *for some integer* k*.*

Now, calculate n^2*:*

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

Since $2k^2 + 2k$ *is an integer, the expression* $2(2k^2 + 2k) + 1$ *is odd.*

Thus, if n *is odd, then* n^2 *is odd. This proves the contrapositive, and hence, if* n^2 *is even, then* n *is even.*

(2) Prove that if** a **and** b **are integers and** ab **is odd, then both** a **and** b **are odd.

We will prove this statement by contrapositive.

***Contrapositive:** The contrapositive of "If ab is odd, then both a and b are odd" is: "If either a or b is even, then ab is even."*

***Proof:** Assume that either a or b is even. Without loss of generality, assume a is even. Then, $a = 2k$ for some integer k.*

Therefore, the product ab becomes:

$$ab = (2k) \times b = 2(kb).$$

Since $2(kb)$ is divisible by 2, ab is even.

Thus, if either a or b is even, then ab is even. This proves the contrapositive, and hence, if ab is odd, then both a and b must be odd.

Solution 1.8.

1. *Prove that for all positive integers n, $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.*

   ***Proof:** We will prove the statement by mathematical induction.*

   ***Base Case:** For $n = 1$,*

   $$1 = 1^2$$

   which is true.

   ***Inductive Step:** Assume the statement holds for some arbitrary positive integer k, i.e.,*

   $$1 + 3 + 5 + \cdots + (2k - 1) = k^2.$$

   We need to prove it holds for $k + 1$:

   $$1 + 3 + 5 + \cdots + (2k - 1) + (2(k + 1) - 1) = (k + 1)^2.$$

   Adding $2(k + 1) - 1 = 2k + 1$ to both sides gives:

   $$k^2 + 2k + 1 = (k + 1)^2.$$

   Hence, the statement holds for $k + 1$.

Therefore, by mathematical induction, for all positive integers n, $1+3+5+\cdots+(2n-1)=n^2$. □

2. *Prove that for all positive integers n, $2^n > n$.*

   Proof: *We will prove the statement by mathematical induction.*

   Base Case: *For $n=1$,*

   $$2^1 = 2 > 1,$$

   which is true.

   Inductive Step: *Assume the statement holds for some arbitrary positive integer k, i.e.,*

   $$2^k > k.$$

   We need to prove it holds for $k+1$:

   $$2^{k+1} = 2 \cdot 2^k > 2 \cdot k = k + k \geq k + 1.$$

   Therefore, $2^{k+1} > k+1$.

   Hence, by mathematical induction, for all positive integers n, $2^n > n$. □

Solution 1.9.

We are tasked with proving that for all $x \in \mathbb{R}$, the inequality

$$|x-1| \leq x^2 - x + 1$$

holds. We'll use a ***proof by disjunction of cases****.*

Case 1: $x - 1 \geq 0$ ***(i.e.,*** $x \geq 1$

If $x - 1 \geq 0$, the absolute value becomes:

$$|x-1| = x - 1.$$

Substituting $|x-1| = x-1$ into the inequality:

$$x - 1 \leq x^2 - x + 1.$$

Rearranging terms:

$$x^2 - 2x + 2 \geq 0.$$

Factoring $x^2 - 2x + 2$ *(or completing the square):*

$$x^2 - 2x + 2 = (x - 1)^2 + 1.$$

Since $(x - 1)^2 \geq 0$ *and* $1 > 0$*, it follows that:*

$$x^2 - 2x + 2 \geq 0.$$

Thus, the inequality holds in this case.

Case 2: $x - 1 < 0$ ***(i.e.,*** $x < 1$

If $x - 1 < 0$*, the absolute value becomes:*

$$|x - 1| = -(x - 1) = 1 - x.$$

Substituting $|x - 1| = 1 - x$ *into the inequality:*

$$1 - x \leq x^2 - x + 1.$$

Rearranging terms:

$$x^2 \geq 0.$$

This inequality is always true because $x^2 \geq 0$ *for all* $x \in \mathbb{R}$*.*

Conclusion:

In both cases, the inequality $|x - 1| \leq x^2 - x + 1$ *holds for all* $x \in \mathbb{R}$*.*

Solution 1.10.

Prove that the following statement is false: "Every positive integer is the sum of three squares."

Proof: *We will provide a counterexample to show that not every positive integer can be expressed as the sum of three squares.*

Consider the integer $n = 7$*.*

Now, we will check if 7 *can be expressed as* $a^2 + b^2 + c^2$ *where* a, b, c *are integers.*

Testing possible combinations:

$$1^2 + 1^2 + 1^2 = 1 + 1 + 1 = 3,$$
$$1^2 + 1^2 + 2^2 = 1 + 1 + 4 = 6,$$
$$1^2 + 2^2 + 2^2 = 1 + 4 + 4 = 9.$$

None of these combinations yield 7.

Therefore, 7 *cannot be expressed as the sum of three squares.*

Since we have found at least one positive integer (specifically 7*) that cannot be written as the sum of three squares, the statement "Every positive integer is the sum of three squares" is false.* □

Chapter 2

Sets, relations and functions

2.1 Sets

2.1.1 Definitions

Definition 2.1.1.
A set is a collection of objects known as elements. An element can be almost anything, such as numbers, functions, or lines. A set is a single object that can contain many elements. Since the elements are those that distinguish one set from another, one method that is used to write a set is to list its elements and surround them with braces. This is called the ***roster method*** *of writing a set, and the list is known as a roster. The braces signify that a set has been defined. For example, the set of all integers between 1 and 10 inclusive is*

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

Read this as "the set containing 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10." The set of all integers between 1 and 10 exclusive is

$$\{2, 3, 4, 5, 6, 7, 8, 9\}$$

If A is a set and a is an element of A, write $a \in A$. The notation $a, b \in A$ means $a \in A$ and $b \in A$. If c is not an element of A, write $c \notin A$.

Here's another way to define sets : a collection of elements that satisfy a property. We then write : $E = \{x, P(x)\}$, $(E = \{-1 \leq x \leq 1\} = [-1, 1])$

Definition 2.1.2.

1. *We denote $\emptyset$ as the empty set, which contains no elements.*
2. *A set with one element is called a singleton.*
3. *A set with two (distinct) elements is called a pair.*
4. *The cardinality of a set E, denoted $card(E) = |E|$, is the number (finite or infinite) of elements in E.*

Let A and B be sets. These sets are equal if they contain exactly the same elements. This is denoted by $A = B$. This means that if an element is in A, it must also be in B, and conversely, if an element is in B, it must also be in A. Formally,

$$A = B \text{ if and only if } (\forall x,\ x \in A \iff x \in B)$$

Definition 2.1.3. *(Inclusion)*
If A and B are sets, we say that A is included in B (or A is a subset of B) if every element of A is also an element of B. This is denoted as:

$$A \subseteq B$$

If A is a subset of B and A is not equal to B (i.e., A contains fewer elements than B), then A is a proper subset of B, denoted as:

$$A \subsetneq B$$

In other words:

- *$A \subseteq B$ means all elements of A are in B.*
- *$A \subsetneq B$ means all elements of A are in B and A is not equal to B.*

Remark 2.1.1.
We always have

1. *$E \subseteq E$ (reflexivity).*
2. *If $F \subseteq E$ and $G \subseteq F$, then $G \subseteq E$ (transitivity).*

3. $(E = F) \Leftrightarrow [(E \subseteq F) \text{ and } (F \subseteq E)]$ *(antisymmetry)*

Definition 2.1.4. *(Complement)*
The complement of a set F with respect to a universal set E is the set of all elements in E that are not in F. It is denoted by F^c or $\overline{F}$.

$$F^c = \{x \in E,\ x \notin E\}. \tag{2.1}$$

Proposition 2.1.1.
We always have

1. $(F^c)^c = F$.
2. $F \subseteq G \Leftrightarrow G^c \subseteq F^c$

Proof 2.1.1.

1. *Obvious.*
2. *Suppose $F \subseteq G$. Let $x \in G^c$. Then $x \notin G$, which implies $x \notin F$ (because $F \subseteq G$), and thus $x \in F^c$. Therefore, $G^c \subseteq F^c$.*

2.1.2 Operations on sets

Definition 2.1.5. *(Intersection)*
The intersection of two sets E and F is the set $E \cap F$ of elements x that are in both E and F. We say that two sets E and F are disjoint if $E \cap F = \emptyset$.

$$E \cap F = \{x \mid x \in E \text{ and } x \in F\}. \tag{2.2}$$

Proposition 2.1.2.
We always have:

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 2.1.6. *(Union)*
The union of two sets E and F is the set $E \cup F$ of elements x that are in E, in F, or in both.

$$E \cup F = \{x \mid x \in E \text{ or } x \in F\}. \tag{2.3}$$

Example 2.1.1.
Consider the following sets:

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

$$F = \{4, 5, 6, 7, 8\}$$

Intersection $E \cap F$***:***

$$E \cap F = \{4, 5\}$$

Union $E \cup F$***:***

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

Proposition 2.1.3.
We always have:

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

Proof 2.1.2.

1. *To prove the relation $(F \cap G)^c = F^c \cup G^c$, we will demonstrate the subset inclusions in both directions.*

   1. Show that $(F \cap G)^c \subseteq F^c \cup G^c$***:***

   Let $x \in (F \cap G)^c$. By definition of the complement, this means $x \notin F \cap G$.

   - *Since $x \notin F \cap G$, it must be that x is not in F or x is not in G. In set notation, this is:*

     $$x \notin F \text{ or } x \notin G$$

   - *This implies that $x \in F^c$ or $x \in G^c$. Therefore, $x \in F^c \cup G^c$.*

   Thus:

   $$x \in (F \cap G)^c \implies x \in F^c \cup G^c$$

So:

$$(F \cap G)^c \subseteq F^c \cup G^c$$

2. Show that $F^c \cup G^c \subseteq (F \cap G)^c$***:***

Let $x \in F^c \cup G^c$*. This means* $x \in F^c$ *or* $x \in G^c$*.*

- *If* $x \in F^c$*, then* $x \notin F$*.*
- *If* $x \in G^c$*, then* $x \notin G$*.*
- *In either case,* x *is not in both* F *and* G*. Hence,* $x \notin F \cap G$*, which means:*

$$x \in (F \cap G)^c$$

Thus:

$$x \in F^c \cup G^c \implies x \in (F \cap G)^c$$

So:

$$F^c \cup G^c \subseteq (F \cap G)^c$$

Conclusion:

Since we have shown both inclusions:

$$(F \cap G)^c \subseteq F^c \cup G^c \quad \textit{and} \quad F^c \cup G^c \subseteq (F \cap G)^c$$

We conclude:

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

2. *Similar to (1).*

Definition 2.1.7. *(Difference)*
If E *and* F *are two sets, the difference* $E \backslash F$ *between* E *and* F *is the set of elements in* E *that are not in* F*. The symmetric difference* $E \triangle F$ *of* E *and* F *is given by:*

$$E \triangle F = (E \backslash F) \cup (F \backslash E). \tag{2.4}$$

Example 2.1.2.
Consider the following sets:

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

$$F = \{4, 5, 6, 7, 8\}$$

We want to find: $E\backslash F$, $F\backslash E$ *and* $E\triangle F = (E\backslash F) \cup (F\backslash E)$.

Calculations:

$$E\backslash F = \{1, 2, 3\}$$

$$F\backslash E = \{6, 7, 8\}$$

$$E\triangle F = (E\backslash F) \cup (F\backslash E) = \{1, 2, 3, 6, 7, 8\}$$

Definition 2.1.8. *(Partition of a Set)*
A partition $\mathcal{A} = \{A_1, A_2, A_3, \ldots, A_n\}$ *of a set* E *is a collection of subsets of* E *such that:*

1. $\forall i, A_i \neq \emptyset$,
2. $\forall i, j$ *such that* $i \neq j$, $A_i \cap A_j = \emptyset$,
3. $\bigcup_{i=1}^{n} A_i = E$

Example 2.1.3.
Consider the set:

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

We want to find a partition of this set. One possible partition is:

$$\mathcal{A} = \{\{1, 2\}, \{3, 4\}, \{5, 6\}\}$$

Verification:

To confirm that $\mathcal{A}$ *is indeed a partition of* E*, we check the following:*

1. ***Non-empty subsets:*** *Each subset in the partition is non-empty.*
   - $\{1, 2\}$ *is non-empty.*
   - $\{3, 4\}$ *is non-empty.*
   - $\{5, 6\}$ *is non-empty.*
2. ***Disjoint subsets:*** *No two subsets overlap.*
   - $\{1, 2\} \cap \{3, 4\} = \emptyset$
   - $\{1, 2\} \cap \{5, 6\} = \emptyset$
   - $\{3, 4\} \cap \{5, 6\} = \emptyset$

3. ***Union of subsets equals the original set:*** *The union of all subsets in the partition must equal the original set E.*

$$\bigcup \mathcal{A} = \{1,2\} \cup \{3,4\} \cup \{5,6\} = \{1,2,3,4,5,6\} = E$$

Thus, $\mathcal{A} = \{\{1,2\},\{3,4\},\{5,6\}\}$ is a valid partition of E.

Definition 2.1.9. *(Cartesian Product)*
The Cartesian product of two sets E and F is the set

$$E \times F = \{(x,y) \mid x \in E \text{ and } y \in F\}. \tag{2.5}$$

The diagonal of a set E is

$$\triangle = \{(x,x) \mid x \in E\} \subset E \times E. \tag{2.6}$$

Example 2.1.4. *Consider the following sets:*

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

$$F = \{a,b\}$$

The Cartesian product $E \times F$ is given by:

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

To find $E \times F$, we create all possible ordered pairs where the first element comes from E and the second element comes from F: Therefore:

$$E \times F = \{(1,a),(1,b),(2,a),(2,b)\}$$

2.2 Relations

2.2.1 Definitions

Definition 2.2.1. *(Relation)*
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 some way.

1. *We say that A is the domain and B is the codomain of the relation $\mathcal{R}$.*

2. *If x is related to y by the relation $\mathcal{R}$, we say that x is related to y by $\mathcal{R}$; or (x, y) satisfies the relation $\mathcal{R}$, 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.*

Example 2.2.1.

1. *Let E be the set of teachers at Mila University, and F be the set of students at Mila University. We define a relation $\mathcal{R}$ from E to F by stating that*

$$\forall (x, y) \in E \times F,\ x\mathcal{R}y \Leftrightarrow x \text{ is the teacher of } y. \tag{2.7}$$

2. *Other examples of human relations include: "is a brother of," "has the same age as."*

3. *Let $A = B = \mathbb{Z}$. We define a relation $\mathcal{R}$ on $\mathbb{Z}$ by stating that*

$$\forall (x, y) \in \mathbb{Z}^2,\ x\mathcal{R}y \Leftrightarrow 2 \mid (x - y). \tag{2.8}$$

   Thus, $1\mathcal{R}7$ since 2 divides $-6 = (1 - 7)$. Note that $18\not\mathcal{R}7$ since 2 does not divide $11 = (18 - 7)$.

4. *The correspondence $\mathcal{R}'$ that links digits to vowels used to write the digit in full text is a relation from the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ to the set $\{a, e, i, o, u, y\}$. For example, $0\mathcal{R}'e$, $0\mathcal{R}'o$, $0\not\mathcal{R}'a$, $9\not\mathcal{R}'y$, $6\mathcal{R}'i$, and $1\not\mathcal{R}'u$.*

Definition 2.2.2. *(Graph of a Relation)*
Let $\mathcal{R}$ be a relation from a set A to a set B. The graph of $\mathcal{R}$ (denoted $G_{\mathcal{R}}$) is the set defined by:

$$G_{\mathcal{R}} = \{(x, y) \in A \times B \mid x\mathcal{R}y\} \tag{2.9}$$

Example 2.2.2.

1. *Referring back to the relation $\mathcal{R}$ from the previous example, we have: $(1, 7) \in G_{\mathcal{R}}$ and $(18, 7) \notin G_{\mathcal{R}}$.*

2. For the relation $\mathcal{R}'$ given in the previous example, we have:

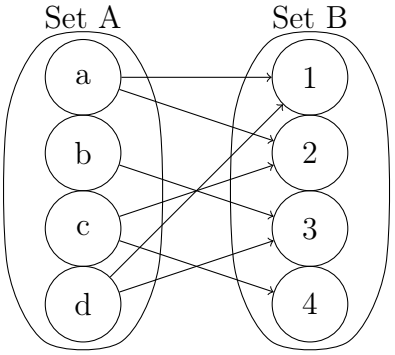
$$G_{\mathcal{R}'} = \{(0,e),(0,o),(1,o),(1,e),(2,o),(3,e),(4,o),(4,u),$$

$$(5,i),(5,e),(6,i),(7,e),(8,e),(8,i),(9,i)\}.$$

Remark 2.2.1.
Given two relations $\mathcal{R} = (A, B, R)$ and $\mathcal{R}' = (A', B', R')$, the statement "the relations $\mathcal{R}$ and $\mathcal{R}'$ are equal" means that $A = A'$, $B = B'$, and $R = R'$: same domain, same codomain, and same graph.

Definition 2.2.3. *(Inverse of relation)*
The inverse of a relation $\mathcal{R}$ from A to B, denoted $\mathcal{R}^{-1}$, is a relation from B to A where $y\mathcal{R}^{-1}x$ if and only if $x\mathcal{R}y$.

Definition 2.2.4. *(A sagittal diagram)*
A sagittal diagram is a graphical representation used to visualize the relationships between elements in different sets. In the context of relations, it can illustrate how elements from one set relate to elements in another set through a given relation.



Sagittal Diagram of a Relation

2.2.2 Properties of a Binary Relation on a Set

We now focus on relations where the domain is the same as the codomain.

Let A be a set and $\mathcal{R}$ is binary relation on A.

Definition 2.2.5. *(Reflexive Relation)*
A relation $\mathcal{R}$ on a set A is called reflexive if every element is related to itself. Formally:

$$\forall x \in A,\ x\mathcal{R}x \tag{2.10}$$

Definition 2.2.6. *(Symmetric Relation)*
A relation $\mathcal{R}$ on a set A is called symmetric if whenever x is related to y, then y is also related to x. Formally:

$$\forall x, y \in A,\ x\mathcal{R}y \implies y\mathcal{R}x \tag{2.11}$$

Definition 2.2.7. *(Antisymmetric Relation)*
A relation $\mathcal{R}$ on a set A is called antisymmetric if whenever x is related to y and y is related to x, then x must be equal to y. Formally:

$$\forall x, y \in A,\ (x\mathcal{R}y \text{ and } y\mathcal{R}x) \implies x = y \tag{2.12}$$

Definition 2.2.8. *(Transitive Relation)*
A relation $\mathcal{R}$ on a set A is called transitive if whenever x is related to y and y is related to z, then x is also related to z. Formally:

$$\forall x, y, z \in A,\ (x\mathcal{R}y \text{ and } y\mathcal{R}z) \implies x\mathcal{R}z \tag{2.13}$$

Example 2.2.3.

