

People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

L'arbi Ben M'hidi Oum El Bouaghi University

Faculty of Exact Sciences and Natural and Life Sciences

Department of Mathematics

1st year university

Course:

Algebra 1

Produced by: **Yamina Soula**

University year: 2023-2024

People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research

L'arbi Ben M'hidi Oum El Bouaghi university

Faculty of Exact Sciences and Natural and Life Sciences

Department of mathematics

1st year university

Course:

Algebra 1

Produced by: Yamina Soula

University year: 2023-2024

Contents

1 Logic Notions **6**
- 1.1 Introduction . . . 6
- 1.2 Notions . . . 6
  - 1.2.1 Logical Operations . . . 6
  - 1.2.2 DeMorgan's Rules . . . 8
- 1.3 Quantifiers . . . 8
  - 1.3.1 Universal Quantifier ∀, or "for all" . . . 8
  - 1.3.2 Existential Quantifier ∃, or "there exists" . . . 9
  - 1.3.3 Negation of Quantifiers . . . 9
- 1.4 Types of Reasoning . . . 9
- 1.5 Exercises . . . 17
- 1.6 Solutions . . . 21

2 Sets and Applications **31**
- 2.1 Introduction . . . 31
- 2.2 Sets . . . 31
  - 2.2.1 Operations on Sets . . . 31
- 2.3 Applications . . . 33
  - 2.3.1 Direct Image, Inverse Image . . . 34
  - 2.3.2 Injection, surjection, bijection . . . 37
  - 2.3.3 Inverse function . . . 39
  - 2.3.4 Extension and Restriction . . . 41
- 2.4 Exercises . . . 43
- 2.5 Solutions . . . 44

3 Binary Relations on a Set **46**
- 3.1 Introduction . . . 46
- 3.2 Binary Relations . . . 46
- 3.3 Equivalence Relation . . . 47
- 3.4 Order Relation . . . 49
  - 3.4.1 Total or Partial Order . . . 49
  - 3.4.2 Least Element, Greatest Element . . . 50
  - 3.4.3 Upper Bound, Lower Bound . . . 50
  - 3.4.4 Infimum and Supremum . . . 51
- 3.5 Exercises . . . 52
- 3.6 Solutions . . . 53

4 Algebraic Structures **56**
- 4.1 Introduction . . . 56
- 4.2 Internal Composition Law . . . 56
- 4.3 Groups . . . 57
  - 4.3.1 Subgroups . . . 58
  - 4.3.2 Group Homomorphisms . . . 59
  - 4.3.3 The kernel and image of a homomorphism . . . 61
- 4.4 Ring Structure . . . 61
  - 4.4.1 Subring . . . 62
  - 4.4.2 Ring Homomorphisms . . . 62
  - 4.4.3 Zero Divisors, Invertible Elements . . . 62

4.4.4 Ideals . . . 63
4.5 Fields . . . 64
4.5.1 Subfields . . . 64
4.6 Exercises . . . 66
4.7 Solutions . . . 69

5 Polynomial Rings **76**
5.1 Introduction . . . 76
5.2 Polynomials, Degree, and Construction of Polynomial Rings . . . 76
5.3 Polynomial Arithmetic . . . 78
5.3.1 Euclidean Division . . . 78
5.3.2 Greatest Common Divisor "gcd" . . . 79
5.3.3 Bézout Identity . . . 79
5.3.4 Least Common Multiple . . . 80
5.3.5 Relation Between *gcd* and *lcm* . . . 80
5.4 Cancellation Law . . . 80
5.5 Remainder Theorem . . . 81
5.6 Factor Theorem . . . 81
5.7 Uniqueness of Euclidean Division . . . 81
5.8 Euclidean Algorithm . . . 82
5.9 Irreducible Polynomials . . . 82
5.10 Units in $A[x]$ . . . 83
5.11 Exercises . . . 84
5.12 Solutions . . . 85

6 Practice Exams with Detailed Solutions **88**
6.1 Introduction . . . 88
6.2 Five Solved Sample Exams . . . 88

Introduction

This document has been prepared as a course support for the module Algebra 1 and Mathematical Tools. It is primarily intended for first-year undergraduate students in mathematics, particularly those enrolled in the MI and ST tracks, as well as first-year students in the national biomedical engineering program. Its main objective is to provide students with the fundamental notions and algebraic techniques required for the study of higher mathematics and related scientific disciplines.

The preparation of this manuscript has been carried out in accordance with the official curriculum prescribed by the Ministry of Higher Education and Scientific Research. The content and organization of the chapters respect the pedagogical framework and learning objectives established for first-year university students. Particular attention has been devoted to presenting the material progressively and rigorously while maintaining clarity and accessibility for beginners encountering abstract mathematical reasoning for the first time.

The purpose of this document is not to replace standard reference textbooks in algebra, but rather to serve as a pedagogical support and a concise guide containing the essential concepts that every first-year student should master. In addition to the theoretical aspects of the course, emphasis has been placed on examples, applications, and solved exercises in order to strengthen students' understanding and develop their mathematical reasoning skills.

This manuscript is organized into six chapters covering the fundamental topics of introductory algebra and mathematical reasoning:

Chapter 1: Logic Notions

Chapter 2: Sets and Applications

Chapter 3: Binary Relations on a Set

Chapter 4: Algebraic Structures

Chapter 5: Polynomial Rings

Chapter 6: Previous Examinations with Detailed Solutions

The first chapter introduces mathematical logic and set theory, which constitute the basic language of modern mathematics and provide the necessary tools for formal reasoning and proof techniques. The second chapter is devoted to applications and binary relations defined on sets, including equivalence relations and order relations, which play a central role in many areas of mathematics.

The following chapters focus on the study of algebraic structures. In particular, groups, rings, integral domains, and polynomial rings are introduced progressively through definitions, properties, examples, and applications. Emphasis is placed on understanding both the abstract theory and the computational aspects of algebraic structures. Numerous solved exercises and additional problems are provided throughout the manuscript to help students develop their problem-solving skills and strengthen their understanding of the theoretical concepts presented in the course.

The sixth and final chapter is dedicated to a collection of previous examinations accompanied by detailed solutions. This chapter aims to familiarize students with the style and level of university examinations while providing them with effective guidance for revision and self-assessment. By working through these exams, students can reinforce their mastery of the course material, improve their methodological approach to problem solving, and gain confidence in preparing for assessments.

Historically, algebraic structures emerged naturally in different branches of mathematics and were not initially studied as independent objects. Over time, mathematicians recognized that many mathematical systems share common structural properties, leading to the development of abstract algebra as a unified field of study. Consequently, modern algebra establishes deep connections with several domains such as number theory, geometry, analysis, topology, physics, computer science, and engineering.

A large variety of algebraic structures satisfy different axiomatic systems, including groups, rings, fields, vector spaces, and modules. For each of these structures, mathematicians define appropriate notions of homomorphisms, substructures, quotient structures, and direct products. These concepts allow the comparison of algebraic systems and reveal important similarities between seemingly different mathematical objects. Furthermore, many fundamental properties are shared among these structures, such as closure properties, morphism

preservation, intersections of substructures, and quotient constructions.

For this reason, algebraic structures are introduced in a general and abstract framework that permits the unified treatment of common constructions and properties before focusing on the specific features of each structure individually. Such an approach not only simplifies mathematical reasoning but also enables students to develop a deeper understanding of abstraction and mathematical rigor.

Given the fundamental importance of algebra in modern mathematics and its applications, this first-year course mainly emphasizes the acquisition of general algebraic concepts, logical reasoning, and proof methods that will serve as indispensable tools throughout the students' academic training. It is hoped that this manuscript will provide students with a solid mathematical foundation and encourage them to pursue further studies in algebra and related mathematical sciences.

Chapter 1

Logic Notions

1.1 Introduction

Mathematical logic constitutes the foundation of all mathematical reasoning and proof techniques. It provides the basic language and methods used to formulate mathematical statements precisely and to determine their validity. In this chapter, we introduce the fundamental notions of logic, including propositions, logical connectives, quantifiers, and methods of reasoning. These concepts are essential tools for understanding and developing rigorous mathematical arguments throughout the study of algebra and other branches of mathematics.

1.2 Notions

Definition 1.2.1

- We call any relation P that is either true or false a "logical proposition".
- When the proposition is true, it is assigned the value 1.
- When the proposition is false, it is assigned the value 0.
- These values are called "Truth values of the proposition".

Example 1.2.2

r

1. "I am taller than you", is a proposition.
2. "$2 + 2 = 4$" is a proposition.
3. "$2 \times 3 = 7$" is a proposition.
4. "For all $x \in \mathbb{R}$; we have $x^2 \geq 0$" is a proposition.
5. "How are you today?" is not a proposition.

Thus, to define a logical proposition, it suffices to give its truth values. Generally, these values are put into a table called a "Truth table".

1.2.1 Logical Operations

Definition 1.2.3 Negation: "$\overline{P}$"

Given a logical proposition P, we call the negation of P the logical proposition $\overline{P}$, which is false when P is true and true when P is false, so we can represent it as follows:

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

Definition 1.2.4 Conjunction: "$\wedge$"

Let P and Q be two logical propositions, we call "conjunction" of P and Q the proposition "$P \wedge Q$ ", which is true when both P and Q are true and false otherwise. Its truth table:

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

Definition 1.2.5 Disjunction "$\vee$"

Let P and Q be two logical propositions, we call "disjunction" of P and Q the proposition "$P \vee Q$ ", which is true if either of the logical propositions P or Q is true. Its truth table:

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

Definition 1.2.6 Implication "$\Rightarrow$"

Consider two logical propositions P and Q, we denote "$P \Rightarrow Q$" the logical proposition that is false if P is true and Q is false. The proposition P $\Rightarrow$ Q reads "P implies Q ".

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

Given two logical propositions P and Q, the truth table of $\overline{P} \vee Q$ is as follows:

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

We see that this table is identical to that of $P \Rightarrow Q$, so we say that the proposition $P \Rightarrow Q$ is equivalent to the proposition $\overline{P} \vee Q$:

Definition 1.2.7 Equivalence "$\Leftrightarrow$"

We say that the two logical propositions P and Q are logically equivalent if they are true simultaneously or false simultaneously, and we denote "$P \Leftrightarrow Q$ ", its truth table is:

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

1.2.2 DeMorgan's Rules

Proposition 1.2.8

Let P and Q be two logical propositions, then:

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

Proof

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

1.

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

2.

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

1.3 Quantifiers

1.3.1 Universal Quantifier $\forall$, or "for all"

A proposition P may depend on a parameter x. For example: "$x^2 \geq 1$ " the assertion $P(x)$ is true or false depending on the value of x.

Definition 1.3.1

$\forall x \in E, P(x)$, is true when the propositions $P(x)$ are true for all elements x in the set E. We read "For all x belonging to E, $P(x)$".

Example 1.3.2

1. $\forall x \in [1; +\infty[$; $x^2 \geq 1$ is a true proposition.
2. $\forall x \in \mathbb{R}$; $x^2 \geq 1$ is a false proposition.

3. $\forall n \in \mathbb{N}$; $n(n+1)$ is divisible by 2 is true.

1.3.2 Existential Quantifier $\exists$, or "there exists"

Definition 1.3.3

$\exists x \in E; P(x)$, is true when we can find at least one x from E for which $P(x)$ is true. We read "there exists x belonging to E such that $P(x)$ is true".

Example 1.3.4

1. $\exists x \in \mathbb{R}$; $x(x-1) < 0$ is true.
2. $\exists n \in \mathbb{N}$;$n^2 - n > n$ is true.
3. $\exists x \in \mathbb{R}$; $x^2 = -4$ is false.

1.3.3 Negation of Quantifiers

Definition 1.3.5

1. The negation of "$\forall x \in E; P(x)$" is "$\exists x \in E; \overline{P(x)}$".
   For example, the negation of "$\forall x \in \mathbb{R}; x^2 \geq 1$ " is the assertion "$\exists x \in \mathbb{R}; x^2 < 1$".
2. The negation of "$\exists x \in E; P(x)$" is "$\forall x \in E; \overline{P(x)}$".
   For example, the negation of "$\exists n \in \mathbb{N}$; $n^2 - n > n$" is the assertion "$\forall n \in \mathbb{N}$; $n^2 - n \leq n$".
3. Negation of complex sentences: for example, the proposition "$\forall x \in E$, $\exists y \in E$; $P(x; y)$"
   its negation is "$\exists x \in E$, $\forall y \in E$; $\overline{P(x; y)}$".
   For example, the negation of "$\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$, $x + y > 0$" is "$\exists x \in \mathbb{R}$, $\forall y \in \mathbb{R}$, $x + y \leq 0$".

Note 1.3.6

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

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

and

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

are different.
The first one is true, the second one is false. Indeed, the first sentence asserts that "For every real number x, there exists a real number y (which may depend on x) such that $x + y > 0$" (for example, for a given x we can take $y = -x + 1$). So, it is a true sentence. On the other hand, the second one reads: "There exists a real number y, such that for every real number x, $x + y > 0$." This sentence is false, it cannot be the same y that works for all x.

1.4 Types of Reasoning

Definition 1.4.1 Direct Reasoning

We want to show that the proposition "$P \Rightarrow Q$" is true. We assume that P is true and then show that Q is true.

Example 1.4.2

Show that

$$\forall x, y \in \mathbb{R}^+, \quad x \leq y \Rightarrow x \leq \frac{x+y}{2} \leq y.$$

Proof

We have

$$x \leq y \Rightarrow x + x \leq x + y \Rightarrow 2x \leq x + y \Rightarrow x \leq \frac{x+y}{2}. \tag{1.1}$$

$$y \geq x \Rightarrow y + y \leq x + y \Rightarrow 2y \geq x + y \Rightarrow y \geq \frac{x+y}{2}. \tag{1.2}$$

From (1.1) and (1.2) we have:

$$x \leq \frac{x+y}{2} \leq y.$$

So

$$\forall x, y \in \mathbb{R}^+, \quad x \leq y \Rightarrow x \leq \frac{x+y}{2} \leq y,$$

is true.

Definition 1.4.3 Case by Case

If we want to verify a proposition $P(x)$ for all x in a set E, we show the proposition $P(x)$ for $x \in A \subset E$, and then for $x \notin A$.

Example 1.4.4

Show that: $\forall x \in \mathbb{R}; |x-1| \leq x^2 - x + 1$.

Proof

1. If

$$x \geq 1, \quad |x-1| = x - 1.$$

Then,

$$x^2 - x + 1 - |x-1| = x^2 - x + 1 - x + 1 = x^2 - 2x + 2 = (x-1)^2 + 1 \geq 0.$$

So

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

2. If

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

Then,

$$x^2 - x + 1 - |x-1| = x^2 - x + 1 - (-x+1) = x^2 - x + 1 + x - 1 = x^2 \geq 0.$$

So

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

Conclusion, in all cases

$$\forall x \in \mathbb{R}; |x-1| \leq x^2 - x + 1.$$

Definition 1.4.5 Contrapositive

Reasoning by "contraposition" is based on the following equivalence:

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

So, if we want to show the assertion "$P \Rightarrow Q$" we actually show that if $\overline{Q}$ is true. Then, $\overline{P}$ is true.

Example 1.4.6

Show that: $\forall n \in \mathbb{N}$; n^2 is even then n is even.

Proof

We want to show that if n is odd $\Rightarrow n^2$ is odd.
$\forall n \in \mathbb{N}$; n is odd, then there exists $k \in \mathbb{N}$ such that $n = 2k + 1$.
Then, $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2k^{'} + 1$. So, n^2 is odd.

Example 1.4.7

Shaw that by Contraposition:

1. If the product of two integers a and b, ab is odd, then both a and b are odd.
2. If x^2 is not divisible by 3, then x is not divisible by 3.

Proof

Proof by Contraposition:

Instead of proving directly, we prove the contrapositive:

1. If either a or b is even, then ab is even.

   Suppose a is even. Then $a = 2k$ for some integer k.

   Then

   $ab = (2k) \times b = 2(kb)$, which is divisible by 2, hence ab is even.

   Similarly, if b is even, the same reasoning applies.

   Therefore, if either

   a or b is even, ab is even.

   By contraposition, if ab is odd, then both a and b are odd.

2. If x is divisible by 3, then x^2 is divisible by 3.

   Suppose

   x is divisible by 3, so $x = 3k$ for some integer k.

   Then

   $x^2 = (3k)^2 = 9k^2 = 3 \times (3k^2)$, which is divisible by 3.

   Thus, if x is divisible by 3, then x^2 is divisible by 3.

   By contraposition, if

   x^2 is not divisible by 3, then x is not divisible by 3.

Definition 1.4.8 Absurd

Reasoning by "absurd" to show that "$P \Rightarrow Q$" is based on the following principle: we assume both that P is true and Q is false. We seek a contradiction. Thus if P is true then Q must be true and therefore "$P \Rightarrow Q$" is true.

Example 1.4.9

Show that: $\forall x, y \in \mathbb{R}^+$. If,

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

Then, $x = y$.

Proof

We assume that $\frac{x}{1+y} = \frac{y}{1+x}$ and $x \neq y$.

Since

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

Then,

$$x(1+x) = y(1+y).$$

So

$$x + x^2 = y + y^2.$$

Hence

$$x^2 - y^2 = -x + y.$$

So,

$$(x-y)(x+y) = -(x-y).$$

Since $x \neq y$. Then, $x - y \neq 0$ and so by dividing by $x - y$ we get $x + y = -1$ this is a contradiction(the sum of two positive numbers is positive). Conclusion, $\forall x, y \in \mathbb{R}^+$. If,

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

Then, $x = y$.

Definition 1.4.10 Counterexample

By counterexample to show that "$\forall x \in E$; $P(x)$" is false. It suffices to find $x \in E$, such that $P(x)$ is false.

Example 1.4.11

Show that "every positive integer is the sum of three squares" is false.

Proof

Let's take a counterexample. Consider the integer $n = 7$, the squares less than 7 are 0; 1; 4 but 0+1+4 $\neq$ 7.

Definition 1.4.12 Recurrence

The principle of "recurrence" allows us to show that a proposition $P(n)$ depending on n, is true for all $n \in \mathbb{N}$. The proof by recurrence proceeds in three steps:

1. **Initialization**: we verify that $P(0)$ is true.
2. **Heredity**: we assume $n > 0$ given with $P(n)$ true. Then, we demonstrate that the proposition $P(n+1)$ at the next rank is true.
3. **Conclusion**: we recall that by the principle of recurrence $P(n)$ is true for all $n \in \mathbb{N}$.

Example 1.4.13

Show that

$$\forall n \in \mathbb{N}, \quad P(n) = \sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

Proof

1. Initialization: For $n = 0$, we have $0^2 = 0$. So, $P(0)$ is true.
2. Heredity: For $n > 0$, we assume that $P(n)$ is true, i.e

$$\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6},$$

is true, and we show that

$$P(n+1) = \sum_{k=0}^{n+1} k^2 = \frac{(n+1)(n+2)(2(n+1)+1)}{6} = \sum_{k=0}^{n+1} k^2 = \frac{(n+1)(n+2)(2n+3)}{6},$$

is true.

$P(n)$ is true so

$$\sum_{k=0}^{n} k^2 = 0^2 + 1^2 + 2^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

We have:

$$\begin{aligned}
\sum_{k=0}^{n+1} k^2 &= 0^2 + 1^2 + 2^2 + ... + n^2 + (n+1)^2, \\
&= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2, \\
&= \frac{(n+1)(n+2) + (2n+3)}{6}, \\
&= \frac{(n+1)(n+2)(2n+3)}{6}.
\end{aligned}$$

Hence $P(n+1)$ is true.

3. Conclusion,

$$\forall\, n \in \mathbb{N}, \quad \sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

Example 1.4.14

Prove that by recurrence

1. $2^n > n^2$ for all $n \geq 5$.
2. $3^n \geq 2n+1$ for all $n \geq 1$.
3. $n! > 2n$ for all $n \geq 4$.
4. $1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2n} = 2 - \frac{1}{2n}$ for all $n \geq 0$.

Proof

Proof by recurrence

1. $2^n > n^2$ for all $n \geq 5$.

   For $n = 5$, $2^5 = 32$, $5^2 = 25$, and $32 > 25$,

   so the base case holds.

   Inductive step: Assume for some

   $$n \geq 5,\ 2^n > n^2.$$

   We want to prove that:

   $$2^{n+1} > (n+1)^2$$

   Start from the left:

   $2^{n+1} = 2 \cdot 2^n > 2 \cdot n^2$ (by inductive hypothesis).

   It suffices to show that

   $2n^2 \geq (n+1)^2 = n^2 + 2n + 1$,

   or equivalently,

   $2n^2 - n^2 - 2n - 1 = n^2 - 2n - 1 \geq 0$.

   Check this inequality for

   $n \geq 5$:

   $n^2 - 2n - 1 = (n-1)^2 - 2 \geq 16 - 2 = 14 > 0$,

   so it holds.

   Therefore,

   $2^{n+1} > (n+1)^2$.

   By induction, the inequality holds for all $n \geq 5$.

2. $3^n \geq 2n+1$ for all $n \geq 1$.

   Base case: For $n = 1$,

   $3^1 = 3$, $2(1) + 1 = 3$,

   so equality holds.

   Inductive step: Assume for some

   $n \geq 1$

   $3^n \geq 2n + 1$.

   We want to prove that:

   $$3^{n+1} \geq 2(n+1) + 1 = 2n + 3.$$

   Start from the left:

$$3^{n+1} = 3 \cdot 3^n \geq 3(2n+1) = 6n+3$$

It suffices to show:

$$6n+3 \geq 2n+3$$

or

$$6n+3-2n-3 = 4n \geq 0,$$

which is true for all $n \geq 1$.

Thus,

$$3n+1 \geq 2(n+1)+1,$$

and by induction, the inequality holds for all $n \geq 1$.

3. $n! > 2n$ for all $n \geq 4$.

Base case: For $n = 4$,

$4! = 24, \qquad 2(4) = 8, \qquad 24 > 8,$

So the base case holds.

Inductive step: Assume for some $n \geq 4$,

$$n! > 2n$$

We want to prove that

$$(n+1)! > 2(n+1).$$

Starting from the left:

$$(n+1)! = (n+1)n! > 2n \cdot (n+1) > 2(n+1).$$

So,

$$(n+1)! > 2(n+1)\cdot$$

By induction, the inequality holds for all $n \geq 4$.

4. $1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2n} = 2 - \frac{1}{2n}$ for all $n \geq 0$.

Case case: For $n = 0$, left side is:

$$\frac{1}{2^0} = 1,$$

and right side is:

$$2 - \frac{1}{2^0} = 2 - 1 = 1,$$

so base case holds.

Inductive step: Assume for some

$n \geq 0$,

$$\sum_{i=0}^{n+1} \frac{1}{2^i} = 2 - \frac{1}{2^{n+1}}.$$

We want to prove:

$$\sum_{i=0}^{n+1} \frac{1}{2^i} = \sum_{i=0}^{n} \frac{1}{2^i} + \frac{1}{2^{n+1}} = 2 - \frac{1}{2^n} + \frac{1}{2^{n+1}}.$$

Simplify the right side:

$$2 - \frac{1}{2^n} + \frac{1}{2^{n+1}} = 2 - \frac{1}{2^n} + \frac{1}{2.2^n} = 2 - \frac{1}{2^n} + \frac{1}{2^{n+1}}$$

Rewrite the two fractions with denominator 2^{n+1}

$$-\frac{1}{2^n} + \frac{1}{2^{n+1}} = -\frac{2}{2^{n+1}} + \frac{1}{2^{n+1}} = -\frac{1}{2^{n+1}}$$

So the sum becomes:

$$2 - \frac{1}{2^{n+1}},$$

which is exactly what we wanted to prove.

Therefore, by induction, the formula holds for all $n \geq 0$

1.5 Exercises

Exercise 1.5.1

Consider the following four statements:

(a) $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y > 0$.
(b) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y > 0$.
(c) $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y > 0$.
(d) $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, y^2 > x$.

1. Are the statements a, b, c, d true or false? Provide their negations.
2. Let P, Q, and R be three statements. Verify by creating a truth table:
   (a) $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$,
   (b) $\overline{(P \Rightarrow Q)} \Leftrightarrow P \wedge \overline{Q}$.

Exercise 1.5.2

Let f function of $\mathbb{R}$ in $\mathbb{R}$. Translate the following expressions into quantifier terms:

1. f is bounded above.
2. f is bounded.
3. f is even.
4. f never equals zero.
5. f is periodic.
6. f is increasing.
7. f is not the zero function.
8. f attains all values in $\mathbb{N}$.

Exercise 1.5.3

Let f: $\mathbb{R} \to \mathbb{R}$. What is the difference in meaning between the two proposed statements?

1. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y = f(x)$ and $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, y = f(x)$.
2. $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}, y = f(x)$ and $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, y = f(x)$.
3. $\forall x \in \mathbb{R}, \exists M \in \mathbb{R}, f(x) \leq M$ and $\exists M \in \mathbb{R}, \forall x \in \mathbb{R}, f(x) \leq M$.

Exercise 1.5.4

Let f: $\mathbb{R} \to \mathbb{R}$ a continuous function. We consider the following assertions:

$$P : \text{"}\forall x \in \mathbb{R}, \quad f(x) = 0\text{"}.$$

$$Q; \text{"}\exists x \in \mathbb{R}, \quad f(x) = 0\text{"}.$$

$$R : \text{"}(\forall x \in \mathbb{R}, \quad f(x) > 0) \text{ or } (\forall x \in \mathbb{R}, \quad f(x) < 0)\text{"}.$$

Among the following implications, which ones are true?
a $P \Rightarrow Q$, **b** $Q \Rightarrow P$,
c $Q \Rightarrow R$, **d** $\overline{R} \Rightarrow Q$,
e $\overline{Q} \Rightarrow \overline{P}$, **f** $\overline{P} \Rightarrow \overline{R}$.

Exercise 1.5.5

1. Solve in $\mathbb{R}^2$ the system
$$\begin{cases} (x-1)(y-2)=0 \\ (x+1)(y+3)=0 \end{cases}$$
2. Prove that the statement
$$(\forall n \in \mathbb{N}^* \setminus \{1\} : 1+\frac{1}{2}+\frac{1}{3}+...+\frac{1}{n} \in \mathbb{N}) \text{ is false}$$

Exercise 1.5.6

1. Give negation of the following propositions:
   a) $\forall x \in \mathbb{R}, \quad 2x > x.$
   b) $\forall x \in \mathbb{R}, \quad x > 0 \Rightarrow \ 2x > x.$
   c) $\exists n \in \mathbb{N}, \quad 5n+11 = 3n+14.$
   d) $\forall \varepsilon \in \mathbb{R}, \quad (\varepsilon > 0) \Rightarrow (\exists n \in \mathbb{N}^* : \frac{1}{n} < \varepsilon)$
2. In the first three cases, indicate which one is true.

Exercise 1.5.7

Write the following sentences and negate them using quantifiers:

a) A : "For every two natural numbers a and b, there is a natural number c that satisfies $ac \neq bc$ or $a = b$."

b) B : "The sum of a rational number and an irrational number is an irrational number."

c) C : " If the sum and product of two real numbers belong to the set Q, then these two numbers belong to Q ".

d) D : " For each x and y of $\mathbb{R}$ we have $xy = 0$ is equivalent to $x = 0$ or $y = 0$."

Exercise 1.5.8

Are the following sentences true or false? Justify your answer.

a) P_1 : "$\forall y \in \mathbb{R}, \exists x \in \mathbb{R} : x - y = 1$"
b) P_2 : "$\exists x \in \mathbb{R}, \forall y \in \mathbb{R} : x - y = 1$"
c) P_3 : "$P_1 \Rightarrow P_2$ ".
d) P_4 : "$P_2 \Rightarrow P_1$ ".

