REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Djilali Bounaama, Khemis Miliana
Faculté des Sciences de la Matière et d'informatique
Conseil Scientifique de la Faculté

جامعة جيلالي بونعامة خميس مليانة
كلية علوم المادة والإعلام الآلي
المجلس العلمي للكلية

Ref : 02 /06/CSF/ 2026

EXTRAIT DU PV
DE LA REUNION ORDINAIRE DU CONSEIL SCIENTIFIQUE
Du 02/05/2026

Objet : : Expertise de polycopié pédagogique

En l'an deux mille vingt-six (2026), le deux (02) mai 09 h 30, une réunion ordinaire du Conseil Scientifique de la Faculté des Sciences de la Matière et de l'Informatique s'est tenue dans la salle de réunion de la faculté (Bloc B).

Suite aux rapports favorables reçus de la part des experts cités ci-après concernant l'expertise du polycopié pédagogique, le CSF a prononcé favorablement pour la conformité du polycopié pédagogique en vue de préparer son habilitation.

- **Auteur du polycopié** : Dr. BOURCHI Soumia (MCB)
- **Intitulé du polycopié** : Algebra I, course and Exercises with solutions
- **Destiné aux étudiants de** : L1 Mathématiques.
- **Experts du polycopié** :

• ABDELAZIZ Meryem	MCA	UHB-Chlef
• HOUASNI Mohamed	MCA	UDB-Khemis Miliana

Président du
Conseil Scientifique de la Faculté SMI
Dr. BOUDERBALA Mihoub

رئيس المجلس العلمي
الدكتور: بودربالة ميهوب

People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

Djilali Bounaâma University – Khemis Miliana

Faculty of Material Sciences and Computer Science

Department of Mathematics

Handout

Algebra 1: Course and Exercises with Solutions

Intended for First-Year Mathematics and Computer Science Undergraduate Students

Prepared by:

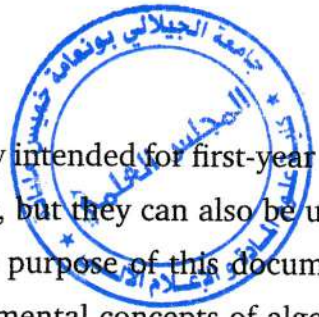
Soumia Bourchi

E-mail: s.bourchi@univ-dbkm.dz

Academic Year:

2025–2026

Preface



The present lecture notes, entitled "Algebra *I*", are primarily intended for first-year undergraduate students (L1) in Mathematics and Computer Science, but they can also be used by students of Mathematics and other scientific disciplines. The purpose of this document is to provide a rigorous and systematic introduction to the fundamental concepts of algebra that underpin much of modern computing theory and discrete mathematics.

This handout includes five chapters. Each chapter organized with definitions, properties, and theorems, and proofs, along with clear examples and exercices with solutions. The teaching method strives to develop the student's ability for abstract thinking, logical reasoning, and symbolic manipulation. Beyond its instructional objective, this work also tries to bridge the gap between pure algebra and computational applications. The Algebra 1 principles discussed here are: logical notions, set theory and application, binary relations on a set, algebraic structures, and rings of polynomials.

These handouts aim to help students understand Algebra 1 thinking required in mathematics and computer science and other sciences, and to prepare them for the study of Algebra 2.

Contents

Introduction

What is algebra? The Algebra 1 course will be devoted to an introduction to the fundamentals of mathematical structures: logical notation, sets and applications, binary relation on a set, groups, rings, fields, as well as rings of polynomials. These structures will be illustrated with examples and exercices with solutions. The most important rules and methods concerning mathematical proofs will be taught and practiced.

In computer science, algebraic thinking happens everywhere: it drives the manipulation of symbolic data, the creation of algorithms, and the precise description of computing processes.

The course Algebra 1 is designed as an introduction to these fundamental subjects. It prepares students for more challenging courses such as Algebra 2, Discrete Mathematics, and Formal Logic

The content is organized into five comprehensive chapters, as follows:

Chapter 1: Logical Concepts

- Truth table, quantifiers, types of reasoning.

Chapter 2: Sets and Applications

- Definitions and examples.
- Applications: Injections, surjection, bijection, direct image, reciprocal image, restriction and extension.

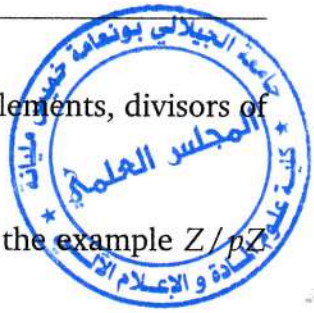
Chapter 3: Binary relations on a set

- Basic definitions: reflexive, symmetric, anti-symmetric, transitive relation.
- Order relation-Definition. Total and partial order.
- Equivalence relation: equivalence class.

Chapter 4: Algebraic structures

- Law of internal composition. Stable part. Properties of an internal composition law.
- Groups: Definitions. Subgroups: Examples-Homomorphism of groups isomorphism of groups. Examples of finite groups Z/nZ $(n = 1,2,3,\dots)$ and the permutation group S_3.

- Rings: Definition- Subrings. Calculation rules in a ring. Invertible elements, divisors of zero-Ring homomorphism and ideals.
- Fields: Definitions – Treatment of the case of a finite field through the example Z/pZ where p is prime, $\mathbb{R}$ and $\mathbb{C}$.



Chapter 5: Rings of polynomials

- Polynomial. Degree.
- Construction of the ring of polynomials.
- Arithmetic of polynomials: Divisibility, Euclidean division, gcd and lcm of two polynomials- coprime polynomials, Decomposition into product of irreducible factors.
- Roots of a polynomial: Roots and degree, Multiplicity of roots.

Chapter 1

Logical notions

This chapter is using logical connectives such as "**and**," "**or**," "**not**," "**if... then**," and "**if and only if**," . It also presents key proof techniques, including **direct proof**, **proof by contrapositive**, **proof by contradiction**, **mathematical induction**, **proof by cases**, and **counterexamples**.

1.1 Foundations of Logic

1.1.1 Basic Definitions

Definition 1.1.1. *A **proposition** (or **statement**) is a declarative statement which is true or false, but not both.*

Remark 1.1.2. *A statement has two logical values : **T** or **1** when the statement is true, **F** or **0** when the statement is false.*

Example 1.1.3. *Consider the following sentences:*

1. *"$2+2=4$"; a proposition true.*
2. *"$2+3=7$"; a proposition false.*
3. *"$7<4$"; a proposition false.*
4. *"The Earth orbits the Sun"; a proposition true.*
5. *"5 is a prime number"; a proposition true.*

6. *"Close the door!"; not a proposition.*
7. *"What time is it?"; not a proposition.*
8. *"$x+3=5$"; depends on x, not true or false.*

Remark 1.1.4. *In logic, we study only declarative sentences that have a truth value (**True** or **False**). Thus, propositions are the fundamental elements used to build more complex logical expressions.*

1.1.2 Logical connectives

From two or more propositions, new propositions can be constructed by applying logical connectives. The principal connectives in propositional logic are **negation** (**"not"**), **conjunction** (**"and"**), **disjunction** (**"or"**), **implication** (**"if ... then"**), and **equivalence** (**"if and only if"**).

Definition 1.1.5. *Let P be a proposition. The **negation** of P, denoted by $\neg P$; $\sim P$ or $\overline{P}$ and read " **not** P ", it is the proposition that is true when P is false, and false when P is true.*

Example 1.1.6. *Let:*

1. *P: "The number 5 is even". Then the negation of P is: "The number 5 is not even."or equivalently, "The number 5 is odd."*
2. *P :" $x > 3$ ". Then the negation of P is: " $x \leq 3$".*
3. *P :"Today is Sunday". Then the negation of P is: "Today is not Sunday".*
4. *P :" All students passed the exam". Then the negation of P is: "At least one student did not pass the exam".*

Definition 1.1.7. *Let P and Q be two propositions. The **conjunction** of P and Q, written $P \wedge Q$ and read " P **and** Q ", is defined as the proposition that is true if and only if both P and Q are true; otherwise, it is false.*

Example 1.1.8. *Let:*
P: "3 is an odd number" and Q: "5 is a prime number".
Then the conjunction $P \wedge Q$ is : "3 is an odd number and 5 is a prime number". This conjunction is true because both propositions are true.

Example 1.1.9. *Let:*
P: "It is raining" and Q: "I am carrying an umbrella".
Then the conjunction $P \wedge Q$ is : "It is raining and I am carrying an umbrella".
This compound proposition is true only if both P and Q are true.

Definition 1.1.10. *Let P and Q be two propositions. The* ***disjunction*** *of P and Q, written $P \vee Q$ and read " P* ***or*** *Q ", is defined as the proposition that is true if at least one of P or Q is true, and false only when both P and Q are false.*

Example 1.1.11. *Let:*

1. *$P : "6 + 5 = 16"$ and $Q : "10 > 3^3"$.*

   Then the disjunction $P \vee Q$ is: $"(6 + 5 = 16) \vee (10 > 3^3)"$ it is true because Q is true.

2. *$P : "\mathbb{Z} \subset \mathbb{N}"$ and Q:" 3 is a prime numbre".*

   Then the disjunction $P \vee Q$ is: "($\mathbb{Z} \subset \mathbb{N}$) $\vee$ (3 is a prime numbre)" is true because both propositions are true.

Example 1.1.12. *Let:*
P : "It is raining" and Q : "It is windy".
Then the disjunction $P \vee Q$ is: "It is raining or it is windy."
This statement is true if at least one of the two conditions holds (raining or windy), and false only when neither is true.

Definition 1.1.13. *Let P and Q be two propositions. The* ***implication****, written $P \Longrightarrow Q$ and read " **if** P, **then** Q", is defined as the proposition that is false only in the case where P is true and Q is false, and true in all other cases.*

Example 1.1.14. *Let:*
P : " x is an even number " and Q : " x is divisible by 2 ".
Then the implication $P \Longrightarrow Q$ is : " If x is an even number, then x is divisible by 2."
This implication is true whenever P is false or Q is true. It is false only when P is true and Q is false.

Example 1.1.15. *Let:*
P : "It is raining" and Q : "The ground is wet"
Then the implication $P \Longrightarrow Q$ is : "If it is raining, then the ground is wet."
This statement is false only when it is actually raining (P true) but the ground is not wet (Q false). In all other situations, the implication is considered true.

