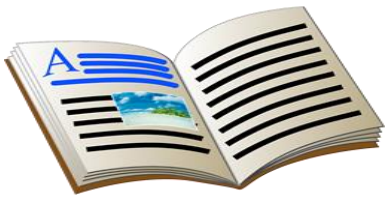
الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Akli Mohand Oulhadj - Bouira -
ⵜⴰⵙⴷⴰⵡⵉⵜ ⴰⴽⵍⵉ ⵎⵓⵃⴻⵏⴷ ⵓⵍⵃⴰⵊ - ⵜⵓⴱⵉⵔⴻⵜ -
Faculté des Sciences Exactes

وزارة التعليم العالي والبحث العلمي
جامعة أكلي محند أولحاج
- البويرة -
كلية العلوم الدقيقة

Département de Mathématiques



Polycopié de cours

En : Informatiques

Spécialité : Systèmes Informatiques (SI)

Niveau : Licence 1

Algèbre 1

Par BOUCHAL LYDIA

Année :2025-2026

Algebra 1 Courses

Dr. BOUCHAL LYDIA

Department of Mathematics, Faculty of Exacts Sciences,
10000, University of Bouira.

Version 1: 2025-2026.

May 25, 2026

Contents

Introduction

Algebra constitutes one of the essential foundations of mathematics and plays a central role in computer science education. It provides the conceptual tools necessary to model, structure, and analyze abstract objects, as well as to formalize rigorous reasoning.

I started writing this handout in my first year of teaching at the University of Bouira in 2024-2025, dedicated to the first year computer science students in the computer science department, and then in 2025-2026 taught in the common core computer science department, where I directed the Algebra 1 module. The objective of this Algebra 1 handout is to introduce the fundamental notions of mathematical logic, sets and applications, binary relations, and the main algebraic structures, such as groups, rings, and fields, as well as the study of polynomials. These concepts form an essential foundation for further studies in mathematics and computer science.

This document is organized into five chapters. Chapter 1 begins with the notions of logic and methods of reasoning. Chapter 2 introduces sets and applications. Subsequently, we present binary relations and fundamental algebraic structures in Chapter 3 and 4 respectively, and concludes with Chapter 5 which presents polynomial rings . Altogether, these elements will enable students to acquire the necessary foundations for understanding the mathematical tools used in computer science.

This handout serves as a pedagogical resource to support lectures, tutorials, and the student's individual work.

This is the first version of the document. Please send your comments and remarks to the email address provided below.

Lydia BOUCHAL
Bouira University, 28 February 2026
e-mails: l.bouchal@univ-bouira.dz
Bouchal_Lydia@outlook.com

Chapter 1

Logical notions

The philosopher Aristotle is often called the father of logic. Logic is about the rules of clear thinking and reasoning. These logical rules provide meaning to mathematical expressions, verify the correctness of programs and algorithms in computer science, and help construct some proofs in software systems.
This chapter presents some fundamentals of logical concepts.

1.1 Definitions

Definition 1.1 (Proposition)

A statement or proposition, is a declarative sentence that is either true or false, but never both at the same time.
To represent statements, we use capital letter P, Q, R, and so on.

Examples 1.1.

1. P_1:*"Algiers is the capital of Algeria" is a true statement.*
2. P_2:*"*25 *is a multiple of* 5*" is a true statement.*
3. P_3:*"The number of letters in the English alphabet is* 12*" is a false statement.*
4. P_4:*"*$7^2 = 48$*" is a false statement.*
5. P_5:*"*$\sqrt{2}$*" is not a statement, because it does not have a truth value.*
6. P_6:*"The number* x *is even" is not a statement, because we cannot determine whether it is true or false without knowing the value of* x*.*

7. *P_7:"The integer n divides 12" is not a statement, because we cannot determine whether it is true or false without knowing the value of n.*

Remark 1.1

1. A statement that is always true is called tautology.
2. In general sentences that express questions, exclamations, opinions and orders are not statements.

Examples 1.2.

(P): *"$x^2 \geq 0$ for all real number x", (P) is a tautology because it is always true.*

(Q): *"$|x| \geq 0$ for all real number x", (Q) is a tautology because it is always true.*

Definition 1.2 (Predicat)

A predicat is a sentence that depends on one or more variables, it is true for certain values assigned to the variables and false for other values. It is denoted by $P(x)$ or $P(x, y)$.

Examples 1.3.

P(x): *"$x < 8$" this proposition is true for values of x strictly less than 8, false for other values of x.*

Q(x): "$e^x \geq 1$"
- ↗ *True if $x \geq 0$.*
- ↘ *False if $x < 0$.*

P(x,y): *"$x^2 + y^2 = x + y$".*

1.2 Logical connectors

Logical connectors, also known as logical operators, are used to combine two or more simple propositions to formulate new propositions.

1.2.1 Negation

Negation

The negation of a proposition P, denoted by $\overline{P}$ or $\rceil P$ or not(P) which is read "not P", has the truth value that is the opposite of the truth value of P; that is, when P is true, then $\overline{P}$ is false, and vice versa.

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

Table 1.1: Truth table for the negation of a proposition.

Examples 1.4.

(P)**:** *"5 is odd" then* $(\overline{P})$ *is "5 is even".*

(Q)**:** *"*$x \leq 17$ *" then* $(\overline{Q})$ *is "*$x > 17$*".*

(R)**:** *"It is raining" then* $(\overline{R})$ *is "It is not raining".*

1.2.2 Conjunction

Conjunction

The conjunction of two propositions P and Q, is the proposition denoted by $(P \wedge Q)$ and read "P and Q". The proposition $(P \wedge Q)$ is true if and only if both P and Q are true at the same time, and it is false in all other cases.

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

Table 1.2: Truth table for the conjunction of two propositions.

Examples 1.5.

1. *"*$(3 > 2) \wedge (9$ *is odd* $)$*" is a true proposition.*
2. *"*$(8 > 4) \wedge (1 < 5)$*" is a false proposition.*

3. *"$n \in \mathbb{N}^*$ is even and odd number" is a false proposition.*
4. *"$(x > -1) \wedge (x < 1)$" means $|x| < 1$, this proposition is true.*
5. *"The sun is hot and water is a liquid", this proposition is true.*
6. *"Water boils at 50 degrees celsius and water freezes at 0 degrees celsius", this proposition is false, because water boils at 100 degrees celsius.*

1.2.3 Disjunction

Disjunction

The disjunction of two propositions P and Q, is the proposition denoted by $(P \vee Q)$ and read "P or Q".
The proposition $(P \vee Q)$ is false if and only if both P and Q are false, and $(P \vee Q)$ is true in all other cases.
In other words, $(P \vee Q)$ means "P is true, or Q is true, or both are true." This is called an inclusive disjunction.

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

Table 1.3: Truth table for the disjunction of two propositions.

Examples 1.6.

1. *"$(11 > 2) \vee (3$ is odd $)$" is a true proposition.*
2. *"$(14 \leq 8) \vee (3 < 2)$" is a false proposition.*
3. *"$n \in \mathbb{N}$ is even or odd number" is a true proposition.*
4. *"$(x \leq 2) \vee (x \geq 5)$".*
   If $x = 1$, then "$(x \leq 2) \vee (x \geq 5)$" is true.
   If $x = 3$, then "$(x \leq 2) \vee (x \geq 5)$" is false.

1.2.4 Implication

Implication

A proposition P implies another proposition Q, denoted by $(P \Rightarrow Q)$, read (P implies Q) or (if P, then Q).
The proposition $(P \Rightarrow Q)$ is false if P is true and Q is false and is true in all other cases.
The implication $(P \Rightarrow Q)$ can be read as:

- P is a sufficient condition for Q.
- Q is a necessary condition for P.

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

Table 1.4: Truth table of the implication.

Examples 1.7.

1. $(0 \leq x \leq 25 \Rightarrow \sqrt{x} \leq 5)$ *is a true proposition.*
2. $(2 + 2 = 5 \Rightarrow x = 2)$ *is a true proposition.*
3. *"If it rains, the road becomes wet."*
   In this proposition, if it rains, then the road will naturally be wet. If it does not rain, the road may be either wet or dry, depending on the circumstances. However, if it rains and the road remains dry, then something is wrong.
4. *"If you obey the law, you never go to prison."*
   In this proposition, people who follow the law don't expect to be imprisoned. Those who break it might be imprisoned, depending on the situation. However, if someone follows the law and is still sent to prison, they feel it is unfair.

Remark 1.2

1. The reciprocal implication of $(P \Rightarrow Q)$ is $(Q \Rightarrow P)$.
2. The contrapositive of the implication $(P \Rightarrow Q)$ is $(\overline{Q} \Rightarrow \overline{P})$.

1.2.5 Equivalence

Equivalence

A proposition P is equivalent to Q is denoted by $(P \Leftrightarrow Q)$, read "P if and only if Q", "if P, then Q, and conversely", or "P is a necessary and sufficient for Q". The equivalence between two propositions P and Q means $(P \Rightarrow Q$ and $Q \Rightarrow P)$.
The proposition $(P \Leftrightarrow Q)$ is true when P and Q have the same value of truth (both true or false simultaneously) and it is false when the propositions P and Q have different truth value.

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

Table 1.5: Truth table for the implication.

Examples 1.8.

1. *For real numbers x and y, $(|x| > |y|) \Leftrightarrow (x^2 > y^2)$.*
2. *For real numbers x and y, $x\,y = 0 \Leftrightarrow (x = 0) \vee (y = 0)$.*
3. *For $n \in \mathbb{N}$, n is even $\Leftrightarrow n^2$ is even.*
4. *"A number is even if and only if it is divisible by 2".*

Remark 1.3

1. Two propositions are equivalent if they have identical truth table.
2. The implication is equivalent to its contrapositive, but it is not equivalent to its reciprocal.

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

Table 1.6: Truth table of the implication, the reciprocal, and the contrapositive.

1.2.6 Exclusive or (Xor)

Exclusive or

A proposition "P or Q but not both" is denoted by $(P \oplus Q)$ read as "exlusive or of P and Q". The proposition $(P \oplus Q)$ is true when exactly one of the two P or Q is true and $(P \oplus Q)$ is false in all other cases.

P	Q	$P \oplus Q$
1	1	0
1	0	1
0	1	1
0	0	0

Table 1.7: Truth table for the exclusive or of two propositions.

Examples 1.9.

1. *Let the propositions be*

   P:"*Player A wins.*" Q:"*Player A wins.*"

   Then, $(P \oplus Q)$ *means: Either player A wins or player B wins, but not both.*

2. *Students chooses either Mathematics or Computer Science, but not both.*

3. *You must exactly take one of the two courses.*

Remark 1.4

The number of rows in a truth table is 2^n where n in the exponent represents the number of propositions, and 2 in the base indicates the two possible truth values (true or false).

- If we have two propositions P and Q, then the truth table has $2^2 = 4$ rows.
- If we have three propositions P, Q and R, then the truth table has $2^3 = 8$ rows.

Properties 1.1

Let P, Q and R be three propositions, the following equivalences are true:

1. $\overline{\overline{P}} \Leftrightarrow P$.
2. $\overline{(P \wedge Q)} \Leftrightarrow (\overline{P} \vee \overline{Q})$.
3. $\overline{(P \vee Q)} \Leftrightarrow (\overline{P} \wedge \overline{Q})$.
4. $(P \Rightarrow Q) \Leftrightarrow (\overline{Q} \Rightarrow \overline{P})$ (Contrapositive).
5. $(P \Rightarrow Q) \Leftrightarrow (\overline{P} \vee Q)$.
6. $\overline{(P \Rightarrow Q)} \Leftrightarrow (P \wedge \overline{Q})$.
7. $[P \vee (Q \vee R)] \Leftrightarrow [(P \vee Q) \vee R]$ ($\vee$ is associative).
   $[P \wedge (Q \wedge R)] \Leftrightarrow [(P \wedge Q) \wedge R]$ ($\wedge$ is associative).
8. $[P \vee (Q \wedge R)] \Leftrightarrow [(P \vee Q) \wedge (P \vee R)]$ ($\vee$ is distributive with respect to $\wedge$).
   $[P \wedge (Q \vee R)] \Leftrightarrow [(P \wedge Q) \vee (P \wedge R)]$ ($\wedge$ is distributive with respect to $\vee$).
9. $[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$.

Proof.
We use a truth table to rigorously demonstrate the validity of each proposition.

(i)

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

1. We have that $\overline{\overline{P}}$ and P have the same truth table, then $\overline{\overline{P}} \Leftrightarrow P$.
2. We have that $\overline{(P \wedge Q)}$ and $(\overline{P} \vee \overline{Q})$ have the same truth table, then $\overline{(P \wedge Q)} \Leftrightarrow (\overline{P} \vee \overline{Q})$.
3. We have that $\overline{(P \vee Q)}$ and $(\overline{P} \wedge \overline{Q})$ have the same truth table, then $\overline{(P \vee Q)} \Leftrightarrow (\overline{P} \wedge \overline{Q})$.

(ii)

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

1. We have that $P \Rightarrow Q$ and $\overline{Q} \Rightarrow \overline{P}$ have the same truth table, then $(P \Rightarrow Q) \Leftrightarrow (\overline{Q} \Rightarrow \overline{P})$.
2. We have that $P \Rightarrow Q$ and $\overline{P} \vee Q$ have the same truth table, then $(P \Rightarrow Q) \Leftrightarrow (\overline{P} \vee Q)$.
3. We have that $\overline{P \Rightarrow Q}$ and $P \wedge \overline{Q}$ have the same truth table, then $(\overline{P \Rightarrow Q}) \Leftrightarrow (P \wedge \overline{Q})$.

(iii)

P	Q	R	$Q \vee R$	$P \vee Q$	$P \vee (Q \vee R)$	$(P \vee Q) \vee R$	$Q \wedge R$	$P \wedge Q$	$P \wedge (Q \wedge R)$	$P \wedge (Q \wedge R)$
1	1	1	1	1	1	1	1	1	1	1
1	1	0	1	1	1	1	0	1	0	0
1	0	1	1	1	1	1	0	0	0	0
1	0	0	0	1	1	1	0	0	0	0
0	1	1	1	1	1	1	1	0	0	0
0	1	0	1	1	1	1	0	0	0	0
0	0	1	1	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0

1. We have that $[P \vee (Q \vee R)]$ and $[(P \vee Q \vee R)]$ have the same truth table, then
$$[P \vee (Q \vee R)] \Leftrightarrow [(P \vee Q \vee R)].$$
2. We have that $[P \wedge (Q \wedge R)]$ and $[(P \wedge Q \wedge R)]$ have the same truth table, then
$$[P \wedge (Q \wedge R)] \Leftrightarrow [(P \wedge Q \wedge R)].$$

(iv)

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

We have that $[P \wedge (Q \vee R)]$ and $[(P \wedge Q) \vee (P \wedge R)]$ have the same truth table, then
$$[P \wedge (Q \vee R)] \Leftrightarrow [(P \wedge Q) \vee (P \wedge R)].$$

P	Q	R	$Q \wedge R$	$P \vee (Q \wedge R)$	$P \vee Q$	$P \vee R$	$(P \vee Q) \vee (P \vee R)$
1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	0	0	0	1	1	1	1
0	1	1	1	1	1	1	1
0	1	0	0	0	1	0	0
0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	0

We have that $[P \vee (Q \wedge R)]$ and $[(P \vee Q) \wedge (P \vee R)]$ have the same truth table, then

$$[P \vee (Q \wedge R)] \Leftrightarrow [(P \vee Q) \wedge (P \vee R)].$$

□

1.3 Quantifiers

A predicate becomes a proposition by adding quantifiers. Consider the following propositions:
"Some students enjoy mathematics," "All birds can fly," "No humans can live without water," "At least one even prime number exists," and "Every morning the sun rises."
Each of these propositions contains a word that expresses quantity, such as "some", "all", "none", "one", and "every". These words are called quantifiers because they specify how many elements in a given set make the proposition true. There are two main types of quantifiers: the universal quantifier and existential quantifier.

1.3.1 Universal quantifier "∀"

Let X be a set, x a variable, and P a predicate whose statement depends on the elements x of X.

- "For every x in X, P is satisfied " is denoted by "$\forall x \in X,\ P(x)$", and is true if $P(x)$ is true for any element x of S.

The symbol $\forall$ reads "for every" or "for any" or "for all", is called the universal quantifier.

Examples 1.10.

1. *The proposition* $(\forall x \in \mathbb{Z},\ x \neq \frac{1}{2})$ *is true.*
2. *The proposition* $(\forall x \in \mathbb{R},\ -1 \leq \sin x \leq 1)$ *is true.*

1.3.2 Existential quantifier "$\exists$"

Let X be a set, x a variable, and P a predicate whose statement depends on the elements x of X.

- "There exists at least one value x in X, such that $P(x)$ is satisfied " is denoted by "$\exists x \in X :\ P(x)$", and is true if there is at least one x of X, for which $P(x)$ is true.

The symbol $\exists$ reads "there exists" or "there exists at least", is called the existential quantifier.

Remark 1.5

To show that $\exists x \in X :\ P(x)$ is true, it is enough to find one value for $x_0 \in X$ such that $P(x_0)$ is true.

Examples 1.11.

1. *The proposition* $(\exists x \in \mathbb{Z} :\ x > -2)$ *is true.*
   For example, if we choose $x_0 = 4$, *then* $x_0 \in \mathbb{Z}$ *and* $x_0 > -2$.

2. *The proposition* $(\exists x \in \mathbb{R} :\ x^2 = 9)$ *is true because, for example,* $x_0 = 3$ *satisfies* $x_0^2 = 9$.

Remark 1.6

1. The quantifier denoted by $\exists !$ means that "there exists a unique".
   "$\exists ! x \in X,\ P(x)$" means that there exists exactly one element x in X satisfying $P(x)$.

2. The negation of "$\forall x \in X,\ P(x)$" is "$\exists x \in X :\ \overline{P(x)}$", which means "there is at least one x such that $P(x)$ is false".

3. The negation of "$\exists x \in X :\ P(x)$" is "$\forall x \in X,\ \overline{P(x)}$", which means "for all x in X, $P(x)$ is false".

Examples 1.12.

1. $\overline{(\forall x \in \mathbb{R},\ \exists y \in \mathbb{R} :\ x + y = 0)} \Leftrightarrow (\exists x \in \mathbb{R} :\ \forall y \in \mathbb{R},\ x + y \neq 0)$.

2. $\overline{(\exists y \in \mathbb{R} :\ \forall x \in \mathbb{R},\ x + y = 0)} \Leftrightarrow (\forall y \in \mathbb{R},\ \exists x \in \mathbb{R} :\ x + y \neq 0)$.

Remark 1.7

1. The order of different quantifiers in a statement is very important.
   For example, the propositions

$$(\forall x \in X, \exists y \in X : \ P(x,y)) \text{ and } (\exists y \in X : \forall x \in X, \ P(x,y))$$

   are completely different.
   In the first one, the value y depend on x and in the second one, a single y must work for all x.

2. In a statement, when quantifiers are all universal quantifiers or they are all existential quantifiers, the order of the variables can be changed without affecting the truth value of the proposition.

$$(\forall x \in X, \ \forall y \in X, \ P(x,y)) \Leftrightarrow (\forall y \in X, \ \forall x \in X, \ P(x,y)).$$

$$(\exists x \in X, \ \exists y \in X, \ P(x,y)) \Leftrightarrow (\exists y \in X, \ \exists y \in X, \ P(x,y)).$$

Examples 1.13.

1. $\exists! a \in \mathbb{R}, \forall x \in \mathbb{R} : \ x + a = x$, *here* $a = 0$ *is the unique solution.*

2. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : \ x + y = 0.$
   This proposition means "for every real number x*, there exists a real number* y*" (possibly depending on* x*) "such that* $x + y = 0$*."*
   For each x*, we can choose* $y = -x$*. Therefore, this proposition is true.*

3. $\exists y \in \mathbb{R} : \forall x \in \mathbb{R}, \ x + y = 0.$
   This proposition means "there exists a real number y *such that for all real numbers* x*,* $x + y = 0$*."*
   This would require one value for y *to satisfy the equation for all* x*, which is impossible. Therefore, this proposition is false.*

Remark 1.8

$$\overline{(\exists! x \in X, \ P(x))} \Leftrightarrow \left[(\forall x \in X, \ \overline{P(x)}) \text{ or } (\exists\, x, y \in X, \ : P(x) \text{ and } P(y) \text{ and } x \neq y\right].$$

Examples 1.14.

1. *The negation of the proposition* $(\exists! x \in \mathbb{N} : x \leq 6)$ *is*

$$\left[(\forall x \in \mathbb{N}, \overline{P(x)} : x > 6) \text{ or } (\exists x, y \in \mathbb{N} : x \leq 6 \text{ and } y \leq 6 \text{ and } x \neq y\right].$$

1.4 Types of reasoning

To show that the proposition $(P \Rightarrow Q)$ is true, one can use the following methods:

1.4.1 Reasoning by truth table

To show that a proposition is true, we verify that its truth table contains only true values.

Examples 1.15. *Let P and Q be two propositions. Show that $[\overline{P} \Rightarrow (Q \vee \overline{P})]$ is true, whatever the truth values of P and Q.*

P	Q	$\overline{P}$	$Q \vee \overline{P}$	$\overline{P} \Rightarrow (Q \vee \overline{P})$
1	*1*	*0*	*1*	*1*
1	*0*	*0*	*0*	*1*
0	*1*	*1*	*1*	*1*
0	*0*	*1*	*1*	*1*

1.4.2 Direct reasoning

To show that $P \Rightarrow Q$ is true, we assume that the statement P is true, and we use what we know about P to deduce that the statement Q is true.

Example 1.1. *Show that the product of two odd numbers is an odd number.*
Let a and b be two odd numbers.
Then, there exist integers $n, m \in \mathbb{Z}$ such that

$$a = 2m + 1,\ b = 2n + 1.$$

Then

$$\begin{aligned} a.b = &\ (2m+1)(2n+1) \\ = &\ 4mn + 2m + 2n + 1 \\ = &\ 2(2mn + m + n) + 1. \end{aligned}$$

Since $(2mn + n + m) \in \mathbb{Z}$, let $k = 2mn + n + m$.
Thus $a.b = 2k + 1$ which is the general form of an odd number.
Therefore, the product $a.b$ is an odd number.

Example 1.2. *Show that if $a, b \in \mathbb{Q}$ then $a + b \in \mathbb{Q}$.*

$$\begin{aligned} a, b \in \mathbb{Q} &\Rightarrow \exists p, p' \in \mathbb{Z} \text{ and } q, q' \in \mathbb{Z}^*, \text{ such that } a = \tfrac{p}{q},\ b = \tfrac{p'}{q'} \\ &\Rightarrow a + b = \tfrac{p}{q} + \tfrac{p'}{q'} = \tfrac{pq' + p'q}{qq'},\ (pq' + p'q) \in \mathbb{Z}, qq' \in \mathbb{Z}^* \\ &\Rightarrow a + b \in \mathbb{Q}. \end{aligned}$$

Remark 1.9

When direct proof of $P \Rightarrow Q$ is difficult to construct, we can instead use an indirect proof. Indirect proofs do not start with supposing that P is true and end with the conclusion that Q is true.
There are two types of indirect proofs: proof by contraposition and proof by contradiction.

1.4.3 Reasoning by contrapositive (contraposition)

It is based on the equivalence $(P \Rightarrow Q) \Leftrightarrow (\overline{Q} \Rightarrow \overline{P})$.
To show that $(P \Rightarrow Q)$ is true, we assume that $\overline{Q}$ is true and we show that $\overline{P}$ is true.

Example 1.3. *Show that* $\forall n \in \mathbb{N}:$ n^2 *is even* $\Rightarrow n$ *is even.*
It is enough to show that its contrapositive is true: n *is odd* $\Rightarrow n^2$ *is odd.*
We suppose that n *is odd and we show that* n^2 *is odd. We have*

$$\begin{aligned} n \text{ is odd} &\Rightarrow \exists k \in \mathbb{N},\ n = 2k+1 \\ &\Rightarrow n^2 = (2k+1)^2,\ k \in \mathbb{N} \\ &\Rightarrow n^2 = (4k^2+2k+1),\ k \in \mathbb{N} \\ &\Rightarrow n^2 = 2(k^2+k)+1,\ k \in \mathbb{N} \\ &\Rightarrow n^2 = 2k'+1,\ k' = (k^2+k) \in \mathbb{N} \\ &\Rightarrow n^2 \text{ is odd}. \end{aligned}$$

Then the contrapositive is true.
Conclusion: $\forall n \in \mathbb{N}:$ n^2 *is even* $\Rightarrow n$ *is even.*

1.4.4 Reasoning by contradiction

It is based on the equivalence $(\overline{P \Rightarrow Q}) \Leftrightarrow (P \wedge \overline{Q})$.
To show that $(P \Rightarrow Q)$ is true, we assume that P is true and that Q is false, and we look for a contradiction.

Example 1.4. *Let* $x, y \geq 0$, *show that* $\frac{x}{1+y} = \frac{y}{1+x} \Rightarrow x = y$.
We reason by contradiction, we assume that $\frac{x}{1+y} = \frac{y}{1+x}$ *and* $x \neq y$, *then*

$$\begin{aligned} \tfrac{x}{1+y} = \tfrac{y}{1+x} &\Rightarrow x(1+x) = y(1+y) \\ &\Rightarrow x + x^2 = y + y^2 \\ &\Rightarrow x^2 - y^2 = y - x \\ &\Rightarrow (x-y)(x+y) = y - x \\ &\Rightarrow (x-y)(x+y) = -(x-y) (\text{ we divide by } x-y \text{ because } x \neq y) \\ &\Rightarrow x + y = -1 \end{aligned}$$

contradiction, because $x, y \geq 0$ and the sum of positive numbers is always positive.
Then we conclude that $\forall x, y \geq 0,\ \frac{x}{1+y} = \frac{y}{1+x} \Rightarrow x = y$.

1.4.5 Reasoning by counter example

Let X be a set, x a variable, and P a predicate whose statement depends on the elements x of X. To show that a proposition $(\forall x \in X,\ P(x))$ is false, we show that its negation $(\exists x \in X,\ \overline{P(x)})$ is true.
Then to show that $(\forall x \in X,\ P(x))$ is false, we provide a counter example by giving an element $x \in X$ that does not satisfy $P(x)$.

Example 1.5. *Show that $\forall a, b \in \mathbb{R}_+$ the identity $\sqrt{a^2 + b^2} = a + b$ is false.*
Counter example:
We take $a = 3$, $b = 4$ we obtain $\sqrt{a^2 + b^2} = \sqrt{3^2 + 4^2} = \sqrt{25} = 5$ and $a + b = 3 + 4 = 7$.
Then the equality $\sqrt{a^2 + b^2} = a + b$ is false.

Example 1.6. *Show that the following assertion is false*

"Any positive number is the sum of three squares less than that integer".

Counter example:
For the integer 7.
The squares less than 7 are: $0^2, 1^2, 2^2$ but $0^2 + 1^2 + 2^2 = 5 \neq 7$

Example 1.7. *Let $f : \mathbb{R} \to \mathbb{R}$ be a function defined by $f(x) = x^2$.*
Show that the following proposition is false:

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

Counter example: *We have $f(2) = f(-2) = 4$ but $2 \neq -2$.*

Example 1.8. *Let f and g be two functions defined on $\mathbb{R}$ such that*

$$\lim_{x \to +\infty} f(x) = +\infty \text{ and } \lim_{x \to +\infty} g(x) = -\infty$$

Can we conclude that $\lim_{x \to +\infty} (f(x) + g(x)) = 0$?
Counter example: *We take $f(x) = x^2$, $g(x) = -x$, we have*

$$\lim_{x \to +\infty} f(x) = \lim_{x \to +\infty} x^2 = +\infty$$

and

$$\lim_{x \to +\infty} g(x) = \lim_{x \to +\infty} -x = -\infty$$

but

$$\lim_{x \to +\infty} (f(x) + g(x)) = \lim_{x \to +\infty} (x^2 - x) = \lim_{x \to +\infty} x^2(1 - \frac{1}{x}) = +\infty \neq 0.$$

Then $\lim_{x \to +\infty} (f(x) + g(x)) = 0$ is false.

1.4.6 Reasoning by induction

To show that a logical statement $P(n)$ is true for each $n \in \mathbb{N}$, we use the proof by induction, it is done in three steps:

1. **Initialization:** We show that $P(n)$ is true for the first value of n.
2. **Heredity:** We assume that the statement $P(n)$ is true for a fixed n, and we show that $P(n+1)$ is true, by using the fact that $P(n)$ is true.
3. **Conclusion:** Deduce that the statement $P(n)$ is true for all natural number n.

Example 1.9. *Show that* $\forall n \in \mathbb{N} : \sum_{k=0}^{n} k = \frac{n(n+1)}{2} \ldots P(n)$.
We use the proof by induction.

1. **Initialization:** *For* $n = 0$, $0 = \frac{0(0+1)}{2} = 0$, *then* $P(0)$ *is true.*

2. **Heredity:** *We assume that the statement* $P(n)$ *is true for a fixed* n, *that is* $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ *is true and we prove that the statement* $P(n)$ *is true at order* $(n+1)$. *we want to show that*

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

We have

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

Then $P(n+1)$ *is true.*

3. **Conclusion:** $\forall n \in \mathbb{N} : \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

1.4.7 Case by case reasoning

Example 1.10. *Show that* $\forall x \in \mathbb{R}, \quad |x-1| \leq x^2 - x + 1$.
We have

$$|x-1| = \begin{cases} x-1, & x \geq 1, \\ -x+1, & x < 1. \end{cases}$$

Case 1: *If* $x \geq 1$.

$$\begin{aligned} x^2 - x + 1 - |x-1| &= x^2 - x + 1 - (x-1) \\ &= x^2 - 2x + 2 \\ &= (x-1)^2 + 1 \geq 0. \end{aligned}$$

Case 2: *If* $x < 1$.

$$\begin{aligned} x^2 - x + 1 - |x-1| &= x^2 - x + 1 - (-x+1) \\ &= x^2 \geq 0. \end{aligned}$$

Then, in each case for all $x \in \mathbb{R}$, *we have* $|x-1| \leq x^2 - x + 1$.

1.5 Exercises

Exercise 1.1. *Let* P, Q *and* R *be three propositions.*

1. *Show that the following propositions are equivalent.*

   (a) $(P \Rightarrow Q) \Leftrightarrow (\overline{Q} \Rightarrow \overline{P})$; **(b)** $(P \Rightarrow Q) \Leftrightarrow (\overline{P} \vee Q)$;

   (c) $[P \wedge (Q \vee R)] \Leftrightarrow [(P \wedge Q) \vee (P \wedge R)]$.

2. *Show without using the truth table that:*

$$[(P \vee R) \Rightarrow Q] \Leftrightarrow [(P \Rightarrow Q) \wedge (R \Rightarrow Q)]\,.$$

3. *Give the negation of the following propositions:*

   (a) $\left[(P \wedge Q) \vee (P \vee Q) \vee (P \vee \overline{Q})\right] \Rightarrow P$;

   (b) $P \Rightarrow \left[(P \wedge Q) \vee (P \vee Q) \vee (P \vee \overline{Q})\right]$.

Exercise 1.2.

1. *For which values of* x *theses propositions are false.*

   (a) $x = 3 \Rightarrow x = 0$. **(b)** $[(x = 1) \vee (x > 2)] \Rightarrow x > 3$.

2. *Describe the parts of* $\mathbb{R}$ *under the following propositions hold true.*

   (a) $[(x = 0) \wedge (x > 1)] \Rightarrow x > 3$. **(b)** $x^2 \geq 0 \Rightarrow x > 4$.

Exercise 1.3. *Let* $A = [0, 1]$. *Consider the following propositions. If a statement is true, provide a proof; if it is false, give a counter example.*

(a) $\forall x \in A, \forall y \in A, x + y \in A$.

(b) $\forall x \in A, \exists y \in A, x + y \in A$.

(c) $\exists x \in A, \forall y \in A, x + y \in A$.

(d) $\exists x \in A, \exists y \in A, x + y \in A$.

Exercise 1.4. *Write in terms of quantifiers the following expressions:*

1. *The square of every real number is non-negative.*
2. *Between any two distinct real numbers, there exists a rational number.*
3. *Some real numbers are strictly greater than their square.*

Exercise 1.5. *Using the appropriate proof method, show that:*

1. *Prove by direct reasoning: The sum of two rational numbers is rational.*
2. *Prove by contraposition: If $n \in \mathbb{N}^*$, then n^2+1 is not the square of a natural number.*
3. *Prove by contradiction: If n is an even integer, then $n^2 - 1$ is not divisible by 8.*
4. *Prove by Induction: For all integers $n \geq 4$ we have $n^2 \leq 2^n$.*
5. *Let a be an integer. Prove by cases: 2 divides $a(a + 1)$.*

1.6 Solution of exercises

Solution of exercise 1.1. *Let P, Q and R be three propositions.*

1. *Show that the following propositions are equivalent.*

   (a) $(P \Rightarrow Q) \Leftrightarrow (\overline{Q} \Rightarrow \overline{P})$;

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

   Since $(P \Rightarrow Q)$ and $(\overline{Q} \Rightarrow \overline{P})$ have the same truth table then $(P \Rightarrow Q) \Leftrightarrow (\overline{Q} \Rightarrow \overline{P})$.

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

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

Since $(P \Rightarrow Q)$ *and* $(\overline{P} \vee Q)$ *have the same truth table then* $(P \Rightarrow Q) \Leftrightarrow (\overline{P} \vee Q)$.

(c) $[P \wedge (Q \vee R)] \Leftrightarrow [(P \wedge Q) \vee (P \wedge R)]$.

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

The propositions $[P \wedge (Q \vee R)]$ *and* $[(P \wedge Q) \vee (P \wedge R)]$ *have the same truth table then*

$$[P \wedge (Q \vee R)] \Leftrightarrow [(P \wedge Q) \vee (P \wedge R)].$$

2. *We show without using the truth table that:* $[(P \vee R) \Rightarrow Q] \Leftrightarrow [(P \Rightarrow Q) \wedge (R \Rightarrow Q)]$.
We have $(P \Rightarrow Q) \Leftrightarrow (\overline{P} \vee Q)$, *then*

$$\begin{aligned}
[(P \vee R) \Rightarrow Q] &\Leftrightarrow \left[\overline{(P \vee R)} \vee Q\right] \\
&\Leftrightarrow \left[(\overline{P} \wedge \overline{R}) \vee Q\right] \quad (\vee \textit{ is distributive with respect to } \wedge) \\
&\Leftrightarrow \left[(\overline{P} \vee Q) \wedge (\overline{R} \vee Q)\right] \\
&\Leftrightarrow \left[(P \Rightarrow Q) \wedge (R \Rightarrow Q)\right].
\end{aligned}$$

3. *Give the negation of the following propositions:*
Since the negation of $P \Rightarrow Q$ *is* $P \wedge \overline{Q}$, *then*

(a) *The negation of* $\left[(P \wedge Q) \vee (P \vee Q) \vee (P \vee \overline{Q})\right] \Rightarrow P$ *is*

$$\left[(P \wedge Q) \vee (P \vee Q) \vee (P \vee \overline{Q}) \wedge \overline{P}\right].$$

(b) *The negation of* $P \Rightarrow \left[(P \wedge Q) \vee (P \vee Q) \vee (P \vee \overline{Q})\right]$ *is*

$$\begin{aligned}\overline{P \Rightarrow \left[(P \wedge Q) \vee (P \vee Q) \vee (P \vee \overline{Q})\right]} &\Leftrightarrow P \wedge \overline{(P \wedge Q) \vee (P \vee Q) \vee (P \vee \overline{Q})} \\ &\Leftrightarrow P \wedge \left(\overline{(P \wedge Q)} \wedge \overline{(P \vee Q)} \wedge \overline{(P \vee \overline{Q})}\right) \\ &\Leftrightarrow P \wedge (\overline{P} \vee \overline{Q}) \wedge (\overline{P} \wedge \overline{Q}) \wedge (\overline{P} \wedge \overline{\overline{Q}}) \\ &\Leftrightarrow P \wedge (\overline{P} \vee \overline{Q}) \wedge (\overline{P} \wedge \overline{Q}) \wedge (\overline{P} \wedge Q).\end{aligned}$$

Solution of exercise 1.2.

1. *The values of* x *for which the propositions are false.*

   (a) $(x = 3) \Rightarrow (x = 0)$.
   This proposition is false when $x = 3$ *is true and* $x = 0$ *is false. If* $x = 3$ *is true then* $3 = 0$ *is false , then* $x = 0$ *is false.*
   Therefore the proposition $(x = 3) \Rightarrow (x = 0)$ *is false for the value* x=3.

   (b) $[(x = 1) \vee (x > 2)] \Rightarrow x > 3$.
   This proposition is false when $[(x = 1) \vee (x > 2)]$ *is true and* $x > 3$ *is false.*
   - *The proposition* $[(x = 1) \vee (x > 2)]$ *is true in these cases:*
     (a) If both $(x = 1)$ *and* $(x > 2)$ *are true (which is impossible).*
     (b) If $(x = 1)$ *is true and* $(x > 2)$ *is false, then* $[(x = 1) \vee (x > 2)]$ *is true for* $x = 1$.
     (c) If $(x = 1)$ *is false and* $(x > 2)$ *is true, then* $[(x = 1) \vee (x > 2)]$ *is true for* $x \in]2, +\infty)$.
   - *The proposition* $x > 3$ *is false for* $x \in]-\infty, 3]$.

   Therefore, the proposition $([(x = 1) \vee (x > 2)] \Rightarrow x > 3)$ *is false for* $x \in \{1\} \cup]2, 3]$.

2. *The parts of* $\mathbb{R}$ *under the propositions hold true.*

   (a) $[(x = 0) \wedge (x > 1)] \Rightarrow x > 3$.
   The proposition $[(x = 0) \wedge (x > 1)]$ *is always false, since if* $x = 0$, *then the condition* $x > 1$ *is false.*
   Therefore, the proposition $[(x = 0) \wedge (x > 1)] \Rightarrow x > 3$ *is true for all* $x \in \mathbb{R}$.

   (b) $x^2 \geq 0 \Rightarrow x > 4$.
   The proposition $x^2 \geq 0$ *is always true for all* $x \in \mathbb{R}$, *so the proposition* $(x^2 \geq 0) \Rightarrow (x > 4)$ *is true, if* $x > 4$ *is true, that is for* $x \in]4, +\infty[$.

Solution of exercise 1.3. *Let* $A = [0, 1]$. *Consider the following propositions. If a statement is true, provide a proof; if it is false, give a counterexample.*

(a) $\forall x \in A, \forall y \in A, x + y \in A$.
This proposition is false.
Counter example: It is sufficient to take $x = 1 \in A$ *and* $y = 1 \in A$, *then* $x + y = 2 \notin A$.