Exercise 1.5.9

Consider the statement P : " $\forall n \in \mathbb{N}$, $(n+1)$odd $\Rightarrow$ n even."

1. Using absurd reasoning, prove that statement P is true.
2. Using counterfactual reasoning, prove that statement P is true.

Exercise 1.5.10

Using successive equivalence reasoning prove the following:

1. $\forall x \in \mathbb{R}_+^* : x + \frac{1}{x} \geq 2.$
2. $\forall x \in]-\infty, \ 1[: \frac{x^2}{x-1} \leq 4$

Exercise 1.5.11

Using case-by-case reasoning, prove the following:

1. $n(n+1)$ is an even number for all n in $\mathbb{N}$
2. $n\ (n+1)(n+2)$ is a multiple of 3 for all n in $\mathbb{N}$

Exercise 1.5.12

1. Show that the statement "$\forall (n,m) \in \mathbb{Z}^2 : (n+m=10) \Rightarrow (n=6 \vee m=4)$" is false.
2. Show that the statement "$\exists x \in \mathbb{R} : (x<1) \Rightarrow (1+x^2>2)$" is true.
3. Show that the statement "ABC is an isosceles triangle with a right angle at A. The measure of angle $\overset{\wedge}{ABC}$ is equal to $50°$ " is false.

Exercise 1.5.13

Prove by recurrence that:
For every natural number n greater than or equal to 12, there is at least a pair $(p,\ q)$ of $\mathbb{N}^2$ such that: $n = 3p + 2q$.

Exercise 1.5.14

Show by recurrence that:

1. $\forall n \in \mathbb{N}^\star$: $1^3 + 2^3 + ... + n^3 = \frac{n^2(n+1)^2}{4}$
2. $\forall n \in \mathbb{N}$, $4^n + 6n - 1$ is a multiple of 9.

Exercise 1.5.15

Show by recurrence

1. $$\forall n \geq 2, \frac{1}{\sqrt{4n+1}} < \frac{1.3.5...(2n-1)}{2.4.6...(2n)} < \frac{1}{\sqrt{3n+1}}$$
2. $$\forall n \geq 1, \quad \sum_{k=1}^{n} \sqrt{k} < \frac{4n+3}{6}\sqrt{n}$$

Exercise 1.5.16

By the absurd show that:

1. $\sqrt{2} \notin \mathbb{Q}$.
2. $\forall n \in \mathbb{N}$, n^2 even $\Rightarrow n$ is even.

Exercise 1.5.17

Prove by absurd that:

$$\forall x \in \mathbb{R}^+, \exists \in \mathbb{N} : x \leq n.$$

Exercise 1.5.18

By contrapositive, show that

1. If $(n^2 - 1)$ is not divisible by 8 then n is even.
2. $\forall \varepsilon > 0$, $|x| \leq \varepsilon \Rightarrow x = 0$.

1.6 Solutions

Solution 1.5.1

1. is false because its negation is $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ x+y \leq 0$, is true.

   let $x \in \mathbb{R}$, there exists $y \in \mathbb{R}$, such that $x+y \leq 0$, for example we can take $y=-(x+1)$ and then $x+y=x-x-1=-1 \leq 0$.

2. is true, for any given x for example we can take $y=-x+1$, and then $x+y=1 \geq 0$. Then negation of **2)** is $\exists x \in \mathbb{R};\ \forall y \in \mathbb{R};\ x+y \leq 0$:

3. is false for example $x=-1$, $y=0$. The negation is $\exists x \in \mathbb{R},\ \exists y \in \mathbb{R},\ x+y \leq 0$.

4. is true, we can take $x=-1$, the negation is $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ y^2 \leq x$.

5. Truth table:

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$ **(1)**	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$ **(2)**	**(1)** $\Leftrightarrow$ **(2)**
1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	1
1	1	0	1	0	0	0	0	1
1	0	1	1	1	1	0	1	1
0	1	1	1	1	0	1	1	1
1	0	0	1	0	0	0	0	1
0	1	0	1	0	0	0	0	1
0	0	1	0	0	0	0	0	1

6.

P	Q	$\overline{Q}$	$P \wedge \overline{Q}$	$P \Rightarrow Q$	$\overline{P \Rightarrow Q}$	$\overline{(P \Rightarrow Q)} \Leftrightarrow P \wedge \overline{Q}$
1	1	0	0	1	0	1
0	0	1	0	1	0	1
1	0	1	1	0	1	1
0	1	0	0	1	0	1

Solution 1.5.2

1. $\exists M \in \mathbb{R},\ \forall x \in \mathbb{R},\ f(x) \leq M$.
2. $\exists M \in \mathbb{R},\ \exists m \in \mathbb{R},\ \forall x \in \mathbb{R},\quad m \leq f(x) \leq M$.
3. $\forall x \in \mathbb{R},\ f(x)=f(-x)$.
4. $\forall x \in \mathbb{R},\ f(x) \neq 0$.
5. $\exists \alpha \in \mathbb{R}^*,\ \forall x \in \mathbb{R},\ f(x+\alpha)=f(x)$.
6. $\forall x \in \mathbb{R},\ \forall y \in \mathbb{R},\ x \leq y \Rightarrow f(x) \leq f(y)$.
7. $\exists x \in \mathbb{R},\ f(x) \neq 0$.
8. $\forall n \in \mathbb{N},\ \exists x \in \mathbb{R},\ f(x)=n$.

Solution 1.5.3

1. The first statement is verified by any function, the second one means that f is constant.
2. The first statement means that f takes every value in $\mathbb{R}$, the second one is absurd.
3. The first statement is always verified, the second one means that f is bounded.

Solution 1.5.4

Only the statements: **a)**, **d)**, **e)** are true. Because:

1. $(\forall x \in \mathbb{R}, f(x) = 0) \Rightarrow (\exists x \in \mathbb{R}, f(x) = 0)$.
2. $[(\exists x \in \mathbb{R}, f(x) \leq 0)\ et\ (\exists x \in \mathbb{R}, f(x) \geq 0)] \Rightarrow [\exists x \in \mathbb{R}, f(x) = 0]$.
3. $(\forall x \in \mathbb{R}, f(x) \neq 0) \Rightarrow (\exists x \in \mathbb{R}, f(x) \neq 0)$, (the contrapositive of 1).

Solution 1.5.5

1)

$$\begin{cases} (x-1)(y-2) = 0 \\ (x+1)(y+3) = 0 \end{cases} \Leftrightarrow (x-1)(y-2) = 0 \wedge (x+1)(y+3) = 0$$

$$\Leftrightarrow (x-1 = 0 \vee y-2 = 0) \wedge (x+1 = 0 \vee y+3) = 0$$

$$\Leftrightarrow (x = 1 \vee y = 2) \wedge (x = -1 \vee y = -3)$$

$$\Leftrightarrow (x = 1 \wedge x = -1) \vee (x = 1 \wedge y = -3) \vee (y = 2 \wedge x = -1) \vee (y = 2 \wedge y = -3)$$

Since Since $(x = 1 \wedge x = -1)$ and $(y = 2 \wedge y = -3)$ are both false statements, then

$$\begin{cases} (x-1)(y-2) = 0 \\ (x+1)(y+3) = 0 \end{cases} \Leftrightarrow (x = 1 \wedge y = -3) \vee (y = 2 \wedge x = -1)$$

$$\Leftrightarrow (x, y) = (1\ , -3) \vee (x, y) = (-1, 2)$$

then the set of solutions to the system is

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

2)

Show that this statement $(\forall n \in \mathbb{N}^* \setminus \{1\} : 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n} \in \mathbb{N})$ is false

It is sufficient to show that its negation is true

We have the negative of the statement is:

$(\exists n \in \mathbb{N}^* \setminus \{1\} : 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n} \notin \mathbb{N})$

Let $n = 2 \in \mathbb{N}^* \setminus \{1\}$.

We have: $1 + \frac{1}{2} = \frac{3}{2} \notin \mathbb{N}$

So, the statement

$(\exists n \in \mathbb{N}^* \setminus \{1\} : 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n} \notin \mathbb{N})$ is true.

Then the statement

$(\forall n \in \mathbb{N}^* \setminus \{1\} : 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n} \in \mathbb{N})$ is false.

Solution 1.5.6

1)

a) the negation is given by

$\exists x \in \mathbb{R} : 2x \leq x$.

b) the negation of proposition (b) is given by

$\exists x \in \mathbb{R} : x > 0 \wedge 2x \leq x$.

c) the negation is given by

$\forall n \in \mathbb{N},\quad 5n + 11 \neq 3n + 14$

d) the negation is given by

$\exists \varepsilon \in \mathbb{R} \quad \varepsilon > 0 \wedge \forall n \in \mathbb{N}^* : \frac{1}{n} \geq \varepsilon$

2)

proposition (**a**) is false because its negation is true.

proposition (**b**) is true. For the proof, we proceed as follows
let $x \in \mathbb{R}$,
suppose that $x > 0$ hence $2x = x + x > x$
this completes the proof
3)
proposition (**c**) is false. Solving the equation $5n + 11 = 3n + 14$
we find that the only solution is $n = \frac{3}{2}$, or $\frac{3}{2} \notin \mathbb{N}$
Therefore
$\forall n \in \mathbb{N} : \quad 5n + 11 \neq 3n + 14$
is true, or proposition " $\exists n \in \mathbb{N}, \quad 5n + 11 = 3n + 14$" is false.

Solution 1.5.7

a) A **:** "$\forall\ a \in \mathbb{N}, \forall\ b \in \mathbb{N}\ , \exists\ c \in \mathbb{N} :\ ac \neq bc \vee a = b.$**".**
Or
A **:** "$\forall\ (a, b) \in \mathbb{N}^2\ , \exists\ c \in \mathbb{N} :\ ac \neq bc \vee a = b.$**".**
its negation is: "$\exists\ a \in \mathbb{N}, \exists\ b \in \mathbb{N}\ , \forall\ c \in \mathbb{N} :\ ac = bc \wedge a \neq b.$**".**

b) B **:** "$\forall\ x \in \mathbb{Q}, \forall\ y \in \mathbb{R} \setminus \mathbb{Q}\ , x + y \in \mathbb{R} \setminus \mathbb{Q}$ **".**
its negation is: "$\exists x \in \mathbb{Q}, \exists\ y \in \mathbb{R} \setminus \mathbb{Q}\ , x + y \notin \mathbb{R} \setminus \mathbb{Q}$ **".**

c) C **:** "$\forall\ (x, y) \in \mathbb{R}^2, (x + y \in \mathbb{Q} \wedge xy \in \mathbb{Q}) \Longrightarrow (x \in \mathbb{Q} \wedge y \in \mathbb{Q})$**".**
its negation is: " $\exists\ (x, y) \in \mathbb{R}^2, (x + y \in \mathbb{Q} \wedge xy \in \mathbb{Q}) \wedge (x \notin \mathbb{Q} \vee y \notin \mathbb{Q})$"

d) D **:** "$\forall\ (x, y) \in \mathbb{R}^2, (xy = 0) \Leftrightarrow (x = 0 \vee y = 0)$**".**
its negation is:
We know that: $P \Leftrightarrow Q$ means $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ i.e. $(P \vee \overline{Q}) \wedge (Q \vee \overline{P})$
So that, the negation of D is: "$\exists\ (x, y) \in \mathbb{R}^2, (xy = 0 \wedge (x \neq 0 \wedge y \neq 0)) \vee ((x = 0 \vee y = 0) \wedge xy \neq 0)$**".**

Solution 1.5.8

a) P_1 **:** "$\forall y \in \mathbb{R}, \exists x \in \mathbb{R} : x - y = 1$"
Let $y \in \mathbb{R}$,
The equation $x - y = 1$ with the unknown x is equivalent to $x = y + 1$.
Since 1 and y are in $\mathbb{R}$, then $x \in \mathbb{R}$.
So, "$\forall y \in \mathbb{R}, \exists x = y + 1 \in \mathbb{R} : x - y = 1$**".**
Then the statement $\mathbf{P_1}$ is true**.**

b) P_2 **:** "$\exists x \in \mathbb{R}, \forall y \in \mathbb{R} : x - y = 1$"
Suppose there is $x \in \mathbb{R}$ such that for each $y \in \mathbb{R}$
$x - y = 1$
We take $x = y$
Then,
$x - y = x - x = 0 \neq 1$
Therefore, statement $\mathbf{P_2}$ is incorrect
i.e., $\mathbf{P_2}$ is false

c) P_3 **:** "$P_1 \Rightarrow P_2$ ".

Know that statement P_1 is true and statement P_2 is false.

So, the statement "$P_1 \Rightarrow P_2$ " is false.

d) P_4 **:** "$P_2 \Rightarrow P_1$ ".

Know that statement P_2 is false and statement P_1 is true.

So, the statement "$P_2 \Rightarrow P_1$ " is true.

Solution 1.5.9

Let the statement P : " $\forall n \in \mathbb{N}$, $(n+1)$odd $\Rightarrow$ n even."

1) Show that P is true using deductive reasoning.

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

$(n+1)$odd $\Rightarrow \exists k \in \mathbb{N} : n+1 = 2k+1$

$\Rightarrow \exists k \in \mathbb{N} : n = 2k$

$\Rightarrow n$ even

So, the statement P is true.

2) Show that P is true using counterfactual reasoning.

Meaning we show that,

" $\forall n \in \mathbb{N}$, n is not even $\Rightarrow$ $(n+1)$ is not odd."

or

" $\forall n \in \mathbb{N}$, n is odd $\Rightarrow$ $(n+1)$ is even."

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

n is odd $\Rightarrow \exists k \in \mathbb{N} : n = 2k+1$

$\Rightarrow \exists k \in \mathbb{N} : n+1 = 2k+2$

$\Rightarrow \exists k \in \mathbb{N} : n+1 = 2(k+1)$

$\Rightarrow (n+1)$ is even

So, the statement P is true.

Solution 1.5.10

Using successive equivalences, show that

1) $\forall x \in \mathbb{R}_+^* : x + \frac{1}{x} \geq 2$?.

$\forall x \in \mathbb{R}_+^* : x + \frac{1}{x} \geq 2 \Leftrightarrow \forall x \in \mathbb{R}_+^*, \frac{x^2+1}{x} \geq 2.$

$\Leftrightarrow \forall x \in \mathbb{R}_+^*, x^2 + 1 \geq 2x$ (puisque $x > 0$)

$\Leftrightarrow \forall x \in \mathbb{R}_+^*, x^2 - 2x + 1 \geq 0$

$\Leftrightarrow \forall x \in \mathbb{R}_+^*, (x-1)^2 \geq 0$

So, $\forall x \in \mathbb{R}_+^* : x + \frac{1}{x} \geq 2 \Leftrightarrow \forall x \in \mathbb{R}_+^*, (x-1)^2 \geq 0.$

Since statement $\forall x \in \mathbb{R}_+^*, (x-1)^2 \geq 0$ is true, then,

$\forall x \in \mathbb{R}_+^* : x + \frac{1}{x} \geq 2$ is true.

2) $\forall x \in]-\infty, 1[: \frac{x^2}{x-1} \leq 4$?.

$\forall x \in]-\infty, 1[: \frac{x^2}{x-1} \leq 4 \Leftrightarrow \forall x \in]-\infty, 1[: x^2 \geq 4(x-1)$ (puisque $x < 1$)

$\Leftrightarrow \forall x \in]-\infty, 1[: x^2 - 4(x-1) \geq 0.$

$\Leftrightarrow \forall x \in]-\infty, 1[: x^2 - 4x + 4 \geq 0.$

$\Leftrightarrow \forall x \in]-\infty, 1[: x^2 - 2(2x) + 2^2 \geq 0.$

$\Leftrightarrow \forall x \in]-\infty, 1[: (x-2)^2 \geq 0.$

So, $\forall x \in]-\infty,\ 1[: \frac{x^2}{x-1} \leq 4 \Leftrightarrow \forall x \in]-\infty,\ 1[, (x-2)^2 \geq 0$.

Since statement $\forall x \in]-\infty,\ 1[, (x-2)^2 \geq 0$ is true, then,

$\forall x \in]-\infty,\ 1[: \frac{x^2}{x-1} \leq 4$ is true.

Solution 1.5.11

Reasoning by separating cases

1) We show that: $n(n+1)$ is an even number for all n in $\mathbb{N}$

• If n is even, then there existe $k \in \mathbb{N}$ such that: $n = 2k$

So, $n(n+1) = 2k(2k+1) = 2p$

such that $p = k(2k+1)$

as $k \in \mathbb{N}$ then $p \in \mathbb{N}$

So $n(n+1)$ is an even number

• If n is odd, then there existe $k \in \mathbb{N}$ such that: $n = 2k+1$

So, $n(n+1) = (2k+1)(2k+2) = 2(2k+1)(k+1) = 2p$

such that $p = (2k+1)(k+1)$

as $k \in \mathbb{N}$ then $p \in \mathbb{N}$

So $n(n+1)$ is an even number

Conclusion: $n(n+1)$ is an even number for every n in $\mathbb{N}$.

2) We show that: $n\ (n+1)(n+2)$ is a multiple of 3 for all n in $\mathbb{N}$

We have three cases:

• If $n = 3k$ such that $k \in \mathbb{N}$, then

$n\ (n+1)(n+2) = 3k\ (n+1)(n+2) = 3p$

such that $p = k\ (n+1)(n+2)$ is natural number.

So, $n\ (n+1)(n+2)$ is a multiple of 3.

• If $n = 3k\ +1$ such that $k \in \mathbb{N}$, then

$$n\ (n+1)(n+2) = n(n+1)(3k+1+2) = n(n+1)(3k+3) = 3n(n+1)(k+1) = 3p$$

such that $p = n(n+1)(k+1)$ is natural number.

So, $n\ (n+1)(n+2)$ is a multiple of 3.

• If $n = 3k\ +2$ such that $k \in \mathbb{N}$, then

$$n\ (n+1)(n+2) = n(3k+2+1)(n+2) = n(3k+3)(n+2) = 3n(k+1)(n+2) = 3p$$

such that $p = n(k+1)(n+2)$ is natural number.

So, $n\ (n+1)(n+2)$ is a multiple of 3.

Conclusion: $n\ (n+1)(n+2)$ is a multiple of 3 for every n in $\mathbb{N}$.

Solution 1.5.12

1) We show the statement "$\forall (n,m) \in \mathbb{Z}^2 : (n+m=10) \Rightarrow (n=6 \vee m=4)$" is false.

We show then that its negation "$\exists (n,m) \in \mathbb{Z}^2 : (n+m=10) \wedge (n \neq 6 \wedge m \neq 4)$" is true.

For $n = -15$ and $m = 25$ we have: $n+m = -15+25 = 10 \wedge (n = -15 \neq 6 \wedge m = 25 \neq 4)$

So, "$\exists (n,m) \in \mathbb{Z}^2 : (n+m=10) \wedge (n \neq 6 \wedge m \neq 4)$" is true.

Then,

"$\forall (n,m) \in \mathbb{Z}^2 : (n+m=10) \Rightarrow (n=6 \vee m=4)$" is false.

2) We show the statement "$\exists x \in \mathbb{R} : (x<1) \Rightarrow (1+x^2>2)$" is true.

For $x=-2\in\mathbb{R}$, $-2<1\Rightarrow 1+(-2)^2=1+4=5>2$.

So, the statement "$\exists x=-2\in\mathbb{R}:(x<1)\Rightarrow(1+x^2>2)$" is true.

3) We show the statement "ABC is an isosceles triangle with a right angle at A. The measure of angle $\overset{\wedge}{ABC}$ is equal to $50°$ " is false.

Assume the statement is true. So,

$\hat{A}=90°,\quad \hat{B}=\hat{C}=50°$ then

$\hat{A}+\hat{B}+\hat{C}=90°+50°+50°=190°$.

This contradicts the fact that the sum of the angles of a triangle equals $180°$.

So, the assumption is false

And from it the statement "ABC is an isosceles triangle with a right angle at A. The measure of angle $\overset{\wedge}{ABC}$ is equal to $50°$ " is false.

Solution 1.5.13

We prove by recurrence that:

For every natural number n greater than or equal to 12, there is at least a pair $(p,\,q)$ of $\mathbb{N}^2$ such that: $n=3p+2q$

i.e. $\forall n\in\mathbb{N}^*\setminus\{1,2,...,11\},\ \exists(p,\,q)\in\mathbb{N}^2:n=3p+2q$

For $n=12$, then

$12=3(2)+2(3)$

then, there is at least a pair $(2,\,3)$ of $\mathbb{N}^2$, such that: $12=3p+2q$

So the statement is true for $n=12$.

Assume the proposition is true for n and prove it is true for $n+1$.

We have according to the assumption

$\forall n\in\mathbb{N}^*\setminus\{1,2,...,11\},\ \exists(p,\,q)\in\mathbb{N}^2:n=3p+2q$

then,

$\exists(p,\,q)\in\mathbb{N}^2:n+1=3p+2q+1$

i.e.

$\exists(p,\,q)\in\mathbb{N}^2:n+1=3p+2q+3-2$

$\exists(p,\,q)\in\mathbb{N}^2:n+1=3(p+1)+2(q-1)$

· If $q\geq 1$ then $q-1\in\mathbb{N}$

· If $q=0$ then $n=3p$

So, $n+1=3(p-1)+2(2)$

Since $n\geq 12$ then $p\geq 4$ And from it $p-1\in\mathbb{N}$

So,

$\exists(p-1,\,2)\in\mathbb{N}^2:n+1=3(p+1)+2(2)$

And the property is true for $n+1$.

Then,

$\forall n\in\mathbb{N}^*\setminus\{1,2,...,11\},\ \exists(p,\,q)\in\mathbb{N}^2:n=3p+2q$

Solution 1.5.14

1. Let's show that $P_n:1^3+2^3+...+n^3=\frac{n^2(n+1)^2}{4},\quad \forall n\in\mathbb{N}^\star$

   • For $n=1$ we have : $1^3=\frac{1^2(2)^2}{4}=1$

   So P_1 is true.

• We suppose that $P_n : 1^3 + 2^3 + ... + n^3 = \frac{n^2(n+1)^2}{4}$ is true.

And we show that: $1^3 + 2^3 + ... + n^3 + (n+1)^3 = \frac{(n+1)^2(n+2)^2}{4}$ is true.

Using P_n we obtain:

$$\begin{aligned} 1^3 + 2^3 + ... + (n+1)^3 &= 1^3 + 2^3 + ... + n^3 + (n+1)^3 \\ &= \frac{n^2(n+1)^2}{4} + (n+1)^3 \\ &= \frac{n^2(n+1)^2 + 4(n+1)^3}{4} \\ &= \frac{(n+1)^2(n^2+4n+4)}{4} \\ &= \frac{(n+1)^2(n+2)^2}{4} \end{aligned}$$

Thus P_{n+1} is true, then $\forall n \in \mathbb{N}^\star : 1^3 + 2^3 + ... + n^3 = \frac{n^2(n+1)^2}{4}$.

2. Let's show that $P_n : 4^n + 6n - 1, \quad \forall n \in \mathbb{N}$ is a multiple of 9,

that's to say $\forall n \in IN$, $\exists k \in \mathbb{IN} \ / \ 4^n + 6n - 1 = 9k$

• For $n = 0$ we have: $\exists k = 0 \in \mathbb{IN}, 1 + 0 - 1 = 0 = 9(0)$, P_0 is true.

• We suppose that: $\forall n \in IN$, $\exists k \in \mathbb{IN} \ / \ 4^n + 6n - 1 = 9k$ is true..

And we show that: $\forall n \in IN$, $\exists ? k^{'} \in \mathbb{IN} \ / \ 4^{n+1} + 6(n+1) - 1 = 9k^{'}$ is true..

$$\begin{aligned} 4^{n+1} + 6(n+1) - 1 &= 4.4^n + 6n + 6 - 1 \\ &= (9-5)4^n + 6n + 5 \\ &= 9(4^n) - 5.4^n - 5(6n) + 36n + 5 \\ &= -5(4^n + 6n - 1) + 9(4^n) + 36n \\ &= -5(9k) + 9(4^n) + 9(4n) \\ &= 9(-5k + 4^n + 4n) \\ &= 9k^{'}, \quad \text{such as } k^{'} = -5k + 4^n + 4n \end{aligned}$$

Solution 1.5.15

1. Let the proposition be $P_n \Leftrightarrow \frac{1}{\sqrt{4n+1}} < \frac{1.3.5...(2n-1)}{2.4.6...(2n)} < \frac{1}{\sqrt{3n+1}}, \qquad \forall n \geq 2$

We have $P_2 \Leftrightarrow \frac{1}{3} < \frac{1\times 3}{2\times 4} < \frac{1}{\sqrt{7}} \Leftrightarrow \frac{1}{3} < \frac{3}{8} < \frac{1}{\sqrt{7}}$

P_2 is true.

We assume that P_n is true for $n \geq 2$, and we show that P_{n+1} is true

Then, we have:

$$\frac{1}{\sqrt{4n+1}}\frac{2n+1}{2n+2} < \frac{1.3.5...(2n-1)(2n+1)}{2.4.6...(2n)(2n+2)} < \frac{1}{\sqrt{3n+1}}\frac{2n+1}{2n+2}$$

We note by D_1 the following difference

$$D_1 = \left(\frac{1}{\sqrt{3n+4}}\right)^2 - \left(\frac{1}{\sqrt{3n+1}}\frac{2n+1}{2n+2}\right)^2$$

We find that

$$\begin{aligned} D_1 &= \frac{1}{3n+4} - \frac{1}{3n+1}\left(\frac{2n+1}{2n+2}\right)^2 \\ &= \frac{(3n+1)(2n+2)^2 - (3n+4)(2n+1)^2}{(3n+4)(3n+1)(2n+2)^2} \\ &= \frac{n}{(3n+4)(3n+1)(2n+2)^2} > 0 \end{aligned}$$

Then

$$n > 2 \Rightarrow \frac{1}{\sqrt{3n+1}}\frac{2n+1}{2n+2} < \frac{1}{\sqrt{3n+4}}$$

And also we note by D_2 the following difference

$$D_2 = \left(\frac{1}{\sqrt{4n+1}}\frac{2n+1}{2n+2}\right)^2 - \left(\frac{1}{\sqrt{4n+5}}\right)^2$$

We find that:

$$\begin{aligned} D_2 &= \left(\frac{1}{\sqrt{4n+1}}\frac{2n+1}{2n+2}\right)^2 - \left(\frac{1}{\sqrt{4n+5}}\right)^2 \\ &= \frac{(4n+5)(2n+1)^2 - (4n+1)(2n+2)^2}{(4n+1)(4n+5)(2n+2)^2} \\ &= \frac{1}{(4n+1)(4n+5)(2n+2)^2} > 0 \end{aligned}$$

Then

$$n > 2 \Rightarrow \frac{1}{\sqrt{4n+5}} < \frac{1}{\sqrt{4n+1}}\frac{2n+1}{2n+2}$$

We have thus proven that:

$$\frac{1}{\sqrt{4n+5}} < \frac{1.3.5...(2n-1)(2n+1)}{2.4.6...(2n)(2n+2)} < \frac{1}{\sqrt{3n+4}}$$

Then P_{n+1} is true.

So P_n is true for $n \geq 2$.

2. Let the proposition be

$$P_n \Leftrightarrow \sum_{k=1}^{n}\sqrt{k} < \frac{4n+3}{6}\sqrt{n}, \quad \forall n \geq 1.$$

We notice that $P_1 \Leftrightarrow 1 < \frac{7}{6}$, then P_1 is true..

We assume that P_n is true for $n \geq 1$, and we show that P_{n+1} is true.