1. *The relation $=$ on the set of integers $\mathbb{Z}$ is reflexive, symmetric, antisymmetric, and transitive.*
2. *The relation $\leq$ on the set of integers $\mathbb{Z}$ is reflexive, antisymmetric, and transitive, but not symmetric.*
3. *The relation $<$ on the set of integers $\mathbb{Z}$ is transitive and antisymmetric, but not reflexive or symmetric.*

Example 2.2.4.

1. *Let $A = B = \mathbb{Z}$ and $R = \{(a, b) \in \mathbb{Z}^2 : 2 \mid (a - b)\}$. Then, $\mathcal{R}$ is reflexive, symmetric, transitive, but not antisymmetric.*
2. *Given the universe $\mathcal{U}$, the relation of inclusion, which relates two subsets of $\mathcal{U}$ (i.e., $X \subseteq Y$), is also reflexive, transitive, and antisymmetric, but not symmetric.*
3. *Let the relation $\mathcal{R}$ be defined on $\mathbb{Z}$ by: $x\mathcal{R}y \Leftrightarrow x$ divides y.*

(a) *Let $x \in \mathbb{Z}$. We have x divides x (even 0 divides 0). Thus, for all $x \in \mathbb{Z}$, $x\mathcal{R}x$, so $\mathcal{R}$ is reflexive.*

(b) *Let $x, y \in \mathbb{Z}$. We have $x\mathcal{R}y \Rightarrow$ (x divides y) $\nRightarrow$ (y divides x). For example, 1 divides 4 and 4 does not divide 1, so $\mathcal{R}$ is not symmetric.*

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

(d) *Let $x, y, z \in \mathbb{Z}$. We have $(x\mathcal{R}y) \wedge (y\mathcal{R}z) \Rightarrow$ ((x divides y) $\wedge$ (y divides z)) $\Rightarrow$ (x divides z) $\Rightarrow x\mathcal{R}z$. Hence, $\mathcal{R}$ is transitive.*

2.2.3 Equivalence Relations

Definition 2.2.9.
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 $\dot{a} = \{x \in A \mid x\mathcal{R}a\}$ is called the **equivalence class** of a modulo $\mathcal{R}$.*

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

Example 2.2.5.
Consider the set $A = \{1, 2, 3, 4, 5, 6\}$ and the relation $\mathcal{R}$ defined by $a\mathcal{R}b$ if and only if $2/(a - b)$.

To verify that $\mathcal{R}$ is an equivalence relation:

- ***Reflexivity:*** *For any $a \in A$, $2/(a - a)$.*
- ***Symmetry:*** *If $a\mathcal{R}b$, then $2/(a - b)$, hence $2/(b - a)$.*
- ***Transitivity:*** *If $a\mathcal{R}b$ and $b\mathcal{R}c$, then $2/(a-b)$ and $2/(b-c)$, hence $2/(a-c)$.*

Therefore, $\mathcal{R}$ is indeed an equivalence relation on A.

Equivalence Classes:

- $\dot{1} = \{1, 3, 5\}$
- $\dot{2} = \{2, 4, 6\}$

Quotient Set:

$$A/\mathcal{R} = \{\dot{1}, \dot{2}\} = \{\{1, 3, 5\}, \{2, 4, 6\}\}$$

This example illustrates how the set A is partitioned into equivalence classes under the relation $\mathcal{R}$.

2.2.4 Order Relation

Definition 2.2.10.
Let $\mathcal{R}$ be a relation on a set A.

1. *$\mathcal{R}$ is called an **order relation** if $\mathcal{R}$ is reflexive, antisymmetric and transitive.*
2. *(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 2.2.2.
Two elements x and y are said to be comparable by $\leq_{\mathcal{R}}$, if $x \leq_{\mathcal{R}} y$ or $y \leq_{\mathcal{R}} x$.

Example 2.2.6.
Consider the set $A = \{1, 2, 3, 4, 5\}$ and define the relation $\leq$ on A such that for any $x, y \in A$, $x \leq y$ if and only if x divides y (i.e., y is divisible by x).

To verify that $\leq$ is a partial order relation:

- ***Reflexivity:** For any $x \in A$, $x \leq x$ because any number divides itself.*

- ***Antisymmetry:*** *If $x \leq y$ and $y \leq x$, then both x divides y and y divides x. This implies $x = y$, hence $\leq$ is antisymmetric.*
- ***Transitivity:*** *If $x \leq y$ and $y \leq z$, then x divides y and y divides z, so x divides z. Thus, $x \leq z$, and $\leq$ is transitive.*

Therefore, $\leq$ is indeed a partial order relation on the set A.

Comparability:

- *Elements* 2 *and* 4 *are comparable because* $2 \leq 4$ *(since* 2 *divides* 4*).*
- *Elements* 3 *and* 5 *are not comparable because neither* 3 *divides* 5 *nor* 5 *divides* 3*.*

Definition 2.2.11. *(Special Elements)*
Let $\mathcal{R}$ be an order relation on a set E, and let A be a subset of E.

1. *An element $m \in E$ is called a minimum of A if*
   (a) *$m \in A$,*
   (b) *for all $x \in A$, we have $m \leq_{\mathcal{R}} x$. (We also say that m is the smallest element of A.)*
2. *An element $M \in E$ is called a maximum of A if*
   (a) *$M \in A$,*
   (b) *for all $x \in A$, we have $x \leq_{\mathcal{R}} M$. (We also say that M is the largest element of A.)*
3. *An extremum is an element that is either a minimum or a maximum.*
4. *An element $u \in E$ is called a lower bound of A if for all $x \in A$, we have $u \leq_{\mathcal{R}} x$. (We also say that A is bounded below by u.)*
5. *An element $U \in E$ is called an upper bound of A if for all $x \in A$, we have $x \leq_{\mathcal{R}} U$. (We also say 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 bounded above.*
7. *An element $v \in E$ is called a greatest lower bound of A (or infimum of A) if*

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

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

8. *An element $V \in E$ is called a least upper bound of A (or supremum of A) if*

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

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

Example 2.2.7.
Consider the set $E = \{1, 2, 3, 4, 5\}$ with the order relation $\leq$.

1. *For subset $A = \{2, 3, 4\}$:*

   - *2 is a minimum of A because $2 \in A$ and $2 \leq 2$, $2 \leq 3$, $2 \leq 4$.*
   - *4 is a maximum of A because $4 \in A$ and $3 \leq 4$, $2 \leq 4$.*

2. *For subset $A = \{2, 3\}$:*

   - *1 is a lower bound of A because $1 \leq 2$, $1 \leq 3$.*
   - *5 is an upper bound of A because $2 \leq 5$, $3 \leq 5$.*
   - *$\inf(A) = 2$ (greatest lower bound of A).*
   - *$\sup(A) = 3$ (least upper bound of A).*

2.3 Functions and mappings.

2.3.1 Functions.

Definition 2.3.1.

- *A relation f from E to F is called a function if every $x \in E$ has at most one image y in F. We also say that f is a function and write $y = f(x)$ instead of xfy. We also write*

$$f : E \to F$$

$$x \mapsto f(x).$$

- *The domain of definition of a function f (denoted D_f) is the set of elements x in E for which $f(x)$ exists.*

Definition 2.3.2.
Let $f : E \to F$ be a function, where A is a subset of E and B is a subset of F.

1. *The image of A under f is defined as*

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

2. *The preimage of B under f is defined as*

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

Definition 2.3.3.
The composition of the function $f : E \to F$ and the function $g : F \to G$ is the function

$$g \circ f : E \to G$$

$$x \mapsto g(f(x)).$$

Example 2.3.1.
Let $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ be defined as follows:

$$f(x) = 2x + 1$$

$$g(x) = x^2$$

To find the composition $g \circ f$, we compute:

$$(g \circ f)(x) = g(f(x)) = g(2x + 1) = (2x + 1)^2$$

Therefore, the composition $g \circ f$ is:

$$(g \circ f)(x) = (2x + 1)^2$$

Definition 2.3.4. *(Restriction of a Function)*
Let $f : E \to F$ be a function. The restriction of f to a subset $A \subseteq E$, denoted $f|_A$, is a new function defined as follows:

- *The domain of $f|_A$ is A, i.e., $\mathrm{dom}(f|_A) = A$.*

- *For each $x \in A$, $f|_A(x) = f(x)$.*

In other words, $f|_A$ is the function that maps each element $x \in A$ to the same value $f(x)$ that f maps x to in the original function f. ***Example:*** *Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. The restriction of f to the interval $[0, 1]$ is denoted $f|_{[0,1]}$ and is defined by:*

$$f|_{[0,1]}(x) = x^2 \quad \text{for } x \in [0, 1].$$

This restriction $f|_{[0,1]}$ is a function from $[0, 1]$ to $\mathbb{R}$, and it retains the same mapping as f but only for the subset $[0, 1]$ of its original domain.

Example 2.3.2. *(Function extension)*
Consider the function $f : \mathbb{R}^* \to \mathbb{R}$ defined by $f(x) = \dfrac{1}{x}$.
• ***Extension of the Domain***
Let's extend the domain of f to $\mathbb{R} \cup \{0\}$. Define $f|_{\mathbb{R}\cup\{0\}}(x)$ as follows:

$$f|_{\mathbb{R}^*\cup\{0\}}(x) = \begin{cases} \dfrac{1}{x} & \text{if } x \in \mathbb{R}, \\ 0 & \text{if } x = 0. \end{cases}$$

Here, we've extended f to include $x = 0$, which was not originally in the domain.

2.3.2 Mapping

Definition 2.3.5.
A function f is a mapping if every element of E maps to exactly one image in F. We denote $\mathcal{F}(E, F)$ the set of all mappings from E to F. A function f is a mapping if and only if its domain of definition is the entire set E.

Proposition 2.3.1.
Let $f : E \to F$ be a mapping.

1. ***For Sets in** E:*

    1. *If $A \subseteq B$, then $f(A) \subseteq f(B)$.*
    2. *We always have $f(A \cup B) = f(A) \cup f(B)$.*
    3. *We always have $f(A \cap B) \subseteq f(A) \cap f(B)$.*

2. ***For Sets in** F:*

1. *If $A \subseteq B$, then $f^{-1}(A) \subseteq f^{-1}(B)$.*
2. *We always have $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.*
3. *We always have $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.*

3. ***Additional Properties:***

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

2.3.3 Injection, surjection, bijection

Let E, F be two sets and $f : E \to F$ be a function.

Definition 2.3.6.

1. *f is injective (One-to-One) if every element of F has at most one preimage in E. In other words:*

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

2. *f is surjective (Onto) if every element of F has at least one preimage in E. In other words:*

$$\forall y \in F, \quad \exists x \in E \text{ such that } f(x) = y.$$

3. *f is bijective (One-to-One Correspondence) if it is both injective and surjective (every element of F has exactly one preimage in E.*

We can make the following remarks:

Remark 2.3.1.

1. *An application is injective if and only if its inverse relation is a function.*
2. *An application is surjective if and only if its image is its target set.*

3. An application is bijective if and only if its inverse relation is an application.

Example 2.3.3.
Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x$. ***Injective (One-to-One):***

To show that f is injective, we need to demonstrate that for any $x_1, x_2 \in \mathbb{R}$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$. Let $x_1, x_2 \in \mathbb{R}$. Suppose $f(x_1) = f(x_2)$. Then, $2x_1 = 2x_2$. Dividing both sides by 2 gives us $x_1 = x_2$. Therefore, f is injective.

Surjective (Onto):

To show that f is surjective, we need to show that for every $y \in \mathbb{R}$, there exists at least one $x \in \mathbb{R}$ such that $f(x) = y$.

Let $y \in \mathbb{R}$. We want to find $x \in \mathbb{R}$ such that $f(x) = y$. From the definition of f, we have $f(x) = 2x$. Setting $2x = y$, we get $x = \frac{y}{2}$. Since $\frac{y}{2} \in \mathbb{R}$ for all $y \in \mathbb{R}$, f is surjective.

Bijective (One-to-One Correspondence):

Since f is both injective and surjective, it is bijective. This means that every element in $\mathbb{R}$ has a unique preimage under f, and every element in $\mathbb{R}$ is mapped to by at least one element in $\mathbb{R}$.

Therefore, $f(x) = 2x$ is an example of a bijective function from $\mathbb{R}$ to $\mathbb{R}$.

Proposition 2.3.2.

1. *If $f : E \to F$ and $g : F \to G$ are two injective, surjective, or bijective functions, then $g \circ f : E \to G$ is also injective, surjective, or bijective respectively.*
2. *An application $f : E \to F$ is bijective if and only if there exists an application $g : F \to E$ such that $g \circ f = \mathrm{Id}_E$ and $f \circ g = \mathrm{Id}_F$. In this case, $g = f^{-1}$.*
3. *If $f : E \to F$ and $g : F \to G$ are two applications with $g \circ f : E \to G$ injective, then f is also injective. Similarly, if $g \circ f$ is surjective, then g is surjective as well.*

Proof 2.3.1.

1. (a) *Suppose f and g are injective functions. Let $x_1, x_2 \in E$ such that $g \circ f(x_1) = g \circ f(x_2)$. Then, $g(f(x_1)) = g(f(x_2)) \Rightarrow f(x_1) = f(x_2)$ (since g is injective) $\Rightarrow x_1 = x_2$. Hence, $g \circ f$ is injective.*

   (b) *Suppose f and g are surjective functions. Let $z \in G$. Then, there exists $y \in F$ such that $g(y) = z$ (since g is surjective). And since f is surjective, there exists $x \in E$ such that $f(x) = y$. Therefore, there exists $x \in E$ such that $g(f(x)) = z$, implying $g \circ f$ is surjective.*

   (c) *This is evident from parts (a) and (b).*

2. *See Tutorial Document.*

3. *See Tutorial Document.*

2.4 Exercices

Exercice 2.1.
Consider the following sets: $A = \{1, 2, 3, 4, 5\}$, $B = \{3, 4, 5, 6, 7\}$ *and*

$C = \{2, 4, 6, 8, 10\}$. *Find the following sets:* $(A \cup B)$, $(B \cap C)$, $(A - B)$ *and* $(A \Delta C)$.

Exercice 2.2.
Let $E = \{a,\ b,\ c\}$ *be a set. Can we write: 1)* $a \in E$, *2)* $a \subset E$, *3)* $\{a\} \subset E$, *4)* $\emptyset \in E$,*5)* $\emptyset \subset E$, *6)* $\{\emptyset\} \subset E$*?*

Exercice 2.3.
Let A, B, *and* C *be three subsets of a set* E. *Prove that:*

1. $A \setminus B = A \cap B^c$.
2. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
3. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
4. $A \triangle B = (A \cup B) \setminus (A \cap B)$.

Exercice 2.4. *(Power set)*
Let $E = \{a, b, c, d\}$. *Find the power set* $\mathcal{P}(E)$ *of* E, *which is the set of all subsets of* E. *Give an example of a partition of* E, *which is a collection of non-empty disjoint subsets of* E *whose union equals* E.

Exercice 2.5.

1. *What is the image of the sets* $\mathbb{R}$, $[0, 2\pi]$, $[0, \frac{\pi}{2}]$, *and the inverse image of the sets* $[0, 1]$, $[3, 4]$, $[1, 2]$ *under the function* $f(x) = \sin(x)$*?*
2. *Let* $f : \mathbb{R} \to \mathbb{R}$ *be defined by* $f(x) = x^2 + 1$. *Consider the sets* $A = [-3, 2]$ *and* $B = [0, 4]$. *Compare* $f(A \setminus B)$ *and* $f(A) \setminus f(B)$.
3. *What condition must function* f *satisfy so that* $f(A \setminus B) = f(A) \setminus f(B)$*?*

Exercice 2.6.
Determine whether the following relations are reflexive, symmetric, antisymmetric, and transitive:

1. $E = \mathbb{Z}$ *and* $x \mathcal{R} y \Leftrightarrow |x| = |y|$.

2. $E = \mathbb{R} \setminus \{0\}$ *and* $x\mathcal{R}y \Leftrightarrow xy > 0$.

3. $E = \mathbb{Z}$ *and* $x\mathcal{R}y \Leftrightarrow x - y$ *is even.*

Identify among the above examples which relations are orders and which are equivalence relations.

Exercice 2.7.
Determine whether the following relations are reflexive, symmetric, antisymmetric, and transitive:

1. $E = \mathbb{R}$ *and* $x\mathcal{R}y \Leftrightarrow x = -y$.

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

3. $E = \mathbb{N}$ *and* $x\mathcal{R}y \Leftrightarrow \exists p, q \geq 1$ *such that* $y = px^q$ *(where* p *and* q *are integers).*

Identify among the above examples which relations are orders and which are equivalence relations.

Exercice 2.8.
Let $E = \mathbb{Z}$*, the set of all integers. Consider the following relations on* E*:*

1. *Relation* $\sim_1$ *defined by* $x \sim_1 y$ *if and only if* $x + y$ *is even.*

2. *Relation* $\sim_2$ *defined by* $x \sim_2 y$ *if and only if* x *and* y *have the same remainder when divided by 5.*

3. *Relation* $\sim_3$ *defined by* $x \sim_3 y$ *if and only if* $x - y$ *is a multiple of 7.*

For each relation $\sim_i$ *(where* $i = 1, 2, 3$*):*

1. *Determine if* $\sim_i$ *is an equivalence relation on* $\mathbb{Z}$*. Explain why or why not.*

2. *If* $\sim_i$ *is an equivalence relation, identify the equivalence classes of* $\mathbb{Z}$ *under* $\sim_i$.

Exercice 2.9.
Let $\mathcal{R}$ *be an equivalence relation on a non-empty set* E*. Show that*

$$\forall x, y \in E, \quad x\mathcal{R}y \quad \Leftrightarrow \quad \dot{x} = \dot{y}.$$

Exercice 2.10.
Let $\mathbb{N}^*$ denote the set of positive integers. Define the relation $\mathcal{R}$ on $\mathbb{N}^*$ by $x\mathcal{R}y$ if and only if x divides y.

1. *Show that $\mathcal{R}$ is a partial order relation on $\mathbb{N}^*$.*
2. *Is $\mathcal{R}$ a total order relation?*
3. *Describe the sets $\{x \in \mathbb{N}^* \mid x\mathcal{R}5\}$ and $\{x \in \mathbb{N}^* \mid 5\mathcal{R}x\}$.*
4. *Does $\mathbb{N}^*$ have a least element? A greatest element?*

Exercice 2.11.
Let f be the function from $\mathbb{R}$ to $\mathbb{R}$ defined by $f(x) = x^2 + x - 2$.