(b) $\forall x \in A,\ \exists y \in A,\ x+y \in A.$

This proposition is true.
Let $x \in [0,1]$, we take $y = 0$ then $x + y = x \in A$. For every $x \in A$ there exist at least one $y \in A$ (for example $y = 0$) such that $x + y \in A$.

(c) $\exists x \in A,\ \forall y \in A,\ x+y \in A.$

This proposition is true.
We need to find $x \in A$ such that for every $y \in A$, we have $x+y \in A$, that is $x+y \leq 1$.
Taking $y = 1$, we obtain $x + 1 \leq 1 \Rightarrow x \leq 0$.
Since $x \in A$, the only possible value is $x = 0$.
Therefore, $\exists x = 0 \in A$ such that $\forall y \in A$, $x + y \in A$.

(d) $\exists x \in A,\ \exists y \in A,\ x+y \in A.$

This proposition is true.
It is enough to find two elements $x \in A$ and $y \in A$, such that $x + y \in A$.
For example, take $x = \frac{1}{2}, y = 0 \in A$. Then $x + y = \frac{1}{2} + 0 = \frac{1}{2} \in A$.

Solution of exercise 1.4. *Write in terms of quantifiers the following expressions:*

1. *The square of every real number is nonnegative.*

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

2. *Between any two distinct real numbers, there exists a rational number.*

$$\forall x, y \in \mathbb{R},\ x < y,\ \exists q \in \mathbb{Q} : x < q < y.$$

3. *Some real numbers are strictly greater than their square.*

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

Solution of exercise 1.5. *Using the appropriate proof method, show that:*

1. *The sum of two rational numbers is rational.*
Proof (Direct reasoning):

$$\begin{aligned} \text{Let } x, y \in \mathbb{Q} &\Rightarrow \exists p, m \in \mathbb{Z} \text{ and } q, n \in \mathbb{Z}^*, \quad \text{such that } x = \tfrac{p}{q},\ y = \tfrac{m}{n}. \\ &\Rightarrow x + y = \tfrac{p}{q} + \tfrac{m}{n} \\ &\qquad = \tfrac{pn+mq}{qn}, \quad (pn+mq) \in \mathbb{Z} \text{ and } qn \in \mathbb{Z} \text{ with } qn \neq 0. \\ &\Rightarrow x + y \in \mathbb{Q}. \end{aligned}$$

2. *If $n \in \mathbb{N}^*$, then $n^2 + 1$ is not the square of a natural number.*
that is

$$\left(n \in \mathbb{N}^* \Rightarrow \forall k \in \mathbb{N}^* : n^2 + 1 \neq k^2\right).$$

Proof by contraposition: *it is based on the following equivalence*

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

We want to show that its contrapositive is true, i.e.

$$\left(\exists k \in \mathbb{N}^* : n^2 + 1 = k^2\right) \Rightarrow n \notin \mathbb{N}^* \ (n = 0).$$

Suppose that $\exists k \in \mathbb{N}$ *such that* $n^2 + 1 = k^2$ *then* $k^2 - n^2 = 1 \Rightarrow (k - n)(k + n) = 1$.
We know that $k - n \in \mathbb{Z}$ *and* $k + n \in \mathbb{N}$, *then:*

$$\begin{cases} (k - n) = 1 \ldots (1) \\ (k + n) = 1 \ldots (2) \end{cases}$$

$(1) + (2)$, *we obtain* $2k = 2$ *then* $k = 1$.
$(1) - (2)$, *we obtain* $-2n = 0$ *then* $n = 0$.
Thus, the only solution is n=0. Therefore the contrapositive is true, then
If $n \in \mathbb{N}^*$, *then* $n^2 + 1$ *is not the square of a natural number.*

3. *If* n *is an even integer, then* $n^2 - 1$ *is not divisible by* 8.
Proof by contradiction: *Suppose that* n *is an even integer and that* $n^2 - 1$ *is divisible by* 8.
Since n *is even, then* $\exists k \in \mathbb{N} : \ n = 2k$. *Thus*

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

By assumption, $\exists m \in \mathbb{N}$ *such that*

$$4k^2 - 1 = 8m \Rightarrow 4k^2 = 8m + 1.$$

Now, $4k^2$ *is divisible by* 4. *However,* $8m + 1$ *has remainder* 1 *when divided by* 4, *so* $8m + 1$ *is not divisible by* 4.
Thus, we obtain equality between a number that is divisible by 4 *and a number that is not divisible by* 4 *contradiction. Therefore our initial assumption is false.*
Hence, if n *is even ,* $n^2 - 1$ *cannot be divisible by* 8.

4. *For all integers* $n \geq 4$ *we have* $n^2 \leq 2^n$.
Proof by Induction: *Let* $P(n)$ *denote "For all integers* $n \geq 4$ *we have* $n^2 \leq 2^n$ *".*

Initialization: *For* $n = 4$, $4^2 = 16 \geq 2^4 = 16$, *then* $P(4)$ *is true.*

Heredity: *We suppose that* $P(n)$ *is true for a fixed* $n \geq 4$ *and we show that* $P(n + 1)$*:*$(n + 1)^2 \leq 2^{n+1}$ *is true.*
We have

$$(n + 1)^2 = n^2 + 2n + 1 = n^2 \left(1 + \frac{1}{n}\right)^2$$

Since, $n \geq 4$ *then* $\frac{1}{n} \leq \frac{1}{4}$*, therefore*

$$\left(1+\frac{1}{n}\right)^2 \leq \left(1+\frac{1}{4}\right)^2 = \frac{25}{16} \leq 2.$$

Then,

$$(n+1)^2 \leq n^2.2 \leq 2^n.2 = 2^{n+1}.$$

Then $P(n+1)$ *is verified,*

Conclusion: *By induction the desired inequality* $n^2 \leq 2^n$ *for all* $n \geq 4$ *is true.*

5. *Let* a *be an integer. Prove by cases:* 2 *divides* $a(a+1)$*.*

   case 1: a **is even** *then* $\exists k \in \mathbb{N}^* : a = 2k$*, thus* $a(a+1) = 2k(2k+1)$ *then* $a(a+1)$ *is an even integer (it is divisible by* 2*).*

   case 1: a **is odd** *then* $\exists k \in \mathbb{N}^* : a = 2k+1$*, thus*

   $$a(a+1) = (2k+1)(2k+2) = 2(2k+1)(k+1)$$

   then $a(a+1)$ *is an even integer (it is divisible by* 2*).*

   Then by cases $a(a+1)$ *is an even integer for integer number* a*.*

Chapter 2

Sets and mappings

2.1 Sets

In mathematics, we often deal with collections of numbers, objects, or ideas that share a common property. To describe and study these collections precisely, we use the concept of sets. A set is simply a well defined group of distinct elements, such as numbers, letters,... The first part of this chapter is devoted to the concept of sets. In particular, we study the laws of operations with sets.

2.1.1 Definitions

Definition 2.1 (Set)

A set X is a collection of distinct objects, well-defined according to a common property. Each of these objects is called an element of X.

- If x is an element of the set X, we say that x belongs to X, and we denoted this by $x \in X$.
- If x is not an element of the set X, we say that x does not belong to X, and we denote this by $x \notin X$.

Example 2.1.

1. *Let X be the set of all capital cities in the world, then the city Tokyo, denoted by x, is an element of X and we write $x \in A$.*
2. *If Y is the set of all capital cities in Africa, then Tokyo, denoted by x, is not an element in the set Y and we write $x \notin Y$.*

Remark 2.1

In general:

1. We use uppercase letters, such as $A, B, \ldots$, to denote sets.
2. The elements of a set are represented by lowercase letters: $a, b, c, \ldots$.
3. We use braces (curly brackets) $\{\}$ to refer to a set.

A set X can be represented in two ways:

Explicitly (In extension): By listing all the elements of the set X.

Implicitly (In comprehension): By stating a property or a rule that characterizes the elements of the set X.

$$X = \{x : \quad x \text{ verify a property } P(x)\}.$$

Example 2.2.

1. *The set* $X = \{n \in \mathbb{N} : \ 0 \leq n \leq 8\}$ *is defined implicitly (in comprehension).*
   The set $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ *is defined explicitly (in extension).*
2. *The set Y={all the vowels in the English alphabet } is defined implicitly (in comprehension).*
   The set $Y = \{a, e, i, o, u\}$ *is defined explicitly (in extension).*

- A set with no elements is called empty set, denoted by $\emptyset$ or $\{\}$.
- A set with only one element, like $X = \{x\}$, is called a singleton set.
- The sets $\{a, b, c\}$ and $\{b, c, a\}$ are the same, because the order of elements does not matter.
- The sets $\{a, b, c\}$ and $\{a, b, b, c, c\}$ are the same, because repeating elements does not change the set.

Example 2.3 (Usual sets).

$\mathbb{N}$**:** *Set of natural numbers.*

$\mathbb{Z}$**:** *Set of relative numbers.*

$\mathbb{D}$**:** *Set of decimal numbers.*

$\mathbb{Q}$**:** *Set of rational numbers.*

$\mathbb{R}$**:** *Set of real numbers.*

$\mathbb{C}$: *Set of complex numbers.*

Definition 2.2 (Cardinality)

The cardinality of a set X is denoted by $Card(X)$ or $|X|$, is the number of distinct elements of X.
If $Card(X)$ is finite, then X is called a finite set. Otherwise, X is called an infinite set.

Example 2.4.

1. $Card(\{0,1,2,8\}) = 4$, *then the set* $\{0,1,2,8\}$ *is finite.*
2. *The set of natural numbers:* $\{0,1,2,3,\ldots\}$ *is infinite.*
3. *The set of prime numbers is infinite (A prime number is a number greater than* 1 *that can be divided exactly only by* 1 *and itself).*
4. $Card(\emptyset) = 0$ *and* $Card(\{\emptyset\}) = 1$.

2.1.2 Relation between sets

Let X be a nonempty set.

Subset

A is called a subset of X or a part of X, if all elements of A belongs to X. We write this as $A \subset X$.
We write

$$\begin{aligned} A \subset X (A \text{ is included in } X) &\Leftrightarrow \forall x,\ (x \in A) \text{ implies } (x \in X). \\ A \not\subset X (A \text{ is not included in } X) &\Leftrightarrow \exists x,\ (x \in A) \text{ and } (x \notin X). \end{aligned}$$

Example 2.5.

1. $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
2. $\mathbb{N} \not\subset \mathbb{R}^*$ *because* $0 \in \mathbb{N}$ *and* $0 \notin \mathbb{R}^*$.

Equality of two sets

Two sets A and B are equal if they have the same elements. We denote this by $A = B$ (read as "A is equal to B").

$$\forall x,\ x \in A \Leftrightarrow x \in B.$$

This means

$$\begin{aligned} A = B &\Leftrightarrow (A \subset B \text{ and } B \subset A). \\ A \neq B &\Leftrightarrow (A \not\subset B \text{ or } B \not\subset A). \end{aligned}$$

Example 2.6. *Consider the following sets:*

1. $A = \{x \in \mathbb{R} :\ x^2 - 5x + 6 = 0\}, \quad B = \{2, 3\}$, *then* $A = B$.
   Indeed, the elements of A *are the real numbers that verify the equation* $x^2 - 5x + 6 = 0$. *Solving this equation, we obtain only two solutions that are equal to* 2 *and* 3. *Hence* $A = \{2, 3\} = B$.

2. $C = \{5, 10, 15\}, \quad D = \{5n :\ n \in \mathbb{N}, 1 \leq n \leq 3\}$, *both sets contain multiples of* 5 *up to* 15, *then* $C = D$.

3. *the sets* $\{\emptyset\} \neq \emptyset$, *the set* $\emptyset$ *is the set that has no elements and* $\{\emptyset\}$ *is the singleton set, and its only element is the empty set.*

Power set

The power set of X denoted by $\mathcal{P}(X)$ is the set of all subsets of X, including the empty set and X itself.

$$\mathcal{P}(X) = \{A,\ A \subset X\}.$$

Example 2.7.

1. *If* $X = \{a\}$, *then* $Card(X) = 1$.
   Thus
   $$Card(\mathcal{P}(X)) = 2^1 = 2.$$
   Therefore,
   $$\mathcal{P}(X) = \{\emptyset, \{a\}\}.$$

2. *If* $X = \{a, b\}$, *then* $Card(X) = 2$.
   Thus
   $$Card(\mathcal{P}(X)) = 2^2 = 4.$$
   Therefore,
   $$\mathcal{P}(X) = \{\emptyset, \{a, b\}, \{a\}, \{b\}\}.$$

3. *If* $X = \{a, b, c\}$, *then* $Card(X) = 3$.
   Thus
   $$Card(\mathcal{P}(X)) = 2^3 = 8.$$
   Therefore,
   $$\mathcal{P}(X) = \{\emptyset, \{a, b, c\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}\}.$$

Properties 2.1

1. $\emptyset \in \mathcal{P}(X)$ and $X \in \mathcal{P}(X)$.
2. $x \in X \Leftrightarrow \{x\} \in \mathcal{P}(X)$.
3. If $X = \emptyset$, then $\mathcal{P}(X) \neq \emptyset$ ($\mathcal{P}(X)$ is never empty even if $X = \emptyset$).
4. $A \in \mathcal{P}(X) \Leftrightarrow A \subset X$.
5. If $Card(X) = n$, then $Card(\mathcal{P}(X)) = 2^n$.

2.1.3 Operations on sets

Just as propositions can be combined in various ways using logical connectives to form new propositions, sets can also be combined to form new sets that has specific properties. We now use these logical connectives to define the corresponding set operations.

Let A and B be two subsets of X, we define the following operations.

Complement of a set

The complement of A in X, denoted by $C_X A$ is the set of elements of X that does not belong to the set A.
$$C_X A = \{x \in X : \ x \notin A\}.$$

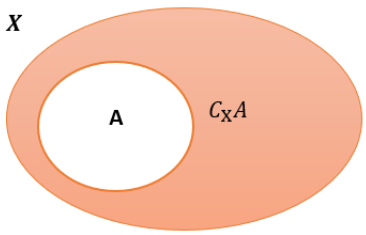


Figure 2.1: $C_X A$ the complement of A in X.

Example 2.8. *Let the following sets:*

$$X = \{-1, 2, 10, 13\},\ Y = \{-1, 2\},\ G = \{10, -1\}$$

then $C_X Y = \{10, 13\}$ *and* $C_X G = \{2, 13\}$.

Union and intersection

Let A and B be two subsets of X. Then

- We denote $A \cup B$ the union of two sets A and B, it is said A union B.

$$A \cup B = \{x :\ x \in A \text{ or } x \in B\}.$$

- We denote $A \cap B$ the intersection of two sets A and B, it is said A intersect B.

$$A \cap B = \{x :\ x \in A \text{ and } x \in B\}.$$

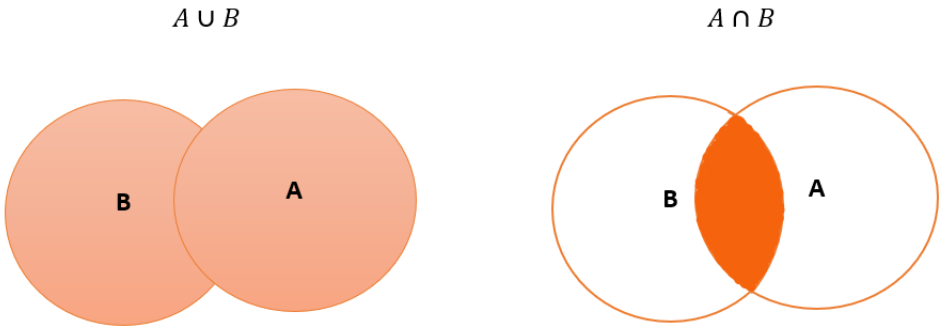


Figure 2.2: $A \cup B$ union of sets A and B, $A \cap B$ intersection of sets A and B.

Remark 2.2

- If $A \cap B = \emptyset$, then A and B are said to be disjoint sets.
- If $A \cup B = X$ and $A \cap B = \emptyset$, then A and B are said to be complementary subsets of X.

Difference of two sets

The difference of two sets A and B, denoted by $A \setminus B$ or $A - B$, is the set of elements that belong to A but not to B.

$$A \setminus B = \{x :\ x \in A \text{ and } x \notin B\}.$$

Symmetric difference

The symmetric difference of two sets A and B is denoted by $A\Delta B$, is the set of elements that belong to either A or B, but not to both.

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

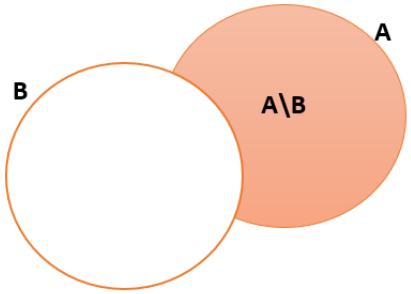


Figure 2.3: $A \setminus B$: the elements of A that are not in B.

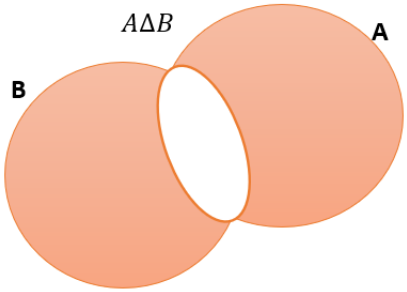


Figure 2.4: $A\triangle B$: the symmetric difference of A and B.

Example 2.9.

1. *Let* $X = \mathbb{R}$, $A = [1, 3]$, *and* $B = [2, 5]$. *Then*

$$A \setminus B = [1, 2[\text{ and } B \setminus A =]3, 5].$$

2. *Let* $X = \mathbb{Z}$, $A = \{-1, 3, 5, 7\}$ *and* $B = \{-2, -1, 5, 7\}$. *Then*

$$A \setminus B = \{3\}, \quad B \setminus A = \{-2\}, \quad A\Delta B = \{-2, 3\}.$$

Example 2.10.
Let the set $X = \{1, 2, 3, 4, 5, 6\}$ *and the define the set* A *representing the odd numbers and the set* B *representing the prime numbers.*

$$X = \{1, 2, 3, 4, 5, 6\} \rightarrow \begin{cases} A = \{1, 3, 5\} \\ B = \{2, 3, 5\} \end{cases} \rightarrow \begin{cases} C_X A = \{2, 4, 6\} \\ A \cup B = \{1, 2, 3, 5\} \\ A \cap B = \{3, 5\} \\ A \setminus B = \{1\} \\ A\triangle B = \{1, 2\}. \end{cases}$$

Definition 2.3 (Intersection and union of families of sets)

Let $X_1, X_2, \ldots, X_n$ be subsets of a set X. Then:

- The intersection $X_1 \cap X_2 \cap \cdots \cap X_n$ is defined as the set of elements x that belong to every set $X_1, X_2, \ldots, X_n$. That is,

$$X_1 \cap X_2 \cap \cdots \cap X_n = \{x,\ \forall i \in \{1, 2, \ldots, n\},\ x \in A_i\}.$$

- The union $X_1 \cup X_2 \cup \cdots \cup X_n$ is defined as the set of all elements x that belong to at least one of the sets $X_1, X_2, \ldots, X_n$. That is,

$$X_1 \cup X_2 \cup \cdots \cup X_n = \{x,\ \exists i \in \{1, 2, \ldots, n\},\ x \in A_i\}.$$

Partition of a set

Let X be a set, the subsets $X_1, X_2, \ldots, X_n \subset X$ form a partition of X if and only if the following conditions are satisfied:

1. $X_i \neq \emptyset,\ \forall i \in \{1, 2, \ldots, n\}$.
2. $X_i \cap X_j = \emptyset,\ \forall i \neq j,\ i, j \in \{1, 2, \ldots, n\}$.
3. $\bigcup_{i=1}^{n} X_i = X_1 \cup X_2 \cup X_3 \cup \cdots \cup X_n = X$.

Example 2.11.

1. *Let $X = \{$Letters in an English alphabet$\}$ this set can be partitioned into sets, for example, $X_1 = \{$Set of vowels$\}$ and $X_2 = \{$Set of consonants$\}$. It is clear that,*
   (a) $X_1 \neq \emptyset$ *and* $X_2 \neq \emptyset$.
   (b) $X_1 \cap A_2 = \emptyset$.
   (c) $X_1 \cup X_2 = X$.

   Then $X_1 = \{$Set of vowels$\}$ and $X_2 = \{$Set of consonants$\}$ form a partition of the set of all letters in an English alphabet.
2. *Let A be a nonempty subset of X, then the set $\{A, (C_X A)\}$ is a partition of X.*
3. *Let $X = [0, 4[$. We set $X_1 = [0, 2[,\ X_2 = [2, 3[,\ X_3 = [3, 4]$, then we have*
   (a) $X_i \neq \emptyset,\ \forall i \in \{1, 2, 3\}$.
   (b) $X_i \cap A_j = \emptyset,\ \forall i \neq j$.

(c) $\bigcup_{i=1}^{3} X_i = X_1 \cup X_2 \cup X_3 = X$.

Then the sets X_1, X_2, X_3 form a partition of the set X.

Properties 2.2

Let X be a nonempty set and let A and B be two subsets of X. Then we have

1. $\left.\begin{array}{l} A \cap X = A \\ A \cup \emptyset = A \end{array}\right\}$ (Identity laws).
2. $\left.\begin{array}{l} A \cap \emptyset = \emptyset \\ A \cup X = X \end{array}\right\}$ (Domination laws).
3. $\left.\begin{array}{l} A \cap A = A \\ A \cup A = A \end{array}\right\}$ (Idempotent laws).
4. $A \cap B = B \cap A, \quad A \cup B = B \cup A.$ (Commutative laws).
5. $\left.\begin{array}{l} (A \cap B) \cap C = A \cap (B \cap C) \\ (A \cup B) \cup C = A \cup (B \cup C) \end{array}\right\}$ (Associative laws).
6. $\left.\begin{array}{l} A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \end{array}\right\}$ (Distributive laws).
7. $\left.\begin{array}{l} C_X(A \cup B) = (C_X A) \cap (C_X B) \\ C_X(A \cap B) = (C_X A) \cup (C_X B) \end{array}\right\}$ (De Morgan's laws).
8. $\left.\begin{array}{l} C_X(C_X A) = A, \quad C_X X = \emptyset, \quad C_X \emptyset = X. \\ A \cup (C_X A) = X, \quad A \cap (C_X A) = \emptyset. \end{array}\right\}$ (Complement laws).

Proof.

4. (Commutative laws)

   (a) $A \cap B = B \cap A$.
   We prove the equality by showing that each set is a subset of the other.

   First, let $x \in A \cap B$. Then, by definition of intersection,

   $$x \in A \quad \text{and} \quad x \in B.$$

   Since the order of the statements does not matter,

   $$x \in B \quad \text{and} \quad x \in A.$$

Hence,

$$x \in B \cap A.$$

Therefore,

$$A \cap B \subseteq B \cap A.$$

Now let $x \in B \cap A$. Then,

$$x \in B \quad \text{and} \quad x \in A.$$

Reversing the order,

$$x \in A \quad \text{and} \quad x \in B,$$

so

$$x \in A \cap B.$$

Therefore,

$$B \cap A \subseteq A \cap B.$$

Since both inclusions hold, we conclude that $A \cap B = B \cap A$.

(b) $A \cup B = B \cup A$.
We prove the equality by showing that each set is a subset of the other.

Let $x \in A \cup B$. Then, by definition of union,

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

Since the order does not matter,

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

Hence,

$$x \in B \cup A.$$

Therefore,

$$A \cup B \subseteq B \cup A.$$

Now let $x \in B \cup A$. Then,

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

Reversing the order,

$$x \in A \quad \text{or} \quad x \in B,$$

so

$$x \in A \cup B.$$

Therefore,

$$B \cup A \subseteq A \cup B.$$

Hence, $A \cup B = B \cup A$.

5. (Associative laws)

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

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

   (b) $(A \cup B) \cup C = A \cup (B \cup C)$

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

6. (Distributive laws)

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

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

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

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

7. (De Morgan's laws)

(a) $C_X(A \cup B) = (C_X A) \cap (C_X B)$

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

(b) $C_X(A \cap B) = (C_X A) \cup (C_X B)$

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

□

2.1.4 Cartesian product

Let A and B be two nonempty sets.

Definition 2.4 (Cartesian product:)

The cartesian product of A and B, denoted by $A \times B$ read A cross B, is the set of all ordered pairs (x, y) such that $x \in A$ and $y \in B$.

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

We observe that:

- $z \in A \times B \Rightarrow \exists x \in A, \exists y \in B$ such that: $z = (x, y)$.
- $(x, y) = (x', y') \Leftrightarrow x = x'$ and $y = y'$.
- $(x, y) \neq (x', y') \Leftrightarrow x \neq x'$ or $y \neq y'$.

Remark 2.3

The number of pairs (x, y) in the cartesian product of A and B is equal to the product of the number of elements in the set A and the number of elements in the set B, that is, $Card(A \times B) = Card(A).Card(B)$.

Example 2.12.

1. *Let* $A = \{1, 2, 3\}$ *and* $B = \{a, b\}$, *then*
$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$$
and $Card(A \times B) = Card(A).Card(B) = 3.2 = 6$.
2. *The cartesian product* $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) : x \in \mathbb{R}$ *and* $y \in \mathbb{R}\}$ *is called the cartesian plan.*
3. $[2, 4] \times \mathbb{R} = \{(x, y) : 2 \leq x \leq 4$ *and* $y \in \mathbb{R}\}$.

Remark 2.4

1. The cartesian product is not commutative; that is $A \times B \neq B \times A$.
For example, in the above case, we have $(1, a) \in A \times B$ but $(1, a) \notin B \times A$.
2. We must not confuse the pair (x, y) and the set $\{x, y\}$.
3. If $x \neq y$ then $(x, y) \neq (y, x)$ but $\{x, y\} = \{y, x\}$.

Definition 2.5 (Generalization: Cartesian products of several sets)

If we consider sets $X_1, X_2, X_3, \ldots, X_n$ we can similarly define $n-$tuples $(x_1, x_2, \ldots, x_n)$ with $x_1 \in X_1$, $x_2 \in X_2$, $\ldots$, $x_n \in X_n$ and the cartesian product

$$X_1 \times X_2 \times \cdots \times X_n = \{(x_1, x_2, \ldots, x_n) \text{ such that } x_1 \in X_1,\ x_2 \in X_2,\ \ldots,\ x_n \in X_n\}.$$

Properties 2.3

1. $A \times B = \emptyset \Leftrightarrow A = \emptyset$ or $B = \emptyset$.
2. $(A \cap B) \times C = (A \times C) \cap (B \times C)$.
3. $(A \cup B) \times C = (A \times C) \cup (B \times C)$.
4. $(A \subset X$ and $B \subset Y) \Rightarrow (A \times B) \subset (X \times Y)$.
5. $A \times B \times C = (A \times B) \times C = A \times (B \times C)$.
6. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

Proof.

1. $A \times B = \emptyset \Leftrightarrow A = \emptyset$ or $B = \emptyset$.

   "$\Rightarrow$" Assume that $A \times B = \emptyset$. We prove that $A = \emptyset$ or $B = \emptyset$.
   Suppose, for contradiction, that

   $$A \neq \emptyset \quad \text{and} \quad B \neq \emptyset.$$

   Then there exists $a \in A$ and $b \in B$. Hence,

   $$(a, b) \in A \times B,$$

   which contradicts the assumption that $A \times B = \emptyset$.
   Therefore, at least one of the sets must be empty:

   $$A = \emptyset \quad \text{or} \quad B = \emptyset.$$

   "$\Leftarrow$" Assume that $A = \emptyset \quad \text{or} \quad B = \emptyset$.
   If $A = \emptyset$, then there is no element $a \in A$, so no ordered pair (a, b) can belong to $A \times B$. Hence,

   $$A \times B = \emptyset.$$

   Similarly, if $B = \emptyset$, then no ordered pair (a, b) can belong to $A \times B$, and therefore

   $$A \times B = \emptyset.$$

   Thus,

   $$A \times B = \emptyset.$$

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

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

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

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

4. $(A \subset X \text{ and } B \subset Y) \Rightarrow (A \times B) \subset (X \times Y)$.
   Suppose that $(A \subset X \text{ and } B \subset Y)$ and lets show that $(A \times B) \subset (X \times Y)$.
   Let

$$\begin{aligned}(x,y) \in (A \times B) = & \{(x,y) : x \in A \text{ and } y \in B\} \\ \subset & \{(x,y) : x \in X \text{ and } y \in Y\} \text{ since } A \subset X \text{ and } B \subset Y \\ = & (X \times Y).\end{aligned}$$

   then $(A \times B) \subset (X \times Y)$.

5. $A \times B \times C = (A \times B) \times C = A \times (B \times C)$. The proof is evident.

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

$$\begin{aligned}(A \times B) \cap (C \times D) = & \{(x,y) : (x,y) \in (A \times B) \text{ and } (x,y) \in (C \times D)\} \\ = & \{(x,y) : (x \in A \text{ and } y \in B) \text{ and } (x \in C \text{ and } y \in D)\} \\ = & \{(x,y) : (x \in A \text{ and } x \in C) \text{ and } (y \in B \text{ and } y \in D)\} \\ = & \{(x,y) : (x \in A \cap C) \text{ and } (y \in B \cap D)\} \\ = & (A \cap C) \times (B \cap D).\end{aligned}$$

□

Remark 2.5

$(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup C)$ is not always true.

Counterexample:
Let $A = [0,5],\ B = [-3,0],\ C = [0,2],\ H = [0,4]$.
We have

$$\left.\begin{array}{l} A \cup B = [-3,5] \\ C \cup D = [0,4] \end{array}\right\} (A \cup B) \times (C \cup D) = [-3,5] \times [0,4].$$

and

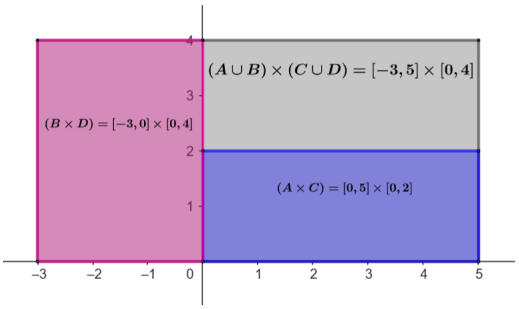
$$\left.\begin{array}{l} A \times C = [0,5] \times [0,2] \\ B \times D = [-3,0] \times [0,4] \end{array}\right\} (A \times C) \cup (B \times D) = ([0,5] \times [0,2]) \cup ([-3,0] \times [0,4]).$$

Then

$$[(A \times C) \cup (B \times D)] \subset (A \cup B) \times (C \cup D)$$

but

$$[(A \cup B) \times (C \cup D)] \not\subset (A \times C) \cup (B \times D).$$



2.2 Mappings

Let X and Y be two nonempty sets.

2.2.1 Definitions

Definition 2.6 (Mapping)

A mapping (or function) from X into Y, is any law f that associates to every element $x \in X$ a unique element $y = f(x)$ of Y and we write $f : X \to Y$.

$$f \text{ a mapping } \Leftrightarrow \forall x \in X, \exists! y \in Y : \quad y = f(x).$$

- X is called the domain of f.
- Y is called the codomain of f.
- $y = f(x)$ is called the image of x under f (or the value of f at x).
- x is called the preimage of y under f.
- We denote by $\mathcal{Y}(X, Y)$ the set of all mappings from X to Y.

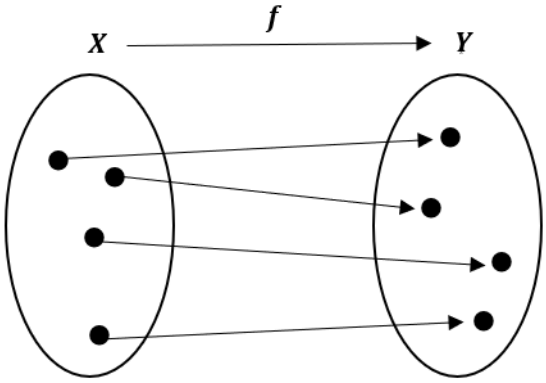


Figure 2.5: f is a mapping

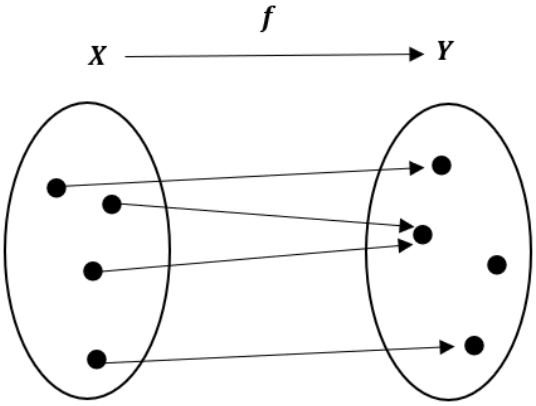


Figure 2.6: f is a mapping

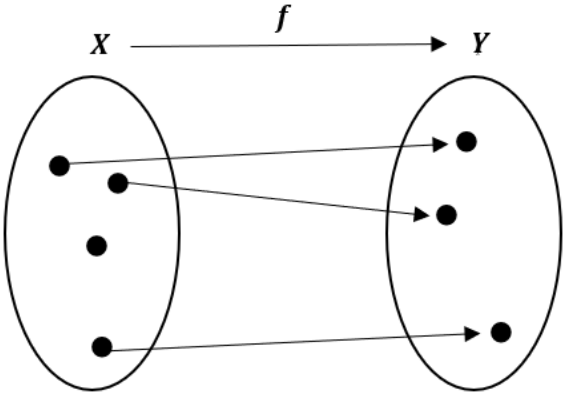


Figure 2.7: f is not a mapping

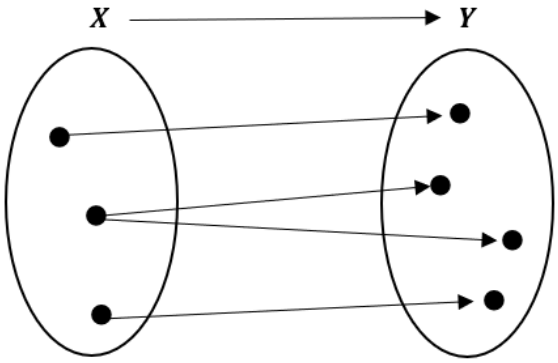


Figure 2.8: f is not a mapping

Example 2.13.

Remark 2.6

Let $f : X \to Y$.

1. f is a mapping $\Leftrightarrow \forall x_1, x_2 \in X,\ (x_1 = x_2 \Rightarrow f(x_1) = f(x_2))$.
2. f is a mapping $\Leftrightarrow \forall x_1, x_2 \in X,\ (f(x_1) \neq f(x_2) \Rightarrow x_1 \neq x_2)$.
3. f is not a mapping $\Leftrightarrow \exists x_1, x_2 \in X,\ x_1 = x_2$ and $f(x_1) \neq f(x_2)$.

Example 2.14.

1. $$\begin{aligned} f : \{0,1,2\} &\to \{1,4,6\} \\ x &\longmapsto x^2. \end{aligned}$$
   f is not a mapping, since $f(0) = 0$ does not belong to the codomain $\{1,4,6\}$; hence, 0 has no image under f.

2. $$\begin{aligned} g : \{0,1,2\} &\to \{0,1,4\} \\ x &\longmapsto x^2. \end{aligned}$$
   g is a mapping, because every element of the domain $\{0,1,2\}$ has exactly one image in the codomain $\{0,1,4\}$.

3. $$\begin{aligned} h : \mathbb{R}^* &\to \mathbb{R} \\ x &\longmapsto \tfrac{1}{x}. \end{aligned}$$
   h is a mapping, since every nonzero real number x has exactly one image $\frac{1}{x}$ in $\mathbb{R}$.

Definition 2.7 (Identity mapping)

The identity mapping on X, denoted by Id_X is a mapping, such that

$$\begin{aligned} Id_X : X &\to X \\ x &\longmapsto Id_X(x) = x. \end{aligned}$$

Definition 2.8 (Graph of mapping)

The graph of a mapping $f : X \to Y$ is a subset of the product $X \times Y$ given by:

$$G_f = \{(x, f(x)) : \quad x \in X\}.$$

Definition 2.9 (Equality of two of mappings)

Two mappings $f : X_1 \to Y_1$ and $g : X_2 \to Y_2$ are equal if and only if $X_1 = X_2$, $Y_1 = Y_2$ and $\forall x \in X_1$ (or $x \in X_2$), $\quad f(x) = g(x)$.

2.2.2 Operations on mappings

Definition 2.10 (Composition of two of mappings)

Let X, Y and Z be three sets and let $f : X \to Y$ and $g : Y \to Z$ be two mappings. The mapping $h : X \to Z$ defined by $h(x) = (g \circ f)(x) = g(f(x))$ is called the composition of f and g.
However, the composite mapping $f \circ g$ is not defined unless $g(Y) \subseteq X$.

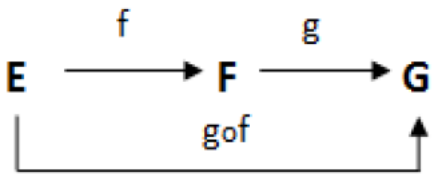


Figure 2.9: The composition $g \circ f$ is well defined

Remark 2.7

1. In general, the composition of mappings is not commutative, that is, $f \circ g \neq g \circ f$. For example, let $X = Y = Z = \mathbb{R}$, and define

$$f(x) = x^2, \ g(x) = 2x + 3.$$

Then,

$$(g \circ f)(x) = g(f(x)) = 2x^2 + 3.$$
$$(f \circ g)(x) = f(g(x)) = (2x + 3)^2 = 4x^2 + 12x + 9.$$

Hence, $(g \circ f) \neq (f \circ g)$.

2. Let X, Y, Z, W ne non-empty sets. We verify that for all mappings for all mappings $f : X \to Y$, $g : Y \to Z$, and $h : Z \to W$, we have

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

We say that the composition is associative.

Definition 2.11

Let $f : X \to X$ be a mapping. The composite mapping $f \circ f$ is also a mapping from X into X; it is denoted by f^2.

More generally, the mapping obtained by composing f with itself k times, where $k \in \mathbb{N}^*$, is again a mapping from X into itself. It is denoted by

$$f^k = \underbrace{f \circ f \circ f \circ \cdots \circ f}_{k \text{ times}}.$$

By convention, we set $f^0 = Id_X$.

Definition 2.12 (Restriction and Extension)

Let $f : X \to Y$ be a mapping.

- The restriction of f to the set $A \subset X$ is the mapping denoted by $f_{|A}$ such that

$$\begin{array}{rl} f_{|A} : A & \to Y \\ x & \longmapsto f_{|A}(x) \end{array}$$

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

- The extension of f to a set B containing X ($X \subset B$) is denoted by $\tilde{f}$ is any mapping

$$\begin{array}{rl} \tilde{f} : B & \to Y \\ x & \longmapsto \tilde{f}(x) \end{array}$$

with $\tilde{f}(x) = f(x)$, $\forall x \in X$.