Then, we have:

$$\sum_{k=1}^{n+1}\sqrt{k} = \sum_{k=1}^{n}\sqrt{k} + \sqrt{n+1} < \frac{4n+3}{6}\sqrt{n} + \sqrt{n+1}$$

We note by D_1 the following difference

$$D = \frac{4n+7}{6}\sqrt{n+1} - \left(\frac{4n+3}{6}\sqrt{n} + \sqrt{n+1}\right)$$

We find that:

$$\begin{aligned} D &= \frac{4n+1}{6}\sqrt{n+1} - \frac{4n+3}{6}\sqrt{n} \\ &= \frac{4n+1}{6}(\sqrt{n+1}-\sqrt{n}) - \frac{2\sqrt{n}}{6} \\ &= \frac{4n+1}{6(\sqrt{n+1}+\sqrt{n})} - \frac{2\sqrt{n}}{6} \\ &= \frac{2n+1-2\sqrt{n(n+1)}}{6(\sqrt{n+1}+\sqrt{n})} \\ &= \frac{(\sqrt{n+1}-\sqrt{n})^2}{6(\sqrt{n+1}+\sqrt{n})} > 0 \end{aligned}$$

Then,

$$\sum_{k=1}^{n+1}\sqrt{k} < \frac{4(n+1)+3}{6}\sqrt{n+1}$$

Therefore, P_{n+1} is true hence P_n is true for $n \geq 1$.

Solution 1.5.16

1. By the absurd we suppose that $\sqrt{2}$ is a rational i.e.,
   $\exists\ a, b \in \mathbb{N}, a \wedge b = 1\ /\ \sqrt{2} = \frac{a}{b} \Rightarrow 2 = \frac{a^2}{b^2} \Rightarrow 2b^2 = a^2$.
   then 2 divides a, a is even $\exists k \in \mathbb{N} : a = 2k$, Thus
   $2b^2 = 4k^2 \Leftrightarrow b^2 = 2k^2$,
   we deduce that b is also even or a, b are prime between them, contradiction, what we assumed at the start is false, i.e.
   $\sqrt{2} \notin \mathbb{Q}$
2. Let $n \in \mathbb{N}$ by the absurd suppose that n^2 is even and n is odd, then $\exists k \in \mathbb{Z}$ such that:
   $n = 2k+1$ hence $n^2 = 2(2k^2+2k)+1 = 2k^{'}+1$, $k^{'} = (2k^2+2k) \in \mathbb{Z}$,
   n^2 is odd contradiction because n^2 is even.
   What we initially assumed is false i.e. $\forall n \in \mathbb{N}, n^2$ even $\Rightarrow n$ is even.

Solution 1.5.17

We prove by absurd that: $\forall x \in \mathbb{R}^+, \exists \in \mathbb{N} : x \leq n$.
Suppose that:
$\exists x \in \mathbb{R}^+, \forall \in \mathbb{N} : x > n$.
So, $n > x$ for all $n \in \mathbb{N}$
We consider the integer part $E(x)$ of the number x
then,
$E(x) \leq x < E(x)\ +1$
Since $x \in \mathbb{R}^+$ then $E(x) \in \mathbb{N}$, so $E(x)+1 \in \mathbb{N}$
and since $E(x)\ +1 > x$
This is a contradiction with the fact that all natural numbers are smaller than x
So the assumption $\exists x \in \mathbb{R}^+, \forall \in \mathbb{N} : x > n$ is false

Hence, his negation is true.

i.e. the statement $\forall x \in \mathbb{R}^+, \exists \in \mathbb{N} : x \leq n$ is true.

Solution 1.5.18

1. Let us show that its contrapositive: n is odd $\Rightarrow (n^2-1)$ is divisible by 8 is true

   Let n be odd then $\exists k \in \mathbb{IN}$ such that $n = 2k+1$ and therefore $n^2 = 4k^2+4k+1$.

   $n^2 - 1 = 4k^2 + 4k = 4k(k+1)$ it is enough to show that $k(k+1)$ is even.

   Let us show that $k(k+1)$ is even, we have two cases:

   • If k is even then $k+1$ is odd so the product of an even number and an odd number is even.

   • If k is odd, then $k+1$ is even so the product is even, it's the same reasoning (you should know that the product of two consecutive numbers is always even).

   Thus $k(k+1)$ is even $\exists k^{'} \in \mathbb{IN} \ / \ k(k+1) = 2k^{'}$, hence $n^2 - 1 = 4(2k^{'}) = 8k^{'}$.

   $n^2 - 1$ is divisible by 8.

2. Let us show that its contrapositive: $x \neq 0 \Rightarrow \exists \varepsilon > 0, |x| > \varepsilon$ is true

   Let $x \neq 0$, there exists $\varepsilon = \frac{|x|}{2} > 0$ such that $|x| > \frac{|x|}{2} = \varepsilon$ because $x \neq 0$ hence the result.

Chapter 2

Sets and Applications

2.1 Introduction

Set theory is one of the fundamental pillars of modern mathematics, as it provides a unified framework for describing mathematical objects and their relationships. In addition, applications (functions) play a central role in connecting different mathematical structures and expressing various mathematical phenomena. This chapter introduces the basic notions of sets, operations on sets, Cartesian products, and mappings between sets. Particular emphasis is placed on the study of injective, surjective, and bijective applications, which constitute essential tools in algebra and many other areas of mathematics.

2.2 Sets

Definition 2.2.1

A set is a collection of elements, for example $\{0, 1\}$, $\mathbb{N}$.

1. The empty set is a set containing no elements, denoted $\emptyset$.
2. We write $x \in E$ if x is an element of E, and $x \notin E$ otherwise.

2.2.1 Operations on Sets

Definition 2.2.2 Inclusion $F \subset E$

If every element of F is an element of E. In other words: $\forall x \in F$, $x \in E$. F is called a subset of E (or a part of E).

Definition 2.2.3 Equality

$$E = F \Leftrightarrow E \subset F \text{ and } F \subset E.$$

Definition 2.2.4 Set of subset of E

We denote by $P(E)$ the Set of subset of E. For example, if $E = \{1, 2, 3\}$. Then,

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

If $card(E) = n$, then $card(P(E)) = 2^n$.

Definition 2.2.5 Difference and Symmetric Difference

Let A and B be two subsets of a set E. We denote:

1. The difference of A and B as the set:
$$A \setminus B = \{x \in A, \quad x \notin B\}.$$
2. The symmetric difference of A and B as the set:
$$A \Delta B = (A \cup B) \setminus (A \cap B).$$

Definition 2.2.6 Complement of a Set

Let $A \subset E$. Then, the complement of A in E is denoted $\complement_E A$, which is defined by:
$$\complement_E A = \{x \in E, \quad x \notin A\}.$$
It is also denoted $E \setminus A$ or A^c, or $\overline{A}$.

Definition 2.2.7 Intersection and Union

1. The intersection of A and B, denoted $A \cap B$, is the set of elements belonging to both A and B.
2. The union of A and B, denoted $A \cup B$, is the set of elements belonging to either A or B.
Formally, we have:
$$A \cap B = \{x, \quad (x \in A) \wedge (x \in B)\}.$$
$$A \cup B = \{x, \quad (x \in A) \vee (x \in B)\}.$$

Definition 2.2.8 Cartesian Product

The Cartesian product of sets A and B is the set of pairs $(x; y)$ where $x \in A$ and $y \in B$.
$$A \times B = \{(x, y), \quad x \in A \text{ and } y \in B\}.$$
If $card(A) = n$, $card(B) = m$. Then, $card(A \times B) = nm$.

Proposition 2.2.9

Let A, B, C be subsets of E. Then,

1. $A \cap B = B \cap A$, $A \cup B = B \cup A$;
2. $A \cap (B \cap C) = (A \cap B) \cap C$, $A \cup (B \cup C) = (A \cup B) \cup C$;
3. $A \cap \emptyset = \emptyset$, $A \cap A = A$, $A \cup \emptyset = A$, $A \cup A = A$;
4. $A \cap B = A \Leftrightarrow A \subset B$,
5. $A \cup B = B \Leftrightarrow A \subset B$;
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
7. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
8. $\complement_E(\complement_E A) = A$;
9. $\complement_E(A \cap B) = \complement_E A \cup \complement_E B$;
10. $\complement_E(A \cup B) = \complement_E A \cap \complement_E B$;

. 11. $A \subset B \Leftrightarrow \complement_E B \subset \complement_E A$.

Proof

8) Let $x \in E$. Then,

$$x \in \complement_E(\complement_E A) \Leftrightarrow x \notin \complement_E A \Leftrightarrow x \in A.$$

Thus,

$$\complement_E(\complement_E A) = \overline{\overline{A}} = A.$$

9) Let $x \in E$. Then,

$$x \in \complement_E(A \cap B) \Leftrightarrow x \notin (A \cap B) \Leftrightarrow (x \notin A) \vee (x \notin B) \Leftrightarrow (x \in \complement_E A) \vee (x \in \complement_E B) \Leftrightarrow x \in (\complement_E A \cup \complement_E B).$$

Thus,

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

Similarly, we prove property (10).

11) $A \subset B \Leftrightarrow \forall x \in E, ((x \in A) \Rightarrow (x \in B)) \Leftrightarrow \forall x \in E, ((x \notin B) \Rightarrow (x \notin A))$ (Contrapositive of the implication)

$$\Leftrightarrow \forall x \in E, (x \in \complement_E B) \Rightarrow (x \in \complement_E A) \Leftrightarrow \complement_E B \subset \complement_E A,$$

thus

$$A \subset B \Leftrightarrow \complement_E B \subset \complement_E A.$$

2.3 Applications

Definition 2.3.1

A mapping or a function $f : E \to F$ is a relation that associates with each element $x \in E$ a unique element of F denoted $f(x)$.

1. f and g are two mappings. $f = g$ if and only if for all $x \in E$, $f(x) = g(x)$.
2. The graph of the mapping $f : E \to F$ is the set denoted G_f defined by
$$G_f = \{(x, f(x)) \in E \times F \ / \ x \in E\}.$$
3. The composition of two mappings f and g such that $f : E \to F$ and $g : F \to G$ is the mapping $g \circ f : E \to G$ defined by:
$$(g \circ f)(x) = g(f(x)).$$

Example 2.3.2

Let $f :]0, +1[\to]0, +1[$ and $g :]0, +1[\to \mathbb{R}$ be defined as

$$f(x) = \frac{1}{x},$$

and

$$g(x) = \frac{x-1}{x+1},$$

respectively:

$$\begin{aligned} g \circ f :]0, +1[&\to \mathbb{R} \\ x &\mapsto g(f(x)), \end{aligned}$$

$$\begin{aligned} g(f(x)) &= g\left(\frac{1}{x}\right), \\ &= \frac{\frac{1}{x}-1}{\frac{1}{x}+1}, \\ &= \frac{1-x}{1+x}, \\ &= -g(x) \end{aligned}$$

Note 2.3.3

The composition of two mappings is not always defined. For example, $g \circ f$ is defined if the codomain of f is the same as the domain of g.

2.3.1 Direct Image, Inverse Image

Definition 2.3.4

1. Let $A \subset E$, and $f : E \to F$ be a mapping, the direct image of A under f is the set

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

i.e.,

$$y \in f(A) \Leftrightarrow \exists x \in A, y = f(x).$$

2. Let $B \subset F$, and $f : E \to F$ be a mapping, the inverse image of B under f is the set

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

i.e.,

$$x \in f^{-1}(B) \Leftrightarrow f(x) \in B.$$

Example 2.3.5

Let

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto f(x) = x^2. \end{aligned}$$

Then,

$$f(\{2\}) = \{4\}.$$

$$f([-1,3]) = \{f(x)/x \in [-1,3]\} = [0,9].$$

$$f([-1,0] \cup [1,3]) = [0;9].$$

$$f^{-1}(\{2\}) = \{\ x \in \mathbb{R}\ \ /\ \ f(x) \in \{2\}\} = \left\{-\sqrt{2},\ \sqrt{2}\right\}.$$

Note 2.3.6

1. $f(A)$ is a subset of F, $f^{-1}(B)$ is a subset of E.
2. The notation $f^{-1}(B)$ does not imply that f is bijective, the inverse image exists for any function.
3. The direct image of a singleton $f(\{x\}) = \{f(x)\}$ is a singleton, whereas the inverse image of a singleton $f^{-1}(\{y\})$ depends on f, it can be a singleton, a set with multiple elements, or even E if f is a constant function.

Proposition 2.3.7

Let $f : E \to F$ be a mapping, A, A' subsets of E, and B, B' subsets of F.

1. $A \subset A' \Rightarrow f(A) \subset f(A^{'})$.
2. $B \subset B' \Rightarrow f^{-1}(B) \subset f^{-1}(B^{'})$.
3. $f(A \cap A') \subset f(A) \cap f(A^{'})$.
4. $f(A \cup A') = f(A) \cup f(A^{'})$.
5. $f^{-1}(B \cap B') = f^{-1}(B) \cap f^{-1}(B^{'})$.
6. $f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B^{'})$.
7. $A \subset f^{-1}(f(A))$.
8. $f(f^{-1}(B)) \subset B$.

Proof

1) Suppose $y \in f(A)$. Then $\exists\, x \in A$ such that $y = f(x)$. Since

$$A \subset A', x \in A'.$$

Then,

$$y \in f(A').$$

Which implies

$$f(A) \subset f(A').$$

2) Let $x \in f^{-1}(B)$. Then, $f(x) \in B$. Since

$$B \subset B', f(x) \in B'.$$

Hence

$$x \in f^{-1}(B').$$

So,

$$f^{-1}(B) \subset f^{-1}(B^{'}).$$

3) Suppose $y \in f(A \cap A')$. Then, there exists

$$x \in (A \cap A')$$

such that $y = f(x)$. Since

$$x \in A, y = f(x) \in f(A),$$

and similarly

$$x \in A',$$

implies

$$y \in f(A').$$

Thus,

$$y \in f(A) \cap f(A^{'}).$$

So,

$$f(A \cap A') \subset f(A) \cap f(A^{'}).$$

4) Suppose

$$y \in f(A \cup A'), \exists x \in A \cup A',$$

such that

$$y = f(x).$$

If $x \in A$, then $y \in f(A)$ and if

$$x \in A'.$$

Then,

$$y \in f(A^{'}),$$

in both cases

$$y \in f(A) \cup f(A^{'}).$$

Hence,

$$f(A \cup A') \subset f(A) \cup f(A^{'}).$$

Conversely, if

$$y \in f(A) \cup f(A^{'}).$$

Then, if $y \in f(A)$ there exists $x \in A$ such that

$$y = f(x),$$

or if

$$y \in f(A').$$

Then, there exists

$$x \in A',$$

such that

$$y = f(x),$$

in both cases

$$y \in f(A \cup A').$$

Therefore,

$$f(A) \cup f(A^{'}) \subset f(A \cup A').$$

By mutual inclusion, we have equality.
5) Proven similarly to (3).
6) Proven similarly to (5).
7) Suppose $x \in A$. Let $B = f(A)$. Then $f(x) \in B$. So,

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

Hence $A \subset f^{-1}(f(A))$.
8) Suppose $y \in f(f^{-1}(B))$. Let $A = f^{-1}(B)$. Then $y \in f(A)$ implies

$$\exists x \in A,\ y = f(x).$$

Since,

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

We have $f(x) \in B$, thus $y \in B$. Which implies

$$f(f^{-1}(B)) \subset B.$$

Definition 2.3.8 Antecedent

1. Let $y \in F$, any element $x \in E$ such that $f(x) = y$ is called an antecedent of y.
2. In terms of inverse image, the set of antecedents of y is $f^{-1}(\{y\})$.

2.3.2 Injection, surjection, bijection

Definition 2.3.9

Let $f : E \to F$ be a function:

1. f is injective if every element of the codomain has at most one pre-image under f.
2. f is surjective if every element of the codomain has at least one pre-image under f.
3. f is bijective if every element of the codomain has exactly one pre-image under f.

This definition can be reformulated as

Definition 2.3.10

1. f is injective if for every $y \in F$, the equation $f(x) = y$ has at most one solution in E.
2. f is surjective if for every $y \in F$, the equation $f(x) = y$ has at least one solution in E.
3. f is bijective if for every $y \in F$, the equation $f(x) = y$ has exactly one solution in E. Alternatively, f is bijective if it is injective and surjective.

Proposition 2.3.11

Let $f : E \to F$ be a function, the following statements are equivalent:

1. f is injective $\Leftrightarrow \forall x_1, x_2 \in E, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
2. f is injective $\Leftrightarrow \forall x_1, x_2 \in E, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$
3. f is surjective $\Leftrightarrow \forall y \in F; \exists x \in E, y = f(x)$.
4. f is surjective $\Leftrightarrow f(E) = F$
5. f is bijective $\Leftrightarrow \forall y \in F; \exists! x \in E, y = f(x)$. The symbol ! denotes uniqueness, i.e., there exists a unique solution for the equation $f(x) = y$.

Example 2.3.12

Let the functions

$$\begin{aligned} f_1 : \quad \mathbb{N} &\to \mathbb{R} \\ x &\mapsto f_1(x) = \frac{1}{1+x}. \end{aligned}$$

$$\begin{aligned} f_2 : \quad \mathbb{R}^+ &\to \mathbb{R} \\ x &\mapsto f_2(x) = x^2. \end{aligned}$$

$$\begin{aligned} f_3 : \quad \mathbb{R} &\to \mathbb{R}^+ \\ x &\mapsto f_3(x) = x^2. \end{aligned}$$

Are the functions f_1, f_2, f_3 injective, surjective, bijective?

Proof

1)

$$\begin{aligned} f_1 : \quad \mathbb{N} &\to \mathbb{R} \\ x &\mapsto f_1(x) = \frac{1}{1+x}. \end{aligned}$$

1. $$\forall x_1, x_2 \in \mathbb{N}, \quad f_1(x_1) = f_1(x_2) \Rightarrow \frac{1}{1+x_1} = \frac{1}{1+x_2} \Rightarrow x_1 = x_2.$$

   So f_1 is injective.

2. $$\forall y \in \mathbb{R}, \quad \frac{1}{1+x} = y \Rightarrow x = \frac{1-y}{y}.$$

   For example for $y = 5$, we get

   $$x = \frac{-4}{5} \notin \mathbb{N}.$$

   So, f_1 is not surjective. Therefore, f_1 is not bijective.

2)

$$\begin{aligned} f_2 : \quad \mathbb{R}^+ &\to \mathbb{R}, \\ x &\mapsto f_2(x) = x^2. \end{aligned}$$

1. $$\forall x_1, x_2 \in \mathbb{R}^+, f_2(x_1) = f_2(x_2) \Rightarrow x_1^2 = x_2^2 \Rightarrow x_1 = \pm x_2 \Rightarrow x_1 = x_2,$$

   (because $x_1, x_2 \in \mathbb{R}^+$). So f_2 is injective.

2. $$\forall y \in \mathbb{R}, \quad x^2 = y \Rightarrow x = \pm\sqrt{y}.$$

   If $y \geq 0$. Then, for

   $$y \in \mathbb{R}^- \nexists x \in \mathbb{R}^+.$$

   Hence, f_2 is not surjective.

   Therefore, f_2 is not bijective.

3)

$$\begin{aligned} f_3 : \quad \mathbb{R} &\to \mathbb{R}^+ \\ x &\mapsto f_3(x) = x^2. \end{aligned}$$

1. $$\forall x_1, x_2 \in \mathbb{R}, \quad f_3(x_1) = f_3(x_2) \Rightarrow x_1^2 = x_2^2 \Rightarrow x_1 = \pm x_2.$$
   $$\exists 2, -2 \in \mathbb{R}, 2 \neq -2.$$

   But $2^2 = (-2)^2$. So, f_3 is not injective.

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

   If $y \geq 0$. Then,

   $$\forall y \in \mathbb{R}^+, \exists x \in \mathbb{R}, y = f_3(x).$$

   Hence f_3 is surjective.

Therefore, f_3 is not bijective.

Proposition 2.3.13

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

1. f injective and g injective $\Rightarrow g \circ f$ injective,
2. f surjective and g surjective $\Rightarrow g \circ f$ surjective,
3. $g \circ f$ injective $\Rightarrow f$ injective,
4. $g \circ f$ surjective $\Rightarrow g$ surjective.

Proof

1. Let $x_1, x_2 \in E$. Then
$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2),$$
because f is injective.
$$\Rightarrow g(f(x_1)) \neq g(f(x_2)),$$
because g is injective
$$\Rightarrow g \circ f(x_1) \neq g \circ f(x_2),$$
which shows that $g \circ f$ is injective.

2. Let $z \in G$. Since g is surjective, there exists $y \in F$ such that $z = g(y)$. We have $y \in F$ and f is surjective. Then, there exists $x \in E$ such that $y = f(x)$. Hence $z = g(f(x))$ and we conclude that:
$$\forall z \in G, \quad \exists x \in E, z = g \circ f(x).$$
It shows that $g \circ f$ is surjective.

3.
$$\forall x_1, x_2 \in E, \quad f(x_1) = f(x_2) \Rightarrow g(f(x_1)) = g(f(x_2)).$$
Because g is a function.
$$\Rightarrow (g \circ f)(x_1) = (g \circ f)(x_2).$$
$$\Rightarrow x_1 = x_2.$$
Because $g \circ f$ is injective, hence f is injective.

4. Let $z \in G$. Then, $g \circ f$ surjective
$$\Rightarrow \exists x \in E, \quad g \circ f(x) = z.$$
$$\Rightarrow \exists x \in E, \quad g(f(x)) = z.$$
$$\Rightarrow \exists y = f(x) \in F, \quad g(y) = z.$$
Thus,
$$\forall z \in G \, \exists y \in F, \quad g(y) = z.$$
Which shows that g is surjective.

2.3.3 Inverse function

Proposition 2.3.14

An application $f : E \to F$ is bijective if and only if there exists a unique function $g : F \to E$ such that
$$f \circ g = \mathrm{Id}_F \quad \text{and} \quad g \circ f = \mathrm{Id}_E.$$
We say that f is invertible and g, denoted f^{-1}, is called the "inverse function" or "reciprocal function" of f.

Proof

1. Suppose there exists a function $g : F \to E$ such that $f \circ g = \mathrm{Id}_F$ and $g \circ f = \mathrm{Id}_E$.

   Let's show that f is bijective.

   (a) Let $y \in F$. Since
   $$f \circ g = \mathrm{Id}_F.$$
   Then,
   $$f \circ g(y) = y.$$
   Thus there exists
   $$x = g(y) \in E,$$
   such that $f(x) = y$, showing that f is surjective.

   (b) Let $x_1, x_2 \in E$. Since $g \circ f = \mathrm{Id}_E$. Then,
   $$g \circ f(x_1) = x_1,$$
   and
   $$g \circ f(x_2) = x_2.$$
   Hence,
   $$f(x_1) = f(x_2) \Rightarrow g(f(x_1)) = g(f(x_2)).$$
   Because g is a function.
   $$\Rightarrow (g \circ f)(x_1) = (g \circ f)(x_2).$$
   $$\Rightarrow x_1 = x_2,$$
   showing that f is injective. From (1) and (2), we deduce that f is bijective.

2. Suppose f is bijective. Let's construct the unique function $g : F \to E$, such that $f \circ g = \mathrm{Id}_F$ and $g \circ f = \mathrm{Id}_E$.
   Since f is bijective, then for every $y \in F$, there exists a unique $x \in E$ such that $y = f(x)$.
   Thus, to every element $y \in F$, we associate a unique element $x \in E$, denoted by $g(x)$, such that $f(x) = y$. We define an application as follows:
   $$\begin{aligned} g &: F \to E \\ y &\mapsto g(y) = x \end{aligned}$$
   Let's show that
   $$f \circ g = \mathrm{Id}_F, \quad \text{and} \quad g \circ f = \mathrm{Id}_E.$$

   (a) Let $y \in F$. Then $g(y) = x$, with $f(x) = y$. So,
   $$f \circ g(y) = f(g(y)) = f(x) = y.$$
   Showing that:
   $$f \circ g = \mathrm{Id}_F.$$

   (b) Let $x \in E$. Then for $y = f(x)$ we have $g(y) = x$. Thus,
   $$g \circ f(x) = g(f(x)) = g(y) = x.$$
   Which shows that:
   $$g \circ f = \mathrm{Id}_E.$$

   (c) Let's show the uniqueness of g. Let $g_1 : F \to E$ satisfying the two previous properties. Then, for every $y \in F$, there exists $x \in E$ such that $y = f(x)$. Thus
   $$g_1(y) = g_1(f(x)) = g_1 \circ f(x) = \mathrm{Id}_E(x) = g \circ f(x) = g(f(x)) = g(y),$$
   which shows that $g_1 = g$.

Example 2.3.15

$f : \mathbb{R} \to]0, +\infty[$ defined by

$$f(x) = \exp(x) = e^x,$$

is bijective. its inverse function is $g :]0, +\infty[\to \mathbb{R}$ defined by $g(y) = \ln(y)$. We indeed have

$$e^{\ln(y)} = y, \forall\ y \in]0, +\infty[, \text{ and } \ln(e^x) = x, \forall x \in \mathbb{R}.$$

Proposition 2.3.16

Let $f : E \to F$ and $g : F \to G$ be bijective applications. The function $g \circ f$ is bijective and its inverse is:

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

Proof

According to proposition 2.5, there exists $u : F \to E$ such that $u \circ f = \mathrm{Id}_E$ and $f \circ u = \mathrm{Id}_F$.
There, also exists $v : G \to F$ such that $v \circ g = \mathrm{Id}_F$ and $g \circ v = \mathrm{Id}_G$.
Then $(g \circ f) \circ (u \circ v) = g \circ (f \circ u) \circ v = g \circ \mathrm{Id}_F \circ v = g \circ v = \mathrm{Id}_E$.
Also, $(u \circ v) \circ (g \circ f) = u \circ (v \circ g) \circ f = u \circ \mathrm{Id}_F \circ f = u \circ f = \mathrm{Id}_E$.
So $g \circ f$ is bijective and its inverse is $u \circ v$.
Since u is the inverse of f and v is the inverse of g, then: $u \circ v = f^{-1} \circ g^{-1}$.

2.3.4 Extension and Restriction

Definition 2.3.17

Let $f : E \to F$ be an application, let $A \subset E$; $B \subset F$ such that $f(A) \subset B$. We call the restriction of f to A as the starting set and B as the arrival set and we denote $f|_A \to B$ the application from A to B which associates. This function has the same rule of calculation as f, only the domain and codomain change.

Note 2.3.18

When we restrict only the domain ($B = F$), we use the notation $f/_A$.

Definition 2.3.19

Let f and g be functions, we say that f is an extension of g if g is a restriction of f.

Example 2.3.20

1. Let $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R}^+ \to \mathbb{R}^+$, defined as:

$$x \mapsto f(x) = x^2,$$

$$x \mapsto g(x) = x^2.$$

That is, g is the restriction of f to $\mathbb{R}^+$,

$$g = f/_{\mathbb{R}^+} \to \mathbb{R}^+.$$

Note that g is increasing and bijective, but f is not.

2. Let $g : \mathbb{R}^* \to \mathbb{R}$ and $f : \mathbb{R} \to \mathbb{R}$, defined as:

$$x \mapsto g(x) = \frac{\sin x}{x},$$

$$x \mapsto f(x) = \begin{cases} \dfrac{\sin x}{x}, \text{ if } x \neq 0 \\ 1, \text{ if } x = 0 \end{cases}$$

The function f is an extension of g,

$$g = f/_{\mathbb{R}^*}.$$

Moreover, we can show that f is continuous on $\mathbb{R}$; and we say that f is the extension by continuity of g.

2.4 Exercises

Exercise 2.4.1

Let A, B, $C \in P(E)$, proving the following:

1. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.
2. $A \subset B \Leftrightarrow A \cup B = B$
3. $A \cup B = A \cap C \Leftrightarrow B \subset A \subset C$

Exercise 2.4.2

Given A, B and C three parts of a set E,

1. Show that:
   (a) $(A \cap B) \cup \complement_E B = A \cup \complement_E B$.
   (b) $(A \setminus B) \setminus C = A \setminus (B \cup C)$.
2. Simplify:
   (a) $\overline{(A \cup B)} \cap \overline{(C \cup \overline{A})}$.
   (b) $\overline{(A \cap B)} \cup \overline{(C \cap \overline{A})}$.