Definition 1.1.16. *Let P and Q be two propositions. The **equivalence** between P and Q, denoted by $P \iff Q$ and read " P if and only if Q," is defined as the proposition that is true when P and Q have identical truth values (both true or both false), and false otherwise.*

Example 1.1.17. *Let:*
P : "It is raining" and Q : "The ground is wet"
The equivalence $P \iff Q$ is:" It is raining if and only if the ground is wet."
This statement is true when both propositions have the same truth value: both are true, or both are false.

Example 1.1.18. *Let:*
P : "x is an even number" and Q : "x is divisible by 2".
Then the equivalence $P \iff Q$ is: "x is an even number if and only if x is divisible by 2".
This proposition is true because both P and Q have the same truth value for any integer x.

1.1.3 Truth Tables

Given a set of propositional variables, such as P, Q and R, suppose the truth values of P, Q and R are False (F) and True (T) respectively.
The truth value of a complex proposition depends on that of its simpler ones.
To systematically represent and analyze these relationships, we use truth tables, which display all possible combinations of truth values for the component propositions and the resulting truth value of the entire logical
The truth table of a statement P, is given by the table:

p
T (or 1)
F (or 0)

The truth table of a statement negation $\overline{P}$, is given by the table:

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

The truth table of a statement conjunction $P \wedge Q$, is given by the table:

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

The truth table of a statement disjunction $P \vee Q$, is given by the table:

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

The truth table of a statement implication $P \Longrightarrow Q$, is given by the table:

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

The truth table of a statement equivalence $P \Longleftrightarrow Q$, is given by the table:

P	Q	P$\Longleftrightarrow Q$
1	1	1
1	0	0
0	1	0
0	0	1

1.1.4 Logical Equivalences

Proposition 1. *Let P, Q and R be logical propositions:*

1. $(P \wedge Q) \Longleftrightarrow (Q \wedge P)$ *(commutativity of and).*
2. $(P \vee Q) \Longleftrightarrow (Q \vee P)$ *(commutativity of or).*
3. $[(P \wedge Q) \wedge R] \Longleftrightarrow [P \wedge (Q \wedge R)]$*(associativity of and).*

4. $[(P \vee Q) \vee R] \iff [P \vee (Q \vee R)]$ *(associativity of or)*
5. $[(P \wedge Q) \vee R] \iff [(P \vee R) \wedge (Q \vee R)]$ *(distributiveness of and with respect to or)*.
6. $[(P \vee Q) \wedge R] \iff [(P \wedge R) \vee (Q \wedge R)]$ *(distributiveness of or with respect to and)*.
7. $\overline{(P \wedge Q)} \iff \overline{P} \vee \overline{Q}$ *(morgan's laws)*
8. $\overline{(P \vee Q)} \iff \overline{P} \wedge \overline{Q}$ *(morgan's laws)*.
9. $(P \Longrightarrow Q) \iff (\overline{P} \vee Q)$ *(implication equivalence)*.
10. $(P \Longrightarrow Q) \iff (\overline{Q} \vee \overline{P})$ *(Contrapositive's laws)*
11. $\overline{\overline{P}} \iff Q$.
12. $(P \wedge P) \iff P$.
13. $(P \vee P) \iff P$.
14. $(P \iff Q) \iff (P \Longrightarrow Q \wedge Q \Longrightarrow P)$.

Proof. By truth table: 5.

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

9.

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

■

1.2 Quantifiers

Definition 1.2.1. *Let E be a set. A **predicate** on E is a statement that contains one or more variables (e.g., x) such that, when each variable is replaced by a specific element of E, the statement becomes a proposition with a definite truth value (true or false). We usually denote predicates by $P(x)$, $Q(x)$ and $R(x)$, ... etc.*

Example 1.2.2. *Let $E = \mathbb{Z}$ (the set of integers). Define the predicate.*

$$P(x) : "x \ \ is \ \ even".$$

Here, x is a variable ranging over $\mathbb{Z}$. If we replace x by a specific integer:

1. *$P(4)$: "4 is even". It is true.*
2. *$P(7)$: "7 is even". It is false.*

Thus, $P(x)$ is a predicate, and for each $x \in E$, $P(x)$ becomes a proposition.

1.2.1 Universal quantifier

Definition 1.2.3. *The universal quantifier, represented by the symbol "$\forall$", expresses the idea of "**for every**", "**for all**", or "**for any**" element of a given set. Symbolically, we write:*

$$\forall x \in E, \quad P(x).$$

which reads as "for all x in E, $P(x)$ is true." .

Example 1.2.4. *Let $E = \mathbb{R}$ (the set of real numbers), we define*

$$P(x) : \ "\forall x \in \mathbb{R}, \quad x^2 \geq 0".$$

This means "for all real numbers x, the square of x is greater than or equal to 0." This statement is true.

1.2.2 Existential quantifier

Definition 1.2.5. *The existential quantifier, represented by the symbol "$\exists$", means "**there exists**", "**Some element**" or "**there is at least one**". Symbolically, we write:*

$$\exists x \in E, \quad P(x).$$

which reads as "there exists an x in E such that $P(x)$ is true."

Example 1.2.6. *Let $E = \mathbb{R}$ (the set of real numbers), we define*

$$P(x) : \text{"}\exists x \in \mathbb{R}, \quad x^2 = 4\text{"}.$$

This means "there exists a real number x such that $x^2 = 4$." This statement is true, because $x = 2$ and $x = -2$ both satisfy the condition.

Remark 1.2.7. *When there exists an element of E satisfying a property $P(x)$, this does not exclude the possibility that there may be several such elements. If there exists one and only one element satisfying this property, we write:*

$$\exists ! \, x \in E, \quad P(x).$$

*where the symbol $\exists !$ means **"there exists exactly one."***

Example 1.2.8. *Let $E = \mathbb{R}$ (the set of real numbers), we define*

$$P(x) : \text{"}\exists ! x \in \mathbb{R}, \quad 2x - 4 = 0\text{"}.$$

This means "there exists exactly one a real number x such that $2x - 4 = 0$." This statement is true. because exists exactly one real number $x = 2$.

1.2.3 Quantifiers Order

Universal followed by Existential

Definition 1.2.9. *Let E and F be two sets, and let $P(x,y)$ be a predicate depending on elements $x \in E$ and $y \in F$. The statement*

$$\forall x \in E,\ \exists y \in F,\ P(x,y)$$

means that for every element x in E, there exists at least one element y in F such that $P(x,y)$ is true.

- *The element y may depend on x; that is, different choices of x may correspond to different elements y satisfying $P(x,y)$.*
- *This expresses a relationship in which each element of E is associated with at least one element of F fulfilling the given property.*

Example 1.2.10. *We define:*

$$\forall x \in \mathbb{R},\ \exists y \in \mathbb{R}, \quad y = x + 1$$

For every real number x, there exists a real number y equal to $x + 1$. Here, y depends on x; for each x, we can find a corresponding y. For example:

$$x = 2 \Rightarrow y = 3, \quad x = -1 \Rightarrow y = 0.$$

This statement is true because we can always choose $y = x + 1$.

Existential followed by Universal

Definition 1.2.11. *Let E and F be two sets, and let $P(x,y)$ be a predicate depending on elements $x \in E$ and $y \in F$. The statement*

$$\exists y \in F,\ \forall x \in E,\ P(x,y)$$

means that there exists at least one element y in F such that, for every element x in E, the statement $P(x,y)$ is true.

- *In this case, the same y must work for all x; that is, y does not depend on x.*

- *This expresses a relationship in which there is at least one element of F that satisfies the property $P(x,y)$ for every element of E simultaneously.*

Example 1.2.12. *We define:*

$$\exists y \in \mathbb{R},\ \forall x \in \mathbb{R}, \quad y = x + 1.$$

This means "a single y satisfies $y = x + 1$ for every x". This is false, because y would have to change with x. No single y can satisfy this equality for all x in $\mathbb{R}$.

Example 1.2.13. *We give two proposition following:*

1. $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R}, \quad y > x.$

   For every real number x, there exists a number y greater than x. True, since we can choose $y = x + 1$.

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

   There exists one number y that is greater than all real numbers. False, since no such largest real number exists.

Negation of Quantified Propositions

When we negate a statement containing a quantifier, we must switch the quantifier and negate the predicate.

1. $\overline{\forall x \in E, \quad P(x)} \Longleftrightarrow \exists x \in E, \quad \overline{P(x)}.$
2. $\overline{\exists x \in E, \quad P(x)} \Longleftrightarrow \forall x \in E, \quad \overline{P(x)}.$
3. $\overline{\forall x \in E,\ \exists y \in F, \quad P(x,y)} \Longleftrightarrow \exists x \in E, \forall y \in F, \quad \overline{P(x,y)}.$
4. $\overline{\forall x \in E\ , \exists y \in F, \quad P(x,y)} \Longleftrightarrow \exists x \in E, \forall y \in F, \quad \overline{P(x,y)}.$

Example 1.2.14. *We give two proposition following:*

1. $\overline{\forall x \in \mathbb{R}, \quad x > 0} \Longleftrightarrow \exists x \in \mathbb{R}, \quad x \leq 0.$
2. $\overline{\exists n \in \mathbb{Z},\ (n\ is\ even) \wedge (n\ is\ prime)} \Longleftrightarrow$

$\forall n \in \mathbb{Z},\ (n\ is\ not\ \ even) \vee (n\ is\ not\ prime).$

1.3 Method of proof

A method of proof is a sequence of logical steps, where each step follows clearly from the previous ones, and the last step validates the statement we want to prove. A proof must prove that the statement is true in every possible case, with no exceptions. In this section, we will study types of proofs, with examples to illustrate each method.