Remark 2.8

$\tilde{f}$ is said to be an extension of f to the set B if the restriction of $\tilde{f}$ to X equals f; that is $\tilde{f}_{|X} = f$.

Example 2.15.

1. *Let*

$$\begin{array}{rl} f : \mathbb{R} & \to \mathbb{R} \\ x & \mapsto f(x) = x^2, \end{array} \qquad \begin{array}{rl} f_{|\mathbb{R}^*} : \mathbb{R}^* & \to \mathbb{R} \\ x & \mapsto f_{|\mathbb{R}^*}(x) = x^2. \end{array}$$

We say that:

- $f_{|\mathbb{R}^*}$ *is the restriction of* f *to the set* $\mathbb{R}^*$.
- f *is the extension of* $f_{|\mathbb{R}^*}$ *to the set* $\mathbb{R}$.

2. *Let*

$$\begin{array}{rl} g : \mathbb{R} & \to \mathbb{R} \\ x & \mapsto f(x) = \sin(x) \end{array} \qquad \begin{array}{rl} g_{|[0,2\pi]} : [0, 2\pi] & \to \mathbb{R} \\ x & \mapsto g_{|[0,2\pi]}(x) = \sin(x). \end{array}$$

We say that:

- $g_{|[0,2\pi]}$ *is the restriction of* g *to the set* $[0, 2\pi]$.
- g *is the extension of* $g_{|[0,2\pi]}$ *to the set* $\mathbb{R}$.

Remark 2.9

Let $f : X \to Y$ be a mapping, and let B be a set such that $X \subset B$. In general, an extension of f to B is not unique.
For example, consider the mapping:

$$\begin{aligned} f : \mathbb{R}^* &\to \mathbb{R} \\ x &\longmapsto f(x) = \tfrac{\sin(x)}{x}, \end{aligned}$$

where $X = \mathbb{R}^*$ and $B = \mathbb{R}$. This function admits infinitely many extensions to $\mathbb{R}$. Indeed, for each $\alpha \in \mathbb{R}$, define the function $\tilde{f}_\alpha : \mathbb{R} \to \mathbb{R}$ by

$$\begin{aligned} \tilde{f}_\alpha : \mathbb{R} &\to \mathbb{R} \\ x &\longmapsto \tilde{f}(x) = \begin{cases} \alpha, & x = 0, \\ \frac{\sin(x)}{x}, & x \in \mathbb{R}^*. \end{cases} \end{aligned}$$

Each choice of α yields a different extension of f to $\mathbb{R}$, showing that the extension is not unique.

2.2.3 Direct image and preimage

Let $f : X \to Y$ be a mapping, $A \subset X$ and $B \subset Y$.

Definition 2.13 (Direct image)

The direct image of A under f is a subset of Y defined by

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

that is,

$$f(A) = \{y \in Y, \quad \exists x \in A : \ y = f(x)\} \subset Y.$$

We write:

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

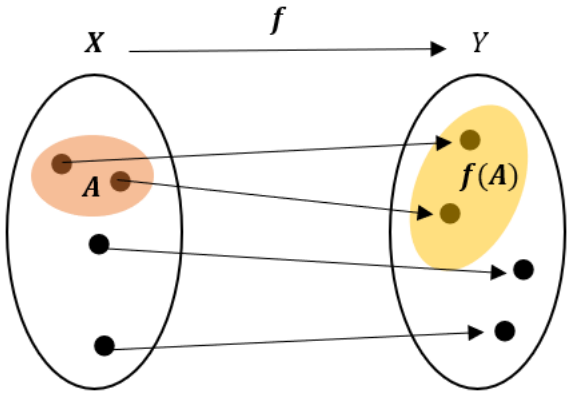


Figure 2.10: The direct image of A under f

Definition 2.14 (Inverse image)

The preimage of B under f is a subset of X defined by

$$f^{-1}(B) = \{x \in X, \quad f(x) \in B\} \subset X.$$

We write:

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

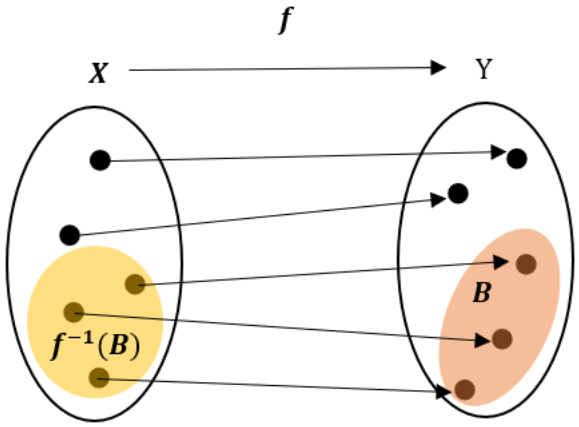


Figure 2.11: The preimage of B under f

Example 2.16.

1. *Let* $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, *then*

$$f(\{-2,2\}) = \{4\}, \quad f([-1,1]) = [0,1], \quad f([-2,2[) = [0,4[, \quad f(\mathbb{R}_+) = f(\mathbb{R}_-) = \mathbb{R}.$$

$$f^{-1}(\{1\}) = \{-1,1\}, \quad f^{-1}(\{-1\}) = \emptyset, \quad f^{-1}(\{-1,4\}) = \{-2,2\}, \quad f^{-1}(\mathbb{R}_-^*) = \emptyset, \quad f^{-1}(\mathbb{R}_+) = \mathbb{R}.$$

2. Let

$$\begin{aligned} g : \mathbb{N} &\to \mathbb{N} \\ n &\mapsto g(n) = 2n + 3. \end{aligned}$$

- *Let* $A = \{0, 1, 2\}$, *then*

$$f(A) = \{f(n), \quad n \in A\} = \{f(0), f(1), f(2)\} = \{3, 5, 7\}.$$

- *Let* $B = \{9\}$, *then*

$$\begin{aligned} f^{-1}(B) &= \{n \in \mathbb{N}, \quad f(n) \in B\} \\ &= \{n \in \mathbb{N}, \quad f(n) = 9\} \\ &= \{n \in \mathbb{N}, \quad 2n + 3 = 9\} \\ &= \{3\}. \end{aligned}$$

2.2.4 Injective, surjective and bijective mapping

Definition 2.15

Let X and Y be two sets, $f : X \to Y$ is a mapping.

1. f is **injective** (one to one), if every element of the codomain Y, **has at most one** (1 or 0) preimage in X, that is

$$f \text{ is injective } \Leftrightarrow \forall x_1, x_2 \in X : \ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2).$$

2. f is **surjective** (onto), if every element of the codomain Y, **has at least one** preimage in X, that is

$$f \text{ is surjective } \Leftrightarrow \forall y \in Y, \ \exists x \in X : \ y = f(x).$$

3. f is **bijective** if every element of the codomain Y, **has a unique** preimage in X, that is

$$\forall y \in Y, \ \exists! x \in X : \ y = f(x).$$

Remark 2.10

Let X and Y be two sets, and let $f : X \to Y$ be a mapping.

1. f is injective $\Leftrightarrow \forall x_1, x_2 \in X : \ x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.
2. f is not injective $\Leftrightarrow \exists x_1, x_2 \in X : \ f(x_1) = f(x_2)$ and $x_1 \neq x_2$.
   In other words, to show that f is not injective, it suffices to find two different elements of X that have the same image.
3. f surjective $\Leftrightarrow f(X) = Y$.
4. f is not surjective $\Leftrightarrow \exists y \in Y, \ \forall x \in X : \ y \neq f(x)$.
   Equivalently, there exists at least one element of Y that is not an image of any element of X.
5. f is bijective $\Leftrightarrow f$ is both injective and surjective.

Example 2.17.

1. *Let $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$*
   - *f is not injective, since there exist $x_1 = -2$ and $x_2 = 2$ in $\mathbb{R}$ such that*
   $$f(x_1) = f(x_2) = 4 \text{ and } x_1 \neq x_1.$$
   - *f is not surjective, because there exists $y = -1 \in \mathbb{R}$ that has no preimage in $\mathbb{R}$.*
2. *Let $g : [0, +\infty[\to [0, +\infty[$ be defined by $g(x) = x^2$. Then g is bijective, since it is both injective (strictly increasing on $[0, +\infty[$) and surjective (every $y \geq 0$ has a preimage $\sqrt{y}$).*

Remark 2.11

Do not confuse the definition of an **injective mapping** with that of a **mapping** itself.

$$f \text{ is injective } \Leftrightarrow \forall x_1, x_2 \in X : \ f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

whereas

$$f \text{ is a mapping } \Leftrightarrow \forall x_1, x_2 \in X, \ x_1 = x_2 \Rightarrow f(x_1) = f(x_2).$$

Proposition 2.1

Let $f : X \to Y$ be a mapping.

(I) Let A_1 and A_2 be two subsets of X, then

1. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
2. $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$.
3. $A_1 \subset A_2 \Rightarrow f(A_1) \subset f(A_2)$.
4. $A_1 \subset f^{-1}(f(A_1))$ with equality if f is injective.

(II) Let B_1 and B_2 be two subsets of Y, then

1. $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.
2. $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.
3. $B_1 \subset B_2 \Rightarrow f^{-1}(B_1) \subset f^{-1}(B_2)$.
4. $f(f^{-1}(B_1)) \subset B_1$ with equality if f is surjective.

Proof.

(I) Let A_1 and A_2 be two subsets of X.

1. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

$$\begin{aligned} \text{Let } y \in f(A_1 \cup A_2) &\Leftrightarrow \exists x \in A_1 \cup A_2 : \ y = f(x) \\ &\Rightarrow x \in A_1 \text{ or } x \in A_2 : \ y = f(x) \\ &\Rightarrow y \in f(A_1) \text{ or } y \in f(A_2) \\ &\Rightarrow y \in f(A_1) \cup f(A_2). \end{aligned}$$

Then, $f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$.
On the other side,

$$\begin{aligned} \text{Let } y \in f(A_1) \cup f(A_2) &\Rightarrow y \in f(A_1) \text{ or } y \in f(A_2) \\ &\Rightarrow (\exists x_1 \in A_1 : \ y = f(x_1)) \text{ or } (\exists x_2 \in A_2 : \ y = f(x_2)) \\ &\Rightarrow (y = f(x_1) \text{ or } y = f(x_2)) \\ &\quad \text{with } (x_1 \in A_1 \Rightarrow x_1 \in A_1 \cup A_2) \text{ and } (x_2 \in A_2 \Rightarrow x_2 \in A_1 \cup A_2) \\ &\Rightarrow \exists x \in (A_1 \cup A_2)(x = x_1 \text{ or } x = x_2) \text{ such that } y = f(x) \in f(A_1 \cup A_2). \end{aligned}$$

Then, $f(A_1) \cup f(A_2) \subset f(A_1 \cup A_2)$.
Conclusion: $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

2. $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$.

$$\begin{aligned} \text{Let } y \in f(A_1 \cap A_2) &\Leftrightarrow \exists x \in A_1 \cap A_2 : \ y = f(x) \\ &\Rightarrow x \in A_1 \text{ and } x \in A_2 : \ y = f(x) \in f(A_1) \text{ and } y = f(x) \in f(A_2) \\ &\Rightarrow y \in f(A_1) \text{ and } y \in f(A_2) \\ &\Rightarrow y \in f(A_1) \cap f(A_2). \end{aligned}$$

Then, $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$.

3. $A_1 \subset A_2 \Rightarrow f(A_1) \subset f(A_2)$.
Suppose that $A_1 \subset A_2$ and we show that $f(A_1) \subset f(A_2)$.

$$\begin{aligned} \text{Let } y \in f(A_1) \Leftrightarrow & \ \exists x \in A_1 : \ y = f(x) \\ \Rightarrow & \ x \in A_2 : \ y = f(x) (\text{ since } A_1 \subset A_2) \\ \Rightarrow & \ y \in f(A_2). \end{aligned}$$

4. $A_1 \subset f^{-1}(f(A_1))$ with equality if f is injective.

$$\text{Let } x \in A_1 \Rightarrow f(x) \in f(A_1) \Rightarrow x \in f^{-1}(f(A)).$$

Then $A_1 \subset f^{-1}(f(A_1))$.
If f is injective, then $A_1 = f^{-1}(f(A_1))$. In fact,

$$\begin{aligned} \text{Let } x \in f^{-1}(f(A_1)) \Rightarrow & \ f(x) \in f(A_1) \\ \Rightarrow & \ \exists x' \in A_1 \text{ such that } f(x) = f(x') \\ \Rightarrow & \ x = x' (\text{ since } f \text{ is injective }) \\ \Rightarrow & \ x \in A_1. \end{aligned}$$

Then $A_1 = f^{-1}(f(A_1))$.

(II) Let B_1 and B_2 be two subsets of Y.

1. $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.

$$\begin{aligned} \text{Let } x \in f^{-1}(B_1 \cup B_2) \Leftrightarrow & \ f(x) \in (B_1 \cup B_2) \\ \Leftrightarrow & \ f(x) \in B_1 \text{ or } f(x) \in B_2 \\ \Leftrightarrow & \ x \in f^{-1}(B_1) \text{ or } x \in f^{-1}(B_2) \\ \Leftrightarrow & \ x \in (f^{-1}(B_1) \cup f^{-1}(B_2)). \end{aligned}$$

Then $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.

2. $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

$$\begin{aligned} \text{Let } x \in f^{-1}(B_1 \cap B_2) \Leftrightarrow & \ f(x) \in (B_1 \cap B_2) \\ \Leftrightarrow & \ f(x) \in B_1 \text{ and } f(x) \in B_2 \\ \Leftrightarrow & \ x \in f^{-1}(B_1) \text{ and } x \in f^{-1}(B_2) \\ \Leftrightarrow & \ x \in f^{-1}(B_1) \cap f^{-1}(B_2). \end{aligned}$$

Then $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

3. $B_1 \subset B_2 \Rightarrow f^{-1}(B_1) \subset f^{-1}(B_2)$.

$$\begin{aligned} \text{Let } x \in f^{-1}(B_1) \Rightarrow & \ f(x) \in B_1 \\ \Rightarrow & \ f(x) \in B_2 (\text{ since } B_1 \subset B_2) \\ \Rightarrow & \ x \in f^{-1}(B_2). \end{aligned}$$

4. $f(f^{-1}(B_1)) \subset B_1$ with equality if f is surjective.

$$\begin{aligned} \text{Let } y \in f(f^{-1}(B_1)) \Rightarrow & \quad \exists x \in f^{-1}(B_1) : \ y = f(x) \\ \Rightarrow & \quad f(x) = y \in B_1. \end{aligned}$$

Then $f(f^{-1}(B_1)) \subset B_1$.
If f is surjective, then $f(f^{-1}(B_1)) = B_1$. In fact,

$$\begin{aligned} \text{Let } y \in B_1 \Rightarrow & \quad y \in Y \\ \Rightarrow & \quad \exists x \in X : \ y = f(x) (\text{ since } f \text{ is surjective }) \\ \Rightarrow & \quad x \in f^{-1}(B_1) (\text{ since } y = f(x) \in B_1 \Leftrightarrow x \in f^{-1}(B_1)) \\ \Rightarrow & \quad y = f(x) \in f(f^{-1}(B_1)). \end{aligned}$$

□

2.2.5 The inverse mapping

Theorem 2.1

Let $f : X \to Y$ be a bijective mapping. The inverse mapping of f, denoted by f^{-1}, is the mapping that assigns to an element $y \in Y$ a unique element $x \in X$ such that $f(x) = y$.

$$\forall y \in Y, \quad f^{-1}(y) = x \Leftrightarrow y = f(x).$$

Remark 2.12

- $f \circ f^{-1} = Id_Y$ means $\forall y \in Y, \ (f \circ f^{-1})(y) = y$.
- $f^{-1} \circ f = Id_X$ means $\forall x \in X, \ (f^{-1} \circ f)(x) = x$.

Proposition 2.2

Let $f : X \to Y$ be a mapping.

1. The mapping $f : X \to Y$ is bijective if and only if there exists a mapping $f^{-1} : Y \to X$ such that

$$f^{-1} \circ f = Id_X \text{ and } f \circ f^{-1} = Id_Y.$$

We say that f is invertible and f^{-1} is its inverse mapping.

2. If f is bijective, then the inverse mapping f^{-1} is unique and it is bijective.

Proof.

" $\Rightarrow$ " Suppose that f is bijective.
Since f is bijective, we have

$$\forall y \in Y, \exists! x \in X : \ y = f(x).$$

We define $f^{-1}(y) = x$. Then

$$\begin{aligned} f^{-1}(y) = x \Rightarrow & \ f(f^{-1}(y)) = f(x) = y, \ \forall y \in Y \\ \Rightarrow & \ f \circ f^{-1} = Id_Y \\ \Rightarrow & \ f \circ f^{-1} \circ f = Id_Y \circ f \\ \Rightarrow & \ \forall x \in X, \ f(f^{-1} \circ f)(x)) = f(x) \\ \Rightarrow & \ \forall x \in X, \ f^{-1} \circ f = x \ \text{ (because } f \text{ is injective)} \\ \Rightarrow & \ f^{-1} \circ f = Id_X \end{aligned}$$

" $\Leftarrow$ " Suppose that f^{-1} exists. We will show that f is bijective.

Injectivity: Let $x_1, x_2 \in X$ and suppose $f(x_1) = f(x_2)$. Then

$$\begin{aligned} f(x_1) = f(x_2) \Rightarrow & \ f^{-1}(f(x_1)) = f^{-1}(f(x_2)) \\ \Rightarrow & \ Id_X(x_1) = Id_X(x_2) \\ \Rightarrow & \ x_1 = x_2. \end{aligned}$$

Hence, f is injective.

Surjectivity: Let $y \in Y$. Set $x = f^{-1}(y) \in X$. Then

$$f(x) = f(f^{-1}(y)) = Id_Y(y) = y.$$

Thus, f is surjective.

□

Example 2.18.
Let the mapping f defined by

$$\begin{aligned} f : \mathbb{R} & \ \to \mathbb{R} \\ x & \ \longmapsto f(x) = 2x - 1. \end{aligned}$$

Show that f is bijective and determine its inverse mapping f^{-1}.

- *f is injective* $\Leftrightarrow \forall x_1, x_2 \in \mathbb{R} : \ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$.
  Let $x_1, x_2 \in \mathbb{R}$ and suppose that $f(x_1) = f(x_2)$, then we have

$$\begin{aligned} f(x_1) = f(x_2) \Leftrightarrow & \ 2x_1 - 1 = 2x_2 - 1 \\ \Rightarrow & \ 2x_1 = 2x_2 \\ \Rightarrow & \ x_1 = x_2 \end{aligned}$$

  then f is injective.

- *f is surjective* $\Leftrightarrow \forall y \in \mathbb{R},\ \exists x \in \mathbb{R} :\ y = f(x)$.
  Let $y \in \mathbb{R}$ and we look for the existence of an $x \in \mathbb{R}$ such that $y = f(x)$.

$$\begin{aligned} y = f(x) \Rightarrow &\ y = 2x - 1 \\ \Rightarrow &\ y + 1 = 2x \\ \Rightarrow &\ x = \tfrac{y+1}{2} \in \mathbb{R}, \end{aligned}$$

  So

$$\forall y \in \mathbb{R},\ \exists x = \frac{y+1}{2} \in \mathbb{R} :\ y = f(x).$$

  Then f is surjective.

- *Is f bijective?*
  Since f is injective and surjective, then f is bijective.

- *Determine the expression of f^{-1} if it exists.*
  We have that f is bijective then there exists a unique inverse mapping f^{-1} of f.

$$\begin{aligned} f(x) = y \Leftrightarrow &\ 2x + 1 = y \\ \Leftrightarrow &\ x = \tfrac{y-1}{2} = f^{-1}(y) \end{aligned}$$

  Then the inverse mapping f^{-1} is given by

$$\begin{aligned} f^{-1} : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto f^{-1}(x) = \tfrac{x-1}{2}. \end{aligned}$$

Example 2.19.
Let the mapping $f : [0,1] \to [0,1]$ defined by $f(x) = x^2$.
Show that f is bijective and determine its inverse mapping f^{-1}.

- *f injective* $\Leftrightarrow \forall x_1, x_2 \in [0,1],\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
  Let $x_1, x_2 \in [0,1]$ and suppose that $f(x_1) = f(x_2)$, then we have

$$\begin{aligned} f(x_1) = f(x_2) \Rightarrow &\ x_1^2 = x_2^2 \\ \Rightarrow &\ |x_1| = |x_2| \\ \Rightarrow &\ x_1 = x_2 (\text{ because } x_1, x_2 \in [0,1]) \end{aligned}$$

  Then f is injective.

- *f surjective* $\Leftrightarrow \forall y \in [0,1],\ \exists x \in [0,1] :\ y = f(x)$.
  Let $y \in [0,1]$, we look for an $x \in [0,1]$ that satisfy $y = f(x)$.
  We have

$$\begin{aligned} f(x) = y \Leftrightarrow &\ x^2 = y \\ \Leftrightarrow &\ x = \sqrt{y} \in [0,1]. \end{aligned}$$

  Then $\forall y \in [0,1],\ \exists x = \sqrt{y} \in [0,1]$ such that $y = f(x)$. Then f is surjective.

- *Is f bijective?*
  Since f is injective and surjective, then f is bijective.

- *Determine the expression of f^{-1} if it exists.*
  The mapping f is bijective, then there exist a unique inverse mapping f^{-1} satisfying:

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

We have

$$\begin{aligned} f(x) = y \Rightarrow \quad & x^2 = y \\ \Rightarrow \quad & x = \sqrt{y} \\ \Rightarrow \quad & f^{-1}(y) = \sqrt{y}. \end{aligned}$$

Then the inverse mapping f^{-1} is given by

$$\begin{aligned} f^{-1} : [0,1] \quad & \to [0,1] \\ x \quad & \mapsto f^{-1}(x) = \sqrt{x}. \end{aligned}$$

2.3 Exercises

Exercise 2.1.

1. *Let the set $X = \{3, 6, 9\}$. determine the power set of set X.*
2. *Let $A = \{a, y, z\}$, $B = \{1, 2\}$, $C = \{8, \#\}$. Determine the cartesian product $A \times B \times C$ and $A \times C \times B$. Comments on the results.*

Exercise 2.2.

1. *Write explicitly the following sets then give their cardinal.*

$$A = \left\{ x \in \mathbb{Z}, \quad \frac{1}{2} \leq \frac{3x-4}{x+2} < 2 \right\}, \quad B = \{(x, y) : x \in \{1, 2, \ldots, 6\},\ y \in \{1, 2, \ldots, 6\},\ x+y = 10\}.$$

2. *Let $X = \{1, 2\}$*

   (i) *Determine $\mathcal{P}(X)$ and $\mathcal{P}(\mathcal{P}(X))$.*

   (ii) *Complete with the correct symbol: $\in$, $\subset$, $\notin$*
   $1 \ldots X$, $\{1\} \ldots X$, $\{1, 2\} \ldots \mathcal{P}(X)$, $\emptyset \ldots X$, $4 \ldots X$,
   $(1, 1) \ldots X \times X$, $\{\emptyset\} \ldots \mathcal{P}(X)$, $\{(1, 2)\} \ldots \mathcal{P}(\mathcal{P}(X))$.

Exercise 2.3.

1. *Let A, B and C be three subsets of a set Y. Show that*

(i) $C_Y(A \cup B) = C_Y(A) \cap C_Y(B)$; **(ii)** $A \cap B = \emptyset \Leftrightarrow A \subset (C_Y B)$;

(iii) $(A \setminus B) \setminus C = A \setminus (B \cup C)$; **(iv)** $(A \times C) \cup (B \times C) = (A \cup B) \times C$;

(v) $A \cup B = A \cap C \Leftrightarrow B \subset A \subset C$ *(supplementary).*

Exercise 2.4. *Consider the following mappings*

$$\begin{array}{rcl} f : \mathbb{N} \to & \mathbb{N} \\ n \mapsto & f(n) = 2n. \end{array} \qquad \begin{array}{rcl} g : \mathbb{N} \to & \mathbb{N} \\ n \mapsto & g(n) = \left\{ \begin{array}{ll} \frac{n}{2}, & n \text{ even}, \\ \frac{n-1}{2}, & n \text{ odd}. \end{array} \right. \end{array}$$

1. *Let* $X = \{2k+1,\ k \in \mathbb{N}\}$, *determine* $f^{-1}(X)$.
2. *Are these mappings injective? surjective? bijective?*
3. *Determine* $(f \circ g)$ *and* $(g \circ f)$, *are they injective? surjective?*

Exercise 2.5. *Let the mapping* $f : \mathbb{R} \to \mathbb{R}$ *defined by:* $f(x) = \frac{x^2-1}{x^2+1}$.
Let $A = [-1, 2]$, $B = \{-4, -2, 2\}$, $C = \{-1, \frac{1}{3}\}$, $D = \{3\}$.

1. *Determine* $f(A)$, $f(B)$, $f^{-1}(C)$ *and* $f^{-1}(D)$.
2. *Is the mapping* f *injective? is it surjective?*
3. *Find the largest possible intervals* $I \subset \mathbb{R}$ *and* $J \subset \mathbb{R}$ *such that the application*

$$\begin{array}{rcl} g : I \to & J \\ x \mapsto & g(x) = f(x) \end{array}$$

is bijective and determine g^{-1}.

Exercise 2.6. *(Supplementary exercise)*
Let X, Y *and* Z *be three sets and* $f : X \to Y$ *and* $g : Y \to Z$ *be two maps. We consider the mapping* $h = g \circ f$.

1. *Show that*
   (i) h *injective and* f *surjective* $\Rightarrow g$ *injective.*
   (ii) h *surjective and* f *injective* $\Rightarrow f$ *surjective.*
2. *Let* $A \subset X$ *and* $B \subset Y$. *Show that*

$$f(A) \cap B = \emptyset \Leftrightarrow A \cap f^{-1}(B) = \emptyset.$$

Exercise 2.7. *(Supplementary)*
Consider the following applications f, g, h and ϕ defined by

$$\begin{aligned} &f : \mathbb{R} \to \mathbb{R}, && g : [-\tfrac{\pi}{2}, \tfrac{\pi}{2}] \to \mathbb{R}, \\ &x \mapsto f(x) = \sin(x), && x \mapsto g(x) = \sin(x) \end{aligned}$$

$$\begin{aligned} &h : \mathbb{R} \to [-1, 1], && \phi : [-\tfrac{\pi}{2}, \tfrac{\pi}{2}] \to [-1, 1], \\ &x \mapsto h(x) = \sin(x), && x \mapsto \phi(x) = \sin(x) \end{aligned}$$

For each mapping, determine whether it is injective, surjective, or bijective.

2.4 Solution of exercises

Solution of exercise 2.1.

1. *Let the set $X = \{3, 6, 9\}$. determine the power set of set X.*

$$\mathcal{P}(X) = \{\emptyset,\ \{3\},\ \{6\},\ \{9\},\ \{3, 6\},\ \{3, 9\},\ \{6, 9\},\ \{3, 6, 9\}\}$$

2. *Let $A = \{a, y, z\},\ B = \{1, 2\},\ C = \{8, \#\}$. Determine the cartesian product $A \times B \times C$ and $A \times C \times B$. Comments on the results. The Cartesian product $A \times B \times C$ is the set of all ordered triples (x, y, z) such that $x \in A$, $y \in B$, and $z \in C$.*

$$\begin{aligned} A \times B \times C = \{&(a, 1, 8), (a, 1, \#), (a, 2, 8), (a, 2, \#), \\ &(y, 1, 8), (y, 1, \#), (y, 2, 8), (y, 2, \#), \\ &(z, 1, 8), (z, 1, \#), (z, 2, 8), (z, 2, \#)\} \end{aligned}$$

The Cartesian product $A \times C \times B$ is:

$$\begin{aligned} A \times C \times B = \{&(a, 8, 1), (a, 8, 2), (a, \#, 1), (a, \#, 2), \\ &(y, 8, 1), (y, 8, 2), (y, \#, 1), (y, \#, 2), \\ &(z, 8, 1), (z, 8, 2), (z, \#, 1), (z, \#, 2)\} \end{aligned}$$

The two Cartesian products are not equal:

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

because the order of elements in ordered triples matters. Changing the order of the sets changes the positions of the elements in the triples.

However, both sets have the same number of elements:

$$Card(A \times B \times C) = Card(A \times C \times B) = 3 \times 2 \times 2 = 12$$

Solution of exercise 2.2.

1. *Write explicitly the following sets then give their cardinal.*

- $A = \{x \in \mathbb{Z}, \quad \frac{1}{2} \leq \frac{3x-4}{x+2} < 2\}$,

Case 1: *If* $x+2 > 0 \Rightarrow x > -2$, *then*

$$\begin{aligned} \tfrac{1}{2} \leq \tfrac{3x-4}{x+2} &\Rightarrow \quad \tfrac{x+2}{2} \leq 3x-4 \\ &\Rightarrow \quad 2 \leq x \ldots\ldots (1) \end{aligned}$$

and

$$\begin{aligned} \tfrac{3x-4}{x+2} < 2 &\Rightarrow \quad 3x-4 < 2(x+2) \\ &\Rightarrow \quad x < 8 \ldots\ldots (2) \end{aligned}$$

Combining (1) *and* (2), *we obtain that* $2 \leq x < 8$.
Then

$$\begin{aligned} A = &\quad \{x \in \mathbb{Z}, \quad \tfrac{1}{2} \leq \tfrac{3x-4}{x+2} < 2\} \\ = &\quad \{x \in \mathbb{Z}, \quad 2 \leq x < 8\} \\ = &\quad \{2,3,4,5,6,7\} \end{aligned}$$

Case 2: *If* $x+2 < 0 \Rightarrow x < -2$, *then*

$$\begin{aligned} \tfrac{1}{2} \leq \tfrac{3x-4}{x+2} &\Rightarrow \quad \tfrac{x+2}{2} \geq 3x-4 \\ &\Rightarrow \quad 2 \geq x \ldots\ldots (3) \end{aligned}$$

and

$$\begin{aligned} \tfrac{3x-4}{x+2} < 2 &\Rightarrow \quad 3x-4 > 2(x+2) \\ &\Rightarrow \quad x > 8 \ldots\ldots (4) \end{aligned}$$

Combining (3) *and* (4), *we obtain that* $8 < x$ *and* $x \leq 2$ *which is a contradiction with* $x < -2$. *So in the case* $x+2 < 0$ *we have no solutions.*

and $Card(A) = 6$.

- $$\begin{aligned} B = &\quad \{(x,y) : x \in \{1,2,\ldots,6\},\ y \in \{1,2,\ldots,6\},\ x+y = 10\}. \\ = &\quad \{(6,4),\ (5,5),\ (4,6)\}. \end{aligned}$$

and $Card(B) = 3$.

2. *Let* $X = \{1,2\}$, *we have* $Card(X) = 2$.

(i) *Determine* $\mathcal{P}(X)$ *and* $\mathcal{P}(\mathcal{P}(X))$.

- $Card(\mathcal{P}(X)) = 2^{Card(X)} = 2^2 = 4$, *then* $\mathcal{P}(X) = \{\emptyset,\ \{1,2\},\ \{1\},\ \{2\}\}$.
- $Card(\mathcal{P}(\mathcal{P}(X))) = 2^{Card(\mathcal{P}(X))} = 2^4 = 16$, *then*

$$\begin{aligned} \mathcal{P}(\mathcal{P}(X)) = \Big\{ &\emptyset;\ \mathcal{P}(X);\ \{\emptyset\};\ \{\{1,2\}\};\ \{\{1\}\};\ \{\{2\}\};\ \{\emptyset,\{1,2\}\};\ \{\emptyset,\{1\}\}; \\ &\{\emptyset,\{2\}\};\ \{\{1,2\},\ \{1\}\};\ \{\{1,2\},\ \{2\}\};\ \{\{1\},\ \{2\}\}; \\ &\{\emptyset,\ \{1,2\},\ \{1\}\};\ \{\emptyset,\ \{1,2\},\ \{2\}\};\ \{\{1,2\},\ \{1\},\ \{2\}\};\ \{\emptyset,\ \{1\},\ \{2\}\}\Big\}. \end{aligned}$$

Remark 2.13

The sets $\{\{1\}\}$ *and* $\{1\}$ *are not equal. In fact,*

- $\{1\}$ *is the set that contains the number* 1*, his unique element is* 1*.*
- $\{\{1\}\}$ *is the set that contains the set* $\{1\}$*, his unique element is not* 1*, it is the set* $\{1\}$*.*

Then

$$1 \in \{1\} \text{ but } 1 \notin \{\{1\}\},$$

and

$$\{1\} \in \{\{1\}\}.$$

(ii) *Complete with the correct symbol:* $\in, \subset, \notin$

- $1 \in X$,
- $\{1,2\} \in \mathcal{P}(X)$,
- $4 \notin X$,
- $\{\emptyset\} \notin \mathcal{P}(X)$,
- $\{1\} \notin X$ *and* $\{1\} \subset X$,
- $\emptyset \notin X$,
- $(1,1) \in X \times X$,
- $\{(1,2)\} \notin \mathcal{P}(\mathcal{P}(X))$, *because* $(1,2)$ *is an element of* $\mathcal{P}(X)$ *then* $\{(1,2)\}$ *is not a subset of* $\mathcal{P}(X)$.

Solution of exercise 2.3. *Let* A, B *and* C *be three subsets of a set* Y*.*

(i) $C_Y(A \cup B) = C_Y(A) \cap C_Y(B)$*;*

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

Then $C_Y(A \cup B) = C_Y(A) \cap C_Y(B)$*.*

(ii) $A \cap B = \emptyset \Leftrightarrow A \subset (C_Y B)$*;*

- *We show that* $A \cap B = \emptyset \Rightarrow A \subset (C_Y B)$*.*
  Suppose that $A \cap B = \emptyset$ *and we show that* $A \subset (C_Y B)$*.*
  Let $x \in A$*, since* $A \cap B = \emptyset$*, then* $x \notin B$ *that is* $x \in C_Y B$*.*
  Then $A \subset (C_Y B)$*.*
  Therefore, $A \cap B = \emptyset \Rightarrow A \subset (C_Y B)$*.*

- *We show that* $A \subset (C_Y B) \Rightarrow A \cap B = \emptyset$.
  We reason by contradiction. suppose that $A \subset (C_Y B)$ *and* $A \cap B \neq \emptyset$.
  Since $A \cap B \neq \emptyset$, *then there exists* $x \in A \cap B$.

$$\begin{aligned} x \in A \cap B \Rightarrow & \quad x \in A \text{ and } x \in B. \\ \Rightarrow & \quad x \in C_Y B \text{ and } x \in B, \text{ (because } (A \subset (C_Y B) \text{).} \end{aligned}$$

  Which is a contradiction.
  Then, $A \cap B = \emptyset$. *Therefore,* $A \subset (C_Y B) \Rightarrow A \cap B = \emptyset$.

Conclusion: $A \cap B = \emptyset \Leftrightarrow A \subset (C_Y B)$.

(iii) $(A \setminus B) \setminus C = A \setminus (B \cup C)$;
We have to show that $[(A \setminus B) \setminus C] \subset [A \setminus (B \cup C)]$ *and* $[A \setminus (B \cup C)] \subset [(A \setminus B) \setminus C]$.

$$\begin{aligned} \text{Let } x \in (A \setminus B) \setminus C \Leftrightarrow & \quad x \in (A \setminus B) \text{ and } x \notin C \\ \Leftrightarrow & \quad (x \in A \text{ and } x \notin B) \text{ and } x \notin C \\ \Leftrightarrow & \quad x \in A \text{ and } (x \notin B \text{ and } x \notin C) \text{ (associativity property)} \\ \Leftrightarrow & \quad x \in A \text{ and } (x \in C_Y B \text{ and } x \in C_Y C) \\ \Leftrightarrow & \quad x \in A \text{ and } x \in (C_Y B) \cap (C_Y C) \\ \Leftrightarrow & \quad x \in A \text{ and } x \in C_Y (B \cup C) \text{ (De Morgan law)} \\ \Leftrightarrow & \quad x \in A \text{ and } x \notin (B \cup C) \\ \Leftrightarrow & \quad x \in A \setminus (B \cup C). \end{aligned}$$

(iv) $(A \times C) \cup (B \times C) = (A \cup B) \times C$;
We have to show that $[(A \times C) \cup (B \times C)] \subset (A \cup B) \times C]$
and $[(A \cup B) \times C] \subset [(A \times C) \cup (B \times C)]$.

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

(v) $A \cup B = A \cap C \Leftrightarrow B \subset A \subset C$

- *We show that* $A \cup B = A \cap C \Rightarrow B \subset A \subset C$.
  Suppose that $A \cup B = A \cap C$ *and we show that* $B \subset A \subset C$.
  - *Let* $x \in B$, *then* $x \in A \cup B$. *By the equality*

$$A \cup B = A \cap C,$$

  we obtain

$$x \in A \cap C.$$

  Hence, $x \in A$. *Therefore,* $B \subset A$.

- *Let $x \in A$, then $x \in A \cup B$. By the equality*

$$A \cup B = A \cap C,$$

we have

$$x \in A \cap C.$$

Hence, $x \in C$. Therefore, $A \subset C$.

Conclusion: $B \subset A \subset C$.

- *We show that $B \subset A \subset C \Rightarrow A \cup B = A \cap C$.*
  Suppose that $B \subset A \subset C$ and we show that $A \cup B = A \cap C$.
  - *Since $B \subset A$, we have $A \cup B = A$.*
  - *Since $A \subset C$, we have $A \cap C = A$.*

  Then $A \cup B = A = A \cap C$, therefore, $A \cup B = A \cap C$.
  Therefore, $B \subset A \subset C \Rightarrow A \cup B = A \cap C$.

Conclusion: $A \cup B = A \cap C \Leftrightarrow B \subset A \subset C$.

Solution of exercise 2.4.

1. *Let $X = \{2k+1,\ k \in \mathbb{N}\}$, determine $f^{-1}(X)$.*

$$\begin{aligned} f^{-1}(X) &= \{n \in \mathbb{N} :\ f(n) \in X\} \\ &= \{n \in \mathbb{N} :\ 2n = 2k+1,\ k \in \mathbb{N}\} \\ &= \{n \in \mathbb{N} :\ n = k + \tfrac{1}{2},\ k \in \mathbb{N}\} \\ &= \emptyset. \end{aligned}$$

   In fact, $f(n)$ is always even, while every element of X is odd, so no $n \in \mathbb{N}$ satisfies $f(n) \in X$. Then $f^{-1}(X) = \emptyset$.

2. *Are these mappings injective? surjective? bijective?*

   - *f is injective $\Leftrightarrow \forall n_1, n_2 \in \mathbb{N}, \quad f(n_1) = f(n_2) \Rightarrow n_1 = n_2$.*
     Let n_1, $n_2 \in \mathbb{N}$, suppose that $f(n_1) = f(n_2)$ and we verify if $n_1 = n_2$.
     We have

$$f(n_1) = f(n_2) \Rightarrow 2n_1 = 2n_2 \Rightarrow n_1 = n_2.$$

     Therefore f is injective.