1. *Give the definition of $f^{-1}(\{4\})$. Calculate $f^{-1}(\{4\})$.*
2. *Is the function f bijective?*
3. *Give the definition of $f([-1, 1])$. Calculate $f([-1, 1])$.*
4. *Give the definition of $f^{-1}([-2, 4])$. Calculate $f^{-1}([-2, 4])$.*

Exercice 2.12.
Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ be defined by $f(x) = \frac{2x}{1+x^2}$.

1. *Is f injective? Is f surjective?*
2. *Show that $f(\mathbb{R}) = [-1, 1]$.*
3. *Show that the restriction $g : [-1, 1] \longrightarrow [-1, 1]$ defined by $g(x) = f(x)$ is a bijection.*

Exercice 2.13.
Let $f : E \to F$, $g : F \to G$, and $h = g \circ f$.

1. *Show that if h is injective, then f is injective. Also, show that if h is surjective, then g is surjective.*
2. *Show that if h is surjective and g is injective, then f is surjective.*
3. *Show that if h is injective and f is surjective, then g is injective.*

2.5 Exercise Solutions

Solution 2.1.

- *Union of A and B:*
$$A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$$
- *Intersection of B and C:*
$$B \cap C = \{4, 6\}$$
- *Set difference $A - B$:*
$$A - B = \{1, 2\}$$
- *Symmetric difference of A and C:*
$$A \Delta C = \{1, 3, 5, 8, 10\}$$

Solution 2.2.

1. *$a \in E$: True. Since $E = \{a, b, c\}$, a is an element of E.*
2. *$a \subset E$: False. a is not a subset of E; $\{a\}$ is a subset of E.*
3. *$\{a\} \subset E$: True. $\{a\}$ is a subset of E because $a \in E$.*
4. *$\emptyset \in E$: False. $\emptyset$ (empty set) is not an element of E.*
5. *$\emptyset \subset E$: True. The empty set $\emptyset$ is a subset of every set, including E.*
6. *$\{\emptyset\} \subset E$: False. $\{\emptyset\}$ is not a subset of E because $\emptyset \notin E$.*

Solution 2.3.

1. *$A \setminus B = A \cap B^c$ By definition:*
$$A \setminus B = \{x \in A \mid x \notin B\},$$
and on the other hand:
$$A \cap B^c = \{x \in A \mid x \in B^c\} = \{x \in A \mid x \notin B\}.$$

Thus:

$$A \setminus B = A \cap B^c.$$

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

Using the distributive property of intersection over union:

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

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

Using the distributive property of union over intersection:

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

This can also be verified using element-based reasoning: If $x \in A \cup (B \cap C)$, then $x \in A$ or $x \in B \cap C$. If $x \in B \cap C$, then $x \in B$ and $x \in C$, so $x \in A \cup B$ and $x \in A \cup C$.
Conversely, if $x \in (A \cup B) \cap (A \cup C)$, then $x \in A \cup B$ and $x \in A \cup C$. This implies $x \in A$, or $x \in B$ and $x \in C$, so $x \in A \cup (B \cap C)$.

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

By the definition of symmetric difference:

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

Using part (1):

$$A \setminus B = A \cap B^c \quad \textit{and} \quad B \setminus A = B \cap A^c.$$

Thus:

$$A \triangle B = (A \cap B^c) \cup (B \cap A^c).$$

On the other hand:

$$(A \cup B) \setminus (A \cap B) = (A \cup B) \cap (A \cap B)^c.$$

Since $(A \cap B)^c = A^c \cup B^c$, *we have:*

$$(A \cup B) \setminus (A \cap B) = (A \cup B) \cap (A^c \cup B^c).$$

Using the distributive property:

$$(A \cup B) \cap (A^c \cup B^c) = [(A \cup B) \cap A^c] \cup [(A \cup B) \cap B^c].$$

Simplifying each term:

$$(A \cup B) \cap A^c = (A \cap A^c) \cup (B \cap A^c) = B \cap A^c,$$

$$(A \cup B) \cap B^c = (A \cap B^c) \cup (B \cap B^c) = A \cap B^c.$$

Thus:

$$(A \cup B) \setminus (A \cap B) = (A \cap B^c) \cup (B \cap A^c).$$

Therefore:

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

Solution 2.4.

The Power Set $\mathcal{P}(E)$

The power set $\mathcal{P}(E)$ *of a set* E *is the set of all subsets of* E, *including the empty set and* E *itself. For* $E = \{a, b, c, d\}$, *the power set* $\mathcal{P}(E)$ *is:*

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

In total, $\mathcal{P}(E)$ *contains* 2^n *subsets, where* $n = 4$ *is the number of elements in* E. *Thus,* $|\mathcal{P}(E)| = 2^4 = 16$.

Example of a Partition of E

A partition of E *is a collection of non-empty, pairwise disjoint subsets of* E *whose union equals* E. *An example of a partition of* E *is:*

$$\mathcal{P}_1 = \{\{a, b\}, \{c\}, \{d\}\}.$$

Verify:

- *Each subset is non-empty:* $\{a, b\}, \{c\}, \{d\} \neq \emptyset$,
- *The subsets are pairwise disjoint:*

$$\{a, b\} \cap \{c\} = \emptyset, \quad \{a, b\} \cap \{d\} = \emptyset, \quad \{c\} \cap \{d\} = \emptyset,$$

- *The union of all subsets equals* E*:*

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

Thus, $\mathcal{P}_1 = \{\{a, b\}, \{c\}, \{d\}\}$ *is a valid partition of* E*.*

Solution 2.5.

1. ***Images and Pre-images under*** $f(x) = \sin(x)$***:***
   (a) *The image of* $\mathbb{R}$ *under* $f(x) = \sin(x)$ *is:*

$$f(\mathbb{R}) = [-1, 1],$$

   because the sine function oscillates between -1 *and* 1 *for all real* x*.*
   (b) *The image of* $[0, 2\pi]$ *under* $f(x) = \sin(x)$ *is:*

$$f([0, 2\pi]) = [-1, 1],$$

   because $\sin(x)$ *completes one full cycle in the interval* $[0, 2\pi]$*.*
   (c) *The image of* $[0, \frac{\pi}{2}]$ *under* $f(x) = \sin(x)$ *is:*

$$f([0, \frac{\pi}{2}]) = [0, 1],$$

   because the sine function is strictly increasing from 0 *to* 1 *in this interval.*
   (d) *The inverse image of* $[0, 1]$ *under* $f(x) = \sin(x)$ *is:*

$$f^{-1}([0, 1]) = \bigcup_{k \in \mathbb{Z}} [2k\pi, 2k\pi + \pi],$$

   as sine is periodic with period 2π*.*

(e) *The inverse image of* $[3,4]$ *under* $f(x)=\sin(x)$ *is:*

$$f^{-1}([3,4])=\emptyset,$$

because $\sin(x)\notin[3,4]$ *for any* $x\in\mathbb{R}$.

(f) *The inverse image of* $[1,2]$ *under* $f(x)=\sin(x)$ *is:*

$$f^{-1}([1,2])=f^{-1}(\{1\})=\bigcup_{k\in\mathbb{Z}}\left\{\frac{\pi}{2}+2k\pi\right\},$$

because $\sin(x)=1$ *occurs only at* $x=\frac{\pi}{2}+2k\pi$ *for* $k\in\mathbb{Z}$, *and* $\sin(x)\notin(1,2]$.

2. ***Comparison of*** $f(A\setminus B)$ ***and*** $f(A)\setminus f(B)$***:***

Let $f(x)=x^2+1$, $A=[-3,2]$, *and* $B=[0,4]$*:*

(a) *The set* $A\setminus B=[-3,0)$, *as* $B=[0,4]$ *removes* $[0,4]$ *from* A.

(b) *The image of* $A\setminus B$ *under* $f(x)$*:*

$$f(A\setminus B)=f([-3,0))=(1,10],$$

because $f(x)=x^2+1$ *is increasing on* $[0,\infty)$ *and symmetric about* $x=0$.

(c) *The image of* A *under* $f(x)$*:*

$$f(A)=f([-3,2])=[1,10],$$

and the image of B *under* $f(x)$*:*

$$f(B)=f([0,4])=[1,17].$$

(d) *The set* $f(A)\setminus f(B)$ *is:*

$$f(A)\setminus f(B)=[1,10]\setminus[1,17]=\emptyset.$$

Comparing:

$$f(A\setminus B)=[1,10),\quad f(A)\setminus f(B)=\emptyset.$$

Thus, $f(A\setminus B)\neq f(A)\setminus f(B)$.

3. ***Condition for*** $f(A\setminus B)=f(A)\setminus f(B)$***:***

*For $f(A \setminus B) = f(A) \setminus f(B)$ to hold, the function f must be **injective** (one-to-one). Injectivity ensures that elements in $A \setminus B$ map uniquely to $f(A \setminus B)$, without overlap from elements in B.*

Solution 2.6.

1. *$E = \mathbb{Z}$ and $x\mathcal{R}y \Leftrightarrow |x| = |y|$:*
   - ***Reflexive**: Yes, since $|x| = |x|$ for all $x \in \mathbb{Z}$.*
   - ***Symmetric**: Yes, since $|x| = |y| \implies |y| = |x|$.*
   - ***Antisymmetric**: No, because $|x| = |y|$ does not imply $x = y$ (e.g., $x = 3, y = -3$).*
   - ***Transitive**: Yes, since $|x| = |y|$ and $|y| = |z|$ imply $|x| = |z|$.*
   - ***Type**: This is an **equivalence relation**, not an order.*
2. *$E = \mathbb{R} \setminus \{0\}$ and $x\mathcal{R}y \Leftrightarrow xy > 0$:*
   - ***Reflexive**: Yes, since $x \cdot x > 0$ for all $x \neq 0$.*
   - ***Symmetric**: Yes, since $xy > 0 \implies yx > 0$.*
   - ***Antisymmetric**: No, because $xy > 0$ does not imply $x = y$ (e.g., $x = 1, y = 2$).*
   - ***Transitive**: Yes, since $xy > 0$ and $yz > 0$ imply $xz > 0$.*
   - ***Type**: This is an **equivalence relation**, not an order.*
3. *$E = \mathbb{Z}$ and $x\mathcal{R}y \Leftrightarrow x - y$ is even:*
   - ***Reflexive**: Yes, since $x - x = 0$, which is even.*
   - ***Symmetric**: Yes, since $x - y$ even implies $y - x$ is even.*
   - ***Antisymmetric**: No, because $x - y$ even does not imply $x = y$ (e.g., $x = 2, y = 4$).*
   - ***Transitive**: Yes, since $x - y$ even and $y - z$ even imply $x - z$ is even.*
   - ***Type**: This is an **equivalence relation**, not an order.*

Summary

- $\mathcal{R}_1$, $\mathcal{R}_2$, *and* $\mathcal{R}_3$ *are all* ***equivalence relations****.*
- *None of them is an* ***order*** *because they fail antisymmetry.*

Solution 2.7.

1. $E = \mathbb{R}$ *and* $x\mathcal{R}y \Leftrightarrow x = -y$*:*
   - ***Reflexive****: No, since* $x = -x$ *only holds for* $x = 0$*, so it is not reflexive.*
   - ***Symmetric****: Yes, since* $x = -y \implies y = -x$*.*
   - ***Antisymmetric****: No, because* $x = -y$ *and* $y = -x$ *do not imply* $x = y$ *(e.g.,* $x = 1, y = -1$*).*
   - ***Transitive****: No, because* $x = -y$ *and* $y = -z$ *imply* $x = -(-z) = z$*, which contradicts the original definition unless* $x = 0$ *or* $z = 0$*.*
   - ***Type****: This is* ***not an equivalence relation*** *because it is not reflexive, and it is* ***not an order*** *because it is not antisymmetric.*
2. $E = \mathbb{R}$ *and* $x\mathcal{R}y \Leftrightarrow \cos^2(x) + \sin^2(y) = 1$*:*
   - ***Reflexive****: Yes, since* $\cos^2(x) + \sin^2(x) = 1$ *for all* $x \in \mathbb{R}$*.*
   - ***Symmetric****: Yes, since* $\cos^2(x) + \sin^2(y) = 1 \implies \cos^2(y) + \sin^2(x) = 1$*.*
   - ***Antisymmetric****: No, because* $\cos^2(x) + \sin^2(y) = 1$ *and* $\cos^2(y) + \sin^2(x) = 1$ *do not imply* $x = y$*.*
   - ***Transitive****: Yes, since* $\cos^2(x) + \sin^2(y) = 1$ *and* $\cos^2(y) + \sin^2(z) = 1$ *imply* $\cos^2(x) + \sin^2(z) = 1$*.*
   - ***Type****: This is* ***an equivalence relation*** *but* ***not an order****.*
3. $E = \mathbb{N}$ *and* $x\mathcal{R}y \Leftrightarrow \exists p, q \geq 1$ *such that* $y = px^q$ *(where* $p, q \in \mathbb{Z}$*):*
   - ***Reflexive****: Yes, since* $x = px^q$ *holds for* $p = 1, q = 1$*, implying* $x\mathcal{R}x$*.*
   - ***Symmetric****: No, since* $y = px^q$ *does not imply* $x = py^q$*.*
   - ***Antisymmetric****: Yes, because if* $y = px^q$ *and* $x = p'y^{q'}$*, then* $x = y$*.*
   - ***Transitive****: Yes, since if* $y = px^q$ *and* $z = p'y^{q'}$*, then* $z = (pp')x^{qq'}$*.*
   - ***Type****: This is a* ***partial order****, not an equivalence relation.*

Solution 2.8.

1. ***Relation*** $\sim_1$*:* $x \sim_1 y$ *if and only if* $x + y$ *is even.*

   Reflexive*: Yes, because* $x + x = 2x$ *is always even for any* $x \in \mathbb{Z}$*.*

   Symmetric*: Yes, because if* $x + y$ *is even, then* $y + x = x + y$*, which is also even.*

   Transitive*: Yes, because if* $x + y$ *is even and* $y + z$ *is even, then* $(x + y) + (y + z) = x + 2y + z$ *is even, implying that* $x + z$ *is even.*

   Equivalence Classes*: The equivalence classes are:*

   $$\dot{0} = \{x \in \mathbb{Z} \mid x \text{ is even}\}, \quad \dot{1} = \{x \in \mathbb{Z} \mid x \text{ is odd}\}.$$

2. ***Relation*** $\sim_2$*:* $x \sim_2 y$ *if and only if* x *and* y *have the same remainder when divided by 5.*

   Reflexive*: Yes, because* $x \mod 5 = x \mod 5$ *for any* $x \in \mathbb{Z}$*.*

   Symmetric*: Yes, because if* $x \mod 5 = y \mod 5$*, then* $y \mod 5 = x \mod 5$*.*

   Transitive*: Yes, because if* $x \mod 5 = y \mod 5$ *and* $y \mod 5 = z \mod 5$*, then* $x \mod 5 = z \mod 5$*.*

   Equivalence Classes*: The equivalence classes are:*

   $$\dot{0} = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 5\}, \quad \dot{1} = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 5\}, \quad \dot{2} = \{x \in \mathbb{Z} \mid x \equiv 2 \quad (\text{m}$$

   $$\dot{3} = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod 5\}, \quad \dot{4} = \{x \in \mathbb{Z} \mid x \equiv 4 \pmod 5\}.$$

3. ***Relation*** $\sim_3$*:* $x \sim_3 y$ *if and only if* $x - y$ *is a multiple of 7.*

   Reflexive*: Yes, because* $x - x = 0$ *is a multiple of 7 for any* $x \in \mathbb{Z}$*.*

   Symmetric*: Yes, because if* $x - y$ *is a multiple of 7, then* $y - x = -(x - y)$ *is also a multiple of 7.*

   Transitive*: Yes, because if* $x - y$ *and* $y - z$ *are multiples of 7, then* $(x - y) + (y - z) = x - z$ *is also a multiple of 7.*

   Equivalence Classes*: The equivalence classes are:*

   $$\dot{0} = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 7\}, \quad \dot{1} = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 7\}, \quad \dot{2} = \{x \in \mathbb{Z} \mid x \equiv 2 \quad (\text{m}$$

$$\dot{3} = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod 7\}, \quad \dot{4} = \{x \in \mathbb{Z} \mid x \equiv 4 \pmod 7\}, \quad \dot{5} = \{x \in \mathbb{Z} \mid x \equiv 5 \pmod 7\}$$

$$\dot{6} = \{x \in \mathbb{Z} \mid x \equiv 6 \pmod 7\}.$$

Solution 2.9.

We will prove the equivalence in two directions.

(1) If** $x\mathcal{R}y$**, then** $\dot{x} = \dot{y}$**:

Since $\mathcal{R}$ is an equivalence relation, it satisfies three properties: reflexivity, symmetry, and transitivity. By the definition of an equivalence relation, if $x\mathcal{R}y$, then x and y belong to the same equivalence class, denoted $\dot{x} = \dot{y}$. This means that the equivalence classes of x and y are identical.

$$x\mathcal{R}y \quad \Rightarrow \quad \dot{x} = \dot{y}.$$

(2) If** $\dot{x} = \dot{y}$**, then** $x\mathcal{R}y$**:

If $\dot{x} = \dot{y}$, then by the definition of equivalence classes, x and y belong to the same equivalence class. Therefore, by the properties of an equivalence relation, $x\mathcal{R}y$.

$$\dot{x} = \dot{y} \quad \Rightarrow \quad x\mathcal{R}y.$$

Thus, we have shown both directions, completing the proof.

Solution 2.10.

Let $\mathbb{N}^*$ denote the set of positive integers. Define the relation $\mathcal{R}$ on $\mathbb{N}^*$ by $x\mathcal{R}y$ if and only if x divides y.

1. ***Show that** $\mathcal{R}$ **is a partial order relation on** $\mathbb{N}^*$**:***

   To show that $\mathcal{R}$ is a partial order, we need to verify that it is reflexive, antisymmetric, and transitive.

   - ***Reflexive:** For any $x \in \mathbb{N}^*$, x divides itself, i.e., $x\mathcal{R}x$.*
   - ***Antisymmetric:** If $x\mathcal{R}y$ and $y\mathcal{R}x$, then x divides y and y divides x. This implies that $x = y$, because the only way two distinct positive integers can divide each other is if they are equal.*
   - ***Transitive:** If $x\mathcal{R}y$ and $y\mathcal{R}z$, then x divides y and y divides z. This implies that x divides z, so $x\mathcal{R}z$.*

Since $\mathcal{R}$ is reflexive, antisymmetric, and transitive, it is a partial order on $\mathbb{N}^*$.