Exercise 2.4.3

Let E, F two sets, $f : E \to F$ is an application, proving the following:

1. $\forall\ A, B \in P(E)$, $f(A \cap B) \subset f(A) \cap f(B)$.
2. $\forall\ A, B \in P(E)$, $f(A \cup B) = f(A) \cup f(B)$.
3. $\forall\ A \in P(F)$, $f^{-1}\ (F \setminus A) = E \setminus f^{-1}(A)$.

Exercise 2.4.4

1. Describe the direct image of $\mathbb{R}$ by the exponential function
2. Find $f([0, 1[)$, $f(\mathbb{R})$, $f(]-1, 2[)$, $f^{-1}\ (\{3\})$, par la fonction f: $x \mapsto x^2$, defined on $\mathbb{R}$.

Exercise 2.4.5

Let f: $[1; +\infty[\to [0; +\infty[$ is a function such that $f(x) = x^2 - 1$ bijective?

Exercise 2.4.6

Let E, F, G three sets, $f : E \to F$, $g : F \to G$ and $h : G \to E$
Proving that is $h \circ g \circ f$ is injective and if $g \circ f \circ h$ and $f \circ h \circ g$ are surjectives. Then, f , g and h are bijectives.

2.5 Solutions

Solution 2.4.1

1. $A \setminus (B \cap C) = A \cap \complement_E(B \cap C) = (A \cap \complement_E B) \cup (A \cap \complement_E C) = (A \setminus B) \cup (A \setminus C)$.
   (a) "$\Rightarrow$"
   Posing that $A \subset B$, we have $B \subset (A \cup B)$, for $x \in A \cup B$ then $x \in A$ or $x \in B$ we have $x \in B$, therefore $(A \cup B) \subset B$, hence $A \cup B = B$.
   (b) "$\Leftarrow$"
   Posing that $A \cup B = B$, because $A \subset (A \cup B)$, on a $A \subset B$.
2. (a) "$\Rightarrow$"
   Posing that $A \cup B = A \cap C$; we have $B \subset (A \cup B) = (A \cap C) \subset A \subset (A \cup B) = (A \cap C) \subset C$.
   (b) "$\Leftarrow$"
   Posing that $B \subset A \subset C, A \cup B = A = A \cap C$.

Solution 2.4.2

1. Let us show that:
   (a) $(A \cap B) \cup \complement_E B \stackrel{?}{=} A \cup \complement_E B$.
   Let $x \in (A \cap B) \cup \complement_E B \Leftrightarrow x \in (A \cap B) \vee x \in \complement_E B$,
   $\Leftrightarrow (x \in A \wedge x \in B) \vee (x \notin B)$
   $\Leftrightarrow (x \in A \vee x \notin B) \wedge (x \in B \vee x \notin B)$
   $\Leftrightarrow x \in (A \cup \complement_E B) \wedge x \in (B \cup \complement_E B)$
   $\Leftrightarrow x \in (A \cup \complement_E B) \cap E$
   $\Leftrightarrow x \in A \cup \complement_E B$
   Because $E = \complement_E B. \cup B$ and $A \cup \complement_E B$ is a subset of E.

   (b) $(A \setminus B) \setminus C \stackrel{?}{=} A \setminus (B \cup C)$.
   $x \in (A \setminus B) \setminus C \Leftrightarrow (x \in A \wedge x \notin B) \wedge (x \notin C)$
   $\Leftrightarrow x \in A \wedge (x \notin B \wedge x \notin C)$
   $\Leftrightarrow x \in A \wedge x \in (\complement_E B \cap \complement_E C)$
   $\Leftrightarrow x \in A \wedge x \notin (B \cup C)$ (Laws of Morgan)
   $\Leftrightarrow x \in A \setminus (B \cup C)$

2. Let's simplify
   (a) $\overline{(A \cup B)} \cap \overline{(C \cup \overline{A})}$
   $\overline{(A \cup B)} \cap \overline{(C \cup \overline{A})} = (\overline{A} \cap \overline{B}) \cap (\overline{C} \cap \overline{\overline{A}})$
   $= (\overline{A} \cap \overline{B}) \cap (\overline{C} \cap A)$
   $= (\overline{A} \cap A) \cap (\overline{C} \cap \overline{B})$
   $= (\phi) \cap (\overline{C} \cap \overline{B})$
   $= \phi$

   (b) $\overline{(A \cap B)} \cup \overline{(C \cap \overline{A})}$
   $\overline{(A \cap B)} \cup \overline{(C \cap \overline{A})} = (\overline{A} \cup \overline{B}) \cup (\overline{C} \cup \overline{\overline{A}})$
   $= (\overline{A} \cup A) \cup (\overline{C} \cup \overline{B})$
   $= E \cup (\overline{C} \cup \overline{B})$
   $= E$

Solution 2.4.3

1. Let $y \in f(A \cap B)$. There exists $x \in (A \cap B)$ such that $y = f(x)$. Since $x \in A$, we have $y = f(x) \in f(A)$, and similarly, as $x \in B$, we have $y \in f(B)$. Therefore, $y \in f(A) \cap f(B)$, which implies $f(A \cap B) \subset f(A) \cap f(B)$.

2. • "$\subset$": Let $y \in f(A \cup B)$. There exists $x \in A \cup B$ such that $y = f(x)$. If $x \in A$, then $y \in f(A)$. If $x \in B$ and $y \in f(B)$, then in both cases $y \in f(A) \cup f(B)$, so $f(A \cup B) \subset f(A) \cup f(B)$.

   • "$\supset$": Let $y \in f(A) \cup f(B)$. If $y \in f(A)$, there exists $x \in A$ such that $y = f(x)$. Since $x \in A \subset (A \cup B)$, we have $y \in f(A \cup B)$. The same argument applies if $y \in f(B)$. Therefore, $f(A) \cup f(B) \subset f(A \cup B)$.
   By showing both inclusions, we have established the equality.

3. $x \in f^{-1}(F \setminus A) \Leftrightarrow f(x) \in F \setminus A \Leftrightarrow f(x) \notin A \Leftrightarrow x \notin f^{-1}(A) \Leftrightarrow x \in E \setminus f^{-1}(A)$.

Solution 2.4.4

1) $\exp(\mathbb{R}) = \mathbb{R}^{*+}$, $f([0,1[) = [0,1[$, $f(\mathbb{R}) = \mathbb{R}^+$, $f(]-1,2[) = [0,4[$, $f^{-1}(\{3\}) = \{-\sqrt{3}, \sqrt{3}\}$.

1

Solution 2.4.5

1. f is injective because, for $x, y \in [1, +\infty[$, $f(x) = f(y)$ implies $x^2 - 1 = y^2 - 1$, which leads to $x = \pm y$. Since $x, y \in [1, +\infty[$, they have the same sign, so $x = y$.

2. f is surjective because, for $y \in [0, +\infty[$, we're looking for an element $x \in [1, +\infty[$ such that $y = f(x) = x^2 - 1$. The real $x = \sqrt{y+1}$ works, so f is surjective. Therefore, f is bijective.

Solution 2.4.6

We have the following implications:

1. $g \circ f$ injective $\Rightarrow$ f injective.

2. $g \circ f$ surjective $\Rightarrow$ g surjective.
   Suppose $h \circ g \circ f$ is injective and both $g \circ f \circ h$ and $f \circ h \circ g$ are surjective.
   Since $(h \circ g) \circ f$ is injective, we have f is injective. And since $f \circ (h \circ g)$ is surjective, we have f is surjective.
   Therefore, f is bijective, and we can introduce f^{-1}.
   By composition, $h \circ g = (h \circ g \circ f) \circ f^{-1}$ is injective, and therefore, g is injective.
   On the other hand, $g \circ f \circ h$ is surjective, and therefore, g is surjective as well. In the end, g is bijective.
   By composition, $h = (h \circ g) \circ g^{-1}$ is injective, and $h = f^{-1} \circ (f \circ h \circ g) \circ g^{-1}$ is surjective. Thus, h is bijective.

Chapter 3

Binary Relations on a Set

3.1 Introduction

Binary relations are fundamental mathematical tools used to describe connections and interactions between elements of a set. They appear naturally in many areas of mathematics and play an essential role in the study of algebraic structures and ordered systems. In this chapter, we introduce the basic concepts of binary relations and investigate their principal properties such as reflexivity, symmetry, antisymmetry, and transitivity. Particular attention is devoted to equivalence relations and order relations, together with their applications and illustrative examples.

3.2 Binary Relations

Definition 3.2.1

A binary relation is defined as any proposition between two objects, which can be either true or false. We denote it as $x\mathcal{R}y$ and read it as "x is related to y".

Example 3.2.2

1. The inequality "$\leq$" is a binary relation on $\mathbb{N}$, $\mathbb{Z}$, or $\mathbb{R}$.
2. Parallelism "$\|$" and orthogonality "$\perp$" are binary relations on the set of lines in a plane or space.
3. The inclusion "$\subset$" is a binary relation on $P(E)$ or on E. The relation "greater than" on the set of students is a binary relation.

Definition 3.2.3

Given a binary relation $\mathcal{R}$ between elements of a non-empty set E, we say that:

1. $\mathcal{R}$ is Reflexive
$$\Leftrightarrow \forall x \in E, \quad x\mathcal{R}x.$$
2. $\mathcal{R}$ is Transitive
$$\Leftrightarrow \forall x; y; z \in E, \quad (x\mathcal{R}y) \wedge (y\mathcal{R}z) \Rightarrow (x\mathcal{R}z).$$
3. $\mathcal{R}$ is Symmetric
$$\Leftrightarrow \forall x; y \in E, \quad (x\mathcal{R}y) \Rightarrow (y\mathcal{R}x).$$
4. $\mathcal{R}$ is Anti-Symmetric
$$\Leftrightarrow \forall x; y \in E, \quad (x\mathcal{R}y) \wedge (y\mathcal{R}x) \Rightarrow x = y.$$

3.3 Equivalence Relation

Definition 3.3.1

We say that a binary relation $\mathcal{R}$ on a set E is an equivalence relation if it is Reflexive, Symmetric and Transitive.

Let $\mathcal{R}$ be an equivalence relation on a set E.

Definition 3.3.2

1. Two elements x and $y \in E$ are *equivalent* if $x\mathcal{R}y$.
2. The equivalence class of an element $x \in E$, denoted as $\dot{x}$, is the set:
$$\dot{x} = \{y \in E,\ x\mathcal{R}y\}.$$
3. x is called a representative of the equivalence class $\dot{x}$.
4. The quotient set of E by the equivalence relation $\mathcal{R}$, denoted as $E/_{\mathcal{R}}$, is the set of equivalence classes of all elements of E.
5. $\dot{x} = \dot{y} \Leftrightarrow x\mathcal{R}y$.

Example 3.3.3

In $\mathbb{R}$, we define the relation $\mathcal{R}$ by:
$$\forall x, y \in \mathbb{R}; x\mathcal{R}y \Leftrightarrow x^2 - 1 = y^2 - 1.$$
Show that $\mathcal{R}$ is an equivalence relation and give the quotient set $\mathbb{R}/_{\mathcal{R}}$.

1. $\mathcal{R}$ is an equivalence relation.
   (a) $\mathcal{R}$ is Reflexive, because
   $$\forall x \in \mathbb{R}, \quad x^2 - 1 = x^2 - 1 \Rightarrow x\mathcal{R}x.$$
   (b) $\mathcal{R}$ is Symmetric, because
   $$\forall x, y \in \mathbb{R}, \quad x\mathcal{R}y \Rightarrow x^2 - 1 = y^2 - 1.$$
   $$\Rightarrow y^2 - 1 = x^2 - 1.$$
   Since equality is symmetric
   $$\Rightarrow y\mathcal{R}x.$$
   (c) $\mathcal{R}$ is Transitive, because
   $$\forall x; y; z \in \mathbb{R}, \quad (x\mathcal{R}y) \wedge (y\mathcal{R}z) \Rightarrow (x^2 - 1 = y^2 - 1).$$
   $$y^2 - 1 = z^2 - 1.$$
   $$\Rightarrow (x^2 - 1 = z^2 - 1),$$
   because equality is Transitive.
   $$\Rightarrow x\mathcal{R}z.$$
   From **i)**, **ii)**, and **iii)**, we conclude that $\mathcal{R}$ is an equivalence relation.
2. Determine the quotient set $\mathbb{R}/_{\mathcal{R}}$.
   Let $x \in \mathbb{R}$. Then,
   $$\forall y \in \mathbb{R}, \quad x\mathcal{R}y \Leftrightarrow x^2 - 1 = y^2 - 1,$$
   $$\Leftrightarrow x^2 - y^2 = 0,$$
   $$\Leftrightarrow (x - y)(x + y) = 0,$$

$$\Leftrightarrow (y = x) \vee (y = -x).$$

Thus,

$$\dot{x} = \{-x, x\}.$$

Hence,

$$\mathbb{R}/_{\mathcal{R}} = \{\{-x, x\},\ x \in \mathbb{R}\}.$$

Example 3.3.4

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

$$x\mathcal{R}y \Leftrightarrow x + y \quad \text{is an even number.}$$

a) Determine whether $\mathcal{R}$ is reflexive.

b) Determine whether $\mathcal{R}$ is symmetric.

c) Determine whether $\mathcal{R}$ is transitive.

d) Deduce the type of the relation $\mathcal{R}$

e) Determine the equivalence class 0, 1.

Solution

a) Reflexivity

For any $x \in Z$

$x + x = 2x$

which is even. Hence, $x\ \mathcal{R}\ x$ for all x

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

b) Symmetry

If $x\ \mathcal{R}\ y$, then $x + y$ is even. Since

$y + x = x + y$,

it follows that $y\ \mathcal{R}\ x$. Therefore,

$\mathcal{R}$ is symmetric.

c) Transitivity

Assume

$x\ \mathcal{R}\ y$ and $y\ \mathcal{R}\ z$. Then:

$x + y$ is even, and $y + z$ is even.

Adding these two equalities:

$(x + y) + (y + z) = x + z + 2y$ which is even. Hence,

$x + z$ is even, and therefore $x\ \mathcal{R}\ z$

Thus,

$\mathcal{R}$ is transitive.

d) Conclusion

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

e)

Equivalence class of 0

$$\overline{0} = \{x \in Z \mid x + 0 \text{ is even}\}$$

So,

$$\overline{0} = \{\text{all even integers}\}$$

Equivalence class of 1

$$\overline{1} = \{x \in Z \mid x+1 \text{ is even}\} = \{x \in Z \mid x \text{ is odd}\}.$$

So,

$$\overline{1} = \{\text{all odd integers}\}.$$

Proposition 3.3.5

Let $\mathcal{R}$ be an equivalence relation on a set E. Then, the equivalence classes form a partition of E, meaning that every equivalence class is non-empty, the union of equivalence classes is equal to E, two equivalence classes are either disjoint or identical,

$$\forall x, y \in E; \dot{x} \cap \dot{y} = \phi, \quad \text{or} \quad \dot{x} = \dot{y}.$$

3.4 Order Relation

Definition 3.4.1

An order relation on a set E is any binary relation that is Reflexive, Anti-Symmetric, and Transitive. We say that $(E; \mathcal{R})$ is an ordered set (by $\mathcal{R}$) an order relation is often denoted as $\leq$.

Example 3.4.2

The relation "$\subset$" is an order relation on $P(E)$.

1. "$\subset$" is Reflexive, because $\forall A \in P(E)$, we have $A \subset A$.
2. "$\subset$" is Transitive, because
$$\forall A, B, C \in P(E), \quad (A \subset B) \wedge (B \subset C) \Rightarrow A \subset C.$$
3. "$\subset$" is Anti-Symmetric, because
$$\forall A, B \in P(E), \quad (A \subset B) \wedge (B \subset A) \Rightarrow A = B.$$

From (1), (2), and (3) we deduce that "$\subset$" is an order relation on E.

Example 3.4.3

1. The relations "$\leq$", "$\geq$" are order relations on $\mathbb{R}$.
2. The relation "/" (divides) is an order relation on $\mathbb{N}$.

3.4.1 Total or Partial Order

Definition 3.4.4

Let E be a set equipped with a relation of order $\mathcal{X}$. We say that $\mathcal{R}$ is a total order relation if

$$\forall x,\ y \in E, \quad x\mathcal{R}y \text{ or } y\mathcal{X}x.$$

Otherwise, we say that the order is partial, meaning that $\exists x, y \in E$; x is not related to y, and y is not related to x.

Example 3.4.5

1. The relations "$\geq$", "$\leq$" are total order relations on $\mathbb{N}$; $\mathbb{Z}$; $\mathbb{Q}$; $\mathbb{R}$.
2. The relation "/" (divides) is a partial order relation on $\mathbb{N}$.
3. The relation "$\subset$" is a partial order relation on $P(E)$.

3.4.2 Least Element, Greatest Element

Definition 3.4.6

Let $(E, \leq)$ be an ordered set and A a subset of E.

1. We say that $m \in A$ is the least element of A (or a minimum) if:
$$\forall x \in A, \quad m \leq x.$$
2. We say that $M \in A$ is the greatest element of A (or a maximum) if:
$$\forall x \in A, \quad x \leq M.$$

Proposition 3.4.7

[Uniqueness of the minimum and maximum] Let $(E, \leq)$ be an ordered set and A a subset of E.

1. If A has a minimum, it is unique: we denote it $min\ A$.
2. If A has a maximum, it is unique: we denote it $max\ A$.

Example 3.4.8

We define on $\mathbb{Z}$, the order relation $\mathcal{R}$ as follows:

$$\forall n, m \in \mathbb{Z}^*, n\mathcal{R}m \Leftrightarrow \exists k \in \mathbb{N}^* : m = kn.$$

1. The least element of $\mathbb{Z}^*$ by $\mathcal{R}$ is 1
2. $\mathbb{Z}$ does not have a greatest element. Let A, B be subsets of $\mathbb{Z}^*$ such that, $A = \{2, -6, -10, -14, -18, -20\}$, $B = \{7, 6, 2, 3, -42\}$ Determine the least element (min), the greatest element (max) of A; B by the relation $\mathcal{R}$ if they exist.
3. min $A = 2$.
4. max $A = \nexists$.
5. min $B = \nexists$.
6. max $B = -42$.

3.4.3 Upper Bound, Lower Bound

Definition 3.4.9

Let $(E, \leq)$ be an ordered set and A a subset of E.

1. We say that $m \in E$ is a lower bound of A if
$$\forall x \in A, \quad m \leq x.$$
We say that A is bounded below.

We say that $M \in E$ is an upper bound of A if

$$\forall x \in A, \quad x \leq M.$$

2. We say that A is bounded above.
3. We say that A is bounded if it is bounded below and above.

3.4.4 Infimum and Supremum

Definition 3.4.10

Let $(E, \leq)$ be an ordered set and A a subset of E.

1. If the set of lower bounds of A has a greatest element, we call it the infimum of A and denote it $inf\ A$.
2. If the set of upper bounds of A has a least element, we call it the supremum of A and denote it $sup\ A$.

Proposition 3.4.11

Let $(E, \leq)$ be an ordered set and A a subset of E

1. If A has a minimum, then it has an infimum and $min\ A = inf\ A$.
2. If A has a maximum, then it has a supremum and $max\ A = sup\ A$.

Note 3.4.12

The least element of A ($min\ A$), if it exists, is a lower bound of A, however, a lower bound of A may not be the least element of A since it may not necessarily be in A. Similarly for the greatest element ($max\ A$) and the upper bound. This remark expresses that the reverse implication in Proposition 3.4.11 is not always true

Example 3.4.13

Let $E = \{1, a, 2, 5, \gamma\}$, consider $(P(E), \subset)$ ordered, and let A be a subset of $P(E)$.

$$A = \{\{a,\ 2\}, \{2, 5, \gamma\}, \{1, 2, \gamma\}, \{a, 2, 5\}\}.$$

Then,

1. The lower bounds of A are: ϕ and $\{2\}$.
2. $inf A = \{2\}$.
3. A does not have a least element, because $inf A \notin A$.
4. The only upper bound of A is: $E = \{1, a, 2, 5, \gamma\}$.
5. $sup A = E$.
6. A does not have a greatest element, because $sup A \notin A$.

3.5 Exercises

Exercise 3.5.1

Let P^* be the set of prime numbers strictly greater than 2.
We consider the relation $\mathcal{R}$ between two elements of P^* defined as:

$$p\mathcal{R}q \Leftrightarrow \frac{p+q}{2} \in P^*.$$

Is the relation $\mathcal{R}$ reflexive, symmetric, and transitive?

Exercise 3.5.2

Let $\mathcal{R}$ be a reflexive and transitive binary relation.
We define a relation $\mathcal{S}$ as:

$$x\mathcal{S}y \Leftrightarrow x\mathcal{R}y \text{ and } y\mathcal{R}x.$$

Show that $\mathcal{S}$ is an equivalence relation and that $\mathcal{R}$ defines a partial order relation on the equivalence classes of $\mathcal{S}$.

Exercise 3.5.3

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

$$(a,b)\mathcal{R}(a',b') \Leftrightarrow ab' = a'b.$$

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

Exercise 3.5.4

We define the relation $\mathcal{R}$ on $\mathbb{R}^2$ by:

$$(x,y)\mathcal{R}(x^{'},y^{'}) \Leftrightarrow \ x+y = x^{'}+y^{'}$$

1. Show that $\mathcal{R}$ is an equivalence relation.
2. Find the equivalence class of the couple $(0,0)$.

Exercise 3.5.5

We define the relation $\mathcal{T}$ on $\mathbb{R}^2$ by

$$(x,y)\mathcal{T}(x^{'},y^{'}) \Leftrightarrow |x-x^{'}| \leq y^{'}-y.$$

1. Verify that $\mathcal{T}$ is an order relation. Is this order total?
2. Let $(a,b) \in \mathbb{R}^2$ represent the set $\{(x,y) \in \mathbb{R}^2 / (x,y)\mathcal{T}(a,b)\}$.

3.6 Solutions

Solution 3.5.1

1. For all $p \in P^*$, $\frac{p+p}{2} = p \in P^*$, so $p\mathcal{R}p$; hence, $\mathcal{R}$ is reflexive.

2. For all $p, q \in P^*$, $p\mathcal{R}q$ implies $\frac{p+q}{2} \in P^*$, which in turn implies $\frac{q+p}{2} \in P^*$, so $q\mathcal{R}p$, making $\mathcal{R}$ symmetric.

3. For all $p, q, r \in P^*$, if $p\mathcal{R}q$ and $q\mathcal{R}r$, then it follows that $\frac{p+q}{2} \in P^*$ and $\frac{q+r}{2} \in P^*$. However, we cannot always deduce that $\frac{p+r}{2} \in P^*$.

To illustrate, consider a counterexample in the form of a table. In this table, the first row contains values of q, the first column contains values of p, and the values inside represent $\frac{p+q}{2}$:

$p \diagdown q$	3	5	7	11	13	17
3	3	4	5	7	8	10
5	4	5	6	8	9	11
7	5	6	7	9	10	12
11	7	8	9	11	12	14
13	8	9	10	12	13	15
17	10	11	12	14	15	17

In this table, for example, $11\mathcal{R}3$ and $3\mathcal{R}7$, but 11 is not in relation with 7. The cited example in this table is the only counterexample. To find more, you would need to create a larger table. Thus, $\mathcal{R}$ is not transitive.

Solution 3.5.2

1. For all x, we have $x\mathcal{R}x$, and $x\mathcal{R}x \Rightarrow Sx\mathcal{S}x$, so $\mathcal{S}$ is reflexive. If $x\mathcal{S}y$, then $x\mathcal{R}y$ and $y\mathcal{R}x$, which implies $y\mathcal{S}x$ as well, making $\mathcal{S}$ symmetric. If $x\mathcal{S}y$ and $y\mathcal{S}z$, then ($x\mathcal{R}y$ and $y\mathcal{R}x$) and ($y\mathcal{R}z$ and $z\mathcal{R}y$), which further leads to ($x\mathcal{R}y$ and $y\mathcal{R}z$) and ($z\mathcal{R}y$ and $y\mathcal{R}x$), implying ($x\mathcal{R}z$) and ($z\mathcal{R}x$) since $\mathcal{R}$ is transitive. Thus, $x\mathcal{S}z$, and $\mathcal{S}$ is transitive. Therefore, $\mathcal{S}$ is an equivalence relation.

2. We define a relation Δ on the set of equivalence classes of $\mathcal{S}$ as:

$$\dot{x}\Delta\dot{y} \Leftrightarrow x\mathcal{R}y$$

The relation Δ is well-defined, reflexive, and transitive. If $\dot{x}\Delta\dot{y}$ and $\dot{y}\Delta\dot{x}$, then $x\mathcal{R}y$ and $y\mathcal{R}x$, which is equivalent to $x\mathcal{S}y$. Consequently, $\dot{x} = \dot{y}$. This is based on the properties of $\mathcal{R}$ as an equivalence relation, implying $xy \Leftrightarrow \dot{x} = \dot{y}$. Therefore, Δ is antisymmetric. Consequently, Δ is indeed a well-defined order relation on the set of equivalence classes of $\mathcal{S}$.

Solution 3.5.3

1. For all $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$: $ab = ab \Rightarrow (a, b)\mathcal{R}(a, b)$, so $\mathcal{R}$ is reflexive.

For all (a, b), $(a', b') \in \mathbb{Z} \times \mathbb{N}^*$: $(a, b)\mathcal{R}(a', b') \Rightarrow ab' = a'b \Rightarrow a'b = ab' \Rightarrow (a', b')\mathcal{R}(a, b)$; thus, $\mathcal{R}$ is symmetric.

For all (a, b), (a', b'), $(a'', b'') \in \mathbb{Z} \times \mathbb{N}^*$: $(a, b)\mathcal{R}(a', b')$ and $(a', b')\mathcal{R}(a'', b'')$, we have:

$$\begin{cases} ab' = a'b & \text{and} \\ a'b'' = a''b' \end{cases}$$

This leads to:

$$\begin{cases} \frac{ab'}{b} = a' & \text{where } b \neq 0, \\ \text{and} \\ a'b'' = a''b'. \end{cases}$$

Multiplying both sides of the first equation by b'', we get:

$$ab'b'' = a''b'b \Rightarrow ab'b'' = a''b'b.$$

This implies:

$$ab'' = a''b.$$

Therefore, $(a,b)\mathcal{R}(a'',b'')$. Thus, $\mathcal{R}$ is transitive, and consequently, $\mathcal{R}$ is an equivalence relation.

2. If $(a,b) \in \dot{\widehat{(p,q)}}$, then $aq = pb$. This means that q divides pb, and since $p \wedge q = 1$, by Gauss's theorem, q divides b. Hence, there exists an integer $d \in \mathbb{Z}$ such that $b = dq$. Substituting this into $aq = pb$, we get $adq = pdq$ where $q \neq 0$, so $a = dp$.