   - *f is surjective $\Leftrightarrow \forall m \in \mathbb{N}, \exists n \in \mathbb{N} :\ f(n) = m$.*
     Let $m \in \mathbb{N}$, we look for the existence of $n \in \mathbb{N}$ such that $f(n) = m$. We have

$$f(n) = m \Rightarrow 2n = m \Rightarrow n = \frac{m}{2}$$

     but $\frac{m}{2}$ is not always a natural number, it is a natural number if only m is an even number. Therefore, f is not surjective for every $m \in \mathbb{N}$.

Conclusion: *f is injective and not surjective, then f is not bijective.*

- *g is injective* $\Leftrightarrow \forall n_1, n_2 \in \mathbb{N}, \quad g(n_1) = g(n_2) \Rightarrow n_1 = n_2$.
  Let n_1, $n_2 \in \mathbb{N}$, suppose that $g(n_1) = g(n_2)$ and we verify if $n_1 = n_2$.

  Case 1: n_1 **and** n_2 **are even** *We have*

  $$g(n_1) = g(n_2) \Rightarrow \frac{n_1}{2} = \frac{n_2}{2} \Rightarrow 2n_1 = 2n_2 \Rightarrow n_1 = n_2.$$

  Then, in this case g is injective.

  Case 2: n_1 **and** n_2 **are odd** *We have*

  $$\begin{aligned} g(n_1) = g(n_2) \Rightarrow & \ \tfrac{n_1-1}{2} = \tfrac{n_2-1}{2} \\ \Rightarrow & \ 2(n_1-1) = 2(n_2-1) \\ \Rightarrow & \ n_1 - 1 = n_2 - 1 \\ \Rightarrow & \ n_1 = n_2. \end{aligned}$$

  Then, in this case g is injective.

  Case 3: n_1 **is odd and** n_2 **is even** *We have*

  $$\begin{aligned} g(n_1) = g(n_2) \Rightarrow & \ \tfrac{n_1-1}{2} = \tfrac{n_2}{2} \\ \Rightarrow & \ 2(n_1-1) = 2n_2 \\ \Rightarrow & \ n_1 - 1 = n_2. \end{aligned}$$

  For example, for $n_1 = 3$ we have $n_1 - 1 = 3 - 1 = 2$. Then $n_2 = 2$. Therefore

  $$\left.\begin{array}{l} g(n_1) = g(3) = \frac{3-1}{2} = 1 \\ g(n_2) = g(2) = \frac{2}{2} = 1 \end{array}\right\} \text{ Then } g(n_1) = g(n_2) \text{ but } n_1 \neq n_2$$

  Then g is not injective in this case.

  Conclusion: *g is not injective on $\mathbb{N}$.*

- *g is surjective* $\Leftrightarrow \forall m \in \mathbb{N}, \exists n \in \mathbb{N} : \ g(n) = m$.
  Let $m \in \mathbb{N}$, we look for the existence of $n \in \mathbb{N}$ such that $g(n) = m$.

  Case 1: $g(n) = m \Rightarrow \frac{n}{2} = m \Rightarrow n = 2m$.
  Then, $\exists n = 2m \in \mathbb{N} : \ g(n) = m$.

  Case 2: $g(n) = m \Rightarrow \frac{n-1}{2} = m \Rightarrow n = 2m + 1$.
  Then, $\exists n = 2m + 1 \in \mathbb{N} : \ g(n) = m$.

  Conclusion: *g is surjective.*

Conclusion: *g is not injective and it is surjective, then g is not bijective.*

3. *Determine $(f \circ g)$ and $(g \circ f)$, are they injective? surjective?*
   The expression of $(f \circ g)$:

   $$\mathbb{N} \xrightarrow{g} \mathbb{N}, \quad \mathbb{N} \xrightarrow{f} \mathbb{N}$$
   $(f \circ g)$ *is well defined .*

$$(f \circ g)(n) = f(g(n)) = 2g(n) = \begin{cases} n & n \text{ even} \\ n-1 & n \text{ odd} \end{cases}$$

- $(f \circ g)$ *is injective* $\Leftrightarrow \forall n_1, n_2 \in \mathbb{N}, \quad (f \circ g)(n_1) = (f \circ g)(n_2) \Rightarrow n_1 = n_2$.
  Let n_1, $n_2 \in \mathbb{N}$, *suppose that* $(f \circ g)(n_1) = (f \circ g)(n_2)$ *and we verify if* $n_1 = n_2$.
  If n_1 *is even and* n_2 *is odd, we have*

  $$(f \circ g)(n_1) = (f \circ g)(n_2) \Rightarrow n_1 = n_2 - 1.$$

  For $n_1 = 2$ *and* $n_2 = 3$, *we have*

  $$(f \circ g)(2) = (f \circ g)(3) = 2 \text{ but } 2 \neq 3.$$

  Then $(f \circ g)$ *is not injective.*
- $(f \circ g)$ *is surjective* $\Leftrightarrow \forall m \in \mathbb{N}, \exists n \in \mathbb{N} : \ (f \circ g)(n) = m$.
  Let $m \in \mathbb{N}$, *we look for the existence of* $n \in \mathbb{N}$ *such that* $(f \circ g)(n) = m$.
  In the expression of $(f \circ g)$, *we remark that the image of* $(f \circ g)$ *does not contains odd numbers the images is always an even number.*
  Then $(f \circ g)$ *is not surjective* $\forall m \in \mathbb{N}$.

The expression of $(g \circ f)$:

$$\mathbb{N} \xrightarrow{f} \mathbb{N}, \quad \mathbb{N} \xrightarrow{g} \mathbb{N}$$
$$(g \circ f) \text{ is well defined .}$$

$$(g \circ f)(n) = g(f(n)) = g(2n) = \frac{2n}{2} = n.$$

Then $(g \circ f)$ *is the identity mapping on* $\mathbb{N}$, *then it is injective and surjective.*

Solution of exercise 2.5.
Let the mapping $f : \mathbb{R} \to \mathbb{R}$ *defined by:* $f(x) = \frac{x^2-1}{x^2+1}$.

1. *Determine* $f(A)$, $f(B)$, $f^{-1}(C)$ *and* $f^{-1}(D)$.
   We draw the table of the variation of the mapping f, *we have*

   $$f'(x) = \frac{4x}{(x^2+1)^2}$$

x	$-\infty$		0		$+\infty$
$f'(x)$		$-$	0	$+$	
$f(x)$	1	↘	f(0)=-1	↗	1

- $f(A) = f([-1,2]) = [f(0), f(-1)] \cup [f(0), f(2)] = [-1,0] \cup [-1, \frac{3}{5}] = [-1, \frac{3}{5}]$.
- $f(B) = \{f(-4), f(-2), f(2)\} = \{\frac{15}{16}, \frac{3}{5}\}$.
- $$\begin{aligned} f^{-1}(C) = & \{x \in \mathbb{R},\ f(x) \in \{-1, \tfrac{1}{3}\}\} \\ = & \{x \in \mathbb{R},\ f(x) = -1 \text{ or } f(x) = \tfrac{1}{3}\} \\ = & \{x \in \mathbb{R},\ \tfrac{x^2-1}{x^2+1} = -1 \text{ or } \tfrac{x^2-1}{x^2+1} = \tfrac{1}{3}\} \\ = & \{x \in \mathbb{R},\ x^2 - 1 = -x^2 - 1 \text{ or } 3x^2 - 3 = x^2 + 1\} \\ = & \{x \in \mathbb{R},\ 2x^2 = 0 \text{ or } 2x^2 = 4\} \\ = & \{x \in \mathbb{R},\ x = 0 \text{ or } x^2 = 2\} \\ = & \{x \in \mathbb{R},\ x = 0 \text{ or } x = \sqrt{2} \text{ or } x = -\sqrt{2}\} \\ = & \{0, \sqrt{2}, -\sqrt{2}\} \end{aligned}$$
- $$\begin{aligned} f^{-1}(D) = & \{x \in \mathbb{R},\ f(x) \in \{3\}\} \\ = & \{x \in \mathbb{R},\ f(x) = 3\} \\ = & \{x \in \mathbb{R},\ \tfrac{x^2-1}{x^2+1} = 3\} \\ = & \{x \in \mathbb{R},\ x^2 - 1 = 3x^2 + 3\} \\ = & \{x \in \mathbb{R},\ -4 = 2x^2\} \\ = & \{x \in \mathbb{R},\ x^2 = -2 \text{ has no solution in } \mathbb{R}\} \\ = & \emptyset \end{aligned}$$

2. Is the mapping f injective? is it surjective?

- *f is injective* $\Leftrightarrow \forall x_1, x_2 \in \mathbb{R}, \quad f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
  We have $f(-2) = f(2) = \frac{3}{5}$, but $2 \neq -2$, then f is not surjective.
- *f is surjective* $\Leftrightarrow \forall y \in \mathbb{R}, \exists x \in \mathbb{R} :\ f(x) = y$.

  Method 1: *We have from the table of the variation of f that $f(\mathbb{R}) = [-1,1[$, then $f(\mathbb{R}) \neq \mathbb{R}$ (The image under f of the domaine of f it is different of its co-domaine).*
  Thus, f is not surjective.

  Method 2: *We have $f^{-1}(\{3\}) = \emptyset$, then $\exists y = 3$ and there is not $x \in \mathbb{R}$ such that $f(x) = 3$. Therefore, f is not surjective.*

  Method 3: *Using the definition of surjectivity.*

3. Find the largest possible intervals $I \subset \mathbb{R}$ and $J \subset \mathbb{R}$ such that the application

$$\begin{aligned} g : I \to & \quad J \\ x \mapsto & \quad g(x) = f(x) \end{aligned}$$

is bijective and determine g^{-1}.

- *The largest interval where g is surjective.*
  We have from the variation table of g, $g(\mathbb{R}) = [-1,1[$, then g is surjective on $J = [-1,1[$.

- *The largest intervals where g is injective.*
  We have
  - *g is strictly increasing on $[0,+\infty[$, then it is injective on $I_1=[0,+\infty[$.*
  - *g is strictly decreasing on $]-\infty,0]$, then it is injective on $I_2=]-\infty,0]$.*

Then the largest intervals where g is injective are $I_1=[0,+\infty[$ and $I_2=]-\infty,0]$ the corresponding image under g in both cases is $J=[-1,1[$.
therefore,

$$\begin{array}{rl} g:I_1 & \to J \\ x\mapsto & g(x)=f(x) \end{array} \text{ is bijective} \qquad \begin{array}{rl} g:I_2 & \to J \\ x\mapsto & g(g)=f(x) \end{array} \text{ is bijective}$$

- *The inverse mapping of g.*
  Since g is bijective then the inverse mapping exists.
  Let $y\in[-1,1[$, we have

$$\begin{array}{rl} g(x)=y\Rightarrow & \frac{x^2-1}{x^2+1}=y \\ \Rightarrow & x^2=\frac{1+y}{1-y} \end{array}$$

since $y\in[-1,1[$, then $\frac{1+y}{1-y}\geq 0$. Thus, $x=\pm\sqrt{\frac{1+y}{1-y}}$.
Then the inverse mapping of g is:

$$\begin{array}{rl} g^{-1}:J & \to I_1 \\ x\mapsto & g^{-1}(x)=\sqrt{\frac{1+y}{1-y}} \end{array} \qquad \begin{array}{rl} g^{-1}:J & \to I_2 \\ x\mapsto & g^{-1}(x)=-\sqrt{\frac{1+y}{1-y}} \end{array}$$

Chapter 3

Binary relations

There are many types of relationships in our everyday life. Relationships exist between people, such as parent-child, student-teacher, and employer-employee. In mathematics, a relation considers the existence of a certain connection or link, often between pairs of objects in a definite order. When such connections are considered between pairs of elements, we call them binary relations.
This chapter introduces the basic concepts of binary relations, including representation, properties (such as reflexivity, symmetry, antisymmetry and transitivity), equivalence relations, and order relations.

3.1 Definitions

Definition 3.1

A **binary relation** $\mathcal{R}$ on nonempty set X is defined by any subset G of $X \times X$ characterized by a certain property that links the elements of X.

- When $(x, y) \in G$, we say that x is related to y via $\mathcal{R}$, and we write $x\mathcal{R}y$.
- We call the **graph** of the relation $\mathcal{R}$ the subset of $X \times X$ denoted $G_{\mathcal{R}}$ defined by

$$G_{\mathcal{R}} = \{(x, y) \in X \times X : \ x\mathcal{R}y\}.$$

Example 3.1.

1. *Let $X = \mathbb{R}$. We define the relation $\mathcal{R}_1$ by*

$$\forall x, y \in \mathbb{R}, \quad x\mathcal{R}_1 y \Leftrightarrow x = y.$$

The graph of $\mathcal{R}_1$ is

$$G_{\mathcal{R}_1} = \{(x, x) \in \mathbb{R} \times \mathbb{R} : \ x \in \mathbb{R}\}.$$

2. *Let $X = \mathbb{R}$. We define the relation $\mathcal{R}_2$ by*

$$\forall x, y \in \mathbb{R}, \quad x\mathcal{R}_2 y \Leftrightarrow x \leq y.$$

The graph of $\mathcal{R}_2$ is

$$\begin{aligned} G_{\mathcal{R}_2} &= \{(x,y) \in \mathbb{R} \times \mathbb{R} : \ x\mathcal{R}_2 y\} \\ &= \{(x,y) \in \mathbb{R} \times \mathbb{R} : \ x \leq y\}. \end{aligned}$$

3. *Let $X = \mathbb{N}^* = \{1, 2, 3, \ldots\}$. We define the relation $\mathcal{R}_3$ by*

$$\forall x, y \in \mathbb{N}^*, \quad x\mathcal{R}_3 y \Leftrightarrow x \text{ divides } y.$$

In other words,

$$x \text{ divides } y \Leftrightarrow \exists k \in \mathbb{N}^* : \ y = kx.$$

The graph of $\mathcal{R}_3$ is

$$\begin{aligned} G_{\mathcal{R}_3} &= \{(x,y) \in \mathbb{N}^* \times \mathbb{N}^* : \ x\mathcal{R}_3 y\} \\ &= \{(x,y) \in \mathbb{N}^* \times \mathbb{N}^* : \ y = kx, \ k \in \mathbb{N}^*\} \\ &= \{(x,kx) \in \mathbb{N}^* \times \mathbb{N}^* : \ y = kx, \ k \in \mathbb{N}^*\}. \end{aligned}$$

Types of relations

Definition 3.2

Let $\mathcal{R}$ be a binary relation on a nonempty set X. We say that the relation $\mathcal{R}$ is

- **Reflexive** if $\forall x \in X, \ x\mathcal{R}x$.
  In a reflexive relation, each element of X is related to itself.
- **Symmetric** if $\forall x, y \in X, \ x\mathcal{R}y \Rightarrow y\mathcal{R}x$.
  In a symmetric relation, if any one element is related to any other element, then the second element is related to the first as well.
- **Antisymmetric** if $\forall x, y \in X, \ (x\mathcal{R}y \text{ and } y\mathcal{R}x) \Rightarrow (x = y)$.
  In an antisymmetric relation, if one element is related to another and the second element is related back to the first, then the two elements must actually be the same.
- **Transitive** if $\forall x, y, z \in X, \ (x\mathcal{R}y \text{ and } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.
  In a transitive relation, if any one element is related to a second element and that second element is related to a third element, then the first element is related to the third element.

Remark 3.1

Let $\mathcal{R}$ be a binary relation on a nonempty set X. We say that the relation $\mathcal{R}$ is

- **Not Reflexive** if $\exists x \in X,\ x \not\mathcal{R} x$.
  There is at least one element in X that is not related to itself.
- **Not symmetric or asymmetric** if $\exists x, y \in X,\ x\mathcal{R}y$ and $y \not\mathcal{R} x$.
  There is at least one pair of elements where one element is related to the other, but the relation does not go in the reverse direction.
- **Not antisymmetric** if $\exists x, y \in X,\ (x\mathcal{R}y$ and $y\mathcal{R}x)$ and $(x \neq y)$.
  There is at least one pair of distinct elements that are mutually related.
- **Not transitive** if $\exists x, y, z \in X,\ (x\mathcal{R}y$ and $y\mathcal{R}z)$ and $x \not\mathcal{R} z$.
  There exists at least one triple of elements x, y and $z \in X$ where x relates to y and y relates to z, but x is does not relate to z.

Example 3.2.

1. *The relation $\mathcal{R}_1$ defined by*

$$\forall x, y \in \mathbb{R}, \quad x\mathcal{R}_1 y \Leftrightarrow x = y,$$

is reflexive, symmetric, transitive and antisymmetric. Indeed,

- *Let $x \in \mathbb{R}$. Since $x = x$, we have $x\mathcal{R}_1 x$.*
  Therefore, the relation $\mathcal{R}_1$ is reflexive.
- *Let $x, y \in \mathbb{R}$, we have $x = y$, then $y = x$.*
  Hence, the relation $\mathcal{R}_1$ is symmetric.
- *Let $x, y \in \mathbb{R}$, we have $x = y$ and $y = x$, then $x = y$.*
  Therefore, the relation $\mathcal{R}_1$ is antisymmetric.
- *Let $x, y, z \in \mathbb{R}$, we have $x = y$ and $y = z$, then $x = z$.*
  Thus, the relation $\mathcal{R}_1$ is transitive.

2. *The relation $\mathcal{R}_2$ defined by*

$$\forall x, y \in \mathbb{R}, \quad x\mathcal{R}_2 y \Leftrightarrow x \leq y,$$

is reflexive,transitive and antisymmetric but $\mathcal{R}_2$ is not symmetric. Indeed,

- *Let $x \in \mathbb{R}$, we have $x \leq x$, then $x\mathcal{R}_2 x$.*
  Therefore, the relation $\mathcal{R}_2$ is reflexive.
- *Let $x, y \in \mathbb{R}$, we have $x \leq y$ and $y \leq x$, then $x = y$.*
  Thus, the relation $\mathcal{R}_2$ is antisymmetric.

- *Let $x, y, z \in \mathbb{R}$, we have $x \leq y$ and $y \leq z$, then $x \leq z$.*
  Hence, the relation $\mathcal{R}_2$ is transitive.
- *The relation $\mathcal{R}_2$ is not symmetric, because*

$$\text{There exist } x, y \in \mathbb{R}, \quad \text{such that } x\mathcal{R}_2 y \text{ and } y\not\mathcal{R}_2 x.$$

For example, $2 \leq 7$ and $7 \not\leq 2$.

3. *The relation $\mathcal{R}_3$ defined by*

$$\forall x, y \in \mathbb{N}^*, \quad x\mathcal{R}_3 y \Leftrightarrow x \text{ divides } y,$$

is reflexive, transitive and antisymmetric but $\mathcal{R}_3$ is not symmetric. Indeed,

- ***Reflexive:*** *Let $x \in \mathbb{N}^*$. Since x divides x, then $x\mathcal{R}_3 x$.*
  Therefore, the relation $x\mathcal{R}_3$ is reflexive.
- ***Antisymmetric:*** *We show that the relation $\mathcal{R}_3$ is antisymmetric, that is*

$$\forall x, y \in \mathbb{N}^*, \ (x\mathcal{R}_3 \text{ and } y\mathcal{R}_3 x) \Rightarrow x = y.$$

Let $x, y \in \mathbb{N}^*$, we have

$$x \text{ divides } y \Leftrightarrow \exists k \in \mathbb{N}^* : \ y = kx$$

$$y \text{ divides } x \Leftrightarrow \exists k' \in \mathbb{N}^* : \ x = k'y$$

then

$$(x = k'y = k'kx) \Rightarrow x(1 - k'k) = 0$$

since $x \in \mathbb{N}^*$, then $x \neq 0$ thus $(1 - k'k) = 0$

$$k'k = 1 \Leftrightarrow k' = k = 1 \text{ (because } k \text{ and } k' \text{ are positive integers).}$$

Then $x = y$.
Therefore, the relation $\mathcal{R}_3$ is antisymmetric.

- ***Transitive:*** *We show that the relation $\mathcal{R}_3$ is transitive, that is*

$$\forall x, y, z \in \mathbb{N}^*, \ (x\mathcal{R}_3 y \text{ and } y\mathcal{R}_3 z) \Rightarrow x\mathcal{R}_3 z.$$

Let $x, y, z \in \mathbb{N}^*$, we have

$$x \text{ divides } y \Leftrightarrow \exists k \in \mathbb{N}^* : \ y = kx$$

$$y \text{ divides } z \Leftrightarrow \exists k' \in \mathbb{N}^* : \ z = k'y$$

then

$$z = k'y = k'kx.$$

We set $z = k''x$ where $k'' = k'k \in \mathbb{N}^*$. Therefore, x divides z.
Hence, the relation $\mathcal{R}_3$ is transitive.

- ***We show that the relation $\mathcal{R}_3$ is not symmetric:***

$$\mathcal{R}_3 \text{ is symmetric } \Rightarrow (\forall x, y \in \mathbb{N}^*,\ x \text{ divides } y \Rightarrow y \text{ divides } x)$$

$$\mathcal{R}_3 \text{ is not symmetric } \Leftrightarrow (\exists x, y \in \mathbb{N}^*,\ x\mathcal{R}_3 y \text{ and } y\not\mathcal{R}_3 x)$$

In fact, when $x = 2$ and $y = 4$, we have 2 divides 4, but 4 does not divide 2. Therefore, the relation $\mathcal{R}_3$ is not symmetric.

Remark 3.2

A relation can be non-symmetric and non-antisymmetric. (The notions of symmetric and antisymmetric are not opposite.)

3.2 Equivalence relation

The main idea behind equivalence relations is that they let us group together things that may look different but share an important similarity or relation. Equivalence relations are useful whenever we care more about which group or category an element belongs to than about the element itself.

3.2.1 Definition

Definition 3.3

A relation $\mathcal{R}$ on a set X is called an **equivalence relation** if it is **reflexive, symmetric** and **transitive**.

Example 3.3.

1. *Whatever the set X, the equality relation $=$ is an equivalence relation.*
2. *The relation $\mathcal{R}_2$ defined by*

$$\forall x, y \in \mathbb{R}, \quad x\mathcal{R}_2 y \Leftrightarrow x \leq y,$$

is not an equivalence relation, because it is not symmetric.

3. *The relation $\mathcal{R}_3$ defined by*

$$\forall x, y \in \mathbb{N}^*, \quad x\mathcal{R}_3 y \Leftrightarrow x \text{ divides } y,$$

is not an equivalence relation, because it is not symmetric.

3.2.2 Equivalence class

Definition 3.4

Let $\mathcal{R}$ be an equivalence relation on a nonempty set X, and let $x \in X$. The set of all elements in X that are related to x via $\mathcal{R}$ is called **equivalence class** of x. It is denoted by $\dot{x}$ or C_x or $\overline{x}$. We write

$$\dot{x} = \{y \in X : \ x\mathcal{R}y\}.$$

Example 3.4.
Let the binary relation $\mathcal{R}$ defined by

$$\forall x, y \in \mathbb{R}, \quad x\mathcal{R}y \Leftrightarrow x^2 = y^2.$$

The relation $\mathcal{R}$ is an equivalence relation. In fact,

1. *We show that the relation $\mathcal{R}$ is reflexive, that is*

   $$\forall x \in \mathbb{R}, \ x\mathcal{R}x.$$

   Let $x \in \mathbb{R}$, $x^2 = x^2$ then $x\mathcal{R}x$. Then $\mathcal{R}$ is reflexive.

2. *We show that the relation $\mathcal{R}$ is symmetric, that is*

   $$\forall x, y \in \mathbb{R}, \ x\mathcal{R}y \Rightarrow y\mathcal{R}x.$$

   Let $x, y \in \mathbb{R}$

   $$\begin{aligned} x\mathcal{R}y &\Rightarrow x^2 = y^2 \\ &\Rightarrow y^2 = x^2 \\ &\Rightarrow y\mathcal{R}x. \end{aligned}$$

   Then $\mathcal{R}$ is symmetric.

3. *We show that the relation $\mathcal{R}$ is transitive, that is*

   $$\forall x, y, z \in \mathbb{R}, \ (x\mathcal{R}y \text{ and } y\mathcal{R}z) \Rightarrow x\mathcal{R}z.$$

   Let $x, y, z \in \mathbb{R}$, we have

   $$\begin{aligned} x\mathcal{R}y &\Leftrightarrow x^2 = y^2 \\ y\mathcal{R}z &\Leftrightarrow y^2 = z^2 \end{aligned}$$

   then $x^2 = y^2 = z^2 \Rightarrow x^2 = z^2 \Leftrightarrow x\mathcal{R}z$.

   Then $\mathcal{R}$ is transitive.

Equivalence class of an element $x \in \mathbb{R}$

- *For every $x \in \mathbb{R}$, we have*

$$\begin{aligned} \dot{x} = \{y \in X : \quad x\mathcal{R}y\} &= \{y \in \mathbb{R} : \quad x^2 = y^2\} \\ &= \{y \in \mathbb{R} : \quad y = x \text{ or } y = -x\} \\ &= \{y, -y\}. \end{aligned}$$

Then, we can deduce the equivalence class of any element in $\mathbb{R}$. The equivalence class of $0 \in \mathbb{R}$ is $\dot{0} = \{0\}$ and the equivalence class of $1 \in \mathbb{R}$ is $\dot{1} = \{-1, 1\}$.

Remark 3.3

1. For every $x \in X$, the equivalence class $\dot{x}$ is not empty, because the equivalence relation is reflexive.

$$\forall x \in X,\ x\mathcal{R}x, \text{ then } \forall x \in X,\ x \in \dot{x}.$$

2. If $x \in \dot{x}$ then x is a representative of the class $\dot{x}$.

3. $\forall x, y \in X,\ x\mathcal{R}y \Leftrightarrow \dot{x} = \dot{y}$.

Proposition 3.1

The intersection of two distinct equivalence classes by a relation $\mathcal{R}$ is empty

$$\forall x, y \in X, \quad \dot{x} \neq \dot{y} \Rightarrow \dot{x} \cap \dot{y} = \emptyset.$$

Proof. We reason by contradiction, we suppose that $\dot{x} \neq \dot{y}$ and $\dot{x} \cap \dot{y} \neq \emptyset$.
Since $\dot{x} \cap \dot{y} \neq \emptyset$, then there exists an element $z \in X$ such that $z \in \dot{x} \cap \dot{y}$, that is

$$z \in \dot{x} \text{ and } z \in \dot{y}.$$

By the definition of equivalence classes, we have

$$(z \in \dot{x} \Rightarrow z\mathcal{R}x) \text{ and } (z \in \dot{y} \Rightarrow z\mathcal{R}y).$$

Since $\mathcal{R}$ is symmetric and transitive, we have

$$x\mathcal{R}z \text{ and } z\mathcal{R}y \Rightarrow x\mathcal{R}y.$$

But if $x\mathcal{R}y$, then $\dot{x} = \dot{y}$, which is a contradiction with $\dot{x} \neq \dot{y}$.
Therefore, our supposition is false, and we conclude that $\dot{x} \cap \dot{y} = \emptyset$. □

3.2.3 Quotient set

Definition 3.5

Let $\mathcal{R}$ be an equivalence relation on a nonempty set X. The **quotient set** (or **set of equivalence classes**) is denoted by $X_{\mathcal{R}}$ and it is defined as the collection of all equivalence classes of elements of X under the relation $\mathcal{R}$.

$$X/\mathcal{R} = \{\dot{x},\ x \in X\}.$$

Proposition 3.2

Let $\mathcal{R}$ be an equivalence relation on a set X, then the quotient set $X/\mathcal{R}$ is a partition of the set X.

Proof. We prove that the quotient set $X/\mathcal{R} = \{\dot{x} \mid x \in X\}$ is a partition of X.
Recall that the equivalence class of $x \in X$ is $\dot{x} = \{y \in X \mid y\mathcal{R}x\}$.
To prove that $X/\mathcal{R}$ is a partition of X, we must verift these three conditions:

1. every equivalence class is nonempty;
2. the union of all equivalence classes is X;
3. two equivalence classes are either equal or disjoint.

(1) Every equivalence class is nonempty. Let $x \in X$. Since $\mathcal{R}$ is reflexive,

$$x\mathcal{R}x.$$

Then $x \in \dot{x}$, so $\dot{x} \neq \emptyset$.

(2) The union of all equivalence classes is X. Let $x \in X$. Since $x \in \dot{x}$ and $\dot{x} \in X/\mathcal{R}$, we have

$$x \in \bigcup_{C \in X/\mathcal{R}} C.$$

Therefore,

$$X \subseteq \bigcup_{C \in X/\mathcal{R}} C.$$

Conversely, every equivalence class is a subset of X, hence

$$\bigcup_{C \in X/\mathcal{R}} C \subseteq X.$$

Thus,

$$\bigcup_{C \in X/\mathcal{R}} C = X.$$

(3) Two equivalence classes are either equal or disjoint. Let $\dot{x}$ and $\dot{y}$ be two equivalence classes such that

$$\dot{x} \cap \dot{y} \neq \emptyset.$$

Choose $z \in \dot{x} \cap \dot{y}$. Then

$$z\mathcal{R}x \quad \text{and} \quad z\mathcal{R}y.$$

Since $\mathcal{R}$ is symmetric, we have $x\mathcal{R}z$.
By transitivity, from $x\mathcal{R}z$ and $z\mathcal{R}y$, we obtain $x\mathcal{R}y$.

Now let $u \in \dot{x}$. Then $u\mathcal{R}x$. Since $x\mathcal{R}y$, transitivity gives $u\mathcal{R}y$. Hence

$$u \in \dot{y}.$$

Therefore, $\dot{x} \subseteq \dot{y}$.

By the same argument, we show that $\dot{y} \subseteq \dot{x}$.

Thus,

$$\dot{x} = \dot{y}.$$

Therefore, any two equivalence classes are either equal or disjoint.

Conclusion: $X/\mathcal{R}$ is a partition of X. □

Example 3.5.
Let $X = \mathbb{Z}$, we define the following binary relation $\mathcal{R}$:

$$\forall x, y \in \mathbb{Z}, \quad x\mathcal{R}y \Leftrightarrow x - y \text{ is a multiple of } 3.$$

We write

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

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

The equivalence class of an element** $m \in \mathbb{Z}$, **is given by:

$$\begin{aligned} \dot{m} = \{y \in \mathbb{Z},\ y\mathcal{R}m\} &= \{y \in \mathbb{Z},\ \exists k \in \mathbb{Z} : y - m = 3k\} \\ &= \{y \in \mathbb{Z},\ \exists k \in \mathbb{Z} : y = m + 3k\} \\ &= \{m + 3k,\ k \in \mathbb{Z}\}. \end{aligned}$$

Then

$$\begin{aligned} \dot{0} &= \{3k,\ k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ \dot{1} &= \{1 + 3k,\ k \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\ \dot{2} &= \{2 + 3k,\ k \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\} \end{aligned}$$

Therefore, the quotient set $\mathbb{Z}/\mathcal{R} = \{\dot{0}, \dot{1}, \dot{2}\}$.
Remark: *In fact,*

$$\dot{0} = \dot{3} = \dot{6} = \cdots$$
$$\dot{1} = \dot{4} = \dot{7} = \cdots$$
$$\dot{2} = \dot{5} = \dot{8} = \cdots$$

Proposition 3.3

Let n be a positive integer, and consider the equivalence relation $\mathcal{R}$ on $\mathbb{Z}$ defined by

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

Then the quotient set $\mathbb{Z}$ by $\mathcal{R}$ is given by

$$\mathbb{Z}/\mathcal{R} = \{\dot{0}, \dot{1}, \dot{2}, \ldots, \overset{\dot{}}{\overbrace{n-1}}\}.$$

3.3 Order relation

3.3.1 Definitions

Definition 3.6 (Order relation)

A binary relation $\mathcal{R}$ on a set X is called an **order relation** if it is **reflexive, anti-symmetric** and **transitive**.

Definition 3.7 (Total order)

An order relation $\mathcal{R}$ defined on a set X is called **total order relation** if **all its elements are comparable to each other**, that is

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

Example 3.6.
For the usual order relation $\leq$ *on* $\mathbb{R}$*, every pair of real numbers is comparable; that is,*

$$\forall x, y \in \mathbb{R}, \ x \leq y \ \text{or} \ y \leq x.$$

Definition 3.8 (Partial order)

An order relation $\mathcal{R}$ defined on a set X is called **partial order relation** if **the order is not total**, that is

$$\exists x, y \in X,\ x \not\mathcal{R} y \text{ and } y \not\mathcal{R} x.$$

Example 3.7.
Let X be a nonempty set, the binary relation $\mathcal{R}$ on $\mathcal{P}(X)$ given by

$$\forall A, B \in \mathcal{P}(X), \quad A \mathcal{R} B \Leftrightarrow A \subset B$$

The inclusion relation $\mathcal{R}$ is an order relation. In fact:

Reflexive: *For every $A \in \mathcal{P}(X)$, we have $A \subset A$, since a set is always contained in itself. This, $\mathcal{R}$ is reflexive.*

Antisymmetric: *Let A, $B \in \mathcal{P}(X)$ be such that*

$$A \subset B \text{ and } B \subset A.$$

Then all elements of A are in B, and all elements of B are in A. Then $A = B$ Thus, $\mathcal{R}$ is antisymmetric.

Transitive: *Let A, B, $C \in \mathcal{P}(X)$ be such that*

$$A \subset B \text{ and } B \subset C.$$

Then every element of A is in B, and every element of B is in C, thus $A \subset C$. Therefore, $\mathcal{R}$ is transitive.

Let $X = \{1, 2, 3, 4\}$. Take $A = \{2\} \in \mathcal{P}(X)$ and $B = \{3, 4\} \in \mathcal{P}(X)$.
We have that $A \not\subset B$ and $B \not\subset A$. Therefore,

$$\text{there exist } A = \{2\}, B = \{3, 4\} \in \mathcal{P}(X) \text{ such that } A \not\mathcal{R} B \text{ and } B \not\mathcal{R} A.$$

Then the order relation $\mathcal{R}$ on $\mathcal{P}(X)$ is a partial order, and we say that $(\mathcal{P}(X), \subset)$ is a partially ordered set.

Remark 3.4

Let X be a nonempty set and let $\mathcal{R}$ be an order relation defined on X.

1. If the relation $\mathcal{R}$ is total then $(X, \mathcal{R})$ is called a totally ordered set.
2. If the relation $\mathcal{R}$ is partial then $(X, \mathcal{R})$ is called a partially ordered set.

3.3.2 Special elements

Let $(X, \mathcal{R})$ be an ordered set, and let A be a subset of X. We say that

- $M \in X$ **is an upper bound of** A if $\forall x \in A,\ x\mathcal{R}M$.
- $m \in X$ **is a lower bound of** A if $\forall x \in A,\ m\mathcal{R}x$.
- A **is bounded** if it is both **upper-bounded and lower-bounded**.
- a **is the greatest element of** A if $a \in A$ **and** a **is an upper bound of** A.
  The greatest element, when it exists, is denoted by $\max(A)$.
- b **is the least element of** A if $b \in A$ **and** b **is a lower bound of** A.
  The least element, when it exists, is denoted by $\min(A)$.
- **The supremum of** A denoted by $\sup(A)$, is the **least upper-bound** of A.
  $\sup(A)$ when it exists, it is unique.
- **The infimum of** A denoted by $\inf(A)$, is the **greatest lower-bound** of A.
  $\inf(A)$ when it exists, it is unique.
- **Maximal element:** $a \in A$ is called maximal element of A if $\forall x \in A,\ a\mathcal{R}x \Rightarrow a = x$.
  That is, there is no element in the set A greater than a, with respect to the relation $\mathcal{R}$.
- **Minimal element:** $b \in A$ is called minimal element of A if $\forall x \in A,\ x\mathcal{R}b \Rightarrow b = x$.
  That is, there is no element in the set A lower than b, with respect to the relation $\mathcal{R}$.

Example 3.8. *We define in* $\mathbb{N}^*$ *the binary relation* $\mathcal{R}$ *by:*

$$\forall x, y \in \mathbb{N}^*,\ x\mathcal{R}y \Leftrightarrow y \text{ is a multiple of } x.$$

We write

$$\forall x, y \in \mathbb{N}^*,\ x\mathcal{R}y \Leftrightarrow \exists k \in \mathbb{N}^* :\ y = kx.$$

The relation $\mathcal{R}$ *is an order relation. Indeed,*
Let $A = \{1, 3, 7\} \subset \mathbb{N}^*$.

$$\begin{aligned} M \in \mathbb{N}^* \text{ is an upper bound of } A &\Rightarrow \forall x \in A,\ x\mathcal{R}M \\ &\Rightarrow 1\mathcal{R}M, 3\mathcal{R}M \text{ and } 7\mathcal{R}M \\ &\Rightarrow M \text{ is a multiple of } 1, M \text{ is a multiple of } 3 \text{ and } M \text{ is a multiple of } 7 \\ &\Rightarrow M \text{ is the common multiple of } 1, 3 \text{ and } 7 \\ &\Rightarrow M \text{ is multiple of } 21. \end{aligned}$$

Then the set of upper bounds of A is the set $\{21k, \quad k \in \mathbb{N}^*\}$, then the smallest upper bound is $\sup(A) = 21$.

$$\begin{aligned} m \in \mathbb{N}^* \text{ is a lower bound of } A \Rightarrow & \quad \forall x \in A,\ m\mathcal{R}x \\ \Rightarrow & \quad m\mathcal{R}1, m\mathcal{R}3 \text{ and } m\mathcal{R}7 \\ \Rightarrow & \quad 1 \text{ is a multiple of } m, 3 \text{ is a multiple of } m \text{ and } 7 \text{ is a multiple of } m \\ \Rightarrow & \quad m \text{ is the common divisor of } 1 \text{ and } 3 \text{ and } 7 \\ \Rightarrow & \quad m = 1. \end{aligned}$$

Then the set of lower bounds of A is the set $\{1\}$, then the greatest lower bound is $\inf(A) = 1$.

3.4 Exercises

Exercise 3.1. *Determine which of the following relations on the set of real numbers are reflexive and/or symmetric and/or transitive:*

(*a*) *The equality relation* $(=)$.

(*b*) *The inequality relation* $(\neq)$.

(*c*) *The greater than or equal to* $(\geq)$ *or less than or equal to* $(\leq)$ *relation.*

(*d*) *The greater than* $(>)$ *or less than* $(<)$ *relation.*

Exercise 3.2.
Noting $A = \{a_1; a_2; a_3\}$ and $B = \{b_1; b_2; b_3; b_4\}$, the relation $\mathcal{R}$ from the set A to the set B is defined by the set of ordered pairs

$$\{(a1, b1); (a_1, b_2); (a_2, b_3); (a_3, b_3); (a_3, b_4)\}.$$

Represent this relation with an arrow diagram.

