Algebra 1

Mathematical logic •
Set theory •
Mappings •
Binary relations •
Algebraic structures •
Polynomial rings •

Level: First Year / Mathematics, Computer Sciences

Academic year: 2024-2025

author: F. SACI

email: f.saci@univ-skikda.dz

20 août 1955 - Skikda University, ALGERIA

Preface

This course is designed primarily for first-year students in Mathematics and Computer Science under the LMD system. The primary goal is to develop a fundamental understanding and skills necessary for working with mathematical expressions, equations, and functions.

This comprehensive course provides a solid foundation in key mathematical concepts, covering logic, set theory, binary relations, mappings, algebraic structures, and rings of polynomials. It starts with Chapter 1: Logic Concepts, where students learn about logical operators, quantifiers, and proof methods. Chapter 2: Sets introduces set theory, including set operations and applications. Chapter 3: Binary Relations explores reflexive, symmetric, transitive, and equivalence relations. Chapter 4: Mappings delves into injective, surjective, and bijective functions. Chapter 5: Algebraic Structures covers groups, rings, and fields, while Chapter 6: Rings of Polynomials focuses on the structure and applications of polynomial rings, particularly in algebraic geometry. This progression equips students with the foundational knowledge required for advanced mathematical studies.

Contents

Chapter 1

Mathematical logic

Contents

In this chapter, we will introduce the foundational elements of classical logic. Logic is the systematic study of arguments. It helps us understand how to draw conclusions from given information by examining the principles of reasoning. Logic is a branch of philosophy that focuses on the structure of arguments. By analyzing arguments, logic shows us whether conclusions logically follow from the premises, helping us evaluate the strength of an argument.

1 Statements and Propositional calculus

In mathematics, we focus on determining the truth or falsity of statements involving mathematical objects.

Definition 1.1. *A statement is a mathematical expression which is either true or false, and it cannot be true and false at the same time. We usually denote it by p, q, r (propositional variables).*

Example 1.1.

1. 34043 *is the sum of two square integers.*

2. *It is raining today in Skikda.*

3. $3 + 4 = 9$

4. *The square root of* 2 *is not a rational number.*

Some of these statements are true and some are false, but each has a well-defined truth value, even if we don't know what it is. On the other hand, something like "n is even" is not a proposition, because it doesn't have a truth value until we know what n is.

2 Truth tables

Let's start with giving truth values to propositional variables. Here and elsewhere 1 means true and 0 means false. for other references, the symbols T and F can be found to indicate both correctness and error, respectively, and the corresponding table is called the truth table for the Proposition p.

p
1
0

For two propositions p and q, the table is as follows:

p	q
1	1
1	0
0	1
0	0

In the case of three statements p, q and r, the truth table has the form:

p	q	r
1	1	1
1	1	0
1	0	1
1	0	0
0	1	1
0	1	0
0	0	1
0	0	0

3 Logical connectives

3.1 Conjunction

Definition 3.1. *The logical connective "**and**" is used to combine two statements. The conjunction of statement p and statement q is written as "p and q". The symbol $\wedge$ represents "and". Thus, "$p \wedge q$" also denotes the conjunction of p and q.*

The conjunction $p \wedge q$ is true only when both p and q are true. Otherwise, it is false.

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

Example 3.1.

1. *The sky is blue **and** it is sunny.*
2. *34043 is a multiple of* 3 ***and*** *34043 is divisible by 17.*
3. *Al quds is the capital of Palestine **and** Algeriais the largest country in Africa.*

3.2 Disjunction

Definition 3.2. *A disjunction is a statement involving "**or**". For two statements p and q, it is written as "p or q". The symbol $\vee$ represents "or". Thus, "$p \vee q$" also denotes the disjunction of "p" and "q".*

The statement $p \vee q$ is false only when "p" and "q" are false (i.e. $p \vee q$ is true if at least one of the two statements is true).

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

Example 3.2.

1. *Sun rises from the east **or** sun rises from the west.*
2. *34043 is a sum of two squares **or** 34043 is divisible by 17.*

3.3 Negation

Definition 3.3. *Usually **not** is used at a suitable place in a statement to obtain the negation of the statement. The negation of a statement "p" is denoted by $\neg p$ or $\bar{p}$.*

The negation of a true statement is false and that of a false statement is true.

p	$\bar{p}$
1	0
0	1

Remark 3.1. *For every statement p we have $\bar{\bar{p}} = p$.*

Example 3.3.

1. *The negation of the proposition $p \wedge q$ is $\bar{p} \vee \bar{q}$.*
2. *The negation of the proposition $p \vee q$ is $\bar{p} \wedge \bar{q}$.*
3. *The negation of the proposition "5 is a prime number and 2 is an odd number" is "5 is not a prime number or 2 is an even number.*

Exercise 3.4.
a) For any statement p, check if

1. *$p \vee \bar{p}$ is always a true statement.*

2. *$p \wedge \bar{p}$ is always a false statement.*

b) For every two statements p and q, prove that

1. *$(p \wedge \bar{p}) \wedge q$ is impossible.*

2. *$(p \vee \bar{p}) \vee q$ represents always a true statement*

3. *$(p \vee \bar{p}) \wedge q$ has the same truth value as q.*

3.4 Implication

Definition 3.4. *A statement of the form "p implies q" (in symbol $p \Rightarrow q$) is called an implication. The statement $p \Rightarrow q$ and the statement "If p, then q" are logically same, p is called the antecedent or the hypothesis, and q is called the consequent or the conclusion.*

The statement formula "If p, then q" $(p \Rightarrow q)$ is false in only one case when p is true but q is false. Hence the truth table is as follows:

p	q	$p \Rightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

Example 3.5. *To comfirm the third line of the previous table, which may seem strange, we have*

$$(p) : \forall n \in \mathbb{N}^* : \quad \frac{1}{n} + \frac{1}{n} = 2n$$
$$(q) : \quad 1 + 1 = 2.$$

It seems clear that the statement p is false and q is true and the implication $p \Rightarrow q$ is true.

Remark 3.2.

The two statements $(p \Rightarrow q)$ and $(\bar{p} \vee q)$ have the same truth values.

p	q	$\bar{p} \vee q$
1	*1*	*1*
1	*0*	*0*
0	*1*	*1*
0	*0*	*1*

Therefore, the statement $(\bar{p} \vee q)$ is called an implication and is written in the form $(p \Rightarrow q)$.

Exercise 3.6. *Identify the truth value of the following statements:*

1. $(2 > 3) \Rightarrow (4 + 5 = 8)$ $\quad (p_1)$
2. $(2 > 3) \Rightarrow (4 + 5 = 9)$ $\quad (p_2)$
3. $(2 < 3) \Rightarrow (4 + 5 = 8)$ $\quad (p_3)$
4. $(2 < 3) \Rightarrow (4 + 5 = 9)$ $\quad (p_4)$

Solution 3.7. 1. (p_1) *is true statement.*

2. (p_2) *is true statement.*
3. (p_3) *is false statement.*
4. (p_4) *is true.*

Remark 3.3.

1. *If P, Q, and R denote three statements, then the composite statement ($P \Rightarrow Q$ and $Q \Rightarrow R$) is written as*
$$(P \Rightarrow Q \Rightarrow R)$$
2. *The implication $Q \Rightarrow P$ is called the converse of $P \Rightarrow Q$.*

3.5 Equivalence

Definition 3.5. *A statement of the form "p if and only if q" (briefly p iff q) is called an equivalence. p implies and implied by q (in symbol $p \Leftrightarrow q$). We also express it by saying that p is a necessary and sufficient condition for q.*

The statement $p \Leftrightarrow q$ is the conjunction of the statement $p \Rightarrow q$ and the statement $q \Rightarrow p$. Thus, the truth table for the equivalence is as follows:

p	q	$p \Leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

Remark 3.4. *We note that $p \Leftrightarrow q$ is true if p and q have the same truth values.*

Properties

For all statements p, q and r it can be shown that

1. $\bar{\bar{p}} \Leftrightarrow p$
2. $p \wedge p \Leftrightarrow p$
3. $p \vee p \Leftrightarrow p$
4. $\wedge$ commutative: $p \wedge q \Leftrightarrow q \wedge p$
5. $\vee$ commutative: $p \vee q \Leftrightarrow q \vee p$
6. $\wedge$ associative: $[(p \wedge q) \wedge r] \Leftrightarrow [p \wedge (q \wedge r)]$
7. $\vee$ associative: $[(p \vee q) \vee r] \Leftrightarrow \vee(q \vee r)]$
8. distributivity of $\wedge$ over $\vee$: $[p \wedge (q \vee r)] \Leftrightarrow [(p \wedge q) \vee (p \wedge r)]$
9. distributivity of $\vee$ over $\wedge$: $[p \vee (q \wedge r)] \Leftrightarrow [(p \vee q) \wedge (p \vee r)]$
10. Morgan's laws $[(\overline{p \wedge q}) \Leftrightarrow (\bar{p} \vee \bar{q})]$ and $[(\overline{p \vee q}) \Leftrightarrow (\bar{p} \wedge \bar{q})]$

Remark 3.5.

If P, Q, and R denote three statements, then the composite statement ($P \Leftrightarrow Q$ and $Q \Leftrightarrow R$) is written as

$$(P \Leftrightarrow Q \Leftrightarrow R)$$

Definition 3.6.

1. *A compound logical statement that is always true, regardless of the truth values of the statements it is composed of, is called a **Tautology**.*
2. *A compound logical statement that is always false, regardless of the truth values of the statements it is composed of, is called a **Contradiction**.*
3. *Two compound logical statements p and q are called logically equivalent if the*

logical statement $p \Leftrightarrow q$ is a tautology.

Example 3.8.

- *$p \vee \bar{p}$ is a tautology.*
- *$p \wedge \bar{p}$ is a contradiction.*

4 Quantifiers

Definition 4.1. *Universal Quantifier Consider the statement "For every river, there is an origin". This can be rewritten as "For every x, x is a river" implies "x has an origin". More generally, we have a statement of the form "For every x, $P(x)$", where $P(x)$ is a valid statement involving x. The symbol "$\forall$" is used for "**for every**", and it is called the **Universal quantifier**.*

Definition 4.2. *Existential Quantifier Consider the statement "There is a man who is immortal". More generally, we have statements of the form "There exists x, $P(x)$", where $P(x)$ is a statement involving x. The symbol "$\exists$" stands for "there exists", and it is called the **Existential quantifier**.*

Remark 4.1. *The order of the quantifiers is very important when presenting any statement.*

Example 4.1.

- $\forall x \in \mathbb{R}^*, \exists y \in \mathbb{R}^* : \ xy = 1$ *is true.*
- $\exists x \in \mathbb{R}^*, \forall y \in \mathbb{R}^* : \ xy = 1$ *is false.*

4.1 The rules of negation for a quantified proposition

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

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

2. The negation of "it exists an element x of E for which the statement $P(x)$ is true" is "for every element x of E, the statement $P(x)$ is false".

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

Example 4.2.

1. *The negation of* $(\forall x \in [0, +\infty[: \ x^3 > 3)$ *is* $(\exists x \in [0, +\infty[: \ x^3 \leq 3)$.
2. *The negation of* $(\exists z \in \mathbb{C} : \ z^2 - z + 1 = 0)$ *is* $(\forall z \in \mathbb{C} : \ z^2 - z + 1 \neq 0)$.

5 Proof Techniques

Mathematical reasoning builds conclusions from accepted premises through logical rules. We can now systematically examine the various proof techniques used to establish mathematical propositions. Each method provides a different approach for constructing valid arguments from initial truths to proven conclusions.

Definition 5.1. *An **axiom** is a proposition that is assumed to be true.*

Definition 5.2. *A **proof** is a method for establishing the truth of a statement.*

5.1 Direct Proof (Proof by Construction)

In a constructive proof one attempts to demonstrate $p \Rightarrow q$ directly. This is the simplest and easiest method of proof available to us. There are only two steps to a direct proof (the second step is, of course, the tricky part):

1. Assume that p is true.
2. Use p to show that q must be true.

Example 5.1.
If a and b are consecutive integers, then their sum $a + b$ is odd.

Assume that a and b are consecutive integers. Because a and b are consecutive we know that $b = a + 1$. Thus, the sum $a + b$ may be re-written as $2a + 1$. Thus, there exists a number k such that $a + b = 2k + 1$ so the sum $a + b$ is odd.

Exercise 5.2. *Using direct reasoning prove the following*

1. $\forall x, y \in \mathbb{R}^+$, *such that* $x \leq y$:

$$x \leq \frac{x+y}{2} \leq y \quad \text{and} \quad x \leq \sqrt{xy} \leq y$$

2. $x \in \mathbb{Q}$ *and* $y \in \mathbb{Q} \Rightarrow x + y \in \mathbb{Q}$.
3. $\forall n \in \mathbb{N}$: n *is odd* $\Rightarrow n^2$ *is odd.*

5.2 Proof by Contradiction

We use this technique to demonstrate $p \Rightarrow q$ by assuming both p and $\bar{q}$ are simultaneously true and deriving a contradiction. When we derive this contradiction it means that one of our assumptions was untenable. Presumably we have either assumed or already proved P to be true so that finding a contradiction implies that $\bar{q}$ must be false. The method of proof by contradiction.

1. Assume that p is true.
2. Assume that $\bar{q}$ is true.
3. Use p and $\bar{q}$ to demonstrate a contradiction.

Remark 5.1. *A proof by contradiction begins by assuming the negation of what we want to prove. Through logical deduction, we derive a contradiction (such as 1 = 2 or $3 > 5$,...). Since this contradiction is impossible, the initial assumption must be false, which means the original statement must be true.*

Example 5.3.
If a and b are consecutive integers, then the sum $a + b$ is odd.

Assume that a and b are consecutive integers. Assume also that the sum $a + b$ is not odd. Because the sum $a + b$ is not odd, there exists no number k such that $a + b = 2k + 1$. However, the integers a and b are consecutive, so we may write the sum $a + b$ as $2a + 1$. Thus, we have derived that $a + b \neq 2k + 1$ for any integer k and also that $a + b = 2a + 1$. This is a contradiction. If we hold that a and b are consecutive then we know that the sum $a + b$ must be odd.