   Therefore,

$$\dot{\widehat{(p,q)}} = \{(dp, dq) \mid d \in \mathbb{Z}\}.$$

Solution 3.5.4

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

   1)

   a) $\mathcal{R}$ is reflective if and only if $\forall (x,y) \in \mathbb{R}^2 : (x,y)\mathcal{R}(x,y)$

   $(x,y)\mathcal{R}(x,y) \Leftrightarrow \ x + y = x + y$

   Hence $\mathcal{R}$ is reflexive.

   b) $\mathcal{R}$ is symmetric if and only if $\forall (x,y), (x',y') \in \mathbb{R}^2 : (x,y)\mathcal{R}(x',y') \Rightarrow (x',y')R(x,y)$

   $(x,y)\mathcal{R}(x',y') \Leftrightarrow x + y = x' + y' \Rightarrow x' + y' = x + y \Leftrightarrow (x',y')R(x,y)$

   Hence $\mathcal{R}$ is symmetric.

   c) $\mathcal{R}$ is transitive if and only if $\forall (x,y), (x',y'), (x'',y'') \in \mathbb{R}^2 : (x,y)\mathcal{R}(x',y') \wedge (x',y')\mathcal{R}(x'',y'') \Rightarrow (x,y)\mathcal{R}(x'',y'')$

$$(x,y)\mathcal{R}(x',y') \wedge (x',y')\mathcal{R}(x'',y'') \Leftrightarrow \begin{cases} x + y = x' + y' \\ \wedge \\ x' + y' = x'' + y'' \end{cases}$$
$$\Rightarrow x + y = x'' + y''$$
$$\Leftrightarrow (x,y)\mathcal{R}(x'',y'')$$

   Hence $\mathcal{R}$ is transitive.

   Thus $\mathcal{R}$ is an equivalence relation.

   2)

   Let's find the equivalence class of the couple $(0,0)$.

$$\begin{aligned} \dot{\widehat{(0,0)}} &= \{(x,y) \in \mathbb{R}^2 / \ (x,y)\mathcal{R}(0,0)\} \\ &= \{(x,y) \in \mathbb{R}^2 / \ x + y = 0 + 0\} \\ &= \{(x,y) \in \mathbb{R}^2 / \ x + y = 0\} \\ &= \{(x,y) \in \mathbb{R}^2 / \ y = -x\} \\ &= \{(x,-x) / x \in \mathbb{R}\}. \end{aligned}$$

Solution 3.5.5

1. $\mathcal{T}$ is an order relation if and only if it is reflexive and antisymmetric and transitive.

a) $\mathcal{T}$ is reflexive if and only if $\forall (x,y) \in \mathbb{R}^2$, $(x,y)\mathcal{T}(x,y)$

$(x,y)\mathcal{T}(x,y) \Leftrightarrow |x-x| \leq y-y \Rightarrow 0 \leq 0$

Hence $\mathcal{T}$ is reflexive.

b) $\mathcal{T}$ is anti-symmetric if and only if

$\forall (x,y),(x^{'},y^{'}) \in \mathbb{R}^2$, $((x,y)\mathcal{T}(x^{'},y^{'}) \wedge (x^{'},y^{'})\ \mathcal{T}(x,y)\ ) \Rightarrow (x,y)=(x^{'},y^{'})$

$(x,y)\mathcal{T}(x^{'},y^{'}) \wedge (x^{'},y^{'})\ \mathcal{T}(x,y) \Rightarrow |x-x^{'}| \leq y^{'}-y$ and $|x^{'}-x| \leq y-y^{'}$

$$\begin{aligned}
&\Rightarrow 2|x-x^{'}| \leq 0\\
&\Rightarrow |x-x^{'}| = 0\\
&\Rightarrow x = x^{'}\\
&\Rightarrow y^{'}-y \geq 0 \ \text{ and } \ y-y^{'} \geq 0\\
&\Rightarrow y^{'}-y \geq 0 \ \text{ and } \ y^{'}-y \leq 0\\
&\Rightarrow y^{'}-y = 0 \ \Rightarrow y^{'} = y
\end{aligned}$$

Hence $(x,y)=(x^{'},y^{'})$, then $\mathcal{T}$ is anti-symmetric.

c) $\mathcal{T}$ is transitive if and only if

$\forall (x,y),(x^{'},y^{'}),(x^{''},y^{"}) \in \mathbb{R}^2$, $((x,y)\mathcal{T}(x^{'},y^{'}) \wedge (x^{'},y^{'})\ \mathcal{T}(x^{"},y^{"})\ ) \Rightarrow (x,y)\mathcal{T}(x^{"},y^{"})$

$((x,y)\mathcal{T}(x^{'},y^{'}) \wedge (x^{'},y^{'})\ \mathcal{T}(x^{"},y^{"})\ ) \Rightarrow |x-x^{'}| \leq y^{'}-y$ and $|x^{'}-x^{"}| \leq y^{"}-y^{'}$

$$\begin{aligned}
&\Rightarrow (y-y^{'} \leq x-x^{'} \leq y^{'}-y) \text{ and } (y^{'}-y^{"} \leq x^{'}-x^{"} \leq y^{"}-y^{'})\\
&\Rightarrow y-y^{"} \leq x-x^{"} \leq y^{"}-y\\
&\Rightarrow \left|x-x^{"}\right| \leq y^{"}-y\\
&\Rightarrow (x,y)\mathcal{T}(x^{"},y^{"})
\end{aligned}$$

Hence $\mathcal{T}$ is transitive, then it is an order relation.

The order is not total because $\exists (x,y)=(1,7)$ and $(x^{'},y^{'})=(3,7)$ such that if we assumes that $(x,y)\mathcal{T}(x^{'},y^{'}) \Rightarrow |1-3| \leq 7-7=0$ which is absurd.

Moreover $(x^{'},y^{'})\mathcal{T}(x,y) \Rightarrow |3-1| \leq 7-7=0$ false

2. Let $(a,b) \in \mathbb{R}^2$, let us determine the set $\{(x,y) \in \mathbb{R}^2 / (x,y)\mathcal{T}(a,b)\}$.

$$\begin{aligned}
(x,y)\mathcal{T}(a,b) &\Leftrightarrow |x-a| \leq b-y\\
&\Leftrightarrow (x-a)^2-(y-b)^2 \leq 0\\
&\Leftrightarrow [(x-a)+(y-b)][(x-a)-(y-b)] \leq 0\\
&\Leftrightarrow [(x-a+y-b) \geq 0 \wedge (x-a)-(y-b) < 0]\\
&\vee\ [(x-a+y-b) < 0 \wedge (x-a)-(y-b) \geq 0].
\end{aligned}$$

we put:

D_1 : the closed half-plane of equations $(x-y-a+b) \geq 0$.

D_2 : the open half-plane of equations $(x+y-a-b) < 0$.

D_3 : the open half-plane of equations $(x-y-a+b) < 0$.

D_4 : the closed half-plane of equations $(x+y-a-b) \geq 0$.

From where

$(a,b) = \{(x,y) \in \mathbb{R}^2 / (x,y)\mathcal{T}(a,b)\} = (D_1 \cap D_2) \cup (D_3 \cap D_4)$.

Chapter 4

Algebraic Structures

4.1 Introduction

Algebraic structures constitute one of the principal foundations of modern algebra and provide a unified framework for studying mathematical systems equipped with operations satisfying specific properties. These structures arise naturally in many branches of mathematics and have numerous applications in physics, computer science, and engineering.
In this chapter, we introduce the fundamental notions of algebraic structures, particularlygroups, rings, and fields, together with their basic properties and examples.
The objective of this chapter is to familiarize students with abstract algebraic reasoning and the study of mathematical structures through axiomatic methods.

4.2 Internal Composition Law

Definition 4.2.1

An internal composition law (LCI) on a set E is any function $\star : E \times E \to E$. A subset F of E is said to be "stable" with respect to the law if

$$\forall x, y \in F;\ x \star y \in F.$$

Example 4.2.2

1. $\cap$ and $\cup$ are internal composition laws on $P(E)$.
2. The sum " $+$ " and the product " $\cdot$ " are $LCIs$ on $\mathbb{N}$, $\mathbb{N}^*$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, but not on $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$.
3. The difference " $-$ " on $\mathbb{R}$, $\mathbb{C}$.
4. The composition " $\circ$ " of mappings defined on F into F.

Example 4.2.3

Let

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

and

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

F is not stable with respect to the intersection $\cap$ and the union $\cup$ because:

$$\exists \{1,2\},\ \{2,3\} \in F,\ \{1,2\} \cap \{2,3\} = \{2\} \notin F,$$

$$\exists \{1,2\},\ \{2,3\} \in F,\ \{1,2\} \cup \{2,3\} = \{1,2,3\} \notin F,$$

Definition 4.2.4

Let $\star$ and $\triangle$ be two internal composition laws (LCI) on a set E, we say that:

1. It is commutative if:
$$\forall x, y \in E, \quad x \star y = y \star x.$$
2. It is associative if:
$$\forall x, y \in E, \quad (x \star y) \star z = x \star (y \star z).$$
3. Exists $e \in E$ is a left neutral element (respectively right neutral) of the law if
$$\forall x \in E; e \star x = x \ (respectively x \star e = x).$$
If e is a neutral element both on the left and right of $\star$ we say that e is a neutral element of $\star$.
4. Let $e \in E$ be a neutral element, we say that an element $x \in E$ is invertible, or symmetric, on the right (respectively on the left) if
$$\exists x' \in E, \quad x \star x' = e \ (respectively x' \star x = e).$$
We say x is invertible (or symmetrical) if it is invertible on the right and on the left of $\star$. and x' is called an inverse (or a symmetric) on the right (respectively on the left) of x.
5. $\star$ is distributive with respect to $\triangle$ if:
$$\forall x, y, z \in E, x \star (y \triangle z) = (x \star y) \triangle (x \star z) \quad \text{and} \quad (y \triangle z) \star x = (y \star x) \triangle (z \star x).$$
6. We say that an element $r \in E$ is right-regular (respectively left-regular) of $Soit$ if
$$\forall x, y \in E, x \star r = y \star r \Rightarrow x = y.$$
$$(respectively \forall x, y \in E, r \star x = r \star y \Rightarrow x = y).$$

Example 4.2.5

1. The sum and the product on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are associative and commutative, and have respective neutral elements 0 and 1.
2. The difference is neither associative nor commutative on $\mathbb{R}$.
3. The composition " $\circ$ " is associative, but not commutative on mappings defined from F into F , it has a neutral element, which is the application Id_F.
4. The laws $\cap$, $\cup$, $\triangle$ on $P(E)$ are associative and commutative. They have respective neutral elements E, ϕ, ϕ.

Note 4.2.6

1. If $\star$ is an associative internal composition law on E that has a neutral element, then this neutral element is unique
2. The neutral element e is invertible (or symmetrical) and its unique inverse (or symmetric) is e.
3. If the symmetric element x' of x exists, it is unique. It is generally denoted by x^{-1}.

4.3 Groups

Definition 4.3.1

A group is a non-empty set G equipped with an internal composition law $\star$, denoted $(G, \star)$ such that :

1. $\star$ is associative ;
2. $\star$ has a neutral element e.
3. every element of G is symmetrical (has a symmetrical) for $\star$.

If it is commutative, we say that $(G, \star)$ is commutative, or abelian.

Example 4.3.2

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ endowed with the sum are abelian groups.
2. $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ endowed with the product are abelian groups.
3. $P(E)$ endowed with $\triangle$ is an abelian group.

Example 4.3.3

The following pairs are not groups.

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

4.3.1 Subgroups

Definition 4.3.4

A subgroup of a group $(G, \star)$ is a non-empty subset H of G such that:

1. $\star$ induces an internal composition law on H.
2. H equipped with this law is a group. In practice, to show that a non-empty subset H of G constitutes a subgroup, it suffices to verify one of the following propositions:

Proposition 4.3.5

Let $(G, \star)$ be a group and $H \subset G$ then, H is a subgroup of

$$G \Leftrightarrow \begin{cases} i) & H \neq \phi, \\ ii) & \forall x, y \in H, \quad x \star y \in H, (H \text{ is closed under } \star), \\ iii) & \forall x \in H, \quad x^{-1} \in H, (x^{-1} \text{ is the inverse of } x.) \end{cases}$$

Proposition 4.3.6

Let $(G, \star)$ be a group and $H \subset G$. Then, H is a subgroup of

$$G \Leftrightarrow \{ \ i) \ H \neq \phi \ \ ii) \ \forall x, y \in H, \quad x \star y^{-1} \in H$$

Note 4.3.7

If e is the neutral element of a group $(G, \star)$, then every subgroup of G contains e and we deduce the following property:

Proposition 4.3.8

Let $(G,\star)$ be a group, e the neutral element of $\star$ and H a subset of G. Then, H is a subgroup of

$$G \Leftrightarrow \{\ i)\ e \in H \quad ii)\ \forall x,y \in H, \quad x \star y^{-1} \in H$$

Example 4.3.9

1. Consider the group $(\mathbb{C}^*\ ,\ \times\ )$. Let

$$U = \{z \in \mathbb{C};\ \ |z| = 1\}\,.$$

Show that U is a subgroup of $\mathbb{C}^*$

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

$$n\mathbb{Z} = \{np,\ p \in \mathbb{Z}\}\,,$$

is a subgroup of $(Z,+)$.

Solution

1. (a) $|1| = 1$. Thus, $1 \in U$. Hence $U \neq \phi$.

(b) Let

$$z_1 z_2 \in U, \quad \left|z_1 \times z_2^{-1}\right| = \left|\frac{z_1}{z_2}\right| = \frac{1}{1} = 1 \Rightarrow z_1 \times z_2^{-1} \in U.$$

Therefore, $(U\ ,\times)$ is a subgroup of $(\mathbb{C}^*\ ,\ \times\ )$.

2. (a) We have $0 \in n\mathbb{Z}$ because

$$\exists p = 0, \quad n \times 0 = 0 \in n\mathbb{Z}.$$

Thus $n\mathbb{Z} \neq \phi$.

(b) For all

$$x, y \in n\mathbb{Z},\ \exists p_1, p_2 \in \mathbb{Z}, x = np_1, y = np_2.$$

Then,

$$x - y = np_1 - np_2 = n(p_1 - p_2) = nh,$$

with

$$h = p_1 - p_2 \in \mathbb{Z}.$$

Therefore $x - y \in nZ$. So, $(n\mathbb{Z},+)$ is a subgroup of $(Z,+)$.

4.3.2 Group Homomorphisms

Definition 4.3.11

Let $(G,\star)$ and $(G^{'},T)$ be two groups. A function f from G to $G^{'}$ is a "group homomorphism" when:

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

- If $G = G'$ and $\star = T$, it is called an endomorphism.
- If f is bijective, it is called an isomorphism.
- If f is a bijective endomorphism, it is called an automorphism.

Example 4.3.12

1. $x \to 2^x$ is an isomorphism from $(\mathbb{R},+)$ to $(\mathbb{R}_+^*,\times)$.
2. $x \to 2x$ is an automorphism of $(\mathbb{R},+)$.

3. $x \to 3\ln x$ is an isomorphism from $(\mathbb{R}_+^*, \times)$ to $(\mathbb{R}, +)$.
4. $z \to |z|$ is a homomorphism from $(\mathbb{C}^*, \times)$ to $(\mathbb{R}_+^*, \times)$.

Example 4.3.13

Show that the composition of two group homomorphisms is a group homomorphism.

Proposition 4.3.14

Let e, e' be the neutral elements of G and G' respectively. Let $f : G \to G'$ be a group homomorphism. Then,

1. $f(e) = e'$.
2. $\forall x \in G;\ f(x^{-1}) = (f(x))^{-1}$ (x^{-1} is the inverse of x).

Proposition 4.3.15

Let $f : (G; *) \to (G'; T)$ be a group homomorphism. Then,

1. The image of a subgroup of G under f is a subgroup of G'.
2. The inverse image of a subgroup of G' under f is a subgroup of G.

Proof

1. Let H be a subgroup of G and show that $f(H)$ satisfies the two conditions of the subgroup characterization.
   (a) Since H is a subgroup of G, then $e \in H$ hence $f(e) \in f(H)$, therefore $f(H) \neq \phi$.
   (b) Let $x', y' \in f(H)$, then there exist $xy \in H$ such that $x' = f(x)$ and $y' = f(y)$, thus according to the second property. We have
   $$x'T(y')^{-1} = f(x)T(f(y))^{-1} = f(x)Tf(y^{-1}) = f(x * y^{-1}),$$
   and since H is a subgroup of G then $(x * y^{-1}) \in H$. Hence
   $$x'T(y')^{-1} = f(x * y^{-1}) \in f(H).$$
   From i) and ii) we deduce that $f(H)$ is a subgroup of G'.
2. Let H' be a subgroup of G'. Then,
   (a) According to the first property $f(e) = e'$ and since H' is a subgroup of G' then $e' \in H'$. Hence
   $$e \in f^{-1}(H').$$
   (b) Let $x, y \in f^{-1}(H')$, then $f(x), f(y) \in H'$ and since H' is a subgroup of G'. Then $f(x)T(f(y))^{-1} \in H'$ and from the second property we deduce that
   $$f(x * y^{-1}) = f(x)Tf(y^{-1}) = f(x)T(f(y))^{-1} \in H',$$
   which shows that
   $$(x * y^{-1}) \in f^{-1}(H').$$
   From i) and ii) we deduce that $f^{-1}(H')$ is a subgroup of G.

4.3.3 The kernel and image of a homomorphism

Definition 4.3.16

Let f be a homomorphism from G to G', e, e' are the neutral elements of G, G' respectively:

1. The kernel of f, denoted $\ker f$, is the set defined by:
$$\ker f = \{x \in G,\ f(x) = e'\} = f^{-1}(e').$$
2. The image of f, denoted $\text{Im } f$, is the set defined by:
$$\text{Im } f = \{f(x),\ x \in G\} = f(G).$$

Proposition 4.3.17

As special cases of proposition 4.3.15. We have:

1. Im f is a subgroup of (G', T),
2. $\ker f$ is a subgroup of $(G, *)$. The following result is much more interesting, as it greatly reduces the work to show that a homomorphism is bijective.

Proposition 4.3.18

Let f: $(G, *) \to (G', T)$ be a group homomorphism. Then,

1. f is injective if and only if $\ker f = \{e\}$, (where e is the neutral element of G).
2. f is surjective if and only if $\text{Im } f = G'$.

4.4 Ring Structure

Definition 4.4.1

A set A equipped with two internal composition laws $+$ and $\times$ is called a ring if:

1. $(A, +)$ is an abelian group (the neutral element of $+$ is denoted by 0 or 0_A).
2. $\times$ is associative and distributive with respect to $+$.
   (a) If furthermore $\times$ is commutative, then $(A, +, \times)$ is called a commutative ring.
   (b) If A has a neutral element for $\times$, it is denoted by 1 or 1_A, and $(A, +, \times)$ is called a unitary ring.

Example 4.4.2

The sets $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ are unitary commutative rings.

Example 4.4.3

Consider the quotient set of $\mathbb{Z}$ by the congruence relation modulo n, defined in example 4.4.2

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

We define on this set the two internal composition laws "+" and "×" as:

$$\forall p, q \in \mathbb{Z}/n\mathbb{Z} :\ \overline{p} + \overline{q} = \widehat{\overline{p+q}} \text{ and } \overline{p} \times \overline{q} = \widehat{\overline{p \times q}},$$

where $+$ and $\times$ are the addition and multiplication defined on $\mathbb{Z}$ respectively. It can be easily verified that

for all $n \in \mathbb{N}$, the quotient set $\mathbb{Z}/n\mathbb{Z}$ equipped with the two operations "$+$" and "$\times$" forms a structure of unitary commutative ring, where 0 and 1 are the neutral elements of "$+$" and "$\times$" respectively.

4.4.1 Subring

Definition 4.4.4

Let $(A, +, \times)$ be a ring. A non-empty subset A' of A is a subring of A when:

1. $1_A \in A$,
2. the laws $+$ and $\times$ induce internal composition laws on A', and with these laws, $(A', +, \times)$ is a ring.

Practically, to show that a non-empty subset A' of A is a subring, it suffices to verify the following proposition:

Proposition 4.4.5

Let $(A, +, \times)$ be a ring and $A' \subset A$. Then, A' is a subring of A

$$\Leftrightarrow \begin{cases} i) A' \neq \emptyset \\ ii) \forall x, y \in A' : x - y \in A' \\ iii) \forall x, y \in A' : x \times y \in A' \end{cases}$$

4.4.2 Ring Homomorphisms

Definition 4.4.6

Let $(A, +, \times)$ and $(B, \oplus, \otimes)$ be two rings and $f : A \to B$. We say that f is a ring homomorphism if:

$$\forall x, y \in A : f(x + y) = f(x) \oplus f(y) \text{ and } f(x \times y) = f(x) \otimes f(y)$$

1. If $A = B$, we say that f is an endomorphism of the ring A.
2. If f is bijective, we say that f is an isomorphism of rings.
3. If f is bijective and $A = B$, we say that f is an automorphism of rings.

Example 4.4.7

Let $z \mapsto \overline{z}$ is an automorphism of rings of $\mathbb{C}$.

Example 4.4.8

Show that the composition of two ring homomorphisms is a ring homomorphism.

4.4.3 Zero Divisors, Invertible Elements

Definition 4.4.9

Let $(A, +, \times)$ be a commutative ring. If there exist in the ring A two elements a and b such that:

$$(a \times b = 0) \wedge (a \neq 0 \wedge b \neq 0).$$

Then a and b are called zero divisors.

Definition 4.4.10

We call a ring integral or complete, any ring that does not contain a zero divisor other than 0 itself, that is:

$$ab = 0 \Leftrightarrow a = 0 \text{ or } b = 0.$$

Example 4.4.11

1. $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, are integral rings.
2. The ring of matrices $M_n(\mathbb{k})$ equipped with the operations $+$ (matrix addition) and $\times$ (matrix multiplication) is not integral, because:

$$\exists A = \begin{pmatrix} 0 & -1 \\ 0 & 5 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R}),$$

$$\exists B = \begin{pmatrix} 2 & -3 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R}).$$

But

$$AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Definition 4.4.12

Let $(A, +, \times)$ be a commutative ring. We say that $x \in A$ is invertible if it has a multiplicative inverse.

Example 4.4.13

1. In $\mathbb{Z}$, the invertible elements are 1 and -1.
2. In the rings $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, all non-zero elements are invertible.

Proposition 4.4.14

In a commutative ring $(A, +, \times)$:

1. 0_A is never invertible.
2. If x is invertible, then it is not a zero divisor.
3. If $x_1, x_2, y \in A$ are integral, with $y \neq 0$ and $x_1 y = x_2 y$, then $x_1 = x_2$.

We say that "we can simplify" (which does not mean divide) by $y \neq 0$: $x_1 y = x_2 y \Rightarrow (x_1 - x_2)y = 0 \Rightarrow x_1 - x_2 = 0$ or $y = 0$ because A is integral $\Rightarrow x_1 = x_2$, since $y \neq 0$.

4.4.4 Ideals

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

Definition 4.4.15

A right (respectively left) ideal of the ring A is any subset $I \subset A$ such that:

1. I is a subgroup of $(A, +)$,
2. $\forall x \in A$, $\forall y \in I$, $x \times y \in I$ (respectively $y \times x \in I$):
   (a) If I is both a right and left ideal of A, we call I a "two-sided ideal" of A.
   (b) If the ring A is commutative, every ideal of A is two-sided, and in this case, we only talk about

. ideals without specifying whether they are right, left, or two-sided.

Example 4.4.16

1. Let $(A, +, \times)$ be a ring, then $I = 0_A$ is a two-sided ideal of A.
2. In the commutative ring $(\mathbb{Z}, +, \times)$, $n\mathbb{Z}$ is an ideal.

Definition 4.4.17

We call principal ideal of a commutative ring $(A, +, \times)$, any ideal I of A such that:

$$\exists x \in A,\ I = xA.$$

The ring A is said to be principal if all its ideals are principal.

4.5 Fields

Definition 4.5.1

An associative ring with unity $(\Bbbk, +, \times)$ is called a field if every nonzero element of $\Bbbk$ is invertible. If $\Bbbk$ is commutative as well, we call $\Bbbk$ a commutative field. It is noteworthy that in practice, all fields used are commutative.

Example 4.5.2

$(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, and $(\mathbb{C}, +, \times)$ are fields.

Proposition 4.5.3

Every field is an integral domain.

Proof

Let $a \in A$ and consider the ring homomorphism $A \to A$, $x \mapsto ax$. Then this ring homomorphism is injective, as its kernel is reduced to 0_A since A is an integral domain.
Since A is finite, this homomorphism is necessarily bijective, and thus there exists $x \in A$ such that $ax = 1_A$. By the commutativity of A, we also have $xa = 1_A$, and thus a has an inverse. Consequently, A is a field.

4.5.1 Subfields

Definition 4.5.4

A subfield of a field $(\Bbbk, +, \times)$ is any subset $\Bbbk'$ of $\Bbbk$ such that, equipped with the restrictions of the operations $+$ and $\times$, it forms a field.

Proposition 4.5.5

$\Bbbk' \subset \Bbbk$ is a subfield of $(\Bbbk, +, \times)$ if and only if

1. $\Bbbk' \neq \emptyset$.
2. $\forall x, y \in \Bbbk'$, $x - y \in \Bbbk'$ and $xy^{-1} \in \Bbbk'$. We also have the following characterization of fields.

Proposition 4.5.6

Let $(\mathbb{k}, +, \times)$ be a commutative ring with unity. Then $\mathbb{k}$ is a field if and only if the only ideals of $\mathbb{k}$ are $0_{\mathbb{k}}$ and $\mathbb{k}$ itself.

Example 4.5.7

$(\mathbb{Z}, +, \times)$ is not a field because the only ideals in $\mathbb{Z}$ are $0_{\mathbb{k}}$, $n\mathbb{Z}$ and $\mathbb{Z}$.

Example 4.5.8

Consider the quotient ring $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$ defined in example 4.3.3 In this ring, we consider the cases $n = 2$, 3, 4.
For instance, let's write down the multiplication tables for the three quotient sets $\mathbb{Z}2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$.

1. In $\mathbb{Z}/2\mathbb{Z} = \{\dot{0}, \dot{1}\}$, the table is:

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

2. In $\mathbb{Z}/3\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\}$, the table is:

$\dot{\times}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{1}$

3. In $\mathbb{Z}/4\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}\}$, the table is:

$\dot{\times}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{0}$	$\dot{2}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

From these tables, we observe that all nonzero elements in $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are invertible, thus $(\mathbb{Z}/2\mathbb{Z}, \dot{+}, \dot{\times})$ and $(\mathbb{Z}/3\mathbb{Z}, \dot{+}, \dot{\times})$ are commutative fields. However, in $\mathbb{Z}/4\mathbb{Z}$, only elements 1 and 3 are invertible, while 2 is not. Therefore, $(\mathbb{Z}/4\mathbb{Z}, \dot{+}, \dot{\times})$ is not a field.

More generally, it can be shown that a necessary and sufficient condition for the ring $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$ to be a field is that the natural number n is a prime number.

4.6 Exercises

Exercise 4.6.1

We equip $\mathbb{R}$ with the internal composition law defined as:

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

1. Show that $\star$ is commutative, associative, and has a neutral element.
2. Determine the symmetrizable elements.

Exercise 4.6.2

Show that $(G, \star)$ is a group and specify whether it is abelian (commutative):

$$x \star y = \frac{x + y}{1 + xy}, \text{ on } G = (-1, 1).$$

Exercise 4.6.3

Let be the set $\mathbb{R}^* \times \mathbb{R}$ provided with internal law $\star$ such that

$$(a, b) \star (\alpha, \beta) = (a\alpha, \frac{\beta}{a} + b\alpha)$$

Show that $(\mathbb{R}^* \times \mathbb{R}, \star)$ is a group, is it commutative?

Exercise 4.6.4

Let be the set $\mathbb{R}_+^* \times \mathbb{R}$ provided with internal law $\star$ such that

$$(a, b) \star (\alpha, \beta) = (a\alpha, a\beta + b)$$

Show that $(\mathbb{R}_+^* \times \mathbb{R}, \star)$ is a group, is it commutative?

Exercise 4.6.5

1. Determine if part H is a subgroup of group G.
   (a) $G = (\mathbb{Z}, +)$; $H = \{\text{even numbers}\}$
   (b) $G = (\mathbb{Z}, +)$; $H = \{\text{odd numbers}\}$.
2. Show that $U = \{z \in \mathbb{C}, |z| = 1\}$ equipped with multiplication is a subgroup of $(\mathbb{C}^*, \times)$.