Exercise 3.3. *We define the binary relation $\mathcal{R}$ on the set $\mathbb{Z}$ by:*

$$\forall a, b \in \mathbb{Z}, \quad a\mathcal{R}b \Leftrightarrow a - b \text{ is divisible by } 4.$$

1. *Show that $\mathcal{R}$ is an equivalence relation.*
2. *Determine the equivalence class of an element $m \in \mathbb{Z}$.*
3. *Determine the quotient set $\mathbb{Z}/\mathcal{R}$.*

Exercise 3.4. *Let $\mathcal{R}$ be a binary relation defined on the set $\mathbb{R}^2$ by:*

$$\forall (x, y); (x', y') \in \mathbb{R}^2 \quad (x, y)\mathcal{R}(x', y') \Leftrightarrow [x \leq x' \text{ and } y \leq y'].$$

1. *Show that $\mathcal{R}$ is an order relation.*
2. *Are these elements $(1,2)$, $(-1,2)$ and $(3,0)$ comparable. The order is it total or partial?*
3. *Let $D = \{(x,y) \in \mathbb{R}^2 : \quad x^2+y^2 \leq 1\}$ be the closed disk with center $(0,0)$ and radius 1. Determine the following, if they exist:*
   (a) *The set M_D of all upper bounds of D, the greatest element $\max D$, and the supremum $\sup D$.*
   (b) *The set m_D of all lower bounds of D, the least element $\min D$, and the infimum $\inf D$.*
   (c) *The maximal element, the minimal element for the set D ?(Supplementary).*

Exercise 3.5. *(Supplementary)*
We define on the set of relative numbers $\mathbb{Z}$, the following binary relation $\mathcal{R}$ by

$$\forall x, y \in \mathbb{Z}, \quad x\mathcal{R}y \Leftrightarrow \exists a \in \mathbb{N},\ y = x^a.$$

1. *Show that the relation $\mathcal{R}$ is an order relation on $\mathbb{Z}$.*
2. *Show that $\mathcal{R}$ is a partial order on $\mathbb{Z}$ and prove that it is not a total order on $\mathbb{Z}$.*

3.5 Solution of exercises

Solution of exercise 3.1.

The set	*The relation*	*Reflexive*	*Symmetric*	*Transitive*
Any nonempty set	$=$	*Yes*	*Yes*	*Yes*
Any nonempty set	$\neq$	*Yes*	*Yes*	*Yes*
Real numbers	$\geq$ *or* $\leq$	*Yes*	*No*	*Yes*
Real numbers	$>$ *or* $<$	*No*	*No*	*Yes*

Solution of exercise 3.2.

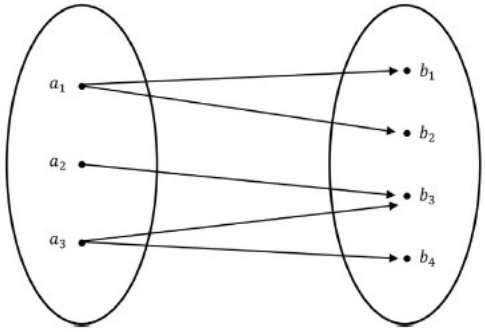


Figure 3.1: Arrow diagram

Solution of exercise 3.3.
We define the binary relation $\mathcal{R}$ on the set $\mathbb{Z}$ by:

$$\forall a, b \in \mathbb{Z}, \quad a\mathcal{R}b \Leftrightarrow a - b \text{ is divisible by } 4.$$

In fact,

$$a - b \text{ is divisible by } 4 \Leftrightarrow \exists k \in \mathbb{Z} : a - b = 4k.$$

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

   - *We show that the relation $\mathcal{R}$ is reflexive, that is $\forall a \in \mathbb{Z}$, $a\mathcal{R}a$.*

   Let $a \in \mathbb{Z}$, we have $a - a = 0$ and 0 is divisible by 4.
   thus,

   $$\forall a \in \mathbb{Z}, \ a\mathcal{R}a.$$

   Therefore, the relation $\mathcal{R}$ is reflexive.

   - *We show that the relation $\mathcal{R}$ is symmetric, that is $\forall a, b \in \mathbb{Z}$, $a\mathcal{R}b \Rightarrow b\mathcal{R}a$.*

   Let $a, b \in \mathbb{Z}$, we have

   $$\begin{aligned} a\mathcal{R}b \Rightarrow & \ a - b \text{ is divisible by } 4 \\ \Rightarrow & \ \exists k \in \mathbb{Z} : a - b = 4k \\ \Rightarrow & \ \exists k \in \mathbb{Z} : b - a = -4k \ (\text{We multiply each side by } -1) \\ \Rightarrow & \ \exists k' = -k \in \mathbb{Z} : b - a = 4k' \\ \Rightarrow & \ b - a \text{ is divisible by } 4. \end{aligned}$$

   Therefore, the relation $\mathcal{R}$ is symmetric.

   - *We show that the relation $\mathcal{R}$ is transitive, that is $\forall a, b, c \in \mathbb{Z}$, $a\mathcal{R}b$ and $b\mathcal{R}c \Rightarrow a\mathcal{R}c$.*

   Let $a, b, c \in \mathbb{Z}$, we have

   $$\begin{aligned} a\mathcal{R}b \text{ and } b\mathcal{R}c \Rightarrow & \ a - b \text{ is divisible by } 4 \text{ and } b - c \text{ is divisible by } 4 \\ \Rightarrow & \begin{cases} \exists k \in \mathbb{Z} : a - b = 4k \ldots (1) \\ \text{and} \\ \exists k' \in \mathbb{Z} : b - c = 4k' \ldots (2) \end{cases} \end{aligned}$$

Adding equations (1) *and* (2)*, we obtain:*

$$a-b+b-c=4k+4k',\ k,k'\in\mathbb{Z}\Rightarrow\ \exists k''=(k+k')\in\mathbb{Z}:\ a-c=4(\underbrace{k+k'}_{k''}).$$

$$\Rightarrow\ a-c \text{ is divisible by } 4$$
$$\Rightarrow\ a\mathcal{R}c.$$

Therefore, the relation $\mathcal{R}$ *is transitive.*
Conclusion: *The binary relation* $\mathcal{R}$ *is reflexive, symmetric and transitive then it is an equivalence relation.*

2. *The equivalence class of an element* $m\in\mathbb{Z}$.
We have

$$\begin{aligned}\dot{m}&=\{a\in\mathbb{Z}:\quad a\mathcal{R}m\}\\&=\{a\in\mathbb{Z}:\quad a-m \text{ is divisible by } 4\}\\&=\{a\in\mathbb{Z},\exists k\in\mathbb{Z}:\quad a-m=4k\}\\&=\{4k+m,\quad k\in\mathbb{Z}\}.\end{aligned}$$

3. *The quotient set* $\mathbb{Z}/\mathcal{R}$.
First, we determine all possible equivalence classes. We have

$$\begin{aligned}\dot{0}&=\{4k,\quad k\in\mathbb{Z}\}=\{\ldots,-8,-4,0,4,8,\ldots\}\\\dot{1}&=\{4k+1,\quad k\in\mathbb{Z}\}=\{\ldots,-7,-3,1,5,9,\ldots\}\\\dot{2}&=\{4k+2,\quad k\in\mathbb{Z}\}=\{\ldots,-6,-2,2,6,10,\ldots\}\\\dot{3}&=\{4k+3,\quad k\in\mathbb{Z}\}=\{\ldots,-5,-1,3,7,11,\ldots\}.\end{aligned}$$

Therefore,

$$\mathbb{Z}/\mathcal{R}=\{\dot{0},\ \dot{1},\ \dot{2},\ \dot{3}\}.$$

Remark: *In fact,*

$$\begin{aligned}\dot{0}&=\dot{4}=\dot{8}\\\dot{1}&=\dot{5}=\dot{9}\\\dot{2}&=\dot{6}=\dot{10}\\\dot{3}&=\dot{7}=\dot{11}.\end{aligned}$$

The equivalence classes repeat because integers that differ by a multiple of 4 belong to the same class, that is, they have the same remainder when divided by 4.

Solution of exercise 3.4.
Let $\mathcal{R}$ *be a binary relation defined on the set* $\mathbb{R}^2$ *by:*

$$\forall(x,y);(x',y')\in\mathbb{R}^2\quad (x,y)\mathcal{R}(x',y')\Leftrightarrow[x\leq x' \text{ and } y\leq y'].$$

1. *We show that the relation* $\mathcal{R}$ *is an order relation.*

   - *We show that the relation* $\mathcal{R}$ *is reflexive, that is*

$$\forall(x,y)\in\mathbb{R}^2,\ (x,y)\mathcal{R}(x,y).$$

Let $(x, y) \in \mathbb{R}^2$, *we have*

$$x \leq x \text{ and } y \leq y \text{ (because the relations } \leq \text{ is reflexive)}$$

thus,

$$\forall (x, y) \in \mathbb{R}^2,\ (x, y)\mathcal{R}(x, y).$$

Therefore, the relation $\mathcal{R}$ *is reflexive.*

- *We show that the relation* $\mathcal{R}$ *is antisymmetric, that is*

$$\forall (x, y); (x', y') \in \mathbb{R}^2,\ [(x, y)\mathcal{R}(x', y') \text{ and } (x', y')\mathcal{R}(x, y)] \Rightarrow (x, y) = (x', y').$$

Let $(x, y); (x', y') \in \mathbb{R}^2$, *we have*

$$\begin{array}{rll} (x, y)\mathcal{R}(x', y') \text{ and } (x', y')\mathcal{R}(x, y) \Rightarrow & [x \leq x' \text{ and } y \leq y'] \text{ and } [x' \leq x \text{ and } y' \leq y] \\ \Rightarrow & [x = x' \text{ and } y = y'] \\ & (\text{ because the relation } \leq \text{ is antisymmetric }) \\ \Rightarrow & (x, y) = (x', y'). \end{array}$$

Therefore, the relation $\mathcal{R}$ *is antisymmetric.*

- *We show that the relation* $\mathcal{R}$ *is transitive, that is*

$$\forall (x, y); (x', y'); (x'', y'') \in \mathbb{R}^2,\ [(x, y)\mathcal{R}(x', y') \text{ and } (x', y')\mathcal{R}(x'', y'')] \Rightarrow (x, y)\mathcal{R}(x'', y'').$$

Let $(x, y); (x', y'); (x'', y'') \in \mathbb{R}^2$, *we have*

$$\begin{array}{rll} (x, y)\mathcal{R}(x', y') \text{ and } (x', y')\mathcal{R}(x'', y'') \Rightarrow & [x \leq x' \text{ and } y \leq y'] \text{ and } [x' \leq x'' \text{ and } y' \leq y''] \\ \Rightarrow & [x \leq x' \leq x'' \text{ and } y \leq y'' \leq y''] \\ \Rightarrow & [x \leq x'' \text{ and } y \leq y''] \\ & (\text{because the relation } \leq \text{ is transitive}) \\ \Rightarrow & (x, y)\mathcal{R}(x'', y''). \end{array}$$

Therefore, the relation $\mathcal{R}$ *is an order relation.*
Conclusion: *Since the relation* $\mathcal{R}$ *is reflexive, symmetric and transitive then it is an equivalence relation.*

2. *Are these elements* $(1, 2)$, $(-1, 2)$ *and* $(3, 0)$ *comparable. The order is it total or partial?*
We have

- $\left.\begin{array}{l} (1, 2)\not\mathcal{R}(-1, 2) \text{ because } 1 \not\leq -1 \text{ and } 2 \leq 2 \\ (-1, 2)\mathcal{R}(1, 2) \text{ because } -1 \leq 1 \text{ and } 2 \leq 2 \end{array}\right\}$ *Hence* $(-1, 2)\mathcal{R}(1, 2)$. *Then,* $(1, 2)$ *and* $(-1, 2)$ ***are comparable.***

- $\left.\begin{array}{l} (1, 2)\not\mathcal{R}(3, 0) \text{ because } 1 \leq 3 \text{ and } 2 \not\leq 0 \\ (3, 0)\not\mathcal{R}(1, 2) \text{ because } 3 \not\leq 1 \text{ and } 0 \leq 2 \end{array}\right\}$ *Then,* $(1, 2)$ *and* $(3, 0)$ ***are not comparable.***

- $\left.\begin{array}{l}(-1,2)\not\mathcal{R}(3,0) \text{ because } -1\leq 3 \text{ and } 2\not\leq 0\\ (3,0)\not\mathcal{R}(-1,2) \text{ because } 3\not\leq -1 \text{ and } 0\leq 2\end{array}\right\}$ *Then,* $(-1,2)and(3,0)$ ***are not comparable.***

The order relation $\mathcal{R}$ *is a partial order (it is not total), because*

$$\exists(1,2)\in\mathbb{R}^2 \text{ and } \exists(3,0)\in\mathbb{R}^2 \text{such that } (1,2)\not\mathcal{R}(3,0) \text{ and } (3,0)\not\mathcal{R}(1,2).$$

3. *Let* $D=\{(x,y)\in\mathbb{R}^2: \quad x^2+y^2\leq 1\}$ *be the closed disk with center* $(0,0)$ *and radius* 1.
We have that:
$$(x,y)\in D\Rightarrow(-1\leq x\leq 1 \text{ and } -1\leq y\leq 1$$

   (a) *The set* M_D *of all upper bounds of* D*, the greatest element* $\max D$*, and the supremum* $\sup D$*.*

   - *The set of upper bounds of* D*:*

$$\begin{array}{rl}(M_1,M_2)\in\mathbb{R}^2 \text{ is an upper bound of } D\Rightarrow & \forall(x,y)\in D,\ (x,y)\mathcal{R}(M_1,M_2)\\ \Rightarrow & x\leq M_1 \text{ and } y\leq M_2\\ \Rightarrow & 1\leq M_1 \text{ and } 1\leq M_2.\end{array}$$

   Therefore, the set of all upper bounds is

$$M_D=\{(M_1,M_2)\in\mathbb{R}^2,\ 1\leq M_1 \text{ and } 1\leq M_2\}.$$

   - *We have* $(1,1)\in M_D$*. It is an upper bound of* D*, but* $(1,1)\notin D$ *since* $1^2+1^2=2\neq 1$*. Therefore, the greatest element* $\max(D)$ *does not exist.*
   - *The supremum of* D *is the least upper bound of* D*; therefore,* $\sup D=(1,1)$*.*

   (b) *The set* M *of all lower bounds of* D*, the least element* $\min D$*, and the infimum* $\inf D$*.*

   - *The set of lower bounds of* D*:*

$$\begin{array}{rl}(m_1,m_2)\in\mathbb{R}^2 \text{ is a lower bound of } D\Rightarrow & \forall(x,y)\in D,\ (m_1,m_2)\mathcal{R}(x,y)\\ \Rightarrow & m_1\leq x \text{ and } m_2\leq y\\ \Rightarrow & m_1\leq -1 \text{ and } m_2\leq -1.\end{array}$$

   Therefore, the set of all lower bounds is

$$m_D=\{(m_1,m_2)\in\mathbb{R}^2,\ m_1\leq -1 \text{ and } m_2\leq -1\}.$$

   - *We have* $(-1,-1)\in m_D$*. It is a lower bound of* D*, but* $(-1,-1)\notin D$ *since* $(-1)^2+(-1)^2=2\neq 1$*. Therefore, the smallest element* $\min(D)$ *does not exist.*
   - *The infimum of* D *is the greatest lower bound of* D*; therefore,* $\inf D=(-1,-1)$*.*

(c) The maximal element, the minimal element for the set D ?(Supplementary)

- $(a_1, a_2) \in D$ ***is the maximal element of*** D *if That is, there is no element* $(x, y) \in D$ *greater than* (a_1, a_2).
  That is, for the unit disk the maximal elements are exactly the boundary points in the first quadrant. ' has the relation $\mathcal{R}$, that can be written in the form
  $$\{(x, y) \in \mathbb{R}^2 : \quad x^2 + y^2 = 1,\ x \geq 0,\ y \geq 0\}.$$
- $(b_1, b_2) \in D$ ***is the maximal element of*** D *if That is, there is no element* $(x, y) \in D$ *smaller than* (b_1, b_2).
  That is, for the unit disk the minimal elements are exactly the boundary points in the third quadrant, that can be written in the form
  $$\{(x, y) \in \mathbb{R}^2 : \quad x^2 + y^2 = 1,\ x \leq 0,\ y \leq 0\}.$$

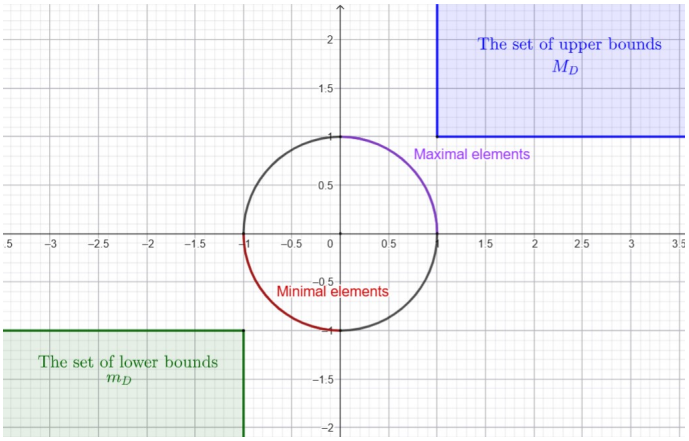


Figure 3.2: Illustration of: The set M_D of all upper bounds of D, The set m_D of all lower bounds of D, The maximal and the minimal elements of the D.

Chapter 4

Algebraic Structures

This chapter introduces important algebraic structures, which are nonempty sets equipped with one or more binary operations satisfying specific properties. The first structure introduced is the group, which play a central role in abstract algebra used to study symmetry and transformations. Then it introduces rings that studies arithmetic with addition and multiplication, the last structure is fields studies arithmetic where division is possible.

4.1 Definitions

4.1.1 Binary operations

Definition 4.1 (Binary operation)

Let X be a nonempty set, the application $(\star)$ given by

$$\begin{aligned} \star : X \times X &\to X \\ (x, y) &\mapsto \star(x, y) = x \star y \end{aligned}$$

is called a **binary operation**, that is

$$\forall x, y \in X, \quad x \star y \in X.$$

In general, we use the notation $x \star y$ instead of $\star(x, y)$

$$\star(x, y) = \left.\begin{array}{l} x \star y \\ x \Delta y \\ x \cdot y \\ xTy \end{array}\right\} \text{are just notations}$$

Example 4.1. *1. The standard operations such as addition and multiplication on* $\mathbb{N}$ *are binary operations*

$$\begin{array}{rl} +:\mathbb{N}\times\mathbb{N} & \to\mathbb{N} \\ (x,y) & \mapsto x+y \end{array} \qquad \begin{array}{rl} .:\mathbb{N}\times\mathbb{N} & \to\mathbb{N} \\ (x,y) & \mapsto x.y \end{array}$$

2. The substraction operation $(-)$ *and division operation* $(\div)$ *are not binary operations on the set* $\mathbb{N}$*.*

4.1.2 Properties

Let $(\star)$ be a binary operation on the set X

(1) The operation $(\star)$ **is commutative on X:** $\forall x, y \in X, \quad x \star y = y \star x.$

(2) The operation $(\star)$ **is associative on X:** $\forall x, y, z \in X, \quad (x \star y) \star z = x \star (y \star z).$

(3) Identity element: The operation $(\star)$ has an identity element denoted by e if

$$\exists e \in X,\ \forall x \in X: \quad x \star e = x \text{ and } e \star x = x.$$

(4) Inverse element: An operation $(\star)$ that has an identity element e, we say that $(\star)$ has an inverse element if

$$\forall x \in X,\ \exists x' \in X: \quad x \star x' = e \text{ and } x' \star x = e.$$

x' is called the inverse element of x, and we say that x is invertible.

Example 4.2.

1. $(\mathbb{R}^*, \cdot)$*, where the operation* $(\cdot)$ *denotes the usual multiplication, we have*

$$e = 1 \text{ is the identity element },$$

and for every $x \in \mathbb{R}^*$*,*

$$x' = \frac{1}{x} \text{ is the inverse element of } x.$$

2. In $(\mathbb{N}, +)$*, where the operation* $(+)$ *is the usual addition, 0 is the only element that has an inverse element.*

3. In $(\mathbb{N}, \cdot)$*, where the operation* $(\cdot)$ *is the usual multiplication, 1 is the only invertible element.*

4. In $(\mathcal{P}(X), \cup)$*, the empty set is the only invertible element, because if*

$$A \cup B = \emptyset, \quad \forall A, B \in \mathcal{P}(X),$$

then $A = \emptyset$ *and* $B = \emptyset$*.*

5. *In* $(\mathcal{P}(X), \cap)$*, the set* X *is the only invertible element, because if*

$$A \cap B = X \quad \forall A, B \in \mathcal{P}(X),$$

then $A = B = X$.

Remark 4.1

The identity element e is always invertible and the inverse of the identity element is the identity element

$$e \star e' = e, \text{ therefore } e' = e.$$

Proposition 4.1

Let $(\star)$ be an intern composition operation on a nonempty set X.

1. The identity element e exists, then it is unique.
2. If the operation $(\star)$ is associative and have identity element, then every invertible element has a unique inverse.
3. If x and y are invertible under the associative operation $(\star)$ on the set X, then $x \star y$ is also invertible, and
$$(x \star y)' = y' \star x'.$$

Proof.

1. We assume that there exists two identity elements e_1 and e_2, then
$$\begin{aligned} &\forall x \in X, \quad x \star e_1 = e_1 \star x = x. \\ &\forall x \in X, \quad x \star e_2 = e_2 \star x = x. \end{aligned}$$
Then
$$e_1 = e_1 \star e_2 \text{ and } e_1 \star e_2 = e_2.$$
2. We assume that there exists two inverse element of x which are x' and x'', then
$$\begin{aligned} x' &= x' \star e \\ &= x' \star (x \star x'') \\ &= (x' \star x) \star x'' \\ &= e \star x'' \\ &= x''. \end{aligned}$$
3. Let x and y be two invertible elements, we denote their inverse element by x' and y', respectively. We have
$$\begin{aligned} (x \star y) \star (y' \star x') &= x \star ((y \star y') \star x') \\ &= x \star (e \star x') \\ &= x \star x' \\ &= e. \end{aligned}$$

Similarly, we can obtain $(y' \star x') \star (x \star y) = e$.
Then $y' \star x' = (x \star y)'$.

□

4.2 Groups

4.2.1 Definitions

Definition 4.2 (Group)

We call a **group** any nonempty set G equipped with a binary operation $(\star)$ that satisfies the following conditions:

1. The operation $(\star)$ is associative.
2. The operation $(\star)$ has a identity element in G, that is:

$$\exists e \in G,\ \forall x \in G,\ x \star e = x \text{ and } e \star x = x.$$

3. Xvery element of G has an inverse in G, that is:

$$\forall x \in G,\ \exists x' \in G,\ x \star x' = e \text{ and } x' \star x = e.$$

We will denote a group by $(G, \star)$, since it is given by both the set G and the operation $(\star)$.

Remark 4.2

We shall always use the symbols e for the identity element in a group and x' for inverse of element an x in the group.

Definition 4.3 (Commutative group)

Let $(G, \star)$ be a group. We say that the group $(G, \star)$ is **commutative** (or **abelian group**), if and only if the operation $(\star)$ is commutative, that is

$$\forall x, y \in G, \quad x \star y = y \star x.$$

Example 4.3.

1. *$(\mathbb{R}^*, \cdot)$ and $(\mathbb{R}, +)$ equipped with the usual multiplication and addition, are commutative groups.*

2. *$(\mathbb{R}, \cdot)$ equipped with the usual multiplication does not form group, although the operation $(\cdot)$ on $\mathbb{R}$ is a binary operation, associative and has an identity element, but the element $0 \in \mathbb{R}$ has not an inverse in $\mathbb{R}$.*

3. *$(\mathbb{Z}^*, \cdot)$ equipped with the usual multiplication does not form group. Indeed, the usual multiplication $(\cdot)$ on $\mathbb{Z}^*$ is a binary operation, associative and has an identity element that is $1 \in \mathbb{Z}^*$. However, not every element has an inverse element in $\mathbb{Z}^*$. For example, the element 2 has not an inverse in $\mathbb{Z}^*$, since there does not exist any $x' \in \mathbb{Z}^*$ such that $2 \cdot x' = 1$ and $x' \cdot 2 = 1$.*

4. *The set $G = \{1, -1\}$ form a commutative group under the usual multiplication $(\cdot)$. It is easy to check the properties. It is clear that for every $x, y \in G$ we have $x \cdot y \in G$ then it is a binary operation, $(\cdot)$ is associative, has identity element $e = 1 \in G$ and each element of G is its own inverse.*

4.2.2 Subgroup

Definition 4.4 (Subgroup)

Let $(G, \star)$ be a group, and let H be a nonempty subset of G. We say that H is a **subgroup** of G if:

1. H is closed with respect to $(\star)$, that is, $\forall x, y \in H, \quad x \star y \in H$.
2. $(H, \star)$ is itself a group; in other words, the restriction of the operation $(\star)$ to $H \times H$ forms a group structure.

Remark 4.3

We use the notation $H \leq G$ to indicate that H is a subgroup of G.

Example 4.4.

1. *$(\mathbb{R}_+^*, \cdot)$ is a subgroup of $(\mathbb{R}^*, \cdot)$. In fact*
   - *For all $x, y \in \mathbb{R}_+^*$, we have $x \cdot y \in \mathbb{R}_+^*$, then the operation $(\cdot)$ is close on $\mathbb{R}_+^*$.*
   - *For all $x, y, z \in \mathbb{R}_+^*$, we have $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, then the operation $(\cdot)$ is associative.*
   - *The identity element is $e = 1 \in \mathbb{R}_+^*$.*
   - *For every $x \in \mathbb{R}_+^*$, the inverse $x' = \frac{1}{x}$ belongs to $\mathbb{R}_+^*$, and $x \cdot x' = x' \cdot x = e$.*

Proposition 4.2 (Subgroup criterion)

Let $(G, \star)$ be a group, and $H \subset G$ such that $H \neq \emptyset$, then

$$H \text{ is a subgroup of } G \Leftrightarrow \forall x, y \in H, \quad x \star y' \in H$$

where y' is the inverse element of y by the operation $(\star)$ in H.

Proof.

"$\Rightarrow$" Suppose that H is a subgroup of G and we show that $\forall x, y \in H,\ x \star y' \in H$.
Let $x, y \in H$. Since H is a subgroup of G, then the inverse element of y exists and $y' \in H$.
Because H is also closed under the operation $(\star)$, it follows that

$$x \star y' \in H.$$

"$\Leftarrow$" Suppose that

$$\forall x, y \in H, \quad x \star y' \in H \ldots\ldots (I)$$

and we want to show that H is a subgroup of G.

1. $H \neq \emptyset$, then $\exists x_0 \in H$ and set $y = x_0$. Then, from (I) we have

   $$x_0 \star x_0' \in H.$$

   But $x_0 \star x_0' = e$. Hence

   $$e \in H.$$

   Then the operation $(\star)$ has an identity element in H.
2. Let $y \in H$. Since $e \in H$, applying (I) with $x = e$ we obtain

   $$e \star y' \in H.$$

   But $e \star y' = y'$, so

   $$y' \in H.$$

   Then the inverse element of $y \in H$ is $y' \in H$.
3. Let $x, y \in H$. From Step 2, we know $y' \in H$.
   Apply (I) to x and y', we obtain

   $$x \star (y')' \in H.$$

   Since $(y')' = y$, we get

   $$x \star y \in H.$$

   Then the operation $(\star)$ is a binary operation.

Conclusion: H contains the identity element, every element in H has an inverse in H, and H is closed with respect to $(\star)$.
Therefore, H is a subgroup of G.

□

Remark 4.4

A group $(G, \star)$ admits at least two subgroups: $(\{e\}, \star)$ and $(G, \star)$, they are called trivial subgroups of the group $(G, \star)$.

Example 4.5.
Let $(\mathbb{Z}, +)$ be an abelian group, and let

$$H = 2\mathbb{Z} = \{2k,\ k \in \mathbb{Z}\}.$$

We show that $(H, +)$ is a subgroup of $(\mathbb{Z}, +)$.
By the subgroup criterion, it suffices to check that for all $x, y \in H$, the element $x + y' \in H$ (where y' is the inverse element of y).
Let $x, y \in H$. Then

$$x = 2k \text{ and } y = 2k', \quad \text{for some } k, k' \in \mathbb{Z}.$$

We have that the inverse element of y in $(\mathbb{Z}, +)$ is

$$y' = -y = -(2k') \in H,$$

since $-(2k') = 2(-k')$ is also a relative number. Therefore,

$$x + y' = 2k + (-2k') = 2(k - k') = 2k'' \in H,$$

where $k'' = k - k'$.
Hence $x + y' \in H$ for all $x, y \in H$, and by the Proposition 4.2.2 $(2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

Remark 4.5

In general, if $n \in \mathbb{N}^*$, then $(n\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

Remark 4.6

Let $(G, \star)$ be a group and let $H \subseteq G$ be a subgroup. By convention, saying that H is a subgroup of G means that H is equipped with the operation $(\star)$ restricted from G.

Properties 4.1

Let $(G, \star)$ be a group and let H_1 and H_2 be two subgroups of G, then

1. $H_1 \cap H_2$ is a subgroup of G.
2. $H_1 \cup H_2$ is not necessarily a subgroup of G.

Proof.

1. We show that $H_1 \cap H_2$ is a subgroup of G.
   Let $x, y \in H_1 \cap H_2$ and we verify that $x \star y' \in H_1 \cap H_2$, with y' denote the inverse element of y.
   We have
   $$x \in H_1 \cap H_2 \Rightarrow x \in H_1 \text{ and } x \in H_2,$$
   and similarly
   $$y \in H_1 \cap H_2 \Rightarrow y \in H_1 \text{ and } y \in H_2$$
   Since H_1 is a subgroup of G, then $x \star y' \in H_1$. Likewise, since H_2 is a subgroup of G, then $x \star y' \in H_2$.
   Therefore, $x \star y' \in H_1 \cap H_2$. By the subgroup criterion, $H_1 \cap H_2$ is a subgroup of G.

2. To show that $H_1 \cup H_2$ is not necessarily a subgroup of G, we give a counter example.
   Let $(\mathbb{Z}, +)$ be an abelian group, and let $(2\mathbb{Z}, +)$ and $(3\mathbb{Z}, +)$ be two subgroups of $(\mathbb{Z}, +)$. Recall that
   $$3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
   $$2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$
   Their union is
   $$2\mathbb{Z} \cup 3\mathbb{Z} = \{\ldots, -6, -4, -3, -2, 0, 2, 3, 4, 6 \ldots\}$$
   We have $3 \in 3\mathbb{Z} \subset (2\mathbb{Z} \cup 3\mathbb{Z})$ and $2 \in 2\mathbb{Z} \subset (2\mathbb{Z} \cup 3\mathbb{Z})$, but
   $$3 + 2 = 5 \notin (2\mathbb{Z} \cup 3\mathbb{Z}).$$
   Hence, the union $(2\mathbb{Z} \cup 3\mathbb{Z})$ is not closed under addition, and therefore it is not a subgroup of $(\mathbb{Z}, +)$.

□

4.2.3 Group homomorphism and group isomorphism

Definition 4.5

Let $(G_1, \star)$ and (G_2, T) be two groups. A mapping

$$\begin{aligned} f : (G_1, \star) &\to (G_2, T) \\ x &\mapsto f(x) \end{aligned}$$

is called a **group homomorphism** (or **group morphism**) if

$$\forall x, y \in G_1, \quad f(x \star y) = f(x) T f(y).$$

Example 4.6.

1.

$$\begin{aligned} f : (\mathbb{R}, +) &\to (\mathbb{R}^*, \cdot) \\ x &\mapsto f(x) = e^x \end{aligned}$$

the mapping f is a group homomorphism.
Indeed, for every $x, y \in \mathbb{R}$ we have

$$f(x + y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y).$$

2.

$$\begin{aligned} g : (\mathbb{Z}, +) &\to (8\mathbb{Z}, +) \\ n &\mapsto g(n) = 8n \end{aligned}$$

the mapping g is a group homomorphism.
Indeed, for every $n, m \in \mathbb{Z}$ we have

$$g(n + m) = 8(n + m) = 8n + 8m = g(n) + g(m).$$

Definition 4.6

A group homomorphism $f : (G_1, \star) \to (G_2, T)$ is called:

1. A **group isomorphism** if the mapping f is bijective.
2. A **group endomorphism** if $G_1 = G_2$ and $* = T$.

4.2.4 The finite group $\mathbb{Z}/n\mathbb{Z}$ $(n = 1, 2, 3, 4, \ldots)$

Let n be an integer such that $n \geq 1$. Let $\mathcal{R}$ be an equivalence relation on $\mathbb{Z}$ defined by

$$\forall x, y \in \mathbb{Z}, \quad x\mathcal{R}y \Leftrightarrow x - y \text{ is a multiple of } n \ (x - y \in \mathbb{Z}).$$

The equivalence class of an element $m \in \mathbb{Z}$, is given by:

$$\begin{aligned} \dot{m} = \{y \in \mathbb{Z},\ y\mathcal{R}m\} &= \{y \in \mathbb{Z},\ \exists k \in \mathbb{Z} : y - m = nk\} \\ &= \{nk + m,\ k \in \mathbb{Z}\}. \\ &= n\mathbb{Z} + m. \end{aligned}$$

The set of all integers modulo n, denoted by $\mathbb{Z}/n\mathbb{Z}$, is defined to be the quotient set:

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

Let $G = \mathbb{Z}/n\mathbb{Z}$, we define the addition operation $(+)$ on G by:

$$\forall x, y \in G, \quad \dot{x} + \dot{y} = \widehat{\dot{x+y}}.$$

Then $(\mathbb{Z}/n\mathbb{Z}, +)$ form a commutative group.
Now, consider the set $G \setminus \{\dot{0}\}$, we define the multiplicative operation $(\cdot)$ on $G \setminus \{\dot{0}\}$ by:

$$\forall x, y \in G \setminus \{\dot{0}\}, \quad \dot{x} \cdot \dot{y} = \widehat{\dot{x \cdot y}}.$$

Then $(G \setminus \{\dot{0}\}, +)$ form a commutative group.

Example 4.7. *Let* $G = \mathbb{Z}/4\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}\} = \{4\mathbb{Z}, 4\mathbb{Z} + 1, 4\mathbb{Z} + 2, 4\mathbb{Z} + 3\}$.
We define the addition operation $(+)$ *on* G *by:*

$$\forall x, y \in G, \quad \dot{x} + \dot{y} = \widehat{\dot{x+y}}.$$

Then $(\mathbb{Z}/4\mathbb{Z}, +)$ *form a commutative group.*

$(+)$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{0}$	$\dot{1}$	$\dot{2}$

Table 4.1: Addition table on $\mathbb{Z}/4\mathbb{Z}$

Now, consider the set $G \setminus \{\dot{0}\}$*, we define the multiplicative operation* $(\cdot)$ *on* $G \setminus \{\dot{0}\}$ *by:*

$$\forall x, y \in G \setminus \{\dot{0}\}, \quad \dot{x} \cdot \dot{y} = \widehat{\dot{x \cdot y}}.$$

Then $(G \setminus \{\dot{0}\}, +)$ *form a commutative group.*

$(\cdot)$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{0}$	$\dot{2}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

Table 4.2: Multiplication table on $\mathbb{Z}/4\mathbb{Z}$

4.2.5 Symmetric group S_3

Proposition 4.3

The set of all bijective mapping from the set $S = \{1, 2, \ldots, n\}$ to itself, endowed with the composition of mappings denote by $\circ$, forms a group denoted by $(S_n, \circ)$.

Proof.

- The composition of two bijective mappings is a bijective.
- Composition of mappings is associative.
- The identity mapping on S is the neutral element.
- Every bijective mapping f has an inverse mapping f^{-1}.

Thus, $(S_n, \circ)$ forms a group. □

Remark 4.7

- Every bijective mapping from $\{1, 2, \ldots, n\}$ to itself is called a permutation.
- For a set S with cardinality n, we use the notation S_n or $A(S)$ to denote the set of all permutations of S.
- The number of bijections from a set of n elements to itself is $n!$, so $Card(S_n) = n!$.
- The group $(S_n, \circ)$ is called symmetric group or permutation group.

Example 4.8. ***(Permutation group*** S_3***)***
Let $S = \{1, 2, 3\}$*. We want to determine all the possible permutations of the set* S*.*
A function from S *to* S *is a permutation only if it is bijective, so each element of* S *must appear exactly once in the list of images. Since the number of ways in which* 3 *elements*

can be connected with 3 elements in a bijective manner is $3! = 6$*, the cardinality of* S_3 *is* $card(S_3) = 3! = 6$.
Then we have the following permutations:

- *Let the mapping* $f : S \to S$ *such that*

$$f(1) = 2,\ f(2) = 3,\ f(3) = 1.$$

and let the mapping $g : S \to S$ *such that*

$$g(1) = 2,\ g(2) = 1,\ g(3) = 3.$$

both are permutations on S.

- *The identity mapping* $Id_S : S \to S$ *such that* $Id_S(x) = x$ *for all* $x \in S$ *is also a permutation.*

- *The mappings* $f \circ g$, $g \circ f$, $f \circ f$ *are also permutations of* S.

Hence, all the possible permutations of the set S *is set* $S_3 = \{I_S,\ f,\ g,\ f \circ g,\ g \circ f,\ f \circ f\}$.

Remark 4.8

We now introduce a notation to represent permutations. Consider the above set S_3.
The mapping f *given above could be written as*

$$f = \left[\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array}\right] \quad \begin{array}{l} \} \ \textit{top row: elements of } S \\ \quad \textit{bottom row: images under } f \end{array}$$

In the first row we write all the members of S *and in the second row we write their respective images.*
Similarly,

$$g = \left[\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 1 & 3 \end{array}\right] \quad \begin{array}{l} \} \ \textit{top row: elements of } S \\ \quad \textit{bottom row: images under } g \end{array}$$

Again since $f \circ g$ *will be given by*

$$\begin{array}{ll} (f \circ g)(1) = & f(g(1)) = f(2) = 3 \\ (f \circ g)(2) = & f(g(2)) = f(1) = 2 \\ (f \circ g)(3) = & f(g(3)) = f(3) = 1 \end{array}$$

Then

$$f \circ g = \left[\begin{array}{ccc} 1 & 2 & 3 \\ 3 & 2 & 1 \end{array}\right].$$

Similarly we write $g \circ f$, $f \circ f$ *and* Id_S.

$$g \circ f = \left[\begin{array}{ccc} 1 & 2 & 3 \\ 1 & 3 & 2 \end{array}\right],\quad f \circ f = \left[\begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \end{array}\right],\quad Id_S = \left[\begin{array}{ccc} 1 & 2 & 3 \\ 1 & 2 & 3 \end{array}\right].$$

- ***We show that*** $(S_3, \circ)$ ***is a group:***

(i) The operation $\circ$ is a binary operation on S_3 $\Leftrightarrow \forall \phi, \psi \in S_3, \quad \phi \circ \psi \in S_3$.