1.3.1 Direct proof

Definition 1.3.1. *A **direct proof** is a logical method used to demonstrate that a mathematical statement of the form*

$$P \Longrightarrow Q$$

is true. In a direct proof:

1. *Assume the hypothesis P is true.*
2. *Use logical deductions, algebraic manipulations, or properties to derive new results.*
3. *Conclude that the statement Q follows from P.*

Exercice 1. *Prove that if n is even, then n^2 is even.*

Solution. *Assume that the integer n is even. There exists an integer k such that $n = 2k$. Compute n^2:*

$$\begin{aligned} \exists k \in \mathbb{Z},\ n = 2k &\Longrightarrow n^2 = (2k)^2 = 4k^2 \\ &\Longrightarrow n^2 = 2(2k^2) \\ &\Longrightarrow n^2 = k' \text{ such that } k' = 2k^2. \end{aligned}$$

Since $2k^2$ is an integer, n^2 is even. Therefore, if n is even, then n^2 is even.

1.3.2 Proof by contrapositive

Definition 1.3.2. *A **proof by contrapositive** is a logical method used to prove a conditional statement of the form*

$$[P \Longrightarrow Q] \Longleftrightarrow [\overline{Q} \Longrightarrow \overline{P}]\,.$$

is true. In a proof by contrapositive:

1. *Assume that the conclusion Q is false (i.e., assume $\overline{Q}$).*
2. *Use logical reasoning and known results to show that the hypothesis P must also be false (i.e., deduce $\overline{P}$).*
3. *Conclude that $P \Longrightarrow Q$ is true.*

Exercice 2. *Prove that if n^2 is even, then n is even.*

Solution. *Contrapositive form: If n is odd, then n^2 is odd.*
Assume that the integer n is odd. Compute n^2:

$$\begin{aligned} \exists k \in \mathbb{Z},\ n = 2k+1 &\Longrightarrow n^2 = (2k+1)^2 = 4k^2 + 2k + 1 \\ &\Longrightarrow n^2 = 2(2k^2 + k) + 1 \\ &\Longrightarrow n^2 = 2k' + 1 \text{ such that } k' = 2k^2 + k. \end{aligned}$$

So n^2 is odd. Therefore, if n is odd, then n^2 is odd.
Since the contrapositive is true, the original statement, "if n^2 is even, then n is even" is also true.

1.3.3 Proof by contradiction

Definition 1.3.3. *A **proof by contradiction**, also called a **proof by absurdity**, it is a logical method used to show that a statement is true by assuming that it is false, and then deriving a contradiction. In contradiction proof:*

1. *Assume the opposite (the negation) of what you want to prove. That is, assume $\overline{P}$.*
2. *Use logical reasoning, known facts, and algebraic or set-theoretic properties to deduce new consequences. Arrive at a contradiction, such as a false statement a conflict with a known theorem.*
3. *Conclude that the initial assumption $\overline{P}$ is false, therefore P must be true*

Exercice 3. *Prove that $\sqrt{2}$ is irrational.*

Solution. *Let P be the statement: "$\sqrt{2}$ is irrational."*
We prove P by contradiction. Suppose that P is false, i.e., assume that: " $\sqrt{2}$ is rational". Then there exist integers a and $b \neq 0$ with no common factors such that

$$\begin{aligned}
\sqrt{2} = \frac{a}{b} &\implies a^2 = 2b^2 \\
&\implies a^2 \text{ is even} \\
&\implies a \text{ is even} \\
&\implies a = 2c, \text{ for some } c \in \mathbb{Z} \\
&\implies (2c)^2 = 2b^2 \\
&\implies 4c^2 = 2b^2 \\
&\implies 2c^2 = b^2 \\
&\implies b^2 \text{ is even} \\
&\implies b \text{ is also even}
\end{aligned}$$

This contradicts the assumption that a and b have no common factors. Therefore, $\sqrt{2}$ is irrational.

1.3.4 Proof by induction

Definition 1.3.4. *A **proof by mathematical induction** is a method used to prove that a statement $P(n)$ is true for all integers $n \geq n_0$ where n_0 is a starting integer (usually 0 or 1), follow these three steps:*

1. ***Base Case (Initial Step)**: Verify that $P(n_0)$ is true.*
2. ***Inductive Step**: Assume that $P(k)$ is true for some integer $k \geq n_0$. And, prove that $P(k+1)$ is also true, using the assumption that $P(k)$ holds.*
3. ***Conclusion**: by the principle of mathematical induction, $P(n)$ is true for all integers $n \geq n_0$.*

Exercice 4. *Prove that for all integers $n \geq 1$,*

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

Solution. 1. *Base case* $(n = 1)$

Left-hand side: 1. *And right-hand side:* $\frac{1(1+1)}{2} = 1$. *So true for* $n = 1$.

2. *Assume that the statement is true for* $n = k$; *that is,*

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

Now, prove it for $n = k + 1$. *Add* $(k + 1)$ *to both sides:*

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

Simplify the right-hand side:

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

Hence, the formula is true for $n = k + 1$.

3. *By the Principle of Mathematical Induction,*

$$1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}; \quad \forall n \geq 1.$$

It is true.

1.3.5 Proof by cases

Definition 1.3.5. *A* ***proof by cases****, also called* ***reasoning by exhaustion****, it is a logical method used to prove a statement by dividing all possible cases into a finite number of possibilities. Follow theses steps:*

1. *Identify all possible cases the given problem.*
2. *Prove that the statement is true in each case.*
3. *Conclude that since all cases the statement being true, the statement is true in general.*

Exercice 5. *Prove that for every integer* n, $n^2 \geq 0$.

Solution. *We consider two possible cases for* n :

- ***Case 1:*** $n \geq 0$.

  Then $n^2 = n \times n \geq 0$ *since the product of two non-negative numbers is non-negative.*

- ***Case 2:*** $n < 0$.

  Then $n = -k$ *for some positive integer* k. *Hence,* $n^2 = (-k)^2 = k^2 \geq 0$.

Therefore, for all integers n, $n^2 \geq 0$.

1.3.6 Proof by counter-example

Definition 1.3.6. *A* ***proof by counter-example*** *is a logical method used to disprove a universal statement of the form* $\forall x \in E,\ P(x)$, *which means "for all* x *in* E, *the property* $P(x)$ *is true".*
To disprove such a statement, it is sufficient to find a single example $x_0 \in E$ *for which* $P(x_0)$ *is false. This* x_0 *is called a counter-example*

Exercice 6. *Statement: "For all integers* n, $n^2 + n + 41$ *is a prime number".*

Solution. *Let* $n = 40$. *Then:* $(40)^2 + 40 + 41 = 1681 = 41 \times 41$. *which is not prime. Thus, the statement is false.*

1.4 Exercises with solutions

Exercice 7. *Determine the truth value of the following statements in* $\mathbb{R}$*:*

1. $\forall x\ , \exists y : x + y = 0$.
2. $\exists y\ , \forall x : x + y = 0$.
3. $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ xy = 1$.
4. $\exists x \in \mathbb{R},\ x^2 + 1 = 0$.

Solution.

1. *True, since for each* x, *we can take* $y = -x$.
2. *False, since no single* y *satisfies the equation for all* x.
3. *False. For* $x \neq 0$, *we can take* $y = \frac{1}{x}$, *but for* $x = 0$, *there is no* y *such that* $0 \cdot y = 1$.

4. *False. Solving $x^2 + 1 = 0$ gives $x^2 = -1$, which has no real solution.*

Exercice 8. *Form the negation of the following propositions.*

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

Solution. *1.*

$$\begin{aligned} \neg\big(\neg(P \vee Q) \vee [(P \Rightarrow Q) \wedge R]\big) &= (P \vee Q) \wedge \neg\big((P \Rightarrow Q) \wedge R\big) \\ &= (P \vee Q) \wedge \big(\neg(P \Rightarrow Q) \vee \neg R\big) \\ &= (P \vee Q) \wedge \big((P \wedge \neg Q) \vee \neg R\big) \end{aligned}$$

2.

$$\begin{aligned} \neg\big([(P \vee Q) \vee R] \Rightarrow (P \wedge R)\big) &= [(P \vee Q) \vee R] \wedge \neg(P \wedge R) \\ &= [(P \vee Q) \vee R] \wedge (\neg P \vee \neg R) \end{aligned}$$

3.

$$\begin{aligned} \neg\big((P \wedge \neg Q) \Leftrightarrow R\big) &= (P \wedge \neg Q \wedge \neg R) \vee (\neg(P \wedge \neg Q) \wedge R) \\ &= (P \wedge \neg Q \wedge \neg R) \vee ((\neg P \vee Q) \wedge R) \end{aligned}$$

Exercice 9. *Write the following sentences using quantifiers:*

1. *"Every even number is divisible by 2."*
2. *"There exists a number whose square is equal to 9".*
3. *"Every natural number is greater than or equal to zero".*
4. *"There exists a real number whose cube equals one".*
5. *"There exists an integer that is both even and prime".*

Solution. *Using quantifiers:*

1. $\forall x \in \mathbb{Z}$, *n is even* $\Longrightarrow$ *n is divisible by 2.*

2. $\exists x \in \mathbb{R},\ x^2 = 9$.

3. $\forall x \in \mathbb{N},\ n \geq 0$.

4. $\exists x \in \mathbb{R},\ x^3 = 1$.

5. $\exists x \in \mathbb{Z}, (n \text{ is even}) \wedge (n \text{ is prime})$.

Exercice 10. *Answer the following questions using direct reasoning.*

1. *Proof that if $a, b \in \mathbb{Q}$, then $ab \in \mathbb{Q}$.*

2. *Show that if m and n are both odd numbers, then mn is odd.*

Solution. 1. *Let $a, b \in \mathbb{Q}$, we can write:*

$$a = \frac{p_1}{q_1}, \quad b = \frac{p_2}{q_2},$$

where $p_1, p_2 \in \mathbb{Z}$ and $q_1, q_2 \in \mathbb{N}$ (or $q_1, q_2 \neq 0$).

Now consider the product:

$$ab = \frac{p_1}{q_1} \times \frac{p_2}{q_2} = \frac{p_1 p_2}{q_1 q_2}.$$

The numerator $p_1 p_2$ is an integer because the product of two integers is an integer. The denominator $q_1 q_2$ is a positive integer because the product of two positive integers is positive.

Therefore,

$$ab = \frac{p_1 p_2}{q_1 q_2},$$

where $p_1 p_2 \in \mathbb{Z}$ and $q_1 q_2 \in \mathbb{N}$. Thus $ab \in \mathbb{Q}$.