Exercise 4.6.6

Let $(G, \star)$ be a group. Demonstrate that the following are subgroups of G:

1. $C(G) = \{x \in G : \forall y \in G, xy = yx\}$, $C(G)$ is called the center of G.
2. $aHa^{-1} = \{aha^{-1} : h \in H\}$ where $a \in G$ and H is a subgroup of G.

Exercise 4.6.7

Are the following mappings homomorphisms of groups? If yes, calculate the kernel and the image, and deduce if they are isomorphisms of groups or automorphisms of groups.

1. $\varphi : (\mathbb{R}^*, \times) \to (\mathbb{R}^*, \times)$, $\varphi : x \mapsto x^n$, $n \in \mathbb{N}$.

2. $\psi : (\mathbb{R}, \times) \to (\mathbb{C}^*, \times)$, $\psi : t \mapsto e^{2\pi i t}$.

Exercise 4.6.8

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

$$\begin{aligned} f + g : \quad G \quad &\to G \\ x \quad &\mapsto f(x) + g(x). \end{aligned}$$

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

Exercise 4.6.9

We denote the set of real numbers as follows:

$$A = \{m + \sqrt{6}n \mid m, n \in \mathbb{Z}\}.$$

1. Show that $(A, +, \times)$ (set equipped with real addition and multiplication) is a subring of $(\mathbb{R}, +, \times)$.
2. Consider the mapping φ from A to itself defined as:

   $$\varphi(m + \sqrt{6}n) = m - \sqrt{6}n.$$

   Show that φ is an automorphism of the ring $(A, +, \times)$ (i.e., it is a bijection and a homomorphism for both operations).
3. For all $x \in A$, define $N(x) = x\varphi(x)$. Show that N is a mapping from A to $\mathbb{Z}$ and it is a homomorphism for multiplication.
4. Show that x is an invertible element in A if and only if $N(x) = \pm 1$.
5. Verify that $5 + 2\sqrt{6}$ is invertible in A and find its inverse.

Exercise 4.6.10

1. Let

   $$G = \{x \in \mathbb{R} \mid x > 0\}$$

   with the operation

   $$x \star y = xy.$$

   Prove that

   a) $(G, \star)$ is a group.

   b) Determine whether the group is abelian.

2. Consider the subset

   $$H = \{6k \mid k \in \mathbb{Z}\}$$

   a) Prove that $(H, +)$ is a subgroup of $(\mathbb{Z}, +)$

   b) Determine all cosets of H in Z

Exercise 4.6.11

Let

$$R = \{a + b\sqrt{2} \mid a, b \in Z\}$$

With the usual addition and multiplication.

a) Prove that $(R, +, \times)$ is a ring.

b) Is $(R, +, \times)$ commutative?

c) Does $(R, +, \times)$ have a unity element?

4.7 Solutions

Solution 4.6.1

1. It is clear that $\star$ is commutative and associative, and accepts a neutral element $e = 0$,

$$x \star 0 = \sqrt{x^2 + 0^2} = |x| = x, \text{ as } x > 0.$$

2. Since $\star$ admits a neutral element, we look for symmetrizable elements if they exist. Suppose y is the symmetric of x. Then,

$$\forall x \in \mathbb{R}^+; \quad x \star y = 0 \Rightarrow \sqrt{x^2 + y^2} = 0 \Rightarrow x^2 = -y^2,$$

which is impossible. Thus, $\nexists y \in \mathbb{R}^+$ such that $x \star y = 0$. Therefore, no element of $\mathbb{R}^{+*}$ accepts a symmetric element. The only symmetrizable element with respect to $\star$ is the neutral element $e = 0$ (the neutral element is symmetrical to itself).

Solution 4.6.2

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

1. According to the question, it's not announced that $\star$ is an internal composition law on G. Therefore, we first verify that $\star$ is indeed a well-defined internal composition law on G, i.e., if $x, y \in G$, then $x \star y \in G$:

   Let's study the function defined on $]-1;1[$ by $f(t) = \frac{t+y}{1+ty}$. It's differentiable on $[-1;1]$, and its derivative satisfies $f'(t) = \dfrac{1 - y^2}{(1 + ty)^2} > 0$ on $]-1;1[$. Thus, f is strictly increasing on $[-1;1]$.

   Since

$$f(-1) = \frac{(-1 + y)}{(1 - y)} = -1,$$

   and

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

   Then,

$$f(-1) < x \star y = f(x) < f(1),$$

   hence $x \star y \in G$.

2. The law is associative: for all

$$x, y, z \in G, \quad x \star (y \star z) = \frac{x + (y \star z)}{1 + x(y \star z)} = \frac{x + \frac{y+z}{1+yz}}{1 + x\frac{y+z}{1+yz}} = \frac{x + y + z + xyz}{1 + xy + xz + yz},$$

   and a similar calculation yields the same result for $(x \star y) \star z$.

3. e is a neutral element for the law, so for all $x \in G$, $x \star e = x \Rightarrow x + e = x + xe^2$, which implies $e(1 - x^2) = 0$, hence $e = 0$. Thus, it admits a neutral element $e = 0$.

4. Every element $x \in G$ is symmetrizable, and the symmetrical element is $-x$. Indeed, $x \star (-x) = (-x) \star x = 0$. Moreover, the law is clearly abelian because for all $x; y \in G$, $x \star y = \frac{x+y}{1+xy} = y \star x$. Therefore, $(G; \star)$ is an abelian group.

Solution 4.6.3

1)

Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in \mathbb{R}^* \times \mathbb{R}$

$$\begin{aligned}[(a_1, b_1) \star (a_2, b_2)] \star (a_3, b_3) &= (a_1 a_2, \tfrac{b_2}{a_1} + b_1 a_2) \star (a_3, b_3) \\ &= (a_1 a_2 a_3, \tfrac{b_3}{a_1 a_2} + (\tfrac{b_2}{a_1} + b_1 a_2) a_3) \\ &= (a_1 a_2 a_3, \tfrac{b_3}{a_1 a_2} + \tfrac{b_2 a_3}{a_1} + b_1 a_2 a_3)\end{aligned}$$

$(a_1,b_1)\star[(a_2,b_2)\star(a_3,b_3)]=(a_1,b_1)\star(a_2a_3,\frac{b_3}{a_2}+b_2a_3)$
$=(a_1a_2a_3,\frac{\frac{b_3}{a_2}+b_2a_3}{a_1}+b_1a_2a_3)$
$=(a_1a_2a_3,\frac{b_3}{a_1a_2}+\frac{b_2a_3}{a_1}+b_1a_2a_3)$
Then, $[(a_1,b_1)\star(a_2,b_2)]\star(a_3,b_3)=(a_1,b_1)\star[(a_2,b_2)\star(a_3,b_3)]$.
therefore the law $\star$ is an associative
2)
$\exists^?(\alpha,\beta)\in\mathbb{R}^*\times\mathbb{R},\forall(a,b)\in\mathbb{R}^*\times\mathbb{R}:(a,b)\star(\alpha,\beta)=(a,b)$
$(a,b)\star(\alpha,\beta)=(a,b)\Rightarrow(a\alpha,\frac{\beta}{a}+b\alpha)=(a,b)$

$$\Rightarrow\begin{cases}a\alpha=a\\ \wedge\\ \frac{\beta}{a}+b\alpha=b\end{cases}$$
$$\Rightarrow\begin{cases}\alpha=\frac{a}{a}=1\\ \wedge\\ \beta+b=b\end{cases}$$
$$\Rightarrow\begin{cases}\alpha=\frac{a}{a}=1\\ \wedge\\ \beta=0\end{cases}$$

Then $e=(1,0)$ is a neutral element in $(\mathbb{R}^*\times\mathbb{R},\star)$
3) $\forall(a,b)\in\mathbb{R}^*\times\mathbb{R},\exists^?(\alpha,\beta)\in\mathbb{R}^*\times\mathbb{R}:(a,b)\star(\alpha,\beta)=(1,0)$
$(a,b)\star(\alpha,\beta)=(1,0)\Rightarrow(a\alpha,\frac{\beta}{a}+b\alpha)=(1,0)$

$$\Rightarrow\begin{cases}a\alpha=1\\ \wedge\\ \frac{\beta}{a}+b\alpha=0\end{cases}$$
$$\Rightarrow\begin{cases}\alpha=\frac{1}{a}\\ \wedge\\ \frac{\beta}{a}+\frac{b}{a}=0\end{cases}$$
$$\Rightarrow\begin{cases}\alpha=\frac{1}{a}\\ \wedge\\ \beta=-b\end{cases}$$

Then $(\mathbb{R}^*\times\mathbb{R},\star)$ is a group.
4) $\star$ is not commutative because:
$\exists\,(1,3),(2,0)\in\mathbb{R}^*\times\mathbb{R}:(1,3)\star(2,0)\neq(2,0)\star(1,3)$.

Solution 4.6.4

1)
Let $(a_1,b_1),(a_2,b_2),(a_3,b_3)\in\mathbb{R}_+^*\times\mathbb{R}$
$[(a_1,b_1)\star(a_2,b_2)]\star(a_3,b_3)=(a_1a_2,a_1b_2+b_1)\star(a_3,b_3)$
$=(a_1a_2a_3,a_1a_2b_3+a_1b_2+b_1)$
and
$(a_1,b_1)\star[(a_2,b_2)\star(a_3,b_3)]=(a_1,b_1)\star(a_2a_3,a_2b_3+b_2)$
$=(a_1a_2a_3,a_1(a_2b_3+b_2)+b_1)$
$=(a_1a_2a_3,a_1a_2b_3+a_1b_2+b_1)$
Then, $[(a_1,b_1)\star(a_2,b_2)]\star(a_3,b_3)=(a_1,b_1)\star[(a_2,b_2)\star(a_3,b_3)]$.
therefore the law $\star$ is an associative.
2)
$\exists^?(\alpha,\beta)\in\mathbb{R}_+^*\times\mathbb{R},\forall(a,b)\in\mathbb{R}_+^*\times\mathbb{R}:(a,b)\star(\alpha,\beta)=(a,b)$
$(a,b)\star(\alpha,\beta)=(a,b)\Rightarrow(a\alpha,a\beta+b)=(a,b)$

$$\Rightarrow\begin{cases}a\alpha=a\\ \wedge\\ a\beta+b=b\end{cases}$$
$$\Rightarrow\begin{cases}\alpha=\frac{a}{a}=1\\ \wedge\\ \beta+b=b\end{cases}$$
$$\Rightarrow\begin{cases}\alpha=\frac{a}{a}=1\\ \wedge\\ \beta=0\end{cases}$$

Then $e = (1, 0)$ is a neutral element in $(\mathbb{R}_+^* \times \mathbb{R}, \star)$.
3) $\forall (a, b) \in \mathbb{R}^* \times \mathbb{R}, \exists^? (\alpha, \beta) \in \mathbb{R}^* \times \mathbb{R} : (a, b) \star (\alpha, \beta) = (1, 0)$
$(a, b) \star (\alpha, \beta) = (1, 0) \Rightarrow (a\alpha, a\beta + b) = (1, 0)$

$$\Rightarrow \begin{cases} a\alpha = 1 \\ \wedge \\ a\beta + b = 0 \end{cases}$$

$$\Rightarrow \begin{cases} \alpha = \frac{1}{a} \\ \wedge \\ a\beta + b = 0 \end{cases}$$

$$\Rightarrow \begin{cases} \alpha = \frac{1}{a} \\ \wedge \\ \beta = \frac{-b}{a} \end{cases}$$

Then $(\mathbb{R}_+^* \times \mathbb{R}, \star)$ is a group.
4) $\star$ is not commutative because:
$\exists\ (1, -3), (2, 0) \in \mathbb{R}^* \times \mathbb{R} : (1, -3) \star (2, 0) \neq (2, 0) \star (1, -3)$.

Solution 4.6.5

1. **(a)**

   H is a subgroup of G. Indeed, $0 \in H$, if $x, y \in H$, then $-x$ and $x + y$ are two even integers and therefore $-x \in H$, $x + y \in H$

   The subgroup characterization theorem tells us that H is a subgroup of G.

   (b)

   $0 \notin H$, and therefore H is not a subgroup of G.

2. $|z| = 1$ then $1 \in U \Rightarrow U \neq \phi$

   Let's $z_1,\ z_2 \ \in U$ and therefore $|z_1| = 1$ and $|z_2| = 1$

   $|z_1 z_2^{-1}| = |\frac{z_1}{z_2}| = |\frac{1}{1}| = 1.$

   then $z_1 z_2^{-1} \in U$

   So, $(U, \times)$ is a subgroup of $(\mathbb{C}^*, \times\ )$

Solution 4.6.6

(a) Let e be the neutral element of G; we have:

$$\forall y \in G; \quad e \star y = ye = ey = y.$$

So $e \in C(G)$; hence $C(G) \neq 0$.

(b) Let $x_1, x_2 \in C(G)$. Then, for all $y \in G$,

$$(x_1 x_2)y = x_1(x_2 y) = x_1(y x_2) = (x_1 y)x_2 = y(x_1 x_2).$$

Thus, $x_1 x_2 \in C(G)$.

(c) Let $x \in C(G)$. Then, for all $y \in G$, $xy = yx$. Multiplying by x^{-1} on the right, we get:

$$xyx^{-1} = yxx^{-1} \Rightarrow xyx^{-1} = y,$$

and similarly, multiplying by x^{-1} on the left, we get:

$$x^{-1}xyx^{-1} = xx^{-1}y \Rightarrow yx^{-1} = x^{-1}y,$$

which implies $x^{-1} \in C(G)$. Thus, we conclude that $C(G)$ is a subgroup of G.

(d) Since H is a subgroup of G, $e \in H$, and thus $aea^{-1} \in G$. But $aea^{-1} = e$, so $e \in aHa^{-1}$.

(b) Let $x = aha^{-1}$ and $y = ahh'a^{-1}$ be two elements of aHa^{-1} with $h; h' \in H$. Then,

$$xy = aha^{-1}ahh'a^{-1} = ahh'a^{-1} \in aHa^{-1}.$$

Since $hh' \in H$ (as H is a subgroup of G). Finally, we have

$$x^{-1} = (aha^{-1})^{-1} = ah^{-1}a^{-1} \in aHa^{-1}.$$

Since $h^{-1} \in H$. Hence, aHa^{-1} is indeed a subgroup of G.

Solution 4.6.7

1. For all
$$x, y \in \mathbb{R}^\star, \quad \varphi(x \times y) = (xy)^n = x^n y^n = \varphi(x)\varphi(y).$$
So, it's a homomorphism.
$$\ker \varphi = \{x \in \mathbb{R}^\star : x^n = 1\}.$$
$$\text{Im } \varphi = \{x^n : x \in \mathbb{R}^\star\}.$$
We characterize two cases:
   - If n is even:
   $$\ker \varphi = \{1, -1\}, \quad \text{Im } \varphi = \mathbb{R}^{+\star}.$$
   - If n is odd:
   $$\ker \varphi = \{1\}, \quad \text{Im } \varphi = \mathbb{R}^\star.$$

   So, φ is an isomorphism of groups if n is odd (in this case, φ is bijective), also, as $\varphi : \mathbb{R}^* \to \mathbb{R}^*$, then φ is a bijective endomorphism and therefore an automorphism of groups if n is odd. (If n is even, φ is not injective and not surjective.)

2. For all
$$t, t' \in \mathbb{R}, \quad \varphi(t + t') = e^{2\pi i(t+t')} = e^{2\pi it}e^{2\pi it'} = \varphi(t) \times \varphi(t').$$
So, it's a homomorphism.
Since $e^{2\pi it} = 1$ if and only if $t \in \mathbb{Z}$. Then,
$$\ker \varphi = \mathbb{Z}.$$
Thus φ is not injective. Also,
$$\text{Im } \varphi = \left\{e^{2\pi it}, t \in \mathbb{R}\right\} = \{z \in \mathbb{C} : |z| = 1\}.$$
So φ is not surjective. Therefore, φ is not an isomorphism.

Solution 4.6.8

First, notice that $(+)$ and $(\circ)$ are indeed internal composition laws on $End(G)$.

1. $(End(G), +)$ is a commutative group. Indeed, the law $(+)$ is associative, the function $0_G : G \to G$; $g \to 0$ is a neutral element for $(+)$, and every element $f \in End(G)$ has an inverse $-f : G \to G$; $x \mapsto -f(x)$.
2. The law is associative.
3. The law $(\circ)$ is distributive with respect to $(+)$. For all $f, g, h \in End(G)$ and all $x \in G$,
$$((f + g) \circ h)(x) = (f + g)(h(x)) = f(h(x)) + g(h(x)) = (f \circ h + g \circ h)(x).$$
Thus, $(End(G); +; \circ)$ forms a ring.

Solution 4.6.9

1. We have $0 + 0\sqrt{6} = 0 \in A$, so $A \neq \phi$. Let $m, n, m', n' \in \mathbb{Z}$;

$$(m + n\sqrt{6}) - (m' + n'\sqrt{6}) = (m - m') + (n - n')\sqrt{6} \in A.$$

$$(m + n\sqrt{6})(m' + n'\sqrt{6}) = (mm' + 6nn') + (mn' + nm')\sqrt{6} \in A.$$

2. For all $a \in A$, $\varphi(\varphi(a)) = a$, so φ is a bijection since every element a of A has $\varphi(a)$ as its antecedent. Now, let's show that φ is a homomorphism for addition and multiplication:

$$\begin{aligned}
\varphi((m + n\sqrt{6}) + (m' + n'\sqrt{6})) &= \varphi((m + m') + (n + n')\sqrt{6}), \\
&= (m + m') - (n + n')\sqrt{6}, \\
&= (m - n\sqrt{6}) + (m' - n'\sqrt{6}), \\
&= \varphi(m + n\sqrt{6}) + \varphi(m' + n'\sqrt{6}). \\
\varphi((m + n\sqrt{6})(m' + n'\sqrt{6})) &= \varphi((mm' + 6nn') + (mn' + nm')\sqrt{6}), \\
&= (mm' + 6nn') - (mn' + nm')\sqrt{6}, \\
&= (m - n\sqrt{6})(m' - n'\sqrt{6}), \\
&= \varphi(m + n\sqrt{6}) \times \varphi(m' + n'\sqrt{6}).
\end{aligned}$$

3. Let $a = m + n\sqrt{6} \in A$,

$$\begin{aligned}
N(a) &= a\varphi(a), \\
&= m + n\sqrt{6}\varphi(m + n\sqrt{6}), \\
&= (m + n\sqrt{6})(m - n\sqrt{6}), \\
&= m^2 - 6n^2.
\end{aligned}$$

So, N is a function from A to $\mathbb{Z}$. For $a, a' \in A$, $N(aa') = aa'\varphi(aa') = aa'\varphi(a)\varphi(a') = a\varphi(a)a'\varphi(a') = N(a)N(a')$, hence N is a homomorphism.

4. $$\Longrightarrow$$

If $N(x) = x\varphi(x) = 1$. Then, $\varphi(x)$ is an inverse of x. If $N(x) = x\varphi(x) = -1$. Then, $-\varphi(x)$ is an inverse of x.

Let x be an invertible element of A, then $\exists y$, $xy = 1$. Since N is a homomorphism, $N(x)N(y) = 1$; but $N(x)$ and $N(y)$ are integers, the only invertible elements of $\mathbb{Z}$ under multiplication are -1 and $+1$.

5. $N(5 + 2\sqrt{6}) = 25 - 24 = 1$. So the inverse of $5 + 2\sqrt{6}$ is $5 - 2\sqrt{6}$.

Solution 4.6.10

1. **a)** Group axioms

Closure:

If $x, y > 0$ then $xy > 0$, so $x \star y \in G$

Associativity:

Multiplication of real numbers is associative:

$(x \star y) \star z = x(yz) = (xy)z = x \star (y \star z)$.

Identity element:

The identity is

$e = 1$, since

$x \star 1 = 1 \star x = 1x = x$.

Inverse:

For $x > 0$, the inverse is

$$x^{-1} = \frac{1}{x}$$

Thus,

$(G, \star)$ is a group.

b) Commutativity

Since

$$xy = yx$$

for all real numbers, the group is abelian.

2. **a)** H is subgroup of $\mathbb{Z}$ if

i) $0 = 6 \cdot 0 \in H$ so $H \neq \phi$

ii) If

$6k,\ \ 6m \in H$ then

$6k - 6m = 6(k - m) \in H$

Thus,

H is a subgroup of $\mathbb{Z}$

b)

Determine all cosets of H in $\mathbb{Z}$

For any integer $a \in \mathbb{Z}$, the coset of H determined by a is

$$a + H = \{a + 6k \mid k \in Z\}.$$

Two integers a and b define the same coset if and only if

$$a \equiv b \pmod 6.$$

Thus, there are exactly six distinct cosets, corresponding to the remainders modulo 6:

$$0 + H = \{6k \mid k \in Z\},$$

$$1 + H = \{6k + 1 \mid k \in Z\},$$

$$2 + H = \{6k + 2 \mid k \in Z\},$$

$$3 + H = \{6k + 3 \mid k \in Z\},$$

$$4 + H = \{6k + 4 \mid k \in Z\},$$

$$5 + H = \{6k + 5 \mid k \in Z\}.$$

Solution 4.6.11

a) Ring axioms

Closed under addition and multiplication.

Addition is **associative** and **commutative**.

Additive identity:

$0 = 0 + 0\sqrt{2}$

Additive inverse:

$-(a + b\sqrt{2}) = -a\ -b\sqrt{2}$

Multiplication is associative.

Distributive laws hold.

Hence,

R is a ring.

b) Commutativity

Multiplication is commutative since

$(a + b\sqrt{2})(c + d\sqrt{2}) = (c + d\sqrt{2})(a + b\sqrt{2})$.

c) Unity

The unity element is

$$1 = 1 + 0\sqrt{2}.$$

Chapter 5

Polynomial Rings

5.1 Introduction

Polynomial rings play a central role in algebra and provide an important bridge between abstract algebraic structures and computational techniques. They extend the notion of numbers and allow algebraic expressions to be manipulated in a structured and rigorous way. In this chapter, we introduce the concept of polynomials over a ring, together with their fundamental properties, operations, and key results. Special attention is given to the structure of polynomial rings and their importance in solving algebraic equations and studying algebraic systems.

5.2 Polynomials, Degree, and Construction of Polynomial Rings

Definition 5.2.1

A polynomial in one variable with coefficients in A is defined as any sequence

$$P = (a_n)_{n\in\mathbb{N}},$$

of elements of A all of which are zero from a certain rank onwards. Polynomials are equipped with the usual operations of addition and multiplication of polynomials.

Let

$$P = (a_n)_{n\in\mathbb{N}}, \quad Q = (b_n)_{n\in\mathbb{N}},$$

be two polynomials in one variable with coefficients in A. Then:

$$P + Q = (a_n + b_n)_{n\in\mathbb{N}}.$$

$$PQ = (c_n)_{n\in\mathbb{N}}, \text{ where } \quad c_n = \sum_{0\leq k\leq n} a_k b_{n-k}.$$

It can be verified that the product of two polynomials is indeed a polynomial.
Let $X = (0, 1, 0, 0, ..., 0)$, $X^0 = (1, 0, 0, ..., 0)$, then it can be shown that $X^i = (0, 0, ..., 0, 1, 0, ...)$ where the 1 is located at the i-th position,

$$X^i X^j = X^{i+j}.$$

Thus any polynomial $P = (a_n)_{n\in\mathbb{N}}$ in one variable with coefficients in A can be written in the form:

$$P = \sum_{i\in\mathbb{N}} a_i X^i = (a_0, a_{1,}..., a_n, 0, ...).$$

Constant polynomials are those of the form $P = (a,\ 0,\ 0, ...)$, in this case, we simply denote $P = a$.
The degree of P, denoted $deg(P)$, is the largest integer n such that $a_n \neq 0$. By convention $deg(0) = -\infty$.

Definition 5.2.2

The set of polynomials in one variable with coefficients in A equipped with the addition and multiplication defined above is a ring. It is denoted by $A[X]$, called the ring of polynomials.

Definition 5.2.3

A polynomial P is said to be monic if its leading coefficient, i.e., the coefficient of the highest degree term, is equal to 1.

Proposition 5.2.4

If A is an integral domain, then for any P; $Q \in A[X]$; we have

$$deg(PQ) = deg(P) + deg(Q).$$

Proof

Let $n = deg(P)$ and $m = deg(Q)$. Let $P = \sum_{i\in\mathbb{N}} a_i X^i$ and $Q = \sum_{i\in\mathbb{N}} b_i X^i$ where a_i, $bi \in A$.

Then, the coefficient of the leading term of PQ is $a_n b_m$. Since $a_n \neq 0$ and $b_m \neq 0$, and A is an integral domain, $a_n b_m \neq 0$. This implies $deg(PQ) = n + m$.

Proposition 5.2.5

If A is an integral domain, then for any P; $Q \in A[X]$; we have

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

Proof

Let $\deg(P) = n$, $\deg(Q) = m$.
Then we can write

$$P(x) = a_n x_n + \cdots + a_0,$$

with

$$a_n \neq 0$$

and

$$Q(x) = b_m x_m + \cdots + b_0,$$

with

$$b_m \neq 0$$

Set

$$d = \max(n, m).$$

When adding the two polynomials, the highest possible degree in $P(x) + Q(x)$ is d
However, it may happen that the leading terms cancel each other.
For example,

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

In this case, the degree decreases.
Therefore, the degree of $P(x) + Q(x)$ cannot exceed d
Hence,

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

This completes the proof.

5.3 Polynomial Arithmetic

To simplify the statements, we will henceforth work over a field $\Bbbk$; where $\Bbbk$ denotes one of the fields $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$.

5.3.1 Euclidean Division

Definition 5.3.1

Let A, $B \in \Bbbk[X]$, we say that B divides A if there exists $Q \in \Bbbk[X]$ such that $A = BQ$. We denote this as $B \backslash A$. We also say that A is a multiple of B or that A is divisible by B.

Theorem 5.3.2 Euclidean Division of Polynomials

Let A, $B \in \Bbbk[X]$, with $B \neq 0$, then there exists a unique polynomial Q and there exists a unique polynomial R such that:

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

Q is called the quotient and R the remainder and this expression is "the Euclidean division" of A by B. Note that the condition $deg\ R < deg\ B$ means $R = 0$ or $0 < deg\ R < deg\ B$. Also $R = 0$ if and only if $B \backslash A$.

Example 5.3.3

Perform the Euclidean division of A by B such that:

$$A = x^3 + 2x^2 - 3 \quad \text{and} \quad B = x^2 - 4.$$

We perform polynomial division similar to the Euclidean division of two integers

$$\text{Then the quotient } Q = x + 2; \text{ and the remainder } R = 4x + 5.$$

So: $A = x^3 + 2x^2 - 3 = (x^2 - 4)\ (x + 2) + (4x + 5) = BQ + R.$

Example 5.3.4

Divide

$$x^3 + 2x^2 - 1$$

by

$$x + 1$$

Using long division:

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

Thus: Quotient:

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

Remainder:

$$R(x) = 0.$$

5.3.2 Greatest Common Divisor "gcd"

Proposition 5.3.5

Let A, $B \in \Bbbk[X]$, with $A \neq 0$ or $B \neq 0$. There exists a unique monic polynomial of highest degree that divides both A and B. This unique polynomial is called the gcd (greatest common divisor) of A and B which is denoted $gcd(A, B)$.

