الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف بالمسيلة

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

كلية الرياضيات والإعلام الآلي
قسم الرياضيات
اللجنة العلمية

رقم: 32 /ق.ر/ 2024

المسيلة في: 2024-03-17

مستخلص محضر اللجنة العلمية ليوم: 2024/03/17
بخصوص اعتماد مطبوعة دروس

وافقت اللجنة العلمية على اعتماد مطبوعة الدروس الخاصة بالأستاذ

سعداوي الخير المعنونة بـ:

Courses and Exercises for Algebra 1

كمرجع للدروس لطلبة **السنة الأولى ليسانس رياضيات**.

وهذا بعد الاطلاع على التقارير الإيجابية للأستاذ الخبير المكلف بالمطبوعة.

رئيس اللجنة العلمية

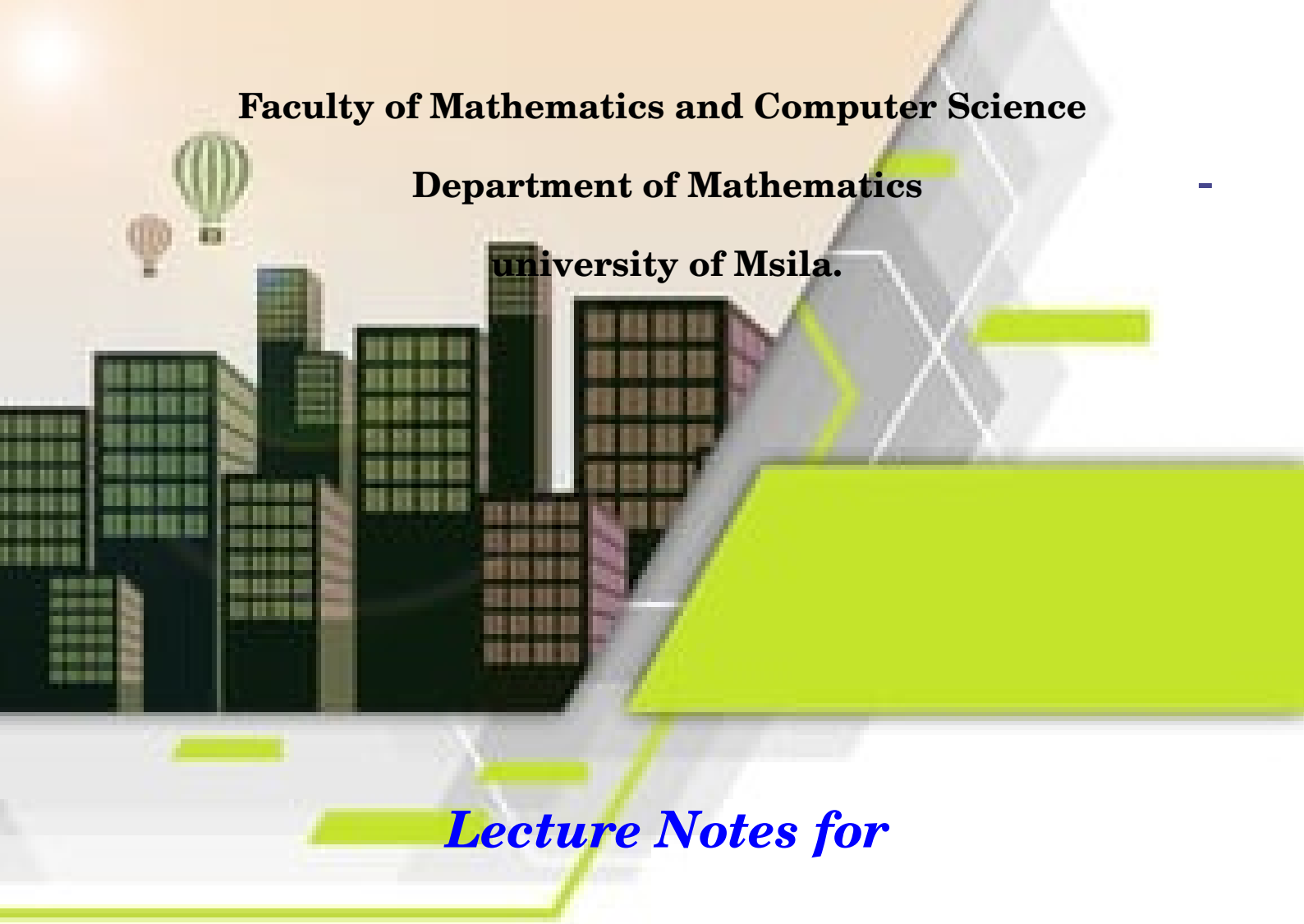
رئيس اللجنة العلمية
لقسم الرياضيات
مرزوقي عبد الكريم

سلمت هذه الشهادة للمعني لاستعمالها في حدود ما يسمح به القانون.

Faculty of Mathematics and Computer Science

Department of Mathematics

university of Msila.



Lecture Notes for

Algebra 01

Courses and Exercises for Algebra 01

Author | **kheir.saadaoui**

2022/2023

Contents

Chapter 1

Logical Concepts

At the intersection of philosophy and mathematics, logic is a fundamental branch that enables the determination of the truth value of propositions and the construction of mathematical reasoning.

This document serves as an introduction to this crucial branch of mathematics. We will define the concepts of proposition and operator, construct truth tables, explain implications, reciprocal implications, and equivalence, before delving into the various types of reasoning used in mathematics.

1.1 Definition

A logical proposition (or assertion) is a statement formed by combining symbols and words, concerning mathematical objects, to which a clear truth value, either true or false, can be assigned.

Let P be a proposition.

By definition, P satisfies the following three principles (or axioms):

- Principle of Identity: P is P

  In other words, if P is true, then P is true, and if P is false, then P is false.

- Principle of Non-contradiction: P cannot be both true and false simultaneously.

- Principle of the Excluded Middle: Either P is true, or P is false.

There is no other truth value in mathematical logic.

These three principles form the foundation of all mathematical reasoning. The last point deserves a moment of attention:

Let P be the proposition "The square of a real number is strictly positive."

So, is it true or false?

The initial intuition might be to say, "It depends on the number." This is true for most numbers, but it is false for zero (since 0^2 is not greater than 0).

The problem is that this response contradicts the Principle of the Excluded Middle. Therefore, it is necessary to unambiguously assign either the value of true or the value of false to this proposition.

Given that there is at least one number (in this case, zero) for which this proposition is false, we will say that proposition P is false.

1.1.1 Some Examples

$\boldsymbol{P}_1$: "The number of letters in the French alphabet is 10."

The proposition $\boldsymbol{P}_1$ is false.

$\boldsymbol{P}_2$**:** "$2 + 2 = 4$"

The proposition $\mathbf{P}_2$ is true.

$\mathbf{P}_3$**:** "x>1"

$\boldsymbol{P}_3$ is not a complete logical proposition because it contains a free variable x. We do not know what x represents (a point? an integer? a vector? a star in the universe?). Therefore, we cannot assign a truth value to the proposition $\mathbf{P}_3$.

$\boldsymbol{P'}_3$: "Let x be a real number, then $x > 1$"

The proposition $\boldsymbol{P'}_3$ is false. Indeed, $\boldsymbol{P'}_3$ is a logical proposition because we have defined the variable x as a real number. However, it is false because, for example, 0 is a real number and $0 < 1$.

Here, a counterexample is used to prove that the proposition $\boldsymbol{P'}_3$ is false.

(This type of reasoning will be further explored later).

Key Takeaways

Logical propositions can only take two values: TRUE or FALSE (hence the name bivalent logic).

It is important to distinguish between a proposition (which is a sentence) and its truth value (which is either TRUE or FALSE). We say that proposition p is false.

1.2 Basic Operators

Operators allow us to construct new propositions from one or more initial propositions.

Let's start with the first (and simplest!) one, the "NOT" operator.

1.2.1 Negation (not): Learning to Say No!

Let **P** be a proposition. We define a proposition "not **P**" which is denoted as "¬**A**" (with a sort of small L elongated downwards) or simply as $\overline{\boldsymbol{P}}$.

If $\boldsymbol{P}$ is true, then $\overline{\boldsymbol{P}}$ is false.

If $\boldsymbol{P}$ is false, then $\overline{\boldsymbol{P}}$ is true.

For those who do programming, the "NOT" operator (denoted as in math) is often written as "!" in computer science.

We can establish the truth table for the negation operator based on its definition.

Definition. A truth table is a table that defines the value of a logical function for each possible combination of inputs.

Explanation. In the first column, we list all the possible values of A (i.e., True or False). In the second column, we place the corresponding truth value of $\bar{A}$.

By convention, and to facilitate the reading of large tables, we write $\boldsymbol{F}$ for the value $FALSE$ and $\boldsymbol{V}$ for the value $TRUE$.

$\boldsymbol{P}$	$\boldsymbol{\overline{P}}$
$\boldsymbol{V}$	$\boldsymbol{F}$
$\boldsymbol{F}$	$\boldsymbol{V}$

It is important to understand how to construct a truth table as we will use it many times in this course.

This connector is quite intuitive as we use it in our daily lives.

Some Examples

P : "Algiers is the capital of Algeria" (its value is $\boldsymbol{V}$)

$\bar{P}$: "Algiers is not the capital of Algeria" (its value is $\boldsymbol{F}$)

Q : "π is an integer" (F)

$\bar{Q}$: "π is not an integer" (V)

R : "5 is an odd number" (V)

$\bar{R}$: "5 is an even number" (F)

This first operator should now seem quite simple to you. In order to construct logical reasoning, we need to use operators that link two logical propositions together (these are called **binary operators**).

1.2.2 Conjunction "and", denoted $\wedge$

Let P and Q be two propositions.

We define a new proposition "P AND Q" which is denoted as "$P \wedge Q$". This new proposition is:

True when both P and Q are true.

False in all other cases.

From this definition, we can derive the truth table for the proposition "$P \wedge Q$":

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

The first two columns list all possible cases for the truth values of P and Q. The last column corresponds to the truth value of the proposition "$P \wedge Q$".

It is important to understand the truth table of the "AND" operator as it is used in many logical reasoning.

Some Examples

Example 1: "5 is a number less than 10 **and** 5 is even."

Let *P*: "5 is a number less than 10." ***P*** is true.

Let *Q*: "5 is even." ***Q*** is false.

The proposition A is the proposition "$P \wedge Q$".

According to the truth table of the "AND" operator, we conclude that proposition A is false.

Example 2: "The letter A is a vowel and T is a consonant."

By reasoning in the same way, we conclude that proposition **B** is true.

1.2.3 Disjunction "or", denoted $\vee$

The second binary operator we are going to study is the "OR" operator.

Let P and Q be two propositions.

We define a new proposition "P or Q" which is denoted as "$P \vee Q$".

This proposition is:

False when both P and Q are false.

True otherwise.

The truth table for the proposition "$P \vee Q$" is as follows:

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

In other words, the proposition "$P \vee Q$" is true only if either P or Q is true (or both!).

Example: "5 is a number less than 10 OR 5 is even"

What is the truth value of this proposition?

Solution: Let $\boldsymbol{P}$: "5 is a number less than 10". It is true.

Let $\boldsymbol{Q}$: "5 is even". It is false.

The proposition "$\boldsymbol{P} \vee \boldsymbol{Q}$"

According to the truth table of the "OR" operator, the proposition in the example is true.

The binary operators "NOT," "AND," and "OR" are the most important in mathematics because they allow us to define all other operators.
We are now at the heart of the matter! Indeed, implications and equivalences are used in the majority of mathematical proofs. Understanding them well allows us to avoid reasoning errors in exams... and in life too!

1.2.4 Notion of Implication "⇒"

Implication is a binary operator (i.e., it connects two propositions).

Let P and Q be two propositions.

We write $P \Rightarrow Q$ (and read "P implies Q").

Multiple Wordings for the Same Concept

$P \Rightarrow Q$ can also be read as:

✓ If P, then Q

✓ It is sufficient for P to have Q

✓ It is necessary for Q to have P

✓ Q is required for P

Hence, every time you hear one of these wordings in everyday language, it is actually an implication.

Example:

"I am joyful if he is here" corresponds to "He is here" $\Rightarrow$ "I am joyful"

"It is raining" $\Rightarrow$ "The ground is wet". If it is raining, then the ground is wet. It means that it is impossible for it to rain and the ground not to be wet.

"If I am tired, I will rest." This means that "I am tired" $\Rightarrow$ "I will rest."

Let P and Q be two propositions.

We define a new proposition "$P \Rightarrow Q$" (read as "P implies Q").

This proposition is:

False when P is true and Q is false.

True otherwise.

The truth table for the proposition "$P \Rightarrow Q$" is as follows:

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

In other words, the proposition "$P \Rightarrow Q$" is false only when P is true and Q is false.

1.2.5 Reciprocal Implication "$\rightleftharpoons$"

Here's one more thing. P and Q are still two propositions. The proposition $Q \Rightarrow P$ is called the reciprocal implication of the proposition $P \Rightarrow Q$. Remember this expression, we will use it again shortly!

1.2.6 Equivalence "$\Leftrightarrow$"

The symbol for equivalence is $\Leftrightarrow$, a double arrow that resembles the implication arrow discussed earlier.

Let P and Q be two propositions.

We define a new proposition "$P \Leftrightarrow Q$" which is read as "P is equivalent to Q".

Alternatively, it can be read as "if and only if Q".

It is also understood as "the implication $P \Rightarrow Q$ and the reciprocal implication $Q \Rightarrow P$".

This proposition has the following truth conditions:

True when P and Q have the same truth value (both true or both false).

False otherwise.

$\boldsymbol{P}$	$\boldsymbol{Q}$	$\boldsymbol{P \Leftrightarrow Q}$
V	V	V
V	F	F
F	V	F
F	F	V

When proving an equivalence, the double implication rule is often employed:

✓ First, we establish one direction of implication,

✓ then we prove the reciprocal implication.

Avoid Confusion!

Do not confuse implications and equivalences.

Whenever determining the truth value of an equivalence, be sure to check the truth value of the double implication.

1.2.7 Properties

1. $(P_1 \Leftrightarrow P_2) \Leftrightarrow (P_1 \Rightarrow P_2) \wedge (P_2 \Rightarrow P_1)$

2. $\overline{\overline{P}}_1 \Leftrightarrow P_1$

3. $P_1 \vee P_1 \Leftrightarrow P_1$

4. $P_1 \vee P_1 \Leftrightarrow P_1$

5. $\overline{P_1 \vee P_2} \Leftrightarrow \overline{P_1} \wedge \overline{P_2}$

6. $\overline{P_1 \wedge P_2} \Leftrightarrow \overline{P_1} \vee \overline{P_2}$

7. $P_1 \wedge (P_2 \wedge P_3) \Leftrightarrow (P_1 \wedge P_2) \wedge P_3$

8. $P_1 \vee (P_2 \vee P_3) \Leftrightarrow (P_1 \vee P_2) \vee P_3$

9. $P_1 \wedge (P_2 \vee P_3) \Leftrightarrow (P_1 \wedge P_2) \vee (P_1 \wedge P_3)$

10. $P_1 \vee (P_2 \wedge P_3) \Leftrightarrow (P_1 \vee P_2) \wedge (P_1 \vee P_3)$

11. $\overline{(P_1 \Rightarrow P_2)} \Leftrightarrow P_1 \wedge \overline{P_2}$

12. $P_1 \Rightarrow P_2 \Leftrightarrow \overline{P_2} \Rightarrow \overline{P_1}$ "Law of contrapositive"

Proof

✓ Let's prove property 1 : $\overbrace{(P_1 \Leftrightarrow P_2)}^{(1)} \overbrace{(P_1 \Rightarrow P_2) \wedge (P_2 \Rightarrow P_1)}^{(2)}$

We use the truth table.

P_1	P_2	$P_1 \Rightarrow P_2$	$P_2 \Rightarrow P_1$	(1): $P_1 \Leftrightarrow P_2$	(2) : $(P_1 \Rightarrow P_2) \wedge (P_2 \Rightarrow P_1)$	(1) $\Leftrightarrow$ (2)
V	V	V	V	V	V	$\boldsymbol{V}$
V	F	F	V	F	F	$\boldsymbol{V}$
F	V	V	F	F	F	$\boldsymbol{V}$
F	F	V	V	V	V	$\boldsymbol{V}$

1.3 Quantifiers

Let P be the proposition "8 is an even number". We can replace the number 8 with any other number to form new propositions. For example, we can write the proposition $P(6)$ as "6 is an even number", which is true, or the proposition $P(3)$ as "3 is an even number", which is false.

We can then write the general form of this proposition as

$P(x)$: "x is an even number", where x is called the argument of the proposition P. The truth value of the proposition $P(x)$ depends on x.

The problem is that I don't know what x is in the proposition $P(x)$. In our example, x is a number, but it needs to be specified because otherwise our proposition doesn't make sense (for example, $P(ABC)$: "Triangle ABC is an even number" doesn't make sense).

Therefore, we have invented quantifiers to indicate that we take our x from a determined set.

1.3.1 The Universal Quantifier "$\forall$"

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

Hold on! What are all these symbols?!

Stay calm, stay calm. You quickly get used to reading these mathematical symbols.

✓ The symbol $\forall$ (a reversed A) is read as "for all" or "for every." It is a quantifier that indicates that the property is true for all objects satisfying the given condition.

✓ x is a mathematical object (a number, a point, a vector...).

✓ The symbol $\in$ means "belongs to" or "is an element of." It is an operator used to indicate that x belongs to a specified set.

The notation $\forall$ comes from the German word "Alle," which means "all" in english.

Example

Translate the proposition into its equivalent mathematical form (using the appropriate quantifier and logical connector).

P: "For all x real number, if x is greater than or equal to 5, then x^2 is greater than or equal to 25."

Correction

The statement "it suffices for P to be true for Q to be true" is translated as $P \Rightarrow Q$. This equivalence is true for all x real numbers, so we use the quantifier $\forall$.

$$P(x) : \underbrace{\forall}_{\text{Quantifier}} \; x \in \mathbb{R}, x \geq 5 \; \underbrace{\Rightarrow}_{\text{Connector}} \; x^2 \geq 25$$

1.3.2 The Existential Quantifier "$\exists$"

The proposition Q: "All students are present."

Try to determine $\overline{Q}$ (in a english sentence).

Watch out! There's a trap!

The negation of "All students are present" is not "All students are absent"! In fact, if even one student is absent, the proposition Q becomes false.

We will say that the opposite proposition of Q is "At least one student is absent."

We need another quantifier to translate "there exists at least one." We could use the negation of the universal quantifier $\forall$, but to simplify the notation, we use the symbol $\exists$ (a reversed E).

Yes, $\exists$ comes from the German word "Existieren," which means "to exist" in english.

$\exists$ is used in the same way as $\forall$.

Example

$P(x) : \exists x \in \mathbb{R}$ such that $x^2 = 1$

The proposition P is read as "There exists at least one real number x whose square is equal to 1."

See how convenient mathematical notation is!

1.3.3 Multiple Quantifiers

Multiple quantifiers can be used in a proposition, and in such cases, the order of the quantifiers is important.

Example Translate into English the propositions P and Q and determine their truth value:

$P(x) : \forall x \in \mathbb{N}, \exists y \in \mathbb{N} : x < y$ (where $\mathbb{N}$ denotes the set of natural numbers)

$Q(x) : \exists x \in \mathbb{N}, \forall y \in \mathbb{N} : x < y$

Correction The proposition P means "For every natural number x, there exists a natural number y greater than x." Proposition P is **true**.

The proposition Q means "There exists a natural number x that is less than every natural number y." Proposition Q is **false**. To prove this, we can use a counterexample. There is no natural number that is less than 0.

These two propositions, despite their similar appearance, have absolutely nothing to do with each other!

Remember that changing the nature or order of quantifiers changes the meaning of the proposition.

1.3.4 Properties

1. $\overline{(\forall x P(x))} \Leftrightarrow (\exists x \overline{P(x)})$

2. $\overline{(\exists x P(x))} \Leftrightarrow (\forall x \overline{P(x)})$

Example Find the negation of the inclusion proposition "$A \subset B$".

Correction The proposition $A \subset B$ is written as "$\forall x; x \in A \Rightarrow x \in B$".

So, the negation of $A \subset B$ is written as $\overline{A \subset B}$ or $A \not\subset B$. It is equivalent to finding $\overline{\forall x; x \in A \Rightarrow x \in B}$. We use property 1:

$\overline{\forall x; x \in A \Rightarrow x \in B} \Leftrightarrow \exists x; \overline{x \in A \Rightarrow x \in B}$ (using $\overline{(P_1 \Rightarrow P_2)} \Leftrightarrow P_1 \wedge \overline{P_2}$)

$\exists x; \overline{x \in A \Rightarrow x \in B} \Leftrightarrow \exists x; x \in A$ and $x \notin B$

In summary:

$A \subset B \Leftrightarrow \forall x; x \in A \Rightarrow x \in B$

$A \not\subset B \Leftrightarrow \exists x; x \in A$ and $x \notin B$

1.4 Types of Reasoning

Now we have all the tools to carry out complete mathematical reasoning.

Reasoning allows us to establish a proposition based on one or more initial propositions that are accepted (or previously proven) by following the rules of logic. In this final part, we will detail three "types" of reasoning, three "methods" to prove a proposition:

- Finding an example or a counterexample
- Proving the contrapositive
- Reasoning by contradiction

These different forms of reasoning should be applied in specific cases.

1.4.1 Example and Counterexample

To show that a proposition of the form "there exists $x \in E$, such that $P(x)$ is true", we find an x for which $P(x)$ is true. This is providing an **example**.

Example: P: "There exist $(x, y, z) \in \mathbb{N}^3$ such that $x^2 = y^2 + z^2$". Show that P is true.

Solution: Let $x = 5$, $y = 4$, and $z = 3$.

x, y, and z satisfy $x^2 = y^2 + z^2$ (since $25 = 16 + 9$).

Therefore, proposition P is true.

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

Example: Let P be the proposition "$\forall n \in \mathbb{N}$, $n^2 + 1$ is a prime number".

Prove that P is false.

Solution: To prove that P is false, we will show that its negation $\neg P$ is true.

$\neg P$ is the proposition "$\exists n \in \mathbb{N}$ such that $n^2 + 1$ is not a prime number".

Let $n = 3$. Then $n^2 + 1 = 10$.

10 is not a prime number.

n is a **counterexample** of proposition P.

Therefore, proposition P is false.

n is an **example** of the proposition $\neg P$.

n is a **counterexample** of the proposition P.

Thus, proposition P is false.

1.4.2 Contrapositive

I hope you remember the truth table for implication! No? Well, try to recall it (in your mind, if possible, or refer to the previous section) before moving on to the next exercise.

Exercise: Let P and Q be two propositions. Show that $(P \Rightarrow Q)$ is equivalent to $(\neg Q \Rightarrow \neg P)$.

Solution: You guessed it right! We will use a truth table to justify this equivalence.

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$	$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$
T	T	F	F	T	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

Therefore, $(P \Rightarrow Q) \overbrace{\Leftrightarrow}^{\text{equivalent to}} (\neg Q \Rightarrow \neg P)$.

1.4.2.1 Definition

The proposition $(\neg Q \Rightarrow \neg P)$ is called the **contrapositive** of the proposition $(P \Rightarrow Q)$.

A proposition and its contrapositive are equivalent, which means that one can be proven to prove the other. For example, to prove $(P \Rightarrow Q)$, we can use contrapositive reasoning to prove $(\neg Q \Rightarrow \neg P)$.

1.4.2.2 Example and Exercise

Example: To prove "If it rains, then the ground is wet", I will prove "If the ground is not wet, then it does not rain."

Exercise: Prove the proposition $P : \forall n \in \mathbb{N}$, if n^2 is even, then n is even.

Hint 1: Let n be a natural number. There are two cases:

- ✓ n is even: $\exists n \in \mathbb{N} : n = 2k$ where $k \in \mathbb{N}$.
- ✓ n is odd: $\exists n \in \mathbb{N} : n = 2k + 1$ where $k \in \mathbb{N}$.

Solution: We will prove this by contrapositive reasoning. Instead of proving that if n^2 is even, then n is even, we will prove that if n is odd, then n^2 is odd.

Assume n is odd: $\exists k \in \mathbb{N} : n = 2k + 1$ where $k \in \mathbb{N}$ (as given in the hint).

So,

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 \quad \text{(Squaring both sides)}$$

Therefore, $n^2 = 2(2k^2 + k) + 1$ (Factorizing) (k is a natural number, so $k^2 + k$ is also a natural number).