2. *Since m is odd, there is an integer j such that $m = 2j + 1$. Similarly, since n is odd, there is an integer k such that $n = 2k + 1$.*

$$\begin{aligned} mn &\implies (2j+1)(2k+1) \\ &\implies 4jk + 2j + 2k + 1 \\ &\implies 2(2jk + j + k) + 1 \end{aligned}$$

As j and k were integers, $2jk + j + k$ is also an integer. Hence, we have found an integer, $p = 2jk + j + k$ such that $mn = 2p + 1$. This implies that mn is odd.

Exercice 11. *The aim of this exercise is to use contrapositive reasoning.*

1. *Prove if a^2 is divisible by 3, then a is divisible by 3.*
2. *Suppose a, b and c are all real numbers and $a > b$. Show that if $ac \leq bc$ then $c \leq 0$.*

Solution. 1. *If a is not divisible by 3, then a^2 is not divisible by 3.*

Let $a = 3k + r$ with $r = 1$ or 2:

$$a^2 = (3k + r)^2 = 9k^2 + 6kr + r^2 = 3(3k^2 + 2kr) + r^2$$

For $r = 1$ or 2, r^2 gives remainder 1. Thus, a^2 is not divisible by 3.

2. *Note that the contrapositive of the statement, if $ac \leq bc$ then $c \leq 0$ is the statement, if $c > 0$, then $ac > bc$. Since we know $a > b$, multiplying both sides of the inequality by the positive number c does not change the direction of the inequality, so $ac > bc$. Thus if $ac \leq bc$ that means that $c \leq 0$.*

Exercice 12. *The aim of this exercise is to use contradiction reasoning.*

1. *Proof if n is an integer such that $n + m = m = m + n$ for every $m \in \mathbb{Z}$, then $n = 0$.*
2. *Prove that there is no smallest positive rational number.*

Solution. 1. *Suppose not. There is an integer $n \neq 0$ such that $n + m = m = m + n$ for all integers m. Then $n + 0 = 0$. Since 0 is the additive identity, then $n + 0 = n$. This implies $n = 0$ which is a contradiction since $n \neq 0$ and $n = 0$ can't both be true at the same time. Hence, our assumption $n \neq 0$ can never hold and n must be 0.*

2. *Suppose, for the sake of contradiction, that there exists a smallest positive rational number, say r. Since $r > 0$ and $r \in \mathbb{Q}$, the number*

$$\frac{r}{2}$$

is also a positive rational number.

Moreover,

$$0 < \frac{r}{2} < r,$$

which contradicts the assumption that r is the smallest positive rational number. Therefore, our assumption is false.

Exercice 13. *Prove the following properties using the principle of mathematical induction.*

1. *For all $n \in \mathbb{N}$, we have: $2^n \geq n$.*
2. *For all $n \in \mathbb{N}$, we have: $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.*
3. *Show that $3^n - 1$ is a multiple of 2 for all $n \in \mathbb{N}$*
4. *Show that for all natural numbers n, $\sum_{i=1}^{n}(2i-1) = n^2$.*

Solution. 1. *Let $P(n)$ be the statement $P(n)$: $2^n \geq n$. We prove by mathematical induction that $P(n)$ is true for all $n \in \mathbb{N}$.*

Step 1. *For $n = 0$, we have $2^0 = 1 \geq 0$. Thus, $P(0)$ is true.*

Step 2. *Assume that $P(n)$ is true for some $n \in \mathbb{N}$, that is,*

$$2^n \geq n.$$

We show that $P(n+1)$ is also true. We have

$$2^{n+1} = 2 \cdot 2^n.$$

Using the induction hypothesis, we obtain $2^{n+1} \geq 2n$. Since $2n \geq n+1$ for all $n \in \mathbb{N}$, it follows that

$$2^{n+1} \geq n+1.$$

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

Step 3. *By the principle of mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$.*

2. ***Step 1.*** *For $n = 1$, we have $1^2 = \dfrac{1(1+1)(2+1)}{6} = 1$. Thus, $P(1)$ is true.*

Step 2. *Assume that $P(n)$ is true for some $n \in \mathbb{N}$, that is,*

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

We show that $P(n+1)$ is also true. Then for $n = k+1$:

$$1^2 + \cdots + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2$$

$$= \frac{(k+1)(2k^2+7k+6)}{6} = \frac{(k+1)(k+2)(2k+3)}{6}$$

Hence true for all $n \in \mathbb{N}$.

Step 3. *By the principle of mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$.*

3. ***Step 1.*** *For $n = 1$, we have $3^1 - 1 = 3 - 1 = 2$, which is a multiple of 2. So the statement is true for $n = 1$.*

   Step 2. *Assume that $3^n - 1$ is a multiple of 2 for some $n \in \mathbb{N}$, i.e.,*

   $$3^n - 1 = 2k \quad \text{for some } k \in \mathbb{Z}.$$

   We want to show that $3^{n+1} - 1$ is also a multiple of 2. We have

   $$\begin{aligned} 3n - 1 = 2k &\implies 3n \times 3 - 1 \times 3 = 2k \times 3 \\ &\implies 3n \times 3 - 3 = 2k \times 3 \\ &\implies 3^{n+1} - 1 = 2 + 2k \times 3 \\ &\implies 3^{n+1} - 1 = 2(1 + k \times 3) \\ &\implies 3^{n+1} - 1 = 2k' \text{ such that } k' = 1 + k \times 3 \end{aligned}$$

   Hence, $3^{n+1} - 1$ is a multiple of 2.

   Step 3. *By the principle of mathematical induction, for all $n \in \mathbb{N}$,*
   $3^n - 1$ is a multiple of 2.

4. ***Step 1.*** *For $n = 1$, we have $\sum_{i=1}^{1}(2i - 1) = 2 \cdot 1 - 1 = 1 = 1^2$. Thus, the statement is true for $n = 1$.*

   Step 2. *Assume that the statement is true for some $k \in \mathbb{N}$, that is,*

   $$\sum_{i=1}^{k}(2i - 1) = k^2.$$

   We must show that it is true for $k + 1$. We compute:

   $$\sum_{i=1}^{k+1}(2i - 1) = \left(\sum_{i=1}^{k}(2i - 1)\right) + \big(2(k + 1) - 1\big).$$

   Using the induction hypothesis, we obtain:

   $$\sum_{i=1}^{k+1}(2i - 1) = k^2 + (2k + 1) = k^2 + 2k + 1 = (k + 1)^2.$$

Hence, the statement is true for $k+1$.

Step 3. *By the principle of mathematical induction, $\sum_{i=1}^{n}(2i-1) = n^2$, $\forall n \in \mathbb{N}$.*

Exercice 14. *Demonstrate the following properties using a proof by cases.*

1. *Show that $n^2 - n$ is even for all integers n.*
2. *$|x-1| \leq x^2 - x + 1$.*

Solution. 1. *Let $x \in \mathbb{R}$. We consider two cases.*

Case 1: *$n = 2k$ (even) $n^2 - n = 2(2k^2 - k)$.*

Case 2: *$n = 2k+1$ (odd) $n^2 - n = 2(2k^2 + k)$.*

In both cases, the result is even.

2. *Let $x \in \mathbb{R}$. We consider two cases.*

Case 1: *$x \geq 1$. In this case, $|x-1| = x-1$. We compute:*

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

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

Case 2: *$x < 1$. In this case, $|x-1| = -(x-1)$. We obtain:*

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

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

In all cases, $|x-1| \leq x^2 - x + 1$.

Exercice 15. *This exercise aims at finding a counter-example.*

1. *Disprove: "For all real numbers x, y, if $x^2 = y^2$, then $x = y$."*
2. *Prove that " If n is an integer and n^2 is divisible by 4, then n is divisible by 4" is false.*

Solution. 1. *Counter example: $x = 2, y = -2$. Then $x^2 = y^2 = 4$ but $x \neq y$. Hence, the statement is false.*

2. *Consider $n = 6$. Then $n^2 = 36$ is divisible by 4, but $n = 6$ is not divisible by 4. Thus, $n = 6$ is a counter example to the statement.*

Chapter 2

Sets and Applications

A **set** is a well-defined collection of distinct objects, while an **application** (or **function**) is a mapping from one set to another that assigns to each element of the first set a unique element of the second. Sets and applications form the foundational language of mathematics.

2.1 Definitions and examples

Definition 2.1.1. *A **set** is any collection of distinct and well-defined objects. The objects are called the **elements of the set**. Generally the name of the set is given using capital letters $E,F,G,H,I\ldots$. The **members** or **elements of the set** are shown by using small letters $x,y,z,\ldots$.*

1. *If x is an element of E, we write $x \in E$.*
2. *If x is not an element of E, we write $x \notin E$.*

Example 2.1.2. *(**Common sets**). We use the following standard symbols:*

1. *U is the universal set*
2. $\mathbb{N} = \{0,1,2,3,\ldots\}$ *(Set of Natural numbers);*
3. $\mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$ *(Set of Integers);*
4. $\mathbb{Q} = \left\{ \frac{p}{q} \ : \ p \in \mathbb{Z} \ ; q \in \mathbb{N}^* \right\}$ *(Set of Rational numbers);*
5. $\mathbb{R}$ *(Set of Real numbers.)*
6. $\mathbb{C} = \{b + ib \mid a,b \in \mathbb{R}, i^2 = -1\}$ *(Set of Complex numbers).*

2.1.1 Methods of writing sets

There are two methods of writing set.

1. **Listing Method (Roster Method)**

   In this method, all the elements of a set are listed explicitly. Each element is written only once and separated by commas. The order of elements is not important, but it is necessary to include "all elements" of the set.

   For example, the set of even numbers between 1 and 9 can be written as

   $$A = \{2,4,6,8\} \quad \text{or} \quad A = \{4,8,2,6\}.$$

   If an element occurs more than once, it is usual to write it only once. For example, in the word "committee," the letters

   $$A = \{c,o,m,i,t,e\}.$$

2. **Rule Method (Set-Builder Form)**

   In this method, we use a variable and a rule to describe elements, rather than listing them all, followed by a vertical bar or colon, and state the property that elements must satisfy.

   For example,

   $$A = \{x \mid x \in \mathbb{N}, 2 < x < 20\}$$

   is read as "Set A is the set of all x such that x is a natural number between 2 and 20."