Exercise 5.4. *Prove by contradiction that:*

1. $\sqrt{2}$ *is irrational.*
2. $\forall a, b \in \mathbb{R}^+ : \frac{a}{1+b} = \frac{b}{1+a} \Rightarrow a = b$

5.3 Proof by Induction

Proof by induction is a very powerful method in which we use recursion to demonstrate an infinite number of facts in a finite amount of space. The most basic form of mathematical induction is where we first create a propositional form whose truth is determined by an integer function. If we are able to show that the propositional form is true for some integer value then we may argue from that basis that the propositional form must be true for all integers.

1. Show that a propositional form $P(n)$ is true for simple case.
2. Assume that $P(n)$ is true for some n, and show that this implies that $P(n + 1)$ is true.
3. Then, by the principle of induction, the propositional form $P(n)$ is true for all n greater or equal to the basis case.

Exercise 5.5. *Prove that the sum of the first n positive integers is given by*

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

Solution 5.6.
First, we need to verify the formula for $n = 1$. If $n = 1$, we get

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

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

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

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

This assumption is called the inductive hypothesis.
We need to show that if the formula holds for $n = k$, then it also holds for $n = k + 1$.
Consider the sum of the first $k + 1$ positive integers

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

Using the inductive hypothesis, we can write

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

The right-hand side may be simplified as

$$\begin{aligned} \frac{k(k+1)}{2} + (k+1) &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

Exercise 5.7. *Prove that:* $\forall x \in \mathbb{R}^*$*:* $\sum_{k=0}^{n} r^k = \frac{r^{n+1} - 1}{r - 1}$.

5.4 Proof by Contrapositive

Proof by contraposition is a method of proof which is not a method all its own. From first-order logic we know that the implication $p \Rightarrow q$ is equivalent to $\bar{q} \Rightarrow \bar{p}$. The second proposition is called the contrapositive of the first proposition. By saying that the two propositions are equivalent we mean that if one can prove $p \Rightarrow q$ then they have also proved $\bar{q} \Rightarrow \bar{p}$, and vice versa.

Exercise 5.8. *Let P and Q be two propositions. Show that $(P \Rightarrow Q)$ is equivalent to $(\neg Q \Rightarrow \neg P)$.*

Solution 5.9. *We will use a truth table to prove 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, $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$.

Exercise 5.10. *Prove that: n^2 is even $\Rightarrow$ n is even.*

Solution 5.11. *Suppose n is not even (n is odd). The product of two odd numbers is odd, hence $n^2 = n.n$ is odd. Thus n^2 is not even.*
Furthermore, if n^2 is even, n has to be even.

Exercise 5.12. *Show by contrapositive that*

1. *$\forall x, y \in \mathbb{R}$, if $x + y > 1$, then $x > \frac{1}{2}$ or $y > \frac{1}{2}$.*
2. *$\forall x, y \in \mathbb{Z}$, if $y \neq 0$, then $x + y\sqrt{2} \notin \mathbb{Q}$.*

5.5 Proof by Cases

The idea behind the proving method is that we break the proof into smaller, more manageable conditions and prove that the overall claim holds for every case.

$$[(p \vee q) \Rightarrow r] \Leftrightarrow [(p \Rightarrow r) \wedge (q \Rightarrow r)]$$

Exercise 5.13. *Prove that for every integer n, $n^2 \geq n$.*

Solution 5.14. *Let $p(n) : n^2 \geq n$. We have three different cases:*
$n \leq -1, n = 0$ and $n \geq 1$.

1. *If $n = 0$:*
   notice that $0^2 \geq 0$, so $p(0)$ holds when $n = 0$.
2. *If $n \geq 1$:*
   the multiplication of both sides by the positive value n yields $n^2 \geq n$
   So, $p(n)$ holds in this case.
3. *If $n \leq -1$:*
   Since $n \leq -1$ and $n^2 \geq 0$, $p(n)$ clearly holds in this case.

Exercise 5.15. *Using case-by-case reasoning prove that*

1. *$\forall n \in \mathbb{N} : n^2 + n + 1$ is an odd number.*
2. *$\forall x \in \mathbb{R} : |x - 1| \leq x^2 - x + 1$.*

5.6 Proof by Counterexample

This proof structure allows us to prove that a statement is not true by providing an example where it does not hold.

Exercise 5.16. *Prove that $(a+b)^2 = a^2 + b^2$ is not an algebraic identity, where $a, b \in \mathbb{R}$.*

Solution 5.17. *We need to find specific real numbers a and b for which the equation is false.*
If $a = 1$ and $b = 2$, then

$$(a + b)^2 = (1 + 2)^2 = 9, \quad \text{while } 1^2 + 2^2 = 5$$

So if $a = 1$ and $b = 2$, then $(a+b)^2 \neq a^2 + b^2$, and hence the statement is not an identity.

Exercise 5.18. *Using reasoning by counterexample, prove that the following propositions are false.*

1. *The sum of two odd numbers is odd.*
2. *Any integer n divisible by 2 and by 6 is divisible by 12.*
3. $\forall x \in \mathbb{R}^+ :\ x^2 + \sqrt{x} > 2$.

Tutorial Sheet 01

Exercise 1:

Using truth table, show the follwing relations:

1. $\overline{(p \wedge q)} \Leftrightarrow (\bar{p} \vee \bar{q})$
2. $\overline{(p \vee q)} \Leftrightarrow (\bar{p} \wedge \bar{q})$
3. $[p \vee (q \wedge \bar{q})] \Leftrightarrow p$
4. $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
5. $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$

Exercise 2:

a) Prove that the follwing is true without using a truth table

1. $p \Rightarrow (q \Rightarrow r) \Leftrightarrow (p \wedge q) \Rightarrow r$.
2. $p \Rightarrow q \Leftrightarrow \bar{q} \Rightarrow \bar{p}$.
3. $\overline{(p \Rightarrow q)} \Leftrightarrow (p \wedge \bar{q})$

b) Let the logical operator f defined by its truth table as:

p	q	$f(p,q)$
1	1	0
1	0	1
0	1	0
0	0	0

1. Prove that $f(p,q) = p \wedge \bar{q}$.
2. Is f associative?

Exercise 3:

Considering the statements:
p: It is raining
q: The weather is humid.
which of the following propositions are logically equivalent? Justify your answer!

i. If it is not raining then the weather is not humid.

ii. It is raining iff the weather is humid.

iii. It is not true that it is not raining or the weather is humid.

iv. It is raining but the weather is not humid.

v. The weather is humid only if it is raining.

Exercise 4:

a) Let the statements
p : Jupiter is a planet.
q : India is an island.
Give verbal sentence describing each of the following statements: $\bar{p}$, $p \vee \bar{q}$, $\bar{p} \vee q$, $p \Rightarrow q$, $p \Leftrightarrow q$
b) Determine the truth value of each of the following statements:

1. If $5+6=2$, then Algeria is the largest country in Africa and the Arab world.
2. China is in Europe or $\sqrt{3}$ is an integer.
3. It is not true that $5+5=9$ or Earth is a planet
4. 11 is a prime number and all the sides of a rectangle are equal.

Exercise 5:

If $A=\{3,4,6,8\}$, determine the truth value of each of the following:

i. $\exists x \in A$, such that $x+4=7$.
ii. $\forall x \in A$, $x+4<10$.
iii. $\forall x \in A$, $x+5 \geq 13$.
iv. $\exists x \in A$, such that x is odd.
v. $\exists x \in A$, such that $(x-3) \in \mathbb{N}$.

Exercise 6:

Write the negation of the following statements:

- $(p \wedge q) \Longrightarrow r$
- $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}\ x+y>0$
- $\forall \varepsilon \in \mathbb{R}_+^*, \exists \alpha \in \mathbb{R}_+^* :\ |x|<\alpha \Longrightarrow |x^2|<\varepsilon$.

Exercise 7:

Using mathematical proof techniques, determine whether the following propositions are true or false:

1. If $(x+1)(y-1)=(x-1)(y+1)$ then $x=y$, for all $x,y \in \mathbb{R}$.
2. Prove that: $\forall n \in \mathbb{N}$: n^3-n is a multiple of 2.
3. Prove that: $\forall n \in \mathbb{N}$: $2^0+2^1+\cdots+2^n=2^{n+1}-1$.
4. Prove that: $\forall x,y \in \mathbb{R}$: $x.y \leq \dfrac{x^2+y^2}{2}$.
5. Prove that: $\forall x \in \mathbb{R}$, $x<2 \Rightarrow x^2<4$.

Chapter 2

Set theory

Contents

1 Basic Concepts

A set is any well-defined list or collection of **distinct** and **unordered** objects, it is usually denoted by capital letters $A, B, X, Y, ...$ The objects comprising the set are called its elements and denoted by lower case letters $a, b, x, y, ...$
The statement "x is an element of A" or equivalently, "x belongs to A" is written $x \in A$, its negation is $x \notin A$.

Example 1.1. *Natural numbers* ($\mathbb{N}$)*, Integers* ($\mathbb{Z}$)*, Rational numbers* ($\mathbb{Q}$)*, real numbers* ($\mathbb{R}$)*, Complex numbers* ($\mathbb{C}$) *are* ***sets*** *of numbers.*

Example 1.2. *The letters of the word "Palestine" define the* ***set***

$$A = \{p, a, l, e, s, t, i, n, e\}$$

Example 1.3. *The elements satisfying a specific relation can be considered as a set:*

$$E = \{x \in \mathbb{R} : \ 0 \leq x \leq 1\} = [0, 1]$$

$$F = \{z \in \mathbb{C} : \ |z|^2 = 2\}$$

Definition 1.1 (The cardinal)**.** *The cardinal of a finite set is a non-negative integer that represents the number of elements (it quantifies the size of the set).*

Example 1.4.

1. *For the set* $A = \{-1, 2, 5, 8, 9\}$*, we write* $card(A) = 5$*.*
2. $card(\mathbb{N}) = +\infty$

Definition 1.2 (The empty set)**.** *The empty set, often denoted as* Φ *or* $\{\}$*, is a set that contains no elements (i.e* $card(\Phi) = 0$*).*

Definition 1.3 (The set of subsets)**.** *The set of subsets, also known as the "power set", of a given set* E *is the collection of all possible subsets of* E*. It is denoted by* $\mathcal{P}(E)$*, if* E *is finite then:*

$$card(\mathcal{P}(E)) = 2^{card(E)}$$

Remark 1.1. *The set of subsets contains the original set and the empty set.*

Example 1.5.
For the set $E = \{1, 2\}$*, we have*

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

and $card(\mathcal{P}(E)) = 4 = 2^2$*.*

2 Relationship between sets

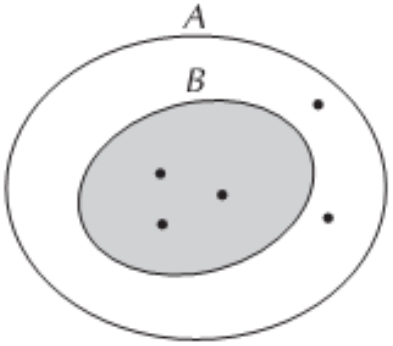
Let A and B be subsets of a non-empty set E.

2.1 Inclusion

we say that B is included in A and write $B \subset A$ if and only if:

$$\forall x \in E : \ x \in B \implies x \in A$$

in other words, B is a subset of A.



if B does not a part of A, we write $B \not\subset A$ such that

$$A \not\subset B \Leftrightarrow \exists x : (x \in A) \wedge (x \notin B)$$

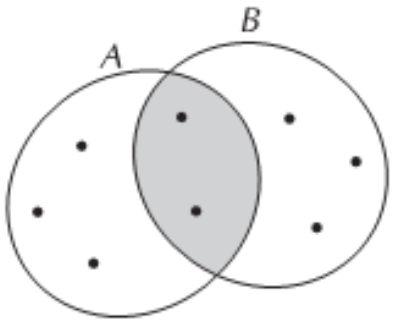
Property 2.1. *Considering A, B and C three subsets of E, the following statements are true:*

1. $A \subset B$ *and* $B \subset A \Leftrightarrow A = B$
2. $A \subseteq B$ *and* $B \subset A \Leftrightarrow A = B$ *or* $A \subset B$
3. $A \subsetneq B \Leftrightarrow A \neq B$ *and* $A \subset B$
4. $A \not\subset B \Leftrightarrow \exists x \in E :\ x \in A$ *and* $x \notin B$
5. $(A \subset B) \wedge (B \subset C) \implies (A \subset C)$

2.2 Intersection

In mathematical notation, the expression $A \cap B$ is read as "A intersect B". It represents the intersection of two sets, meaning it includes the elements that are **common to both** sets A and B, i.e.

$$A \cap B = \{x, (x \in A) \wedge (x \in B)\}$$



Example 2.1. *Let $A = \{\alpha, \beta, 1, 3\}$ and $B = \{\beta, 0, 3\}$, we have*

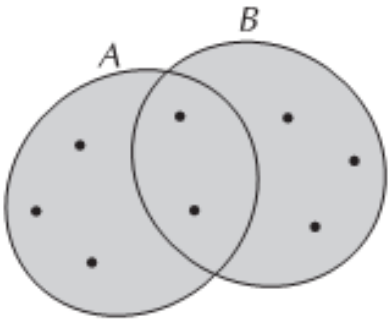
$$A \cap B = \{\beta, 3\}$$

Remark 2.1. *If $A \cap B = \Phi$, we say that A and B are **distinct**.*

2.3 Union

The notation $A \cup B$ is read as A union B, it represents a new set of all elements which **belong** to A **or** B, hence

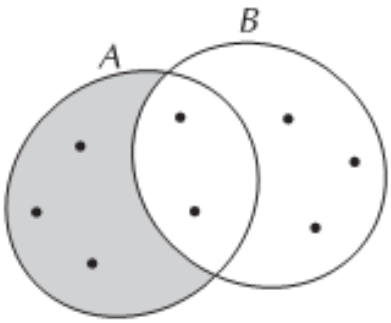
$$A \cup B = \{x, (x \in A) \vee (x \in B)\}$$



2.4 Difference

The difference of sets, often denoted as $A \setminus B$ or $A - B$, represents the set of elements that belong to A but not belong to B, i.e.

$$\begin{aligned} A - B &= A \setminus B \\ &= \{x : (x \in A) \wedge (x \notin B)\} \\ &= \{x : (x \in A) \wedge (x \in C_E B)\} \\ &= A \cap C_E B \end{aligned}$$



Remark 2.2.