Let $\phi, \psi \in S_3$. Since the composition of two bijective mappings is itself bijective, we have $\phi \circ \psi \in S_3$.

Therefore, the operation $\circ$ is a binary operation on S_3.

(ii) The operation $\circ$ associative $\Leftrightarrow \forall \phi, \psi, \theta \in S_3, \quad \phi \circ (\psi \circ \theta) = (\phi \circ \psi) \circ \theta$.

Let $\phi, \psi, \theta \in S_3$. Composition of mappings is always associative, hence

$$\phi \circ (\psi \circ \theta) = (\phi \circ \psi) \circ \theta$$

Therefore, the operation $\circ$ is associative on S_3.

(iii) The operation $\circ$ has an identity element $\Leftrightarrow \exists e \in S_3, \ \forall \phi \in S_3, \ $ *such that*

$$\phi \circ e = \phi \text{ and } e \circ \phi = \phi.$$

Let $\phi \in S_3$, from

$$\begin{aligned} \phi \circ e = \phi \Rightarrow & \quad e = \phi^{-1} \circ \phi \\ \Rightarrow & \quad e = Id_S. \end{aligned}$$

and

$$\begin{aligned} e \circ \phi = \phi \Rightarrow & \quad e = \phi \circ \phi^{-1} \phi \\ \Rightarrow & \quad e = Id_S. \end{aligned}$$

We conclude that the neutral element is $e = Id_S \in S_3$.

Thus, the operation $\circ$ has a neutral element.

(iv) The operation $\circ$ has an inverse element $\Leftrightarrow \forall \phi \in S_3, \ \exists \phi' \in S_3, \ $ *such that*

$$\phi \circ \phi' = e \text{ and } \phi' \circ \phi = e.$$

Let $\phi \in S_3$. From

$$\phi \circ \phi' = e \Rightarrow \phi \circ \phi' = Id_S \Rightarrow \phi' = \phi^{-1} \circ Id_S \Rightarrow \phi' = \phi^{-1}$$

and

$$\phi' \circ \phi = e \Rightarrow \phi' \circ \phi = Id_S \Rightarrow \phi' = Id_S \circ \phi^{-1} \Rightarrow \phi' = \phi^{-1}.$$

We conclude that every element $\phi \in S_3$ has an inverse element $\phi' = \phi^{-1}$.

Conclusion: *$(S_3, \circ)$ is a group, that is not commutative.*

Remark 4.9

The symmetric group $(S_3, \circ)$ is not a commutative group.

In fact, let $f, g \in S_3$ such that

$$f(1) = 2, \ f(2) = 3, \ f(3) = 1.$$

and

$$g(1) = 2,\ g(2) = 1,\ g(3) = 3.$$

We compute the compositions as follows:

$$\begin{aligned}(f \circ g)(1) &= f(g(1)) = f(2) = 3\\ (f \circ g)(2) &= f(g(2)) = f(1) = 2\\ (f \circ g)(3) &= f(g(3)) = f(3) = 1\end{aligned}$$

Thus,

$$f \circ g = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}.$$

and

$$\begin{aligned}(g \circ f)(1) &= g(f(1)) = g(2) = 1\\ (g \circ f)(2) &= g(f(2)) = g(3) = 3\\ (g \circ f)(3) &= g(f(3)) = g(1) = 2\end{aligned}$$

Hence,

$$g \circ f = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}.$$

Then $f \circ g \neq g \circ f$. Therefore, the composition of mappings is not commutative on S_3.

4.3 Rings

4.3.1 Definitions

Definition 4.7 (Ring)

Let R be a nonempty set equipped with two binary operations $(+)$ and $(\cdot)$ in R. We say that $(R, +, \cdot)$ is a **ring** if and only if the following conditions are verified:

1. $(R, +)$ is an abelian group.
2. The operation $(\cdot)$ is associative in R, that is
$$\forall x, y, z \in R,\ x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$
3. The operation $(\cdot)$ is distributive from the left and from the right with respect to $(+)$, that is
$$\forall x, y, z \in R, \quad x \cdot (y + z) = (x \cdot y) + (x \cdot z) \quad \text{(Left)}$$
$$\forall x, y, z \in R, \quad (y + z) \cdot x = (y \cdot x) + (z \cdot x) \quad \text{(Right)}.$$

Definition 4.8 (Commutative ring)

Let $(R, +, \cdot)$ be a ring, we say that the ring R is commutative if and only if **the operation $(\cdot)$ is commutative** that is

$$\forall x, y \in R, \quad x \cdot y = y \cdot x.$$

Definition 4.9 (Unit element)

Let $(R, +, \cdot)$ be a ring. The **unit element** denoted by 1_R is an element such that

$$\exists 1_R \in R, \ \forall x \in R, \quad x \cdot 1_R = 1_R \cdot x = x.$$

(the unit element is the identity element for the second operation $(\cdot)$).

Remark 4.10

If the unity element exists in a ring, then it is unique.

Remark 4.11

Let $(R, +, \cdot)$ be a ring.

1. In a ring R we denote by 0_R the identity element for the first operation $(+)$.
2. In a ring R we denote by 1_R the unit element for the second operation $(\cdot)$.

Definition 4.10 (Ring with unity)

Let $(R, +, \cdot)$ be a ring. A **ring with unity** is a ring R that **contains a unit element** $1_R \in R$ such that

$$\forall x \in R, \quad x \cdot 1_R = 1_R \cdot x = x.$$

Example 4.9.

1. $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ *with the usual addition* $+$ *and multiplication* $\cdot$ *form rings and these are all commutative rings with unity.*
2. *The set* X *of all even integers with usual addition* $+$ *and multiplication* $\cdot$ *forms a commutative ring without unity.*
3. *The set* F *of all odd integers is not a ring because the sum of two odd integers is an even integers than the first operation addition* $+$ *is not an intern composition operation.*

4. *Let I be an interval of $\mathbb{R}$ and let R denote the set of continuous functions such that $f : I \to \mathbb{R}$, then $(R, +, \cdot)$ forms a structure of a commutative ring with unity by setting . Specifically, for all $f, g \in R$ and all $x \in I$, the operations are defined by*

$$(f + g)(x) = f(x) + g(x), \qquad (f \cdot g)(x) = f(x) \cdot g(x).$$

Where

The identity element is	*The inverse element is*	*The unit element is*
$0_R : I \to \mathbb{R}$	$-f : I \to \mathbb{R}$	$1_R : I \to \mathbb{R}$
$x \longmapsto f(x) = 0$	$x \longmapsto -f(x)$	$x \longmapsto f(x) = 1$

4.3.2 Calculation rules in a ring

Let $(R, +, \cdot)$ be a ring.

1. $\forall x \in R, \quad x \cdot 0_R = 0_R \cdot x = 0_R$.
2. $\forall x, y \in R, \quad x \cdot y' = x' \cdot y = (x \cdot y)'$.
3. $\forall x, y \in R, \quad x' \cdot y' = x \cdot y$.
4. $\forall x, y, z \in R, \quad x \cdot (y + z') = x \cdot y + (x \cdot z)'$.

Proof.

1. Let 0_R be the identity element for the first operation $(+)$, then $0_R + 0_R = 0_R$. We have

$$x \cdot 0_R = x \cdot (0_R + 0_R) = x \cdot 0_R + x \cdot 0_R, \quad ((\cdot) \text{ is distributive from the left })$$

and

$$0_R \cdot x = (0_R + 0_R) \cdot x = 0_R \cdot x + 0_R \cdot x. \quad ((\cdot) \text{ is distributive from the right })$$

Then

$$\begin{aligned} 0_R = (0_R \cdot x) + (0_R \cdot x)' &= (0_R \cdot x + 0_R \cdot x) + (0_R \cdot x)' \\ &= 0_R \cdot x + (0_R \cdot x + (0_R \cdot x)') \\ &= 0_R \cdot x + 0_R \\ &= 0_R \cdot x, \end{aligned}$$

and

$$\begin{aligned} 0_R = (x \cdot 0_R) + (x \cdot 0_R)' &= (x \cdot 0_R + x \cdot 0_R) + (x \cdot 0_R)' \\ &= x \cdot 0_R + (x \cdot 0_R + (x \cdot 0_R)') \\ &= x \cdot 0_R + 0_R \\ &= x \cdot 0_R. \end{aligned}$$

Then $\forall x \in R, \quad x \cdot 0_R = 0_R \cdot x = 0_R$.

2. From (1) we have $\forall x \in R, \quad x \cdot 0_R = 0_R$, we get

$$\begin{aligned} a \cdot (y' + y) = 0_R \Rightarrow & \quad a \cdot y' + a \cdot y = 0_R \\ \Rightarrow & \quad a \cdot y' + a \cdot y + (a \cdot y)' = 0_R + (a \cdot y)' \\ \Rightarrow & \quad a \cdot y' = 0_R + (a \cdot y)' \\ \Rightarrow & \quad a \cdot y' = 0_R. \end{aligned}$$

   Similarly, we can prove that $x' \cdot y = (x \cdot y)'$.

3. Let $x, y \in R$, we have

$$x' \cdot y' = (x \cdot y')' = ((x \cdot y)')' = x \cdot y.$$

4. $\forall x, y \in R$, we have

$$x \cdot (y + z') = x \cdot y + x \cdot z' = x \cdot y + (x \cdot z)'$$

□

Definition 4.11 (zero divisors)

Let $(R, +, \cdot)$ be a ring, if

$$\exists x, y \in R, \text{ such that } x \neq 0_R \text{ and } y \neq 0_R \text{ and } x \cdot y = 0_R.$$

Then x and y are called **zero divisors.**

Example 4.10.

1. *In* $(\mathbb{Z}^*, +, \cdot)$ *there is no zero divisors.*

2. *Let* $(\mathbb{Z}/6\mathbb{Z}, +, \cdot)$ *be a ring, with* $\mathbb{Z}/6\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}\}$.
   The neutral element for the first operation $(+)$ *is* $\dot{0}$*, we have*

$$\dot{2} \cdot \dot{3} = \dot{6} = \dot{0}$$

   but $\dot{2} \neq \dot{0}$ *and* $\dot{3} \neq \dot{0}$*, then* $\dot{2}$ *and* $\dot{3}$ *are zero divisors.*

Remark 4.12

In general in a ring $(R, +, \cdot)$, if $x \cdot y = 0_R$ does not necessarily implies that $x = 0_A$ or $y = 0_R$.

Definition 4.12 (Integral domain)

A commutative ring $(R, +, \cdot)$ is called an **integral domain** if

$$\forall x, y \in R, \quad x \cdot y = 0_R \Rightarrow x = 0_R \text{ or } y = 0_R.$$

In other words a commutative ring R is called an integral domain if R has no zero divisors.

Example 4.11.

1. *$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}$ are integral domains.*
2. *$\mathbb{Z}/4\mathbb{Z}$ is not an integral domain, since $\dot{2} \cdot \dot{2} = \dot{0}$.*
3. *The ring $(\mathcal{C}([0,1], +, \cdot))$ is not an integral domain, because for*

$$f(x) = \begin{cases} 0 & \text{if } 0 \leq x \leq \frac{1}{2} \\ x - \frac{1}{2} & \text{if } \frac{1}{2} < x \leq 1 \end{cases} \quad \text{and } g(x) = \begin{cases} x - \frac{1}{2} & \text{if } 0 \leq x \leq \frac{1}{2} \\ 0 & \text{if } \frac{1}{2} < x \leq 1. \end{cases}$$

We obtain $f(x) \cdot g(x) = 0$ but $f \neq 0$ and $g \neq 0$.

4.3.3 Subring

Definition 4.13 (Subring)

Let $(R, +, \cdot)$ be a ring. A nonempty subset $S \subset R$ is called a **subring** of R if

1. $(S, +)$ is a subgroup of $(R, +)$.
2. The set S is closed under the second operation $(\cdot)$, that is $\forall x, y \in S, \quad x \cdot y \in S$.

Example 4.12.

1. *$(\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{R}, +, \cdot)$.*
2. *$(\mathbb{Q}, +, \cdot)$ is a subrinf of $(\mathbb{R}, +, \cdot)$.*

Remark 4.13

1. If $(R, +, \cdot)$ is a ring, then $(\{0_R\}, +, \cdot)$ and $(R, +, \cdot)$ are always subrings of $(R, +, \cdot)$ called trivial subrings (0_R is the neutral element of $(\{0_R\}, +)$).
2. A subring of an integral domain is an integral domain.

Proposition 4.4 (Subring criterion)

Let $(R,+,\cdot)$ be a ring and let S be a nonempty subset of R. We say that $(S,+,\cdot)$ is a **subring** of R if it verifies the following two conditions:

1. $\forall x,y\in S,\quad x+y'\in S$, with y' is the inverse element of y with respect the first operation $(+)$.
2. $\forall x,y\in S,\quad x+y\in S$ and $x\cdot y\in S$.

Example 4.13. *Let $R=\mathbb{Z}/8\mathbb{Z}=\{\dot{0},\dot{1},\dot{2},\dot{3},\dot{4},\dot{5},\dot{6},\dot{7}\}$ and let S be a subset of R given by*

$$S=\{\dot{\widehat{2r}},\quad r\in\mathbb{Z}\}=\{\dot{0},\dot{2},\dot{4},\dot{6}\}.$$

Then S is a subring of R. In fact, we have

1. *$S\neq\emptyset$.*
2. *Let $x,y\in S$, then $x=\dot{\widehat{2r}}$ and $y=\dot{\widehat{2r'}}$ with $r,r'\in\mathbb{Z}$, then we have,*

$$y'=\dot{\widehat{8-2r'}}=\dot{\widehat{2(4-r')}}=\dot{\widehat{2r''}},\ \text{with } r''=4-r'.$$

Thus

$$x+y'=\dot{\widehat{2r}}+\dot{\widehat{2r''}}=\dot{\widehat{2(r+r'')}}\in S$$

3. *Let $x,y\in S$, then $x=\dot{\widehat{2r}}$ and $y=\dot{\widehat{2r'}}$ with $r,r'\in\mathbb{Z}$, then we have,*

$$x\cdot y=\dot{\widehat{2r}}\cdot\dot{\widehat{2r'}}=(\widehat{2r})\dot{\cdot}(\widehat{2r'})=\dot{\widehat{2(rr')}}\in S.$$

Remark 4.14

1. A subring of a commutative ring is commutative.
2. A subring of a ring with unity is not necessarily a ring with unity.
   For example $(3\mathbb{Z},+,\cdot)$ is a subring of the ring with unity $(\mathbb{Z},+,\cdot)$, but $3\mathbb{Z}$ is not a ring with unity because the unit element of $(\mathbb{Z},+,\cdot)$ is $1_{\mathbb{Z}}=1$ and $1\notin 3\mathbb{Z}$.

4.3.4 Ring homomorphism

Definition 4.14

Let $(R_1, +, \cdot)$ and $(R_2, \star, T)$ be two rings. A mapping

$$\begin{aligned} f : (R_1, +, \cdot) &\to (R_2, \star, T) \\ x &\mapsto f(x) \end{aligned}$$

is called a **ring homomorphism** if

1. $\forall x, y \in R_1, \quad f(x + y) = f(x) \star f(y).$
2. $\forall x, y \in R_1, \quad f(x \cdot y) = f(x) T f(y).$

Example 4.14. *Consider the mapping* $f : (\mathbb{C}, +, \cdot) \to (\mathbb{C}, +, \cdot)$ *such that* $f(a+ib) = a-ib$, *then* f *is a homomorphism. In fact,*

1. *Let* $x = a + ib \in \mathbb{C}$ *and* $y = c + id \in \mathbb{C}$, *then*

$$\begin{aligned} f(x + y) = &\quad f(a + ib + c + id) \\ = &\quad f((a + c) + i(b + d)) \\ = &\quad (a + c) - i(b + d) \\ = &\quad (a - ib) + (c + id) \\ = &\quad f(x) + f(y) \end{aligned}$$

2. *Let* $x = a + ib \in \mathbb{C}$ *and* $y = c + id \in \mathbb{C}$, *then*

$$\begin{aligned} f(x \cdot y) = &\quad f((a + ib) \cdot (c + id)) \\ = &\quad f((ac - bd) + i(bc + ad)) \\ = &\quad (ac - bd) - i(bc + ad) \\ = &\quad (ac - ibc) - bd - iad \\ = &\quad (c - ib)c - id(a - ib) \\ = &\quad (c - ib) \cdot (c - id) \\ = &\quad f(c + ib) \cdot f(c + id) \\ = &\quad f(x) \cdot f(y) \end{aligned}$$

Proposition 4.5

Let $f : (R_1, +, \cdot) \to (R_2, \star, T)$ be a ring homomorphism, then:

1. $f(0_{R_1}) = 0_{R_2}$
2. $f(x') = (f(x))'$
3. $f(x + y') = f(x) \star f(y') = f(x) \star (f(y))'$

Proof.

1. Since $0_{R_1} + 0_{R_1} = 0_{R_1}$, then

$$\begin{aligned} f(0_{R_1} + 0_{R_1}) = f(0_{R_1}) \Rightarrow & \quad f(0_{R_1}) \star f(0_{R_1}) = f(0_{R_1}) \\ \Rightarrow & \quad f(0_{R_1}) \star f(0_{R_1}) = f(0_{R_1}) \star 0_{R_2} \\ \Rightarrow & \quad f(0_{R_1}) = 0_{R_2} \end{aligned}$$

2. Since $x + x' = 0_{R_1}$, then

$$\begin{aligned} f(x + x') = f(0_{R_1}) \Rightarrow & \quad f(x) \star f(x') = f(0_{R_1}) = 0_{R_2} \\ \Rightarrow & \quad f(x) \star (f(x')) = 0_{R_2} \\ \Rightarrow & \quad (f(x))' \star f(x) \star (f(x')) = (f(x))' \star 0_{R_2} \\ \Rightarrow & \quad 0_{R_2} \star (f(x')) = (f(x))' \star 0_{R_2} \\ \Rightarrow & \quad (f(x')) = (f(x))' \end{aligned}$$

3. Let $x, y \in R_1$, then

$$\begin{aligned} f(x + y') = & \quad f(x) \star f(y') \\ = & \quad f(x) \star (f(y))' \end{aligned}$$

□

Definition 4.15

A ring homomorphism $f : (R_1, +, \cdot) \to (R_2, \star, T)$ is called:

1. A **group isomorphism** if the mapping f is bijective.
2. A **group endomorphism** if $R_1 = R_2$ and $(+) = (\star)$ and $(cdot) = (T)$.

4.3.5 Ideals

Definition 4.16 (Ideal)

Let I be a non empty subset I a ring $(R, +, \cdot)$, then:
I is called a right ideal of R if:

1. $\forall x, y \in I$, we have $x + y' \in I$, with y' is the inverse element of y with respect to the operation $(+)$.
2. $\forall x \in I$ and $\forall\, r \in R$, we have $x \cdot r \in I$ (Stability under multiplication by elements of the ring from the right).

I is called a left ideal of R if:

1. $\forall x, y \in I$, we have $x + y' \in I$, with y' is the inverse element of y with respect to the operation $(+)$.
2. $\forall x \in I$ and $\forall\, r \in R$, we have $r \cdot x \in I$ (Stability under multiplication by elements of the ring from the left).

I is called a two sided or both sided ideal, if it is both left and right ideal. In fact, if we say I is an ideal of R, it would mean, I is two sided ideal of R.

Remark 4.15

Let $(R, +, \cdot)$ be a ring. The trivial subrings $(R, +, \cdot)$ and $(\{0_R\}, +, \cdot)$ are always two sided ideal of the R. Any ideal other than these two is called a proper ideal or non trivial ideal.

Example 4.15. *For all $n \in \mathbb{Z}$, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.*

Example 4.16. *Let $(\mathbb{Z}, +, \cdot)$ be the ring of integers, and define $X = \{2k, \quad k \in \mathbb{Z}\}$ as the set of even integers, then X is an ideal of $\mathbb{Z}$.*
In fact, let $x, y \in X$. Then there exist $n, m \in \mathbb{Z}$ such that $x = 2n$ and $y = 2m$. Hence,

$$x + y' = 2n - 2m = 2(n - m) \in X,$$

so X is a subgroup of $(\mathbb{Z}, +)$.

Now let $x \in X$ and $r \in \mathbb{Z}$. Writing $x = 2m$ for some $m \in \mathbb{Z}$, we obtain

$$x \cdot r = (2n)r \in X \text{ and } r \cdot x = r(2n) \in X.$$

Therefore, X is both sided idea of $\mathbb{Z}$.

Example 4.17. *Let* $\mathcal{C}(\mathbb{R},\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} : f \text{ is a mapping }\}$. *Let* $(\mathcal{C}(\mathbb{R},\mathbb{R}),+,\cdot)$ *be a ring, with usual addition and multiplication operations. Fixe any* $x_0 \in \mathbb{R}$ *and define*

$$I = \{f \in \mathcal{C}(\mathbb{R},\mathbb{R}) : \ f(x_0) = 0\}.$$

Then I *is an ideal of* $\mathcal{C}(\mathbb{R},\mathbb{R})$.
In fact, let $f, g \in I$. *Since* $(-g)(x_0) = -g(x_0) = 0$, *we have*

$$(f-g)(x_0) = f(x_0) - g(x_0) = 0,$$

which shows that $f - g \in I$. *Hence,* I *is a subgroup of* $(\mathcal{C}(\mathbb{R},\mathbb{R}),+)$. *Let* $f \in I$ *and* $h \in \mathcal{C}(\mathbb{R},\mathbb{R})$. *Then*

$$(f \cdot h)(x_0) = f(x_0) \cdot g(x_0) = 0,$$

so $fh \in I$. *Similarly,* $hf \in I$. *Therefore,* I *is a both sided ideal of* $\mathcal{C}(\mathbb{R},\mathbb{R})$.

Remark 4.16

A subring may not be an ideal.

Example 4.18. *Let* $(\mathbb{Z},+,\cdot)$ *be a subring of* $(\mathbb{Q},+,\cdot)$.
Take $8 \in \mathbb{Z}$ *and* $\frac{1}{3} \in \mathbb{Q}$. *Then*

$$8 \cdot \frac{1}{3} \notin \mathbb{Z}.$$

Hence, $\mathbb{Z}$ *is not closed under multiplication by arbitrary elements of* $\mathbb{Q}$, *and therefore* $\mathbb{Z}$ *is not an ideal of* $\mathbb{Q}$.

4.4 Fields

4.4.1 Definitions

Definition 4.17 (Field)

Let F be a nonempty set, and let $(+)$ and $(\cdot)$ be two binary operations on F. We say that $(K,+,\cdot)$ is a field if and only if:

1. $(F,+)$ is an abelian group.
2. $(F \setminus \{0_K\},\cdot)$ is a group.
3. The second operation $(\cdot)$ is distributive with respect to the first operation $(+)$ from the right and from the left.

Definition 4.18 (Field)

Let F be a nonempty set, and let $(+)$ and $(\cdot)$ be two binary operations on F. We say that $(K, +, \cdot)$ is a **field** if and only if:

1. $(F, +, \cdot)$ is a ring with unity.
2. Every non-zero element of F is invertible with respect to the second operation $(\cdot)$ that is:

$$\forall x \in F,\ x \neq 0_F,\ \exists x^{-1} \in F, \quad x \cdot x^{-1} = x^{-1} \cdot x = 1_K$$

with

- 0_F is the identity element with respect to the first operation $(+)$;
- 1_F is the unit element;
- x^{-1} is the inverse element of x with respect to the second operation $(\cdot)$.

Example 4.19.

1. *$(\mathbb{Z}, +, \cdot)$ is not a field because the only elements that have multiplicative inverses with respect to the second operation $(\cdot)$ are 1 and -1.*

Remark 4.17

1. A field $(F, +, \cdot)$ contains at least two elements: the identity element 0_F and the unit element 1_F.
2. In a field F, every $x \in F$ with $x \neq 0_F$ is invertible, then x is not a zero divisor, in fact if

$$\forall y \in F, \quad x \cdot y = 0_F$$

then

$$\begin{aligned} x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0_F &\Rightarrow (x^{-1} \cdot x) \cdot y = 0_F \\ &\Rightarrow 1_F \cdot y = 0_F \\ &\Rightarrow y = 0_F. \end{aligned}$$

Therefore, a field is necessarily an integral domain.

4.4.2 The field $\mathbb{Z}/p\mathbb{Z}$, p prime

Theorem 4.1

The ring $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a field, if and only if p is prime.

Proof. Let

$$\mathbb{Z}/p\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \ldots, \widehat{\dot{p-1}}\},$$

and

$$\dot{m} = p\mathbb{Z} + m, \quad m \in \mathbb{Z}.$$

Suppose p is not prime. Then there exist integers x and y with $0 < x, y < p$ such that $p = xy$.
In $\mathbb{Z}/p\mathbb{Z}$, we have

$$\dot{x} \cdot \dot{y} = \dot{p} = \dot{0}.$$

Thus $\mathbb{Z}/p\mathbb{Z}$ contains zero divisors, and by Remark 4.4.1 it cannot be a field.

Conversely, assume p is prime and let x be an integer with $0 < x < p$.
We must find an integer y such that $\dot{x} \cdot \dot{y} = \dot{1}$ in $\mathbb{Z}/p\mathbb{Z}$, that is

$$\dot{x} \cdot \dot{y} = \dot{1} \Leftrightarrow xy = 1 + kp \text{ for some integer } k.$$

Because p is prime, then $\gcd(p, x) = 1$.
By the Bézout's identity, there exist integers r and s such that

$$rp + sx = 1.$$

Rewriting gives $sx = 1 - rp$, so in $\mathbb{Z}/p\mathbb{Z}$ we have

$$\dot{s} \cdot \dot{x} = \dot{1}.$$

Therefore $y = s$ is the multiplicative inverse of x in $\mathbb{Z}/p\mathbb{Z}$.

Hence every nonzero element of $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse when p is prime, and therefore $\mathbb{Z}/p\mathbb{Z}$ is a field. □

4.5 Exercises

Exercise 4.1.
We define on $\mathbb{R}$ the intern composition law $(\star)$ by:

$$\forall x, y \in \mathbb{R} : \quad x \star y = |x| + |y|.$$

1. *Is the law $(\star)$ associative? commutative? has neutral element? Justify your answers.*
2. *Is $(\mathbb{R}, \star)$ a group? Justify your answer.*

Exercise 4.2.
We define the operation $\star$ on the set $\mathbb{R}$ by: $\forall x, y \in \mathbb{R}, \quad x \star y = x + y - 3$.

1. *Show that* $(\mathbb{R}, \star)$ *is a commutative group.*

2. *Let* $H = \{2k+1,\ k \in \mathbb{Z}\}$. *Verify that* $(H, \star)$ *is a subgroup of* $(\mathbb{R}, \star)$.

3. *Let* f *be a mapping from* $(\mathbb{R}, +)$ *to* $(\mathbb{R}, \star)$ *defined by*

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

Here the operation $(+)$ *denotes the usual addition operation on* $\mathbb{R}$.
Determine the value of $\lambda \in \mathbb{R}$ *for which* f *is a group homomorphism.*

Exercise 4.3.
We define on $\mathbb{R}$ *the binary operation* $(\star)$ *by:* $\forall x, y \in \mathbb{R}: \quad x \star y = x + y + \frac{1}{6}$.

1. *Show that* $(\mathbb{R}, \star)$ *is a commutative group.*

2. *Let* $H = \{x = \frac{2n-1}{6},\ n \in \mathbb{Z}\}$. *Show that* H *is a subgroup of* $(\mathbb{R}, \star)$.

3. *Let*

$$\begin{array}{rccc} g : (\mathbb{R}, \star) & \to & (H, +) \\ x & \mapsto & f(x) = 3x + \frac{1}{2} \end{array}$$

Show that g *is a group homomorphism from group* $(\mathbb{R}, \star)$ *to group* $(H, +)$ *(Here the law* $(+)$ *denotes the usual addition operation).*

Exercise 4.4. *We define two binary operations on* $\mathbb{R}$ *by*

$$\forall x, y \in \mathbb{R},\ x \oplus y = x + y - 1 \text{ and } x \otimes y = x + y - xy.$$

1. *Show that* $(\mathbb{R}, \oplus, \otimes)$ *forms a ring.*

2. *Determine whether* $(\mathbb{R}, \oplus, \otimes)$ *is a field.*

4.6 Solution of exercises

Solution of exercise 4.1.
We define on $\mathbb{R}$ *the binary operation* $(\star)$ *by:*

$$\forall x, y \in \mathbb{R}: \quad x \star y = |x| + |y|.$$

1. *Is the law* $(\star)$ *associative? commutative? has neutral element?*

Associativity: *The law* $(\star)$ *is associative* $\Leftrightarrow \forall x, y, z \in \mathbb{R}: \quad x \star (y \star z) = (x \star y) \star z$.

Let $x, y, z \in \mathbb{R}$, *we have*

$$x \star (y \star z) = x \star (|y| + |z|) = \quad |x| + ||y| + |z|| = |x| + |y| + |z| \ldots\ldots (1)$$

$$(x \star y) \star z = (|x| + |y|) \star z = \quad ||x| + |y|| + |z| = |x| + |y| + |z| \ldots\ldots (2)$$

Since $(1) = (2)$, *then the law* $\star$ *is associative.*

Commutativity: *The law* $(\star)$ *is commutative* $\Leftrightarrow \forall x, y \in \mathbb{R}: \quad x \star y = y \star x$.

Let $x, y \in \mathbb{R}$, *we have*

$$x \star y = |x| + |y| = |y| + |x| = y \star x$$

Then the law $\star$ *is commutative.*

Identity element:

The law $(\star)$ *has identity element* $\Leftrightarrow \exists e \in \mathbb{R},\ \forall x \in \mathbb{R},\ x \star e = x$ *and* $e \star x = x$.

Since the law $(\star)$ *is commutative, we look for the existence of an identity element using one equation, for example we use* $x \star e = x$.
Let $x \in \mathbb{R}$ *we have,*

$$x \star e = x \Rightarrow \quad |x| + |e| = x$$

$$\Rightarrow \quad \begin{cases} x + |e| = x, & x \geq 0 \\ -x + |e| = x, & x < 0. \end{cases}$$

$$\Rightarrow \quad \begin{cases} |e| = x - x, & x \geq 0 \\ |e| = 2x, & x < 0. \end{cases}$$

$$\Rightarrow \quad \begin{cases} |e| = 0, & x \geq 0 \\ |e| = 2x, & x < 0. \end{cases}$$

Then the identity element does not exist because if it exists it is unique.

2. $(\mathbb{R}, \star)$ *is not a group because the law* $(\star)$ *has not identity element.*

Solution of exercise 4.2.
We define the operation $\star$ *on the set* $\mathbb{R}$ *by:* $\forall x, y \in \mathbb{R}, \quad x \star y = x + y - 3$.

1. *We show that* $(\mathbb{R}, \star)$ *is a commutative group.*

(a) The operation $\star$ **is a binary operations** $\Leftrightarrow \forall x, y \in \mathbb{R}, \quad x \star y \in \mathbb{R}$.

Let $x, y \in \mathbb{R}$, *we have* $x \star y = x + y - 3 \in \mathbb{R}$ *because the sum and the substraction of real numbers is a real number.*
Then the operation $\star$ *is a binary operation.*

(b) The operation $\star$ is commutative $\Leftrightarrow \forall x, y \in \mathbb{R}, \quad x \star y = y \star x$.
Let $x, y \in \mathbb{R}$, we have

$$\begin{aligned} x \star y &= x + y - 3 \\ &= y + x - 3 \text{ because the usual addition is commutative} \\ &= y \star x \end{aligned}$$

Then $x \star y = y \star x$, the operation $\star$ is commutative.

(c) The operation $\star$ associative $\Leftrightarrow \forall x, y, z \in \mathbb{R}, \quad x \star (y \star z) = (x \star y) \star z$.
Let $x, y, z \in \mathbb{R}$, we have

$$\begin{aligned} x \star (y \star z) &= x \star (y + z - 3) \\ &= x + y + z - 3 - 3 \\ &= x + y + z - 6 \ldots (1) \end{aligned}$$

and

$$\begin{aligned} (x \star y) \star z &= (x + y - 3) \star z \\ &= x + y - 3 + z - 3 \\ &= x + y + y - 6 \ldots (2) \end{aligned}$$

Since $(1) = (2)$, then the operation $\star$ is associative.

(d) The operation $\star$ has an identity element $\Leftrightarrow \exists e \in \mathbb{R}, \ \forall x \in \mathbb{R}, \ x \star e = x$ *and* $e \star x = x$.
Since the operation $\star$ is commutative it is enough to look for the existence of identity element $e \in \mathbb{R}$ using one equation, for example, we use the equation $x \star e = x$.
Let $x \in \mathbb{R}$, we have

$$\begin{aligned} x \star e = x \Rightarrow & \quad x + e - 3 = x \\ \Rightarrow & \quad e = x - x + 3 \\ \Rightarrow & \quad e = 3 \in \mathbb{R}, \end{aligned}$$

then the operation $\star$ has an identity element $e = 3 \in \mathbb{R}$.

(e) The operation $\star$ has an inverse element $\Leftrightarrow \forall x \in \mathbb{R}, \exists x' \in \mathbb{R},$ *such that* $x \star x' = e$ *and* $x' \star x = e$.
Since the operation $\star$ is commutative it is enough to look for the existence of inverse element using $x' \in \mathbb{R}$ using one equation, for example we use $x \star x' = e$.
Let $x \in \mathbb{R}$, we have

$$\begin{aligned} x * x' = e \Rightarrow & \quad x + x' - 3 = 3 \\ \Rightarrow & \quad x' = 3 + 3 - x \\ \Rightarrow & \quad x' = 6 - x \in \mathbb{R} \end{aligned}$$

then every element $x \in \mathbb{R}$ has an inverse element $x' = 6 - x \in \mathbb{R}$.

Conclusion: *$(\mathbb{R}, \star)$ is a commutative group.*

2. Let $H = \{2k+1,\ k \in \mathbb{Z}\}$. Verify that $(H, \star)$ is a subgroup of $(\mathbb{R}, \star)$.

$$(H,\star) \text{ is a subgroup of } (\mathbb{R},\star) \Leftrightarrow \quad [\forall x, y \in H,\ x \star y' \in H.]$$
$$(\text{ with } y' \text{ is the inverse element of } y)$$

Let $x, y \in H$, we have

$$x \in H \Rightarrow x = 2k+1, \quad k \in \mathbb{Z}$$
$$y \in H \Rightarrow y = 2k'+1, \quad k' \in \mathbb{Z}$$

The inverse element of y is

$$\begin{aligned} y' &= 6 - y \\ &= 6 - (2k'+1) \\ &= -2k' + 5 \end{aligned}$$

Hence

$$\begin{aligned} x \star y' &= x + y' - 3 \\ &= (2k+1) + (-2k'+5) - 3 \\ &= 2k - 2k' + 3 \\ &= 2(k - k' + 2) + 1 \\ &= 2k'' + 1, \quad k'' = k - k' + 2 \in \mathbb{Z} \end{aligned}$$

Then $x \star y' = 2k'' + 1$, therefore, $x \star y' \in H$.
Conclusion: *$(H, \star)$ is a subgroup of $(\mathbb{R}, \star)$.*

3. Consider the application

$$\begin{aligned} f : (\mathbb{R}, +) &\to (\mathbb{R}, \star) \\ x &\mapsto f(x) = \lambda - x \end{aligned}$$

Let's determine the value of $\lambda \in \mathbb{R}$ for which f is a group homomorphism.

$$f \text{ is a group homomorphism } \Leftrightarrow \forall x, y \in \mathbb{R},\ f(x+y) = f(x) \star f(y)$$

Let $x, y \in \mathbb{R}$, we have

$$\begin{aligned} f(x+y) &= \lambda - (x+y) \\ &= \lambda - x - y \ldots (3) \end{aligned}$$

and

$$\begin{aligned} f(x) \star f(y) &= (\lambda - x) + (\lambda - y) - 3 \\ &= (2\lambda - 3) - x - y \ldots (4) \end{aligned}$$

the expressions (3) and (4) are equal if and only if $\lambda = 2\lambda - 3$.
Then

$$\begin{aligned} \lambda = 2\lambda - 3 \Rightarrow \quad & \lambda - 2\lambda = -3 \\ \Rightarrow \quad & -\lambda = -3 \\ \Rightarrow \quad & \lambda = 3 \end{aligned}$$

Therefore, f is a group homomorphism for $\lambda = 3$

Solution of exercise 4.3.
We define on $\mathbb{R}$ *the binary operation* $(\star)$ *by:* $\forall x, y \in \mathbb{R}: \quad x \star y = x + y + \frac{1}{6}$.

1. *We show that* $(\mathbb{R}, \star)$ *is a commutative group.*

   (a) The operation $\star$ **is a binary operations** $\Leftrightarrow \forall x, y \in \mathbb{R}, \quad x \star y \in \mathbb{R}$.
   Let $x, y \in \mathbb{R}$, *we have* $x \star y = x + y + \frac{1}{6} \in \mathbb{R}$ *because the sum and the substraction of real numbers is a real number.*
   Then the operation $\star$ *is a binary operation.*

   (b) The operation $\star$ **is commutative** $\Leftrightarrow \forall x, y \in \mathbb{R}, \quad x \star y = y \star x$.
   Let $x, y \in \mathbb{R}$, *we have*

   $$\begin{aligned} x \star y &= x + y + \tfrac{1}{6} \\ &= y + x + \tfrac{1}{6} \text{ because the usual addition is commutative} \\ &= y \star x \end{aligned}$$

   Then $x \star y = y \star x$, *the operation* $\star$ *is commutative.*

   (c) The operation $\star$ **associative** $\Leftrightarrow \forall x, y, z \in \mathbb{R}, \quad x \star (y \star z) = (x \star y) \star z$.
   Let $x, y, z \in \mathbb{R}$, *we have*

   $$\begin{aligned} x \star (y \star z) &= x \star (y + z + \tfrac{1}{6}) \\ &= x + y + z + \tfrac{1}{6} + \tfrac{1}{6} \\ &= x + y + z + \tfrac{1}{3} \ldots (1) \end{aligned}$$

   and

   $$\begin{aligned} (x \star y) \star z &= (x + y + \tfrac{1}{6}) \star z \\ &= x + y + \tfrac{1}{6} + z + \tfrac{1}{6} \\ &= x + y + y + \tfrac{1}{6} \ldots (2) \end{aligned}$$

   Since $(1) = (2)$, *then the operation* $\star$ *is associative.*

   (d) The operation $\star$ **has an identity element** $\Leftrightarrow \exists e \in \mathbb{R}, \ \forall x \in \mathbb{R}, \ x \star e = x$ *and* $e \star x = x$.
   Since the operation $\star$ *is commutative it is enough to look for the existence of identity element* $e \in \mathbb{R}$ *using one equation, for example, we use the equation* $x \star e = x$.
   Let $x \in \mathbb{R}$, *we have*

   $$\begin{aligned} x \star e = x \Rightarrow \quad & x + e + \tfrac{1}{6} = x \\ \Rightarrow \quad & e = x - x - \tfrac{1}{6} \\ \Rightarrow \quad & e = -\tfrac{1}{6} \in \mathbb{R}, \end{aligned}$$

   then the operation $\star$ *has an identity element* $e = -\frac{1}{6} \in \mathbb{R}$.