2. ***Is $\mathcal{R}$ a total order relation?***

   A relation is a total order if it is a partial order and, for any two elements x and y in $\mathbb{N}^*$, either $x\mathcal{R}y$ or $y\mathcal{R}x$ holds. In this case, $\mathcal{R}$ is not a total order because, for example, 2 and 3 do not divide each other, so neither $2\mathcal{R}3$ nor $3\mathcal{R}2$ holds. Therefore, $\mathcal{R}$ is not a total order.

3. ***Describe the sets $\{x \in \mathbb{N}^* \mid x\mathcal{R}5\}$ and $\{x \in \mathbb{N}^* \mid 5\mathcal{R}x\}$:***

   - *The set $\{x \in \mathbb{N}^* \mid x\mathcal{R}5\}$ is the set of all positive integers that divide 5. The divisors of 5 are 1 and 5, so:*

   $$\{x \in \mathbb{N}^* \mid x\mathcal{R}5\} = \{1, 5\}.$$

   - *The set $\{x \in \mathbb{N}^* \mid 5\mathcal{R}x\}$ is the set of all positive integers divisible by 5. This set is:*

   $$\{x \in \mathbb{N}^* \mid 5\mathcal{R}x\} = \{5, 10, 15, 20, 25, \dots\}.$$

4. ***Does $\mathbb{N}^*$ have a least element? A greatest element?***

   - ***Least element:*** *The least element in $\mathbb{N}^*$ with respect to the relation $\mathcal{R}$ is 1, because 1 divides all positive integers. Therefore, 1 is the least element.*
   - ***Greatest element:*** *The greatest element in $\mathbb{N}^*$ with respect to the relation $\mathcal{R}$ does not exist because there is no single integer that is divisible by all positive integers. Thus, there is no greatest element.*

Solution 2.11.
Let f be the function from $\mathbb{R}$ to $\mathbb{R}$ defined by $f(x) = x^2 + x - 2$.

1. ***Definition of $f^{-1}(\{4\})$:*** *The set $f^{-1}(\{4\})$ is the preimage of $\{4\}$ under f, i.e., it consists of all $x \in \mathbb{R}$ such that $f(x) = 4$.*

   $$f(x) = 4 \quad \Rightarrow \quad x^2 + x - 2 = 4$$

   Solving this equation:

   $$x^2 + x - 6 = 0$$

Factorizing:

$$(x-2)(x+3)=0$$

Thus, $x=2$ *or* $x=-3$*. Therefore,* $f^{-1}(\{4\})=\{2,-3\}$*.*

2. ***Is the function*** f ***bijective?***

   Injectivity: f *is not bijective because* f *is not injective.*

   Surjectivity: For surjectivity, we would need to show that for every $y\in\mathbb{R}$*, there exists* $x\in\mathbb{R}$ *such that* $f(x)=y$*. However, since the function is quadratic and opens upwards, it is not surjective over* $\mathbb{R}$*. Specifically,* $f(x)=x^2+x-2$ *has a minimum value, but no maximum, meaning it cannot take all real values. Therefore,* f *is not surjective.*

   Since f *is neither injective nor surjective, it is not bijective.*

3. ***Definition of*** $f([-1,1])$***:*** *The set* $f([-1,1])$ *is the image of the interval* $[-1,1]$ *under the function* f*, i.e., it is the set of all values* $f(x)$ *for* $x\in[-1,1]$*.*

   To calculate $f([-1,1])$*, we need to find the minimum and maximum values of* $f(x)=x^2+x-2$ *on the interval* $[-1,1]$*.*

   First, evaluate $f(x)$ *at the endpoints of the interval:*

$$f(-1)=(-1)^2+(-1)-2=1-1-2=-2$$

$$f(1)=1^2+1-2=1+1-2=0$$

   Next, compute the derivative of $f(x)$*:*

$$f'(x)=2x+1$$

   Setting $f'(x)=0$ *to find critical points:*

$$2x+1=0 \quad \Rightarrow \quad x=-\frac{1}{2}$$

   Since $-\frac{1}{2}\in[-1,1]$*, we evaluate* f *at* $x=-\frac{1}{2}$*:*

$$f\left(-\frac{1}{2}\right)=\left(-\frac{1}{2}\right)^2+\left(-\frac{1}{2}\right)-2=\frac{1}{4}-\frac{1}{2}-2=-\frac{9}{4}$$

   Thus, the minimum value of $f(x)$ *on* $[-1,1]$ *is* $-\frac{9}{4}$*, and the maximum value is 0.*

Therefore, $f([-1,1]) = \left[-\frac{9}{4}, 0\right]$.

4. ***Definition of*** $f^{-1}([-2,4])$***:*** *The set* $f^{-1}([-2,4])$ *is the preimage of the interval* $[-2,4]$*, i.e., it consists of all* $x \in \mathbb{R}$ *such that* $f(x) \in [-2,4]$.

   We need to solve for x *such that* $-2 \leq f(x) = x^2 + x - 2 \leq 4$.

   First, solve $f(x) \geq -2$*:*

$$x^2 + x - 2 \geq -2 \quad \Rightarrow \quad x^2 + x \geq 0$$

   Factoring:

$$x(x+1) \geq 0$$

   This inequality holds when $x \leq -1$ *or* $x \geq 0$.

   Next, solve $f(x) \leq 4$*:*

$$x^2 + x - 2 \leq 4 \quad \Rightarrow \quad x^2 + x - 6 \leq 0$$

   Factoring:

$$(x-2)(x+3) \leq 0$$

   This inequality holds when $-3 \leq x \leq 2$.

   Combining the two results, we have:

$$-3 \leq x \leq -1 \quad \textit{or} \quad 0 \leq x \leq 2$$

   Therefore, the set $f^{-1}([-2,4]) = [-3,-1] \cup [0,2]$.

Solution 2.12.

1. ***Injectivity:***

   A function f *is injective if* $f(x_1) = f(x_2)$ *implies* $x_1 = x_2$*. Let's assume* $f(x_1) = f(x_2)$*, which gives:*

$$\frac{2x_1}{1+x_1^2} = \frac{2x_2}{1+x_2^2}.$$

   Simplifying this equation:

$$x_1(1+x_2^2) = x_2(1+x_1^2),$$

which does not necessarily imply $x_1 = x_2$. Therefore, the function is ***not injective****.*

Counterexample: *Take $x_1 = 2$ and $x_2 = \frac{1}{2}$:*

$$f(2) = \frac{4}{5}, \quad f\left(\frac{1}{2}\right) = \frac{4}{5}.$$

Clearly, $f(2) = f\left(\frac{1}{2}\right)$, but $2 \neq \frac{1}{2}$, proving that the function is not injective.

2. ***Surjectivity:***
   A function f is surjective if for every $y \in \mathbb{R}$, there exists an $x \in \mathbb{R}$ such that $f(x) = y$. We know that the function $f(x) = \frac{2x}{1+x^2}$ has a maximum at $x = 1$ where $f(1) = 1$ and a minimum at $x = -1$ where $f(-1) = -1$, and as $x \to \pm\infty$, $f(x) \to 0$. Therefore, the range of $f(x)$ is $(-1, 1)$, and the function is ***not surjective*** *because it cannot take values outside of this interval.*

3. ***Range of $f(x)$:***
   We now show that the range of $f(x) = \frac{2x}{1+x^2}$ is $[-1, 1]$. To do this, we need to find the maximum and minimum values of $f(x)$.

   First, we calculate the derivative of $f(x)$:

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

   Setting $f'(x) = 0$ gives:

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

   Evaluating $f(x)$ at $x = 1$ and $x = -1$:

$$f(1) = \frac{2 \times 1}{1 + 1^2} = 1, \quad f(-1) = \frac{2 \times (-1)}{1 + (-1)^2} = -1.$$

   As $x \to \pm\infty$, $f(x) \to 0$. Therefore, the range of $f(x)$ is $[-1, 1]$, so we have shown that:

$$f(\mathbb{R}) = [-1, 1].$$

4. ***Restriction $g(x) = f(x)$ on $[-1, 1]$:***
   Now, we need to show that the restriction of f to $[-1, 1]$, which we denote by $g(x) = f(x)$, is a bijection.

Injectivity: *Since the derivative $f'(x)$ is positive over the entire interval $[-1, 1]$, the function $f(x) = \frac{2x}{1+x^2}$ is strictly increasing on this interval.*

Therefore, the function $f(x)$ is ***injective*** *on $[-1, 1]$.*

Surjectivity: *The range of $f(x)$ on $[-1, 1]$ is $[-1, 1]$, so the restriction $g(x)$ is surjective.*

Since $g(x)$ is both injective and surjective, it is a bijection.

Solution 2.13.
Let $f : E \to F$, $g : F \to G$, and $h = g \circ f$.

1. ***Injectivity of f:*** *Show that if h is injective, then f is injective. Also, show that if h is surjective, then g is surjective.*

   Proof:

   1.1 Injectivity of f: Assume that $h = g \circ f$ is injective. To show that f is injective, we need to prove that for any $x_1, x_2 \in E$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$.

   Since $h(x_1) = g(f(x_1))$ and $h(x_2) = g(f(x_2))$, if $f(x_1) = f(x_2)$, then

   $$h(x_1) = h(x_2).$$

   Since h is injective, it follows that

   $$x_1 = x_2.$$

   Hence, f is injective.

   1.2 Surjectivity of g: Assume that $h = g \circ f$ is surjective. To show that g is surjective, we need to prove that for every $y \in G$, there exists some $x \in F$ such that $g(x) = y$.

   Since h is surjective, for each $y \in G$, there exists $x \in E$ such that $h(x) = g(f(x)) = y$. Therefore, for every $y \in G$, we can find an $x \in F$ such that $g(x) = y$, which proves that g is surjective.

2. ***Surjectivity of f:*** *Show that if h is surjective and g is injective, then f is surjective.*

   Proof:

Assume that h is surjective and g is injective. To prove that f is surjective, we need to show that for every $y \in F$, there exists some $x \in E$ such that $f(x) = y$.

Since h is surjective, for each $y \in G$, there exists $z \in E$ such that $h(z) = g(f(z)) = y$. Since g is injective, there exists a unique $x \in F$ such that $f(x) = y$, which implies that f is surjective.

3. ***Injectivity of** g**:** *Show that if h is injective and f is surjective, then g is injective.*

   Proof:

   Assume that h is injective and f is surjective. To show that g is injective, we need to prove that if $g(x_1) = g(x_2)$, then $x_1 = x_2$.

   Since $h(x_1) = g(f(x_1))$ and $h(x_2) = g(f(x_2))$, if $g(x_1) = g(x_2)$, we have

   $$h(x_1) = h(x_2).$$

   Since h is injective, it follows that

   $$f(x_1) = f(x_2).$$

   Since f is surjective, there exists some $x \in F$ such that $f(x) = y$, and therefore, $g(x_1) = g(x_2)$.

   Hence, g is injective.

Chapter 3

Algebraic Structures

3.1 Law of internal composition

Definition 3.1.1.
Let E be a non-empty set.

1. *A **law of internal composition** on E is a function from $E \times E$ to E. If T denotes this function, then the image of the pair $(x, y) \in E \times E$ under T is denoted as xTy.*
2. *An **structured set** is any pair (E, T) where E is a non-empty set and T is a law of internal composition on E.*

Example 3.1.1.
The most common internal composition laws are:

1. $+$ *in* $\mathbb{N}, \mathbb{N}^*, \mathrm{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, *but not in* $\mathrm{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$
2. $-$ *in* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
3. $\times$ *in* $\mathbb{N}, \mathbb{N}^*, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
4. $/$ *in* $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$
5. 0 *(composition of functions) in the set of functions from* E *to* E
6. *The law* $\oplus$ *defined on* $\mathbb{R}^2$ *by* $(x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$
7. *The law* T *defined on* $\mathbb{R}$ *by* $xTy = x + y - xy$

8. *The laws* $\cup$, $\cap$ *(union, intersection) defined on* $P(E)$ *(power set of a set* E*)*

Definition 3.1.2. *(Properties of laws)*
Let (E, T) *be a structured set.*

1. *The law* T *is called* ***associative*** *on* E *if* $(xTy)Tz = xT(yTz)$ *for all* x, y, z *in* E*.*

2. *The law* T *is called* ***commutative*** *on* E *if* $xTy = yTx$ *for all* x, y *in* E*.*

Example 3.1.2.
Addition and multiplication are associative and commutative on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$*.*

Definition 3.1.3. *(Properties of laws)*
Let (E, T) *be a structured set.*

1. *An element* e *of* E *is called* ***neutral*** *for the law* T *if,*

$$\forall x \in E,\ xTe = eTx = x.$$

2. *If* (E, T) *has a neutral element* e*, then an element* x *of* E *is said to be invertible (or symmetrizable) for the law* T *if there exists an element* x' *in* E *such that:*

$$xTx' = x'Tx = e$$

The element x' *is then called the symmetric element of* x *for the law* T*.*

Proposition 3.1.1.
Let (E, T) *be a structured set. If the neutral element of* E *for the law* T *exists, then it is unique.*

Proof 3.1.1.
Suppose there exist two neutral elements e *and* e'*. Then,*

$$e' = eTe' = e$$

which implies $e = e'$*.*

Proposition 3.1.2.
Let (E, T) *be a structured set where the law* T *is associative and has a neutral element.*

1. *If $x \in E$ is symmetrizable, then its symmetric element is unique.*
2. *If $x \in E$ and $y \in E$ are symmetrizable, then xTy is symmetrizable and its symmetric element $(xTy)'$ is given by $(xTy)' = y'Tx'$ where x' denotes the symmetric element of x and y' denotes the symmetric element of y.*

Proof 3.1.2.

1. *Let's suppose an element x has two symmetric elements x' and x''. Then,*

$$xTx' = e \Rightarrow x''T(xTx') = x'' \Rightarrow (x''Tx)Tx' = x'' \Rightarrow x' = x''.$$

2. *We have*

$$(y'Tx')T(xTy) = y'T(x'Tx)Ty = y'Ty = e.$$

Also,

$$(xTy)T(y'Tx') = xT(yTy')Tx' = xTx' = e.$$

Thus, $(xTy)' = y'Tx'$.

3.2 Groups

3.2.1 Group Structure

Definition 3.2.1.
Let (G, T) be a structured set.

1. *We say that (G, T) is a **group** if*
   (a) *the operation T is associative on G,*
   (b) *there exists a neutral element for the operation T in G,*
   (c) *every element of G is symmetrizable for the operation T.*

   *We also say that the set G has a **group structure** for the operation T.*
2. *We say that the group (G, T) is **commutative (or abelian)** if the operation T is commutative on G.*

Example 3.2.1.
First, examples of groups are provided:

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

Example 3.2.2.
For various reasons (to be determined), the following pairs are not groups:

1. $(\mathbb{N}, +)$, $(\mathbb{R}, \times)$.
2. $(\mathcal{P}(E), \cup)$, $(\mathcal{P}(E), \cap)$.

3.2.2 Subgroups

Definition 3.2.2. *(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. *With this law, H forms a group. We denote this as $H < G$.*

Proposition 3.2.1.
The subset $H \subset G$ is a ***subgroup*** *of a group $(G, *)$ if and only if*

1. $H \neq \varnothing$,
2. $\forall (x, y) \in H^2,\ x * y \in H$,
3. $\forall x \in H,\ x^{-1} \in H$.

Example 3.2.3.

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

Proposition 3.2.2.
The subset $H \subset G$ is a subgroup of a group $(G, *)$ if and only if

1. $H \neq \varnothing$,

2. $\forall (x, y) \in H^2,\ x * y^{-1} \in H$.

Proposition 3.2.3.
The intersection of any family of subgroups of a group $(G, *)$ is a subgroup of $(G, *)$.

Proof 3.2.1.
Let $(H_i)_{i \in I}$ be a family of subgroups of a group G. Define $K = \bigcap_{i \in I} H_i$, the intersection of all H_i. The set K is non-empty since it contains the identity element e, which belongs to each subgroup H_i. Let x and y be two elements of K. For every $i \in I$, we have $x * y^{-1} \in H_i$ because H_i is a subgroup. Therefore, $x * y^{-1} \in K$. This proves that K is a subgroup of G.

Remark 3.2.1.
The arbitrary union of subgroups of a group $(G, *)$ is not necessarily a subgroup of $(G, *)$.

Example 3.2.4.
Let T be the internal composition law defined on $\mathbb{R}^2$ by

$$\forall (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2, \quad (x_1, y_1) * (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

We have $(\mathbb{R}^2, T)$ is a group, $\mathbb{R} \times \{0\}$ and $\{0\} \times \mathbb{R}$ are two subgroups of $(\mathbb{R}^2, T)$ but $\mathbb{R} \times \{0\} \cup \{0\} \times \mathbb{R}$ does not form a subgroup of $(\mathbb{R}^2, T)$.

Proposition 3.2.4.
The union of two subgroups H and K of the same group $(G, *)$ is a subgroup $(H \cup K < G)$ if and only if $H \subset K$ or $K \subset H$.

Proof 3.2.2.
Suppose $H \cup K$ is a subgroup of G and H is not included in K, meaning there exists $h \in H$ such that $h \notin K$. Let's show that $K \subset H$. Take any $k \in K$. We have $h * k \in H \cap K$. However, $h * k \notin K$ because otherwise $h = (h * k) * k' \in K$. Hence, $h * k \in H$, implying $k = h' * (h * k) \in H$.

3.2.3 Examples of Groups

3.2.3.1 The Group $\mathbb{Z}/n\mathbb{Z}$

It is initially clear that if n is a positive integer (which we can assume to be positive and non-zero), the set $n\mathbb{Z}$ consisting of integers of the form nk, where k ranges over $\mathbb{Z}$ (the set of multiples of n), is an additive subgroup of $(\mathbb{Z}, +)$.

Proposition 3.2.5.
Every subgroup of $(\mathbb{Z}, +)$ is of the form $n\mathbb{Z}$.

Proof 3.2.3.
Let S be a subgroup of $\mathbb{Z}$ other than $\{0\}$ and $\mathbb{Z}$. Hence, S does not contain 1. The set of positive integers in S, denoted by S^+, has a smallest element n which is at least 2 (since S is countable and bounded below). Every integer of the form kn, where k is a natural number, belongs to S (clear from induction since $kn = n + n + \ldots + n$). Therefore, S contains $n\mathbb{Z}$.

By Euclidean division, every positive integer in S^+ that is not of the form kn can be written as $a = kn + r$, where $0 < r < n$. It follows that $r = a - kn > 0$. Since both a and kn are in S^+, r must also be in S^+. This contradicts n being the smallest element of S^+, hence $r = 0$. This shows that $S = n\mathbb{Z}$.