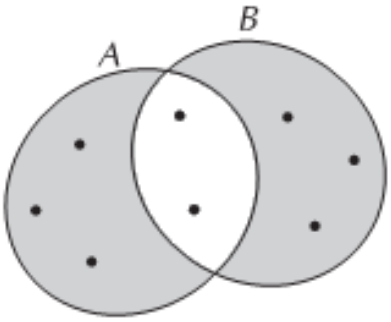
- $A \setminus B = \Phi \Leftrightarrow A \subset B$
- *For any two finite sets A and B, we have*

$$card(A \setminus B) = card(A) - card(A \cap B)$$

2.5 Symmetric difference

The mathematical notation $A\Delta B$, expresses the symmetric difference of the sets A and B, such that

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



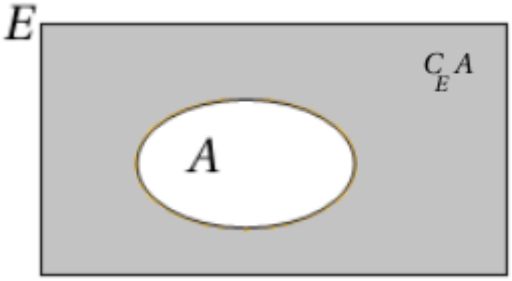
Example 2.2. *the symmetric difference of* $A = \{0, 2, 4, 6, 8\}$ *and* $B = \{1, 2, 3, 4, 5, 6, 7\}$ *is*

$$\begin{aligned} A\Delta B &= (A \setminus B) \cup (B \setminus A) \\ &= \{0, 8\} \cup \{1, 3, 5, 7\} \\ &= \{0, 8, 1, 3, 5, 7, 8\} \end{aligned}$$

3 The complement

The complement of set A with respect to the universal set E denoted by $C_E A$ (or $\overline{A}$, A^c), contains all elements of E that are not in the set A, i.e.

$$C_E A = \{x \in E : \ x \notin A\}$$



Example 3.1. *Consider the sets* $E = \{1, 2, 3, 4, 5\}$ *and* $A = \{3, 4\}$*, we write*

$$C_E A = \{1, 2, 5\}$$

Remark 3.1. *It is clear that:*

1. $A \cap C_E A = \Phi$
2. $A \cup C_E A = E$
3. $C_E E = \Phi$
4. $C_E \Phi = E$

4 Properties

Let the universal set E and its three subsets A, B and C. the following properties are satisfied

1. $(A \cap B) \subset A$ and $(A \cap B) \subset B$
2. $A \subset (A \cup B)$ and $B \subset (A \cup B)$
3. $C_E(C_E A) = A$
4. $A \cup \Phi = \Phi$ and $A \cap \Phi = \Phi$
5. $A \cup C_E A = E$ and $A \cap C_E A = \Phi$
6. Commutativity: $A \cap B = B \cap A$ and $A \cup B = B \cup A$
7. Associativity: $(A \cap B) \cap C = A \cap (B \cap C)$ and $(A \cup B) \cup C = A \cup (B \cup C)$
8. Ditributivity: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proposition 4.1.

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

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

(a) Show that $(F \cap G)^c \subseteq F^c \cup G^c$:
Let $x \in (F \cap G)^c$. By definition of the complement, this means $x \notin F \cap G$. Then

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

this implies that $x \in F^c$ or $x \in G^c$.
hence,

$$x \in F^c \cup G^c$$

thus

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

therefore

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

(b) Show that $F^c \cup G^c \subseteq (F \cap G)^c$:
Let $x \in F^c \cup G^c$, this means $x \in F^c$ or $x \in G^c$.

- If $x \in F^c$, then $x \notin F$.
- If $x \in G^c$, then $x \notin G$.

In either case, x is not in both F and G. Hence, $x \notin F \cap G$, therefore

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

thus

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

then

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

Consequently

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

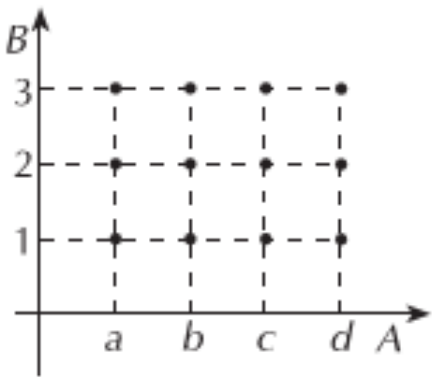
2. Similar to (1).

□

5 Cartesian Product

Given two sets A and B, the notation $A \times B$ denotes the set of cartesian product of A and B, it is a new set that contains all possible ordered pairs (a, b) where $a \in A$ and $b \in B$, i.e.

$$A \times B = \{(a, b) : \ (a \in A) \wedge (b \in B)\}$$



Example 5.1. *For the sets* $A = \{0, 2, 4, 6\}$ *and* $B = \{\alpha, \beta, \gamma\}$*, we get*

$A \times B$	α	β	γ
0	$(0, \alpha)$	$(0, \beta)$	$(0, \gamma)$
2	$(2, \alpha)$	$(2, \beta)$	$(2, \gamma)$
4	$(4, \alpha)$	$(4, \beta)$	$(4, \gamma)$
6	$(6, \alpha)$	$(6, \beta)$	$(6, \gamma)$

or

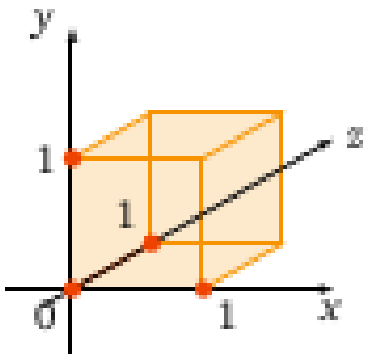
$$A \times B = \{(0, \alpha), (0, \beta), (0, \gamma), (2, \alpha), (2, \beta), (2, \gamma), (4, \alpha), (4, \beta), (4, \gamma), (6, \alpha), (6, \beta), (6, \gamma)\}$$

Property 5.1.

$$A \times B \neq B \times A$$

Example 5.2. *All the following sets are a cartesian products of some given sets*

1. $\mathbb{R}^2 = \{(x, y) : \ x, y \in \mathbb{R}\}$
2. $[0, 1] \times [0, 1] \times [0, 1] = \{(x, y, z) : \ 0 \leq x, y, z \leq 1\}$



University 20 août 1955-Skikda
Faculty of Sciences
Department of Computer Science
Level: L1
Module: **Algebra 1**
Academic year: 2024-2025

Tutorial Sheet 02

Exercise 1:

Check if the following statements are true or false and justify your assessment:

1. For any two disjoint sets A and B: $A \setminus B = \Phi$.
2. $C_E(C_E A) = A$.
3. For all three sets A, B and C: $(A \cap C) = (A \cup B) \Leftrightarrow B \subset A \subset C$.
4. The set $I = \bigcap_{n=1}^{+\infty}]-\frac{1}{2}, 2+\frac{1}{n}[$ represents the domain $I = [-1,2[$.
5. $(A \cup B) \times C = (A \times C) \cap (B \times C)$.
6. For every non-empty set E: $\Phi \subset E$.

Exercise 2:

Let A, B and C be three subsets of E. Prove the following:

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

Exercise 3:

Let A, B and C be subsets of the non-empty set E.

1. Prove that:
   - (a) $C_E(A \cap B) = C_E(A) \cup C_E(B)$.
   - (b) $C_E(A \cup B) = C_E(A) \cap C_E(B)$.
2. Simplify every expression of the following:
   - (a) $A \cup (A \cap B)) \cap B$.
   - (b) $((A \cup B) \cap (B \cap C)) \cup (A \cup C)$.
   - (c) $C_E(A \cup B) \cap (C \cup C_E A)$.

Exercise 4:

For every two non-empty sets A and B, Prove that:

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

using the following three different methods: truth table, method of elements and finally set theory properties.

Exercise 5:

Let A, B and C be subsets of the non-empty set E. Demonstrate the following:

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

Exercise 6:

Consider $A, B \subset E$. Solve the following equations with the unknown $X \subset E$:

1. $A \cup X = B$.
2. $A \cap X = B$.

Exercise 7:

1. Prove the following property using two different methods:

$$\forall A, B \in \mathscr{P}(E) : (A \cap B = A \cup B) \Rightarrow A = B.$$

2. Prove that:

$$\forall A, B, C \in \mathscr{P}(E) : (A \cap B \cap C) \cup (C_E(A) \cup C_E(B) \cup C_E(C)) = E.$$

Chapter 3

Third chapter: Mappings

Contents

1 Function Concept

Let E and F be two no-empty set.
We call function h from E to F, the relation connecting every element of E by at most an element of F, we write

$$h : E \longrightarrow F$$

or

$$E \xrightarrow{\quad h \quad} F$$

in this case, E and F are called respectively input set and output set (or the domain and codomain of h). In fact, the expression $y = h(x)$ means that $x \in E$ and $y \in F$.

Example 1.1.
Considering the sets $A = \{1, 2, 3, 4\}$ *and* $B = \{2, 5, 7\}$.
For all $x \in A$, $f_1(x) = \{(1, 2), (2, 5), (3, 7), (4, 7)\}$ *represents a function from* A *into* B.
For all $x \in A$, $f_2(x) = \{(1, 2), (2, 3), (2, 5), (4, 7)\}$, $x \in A$ *is not a function from* A *into* B.
$f_3 = A \times B$ *is not a function from* A *into* B.

2 Mapping concept

Consider sets A and B. the transformation, the mapping or the map from A to B represents any subset T of the Cartesian product $A \times B$ that satisfies the following condition:

For every a from A there is a **unique** b from B such that $(a, b) \in T$.

We write

$$\begin{array}{rccc} T: & A & \longrightarrow & B \\ & x & \longmapsto & y = T(x) \end{array}$$

Remark 2.1.
We can summarize that the relation $f : E \longrightarrow F$ is a mapping if and only if

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

Remark 2.2.
Every mapping is a function, but the opposite is not true.

Example 2.1.
The map $Id_E : E \longrightarrow E$ defined as

$$\forall x \in E: \ id_E(x) = x$$

*is called The **identity** mapping on E.*

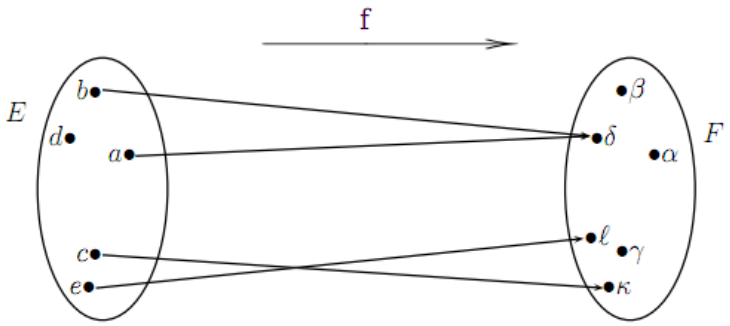
Example 2.2.
Let E and F be two non-empty sets, and the constant $c \in F$, the mapping $f : E \longrightarrow F$ defined as

$$\forall x \in E: \ f(x) = c$$

*is called the **constant map**.*

Example 2.3.

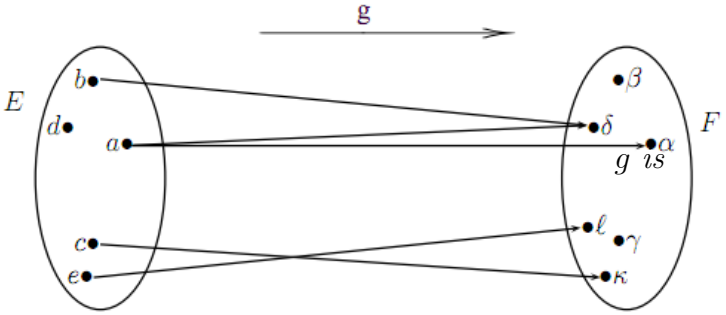
Let it be that E and F are sets and that $f : E \longrightarrow F$ as the corresponding drawing shows.



f is not a map because the element $d \in E$ has no image in the set F.

Example 2.4.

Consider the transformation $g : E \longrightarrow F$ shown in the corresponding figure



not a map because the element $a \in E$ has two images in the output set F.

3 Equality of Mappings

Two mappings $f : E_1 \longrightarrow F_1$ and $g : E_2 \longrightarrow F_2$ are equal if and only if:

1. $E_1 = E_2$
2. $F_1 = F_2$
3. $\forall x \in E_1 : \ f(x) = g(x)$.

4 Mapping curve

The geometric presentation of a mapping f is considered as the set

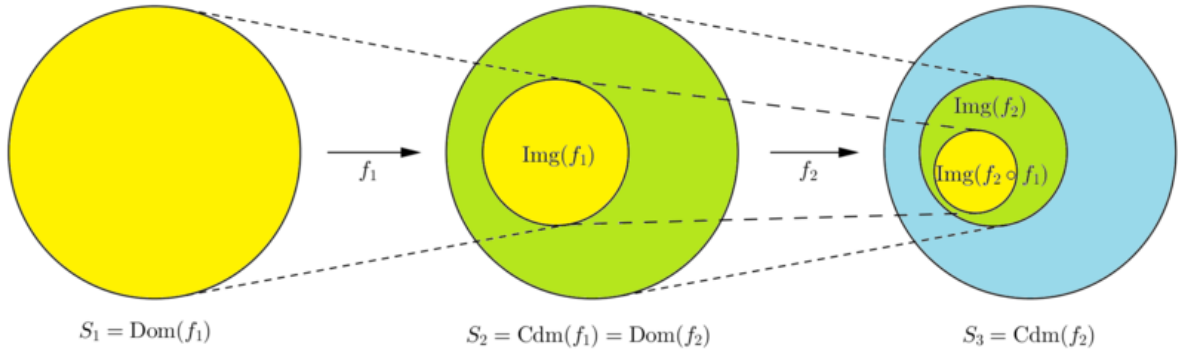
$$\Gamma_f = \{(x, f(x)), x \in E\}$$

5 Composition of Mappings

Consider the non-empty sets S_1, S_2 and S_3.
Let $f_1 : S_1 \longrightarrow S_2$ and $f_2 : S_2 \longrightarrow S_3$ be mappings such that the domain of f_2 is the same set as the codomain of f_1.