Euclidean Algorithm

Let A and B be polynomials, $B \neq 0$. We compute successive Euclidean divisions,

$$\begin{array}{ll} A = BQ_1 + R_1 & deg\ R_1 < deg\ B \\ B = R_1Q_2 + R_2 & deg\ R_2 < deg\ R_1 \\ R_1 = R_2Q_3 + R_3 & deg\ R_3 < deg\ R_2 \\ \vdots & \vdots \\ R_{k-2} = R_{k-1}Q_k + R_k & deg\ R_k < deg\ R_{k-1} \\ R_{k-1} = R_kQ_{k+1} & \end{array}$$

The degree of the remainder decreases with each division. We stop the algorithm when the remainder is zero. The gcd is the last non-zero remainder R_k.

Example 5.3.6

Determine the $gcd(A, B)$, where

$$A = x^5 + 3x^4 + x^3 + x^2 + 3x + 1,$$

$$B = x^4 + 2x^3 + x + 2,$$

$$x^5 + 3x^4 + x^3 + x^2 + 3x + 1 = (x^4 + 2x^3 + x + 2)(x + 1) + x^4 + x^3 + x + 1.$$

Then,

$$x^4 + 2x^3 + x + 2 = (-x^3 - 1)(-x - 2).$$

So the

$$gcd(A, B) = x^3 + 1.$$

Example 5.3.7

Find the gcd of $P(x) = x^2 - 1$ and $Q(x) = x^2 + x$. Factorization gives:

$$P(x) = (x - 1)(x + 1),$$

$$Q(x) = x(x + 1).$$

Hence,

$$gcd(P, Q) = x + 1.$$

Definition 5.3.8

Let A, $B \in \Bbbk[X$. We say that A and B are coprime if $gcd(A, B) = 1$.

5.3.3 Bézout Identity

Definition 5.3.9

If $D(x) = \text{gcd}\ (P(x), Q(x))$, then there exist polynomials $A(x)$, $B(x)$ such that:
$A(x)P(x) + B(x)Q(x) = D(x)$.

5.3.4 Least Common Multiple

Proposition 5.3.10

Let A, $B \in \Bbbk[X]$ be non-zero polynomials, then there exists a unique monic polynomial M of least degree such that $A \backslash M$ and $B \backslash M$. This unique polynomial is called the lcm (least common multiple) of A and B denoted $lcm(A, B)$.

5.3.5 Relation Between *gcd* and *lcm*

Theorem 5.3.11

For nonzero polynomials $P(x)$ and $Q(x)$,

$$P(x)Q(x) = gcd(P(x), Q(x)).lcm(P(x), Q(x))$$

Example 5.3.12

Let

$$P(x) = x(x+1),$$
$$Q(x) = (x+1)(x+2).$$

Then

$$gcd(P, Q) = x + 1$$

and

$$lcm(P, Q) = x(x+1)(x+2).$$

So,

$$P(x)Q(x) = x(x+1)^2(x+2) = gcd(P(x), Q(x)).lcm(P(x), Q(x)).$$

5.4 Cancellation Law

Theorem 5.4.1

Let $P(x), Q(x), R(x) \in \mathbb{R}[x]$, with $P(x) \neq 0$.
If

$$P(x)Q(x) = P(x)R(x),$$

then

$$Q(x) = R(x).$$

Proof

Subtract both sides:

$$P(x)(Q(x) - R(x)) = 0.$$

Since
$\mathbb{R}[x]$ has no zero divisors (when $\mathbb{R}$ is an integral domain), we get

$$Q(x) - R(x) = 0.$$

Hence

$$Q(x) = R(x).$$

5.5 Remainder Theorem

Theorem 5.5.1

Let $P(x) \in A[x]$ and $a \in A$.
The remainder of the division of $P(x)$ by $x - a$ is $P(a)$

Example 5.5.2

For

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

divide by

$$x - 1$$

We compute:

$$P(1) = 1 - 2 + 1 = 0.$$

Hence the remainder is $P(1) = 0$.

5.6 Factor Theorem

Theorem 5.6.1

Let $P(x) \in A[x]$ and $a \in A$. Then

$$P(a) = 0 \Leftrightarrow (x - a) \mid P(x)$$

Example 5.6.2

Consider $P(x) = x^2 - 1$.
Since $P(1) = 0$, then $x - 1$ divides $P(x)$ Indeed,

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

5.7 Uniqueness of Euclidean Division

Theorem 5.7.1

The quotient and remainder in Euclidean division are unique.

$$P = DQ_1 + R_1$$

$$P = DQ_2 + R_2$$

with

$$deg(R_1), deg(R_2) < deg(D),$$

then

$$Q_1 = Q_2, \quad R_1 = R_2.$$

5.8 Euclidean Algorithm

Theorem 5.8.1

The *gcd* of two polynomials can be computed using successive Euclidean divisions.

Example 5.8.2

Find the *gcd* of $P(x) = x^3 - x, \qquad Q(x) = x^2 - 1.$
Using Euclidean division:

$$x^3 - x = x(x^2 - 1) + 0.$$

Hence,

$$gcd(P, Q) = x^2 - 1.$$

5.9 Irreducible Polynomials

Definition 5.9.1

A nonconstant polynomial $P(x) \in A[x]$ is called irreducible if it cannot be written as a product of two nonconstant polynomials

Example 5.9.2

Consider the polynomial

$$P(x) = x^2 + 1$$

We study whether this polynomial is reducible or irreducible.

1) Over the field $\mathbb{R}$
We solve the equation

$$x^2 + 1 = 0.$$

This gives

$$x^2 = -1.$$

Since there is no real number whose square is equal to -1, the polynomial has no real roots.
Therefore,
$P(x)$ cannot be factored into linear polynomials over $\mathbb{R}$
Hence,
$x^2 + 1$ is irreducible over $\mathbb{R}$

2) Over the field $\mathbb{C}$
In the complex numbers, we have $i^2 = -1$.

Thus, the equation

$$x^2 + 1 = 0$$

has the roots $x = i$ and $x = -i$. Therefore,

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

Hence, the polynomial is reducible over $\mathbb{C}$ **Conclusion** The polynomial $x^2 + 1$ is:irreducible over $\mathbb{R}$, reducible over
$\mathbb{C}$ This shows that irreducibility depends on the field considered.

5.10 Units in $A[x]$



Theorem 5.10.1

The invertible elements (units) in $A[x]$ are exactly the nonzero constant polynomials

5.11 Exercises

Exercise 5.11.1

Perform the Euclidean division of A by B.

1. $A = x^5 - 7x^4 - x^2 - 9x + 9$, $B = x^2 - 5x + 4$.
2. $A = x^3 + x^2 - 2x + 1$, $B = x^2 + 2x + 1$.

Exercise 5.11.2

Determine the GCD and LCM of the following polynomials.

1. $P(x) = x^4 - 3x^3 + x^2 + 4$ and $Q(x) = x^3 - 3x^2 + 3x - 2$.
2. $P(x) = x^5 - x^4 + 2x^3 - 2x^2 + 2x - 1$ and $Q(x) = x^5 - x^4 + 2x^2 - 2x + 1$.
3. $P(x) = x^n - 1$ and $Q(x) = (x-1)^n$, where $n \geq 1$.

Exercise 5.11.3

1. Factorize the polynomial $(x^2 - x + 1)^2 + 1$ in $\mathbb{R}[X]$.
2. Factorize the polynomial $P(x) = x^9 + x^6 + x^3 + 1$ in $\mathbb{C}[X]$.

Exercise 5.11.4

Consider the polynomial

$$P(x) = x^4 - 6x^3 + 9x^2 + 9.$$

1. Factorize $x^4 - 6x^3 + 9x^2$ into irreducible factors in $\mathbb{R}[X]$.
2. Deduce a factorization of P into irreducible factors in $\mathbb{C}[X]$, and then in $\mathbb{R}[X]$.

Exercise 5.11.5

Consider the two polynomials:

$$P(x) = x^3 - 9x^2 + 26x - 24,$$
$$Q(x) = x^3 - 7x^2 + 7x + 15.$$

Factorize these two polynomials into irreducible factors in $\mathbb{R}[X]$, knowing that they have a common root.

Exercise 5.11.6

Determine the rest of the Euclidean division of the polynomial.

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

by

$$Q = X^2 + X + 1.$$

5.12 Solutions

Solution 5.11.1

1. $x^5 - 7x^4 - x^2 - 9x + 9 = (x^2 - 5x + 4)(x^3 - 2x^2 - 14x - 63) - 268x + 261$.
2. $x^3 + x^2 - 2x + 1 = (x^2 + 2x + 1)(x - 1) - x + 2$.

Solution 5.11.2

We apply the Euclidean algorithm. The last non-zero remainder gives the greatest common divisor (gcd) of the two polynomials. We have successively:

1. $P(x) = x^4 - 3x^3 + x^2 + 4 = (x^3 - 3x^2 + 3x - 2)x + (-2x^2 + 2x + 4)$.

   $Q(x) = x^3 - 3x^2 + 3x - 2 = (-2x^2 + 2x + 4)(\frac{-1}{2}x + 1) + (3x - 6)$.

   $-2x^2 + 2x + 4 = (3x - 6)(\frac{2}{3}x - \frac{2}{3}) = 3(x - 2)(\frac{2}{3}x - \frac{2}{3})$.

   So the $gcd(P, Q) = x - 2$.

2. We repeat the same process:

$$P(x) = x^5 - x^4 + 2x^3 - 2x^2 + 2x - 1 = (x^5 - x^4 + 2x^2 - 2x + 1)1 + (2x^3 - 4x^2 + 4x - 2).$$

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

$$2x^3 - 4x^2 + 4x - 2 = (x^2 - x + 1)(2x - 2) + 0.$$

   So the $gcd(P, Q) = x^2 - x + 1$.

3. The non-constant divisors of Q are polynomials of the form $c(x-1)^p$, with $1 \leq p \leq n$. Among these divisors, only those of the form $c(x-1)$ also divide P (for example, because 1 is a simple root of P and not a double root, or because we know how to decompose P into irreducible factors...). Thus, the $gcd(P, Q) = x - 1$.

Solution 5.11.3

1. We begin by factoring the polynomial in $\mathbb{C}[X]$, noticing that it is a difference of two squares:

$$\begin{aligned}(x^2 - x + 1)^2 + 1 &= (x^2 - x + 1)^2 - i^2 = (x^2 - x + 1 - i)(x^2 - x + 1 + i),\\ &= (x + i)(x - 1 - i)(x - i)(x - 1 + i),\\ &= (x^2 + 1)(x^2 - 2x + 2).\end{aligned}$$

   We then factor each of the degree 2 polynomials in $\mathbb{C}$, for example by calculating their discriminant or by noticing that i (resp. $-i$) are obvious roots. We find:

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

   By grouping the conjugate terms, we finally find:

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

   This is the decomposition in $\mathbb{R}[X]$.

2. We'll begin by decomposing $Q(x) = x^3 + x^2 + x + 1$, where -1 is an obvious root. We deduce:

$$Q(X) = (x^2 + 1)(x + 1) = (x + 1)(x - i)(x + i).$$

   Since $P(x) = Q(x^3)$, we now need to find the 3^{rd} roots of 1, i, and $-i$. This gives us:

$$P(x) = (x + 1)(x - e^{\frac{i\pi}{3}})(x - e^{\frac{-i\pi}{3}})(x - e^{\frac{i\pi}{2}})(x - e^{\frac{-i5\pi}{6}})(x - e^{\frac{-i\pi}{6}})(x - e^{\frac{-i\pi}{2}})(x - e^{\frac{i5\pi}{6}})(x - e^{\frac{i\pi}{6}}).$$

Solution 5.11.4

1. We simply write:
$$x^4 - 6x^3 + 9x^2 = x^2(x^2 - 6x + 9) = x^2(x-3)^2.$$

$$\begin{aligned} x^4 - 6x^3 + 9x^2 + 9 &= (x(x-3))^2 - (3i)^2, \\ &= (x(x-3) - 3i)(x(x-3) + 3i), \\ &= (x^2 - 3x - 3i)(x^2 - 3x + 3i) \end{aligned}$$

We factorize $(x^2 - 3x - 3i)$
$$\Delta = 9 + 12i = (\sqrt{3}(2+i))^2.$$

Hence the roots are:
$$x_1 = \frac{3}{2} - \sqrt{3} - \frac{\sqrt{3}}{2}i,$$

and
$$x_2 = \frac{3}{2} + \sqrt{3} + \frac{\sqrt{3}}{2}i.$$

Therefore,
$$x^2 - 3x - 3i = \left(x - \left(\frac{3}{2} - \sqrt{3} - \frac{\sqrt{3}}{2}i\right)\right)\left(x - \left(\frac{3}{2} + \sqrt{3} + \frac{\sqrt{3}}{2}i\right)\right)$$

We factorize $(x^2 - 3x + 3i)$
$$Delta = 9 - 12i = (\sqrt{3}(2-i))^2.$$

Hence the roots are:
$$x_1 = \frac{3}{2} + \sqrt{3} - \frac{\sqrt{3}}{2}i,$$

and
$$x_2 = \frac{3}{2} - \sqrt{3} + \frac{\sqrt{3}}{2}i$$

Therefore,
$$x^2 - 3x + 3i = \left(x - \left(\frac{3}{2} + \sqrt{3} - \frac{\sqrt{3}}{2}i\right)\right)\left(x - \left(\frac{3}{2} - \sqrt{3} + \frac{\sqrt{3}}{2}i\right)\right).$$

So the decomposition of P into irreducible factors of $\mathbb{C}[X]$ is thus,
$P(x) = \left[\left(x - \left(\frac{3}{2} - \sqrt{3} - \frac{\sqrt{3}}{2}i\right)\right)\right]\left[\left(x - \left(\frac{3}{2} + \sqrt{3} + \frac{\sqrt{3}}{2}i\right)\right)\right]\left[\left(x - \left(\frac{3}{2} + \sqrt{3} - \frac{\sqrt{3}}{2}i\right)\right)\right]$
$\left[\left(x - \left(\frac{3}{2} - \sqrt{3} + \frac{\sqrt{3}}{2}i\right)\right)\right]$.

To obtain the decomposition into irreducible factors of $\mathbb{R}[X]$, we group the conjugate complex roots, giving
$$P(x) = \left[x^2 - (2\sqrt{3}+3)x + 3\sqrt{3} + 6\right]\left[x^2 + (2\sqrt{3}-3)x - 3\sqrt{3} + 6\right].$$

Solution 5.11.5

If a is a common root of P and Q, then $x - a$ divides the $\gcd(P, Q)$. We start by finding this gcd, for example by applying the Euclidean algorithm. Here, we have

$$x^3 - 9x^2 + 26x - 24 = x^3 - 7x^2 + 7x + 15 + (-2x^2 + 19x - 39).$$

$$x^3 - 7x^2 + 7x + 15 = (-2x^2 + 19x - 39)(-\frac{1}{2}x - \frac{5}{4}) + (\frac{45}{4}x - \frac{135}{4}).$$

$$-2x^2 + 19x - 39 = (\frac{45}{4}x - \frac{135}{4})(\frac{-8}{45}x + \frac{52}{45}).$$

So the $\gcd(P, Q)$ is thus $(\frac{45}{4}x - \frac{135}{4})$, or equivalently $x - 3$. We then divide P and Q by $x - 3$, and we find:
$$P(x) = (x-3)(x^2 - 6x + 8),$$

and

$$Q(x) = (x-3)(x^2-4x-5).$$

We further factorize each of the degree 2 polynomials to finally find:

$$P(x) = (x-3)(x-2)(x-4)$$

and

$$Q(x) = (x+1)(x-3)(x-5).$$

N.B : We could also have factored these polynomials by searching for obvious roots.

Solution 5.11.6

The degree of the reste divides P by Q, It is equal to one at most. It therefore takes the rest of the desired division.

Formula $R(X) = aX + b$ It belongs to $\mathbb{R}[X]$.

If we note the quotient P by Q of symbol S was

$$P(X) = S(X)(X^{\,2} + X + 1) + R(X)$$

But we know that it is in $\mathbb{C}[X]$ we have:

$X^{\,2} + X + 1 = (X - j)(X - \bar{j}\ )$ such as $j = \exp\left(\frac{2\pi i}{3}\right)$

If we consider the previous equality in $\mathbb{C}[X]$ we conclude that $R(j) = P(j)$

This equality is sufficient to determine the constants a and b.

In fact, we have:

$$\begin{aligned} P(j) &= (1+j)^{2n+1} + j^{n+2} \\ &= (-j^{\,2})^{2n+1} + j^{\,n+2} \\ &= -j^{\,n+2} + j^{\,n+2} = 0 \end{aligned}$$

And the relation $aj + b = 0$ such that $(a, b) \in \mathbb{R}^2$ is equivalent to $a = b = 0$, i.e. $R = 0$.

Chapter 6

Practice Exams with Detailed Solutions

6.1 Introduction

This chapter contains a collection of practice exams designed to heip students review the main concepts and improve their problem-solving skills. Each exam is followed by detailed solutions to provide clear explanations and guide students step by step toward the correct answers. Students are encouraged to attempt the exercises independently before consulting the solutions in order to maximize their understanding and preparation for examinations.

6.2 Five Solved Sample Exams

Model Exam 1

? Exercise 1 (7.5 points)

Given A, B and C three parts of a set E,

1. Show that:
   - **a.** $(A \cap B) \cup \complement_E B = A \cup \complement_E B$.
   - **b.** $(A \setminus B) \setminus C = A \setminus (B \cup C)$.
   - **c.** $A \setminus (B \cap C) = (A \setminus B) \cap (A \setminus C)$.
2. Simplify:
   - **a.** $\overline{(A \cup B)} \cap \overline{(C \cup \overline{A})}$.
   - **b.** $\overline{(A \cap B)} \cup \overline{(C \cap \overline{A})}$.

? Exercise 2 (7.5 points)

We define the relation $\mathcal{R}$ on $\mathbb{R}^2$ by:

$$(x, y)\mathcal{R}(x', y') \Leftrightarrow \ x + y = x' + y'$$

1. Show that $\mathcal{R}$ is an equivalence relation.
2. Find the equivalence class of the couple $(0, 0)$.

? Exercise 3 (5 points)

1. Determine if part H is a subgroup of group G.
   a. $G = (\mathbb{Z}, +)$; $H = \{\text{even numbers}\}$
   b. $G = (\mathbb{Z}, +)$; $H = \{\text{odd numbers}\}$.
2. Show that $U = \{z \in \mathbb{C}, |z| = 1\}$ equipped with multiplication is a subgroup of $(\mathbb{C}^*, \times)$.

The Model Solution for the 1 Exam

Solution of Exercise 1

1. Show that:

a. $(A \cap B) \cup \complement_E B \overset{?}{=} A \cup \complement_E B$.

Let $x \in (A \cap B) \cup \complement_E B \Leftrightarrow x \in (A \cap B) \vee x \in \complement_E B$,

$\Leftrightarrow (x \in A \wedge x \in B) \vee (x \notin B)$

$\Leftrightarrow (x \in A \vee x \notin B) \wedge (x \in B \vee x \notin B)$

$\Leftrightarrow x \in (A \cup \complement_E B) \wedge x \in (B \cup \complement_E B)$

$\Leftrightarrow x \in (A \cup \complement_E B) \cap E$

$\Leftrightarrow x \in A \cup \complement_E B$.....(1.5 pts)

Because $E = \complement_E B \cup B$ and $A \cup \complement_E B$ is a subset of E.

b. $(A \setminus B) \setminus C \overset{?}{=} A \setminus (B \cup C)$.

$x \in (A \setminus B) \setminus C \Leftrightarrow (x \in A \wedge x \notin B) \wedge (x \notin C)$

$\Leftrightarrow x \in A \wedge (x \notin B \wedge x \notin C)$

$\Leftrightarrow x \in A \wedge x \in (\complement_E B \cap \complement_E C)$

$\Leftrightarrow x \in A \wedge x \notin (B \cup C)$ (Morgan's Laws)

$\Leftrightarrow x \in A \setminus (B \cup C)$.....(1.5 pts)

c. $A \setminus (B \cap C) \overset{?}{=} (A \setminus B) \cap (A \setminus C)$.

$x \in A \setminus (B \cap C) \Leftrightarrow (x \in A \wedge (x \notin B \wedge x \notin C)$

$\Leftrightarrow (x \in A \wedge x \notin B) \wedge (\in A \wedge x \notin C)$

$\Leftrightarrow x \in (A \setminus B) \wedge x \in (A \setminus C)$

$\Leftrightarrow x \in (A \setminus B) \cap (A \setminus C)$.....(1.5 pts)

2. Simplify

a. $\overline{(A \cup B)} \cap \overline{(C \cup \overline{A})}$

$\overline{(A \cup B)} \cap \overline{(C \cup \overline{A})} = (\overline{A} \cap \overline{B}) \cap (\overline{C} \cap \overline{\overline{A}})$

$= (\overline{A} \cap \overline{B}) \cap (\overline{C} \cap A)$

$= (\overline{A} \cap A) \cap (\overline{C} \cap \overline{B})$

$= (\phi) \cap (\overline{C} \cap \overline{B})$

$= \phi$ .....(1.5 pts)

b. $\overline{(A \cap B)} \cup \overline{(C \cap \overline{A})}$

$\overline{(A \cap B)} \cup \overline{(C \cap \overline{A})} = (\overline{A} \cup \overline{B}) \cup (\overline{C} \cup \overline{\overline{A}})$

$= (\overline{A} \cup A) \cup (\overline{C} \cup \overline{B})$

$= E \cup (\overline{C} \cup \overline{B})$

$= E$ .....(1.5 pts)

Solution of Exercise 2

1. $\mathcal{R}$ it is an equivalence relation if and only if it is reflexive, symmetric and transitive.....(0.5)

a. $\mathcal{R}$ is reflexive if and only if $\forall (x, y) \in \mathbb{R}^2 : (x, y)\mathcal{R}(x, y)$

$(x, y)\mathcal{R}(x, y) \Leftrightarrow \ x + y = x + y$

Then $\mathcal{R}$ is reflexive.....(1.5)

b. $\mathcal{R}$ is symmetric if and only if $\forall (x,y),\ (x^{'},y^{'}) \in \mathbb{R}^2$:

$(x,y)\mathcal{R}(x^{'},y^{'}) \Rightarrow (x^{'},y^{'})R(x,y)$

$(x,y)\mathcal{R}(x^{'},y^{'}) \Leftrightarrow x+y = x^{'}+y^{'} \Rightarrow x^{'}+y^{'} = x+y \Leftrightarrow (x^{'},y^{'})R(x,y)$

Then $\mathcal{R}$ is symmetric.....(1.5)

c. $\mathcal{R}$ is transitive if and only if $\forall (x,y),\ (x^{'},y^{'}),\ (x^{''},y^{''}) \in \mathbb{R}^2 : (x,y)\mathcal{R}(x^{'},y^{'}) \wedge (x^{'},y^{'})R(x^{''},y^{''}) \Rightarrow (x,y)\mathcal{R}(x^{''},y^{''})$

$$(x,y)\mathcal{R}(x^{'},y^{'}) \wedge (x^{'},y^{'})R(x^{''},y^{''}) \Leftrightarrow \begin{cases} x+y = x^{'}+y^{'} \\ \wedge \\ x^{'}+y^{'} = x^{''}+y^{''} \end{cases}$$

$$\Rightarrow x+y = x^{''}+y^{''}$$

$$\Leftrightarrow (x,y)\mathcal{R}(x^{''},y^{''})$$

Then $\mathcal{R}$ is transitive.....(1.5)

Also $\mathcal{R}$ is an equivalence relation.

2. Let's find the equivalence class of the pair $(0,0)$.

$$\begin{aligned} \dot{\widehat{(0,0)}} &= \{(x,y) \in \mathbb{R}^2 / \ (x,y)\mathcal{R}(0,0)\} \\ &= \{(x,y) \in \mathbb{R}^2 / \ x+y=0+0\} \\ &= \{(x,y) \in \mathbb{R}^2 / \ x+y=0\} \\ &= \{(x,y) \in \mathbb{R}^2 / \ y=-x\} \\ &= \{(x,-x)/x \in \mathbb{R}\} \end{aligned}$$.....(2.5)

Solution of Exercise 3

1. **a.** H is a subgroup of G. Indeed, $0 \in H$, if $x,y \in H$, then $-x$ and $x+y$ are both even integers, and therefore $-x \in H$, $x+y \in H$. The subgroup characterization theorem tells us that H is a subgroup of G.....(1.5)

.

b.

$0 \notin H$, therefore, H is not a subgroup of G.....(1.5)

2. $|z| = 1$ then, $1 \in U \Rightarrow U \neq \phi$

Let $z_1,\ z_2 \ \in U$ and then $|z_1| = 1$ et $|z_2| = 1$

$|z_1 z_2^{-1}| = |\frac{z_1}{z_2}| = \frac{|z_1|}{|z_2|} = 1$ then $z_1 z_2^{-1} \in U$

So, $(U,\times)$ is a subgroup of$(\mathbb{C}^*,\times)$.....(2.0 pts)

Model Exam 2

? Exercise 1 (7 points)

Let I be an interval and let $f : I \to \mathbb{R}$ be a function. Using quantifiers terms, write the following propositions symbolically, and give their negations

1. f is the zero function
2. f is even.
3. f is constant

? Exercise 2 (6 points)

On the set $\mathbb{R}$, we define a relation $\mathcal{R}$ as follows

$$\forall x, y \in \mathbb{R}, \text{x } \mathcal{R} \text{ y } \Leftrightarrow \cos^2 y + \sin^2 x = 1$$

Is the relation $\mathcal{R}$ reflexive? symmetric? anti-symmetric? transitive?

? Exercise 3 (7 points)

on the set $\mathbb{C}$, we define the internal composition law $*$ as follows:

$$\forall (a, b, c, d) \in \mathbb{R}^4 : (a + ib) * (c + id) = ac + i(ad + bc)$$

1. show that $*$ is commutative and associative and accepts $e = 1$ as a neutral element in $\mathbb{C}$.
2. Is ($\mathbb{C}$,$*$) group?

The Model Solution for the 2 Exam

Solution of Exercise 1

1. f is the null function means that f is identically null, i.e. it is null for all values of I
   Thus, using quantifiers:

$$\forall x \in I: \ f(x) = 0$$

   its negation is therefore

$$\exists x \in I: \ f(x) \neq 0$$

2. f is even i.e.

$$\forall x \in I : f(x) = f(-x).$$

   its negation is:

$$\exists x \in I : f(x) \neq f(-x).$$

3. f is constant i.e.

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

   its negation is:

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

Solution of Exercise 2

1. $\mathcal{R}$ is reflexive
Let $x \in \mathbb{R}$. Then the following trigonometric formula is well known
$\cos^2 x + \sin^2 x = 1$,
equivalent to $x\mathcal{R}x$ i.e. $\mathcal{R}$ is reflexive.

2. $\mathcal{R}$ is also symmetric
To see this, let x, $y \in \mathbb{R}$ then
$x\mathcal{R}y \Leftrightarrow \cos^2 y + \sin^2 x = 1$
since
$\forall x, y \in \mathbb{R}, \ \cos^2 y + \sin^2 y = 1$ and $\cos^2 x + \sin^2 x = 1$,
So
$\cos^2 y + \sin^2 x = 1 \Leftrightarrow \cos^2 y + \sin^2 x = \cos^2 y + \sin^2 y$
hence
$\sin^2 y = \sin^2 x$
similarly we obtain
$\cos^2 y + \sin^2 x = 1 \Leftrightarrow \cos^2 y + \sin^2 x = \cos^2 x + \sin^2 x$
From which,
$\cos^2 y = \cos^2 x$.
We therefore obtain
$\cos^2 y + \sin^2 x = 1 \Leftrightarrow \cos^2 x + \sin^2 y = 1 \Leftrightarrow y\mathcal{R}x$
i.e. $\mathcal{R}$ is symmetric.