We easily show that the congruence relation modulo n, where $n \in \mathbb{N}$, due to Gauss, denoted by $\equiv$, is defined as:

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

$x \equiv y[n]$ reads as "x is congruent to y modulo n," which is an equivalence relation defined in $(\mathbb{Z}, +)$. The quotient set is finite and can thus be written:

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

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

- Quotient addition on $\mathbb{Z}/n\mathbb{Z}$ induced by $\mathbb{Z}$ is:

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

- Quotient multiplication on $\mathbb{Z}/n\mathbb{Z}$ induced by $\mathbb{Z}$ is:

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

Proposition 3.2.6.
The set $(\mathbb{Z}/n\mathbb{Z}, \overset{\bullet}{+})$ is a commutative additive group (the quotient group of $\mathbb{Z}$ by the congruence relation).

Proof 3.2.4. *Leave it to the reader.*

3.2.3.2 Group of Permutations

Definition 3.2.3.
Let E be a set. A permutation of E is a bijection from E to itself. We denote by S_E the set of permutations of E. If $E = \{1, \ldots, n\}$, we simply denote it by S_n. The set S_E, equipped with the composition of mappings, forms a group with identity $e = id$, called the symmetric group on the set E.

Example 3.2.5.
Let's assume $E = \{1, 2, 3, 4, 5\}$. A permutation $\sigma \in S_5$ is represented as follows:

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

which means $\sigma(1) = 3$, $\sigma(2) = 5$, and so on.

3.2.4 Group Homomorphisms

Definition 3.2.4.
*Let $(G, *)$ and (H, T) be two groups. A function f from G to H is a **group homomorphism** if:*

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

Moreover:

1. *If $G = H$ and $* = T$, it is called an **endomorphism**.*
2. *If f is bijective, it is an **isomorphism**.*

3. *If f is a bijective endomorphism, it is an* ***automorphism****.*

Example 3.2.6.
The map $x \mapsto 2x$ defines an automorphism of $(\mathbb{R}, +)$.

Example 3.2.7.
The function $f : \mathbb{R} \to \mathbb{R}_+^*$, where $\mathbb{R}_+^*$ is the set of positive real numbers under multiplication, defined by $f(x) = \exp(x)$, is a group homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_+^*, \times)$ because $\exp(x + y) = \exp(x) \times \exp(y)$ for all $x, y \in \mathbb{R}$.

Proposition 3.2.7. *(Properties of Group Homomorphisms)*
Let f be a homomorphism from $(G, *)$ to (H, T):

1. *$f(e_G) = e_H$.*
2. *$\forall x \in G,\ f(x') = (f(x))'$.*
3. *If f is an isomorphism, then its inverse f^{-1} is also an isomorphism from (H, T) to $(G, *)$.*
4. *If $G' < G$ (subgroup of G), then $f(G') < H$.*
5. *If $H' < H$ (subgroup of H), then $f^{-1}(H') < G$.*

Definition 3.2.5.
Let f be a homomorphism from G to H:

1. *The kernel of f, denoted $Ker(f)$, is the set of pre-images of e_H:*

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

   (Note: f is not assumed to be bijective; hence there's no mention of the inverse bijection of f.)

2. *The image of f, denoted $Im(f)$, is $f(G)$ (set of images by f of elements of G).*

Remark 3.2.2.
According to the last two points of Proposition 1, the kernel and image of f are respective subgroups of G and H.

Proposition 3.2.8.
Let f be a homomorphism from $(G, *)$ to (H, T):

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

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

Proof 3.2.5.
The point (1) follows directly from the definition of surjectivity. To prove (2), suppose first that f is injective. Let $x \in Ker(f)$. Then $f(x) = e_H$, and since $f(e_G) = e_H$ as stated, we conclude $f(x) = f(e_G)$, which implies $x = e_G$ by injectivity of f. Thus, $Ker(f) = \{e_G\}$. Conversely, suppose $Ker(f) = \{e_G\}$ and show that f is injective. Consider $x, y \in G$ such that $f(x) = f(y)$. Then $f(x)Tf(y)' = e_H$, so $f(x * y') = e_H$, meaning $x * y' \in Ker(f)$. The assumption $Ker(f) = \{e_G\}$ then implies $x * y' = e_G$, hence $x = y$. Injectivity of f is thus demonstrated, completing the Proof.

3.3 Ring Structure

Definition 3.3.1.
A ring *is a set equipped with two binary operations $(A, *, T)$ such that:*

1. *$(A, *)$ is a commutative group with identity element denoted by 0_A.*

2. *The operation T is associative and distributive on the left and right with respect to $*$:*

$$\forall x, y, z \in A, \quad xT(y * z) = xTy * xTz \quad \text{and} \quad (x * y)Tz = xTz * yTz.$$

3. *The operation T has a neutral element different from 0_A, denoted by 1_A.*

Example 3.3.1.
$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, and $(\mathbb{C}, +, \times)$ are well-known rings.

Remark 3.3.1.

1. *If the operation T is commutative, the ring is called commutative or abelian.*

2. *The set $A - \{0_A\}$ is denoted by A^*.*

3. *For simplicity, we temporarily use the additive $(+)$ and multiplicative $(\times)$ notations instead of the internal operations $*$ and T. Therefore, we refer to the ring $(A, +, \times)$ instead of $(A, *, T)$.*

Definition 3.3.2.

1. *A commutative ring* $(A, +, \times)$ *is called* ***integral*** *if it is*
   (a) *non-zero (i.e.,* $1_A \neq 0_A$*),*
   (b) $\forall (x, y) \in A^2, \quad x \times y = 0 \Rightarrow (x = 0 \text{ or } y = 0)$.
2. *When a product* $a \times b$ *is zero but neither* a *nor* b *is zero,* a *and* b *are called zero divisors.*

Example 3.3.2.

1. $(\mathbb{Z}, +, \times)$ *of integers is integral: it has no zero divisors.*
2. *The ring* $\mathbb{Z}/6\mathbb{Z}$ *of residue classes modulo* 6 *is not integral because* $\overset{\bullet}{2} \times \overset{\bullet}{3} = \overset{\bullet}{6}$*, hence* $\overset{\bullet}{2} \times \overset{\bullet}{3} = \overset{\bullet}{0}$*. Similarly,* $\mathbb{Z}/4\mathbb{Z}$*.*

Proposition 3.3.1.
Let $(A, +, \times)$ *be a ring. The following rules apply in rings:*

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

Proof 3.3.1.

1. $x \times 0_A = x \times (0_A + 0_A) = x \times 0_A + x \times 0_A$*. Therefore, by the regularity of elements in the group* $(A, +)$*,* $x \times 0_A = 0_A$*. Similarly for the other side.*
2. $x \times y + (-x) \times y = (x + (-x)) \times y = 0_A \times y = 0_A$*. Thus,* $(-x) \times y = -(x \times y)$*. Similarly for the other equality.*
3. $(-1_A) \times x + x = (-1_A) \times x + 1_A \times x = (-1_A + 1_A) \times x = 0_A \times x = 0_A$*. Hence,* $(-1_A) \times x = -x$.

4. *Left to the reader.*

5. *Left to the reader.*

Notations and Conventions

Let $(A, *, T)$ be a ring. Let n be a non-zero natural number and x an element of A.

1. We denote by nx the element of A that is equal to the composition by the first operation $*$ of n terms equal to x. In other words, for all $n \in \mathbb{N}^*$ and $x \in A$,
$$nx = \underbrace{x * x * \ldots * x}_{\text{n times}}.$$
In particular, for $n = 1$, we have $1 \cdot x = x$ for all $x \in A$.

2. Similarly, we denote by x^n the element of A that is equal to the composition by the second operation T of n terms equal to x. In other words, for all $n \in \mathbb{N}^*$ and $x \in A$,
$$x^n = \underbrace{xTxT \ldots Tx}_{\text{n times}}.$$
In particular, for $n = 1$, we have $x^1 = x$ for all $x \in A$.

3. What about $n = 0$? Let 0_A denote the zero element and 1_A denote the unit element of $(A, *, T)$ (this notation is somewhat unfortunate here because it recalls the additive notation and the multiplicative notation that we are precisely trying to avoid). Then, by convention, for all $x \in A$, $0 \cdot x = 0_A$ and $x^0 = 1_A$.

3.3.1 Subrings

Definition 3.3.3.

*Let $(A, *, T)$ be a ring. A non-empty subset A_1 of A is a **subring** of A if:*

1. $1_A \in A_1$;

2. *the operations $*$ and T induce binary operations on A_1, and with these operations, $(A_1, *, T)$ is a ring.*

Proposition 3.3.2.

A subset A_1 of A is a subring if and only if:

1. $(A_1, *)$ *is a subgroup of* $(A, *)$*;*
2. $1_A \in A_1$*;*
3. $\forall (x, y) \in A_1^2, \quad xTy \in A_1$ *(*T *induces a binary operation on* A_1*).*

Example 3.3.3.
$(\mathbb{Z}, +, \times)$ *is a subring of* $(\mathbb{Q}, +, \times)$*, which is a subring of* $(\mathbb{R}, +, \times)$*, which is a subring of* $(\mathbb{C}, +, \times)$*.*

3.3.2 Ring Homomorphisms

Definition 3.3.4.
Let $(A, +_A, \times_A)$ *and* $(B, +_B, \times_B)$ *be two rings. 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* $f(x \times_A y) = f(x) \times_B f(y)$*.*

3.3.3 Ideals in a Commutative Ring

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

Definition 3.3.5. *(Ideal)*
A subset I *of* A *is an ideal of a 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 3.3.3.
A subset I *of* A *is an ideal of a ring* $(A, +, \times)$ *if and only if*

1. I *contains the zero element* 0_A*,*
2. *for all* $x, y \in I$*,* $x - y \in I$*,*
3. $\forall a \in A, \forall x \in I$*,* $ax \in I$*.*

Example 3.3.4.

1. *Any non-trivial ring has at least two ideals: the trivial ideal* $\{0\}$ *and* A *itself. Ideals of* A *that are distinct from* A *are called proper ideals.*

2. *Any element* x *of* A *defines a principal ideal:* $\langle x \rangle = xA = \{ax \mid a \in A\}$. *It is the smallest ideal containing* x, *and we say it is generated by* x. *If* x *is invertible (and only in this case),* $xA = A$.

3. *More generally, if* $x_1, \ldots, x_n \in A$, *the smallest ideal containing* $x_1, \ldots, x_n$ *is:*

$$\langle x_1, \ldots, x_n \rangle = x_1 A + \ldots + x_n A = \{a_1 x_1 + \ldots + a_n x_n \mid a_1, \ldots, a_n \in A\}.$$

Indeed, it is immediately verified that $I = x_1 A + \ldots + x_n A$ *is non-empty and stable under linear combinations, hence it is an ideal; and of course, any ideal containing the* x_i *must contain* I. *We say* I *is generated by* $\{x_1, \ldots, x_n\}$.

3.4 Field Structure

Definition 3.4.1. ***(Field)***

1. ***A field*** *is a commutative ring in which every non-zero element is invertible.*

2. *Moreover, if the second operation* $\times$ *is commutative on* K, *then we say that the field* $(K, +, \times)$ *is commutative.*

Example 3.4.1.
$(\mathbb{Q}, +, \times)$ *and* $(\mathbb{R}, +, \times)$ *are commutative fields.*

Definition 3.4.2. ***Subfield***
Let $(K, +, \times)$ *be a field and let* K_1 *be a non-empty subset of* K.
We say that K_1 *is* ***a subfield*** *of* K *if* K_1 *is stable under* $+$ *and* $\times$ *in* K, *and* K_1 *equipped with the induced operations from* K *forms a field itself.*

Example 3.4.2.
$(\mathbb{Q}, +, \times)$ *is a subfield of* $(\mathbb{R}, +, \times)$.

Proposition 3.4.1.
Let $(K, +, \times)$ *be a field. A subset* K_1 *of* K *is a subfield if and only if:*

1. $(K_1, +)$ *is a subgroup of* $(K, +)$,

2. *for all* $x, y \in K_1$, $x \times y \in K_1$ *(stability of* K_1 *under* $\times$*),*

3. K_1 *contains the identity element of* K*, and the inverse of every* $x \in K_1$ *in* $(K, \times)$ *is also an element of* K_1*.*

3.5 Exercises

Exercice 3.1.
Consider on $\mathbb{R}$ the binary operation $*$ defined by $x*y = x+y-xy$. Is this operation associative, commutative? Does it have a neutral element? Does a real number x have an inverse under this operation? Provide a formula for the n-th power of an element x under this operation.

Exercice 3.2.
We define an internal composition law $*$ on $\mathbb{R}$ by

$$\forall (a,b) \in \mathbb{R}^2, \quad a * b = \ln(e^a + e^b).$$

What are its properties? Does it have a neutral element? Are there regular elements?

Exercice 3.3.
We are given an internal composition law defined by:

$$\forall x, y \in \mathbb{R}^+, x \star y = \sqrt{x^2 + y^2}$$

Show that this operation is commutative, associative, and that there exists a neutral element. Show that no element has an inverse for this operation.

Exercice 3.4.
We define, for (x,y) and (x',y') in $\mathbb{R}^* \times \mathbb{R}$, the operation $\star$ by:

$$(x,y) \star (x',y') = (xx', xy' + y).$$

Prove that $(\mathbb{R}^* \times \mathbb{R}, \star)$ is a group. Is it commutative? Simplify $(x,y)^n$ for all $(x,y) \in \mathbb{R}^* \times \mathbb{R}$ and for all $n \in \mathbb{N}^*$.

Exercice 3.5.
We define on $\mathbb{R}$, the composition law $\circ$ by:

$$x \circ y = x + y - 2, \quad \forall x, y \in \mathbb{R}.$$

1. *Show that $(\mathbb{R}, \circ)$ is an abelian group.*
2. *Let $n \in \mathbb{N}$. We define $x(1) = x$ and $x(n+1) = x(n) \circ x$.*
   (a) *Calculate $x(2), x(3)$, and $x(4)$.*

(b) Show that for all $n \in \mathbb{N}$: $x(n) = nx - 2(n-1)$.

3. *Let $A = \{x \in \mathbb{R} \mid x \text{ is even}\}$. Show that $(A, \circ)$ is a subgroup of $(\mathbb{R}, \circ)$.*

Exercice 3.6.
Exercise 3: Let $(G, \cdot)$ be a group, and denote by $Z(G) = \{x \in G \mid \forall y \in G, xy = yx\}$ the center of G.

1. *Show that $Z(G)$ is a subgroup of G.*
2. *Show that G is commutative if and only if $Z(G) = G$.*

Exercice 3.7.
Let $(G, \cdot)$ be a non-commutative group with neutral element e. For $a \in G$, define a function $f_a : G \to G$ by

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

1. *Show that f_a is an endomorphism of the group $(G, \cdot)$.*
2. *Verify that for all $a, b \in G$, $f_a \circ f_b = f_{a \cdot b}$.*
3. *Show that f_a is bijective and determine its inverse function.*

Exercice 3.8.
Let $(A, +, \cdot)$ be a ring with identities 0 and 1 for addition and multiplication respectively. We define the following operations $\star$ and $\diamond$ on A:

$$\forall a, b \in A, \quad a \star b = a + b + 1$$

$$\forall a, b \in A, \quad a \diamond b = a \cdot b + a + b$$

1. *Show that $(A, \star, \diamond)$ is a ring.*
2. *Show that the map $f : (A, +, \cdot) \to (A, \star, \diamond)$ given by $f(a) = a - 1$ is an isomorphism of rings.*

Exercice 3.9.
Show that $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ is a field.

3.6 Exercise Solutions

Solution 3.1.

1. ***Associativity:***
   To check if $*$ is associative, we verify if $(x * y) * z = x * (y * z)$ for all $x, y, z \in \mathbb{R}$.

   Let's calculate:

   $$x * y = x + y - xy,$$

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

   Now calculate:

   $$y * z = y + z - yz,$$

   $$x * (y * z) = x * (y + z - yz) = x + (y + z - yz) - x(y + z - yz).$$

   Simplifying gives:

   $$x + y + z - xy - xz - yz + xyz,$$

   which equals $(x * y) * z$. Hence, $*$ is associative.

2. ***Commutativity:***
   To check if $*$ is commutative, we verify if $x * y = y * x$ for all $x, y \in \mathbb{R}$.

   Calculating $y * x$ gives:

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

   Therefore, $*$ is commutative.

3. ***Neutral Element:***
   We seek a real number e such that $x * e = e * x = x$ for all $x \in \mathbb{R}$.

   Setting $x * e = x$ gives:

   $$x + e - xe = x.$$

   Simplifying gives $e - xe = 0$, so $e(1 - x) = 0$. For all $x \neq 1$, we have $e = 0$.

   Therefore, the neutral element e is 0.

4. ***Inverse Element:***

   We look for a real number y such that $x*y = y*x = e$, where e is the neutral element.

   Solving $x * y = 0$ gives:

   $$x + y - xy = 0.$$

   Rearranging gives:

   $$y - xy = -x,$$

   $$y(1 - x) = -x.$$

   So,

   $$y = \frac{-x}{1 - x}.$$

   Hence, the inverse of x under $*$ is $\frac{-x}{1-x}$, provided $x \neq 1$.

5. ***Formula for n-th Power:***

   We consider the operation $*$ defined on $\mathbb{R}$ by:

   $$x * y = x + y - xy, \quad \textit{for all } x, y \in \mathbb{R}.$$

   We aim to derive a formula for x^{*n}, defined as:

   $$x^{*n} = \underbrace{x * x * \cdots * x}_{n \text{ times}}.$$

   Special cases

   - *For $n = 1$:*

     $$x^{*1} = x.$$

   - *For $n = 2$:*

     $$x^{*2} = x * x = x + x - x^2 = 2x - x^2.$$

   - *For $n = 3$:*

     $$x^{*3} = x^{*2} * x = (2x - x^2) * x.$$

     By computation, we find:

     $$(2x - x^2) * x = (2x - x^2) + x - (2x - x^2)x = 3x - 3x^2 + x^3.$$

General formula

From the special cases, we observe that the n-th power can be written as:

$$x^{*n} = nx - \binom{n}{2}x^2 + \binom{n}{3}x^3 - \cdots + (-1)^{n-1}\binom{n}{n}x^n,$$

where the coefficients are the binomial coefficients.