Definition 5.1. *The composite mapping $f_2 \circ f_1$ is defined as:*

$$\forall x \in S_1 : \ f_2 \circ f_1(x) = f_2[f_1(x)]$$



Exercise 5.1. *Prove that the composite of maps $f : E \longrightarrow F$ and $g : F \longrightarrow H$ is a map.*

Solution Let $x_1, x_2 \in E$. If $x_1 = x_2$ then $f(x_1) = f(x_2)$ because f is a map.
Since g is also a map, we write $g[f(x_1)] = g[f(x_2)]$ which means that

$$g \circ f(x_1) = g \circ f(x_2)$$

therefore $g \circ f$ is a map.

Remark 5.1.
Through the maps $f : E \longrightarrow F$ and $g : S \longrightarrow H$, one may define the composite map $g \circ f : E \longrightarrow H$, if and only if:

$$f(E) \subset S$$

Example 5.2.
The composite of the two maps

$$f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^3 \end{array} \quad \textit{and} \quad g : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & e^x \end{array}$$

is as following

$$g \circ f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & e^{x^3} \end{array}$$

6 Injectivity, surjectivity and bijectivity

Considering the non-empty sets E and F, and the mapping $f : E \longrightarrow F$.

Definition 6.1 (Injectivity)**.** *f is said to be injective if each element in the domaine is associated with a unique element in the codomain, i.e.,*

$$\forall x, y \in E : \ f(x) = f(y) \implies x = y$$

or simply

$$\forall x, y \in E : \ x \neq y \implies f(x) \neq f(y)$$

Remark 6.1.

1. *Injectivity is often called **one-to-one** because it ensures that each element in the domain pairs to a **distinct** element in the codomain.*

2. *The nagatin of injectivity statement is*

$$\exists x, y \in E : \ f(x) = f(y) \implies x \neq y$$

Example 6.1.

1. *The constant mapping where its domain contains at least two elements is not injective.*

2. *The identity mapping is injective.*

Example 6.2.
The mapping

$$f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & 5x - 3 \end{array}$$

is injective since

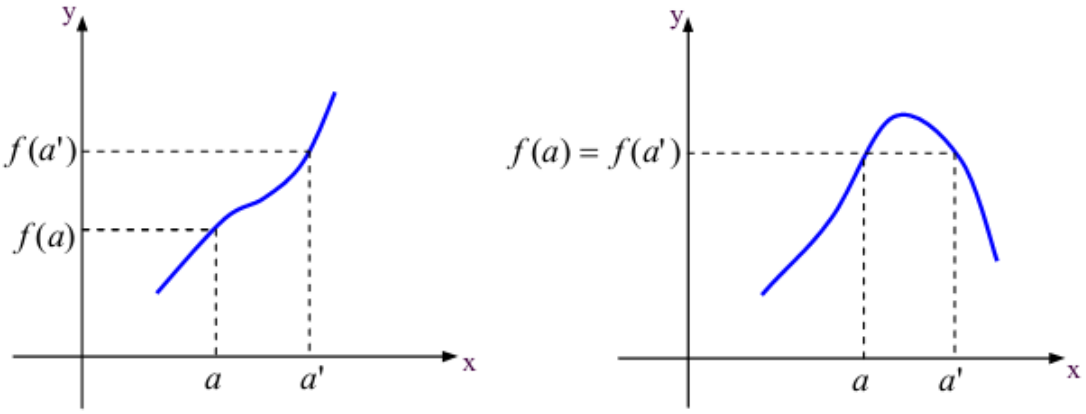
$$\begin{array}{lll} \forall x, y \in \mathbb{R} : f(x) = f(y) & \implies & 5x - 3 = 5y - 3 \\ & \implies & x = y \end{array}$$

Example 6.3.
The map

$$\begin{array}{rccc} g: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & x^2 \end{array}$$

is not injective since $f(-1) = f(1)$ *while* $-1 \neq 1$.

Example 6.4. *Graphically, it can be deduced whether a mapping is injective or not, for example*



the curve on the left indicates that its correponding mapping is ***injective****, while the curve on the right shows that the corresponding mapping is* ***non injective****.*

Definition 6.2 (Surjectivity)**.** *The mapping* f *is said to be surjective if*

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

which means that

$$F = f(E)$$

Remark 6.2.
f *is surjective if every element in the codomain (the set of outputs) has* ***at least*** *one corresponding element in the domain (the set of inputs). in other words, the mapping* ***covers*** *the* ***entire*** *codomain.*

Example 6.5.
Consider the mapping

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & 3x+1 \end{array}$$

then, $\begin{array}{lcl} y = f(x) & \Leftrightarrow & y = 3x+1 \\ & \Leftrightarrow & x = \frac{y-1}{3} \end{array}$
which implies that f *is surjective because*

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

Example 6.6.
The mapping

$$\begin{array}{rccc} g: & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & 2x-5 \end{array}$$

is not surjective since $y = 2$ *has no* $x \in \mathbb{Z}$ *such that:* $f(x) = 2$*, in fact* $2x - 5 = 2 \Leftrightarrow x = \frac{3}{2} \notin \mathbb{Z}$.
However, g *is injective as*

$$f(x) = f(x') \implies x = x'$$

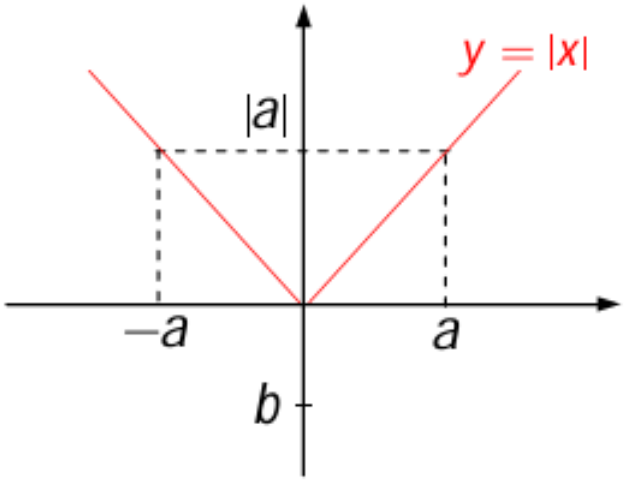
Exercise 6.7. *Let the mapping* f *be defined as*

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & y = |x| \end{array}$$

1. *Plot (draw) the graph of the mapping* f.
2. *Study the injectivity and surjectivity of* f.

Solution

1. Graphical representation



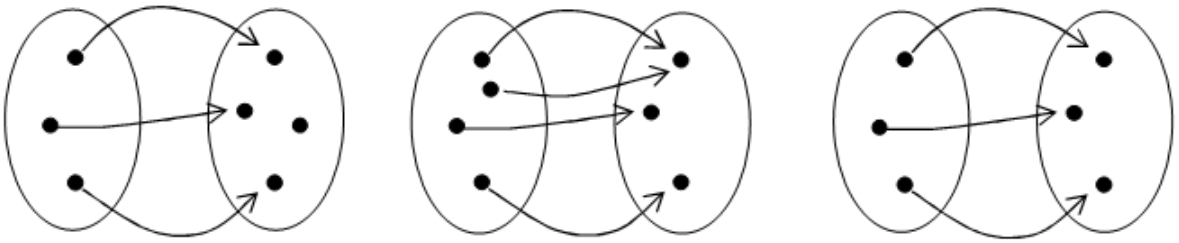
2. Since for every two real numbers a and $-a$ have the same image, f is not injective. Moreover, we notice that the negative elements of the codomain do not correspond to images of any real numbers. This implies that f is not surjective.

Definition 6.3 (Bijectivity)**.** *f is a **bijective** mapping, or simply a **bijection**, if every element in the domain is **uniquely** associated with an element in the codomain, and vice versa, i. e.,*

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

Remark 6.3.
*A bijective mapping is **both** injective (one-to-one) and surjective (onto).*

Example 6.8. *Let consider the charts (visual representation) of three distinct mappings*



from left to right, the mappings are injective not surjective, surjective non injective and finally bijective.

Example 6.9.
The mapping

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & 5x-3 \end{array}$$

is a bijection as

$$\forall y \in \mathbb{R}, \exists! x = \frac{y+3}{5} \in \mathbb{R} : f(x) = y$$

7 Inverse mapping

Proposition 7.1. *Considering the sets E and F, and the mapping $f : E \longrightarrow F$. The following statement is true*

$$f \quad \textit{bijection} \Leftrightarrow f \quad \textit{invertible}$$

Proof. 1. $\Longrightarrow$) Assume that f is a bijection, and let

$$R = \{(x, f(x)),\ x \in E\} \subset E \times F$$

be the correspondent relation, which means that for each element $y \in F$, it exists just one element $x \in E$ such that $(x, y) \in R$.
Consider the relation

$$R' = \{(y, x),\ (x, y) \in R\} \subset F \times E$$

hence

$$(y, x) \in R' \Leftrightarrow (x, y) \in R$$

we can say that R' is associated to a mapping from F to E because for all $y \in F$, it exists unique element $x \in E$, such that $(y, x) \in R'$.
Let $g : F \longrightarrow E$ be the associated mapping to R'. It is clear that

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

and

$$f \circ g(y) = f[g(y)] = f(x) = y = Id_F(y),\ \forall y \in F$$

therefore

$$g \circ f = Id_E \ \wedge \ f \circ g = Id_F$$

consequently f is invertible and g is its inverse mapping.

2. $\Leftarrow$) Assume that f is invertible and $g : F \longrightarrow E$ is its inverse mapping.
So, f is surjective, since for any $y \in F$:

$$\begin{aligned} y &= Id_F(y) \\ &= f \circ g(y) \\ &= f[g(y)] \in Im(f) \end{aligned}$$

moreover, f is a bijection because if $f(x) = f(x')$ we get

$$\begin{aligned} x &= Id_E(x) \\ &= g \circ f(x) \\ &= g[f(x)] \\ &= g[f(x')] \\ &= Id_E(x') \\ &= x' \end{aligned}$$

consequently, f is a bijection.

□

Lemma 7.2. *Considering the no-empty sets X, Y, Z and W, and the mappings $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$, $h : Z \longrightarrow W$, then*

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Proposition 7.3. *If $f : E \longrightarrow F$ is invertible, then its inverse mapping is unique.*

Proof. Assume that $g, h : F \longrightarrow E$ are two inverse mappings of f, then

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

hence the inverse mapping of f is unique. □

Remark 7.1. *Considering the map $f : E \longrightarrow F$.*

1. *The invertible relation of f associate to each element of F just one element of E, which means that it is a map.*
2. *The inverse map of f is often denoted as f^{-1}.*
3. *If the inverse mapping exists, it is **unique**.*

Property 7.1. *For the non-empty sets E and F, and the bijective mapping $f : E \longrightarrow F$, the following properties are true*

1. *$f^{-1} : F \longrightarrow E$ is a bijection.*
2. *$y = f(x) \Leftrightarrow x = f^{-1}(y)$*
3. *$f \circ f^{-1} = Id_F$.*

4. $f^{-1} \circ f = Id_E$.

5. $(f^{-1})^{-1} = f$.

Exercise 7.4. *Consider the mapping*

$$\begin{array}{rccc} g: & \mathbb{R} \setminus \{2\} & \longrightarrow & F \\ & x & \longmapsto & \frac{x}{x-2} \end{array}$$

such that $F \subset \mathbb{R}$
Determine the set F *for which* g *can be bijective, and compute* g^{-1}.

Solution

For $y \in F$, we have

$$\begin{array}{rcl} y = g(x) & \Leftrightarrow & y = \frac{x}{x-2} \\ & \Leftrightarrow & yx - 2y = x \\ & \Leftrightarrow & x(y-1) = 2y \\ & \Leftrightarrow & x = \frac{2y}{y-1}, \text{ such that } y \neq 1 \end{array}$$

but

$$x = \frac{2y}{y-1} \in \mathbb{R} \setminus \{2\}?$$

assuming that

$$\begin{array}{rcl} \frac{2y}{y-1} = 2 & \Leftrightarrow & 2y = 2y - 2 \\ & \Leftrightarrow & 2 = 0, \text{ impossible} \end{array}$$

thus $x = \frac{2y}{y-1} \neq 2 \Leftrightarrow x = \frac{2y}{y-1} \in \mathbb{R} \setminus \{2\}$
it follows that

$$\forall y \in \mathbb{R} \setminus \{1\}, \exists! x = \frac{y}{y-1} \in \mathbb{R} \setminus \{2\} : \ g(x) = y$$

in consequence, g is a bijection if $F = \mathbb{R} \setminus \{1\}$.
The inverse mapping of g is

$$\begin{array}{rccc} g^{-1}: & \mathbb{R} \setminus \{1\} & \longrightarrow & \mathbb{R} \setminus \{2\} \\ & y & \longmapsto & \frac{2y}{y-1} \end{array}$$

Theorem 7.5. *For any mappings* $f : E \longrightarrow F$ *and* $g : F \longrightarrow G$, *the following statements are true*

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

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

3. *(*f *bijective)*$\wedge$*(*g *bijective)* $\implies$ *(*$g \circ f$ *is a bijection and* $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$*)*

4. $g \circ f$ *injective* $\implies$ f *injective*

5. $g \circ f$ *surjective* $\implies$ g *surjective*

6. $g \circ f$ *bijective* $\implies$ *(*f *injective)* $\wedge$ *(*g *surjective)*

Proof.

1. We have $g \circ f : E \longrightarrow G$.
   Assuming that f and g are injections, consequently

$$\begin{array}{rcl} \forall x, x' \in E, x \neq x' & \Longrightarrow & f(x) \neq f(x') \\ & \Longrightarrow & g[f(x)] \neq g[f(x')] \\ & \Longrightarrow & g \circ f(x) \neq g \circ f(x') \end{array}$$

   so $g \circ f$ is injective.

□

8 Direct image and inverse image

Let A be a part of the set E, we denote by $f(A)$ the set containing the images of the elements of A under the mapping f, and we write

$$\begin{array}{rcl} f(A) & = & \{f(x) : x \in A\} \\ & = & \{y \in F : \ \exists x \in A, y = f(x)\} \subset F \end{array}$$

Consider $B \subset F$, we denote by $f^{-1}(B)$ the elements of E which their images by f belong to the subset B, and we write

$$\begin{array}{rcl} f^{-1}(B) & = & \{x \in E : f(x) \in B\} \\ & = & \{x \in E : \ \exists y \in B, y = f(x)\} \subset E \end{array}$$

Theorem 8.1. *Consider the mapping $f : E \longrightarrow F$, and the sets A, $B \subset E$, and M, $N \subset F$, the following statements are true:*

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

Proof.