(e) The operation $\star$ has an inverse element $\Leftrightarrow \forall x \in \mathbb{R}, \exists x' \in \mathbb{R},$ *such that* $x \star x' = e$ *and* $x' \star x = e$.
Since the operation $\star$ *is commutative it is enough to look for the existence of inverse element using* $x' \in \mathbb{R}$ *using one equation, for example we use* $x \star x' = e$.
Let $x \in \mathbb{R}$, *we have*

$$\begin{aligned} x * x' = e \Rightarrow \quad & x + x' + \tfrac{1}{6} = -\tfrac{1}{6} \\ \Rightarrow \quad & x' = -\tfrac{1}{6} - \tfrac{1}{6} - x \\ \\ \Rightarrow \quad & x' = -\tfrac{1}{3} - x \in \mathbb{R} \end{aligned}$$

then every element $x \in \mathbb{R}$ *has an inverse element* $x' = -\frac{1}{3} - x \in \mathbb{R}$.

Conclusion: $(\mathbb{R}, \star)$ *is a commutative group.*

2. *Let* $H = \{x = \frac{2n-1}{6},\ n \in \mathbb{Z}\}$. *We show that* H *is a subgroup of* $(\mathbb{R}, \star)$.

$$(H, \star) \text{ is a subgroup of } (\mathbb{R}, \star) \Leftrightarrow \quad [\forall x, y \in H,\ x \star y' \in H.]$$
$$(\text{ with } y' \text{ is the inverse element of } y)$$

Let $x, y \in H$, *we have*

$$x \in H \Rightarrow x = \frac{2n-1}{6}, \quad n \in \mathbb{Z}$$
$$y \in H \Rightarrow y = \frac{2m-1}{6}, \quad m \in \mathbb{Z}$$

The inverse element of y *is*

$$\begin{aligned} y' = \quad & -\tfrac{1}{3} - y \\ = \quad & -\tfrac{1}{3} - \tfrac{2m-1}{6} \\ = \quad & -\tfrac{2}{6} - \tfrac{2m-1}{6} \\ = \quad & \tfrac{-2-2m+1}{6} \\ = \quad & \tfrac{-2m-1}{6} \end{aligned}$$

Hence

$$\begin{aligned} x \star y' = \quad & x + y' + \tfrac{1}{6} \\ = \quad & (\tfrac{2n-1}{6}) + (\tfrac{-2m-1}{6}) - \tfrac{1}{6} \\ = \quad & \tfrac{2n-2m-1-1-1}{6} \\ = \quad & \tfrac{2(n-m-1)-1}{6} \\ = \quad & \tfrac{2k-1}{6}, \quad k = n - m - 1 \in \mathbb{Z} \end{aligned}$$

Then $x \star y' = \frac{2k-1}{6}$, *therefore,* $x \star y' \in H$.
Conclusion: $(H, \star)$ *is a subgroup of* $(\mathbb{R}, \star)$.

3. *Let*

$$\begin{aligned} g : (\mathbb{R}, \star) &\to (H, +) \\ x &\mapsto f(x) = 3x + \tfrac{1}{2} \end{aligned}$$

We show that g *is a group homomorphism from group* $(\mathbb{R}, \star)$ *to group* $(H, +)$.

$$g \text{ is a group homomorphism } \Leftrightarrow \forall x, y \in \mathbb{R},\ g(x \star y) = g(x) + g(y)$$

Let $x, y \in \mathbb{R}$, *we have*

$$\begin{aligned} g(x \star y) &= 3(x + y + \tfrac{1}{6}) + \tfrac{1}{2} \\ &= 3x + 3y + \tfrac{1}{2} + \tfrac{1}{2} \\ &= 3x + 3y + 1 \ldots (3) \end{aligned}$$

and

$$\begin{aligned} g(x) + g(y) &= (3x + \tfrac{1}{2}) + (3y + \tfrac{1}{2}) \\ &= 3x + 3y + 1 \ldots (4) \end{aligned}$$

the expressions (3) *and* (4) *are equal. Then,* g *is a group homomorphism.*

Solution of exercise 4.4. *We define two binary operations on* $\mathbb{R}$ *by*

$$\forall x, y \in \mathbb{R},\ x \oplus y = x + y - 1 \text{ and } x \otimes y = x + y - xy.$$

1. *We show that* $(\mathbb{R}, \oplus, \otimes)$ *forms a ring.*

$$(\mathbb{R}, \oplus, \otimes) \text{ forms a ring if } \begin{cases} \textbf{(i)} (\mathbb{R}, \oplus) \text{ is a commutative group.} \\ \textbf{(ii)} \text{ The operation } (\oplus) \text{ is associative in } \mathbb{R}, \text{ that is} \\ \forall x, y, z \in \mathbb{R}, \quad x \otimes (y \otimes z) = (x \otimes y) \otimes z. \\ \textbf{(iii)} \text{ The operation } (\otimes) \text{ is distributive from the left and from} \\ \text{the right with respect to } (\oplus), \text{ that is } \forall x, y, z \in \mathbb{R}, \\ x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z) \quad (\textit{Left}) \\ (y \oplus z) \cdot x = (y \otimes x) \oplus (z \otimes x) \quad (\textit{Right}). \end{cases}$$

(i) We verify that $(\mathbb{R}, \oplus)$ **is a commutative group.**

(a) Binary operation: *For every* $x, y \in \mathbb{R}$, *we have* $x \oplus y \in \mathbb{R}$ *and* $x \otimes y \in \mathbb{R}$.
Then the operations $\oplus$ *and* $\otimes$ *are a binary operations.*

(b) $\oplus$ **is commutative:** $\forall x, y \in \mathbb{R}, \quad x \oplus y = y \oplus x$.
Let $x, y \in \mathbb{R}$, *we have*

$$\begin{aligned} x \oplus y &= x + y - 1 \\ &= y + x - 1 \text{ because the usual addition is commutative} \\ &= y \oplus x \end{aligned}$$

Then $x \oplus y = y \oplus x$, *the operation* $\oplus$ *is commutative.*

(c) $\oplus$ **associative:** $\forall x, y, z \in \mathbb{R}, \quad x \oplus (y \oplus z) = (x \oplus y) \oplus z.$
Let $x, y, z \in \mathbb{R}$*, we have*

$$\begin{aligned} x \oplus (y \oplus z) = &\ x \oplus (y + z - 1) \\ = &\ x + y + z - 1 - 1 \\ = &\ x + y + z - 2 \ldots (1) \end{aligned}$$

and

$$\begin{aligned} (x \oplus y) \oplus z = &\ (x + y - 1) \oplus z \\ = &\ x + y - 1 + z - 1 \\ = &\ x + y + y - 2 \ldots (2) \end{aligned}$$

Since $(1) = (2)$*, then the operation* $\oplus$ *is associative.*

(d) $\oplus$ **has an identity element:** $\exists e \in \mathbb{R},\ \forall x \in \mathbb{R},\ x \oplus e = x$ *and* $e \oplus x = x.$
Since the operation $\oplus$ *is commutative it is enough to look for the existence of neutral element* $e \in \mathbb{R}$ *using one equation, for example we use the equation* $x \oplus e = x.$
Let $x \in \mathbb{R}$*, we have*

$$\begin{aligned} x \oplus e = x \Rightarrow &\ x + e - 1 = x \\ \Rightarrow &\ e = x - x + 1 \\ \Rightarrow &\ e = 1 \in \mathbb{R} \end{aligned}$$

then the operation $\oplus$ *has an identity*
element $e = 1 \in \mathbb{R}.$

(e) $\oplus$ **has an inverse element:** $\forall x \in \mathbb{R}, \exists x' \in \mathbb{R},$ *such that*

$$x \oplus x' = e \text{ and } x' \oplus x = e.$$

Since the operation $\oplus$ *is commutative it is enough to look for the existence of inverse element using* $x' \in \mathbb{R}$ *using one equation, for example we use* $x \oplus x' = e.$
Let $x \in \mathbb{R}$*, we have*

$$\begin{aligned} x \oplus x' = e \Rightarrow &\ x + x' - 1 = 1 \\ \Rightarrow &\ x' = 1 + 1 - x \\ \Rightarrow &\ x' = 2 - x \in \mathbb{R} \end{aligned}$$

then every element $x \in \mathbb{R}$ *has an inverse element* $x' = 2 - x \in \mathbb{R}.$

Conclusion: $(\mathbb{R}, \oplus)$ *is a commutative group.*

We verify the conditions on the second binary operation

(ii) The operation $(\otimes)$ is associative in $\mathbb{R}$ $\forall x, y, z \in \mathbb{R},\ x \otimes (y \otimes z) = (x \otimes y) \otimes z$.
Let $x, y, z \in \mathbb{R}$, we have

$$\begin{aligned} x \otimes (y \otimes z) &= x \otimes (y + z - yz) \\ &= x + (y + z - yz) - x(y + z - yz) \\ &= x + y + z - yz - xy + xz + xyz \\ &= x + y + z - yz - xy - xz + xyz \ldots\ldots (3) \end{aligned}$$

and

$$\begin{aligned} (x \otimes y) \otimes z &= (x + y - xy) \otimes z \\ &= (x + y - xy) + z - (x + y - xy)z \\ &= x + y - xy + z - (xz + yz - xyz) \\ &= x + y + z - xy - xz - yz + xyz \\ &= x + y + z - yz - xy - xz + xyz \ldots\ldots (4) \end{aligned}$$

Since $(3) = (4)$, then the operation $\otimes$ is associative.

(iii) The distributivity of the operation $(\otimes)$ with respect to $(\oplus)$: *That is*

$$\forall x, y, z \in \mathbb{R}, \quad x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z) \quad (\textit{Left})$$

$$\forall x, y, z \in \mathbb{R}, \quad (y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x) \quad (\textit{Right}).$$

- **We verify that $(\otimes)$ is distributive from the left with respect to $(\oplus)$**

Let $x, y, z \in \mathbb{R}$, we have

$$\begin{aligned} x \otimes (y \oplus z) &= x \otimes (y + z - 1) \\ &= x + (y + z - 1) - x(y + z - 1) \\ &= x + y + z - 1 - xy - xz + x \\ &= 2x + y + z - xy - xz - 1 \ldots\ldots (5) \end{aligned}$$

and

$$\begin{aligned} (x \otimes y) \oplus (x \otimes z) &= (x + y - xy) \oplus (x + z - xz) \\ &= (x + y - xy) + (x + z - xz) - 1 \\ &= 2x + y + z - xy - xz - 1 \ldots\ldots (6) \end{aligned}$$

Then $(5) = (6)$, then $(\otimes)$ is distributive from the left with respect to $(\oplus)$

- **We verify that $(\otimes)$ is distributive from the right with respect to $(\oplus)$**

Let $x, y, z \in \mathbb{R}$, we have

$$\begin{aligned} (y \oplus z) \otimes x &= (y + z - 1) \otimes x \\ &= (y + z - 1) + x - (y + z - 1)x \\ &= y + z - 1 + x - yx - zx + x \\ &= 2x + y + z + x - yx - zx - 1 \ldots\ldots (7) \end{aligned}$$

and

$$\begin{aligned}(y \otimes x) \oplus (z \otimes x) &= (y + x - yx) \oplus (z + x - zx) \\ &= (y + x - yx) + (z + x - zx) - 1 \\ &= 2x + y + z - yx - zx - 1 \ldots\ldots (8)\end{aligned}$$

Then $(7) = (8)$*, then* $(\otimes)$ *is distributive from the left with respect to* $(\oplus)$

Conclusion: $(\mathbb{R}, \oplus, \otimes)$ *is a ring.*

2. *Determine whether* $(\mathbb{R}, \oplus, \otimes)$ *is a field if and only if*

   (a) $(\mathbb{R}, \oplus, \otimes)$ *is a ring with unity.*

   (b) *Every element of* $\mathbb{R} \setminus \{e\}$ *is invertible for the second operation* $(\otimes)$*, that is:*

$$\forall x \in \mathbb{R},\ x \neq e,\ \exists x^{-1} \in \mathbb{R}, \quad x \otimes x^{-1} = 1_{\mathbb{R}} \text{ and } x^{-1} \otimes x = 1_{\mathbb{R}}$$

with

- e *is the identity element with respect to the first operation* $\oplus$*.*
- $1_{\mathbb{R}}$ *is the unit element with respect to the second operation* $\otimes$*.*
- x^{-1} *is the inverse element of* x *with respect to the second operation* $(\otimes)$*.*

We show that $(\mathbb{R}, \oplus, \otimes)$ **is a ring with unity**

We have that $(\mathbb{R}, \oplus, \otimes)$ *is a ring it remains verify if* $(\mathbb{R}, \oplus, \otimes)$ *has a unit element* $1_{\mathbb{R}} \in \mathbb{R}$*, that is*

$$\exists 1_{\mathbb{R}},\ \forall x \in \mathbb{R}, \quad x \otimes 1_{\mathbb{R}} = x \text{ and } 1_{\mathbb{R}} \otimes x = x.$$

Let $x \in \mathbb{R}$*, we have*

$$\begin{aligned}x \otimes 1_{\mathbb{R}} = x \Rightarrow\ & x + 1_{\mathbb{R}} - x1_{\mathbb{R}} = x \\ \Rightarrow\ & 1_{\mathbb{R}}(1 - x) = x - x \\ \Rightarrow\ & 1_{\mathbb{R}}(1 - x) = 0 \\ \Rightarrow\ & 1_{\mathbb{R}} = 0\end{aligned}$$

Therefore, the unit element is $1_{\mathbb{R}} = 0 \in \mathbb{R}$*.*
Conclusion: *Since* $(\mathbb{R}, \oplus, \otimes)$ *is a ring and has a unit element then* $(\mathbb{R}, \oplus, \otimes)$ *is a ring with unity*

We verify if every element of $x \in \mathbb{R} \setminus \{e\}$ **is invertible for the second operation** $(\otimes)$ *that is:*

$$\forall x \in \mathbb{R},\ x \neq e,\ \exists x^{-1} \in \mathbb{R}, \quad x \otimes x^{-1} = 1_{\mathbb{R}} \text{ and } x^{-1} \otimes x = 1_{\mathbb{R}}$$

Let $x \in \mathbb{R} \setminus \{1\}$*, we have*

$$\begin{aligned}x \otimes x^{-1} = 1_{\mathbb{R}} \Rightarrow\ & x + x^{-1} - xx^{-1} = 0 \\ \Rightarrow\ & x + x^{-1}(1 - x) = 0 \\ \Rightarrow\ & x^{-1}(1 - x) = -x \\ \Rightarrow\ & x^{-1} = \tfrac{-x}{(1-x)} \text{is well defined because } x \neq 1.\end{aligned}$$

Therefore, every element different from the identity element e is invertible with respect to the second operation, that is

$$\forall x \in \mathbb{R},\ x \neq 1,\ \exists x^{-1} = \frac{-x}{(1-x)} \in \mathbb{R}, \quad x \otimes x^{-1} = 0 \text{ and } x^{-1} \otimes x = 0.$$

Conclusion: $(\mathbb{R}, \oplus, \otimes)$ *is a field.*

Chapter 5

Polynomials rings

Let $(\mathbb{F}, +, \cdot)$ be a field, where $\mathbb{F}$ denotes either $\mathbb{R}$, $\mathbb{Q}$, or $\mathbb{C}$. In what follows, we denote by $0_{\mathbb{F}}$ the identity element (additive identity) of $(\mathbb{F}, +, \cdot)$ and by $1_{\mathbb{F}}$ the unit element (multiplicative identity) of $(\mathbb{F}, +, \cdot)$.

Definition 5.1

Let $\mathbb{F}$ be a field. A polynomial P over $\mathbb{F}$ with the variable x is a of the form

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

where $a_0, a_1, a_2, \ldots, a_n \in \mathbb{F}$ and $n \in \mathbb{N}$.

- The elements $a_0, a_1, a_2, \ldots, a_n$ are called coefficients of the polynomial P.
- x is called the variable or the indeterminate.
- We denote by $\mathbb{F}[x]$ the set of the polynomials in one variable x with coefficients in $\mathbb{F}$.

$$\mathbb{F}[x] = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \quad a_0, a_1, a_2, \ldots, a_n \in \mathbb{F},\ n \geq 0\}.$$

Definition 5.2

Let P be a polynomial of $\mathbb{F}[x]$, such that

$$P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n.$$

- The degree of a polynomial P is the largest integer $n \in \mathbb{N}$ such that $a_n \neq 0$, denoted by $\deg(P) = n$ and we say that a_n is the leading coefficient and a_nx^n is the leading term.
$$\deg(P) = \max\{n \in \mathbb{N} : \quad a_n \neq 0\}.$$
- We say that degree of P is zero if $a_0 \neq 0$ and $a_i = 0$ for all $i \geq 1$. In this case P is called a constant polynomial.
- Clearly, $\deg(P(x)) = \deg(-P(x))$.
- If all the coefficients a_i for $i = \overline{1,n}$ are equal to zero, that is $P(x) = 0$, then P is called the zero polynomial and we denote it by $0_{\mathbb{F}[x]}$. For convenience, we say that $\deg(0_{\mathbb{F}[x]}) = -\infty$.
- The valuation of a polynomial P is the smallest integer $n \in \mathbb{N}$ such that $a_n \neq 0$, denoted by $val(P)$.
$$val(P) = \min\{n \in \mathbb{N} : \quad a_n \neq 0\}.$$
- A monic polynomial is a polynomial whose leading coefficient is 1.
- A polynomial P is called monomial if $val(P) = \deg(P)$. In other terms, a monomial is a polynomial that has only one non-zero term $P(x) = a_kx^k$.

Example 5.1.

1. $P(x) = x^3 + 4x + 5$, *the polynomial* P *is monic, because its leading term is* x^3 *and its coefficient is* 1.
2. $Q(x) = 2x^4 + 4x + 5$, *the polynomial* Q *is not monic, because its leading term is* $2x^4$ *and its coefficient is* 2 *which is different from* 1.

Example 5.2.

1. *For* $P(x) = 1 + (5 + i)x^4$ *we have* $\deg(P) = 4$ *and* $val(P) = 0$.
2. *For* $Q(x) = 8x^2 + 2x^3 + x^4$ *we have* $\deg(P) = 4$ *and* $val(P) = 2$.

Remark 5.1

- For every non zero polynomial $P \in \mathbb{F}[x]$, we have $val(P) \leq \deg(P)$.
- A polynomial is a finite sum of monomials.

5.1 Operations on polynomials

Let P and Q be two polynomials of $P \in \mathbb{F}[x]$, such that

$$P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad a_i \in \mathbb{F},\ n \in \mathbb{N},$$

$$Q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m, \quad b_i \in \mathbb{F},\ m \in \mathbb{N}.$$

1. We say that $P(x) = Q(x)$ if and only if $n = m$ and $a_i = b_i$ for all i.
2. The *sum* of P and Q, denoted by $P + Q$, is the polynomial in $\mathbb{F}[x]$ defined by

$$P(x) + Q(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots$$

Moreover, the following properties hold:

- $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$.
- $Val(P + Q) \geq \min(val(P), val(Q))$.

Example 5.3.
Let

$$P(x) = 1 - 2x + 3x^2 + x^3 \text{ and } Q(x) = 2x + 3x^2 - x^3.$$

Then

$$\deg(P) = 3,\ val(P) = 0 \quad \deg(Q) = 3,\ val(Q) = 1.$$

We compute

$$\begin{aligned} P(x) + Q(x) &= (1 - 2x + 3x^2 + x^3) + (2x + 3x^2 - x^3) \\ &= 1 + (-2 + 2)x + (3 + 3)x^2 + (1 - 1)x^3 \\ &= 1 + 6x^2. \end{aligned}$$

Therefore,

$$\deg(P + Q) = 2 \leq \max(\deg(P), \deg(Q)) = 3,$$

and

$$val(P + Q) = 0 \geq \min(val(P), val(Q)) = 0.$$

3. Let $P, Q \in \mathbb{F}[x]$ be two polynomials, written as

$$P(x) = \sum_{k=0}^{n} a_k x^k \text{ and } Q(x) = \sum_{k=0}^{m} b_k x^k.$$

The product of P and Q, denoted by $P \cdot Q$ is a polynomial in $\mathbb{F}[x]$ given by

$$\begin{aligned} P(x) \cdot Q(x) = & \sum_{i=0}^{n+m} c_k i^i \\ = & c_0 + c_1 x + c_2 x^2 + \cdots + c_{n+m} x^{n+m} \end{aligned}$$

where the coefficients c_i are defined by the convention formula

$$c_i = \sum_{k=0}^{i} a_k b_{i-k} \text{ for all } i \in \{0, 1, n+m\}.$$

Thus, each coefficient c_i is obtained by summing all products $a_k b_{i-k}$ whose indices add up to i.
Moreover, the following properties hold:

- $\deg(P \cdot Q) = \deg(P) + \deg(Q)$.
- $Val(P \cdot Q) = Val(P) + Val(Q)$.

Example 5.4.
Let

$$P(x) = 1 + 3x + 2x^2 \text{ and } Q(x) = 1 + 2x.$$

Then

$$P(x) \cdot Q(x) = c_0 + c_1 x + c_2 x^2 + c_3 x^3$$

with the coefficients are given by

$$\begin{aligned} c_0 =& a_0 b_0 = (1)(1) = 1 \\ c_1 =& a_0 b_1 + a_1 b_0 = (1)(2) + (3)(1) = 5 \\ c_2 =& a_0 b_2 + a_1 b_1 + a_2 b_0 = (1)(0) + (3)(2) + (2)(1) = 8 \\ c_3 =& a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = (1)(0) + (3)(0) + (2)(2) + (0)(1) = 4 \end{aligned}$$

Therefore,

$$P(x) \cdot Q(x) = 1 + 5x + 8x^2 + 4x^3.$$

- $\deg(P \cdot Q) = \deg(P) + \deg(Q) = 2 + 1 = 3.$
- $val(P \cdot Q) = val(P) + val(Q) = 0 + 0 = 0.$

5.2 Construction of the ring of polynomials

Proposition 5.1

Let $(\mathbb{F}, +, \cdot)$ be a field, Then $(\mathbb{F}[x], +, \cdot)$ with the usual addition and multiplication operations forms a ring structure.

Proof.
We show that $(\mathbb{F}[x], +, \cdot)$ forms a ring.

$(\mathbb{F}[x], +, \cdot)$ forms a ring if
$$\begin{cases} \textbf{(i)}(\mathbb{F}[x], +) \text{ is a commutative group.} \\ \textbf{(ii)} \text{ The law } (+) \text{ is associative in } \mathbb{F}[x], \text{ that is} \\ \forall P, Q, R \in \mathbb{F}[x], \quad P \cdot (Q \cdot R) = (P \cdot Q) \cdot R. \\ \textbf{(iii)} \text{ The law } (\cdot) \text{ is distributive from the left and from the right} \\ \text{ with respect to } (+), \text{ that is } \forall P, Q, R \in \mathbb{F}[x], \\ P \cdot (Q + R) = (P \cdot Q) + (P \cdot R) \quad \text{(Left)} \\ \text{ and} \\ (Q + R) \cdot P = (Q \cdot P) + (R \cdot P) \quad \text{(Right)}. \end{cases}$$

(**i**) We verify that $(\mathbb{F}[x], +)$ is a commutative group.

(a) Intern composition law: For every $P, Q \in \mathbb{F}[x]$, we have

$$P + Q \in \mathbb{F}[x] \text{ and } P \cdot Q \in \mathbb{F}[x].$$

Then, the laws $(+)$ and $(\cdot)$ are an intern composition laws.

(b) The law $(+)$ is commutative: Let $P, Q \in \mathbb{F}[x]$, we have

$$P + Q = Q + P.$$

Then, the law $(+)$ is commutative.

(c) The law $(+)$ is associative: Let $P, Q, R \in \mathbb{F}[x]$, we have

$$P + (Q + R) = (P + Q) + R.$$

Then, the law $(+)$ is associative.

(d) The law $(+)$ has an identity element: Let $P \in \mathbb{F}[x]$, we have

$$P + 0_{\mathbb{F}[x]} = P \text{ and } 0_{\mathbb{F}[x]} + P = P.$$

Then, the law $(+)$ has a neutral element which is $0_{\mathbb{F}[x]} \in \mathbb{F}[x]$.

(e) The law $(+)$ has an inverse element:
Let $P \in \mathbb{F}[x]$ with $P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, then it has an inverse element $(-P) \in \mathbb{F}[x]$ with $-P(x) = -a_0 - a_1 x - a_2 x^2 - \cdots - a_n x^n$, such that

$$P + (-P) = 0_{\mathbb{F}[x]} \text{ and } (-P) + P = 0_{\mathbb{F}[x]}.$$

Conclusion: $(\mathbb{F}[x], +)$ is a commutative group.

(**ii**) **The law** $(\cdot)$ **is associative** Let $P, Q, R \in \mathbb{F}[x]$, we have

$$P \cdot (Q \cdot R) = (P \cdot Q) \cdot R.$$

Then the law $(\cdot)$ is associative.

(**iii**) **The law** $(\cdot)$ **is distributive from the left and from the right with respect to** $(+)$**:**

- **We verify that** $(\cdot)$ **is distributive from the left with respect to** $(+)$
  Let $P, Q, R \in \mathbb{F}[x]$, we have

  $$x \cdot (y + z) = (x \cdot y) + (x \cdot z).$$

  Then $(\cdot)$ is distributive from the left with respect to $(+)$
- **We verify that** $(\cdot)$ **is distributive from the right with respect to** $(+)$

  Let $P, Q, R \in \mathbb{F}[x]$, we have

  $$(Q + R) \cdot P = (Q \cdot P) + (R \cdot P).$$

  Then $(\cdot)$ is distributive from the left with respect to $(+)$

Conclusion: $(\mathbb{F}[x], +, \cdot)$ is a ring.

□

5.3 Polynomial arithmetic

In this section, we examine divisibility and Euclidean division of polynomials, define the GCD and LCM of two polynomials, and introduce coprime polynomials. We conclude with factorization into irreducible factors, which parallels prime factorization for integers.

Definition 5.3 (Divisibility)

Let A and B be two polynomials on $\mathbb{F}[x]$ with $A \neq 0_{\mathbb{F}[x]}$, we say that A divides B (or A is a divisor of B, or B is a factor of A) and we write $A|B$ if

$$\exists Q \in \mathbb{F}[x] \text{ such that } B = QA.$$

Example 5.5.

1. *Every polynomial divides the zero polynomial.*
2. *The only multiple of a zero polynomial is the zero polynomial.*
3. *Let $P \in \mathbb{F}[x]$ be a nonzero polynomial and $\lambda \in \mathbb{F}$, with $\lambda \neq 0$, then λP and λ are divisors of P.*
4. *$(x+1)|(x^2+3x+2)$ in $\mathbb{R}[x]$, because $x^2+3x+2=(x+2)(x+1)$. In fact,*

$$\begin{array}{r|l} x^2+3x+2 & x+1 \\ -(x^2+x) & x+2 \\ \hline 2x+2 & \\ -(2x+2) & \\ \hline 0 & \end{array}$$

   Since the remainder is 0, it follows that $x+1$ divides x^2+3x+2 in $\mathbb{R}[x]$.

5. *$(x^2+x+1)|(x^5+x+1)$ in $\mathbb{R}[x]$, because $x^5+x+1=(x^3-x^2+1)(x^2+x+1)$.*

$$\begin{array}{r|l} x^5+x+1 & x^2+x+1 \\ -(x^5+x^4+x^3) & x^3-x^2+1 \\ \hline -x^4-x^3+x+1 & \\ -(-x^4-x^3-x^2) & \\ \hline x^2+x+1 & \\ -(x^2+x+1) & \\ \hline 0 & \end{array}$$

   Since the remainder is 0, it follows that x^2+x+1 divides x^5+x+1 in $\mathbb{R}[x]$.

6. *For every $n \in \mathbb{N}$, the polynomial $x-1$ divides X^n-1. Indeed, we have the factorization*

$$x^n-1=(x-1)(x^{n-1}+x^{n-2}+\cdots+x+1).$$

   For example,

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

   and

$$x^4-1=(x-1)(x^3+x^2+x+1).$$

   Thus, $x-1$ is a divisor of x^n-1 for every positive integer n.

Remark 5.2

Let A and B be two polynomials in $\mathbb{F}[x]$, we have

1. If B is not the zero polynomial and $A|B$, then $\exists! Q \in \mathbb{F}[x]$ such that $B=QA$.
2. If A and B are two non zero polynomials and $A|B$ then $\deg(A) \leq \deg(B)$.

Proposition 5.2

Let A, B, C be three non zero polynomials in $\mathbb{F}[x]$.

1. If $A|B$ and $B|A$, then $A|C$.
2. If $A|B$ and $B|A$, then $\exists \lambda \in \mathbb{F}$ with $\lambda \neq 0_{\mathbb{F}}$ such that $B = \lambda A$.
3. If $A|B$ and $A|C$, then $A|(A+B)$.
4. If $A|B$ and $C|D$, then $AC|BD$.
5. $A^k|B^k$, for all $k \in \mathbb{F}$.

Proof.
We prove only the second statement, as the remaining propositions follow immediately.
Let $A, B \in \mathbb{F}[x]$ be two non zero polynomials such that $A|B$ and $B|A$.
Since $A|B$ and A is a non zero polynomial, then there exists a polynomial $Q \in \mathbb{F}[x]$ such that $B = QA$. Taking degrees, we obtain

$$\deg(B) = \deg(Q) + \deg(A)$$

On the other hand, since $B|A$, we have $\deg(B) \leq \deg(A)$. It follow that $\deg(Q) = 0$, and hence Q is the constant polynomial. □

Theorem 5.1 (Euclidean division)

Let $A, B \in \mathbb{F}[x]$ with $B \neq 0_{\mathbb{F}[x]}$. Then there exist unique polynomials Q and R such that

$$A = B \cdot Q + R \text{ with } \deg(R) < \deg(B) \ldots\ldots\ldots (*)$$

This decomposition (expression $(*)$) is called the Euclidean division (or division algorithm) of A by B.
The polynomial Q is called the quotien,t and R is called the remainder.

Proof.

- If $A = 0_{\mathbb{F}[x]}$, it is enough to take $Q = 0_{\mathbb{F}[x]}$ and $R = 0_{\mathbb{F}[x]}$.
- If B is the constant polynomial equals to b, it is enough to take $Q = \dfrac{A}{b}$ and $R = 0_{\mathbb{F}[x]}$.
- If $A \neq 0_{\mathbb{F}[x]}$ and B is a non constant polynomial. We show the existence of polynomials Q and R by induction on the degree of A.
  - If $\deg(A) < \deg(B)$, then $A = 0_{\mathbb{F}[x]}B + A$.

– If $\deg(A) \geq \deg(B)$, we use the proof by induction.
We set $n = \deg(A)$ and $m = \deg(B)$ and we denote by a the leading coefficient of A and b is the leading coefficient of B.
We write $A = ax^n + U$ and $B = bx^m + C$, then $U = 0$ or $\deg(U) < n$ similarly $C = 0$ or $\deg(C) < m$.
From induction hypotheses, there exists polynomials Q_1 and R_1, such that

$$U = BQ_1 + R_1 \text{ and } R_1 = 0 \text{ or } \deg(R_1) < m.$$

On the other hand, we have

$$ax^n = \frac{a}{b}x^{n-m}(bx^m) = \frac{a}{b}x^{n-m}(B - C) = \frac{a}{b}x^{n-m}B - \frac{a}{b}x^{n-m}C.$$

Since the degree of a product polynomials is the sum of degrees, we deduce that

$$-\frac{a}{b}x^{n-m}C = 0 \text{ or } \deg(-\frac{a}{b}x^{n-m}C) = n - m + \deg(C) < n.$$

Using induction hypotheses, there exists polynomials Q_2 and R_2 such that

$$-\frac{a}{b}x^{n-m}C = BQ_2 + R_2 \text{ and } R_2 = 0 \text{or } \deg(R_2) < m.$$

Finally we obtain

$$A = ax^n + U = \frac{a}{b}x^{n-m}B + BQ_2 + R_2 + BQ_1 + R_1 = B(\frac{a}{b}x^{n-m} + Q_2 + Q_1) + (R_2 + R_1).$$

If $R_1 \neq 0$ and $R_2 \neq 0$, then

$$R_1 + R_2 = 0 \text{ or } \deg(R_1 + R_2) \leq max(\deg(R_1), \deg(R_2)) < m.$$

In all cases, we have that

$$R_1 + R_2 = 0 \text{ or } \deg(R_1 + R_2) < m.$$

Which ends the proof of the existence.

Now, we show the unicity. Let Q_1, R_1, Q_2, R_2 be polynomials in $\mathbb{F}[x]$ such that:

$$A = BQ_1 + R_1 \text{ and } A = BQ_2 + R_2, \text{ xhith } \deg(R_1) < \deg(B) \text{ and } \deg(R_2) < \deg(B) \ldots (1)$$

The we have

$$R_1 - R_2 = B(Q_2 - Q_1) \text{ or } \deg(R_1 - R_2) < \deg(B)$$

If $Q_1 \neq Q_2$ then $\deg(Q_2 - Q_1) \geq 0$ so

$$\deg(R_1 - R_2) = \deg(B(Q_2 - Q_1)) = \deg(B) + \deg(Q_2 - Q_1) \geq \deg(B) \ldots (2)$$

from (1) and (2) we obtain

$$\deg(B) > \deg(R_1 - R_2) \geq \deg(B)$$

hence $Q_1 = Q_2$ and so $R_1 = R_2$. □

Remark 5.3

In the Euclidian division of a polynomial A by a polynomial B, if the remainder R is equal to zero, then we say that B divides A, and we write $B|A$.

Example 5.6. *Determine the quotient and the remainder in each Euclidean division*

1. *let* $A(x) = x^3 + 2x - 1$ *and* $B(x) = x^2 - 1$.
   We perform the Euclidean division of $A(x)$ *by* $B(x)$*:*

$$\begin{array}{r|l} x^3 + 2x - 1 & x^2 - 1 \\ \hline -(x^3 - x) & x \\ \hline 3x - 1 & \end{array}$$

   Since $\deg(3x-1) = 1 < \deg(x^2-1) = 2$*, the division stops here. Hence,*

$$A(x) = xB(x) + (3x - 1).$$

   Therefore, the quotient is The quotient is $Q(x) = x$ *and the remainder is* $R(x) = 3x - 1$.

2. $A(x) = x^5 - 2x^4 + x^2 - 1$ *and* $B(x) = 2x^3 + x - 1$.
   We perform the Euclidean division of $A(x)$ *by* $B(x)$*:*

$$\begin{array}{r|l} x^5 - 2x^4 + x^2 - 1 & 2x^3 + x - 1 \\ \hline -(x^5 + \frac{1}{2}x^3 - \frac{1}{2}x^2) & \frac{1}{2}x^2 - \frac{1}{2}x - \frac{1}{4} \\ \hline -x^4 - \frac{1}{2}x^3 + \frac{3}{2}x^2 - 1 & \\ -(x^4 - \frac{1}{2}x^2 + \frac{1}{2}x) & \\ \hline -\frac{1}{2}x^3 + 2x^2 - \frac{1}{2}x - 1 & \\ -(-\frac{1}{2}x^3 - \frac{1}{4}x + \frac{1}{4}) & \\ \hline 2x^2 - \frac{1}{4}x - \frac{5}{4} & \end{array}$$

   Since $\deg(2x^2 - \frac{1}{4}x - \frac{5}{4}) = 2 < \deg(2x^3 + x - 1) = 3$*, the division stops here. Hence,*

$$A(x) = B(x)(\frac{1}{2}x^2 - \frac{1}{2}x - \frac{1}{4}) + 2x^2 - \frac{1}{4}x - \frac{5}{4}.$$

   Therefore, the quotient is $Q(x) = \frac{1}{2}x^2 - \frac{1}{2}x - \frac{1}{4}$ *and the remainder is* $R(x) = 2x^2 - \frac{1}{4}x - \frac{5}{4}$.

3. $A(x) = x^5 + x + 1$ *and* $B(x) = x^2 + x + 1$.
   We perform the Euclidean division of $A(x)$ *by* $B(x)$*:*

$$\begin{array}{r|l} x^5 + x + 1 & x^2 + x + 1 \\ \hline -(x^5 + x^4 + x^3) & x^3 - x^2 + 1 \\ \hline -x^4 - x^3 + x + 1 & \\ -(x^4 - x^3 - x^2) & \\ \hline x^2 + x + 1 & \\ x^2 + x + 1 & \\ \hline 0 & \end{array}$$

Since $\deg(0) = 0 < \deg(x^2+x+1) = 2$, *the division stops here. Hence,*

$$A(x) = B(x)(x^3 - x^2 + 1).$$

Therefore, the quotient is $Q(x) = x^3 - x^2 + 1$ *and the remainder is* $R(x) = 0$, *then* $B|A$.

4.

5. $A(x) = x^5 + x^2 + 1$ *and* $B(x) = x^2 + x + 1$.
We perform the Euclidean division of $A(x)$ *by* $B(x)$*:*

$$\begin{array}{r|l} x^5 + x + 1 & x^2 + x + 1 \\ \cline{2-2} -(x^5 + x^2 + 1) & x^3 - x^2 + 2 \\ \cline{1-1} -x^4 - x^3 + x^2 + 1 & \\ -(x^4 - x^3 - x^2) & \\ \cline{1-1} x^2 + 1 & \\ -(2x^2 + 2x + 2) & \\ \cline{1-1} -2x - 1 & \end{array}$$

Since $\deg(-2x-1) = 1 < \deg(x^2+x+1) = 2$, *the division stops here. Hence,*

$$A(x) = B(x)(x^3 - x^2 + 2) + -2x - 1.$$

Therefore, the quotient is $Q(x) = x^3 - x^2 + 2$ *and the remainder is* $R(x) = -2x - 1$.

Proposition 5.3 (Greatest common divisor (gcd))

If A and B are two non zero polynomials of $\mathbb{F}[x]$, then there exists a unique monic polynomial D of greatest degree that divides A and B.
This polynomial D is called the greatest common divisor of A and B, and it is denoted by $\gcd(A, B)$.

Example 5.7.