Hence, $n^2 = 2h + 1$, where $h = (2k^2 + k) \in \mathbb{N}$, and it is odd.

We have shown that if n is odd, then n^2 is odd. Thus, $\forall n \in \mathbb{N}$, if n^2 is even $\Rightarrow$ n is even.

This completes the proof.

1.4.3 Reasoning by Contradiction

Why introduce absurdity in logical reasoning?!

It may sound strange, but rest assured, reasoning by contradiction (contrary to its name) is not absurd at all. It is, in fact, very logical!

This reasoning is based on the principle of excluded middle, which states that if a proposition is not false, then it is true. For example, imagine you know that something is true, but you don't know how to prove it. By reasoning by contradiction, you start by assuming that this thing is false. Then, by following the rules of logic, you deduce the consequences of this assumption and arrive at an irrefutable contradiction (like $1 = 2$ or 2 and 4 are coprime). You conclude that your initial assumption must be false, i.e., the thing you wanted to prove is not false, so it must be true.*

1.4.3.1 Definition

Reasoning by contradiction is a form of logical reasoning. It consists of:

✓ either proving that a proposition P is true by proving the absurdity of the proposition $\neg P$,

✓ or proving that a proposition P is false by logically deducing absurd consequences.

Now, let's see reasoning by contradiction in all its glory through one of its classic examples: the irrationality of $\sqrt{2}$.

1.4.3.2 Example

We want to prove that proposition P is true.

$$P\text{: "}\sqrt{2} \notin \mathbb{Q}\text{", "}\sqrt{2}\text{ is an irrational number"}$$

We reason by contradiction. So, we will show that the proposition $\neg P$ is absurd.

$\neg P$ is translated as "$\sqrt{2} \in \mathbb{Q}$" or "$\sqrt{2}$ is a rational number".

If $\sqrt{2} \in \mathbb{Q}$, it can be expressed as a fraction, i.e., there exist $p \in \mathbb{Z}$ and $q \in \mathbb{Z}$ such that $\sqrt{2} = \frac{p}{q}$, where p and q are coprime.

We simplify this equation:

$$2 = \frac{p^2}{q^2} \quad \text{(Squared both sides)}$$

$$So, 2q^2 = p^2 \text{ (By multiplying both sides by } q^2).$$

Therefore, p^2 is even, and thus, p is even (proved by contrapositive in the previous section). Therefore, $\exists k \in \mathbb{Z}$ such that $p = 2k$ (as seen before).

By substituting into the previous equation, we get: $2q^2 = (2k)^2 \Rightarrow q^2 = (2k)^2 = 4k^2$. So, q^2 is even, and thus, q is even, which is impossible since p and q are coprime.

This leads to a contradiction.

Therefore, the proposition $\neg P$ is false.

Thus, $\sqrt{2}$ is an irrational number.

In the case where the proposition to be proven is of the form $P \Rightarrow Q$, reasoning by contradiction consists of proving that the proposition $P \wedge \neg Q$ is false. To do this, we assume that P is true and Q is false, deduce the consequences logically, and show that we arrive at a contradiction.

1.5 Corrected Exercises

Exercise 1. Among the following expressions, which ones are propositions? For propositions, indicate whether they are true or false.

(a) $2 + 3 = 5$

(b) $\forall n \in \mathbb{N}, \quad n + 2 = 4$

(c) $\exists n \in \mathbb{N} \quad n + 2 = 3$

(d) This exercise is difficult

(e) $x \in \mathbb{N}$

Solution.

a. This expression is a true proposition.

b. This expression is a false proposition because for $n = 1 \in \mathbb{N}$, we have $n + 2 = 3 \neq 4$.

c. This expression is a true proposition because there exists an element $n = 1 \in \mathbb{N}$ such that $n + 2 = 3$.

d. This expression is not a proposition because we cannot assign a truth value to it.

e. This expression is not a proposition because we don't know the nature of the element x, so we cannot assign a truth value to it.

Exercise 2. In the Mathematics and Computer Science Bachelor's program, a student who is admitted to the second year must choose between Mathematics or Computer Science but not both simultaneously. This is the exclusive OR ($\underline{\vee}$). Provide the truth table.

Solution. Here is the truth table for the "exclusive OR." It is different from the truth table for the disjunction ($\vee$) because, in this particular case, the "exclusive OR" is true only when the two assertions P and Q are different. Thus, one can choose both at the same time.

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

Exercise 3. In which cases are the following propositions true?

(a) $(P \Longrightarrow Q) \wedge (\bar{P} \Longrightarrow Q)$

(b) $\overline{P \wedge (\overline{Q \wedge R})} \Leftrightarrow Q$

(c) $((P \vee Q) \Longrightarrow R) \Longleftrightarrow (P \Longrightarrow R) \wedge (Q \Longrightarrow R)$.

Solution.

a. $(P \Longrightarrow Q) \wedge (\bar{P} \Longrightarrow Q)$

P	Q	$\bar{P}$	$P \Longrightarrow Q$	$\bar{P} \Longrightarrow Q$	$(P \Longrightarrow Q) \wedge (\bar{P} \Longrightarrow Q)$
1	0	0	0	1	0
0	1	1	1	1	1
1	1	0	1	1	1
0	0	1	1	0	0

b. $\overline{P \wedge (\overline{Q \wedge R})} \Leftrightarrow Q$ (Homework for students)

c. $\underbrace{((P \vee Q) \Longrightarrow R)}_{(1)} \Longleftrightarrow \underbrace{(P \Longrightarrow R) \wedge (Q \Longrightarrow R)}_{(2)}$

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

Exercise 4. Consider the following four propositions:

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

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

c- $\forall x \in \mathbb{R}, \forall y \in \mathbb{R} \quad x + y > 0$

d- $\exists x \in \mathbb{R}, \forall y \in \mathbb{R} \quad y^2 > x.$

Are these propositions true or false? Provide their negations.

Solution.

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

The assertion (a) is false: Can we find a real number x such that for every real number y, their sum is always positive? It is not always true, for example, we can take $y = -(x+1)$. We would have $x + y = x - x - 1 = -1 < 0$.

The negation of assertion (a) is: $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}; \quad x + y \leq 0$, which is a true statement.

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

The assertion (b) is true: Indeed, for every real number x, there exists a y dependent on x. Let's take, for example, $y = -x + 1$, which implies that $x + y = x - x + 1 = 1 > 0$.

The negation of assertion (b) is: $\exists x \in \mathbb{R}, \forall y \in \mathbb{R} \quad x + y \geq 0$, which is a false statement.

c. The assertion (c) is false. We just need to find an x and a y that do not satisfy (c). For example, let $x < 0$ and $y < 0$.

The negation of this assertion is: $\exists x \in \mathbb{R}, \exists y \in \mathbb{R} x + y \leq 0$, which is a true statement.

d. Homework for the students.

Exercise 5.

1. Using proof by contradiction, prove that

(a) $\sqrt{2}$ is not a rational number.

(b) If $n \in \mathbb{N}^*$, then $n^2 + 1$ is not a perfect square.

2. Prove by induction

(a) $\forall n \in \mathbb{N}^* 1 + 2^2 + 3^2 + \ldots\ldots\ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$

(b) $\forall n \in \mathbb{N} 2^n > n$.

3. Using proof by contrapositive, prove that if the integer $(n^2 - 1)$ is not divisible by 8, then n is even.

Solution.

1. Using proof by contradiction, prove that

(a) $\sqrt{2}$ is not a rational number.

Assume, by contradiction, that $\sqrt{2}$ is rational: that is, there exist positive integers a and b such that

$$\sqrt{2} = \frac{a}{b} \Rightarrow a = \sqrt{2}b \Rightarrow 2b^2 = a^2.$$

Then, we deduce that a^2 is even, which implies that a is also even (see the example from the course). In other words, there exists a positive integer k such that

$$a^2 = 4k^2 = 2b^2 \Rightarrow b^2 = 2k^2.$$

Thus, b^2 is even, which means that b is also even. Therefore, we can simplify the fraction $\frac{a}{b}$ by 2, contradicting the assumption that a and b are coprime (i.e., the fraction cannot be further simplified).

(b) Homework.

2. Prove by induction

(a) $\forall n \in \mathbb{N}^* 1 + 2^2 + 3^2 + \ldots\ldots\ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

1- Verify if this proposition holds for $n = 1$ and 2.

For $n = 1$, we have $\frac{1(1+1)(2+1)}{6} = 1$, which is true.

For $n = 2$, we have $\frac{2(2+1)(4+1)}{6} = 1 + 2^2 = 5$, which is true.

2- Assume that this proposition is true for n, i.e., ($P(n)$ is true). Show that the proposition ($P(n+1)$ is true).

3- Based on 2, we have

$$P(n) \Leftrightarrow \forall n \in \mathbb{N}^* 1 + 2^2 + 3^2 + \ldots\ldots\ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Then, we have

$$\begin{aligned}
&\underbrace{1 + 2^2 + 3^2 + \ldots\ldots\ldots + n^2}_{P(n)} + (n+1)^2 \\
=&\frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\
=&\frac{n(n+1)(2n+1)}{6} + \frac{6(n+1)^2}{6} \\
=&(n+1)\left[\frac{n(2n+1)+6(n+1)}{6}\right] = (n+1)\left[\frac{2n^2+7n+6}{6}\right] \\
=&\frac{(n+1)(n+2)(2n+3)}{6} = P(n+1).
\end{aligned}$$

b. $\forall n \in \mathbb{N} 2^n > n$. Homework.

3. Using proof by contrapositive, prove that if the integer $(n^2 - 1)$ is not divisible by 8, then n is even.

$\underbrace{\text{Let } P : \left(n^2 - 1\right) \text{ is not divisible by } 8}_{P} \Rightarrow$

Now, we need to use the contrapositive

$\underbrace{Q : \ n \text{ is odd: that is, } \exists \text{ an integer } k \text{ such that } n = 2k+1}_{\bar{Q}} \Rightarrow$

$\underbrace{\left(n^2 - 1\right) \text{ is divisible by } 8 : \text{ that is, } \exists 1}_{\bar{P}}$

Assume that n is odd, so there exists an integer k such that $n = 2k + 1$, which implies that $n^2 = (2k+1)^2$.

Then,

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

Now, we have two cases: k is even or k is odd.

1- If we assume that k is even, then there exists an integer k' such that $k = 2k'$, and we have

$$\begin{aligned}
n^2 - 1 &= 4k^2 + 4k \\
&= 4\left(2k'\right)^2 + 4\left(2k'\right) \\
&= 8k'^2 + 8k' = 8\left(k'^2 + k'\right) = 8p.
\end{aligned}$$

2- If k is odd, then there exists an integer k'' such that $k = 2k'' + 1$, and we have:

$$\begin{aligned} n^2 - 1 &= 4\left(2k'' + 1\right)^2 + 4\left(2k'' + 1\right) \\ &= 4\left(2k''\right)^2 + 4\left(2k''\right) + 4 + 4\left(2k''\right) + 4 \\ &= 8k''^2 + 8k'' + 8k'' + 8 \\ &= 8\left(k''^2 + 2k'' + 1\right) = 8p'. \end{aligned}$$

Thus, $(n^2 - 1)$ is divisible by 8.

1.6 Unsolved Exercises

Exercise 1. Let P, Q, and R be three propositions. Prove the following properties:

1. $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$
2. $(P \Leftrightarrow Q) \Leftrightarrow ((\neg P \wedge \neg Q) \vee (\neg Q \wedge \neg P))$
3. $(P \wedge (\neg Q \wedge \neg R)) \Leftrightarrow ((P \wedge \neg Q) \vee (P \wedge \neg R))$

Exercise 2. Rewrite the following sentences using quantifiers:

1. f is a constant function on $\mathbb{R}$.
2. The graph of the function f intersects the line $y = x$.
3. The equation $\sin x = x$ has one and only one solution in $\mathbb{R}$.
4. For every integer, there exists an integer that is strictly greater.

Exercise 3. Negate the following formulas:

1. $0 \leq x \leq 25 \Rightarrow \sqrt{x} \leq 5$.
2. $0 < x \leq 1$ or $2 \leq y < 3$.
3. $\exists x \in \mathbb{R} \mid \cos(x) = 0$ and $\exists x \in \mathbb{R} \mid \sin(x) = 0$.
4. $\forall \epsilon > 0, \exists \alpha > 0 \mid \forall x \in D_f, (|x - x_0| < \alpha \Rightarrow |f(x) - f(x_0)| \geq \epsilon)$.

Exercise 4. Are the following assertions true or false?

(a) $\exists x \in \mathbb{R} \mid \forall y \in \mathbb{R} : x + y > 0$;

(b) $\forall x \in \mathbb{R} : \exists y \in \mathbb{R} \mid x + y > 0$;

(c) $\forall x \in \mathbb{R} : \forall y \in \mathbb{R} : x + y > 0$;

(d) $\exists x \in \mathbb{R} \mid \forall y \in \mathbb{R} : y^2 > x$.

Exercise 5. Prove the following formulas:

1. $|x| < 0.1 \Rightarrow |2x^2 - x| < 0.12$ (Direct proof).

2. For any integer n, $n^2 + 3n$ is even (Proof by cases).

3. $\forall n \in \mathbb{N} : n^2$ is even $\Rightarrow n$ is even (Contrapositive).

4. $\sqrt{2}$ is irrational (Proof by contradiction).

5. $\forall a, b \in \mathbb{R}^+ : \frac{a}{1+b} = \frac{b}{1+a} \Rightarrow a = b$ (Proof by contradiction).

6. $\forall n \in \mathbb{N} : 2^n > n$ (Proof by induction).

7. For real numbers a, b, c, and d such that $a \leq b$ and $c \leq d$, is it always true that $ac \leq bd$? (Counterexample).

Exercise 6.

1. Let a and b be two nonzero natural numbers. Prove that

$$((\exists k \in \mathbb{N} \mid b = ka) \text{ and } (\exists k \in \mathbb{N} \mid a = kb)) \Rightarrow (a = b)$$

2. Prove by induction the following equalities:

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \quad \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \quad \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

3. Let $n \in \mathbb{N}$. Prove by contradiction that $n^2 + 1$ is not a perfect square.

Chapter 2

Sets and Functions

2.1 Definitions and Examples

2.1.1 Sets and Elements

* Intuitively, a set is a collection of objects. The objects in a set are called elements of that set, and an element a belongs to E (written as $a \in E$) or does not belong to E (written as $a \notin E$).

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

* A set $E = \{a\}$, consisting of a single element, is called a singleton.

* Let E be a set. If a set A is contained in E, we say that A is a subset or a sub-set of E. The elements of E that do not belong to set A form a new set called the complement of A in E, denoted as A^c or $C_E(A)$. Formally, $C_E(A) = \{x \in E \mid x \notin A\}$.

2.1.2 Set Operations

Given two sets A and B, we can construct other sets.

* We say that A is included in B (A is a subset of B or a part of B) and we denote it as $A \subset B$ if every element of A is also an element of B.

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

* We say that A and B are equal if and only if $A \subset B$ and $B \subset A$.

* Given two sets A and B, the union of A and B, denoted as $A \cup B$ (read as "A union B"), is the set of elements that belong to either A or B.

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

* Given two sets A and B, the intersection of A and B, denoted as $A \cap B$ (read as "A intersect B"), is the set of elements that belong to both A and B.

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

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

Example In $\mathbb{N}$ (the set of natural numbers), if we denote by $\mathcal{D}(n)$ the set of divisors of the natural number n, we have

$$\mathcal{D}(24) \cup \mathcal{D}(16) = \{1, 2, 3, 4, 6, 8, 12, 16, 24\} \quad \text{and} \quad \mathcal{D}(24) \cap \mathcal{D}(16) = \{1, 2, 3, 4, 8\}$$

2.1.3 Properties and Rules of Calculations

Here are some properties and rules of calculations on sets.

Proposition 2.1 Let A, B, C be subsets of a set E. Then:

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

2. $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$.

3. $A \cup B = B \cup A$, $A \cap B = B \cap A$ (Commutativity).

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

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

Proof. We prove that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$$\begin{aligned} \text{Let } x \in A \cup (B \cap C) &\Leftrightarrow x \in A \text{ or } x \in (B \cap C) \\ &\Leftrightarrow x \in A \text{ or } (x \in B \text{ and } x \in C) \\ &\Leftrightarrow (x \in A \text{ or } x \in B) \text{ and } (x \in A \text{ or } x \in C) \\ &\Leftrightarrow (x \in A \cup B) \text{ and } (x \in A \cup C) \\ &\Leftrightarrow x \in (A \cup B) \cap (A \cup C). \end{aligned}$$

□

Definition 2.1 (Power Set) Let E be a set. We admit the existence of a set denoted by $\mathcal{P}(E)$ such that the following equivalence holds:

$$X \in \mathcal{P}(E) \Leftrightarrow X \subset E$$

$\mathcal{P}(E)$ is called the power set of E.

Remark 2.1 If $\text{card}(E) = n$, then $\text{card}(\mathcal{P}(E)) = 2^n$.

Example If $E = \{1, 2, 3\}$, then $\text{card}(\mathcal{P}(E)) = 2^3 = 8$ and

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

Definition 2.2 (Set Difference) Let A, B be two subsets of E.

1. The difference of A and B, denoted $A \setminus B$, consists of elements that are in A but not in B, i.e., $A \setminus B = A \cap C_E(B)$.
2. The symmetric difference of A and B, denoted $A \triangle B$, is the set $(A \setminus B) \cup (B \setminus A)$ or $(A \cup B) \setminus (A \cap B)$.

Example 1. In $\mathbb{N}$, we have $\mathcal{D}(24) \setminus \mathcal{D}(16) = \{3, 6, 12, 24\}$ and $\mathcal{D}(16) \setminus \mathcal{D}(24) = \{16\}$. Also, $\mathcal{D}(24) \triangle \mathcal{D}(24) = \{6, 12, 16, 24\}$.

2. The set $\mathbb{R} \setminus \mathbb{Q}$ contains irrational numbers like π.

Remark 2.2 When $A \subset E$, we have $E \setminus A = C_E(A)$.

Proposition 2.2 Let A, B be two subsets of E. Then:

1. $A \setminus A = \emptyset$.
2. $A \setminus \emptyset = A$.
3. $A \cup C_E(A) = E$.
4. $A \cap C_E(A) = \emptyset$.
5. $C_E(C_E(A)) = A$.
6. $C_E(A \cap B) = C_E(A) \cup C_E(B)$.
7. $C_E(A \cup B) = C_E(A) \cap C_E(B)$.

Proof. We prove that $C_E(A \cap B) = C_E(A) \cup C_E(B)$.

$$\begin{aligned}
&\text{Let } x \in C_E(A \cap B) \Leftrightarrow x \notin (A \cap B) \\
&\Leftrightarrow \overline{x \in (A \cap B)} \\
&\Leftrightarrow \overline{x \in A \text{ and } x \in B} \\
&\Leftrightarrow \overline{x \in A} \text{ or } \overline{x \in B} \\
&\Leftrightarrow x \notin A \text{ or } x \notin B \\
&\Leftrightarrow x \in C_E(A) \cup C_E(B).
\end{aligned}$$

□

Definition 2.3 (Partition) Let E be a set. A partition of E is a set $\{E_i\}$ of subsets of E that satisfies the following two conditions:

1. $E = \bigcup_{i \in I} E_i$
2. $E_i \cap E_j = \emptyset$ for all $i \neq j \in I$.

Example Let A be a subset of E. Then the set $\{A, C_E(A)\}$ is a partition of E.

Definition 2.4 (Cartesian Product) Let A, B be two sets. The Cartesian product, denoted $A \times B$, is the set of pairs (x, y) where $x \in A$ and $y \in B$.

$$A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}$$

Example

1. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$.

2. Let $A = \{1, 2, 3\}$ and $B = \{a, b\}$. Then $A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$.

Generalization If we consider sets $A_1, A_2, \ldots, A_n$, we can similarly define n-tuples $(x_1, x_2, \ldots, x_n)$ where $x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n$.

$$A_1 \times A_2 \times \ldots \times A_n = \{(x_1, x_2, \ldots, x_n) \mid x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n\}.$$

Proposition 2.3 Let A, B, C, D be four subsets of E. Then:

1. $(A \times C) \cup (B \times C) = (A \cup B) \times C$.

2. $(A \times C) \cup (A \times D) = A \times (C \cup D)$.

3. $(A \times C) \cap (B \times D) = (A \cap B) \times (C \cap D)$.

Proof. We prove that $(A \times C) \cup (B \times C) = (A \cup B) \times C$.

$$\begin{aligned}(A \times C) \cup (B \times C) &= \{(x, y) \mid (x, y) \in A \times C \text{ or } (x, y) \in B \times C\} \\ &= \{(x, y) \mid (x \in A \text{ and } y \in C) \text{ or } (x \in B \text{ and } y \in C)\} \\ &= \{(x, y) \mid (x \in A \text{ or } x \in B) \text{ and } y \in C\} \\ &= (A \cup B) \times C.\end{aligned}$$

□

2.1.4 Definitions and Examples

Definition 2.5 Let E, F be two sets. We say that f is a function from E to F if for every element $x \in E$, there exists a unique element $y \in F$ such that $f(x) = y$, and we write

$$f : E \longrightarrow F \quad \text{or} \quad E \xrightarrow{f} F$$

* The set E is called the domain and F is called the codomain. The element x is called the pre-image and y is called the image of x under f.

* We denote by $\mathfrak{F}(E,F)$ the set of all functions from E to F.

Example

1. $\begin{array}{ccccc} f : \{1,2,3\} & \longrightarrow & \{2,4,5\} \\ x & \mapsto & x^2 \end{array}$ is not a function.

2. The identity function $\begin{array}{ccc} f : E & \longrightarrow & E \\ x & \mapsto & x \end{array}$ is a function and will be very useful in the following.

3. The projections $\begin{array}{ccc} P_x : E \times F & \longrightarrow & E \\ (x,y) & \mapsto & P_x(x,y) = x \end{array}$ $\begin{array}{ccc} P_y : E \times F & \longrightarrow & F \\ (x,y) & \mapsto & P_y(x,y) = y \end{array}$ are also functions.

Definition 2.6 (Restrictions and Extensions) Let f be a function from E to F.

1. The restriction of f to a subset $A \subset E$ is the function denoted $f_{|A} : A \longrightarrow F$ defined by

$$f_{|A} = f(x), \quad \forall x \in A$$

2. The extension of f to a set E' containing E is any function g from E' to F whose restriction is f.

Example If f is the identity function from $\mathbb{R}^+$ to itself, it has infinitely many extensions to $\mathbb{R}$, among which:

1. The identity function on $\mathbb{R}$.

2. The absolute value function from $\mathbb{R}$ to itself.

3. The function h defined by $h(x) = \frac{1}{2}(x + |x|)$, which is identically zero on $\mathbb{R}^-$.

2.1.5 Direct Image and Inverse Image

Definition 2.7 Let E, F be two sets.

1. For $A \subset E$ and $f : E \longrightarrow F$, the direct image of A under f is a subset of F defined by

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

2. For $B \subset F$ and $f : E \longrightarrow F$, the inverse image of B under f is a subset of E defined by

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

Example Let f be a given function:

$$\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \mapsto & 2n+1 \end{array}$$

1. Let $A = \{0, 1, 2\}$, then $f(A) = \{f(n) \mid n \in A\} = \{f(0), f(1), f(2)\} = \{1, 3, 5\}$.

2. Let $B = \{5\}$, then $f^{-1}(B) = \{n \in \mathbb{N} \mid f(n) \in B\} = \{n \in \mathbb{N} \mid f(n) = 5\} = \{2\}$.

Proposition 2.4 Let $f : E \longrightarrow F$ be a function, A_1, A_2 be two subsets of E, and B_1, B_2 be two subsets of F. Then

(1) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2), \quad f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$;

(2) If $A_1 \subset A_2$, then $f(A_1) \subset f(A_2)$;

(3) $A_1 \subset f^{-1}(f(A_1))$;

(4) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2), \quad f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$;

(5) If $B_1 \subset B_2$, then $f^{-1}(B_1) \subset f^{-1}(B_2)$;

(6) $f(f^{-1}(B_1)) \subset B_1$.

Proof: We prove property (2).

Let $y \in f(A_1)$, then $\exists x \in A_1 \mid f(x) = y$, and since $A_1 \subset A_2$, there exists $x \in A_2 \mid f(x) = y$. Therefore, $y \in f(A_2)$.