   Another example,

   $$B = \{x \mid x \text{ is a prime number between 1 and 10}\},$$

   represents the set of all prime numbers between 1 and 10. Using the listing method, set B can be written as

   $$B = \{2,3,5,7\}.$$

The set of rational numbers $\mathbb{Q}$ can also be expressed in set-builder form as

$$\mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z},\ q \in \mathbb{N}^* \right\},$$

and read as "$\mathbb{Q}$ is the set of all numbers of the form $\frac{p}{q}$ where q is a non-zero natural number."

Example 2.1.3.

Rule method or Set builder form	*Listing method or Roster method*
$E = \{x \mid x \text{ is a letter of the word 'LISTEN'.}\}$	$E = \{L, I, S, T, E, N\}$
$F = \{y \mid y \text{ is a number such that } y^2 = 4\}$	$F = \{-2, 2\}$
$G = \{z \mid z \text{ is a multiple of } 2 \text{ and is less than} 10\}$	$G = \{2, 4, 6, 8, 10\}$

2.1.2 Types of sets

Definition 2.1.4. *A set consisting of a single element is called a* ***singleton set****.*

Example 2.1.5. *Let $E = \{2\}$, E is the set of even prime numbers.*

Definition 2.1.6. *If there is not a single element in the set which satisfies the given condition then it is called a* ***null set*** *or an* ***empty set****. Null set is represented by $\{\}$ or a symbol "$\emptyset$".*

Example 2.1.7. *Let $E = \{x \mid x$ is natural number between 3 and 4.$\}$ or write $E = \{\}$ or $\emptyset$.*

Definition 2.1.8. *If a set is a null set or number of elements are limited and countable then it is called as "****finite set****".*

Example 2.1.9. *Let $E = \{1, 2, 3, 5, 6\}$ is finite set.*

Definition 2.1.10. *If number of elements in a set is unlimited and uncountable then the set is called "****infinite set****".*

Example 2.1.11. *Let $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is infinite set.*

Definition 2.1.12. *Let E be a finite set. The number of elements in E is called the* ***cardinal*** *(or* ***cardinality****) of E, and it is denoted by $\text{card}(E)$ or $|E|$.*
Otherwise, if the number of elements does not exist, the set is said to be ***infinite****.*

Example 2.1.13. *Let $E = \{x \in \mathbb{N} : 0 \leq x \leq 5\} = \{0, 1, 2, 3, 4, 5\}$. Then $\text{card}(E) = 6$.*

Remark 2.1.14.

- *The cardinality of empty set is* $card(\varnothing) = 0$.
- *The cardinality of singleton is* 1.

Definition 2.1.15. *Let E be a set. The subsets of E form a set called the* ***power set*** *of E, denoted by $\mathcal{P}(E)$:*

$$\mathcal{P}(E) = \{x \mid x \subseteq E\}.$$

Proposition 2. *Let E be a set of a set U. If E is a finite set with $card(E) =\mid n \mid$, then*

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

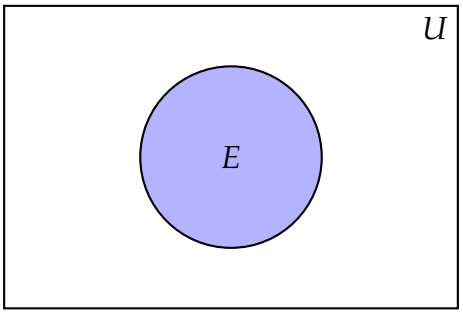
Example 2.1.16. *Let $E = \{1,2,3\}$. Then* $\text{card}(E) = 3$ *and* $\text{card}(\mathcal{P}(E)) = 8$. *Indeed,*

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

2.2 Set Operations

Venn diagrams

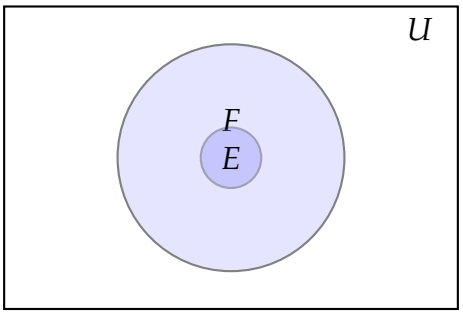
British logician John Venn was the first to use closed figures to represent sets. Such representations are called "**Venn diagrams**". Venn diagrams are very useful, in order to understand and illustrate the relationship among sets and to solve the examples based on the sets.
Let E is set of a set U.



2.2.1 Subset and Equality

Definition 2.2.1. *Let E and F be two sets of a set U. We say that E is **included** in F, or that E **contains** F, or that E is a **subset** of E (written $E \subseteq F$) if every element of E is also an element of F. That is,*

$$E \subseteq F \iff \forall x : x \in E \text{ such that } x \in F.$$



Example 2.2.2. *Let $E = \{1,2,3\}$ and $F = \{1,2,3,4\}$. Then $E \subseteq F$ but $E \neq F$.*

Definition 2.2.3. *Let E and F be two sets of a set U. We say that a set E is **not included** in a set F if there exists at least one element of E that does not belong to F. We write: $E \not\subset F$. That is,*

$$E \not\subset F \iff \exists x : x \in E \text{ such that } x \notin F.$$

Example 2.2.4. *Let $E = \{1,2,3\}$ and $F = \{2,3,4\}$. Then, $E \not\subset F$. Because $1 \in E$ but $1 \notin F$.*

Definition 2.2.5. *Let E and F be two sets of a set U. We say two sets E and F are **equal** if they have the same elements. That is,*

$$E = F \iff E \subseteq F \wedge F \subseteq E.$$

Example 2.2.6. *Let $E = \{1,5,5,5,3,3,1\}$ and $F = \{1,3,5\}$. Then $E = F$.*

Example 2.2.7. *Let*

$$E = \{x \in \mathbb{R} :| x - 1 | \leq 1\}, \quad F = [0,2], \quad G = [0,2[.$$

We have:

$$E = F, \quad E \neq G, \quad F \neq G, \quad G \subseteq F.$$

Proposition 3. *Let E and F be subsets of a set U. Then:*

1. *Every set is a subset of itself. i.e. $E \subseteq E$.*
2. *Empty set is a subset of every set i.e. $\emptyset \subseteq E$.*

3. *If* $E \subseteq F$ *and* $F \subseteq E$, *then* $E = F$.

4. *If* $E = F$, *then* $E \subseteq F$ *and* $F \subseteq E$.

5. *If* $E \subseteq F$ *and* $\text{card}(E) = \text{card}(F)$, *then* $E = F$.

6. *If* $E \subseteq F$; $\text{card}(E) = \text{card}(U) - \text{card}(F)$.

Definition 2.2.8. *Let* E *and* F *be two sets of a set* U. *We say* E *is a* ***proper subset*** *of* F *if and only if* $E \subseteq F$ *and* $E \neq F$. *This is denoted by* $E \subset F$. *That is,*

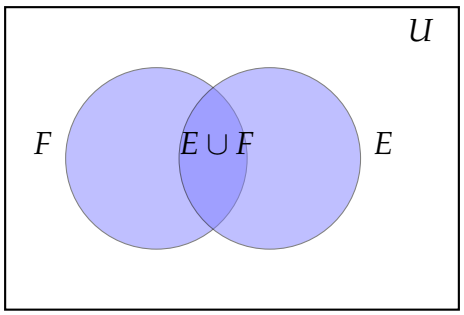
$$E \subset F \iff \forall x : (x \in E \text{ such that } x \in F) \wedge \exists x : (x \notin E \wedge x \in F).$$

2.2.2 Union and Intersection

Definition 2.2.9. *Let* E *and* F *be subsets of a set* U. *The* ***union*** *of* E *and* F, *denoted* $E \cup F$, *is the set of all elements* x *such that* $x \in E$ *or* $x \in F$. *In other words,*

$$x \in E \cup F \iff x \in E \text{ or } x \in F.$$

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



Proposition 4. *Let* E, F, *and* H *be subsets of a set* U. *Then:*

1. $E \cup F = F \cup E$ *and* $(E \cup F) \cup H = E \cup (F \cup H)$

2. $E \subseteq E \cup F$ *and* $F \subseteq E \cup F$

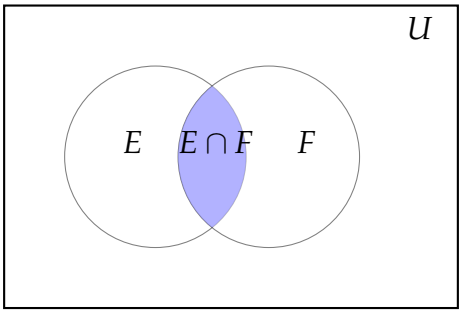
3. $E \cup \emptyset = E, \quad E \cup E = E, \quad E \cup U = U.$

Example 2.2.10. *Let* $E = \{1,3,5,7\}$; $F = \{2,3,6,8\}$. *So* $E \cup F = \{1,2,3,5,6,7,8\}$.

Definition 2.2.11. *Let E and F be subsets of a set U. The* ***intersection*** *of E and F, denoted $E \cap F$, is the set of all elements x such that $x \in E$ and $x \in F$. In other words,*

$$x \in E \cap F \iff x \in E \text{ and } x \in F.$$

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



Proposition 5. *Let E, F, and H be subsets of a set U. Then:*

1. $E \cap F = F \cap E$ *and* $(E \cap F) \cap H = E \cap (F \cap H)$
2. $E \cap (E \cup F) = E$
3. $E \cap \emptyset = \emptyset, \quad E \cap E = E, \quad E \cap U = E.$
4. $E \cap (F \cup H) = (E \cap F) \cup (E \cap H), \quad E \cup (F \cap H) = (E \cup F) \cap (E \cup H)$
5. *If E and F are finite, then:*
   - *(a)* $\text{card}(E \cup F) = \text{card}(E) + \text{card}(F) - \text{card}(E \cap F)$
   - *(b)* $\text{card}(E \cap F) \leq \min(\text{card}(E), \text{card}(F))$

Example 2.2.12. *Let $E = \{1,3,5,7\}$; $F = \{2,3,6,8\}$.*
The element 3 is common in set E and F. So $E \cap F = \{3\}$.