3. $\mathcal{R}$ is not anti-symmetric
We must show
$\exists x, y \in \mathbb{R}, \ x\mathcal{R}y \wedge y\mathcal{R}x$ but $x \neq y$
We have $0\mathcal{R}2\pi$ because:
$\cos^2(2\pi) + \sin^2 0 = 1 + 0 = 1$
and

$2\pi\mathcal{R}0$ because:
$\cos^2 0 + \sin^2(2\pi) = 1 + 0 = 1$,
but $0 \neq 2\pi$
So $\mathcal{R}$ is not anti-symmetric.

4. $\mathcal{R}$ is transitive relation
let $x, y, z \in \mathbb{R}$ such that
$x\mathcal{R}y \wedge y\mathcal{R}z$, i. e.
$\cos^2 y + \sin^2 x = 1 \quad \wedge \quad \cos^2 z + \sin^2 y = 1$
Whence
$\cos^2 y + \sin^2 x + \cos^2 z + \sin^2 y = 1 + 1 = 2$
Or else
$\cos^2 z + \sin^2 x + [\cos^2 y + \sin^2 y] = 2$
$\cos^2 z + \sin^2 x + 1 = 2$
$\cos^2 z + \sin^2 x = 2 - 1 = 1$
i. e. $x\mathcal{R}z$ so, $\mathcal{R}$ is transitive.
In conclusion $\mathcal{R}$ is an equivalence relation but it is not an order relation.

Solution of Exercise 3

1. For every $z = a + ib$ and $z^{'} = c + id$ of $\mathbb{C}$
We consider the internal composition law $*$ as follows:

$$z * z^{'} = (a + ib) * (c + id) = ac + i(ad + bc)$$

a. We prove that $*$ is a commutative operation in $\mathbb{C}$
For every $z = a + ib$ and $z^{'} = c + id$ in $\mathbb{C}$ we have:

$$\begin{aligned} z * z^{'} = (a + ib) * (c + id) &= ac + i(ad + bc) \\ &= ca + i(cb + da) \\ &= (c + id) * (a + ib) \\ &= z^{'} * z \end{aligned}$$

because $(\times)$ is a commutative operation in $\mathbb{R}$.

b. We prove that $*$ is an associative operation in $\mathbb{C}$
For every $z = a + ib$, $z^{'} = c + id$ and $z^{"} = e + if$ in $\mathbb{C}$ we have:

$$\begin{aligned} (z * z^{'}) * z^{"} &= [ac + i(ad + bc)] * z^{"} \\ &= (ac + i(ad + bc)) * (e + if\ ) \\ &= [ace + i(acf + (ad + bc)e)] \\ &= ace + i(acf + ade + bce).....(1) \end{aligned}$$

$$\begin{aligned} z * (z^{'} * z^{"}) &= (a + ib) * [(c + id\ ) * (e + if)] \\ &= (a + ib) * [ce + i(cf + de)] \\ &= [ace + i(a(cf + de) + bce)] \\ &= ace + i(acf + ade + bce).....(2) \end{aligned}$$

From (1) and (2) we have:
$(z * z^{'}) * z^{"} = z * (z^{'} * z^{"})$
So $*$ is an associative operation in $\mathbb{C}$.

c. We prove that $*$ has $e = 1$ as a neutral element in $\mathbb{C}$.
For every $z = a + ib$ in $\mathbb{C}$ we have:

$$\begin{aligned} z * 1 = (a + ib) * (1 + i\ 0) = \\ = (a \times 1 + i(a \times 0 + b \times 1) \\ = (a + ib) = z \end{aligned}$$

So $e = 1$ is a neutral element in $\mathbb{C}$.for $*$

2. Is ($\mathbb{C}$,$*$) group?
   we have $0 \in \mathbb{C}$
   $\forall z = a + ib \in \mathbb{C}$, $z * 0 = (a + ib) * (0 + i\ 0)$
   $= (a \times 0 + i(a \times 0 + b \times 0))$
   $= 0 + i \times 0 = 0 \neq 1$
   Hence, 0 is not accept the symmetrical element in $\mathbb{C}$ equipped by the law $*$
   So ($\mathbb{C}$,$*$) is not group.

Model Exam 3

? Exercise 1 (7 points)

1. Give negation of the following propositions:
   - **a.** $\forall x \in \mathbb{R}, \quad 2x > x.$
   - **b.** $\forall x \in \mathbb{R}, \quad x > 0 \Rightarrow \ 2x > x.$
   - **c.** $\exists n \in \mathbb{N}, \quad 5n + 11 = 3n + 14.$
   - **d.** $\forall \varepsilon \in \mathbb{R}, \quad (\varepsilon > 0) \Rightarrow (\exists n \in \mathbb{N}^* : \frac{1}{n} < \varepsilon)$
2. In the first three cases, indicate which one is true.

? Exercise 2 (6 points)

On the set $\mathbb{R}$, we define a relation $\mathcal{R}$ as follows

$$\forall x, y \in \mathbb{R}, \quad x\mathcal{R}y \Leftrightarrow e^x \leq e^y$$

Is the relation $\mathcal{R}$ reflexive? symmetric? anti-symmetric? transitive?

? Exercise 3 (7 points)

We equip $A = \mathbb{R} \times \mathbb{R}$ with two laws defined by:

$$\begin{cases} (x, y) + (x', y') = (x + x', y + y') \\ \text{and} \\ (x, y) \star (x', y') = (xx', xy' + x'y) \end{cases}$$

1. Show that $(A, +)$ is a commutative group.
2. - **a.** Show that the law $\star$ is commutative.
   - **b.** Show that $\star$ is associative
   - **c.** Determine the neutral element of A for the law $\star$.
   - **d.** Show that $(A, +, \star)$ is a commutative ring.

The Model Solution for the 3 Exam

Solution of Exercise 1

1. **a.** the negation is given by
   $\exists x \in \mathbb{R} : 2x \leq x$.....(1*pt*)
   b. the negation of proposition (b) is given by
   $\exists x \in \mathbb{R} : x > 0 \wedge 2x \leq x$.....(1*pt*)
   c. the negation is given by
   $\forall n \in \mathbb{N}, \quad 5n + 11 \neq 3n + 14$.....(1*pt*)
   d. the negation is given by
   $\exists \varepsilon \in \mathbb{R} \quad \varepsilon > 0 \wedge \forall n \in \mathbb{N}^* : \frac{1}{n} \geq \varepsilon$.....(1*pt*)
2. proposition (**a**) is false because its negation is true.
   proposition (**b**) is true. For the proof, we proceed as follows
   let $x \in \mathbb{R}$,
   suppose that $x > 0$ hence $2x = x + x > x$
   this completes the proof.....(3*pt*)
   and we have the proposition (**c**) is false. Solving the equation $5n + 11 = 3n + 14$
   we find that the only solution is $n = \frac{3}{2}$, or $\frac{3}{2} \notin \mathbb{N}$
   Therefore
   $\forall n \in \mathbb{N} : \quad 5n + 11 \neq 3n + 14$
   is true, or proposition " $\exists n \in \mathbb{N}, \quad 5n + 11 = 3n + 14$" is false.

Solution of Exercise 2

1. $\mathcal{R}$ is reflexive because:
   $\forall x \in \mathbb{R}, \ \ e^x \leq e^x$, So, $x\mathcal{R}x$.....(1.5*pt*)
2. $\mathcal{R}$ is not symmetric because:
   $\exists\ 0, 1 \in \mathbb{R}, \ \ e^0 = 1 \leq e^1$ but $e^1 \not\leq e^0$.....(1.5*pt*)
3. $\mathcal{R}$ is anti-symmetric because:
   $\forall x, y \in \mathbb{R}, \ \ x\mathcal{R}y \wedge y\mathcal{R}x \Leftrightarrow e^x \leq e^y \wedge e^y \leq e^x$
   $\Rightarrow e^x = e^y \Leftrightarrow x = y$.....(1.5*pt*)
4. $\mathcal{R}$ is transitive because:
   $\forall x, y, z \in \mathbb{R}$, $x\mathcal{R}y \wedge y\mathcal{R}z \Leftrightarrow e^x \leq e^y \wedge e^y \leq e^z \Rightarrow e^x \leq e^z \Leftrightarrow x\mathcal{R}z$.....(1.5*pt*)

   In conclusion $\mathcal{R}$ is an order relation but it is not an equivalence relation.

Solution of Exercise 3

1. $(x, y) + (x', y') = (x + x', y + y') \in A$ so the law $+$ is internal.....(0.5*pt*)

   Let (x, y), (x', y'), $(x'', y'') \in A$, we have:

$$\begin{aligned}(x,y)+[(x^{'},y^{'})+(x^{''},y^{''})] &= (x,y)+(x^{'}+x^{''},y^{'}+y^{''})\\ &= (x+(x^{'}+x^{''}),y+(y^{'}+y^{''}))\\ &= ((x+x^{'})+x^{''},(y+y^{'})+y^{''})\\ &= [(x,y)+(x^{'},y^{'})]+(x^{''},y^{''}).\end{aligned}$$

So the law $+$ is associative.....(1*pt*)

Let (x,y), $(x^{'},y^{'})\in A$, we have:

$$\begin{aligned}(x,y)+(x^{'},y^{'}) &= (x+x^{'},y+y^{'})\\ &= (x^{'}+x,y^{'}+y)\\ &= (x^{'},y^{'})+(x,y).\end{aligned}$$

So the $+$ law is commutative.....(1*pt*)

Let $(a,b)\in A=\mathbb{R}\times\mathbb{R}$, such that $(x,y)+(a,b)=(x,y)$,
it is clear that $(a,b)=(0,0)$ is the unique neutral element.....(1*pt*)

Let $(x^{'},y^{'})\in A=\mathbb{R}\times\mathbb{R}$ such that $(x,y)+(x^{'},y^{'})=(0,0)$
this is equivalent to:

$$(x+x^{'},y+y^{'})=(0,0)\Leftrightarrow\left\{\begin{array}{l}x+x^{'}=0\\ y+y^{'}=0\end{array}\right.\Leftrightarrow\left\{\begin{array}{l}x^{'}=-x\\ y^{'}=-y\end{array}\right.$$

So the symmetric of (x,y) is $(-x,-y)$.....(1*pt*)

So $(A,+)$ is a commutative group.

2. **a.** $\forall\ (x,y),(x^{'},y^{'})\in A:(x,y)\star(x^{'},y^{'})=(xx^{'},xy^{'}+x^{'}y)$

$$\begin{aligned}&= (x^{'}x,y^{'}x+yx^{'})\\ &= (x^{'}x,\ x^{'}y+xy^{'})\\ &= (x^{'},y^{'})\star(x,y)\end{aligned}$$

So $\star$ is commutative.....(0.5*pt*)

b. $\forall\ (x,y),(x^{'},y^{'}),\ (x^{''},y^{''})\in A:$

$$\begin{aligned}[(x,y)\star(x^{'},y^{'})]\star(x^{''},y^{''}) &= (xx^{'},xy^{'}+x^{'}y)\star(x^{''},y^{''})\\ &= (xx^{'}x^{''},xx^{'}y^{''}+x^{''}(xy^{'}+x^{'}y))\\ &= (xx^{'}x^{''},xx^{'}y^{''}+x^{''}xy^{'}+x^{''}x^{'}y))\text{.....(1)}\end{aligned}$$

$$\begin{aligned}(x,y)\star[(x^{'},y^{'})\star(x^{''},y^{''})] &= (x,y)\star(x^{'}x^{''},x^{'}y^{''}+x^{''}y^{'})\\ &= (xx^{'}x^{''},x(x^{'}y^{''}+x^{''}y^{'})+x^{'}x^{''}y)\\ &= (xx^{'}x^{''},xx^{'}y^{''}+xx^{''}y^{'}+x^{'}x^{''}y)\\ &= (xx^{'}x^{''},xx^{'}y^{''}+x^{''}xy^{'}+x^{''}x^{'}y)\text{.....(2)}\end{aligned}$$

From (1) and (2) we find that:

$$[(x,y)\star(x^{'},y^{'})]\star(x^{''},y^{''})=(x,y)\star[(x^{'},y^{'})\star(x^{''},y^{''})]$$

So the law $\star$ is associative.....(0.5*pt*)

c.

Let $(e,f)\in A$ such that for all $(x,y)\in A$,

$$(x,y)\star(e,f\ )=(x,y)\Leftrightarrow\left\{\begin{array}{l}xe=x\\ xf+ey=y\end{array}\right.\Leftrightarrow\left\{\begin{array}{l}e=1\\ f=0\end{array}\right.$$

$(1,0) \in A$ is the neutral element of A for the law $\star$.....$(0.5pt)$

d.

All the properties for a set with two laws to be a ring are in the previous questions except the distributivity of $\star$ with respect to addition $(+)$ (to the left or to the right since the law $\star$ is commutative, it is moreover this commutativity which makes the ring commutative).

$$\begin{aligned}(x,y)\star[(x^{'},y^{'})+(x^{''},y^{''})] &= (x,y)\star(x^{'}+x^{''},y^{'}+y^{''})\\ &= (x(x^{'}+x^{''}),\, x(y^{'}+y^{''})+(x^{'}+x^{''})y)\\ &= (xx^{'}+xx^{''},\, xy^{'}+xy^{''}+x^{'}y+x^{''}y)\\ &= (xx^{'}+xx^{''},\, xy^{'}+x^{'}y+xy^{''}+x^{''}y)\\ &= (xx^{'},\, xy^{'}+x^{'}y)+(xx^{''},xy^{''}+x^{''}y)\\ &= [(x,y)\star(x^{'},y^{'})]+[(x,y)\star(x^{''},y^{''})]\end{aligned}$$ .....$(1pt)$

And here $(A,+,\star)$ is a commutative ring.

Model Exam 4

? Exercise 1 (6 points)

Let

$$A = \{1, 2, 3, 4\}, \quad B = \{2, 4, 6, 8\}$$

and let

$$f : A \to B$$

be defined by

$$f\ (x) = 2x$$

1. Determine: $f\ (2)$, $f\ (A)$
2. Is f injective?
3. Is f surjective?
4. Determine the inverse image of the set $\{4, 8\}$

? Exercise 2 (7 points)

Let the following relation $\mathcal{R}$ be defined on $\mathbb{R}$

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

1. Verify whether this relation is an equivalence relation.
2. Find the equivalence classes of 0 and 3.

? Exercise 3 (7 points)

Let

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \quad a \in \mathbb{R} \right\}$$

1. Prove that $(G, \cdot)$ is a group, where "$\cdot$" denotes matrix multiplication.
2. Is this group commutative (abelian)?

The Model Solution for the 4 Exam

Solution of Exercise 1

We have:

$$A = \{1, 2, 3, 4\}, \quad B = \{2, 4, 6, 8\}$$

and the application

$$\begin{array}{rcl} f & : & A \to B, \\ f(x) & = & 2x \end{array}$$

1. Determine $f\ (2)$ and $f\ (A)$

   a. Compute $f\ (2)$

   $$f\ (2) = 2 \times 2 = 4$$

   Thus,

   $$f(2) = 4$$

   b. Determine $f\ (A)$

   We calculate the image of each element of A

   $$\begin{array}{l} f\ (1) = 2 \\ f\ (2) = 4 \\ f\ (3) = 6 \\ f\ (4) = 8 \end{array}$$

   Therefore,

   $$f\ (A) = \{2, 4, 6, 8\}$$

   Hence,

   $$f\ (A) = B$$

2. Is f injective?

   An application is injective if: $f(x_1) = f(x_2) \Rightarrow x_1 = x_2, \quad \forall x_1, x_2 \in A$

   Suppose:

   $\forall x_1, x_2 \in A$:

   $f(x_1) = f(x_2)$

   Then:

   $2x_1 = 2x_2$

   Dividing by 2, we obtain:

   $x_1 = x_2$

   Thus,

   f is injective.

3. Is f surjective?

   An application is surjective if every element of B has a preimage in A

   We have:

   $f(A) = \{2, 4, 6, 8\} = B$

   Therefore, every element of B is reached by f

   Hence,

   $$f \text{ is surjective}$$

4. Determine the inverse image of $\{4, 8\}$

   We search for all elements $x \in A$ such that: $f(x) \in \{4, 8\}$

   Now:

   $$f(2) = 4, \ f(4) = 8$$

   Thus,

   $$f^{-1}(\{4, 8\}) = \{2, 4\}$$

Solution of Exercise 2

1. Consider the relation defined on real Number $\mathbb{R}$

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

   We verify whether this relation is an equivalence relation.

   a. Reflexive Property

   For every $x \in \mathbb{R}$

   $$x^2 = x^2$$

   Hence,

   $$x\mathcal{R}x$$

   Therefore, the relation is reflexive.

   b. Symmetric Property

   Assume that

   $x\mathcal{R}y$ then, $x^2 = y^2$

   By exchanging the two sides, we obtain

   $y^2 = x^2$ thus, $y\mathcal{R}x$

   Therefore, the relation is symmetric.

   c. Transitive Property

   Assume that

   $$x\mathcal{R}y \text{ and } y\mathcal{R}z$$

   Then,

   $$x^2 = y^2 \text{ and } y^2 = z^2$$

Hence,

$$x^2 = z^2$$

Therefore,

$$x\mathcal{R}z$$

So the relation is transitive.

Conclusion

Since the relation is reflexive, symmetric, and transitive, it is an equivalence relation.

2. **Equivalence Classes**

a. Equivalence class of 0

$$\dot{0} = \{x \in \mathbb{R}; \quad x\mathcal{R}0\}$$

We have

$$x\mathcal{R}0 \Leftrightarrow x^2 = 0^2 = 0$$

Thus,

$$x = 0$$

Hence,

$$\dot{0} = \{0\}$$

b. Equivalence class of 3

$$\dot{3} = \{x \in \mathbb{R}; \quad x \,\mathrm{Re}\, 3\}$$

We have

$$x\mathcal{R}3 \Leftrightarrow x^2 = 3^2 = 9$$

Thus,

$$x = \pm 3$$

Hence,

$$\dot{0} = \{-3,\ 3\}$$

Solution of Exercise 3

Let

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \quad a \in \mathbb{R} \right\}$$

Where "$\cdot$" denotes matrix multiplication.

We verify the group properties on Matrix Multiplication.

1) Proof that $(G, \cdot)$ is a group

To show that G is a group under matrix multiplication, we verify the following properties.

a) Closure

Let

$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in G \quad \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in G$, with $a, b \in \mathbb{R}$

Then,

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$$

Since $a + b \in \mathbb{R}$, we have:

$$\begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} \in G$$

Hence, G is closed under matrix multiplication.

b) Associativity

Matrix multiplication is associative for all matrices. Therefore,

For all elements $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ of G

$$\left[\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right] \cdot \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b+c \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \left[\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b+c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b+c \\ 0 & 1 \end{pmatrix}$$

So,

$$\left[\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right] \cdot \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \left[\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\right]$$

With a, b, $c \in \mathbb{R}$

c) Identity Element

Consider the matrix

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Since $0 \in \mathbb{R}$, we have $I \in G$

Moreover,

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

Thus,

I is the identity element of G

d) Inverse Element

Let

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

We seek a matrix $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in G, \quad x \in \mathbb{R}$ such that

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

Now,

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+x \\ 0 & 1 \end{pmatrix}$$

This equals the identity matrix when

$$a + x = 0$$

Hence,

$$x = -a \ \in \mathbb{R}$$

Therefore,

$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}$ which belongs to G

Conclusion

All group properties are satisfied, therefore $(G, \cdot)$ is a group.

2) Is the group commutative?

Let

$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in G \quad \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in G$, with $a, b \in \mathbb{R}$

We compute:

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+a \\ 0 & 1 \end{pmatrix}$$

Since $a + b = b + a$, we obtain

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

Therefore, the group is commutative (abelian).

Model Exam 5

? Exercise 1 (7 points)

Let E be a set and A, B and C three parts of E, prove that:

1. $C_E(A \cap B) = C_E A \cup C_E B$.
2. $C_E(A \cup B) = C_E A \cap C_E B$.
3. $A/(B \cap C) = A/B \cup A/C$.

? Exercise 2 (6 points)

Consider the functions $f_1 : \mathbb{N} \to \mathbb{R}$, $f_2 : \mathbb{R}^+ \to \mathbb{R}$, defined as:

$$f_1(x) = \frac{1}{1+x}, \qquad f_2(x) = x^2,$$

Are the functions f_1 and f_2, injective, surjective, or bijective?

? Exercise 3 (7 points)

In $\mathbb{R}$, we define the relation $\mathcal{R}$ as:

$$\forall x, y \in \mathbb{R}; x\mathcal{R}y \Leftrightarrow x^2 - 1 = y^2 - 1$$

Show that $\mathcal{R}$ is an equivalence relation and determine the quotient set $\mathbb{R}/_{\mathcal{R}}$.

The Model Solution for the 5 Exam

Solution of Exercise 1

1. Let $x \in E$. Then,

   $x \in \complement_E(A \cap B) \Leftrightarrow x \notin (A \cap B) \Leftrightarrow (x \notin A) \vee (x \notin B) \Leftrightarrow (x \in \complement_E A) \vee (x \in \complement_E B) \Leftrightarrow x \in (\complement_E A \cup \complement_E B)$.

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

2. Let $x \in E$. Then,

   $x \in \complement_E(A \cup B) \Leftrightarrow x \notin (A \cup B) \Leftrightarrow (x \notin A) \wedge (x \notin B) \Leftrightarrow (x \in \complement_E A) \wedge (x \in \complement_E B) \Leftrightarrow x \in (\complement_E A \cap \complement_E B)$.

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

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

Solution of Exercise 2

1.
$$\begin{array}{l} f_1 : \mathbb{N} \to \mathbb{R} \\ x \mapsto f_1(x) = \frac{1}{1+x} \end{array}$$

• $\forall x_1, x_2 \in \mathbb{N}$, $f_1(x_1) = f_1(x_2) \Rightarrow \frac{1}{1+x_1} = \frac{1}{1+x_2} \Rightarrow x_1 = x_2$

Therefore f_1 is injective.

• $\forall y \in \mathbb{R}$, $\frac{1}{1+x} = y \Rightarrow x = \frac{1-y}{y}$, for example, when $y = 5$, we get $x = \frac{-4}{5} \notin \mathbb{N}$, hence, f_1 is not surjective.

As a consequence f_1 is not bijective.

2.
$$\begin{array}{l} f_2 : \mathbb{R}^+ \to \mathbb{R} \\ x \mapsto f_2(x) = x^2 \end{array}$$

• $\forall x_1, x_2 \in \mathbb{R}^+$, $f_2(x_1) = f_2(x_2) \Rightarrow x_1^2 = x_2^2 \Rightarrow x_1 = \pm x_2 \Rightarrow x_1 = x_2$ (because $x_1, x_2 \in \mathbb{R}^+$)

Then f_2 is injective.

• $\forall y \in \mathbb{R}$, $x^2 = y \Rightarrow x = \pm\sqrt{y}$; if $y \geq 0$; then for $y \in \mathbb{R}^-$; $\nexists x \in \mathbb{R}^+$; then f_2 is not surjective.

As a consequence f_2 bijective.

Solution of Exercise 3

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

   i. $\mathcal{R}$ is a reflexive relation, because: $\forall x \in \mathbb{R}$; $x^2 - 1 = x^2 - 1 \Rightarrow x\mathcal{R}x$

   ii. $\mathcal{R}$ is a symmetric relation, because: $\forall x, y \in \mathbb{R}$, $x\mathcal{R}y \Rightarrow x^2 - 1 = y^2 - 1$

   $\Rightarrow y^2 - 1 = x^2 - 1$ because egality is symmetric

   $\Rightarrow y\mathcal{R}x$

iii. $\mathcal{R}$ is a transitive relation, because:
$\forall x; y; z \in \mathbb{R}$, $(x\mathcal{R}y) \wedge (y\mathcal{R}z) \Rightarrow (x^2 - 1 = y^2 - 1) \wedge (y^2 - 1 = z^2 - 1)$
$\Rightarrow (x^2 - 1 = z^2 - 1)$ because egality is transitive.
$\Rightarrow x\mathcal{R}z$
From **i)**, **ii)** et **iii)** , we conclude that $\mathcal{R}$ is an equivalence relation.

2. Determine the quotient set $\mathbb{R}/_{\mathcal{R}}$.
Let $x \in \mathbb{R}$, then: $\forall y \in \mathbb{R}$, $x\mathcal{R}y \Leftrightarrow x^2 - 1 = y^2 - 1$
$\Leftrightarrow x^2 - y^2 = 0$
$\Leftrightarrow (x - y)(x + y) = 0$
$\Leftrightarrow (y = x) \vee (y = -x)$
therefore: $\dot{x} = \{-x, x\}$, consequently,
$\mathbb{R}/_{\mathcal{R}} = \{\{-x, x\}, \ x \in \mathbb{R}\}$.

Conclusion

This manuscript has been designed as an introductory guide to the fundamental concepts of algebra and mathematical reasoning for first-year university students. Throughout its six chapters, the document has presented the essential notions required for the study of higher mathematics, ranging from logic and set theory to algebraic structures and polynomial rings, while also providing a collection of previous examinations with detailed solutions to support revision and self-assessment.

The progressive organization of the material aims to facilitate the transition from elementary mathematical knowledge to a more rigorous and abstract mode of thinking. By combining theoretical developments with numerous examples, applications, solved exercises, and examination problems, this manuscript seeks not only to transmit mathematical knowledge but also to develop students' analytical abilities, logical reasoning, and problem-solving skills.

The concepts introduced in this course constitute the foundation of many advanced subjects encountered in mathematics, computer science, engineering, and other scientific disciplines. A solid understanding of logic, sets, relations, algebraic structures, and polynomial rings is therefore indispensable for future studies and for the development of a rigorous mathematical culture.

Although no single document can cover all aspects of algebra in depth, it is hoped that this manuscript will serve as a useful pedagogical resource, enabling students to acquire the essential knowledge and techniques prescribed by the official curriculum. Furthermore, it is expected to encourage intellectual curiosity, mathematical rigor, and a deeper appreciation of the role of abstraction in modern mathematics.

Finally, the author hopes that this work will contribute to the academic success of students and provide them with a solid foundation for their future studies in mathematics and related scientific fields.

Bibliography

[1] Azouly, E., Avignant,J., Auliac, G., (2002). Problèmes Corrigés de mathématiques , DEUG MIAS/SM, Ediscience (Dunod pour la nouvelle é dition) Paris

[2] Azouly, E., Avignant,J., Auliac, G., (2003). les mathématiques en Licence, 1‘ere. Tome 1 : Cours+ exercices, MIAS.MASS.SM, Ediscience(Dunod pour la nouvelle édition) Paris.

[3] Lang, S., (2004). Algèbre: Cours+ exercices, 3 ème édition, Dunod.

[4] Mignotte M. et Nervi, J., (2004). Algèbre: licences sciences 1 è re annéé, Ellipses, Paris.

[5] Franchini, J. et Jacquens, J.C., Algèbre: Cours, exercices corrigés, travaux dirigés, Ellipses, Paris, 199.

[6] Godement, R., (1966). Cours d'algèbre. Hermann.

[7] Mortad, M.H., (2012). Exercices Corrigés d'Algèbre, Première Année L.M.D., Edition "Dar el Bassair"(Alger-Algérie).

[8] Queysanne, M., (1971). Algèbre, collection U, Armand Colin.

[9] Anton, H. (2013). Elementary Linear Algebra (11th ed.). Wiley.

[10] Lay, D. C., Lay, S. R., & McDonald, J. J. (2015). Linear Algebra and Its Applications (5th ed.).

[11] hutz, S., & Lipson, M. (2017). Schaum's Outline of Linear Algebra (6th ed.). McGraw-Hill Education.

[12] Strang, G. (2016). Introduction to Linear Algebra (5th ed.) Wellesley-Cambridge Press.

[13] Sheldon Axler, (2015). Linear Algebra Done Right, Edition (common): 3rd Edition