□

Definition 2.8 (Composition) Let E, F, G be three sets, and f, g be two functions such that

$$E \xrightarrow{f} F \xrightarrow{g} G$$

Then we can obtain a function from E to G, denoted by $h = g \circ f$, and called the composition of f and g, defined as

$$\forall x \in E, h(x) = g \circ f(x) = g[f(x)]$$

Remark 2.3 In general, $f \circ g \neq g \circ f$. This is illustrated by real functions

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

$$f \circ g(x) = f[g(x)] = f(2x+1) = (2x+1)^2, \quad g \circ f(x) = g[f(x)] = g\left(x^2\right) = 2x^2 + 1.$$

Therefore, $f \circ g \neq g \circ f$.

* However, function composition is associative: $h \circ (g \circ f) = (h \circ g) \circ f$.

2.1.6 Injection, Surjection, Bijection

Definition 2.9 Let E, F be two sets and $f : E \longrightarrow F$ be a function.

1. f is injective if and only if

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

2. f is surjective if and only if

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

* Another formulation: f is surjective if and only if $f(E) = F$.

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

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

Remark 2.4 If f is bijective, and only in this case, to each $y \in F$ is associated a unique $x \in E$.

We can define a bijective function, denoted as

$$f^{-1} : F \longrightarrow E$$

and called the inverse function of f. We have the equivalence

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

Example Let $f : \mathbb{N} \longrightarrow \mathbb{Q}$ be defined by $f(x) = \frac{1}{1+x}$. Let's show that f is injective. Assume $x, x' \in \mathbb{N}$ such that $f(x) = f(x')$. Then $\frac{1}{1+x} = \frac{1}{1+x'}$, which implies $1 + x = 1 + x'$ and thus $x = x'$. Therefore, f is injective.

However, f is not surjective. We need to find an element y that does not have a pre-image under f. Here it is easy to see that we always have $f(x) \leq 1$, so for example $y = 2$ has no pre-image. Hence, f is not surjective and therefore not bijective.

Theorem 2.1 Let E, F, G be three sets and f, g be two functions such that $f : E \longrightarrow F$ and $g : F \longrightarrow G$

1. If f and g are injective, then $g \circ f$ is injective.
2. If f and g are surjective, then $g \circ f$ is surjective.
3. If f and g are bijective, then $g \circ f$ is bijective.
4. If f and g are bijective, then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof

1. Since f and g are injective, we have

$$(g \circ f)(x) = (g \circ f)(y) \Rightarrow f(x) = f(y) \Rightarrow x = y.$$

2. Since f and g are surjective, we have

$$(g \circ f)(E) = g[f(E)] = g(F) = G.$$

3. Follows directly from (1) and (2).

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

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

   On the other hand,

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

   Therefore, $(g \circ f)^{-1}(z) = (f^{-1} \circ g^{-1})(z) \quad \forall z \in G$. Hence, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

2.2 Exercises with Solutions

Exercise 1.

1. Let $A = \{1, 2, 3, 4, 5\}$. Determine whether the following statements are true:

$$2 \in A, 3 \subset A, \emptyset \in A, \{\emptyset\} \subset A, A \cup \{\emptyset\} = A$$

2. Let $B = \{1, 2\}$ and $C = \{1, 3\}$ be two sets.

(a) Determine $B \cap C, B \cup C, C_A(B), C_A(C), A \backslash B$, and $B \triangle C$.

(b) Determine $B \times C, B \times \emptyset, B \times \{\emptyset\}$, and $\mathcal{P}(\mathcal{P}(B))$.

Exercise 2. Let A, B, C be three subsets of the set E. Show that:

1. $A \cap B = \emptyset \Leftrightarrow A \subset C_E(B)$

2. $A \subset B \Leftrightarrow C_E(B) \subset C_E(A)$.

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

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

5. $C_E(A) \Delta C_E(B) = A \triangle B, \quad C_E(A \triangle B) = C_E(A) \triangle B (*)$

6. $(A \times C) \cup (B \times C) = (A \cup B) \times C$.

7. $A \subset B \Rightarrow \mathcal{P}(A) \subset \mathcal{P}(B)$.

Exercise 3. Let A, B, C be three subsets of the set E. Show that:

1. $A = B \Leftrightarrow A \cap B = A \cup B$.

2. $A \cup B = A \cap C \Leftrightarrow B \subset A \subset C$.

3. $A \cap B = \emptyset \Leftrightarrow C_E(A) \cup C_E(B) = E$.

4. $A \triangle B = \emptyset \Leftrightarrow A = B$.

5. $(A \cap B) \backslash C = (A \backslash C) \cap (B \backslash C) = (A \backslash C) \cap B = (B \backslash C) \cap A$.

Exercise 4. Let $f : E \longrightarrow F$ be a function. Let A, B be two subsets of the set E and C, D be two subsets of the set F. Show that:

1. $f(A \cap B) \subset f(A) \cap f(B), \quad f(A \cup B) = f(A) \cup f(B) (*)$

2. f is injective $\Leftrightarrow f(A \cap B) = f(A) \cap f(B)$.

3. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D), \quad f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)(*)$

4. $f\left(f^{-1}(C)\right) \subset C$.

5. f is surjective $\Leftrightarrow f\left(f^{-1}(C)\right) = C$.

6. $f^{-1}\left(C_F(C)\right) = C_E f^{-1}(C)$. 7. $f^{-1}(C \triangle D) = f^{-1}(C) \Delta f^{-1}(D)$.

Exercise 5. Consider the function f defined by

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x) = \frac{2x}{1+x^2} \end{aligned}$$

1. Is f injective? Surjective?

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

3. Show that the function g defined by

$$\begin{aligned} g : [-1,1] &\longrightarrow [-1,1] \\ x &\longmapsto g(x) = f(x) \end{aligned}$$

is a bijection and find its inverse function g^{-1}.

Exercise 6. Let E be a non-empty set. Consider a function f from E to $\mathbb{R}$ such that

$$\begin{cases} \text{i) } f(\phi) = 0, \\ \text{ii) } f(E) = 1, \\ \text{iii) } \forall A, B \in \mathcal{P}(E) : f(A \cup B) = f(A) + f(B), \text{ if } A \cap B = \phi. \end{cases}$$

1. For any subset A of E, express $f\left(C_E^A\right)$ in terms of $f(A)$.

2. Prove that $\forall A, B \in \mathcal{P}(E) : f(A \cup B) = f(A) + f(B) - f(A \cap B)$.

3. Furthermore, suppose that

$$\text{iv) } \forall A \in \mathcal{P}(E) : f(A) \geq 0.$$

(a) Show that $\forall A, B \in \mathcal{P}(E) : A \subset B \Rightarrow f(A) \leq f(B)$.

(b) Show that $\forall A \in \mathcal{P}(E) : 0 \leq f(A) \leq 1$.

2.2.1 Solution

Exercise 1.

1.

* $2 \in A$ means that 2 is an element of A. This is true because the elements of A are 1, 2, and 3.
* $3 \subset A$ means that 3 is a subset of A. This is false because 3 is an element of A and not a subset of A.
* $\phi \in A$ means that ϕ is an element of A. This is false because the elements of A are 1, 2, and 3, but ϕ is not among these elements.
* $\{\phi\} \subset A$ means that the singleton $\{\phi\}$ is a subset of A. This is false because $\{\phi\}$ is a subset of $P(A)$ (the power set of A) and not a subset of A.
* $A \cup \{\phi\} = \{1, 2, 3, \phi\}$. This is false because A has three elements.

2.

a) $B \cap C = \{1\}; B \cup C = \{1, 2, 3\}; C_A(B) = \{3, 4, 5\}; C_A(C) = \{2, 4, 5\}; A \backslash B = \{3, 4, 5\}.$

$B \triangle C = \{B \cup C) \backslash (B \cap C) = \{1, 2, 3\} \backslash \{1\} = \{2, 3\}$

b)

* $B \times C = \{(x, y) \mid x \in B \wedge y \in C\} = \{(1, 1), (1, 3), (2, 1), (2, 3)\}.$
* $B \times \phi = \{(x, y) \mid x \in B \wedge y \in \phi\}$, where ϕ does not contain any elements, so $B \times \phi = \phi.$
* $B \times \{\phi\} = \{(x, y) \mid x \in B \wedge y \in \{\phi\}\} = \{(1, \phi), (2, \phi)\}.$
* $P(B) = \{\phi, B, \{1\}, \{2\}\}$,so

$$P(P(B)) = \{\phi; P(B); \{\phi\}; \{B\}; \{\{1\}\}; \{\{2\}\}; \{\phi, B\}; \{\phi, \{1\}\}; \{\phi, \{2\}\}; \{B, \{1\}\}; \{B, \{2\}\}; \{\{1\}, \{2\}\}; \{\phi, B, \{1\}\}; \{\phi, B, \{2\}\}; \{B, \{1\}, \{2\}\}; \{\phi, \{1\}, \{2\}\}.$$

Exercise 2.

1. $A \cap B = \phi \Leftrightarrow A \subset C_E(B).$

$\Rightarrow$ We have $A \cap B = \phi$. Let $x \in A$ and assume that $x \notin C_E(B)$.

Then $x \notin C_E(B) \Rightarrow x \in C\,(C_E(B)) = B \Rightarrow x \in A \cap B \Rightarrow A \cap B \neq \phi$, which is absurd. Thus, $x \in C_E(B)$.

$\Leftarrow$ We assume that $A \cap B \neq \phi$. Then, $\exists x \in E / x \in A \cap B \Rightarrow x \in A \wedge x \in B$ and since $A \subset C_E(B)$, we have $x \in C_E(B) \wedge x \in B \Rightarrow x \in C_E(B) \cap B = \phi$, which is a contradiction. Therefore, $A \cap B = \phi$.

2. $A \subset B \Leftrightarrow C_E(B) \subset C_E(A)$.

$\Rightarrow$ Let's assume that $A \subset B$ and $x \in C_E(B)$. Then $x \in C_E(B) \Rightarrow x \notin B$ and since $A \subset B$, we have $x \notin A \Rightarrow x \in C_E(A) \Rightarrow C_E(B) \subset (A)$.

$\Leftarrow$ We have $C_E(B) \subset C_E(A)$. Then $x \in A \Rightarrow x \notin C_E(A) \Rightarrow x \notin C_E(B) \Rightarrow x \in B$. Therefore, $A \subset B$.

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

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

The same applies to the union.

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

$$A \backslash (B \cup C) \overset{\text{Def}}{=} A \cap C(B \cup C) \overset{(3)}{=} A \cap \Big(\; C_E(B) \;\; \cap \;\; C_E(C) \; \Big)$$
$$= (A \cap C_E(B)) \cap (A \cap C_E(C)) \overset{\text{Def}}{=} (A \backslash B) \cap (A \backslash C).$$

5. $C_E(A) \Delta C_E(B) = A \triangle B$.

According to the definition: $A \Delta B = (A \backslash B) \cup (B \backslash A) = (A \cap C_E(B)) \cup (B \cap C_E(A))$. By replacing A with $C_E(A)$ and B with $C_E(B)$ in the previous formula

$$C_E(A) \Delta C_E(B) = (\, C_E(A) \backslash C_E(B)) \cup (C_E(B) \backslash C_E(A)\,) =$$
$$C_E(A) \cap C_E(B) \cup C_E(B) \cap C_E(A) =$$
$$(A \cap C_E(B)) \cup (B \cap C_E(A)) = A \Delta B$$

Since $\cap$ and $\cup$ are commutative laws.

6. $(A \times C) \cup (B \times C) = (A \cup B) \times C$.

$$\begin{aligned}(A \times C) \cup (B \times C) &= \{(x,y)/(x,y) \in A \times C \text{ or } (x,y) \in B \times C\} \\ &= \{(x,y) \mid (x \in A \text{ and } y \in C) \text{ or } (x \in B \text{ and } y \in C\} \\ &= \{(x,y) \mid (x \in A \text{ or } x \in B) \text{ and } y \in C\} \\ &= (A \cup B) \times C.\end{aligned}$$

7. $A \subset B \Rightarrow P(A) \subset P(B)$.

According to the definition: $P(A) = \{X \mid X \subset A\}$, we have:

$X \in P(A) \Rightarrow X \subset A$ and since $A \subset B$, we have $X \subset B \Rightarrow x \in P(B)$. Therefore, the inclusion holds.

Exercise 4.

1. $f(A \cap B) \subset f(A) \cap f(B)$.

Let $y \in f(A \cap B)$, which means there exists $x \in A \cap B$ such that $y = f(x)$. Since $x \in A$, we have $y = f(x) \in f(A)$. Similarly, since $x \in B$, we have $y \in f(B)$. Hence, $y \in f(A) \cap f(B)$.

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

2. f is injective $\Leftrightarrow f(A \cap B) = f(A) \cap f(B)$.

$\Leftarrow$ Let's assume that $f(A \cap B) = f(A) \cap f(B)$. We need to prove that f is injective.

Assume that $f(x_1) = f(x_2)$ for some $x_1, x_2 \in E$. Let $A = \{x_1\}$ and $B = \{x_2\}$. We have $f(x_1) = f(x_2) \in f(A) \cap f(B) = f(A \cap B)$, which means $f(A \cap B) \neq \phi$. This implies $A \cap B \neq \phi$, which contradicts the assumption $x_1 = x_2$. Therefore, f is injective.

$\Longrightarrow$ We assume that f is injective. We need to prove that $f(A \cap B) = f(A) \cap f(B)$.

We already proved in part (1) that $f(A \cap B) \subset f(A) \cap f(B)$. Now let's prove the other inclusion. Let $y \in f(A) \cap f(B)$. Then $y \in f(A)$ and $y \in f(B)$.

$$\Rightarrow \exists x \in A | y = f(x) \quad \wedge \quad \exists \bar{x} \in B | y = f(x') .$$

Since $f(x) = f(x')$ and f is injective, we have $x = \bar{x}$.

$$\Rightarrow x \in A \cap B \Rightarrow f(x) \in f(A \cap B) \Rightarrow y \in f(A \cap B).$$

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

3. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$

$$\begin{aligned} f^{-1}(C \cap D) &= \{x; f(x) \in C \cap D\} \\ &= \{x; f(x) \in C \wedge f(x) \in D\} \\ &= \{(x; f(x) \in C) \text{ and } (x; f(x) \in D)\} \\ &= f^{-1}(C) \cap f^{-1}(D). \end{aligned}$$

4. If $f(x) \in f(f^{-1}(C))$, then $x \in C$

Therefore, $f(f^{-1}(C)) \subset C$.

5. f is surjective $\Leftrightarrow f(f^{-1}(C)) = C$.

$\Longrightarrow$ We need to prove that for every $y \in F$, there exists $x \in E$ such that $y = f(x)$.

For every $y \in F$, we have $y \in \{y\}$ and according to the hypothesis, we can write $\{y\} = f(f^{-1}(\{y\}))$.

Therefore, there exists an element $x \in E$ with $x \in f^{-1}(\{y\}) \Rightarrow f(x) \in \{y\} \Rightarrow f(x) = y$.

$\Longleftarrow$ We have $f(f^{-1}(C)) \subset C$ according to (4). Now we need to prove that $C \subset f(f^{-1}(C))$.

Let $y \in C$, which means $y \in F$. Since f is surjective, there exists $x \in E$ such that $y = f(x)$.

$$\Rightarrow \exists x \in E | y = f(x) \wedge \exists \bar{x} \in B | y = f(x') .$$

$$\Rightarrow f(x) = f(x') \quad \text{and since } f \text{ is injective} \quad x = \bar{x}$$

$$\Rightarrow x \in f^{-1}(C) \Rightarrow f(x) \in f\left(f^{-1}(C)\right)$$

Therefore, $y \in f\left(f^{-1}(C)\right)$. Hence, $f\left(f^{-1}(C)\right) \supset C$.

(6) $f^{-1}\left(C_F(C)\right) = C_E f^{-1}(C)$.

$$x \in f^{-1}\left(C_F(C)\right) \Leftrightarrow f(x) \in C_E(C) \Leftrightarrow f(x) \notin C \Leftrightarrow x \notin f^{-1}(C)$$

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

(7) $f^{-1}(C \triangle D) = f^{-1}(C) \Delta f^{-1}(D)$.

$$\begin{aligned} f^{-1}(C \triangle D) &= f^{-1}((C \backslash D) \cup (D \backslash C)) = f^{-1}(C \backslash D) \cup \hat{f}^{-1}(D \backslash C) \\ &= f^{-1}(C \cap C_F(D)) \cup f^{-1}(D \cap C_F(C)) \\ &= \left(f^{-1}(C) \cap f^{-1}(C_F(D))\right) \cup \left(f^{-1}(D) \cap f^{-1}(C_F(C))\right). \\ &= \left(f^{-1}(C) \cap C_E f^{-1}(D)\right) \cup \left(f^{-1}(D) \cap C_E f^{-1}(C)\right). \\ &= \left(f^{-1}(C) \backslash f^{-1}(D)\right) \cup \left(f^{-1}(D) \backslash f^{-1}(C)\right) \\ &= f^{-1}(C) \Delta f^{-1}(D). \end{aligned}$$

Exercise 5.

1. f is not injective because $f(2) = f(1/2) = \frac{4}{5}$ but $2 \neq \frac{1}{2}$.

f is not surjective because the value "2" does not have a preimage.

To show this, we can solve the equation $f(x) = 2$ which leads to $x^2 - x + 1 = 0$ and this equation has no real solutions.

2. We know that $f(\mathbb{R}) = [-1, 1]$ if the equation $f(x) = y$ has a unique solution x for every $y \in [-1, 1]$.

$$f(x) = y \Rightarrow yx^2 - 2x + y = 0 \ldots\ldots (*)$$

$$\Delta = 1 - y^2$$

$(*)$ has a solution if and only if $\Delta \geq 0$, so there are solutions if and only if $y \in [-1, 1]$.

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

3. g is bijective if and only if g is injective and surjective.

$\Longrightarrow$ We assume that g is bijective. We need to prove that for every $y \in [-1,1]$, the equation $g(x) = y$ has a unique solution.

So for every $y \in [-1,1]$, there exists a unique $x \in [-1,1]$ such that $g(x) = y$.

Let's find the solution to $g(x) = x$:

$$\begin{cases} x = \frac{1-\sqrt{1-y^2}}{y}, & \in [-1,1] \\ x = \frac{1+\sqrt{1-y^2}}{y}, & \notin [-1,1] \end{cases}$$

We can see that $\frac{1+\sqrt{1-y^2}}{y} \notin [-1,1]$, so the only solution is $x = \frac{1-\sqrt{1-y^2}}{y}$. Therefore, g is bijective.

$$\begin{aligned} g^{-1} : [-1,1] &\longrightarrow [-1,4] \\ y &\longmapsto g^{-1}(y) = \frac{1-\sqrt{1-y^2}}{y} \end{aligned}$$

Chapter 3

Binary Relations on a Set

3.1 Basic Definitions

Definition 3.1 (Binary Relation) Let E be a set. A binary relation $\mathcal{R}$ on E is a property that applies to pairs of elements from E. We denote $x\mathcal{R}y$ to indicate that the property is true for the pair $(x, y) \in E \times E$.

Example

1. The inequality $\leq$ is a relation on $\mathbb{N}, \mathbb{Z}$, and $\mathbb{R}$.
2. The inclusion relation in the power set of E: $A\mathcal{R}B \Leftrightarrow A \subset B$.
3. The divisibility relation on the integers: $m\mathcal{R}n \Leftrightarrow m$ divides n.

Definition 3.2 Let $\mathcal{R}$ be a relation on a set E.

1. $\mathcal{R}$ is reflexive if for every $x \in E$, $x\mathcal{R}x$ holds.
2. $\mathcal{R}$ is symmetric if for all $x, y \in E$, $x\mathcal{R}y \Rightarrow y\mathcal{R}x$.
3. $\mathcal{R}$ is antisymmetric if for all $x, y \in E$, $(x\mathcal{R}y \wedge y\mathcal{R}x) \Rightarrow x = y$.
4. $\mathcal{R}$ is transitive if for all $x, y, z \in E$, $(x\mathcal{R}y \wedge y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.

3.2 Equivalence Relations

Definition 3.3 (Equivalence Relation) A binary relation $\mathcal{R}$ on E is an equivalence relation if and only if it is reflexive, symmetric, and transitive.

Example 1 The relation $\mathcal{R}$ of "being parallel" is an equivalence relation for the set E of affine lines in the plane:

1. Reflexivity: A line is parallel to itself.
2. Symmetry: If line D is parallel to D', then D' is parallel to D.
3. Transitivity: If line D is parallel to D' and D' is parallel to D'', then D is parallel to D''.

Example 2 Consider the following relation on $\mathbb{Z}$:

$$x\mathcal{R}y \Leftrightarrow \exists k \in \mathbb{Z} \mid x - y = 2k$$

1. $\mathcal{R}$ is reflexive because $\exists k = 0 \mid x - x = 2k = 0$, thus $x\mathcal{R}x$.
2. Suppose $x\mathcal{R}y$, then $\exists k \in \mathbb{Z} \mid x - y = 2k \Rightarrow y - x = 2k'$ with $k' = -k \in \mathbb{Z}$. Therefore, $y\mathcal{R}x$. Hence, $\mathcal{R}$ is symmetric.
3. Suppose $x\mathcal{R}y$ and $y\mathcal{R}z$. Then, $(\exists k \in \mathbb{Z} \mid x - y = 2k)$ and $(\exists k' \in \mathbb{Z} \mid y - z = 2k')$ by adding these equations, we obtain $x - z = 2k''$ with $k'' = (k + k') \in \mathbb{Z}$. Thus, $x\mathcal{R}z$. Therefore, $\mathcal{R}$ is transitive. Consequently, $\mathcal{R}$ is an equivalence relation.

Definition 3.4 Let $\mathcal{R}$ be an equivalence relation on a set E. The equivalence class of an element $x \in E$ is the set of elements in E that are related to x by $\mathcal{R}$, denoted by $\mathcal{C}(x)$ or $\bar{x}$:

$$\bar{x} = \{y \in E \mid y\mathcal{R}x\}$$

Definition 3.5 Let $\mathcal{R}$ be an equivalence relation on a set E. The quotient set of E by $\mathcal{R}$ is the set of equivalence classes of $\mathcal{R}$, denoted by $E/\mathcal{R}$:

$$E/\mathcal{R} = \{\bar{x} \mid x \in E\}$$

Example In the previous example, we have

$$\begin{aligned}\bar{x} &= \{y \in E \mid y\mathcal{R}x\} \\ &= \{y \in E \mid x - y = 2k\} \\ &= \{x - 2k : k \in \mathbb{Z}\} \\ &= \{\ldots, x-4, x-2, x, x+2, x+4, \ldots\}.\end{aligned}$$

$\overline{0} = \{y \in E \mid 0\mathcal{R}y\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$, $\overline{1} = \{y \in E \mid 1\mathcal{R}y\} = \{\ldots, -3, -1, 1, 3, \ldots\}$

and $\overline{2} = \overline{0}$.**Therefore,**$\mathbb{Z}/\mathcal{R} = \{\bar{x} \mid x \in E\} = \{\overline{0}, \overline{1}\}$

Proposition 3.1 Let $\mathcal{R}$ be an equivalence relation on E. Then

1. An equivalence class is a subset of the set E, i.e., for all $x \in E$, $\bar{x} \subset E$.
2. An equivalence class is never empty, i.e., for all $x \in E$, $\bar{x} \neq \phi$.
3. The intersection of two distinct equivalence classes is empty, i.e., for all $x, y \in E$, $\bar{x} \cap \bar{y} = \phi$.
4. For all $x, y \in E$, $x\mathcal{R}y \Leftrightarrow \bar{x} = \bar{y}$.

Theorem 3.1 Let $\mathcal{R}$ be an equivalence relation on E. The equivalence classes $(\bar{x})_{x \in E}$ form a partition of E:

$$E = \cup_{x \in E} \bar{x}$$

3.3 Order Relation

Definition 3.6 (Order Relation) A binary relation $\mathcal{R}$ on E is an order relation if and only if it is reflexive, antisymmetric, and transitive. We then say that $(E, \mathcal{R})$ is an ordered set.

Example.

1. The inequality $\leq$ is an order relation on $\mathbb{N}, \mathbb{Z}$, and $\mathbb{R}$.
2. The inclusion relation in the power set of E is an order relation: $A\mathcal{R}B \Leftrightarrow A \subset B$.

Definition 3.7 Let $\mathcal{R}$ be an order relation on E. Two elements x and y of E are said to be comparable if $x\mathcal{R}y$ or $y\mathcal{R}x$.