1. Assume that $y \in F$, such that

$$\begin{array}{rcl} y \in f(A \cup B) & \Leftrightarrow & \exists x \in A \cup B : y = f(x) \\ & \Leftrightarrow & \exists x[((x \in A) \vee (x \in B)) \wedge (y = f(x))] \\ & \Leftrightarrow & \exists x[(x \in A) \wedge (y = f(x)) \vee (x \in B) \wedge (y = f(x))] \\ & \Leftrightarrow & [\exists x((x \in A) \wedge (y = f(x)))] \vee [\exists x((x \in B) \wedge (y = f(x)))] \\ & \Leftrightarrow & (y \in f(A)) \vee (y \in f(B)) \\ & \Leftrightarrow & y \in f(A) \cup f(B) \end{array}$$

   it means that

$$f(A \cup B) = f(A) \cup f(B)$$

2. Assume that $y \in F$, such that

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

thus

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

3. Assuming $x \in E$, such that

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

therefore

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

4. for any $x \in E$, we have

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

it follows that

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

5. Considering $x \in E$, so

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

thus

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

□

Theorem 8.2. *Considering the mapping $f : E \longrightarrow F$ and the subsets $E_1,\ E_2 \subset E$, the following statement is true*

$$E_1 \subseteq E_2 \implies f(E_1) \subseteq f(E_2)$$

Proof. Assume that $E_1 \subseteq E_2$ and y is an element of $f(E_1)$, it means that

$$\begin{aligned} y \in f(E_1) &\implies \exists x \in E_1 : y = f(x) \\ &\implies x \in E_2 : y = f(x) \\ &\implies y \in f(E_2) \end{aligned}$$

thus

$$E_1 \subseteq E_2 \implies f(E_1) \subseteq f(E_2)$$

□

9 Mapping restriction and extension

Definition 9.1. *Consider the mapping $f : E \longrightarrow F$.*

- *We call **restriction** of f on the non-empty set $A \subset E$, the mapping $g : A \longrightarrow F$, such that*
$$\forall x \in A : \ g(x) = f(x)$$
and we write $g = f|_A$.
- *Consider the set S such that $E \subset S$, we call **extension** of f on the set S, every mapping $h : S \longrightarrow F$ such that f represents an abbreviation of h on the set E.*

Example 9.1.
The mapping

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \ln(|x|) \end{array}$$

is an extension of the mapping

$$\begin{array}{rccc} g: & \mathbb{R}^+ & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \ln(x) \end{array}$$

Remark 9.1.
All previous mappings concepts remain equally applicable to functions.

Tutorial Sheet 03

Exercise 1:

Check if the following statements are true or false and justify your answer:

1. For any two sets $A, B \subset E$, we have: $f(A \cap B) = f(A) \cap f(B)$.
2. For any mapping f: $A \neq \Phi \Rightarrow f(A) \neq \Phi$.
3. For any invertible mapping $f : E \longrightarrow F$ and $A \subset E, B \subset F$, we have: $f(A \cap f^{-1}(B)) = f(A) \cap B$.
4. For any two sets $A, B \subset E$, we have: $f(A \setminus B) = f(A) \setminus f(B)$.
5. For any invertible mapping $f : E \longrightarrow F$ and $M, N \subset F$, we have: $f^{-1}(M \triangle N) = f^{-1}(M) \triangle f^{-1}(N)$.

Exercise 2:

Check if the following relations define a mapping

1. $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = \dfrac{1}{x}$.
2. $f : \mathbb{R}^2 \to \mathbb{R}$ such that $f(x, y) = x + y$.
3. $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = \begin{cases} x & x < 0 \\ 0 & x \geq 0 \end{cases}$

Exercise 3:

Study the injectivity, surjectivity and bijectivity of the following mappings:

1. $f : \mathbb{Z} \to \mathbb{N}$ such that $f(x) = x^2$.
2. $g : \mathbb{R} \setminus \{1\} \to \mathbb{R}$ such that $g(x) = \dfrac{x+1}{x-1}$.
3. $h : \mathbb{C} \to \mathbb{C}$ such that $h(z) = e^z$.
4. For any non-empty set A, $T : \mathscr{P}(A) \to \mathscr{P}(A)$ such that $T(X) = X^c$.
5. $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = \dfrac{k(x)}{\sqrt{1 + k(x)^2}}$., where the mapping $k : \mathbb{R} \to \mathbb{R}$ is a bijection.

Exercise 4:

Let A, B and C be three non-empty sets and let $f : A \to B$ and $g : B \to C$ be two mappings. Prove that:

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

Exercise 5:

Let A, B and C be three non-empty sets and let $f : A \to B$ and $g : B \to C$. be two mappings. Prove that:

1. $g \circ f$ is injective and f is surjective $\Rightarrow g$ is injective.
2. $g \circ f$ is surjective and f is injective $\Rightarrow g$ is surjective.
3. $g \circ f = Id_A \Rightarrow g$ is surjective and f is injective .
4. Deduce that:

$$(g \circ f = Id_A) \wedge (f \circ g = Id_B) \Rightarrow f \text{ and } g \text{ are bijective such that } f = g^{-1}$$

Exercise 6:

Consider the mapping

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

1. Prove that the mapping f is injective and surjective? what do you deduce?
2. Find the expression of the mapping $f \circ f(x)$.
3. Find by two different methods the expression of $f^{-1}(x)$.

Exercise 7:

Consider the mapping $f : E \to F$ such that E and F are non-empty sets with $card(E) = card(F) = n$. Prove that the following propositions are equivalent:

1. f is injective.
2. f is surjective.
3. f is bijective.

Chapter 4

Binary relations

Contents

1 Basic concept

Definition 1.1. *Considering the non-empty sets E and F. A **binary relation** R from E to F is a subset of the cartesian product $\Omega = E \times F$.*
If the pair $(a, b) \in \Omega$, we say that a is related to b, and we write

$$a \; R \; b$$

Remark 1.1.
If $F = E$, we say that the binary relation R is from E to E.

2 Properties

Considering the binary relation R defined on the non-empty set E. The main properties of the binary relation R are as following

Property 2.1.

1. *R is **reflexive** if*

$$\forall x \in E : x \; R \; x$$

in other words, every element is related to itself.

2. R *is* ***symmetric*** *if*

$$\forall (x, y) \in E^2 : x \; R \; y \implies y \; R \; x$$

it means that, if x *is related to* y*, then* y *is related to* x*.*

3. R *is* ***antisymmetric*** *if*

$$\forall (x, y) \in E^2 : (x \; R \; y) \wedge (y \; R \; x) \implies x = y$$

4. R *is* ***transitive*** *if* $\forall (x, y, z) \in E^3 : (x \; R \; y) \wedge (y \; R \; z) \implies (x \; R \; z)$

Example 2.1.
Let the binary relations defined on the set of integers $\mathbb{Z}$ *as*

$$x \; R_1 \; y : x = y$$

$$x \; R_2 \; y : x^2 = y^2$$

$$x \; R_3 \; y : x + y \leq 2$$

it is clear to notice that
R_1 *is reflexive, symmetric, antisymmetric and transitive.*
R_2 *is reflexive, symmetric, transitive and it is not antisymmetric.*
R_3 *is neither reflexive, antisymmetric, nor transitive, but it is symmetric.*

Example 2.2.
In the set of complex numbers $\mathbb{C}$ *the relation*

$$z \; R \; z' : |z| \leq |z'|$$

is reflexive, transitive but it is not symmetric.

3 Equivalence relation

Let the binary relation R defined on the non-empty set E.
R is called an **Equivalence relation** in E if and only if R is:

- reflexive.
- symmetric.
- transitive.

Example 3.1.
If E *is a non-empty set, then*

the equality is an equivalence relation on E*.*

3.1 Equivalence class

Definition 3.1. *Let the equivalence relation R defined on the non-empty set E. The equivalence class of the element $'a' \in E$, denoted $\dot{a}$, is the set of all elements in E that are related to $'a'$ by R. Mathematically, it is represented as*

$$\dot{a} = \{x \in E : \ x \ R \ a\}$$

obviously, $\dot{a}$ is a subset of E.

Theorem 3.2. *Let the equivalence relation R defined on the non-empty set E. For every $a, b \in E$, the following statements are true*

$$\begin{array}{lrcl} 1) & a \ R \ b & \Leftrightarrow & \dot{a} = \dot{b} \\ 2) & a \not R b & \Leftrightarrow & \dot{a} \cap \dot{b} = \Phi \end{array}$$

Remark 3.1.
The notation $E/\ R$= denote all equivalence classes in E with respect to R

$$E/\ R = \{\dot{a}, a \in E\}$$

it represents a partition of E.

Example 3.3. *Given $E = \{1, 2, 3, 4, 5\}$ and the equivalence relation R baised on the remainderwhen devided by 2. In this case, the equivalent classes are*

$$\dot{0} = \{2, 4\} \ \textit{even numbers}$$

$$\dot{1} = \{1, 3, 5\} \ \textit{odd numbers}$$

Therefore, $E/\ R = \{\dot{0}, \dot{1}\} = \{\{2, 4\}, \{1, 3, 5\}\}$

Exercise 3.4. *Let in $\mathbb{Z}$ the relation*

$$x \ R \ y \Leftrightarrow x \equiv y[2]$$

1. *Prove that R is an equivalence relation.*
2. *Find $\dot{0}, \ \dot{1}$, what do you deduce?*

Solution

1. We have for all $x, y \in \mathbb{Z}$:

$$\begin{array}{rcl} x \ R \ y & \Leftrightarrow & x \equiv y[2] \\ & \Leftrightarrow & \exists k \in \mathbb{Z} : \ x - y = 2k \end{array}$$

we know that

$$\begin{array}{rcl} x - x = 0 & \Leftrightarrow & x - x = 2k, \ k = 0 \\ & \Leftrightarrow & x \equiv x[2] \\ & \Leftrightarrow & x \ R \ x \end{array}$$

then R is reflexive.
Furthermore,

$$\begin{array}{rcl} x\ R\ y & \Leftrightarrow & x-y=2k \\ & \Leftrightarrow & y-x=2(-k) \\ & \Leftrightarrow & y-x=2k',\ k'=-2k, k'\in\mathbb{Z} \\ & \Leftrightarrow & y\equiv x[2] \\ & \Leftrightarrow & y\ R\ x \end{array}$$

then R is symmetric.
Assume that $x, y, z \in \mathbb{Z}$ such that

$$\begin{cases} x\ R\ y \\ \text{ and } \\ y\ R\ z \end{cases} \Leftrightarrow \begin{cases} x-y=2k,\ k\in\mathbb{Z} \\ \text{ and } \\ y-z=2k',\ k'\in\mathbb{Z} \end{cases} \Leftrightarrow \begin{cases} y=x-2k \\ \text{ and } \\ y-z=2k' \end{cases}$$

it means that

$$\begin{array}{rcl} (x-2k)-z=2k' & \Leftrightarrow & x-z=2k",\ k"=k+k',\ k"\in\mathbb{Z} \\ & \Leftrightarrow & x\equiv z[2] \\ & \Leftrightarrow & x\ R\ z \end{array}$$

then R is transitive.
Therefore, we conclude that R is an equivalence relation.

2. We have

$$\begin{array}{rcl} \dot{0} & = & \{x\in\mathbb{Z}:\ x\ R\ 0\} \\ & = & \{0+2k,\ k\in\mathbb{Z}\} \\ & = & \{...,-6,-4,-2\}\cup\{0,2,4,...\} \end{array}$$

and

$$\begin{array}{rcl} \dot{1} & = & \{x\in\mathbb{Z}:\ x\ R\ 1\} \\ & = & \{1+2k,\ k\in\mathbb{Z}\} \\ & = & \{...,-5,-3,-1\}\cup\{1,3,5,...\} \end{array}$$

hence

$$\mathbb{Z}/\ R=\{\dot{0},\dot{1}\}$$

which means $\dot{0}$ and $\dot{1}$ represent a partition of $\mathbb{Z}$.

4 Partial Order relation

The binary relation R defined on E, is said to be **partial order relation** if and only if

- R is reflexive.
- R is antisymmetric.
- R is transitive.

Remark 4.1.
*The order relation is used to **compare** elements in the set based on certain **creteria**.*

Example 4.1.

1. *$\leq$ is a partial order relation on $\mathbb{R}$.*
2. *$<$ is not a partial order relation on $\mathbb{R}$, because it is not reflexive.*

Exercise 4.2. *Let E be a non-empty set, and let its partition denoted as $\mathcal{P}(E)$. Prove that the binary relation " $\subset$ " is a partial order relation in the set $\mathcal{P}(E)$.*

Solution

For every set $A \in \mathcal{P}(E)$, we write

$$A \subset A$$

hence, $\subset$ is a reflexive relation.
Let the sets $A, B \in \mathcal{P}(E)$, it is clear that if we have

$$(A \subset B) \wedge (B \subset A)$$

this leads to $A = B$, which means $\subset$ is antisymmetric relation.
For every $A, B, C \in \mathcal{P}(E)$:

$$\begin{aligned}(A \subset B) \wedge (B \subset C) &\Leftrightarrow \forall x[[(x \in A) \implies (x \in B)] \wedge [(x \in B) \implies (x \in C)]] \\ &\Leftrightarrow \forall x[(x \in A) \implies (x \in C)], (\text{ because } \implies \text{ is a transitive relation}) \\ &\Leftrightarrow A \subset C\end{aligned}$$

then $\subset$ is a transitive relation.
Consequently, $\subset$ is a partial order relation in $\mathcal{P}(E)$.

4.1 Special elements in an ordered relation

Considering the ordered set E, where the partial order relation is $\leq$.
We say that

1. $m \in E$ is the minimum (smallest element) of E if

$$\forall x \in E : m \leq x$$

2. $M \in E$ is the maximum (biggest element) of E if

$$\forall x \in E : x \leq M$$

Property 4.1. *Considering the ordered set E, where the order relation is $\leq$.*
*If E has a minimum or maximum, then it is **unique**.*

Proof. Assuming the existence of two lower bounds in E, denoted as m and m', this means

$$\begin{cases} m \leq m' \\ \text{and} \\ m' \leq m \end{cases} \implies m = m'$$

Using a similar approach, we can demonstrate that the upper bound if it exists it is unique. □

Remark 4.2.
The unique relation which is both equivalence relation and partial order relation is equality $'='$.