Proof by induction

- ***Base case:*** *For $n = 1$, we have $x^{*1} = x$, which matches the formula.*
- ***Inductive step:*** *Assume that:*

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

We want to show that:

$$x^{*(n+1)} = \sum_{k=1}^{n+1}(-1)^{k-1}\binom{n+1}{k}x^k.$$

By definition:

$$x^{*(n+1)} = x^{*n} * x = x^{*n} + x - x^{*n} \cdot x.$$

Substituting the formula for x^{*n} and simplifying, we recover exactly the terms corresponding to:

$$\sum_{k=1}^{n+1}(-1)^{k-1}\binom{n+1}{k}x^k.$$

This completes the proof by induction.

Final formula

The n-th power for the operation $*$ is given by:

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

where $\binom{n}{k}$ is the binomial coefficient.

Solution 3.2.

We are given the binary operation $*$ on $\mathbb{R}$ defined by

$$a * b = \ln(e^a + e^b).$$

We will now examine the properties of this operation.

1. Commutativity *To check if $*$ is commutative, we need to verify if*

$$a * b = b * a \quad \textit{for all} \quad a, b \in \mathbb{R}.$$

Using the definition of the operation:

$$a * b = \ln(e^a + e^b) \quad \textit{and} \quad b * a = \ln(e^b + e^a).$$

Since $e^a + e^b = e^b + e^a$, we have:

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

Thus, the operation $*$ is ***commutative****.*

2. Associativity *To check if $*$ is associative, we need to verify if*

$$(a * b) * c = a * (b * c) \quad \textit{for all} \quad a, b, c \in \mathbb{R}.$$

We calculate both sides using the definition of $*$:

- Left-hand side:

$$(a * b) * c = \ln(e^a + e^b) * c = \ln\left(e^{\ln(e^a+e^b)} + e^c\right) = \ln\left((e^a + e^b) + e^c\right)$$

- Right-hand side:

$$a * (b * c) = a * \ln(e^b + e^c) = \ln\left(e^a + e^{\ln(e^b+e^c)}\right) = \ln\left(e^a + (e^b + e^c)\right)$$

Since the two expressions are equal, the operation is ***associative****.*

3. Neutral Element *To find a neutral element $e \in \mathbb{R}$, we need to solve the equation*

$$a * e = a \quad \textit{for all} \quad a \in \mathbb{R}.$$

Using the definition of $*$:

$$a * e = \ln(e^a + e^e) = a.$$

This simplifies to:

$$e^a + e^e = e^a \quad \Rightarrow \quad e^e = 0.$$

Since $e^e = 0$ has no real solution, there is ***no neutral element****.*

4. Regular Elements *An element x is regular if there exists an inverse x^{-1} such that*

$$x * x^{-1} = e.$$

Since there is no neutral element, there are ***no regular elements****.*

Conclusion *- The operation $*$ is* ***commutative****. - The operation $*$ is* ***associative****. - There is* ***no neutral element****. - There are* ***no regular elements****.*

Solution 3.3.

Solution *We are given the operation $\star$ defined on $\mathbb{R}^+$ as:*

$$\forall x, y \in \mathbb{R}^+, \quad x \star y = \sqrt{x^2 + y^2}.$$

We will analyze the properties step by step.

1. Commutativity *To check if the operation $\star$ is commutative, compute:*

$$x \star y = \sqrt{x^2 + y^2}, \quad y \star x = \sqrt{y^2 + x^2}.$$

Since addition is commutative, $x^2 + y^2 = y^2 + x^2$, it follows that:

$$x \star y = y \star x.$$

Thus, the operation $\star$ is ***commutative****.*

2. Associativity *To verify associativity, we need to check if:*

$$(x \star y) \star z = x \star (y \star z).$$

Compute $(x \star y) \star z$***:***

$$x \star y = \sqrt{x^2 + y^2}, \quad (x \star y) \star z = \sqrt{(\sqrt{x^2 + y^2})^2 + z^2} = \sqrt{x^2 + y^2 + z^2}.$$

Compute $x \star (y \star z)$***:***

$$y \star z = \sqrt{y^2 + z^2}, \quad x \star (y \star z) = \sqrt{x^2 + (\sqrt{y^2 + z^2})^2} = \sqrt{x^2 + y^2 + z^2}.$$

Since both expressions are equal:

$$(x \star y) \star z = x \star (y \star z).$$

Thus, the operation $\star$ is ***associative****.*

3. Existence of a Neutral Element *A neutral element $e \in \mathbb{R}^+$ satisfies:*

$$x \star e = x, \quad \forall x \in \mathbb{R}^+.$$

Using the definition of $\star$:

$$x \star e = \sqrt{x^2 + e^2} = x.$$

Squaring both sides:

$$x^2 + e^2 = x^2 \quad \Longrightarrow \quad e^2 = 0 \quad \Longrightarrow \quad e = 0.$$

The neutral element is therefore $e = 0$.

4. Existence of Inverse Elements *Let us suppose that a symmetric element exists. However, $x \star x' = \sqrt{x^2 + x'^2} = 0$ then $x^2 + x'^2 = 0$ then then $x = x' = 0$. So if $x > 0$, there is no symmetric element.*

Conclusion

- *The operation $\star$ is* ***commutative****.*
- *The operation $\star$ is* ***associative****.*
- *The neutral element is therefore $e = 0$.*
- *If $x > 0$, there is no symmetric element.*

Solution 3.4.

1. Proving that $(\mathbb{R}^* \times \mathbb{R}, \star)$ ***is a Group: Closure:*** *Given two elements (x, y) and (x', y') in $\mathbb{R}^* \times \mathbb{R}$, the operation $\star$ is defined as:*

$$(x, y) \star (x', y') = (xx', xy' + y).$$

Since $x, x' \in \mathbb{R}^*$ and $y, y' \in \mathbb{R}$, it follows that $xx' \in \mathbb{R}^*$ and $xy' + y \in \mathbb{R}$, so the result is in $\mathbb{R}^* \times \mathbb{R}$. Therefore, the operation is closed.

Associativity: *We need to prove that:*

$$((x, y) \star (x', y')) \star (x'', y'') = (x, y) \star ((x', y') \star (x'', y'')).$$

First, compute the left-hand side:

$$(x, y) \star (x', y') = (xx', xy' + y),$$

and then:

$$(xx', xy' + y) \star (x'', y'') = (xx'x'', (xy' + y)y'' + (xy' + y)).$$

Now, compute the right-hand side:

$$(x', y') \star (x'', y'') = (x'x'', x'y'' + y'),$$

and then:

$$(x, y) \star (x'x'', x'y'' + y') = (x(x'x''), x(x'y'' + y') + y).$$

Since both sides are equal, the operation $\star$ is associative.

Neutral Element: *We look for a neutral element (e_1, e_2) such that:*

$$(x, y) \star (e_1, e_2) = (x, y) \quad \textit{and} \quad (e_1, e_2) \star (x, y) = (x, y).$$

From the equation:

$$(x, y) \star (e_1, e_2) = (xe_1, xe_2 + y),$$

we must have $e_1 = 1$ and $e_2 = 0$.

Thus, the neutral element is $(1, 0)$.

Inverses: *We look for the inverse of (x, y) such that:*

$$(x, y) \star (x', y') = (1, 0).$$

From the equation:

$$(xx', xy' + y) = (1, 0),$$

we get:

$$xx' = 1 \quad \textit{and} \quad xy' + y = 0.$$

Thus, $x' = \frac{1}{x}$ and $y' = -\frac{y}{x}$.

Therefore, the inverse of (x, y) *is* $\left(\frac{1}{x}, -\frac{y}{x}\right)$.

2. Is the operation $\star$ ***Commutative?***

To check if the operation is commutative, we need to verify if:

$$(x, y) \star (x', y') = (x', y') \star (x, y).$$

We have:

$$(x, y) \star (x', y') = (xx', xy' + y),$$

and

$$(x', y') \star (x, y) = (x'x, x'y + y').$$

For the operation to be commutative, we must have:

$$xx' = x'x \quad \textit{and} \quad xy' + y = x'y + y'.$$

The first condition $xx' = x'x$ *holds because multiplication in* $\mathbb{R}^*$ *is commutative. However, the second condition* $xy' + y = x'y + y'$ *is not always true, as the terms involve different variables. Thus, the operation is* ***not commutative****.*

3. Simplifying $(x, y)^n$***:***

To compute $(x, y)^n$ *using the operation* $\star$*, we observe the following pattern:*

$$(x, y)^n = (x^n, nxy + y(1 + 2 + \cdots + (n - 1))).$$

The sum $1 + 2 + \cdots + (n - 1)$ *is the sum of the first* $n - 1$ *integers, which is given by:*

$$\frac{(n - 1)n}{2}.$$

Thus, we have:

$$(x, y)^n = (x^n, nxy + \frac{(n - 1)n}{2}y).$$

Summary:

- $(\mathbb{R}^* \times \mathbb{R}, \star)$ *is a group.*
- *The operation is* ***not commutative****.*
- $(x, y)^n = (x^n, nxy + \frac{(n-1)n}{2}y)$.

Solution 3.5.

We define on $\mathbb{R}$*, the composition law* $\circ$ *by:*

$$x \circ y = x + y - 2, \quad \forall x, y \in \mathbb{R}.$$

1. *Show that* $(\mathbb{R}, \circ)$ *is an abelian group.*

   To show that $(\mathbb{R}, \circ)$ *is an abelian group, we need to verify the following properties:*

   - ***Closure:*** *For all* $x, y \in \mathbb{R}$*, we need to show that* $x \circ y \in \mathbb{R}$*.*

     $$x \circ y = x + y - 2,$$

     which is clearly in $\mathbb{R}$*, so the operation is closed.*

   - ***Associativity:*** *We need to show that for all* $x, y, z \in \mathbb{R}$*,*

     $$(x \circ y) \circ z = x \circ (y \circ z).$$

     We compute both sides:
     - Left-hand side:

     $$(x \circ y) \circ z = (x + y - 2) \circ z = (x + y - 2) + z - 2 = x + y + z - 4.$$

     - Right-hand side:

     $$x \circ (y \circ z) = x \circ (y + z - 2) = x + (y + z - 2) - 2 = x + y + z - 4.$$

     Since both sides are equal, the operation is associative.

   - ***Neutral element:*** *We need to find the neutral element* $e \in \mathbb{R}$ *such that for all* $x \in \mathbb{R}$*,*

     $$x \circ e = x \quad \text{and} \quad e \circ x = x.$$

     Using the operation:

     $$x \circ e = x + e - 2 = x \quad \Rightarrow \quad e = 2.$$

     Therefore, the neutral element is $e = 2$*.*

- ***Inverses:*** *We need to find the inverse of each* $x \in \mathbb{R}$*, i.e., an element* $y \in \mathbb{R}$ *such that:*

$$x \circ y = 2.$$

Using the operation:

$$x \circ y = x + y - 2 = 2 \quad \Rightarrow \quad y = 4 - x.$$

Therefore, the inverse of x *is* $4 - x$*.*

- ***Commutativity:*** *We need to show that* $x \circ y = y \circ x$*. Since*

$$x \circ y = x + y - 2 \quad \textit{and} \quad y \circ x = y + x - 2,$$

and since addition is commutative, $x + y = y + x$*, so* $x \circ y = y \circ x$*.*

Since we have shown closure, associativity, the existence of an identity element, inverses, and commutativity, we conclude that $(\mathbb{R}, \circ)$ *is an abelian group.*

2. *Let* $n \in \mathbb{N}$*. We define* $x(1) = x$ *and* $x(n+1) = x(n) \circ x$*.*

Solution:

(a) ***Calculate*** $x(2), x(3), x(4)$***:***

We compute $x(2), x(3), x(4)$ *based on the recursive definition of* $x(n)$*:*

- $x(2) = x(1) \circ x = x \circ x = x + x - 2 = 2x - 2$. - $x(3) = x(2) \circ x = (2x-2) \circ x = (2x-2) + x - 2 = 3x - 4$. - $x(4) = x(3) \circ x = (3x-4) \circ x = (3x-4) + x - 2 = 4x - 6$.

Thus, we have:

$$x(2) = 2x - 2, \quad x(3) = 3x - 4, \quad x(4) = 4x - 6.$$

(b) ***Show that for all*** $n \in \mathbb{N}$***,*** $x(n) = nx - 2(n-1)$***:***

We will prove this by induction on n*.*

- ***Base case*** *(*$n = 1$*):*

$$x(1) = x = 1x - 2(1-1) = x.$$

So the base case holds.

- ***Inductive step:*** *Assume the formula holds for some n, i.e., assume:*

$$x(n) = nx - 2(n-1).$$

We need to show that:

$$x(n+1) = (n+1)x - 2n.$$

From the definition of $x(n+1)$:

$$x(n+1) = x(n) \circ x = (nx - 2(n-1)) \circ x = (nx - 2(n-1)) + x - 2 = (n+1)x - 2n.$$

Thus, the formula holds for $n+1$, completing the induction.
Therefore, for all $n \in \mathbb{N}$, we have:

$$x(n) = nx - 2(n-1).$$

3. *Let $A = \{x \in \mathbb{R} \mid x \text{ is even}\}$. Show that $(A, \circ)$ is a subgroup of $(\mathbb{R}, \circ)$.*

Solution:

We need to verify that $(A, \circ)$ is a subgroup of $(\mathbb{R}, \circ)$. To do this, we must check the following properties:

- ***Closure:*** *Let $x, y \in A$. Since x and y are even, we have $x = 2m$ and $y = 2n$ for some $m, n \in \mathbb{Z}$. Now, check if $x \circ y \in A$:*

$$x \circ y = x + y - 2 = 2m + 2n - 2 = 2(m + n - 1).$$

Since $m + n - 1$ is an integer, $x \circ y$ is even. Thus, A is closed under $\circ$.

- ***Identity element:*** *The identity element of $(\mathbb{R}, \circ)$ is 2. We check if $2 \in A$. Since 2 is even, the identity element belongs to A.*

- ***Inverses:*** *Let $x \in A$. Since x is even, $x = 2m$ for some $m \in \mathbb{Z}$. The inverse of x in $(\mathbb{R}, \circ)$ is $4 - x$. We need to check if the inverse is also in A:*

$$4 - x = 4 - 2m = 2(2 - m),$$

which is even. Therefore, the inverse of x is also in A.

- ***Commutativity:*** *Since $(\mathbb{R}, \circ)$ is commutative, $(A, \circ)$ inherits commutativity.*

Since $(A, \circ)$ is closed, contains the identity element, has inverses for all its elements, and is commutative, it is a subgroup of $(\mathbb{R}, \circ)$.

Solution 3.6.

1.

2. ***To show that $Z(G)$ is a subgroup of G, we need to verify the following properties:***

   - ***Closure:*** *Let $x, z \in Z(G)$. We need to show that $x \cdot z \in Z(G)$, i.e., $(x \cdot z) \cdot y = y \cdot (x \cdot z)$ for all $y \in G$.*
     Since $x \in Z(G)$ and $z \in Z(G)$, we have:

     $$x \cdot y = y \cdot x \quad \text{and} \quad z \cdot y = y \cdot z \quad \text{for all } y \in G.$$

     Now, for $x \cdot z$, we compute:

     $$(x \cdot z) \cdot y = x \cdot (z \cdot y) = x \cdot (y \cdot z) = (x \cdot y) \cdot z = (y \cdot x) \cdot z = y \cdot (x \cdot z),$$

     which shows that $x \cdot z \in Z(G)$. Thus, $Z(G)$ is closed under the group operation.
   - ***Identity element:*** *The identity element $e \in G$ satisfies $e \cdot y = y \cdot e = y$ for all $y \in G$. Since the identity element commutes with every element of G, we have $e \in Z(G)$.*
   - ***Inverses:*** *Let $x \in Z(G)$. We need to show that the inverse of x, denoted x^{-1}, is also in $Z(G)$. Since $x \in Z(G)$, we know that $x \cdot y = y \cdot x$ for all $y \in G$.*
     To show that $x^{-1} \in Z(G)$, we compute:

     $$x^{-1} \cdot y = (x \cdot x^{-1}) \cdot y = x \cdot (x^{-1} \cdot y) = (x \cdot y) \cdot x^{-1} = y \cdot x^{-1} \quad \text{for all } y \in G.$$

     Thus, $x^{-1} \in Z(G)$, and every element of $Z(G)$ has an inverse in $Z(G)$.

   Therefore, $Z(G)$ is a subgroup of G.

3. ***Show that G is commutative if and only if $Z(G) = G$.***

- ***If** G **is commutative, then** $Z(G) = G$**:***

  If G is commutative, then for all $x, y \in G$, we have $x \cdot y = y \cdot x$. Thus, every element of G commutes with every other element of G, which means that $Z(G) = G$.

- ***If** $Z(G) = G$**, then** G **is commutative:***

  If $Z(G) = G$, then every element $x \in G$ commutes with every element $y \in G$, i.e., $x \cdot y = y \cdot x$ for all $x, y \in G$. This means that G is commutative.

Therefore, G is commutative if and only if $Z(G) = G$.

Solution 3.7.

1. ***Show that** f_a **is an endomorphism of the group** $(G, \cdot)$.*

   To show that f_a is an endomorphism of G, we need to check that f_a preserves the group operation. That is, we need to verify that for all $x, y \in G$,

   $$f_a(x \cdot y) = f_a(x) \cdot f_a(y).$$

   Compute both sides:

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

   On the other hand:

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

   Using the associativity of the group operation:

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

   Hence, we have:

   $$f_a(x \cdot y) = f_a(x) \cdot f_a(y).$$

   Therefore, f_a is an endomorphism of G.

2. ***Verify that for all** $a, b \in G$**,** $f_a \circ f_b = f_{a \cdot b}$.*

   We want to show that $f_a \circ f_b = f_{a \cdot b}$, i.e., for all $x \in G$,

   $$f_a(f_b(x)) = f_{a \cdot b}(x).$$

First, compute $f_a(f_b(x))$*:*

$$f_b(x) = b \cdot x \cdot b^{-1},$$

so

$$f_a(f_b(x)) = a \cdot (b \cdot x \cdot b^{-1}) \cdot a^{-1} = (a \cdot b) \cdot x \cdot (a \cdot b)^{-1}.$$

Now, compute $f_{a \cdot b}(x)$*:*

$$f_{a \cdot b}(x) = (a \cdot b) \cdot x \cdot (a \cdot b)^{-1}.$$

Therefore, we have:

$$f_a(f_b(x)) = f_{a \cdot b}(x).$$

Thus, $f_a \circ f_b = f_{a \cdot b}$*.*

3. ***Show that*** f_a ***is bijective and determine its inverse function.***

   To show that f_a *is bijective, we need to prove that it is both injective and surjective.*

   - ***Injectivity:*** *To show that* f_a *is injective, we need to prove that if* $f_a(x) = f_a(y)$*, then* $x = y$*. Suppose:*

     $$f_a(x) = f_a(y) \quad \Rightarrow \quad a \cdot x \cdot a^{-1} = a \cdot y \cdot a^{-1}.$$

     Multiply both sides by a^{-1} *on the left and* a *on the right:*

     $$a^{-1} \cdot (a \cdot x \cdot a^{-1}) \cdot a = a^{-1} \cdot (a \cdot y \cdot a^{-1}) \cdot a \quad \Rightarrow \quad x = y.$$

     Hence, f_a *is injective.*

   - ***Surjectivity:*** *To show that* f_a *is surjective, we need to prove that for every* $z \in G$*, there exists an* $x \in G$ *such that* $f_a(x) = z$*. We want to find* x *such that:*

     $$a \cdot x \cdot a^{-1} = z.$$

     Multiply both sides by a^{-1} *on the left and* a *on the right:*

     $$a^{-1} \cdot (a \cdot x \cdot a^{-1}) \cdot a = a^{-1} \cdot z \cdot a \quad \Rightarrow \quad x = a^{-1} \cdot z \cdot a.$$

     Therefore, for any $z \in G$*, we can find* $x = a^{-1} \cdot z \cdot a$ *such that* $f_a(x) = z$*. Hence,* f_a *is surjective.*

Since f_a is both injective and surjective, it is bijective.