Definition 3.8 (Total Order and Partial Order) Let $\mathcal{R}$ be an order relation on E. If any two elements x and y are always comparable, we say that $\mathcal{R}$ is a total order relation and the set E is called totally ordered. Otherwise (i.e., if there exist at least two non-comparable elements x and y), we say that $\mathcal{R}$ is a partial order relation and the set E is called partially ordered.

Example.

1. $\leq$ is a total order on $\mathbb{N}, \mathbb{Z}$, and $\mathbb{R}$.
2. The divisibility relation in $\mathbb{N}^*$ is a partial order.

Definition 3.9 Let $\mathcal{R}$ be an order relation on E, and let M, m be two elements of E.

1. M is an upper bound of a subset A of E if $x\mathcal{R}M$ for every $x \in A$.
2. m is a lower bound of a subset A of E if $m\mathcal{R}x$ for every $x \in A$.

Example.

1. The set $\{8, 10, 12\}$ is bounded above by 120 and bounded below by 2 for the divisibility relation "/" on $\mathbb{N}$.
2. $\mathcal{P}(E)$ is bounded below by $\emptyset$ and bounded above by E for the inclusion relation $\subset$.

3.4 Exercises with Solutions

Exercise 1. In $\mathbb{R}$, the binary relation $\mathcal{R}$ is defined as follows:

$$\forall x, y \in \mathbb{R} : x\mathcal{R}y \Longleftrightarrow x^2 - 1 = y^2 - 1$$

1. Show that $\mathcal{R}$ is an equivalence relation on $\mathbb{R}$.
2. Determine the quotient set $\mathbb{R}/\mathcal{R}$.

Exercise 2. For every $n \in \mathbb{N}^*$, a binary relation on $\mathbb{Z}$ is defined by

$$\forall x, y \in \mathbb{Z} : x\mathcal{R}y \Longleftrightarrow \exists k \in \mathbb{Z} \mid x - y = kn$$

1. Show that $\mathcal{R}$ is an equivalence relation on $\mathbb{Z}$.

2. Assume that $n = 3$:

(a) Determine the equivalence class of $x \in \mathbb{Z}$. Deduce the classes $\overline{0}, \overline{1}, \overline{2}$.

(b) Show that $\forall m \in \mathbb{Z} : \overline{0} = \overline{3m}, \overline{1} = \overline{3m+1}, \overline{2} = \overline{3m+2}$.

(c) Show that $\overline{0} \cap \overline{1} = \emptyset, \overline{1} \cap \overline{2} = \emptyset, \overline{0} \cap \overline{2} = \emptyset$. Deduce the quotient set $\mathbb{Z}/\mathcal{R}$.

Exercise 3. Let E be a set and let A be a subset of E. A binary relation $\mathcal{R}$ is defined on $\mathcal{P}(E)$ as follows:

$$\forall X, Y \in \mathcal{P}(E) : X\mathcal{R}Y \Longleftrightarrow A \cap X = A \cap Y$$

1. Show that $\mathcal{R}$ is an equivalence relation on $\mathcal{P}(E)$.

2. Determine the equivalence classes of $\emptyset$ and E. Deduce $\bar{A}$ and $\overline{C_E(A)}$.

Exercise 4. Let $\mathcal{R}$ be a binary relation on $\mathbb{R}^3$ defined by

$$(x, y, z)\mathcal{R}(a, b, c) \Longleftrightarrow (|x - a| \leq b - y \text{ and } z = c).$$

1. Show that $\mathcal{R}$ is a partial order relation on $\mathbb{R}^3$.

2. Is the order total on $\mathbb{R}^3$?

Exercise 5. A binary relation $\mathcal{R}$ is defined on $\mathbb{R}^2$ as follows:

$$\forall\, (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2 : (x_1, y_1)\, \mathcal{R}\, (x_2, y_2) \Longleftrightarrow x_1 \leq x_2 \text{ and } y_1 \leq y_2.$$

1. Show that $\mathcal{R}$ is an order relation on $\mathbb{R}^2$.

2. Are the elements $(2, 4), (3, 1)$ of $\mathbb{R}^2$ comparable by $\mathcal{R}$?

3. Is the order total on $\mathbb{R}^2$?

4. Determine the set of upper bounds of $A = \{(1, 2), (3, 1)\} \subset \mathbb{R}^2$.

Exercise 6. Determine whether the following relations $\mathcal{R}$ are order relations:

1. $\forall x, y \in \mathbb{R} : x\mathcal{R}y \iff e^x \leq e^y$;

2. $\forall x, y \in \mathbb{R} : x\mathcal{R}y \iff |x| \leq |y|$;

3. $\forall x, y \in \mathbb{N} : x\mathcal{R}y \iff \exists p, q \geq 1 \mid y = px^q$ (where p and q are integers);

4. $\forall x, y \in \mathbb{N}^* : x\mathcal{R}y \iff \exists m \in \mathbb{N}^* \mid y = mx$;

5. $\forall x, y \in]1, +\infty[: x\mathcal{R}y \iff \frac{x}{1+x^2} \geq \frac{y}{1+y^2}$.

3.4.1 Solution

Exercise 1.

1. $\forall x, y \in \mathbb{R} : x\mathcal{R}y \iff x^2 - 1 = y^2 - 1$

(i) Reflexivity: $\forall x \in \mathbb{R}, x^2 - 1 = x^2 - 1 \Rightarrow xRx$.

(ii) Symmetry: $x\mathcal{R}y \Leftrightarrow x^2 - 1 = y^2 - 1 \Rightarrow y^2 - 1 = x^2 - 1 \Rightarrow y\mathcal{R}x$.

(iii) Transitivity:

$$\begin{cases} x\mathcal{R}y \\ y\mathcal{R}z \end{cases} \Leftrightarrow \begin{cases} x^2 - 1 = y^2 - 1 \\ y^2 - 1 = z^2 - 1 \end{cases} \Rightarrow x^2 - 1 = z^2 - 1 \Rightarrow x\mathcal{R}z.$$

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

2. $\mathbb{R}/\mathbb{R} = \{\bar{x} : x \in \mathbb{R}\}$.

We have $\bar{x} = \{y \in \mathbb{R} \mid y\mathbb{R}x\} = \{y \in \mathbb{R} \mid y^2 - 1 = x^2 - 1\} = \{x, -x \mid x \in \mathbb{R}\}$

Thus, $\mathbb{R}/\mathbb{R} = \{\{x_1 - x\}, x \in \mathbb{R}\}$.

Exercise 2.

1. $\forall x, y \in \mathbb{Z} : x\mathcal{R}y \Leftrightarrow \exists k \in \mathbb{Z} \mid x - y = kn$.

- Reflexivity: We know that $\forall x \in \mathbb{Z} : x - x = 0 = 0 \cdot n$ with $k = 0 \in \mathbb{Z}$, so $x\mathcal{R}x$.
- Symmetry: $x\mathcal{R}y \Leftrightarrow x - y = kn \Rightarrow y - x = (-k) \cdot n = k' \cdot n$ with $k' = -k \in \mathbb{Z}$. Thus, $y\mathcal{R}x$.

- Transitivity:

$$\begin{cases} x\mathcal{R}y \\ y\mathcal{R}z \end{cases} \Leftrightarrow \begin{cases} x-y = k_1 \cdot n/k_1 \in \mathbb{Z} \\ y-z = k_2 \cdot n/k_2 \in \mathbb{Z} \text{ gives:} \end{cases} \text{; Summing both sides:}$$

$$x - z = (k_1 + k_2)n = k_3 \cdot n \text{ with } k_3 = k_1 + k_2 \in \mathbb{Z}$$

Therefore, $x\mathcal{R}z$

2. For $n = 3 : \forall x, y \in \mathbb{Z} : x\mathcal{R}y \Leftrightarrow \exists k \in \mathbb{Z} : x - y = 3k$.

(a) For any

$$\begin{aligned} x \in \mathbb{Z} : \bar{x} &= \{y \in \mathbb{Z} : y\mathcal{R}x\} = \{y \in \mathbb{Z} : y = x + 3k\} \\ &= \{x + 3k \mid k \in \mathbb{Z}\}. \end{aligned}$$

In particular:

$$\bar{0} = \{y \in \mathbb{Z} : y\mathcal{R}0\} = \{3k \mid k \in \mathbb{Z}\} = 3\mathbb{Z}$$

$$\bar{1} = \{y \in \mathbb{Z} : y\mathcal{R}1\} = \{3k+1 \mid k \in \mathbb{Z}\} = 3\mathbb{Z}+1$$

$$\bar{2} = \{y \in \mathbb{Z} : y\mathcal{R}2\} = \{3k+2 \mid k \in \mathbb{Z}\} = 3\mathbb{Z}+2.$$

(b)

For all $m \in \mathbb{Z}$:

$$\begin{cases} \bar{0} = 3\bar{m} \\ \bar{1} = 3\bar{m} + 1 \\ \bar{2} = 3\bar{m} + 2 \end{cases} \quad \text{because} \quad \forall m \in \mathbb{Z} : \begin{cases} 0\mathcal{R}(3m) \\ 1\mathcal{R}(3m+1) \\ 2\mathcal{R}(3m+2) \end{cases} .$$

Indeed, for all $m \in \mathbb{Z}$:

$$\begin{cases} 0 - (3m) = 3(-m) \\ 1 - (3m+1) = 3(-m) \\ 2 - (3m+2) = 3(-m) \end{cases} , \quad -m \in \mathbb{Z} .$$

(C)

We have:

$$\begin{cases} \bar{0} \cap \bar{1} = \emptyset \\ \bar{1} \cap \bar{2} = \emptyset \\ \bar{0} \cap \bar{2} = \emptyset \end{cases} \text{, because } \begin{cases} 0 \not\mathcal{R} 1 \\ 1 \not\mathcal{R} 2 \\ 0 \not\mathcal{R} 2 \end{cases} \text{ .Indeed, } \begin{cases} 0 - 1 = -1 \neq 3k_1 \\ 1 - 2 = -1 \neq 3k_2 \\ 0 - 2 = -2 \neq 3k_3 \end{cases} , \quad k_1, k_2, k_3 \in \mathbb{Z} \, .$$

We know that:

$$\begin{aligned} \mathbb{Z}/R &= \{\bar{x} : x \in \mathbb{Z}\} \\ &= \{\bar{x} : x = 3m\} \cup \{\bar{x} : x = 3m + 1\} \cup \{\bar{x} : x = 3x + 2\}. \\ &= \{\bar{0}, \bar{1}, \bar{2}\}. \end{aligned}$$

Exercise 4. $(x, y, z)R(a, b, c) \Leftrightarrow (|x - a| \leqslant b - y \text{ and } z = c)$

(1)

(i) Reflexivity: $(x, y, z)R(x, y, z) \Leftrightarrow (|x - x| = 0 \leqslant y - y = 0 \text{ and } z = z)$, hence R is reflexive.

(ii) Anti-symmetry: Suppose $(v, y, z)R(a, b, c)$ and $(a, b, c)R(x, y, z)$

This implies $[(|x - a| \leqslant b - y \quad (*) \text{ and } |a - x| \leqslant y - b \quad (**)) \text{ and } z = c]$

Then, $(*) + (**)$ gives: $x = a$, replacing $x = a$ in $(*)$ and $(**)$ we find $y = b$. Thus, $(x, y, z) = (a, b, c)$. Therefore, R is anti-symmetric.

(iii) Transitivity: Suppose $(v, y, z)R(a, b, c)$ and $(a, b, c)R(\alpha, \beta, \gamma)$

This implies $[(|x - a| \leqslant b - y \ (*) \text{ and } |a - \alpha| \leqslant \beta - b \ (**)) \text{ and } z = c = \gamma]$

Thus, $(*) + (**)$ gives $(|x - a| + |a - \alpha| \leqslant b - y + \beta - b \text{ and } z = c = \gamma)$.

And since $(|x - \alpha| = |x - a + a - \alpha| \leqslant |x - a| + |a - \alpha| \leqslant y + \beta \text{ and } z = \gamma)$ implies $(x, y, z)R(\alpha, \beta, \gamma)$. Hence, R is transitive.

Therefore, R is a partial order relation on $\mathbb{R}^3$.

(2) R is not total because $\exists (x, y, z) = (0, 0, 2) \in \mathbb{R}^3$ and $(a, b, c) = (0, 0, 3) \in \mathbb{R}^3$ such that $(0, 0, 2) \not\mathcal{R} (0, 0, 3)$ and $(0, 0, 3) \not\mathcal{R} (0, 0, 2)$.

Exercise 5. $\forall \, (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2 : x_1 \leqslant x_2 \text{ and } y_1 \leqslant y_2$.

(1)

(i) Reflexivity: We know that

$$\forall (x,y) \in \mathbb{R}^2 : \begin{cases} x \leqslant x \\ y \leqslant y \end{cases} \Rightarrow (x,y)R(x,y) \Rightarrow R \text{ is reflexive.}$$

(ii) Anti-symmetry: Suppose $(x_1, y_1)\, R\, (x_2, y_2)$ and $(x_1, y_2)\, R\, (x_1, y_1)$

$$\Rightarrow \begin{cases} x_1 \leqslant x_2 \wedge y_1 \leqslant y_2 \\ \wedge \\ x_2 \leqslant x_1 \wedge y_2 \leqslant y_1 \end{cases} \Rightarrow \begin{cases} x_1 = x_2 \\ \wedge \\ y_1 = y_2 \end{cases} \Rightarrow (x_1, y_1) = (x_2, y_2)\ .$$ Thus, R is anti-symmetric.

(iii) Transitivity: Let $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R}^2$

$$\begin{cases} (x_1, y_1)\, R\, (x_2, y_2) \\ \wedge \\ (x_2, y_2)\, R\, (x_3, y_3) \end{cases} \Rightarrow \begin{cases} x_1 \leqslant x_2 \wedge y_1 \leqslant y_2 \\ \wedge \\ x_2 \leqslant x_3 \wedge y_2 \leqslant y_3 \end{cases} \Rightarrow \begin{cases} x_1 \leqslant x_3 \\ \wedge \\ y_1 \leqslant y_3 \end{cases} \Rightarrow (x_1, y_1)\, R\, (x_3, y_3)$$

Therefore, R is transitive. Hence, R is a partial order relation on $\mathbb{R}^2$.

(2) $(2,4)$ and $(3,1)$ are not comparable because $(1,4)$ and $(3,1)$ do not satisfy the relation. In fact, $\begin{cases} 2 \leqslant 3 \\ \wedge \\ 4 \not\leqslant 1 \end{cases}$ and $\begin{cases} 3 \not\leqslant 2 \\ \wedge \\ 1 \leqslant 2 \end{cases} \Rightarrow \begin{cases} (2,4) \not R (3,1) \\ \wedge \\ (3,1) \not R (2,4) \end{cases}$

(3) The order is partial because $\exists a = (2,4)$ and $b = (3,1)$ where $a \not R b$ and $b \not R a$.

(4) $t = (x, y) \in \mathbb{R}^2$ is an upper bound of A if $\forall a \in A : aRt$.

$$\Rightarrow \begin{cases} (1,2)R(x,y) \\ \wedge \\ (3,1)R(x,y) \end{cases} \Rightarrow \begin{cases} 1 \leqslant x \wedge 2 \leqslant y. \\ \wedge \\ 3 \leqslant x \wedge 1 \leqslant y. \end{cases} \Rightarrow \begin{cases} x \geqslant 3 \\ \wedge \\ y \geqslant 2 \end{cases}$$

$$\Rightarrow \underset{\mathbb{R}^2}{\text{Maj}}(A) = \{(x,y) : x \geqslant 3 \wedge y \geqslant 2\}.$$

Chapter 4

Algebraic Structures

4.1 Internal Composition Laws and Their Properties

4.1.1 Internal Composition Laws

Definition 4.1 Let E be a set. An internal composition law $*$ on E is a mapping from $E \times E$ to E:

$$\begin{aligned} * : E \times E &\longrightarrow E \\ (x, y) &\mapsto x * y \end{aligned}$$

Notations

1. Instead of "internal composition law," we also say "operation of internal composition" or simply "internal operation."
2. $(E, *)$ is often used to denote a set E equipped with an internal operation $*$.

Example.

1. The laws $\cup$ (union), $\cap$ (intersection), and $\triangle$ (symmetric difference) on $\mathcal{P}(E)$ (the power set of E).
2. The law (composition) on $\mathcal{F}(E)$ (the set of functions from E to E).

3. The laws + and × on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$.

4. Let * be defined on $\mathbb{R}$ by $x * y = \frac{1}{x+y}$. Then * is not an internal operation since $(-1, 1)$ does not have an image.

Definition 4.2 (Stable Subset for an Operation) Let E be a set equipped with an internal composition law * and F be a subset of E. We say that F is stable under the law * if

$$\forall (x, y) \in F \times F : x * y \in F$$

Example.

1. $\mathbb{R}^+$ and $\mathbb{R}^-$ are two stable subsets of $\mathbb{R}$ under the operation +.

2. For the operation ×, $\mathbb{R}^+$ is still a stable subset, but $\mathbb{R}^-$ is not.

4.1.2 Properties of internal composition laws

Definition 4.3 (Commutativity and Associativity) Let E be a set equipped with an internal composition law $*$.

We say that $*$ is commutative if $\forall (x, y) \in E^2 : x * y = y * x$.

We say that $*$ is associative if $\forall (x, y, z) \in E^3 : (x * y) * z = x * (y * z)$.

Example.

1. The addition and multiplication laws on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are commutative and associative.

2. Also, the union ($\cup$), intersection ($\cap$), and symmetric difference ($\triangle$) laws on $\mathcal{P}(E)$ are commutative and associative.

3. The composition law ($\circ$) on $\mathcal{F}(E)$ is associative but not commutative, because $f \circ g \neq g \circ f$ in general.

4. Let $*$ be the law defined on $\mathbb{Q}$ by: $x * y = \frac{x+y}{2}$. Then $*$ is commutative,

   because $x * y = \frac{x+y}{2} = \frac{y+x}{2} = y * x$, but it is not associative,

because $(-1 * 0) * 1 = \frac{1}{4} \neq -1 * (0 * 1) = \frac{-1}{4}$.

Definition 4.4 (Neutral Element) Let E be a set equipped with an internal composition law *. Let e be an element of E. We say that e is the neutral element for the law *, if

$$\forall x \in E : x * e = e * x = x$$

Remark 4.1 If the law $*$ is commutative, the equality $x * e = e * x$ is automatically satisfied.

Example.

1. In $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$, 0 is neutral for the addition law, and 1 is neutral for the multiplication law.
2. In $\mathcal{P}(E)$, the empty set ($\emptyset$) is neutral for the union law ($\cup$), and E is neutral for the intersection law ($\cap$).
3. Let $*$ be the law defined on $\mathbb{R}$ by: $x * y = x + y - 1$. Then $e = 1$ is a neutral element, because $x * e = x \Rightarrow x + e - 1 = x$. Thus, $e = 1$.

Proposition 4.1 (Uniqueness of the Neutral Element) The neutral element of E for the law * if it exists, is unique.

Proof. Indeed, let e' be another neutral element for $*$, then $e' = e' * e = e * e' = e$. Thus, the neutral element is unique.

Definition 4.5 (Inverse Element) Let E be a set equipped with an internal composition law * and let e be a neutral element. We say that the element x of E has an inverse element x' of E, if $\forall x \in E : x * x' = x' * x = e$.

Example.

1. In $\mathbb{R}$, the invertible elements for the multiplication law ($\times$) are the non-zero elements.
2. Let $*$ be the law defined on $\mathbb{R}$ by: $x * y = x + y - 1$. Then $x \in \mathbb{R}$ has an inverse element $x' = 2 - x$, because $x * x' = 1 \Rightarrow x + x' - 1 = 1$. Thus, $x' = 2 - x$.

4.1.3 Properties of internal composition laws

Definition 4.3 (Commutativity and Associativity) Let E be a set equipped with an internal composition law $*$.

We say that $*$ is commutative if $\forall (x, y) \in E^2 : x * y = y * x$.

We say that $*$ is associative if $\forall (x, y, z) \in E^3 : (x * y) * z = x * (y * z)$.

Example.

1. The addition and multiplication laws on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are commutative and associative.
2. The union ($\cup$), intersection ($\cap$), and symmetric difference ($\triangle$) laws on $\mathcal{P}(E)$ are commutative and associative.
3. The composition law ($\circ$) on $\mathcal{F}(E)$ is associative but not commutative, because $f \circ g \neq g \circ f$ in general.
4. Let $*$ be the law defined on $\mathbb{Q}$ by: $x * y = \frac{x+y}{2}$. Then $*$ is commutative, because $x * y = \frac{x+y}{2} = \frac{y+x}{2} = y * x$, but it is not associative, because $(-1 * 0) * 1 = \frac{1}{4} \neq -1 * (0 * 1) = \frac{-1}{4}$.

Definition 4.4 (Neutral Element) Let E be a set equipped with an internal composition law $*$. Let e be an element of E. We say that e is the neutral element for the law $*$ if $\forall x \in E : x * e = e * x = x$.

Remark 4.1 If the law $*$ is commutative, the equality $x * e = e * x$ is automatically satisfied.

Example.

1. In $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, 0 is the neutral element for the addition law, and 1 is the neutral element for the multiplication law.
2. In $\mathcal{P}(E)$, the empty set $\emptyset$ is the neutral element for the union law $\cup$, and E is the neutral element for the intersection law $\cap$.

3. Let $*$ be the law defined on $\mathbb{R}$ by: $x * y = x + y - 1$. Then $e = 1$ is a neutral element, because $x * e = x + e - 1 = x$. Thus, $e = 1$.

Proposition 4.1 (Uniqueness of the Neutral Element) The neutral element of E for the law $*$, if it exists, is unique.

Proof. Indeed, let e' be another neutral element for $*$, then $e' = e' * e = e * e' = e$. Thus, the neutral element is unique.

Definition 4.5 (Inverse Element) Let E be a set equipped with an internal composition law $*$ and let e be a neutral element. We say that the element x of E has an inverse element x' of E if $\forall x \in E : x * x' = x' * x = e$.

Example.

1. In $\mathbb{R}$, the invertible elements for the multiplication law are the non-zero elements.

2. Let $*$ be the law defined on $\mathbb{R}$ by: $x * y = x + y - 1$. Then each $x \in \mathbb{R}$ has an inverse element $x' = 2 - x$, because $x * x' = x + x' - 1 = 1$. Thus, $x' = 2 - x$.

Proposition 4.2 Let E be a set equipped with an associative internal composition law $*$ that has a neutral element.

1. The inverse element x' of x for the law $*$ in E, if it exists, is unique.

2. If $x, y \in E$ are invertible, then $x * y$ is invertible, and its inverse is given by

$$(x * y)' = y' * x'$$

Definition 4.6 (Distributivity) Let E be a set equipped with two internal composition laws $*$ and $\top$.

We say that $*$ is left distributive with respect to $\top$ if

$$\forall (x, y, z) \in E^3 : x * (y \top z) = (x * y) \top (x * z).$$

We say that $*$ is right distributive with respect to $\top$ if

$$\forall (x, y, z) \in E^3 : (x \top y) * z = (x * z) \top (y * z).$$

Remark 4.2 If the law $*$ is commutative, then one of these properties implies the other.

Example

1. In $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, the multiplication law $\times$ is left distributive with respect to the addition law $+$.
2. In $\mathcal{P}(E)$, the laws $\cup$ and $\cap$ are left distributive with respect to each other.
3. Let $*$ be the law defined on $\mathbb{R}$ by $x * y = x + y - xy$, and let $\top$ be the law defined on $\mathbb{R}$ by $x \top y = x + y - 1$. Since the law $*$ is commutative, it suffices to demonstrate left distributivity with respect to $\top$:

$$\begin{aligned} x * (y \top z) &= x * (x + y - 1) \\ &= 2x + y + z - xy - xz - 1 \quad \ldots\ldots \quad (1) \\ (x * y) \top (x * z) &= (x + y - xy) \top (x + z - xz) \\ &= 2x + y + z - xy - xz - 1 \quad \ldots\ldots \quad (2) \end{aligned}$$

$(1) = (2)$ So the law $*$ is left distributive with respect to the law $\top$.

4.2 Algebraic Structures

4.2.1 Groups

4.2.1.1 Definitions and Examples

Definition 4.7 (Group) A group is a non-empty set equipped with an internal composition law $(G, *)$ such that:

- $*$ is associative;
- $*$ has a neutral element e;
- every element in G is invertible (has an inverse) for $*$.

Remark 4.3 If $*$ is commutative, we say that $(G, *)$ is commutative or abelian.