4.2 Total order relations

A partial order is "partial" because there can be two elements with no relation between them. For example, in the "divides" partial order on $\{1, 2, \ldots, 10\}$, there is no relation between 3 and 5 (since neither divides the other).

Definition 4.1. *A total order relation is a partial order in which every element of the set is comparable with every other element of the set.*

Remark 4.3. *The total order is a specific case of partial order relation, into other words, all total order relations are partial order relations, but the converse is not always true.*

Example 4.3. *The "$\leq$" partial order on $\mathbb{R}$ is a total order relation because for any pair of real numbers x and y, either $x \leq y$ or $y \leq x$.*

Example 4.4. *The "divides" partial order on $E = \{1, 2, 3, \ldots, 12\}$ is not a total order because $2 \nmid 5$ and $5 \nmid 2$.*

Exercise 4.5. *Let the set $E = \{1, 2, 3\}$, and let its partition (the power set) $\mathcal{P}(E)$. Is "$\subset$" a total order relation in $\mathcal{P}(E)$?*

Tutorial Sheet 04

Exercise 1:

Let E be the set of all mappings from $\mathbb{R}$ to $\mathbb{R}$, and let the binary relation $\mathscr{R}$ defined as:

$$\forall f,g \in E,\ \ f\mathscr{R}g \Leftrightarrow \exists \alpha,\beta \in \mathbb{R}_+^*; \forall x \in \mathbb{R} : \alpha f(x) \leq g(x) \leq \beta f(x).$$

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

Exercise 2:

Let $E = \{1,2,3,5,8,14,17\}$ and let $\mathscr{R}$ be the relation defined as:

$$x\mathscr{R}y \Leftrightarrow \frac{x+y}{2} \in \mathbb{N}$$

1. Prove that $\mathscr{R}$ is an equivalence relation over E.
2. Find the equivalence classes of every element $x \in E$.

Exercise 3:

Let $\mathscr{R}$ be the binary relation defined on $\mathbb{R}$ by:

$$x\mathscr{R}y \Leftrightarrow \cos^2(x) + \sin^2(y) = 1.$$

1. Prove that $\mathscr{R}$ is an equivalence relation. Is $\mathscr{R}$ a partial order relation?
2. Determine the equivalence classes of $\frac{\pi}{3}$ and $\frac{\pi}{2}$.
3. Determine $\mathbb{R}_{/\mathscr{R}}$.

Exercise 4:

Let $\mathscr{R}$ be the binary relation defined on $\mathbb{N}^*$ by:

$$x\mathscr{R}y \Leftrightarrow y \ \text{ is divisible by } \ x.$$

1. Prove that $\mathscr{R}$ is a partial order relation.
2. Is the relation $\mathscr{R}$ total? Justify your answer.

Exercise 5:

Let $\mathscr{R}$ be the binary relation defined on $\mathbb{N}^*$ by: $\qquad x\mathscr{R}y \Leftrightarrow \exists n \in \mathbb{N}^* : y = x^n$

1. Prove that $\mathscr{R}$ is a partial order relation. Is $\mathscr{R}$ total?

Chapter 5

Algebraic structures

Contents

1 internal composition law

Definition 1.1 (internal operation)**.** *Consider a non-empty set E, any mapping f of $E \times E$ on E is called an internal composition law (or internal opertaion) on E.*

$$\begin{array}{rccl} f: & E \times E & \longrightarrow & E \\ & (x,y) & \longmapsto & z = f(x,y) \end{array}$$

the internal composition law on E is often denoted as $*$, $\bullet$ or $\oplus$, ... Briefly, one can write $(E,*)$ and $z = x * y$ such that $(x,y,z) \in E \times E \times E$.

Remark 1.1. *$*$ is an internal composition law on E if and only if*

$$\forall x, y \in E: \ x * y \in E$$

Example 1.1. *1. Addition "$+$" and multiplication "$\bullet$" on the set of whole numbers are internal composition laws on $\mathbb{N}$, since*

$$\forall x, y \in \mathbb{N}: \ x + y \in \mathbb{N}$$

$$\forall x, y \in \mathbb{N} : \ x \bullet y \in \mathbb{N}$$

2. *Subtraction "$-$" is not an internal composition law on* $\mathbb{N}$.

3. *Division on the set of integers is not an internal composition law on* $\mathbb{N}$*, since the results obtained are not all elements of* $\mathbb{N}$.

Example 1.2.
For any non-empty set E*. The intersection "*$\cap$*" and union "*$\cup$*" operations are two internal composition laws on* $\mathcal{P}(E)$*, since*

$$\forall A, B \in \mathcal{P}(E) : \ A \cap B \in \mathcal{P}(E)$$

$$\forall A, B \in \mathcal{P}(E) : \ A \cup B \in \mathcal{P}(E)$$

2 Properties

Let $*$ and $\perp$ two internal composition laws on E,

1. $*$ is **associative** if and only if

$$\forall x, y, z \in E : (x * y) * z = x * (y * z)$$

2. $*$ is **commutative** if and only if

$$\forall x, y \in E : x * y = y * x$$

3. **The neutral element (identity element)** we say that $e \in E$ is a neutral element with respect to $*$ if and only if

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

if an identity element exists, it is **unique**.

4. **Inverse element** If $e \in E$ is the identity element of $*$. We say that $x' \in E$ is the inverse element of $x \in E$ with respect to $*$ if and only if

$$\forall x \in E, \ \exists x' \in E : x * x' = x' * x = e$$

In the case where $*$ is not commutative, x' is called right or left inverse element of x if

$$\forall x \in E, \ \exists x' \in E : x * x' = e$$

or

$$\forall x \in E, \ \exists x' \in E : x' * x = e$$

respectively.

5. $*$ is **distributive** over $\perp$ on the right and left if and only if

$$\forall x, y, z \in E : x * (y \perp z) = (x * y) \perp (x * z) \tag{5.1}$$

$$\forall x, y, z \in E : (x \perp y) * z = (x * z) \perp (y * z) \tag{5.2}$$

Remark 2.1. *In a commutative operation, defining the identity and inverse elements on one side is enough due to the symmetry of the operation.*

Example 2.1.

1. *Addition* $+$ *and multiplication* $\bullet$ *are commutative operations in* $\mathbb{R}$.
2. *Intersection* $\cap$ *and union* $\cup$ *are commutative operations in* $\mathcal{P}(E)$.
3. $\circ$ *is not commutative since*
$$f \circ g \neq g \circ f$$

Exercise 2.2. *Consider the internal law* $*$ *in* $\mathbb{R}$ *defined as*

$$x * y = x + y - 2$$

1. *Determine the identity element with respect to* $*$.
2. *Determine the inverse element.*

Solution It is clear that $*$ is commutative in $\mathbb{R}$

$$\forall x, y \in \mathbb{R} : \ x * y = x + y - 2 = y + x - 2 = y * x$$

Therefore, defining the identity and inverse elements on one side is enough.

1. e is the identity element if
$$\forall x \in \mathbb{R} : x * e = e * x = x$$
then
$$\begin{array}{rcccrcl} x * e & = & x & \Leftrightarrow & x + e - 2 & = & x \\ & & & \Leftrightarrow & e & = & 2 \end{array}$$
hence $e = 2 \in \mathbb{R}$ is the identity element of $*$.
2. $x' \in \mathbb{R}$ is the inverse element of $x \in \mathbb{R}$ with respect to $*$ if
$$\forall x \in \mathbb{R}, \exists x' \in \mathbb{R} : x * x' = x' * x = e$$
so
$$\begin{array}{rcccrcl} x * x' & = & e & \Leftrightarrow & x + x' - 2 & = & 2 \\ & & & \Leftrightarrow & x' & = & 4 - x \end{array}$$
then
$$\forall x \in \mathbb{R}, \exists x' = (4 - x) \in \mathbb{R} : x * x' = x' * x = 2$$
consequently, the inverse element of every element $x \in \mathbb{R}$ with respect to $*$ is $x' = (4 - x)$.

3 Group and semigroup

3.1 Group

Definition 3.1. *Let G a nonempty set, and let $*$ be an internal operation defined on G. We say that the* ***structure*** *$(G,*)$ is a* ***group*** *if the following properties are satisfied:*

1. *$*$ is associative.*
2. *The identity element e exists.*
3. *Every element of G has an inverse.*

Remark 3.1. *In addition to the previous properties, if $*$ is commutative, we say that $(G,*)$ is a* ***commutative group*** *or an* ***abelien group****.*

Example 3.1.

- *The algebraic structures $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{Q}^*,\times)$ and $(\mathbb{R}^*,\times)$ represent classical examples of groups.*
- *$(\mathbb{N},+)$ is not a group because the identity element does not exist.*

3.2 semigroup

Definition 3.2. *Consider the group $(G,*)$ and the set $H \subset G$. H is called* ***semigroup*** *of G if*

1. *$H \neq \Phi$*
2. *The identity element $e \in H$.*
3. *$\forall x,y \in H : x * y \in H$*
4. *Every element $x \in H$ its inverse element $x' \in H$.*

Example 3.2. *For each $n \in \mathbb{N}$:*
$H = \{n.p,\ p \in \mathbb{Z}\}$ is a semigroup of $(\mathbb{Z},+)$ as

1. *for $p = 0$, we get $n.0 = 0 = e$*
   hence
   $$H \neq \Phi \text{ and } e \in H$$
2. *For every two elements $x,y \in H$, we write*
   $$\begin{cases} \exists p \in \mathbb{Z} : x = n.p \\ \exists p' \in \mathbb{Z} : y = n.p' \end{cases}$$
   then
   $$\begin{aligned} x+y &= n.p + n.p' \\ &= n.(p+p') \\ &= n.p'', p'' = (p+p') \in \mathbb{Z} \end{aligned}$$
   which means that $x+y \in H$.

3. $\forall x \in H, -x \in H$ *since* $x \in H$ *means the existence of* $p \in \mathbb{Z}$ *such that* $x = np$, *consequently*

$$\begin{aligned} -x &= -n.p \\ &= n.(-p) \\ &= n.p',\ p' = (-p) \in H \quad \textit{since} \quad (-p) \in \mathbb{Z} \end{aligned}$$

4 Ring and subring

4.1 Ring

Definition 4.1. *Let R be a nonempty set equipped with two internal operations, the first is called addition, denoted by $+$, and the second is called multiplication, denoted by $\bullet$. The structure $(R, +, \bullet)$ is called* ***ring*** *if*

1. *$(R, +)$ is a commutative group.*
2. *$\bullet$ is associative.*
3. *$\bullet$ distributes over $+$, given any three elements a ,b and c in R:*

$$(a + b) \bullet c = a \bullet c + b \bullet c \wedge c \bullet (a + b) = c \bullet a + c \bullet b$$

Remark 4.1.

1. *If $\bullet$ is commutative, we say that $(R, +, \bullet)$ is a* ***commutative ring****.*
2. *$(R, +, \bullet)$ is called* ***unital ring*** *if the identity element with respect to $\bullet$ exists and belongs to R.*

Example 4.1.

1. *$(\mathbb{Z}, +, \bullet)$ is a commutative ring.*
2. *$(\mathbb{Q}, +, \bullet)$ is a commutative ring.*

4.2 Subring

Definition 4.2. *A subset S of R is called a subring if any one of the following equivalent conditions holds:*

1. *$S \neq \Phi$*
2. *$\forall x, y \in S : x + y \in S$*
3. *Every $x \in S$ has an inverse element $x' \in S$ with respect to addition "+".*
4. *$\forall x, y \in S : x \bullet y \in S$*

Example 4.2. *The set S of even integers is a subring of $\mathbb{Z}$, because*

1. *Obviously $0 \in S$. Therefore, S is a nonempty subset of the ring $\mathbb{Z}$ of integers.*
2. *If $a, b \in S$, we can write $a = 2c$ and $b = 2d$, hence*

$$a + b = 2(c + d) \in S$$

$$a \bullet b = 4c \bullet d = 2(2c \bullet d) \in S$$

3. *If $a \in S$, we write $a = 2c$ then*

$$-a = -2c = 2(-c) = 2d, \text{ where } d = -c, \text{ hence } -a \in S$$

5 Field and subfield

5.1 Field

Definition 5.1. *Let K be a nonempty set. The algebraic structure $(K, +, \bullet)$ is called* ***field*** *if the following properties are satisfied*

1. *$(K, +)$ is a commutative group.*
2. *$(K - \{0\}, \bullet)$ is a group.*
3. *$\bullet$ distributes over $+$ on right and left sides.*

Remark 5.1. *A field $(K, +, \bullet)$ is a commutative ring in which every element x has a inverse with respect to the multiplication " $\bullet$ " except the element zero "0".*

Example 5.1.

1. *$(\mathbb{C}, +, \bullet)$ is a field (it is the largest field that we have).*
2. *$(\mathbb{R}, +, \bullet)$ is a field.*

Example 5.2. *Rational numbers set $\mathbb{Q}$ (numbers that can be written as fractions $\frac{a}{b}$, where a and b are integers, and $b \neq 0$), is a field. Indeed, the additive inverse of such fraction is $-\frac{a}{b}$, and the multiplicative inverse (provided that $a \neq 0$) is $\frac{b}{a}$, which can be seen as follows:*

$$\frac{b}{a}\frac{a}{b} = \frac{ba}{ab} = 1$$

and $\bullet$ is distributive over $+$ since

$$\begin{aligned}
\frac{a}{b} \bullet (\frac{c}{d} + \frac{e}{f}) &= \frac{a}{b} \bullet (\frac{c}{d} \bullet \frac{f}{f} + \frac{e}{f} \bullet \frac{d}{d}) \\
&= \frac{a}{b} \bullet (\frac{c \bullet f}{d \bullet f} + \frac{e \bullet d}{f \bullet d}) \\
&= \frac{a}{b} \bullet (\frac{c \bullet f + e \bullet d}{d \bullet f}) \\
&= \frac{a \bullet (c \bullet f + e \bullet d)}{b \bullet d \bullet f} \\
&= \frac{a \bullet c \bullet f + a \bullet e \bullet d}{b \bullet d \bullet f} \\
&= \frac{a \bullet c \bullet f}{b \bullet d \bullet f} + \frac{a \bullet e \bullet d}{b \bullet d \bullet f} \\
&= \frac{a \bullet c}{b \bullet d} + \frac{a \bullet e}{b \bullet f} \\
&= \frac{a}{b} \bullet \frac{c}{d} + \frac{a}{b} \bullet \frac{e}{f}
\end{aligned}$$

5.2 Subfield

Definition 5.2. *Consider that $(K, +, \bullet)$ is a field. We say that K' is a **subfield** of K if and only if*

1. $K' \neq \Phi$
2. $\forall x, y \in K' : \ x - y \in K'$
3. $\forall x, y \in K' : \ x \bullet y^{-1} \in K'$

Remark 5.2. *Let K be a field. A subset $K' \subseteq K$ is called a subfield of K if K' is a field itself with respect to the operations of K.*

Example 5.3.