1. *If* P *is a monic polynomial, then* $\gcd(P, 0_{\mathbb{F}}[x]) = P$.
In fact, if Q *is a monic divisor polynomial of* P, *then we have* $\deg(Q) \leq \deg(P)$, *then* P *is a monic polynomial of greater degree that divides* P *and* $0_{\mathbb{F}}[x]$ *and since the gcd is unique then we deduce that* $\gcd(P, 0_{\mathbb{F}}[x]) = P$.

2. *For every polynomial* P *we have* $\gcd(P, 1) = 1$.

3. *If* P *is a non zero polynomial and if* Q *is a monic divisor of* P, *then* $\gcd(P, Q) = Q$.

4. $\gcd(x^{12} - 1, x^8 - 1) = x^4 - 1$.

Properties 5.1 (Greatest common divisor (gcd))

The greatest common divisor (gcd) of two polynomials A and B is a polynomial D with the following properties:

1. D divides both A and B.
2. Any polynomial dividing both A and B must also divides D.

Proposition 5.4

Let P and Q be two polynomials of $\mathbb{F}[x]$, not both zero. Then:

1. $\gcd(P, Q)$ is a monic polynomial.
2. For every $\alpha \in \mathbb{F}$ with $\alpha \neq 0_{\mathbb{F}}$, we have $\gcd(\alpha P, Q) = \gcd(P, Q)$.
3. If P is a non zero polynomial, then $\gcd(P, 0) = \frac{1}{\beta}P$, where β is the leading coefficient of P.
4. If $A = QB + R$, then $\gcd(A, B) = \gcd(B, R)$.

Proof.

1. Let $D = \gcd(P, Q)$, then
   - $D|P$ and $D|Q$,
   - If $C|P$ and $C|Q$, then $C|D$.

   If $\lambda \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$, then λD also divides P and Q.
   Let β be the leading coefficient of D. Since $\beta \neq 0$, define

   $$D_0 = \frac{1}{\beta}.$$

   Then
   - D_0 is monic,
   - $D_0|P$ and $D_0|Q$.

   Thus the gcd can always be chosen monic. By convention, we define $\gcd(P, Q)$ to be this unique monic polynomial.

2. Let $D = \gcd(P, Q)$. Since $\alpha \neq 0_{\mathbb{F}}$, multiplication by α does not change divisibility, that is:
   - If $D|P$, then $D|\alpha P$.

- If $D|\alpha P$, then $D|P$.

Thus P and αP have the same divisors.
Therefore, the common divisors of (P, Q) are the same as those of $(\alpha P, Q)$. Since the grater common divisor is a monic polynomial then

$$\gcd(\alpha P, Q) = \gcd(P, Q).$$

3. We know that every polynomial divides the zero polynomial. Thus the common divisors of P and 0 are the divisors of P and therefore, the greatest common divisor of P and 0 is the polynomial P itself. Since the greater common divisor of two polynomials is defined to be monic, then we divide by the leading coefficient β, then

$$\gcd(P, 0) = \frac{1}{\beta}P.$$

4. Let D be any common divisor of A and B. Since $R = QB - A$, it follows that the polynomial D divides also R.
Thus every common divisor of A and B is also a common divisor of B and R.
In particular,

$$\gcd(A, B)|\gcd(B, R).$$

Conversely, let D be any common divisor of B and R. Since $A = QB + R$, it follows that the polynomial D divides also A. Thus every common divisor of B and R is also a common divisor of A and B.
In particular,

$$\gcd(B, R)|\gcd(A, B).$$

Since both $\gcd(B, R)$ and $\gcd(A, B)$ are monic polynomials and divide each other, they must be equal. Therefore,

$$\gcd(B, R) = \gcd(A, B).$$

□

Proposition 5.5

Let A and B be two non zero polynomials of $\mathbb{F}[x]$. Then

1. Every divisor of A and B divides $\gcd(A, B)$.
2. For every monic polynomial P, we have $\gcd(AP, BP) = P\gcd(A, B)$.

Proof.

1. Let $D = \gcd(A, B)$, and let C be any polynomial such that

$$C|A \text{ and } C|B.$$

By definition of the greatest common divisor, D is a common divisor of A and B with the highest degree among all the other divisors.
Since C is also a common divisor of A and B, we must have

$$\deg(C) \leq \deg(D).$$

Because both C and D divide A and B, and D is the polynomial of greatest degree, it follows that every common divisor divides the GCD . Hence,

$$C|D.$$

Therefore, every divisor of A and B divides $\gcd(A, B)$.

2. Let P be a monic polynomial and let $D = \gcd(A, B)$. Since $D|A$ and $D|B$, it follows that $DP|AP$ and $DP|BP$. Hence DP is a common divisor of AP and BP, so

$$DP|\gcd(AP, BP).$$

In particular, $P|\gcd(AP, BP)$.
Let $G = \gcd(AP, BP)$. Since $P|G$, we may write

$$G = QP$$

for some polynomial Q. Because both G and P are monic, their leading coefficients are 1, and therefore Q must also be monic.
Now, since $G = QP$ divides both AP and BP, it follows that $Q|A$ and $Q|B$. Hence $Q|D$.
On the other hand, we already know that $DP|G$, that is $DP|QP$. Since $P \neq 0_{\mathbb{F}[x]}$, we can cancel P to obtain $D|Q$.
Thus

$$D|Q \text{ and } Q|D.$$

Therefore, there exists a nonzero constant $a \in \mathbb{F}$, such that $D = aQ$. Since both D and Q are monic, we must have $a = 1$. Hence $D = Q$.
Substituting back, we conclude

$$\gcd(AP, BP) = QP = DP = P\gcd(A, B).$$

□

Definition 5.4 (Least common multiple (lcm))

If A and B are two non zero polynomials of $\mathbb{F}[x]$, then there exists a unique monic polynomial M of smallest degree such that $A|M$ and $B|M$.
This polynomial M is called the least common multiple of A and B, it is denoted by $\text{lcm}(A, B)$.

Example 5.8.

1. *Let* $A(x) = x - 1$ *and* $B(x) = x^2 - 1$ *in* $\mathbb{R}[x]$. *We have that*

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

Therefore, the smallest monic polynomial divisible by both $x - 1$ *and* $x^2 - 1$ *is*

$$\text{lcm}(x - 1, x^2 - 1) = x^2 - 1.$$

2. *Let* $A(x) = x^2 - x$ *and* $B(x) = x^2 - 1$ *in* $\mathbb{R}[x]$. *We have:*

$$A(x) = x(x + 1), \quad B(x) = (x - 1)(x + 1).$$

Therefore, the least common multiple is

$$\text{lcm}(A, B) = x(x + 1)(x - 1) = x^3 - x.$$

Properties 5.2 (Least common multiple (lcm))

The least common divisor (lcm) of two polynomials A and B is a polynomial M with the following properties:

1. M is a multiple of both A and B;
2. Any polynomial that is a multiple of both A and B must be also a multiple of M.
3. Let C be a nonzero monic polynomial. Then $\text{lcm}(CA, CB) = C\ \text{lcm}(A, B)$.

Definition 5.5 (Euclidean Algorithm)

Let A and B be two polynomials in $\mathbb{F}[x]$ with $B \neq 0_{\mathbb{F}[x]}$. We calculate the successive Euclidean divisions of polynomials.

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

We stop algorithm when a division yields a remainder equal to zero.

Definition 5.6

The greatest common divisor (gcd) of two polynomials A and B can be determined using the Euclidean algorithm.

- If $R_1 = 0$, then $\gcd(A, B) = B$.
- Otherwise, is the last nonzero remainder R_k that is $\gcd(A, B) = R_k$.

Example 5.9. *Find the greatest common divisor (gcd) of the following polynomials in the polynomial ring* $\mathbb{R}[x]$*:*

1. *Let* $A = x^4 - 1$ *and* $B = x^3 - 1$*. We apply the Euclidean algorithm.*
   Step 1. *Divide* $x^4 - 1$ *by* $x^3 - 1$*, gives*

$$\begin{array}{r|l} x^4 - 1 & x^3 - 1 \\ \cline{2-2} -(x^4 - x) & x \\ \cline{1-1} x - 1 & \end{array}$$

   Since $\deg(x - 1) = 1 < \deg(x^3 - 1) = 3$*, we continue the division process.*
   Step 2. *Divide* $x^3 - 1$ *by* $x - 1$*, we obtain*

$$\begin{array}{r|l} x^3 - 1 & x - 1 \\ \cline{2-2} -(x^3 - x^2) & x^2 + x + 1 \\ \cline{1-1} x^2 - 1 & \\ -(x^2 - x) & \\ \cline{1-1} x - 1 & \\ -(x - 1) & \\ \cline{1-1} 0 & \end{array}$$

   Since the remainder is 0*, the algorithm terminates. Then we have*

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

Therefore, the greatest common divisor of A and B is $\gcd(A,B) = (x-1)$.

2. *Let* $A = x^4 + x^3 + 2x^2 + x + 1$ *and* $B = x^3 - 1$. *We apply the Euclidean algorithm:*

$$\begin{aligned} A &= B(x+1) + 2(x^2+x+1) \\ B &= (x^2+x+1)(x-1) \end{aligned}$$

Therefore, the greatest common divisor of A and B is $\gcd(A,B) = (x^2+x+1)$.

3. *Let* $B = x^2 + 1$ *and* $A = x^6 + x^3 + x + 1$. *We apply the Euclidean algorithm:*

$$A = (x^2+1)(x^4 - x^2 + x + 1).$$

Therefore, the greatest common divisor of A and B is $\gcd(A,B) = x^2 + 1$.

Remark 5.4

Since $\gcd(\lambda P, Q) = \gcd(P,Q)$ for any $\lambda \in \mathbb{F}$ with $\lambda \neq 0_{\mathbb{F}}$, we can replace one of the remainder R_k obtained with λR_n, where $\lambda \neq 0_{\mathbb{F}}$.

Example 5.10.
We apply the Euclidian algorithm to determine the greater common divisor of the polynomials

$$A(x) = x^4 + 4x^3 + x^2 - 16 \text{ and } B(x) = x^3 + 3x^2 - 3x + 4.$$

The division steps are as follows:

- $A(x) = B(x)(x+1) + (x^2 - x - 20)$,
- $B(x) = (x^2 - x - 20)(x+4) + 21(x+4)$,
- *Factorizing the remainder:* $(x^2 - x - 20) = (x+4)(x-5)$,

Therefore, the greater common divisor of A and B is $\gcd(A,B) = x + 4$.

Definition 5.7 (Coprime polynomials)

Let A and B be two polynomials of $\mathbb{F}[x]$ not both zero, we say that A and B are coprime polynomials if $\gcd(A,B) = 1$.

Lemma 5.1

Let A and B be two no zero polynomials of $\mathbb{F}[x]$. The quotients of A and B on their greater common divisor are coprime polynomials.

Proof.
Let $D = \gcd(A, B)$ and $D_1 = \gcd(A_1, B_1)$, where $A_1 = \frac{A}{D}$ and $B_1 = \frac{B}{D}$. Since both D and D_1 are monic polynomials, their product DD_1 is also a monic.
Because $D_1|A_1$, then DD_1 divide $DA_1 = A$. Similarly, since $D_1|B_1$, then DD_1 divide $DB_1 = B$.
Therefore, DD_1 is a common divisor of A and B.
By definition of the greatest common divisor, the degree of any common divisor of A and B cannot exceed $\deg(D)$. hence,

$$\deg(DD_1) \leq \deg(D).$$

But

$$\deg(DD_1) = \deg(D) + \deg(D_1),$$

so we must have $\deg(D_1) = 0$. Therefore, D_1 is a constant polynomial. Since D_1 is a monic, it follows that $D_1 = 1$. □

Theorem 5.2

Let A and B be two non zero polynomials of $\mathbb{F}[x]$. If $D = \gcd(A, B)$, then there exists polynomials U and V such that $D = AU + BV$.

Example 5.11. *Consider these polynomials:*

$$A(x) = x^4 + 4x^3 + x^2 - 16 \text{ and } B(x) = x^3 + 3x^2 - 3x + 4.$$

Their greatest common divisor is given by $\gcd(A, B) = x + 4$.
From the euclidian algorithm, we obtain:

$$\begin{aligned} 21(x+4) &= B - (x^2 - x - 20)(x+4) \\ &= B - (A - (x-1)B)(x+4) \\ &= (x^2 + 5x + 5)B(x+4)A \end{aligned}$$

Consequently, we obtain the Bézout formula:

$$(x^4 + 4x^3 + x^2 - 16)U + (x^3 + 3x^2 - 3x + 4)V = x + 4$$

where

$$U = -\frac{1}{21}(x+4) \text{ and } V = \frac{1}{21}(x^2 + 5x + 5).$$

5.4 Roots of a polynomial

Definition 5.8

Let $P \in \mathbb{F}[x]$ and $\lambda \in \mathbb{F}$, we say that λ is the zero (root) of the polynomial P in $\mathbb{F}$ if and only if $P(\alpha) = 0$.

Example 5.12.

1. *$P(x) = x^2 + 2x - 3$, the value 1 is a zero of the polynomial P in $\mathbb{R}$ because*
$$P(1) = 1^2 + 2(1) - 3 = 0.$$
2. *i is a zero of the polynomial $Q(x) = x^2 + 1$ in $\mathbb{C}$ because*
$$Q(i) = i^2 + 1 = -1 + 1 = 0.$$
3. *1 is not a zero of the polynomial $R(x) = x^4 + 3x - 5$ in $\mathbb{C}$ because*
$$R(1) = 1^4 + 3(1) - 5 = -1 \neq 0.$$
‘
4. *$S(x) = 5x^2 - 25x + 30$ is a polynomial in $\mathbb{R}[x]$ it has the following factorization $P(x) = 5(x-2)(x-3)$, then P has two roots $\lambda_1 = 2$ and $\lambda_2 = 3$, since $S(2) = 0$ and $S(3) = 0$.*
5. *The polynomial $P(x) = x^2 + 1$ in $\mathbb{R}[x]$ has no roots in $\mathbb{R}$.*

Proposition 5.6

Let $P \in \mathbb{F}[x]$ and $\lambda \in \mathbb{F}$.
The remainder of the euclidian division of P over $x - \lambda$ is equal to $P(\lambda)$.

Proof.
The euclidian division of P over $x - \lambda$ is in the form
$$P(x) = Q(x)(x - \lambda) + R(x), \text{ with } \deg(R) < \deg(Q).$$
Since $\deg(x - \lambda) = 1$, then $\deg(R) = -\infty$ or $\deg(R) = 0$. In any case, the polynomial $R(x) = c$, with $c \in \mathbb{F}$.
In the other hand,
$$\begin{aligned} P(\lambda) &= Q(\lambda)(\lambda - \lambda) + R(\lambda) \\ &= Q(\lambda)(\lambda - \lambda) + c \\ &= c \end{aligned}$$
Therefore, $P(\lambda) = R(\lambda)$. □

Corollary 5.1

Let $P \in \mathbb{F}[x]$ and $\lambda \in \mathbb{F}$. The element $\lambda \in \mathbb{F}$ is a zero (root) of the polynomial P if and only if $(x - \lambda)$ divides P. In other terms

$$P(\lambda) = 0 \Leftrightarrow \exists Q \in \mathbb{F}[x],\ P(x) = (x - \lambda)Q(x).$$

Proposition 5.7

Let $n \in \mathbb{N}$. If $P \in \mathbb{F}[x]$ is a polynomial of degree n, then P has at most n roots in $\mathbb{F}$.

Proof.
We prove this result by induction on n.

- If $n = 1$, there exist $a, b \in \mathbb{F}$ such that $P = ax + b$ and $a \neq 0_{\mathbb{F}}$. The polynomial P has then exactly one root $\frac{-b}{a}$.
- If $n \geq 2$, then either P has no roots in $\mathbb{F}$ (and in this case there is at most n roots), or P has at least one root in $\mathbb{F}$. Suppose that the element $a \in \mathbb{F}$ is a root of P. By the previous corollary, there exists a polynomial $Q \in \mathbb{F}[x]$ such that $P = (x - a)Q$. The polynomial Q is pf degree $n - 1$, then from induction hypothesis, Q has at most $n - 1$ roots. It follows that P has at most n roots.

□

Example 5.13.

1. *The polynomial $P(x) = x^2 - 2$ has no roots in $\mathbb{C}$, but it has two real roots, that are $\sqrt{2}$ and $-\sqrt{2}$.*
2. *The polynomial $Q(x) = x^4 + 1$, has no real roots, but it has four complexe roots:*

$$\frac{1+i}{\sqrt{2}},\ \frac{1-i}{\sqrt{2}},\ \frac{-1-i}{\sqrt{2}},\ \frac{-1+i}{\sqrt{2}}.$$

Definition 5.9

Let $P \in \mathbb{F}[x]$ and let $k \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$. We say that $\lambda \in \mathbb{F}$ is a root of multiplicity (or order) k of P if $(x - \lambda)^k$ divides P, while $(x - \lambda)^{k+1}$ does not divide P.
When

- $k = 1$ we say that λ is a simple root of P or is a root of multiplicity 1.
- $k = 2$ we say that λ is a double root of P or is a root of multiplicity 2.
- $k = 3$ we say that λ is a triple root of P or is a root of multiplicity 3.

Properties 5.3

1. If $\lambda_1, \lambda_2, \ldots, \lambda_k$ are distinct roots of p, then $(x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_k)$ divides P.
2. If $\deg(P) = n$, then P has at most n distinct roots.
3. If λ is a root of multiplicity k, then $P(\lambda) = P'(\lambda) = \cdots = P^{k-1}(\lambda) = 0$ and $P^{(k)}(\lambda) \neq 0$.

Theorem 5.3 (Alembert-Gauss theorem)

Every non constant polynomial in $\mathbb{C}[x]$ has at least one root in $\mathbb{C}$.

Example 5.14. *Consider the following polynomial with real coefficients of second order $P(x) = ax^2 + bx + c$ with $a \neq 0$, then the polynomial P has exactly two roots in $\mathbb{C}$.*
Let $\Delta = b^2 - 4ac$ be the discriminant of P.

- *If $\Delta > 0$, then P has two distinct real roots.*
- *If $\Delta < 0$, then P has two distinct complexe roots.*
- *If $\Delta = 0$, then P has a real double root.*

Theorem 5.4

A polynomial that has more zeros, then its degree is necessary zero.

Corollary 5.2

The zero polynomial is the only polynomial which admits an infinity of zeros.

5.5 Factorization into a product of irreducible factors

For every polynomial $P \in \mathbb{F}[x]$ and every nonzero element $\lambda \in \mathbb{K}$, we have $P = \left(\frac{1}{\lambda}\right)\lambda P$. There are polynomials for which there is no other factorization: irreducible polynomials. The corresponding notion in arithmetic is that of a prime number.

Definition 5.10

A non constant polynomial $P \in \mathbb{F}[x]$ is irreductible, if its only divisors are constant polynomials and polynomials of the form λP with $\lambda \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$.
Otherwise, we say that P it is irreductible if the polynomial is not irreductible.

Example 5.15.

1. *Every polynomial of degree* 1 *is irreductible over* $\mathbb{F}$.
2. *The polynomial of the form* ax^2+bx+c *in* $\mathbb{R}[x]$ *are irreductible over* $\mathbb{R}$ *if and only if* $b^2-ac<0$.
3. *The polynomials of the form* ax^2+bx+c *in* $\mathbb{C}[x]$ *are reductible over* $\mathbb{C}$.
   For example,
   - $P(x)=x^2+1=(x-i)(x+i)$ *is reductible in* $\mathbb{C}[x]$ *and irreductible in* $\mathbb{R}[x]$.
   - *Let* $Q(x)=x^2-2$, *the the polynomial* Q *is reductible in* $\mathbb{R}[x]$ *since* $x-\sqrt{2}$ *as divisor, but* Q *is irreductible in* $\mathbb{Q}[x]$.

Lemma 5.2

Let Q be a non zero polynomial and P is an irreductible polynomial. Then either P divides Q or P and Q are relatively prime.

Proof. Let $D=\gcd(P,Q)$. In particular, D is a monic divisor of P, therefore,

$$D=1 \text{ or } D=\left(\frac{1}{\lambda}\right)P,$$

if λ is the leading coefficient of the polynomial P. Then, P divides Q. □

Lemma 5.3 (Euclide Lemma)

Let A and B be two nonzero polynomials and P is an irreductible polynomial. If P divides AB then P divide A or P divides B.

Theorem 5.5 (Decomposition into irreductibles factors)

For any monic polynomial $P\in\mathbb{F}[x]$ with $\deg(P)\geq 1$, there exist a unique positive natural number r and monic irreductible polynomials $P_1,P_2,\ldots,P_n$ pairwise distinct in $\mathbb{F}[x]$, and positive natural numbers $\alpha_1,\alpha_2,\ldots,\alpha_r$ as well as a unique element $\lambda\in\mathbb{F}^*$ such that

$$\begin{aligned} P &= \lambda\prod_{i=1}^{r}P_i^{\alpha_i} \\ &= \lambda P_1^{\alpha_1}P_2^{\alpha_2}\cdots P_r^{\alpha_r} \end{aligned}$$

Proof.
We prove the existence of such a factorization by induction on the degree of P.

- If $\deg P=1$, then P is irreducible and monic, so the result holds.

- Suppose that $\deg P \geq 2$.
  Let P_1 be a non-constant monic divisor of P of minimal degree among all non-constant monic divisors of P. Any monic divisor of P_1 also divides P, hence its degree is either 1 or equal to $\deg P_1$. Therefore, P_1 is irreducible.

  If $\deg P = \deg P_1$, then $P = P_1$ and we are done.

  If $\deg P > \deg P_1$, let Q be the quotient of P over P_1. The polynomial Q is non-constant, monic, and of strictly smaller degree than P. By the induction hypothesis, Q admits a factorization into monic irreducible polynomials. Hence,

$$P = P_1 Q$$

  is a factorization of P into monic irreducible polynomials.

We now prove uniqueness, again by induction on $\deg P$.

Suppose

$$P = P_1 \cdots P_r \quad \text{and} \quad P = Q_1 \cdots Q_s,$$

where r, s are positive integers and the P_i, Q_j are monic irreducible polynomials.

By Euclid's lemma, P_1 divides at least one of the Q_j. After reordering the Q_j, we may assume that P_1 divides Q_1. Since Q_1 is irreducible and P_1 is non-constant, there exists $\lambda \in K$ such that

$$P_1 = \lambda Q_1.$$

Because both P_1 and Q_1 are monic, it follows that $\lambda = 1$, hence $P_1 = Q_1$.

If $\deg P = \deg P_1$, then $P = P_1$ and $r = s = 1$. If $\deg P > \deg P_1$, we cancel $P_1 = Q_1$ and apply the induction hypothesis to the quotient $\frac{P}{P_1}$ to conclude that the remaining factors coincide up to permutation.

This completes the proof. □

Proposition 5.8

Let $P \in \mathbb{F}[x]$ be a polynomial of degree 2 or 3. Then the polynomial P is irreductible if and only if P has no roots in $\mathbb{F}$.

Proof.
If P has a root λ in $\mathbb{F}$, then $X - \lambda$ divides P, and the quotient Q is a nonconstant polynomial, by the hypothesis on the degree of P. It follows that P is not irreducible.

Conversely, suppose that P is not irreducible. Then there exist nonconstant polynomials Q and R such that

$$P = QR.$$

Thus,

$$\deg P = \deg Q + \deg R.$$

Since $\deg P$ is equal to 2 or 3, and since $\deg Q \geq 1$ and $\deg R \geq 1$, it follows that one of the polynomials Q or R must have degree 1.

Suppose, for example, that Q has degree 1. Then

$$Q = aX + b, \quad a \neq 0.$$

We have $Q\left(\frac{-b}{a}\right) = 0$. Moreover,

$$P\left(\frac{-b}{a}\right) = Q\left(\frac{-b}{a}\right) R\left(\frac{-b}{a}\right) = 0.$$

Therefore, P has a root in $\mathbb{F}$. □

Definition 5.11 (Factorization in $\mathbb{C}$)

Let $P \in \mathbb{C}[x]$ be a polynomial of degree $n \geq 1$. The factorization of P is given by

$$P = \lambda(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \cdots (x - \alpha_r)^{k_r},$$

where $\lambda \in \mathbb{C} \setminus \{0\}$, $\alpha_1, \alpha_2, \ldots, \alpha_r$ are the distinct roots of P, and $k_1, k_2, \ldots, k_r$ are positive integers denoting their respective multiplicities. Moreover, $k_1 + k_2 + \cdots + k_r = n$.

Definition 5.12 (Factorization in $\mathbb{R}$)

Let $P \in \mathbb{R}[x]$ be a polynomial of degree $n \geq 1$. The factorization of P is given by

$$P = \lambda(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \ldots (x - \alpha_r)^{k_r} Q_1^{l_1} Q_2^{l_2} \cdots Q_s^{l_s}$$

where:

- $\lambda \in \mathbb{R} \setminus \{0\}$,
- $\alpha_1, \cdots, \alpha_r$ are the distinct real roots of P, with multiplicities $k_1, \ldots, k_r \geq 1$,
- each $Q_j(x)$ is an irreducible polynomial over $\mathbb{R}$ of degree 2,
- each Q_j is of the form

$$Q_j(x) = x^2 + \beta_j x + \gamma_j, \qquad \text{with } \Delta_j = \beta_j^2 - 4\gamma_j < 0,$$

and $\ell_j \geq 1$.

Example 5.16.
Let

$$P(x) = 2x^4(x - 1)^3(x^2 + 1)^2(x^2 + x + 1).$$

The polynomial P is already factored into irreductible factors over $\mathbb{R}[x]$. To factor $P(x)$ over $\mathbb{C}[x]$, we decompose each quadratic factor into linear factors. We have

$$x^2+1=(x-i)(x+i) \text{ and } x^2+x+1=\left(x-\frac{-1+i\sqrt{3}}{2}\right)\left(x+\frac{-1+i\sqrt{3}}{2}\right).$$

Therefore, the factorization of $P(x)$ over $\mathbb{C}[x]$ is

$$P(x)=2x^4(x-1)^3(x-i)^2(x+i)^2\left(x-\frac{-1+i\sqrt{3}}{2}\right)\left(x+\frac{-1+i\sqrt{3}}{2}\right).$$

5.6 Exercises

Exercise 5.1.

1. *Let $n\in\mathbb{N}^*$. Determine the remainder of the Euclidean division of*

$$A=x^{2n}+3(x+1)^n+2 \text{ by } B=x(x+1).$$

2. *Determine a polynomial P of degree 3 in $\mathbb{R}[x]$ such that the remainder of the Euclidean division of P by x^2-2x+1 is $3x-3$ and the remainder of the Euclidean division of P by x^2-4 is $4x-1$.*

Exercise 5.2. *Determine the greater common divisor of these polynomials:*

1. $P(x)=x^6-x^4-x^2+1;\quad Q(x)=x^4+2x^3-2x-1.$
2. $P(x)=x^5-x^4+2x^3-2x^2+2x-1;\quad Q(x)=x^5-x^4+2x^2-2x+1.$
3. $P(x)=x^n-1;\quad Q(x)=(x-1)^n,\ n\geq 1.$

Exercise 5.3.

1. *Factorize the following polynomials in $\mathbb{R}[x]$:*

$$P(x)=x^4-1,\quad Q(x)=x^2-1.$$

Determine the least common multiple $\operatorname{lcm}(P,Q)$.

2. *Factorize the following polynomials in $\mathbb{C}[x]$:*

$$R(x)=x^2-ix,\quad S(x)=x^2+1.$$

Determine the least common multiple $\operatorname{lcm}(R,S)$.

Exercise 5.4.
Let the polynomial:

$$P(x) = x^3 + 2x^2 - x - 2.$$

1. *Show that the polynomial P has three roots in $\mathbb{Z}$, then determine their values.*
2. *Deduce a factorization of P.*

Exercise 5.5.
Consider the polynomial

$$P(x) = x^5 + x^4 + 2x^3 + 2x^2 + x + 1.$$

1. *Determine the* $\gcd(P, P')$.
2. *Determine the common roots of P and P'. Deduce the multiple roots of P in $\mathbb{C}[x]$ and their multiplicities.*
3. *Show that $(x+1)^2$ divide P.*
4. *Factorize P in $\mathbb{R}[x]$.*

Exercise 5.6.

1. *Do there exist polynomials $P, Q \in \mathbb{Q}[x]$ such that*

$$(x^6 - 1)P + (x^{10} - 1)Q = x^2 + 1\,?$$

If Yes, determine all such polynomials $P, Q \in \mathbb{Q}[x]$ satisfying this equation.

2. *Do there exist polynomials $P, Q \in \mathbb{Q}[x]$ such that*

$$(x^6 - 1)P + (x^{10} - 1)Q = x^3 + x^2 - x - 1.$$

5.7 Solution of exercises

Solution of exercise 5.1.

1. *Let $n \in \mathbb{N}^*$. Determine the remainder of the Euclidean division of*

$$A = x^{2n} + 3(x+1)^n + 2 \;\; \textit{by} \;\; B = x(x+1).$$

We perform the Euclidean division of A by B:

$$A = BQ + R \quad \textit{with} \quad \deg(R) < \deg(B) = 2.$$

Thus, $\deg(R) \leq 1$, *that is,* $R = ax + b$. *Then,*

$$x^{2n} + 3(x+1)^n + 2 = x(x+1)Q + ax + b.$$

For $X = 0$, *we obtain* $b = 5$.
For $x = -1$, *we obtain* $a = 2$. *Finally,*

$$R = 2x + 5.$$

Solution of exercise 5.2.

1. $P(x) = x^6 - x^4 - x^2 + 1; \quad Q(x) = x^4 + 2x^3 - 2x - 1.$
We apply the Euclid's algorithm. The last non-zero remainder gives a gcd *of the two polynomials.*
The successive divisions gives

$$\begin{aligned} x^6 - x^4 - x^2 + 1 &= (x^4 + 2x^3 - 2x - 1)(x^2 - 2x + 3) + (-4x^3 - 4x^2 + 4x + 4) \\ x^4 + 2x^3 - 2x - 1 &= (-4x^3 - 4x^2 + 4x + 4)(-\tfrac{1}{4}x - \tfrac{1}{4}) + (-x + 1) \\ -4x^3 - 4x^2 + 4x + 4 &= (-x + 1)(4x^2 + 8x + 4) \end{aligned}$$

Therefore, $\gcd(P, Q) = -x + 1$.

2. $P(x) = x^5 - x^4 + 2x^3 - 2x^2 + 2x - 1; \quad Q(x) = x^5 - x^4 + 2x^2 - 2x + 1.$
We apply the Euclid's algorithm. The last non-zero remainder gives a gcd of the two polynomials.
The successive divisions gives

$$\begin{aligned} x^5 - x^4 + 2x^3 - 2x^2 + 2x - 1 &= (x^5 - x^4 + 2x^2 - 2x + 1)(1) + (2x^3 - 4x^2 + 4x - 2) \\ x^5 - x^4 + 2x^2 - 2x + 1 &= (2x^3 - 4x^2 + 4x - 2)(\tfrac{1}{2}x^2 + \tfrac{1}{2}x) + (x^2 - x + 1) \\ 2x^3 - 4x^2 + 4x - 2 &= (x^2 - x + 1)(2x - 2) \end{aligned}$$

Therefore, $\gcd(P, Q) = x^2 - x + 1$.

3. $P(x) = x^n - 1; \quad Q(x) = (x-1)^n, \ n \geq 1.$
All the non constant divisors of the polynomial Q *are of powers of* $(x-1)$, *that is*

$$(x-1), (x-1)^2, \ldots, (x-1)^n$$

. We check which of these divisors also divide the polynomial P. *We know that*

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + 1)$$

then $(x-1)$ *divides the polynomial* P.
But the polynomial $(x-1)^2$ *does not divide* P, *because* 1 *is a simple root not a double root, then both polynomials contain the factor* $(x-1)$, *but only once in* P.
Therefore, $\gcd(P, Q) = x - 1$.

Solution of exercise 5.3.

1. *We factorize the polynomials P and Q in $\mathbb{R}[x]$, we have:*

$$P(x) = x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1)$$
$$Q(x) = x^2 - 1 = (x - 1)(x + 1)$$

The the least common multiple takes each irreducible factor with the highest power appearing. Therefore,

$$\text{lcm}(P, Q) = (x - 1)(x + 1)(x^2 + 1)$$

2. *We factorize the following polynomials in $\mathbb{C}[x]$. We have:*

$$R(x) = x^2 - ix = x(x - i)$$
$$S(x) = x^2 + 1 = (x - i)(x + i)$$

The the least common multiple takes each irreducible factor with the highest power appearing. Therefore,

$$\text{lcm}(R, S) = x(x - i)(x + i)$$

Solution of exercise 5.4.
Let the polynomial:

$$P(x) = x^3 + 2x^2 - x - 2.$$

1. *Show that the polynomial P has three roots in $\mathbb{Z}$, then determine their values.*
Let $m \in \mathbb{Z}$ be a root of P, then

$$\begin{aligned} P(m) = 0 \Leftrightarrow & \quad m^3 + 2x^2 - x - 2 = 0 \\ \Leftrightarrow & \quad m^3 + 2m^2 - m = 2 \\ \Leftrightarrow & \quad m(m^2 + 2m - 1) = 2. \end{aligned}$$

Since m and $m^2 + 2m - 1$ are integers, their product is 2. The integer divisors of 2 are $\pm 1, \pm 2$. We examine the possible cases:

- $m = 1$*:* $m^2 + 2m - 1 = 1 + 2 - 1 = 2$*, product* $1 \times 2 = 2$
- $m = 2$*:* $m^2 + 2m - 1 = 4 + 4 - 1 = 7$*, product* $2 \times 7 = 14$
- $m = -1$*:* $m^2 + 2m - 1 = 1 - 2 - 1 = -2$*, product* $(-1) \times (-2) = 2$
- $m = -2$*:* $m^2 + 2m - 1 = 4 - 4 - 1 = -1$*, product* $(-2) \times (-1) = 2$

The possible integer roots are therefore $m = 1$, $m = -1$ and $m = -2$. A quick verification:

$$P(1) = 1+2-1-2 = 0, \quad P(-1) = -1+2+1-2 = 0, \quad P(-2) = -8+8+2-2 = 0.$$

Thus, P has three integer roots: 1, -1 and -2.

2. *Deduce a factorization of P.*
Since $-1, -2$ and 1 are the three roots of the polynomial P, then its factorization is given by
$$P(x) = (x+1)(x+2)(x-1).$$

Solution of exercise 5.5.
Consider the polynomial
$$P(x) = x^5 + x^4 + 2x^3 + 2x^2 + x + 1.$$

1. *Determine the* $\gcd(P, P')$.
The first derivative of P is
$$P'(x) = 5x^4 + 4x^3 + 6x^2 + 4x + 1.$$
We apply the Euclid's algorithm. The last non-zero remainder gives a gcd of the polynomials P and P'.
The successive divisions gives
$$\begin{aligned} x^5 + x^4 + 2x^3 + 2x^2 + x + 1 &= P'(x)(\tfrac{1}{5}x + \tfrac{1}{5}) + \tfrac{8}{25}(2x^3 + 3x^2 + 2x + 3) \\ 5x^4 + 4x^3 + 6x^2 + 4x + 1 &= (2x^3 + 3x^2 + 2x + 3)(\tfrac{5}{2}x - \tfrac{7}{4}) + \tfrac{25}{4}(x^2 + 1) \\ 2x^3 + 3x^2 + 2x + 3 &= (x^2 + 1)(2x + 3) \end{aligned}$$
Therefore, $\gcd(P, Q) = x^2 + 1$.

2. *The common roots of P and P' are the roots of the gcd:*
$$x^2 + 1 = 0 \Rightarrow x = i \text{ or } x = -i.$$
Multiple roots of P in $\mathbb{C}[x]$ are exactly the roots of the gcd. Therefore, the multiple roots are:
$$x = i \quad \text{and} \quad x = -i.$$
Each has multiplicity 2.

3. *Show that $(x^+1)^2$ divide P.*
Since P is divisible by $(x-i)^2(x+i)^2 = ((x-i)(x+i))^2 = (x^2+1)^2$.

4. *Factorize P in $\mathbb{R}[x]$.*
We divide P by $(x^2+1)^2 = x^4 + 2x^2 + 1$ and we obtain
$$P(x) = (x+1)(x^2+1)^2.$$

Solution of exercise 5.6.

1. *We compute the greater common divisor of the polynomials* (x^6-1) *and* $(x^{10}-1)$*, using the Euclide Algorithm. We have*

$$\begin{aligned}(x^{10}-1) &= (x^6-1)x^4+(x^4-1)\\ (x^6-1) &= (x^4-1)x^2+(x^2-1)\\ (x^4-1) &= (x^2-1)(x^2+1).\end{aligned}$$

Therefore, $\gcd(x^{10}-1,x^6-1)=x^2-1$.
Then $x^2-1|x^{10}-1$ *and* $x^2-1|x^6-1$*, thus*

$$x^6-1=(x^2-1)(x^4+x^2+1)$$

and

$$x^{10}-1=(x^2-1)(x^8+x^6+x^4+x^2+1)$$

Consequently, every polynomial $P,Q\in\mathbb{Q}[x]$*,* x^2-1 *is a divisor of*

$$(x^6-1)P+(x^{10}-1)Q.$$

On the other side, we have $\gcd(x^2+1,x^2-1)=2$ *and* x^2-1 *is not a divisor of* x^2+1*. Therefore, there is no polynomials* $P,Q\in\mathbb{Q}[x]$ *such that*

$$(x^6-1)P+(x^{10}-1)Q=x^2+1.$$

2. *We have that* $\gcd(x^{10}-1,x^6-1)=x^2-1$*, then from Bezout theorem there exists two polynomials* $U,V\in\mathbb{Q}[x]$ *such that*

$$(x^6-1)U+(x^{10}-1)V=x^2-1.$$

On the other side, we have

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

Therefore there exist polynomials $Q\in\mathbb{Q}[x]$ *such that*

$$(x^6-1)P+(x^{10}-1)Q=x^3+x^2-x-1.$$

For example, we take:

$$P=(x+1)U \text{ and } Q=(x+1)V.$$

Bibliography

[1] Stéphane Balac and Frédéric Sturm. *Algèbre et analyse: cours de mathématiques de première année avec exercices corrigés*. EPFL Press, 2003.

[2] Damien Etienne. *Exercices corrigés d'algèbre linéaire*. De Boeck, 2006.

[3] Ioannis Farmakis and Martin Moskowitz. *A Graduate Course in Algebra*. World Scientific, 2017.

[4] Linda Gilbert and Jimmie Gilbert. Elements of modern algebra 7th (seventh) edition, 2008.

[5] Ali Grami. *Discrete mathematics: essentials and applications*. Academic Press, 2022.

[6] Vijay K Khanna and SK Bhamri. *A course in abstract algebra*. Vikas Publishing House, 2016.

[7] François Liret and Dominique Martinais. *Algèbre-1re année-2e éd.: Cours et exercices avec solutions*. Dunod, 2021.