Example

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are abelian groups;
2. The set $\mathcal{P}(E)$ equipped with the symmetric difference $\triangle$ is an abelian group;
3. $(\mathbb{N}, +)$, $(\mathbb{R}, \times)$, $(\mathcal{P}(E), \cap)$, and $(\mathcal{P}(E), \cup)$ are not groups.

Definition 4.8 (Subgroup) Let $(G, *)$ be a group and let H be a non-empty subset of G. We say that H is a subgroup of G if:

1. H is closed under $*$, i.e., for every $(x, y) \in H^2$, $x * y \in H$;
2. H is closed under taking inverses, i.e., for every $x \in H$, x' (the inverse of x) is also in H.

Example

1. Let $(G, *)$ be a group, then e_G and G are subgroups (called trivial subgroups);
2. Let $(\mathbb{Z}, +)$ be a group. Then $3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, defined by

$$3\mathbb{Z} = \{3z : z \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

3. Let $(G, \cdot)$ be a group. Then the set $Z(G) = \{x \in G : \forall y \in G, xy = yx\}$ is a subgroup of G called the center of G.

Theorem 4.1 (Characterization of Subgroups) Let $(G, *)$ be a group and let H be a non-empty subset of G. Then H is a subgroup of G if and only if

$$\forall (x, y) \in H^2, x * y' \in H$$

Proposition 4.3 (Intersection of Subgroups) Let $(G, *)$ be a group and let $\{H_i\}_{i \in I}$ be a family of subgroups of G. Then $\cap_{i \in I} H_i$ is a subgroup of G.

Remark 4.4 The union of two subgroups of G is not necessarily a subgroup of G. For example, $2\mathbb{Z}$ and $3\mathbb{Z}$ are two subgroups of $(\mathbb{Z}, +)$, but their union is not a subgroup since 2 and 3 are in $2\mathbb{Z} \cup 3\mathbb{Z}$ while $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

4.2.1.2 Group Homomorphisms

Definition 4.9 Let $(G_1, *)$ and $(G_2, \perp)$ be two groups. A group homomorphism (or simply morphism) from G_1 to G_2 is a function $f : G_1 \longrightarrow G_2$ such that for all $x, y \in G_1$,

$$f(x * y) = f(x) \perp f(y)$$

Example

Let f be defined as $\begin{array}{rccl} f: & \mathbb{R} & \longrightarrow & \mathbb{R}^* \\ & x & \mapsto & f(x) = 2^x \end{array}$. Then f is a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^*, \times)$ because

$$\forall x, y \in \mathbb{R}, f(x + y) = 2^{x+y} = 2^x \times 2^y = f(x) \times f(y)$$

Remark 4.5 Let $(G_1, *)$ and $(G_2, \perp)$ be two groups and f be a homomorphism from G_1 to G_2. Then:

1. If f is bijective, then we say that f is an isomorphism;

2. If f is defined from $(G_1, *)$ to itself, then we say that f is an endomorphism;

3. If f is a bijective endomorphism, then we say that f is an automorphism.

Example

1. The exponential function is an isomorphism from the group $(\mathbb{R}, +)$ to $(\mathbb{R}_+^*, \times)$;

2. The natural logarithm function is an isomorphism from the group $(\mathbb{R}_+^*, \times)$ to $(\mathbb{R}, +)$.

Proposition 4.4 Let $(G_1, *)$ and $(G_2, \perp)$ be two groups with neutral elements e_1 and e_2, respectively, and let f be a homomorphism from G_1 to G_2. Then:

1. $f(e_1) = e_2$;

2. For all $x \in G_1$, $(f(x))' = f(x')$.

Proposition 4.5 Let $(G_1, *)$ and $(G_2, \perp)$ be two groups with neutral elements e_1 and e_2, respectively, and let f be a homomorphism from G_1 to G_2. Then:

1. If H is a subgroup of G_1, then $f(H)$ is a subgroup of G_2;

2. If H' is a subgroup of G_2, then $f^{-1}(H)$ is a subgroup of G_1.

Definition 4.10 (Kernel and Image of a Homomorphism) Let $(G_1, *)$ and $(G_2, \perp)$ be two groups, and let f be a homomorphism from G_1 to G_2. Then:

1. The kernel of f is defined as

$$\mathrm{Ker}(f) = f^{-1}(e) = \{x \in G_1 : f(x) = e_2\}$$

2. The image of f is defined as

$$\mathrm{Im}(f) = f(G_1) = \{f(x) \in G_2 : x \in G_1\}$$

Example Let f be the homomorphism given in Example 4.9. Then

$$\mathrm{Ker}(f) = \{x \in \mathbb{R} : f(x) = 1\} = \{x \in \mathbb{R} : 2^x = 1\} = \{0\}$$

and $\mathrm{Im}(f) = \{f(x) : x \in \mathbb{R}\}$. We have $f(x) = y$, which implies $2^x = y$, and this implies $x \ln 2 = \ln y$, so $x = \frac{\ln y}{\ln 2}$. Hence, $\mathrm{Im}(f) = \mathbb{R}_+^*$.

Theorem 4.2 Let f be a homomorphism from $(G_1, *)$ to $(G_2, \perp)$. Then:

1. $\mathrm{Ker}(f)$ is a subgroup of G_1;

2. $\mathrm{Im}(f)$ is a subgroup of G_2;

3. f is injective if and only if $\mathrm{Ker}(f) = \{e_1\}$;

4. f is surjective if and only if $\mathrm{Im}(f) = G_2$.

4.2.1.3 Rings

Definition 4.11 (Ring) Let A be a set equipped with two binary operations, $*$ and $\perp$. $(A, *, \perp)$ is called a ring if:

1. $(A, *)$ is a commutative group;

2. $\perp$ is associative;

3. $\perp$ is distributive over $*$.

Remark 4.6

1. If $\perp$ is commutative, then $(A, *, \perp)$ is called a commutative ring.

2. If $\perp$ has a neutral element, then $(A, *, \perp)$ is called a unitary ring.

Example

1. $(\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are commutative rings;

2. Let E be a set, $(\mathcal{P}(E), \triangle, \cap)$ is a commutative ring;

3. Let A be the set of functions from $\mathbb{C}$ to $\mathbb{C}$ of the form $z \mapsto \alpha z + \beta \bar{z}$. $(A, +, \circ)$ is a non-commutative ring.

Definition 4.12 (Subring) Let $(A, +, \cdot)$ be a ring and B be a subset of A. B is called a subring of $(A, +, \cdot)$ if and only if:

1. $B \neq \emptyset$ $(0_A \in B)$;

2. $(B, +)$ is a subgroup of A;

3. B is closed under $\cdot$.

Alternatively,

1. $0_A \in B$

2. For all $a, b \in B$, $a - b \in B$;

3. For all $a, b \in B$, $a \cdot b \in B$.

Example

1. $(\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are all subrings of each other;

2. The set $\left\{r + s\sqrt{2} : (r, s) \in \mathbb{Q}^2\right\}$ is a subring of $(\mathbb{R}, +, \times)$.

Definition 4.13 (Ring Homomorphism) Let $(A, +, \cdot)$ and $(B, +, \cdot)$ be two rings. A function f from A to B is called a homomorphism if:

1. $f(1_A) = 1_B$
2. For all $a, b \in A$, $f(a+b) = f(a) + f(b)$;
3. For all $a, b \in A$, $f(a \cdot b) = f(a) \cdot f(b)$.

Remark 4.7 In particular, f is a group homomorphism from $(A, +)$ to $(A, +)$.

Definition 4.14 (Invertible Element) An element of a ring $(A, +, \cdot)$ is called invertible if it has a symmetrical element for the second operation (if it has an inverse for the operation).

Definition 4.15 (Zero Divisor) A non-zero element x of a ring A is a zero divisor if its product with another non-zero element equals zero:

$$\exists y \neq 0 \mid xy = 0 \quad \text{or} \quad yx = 0.$$

Example

1. In $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$, all non-zero elements are invertible;
2. In the set of functions from $\mathbb{R}$ to $\mathbb{R}$, any function f that vanishes is a zero divisor, and the invertible elements are the functions that do not vanish.

4.2.1.4 Ideal in a Ring

Definition 4.16 (Ideal) Let $(A, +, \cdot)$ be a ring. A non-empty subset I of A is called an ideal of A if and only if:

1. I is a subgroup of $(A, +, \cdot)$;
2. For $x \in I$ and $a \in A$, $x \cdot a \in I$ and $a \cdot x \in I$.

Example The set $\mathbb{Z}$ is not an ideal of $(\mathbb{R}, +, \times)$ because $\frac{1}{5} \in \mathbb{R}$ and $3 \in \mathbb{Z}$ while $\frac{3}{5} \notin \mathbb{Z}$.

Remark 4.8 It is easy to verify that:

1. The intersection of ideals of A is an ideal of A.
2. The image of an ideal under a surjective ring homomorphism is an ideal.
3. The kernel of a ring homomorphism is an ideal.

4.2.1.5 Rules of Calculation in a Ring

Let us recall the binomial theorem, which extends from $\mathbb{Z}$ to commutative rings, but also to arbitrary rings.

Proposition 4.6 Let $(A, +, \cdot)$ be a ring, $a, b \in A$ with $a \cdot b = b \cdot a$, and $n \in \mathbb{N}^*$. Then:

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}.$$

Proof By induction on $\mathbb{N}$ and using the Pascal's triangle.

Remark 4.9 Let $x, y \in A$ and $n \in \mathbb{N}^*$, then $x - y \mid x^n - y^n$ and more precisely:

$$x^n - y^n = (x-y) \sum_{k=0}^{n-1} x^k y^{n-1-k}.$$

* A particular case of the above: if $1 - x$ is invertible, we can calculate $\sum_{k=0}^{n-1} x^k$ using the formula:

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

4.2.2 Fields

Definition 4.17 (Field) A field is a commutative ring in which every non-zero element is invertible for the second operation.

Remark 4.10 If the second operation is also commutative, the field $(K, +, \cdot)$ is called a commutative field.

Example

$\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are fields, but $\mathbb{Z}$ is not (2 is not invertible).

Definition 4.18 (Subfield) Let $(K, +, \cdot)$ be a field, a subfield of K is a subset K_1 of K such that $(K_1, +, \cdot)$ is a field, i.e., for all x, y in K_1, we have $x - y \in K_1$ and $xy^{-1} \in K_1$.

Example

1. $(\mathbb{Q}, +, \times), (\mathbb{R}, +, \times)$, and $(\mathbb{C}, +, \times)$ are all subfields of each other;

2. The set $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a commutative field that contains $\mathbb{Q}$ as a subfield.

4.3 Solved Exercises

Exercise 1. We define on $\mathbb{R}$ an internal composition law $*$ as follows:

$$\forall a, b \in \mathbb{R} : a * b = \ln\left(e^a + e^b\right)$$

1. Is the law $*$ commutative? Associative? Does it have a neutral element?

2. Let $a, b \in \mathbb{R}$. We define an internal composition law $\perp$ on $\mathbb{R}$ as follows:

$$\forall x, y \in \mathbb{R} : x \perp y = ax + by$$

Determine a, b such that the law $\perp$ is: (1) associative, (2) has a neutral element.

Exercise 2. Let $G = \mathbb{R}^* \times \mathbb{R}$ and $*$ be the internal composition law defined on G as follows:

$$\forall (x, y), (x', y') \in G : (x, y) * (x', y') = (xx', xy' + y)$$

1. Show that $(G, *)$ is a non-commutative group.

2. Show that the set $H = \mathbb{R}_+^* \times \mathbb{R}$ is a subgroup of $(G, *)$.

Exercise 3. Let $\left(\mathbb{R}_+^*, \times\right)$ and $(\mathbb{R}, +)$ be two groups, and let $f : \mathbb{R}_+^* \longrightarrow \mathbb{R}$ be the function defined as follows:

$$f(x) = \ln(x)$$

1. Show that f is a homomorphism from $\left(\mathbb{R}_+^*, \times\right)$ to $(\mathbb{R}, +)$.

2. Calculate $Ker(f)$. What can you conclude?

3. Is f surjective?

Exercice4. We equip the set $A = \mathbb{Z}^2$ with two operations defined by:

$$(x, y) + (x', y') = (x + x', y + y') \text{ and } (x, y) \star (x', y') = (xx', xy' + x'y)$$

1. Show that $(A, +)$ is a commutative group. $(*)$

2. Show that the operation $\star$ is commutative and associative.

3. Determine the neutral element for the operation $\star$.

4. Show that $(A, +, \star)$ is a commutative unitary ring.

5. Show that $B = \{(a, 0) \mid a \in \mathbb{Z}\}$ is a subring of $(A, +, \star)$.

6. We equip the set $K = \mathbb{R}$ with the usual addition and multiplication.

(a) Why is $(K, +, \cdot)$ a field?

(b) Let $L = \{x \in \mathbb{R}, \exists \alpha, \beta \in \mathbb{Q} \mid x = \alpha + \beta\sqrt{3}\}$ be a subset of $\mathbb{R}$.

Show that $(L, +,.) is a subfield of$ (K,+,.).

Exercice5.

(1) Consider a set E defined by $E = \{(a, b) \in \mathbb{R}^2 : a \neq 0\}$ and define on E a composition law $*$ by

$$\forall\,(a_1, b_1), (a_2, b_2) \in E : (a_1, b_1) * (a_2, b_2) = (a_1a_2, a_1b_2 + b_1)$$

(a) Verify that $*$ is an internal law on E and find $(2, 0) * (1, 1)$

(b) Show that $(E, *)$ is a non-commutative group.

(c) Determine the set $H = \{(x, y) \in E, \forall (a, b) \in E : (x, y) * (a, b) = (a, b) * (x, y)\}$

(2) Let $F = \{(a, b) \in E : b = 0\}$ be a subset of E.

(a) Show that F is a subgroup of E.

(3) Consider a function f defined by

$$f : (E, *) \longrightarrow (\mathbb{R}^*, .)$$

$$(a, b) \longmapsto f((a, b)) = a$$

(a) Show that f is a group homomorphism from $(E, *)$ to the group $(\mathbb{R}^*, .)$

(b) Determine the kernel of f.

(4) Let $\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2}, m, n \in \mathbb{Z}\}$ be a subset of $\mathbb{R}$.

(a) Show that $\mathbb{Z}[\sqrt{2}]$ equipped with addition and multiplication of real numbers is a subring of $\mathbb{R}$.

4.3.1 Solutions

Exercise 1.

(1)

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

  Therefore, $*$ is commutative.

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

  Therefore, $*$ is associative.

- $a * e = a \Leftrightarrow \ln\left(e^a + e^e\right) = a \Leftrightarrow e^e = 0$.

  Thus, there is no neutral element.

(2)

- $\perp$ is associative $\Leftrightarrow \forall x, y, z \in \mathbb{R}$, $(x \perp y) \perp z = x \perp (y \perp z)$.

  $\Leftrightarrow \forall x, y, z \in \mathbb{R}$, $a^2x + aby + bz = ax + aby + b^2z$.

  Therefore, $a^2 = a$ and $ab = ba$ and $b = b^2$.

  Hence, ($a = 0$ or $a = 1$) and ($b = 0$ or $b = 1$).

- $\perp$ has a neutral element $e \in \mathbb{R}$ if $\forall x \in \mathbb{R}$, $x \perp e = e \perp x = x$.

  $\Leftrightarrow \forall x \in \mathbb{R}$, $ax + be = ae + bx = x$.

  $\Leftrightarrow a = 1$ and $e = 0$ and $b = 1$.

Exercise 2.

(1)

- $((x, y) * (x', y')) * (x'', y'') = (xx', xy' + y) * (x'', y'')$
  $= (xx'x'', xx''y' + xy'' + y)$ and

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

Thus, $*$ is associative.

- $(x, y) * (1, 0) = (x, y)$ and $(1, 0) * (x, y) = (x, y)$.

Hence, $(1, 0)$ is the neutral element.

- $(x,y) * \left(\frac{1}{x}, \frac{-y}{x}\right) = (1,0)$ and $\left(\frac{1}{x}, -\frac{y}{x}\right) * (x,y) = (1,0)$.

Therefore, every element is symmetrizable. Thus, $(G,*)$ is a group.

- $(1,2) * (3,4) = (3,6)$ and $(3,4) * (1,2) = (3,10)$.

Therefore, the group is not commutative.

(2) $H = \mathbb{R}_+^* \times \mathbb{R}$ is a subset of G.

- $(1,0) \in H$,
- $\forall (x,y), (x',y') \in H$, $(x,y) * (x',y') \in H$ since $x\bar{x} > 0$,
- $\forall (x,y) \in H$, $(x,y)^{-1} = \left(\frac{1}{x}, \frac{-y}{x}\right) \in H$ since $\frac{1}{x} > 0$.

Therefore, H is a subgroup of G.

Exercise 3.

(1) f is a homomorphism from $\left(\mathbb{R}_+^*, \cdot\right)$ to $(\mathbb{R}, +)$. Let:

$$\begin{aligned} x_1, x_2 \in \mathbb{R}_+^* : f(x_1 \cdot x_2) &= \ln(x_1 \cdot x_2) = \ln x_1 + \ln x_2 \\ &= f(x_1) + f(x_2) \end{aligned}$$

(2)

$$\begin{aligned} \ker(f) &= \left\{x \in \mathbb{R}_+^* : f(x) = 0\right\} \\ &= \left\{x \in \mathbb{R}_+^* : \ln x = 0\right\} \\ &= \left\{x \in \mathbb{R}_+^* : e^{\ln(x)} = e^0 = 1\right\} \\ &= \left\{x \in \mathbb{R}_+^* : x = 1\right\} \\ &= \{1\} \end{aligned}$$

Thus, f is injective.

(3) f is surjective because:

$$\forall y \in \mathbb{R}, \exists x = e^y \in \mathbb{R}_+^* \text{ such that } f(x) = f(e^y) = \ln(e^y) = y.$$

Exercise 4.

(1) $(*)$

(2) $(x,y)*(x',y') = (xx', xy'+x'y) = (x'x, x'y+xy') = (x',y')*(x,y)$.

Therefore, $*$ is commutative.

(3) For

$$\begin{aligned}[(x,y)*(x',y')]*(x'',y'') &= (xx', xy'+x'y)*(x'',y'') = (xx'x'', xx'y''+x''(xy'+x'y)) \\ &= (xx'x'', xx'y''+xx''y'+x'x''y)\,, \\ (x,y)*[(x',y')*(x'',y'')] &= (x,y)*(x'x'', x'y''+x''y') = (xx'x'', x(x'y''+x''y')+x'x''y) \\ &= (xx'x'', xx'y''+xx''y'+x'x''y)\,.\end{aligned}$$

The operation $*$ is associative.

(4) All the properties of a ring are satisfied based on the previous questions, except for the distributivity of $*$ over addition:

$$\begin{aligned}(x,y)*[(x',y')+(x'',y'')] &= (x,y)*(x'+x'', y'+y'') \\ &= (x(x'+x''), x(y'+y'')+(x'+x'')y) \\ &= (xx'+xx'', xy'+x'y+xy''+x''y) \\ &= (xx', xy'+x'y)+(xx'', xy''+x''y) \\ &= [(x,y)*(x',y')]+[(x,y)*(x'',y'')]\,.\end{aligned}$$

Thus, $(A,+,*)$ is a commutative ring.

(5) $B = \{(a,0) \mid a \in \mathbb{Z}\}$

- $B \subset \mathbb{Z}^2$ and $(1,0) \in A$.
- $\forall (a,0),(b,0) \in B$, we have $(a,0)-(b,0) = (a-b,0) \in B$.
- $\forall (a,0),(b,0) \in B$, we have $(a,0)*(b,0) = (ab,0) \in B$.

Therefore, B is a subring of $(\mathbb{Z}^2,+,*)$.

(6)

(a) $(k,+,\cdot)$ is a field because

$$\begin{cases} \text{(i) } (K,+,\cdot) \text{ is a commutative ring } ((*)) \\ \text{(ii) every nonzero element has a multiplicative inverse.} \end{cases}$$

(b) $(L, +, \cdot)$ is a subfield of $(k, +, \cdot)$ if and only if:

(i) $\forall x, y \in L : x - y \in L$

(ii) $\forall x, y \in L : xy \in L$

(iii) $\forall x \in L^* : x^{-1} \in L$.

Let's assume that $x = \alpha_1 + \beta_1\sqrt{3}, y = \alpha_2 + \beta_2\sqrt{3} \in L$

(i) We have: $x - y = (\alpha_1 - \alpha_2) + (\beta_1 - \beta_2)\sqrt{3} = \alpha_3 + \beta_3\sqrt{3} \in L$.

because: $\alpha_3 = \alpha_1 - \alpha_2, \beta_3 = \beta_1 - \beta_2 \in \mathbb{Q}$.

(ii) We also have:

$$xy = \left(\alpha_1 + \beta_1\sqrt{3}\right)\left(\alpha_2 + \beta_2\sqrt{3}\right) = (\alpha_1\alpha_2 + 3\beta_1\beta_2) + (\alpha_1\beta_2 + \beta_1\alpha_2)\sqrt{3}$$
$$= \alpha' + \beta'\sqrt{3} \in L.$$

because: $\alpha' = \alpha_1\alpha_2 + 3\beta_1\beta_2, \beta' = \alpha_1\beta_2 + \beta_1\alpha_2 \in \mathbb{Q}$.

(iii) Let $x = \alpha_1 + \beta_1\sqrt{3} \in L^*$, which means $\alpha_1 \neq 0$ and $\beta_1 \neq 0$. Then,

$$x^{-1} = \frac{1}{x} = \frac{1}{\alpha_1 + \beta_1\sqrt{3}} = \frac{\alpha_1 - \beta_1\sqrt{3}}{\alpha_1^2 - 3\beta_1^2} = \frac{\alpha_1}{\alpha_1^2 - 3\beta_1^2} + \frac{-\beta_1}{\alpha_1^2 - 3\beta_1^2}\sqrt{3} = a + b\sqrt{3} \in L.$$

because: $a = \frac{\alpha_1}{\alpha_1^2 - 3\beta_1^2}, b = \frac{-\beta_1}{\alpha_1^2 - 3\beta_1^2} \in Q$

Therefore, $(L, +, \cdot)$ is a subfield of $(k, +, \cdot)$.

Chapter 5

Polynomial Rings

In this chapter, we introduce the concept of a polynomial over a field or a commutative ring. Throughout the chapter, $\mathbb{K}$ denotes a field and $\mathbb{A}$ denotes a unitary commutative ring.

5.1 Definitions

Definition 5.1. Let $(\mathbb{A}, +, \cdot)$ be a unitary commutative ring.

A polynomial P in one variable X with coefficients in $\mathbb{A}$ is defined as an algebraic expression of the form

$$P = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n + \ldots$$

where the $a_i \in \mathbb{A}$ are zero except for a finite number.

Another definition is given by:

Definition 5.2. A polynomial in one variable x with coefficients in $\mathbb{A}$ is a sequence $P = (a_n)_{n\in\mathbb{N}}$ of elements in $\mathbb{A}$ that are zero from a certain rank.

1. The a_n are called the coefficients of P.
2. The largest index n for which $a_n \neq 0$ (if it exists) is called the degree of P and denoted $\deg(P)$, and in this case, a_nX^n is called the leading term of P.
3. If all the a_i are zero, P is called the zero polynomial, denoted as 0, and conventionally $\deg(0) = -\infty$.

4. If the leading term of P is $1X^n$, the polynomial P is said to be monic.

5. Each element a of $\mathbb{A}$ is a polynomial, called a constant polynomial.

6. The set of polynomials in one variable X with coefficients in $\mathbb{A}$ is denoted as $\mathbb{A}[X]$.

Polynomials are equipped with the usual operations of addition, multiplication of polynomials, and scalar multiplication by $\lambda \in \mathbb{A}$: Let $P = (a_n)_{n\in\mathbb{N}}, Q = (b_n)_{n\in\mathbb{N}}$ be two polynomials in one variable with coefficients in $\mathbb{A}$. Then:

1. $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$,

2. $PQ = (c_n)_{n\in\mathbb{N}}$ with $c_n = \sum_{0\leq k\leq n} a_k b_{n-k}$,

3. $\lambda P = (\lambda a_n)_{n\in\mathbb{N}}$.

Definition 5.3.

The set $\mathbb{A}[X]$ of polynomials in one variable with coefficients in $\mathbb{A}$, equipped with the addition and multiplication defined above, forms a commutative ring.

Proposition 5.1. If $\mathbb{A}$ is an integral domain, then for all $P, Q \in \mathbb{A}[X]$, we have:

1. $\deg(PQ) = \deg(P) + \deg(Q)$.