To find the inverse of f_a, we need to find a function $f_{a^{-1}}$ such that:

$$f_{a^{-1}}(f_a(x)) = x \quad \textit{and} \quad f_a(f_{a^{-1}}(x)) = x.$$

We compute:

$$f_{a^{-1}}(f_a(x)) = f_{a^{-1}}(a \cdot x \cdot a^{-1}) = a^{-1} \cdot (a \cdot x \cdot a^{-1}) \cdot a = x.$$

Therefore, the inverse of f_a is $f_{a^{-1}}$, and we have:

$$f_a^{-1} = f_{a^{-1}}.$$

Solution 3.8.

1. ***Show that*** $(A, \star, \diamond)$ ***is a ring.*** *To show that $(A, \star, \diamond)$ is a ring, we need to verify the following properties:*

   - $\star$ *is associative.*
   - $\diamond$ *is associative.*
   - $\star$ *is commutative.*
   - $\diamond$ *is distributive over $\star$.*
   - 0 *is the identity element for $\star$.*
   - 1 *is the identity element for $\diamond$.*

   1. $\star$ is associative: *We need to show that $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in A$.*

   $$(a \star b) \star c = (a + b + 1) \star c = (a + b + 1) + c + 1 = a + b + c + 2.$$

   $$a \star (b \star c) = a \star (b + c + 1) = a + (b + c + 1) + 1 = a + b + c + 2.$$

   Since both sides are equal, $\star$ is associative.

   2. $\diamond$ is associative: *We need to show that $(a \diamond b) \diamond c = a \diamond (b \diamond c)$ for all $a, b, c \in A$.*

   $$(a \diamond b) \diamond c = (a \cdot b + a + b) \diamond c = (a \cdot b + a + b) \cdot c + (a \cdot b + a + b) + c.$$

Simplifying this:

$$= a \cdot b \cdot c + a \cdot c + b \cdot c + a + b + c.$$

Now compute $a \diamond (b \diamond c)$*:*

$$a \diamond (b \diamond c) = a \diamond (b \cdot c + b + c) = a \cdot (b \cdot c + b + c) + a + (b \cdot c + b + c).$$

Simplifying this:

$$= a \cdot b \cdot c + a \cdot b + a \cdot c + a + b \cdot c + b + c.$$

Re-arranging terms:

$$= a \cdot b \cdot c + a \cdot c + b \cdot c + a + b + c.$$

Hence, both sides are equal, so $\diamond$ *is associative.*

3. $\star$ ***is commutative:*** *We need to show that* $a \star b = b \star a$ *for all* $a, b \in A$*.*

$$a \star b = a + b + 1 \quad \textit{and} \quad b \star a = b + a + 1.$$

Since addition is commutative in A*, we have* $a \star b = b \star a$*, so* $\star$ *is commutative.*

4. Distributivity of $\diamond$ ***over*** $\star$***:*** *We need to show that* $a \diamond (b \star c) = (a \diamond b) \star (a \diamond c)$ *for all* $a, b, c \in A$*.*

$$a \diamond (b \star c) = a \diamond (b + c + 1) = a \cdot (b + c + 1) + a + (b + c + 1).$$

Simplifying:

$$= a \cdot b + a \cdot c + a + a + b + c + 1 = a \cdot b + a \cdot c + 2a + b + c + 1.$$

Now, compute $(a \diamond b) \star (a \diamond c)$*:*

$$(a \diamond b) = a \cdot b + a + b, \quad (a \diamond c) = a \cdot c + a + c.$$

$$(a \diamond b) \star (a \diamond c) = (a \cdot b + a + b) \star (a \cdot c + a + c) = (a \cdot b + a + b) + (a \cdot c + a + c) + 1.$$

Simplifying:

$$= a \cdot b + a \cdot c + a + a + b + c + 1 = a \cdot b + a \cdot c + 2a + b + c + 1.$$

Hence, $a \diamond (b \star c) = (a \diamond b) \star (a \diamond c)$*, so* $\diamond$ *is distributive over* $\star$*.*

5. Identity element for $\star$***:*** *We need to show that* 0 *is the identity element for* $\star$*.*

$$a \star 0 = a + 0 + 1 = a + 1 \quad \textit{and} \quad 0 \star a = 0 + a + 1 = a + 1.$$

So, 0 *is the identity element for* $\star$*.*

6. Identity element for $\diamond$***:*** *We need to show that* 1 *is the identity element for* $\diamond$*.*

$$a \diamond 1 = a \cdot 1 + a + 1 = a + a + 1 = 2a + 1 \quad \textit{and} \quad 1 \diamond a = 1 \cdot a + 1 + a = a + 1 + a = 2a + 1.$$

Thus, 1 *is the identity element for* $\diamond$*.*

Therefore, $(A, \star, \diamond)$ *is a ring.*

2. ***Show that the map*** $f : (A, +, \cdot) \to (A, \star, \diamond)$ ***given by*** $f(a) = a - 1$ ***is an isomorphism of rings.***

Solution: *We need to show that* f *is a ring isomorphism. This requires that:*

- f *is a homomorphism, i.e., it preserves both addition and multiplication.*
- f *is bijective.*

1. Homomorphism for $\star$***:*** *We need to show that* $f(a \star b) = f(a) \star f(b)$*. We compute:*

$$f(a \star b) = f(a + b + 1) = (a + b + 1) - 1 = a + b,$$

and

$$f(a) \star f(b) = (a - 1) \star (b - 1) = (a - 1) + (b - 1) + 1 = a + b - 1.$$

Since both sides are equal, f *preserves* $\star$*.*

2. Homomorphism for $\diamond$***:*** *We need to show that* $f(a \diamond b) = f(a) \diamond f(b)$*. We compute:*

$$f(a \diamond b) = f(a \cdot b + a + b) = a \cdot b + a + b - 1,$$

and

$$f(a) \diamond f(b) = (a-1) \diamond (b-1) = (a-1) \cdot (b-1) + (a-1) + (b-1).$$

Expanding this:

$$= a \cdot b - a - b + 1 + a - 1 + b - 1 = a \cdot b + a + b - 1.$$

Hence, f preserves $\diamond$.

3. Bijectivity: *The map $f(a) = a - 1$ is clearly bijective because it is a linear map with an inverse $f^{-1}(a) = a + 1$.*

Therefore, f is an isomorphism of rings.

Solution 3.9.
Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.

1. *Show that $(\mathbb{Z}[\sqrt{2}], +, \times)$ is a ring.*
2. *Let $N(a + b\sqrt{2}) = a^2 - 2b^2$.* ***Show that for all $x, y \in \mathbb{Z}[\sqrt{2}]$, we have $N(xy) = N(x)N(y)$.***
3. *Deduce that the invertible elements of $\mathbb{Z}[\sqrt{2}]$ are those of the form $a + b\sqrt{2}$ with $a^2 - 2b^2 = \pm 1$.*

Solution 3.10.

1. *It is sufficient to prove that $\mathbb{Z}[\sqrt{2}]$ is a subring of $(\mathbb{R}, +, \times)$. But $\mathbb{Z}[\sqrt{2}]$ is stable under the addition operation:*

$$(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2}.$$

It is also stable under multiplication:

$$(a + b\sqrt{2}) \times (a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2}.$$

It is stable under negation:

$$-(a + b\sqrt{2}) = -a + (-b)\sqrt{2}.$$

Moreover, $1 \in \mathbb{Z}[\sqrt{2}]$, which completes the proof that $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{R}$.

2. *Let $x = a + b\sqrt{2}$ and $y = a' + b'\sqrt{2}$. Using the formula for the product obtained in the previous question, we have:*

$$N(xy) = (aa' + 2bb')^2 - 2(ab' + a'b)^2 = (aa')^2 - 2(ab')^2 - 2(a'b)^2 + 4(bb')^2.$$

On the other hand,

$$N(x) \times N(y) = (a^2 - 2b^2)(a'^2 - 2b'^2) = (aa')^2 - 2(ab')^2 - 2(a'b)^2 + 4(bb')^2.$$

3. *Now, suppose $x = a + b\sqrt{2}$ is invertible with inverse y. Then, $N(xy) = N(1) = 1$, and therefore $N(x)N(y) = 1$. Since $N(x)$ and $N(y)$ are both integers, we must have $N(x) = \pm 1$. Conversely, if $N(x) = \pm 1$, then using the conjugate:*

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \pm(a - b\sqrt{2}),$$

which shows that $a + b\sqrt{2}$ is invertible with inverse $\pm(a - b\sqrt{2})$.

Solution 3.11.

We will begin by proving that $\mathbb{Q}(i)$ is a subring of $\mathbb{C}$. To do this, we observe that:

$$1 \in \mathbb{Q}(i)$$

If $z = a + bi$ and $z' = a + bi' \in \mathbb{Q}(i)$, then:

$$z - z' = (a - a') + i(b - b') \in \mathbb{Q}(i)$$

and

$$zz' = (a + bi)(a' + bi') = (aa' - bb') + i(ab' + a'b) \in \mathbb{Q}(i).$$

Next, let $z = a + bi \in \mathbb{Q}(i)$ with $z \neq 0$. Then:

$$\frac{1}{z} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} + i\frac{-b}{a^2 + b^2} \in \mathbb{Q}(i).$$

Thus, $\frac{1}{z}$ is in $\mathbb{Q}(i)$, and therefore every non-zero element of $\mathbb{Q}(i)$ has an inverse in $\mathbb{Q}(i)$. This completes the proof that $\mathbb{Q}(i)$ is a field.

Chapter 4

Rings of Polynomials

Introduction

Throughout this chapter we shall assume that $\mathbb{A}$ is a commutative ring with identity $1 \neq 0$.

4.1 Definitions

Definition 4.1.1.
Any expression of the form

$$P(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

where $a_i \in \mathbb{A}$ and $a_n \neq 0$, is called a polynomial over $\mathbb{A}$ with indeterminate x.

1. *The elements $a_0, a_1, \ldots, a_n$ are called the coefficients of P.*
2. *The coefficient a_n is called the **leading coefficient**.*
3. *A polynomial is called **monic** if the leading coefficient is 1.*
4. *If n is the largest nonnegative number for which $a_n \neq 0$, we say that the degree of P is n and write $\deg P(x) = n$.*
5. *If $f = 0$ is the zero polynomial, then the degree of P is defined to be $-\infty$.*

6. *We will denote the set of all polynomials with coefficients in a ring* $\mathbb{A}$ *by* $\mathbb{A}[x]$.

7. *Two polynomials are equal exactly when their corresponding coefficients are equal; that is, if we let*

$$p(x) = a_0 + a_1x + \cdots + a_nx^n$$

and

$$q(x) = b_0 + b_1x + \cdots + b_mx^m,$$

then $p(x) = q(x)$ *if and only if* $a_i = b_i$ *for all* $i \geq 0$.

To show that the set of all polynomials forms a ring, we must first define addition and multiplication. We define the sum of two polynomials as follows. Let

$$p(x) = a_0 + a_1x + \cdots + a_nx^n$$

and

$$q(x) = b_0 + b_1x + \cdots + b_mx^m.$$

Then the sum of $p(x)$ and $q(x)$ is

$$p(x) + q(x) = c_0 + c_1x + \cdots + c_kx^k,$$

where $c_i = a_i + b_i$ for each i. We define the product of $p(x)$ and $q(x)$ to be

$$p(x)q(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n},$$

where

$$c_i = \sum_{k=0}^{i} a_kb_{i-k} = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0.$$

for each i. Notice that in each case some of the coefficients may be zero.

Example 4.1.1.
Suppose that

$$p(x) = 3 + 0x + 0x^2 + 2x^3 + 0x^4$$

and

$$q(x) = 2 + 0x - x^2 + 0x^3 + 4x^4$$

are polynomials in $\mathbb{Z}[x]$. If the coefficient of some term in a polynomial is zero, then we usually just omit that term. In this case, we would write

$$p(x) = 3 + 2x^3 \quad \textit{and} \quad q(x) = 2 - x^2 + 4x^4.$$

The sum of these two polynomials is

$$p(x) + q(x) = 5 - x^2 + 2x^3 + 4x^4.$$

The product,

$$p(x)q(x) = (3 + 2x^3)(2 - x^2 + 4x^4) = 6 - 3x^2 + 4x^3 + 12x^4 - 2x^5 + 8x^7,$$

can be calculated either by determining the c_i's in the definition or by simply multiplying polynomials in the same way as we have always done.

Theorem 4.1.1.
Let $\mathbb{A}$ be a commutative ring with identity. Then $\mathbb{A}[x]$ is a commutative ring with identity.

Proof 4.1.1.
Our first task is to show that $\mathbb{A}[x]$ is an abelian group under polynomial addition. The zero polynomial, $f(x) = 0$, is the additive identity. Given a polynomial $p(x) = \sum_{i=0}^{n} a_i x^i$, the inverse of $p(x)$ is easily verified to be

$$-p(x) = \sum_{i=0}^{n} (-a_i)x^i = -\sum_{i=0}^{n} a_i x^i.$$

Commutativity and associativity follow immediately from the definition of polynomial addition and from the fact that addition in $\mathbb{A}$ is both commutative and associative.

To show that polynomial multiplication is associative, let

$$p(x) = \sum_{i=0}^{m} a_i x^i, \quad q(x) = \sum_{i=0}^{n} b_i x^i, \quad r(x) = \sum_{i=0}^{p} c_i x^i.$$

Then

$$\begin{aligned}
[p(x)q(x)]r(x) &= \left[\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right)\right]\left(\sum_{i=0}^{p} c_i x^i\right) \\
&= \left[\sum_{i=0}^{m+n}\left(\sum_{j=0}^{i} a_j b_{i-j}\right) x^i\right]\left(\sum_{i=0}^{p} c_i x^i\right)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=0}^{m+n+p} \left(\sum_{j=0}^{i} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) c_{i-j} \right) x^i \\
&= \sum_{i=0}^{m+n+p} \left(\sum_{j+k+l=i} a_j b_k c_l \right) x^i \\
&= \sum_{i=0}^{m+n+p} \left(\sum_{j=0}^{i} a_j \left(\sum_{k=0}^{i-j} b_k c_{i-j-k} \right) \right) x^i \\
&= \left(\sum_{i=0}^{m} a_i x^i \right) \left(\sum_{i=0}^{n+p} \left(\sum_{j=0}^{i} b_j c_{i-j} \right) x^i \right) \\
&= \left(\sum_{i=0}^{m} a_i x^i \right) \left[\left(\sum_{i=0}^{n} b_i x^i \right) \left(\sum_{i=0}^{p} c_i x^i \right) \right] \\
&= p(x)[q(x)r(x)].
\end{aligned}
$$

The commutativity and distribution properties of polynomial multiplication are proved in a similar manner. We shall leave the proofs of these properties as an exercise.

Proposition 4.1.1.
Let $p(x)$ and $q(x)$ be polynomials in $\mathbb{A}[x]$, where $\mathbb{A}$ is an integral domain. Then

1. $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$
2. $\deg(p(x) + q(x)) \leq \max(\deg(p(x)), \deg(q(x)))$

Furthermore, $\mathbb{A}[x]$ is an integral domain.

Proof 4.1.2.

1. *Suppose that we have two nonzero polynomials*

$$p(x) = a_m x^m + \cdots + a_1 x + a_0$$

and

$$q(x) = b_n x^n + \cdots + b_1 x + b_0$$

with $a_m \neq 0$ and $b_n \neq 0$. The degrees of p and q are m and n, respectively. The leading term of $p(x)q(x)$ is $a_m b_n x^{m+n}$, which cannot be zero since $\mathbb{A}$ is an integral domain; hence, the degree of $p(x)q(x)$ is $m+n$, and $p(x)q(x) \neq 0$.

Since $p(x) \neq 0$ and $q(x) \neq 0$ imply that $p(x)q(x) \neq 0$, we know that $\mathbb{A}[x]$ must also be an integral domain.

2. *Trivial.*

Let $\mathbb{U}(\mathbb{A})$ denote the units (invertible elements) of $\mathbb{A}$.

Proposition 4.1.2.
If $\mathbb{A}$ is an integral domain, then the units of $\mathbb{A}[X]$ are exactly the constant polynomials $P = a$ where $a \in \mathbb{U}(\mathbb{A})$.

Proof 4.1.3.
Let P be invertible in $\mathbb{A}[X]$. There exists $Q \in \mathbb{A}[X]$ such that $PQ = 1$. Thus, $\deg(P) + \deg(Q) = 0$ implies $\deg(P) = \deg(Q) = 0$. Hence, P and Q are constant invertible elements.

4.2 Polynomial Arithmetic

4.2.1 Associated Polynomials

Definition 4.2.1.
Two polynomials P and Q in $\mathbb{A}[X]$ are said to be associated if there exists $a \in \mathbb{U}(\mathbb{A})$ such that $P = aQ$.

Example 4.2.1.
The set of polynomials associated with $X^2 + 1$ in $\mathbb{Z}[X]$ is

$$\{X^2 + 1, -(X^2 + 1)\}$$

since the only units in $\mathbb{Z}$ are 1 and -1.

Proposition 4.2.1.

1. *The relation "being associated" is an equivalence relation on $\mathbb{A}[X]$.*
2. *If P and Q are associated and have the same leading coefficient, then $P = Q$.*
3. *If $\mathbb{A}$ is a field, then every polynomial P is associated with a unique unitary polynomial.*

4.2.2 Division

Definition 4.2.2.
Let $P, Q \in \mathbb{A}[X]$. We say that P divides Q, denoted as $P|Q$, if there exists $R \in \mathbb{A}[X]$ such that $Q = PR$.