Definition 2.2.13. *Let E and F be two subsets of U. Two sets E and F are* ***disjoint*** *if:*

$$E \cap F = \emptyset.$$

2.2.3 Set Partition

Definition 2.2.14. *Let E is subsets of U. A collection of nonempty sets $\{E_1, E_2, ..., E_n\}$ is a* ***partition*** *of a set E if and only if: $E = E_1 \cup E_2 \cup ... \cup E_n$. $E_1, E_2, ..., E_n$ are mutually disjoint $E_i \cap E_j = \varnothing$, $i \neq j$, $i, j = 1, 2, ...n$.*

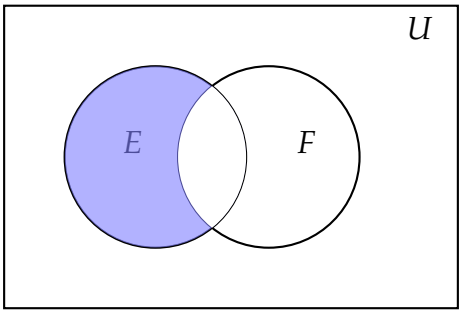
Example 2.2.15. *Let $E = \mathbb{Z}$, we have two partition:*
$E_1 = \{x \in E \mid x \ \ is \ \ even\}$.
$E_2 = \{x \in E \mid x \ \ is \ \ odd\}$.

2.2.4 Difference sets and Symmetric Difference

Definition 2.2.16. *Let E and F be two sets of the set U. The* ***difference*** *of E and F, denoted $E \setminus F$, is the set of all elements $x \in E$ such that $x \notin F$. Equivalently,*

$$x \in E \setminus F \iff x \in E \cap C_U(F).$$

$$E \setminus F = \{x \mid x \in E \ and \ x \notin F\}.$$



Proposition 6. *Let E, F, and H be subsets of a set U. Then:*

1. $E \setminus \varnothing = E, \quad E \setminus E = \varnothing, \quad \varnothing \setminus E = \varnothing.$
2. *If $E \subseteq F$, then $E \setminus F = \varnothing \iff E \subset F$.*
3. *If $E \cap F = \varnothing$, $E \setminus F = E$.*
4. $E \setminus (F \cup H) = (E \setminus F) \cap (E \setminus H), \quad E \setminus (F \cap H) = (E \setminus F) \cup (E \setminus H).$
5. *If E and F are finite we have: $card(E \setminus F) = card(E) - card(E \cap F)$.*

Example 2.2.17. *Let $U = \mathbb{R}, \quad E = [1,2], \quad F = [0,3]$*

$$E \setminus F = \varnothing, \quad F \setminus E = [0,1[\cup]2,3]$$

Definition 2.2.18. *Let E and F be two subsets of U. The* ***symmetric difference*** *of set E and set F is the set containing those elements in exactly one of E and F. denoted by:*

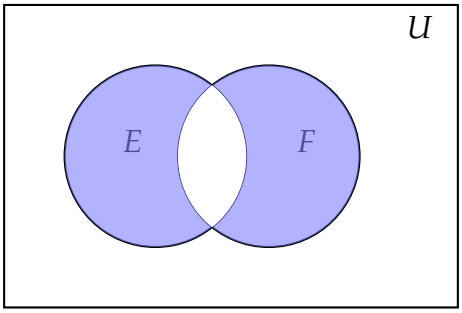
$$x \in E \triangleleft F \Longleftrightarrow \{x \in (E \setminus F) \vee x \in (F \setminus E)\}.$$

We can write:

$$E \triangleleft F = (E \setminus F) \cup (F \setminus E),$$

$$E \triangleleft F = (E \cup F) \setminus (F \cup E),$$

$$E \triangleleft F = (E \cap F^c) \cup (E^c \cap F).$$



Proposition 7. *Let E, F, and H be subsets of a set U. Then:*

1. $E \triangleleft F = F \triangleleft E, \quad E \triangleleft \emptyset = E, \quad E \triangleleft E = \emptyset.$
2. $E \triangleleft U = U \setminus E.$
3. $E \triangleleft F = \overline{E} \triangleleft \overline{F}.$
4. $(E \triangleleft F) \triangleleft H = E \triangleleft (F \triangleleft H).$
5. $E \triangleleft F = \emptyset \Longleftrightarrow (E \cup F) \setminus (F \cup E) = \emptyset \Longleftrightarrow E = F.$
6. *If E and F are finite we have:*

$$card(E \triangleleft F) = card(E) + card(F) - 2card(E \cap F).$$

Example 2.2.19. *Let* $U = \mathbb{N}, \quad E = \{0,2,3,6\}, \quad F = \{1,2,6\}$

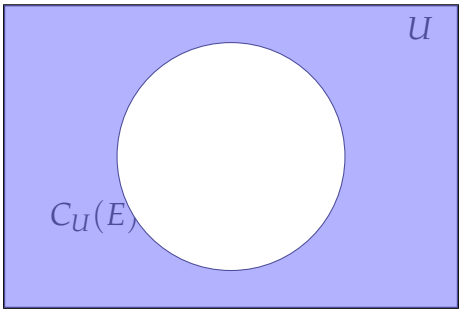
$$E \Delta F = (E \setminus F) \cup (F \setminus E) = \{0,1,3\}$$

2.2.5 Complement

Definition 2.2.20. *Let $E \subseteq U$. The* ***complement*** *of E in U, denoted $C_U(E)$; E^c or $U \setminus E$, it is the set of all elements $x \in U$ such that $x \notin E$. In other words,*

$$x \in C_U(E) \iff x \in U \text{ and } x \notin E.$$

$$C_U(E) = \{x \in U \mid x \notin E\}.$$



Proposition 8. *Let E and F be subsets of a set U. Then:*

1. $C_U(E) \subseteq U, \quad C_U(U) = \emptyset, \quad C_U(\emptyset) = U.$
2. $E \cap C_U(E) = \emptyset, \quad E \cup C_U(E) = U, \quad C_U(C_U(E)) = E.$
3. $C_U(E \cap F) = C_U(E) \cup C_U(F) = C_U(E \setminus F), \quad C_U(E \cup F) = C_U(E) \cap C_U(F).$
4. *If U is finite, then* $\text{card}(C_U(E)) = \text{card}(U) - \text{card}(E)$.

Proof. 3. For any $x \in U$:

$$x \in C_U(E \setminus F) \iff x \notin (E \setminus F) \iff x \notin E \text{ or } x \in F \iff x \in C_U(E) \cup C_U(F).$$

Thus, we have the identity: $C_U(E \setminus F) = C_U(E) \cup C_U(F)$.

■

Example 2.2.21. *Let $U = \{1,2,3,4,5,6,7\}$, $E = \{2,4,6\}$, and $F = \{1,2,3,4\}$.*

$$E \cup F = \{1,2,3,4,6\}, \quad E \cap F = \{2,4\}, \quad E \setminus F = \{6\}, \quad E^c = \{1,3,5,7\}.$$

2.2.6 Cartesian product

Definition 2.2.22. *The **Cartesian product** of two sets E and F, denoted by $E \times F$, is the set of all ordered pairs (x,y) where $x \in E$ and $y \in F$.*

$$E \times F = \{(x,y) | x \in E \wedge y \in F\}.$$

Definition 2.2.23. *The Cartesian product of n sets $E_1, E_2, ..., E_n$ denoted by $E_1 \times E_2 \times ... \times E_n$, is the set of all tuples $(x_1, x_2, ..., x_n)$ where $x_i \in E_i$ for $i = 1, ..., n$.*

Proposition 9. *If E, F, H and G are any sets, then:*

1. $E \times F \neq F \times E$.
2. $E \times \emptyset = \emptyset \times E = \emptyset$.
3. $(E \times G) \cup (F \times G) = (E \cup F) \times G$.
4. $(E \times F) \cup (E \times G) = E \times (F \cup G)$
5. $(E \times G) \cap (F \times H) = (E \cap F) \times (G \cap H)$.

Proof. 4.

$$\begin{aligned}(E \times G) \cup (F \times G) &= \{(x,y) \mid (x,y) \in E \times G \text{ or } (x,y) \in F \times G\} \\ &= \{(x,y) \mid (x \in E \text{ and } y \in G) \text{ or } (x \in F \text{ and } y \in G)\} \\ &= \{(x,y) \mid (x \in E \text{ or } x \in F) \text{ and } y \in G\} \\ &= \{(x,y) \mid x \in E \cup F \text{ and } y \in G\} \\ &= (E \cup F) \times G.\end{aligned}$$

■

Definition 2.2.24. ***(Cardinality of Cartesian product)**. In general, if E_i are finite sets, we have:*

$$| E_1 \times E_2 \times ... \times E_n | = | E_1 | \times | E_2 | \times ... \times | E_n |.$$

Example 2.2.25. *Let $E = \{1,3\}$, $F = \{2,7\}$.*

$$E \times F = \{(1,2),(1,7),(3,2),(3,7)\}.$$

2.3 Applications of Sets

Definition 2.3.1. *Given two sets E and F, and a correspondence f that assigns to each element x of E a unique element y of F, the correspondence f is called a **function** (or **mapping**) from E to F. It is denoted by:*

$$\begin{array}{rccc} f: & E & \longrightarrow & F \\ & x & \longmapsto & y = f(x) \end{array}.$$

- *The set E is called the **domain**, denoted by $Dom(f) = E$.*
- *The set F is called the **codomain**, denoted by $Codom(f) = F$.*
- *The element $x \in E$ is called the **pre-image** (or **antecedent**) of y.*
- *And $y = f(x)$ is called the **image** (or **range**) of x under f, denoted by:*
  $Im(f) = \{f(x) \mid x \in E\} \subseteq F$.

Proposition 10. *Let E and F two sets, and f is an application of E in F if and only if:*

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

or

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

Example 2.3.2.