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

Proof

1. If either of the two polynomials is zero, then $PQ = 0$, and the equation becomes $-\infty = -\infty$, which is true. So, we assume that P and Q are non-zero. Let $n = \deg(P)$ and $m = \deg(Q)$. We can write $P = \sum a_i X^i$ and $Q = \sum b_i X^i$, where $a_i, b_i \in \mathbb{A}$. Then the coefficient of the leading term of PQ is $a_n b_m$. Now, $a_n \neq 0$ and $b_n \neq 0$, and since $\mathbb{A}$ is an integral domain, $a_n b_n \neq 0$. This implies that $\deg(PQ) = n + m$.

2. Obvious.

Let $\mathbb{U}(A)$ denote the set of invertible elements in $\mathbb{A}$.

Proposition 5.2

If $\mathbb{A}$ is an integral domain, then the invertible elements in $\mathbb{A}[X]$ are the constant polynomials $P = a$ where $a \in \mathbb{U}(A)$.

Proof.

Let P be invertible in $\mathbb{A}[X]$. There exists $Q \in \mathbb{A}[X]$ such that $PQ = 1$. Then, we have $\deg(P) + \deg(Q) = 0$, and $\deg(P) = \deg(Q) = 0$. Thus, P and Q are constant and invertible elements.

5.2 Polynomial Arithmetic

5.2.1 Associated Polynomials

Definition 5.4.

Two polynomials P and Q in $\mathbb{A}[X]$ are said to be associated if there exists $a \in \mathbb{U}(A)$ such that $P = a.Q$.

Example.

The set of polynomials associated with $X^2 + 1$ in $\mathbb{Z}[X]$ is $\{X^2 + 1, -(X^2 + 1)\}$ since the only units in $\mathbb{Z}$ are 1 and -1.

Proposition 5.3.

1. The relation "being associated" is an equivalence relation on $\mathbb{A}[X]$.

2. If P and Q are associated and have the same leading coefficient, then $P = Q$.

3. If $\mathbb{A}$ is a field, then every polynomial P is associated with a unique monic polynomial.

Proposition 5.4 Let P and Q be two polynomials in $A[X]$. Then $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$ and $\deg(P \cdot Q) = \deg(P) + \deg(Q)$.

Example. In $\mathbb{Q}[X]$, let $P = 3X^2 - 1$ and $Q = \frac{1}{2}X^3 + 4X$. Then $P + Q = \frac{1}{2}X^3 + 3X^2 + 4X - 1$ and $P \cdot Q = \frac{3}{2}X^5 - \frac{23}{2}X^3 - 4X$.

Definition 5.5 (Divisibility) Let P, B be two polynomials in $A[X]$. We say that B divides P if there exists $Q \in A[X]$ such that $P = Q \cdot B$. We denote this as $B \mid P$.

We also say that P is a multiple of B or P is divisible by B.

Example.

1. Every invertible element a in the ring A divides every polynomial P in $A[X]$. Indeed, $P = a \cdot (a^{-1}P)$.
2. $X + 1$ divides $X^2 + X$. Indeed, $X^2 + X = X(X + 1)$.

Remark. If B divides P and $P \neq 0$, then $\deg(B) \leq \deg(P)$ (since $P = Q \cdot B$ implies $\deg(P) = \deg(Q) + \deg(B)$).

Proposition 5.5 Let A, B, C be polynomials in $K[X]$. Then:

1. If $A \mid B$ and $B \mid A$, then there exists $\lambda \in \mathbb{K}^*$ such that $A = \lambda B$.
2. If $A \mid B$ and $B \mid C$, then $A \mid C$.
3. If $C \mid A$ and $C \mid B$, then $C \mid (AU + BV)$ for any $U, V \in K[X]$.

Definition 5.6 (Euclidean Division of Polynomials) Let P, B be two polynomials in $A[X]$. If the leading coefficient of B is invertible in A, then there exists a pair $(Q; R) \in A[X]^2$ such that $P = QB + R$ and $\deg(R) < \deg(B)$.

Example. Division of $P = 3X^5 - 2X^3 - 5X^2 + 1$ by $B = 2X^3 + \frac{1}{2}X^2 - X$:

$3X^5 + 0X^4 - 2X^3 - 5X^2 + 0X + 1$	$\frac{1}{2}X^3 + 2X^2 - X + 0$
$-12X^4 + 4X^3 - 5X^2 + 0X + 1$	$6X^2 - 24X + 104$
$52X^3 - 29X^2 + 0X + 1$	
$-237X^2 + 104X + 1$	

Therefore, the quotient is $Q = 6X^2 - 24X + 104$ and the remainder is $R = -237X^2 + 104X + 1$.

The existence of the Euclidean division allows us to develop the properties of divisibility: GCD, LCM, Bézout's theorem, Euclidean algorithm, Gauss's theorem, and factorization into irreducible factors, entirely analogous to $\mathbb{Z}$.

Definition 5.7 The greatest common divisor (GCD) of two polynomials A and B is a polynomial D that divides both A and B, and any polynomial dividing both A and B must also divide D. The least common multiple (LCM) is a polynomial M that is a multiple of both A and B, and any polynomial that is a multiple of both A and B must also be divisible by M.

Remark 5.3 Let $P_1, P_2, \ldots, P$ be polynomials in $K[X]$.

1. The GCD and LCM remain unchanged when permuting the P_i.
2. $PGCD(\lambda_1 P_1; \lambda_2 P_2, \ldots, \lambda_s P_s) = PGCD(P_1, P_2, \ldots, P_s)$ and

   $PPCM(\lambda_1 P_1; \lambda_2 P_2, \ldots, \lambda_s P_s) = PPCM(P_1, P_2, \ldots, P_s)$ for $\lambda_1, \lambda_2, \ldots, \lambda_s \in K$

Example. Let $A := X^6 + X^5 + X^4 + X^2 + X + 1$ and $B := X^5 + X^4 + X^3 + X^2 + X + 1$. Then:

$A = BQ_1 + R_1$ (with $Q_1 = X$ and $R_1 = 1 - X^3$)

$B = R_1 Q_2 + R_2$ (with $Q_2 = -X^2 - X - 1$ and $R_2 = 2X^2 + 2X + 2$)

$R_1 = R_2 Q_3 + R_3$ (with $Q_3 = \frac{1}{2}$ and $R_3 = 0$)

Therefore, $R_2 = 2X^2 + 2X + 2$ is the GCD and $\mathrm{PPCM}(A, B) \cdot \mathrm{GCD}(A, B) = A \cdot B$, so $\mathrm{PPCM}(A, B) = X^9 + X^8 + X^7 + X^6 + 2X^5 + 2X^4 + X^3 + X^2 + X + 1$.

Definition 5.8 (Irreducible Polynomial) A polynomial $P \in K[X]$ is called irreducible if it is non-constant and the only factorizations $P = QR$ (with $Q, R \in K[X]$) occur when P or Q is constant.

Remark 5.4

1. The notion of irreducible polynomials corresponds to that of prime numbers in $\mathbb{Z}$.
2. The irreducible polynomials in $\mathbb{C}[X]$ are the polynomials of degree one.

3. The irreducible polynomials in $\mathbb{R}[X]$ are the polynomials of degree one and the polynomials of degree two of the form $P = aX^2 + bX + c$ with $b^2 - 4ac < 0$.

Example. $X^2 + 1$ is irreducible in $R[X]$ because it cannot be written as a product of two polynomials of degree 1 with coefficients in $\mathbb{R}$.

The same polynomial $X^2 + 1$ is reducible in $C[X]$ since $X^2 + 1 = (X + i)(X - i)$.

Theorem 5.1

1. (Euclid) Let P be an irreducible polynomial in $K[X]$ that divides QR. Then P divides Q or R.

2. (Gauss) If $\mathrm{GCD}(P, Q) = 1$ and P divides QR, then P divides R.

Proof. The proof is entirely analogous to the one done in $\mathbb{Z}$.

5.3 Roots of a Polynomial and Factorization

Definition 5.9 Let $P \in K[X]$ and $\alpha \in K$. We say that α is a root (or zero) of P if $P(\alpha) = 0$.

Proposition 5.6 Let $P \in K[X]$, then

$$P(\alpha) = 0 \Leftrightarrow X - \alpha \text{ divides } P$$

Definition 5.10 Let $k \in \mathbb{N}^*$. We say that α is a root of multiplicity (or order) k of P if $(X - \alpha)^k$ divides P while $(X - \alpha)^{k+1}$ does not divide P. When $k = 1$, we refer to it as a simple root, when $k = 2$, it is a double root, and so on.

Example 5.7 -3 is a double root and 1 is a simple root of the polynomial $P = X^3 + 5X^2 + 3X - 9$ in $\mathbb{R}[X]$, since $P = (X + 3)^2(X - 1)$.

Definition 5.11 Let $P = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ be a polynomial. The derivative of P is $P' = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots + a_1$. We denote $P^{(r)}$ as the r-th derivative defined by $P^{(r+1)} = \left(P^{(r)}\right)'$.

Remark 5.5 The following properties are equivalent:

1. P has a root of order r at $X = \alpha$

2. $P(\alpha) = P'(\alpha) = \ldots = P^{(r-1)}(\alpha) = 0$ and $P^{(r)}(\alpha) \neq 0$

Example Let the polynomial $B = X^4 - 2X^3 + 2X^2 - 2X + 1$ in $\mathbb{R}[X]$. We have $\alpha = 1$ as a double root of B since $B(1) = 0, B'(1) = 0, B''(1) \neq 0$.

Theorem 5.2 (Fundamental Theorem of Algebra) Every non-constant polynomial in $\mathbb{C}[X]$ has at least one root in $\mathbb{C}$. In other words, the irreducible polynomials in $\mathbb{C}[X]$ are polynomials of degree 1.

The proof of this theorem goes beyond the scope of the first-year algebra course.

Theorem 5.3 (Decomposition into Irreducible Factors) For any polynomial P in $K[X]$ with $\deg P \geq 1$, there exist unique unit irreducible polynomials $P_1, P_2, \ldots, P_r$, pairwise distinct in $K[X]$, and positive natural numbers $\alpha_1, \alpha_2, \ldots, \alpha_r$, as well as a unique element $\lambda \in K^*$ such that $P = \lambda \prod_{i=1}^{r} P_i^{\alpha_i}$

This is, of course, analogous to the prime factorization of a number.

Theorem 5.4 (Factorization in C) Let $P \in \mathbb{C}[X]$ with degree $n \geq 1$. The factorization of P is given by $P = \lambda (X - \alpha_1)^{k_1} (X - \alpha_2)^{k_2} \ldots (X - \alpha_r)^{k_r}$, where $\alpha_1, \alpha_2, .., \alpha_r$ are the distinct roots of P and $k_1, k_2, \ldots, k_r$ are their multiplicities.

Theorem 5.5 (Factorization in R) Let $P \in \mathbb{C}[X]$ with degree $n \geq 1$. The factorization of P is given by $P = \lambda (X - \alpha_1)^{k_1} (X - \alpha_2)^{k_2} \ldots (X - \alpha_r)^{k_r} Q_1^{l_1} \ldots Q_s^{l_s}$, where α_i are the distinct real roots with multiplicity k_i and the Q_i are irreducible polynomials of degree $2 : Q_i = X^2 + \beta_i X + \gamma_i$ with $\Delta = \beta_i^2 - 4\gamma_i < 0$.

Example Let $P = 2X^4(X-1)^3 (X^2+1)^2 (X^2+X+1)$, which is already factored into irreducible factors in $\mathbb{R}[X]$, but its factorization in $\mathbb{C}[X]$ is

$$P = 2X^4(X-1)^3(X-i)^2(X+i)^2 \left(X - \tfrac{-1+i\sqrt{3}}{2}\right) \left(X - \left(\tfrac{-1+i\sqrt{3}}{2}\right)^2\right).$$

5.4 Exercises

Exercise 1. Consider the polynomial $P = X^4 + 5X^3 + 10X^2 + 12X + 8$.

1. Show that -2 is a double root of the polynomial P.
2. Factorize P in $\mathbb{R}[X]$.
3. Deduce the roots of P in $\mathbb{C}$.

Exercise 2. Consider the polynomial $P = X^4 + X^2 + 1$.

1. Determine the roots of P in $\mathbb{C}$.
2. Factorize P in $\mathbb{C}[X]$.
3. Deduce a factorization of P in $\mathbb{R}[X]$.

Exercise 3. Let $n \in \mathbb{N}$. Consider the polynomial $P_n = X^n$.

1. Determine the remainder of the division of P_n by $A_1 = X^2 - 3X - 4$.
2. Determine the remainder of the division of P_n by $A_2 = X^2 + 1$.

Exercise 4. Consider the polynomial $P = X^4 - 4X^3 + 5X^2 - 2X - 6$.

1. We aim to show that P does not have a double root.
   - **(a)** Perform the Euclidean division of $2P$ by $\frac{1}{2}P'$. Let R be the remainder of this division.
   - **(b)** Perform the Euclidean division of $\frac{1}{2}P'$ by R. Let T be the remainder of this division.
   - **(c)** Show that if a is a double root of P, then a is a root of R and T.
   - **(d)** Show that P does not have a double root.
2. We aim to factorize P in $\mathbb{R}[X]$.
   - **(a)** Let $X = Y + 1$ and $Q(Y) = P(Y + 1)$. Calculate $Q(Y)$.
   - **(b)** Find the roots of Q in $\mathbb{C}$. Deduce the roots of P in $\mathbb{C}$.

(c) Factorize P in $\mathbb{C}[X]$, then in $\mathbb{R}[X]$.

Exercise 5. Consider the polynomial $P = X^4 + 2X^3 - X^2 - 2X + 10$. For any $z \in \mathbb{C}$, let $P(z) = z^4 + 2z^3 - z^2 - 2z + 10$

1. Let $x \in \mathbb{R}\backslash\{0\}$. Give the expression of $P(x(1+\imath))$ in the form $P(x(1+\imath)) = Q(x) + \imath R(X)$, where Q and R are polynomials with real coefficients.

2. Do the equations $Q(x) = 0$ and $R(x) = 0$ have any common roots?

3. Find two complex conjugate roots of the equation $P(z) = 0$.

4. Factorize P as a product of two second-degree trinomials with real coefficients and deduce the complex roots of P.

Exercise 6. Determine the real numbers p and q such that the polynomial $P = X^3 + pX + q$ is divisible by the polynomial $Q = X^2 + 3X - 1$.

Exercise 7. Let $n \in \mathbb{N}$. Show that the polynomial $X^2 - X + 1$ divides the polynomial $P_n = (X-1)^{n+2} + X^{2n+1}$.

Exercise 8. Let $n \in \mathbb{N}\backslash\{0,1\}$. Calculate the remainder of the Euclidean division of the polynomial $P_n = (X-3)^{2n} + (X-2)^n - 2$ by the polynomial $(X-2)^2$.

Exercise 9. Factorize the polynomial $P = X^6 + 1$ in $\mathbb{R}[X]$.

Exercise 10. Determine $\lambda \in]0, \infty[$ such that the polynomial $P = X^3 - 3X + \lambda$ has a double root. What is the other root of P?

Exercise 11. Let $n \in \mathbb{N}$. Show that the polynomial $P_n = 1 + X + \frac{X^2}{2} + \frac{X^3}{3!} + \ldots + \frac{X^n}{n!}$ does not have multiple roots.

Exercise 12. Determine all polynomials P such that $(X^2+1)P'' - 6P = 0$ and $P(1) = 2$.

Exercise 13. Consider the polynomial $P = X^4 + 12X - 5$. Factorize P in $\mathbb{R}[X]$ and in $\mathbb{C}[X]$, knowing that it has two roots whose product is -1.

Exercise 14. Solve the system in $(x, y, z) \in \mathbb{R}^3$:

$$\begin{cases} x + y + z = 2 \\ xyz = -\frac{1}{2} \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{1}{2} \end{cases}$$

Exercise 15. Let $n \in \mathbb{N}\backslash\{0\}$. Factorize the polynomial

$$P_n = 1 - X + \frac{X(X-1)}{2!} - \frac{X(X-1)(X-2)}{3!} + \ldots + (-1)^n \frac{X(X-1)(X-2)\ldots(X-n+1)}{n!}$$

Exercise 16. Determine all polynomials $P \in \mathbb{R}[X]$ such that P' divides P.

Chapter 6

Solved Exams

6.1 Exam 01

Exercise 1. (6 p)

I) Let $\mathrm{P}_1, \mathrm{P}_2$ be two propositions. Prove the following properties in the same truth table:

1. $(\neg \mathrm{P}_1 \Rightarrow \mathrm{P}_2) \Leftrightarrow (\mathrm{P}_1 \wedge \neg \mathrm{P}_2)$

2. $(\mathrm{P}_1 \Rightarrow \mathrm{P}_2) \Leftrightarrow (\neg \mathrm{P}_2 \Rightarrow \neg \mathrm{P}_1)$

II) Let P, Q be two polynomials in $\mathbb{K}[X]$. If $P \times Q = 0$, show that either $P = 0$ or $Q = 0$.

Exercise 02. (8 p) Let A and B be two subsets of a set E. The symmetric difference of A and B, denoted $A\Delta B$, is defined as

$$A\Delta B = (A \backslash B) \cup (B \backslash A)$$

1. Is the symmetric difference of two sets commutative?

2. Determine the following sets: $A\Delta\emptyset, A\Delta A$, and $A\Delta B$ if $A \subset B$.

3. Show that $A\Delta B = C_E A \Delta C_E B$.

4. Show that $A\Delta B = (A \cap C_E B) \cup (B \cap C_E A)$.

5. Determine the set $(A\Delta B) \cup (A\Delta C_E B)$.

Exercise 03. (6 p) Let $(G, \cdot)$ be a group, and for any $a \in G$, define the function

$$f_a : G \longrightarrow G$$
$$x \mapsto f_a(x) = axa^{-1}$$

1. Show that f_a is a homomorphism of G.

2. Calculate the $\ker(f_a)$. What can you conclude?

3. Show that $f_a \circ f_b = f_{ab}$.

4. Is $f_a \circ f_b$ an automorphism of G?

6.1.1 Solution

Exercise 1. (6 p)

I) -

P_1	P_2	$\neg P_1$	$\neg P_2$	$P_1 \Rightarrow P_2$	$\neg P_2 \Rightarrow \neg P_1$	$\neg(P_1 \Rightarrow P_2)$	$P_1 \wedge \neg P_2$	$\Leftrightarrow (1°)$	$\Leftrightarrow (2°)$
1	1	0	0	1	1	0	0	1	1
1	0	0	1	0	0	1	1	1	1
0	1	1	0	1	1	0	0	1	1
0	0	1	1	1	1	0	0	1	1

II) Let $(P; Q) \in \mathbb{K}[X]$ such that $P \times Q = 0$. Then we have $\deg(P) + \deg(Q) = \deg(P \times Q) = -\infty$.

Therefore, either $\deg(P)$ or $\deg(Q)$ equals $-\infty$, which is exactly the required property.

Exercise 02. (8 p)

1. It is commutative because $\cup$ is commutative.

2. $A\Delta\emptyset = (A\backslash\emptyset) \cup (\emptyset\backslash A) = A$, $A\Delta A = A$, and if $A \subset B$ then $A\Delta B = B\backslash A$.

3.

$$\begin{aligned} A\Delta B &= \{x \in E, \quad (x \in A \backslash B) \vee (x \in B \backslash A)\} \\ &= \{x \in E, \quad (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\} \\ &= \{x \in E, \quad (x \notin C_E A \wedge x \in C_E B) \vee (x \notin C_E B \wedge x \in C_E A)\} \\ &= \{x \in E, \quad (x \in C_E B \backslash C_E A) \vee (x \in C_E A \backslash C_E B)\} \\ &= C_E A \Delta C_E B. \end{aligned}$$

4. $A\Delta B = (A \cap C_E B) \cup (B \cap C_E A)$

$$\begin{aligned} A\Delta B &= \{x \in E, \quad (x \in A \backslash B) \vee (x \in B \backslash A)\} \\ &= \{x \in E, \quad (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\} \\ &= \{x \in E, \quad (x \in A \wedge x \in C_E B) \vee (x \in B \wedge x \in C_E A)\} \\ &= \{x \in E, \quad x \in (A \cap C_E B) \vee x \in (B \cap C_E A)\} \\ &= (A \cap C_E B) \cup (B \cap C_E A)\,. \end{aligned}$$

5. We have

$$\begin{aligned} (A\Delta B) \cup (A\Delta C_E B) &= ((A \cap C_E B) \cup (B \cap C_E A)) \cup ((A \cap B) \cup (C_E B \cap C_E A)) \\ &= ((A \cap C_E B) \cup (A \cap B)) \cup ((B \cap C_E A) \cup (C_E B \cap C_E A)) \\ &= (A \cap (C_E B \cup B)) \cup ((B \cup C_E B) \cap C_E A) \\ &= (A \cap E) \cup (E \cap C_E A) \\ &= A \cup C_E A = E \end{aligned}$$

Exercise 03. (6 p)

1. f_a is a homomorphism of G.

For any $x, y \in G$, $f_a(xy) = a(xy)a^{-1} = a\left(xa^{-1}ay\right)a^{-1} = \left(axa^{-1}\right)\left(aya^{-1}\right) = f_a(x)f_a(y)$.

2.

$$\begin{aligned} \ker\left(f_a\right) &= \{x \in G, \quad f_a(x) = 1\} \\ &= \left\{x \in G, \quad axa^{-1} = 1\right\} \\ &= \left\{x \in G, \quad a^{-1}axa^{-1}a = a^{-1}a\right\}1\} \\ &= \{x \in G, \quad x = 1\} \\ &= \end{aligned}$$

So f_a is injective.

3. Let $x \in G$

$$(f_a \circ f_b)(x) = (f_a(f_b(x))) = \left(f_a\left(bxb^{-1}\right)\right) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = f_{ab}(x)$$

4. ($f_a \circ f_b$ is an automorphism of G) $\Longleftrightarrow$ (f_{ab} is a bijective homomorphism)

i) f_{ab} is a homomorphism

$$f_{ab}(xy) = (ab)xy(ab)^{-1} = (ab)x(ab)^{-1}(ab)y(ab)^{-1} = f_a(x)f_a(y)$$

ii)

(a) f_{ab} is injective

$$\begin{aligned}\ker(f_{ab}) &= \{x \in G, \quad f_{ab}(x) = 1\} \\ &= \{x \in G, \quad (ab)x(ab)^{-1} = 1\} \\ &= \{1\}\end{aligned}$$

So f_{ab} is injective.

(b) f_{ab} is surjective: Let $y \in G$, then $\exists x = (ab)^{-1}yab \in G$ such that $f_{ab}(x) = f_{ab}((ab)^{-1}y(ab)) = y$.

6.2 Exam 02

Exercise 01 (8 p)

Let $\mathrm{P}_1, \mathrm{P}_2$, and P_3 be three propositions. Prove the following properties.