1. $(\mathbb{C}, +, \bullet)$ *is not a subfield of any other field.*
2. $(\mathbb{R}, +, \bullet)$ *is a subfield of* $(\mathbb{C}, +, \bullet)$.
3. $(\mathbb{Q}, +, \bullet)$ *is a subfield of* $(\mathbb{R}, +, \bullet)$.

Tutorial Sheet 05

Exercise 1:

Let the internal composition law $*$ defined in $\mathbb{R}$ as

$$\forall x,y \in \mathbb{R}: \quad x*y = x.y + (x^2-1).(y^2-1)$$

1. Compute $(2*3)*4$ and $2*(3*4)$, what do you deduce?
2. Prove that $*$ is commutative and find its identity element in $\mathbb{R}$.

Exercise 2:

Consider the set $G = \{2^k, \ k \in \mathbb{Z}\}$.
Prove that $(G,\times)$ is a commutative group.

Exercise 3:

Let the group $(G,.)$, and the set $H = \{x \in G: \ x.y = y.x; \ \forall y \in G\}$.
Prove that H is a semigroup of G.

Exercise 4:

Let the set $S = \{a,b\}$ and the operations $\oplus$ and $\otimes$ defined through the following tables

$\oplus$	a	b
a	a	b
b	b	a

$\otimes$	a	b
a	a	a
b	a	b

Prove that $(S,\oplus,\otimes)$ is a ring.

Exercise 5:

Show that $A = \{a+b\sqrt{2}; \ \ a,b \in \mathbb{Q}\}$ is a subring of $(\mathbb{R},+,\times)$.

Exercise 6:

Let the set of real numbers $\mathbb{R}$ equipped with the following internal operations $\oplus$ and $\otimes$ defined for every $x,y \in \mathbb{R}$ as

$$x \oplus y = x+y-1, \qquad x \otimes y = x+y-xy$$

Prove that the structure $(\mathbb{R},\oplus,\otimes)$ is a field.

Chapter 6

Polynomial rings

Contents

In this chapter, $\mathbb{K}$ denotes one of the fields $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.

1 Main concepts

Definition 1.1. *Let $(\mathbb{R}, +, \dot{})$ be a ring. A polynomial, P, of one indeterminate $x \in \mathbb{R}$ is an expression of the form*

$$P(x) = \sum_{k=0}^{n} a_k x^k = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where $n \geq 0$, and the coefficients $a_0, a_1, a_2, \ldots, a_n \in \mathbb{R}$. If $a_n \neq 0$, then the degree of P is n.

Remark 1.1. *1. If the degree of f is n, we write $deg(P(x)) = n$. The set of all polynomials in the indeterminate x with coefficients in $\mathbb{R}$ is denoted by $\mathbb{R}[X]$.*

2. If $P(x) = 0$, then the degree of P is undefined, but for convenience we say that $deg(P) = -\infty$.

3. *If $P = a_0$ such that $a_0 \in \mathbb{R}$, then P is a constant polynomial. In this case, if $a_0 \neq 0$ then $deg(P) = 0$.*

Example 1.1.

1. *$P_1(x) = x^2 + x + 2$ is a degree two polynomial in $\mathbb{Z}_3[x]$.*
2. *For every nonzero natural number m, the expression $P_2(x) = x^m - 3$ represents a degree m polynomial in $\mathbb{Z}_4[x]$.*
3. *$P_3(x) = -1$ is a degree zero polynomial in $\mathbb{Z}_2[x]$.*
4. *$g(x) = \pi x^3 + (1 + i)x$ is a degree three polynomial in the ring $\mathbb{C}[x]$.*

2 Operations on polynomials

Let the polynomials $P = \sum_{k=0}^{n} a_k x^k$ and $Q = \sum_{k=0}^{n} b_k x^k$, where the coefficients $a_k, b_k \in \mathbb{K}$.

- **Equality**:
$$P = Q \iff \forall k,\ a_k = b_k$$
- **Addition**:
$$\begin{aligned} P + Q &= \sum_{k=0}^{n} (a_k + b_k) x^k \\ &= \sum_{k=0}^{n} c_k x^n \end{aligned}$$
such that $c_k = a_k + b_k,\ k = \overline{0, n}$.
- **Multiplication**: Let the polynomials $P = \sum_{k=0}^{n} a_k x^k$ and $Q = \sum_{k=0}^{m} b_k x^k$, where $a_k, b_k \in \mathbb{K}$. Then
$$P \times Q = \sum_{k=0}^{r} c_k x^k$$
such that $r = n + m,\ c_k = \sum_{i+j=k} a_i + b_j$ with $k = \overline{0, r}$
- **Multiplication by scalars**: For any $\lambda \in \mathbb{K}$,
$$\lambda P = \sum_{k=0}^{n} \lambda a_k x^k$$

Property 2.1.
For any P, Q and R in $\mathbb{K}[X]$, the following statements are true

1. $0 + P = P, \qquad P + Q = Q + P, \qquad (P + Q) + R = P + (Q + R)$
2. $1.P = P, \qquad P \times Q = Q \times P, \qquad (P \times Q) \times R = P \times (Q \times R)$
3. $P \times (Q + R) = P \times Q + P \times R$

4. $deg(P \times Q) = deg(P) + deg(Q)$

5. $deg(P + Q) \leq \max\{deg(P), deg(Q)\}$

Definition 2.1 (Associated polynomials)**.**
*Let $P(x),\ Q(x) \in \mathbb{K}[X]$. The polynomials $P(x)$ and $Q(x)$ are said to be **associated** if there exists a unit u such that*

$$P(x) = uQ(x)$$

This means that $P(x)$ and $Q(x)$ are scalar multiples of each other by a unit factor.

Example 2.1. *The set of polynomials associated with $X^2 + 4$ in $\mathbb{Z}[X]$ is*

$$\{X^2 + 4, -(X^2 + 4)\}$$

since the only units in $\mathbb{Z}$ are 1 and -1.

Proposition 2.2.

1. *The relation "being associated" is an equivalence relation on $\mathbb{K}[X]$.*
2. *If P and Q are associated and have the same leading coefficient, then $P = Q$.*
3. *If $\mathbb{K}$ is a field, then every polynomial P is associated with a unique unitary polynomial.*

3 Polynomial Division

Definition 3.1. *Let $A, B \in \mathbb{K}[X]$, the polynomial B divides A if it exists $Q \in \mathbb{K}[X]$, such that $A = BQ$.*

Remark 3.1. *In the case where B divides A, one can write*

1. *$B|A$, or simply A is divisible by B.*
2. *A is a multiple of B.*

Example 3.1.

1. $A|A$
2. $1|A$
3. $A|\alpha A,\ \forall \alpha \in \mathbb{K}$
4. $A|0$

Proposition 3.2. *Let $A, B, C \in \mathbb{K}[X]$*

- *If $A|B$ and $B|A$, there exists $\gamma \in \mathbb{K}^*$ such that $A = \gamma B$.*
- *If $A|B$ and $B|C$ then $A|C$.*
- *If $C|A$ and $C|B$ then $C|(AU + BV)$ for all $U, V \in \mathbb{K}[X]$.*

Definition 3.2 (Euclidean Division of Polynomials)**.** *Let P, B be two polynomials in $\mathbb{K}[X]$, with $B \neq 0$. There there exists a pair $(Q, R) \in \mathbb{K}[X]^2$ such that*

$$P = QB + R, \text{ where } \deg(R) < \deg(B)$$

Q and R afre repectively the quotient and the rest of the Euclidean division.

Remark 3.2. *Note that $R = 0$ if and only if $B|A$.*

Example 3.3.
For the polynomials $A = X^3 + X^2 - 1$, and $B = X^2 + 1$, we have the following Euclidean division

$$\begin{array}{rrrr|rr} X^3 & +X^2 & -1 & & X^2 & +1 \\ \cline{5-6} X^3 & +X & & & X & +1 \\ \cline{1-3} & X^2 & -X & -1 & & \\ & X^2 & +1 & & & \\ \cline{2-4} & & -X & -2 & & \end{array}$$

then

$$\underbrace{X^3 + X^2 - 1}_{A} = \underbrace{(X^2 + 1)}_{B}\underbrace{(X + 1)}_{Q} + \underbrace{(-X - 2)}_{R}$$

Example 3.4.
For the polynomials $A = 2X^3 - X^2 - 2X + 1$, and $B = X^2 + X + 1$, we have the following Euclidean division

$$\begin{array}{rrrr|rrr} 2X^3 & -X^2 & -2X & +1 & X^2 & +X & +1 \\ \cline{5-7} 2X^3 & +2X^2 & +2X & & 2X & -3 & \\ \cline{1-3} & -3X^2 & -4X & +1 & & & \\ & -3X^2 & -3X & -3 & & & \\ \cline{2-4} & & -X & +4 & & & \end{array}$$

then

$$\underbrace{2X^3 - X^2 - 2X + 1}_{A} = \underbrace{(X^2 + X + 1)}_{B}\underbrace{(2X - 3)}_{Q} + \underbrace{(-X + 4)}_{R}$$

3.1 Greatest common divisor (gcd)

Proposition 3.5. *Let $A, B \in \mathbb{K}[X]$, with $A \neq 0$ or $B \neq 0$. There exists a unique unit polynomial of greatest degree which divides both A and B. This unique polynomial is called the gcd (greatest common divisor) of A and B which we note* $\gcd(A, B)$.

Remark 3.3.

- $\gcd(A, B)$ *is a unit polynomial*
- *If $A|B$ and $A \neq 0$,* $\gcd(A, B) = \frac{1}{\lambda}A$, *where λ is the dominant coefficient of A*
- *For all $\lambda \in \mathbb{K}^*$,* $\gcd(\lambda A, B) = \gcd(A, B)$
- *If $A = BQ + R$ then* $\gcd(A, B) = \gcd(B, R)$.

3.2 Euclid's algorithm

Let A and B be polynomials, $B \neq 0$, we calculate the successive Euclidean divisions as follows

$$\begin{aligned}
A &= BQ_1 + R_1, \quad \deg R_1 < \deg B \\
B &= R_1Q_2 + R_2, \quad \deg R_2 < \deg R_1 \\
R_1 &= R_2Q_3 + R_3, \quad \deg R_3 < \deg R_2 \\
&\vdots \\
R_{k-2} &= R_{k-1}Q_k + R_k, \quad \deg R_k < \deg R_{k-1} \\
R_{k-1} &= R_kQ_{k+1}
\end{aligned}$$

The degree of the remainder decreases with each division. The algorithm is stopped when the remainder is zero. The gcd is the last non-zero remainder R_k.

Example 3.6. *Let's calculate the gcd of $A = X^4 - 1$ and $B = X^3 - 1$. We apply Euclid's algorithm*

$$\begin{aligned}
X^4 - 1 &= X(X^3 - 1) + X - 1 \\
X^3 - 1 &= (X^2 + X + 1)(X - 1) + 0
\end{aligned}$$

The gcd is the last non-zero remainder, i.e

$$\gcd(X^4 - 1, X^3 - 1) = X - 1$$

Definition 3.3. *Let $A, B \in \mathbb{K}[X]$. We say that A and B are coprime if* $\gcd(A, B) = 1$

Example 3.7. *$A = X^3 + X^2 + X + 1$, $B = X^2 + X + 1$ Are coprime.*

Remark For any A, B we can reduce to coprime polynomials: if $\gcd(A, B) = D$ then A and B are written: $A = DA'$, $B = DB'$ with $\gcd(A', B') = 1$.

3.3 Bézout's theorem

Theorem 3.8. *Let $A, B \in \mathbb{K}[X]$ be polynomials such that $A \neq 0$ or $B \neq 0$. We note $D = \gcd(A, B)$. There exist two polynomials $U, V \in \mathbb{K}[X]$ such that $AU + BV = D$.*

This theorem follows from Euclid's algorithm and more specifically from its ascent as we see in the following example

Example 3.9. *We know that*

$$\gcd(X^4 - 1, X^3 - 1) = X - 1$$

and we have

$$X^4 - 1 = X(X^3 - 1) + X - 1 \Rightarrow 1(X^4 - 1) - X(X^3 - 1) = X - 1$$

Then $U = 1$ and $V = -X$.

Corollary 3.10. *Let A and B be two polynomials. A and B are coprime if and only if there exist two polynomials U and V such that $AU + BV = 1$.*

Example 3.11. *$A = X^3 + X^2 + X + 1$, $B = X^2 + X + 1$ are coprime because*

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

thus

$$A = XB + 1$$

therefore

$$A(1) + B(-X) = 1$$

Corollary 3.12. *Let $A, B, C \in \mathbb{K}[X]$ be polynomials such that $A \neq 0$ or $B \neq 0$. If $C|A$ and $C|B$ then $C|\gcd(A, B)$.*

Corollary 3.13 (Gauss lemma)**.** *Let $A, B, C \in \mathbb{K}[X]$. If $A|BC$ and $\gcd(A, B) = 1$ then $A|C$.*

3.4 Least common multiple (lcm)

Definition 3.4. *Let $A, B \in \mathbb{K}[X]$ be non-zero polynomials, then there exists a unique unitary polynomial M of smallest degree such that $A|M$ and $B|M$. This unique polynomial is called the lcm (least common multiple) of A and B, which we denote by $lcm(A, B)$.*

Example 3.14.
It's clear that

$$lcm(X(X-2)^2(X^2+1)^4, (X+1)(X-2)^3(X^2+1)^3) = X(X+1)(X-2)^3(X^2+1)^4$$

Proposition 3.15. *Let $A, B \in \mathbb{K}[X]$ be non-zero polynomials and $M = lcm(A, B)$, if $C \in \mathbb{K}[X]$ is a polynomial such that $A|C$ and $B|C$, then $M|C$.*

4 Roots of a polynomial

4.1 Roots and degree

Definition 4.1. *Let $P = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_2X^2 + a_1X + a_0 \in \mathbb{K}[X]$ and let $\alpha \in \mathbb{K}$. For an element $x \in \mathbb{K}$, we note $P(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_2x^2 + a_1x + a_0$. We say that α is a root (or a zero) of P if*

$$P(\alpha) = 0$$

Example 4.1. *$\alpha = 2$ is a root of $P(x) = x^2 - x - 2$ because $P(2) = 0$.*

Proposition 4.2. *$P(\alpha) = 0 \Leftrightarrow x - \alpha$ divides P.*

Example 4.3.
$P(x) = x^3 + 5x^2 + 3x - 9$, $P(-3) = 0$ then $(x + 3)$ divides $P(x)$ indeed $P(x) = (x + 3)(x^2 + 2x - 3)$.