1. *This maps each natural number n to an odd number $2n+1$.*

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

2. *This maps each real number x to its square.*

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

3. *This is the identity function on a set E.*

$$\begin{array}{rccc} \mathrm{Id}_E: & E & \longrightarrow & E \\ & x & \longmapsto & x. \end{array}$$

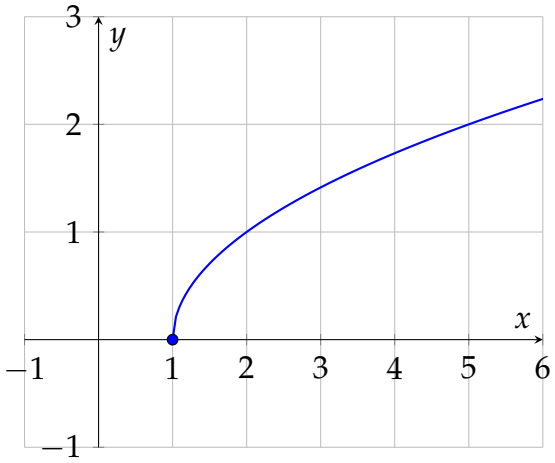
Definition 2.3.3. *Let E and F are two sets and $f : E \to F$ be a function. The **domain of definition** of f is the set of all $x \in E$ such that there exists $y \in F$ satisfying $y = f(x)$. This set is denoted by D_f, and we write:*

$$D_f = \{ x \in E \mid \exists y \in F,\, y = f(x) \}.$$

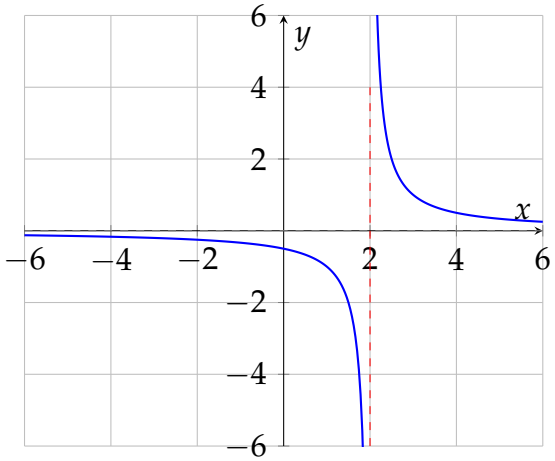
Definition 2.3.4. *Let $f : E \to F$. The **graph** of f is the set of all pairs $(x,y) \in E \times F$ such that $y = f(x)$. It is denoted by $\mathrm{Gr}(f)$, and we write:*

$$\mathrm{Gr}(f) = \{ (x,y) \in E \times F \mid y = f(x) \}.$$

Example 2.3.5. *Let $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \sqrt{x-1}$. The function is defined only when $x - 1 \geq 0 \Rightarrow x \geq 1$. Hence, it is $D_f = [1, +\infty[$. The graph of f is the set $\mathrm{Gr}(f) = \left\{ (x,y) \in \mathbb{R}^2 \mid y = \sqrt{x-1} \right\}$.*



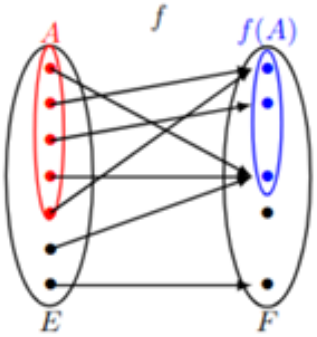
Example 2.3.6. *Let $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \frac{1}{x-2}$. Then $f(x)$ is defined for all real numbers except $x = 2$. Hence, it is $D_f = \mathbb{R} \setminus \{2\}$. The graph of f is the set $\mathrm{Gr}(f) = \left\{ (x,y) \in \mathbb{R}^2 \mid y = \frac{1}{x-2} \right\}$.*



2.3.1 Direct image and inverse image

Definition 2.3.7. *If $A \subseteq E$, the **direct image** of A under f is the subset of F defined by:*

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



Example 2.3.8. *Let f be the function defined by*

$$\begin{array}{rccc} f: & [0,3] & \longrightarrow & [0,5] \\ & x & \longmapsto & y = f(x) = 2x+1. \end{array}.$$

1. *Let's calculate $f(\{2\})$:*

$$\begin{aligned} f(\{2\}) &= \{f(x) \mid x \in \{2\}\} \\ &= \{2x+1 \mid x = 2\}. \end{aligned}$$

Hence, $f(\{2\}) = \{5\}$.

2. *Let's calculate $f([0,1])$:*

$$\begin{aligned} f([0,1]) &= \{f(x) \mid x \in [0,1]\} \\ &= \{2x+1 \mid 0 \leq x \leq 1\} \end{aligned}$$

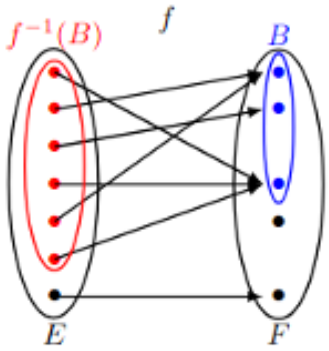
$$f([0,1]) = \{f(x) \mid x \in [0,1]\} = \{2x+1 \mid 0 \leq x \leq 1\}.$$

Since $0 \leq x \leq 1 \implies 0 \leq 2x \leq 2 \implies 1 \leq 2x+1 \leq 3$,

$$f([0,1]) = [1,3] \subset [0,5].$$

Definition 2.3.9. *If $B \subseteq F$, the **inverse image** of B under f is the subset of E defined by:*

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



Example 2.3.10. *Let f be the function defined by*

$$\begin{array}{rccc} f: & [0,2] & \longrightarrow & [0,4] \\ & x & \longmapsto & y = f(x) = (x-1)^2. \end{array}.$$

1. *We want to find $f^{-1}(\{0\})$:*

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

   Hence, $f^{-1}(\{0\}) = \{1\}$.

2. *We want to find $f^{-1}(]0,1[)$:*

$$\begin{aligned} f^{-1}(]0,1[) &= \{x \in [0,2] \mid f(x) \in]0,1[\} \\ &= \{x \in [0,2] \mid 0 < (x-1)^2 < 1\} \\ &= \{x \in [0,2] \mid |x-1| < 1\} \\ &= \{x \in [0,2] \mid -1 < x-1 < 1\} \\ &= \{x \in [0,2] \mid 0 < x < 2\} \end{aligned}$$

   Exclude the point where $(x-1)^2 = 0$, i.e., $x = 1$. Thus,

$$f^{-1}(]0,1[) =]0,1[\cup]1,2[.$$

Proposition 11. *Let $A, B \subseteq E$; $C, D \subseteq F$; and $f : E \to F$ be a function with inverse mapping f^{-1}. Then:*

1. *If $E \subset F$, then $f(E) \subset f(F)$.*
2. $f(A \cup B) = f(A) \cup f(B)$.
3. $f(A \cap B) \subseteq f(A) \cap f(B)$.
4. $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.
5. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.
6. $f(A) \subseteq B \iff A \subseteq f^{-1}(B)$;
7. $f\big(f^{-1}(B)\big) = B, \quad f^{-1}\big(f(A)\big) = A$;
8. $f(A \setminus B) \subseteq f(A) \setminus f(B)$

Proof. 1. Assume $E \subseteq F$.
Take an arbitrary element $y \in f(E)$. By definition of the image of a set, there exists $x \in E$ such that $y = f(x)$. Since $E \subseteq F$, we have $x \in F$. Hence, by the definition of the image, $y = f(x) \in f(F)$. Because $y \in f(F)$ for every $y \in f(E)$, we conclude that: $f(E) \subseteq f(F)$.
2. (a) Take any $y \in f(A \cup B)$. There exists $x \in A \cup B$ such that $y = f(x)$.
Since $x \in A \cup B$, we have $x \in A$ or $x \in B$.

- If $x \in A$, then $y = f(x) \in f(A) \subseteq f(A) \cup f(B)$.
- If $x \in B$, then $y = f(x) \in f(B) \subseteq f(A) \cup f(B)$.

Hence, in both cases, $y \in f(A) \cup f(B)$. Therefore, $f(A \cup B) \subseteq f(A) \cup f(B)$.
(b) Take any $y \in f(A) \cup f(B)$. Then $y \in f(A)$ or $y \in f(B)$.

- If $y \in f(A)$, there exists $x \in A \subseteq A \cup B$ such that $y = f(x)$.
- If $y \in f(B)$, there exists $x \in B \subseteq A \cup B$ such that $y = f(x)$.

In both cases, $y \in f(A \cup B)$. Therefore, $f(A) \cup f(B) \subseteq f(A \cup B)$.
We conclude by (a) and (b) that: $f(A \cup B) = f(A) \cup f(B)$. ■

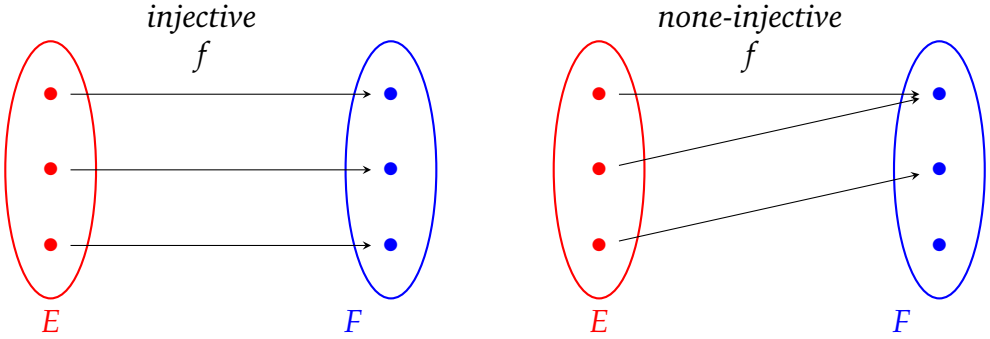
2.3.2 Injective, Surjective, and Bijective Functions

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

Definition 2.3.11. *The function f is said to be **injective** (or **one-to-one**) if every element of F is the image of at most one element of E; that is,*

$$\forall x_1, x_2 \in E,\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

$$\forall x_1, x_2 \in E,\ x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2).$$



Example 2.3.12. *Let:*

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & f(x) = 2x + 3. \end{array}$$

$$\begin{aligned} \forall x_1, x_2 \in \mathbb{R}:\ f(x_1) = f(x_2) &\Rightarrow 2x_1 + 3 = 2x_2 + 3 \\ &\Rightarrow 2x_1 = 2x_2 \\ &\Rightarrow x_1 = x_2 \end{aligned}$$

Thus, f is injective.