1. $(\mathrm{P}_1 \vee (\mathrm{P}_2 \wedge \mathrm{P}_3)) \Leftrightarrow ((\mathrm{P}_1 \vee \mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \mathrm{P}_3))$

2. $(\mathrm{P}_1 \vee (\neg\mathrm{P}_2 \vee \mathrm{P}_3)) \Leftrightarrow ((\mathrm{P}_1 \vee \neg\mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \neg\mathrm{P}_3))$

Exercise 02 (8 p) Let A and B be two subsets of a set E. The symmetric difference of A and B, denoted as $A\Delta B$, is defined as

$$A\Delta B = (A \backslash B) \cup (B \backslash A)$$

1. Is the symmetric difference of two sets commutative?

2. Specify the following sets: $A\Delta\emptyset, A\Delta A$, and $A\Delta B$ if $A \subset B$.

3. Show that $A\Delta B = C_E A \Delta C_E B$.

4. Show that $A\Delta B = (A \cap C_E B) \cup (B \cap C_E A)$.

5. Specify the set $(A\Delta B) \cup (A\Delta C_E B)$.

Exercise 03 (4 p) Determine the injections, surjections, and bijections among the following functions:

$$f : \mathbb{R} \to \mathbb{R} \quad g : \mathbb{R}_+ \to \mathbb{R}$$

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

$$h : \mathbb{R} \to \quad \mathbb{R}_+ \quad k : \mathbb{R}_+ \to \quad \mathbb{R}_+$$

$$x \mapsto h(x) = x^2 \mapsto k(x) = x^2$$

6.2.1 Solution

Exercise 01 (8 p)

1. $(\mathrm{P}_1 \vee (\mathrm{P}_2 \wedge \mathrm{P}_3)) \Leftrightarrow ((\mathrm{P}_1 \vee \mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \mathrm{P}_3))$

P_1	P_2	P_3	$(\mathrm{P}_2 \wedge \mathrm{P}_3)$	$\mathrm{P}_1 \vee (\mathrm{P}_2 \wedge \mathrm{P}_3)$	$\mathrm{P}_1 \vee \mathrm{P}_2$	$\mathrm{P}_1 \vee \mathrm{P}_3$	$(\mathrm{P}_1 \vee \mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \mathrm{P}_3)$	$\Leftrightarrow$
1	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1	1
1	0	1	0	1	1	1	1	1
1	0	0	0	1	1	1	1	1
0	1	1	1	1	1	1	0	1
0	1	0	0	0	1	0	1	1
0	0	1	0	0	0	1	0	1
0	0	0	0	0	0	0	1	1

2. $(\mathrm{P}_1 \vee (\neg\mathrm{P}_2 \vee \mathrm{P}_3)) \Leftrightarrow ((\mathrm{P}_1 \vee \neg\mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \neg\mathrm{P}_3))$

We have $(\neg\mathrm{P}_2 \vee \mathrm{P}_3) \Leftrightarrow (\neg\mathrm{P}_2 \wedge \neg\mathrm{P}_3)$, so

$$(\mathrm{P}_1 \vee (\neg\mathrm{P}_2 \vee \mathrm{P}_3)) \Leftrightarrow (\mathrm{P}_1 \vee (\neg\mathrm{P}_2 \wedge \neg\mathrm{P}_3)) \overset{(1)}{\Leftrightarrow} ((\mathrm{P}_1 \vee \neg\mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \neg\mathrm{P}_3))$$

Exercise 02 (8 p)

1. It is commutative because $\cup$ is commutative.

2. $A\Delta\emptyset = (A\backslash\emptyset) \cup (\emptyset\backslash A) = A, A\Delta A = A$ and if $A \subset B$ then $A\Delta B = B\backslash A$.

3.

$$\begin{aligned} A\Delta B &= \{x \in E, \quad (x \in A\backslash B) \vee (x \in B\backslash A)\} \\ &= \{x \in E, \quad (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\} \\ &= \{x \in E, \quad (x \notin C_E A \wedge x \in C_E B) \vee (x \notin C_E B \wedge x \in C_E A)\} \\ &= \{x \in E, \quad (x \in C_E B\backslash C_E A) \vee (x \in C_E A\backslash C_E B)\} \\ &= C_E A\Delta C_E B. \end{aligned}$$

4. $A\Delta B = (A \cap C_E B) \cup (B \cap C_E A)$

$$\begin{aligned} A\Delta B &= \{x \in E, \quad (x \in A\backslash B) \vee (x \in B\backslash A)\} \\ &= \{x \in E, \quad (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\} \\ &= \{x \in E, \quad (x \in A \wedge x \in C_E B) \vee (x \in B \wedge x \in C_E A)\} \\ &= \{x \in E, \quad x \in (A \cap C_E B) \vee x \in (B \cap C_E A)\} \\ &= (A \cap C_E B) \cup (B \cap C_E A)\,. \end{aligned}$$

5. Ona

$$\begin{aligned} (A\Delta B) \cup (A\Delta C_E B) &= ((A \cap C_E B) \cup (B \cap C_E A)) \cup ((A \cap B) \cup (C_E B \cap C_E A)) \\ &= ((A \cap C_E B) \cup (A \cap B)) \cup ((B \cap C_E A) \cup (C_E B \cap C_E A)) \\ &= (A \cap (C_E B \cup B)) \cup ((B \cup C_E B) \cap C_E A) \\ &= (A \cap E) \cup (E \cap C_E A) \\ &= A \cup C_E A = E \end{aligned}$$

Exercise 03 (4 p) Injections, surjections, and bijections:

- g is injective because for any $x_1, x_2 \in \mathbb{R}_+$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$.
- h is surjective because for any $y \in \mathbb{R}_+$, there exists $x \in \mathbb{R}$ such that $f(x) = y$.
- k is bijective.

6.3 Exam 03

Exercise 01 (5p)

I) Let P_1, P_2, and P_3 be propositions. Prove that:

1. $(P_1 \vee (P_2 \wedge P_3)) \Leftrightarrow ((P_1 \vee P_2) \wedge (P_1 \vee P_3))$

II) Let $\mathcal{R}$ be an equivalence relation on a set E. Prove that:

1. $\forall x, y \in E, \quad x\mathcal{R}y \Longleftrightarrow \bar{x} = \bar{y}$.

2. $\forall x, y \in E, \quad x\mathcal{R}y \Longrightarrow \bar{x} \cap \bar{y} = \phi$

Exercise 02 (7p) Let $g : E \longrightarrow F$ be a function. Let A and B be two subsets of F. Prove that:

1. $A \backslash B = A \cap C_F B$

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

3. $g^{-1}(A \cup B) = g^{-1}(A) \cup g^{-1}(B)$

4. $g^{-1}(A \cap B) = g^{-1}(A) \cap g^{-1}(B)$

5. $g^{-1}\left(C_F B\right) = C_E g^{-1}(B)$

6. Explicitly describe the set $g^{-1}(A \Delta B)$

Exercise 03 (5p) Let $(\mathbb{R}, +)$ and $\left(\mathbb{R}_+^*, \times\right)$ be two groups. Consider the function

$$f : \mathbb{R} \longrightarrow \mathbb{R}_+^*$$

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

1. Show that f is a homomorphism from $(\mathbb{R}, +)$ to $\left(\mathbb{R}_+^*, \times\right)$.

2. Calculate the $\ker(f)$. What do you conclude?

3. Is f surjective?

Exercise 04 (5p) Let $h : E \longrightarrow F$ be a function. B is a subset of F. Show that

$$\left(B = h\left(h^{-1}(B)\right)\right) \Longleftrightarrow (h \text{ is surjective })$$

6.3.1 Solution

Exercise 01 (5p)

I) $(P_1 \vee (P_2 \wedge P_3)) \Leftrightarrow ((P_1 \vee P_2) \wedge (P_1 \vee P_3))$.

P_1	P_2	P_3	$(P_2 \wedge P_3)$	$P_1 \vee (P_2 \wedge P_3)$	$P_1 \vee P_2$	$P_1 \vee P_3$	$(P_1 \vee P_2) \wedge (P_1 \vee P_3)$	$\Longleftrightarrow$
1	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1	1
1	0	1	0	1	1	1	1	1
1	0	0	0	1	1	1	1	1
0	1	1	1	1	1	1	1	1
0	1	0	0	0	1	0	0	1
0	0	1	0	0	0	1	0	1
0	0	0	0	0	0	0	0	1

II)

1) Let $z \in \bar{x}$.

$$z \in \bar{x} \Longleftrightarrow x\mathcal{R}z$$

$$(\text{since } x\mathcal{R}y) \Longleftrightarrow z\mathcal{R}x$$

$$\Longleftrightarrow z\mathcal{R}y$$

$$\Longleftrightarrow z \in \bar{y}$$

2) We will prove the contrapositive $(\bar{x} \cap \bar{y} \neq \emptyset \Longrightarrow x\mathcal{R}y)$

$$z \in \bar{x} \cap \bar{y} \Longrightarrow z \in \bar{x} \text{ and } z \in \bar{y}$$

$$\Longrightarrow x\mathcal{R}z \text{ and } z\mathcal{R}y$$

$$\Longrightarrow x\mathcal{R}y$$

Exercise 02 (7p) Let $g : E \longrightarrow F$ be a function. Let A and B be two subsets of F. Prove that:

1. $x \in A \backslash B \Longleftrightarrow x \in A \wedge x \notin B \Longleftrightarrow x \in A \wedge x \in C_F B \Longleftrightarrow x \in A \cap C_F B$

2.

$$x \in C_F(A \cup B) \iff x \in F \wedge (x \notin (A \cup B)) \iff x \in F \wedge (x \notin A \wedge x \notin B) \iff$$
$$(x \in F \wedge x \notin A) \wedge (x \in F \wedge x \notin B) \iff x \in F \backslash A \wedge x \in F \backslash B \iff x \in C_F A \cap C_F B$$

3.

$$x \in g^{-1}(A \cup B) \iff g(x) \in A \cup B \iff g(x) \in A \vee g(x) \in B$$
$$\iff x \in g^{-1}(A) \vee x \in g^{-1}(B) \iff x \in g^{-1}(A) \cup g^{-1}(B)$$

4.

$$x \in g^{-1}(A \cap B) \iff g(x) \in (A \cap B) \iff g(x) \in A \wedge g(x) \in B$$
$$\iff x \in g^{-1}(A) \wedge x \in g^{-1}(B) \iff x \in g^{-1}(A) \cap g^{-1}(B)$$

5. $x \in g^{-1}\left(C_F B\right) \iff g(x) \in C_F B \iff g(x) \notin B \iff x \notin g^{-1}(B) \iff x \in C_E g^{-1}(B)$

6. $g^{-1}(A \Delta B) = g^{-1}((A \backslash B) \cup (B \backslash A)) \overset{(2)}{=} g^{-1}(A \backslash B) \cup g^{-1}(B \backslash A) \overset{(1)}{=} g^{-1}\left(A \cap C_F B\right) \cup g^{-1}\left(C_F A \cap B\right)$

$\overset{(3)}{=} \left(g^{-1}(A) \cap g^{-1}\left(C_F B\right)\right) \cup \left(g^{-1}\left(C_F A\right) \cap g^{-1}(B)\right) \overset{(4)}{=} \left(g^{-1}(A) \cap C_E g^{-1}(B)\right) \cup \left(C_E g^{-1}(A) \cap g^{-1}(B)\right)$

$\overset{(4)}{=} \left(g^{-1}(A) \cap C_E g^{-1}(B)\right) \cup \left(C_E g^{-1}(A) \cap g^{-1}(B)\right) \overset{(1)}{=} \left(g^{-1}(A) \backslash f^{-1}(B)\right) \cup \left(g^{-1}(B) \backslash g^{-1}(A)\right) =$

$g^{-1}(A) \Delta g^{-1}(B)$.

Exercise 03 (5p)

1. f is a homomorphism from $(\mathbb{R}, +)$ to $\left(\mathbb{R}_+^*, \cdot\right)$.

For $x_1, x_2 \in \mathbb{R}$, we have $f\left(x_1 + x_2\right) = 2^{x_1 + x_2} = 2^{x_1} 2^{x_2} = f\left(x_1\right) f\left(x_2\right)$.

2.

$$\begin{aligned}
\ker(f) &= \{x \in \mathbb{R} : \quad f(x) = 1\} \\
&= \{x \in \mathbb{R} : \quad 2^x = 1\} \\
&= \{x \in \mathbb{R} : \quad \ln\left(2^x\right) = \ln(1) = 0\} \\
&= \{x \in \mathbb{R} : \quad x \ln(2) = 0\} \\
&= \{x \in \mathbb{R} : \quad x = 0\} \\
&= \{0\}
\end{aligned}$$

Therefore, f is injective.

3. f is surjective because $\forall y \in \mathbb{R}_+^*$, $\exists x = \frac{\ln(y)}{\ln(2)} \in \mathbb{R}$ such that

$$f(x) = f\left(\frac{\ln(y)}{\ln(2)}\right) = 2^{\frac{\ln(y)}{\ln(2)}} = e^{\ln\left(2^{\ln(y)}\ln(2)\right.} = e^{\frac{\ln(y)}{\ln(2)}\ln(2)} = e^{\ln(y)} = y$$

Exercise 04 (5p)

1) $(B = h\left(h^{-1}(B)\right)) \Longrightarrow (h$ is surjective) Assume that $B = h\left(h^{-1}(B)\right)$ for any subset B of F.

$[(h$ is surjective $) \Longleftrightarrow (h(E) = F)]$ We have $h(E) \subset F$ because h is a function. It remains to show that $F \subset h(E)$. According to the proposition, we have $F = h\left(h^{-1}(F)\right)$ but $h^{-1}(F) \subset E$, so $h\left(h^{-1}(F)\right) \subset h(E)$, hence $F \subset h(E)$.

2) (h is surjective) $\Longrightarrow (B = h\left(h^{-1}(B)\right))$ Assume that h is surjective. We need to show that $B = h\left(h^{-1}(B)\right)$:

(i) $B \subset h\left(h^{-1}(B)\right)$, let $y \in B$, then $\exists x \in E$ such that $h(x) = y$ (since h is surjective), therefore $h(x) \in B \Longrightarrow x \in h^{-1}(B) \Longrightarrow h(x) \in h\left(h^{-1}(B)\right) \Longrightarrow y \in h\left(h^{-1}(B)\right)$

(ii) $h\left(h^{-1}(B)\right) \subset B$, let $y \in h\left(h^{-1}(B)\right)$, then $\exists x \in h^{-1}(B)$ such that $h(x) = y$, hence $h(x) = y \in B$.

6.4 Examen 04

Exercise 01 (6p) Let $(G_1, *)$ and $(G_2, \perp)$ be two groups, and f be a homomorphism from $(G_1, *)$ to $(G_2, \perp)$. Prove that:

1. $f\left(e_1\right) = e_2$

2. $\forall x \in G_1 : \quad [f(x)]' = f\left(x'\right)$.

3. $\ker(f)$ is a subgroup of G_1.

4. $(\ker(f) = e_1) \Longleftrightarrow (f$ is injective).

Exercise 02 (8p) Let $g : E \longrightarrow F$ be a function. Let A and B be two subsets of F. Prove that:

1. $A \backslash B = A \cap C_F B$

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

3. $g^{-1}(A \cup B) = g^{-1}(A) \cup g^{-1}(B)$

4. $g^{-1}(A \cap B) = g^{-1}(A) \cap g^{-1}(B)$

5. $g^{-1}\left(C_F B\right) = C_E g^{-1}(B)$

6. Explicit the set $g^{-1}(A \Delta B)$

Exercise 03 (6p) Prove the following propositions by contrapositive or by contradiction:

1. (n^2 is even) $\Longrightarrow$ (n is even).($\forall n \in \mathbb{N}$)

2. $\sqrt{2} \notin \mathbb{Q}$

6.4.1 Solution

Exercise 01 (6p)

1. $f\left(e_1\right) = e_2$.

Proof: We have $e_1 = e_1 * e_1$, so $f\left(e_1\right) = f\left(e_1 * e_1\right) \overset{f \text{ hom}}{=} f\left(e_1\right) \perp f\left(e_1\right)$. This implies $f\left(e_1\right) = e_2$.

2. $\forall x \in G_1 : \quad [f(x)]' = f\left(x'\right)$.

Proof: We have $f\left(x'\right) \perp f(x) = f\left(x' * x\right) = f\left(e_1\right) \overset{(1)}{=} e_2$. Therefore, $(f(x))' = f\left(x'\right)$.

3. $\ker(f)$ is a subgroup of G_1.

$\ker(f)$ is a subgroup of G_1 if and only if

$$\forall (x, y) \in \ker(f) \times \ker(f) \Longrightarrow x * y' \in \ker(f).$$

For any $x, y \in \ker(f)$, we have $f(x) = e_2$ and $f(y) = e_2$. To show that $x * y' \in \ker(f)$, we evaluate $f\left(x * y'\right)$ as follows:

$$f\left(x * y'\right) = f(x) \perp f\left(y'\right) \overset{(1)}{=} f(x) \perp [f(y)]' = e_2 \perp e_2 = e_2.$$

Thus, $f\left(x * y'\right) = e_2$ implies $x * y' \in \ker(f)$.

4. $(\ker(f) = \{e_1\}) \Longleftrightarrow (f \text{ is injective})$.

$\Longrightarrow$) Assume that $\ker(f) = \{e_1\}$. Let $x_1, x_2 \in G_1$ such that $f(x_1) = f(x_2)$. We have $f(x_1') \perp f(x_1) = f(x_1') \perp f(x_2)$. Since f is a homomorphism, we obtain $e_1 = f(x_1' * x_2)$, which implies $x_1' * x_2 \in \ker(f) = \{e_1\}$. Therefore, $x_1' * x_2 = e_1$, which implies $x_1 = x_2$. This shows that f is injective.

$\Longleftarrow$) Assume that f is injective.

Let $x \in \ker(f)$. Then $f(x) = e_2 = f(e_1)$, which implies $x = e_1$ (since f is injective). Thus, $\ker(f) = \{e_1\}$.

Exercise 02 (8p) Let $g : E \longrightarrow F$ be a function, and let A and B be two subsets of F. We need to show the following:

1. $x \in A \backslash B \Longleftrightarrow x \in A \wedge x \notin B \Longleftrightarrow x \in A \wedge x \in C_F B \Longleftrightarrow x \in A \cap C_F B$

2.

$$\begin{aligned} x \in C_F(A \cup B) &\Longleftrightarrow x \in F \wedge (x \notin (A \cup B)) \\ &\Longleftrightarrow x \in F \wedge (x \notin A \wedge x \notin B) \\ &\Longleftrightarrow (x \in F \wedge x \notin A) \wedge (x \in F \wedge x \notin B) \\ &\Longleftrightarrow x \in F \backslash A \wedge x \in F \backslash B \\ &\Longleftrightarrow x \in C_F A \cap C_F B \end{aligned}$$

3.

$$\begin{aligned} x \in g^{-1}(A \cup B) &\Longleftrightarrow g(x) \in A \cup B \\ &\Longleftrightarrow g(x) \in A \vee g(x) \in B \\ &\Longleftrightarrow x \in g^{-1}(A) \vee x \in g^{-1}(B) \\ &\Longleftrightarrow x \in g^{-1}(A) \cup g^{-1}(B) \end{aligned}$$

4.

$$\begin{aligned} x \in g^{-1}(A \cap B) &\iff g(x) \in (A \cap B) \\ &\iff g(x) \in A \wedge g(x) \in B \\ &\iff x \in g^{-1}(A) \wedge x \in g^{-1}(B) \\ &\iff x \in g^{-1}(A) \cap g^{-1}(B) \end{aligned}$$

5. $x \in g^{-1}\left(C_F B\right) \iff g(x) \in C_F B \iff g(x) \notin B \iff x \notin g^{-1}(B) \iff x \in C_E g^{-1}(B)$

6. $g^{-1}(A \Delta B) = g^{-1}((A \backslash B) \cup (B \backslash A)) \overset{(2)}{=} g^{-1}(A \backslash B) \cup g^{-1}(B \backslash A) \overset{(1)}{=} g^{-1}\left(A \cap C_F B\right) \cup g^{-1}\left(C_F A \cap B\right)$

$\overset{(3)}{=} \left(g^{-1}(A) \cap g^{-1}\left(C_F B\right)\right) \cup \left(g^{-1}\left(C_F A\right) \cap g^{-1}(B)\right) \overset{(4)}{=} \left(g^{-1}(A) \cap C_E g^{-1}(B)\right) \cup \left(C_E g^{-1}(A) \cap g^{-1}(B)\right)$

$\overset{(4)}{=} \left(g^{-1}(A) \cap C_E g^{-1}(B)\right) \cup \left(C_E g^{-1}(A) \cap g^{-1}(B)\right) \overset{(1)}{=} \left(g^{-1}(A) \backslash f^{-1}(B)\right) \cup \left(g^{-1}(B) \backslash g^{-1}(A)\right) =$

$g^{-1}(A) \Delta g^{-1}(B)$

Exercise 03 (6p) Prove the following propositions by contrapositive or by contradiction:

1. (n^2 is even) $\Longrightarrow$ (n is even).($\forall n \in \mathbb{N}$)

By contrapositive, it suffices to show the implication

$$(n \text{ is odd}) \Longrightarrow \left(n^2 \text{ is odd}\right).$$

Assume that n is odd. Then $n = 2k + 1$, which implies $n^2 = (2k + 1)^2 = 2(k^2 + k) + 1 = 2k' + 1$, where k' is an integer. We see that n^2 is odd. This proves the implication $(*)$, which completes the proof.

2. $\sqrt{2} \notin \mathbb{Q}$. We use proof by contradiction.

Suppose that $\sqrt{2} \in \mathbb{Q}$, so $\sqrt{2} = \frac{p}{q}$ with $p \wedge q = 1$. Then we have $2 = \frac{p^2}{q^2}$, which implies $p^2 = 2q^2$. It follows that p is even, and by the same reasoning, we find that q is even. This contradicts the assumption that $p \wedge q = 1$.

6.5 Exam 05

Exercise 01 (5p) Let $\left(\mathbb{R}_+^*, \times\right)$ and $(\mathbb{R}, +)$ be two groups. Consider the function

$$\begin{array}{rcl} f : \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ x & \mapsto f(x) = \ln(x) & \end{array}$$

1. Show that f is a homomorphism from $\left(\mathbb{R}_+^*, \times\right)$ to $(\mathbb{R}, +)$.

2. Calculate the $\ker(f)$. What can you conclude?

3. Is f surjective?

Exercise 02 (5p) Let $g : E \longrightarrow F$ be a function. Let A, B, and C be subsets of E. Show that:

1. $A \backslash B = A \cap C_E B$

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

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

4. $[g(A \cap B) = g(A) \cap g(B)] \Longrightarrow [g \text{ is injective}]$.

Exercise 03 (5p) Let:

$$\begin{array}{c} f : \mathbb{N} \longrightarrow \mathbb{N} \\ n \mapsto f(n) = n + 1 \end{array} \quad \text{and} \quad \begin{array}{c} g : \mathbb{N} \longrightarrow \mathbb{N} \\ n \mapsto g(n) \end{array} = \begin{cases} 0 & \text{if } n = 0 \\ n - 1 & \text{if } n \neq 0 \end{cases}$$

1. Study the injectivity and surjectivity of f and g.

2. Calculate $f \circ g$ and $g \circ f$.

Exercise 04 (4p) Let $\mathcal{R}$ be a binary relation on $\mathbb{R}^3$ defined by

$$(x, y, z)\mathcal{R}(a, b, c) \Longleftrightarrow (|x - a| \leq b - y \quad \text{and} \quad z = c)$$

1. Show that it is a partial order relation. Is it total?

6.5.1 Solution

Exercise 01 (5p)

1. f is a homomorphism from $\left(\mathbb{R}_+^*, \cdot\right)$ to $(\mathbb{R}, +)$.

Let $x_1, x_2 \in \mathbb{R}_+^*$. We have $f(x_1 \cdot x_2) = \ln(x_1 \cdot x_2) = \ln(x_1) + \ln(x_2) = f(x_1) + f(x_2)$.

2.

$$\begin{aligned}\ker(f) &= \left\{x \in \mathbb{R}_+^* : f(x) = 0\right\} \\ &= \left\{x \in \mathbb{R}_+^* : \ln(x) = 0\right\} \\ &= \left\{x \in \mathbb{R}_+^* : e^{\ln(x)} = e^0 = 1\right\} \\ &= \left\{x \in \mathbb{R}_+^* : x = 1\right\} \\ &= \{1\}\end{aligned}$$

Therefore, f is injective.

3. f is surjective because:

For any $y \in \mathbb{R}$, there exists $x = e^y \in \mathbb{R}_+^*$ such that $f(x) = f(e^y) = \ln(e^y) = y$.

Exercise 02 (5p) Let $g : E \longrightarrow F$ be a function, and let A, B, and C be three subsets of E.

We need to prove the following:

1. $x \in A\backslash B \iff x \in A \wedge x \notin B \iff x \in A \wedge x \in C_E B \iff x \in A \cap C_E B$

2. $x \in C_E(A \cup B) \iff x \in E \wedge (x \notin (A \cup B)) \iff x \in E \wedge (x \notin A \wedge x \notin B) \iff$

$(x \in E \wedge x \notin A) \wedge (x \in E \wedge x \notin B) \iff x \in E\backslash A \wedge x \in E\backslash B \iff x \in C_E A \cap C_E B$

3. $A\backslash(B \cup C) \overset{(1)}{=} A \cap C_E(B \cup C) \overset{(2)}{=} A \cap (C_E B \cap C_E C) = (A \cap C_E B) \cap (A \cap C_E C) = (A\backslash B) \cap (A\backslash C)$

4. Let $x_1, x_2 \in E$ such that $g(x_1) = g(x_2)$.

Let $A = \{x_1\}$ and $B = \{x_2\}$.

We have $g(x_1) = g(x_2) \in g(A) \cap g(B) = g(A \cap B)$.

Therefore, $g(A \cap B) \neq \emptyset$, and consequently, $A \cap B \neq \emptyset$.

This implies $x_1 = x_2$.