Definition 4.2. *Let $k \in \mathbb{N}^*$. We say that α is a root of multiplicity k of P if $(x - \alpha)^k$ divides P while $(x - \alpha)^{k+1}$ does not divide P. When $k = 1$ we say that α is a simple root, when $k = 2$ we say that α is a double root, etc. We also say that α is a root of order k.*

Proposition 4.4. *The following assertions are equivalent*

a) α *is a root of multiplicity* k *of* P.

b) There exists $Q \in \mathbb{K}[X]$ *such that* $P = (x-\alpha)^k Q$, *with* $Q(\alpha) \neq 0$.

c) $P(\alpha) = P'(\alpha) = P''(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0$ *and* $P^{(k)}(\alpha) \neq 0$.

Example 4.5.
2 *is a root of multiplicity 3 of* $P(x) = x^5 - 14x^4 + 75x^3 - 194x^2 + 244x - 120$ *because* $P(2) = P'(2) = P''(2) = 0$ *and* $P^{(3)}(2) \neq 0$.

$\forall x \in \mathbb{R}$, $P'(x) = 5x^4 - 56x^3 + 225x^2 - 388x + 244$ $P''(x) = 20x^3 - 168x^2 + 450x - 388$ $P^{(3)}(x) = 60x^2 - 336x + 450$

4.2 d'Alembert-Gauss theorem

Theorem 4.6 (d'Alembert-Gauss theorem)**.** *Any polynomial with complex coefficients of degree* $n \geq 1$ *has at least one root in* $\mathbb{C}$. *It admits exactly* n *roots if we count each root with multiplicity.*

Theorem 4.7. *Let* $P \in \mathbb{K}[X]$ *of degree* $n \geq 1$. *Then* P *admits at most* n *roots in* $\mathbb{K}$.

4.3 Decomposition into a product of irreducible factors

Definition 4.3. *Let* $P \in \mathbb{K}[X]$ *be a polynomial of degree* ≥ 1, *we say that* P *is irreducible if for all* $Q \in \mathbb{K}[X]$ *dividing* P, *then, either* $Q \in \mathbb{K}^*$, *or there exists* $\lambda \in \mathbb{K}^*$ *such that* $Q = \lambda P$.

Remark 4.1.

1. *An irreducible polynomial* P *is therefore a non-constant polynomial whose only divisors of* P *are the constants or* P *itself.*
2. *The notion of an irreducible polynomial for the arithmetic of* $\mathbb{K}[X]$ *corresponds to the notion of a prime number for the arithmetic of* $\mathbb{Z}$.
3. *Otherwise, we say that* P *is reducible; there then exist polynomials* A, B *of* $\mathbb{K}[X]$ *such that* $P = AB$, *with* $\deg A \geq 1$ *and* $\deg B \geq 1$.

Example 4.8.

- *All polynomials of degree 1 are irreducible. Therefore there are infinitely many irreducible polynomials.*
- $X^2 - 4 = (X-2)(X+2)$ *is reducible.*
- $X^2 + 9 = (X - 3i)(X + 3i)$ *is reducible in* $\mathbb{C}[X]$ *and irreducible in* $\mathbb{R}[X]$.

Proposition 4.9 (Euclid's Lemma)**.** *Let* $P \in \mathbb{K}[X]$ *be an irreducible polynomial and let* $A, B \in \mathbb{K}[X]$. *If* $P|AB$ *then* $P|A$ *or* $P|B$.

Theorem 4.10. *Any non-constant polynomial $A \in \mathbb{K}[X]$ is written as a product of unitary irreducible polynomials: $A = \lambda P_1^{k_1} P_2^{k_2} \dots P_r^{k_r}$. Where $\lambda \in \mathbb{K}^*$, $r \in \mathbb{N}^*$, $k_i \in \mathbb{N}^*$ and P_i are distinct irreducible polynomials. Moreover, this decomposition is unique up to the order of the factors.*

This is of course the analogue of the decomposition of a number into prime factors.

Theorem 4.11. *The irreducible polynomials of $\mathbb{C}[X]$ are the polynomials of degree 1.*

Therefore for $P \in \mathbb{C}[X]$ of degree $n \geq 1$ the factorization is written $P = \lambda(X - \alpha_1)^{k_1}(X - \alpha_2)^{k_2} \cdots (X - \alpha_r)^{k_r}$, where $\alpha_1, \dots, \alpha_r$ are the distinct roots of P and $k_1, \dots, k_r$ are their multiplicities.

Example 4.12.
$P(X) = (X-1)^2(X^2+4)^2(X^2+2)(X^2+X+1)$ is already decomposed into irreducible factors in $\mathbb{R}[X]$ while its decomposition in $\mathbb{C}[X]$ is

$P(X) = (X-1)^2(X-2i)^2(X+2i)^2(X-i\sqrt{2})(X+i\sqrt{2})(X-j)(X-j^2)$

where $j = e^{\frac{2i\pi}{3}} = \frac{-1+i\sqrt{3}}{2}$.

Tutorial Sheet 06

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:

I) Determine $\lambda \in]0, \infty[$ such that $P = X^3 - 3X + \lambda$ has a double root. What is the other root of P?
II) Let $n \in \mathbb{N}$. Show that the polynomial $P_n = 1 + X + \frac{X^2}{2} + \frac{X^3}{3!} + \cdots + \frac{X^n}{n!}$ does not have multiple roots.

Exercise 3:

Divide A by B using Euclidean division for the following cases:

1. A = $3X^5 + 4X^2 + 1$ and B = $X^2 + 2X + 3$.
2. A = $3X^5 + 2X^4 - X^2 + 1$ and B = $X^3 + X + 2$.
3. A = $X^4 - X^3 + X - 2$ and B = $X^2 - 2X + 4$.

Exercise 4:

Let P, Q, R, S $\in \mathbb{K}[X]$. Prove that

1. If P | Q and Q | P then P and Q are associated.
2. If P is associated to R and Q is associated to S then P | Q $\Leftrightarrow$ R | S.

Exercise 5:

Let P, Q, R, S $\in \mathbb{K}[X]$. Prove the following statements

1. If P | Q and Q | R then P | R.
2. If P | Q and P | R then P | Q + R.
3. If P | Q and Q $\neq 0$ then deg(P) $\leq$ deg(Q).
4. If P | Q and R | S then PR | QS.
5. If P | Q then $P^n | Q^n$ for all n ≥ 1.

Exercise 6:

Find the gcd of the following polynomials:

1. $X^3 - X^2 - X - 2$ and $X^5 - 2X^4 + X^2 - X - 2$.
2. $X^4 + X^3 - 2X + 1$ and $X^3 + X + 1$.

Exercise 7:

1. Reducible polynomials in $\mathbb{K}[X]$ have degree greater than or equal to 2.
2. All polynomials of degree 1 are irreducible.

Exercise 8:

Determine all polynomials $P \in \mathbb{R}[X]$ such that P' devides P.

Previous Exams

Algebra 1 Exam - First session

Time: $1^h : 30$

The use of calculator is strictly prohibited.

Exercise 1: (6 pts)

State whether the following are **True** or **False**, and **Justify** your answer

1. The addition $(+)$ is an internal operation in the set $\{-5,-2,0,1,6\}$.
2. For every two statements p and q, the expression $(p \vee \bar{p}) \wedge q$ has the same truth value as q.
3. For every non-empty sets A, B and C: $\overline{(A \cup B)} \cap \overline{(C \cup \bar{A})} = \Phi$.
4. For any two mappings f and g: $f \circ g(x) = g \circ f(x)$.
5. The cosine function is bijective on $[-\pi, \pi]$.
6. $\exists x \in \mathbb{R}^*, \forall y \in \mathbb{R}^* : \ xy = 1$.

Exercise 2: (7 pts)

I) Let the mapping $f : \mathbb{R} - \{-3\} \to F$ defined by $f(x) = \frac{x}{x+3}$.

1. Is f injective ?
2. Find the set F such that f be a surjective mapping.

II) Let the binary relation defined by

$$a \mathscr{R} b \iff a^2 - b^2 = a - b, \qquad \forall a, b \in \mathbb{R}$$

1. Prove that $\mathscr{R}$ is an equivalence relation.
2. Find the equivalence class of 7.

Exercise 3: (7 pts)

Consider the set of real numbers $\mathbb{R}$ equipped with the following operations $\oplus$ and $\otimes$, defined for all $x, y \in \mathbb{R}$ as

$$x \oplus y = x + y - 1, \qquad x \otimes y = x + y - xy$$

Prove that the algebraic structure $(\mathbb{R}, \oplus, \otimes)$ is a field.

Algebra 1 Exam - First session

Time: $1^h : 30$

The use of calculator is strictly prohibited.

Exercise 1: (6 pts)

State whether the following are **T**rue or **F**alse, **J**ustify your answer

1. The algebraic structure $(\mathbb{N}, +)$ is a group.
2. For every statement p, the statement (p or $\bar{p}$) is always true.
3. If the mappings $f = \{(5,2),(6,3)\}$ and $g = \{(2,5),(3,6)\}$, then $f \circ g = \{(2,2),(3,2)\}$.
4. For any non-empty set E, the binary relation $\subset$ represents a total order relation in $\mathscr{P}(E)$.
5. The mapping $g : \mathbb{R} \to \mathbb{R}$ defined as $g(x) = x|x|$ is bijective.

Exercise 2: (7 pts)

Let the mapping $f(x) = \frac{1}{x-1}$ such that $x \neq 1$.
I) Let $g(x) = \frac{1}{x} + 1$, $x \neq 0$.

1. Compute $f \circ g$ and $g \circ f$.
2. What do you deduce ?

II) Let $\mathscr{R}$ be the binary relation defined on $\mathbb{R}\backslash\{1\}$ by

$$\forall x, y \in \mathbb{R} : \quad x \mathscr{R} y \iff |f(x)| = |f(y)|$$

1. Prove that $\mathscr{R}$ is an equivalence relation.
2. Find the equivalence classe of 0.

Exercise 3: (7 pts)

Consider the set $G = \mathbb{R}\backslash\{-1\}$, and the operation $\odot$ defined as

$$x \odot y = x + y + x.y, \qquad \forall x, y \in G$$

1. Prove that $\odot$ is an internal composition law in G.
2. Prove that $(G, \odot)$ is a commutative group.
3. Solve in G the equation: $2 \odot x \odot 3 = 7$.

20 août 1955 - Skikda University

Faculty of Technology | Specialized engineering | Department of Technology

Level: First Year | Academic year: 2023-2024

Algebra 1 Exam - Second Session

Time: $1^h : 30$

The use of calculator is strictly prohibited.

Exercise 1: (7.5 pts)

State whether the following are **T**rue or **F**alse, **J**ustify your answer

1. For any statement P, the statement $(P \wedge \overline{P})$ is always false.
2. The addition $(+)$ is an internal operation in the set $\{-3,-1,0,1,3\}$.
3. Let the nonempty set E. For any two sets $A, B \in \mathscr{P}(E)$: $(A \cup B)^c \neq A^c \cap B^c$
4. For any two mappings f and g: $f \circ g(x) = g \circ f(x)$.
5. For any mapping f: $f \circ f(x) = f^2(x)$.
6. In the set of complex numbers $\mathbb{C}$ the relation $z\,R\,z' : |z| \leq |z'|$ represents an order relation.
7. The mapping $f : \mathbb{R} \to \mathbb{R}^+$ defined by $f(x) = x^2$ is injective.
8. Every surjective mapping is bijective.

Exercise 2: (5.5 pts)

Let the mapping $f : E \to F$ defined by $f(x) = \frac{x}{x+3}$.

1. Find E the domain of definition of f.
2. Compute $f \circ f$.
3. Prove that f is injective.
4. Find the set F such that f be a surjective mapping.

Exercise 3: (7 pts)

Let the internal composition law Δ defined in $\mathbb{R}$ as

$$\forall x, y \in \mathbb{R} : \quad x \Delta y = x.y + (x^2 - 1).(y^2 - 1)$$

1. Compute $(2\Delta 3)\Delta 4$ and $2\Delta(3\Delta 4)$, what do you deduce?
2. Prove that Δ is commutative and find its identity element in $\mathbb{R}$.
3. Is $(\mathbb{R}, \Delta)$ a group?

Bibliography

[1] C. Baba Hamed, K. Benhabib, Algèbre I, Rappel de cours et exercices avec solutions. O.p.u, 1985.

[2] C. Degrave et D. Degrave, Algèbre 1ère année : cours, méthodes, exercices résolus, Bréal, 2003.

[3] D. Duverney, S. Heumez, G. Huvent, Toutes les mathématiques - Cours, exercices corrigés - MPSI, PCSI, PTSI, TSI, Ellipses, 2004.

[4] J. Franchini et J. C. Jacquens, Algèbre : cours, exercices corrigés, travaux dirigés, Ellipses, Paris, 1996.

[5] M. Mignotte et J. Nervi, AlgÃ¨bre : licences sciences 1ère année, Ellipses, Paris, 2004.

[6] M.L. O'Leary, A first course in mathematical logic and set theory. John Wiley, 2015.

[7] M. Serfati, Exercices de mathématiques. 1. Algèbre, Belin, Collection DIA, 1987.