Example 4.2.2.

1. *The polynomial $X - 1$ divides $X^2 - 1$ in $\mathbb{Z}[X]$.*
2. *The polynomial $X - 3$ does not divide $X^2 - 1$ in $\mathbb{Z}[X]$.*

Proposition 4.2.2.
Let $P, Q, R, S \in A[X]$.

1. *If $P|Q$ and $Q|R$, then $P|R$.*
2. *If $P|Q$ and $P|R$, then $P|(Q + R)$.*
3. *If $P|Q$ and $Q \neq 0$, then $\deg(P) \leq \deg(Q)$.*
4. *If $P|Q$ and $R|S$, then $PR|QS$.*
5. *If $P|Q$, then $P^n|Q^n$ for all $n \geq 1$.*

Proposition 4.2.3.
Let $P, Q, R, S \in A[X]$.

1. *If $P|Q$ and $Q|P$, then P and Q are associated.*
2. *If P is associated with R and Q is associated with S, then $P|Q \iff R|S$.*

4.2.3 Euclidean Division

Theorem 4.2.1. *(Euclidean Division)*
Let $A, B \in \mathbb{K}[X]$ be two polynomials with coefficients in a field $\mathbb{K}$ such that $B \neq 0$. Then there exists a unique pair (Q, R) of $\mathbb{K}[X]$ such that $A = BQ + R$ and $\deg(R) < \deg(B)$.

Example 4.2.3.
Let $A = x^3 + x + 1$ and $B = x + 1$. Then we have $A = B(x^2 - x + 2) - 1$.

Recall that a subset I of a ring $\mathbb{A}$ is an ideal if the following two conditions hold:

1. $(I, +)$ is a subgroup of $(A, +)$,
2. For every $a \in A$, $aI \subset I$. In other words, for all $a \in A$ and $x \in I$, $ax \in I$.

Theorem 4.2.2.
The ring $\mathbb{K}[X]$ is principal (In other words, every ideal $I \subseteq \mathbb{K}[X]$ can be written as $I = (P(X))$ for some $P(X) \in \mathbb{K}[X]$).

Proof 4.2.1.
Let I be an ideal of $\mathbb{K}[X]$ containing a nonzero polynomial. We want to show that I is principal, i.e., there exists a polynomial P such that I is exactly the set of multiples of P. Let $D = \{\deg(S) \mid S \in I, S \neq 0\}$. This is a non-empty subset of $\mathbb{N}$, so it has a minimum n. Let P be a polynomial of degree n in I. Since I is an ideal, all multiples of P are in I. Conversely, we want to show that every element of I is a multiple of P. So let $A \in I$. We know there exist Q, R such that $A = PQ + R$ with $\deg(R) < n$. Since $-PQ \in I$, we have $R = A - PQ \in I$. As $\deg(R) < n$, by the definition of n, we have $R = 0$, i.e., $A = PQ$, and A is indeed a multiple of P.

4.2.4 Irreducible Polynomials

Recall that the invertible polynomials in $\mathbb{A}[X]$ are the constant polynomials $P = a \in \mathbb{U}(A)$. Thus, since all non-zero elements in a field are invertible, the invertible polynomials in $\mathbb{K}[X]$ are the non-zero constant polynomials.

Definition 4.2.3.
A polynomial $P \in \mathbb{K}[X]$ is called irreducible if it is not invertible and if the equality $P = QR$ implies that either Q or R is invertible.

We say that a polynomial P is reducible if it is not irreducible.

Example 4.2.4.

1. *The polynomial $P(X) = 3$ is invertible in $\mathbb{Q}[X]$, so it is not irreducible.*
2. *The polynomial $P(X) = X^2 + 1$ is irreducible if we consider it as an element of $\mathbb{R}[X]$, but it is reducible if we consider it as an element of $\mathbb{C}[X]$, because $X^2 + 1 = (X - i)(X + i)$.*

The notion of irreducible polynomials depends on the field $\mathbb{K}$.

Proposition 4.2.4.

1. *Reducible polynomials in* $\mathbb{K}[X]$ *have degree greater than or equal to* 2.
2. *All polynomials of degree* 1 *are irreducible.*

4.2.5 Greatest Common Divisor

Let $P_1, ..., P_n \in \mathbb{K}[X]$. Since $\mathbb{K}[X]$ is principal, the ideal

$$< P_1, ..., P_n >= \{P_1A_1 + P_2A_2 + \cdots + P_nA_n \mid A_1, A_2, \ldots, A_n \in \mathbb{K}[X]\}.$$

is generated by a unique unit polynomial P. This polynomial is called the **greatest common divisor** *gcd* of P_i and is denoted

$$P = \gcd(P_1, ..., P_n).$$

Proposition 4.2.5. ***Properties of*** *gcd*
Let $P, Q \in \mathbb{K}[X]$. *Then*

1. $\gcd(P, Q)$ *is a common divisor of* P *and* Q.
2. *If* D *is another common divisor of* P *and* Q, *then* D *divides* $\gcd(P, Q)$.
3. *There exist polynomials* $(U, V) \in \mathbb{K}[X]^2$ *such that*

$$PU + QV = \gcd(P, Q).$$

Definition 4.2.4.
Let $P, Q \in \mathbb{K}[X]$. *We say that* P *and* Q *are coprime if* $\gcd(P, Q) = 1$.

In other words, if $\gcd(P, Q) = 1$, then only non-zero constants divide both P and Q.

4.2.6 Factorization

Theorem 4.2.3.
Let $P \in \mathbb{K}[X]$ be a non-zero polynomial. Then P decomposes uniquely up to the order of factors as:

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

where P_i are distinct, unit, irreducible polynomials in $\mathbb{K}[X]$ and $\alpha \in \mathbb{K}^*$ is the leading coefficient of P.

Example 4.2.5.
Consider the polynomial $P = x^2 + 1$. Then P exists in both $\mathbb{R}[X]$ and $\mathbb{C}[X]$. However, care must be taken as its factorization differs in these two rings:

1. *P factors as $(X - i) \cdot (X + i)$ in $\mathbb{C}[X]$.*
2. *P is irreducible in $\mathbb{R}[X]$.*

Proposition 4.2.6.
Let P and Q be two non-zero polynomials. Let $P = aP_1^{\alpha_1} P_2^{\alpha_2} ... P_n^{\alpha_n}$ and $Q = bP_1^{\beta_1} P_2^{\beta_2} ... P_n^{\beta_n}$ be their decompositions into irreducible factors where $\alpha_i, \beta_i \geq 0$ for all $i \in \{1, ..., n\}$. Then

$$P \text{ divides } Q \Leftrightarrow \alpha_j \leq \beta_j \text{ for all } 1 \leq j \leq n$$

.

4.3 Polynomial Functions

Let $P \in \mathbb{K}[X]$. We denote by f_P the polynomial function associated with P, defined as:

$$\begin{aligned} f_P : \mathbb{K} &\longrightarrow \mathbb{K} \\ x &\mapsto P(x). \end{aligned}$$

Definition 4.3.1.
Let $P \in \mathbb{K}[X]$. We say that $x \in \mathbb{K}$ is a root of P if $f_P(x) = 0$ (or $P(x) = 0$).

Proposition 4.3.1.
Let $P \in \mathbb{K}[X]$ and $\alpha \in \mathbb{K}$. Then α is a root of P if and only if the polynomial $(x - \alpha)$ divides P.

Definition 4.3.2.
Let $P \in \mathbb{K}[X]$ and let α be a root of P. We say that α has multiplicity k if and only if $(x-\alpha)^k$ divides P and $(x-\alpha)^{k+1}$ does not divide P.

In other words, α is a root of P of multiplicity k if and only if
$P = (x-\alpha)^k Q$ and $Q(\alpha) \neq 0$.

Example 4.3.1.
To determine the multiplicity of a root, we can perform successive Euclidean divisions. Let $P = x^3 - 3x^2 + 4$. It can be verified easily that 2 is a root of P. Furthermore, we find $P(x) = (x-2)^2 Q(x)$ with $Q(x) = x + 1$ and $Q(2) \neq 0$.

Theorem 4.3.1.
Let $P \in \mathbb{K}[X]$ and $\alpha_1, ..., \alpha_r$ be pairwise distinct roots of multiplicative $k_1, ..., k_r$, respectively. Then, there exists $Q \in \mathbb{K}[X]$ such that

$$P = (x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}...(x-\alpha_r)^{k_r} Q$$

and $Q(\alpha_i) \neq 0$ for all i. In particular, P has a degree of at least $k_1 + ... + k_r$.

4.4 Exercises

Exercice 4.1.
Find the polynomial P of degree less than or equal to 3 such that: $P(0) = 1$, $P(1) = 0$, $P(-1) = -2$, and $P(2) = 4$.

Exercice 4.2.
Perform the Euclidean division of A by B for the following cases:

1. *$A = 3X^5 + 4X^2 + 1$ and $B = X^2 + 2X + 3$.*
2. *$A = 3X^5 + 2X^4 - X^2 + 1$ and $B = X^3 + X + 2$.*
3. *$A = X^4 - X^3 + X - 2$ and $B = X^2 - 2X + 4$.*

Exercice 4.3.
Let $P, Q, R, S \in A[X]$.

1. *If $P|Q$ and $Q|R$ then $P|R$.*

2. *If* $P|Q$ *and* $P|R$ *then* $P|Q+R$.

3. *If* $P|Q$ *and* $Q \neq 0$ *then* $\deg(P) \leq \deg(Q)$.

4. *If* $P|Q$ *and* $R|S$ *then* $PR|QS$.

5. *If* $P|Q$ *then* $P^n|Q^n$ *for all* $n \geq 1$.

Exercice 4.4.
Let $P, Q, R, S \in A[X]$.

1. *If* $P|Q$ *and* $Q|P$ *then* P *and* Q *are associated.*

2. *If* P *is associated to* R *and* Q *is associated to* S *then* $P|Q \Leftrightarrow R|S$.

Exercice 4.5.
Find the gcd of the following polynomials:

1. $X^3 - X^2 - X - 2$ *and* $X^5 - 2X^4 + X^2 - X - 2$.

2. $X^4 + X^3 - 2X + 1$ *and* $X^3 + X + 1$.

Exercice 4.6.

1. *Reducible polynomials in* $\mathbb{K}[X]$ *have degree greater than or equal to* 2.

2. *All polynomials of degree* 1 *are irreducible.*

4.5 Exercise Solutions

Solution 4.1.
Let $P(x) = ax^3 + bx^2 + cx + d$.

Given:

$$P(0) = d = 1$$

So, $d = 1$.

$$P(1) = a + b + c + d = 0$$

Substitute $d = 1$*:*

$$a + b + c + 1 = 0 \Rightarrow a + b + c = -1$$

$$P(-1) = -a + b - c + d = -2$$

Substitute $d = 1$*:*

$$-a + b - c + 1 = -2 \Rightarrow -a + b - c = -3$$

$$P(2) = 8a + 4b + 2c + d = 4$$

Substitute $d = 1$*:*

$$8a + 4b + 2c + 1 = 4 \Rightarrow 8a + 4b + 2c = 3$$

Now solve the system of equations:

From $a + b + c = -1$ *and* $-a + b - c = -3$*: Add these equations:*

$$2b = -4 \Rightarrow b = -2$$

Substitute $b = -2$ *into* $a + b + c = -1$*:*

$$a - 2 + c = -1 \Rightarrow a + c = 1$$

Substitute $b = -2$ *into* $8a + 4b + 2c = 3$*:*

$$8a - 8 + 2c = 3 \Rightarrow 8a + 2c = 11$$

Now solve $a + c = 1$ *and* $8a + 2c = 11$*:*

Multiply $a + c = 1$ *by 2:*

$$2a + 2c = 2$$

Subtract from $8a + 2c = 11$*:*

$$6a = 9 \Rightarrow a = \frac{3}{2}$$

Substitute $a = \frac{3}{2}$ *into* $a + c = 1$*:*

$$\frac{3}{2} + c = 1 \Rightarrow c = -\frac{1}{2}$$

So, $a = \frac{3}{2}$, $b = -2$, $c = -\frac{1}{2}$, $d = 1$.

Therefore, the polynomial $P(x)$ *is:*

$$P(x) = \frac{3}{2}x^3 - 2x^2 - \frac{1}{2}x + 1$$

Solution 4.2.

1. *For* $A = 3X^5 + 4X^2 + 1$ *and* $B = X^2 + 2X + 3$*:*

$$Q = 3X^3,$$
$$R = -6X^2 + 1.$$

2. *For* $A = 3X^5 + 2X^4 - X^2 + 1$ *and* $B = X^3 + X + 2$*:*

$$Q = 3X^2 - X,$$
$$R = 2X^2 + X + 1.$$

3. *For* $A = X^4 - X^3 + X - 2$ *and* $B = X^2 - 2X + 4$*:*

$$Q = X^2,$$
$$R = -X^3 + 3X - 10.$$

Solution 4.3.

1. *Suppose $P \mid Q$ and $Q \mid R$. Then there exist polynomials $A(X), B(X), C(X) \in A[X]$ such that $Q = PA$ and $R = QB$. Substituting $Q = PA$ into $R = QB$, we get $R = P(AB)$, which implies $P \mid R$.*

2. *If $P \mid Q$ and $P \mid R$, then there exist polynomials $A(X), B(X) \in A[X]$ such that $Q = PA$ and $R = PB$. Therefore, $Q + R = PA + PB = P(A + B)$, which shows that $P \mid (Q + R)$.*

3. *Assume $P \mid Q$ and $Q \neq 0$. Then $Q = PA$ for some polynomial $A(X)$, implying $\deg(Q) = \deg(PA) = \deg(P) + \deg(A)$. Since $\deg(Q) \geq \deg(P)$, we conclude $\deg(P) \leq \deg(Q)$.*

4. *Given $P \mid Q$ and $R \mid S$, there exist polynomials $A(X), B(X), C(X), D(X) \in A[X]$ such that $Q = PA$ and $S = RC$. Therefore, $QS = (PA)(RC) = (PR)(AC)$, which means $PR \mid QS$.*

5. *If $P \mid Q$, then there exists a polynomial $A(X) \in A[X]$ such that $Q = PA$. Thus, $Q^n = (PA)^n = P^n A^n$, which shows $P^n \mid Q^n$ for all $n \geq 1$.*

Solution 4.4.

1. ***Part 1:***

   Claim: *If $P \mid Q$ and $Q \mid P$, then P and Q are associated.*

   Proof:

   If $P \mid Q$, then there exists $A \in A[X]$ such that $Q = P \cdot A$.

   If $Q \mid P$, then there exists $B \in B[X]$ such that $P = Q \cdot B$.

   Combining these, $Q = P \cdot A$ and substituting in $P = Q \cdot B$, we get $P = P \cdot A \cdot B$.

   Since $P \neq 0$, dividing by P gives $1 = A \cdot B$, implying A and B are units.

   Therefore, P and Q are associated.

2. ***Part 2:***

   Claim: *If P is associated to R and Q is associated to S, then $P \mid Q \iff R \mid S$.*

   Proof:

Assume $P = u \cdot R$ and $Q = v \cdot S$ for units $u, v \in A[X]$.

$P \mid Q$ implies $Q = P \cdot A$, so $Q = u \cdot R \cdot A$.

$R \mid S$ implies $S = R \cdot B$, so $Q = v \cdot S = v \cdot R \cdot B$.

Therefore, $P \mid Q \iff R \mid S$ because $u \cdot R \cdot A = v \cdot R \cdot B$ implies $u = v$ (since $R \neq 0$).

Solution 4.5.

1. *Let $P(X) = X^3 - X^2 - X - 2$ and $Q(X) = X^5 - 2X^4 + X^2 - X - 2$. Apply the Euclidean algorithm:*

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

Continuing this process, we find:

$$\gcd(P(X), Q(X)) = \frac{5}{2}X^2 - \frac{3}{2}X - 2.$$

Therefore, the gcd of $X^3 - X^2 - X - 2$ and $X^5 - 2X^4 + X^2 - X - 2$ is $\frac{5}{2}X^2 - \frac{3}{2}X - 2$.

2. *Let $R(X) = X^4 + X^3 - 2X + 1$ and $S(X) = X^3 + X + 1$. Apply the Euclidean algorithm:*

$$R(X) = S(X) \cdot X + (X^2 - 2X),$$
$$S(X) = (X^2 - 2X) \cdot X + (X + 1),$$
$$X^2 - 2X = (X + 1) \cdot (X - 2).$$

Thus,

$$\gcd(R(X), S(X)) = X + 1.$$

Therefore, the gcd of $X^4 + X^3 - 2X + 1$ and $X^3 + X + 1$ is $X + 1$.

Solution 4.6.

1. *Reducible polynomials in $\mathbb{K}[X]$ have degree greater than or equal to 2. Let $p(X)$ be a polynomial in $\mathbb{K}[X]$. Consider the cases when the degree of $p(X)$ is less than 2:*

- *If the degree is* 0*, then* $p(X)$ *is a constant polynomial. Constant polynomials are not considered reducible in the sense of factorization into non-constant polynomials.*
- *If the degree is* 1*, then* $p(X)$ *is of the form* $aX + b$*, where* $a \neq 0$*. Polynomials of degree* 1 *cannot be factored into smaller degree polynomials in* $\mathbb{K}[X]$*; hence, they are irreducible.*

Therefore, polynomials that are reducible must have a degree greater than or equal to 2*.*

2. *All polynomials of degree* 1 *are irreducible. A polynomial of degree* 1 *is of the form* $p(X) = aX + b$*, where* $a \neq 0$*. Such polynomials cannot be factored into polynomials of smaller degree in* $\mathbb{K}[X]$*, and hence they are irreducible.*

Bibliography

[1] M. Mignotte et J. Nervi, *Algèbre : licences sciences 1ère année*, Ellipses, Paris, 2004.

[2] J. Franchini et J. C. Jacquens, *Algèbre : cours, exercices corrigés, travaux dirigés*, Ellipses, Paris, 1996.

[3] C. Degrave et D. Degrave, *Algèbre 1ère année : cours, méthodes, exercices résolus*, Bréal, 2003.

[4] S. Balac et F. Sturm, *Algèbre et analyse : cours de mathématiques de première année avec exercices corrigés*, Presses Polytechniques et Universitaires romandes, 2003.

[5] T. W. Judson, F. Stephen, *Abstract Algebra: Theory and Applications*, Austin State University, Retrieved August 27, 2010.

[6] D. S. Dummit, R. M. Foote, *Abstract Algebra*, 3rd ed., John Wiley and Sons, 2004.

.