Exercise 03 (6p)

1)

- f is injective if and only if $\forall n_1, n_2 \in \mathbb{N} : f(n_1) = f(n_2) \Longrightarrow n_1 = n_2$.

  Let $n_1, n_2 \in \mathbb{N}$ such that $f(n_1) = f(n_2)$. Then $n_1 + 1 = n_2 + 1$, which implies $n_1 = n_2$. Thus, f is injective.

- f is not surjective because: $\exists y = 0 \in \mathbb{N}$ such that $\forall n \in \mathbb{N}$, $f(n) \neq y$.
- g is not injective because: $\exists n_1 = 0, n_2 = 1 \in \mathbb{N}$ such that $g(0) = 0 = g(1)$ but $0 \neq 1$.
- g is surjective if and only if: $\forall y \in \mathbb{N}$, $\exists n = y + 1 \in \mathbb{N}$ such that $g(n) = g(y + 1) = y$.

2)

- For any $n \in \mathbb{N}$, $(f \circ g)(n) = f(g(n)) = g(n) + 1 = \begin{cases} 1 & \text{if } n = 0 \\ n & \text{if } n \neq 0 \end{cases}$.
- For any $n \in \mathbb{N}$, $(g \circ f)(n) = g(f(n)) = g(n + 1) = n$.

Exercise 04 (4p)

1) $\mathcal{R}$ is reflexive if $(x, y, z)\mathcal{R}(x, y, z)$. Since $(|x - x| = 0 \leq y - y = 0$ and $z = z)$, we have $\mathcal{R}$ is reflexive.

2) $\mathcal{R}$ is anti-symmetric if $[(x, y, z)\mathcal{R}(a, b, c)$ and $(a, b, c)\mathcal{R}(x, y, z)] \Longrightarrow (x, y, z) = (a, b, c)$. Suppose $(x, y, z)\mathcal{R}(a, b, c)$ and $(a, b, c)\mathcal{R}(x, y, z)$. This implies $[(|x-a| \leq b-y(*)$ and $|a-x| \leq y - b(**))$ and $z = c]$, then $(*) + (**)$ gives $x = a$, replacing $x = a$ in $(*)$ and $(**)$ we find $y = b$.

Therefore, $(x, y, z) = (a, b, c)$, and $\mathcal{R}$ is anti-symmetric.

3) $\mathcal{R}$ is transitive if $(x, y, z)\mathcal{R}(a, b, c)$ and $(a, b, c)\mathcal{R}(\alpha, \beta, \gamma) \Longrightarrow (x, y, z)\mathcal{R}(\alpha, \beta, \gamma)$. Suppose $(x, y, z)\mathcal{R}(a, b, c)$ and $(a, b, c)\mathcal{R}(\alpha, \beta, \gamma)$, this implies $[(|x - a| \leq b - y \quad (*)$ and $|a - \alpha| \leq \beta - b(**))$ and $z = c = \gamma]$. Then $(*) + (**)$ gives $(|x - a| + |a - \alpha| \leq b - y + \beta - b$ and

$z = c = \gamma$), and since ($|x - \alpha| = |x - a + a - \alpha| \leq |x - a| + |a - \alpha| \leq y + \beta$ and $z = \gamma$), we have $(x, y, z)\mathcal{R}(\alpha, \beta, \gamma)$.

Therefore, $\mathcal{R}$ is transitive. From $(1), (2)$, and (3), we can conclude that $\mathcal{R}$ is a partial order relation on $\mathbb{R}^3$.

- $\mathcal{R}$ is not total because $\exists(x, y, z) = (0, 0, 2) \in \mathbb{R}^3$ and $(a, b, c) = (0, 0, 3) \in \mathbb{R}^3$ such that $(0, 0, 2)\mathcal{R}(0, 0, 3)$ and $(0, 0, 3)\mathcal{R}(0, 0, 2)$.

Exercise 05 (4p) Let $f : E \longrightarrow F$ and $g : F \longrightarrow G$ be two arbitrary functions.

1. (If f and g are injective) $\Longrightarrow g \circ f$ is injective.

2. (If f and g are surjective) $\Longrightarrow g \circ f$ is surjective.

3. (If f and g are bijective) $\Longrightarrow ((g \circ f)^{-1} = f^{-1} \circ g^{-1})$.

6.6 Exam 06

Exercise 01 (6p)

I) Let $\mathrm{P}_1, \mathrm{P}_2$, and P_3 be propositions. Prove that:

1. $(\mathrm{P}_1 \vee (\mathrm{P}_2 \wedge \mathrm{P}_3)) \Leftrightarrow ((\mathrm{P}_1 \vee \mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \mathrm{P}_3))$

II) Let $\mathcal{R}$ be an equivalence relation on a set E. Show that:

1. $\forall x, y \in E, \quad x\mathcal{R}y \Longleftrightarrow \bar{x} = \bar{y}$.

2. $\forall x, y \in E, \quad x\mathcal{R}y \Longrightarrow \bar{x} \cap \bar{y} = \emptyset$

Exercise 02 (6p) Let $g : E \longrightarrow F$ be a function. Let A and B be two subsets of F. Show that:

1. $A \backslash B = A \cap C_F B$

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

3. $g^{-1}(A \cup B) = g^{-1}(A) \cup g^{-1}(B)$

4. $g^{-1}(A \cap B) = g^{-1}(A) \cap g^{-1}(B)$

5. $g^{-1}\left(C_F B\right) = C_E g^{-1}(B)$

6. Explicitly determine the set $g^{-1}(A \Delta B)$

Exercise 03 (3p) Consider the groups $(\mathbb{R}, +)$ and $\left(\mathbb{R}_+^*, \times\right)$. Let the function

$$f : \mathbb{R} \longrightarrow \mathbb{R}_+^*$$

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

1. Show that f is a homomorphism from $(\mathbb{R}, +)$ to $\left(\mathbb{R}_+^*, \times\right)$.

2. Calculate $\ker(f)$. What do you conclude?

3. Is f surjective?

Exercise 04 (5p) Let $h : E \longrightarrow F$ be a function. B is a subset of F. Show that

$$\left(B = h\left(h^{-1}(B)\right)\right) \Longleftrightarrow (h \text{ is surjective })$$

6.6.1 Solution

Exercise 01 (5p)

I) $(\mathrm{P}_1 \vee (\mathrm{P}_2 \wedge \mathrm{P}_3)) \Leftrightarrow ((\mathrm{P}_1 \vee \mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \mathrm{P}_3))$.

P_1	P_2	P_3	$(\mathrm{P}_2 \wedge \mathrm{P}_3)$	$\mathrm{P}_1 \vee (\mathrm{P}_2 \wedge \mathrm{P}_3)$	$\mathrm{P}_1 \vee \mathrm{P}_2$	$\mathrm{P}_1 \vee \mathrm{P}_3$	$(\mathrm{P}_1 \vee \mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \mathrm{P}_3)$	$\Longleftrightarrow$
1	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1	1
1	0	1	0	1	1	1	1	1
1	0	0	0	1	1	1	1	1
0	1	1	1	1	1	1	1	1
0	1	0	0	0	1	0	0	1
0	0	1	0	0	0	1	0	1
0	0	0	0	0	0	0	0	1

II)

1) Let $z \in \bar{x}$.

$$z \in \bar{x} \iff x\mathcal{R}z$$
$$(\text{since } x\mathcal{R}y) \iff z\mathcal{R}x$$
$$\iff z\mathcal{R}y$$
$$\iff z \in \bar{y}$$

2) We will prove the contrapositive ($\bar{x} \cap \bar{y} \neq \emptyset \Longrightarrow x\mathcal{R}y$).

$$z \in \bar{x} \cap \bar{y} \Longrightarrow z \in \bar{x} \text{ and } z \in \bar{y}$$
$$\Longrightarrow x\mathcal{R}z \text{ and } z\mathcal{R}y$$
$$\Longrightarrow x\mathcal{R}y$$

Exercise 02 (7p) Let $g : E \longrightarrow F$ be a function. Let A and B be two subsets of F. Show that:

1. $x \in A\backslash B \iff x \in A \wedge x \notin B \iff x \in A \wedge x \in C_F B \iff x \in A \cap C_F B$

2. $x \in C_F(A \cup B) \iff x \in F \wedge (x \notin (A \cup B)) \iff x \in F \wedge (x \notin A \wedge x \notin B) \iff$

$(x \in F \wedge x \notin A) \wedge (x \in F \wedge x \notin B) \iff x \in F\backslash A \wedge x \in F\backslash B \iff x \in C_F A \cap C_F B$

3. $x \in g^{-1}(A \cup B) \iff g(x) \in A \cup B \iff g(x) \in A \vee g(x) \in B$

$\iff x \in g^{-1}(A) \vee x \in g^{-1}(B) \iff x \in g^{-1}(A) \cup g^{-1}(B)$

4. $x \in g^{-1}(A \cap B) \iff g(x) \in (A \cap B) \iff g(x) \in A \wedge g(x) \in B \iff$

$x \in g^{-1}(A) \wedge x \in g^{-1}(B) \iff x \in g^{-1}(A) \cap g^{-1}(B)$

5. $x \in g^{-1}(C_F B) \iff g(x) \in C_F B \iff g(x) \notin B \iff x \notin g^{-1}(B) \iff x \in C_E g^{-1}(B)$

6. $g^{-1}(A\Delta B) = g^{-1}((A\backslash B)\cup(B\backslash A)) \overset{(2)}{=} g^{-1}(A\backslash B)\cup g^{-1}(B\backslash A) \overset{(1)}{=} g^{-1}(A \cap C_F B)\cup g^{-1}(C_F A \cap B)$

$\overset{(3)}{=} (g^{-1}(A) \cap g^{-1}(C_F B))\cup(g^{-1}(C_F A) \cap g^{-1}(B)) \overset{(4)}{=} (g^{-1}(A) \cap C_E g^{-1}(B))\cup(C_E g^{-1}(A) \cap g^{-1}(B))$

$\overset{(4)}{=} (g^{-1}(A) \cap C_E g^{-1}(B))\cup(C_E g^{-1}(A) \cap g^{-1}(B)) \overset{(1)}{=} (g^{-1}(A)\backslash f^{-1}(B))\cup(g^{-1}(B)\backslash g^{-1}(A)) =$

$g^{-1}(A)\Delta g^{-1}(B)$.

Exercise 03 (5p)

1. f is a homomorphism from $(\mathbb{R},+)$ to $\left(\mathbb{R}_+^*,\cdot\right)$.

Let $x_1, x_2 \in \mathbb{R}$. We have $f(x_1+x_2) = 2^{x_1+x_2} = 2^{x_1}\cdot 2^{x_2} = f(x_1)\cdot f(x_2)$.

2.

$$\begin{aligned}\ker(f) &= \{x\in\mathbb{R} : f(x)=1\}\\ &= \{x\in\mathbb{R} : 2^x = 1\}\\ &= \{x\in\mathbb{R} : \ln(2^x) = \ln(1) = 0\}\\ &= \{x\in\mathbb{R} : x\ln(2) = 0\}\\ &= \{x\in\mathbb{R} : x = 0\}\\ &= \{0\}\end{aligned}$$

Therefore, f is injective.

3. f is surjective because:

$$\forall y\in\mathbb{R}_+^*, \exists x = \tfrac{\ln(y)}{\ln(2)} \in \mathbb{R} : f(x) = f\left(\tfrac{\ln(y)}{\ln(2)}\right) = 2^{\frac{\ln(y)}{\ln(2)}} = e^{\ln\left(2^{\ln(y)}\ln(2)\right)} = e^{\frac{\ln(y)}{\ln(2)}\ln(2)} = e^{\ln(y)} = y$$

Exercise 04 (3p)

1) $(B = h(h^{-1}(B))) \Longrightarrow (h$ is surjective) Suppose $B = h(h^{-1}(B))$ for any subset B of F.

$[(h$ is surjective $) \Longleftrightarrow (h(E) = F)]$ We have $h(E)\subset F$ because h is a function, and it remains to show that $F\subset h(E)$. According to the proposition, we have $F = h(h^{-1}(F))$, but $h^{-1}(F)\subset E$, so $h(h^{-1}(F))\subset h(E)$, and therefore $F\subset h(E)$.

2) (h is surjective) $\Longrightarrow (B = h(h^{-1}(B)))$ Suppose h is surjective, and we need to show that $B = h(h^{-1}(B))$:

(i) $B\subset h(h^{-1}(B))$, let $y\in B$ then $\exists x\in E$ such that $h(x) = y$ (since h is surjective), so $h(x)\in B \Longrightarrow x\in h^{-1}(B) \Longrightarrow h(x)\in h(h^{-1}(B)) \Longrightarrow y\in h(h^{-1}(B))$

(ii) $h(h^{-1}(B))\subset B$, let $y\in h(h^{-1}(B))$ then $\exists x\in h^{-1}(B)$, $h(x) = y$ so $h(x) = y\in B$.

6.7 Exam 07

Exercise 01 (4p)

1) Let $n \in \mathbb{N}$. Prove by cases that $n(n^2+2)$ is a multiple of 3.

2) Prove by contradiction that $(\forall n \in \mathbb{N}^*, \exists p \in \mathbb{N}^* : n = p^2) \Rightarrow (\forall q \in \mathbb{N}^* : 2n \neq q^2)$.

Exercise 02 (6p)

1. Solve the equation $-x^2 + x = 0$ in $\mathbb{R}$.

2. For each $a \in \mathbb{R}$, solve the equation $-x^2 + x - a = 0$ in $\mathbb{R}$.

3. Let $f : \mathbb{R} \to \mathbb{R}'$ be a function defined by: For all $x \in \mathbb{R}$, $f(x) = x(1-x)$. Is f injective? Is f surjective?

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

Exercise 03 (4p)

Let $\mathcal{R}$ be the relation defined on $\mathbb{Z}$ as:

$$\forall a, b \in \mathbb{Z} \quad : a\mathcal{R}b \Leftrightarrow (a - b \text{ is divisible by 2 or by 3})$$

• Study the reflexivity, symmetry, antisymmetry, and transitivity of $\mathcal{R}$. Conclude.

Exercise 04 (6p)

Let $*$ be the composition law defined on $\mathbb{R}$ as: $\forall x, y \in \mathbb{R} : x * y = x + y + \frac{1}{10}$.

1. Show that $(\mathbb{R}, *)$ is an abelian group.

2. Show that the function g defined as: $g(x) = 5x + \frac{1}{2}$ is a homomorphism from the group $(\mathbb{R}, *)$ to the group $(\mathbb{R}, +)$.

3. Let $H = \left\{\frac{2n-1}{10}, n \in \mathbb{Z}\right\}$. Show that $(H, *)$ is a subgroup of $(\mathbb{R}, *)$.

6.7.1 Solution

Exercise01 (4p)

1) Let $n \in \mathbb{N}$. We have:

$\underline{1^{\text{st}}\ \textbf{case}}$: If $n = 3k$, with $k \in \mathbb{N}$, then $n(n^2+2) = 3k((3k)^2+2)$, which is a multiple of 3.

$\underline{2^{\text{nd}}\ \textbf{case}}$: If $n = 3k+1$, with $k \in \mathbb{N}$, then $n(n^2+2) = (3k+1)((3k+1)^2+2) = (3k+1)(9k^2+6k+1+2)$

$= 3(3k+1)(3k^2+2k+1)$ which is a multiple of 3

.

$\underline{3^{\text{rd}}\ \textbf{case}}$: If $n = 3k+2$, with $k \in \mathbb{N}$, then

$$\begin{aligned} n(n^2+2) &= (3k+2)((3k+2)^2+2) = (3k+2)(9k^2+12k+4+2) \\ &= 3(3k+2)(3k^2+4k+2) \text{ which is a multiple of 3.} \end{aligned}$$

Therefore, in all cases, $n(n^2+2)$ is a multiple of 3.

2) Suppose that $(\forall n \in \mathbb{N}^*, \exists p \in \mathbb{N}^* : n = p^2)$ and $(\exists q \in \mathbb{N}^* : 2n = q^2)$.

Let $n \in \mathbb{N}^*$, then $n = p^2$ and $2n = q^2$ with $p, q \in \mathbb{N}^*$, so $2p^2 = q^2$, which implies $\sqrt{2} = \frac{q}{p} \in \mathbb{Q}$, which is absurd since $\sqrt{2}$ is irrational.

Exercise02 (6p)

1) $-x^2 + x = 0 \Leftrightarrow x(1-x) = 0 \Leftrightarrow (x = 0 \text{ or } x = 1)$, so the set of solutions is $S = \{0, 1\}$.

2) $-x^2 + x - a = 0$ is a quadratic equation, let's calculate its discriminant: $\Delta = 1 - 4a$

If $a > \frac{1}{4}$, then $\Delta < 0$, so there are no solutions in $\mathbb{R}$.

If $a \leq \frac{1}{4}$, then $\Delta \geq 0$, so we have the solutions: $x_1 = \frac{1+\sqrt{1-4a}}{2}$ and $x_2 = \frac{1-\sqrt{1-4a}}{2}$.

3) From 1), we have: $f(1) = f(0)$ but $1 \neq 0$, so f is not injective.

From 2), we have: $y = 1$ has no pre-image, so f is not surjective.

4.1) Let $x_1, x_2 \in \left[\frac{1}{2}, +\infty\right[$:

$$g(x_1) = g(x_2) \Rightarrow x_1(1-x_1) = x_2(1-x_2) \Rightarrow x_1 - x_2 = {x_1}^2 - {x_2}^2$$

$$\Rightarrow x_1 - x_2 = (x_1 - x_2)(x_1 + x_2) \Rightarrow (x_1 - x_2)(x_1 + x_2 - 1) = 0$$

$$\Rightarrow (x_1 - x_2 = 0) \text{ or } (x_1 + x_2 - 1 = 0) \Rightarrow (x_1 = x_2) \text{ or } (x_1 = 1 - x_2)$$

$$\Rightarrow (x_1 = x_2) \text{ or } \left(x_1 = x_2 = \frac{1}{2}\right), \text{ because } 1 - x_2 \geq \frac{1}{2} \Rightarrow x_2 \leq \frac{1}{2} \Rightarrow x_2 = \frac{1}{2}$$

$$\Rightarrow x_1 = x_2$$

Therefore, g is injective.

4.2) Let $y \in]-\infty, \frac{1}{4}]$. According to 2), the equation $g(x) = y$ has at least one solution x in $\mathbb{R}$.

We have $x_1 - \frac{1}{2} = \frac{1+\sqrt{1-4y}}{2} - \frac{1}{2} = \frac{\sqrt{1-4y}}{2} \geq 0$ which implies $x_1 \geq \frac{1}{2}$.

and $x_2 - \frac{1}{2} = \frac{1-\sqrt{1-4y}-1}{2} = \frac{-\sqrt{1-4y}}{2} \leq 0$ which implies $x_2 \leq \frac{1}{2}$.

Therefore, we can take $x = \frac{1+\sqrt{1-4y}}{2} \in \left[\frac{1}{2}, +\infty\right[$, to have $y = g(x)$.

Hence, g is surjective.

Therefore, g is bijective.

Exercice03 (4p)

1) Let $a \in \mathbb{Z}$. We have $a - a = 0$ which is divisible by 2 or by 3, i.e., $a\mathcal{R}a$.

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

2) Let $a, b \in \mathbb{Z}$. We have:

$a\mathcal{R}b \Rightarrow a - b$ is divisible by 2 or by 3

$\Rightarrow b - a$ is divisible by 2 or by 3

$\Rightarrow b\mathcal{R}a$

Therefore, $\mathcal{R}$ is symmetric.

3) For example, $(6 - 3)$ is divisible by 2 or by 3, and $(3 - 6)$ is divisible by 2 or by 3, but $(3 \neq 6)$.

This means that there exist $a, b \in \mathbb{Z}$ such that $a\mathcal{R}b$, $b\mathcal{R}a$, and $a \neq b$.

Therefore, $\mathcal{R}$ is not antisymmetric.

4) For example, $(6-3)$ is divisible by 2 or by 3, $(3-1)$ is divisible by 2 or by 3, but $(6-1)$ is not divisible by 2 or by 3.

This means that there exist $a, b, c \in \mathbb{Z}$ such that $a\mathcal{R}b$, $b\mathcal{R}_c$, and $\overline{a\mathcal{R}_c}$.

Therefore, $\mathcal{R}$ is not transitive.

From the above observations, we conclude that $\mathcal{R}$ is neither a relation of order nor a relation of equivalence.

Exercice04 (6p)

1.1) Let $x, y \in \mathbb{R}$. We have $x + y + \frac{1}{10} \in \mathbb{R}$, which means $x * y \in \mathbb{R}$.

Therefore, $*$ is an internal law in $\mathbb{R}$.

1.2) Let $x, y \in \mathbb{R}$. We have:

$x * y = x + y + \frac{1}{10} = y + x + \frac{1}{10} = y * x$

Therefore, $*$ is a commutative law.

1.3) Let $x, y, z \in \mathbb{R}$. We have:

$(x * y) * z = \left(x + y + \frac{1}{10}\right) * z = x + y + \frac{1}{10} + z + \frac{1}{10} = \left(x + \left(y + z + \frac{1}{10}\right) + \frac{1}{10}\right) =$
$\left(x + (y * z) + \frac{1}{10}\right) = x * (y * z)$

Therefore, $*$ is associative.

1.4) Let's find $e \in \mathbb{R}$ such that for all $x \in \mathbb{R}$, $x * e = e * x = x$.

We have: $x * e = x \Leftrightarrow x + e + \frac{1}{10} = x \Leftrightarrow e = -\frac{1}{10}$

Since $-\frac{1}{10} \in \mathbb{R}$ and $*$ is commutative, $e = -\frac{1}{10}$ is the neutral element of the law $*$.

1.5) Let $x \in \mathbb{R}$. We are looking for $x' \in \mathbb{R}$ such that $x * x' = x' * x = -\frac{1}{10}$.

We have: $x * x' = -\frac{1}{10} \Leftrightarrow x + x' + \frac{1}{10} = -\frac{1}{10} \Leftrightarrow x' = -x - \frac{1}{5}$

Since $-x-\frac{1}{5}\in\mathbb{R}$ and $*$ is commutative, $x'=-x-\frac{1}{5}$ is the inverse of x with respect to the law $*$.

Therefore, $(\mathbb{R},*)$ is an abelian group.

2) Let $x,y\in\mathbb{R}$. We have:

$g(x*y)=g\left(x+y+\frac{1}{10}\right)=5\left(x+y+\frac{1}{10}\right)+\frac{1}{2}=5x+5y+\frac{1}{2}+\frac{1}{2}=\left(5x+\frac{1}{2}\right)+\left(5y+\frac{1}{2}\right)=g(x)+g(y)$.

Therefore, g is a homomorphism from the group $(\mathbb{R},*)$ to the group $(\mathbb{R},+)$.

3) We have: $e=-\frac{1}{10}=\frac{2(0)-1}{10}\in H$.

Let $x,y\in H$. Then $\exists n,m\in\mathbb{Z}$ such that $x=\frac{2n-1}{10}$ and $y=\frac{2m-1}{10}$. We have:

$$x*y^{-1}=x*\left(-y-\frac{1}{5}\right)=\left(\frac{2n-1}{10}\right)*\left(-\frac{2m-1}{10}-\frac{1}{5}\right)=\left(\frac{2n-1}{10}\right)*\left(\frac{-2m-1}{10}\right)=\frac{2n-1}{10}+\frac{-2m-1}{10}+\frac{1}{10}$$
$$=\frac{2(n-m)-1}{10}\in H,\ \text{since } n-m\in\mathbb{Z}.$$

Therefore, $(H,*)$ is a subgroup of $(\mathbb{R},*)$.

bibliography

[**1**] J. Franchini et J. C. Jacquens, Algèbre : cours, exercices corrigés, travaux dirigés, Ellipses, Paris, 1996.

[**2**] C. Degrave et D. Degrave, Algèbre 1ère année : cours, méthodes, exercices résolus, Bréal, 2003.

[**3**] S. Balac et F. Sturm, Algèbre et analyse : cours de mathématiques de première année avec exercices corrigés„ Presses Polytechniques et Universitaires romandes, 2003

[**4**] M. Gran, fiches de TD (L1), Université du Littoral Côte d'Opale.

[**5**] M. Serfati, Exercices de mathématiques. 1. Algèbre, Belin, Collection DIA, 1987.

[**6**] D. Duverney, S. Heumez, G. Huvent, Toutes les mathématiques – Cours, exercices corrigés – MPSI, PCSI, PTSI, TSI, Ellipses, 2004.