Example 2.3.13. *Let :*

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & f(x) = x^2. \end{array}$$

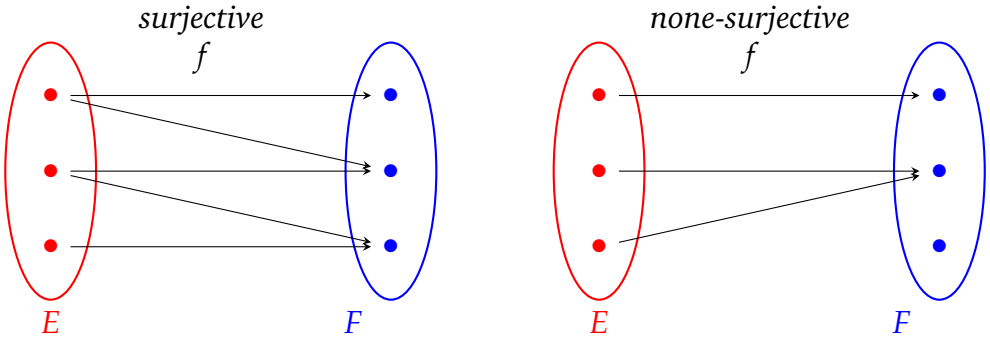
However, for the function $f(x) = x^2$:

$$f(1) = (1)^2 = 1, \quad f(-1) = (-1)^2 = 1$$

Since: $1 \neq -1$, but $f(1) = f(-1)$. The function f is not injective.

Definition 2.3.14. *The function f is said to be **surjective** (or **onto**) if every element of F is the image of at least one element of E; that is,*

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



Example 2.3.15. *Let:*

$$\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & f(n) = 3n + 5. \end{array}$$

$$\begin{array}{rcl} \forall y \in \mathbb{N}, \exists n \in \mathbb{N} \text{ such that } y = f(n) & \Rightarrow & y = 3n + 5 \\ & \Rightarrow & n = \dfrac{y-5}{3} \end{array}$$

However, n must be a natural number.
For example, if $y = 1$ or $y = 2$, then

$$n = \frac{1-5}{3} = -\frac{4}{3} \notin \mathbb{N}, \quad n = \frac{2-5}{3} = -1 \notin \mathbb{N}.$$

Therefore, some $y \in \mathbb{N}$ do not have a preimage in $\mathbb{N}$.The function f is not surjective in $\mathbb{N}$.

Example 2.3.16. *Let:*

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R}^+ \\ & x & \longmapsto & f(x) = x^2. \end{array}$$

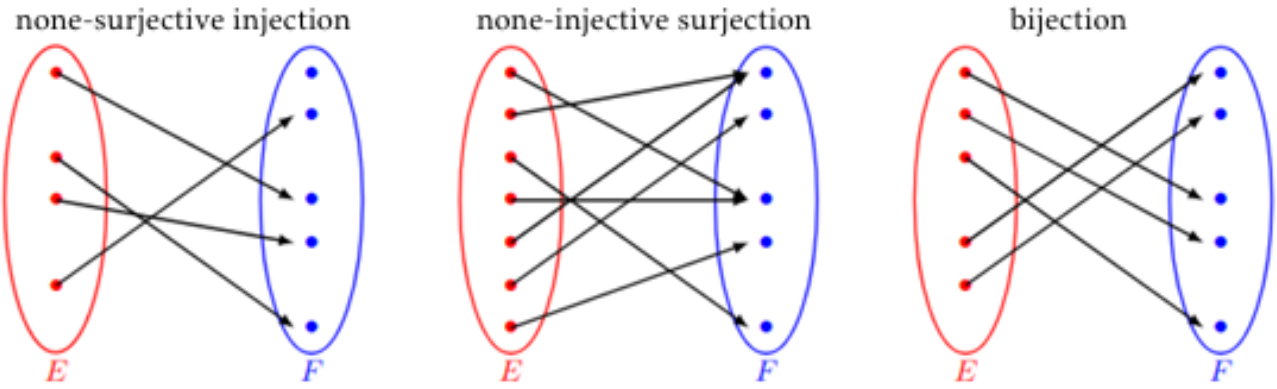
$$\begin{array}{rcl} \forall y \in \mathbb{R}_+, \exists x \in \mathbb{R} \text{ such that } y = f(x) & \Rightarrow & y = x^2 \\ & \Rightarrow & x = \sqrt{y} \quad \text{or} \quad x = -\sqrt{y}. \end{array}$$

Hence, every non-negative real number has a preimage. .The function f is surjective onto $\mathbb{R}^+$.

Definition 2.3.17. *The function f is said to be **bijective** if it is both injective and surjective; that is, if and only if*

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

If f is not injective or not surjective, then it is not bijective.



Example 2.3.18. *Let*

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & f(x) = -2x + 5. \end{array}$$

1.

$$\begin{aligned} \forall x_1, x_2 \in \mathbb{R};\ f(x_1) = f(x_2) &\implies -2x_1 + 5 = -2x_2 + 5. \\ &\implies -2x_1 = -2x_2 \\ &\implies x_1 = x_2 \\ &\implies f \text{ is injective.} \end{aligned}$$

2.

$$\begin{aligned} \forall y \in \mathbb{R}:\ f(x) = y &\implies y = -2x + 5 \\ &\implies -2x = y - 5 \\ &\implies x = \frac{5 - y}{2} \in \mathbb{R} \\ &\implies f \text{ is surjective.} \end{aligned}$$

f is both injective and surjective. Therefore, f is bijective.

Remark 2.3.19. *If f is bijective, then* $\mathrm{Card}(E) = \mathrm{Card}(F)$.

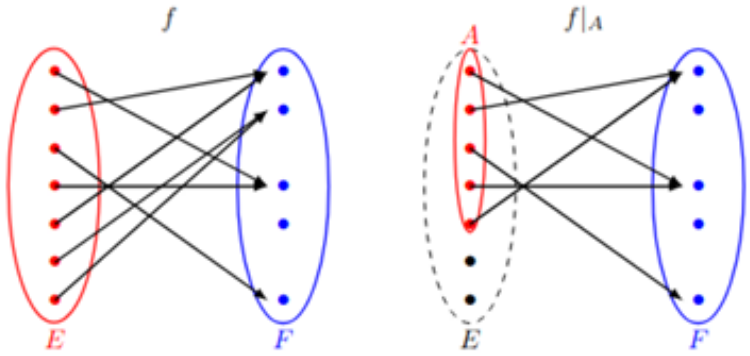
2.3.3 Restriction and Extension of a Function

Definition 2.3.20. *Let E and F are two sets, $f : E \to F$ be a function and let $A \subseteq E$. The* ***restriction*** *of f to A, denoted $f_{|A}$, is the function from A to F defined by:*

$$\begin{array}{rccc} f_{|A}: & A & \longrightarrow & F \\ & x & \longmapsto & f_{|A}(x) = f(x). \end{array}$$

That is to say:

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

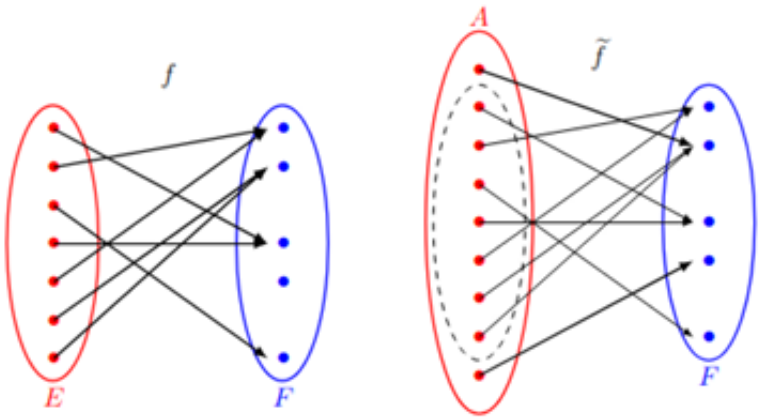


Definition 2.3.21. *Let E and F are two sets, $f : E \to F$ be a function and let A be a set such that $E \subset A$. We call* ***extension*** *of f (or* ***prolongation****) on A any application*

$$\begin{array}{rccc} \tilde{f}: & A & \longrightarrow & F \\ & x & \longmapsto & \tilde{f}\,|_E\,(x) = f(x). \end{array}$$

That is to say:

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

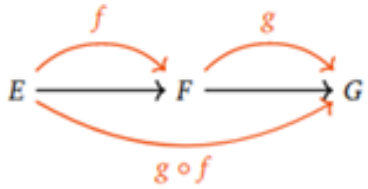


2.3.4 Composition of Functions

Definition 2.3.22. *Let E, f and G are three sets, $f : E \to F$ and $g : F \longrightarrow G$. The* ***composition of the functions*** *f and g, denoted by $g \circ f$, is the function from E to G defined by:*

$$(g \circ f)(x) = g(f(x)), \quad \forall x \in E.$$

In other words, we first apply f, then g.



Example 2.3.23. *Let*

$$f : \mathbb{R} \longrightarrow \mathbb{R}, \quad f(x) = 2x + 1,$$

and

$$g : \mathbb{R} \longrightarrow \mathbb{R}, \quad g(x) = x^2.$$

Then the composition $g \circ f$ is given by:

$$(g \circ f)(x) = g(f(x)) = (2x + 1)^2 = 4x^2 + 4x + 1.$$

Similarly, the reverse composition $f \circ g$ is:

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

Remark 2.3.24. *In general, $g \circ f \neq f \circ g$.*

Proposition 12. *Let $f : E \longrightarrow F$ and $g : F \longrightarrow G$ be two applications.*

1. *If f and g are injective, then $g \circ f$ is injective.*
2. *If f and g are surjective, then $g \circ f$ is surjective.*
3. *If f and g are bijective, then $g \circ f$ is bijective.*

2.4 Exercises with solutions

Exercice 16. *Let $U = \{1,2,3,4,5,6\}$, $E = \{1,2,3\}$, $F = \{3,4,5\}$.*

1. *Compute $E \cup F, E \cap F, E \setminus F, F \setminus E$.*
2. *Compute the complements E^c, F^c with respect to U.*
3. *Verify that $E \setminus F = E \cap F^c$.*

Solution. 1. $E \cup F = \{1,2,3,4,5\}$, $E \cap F = \{3\}$, $E \setminus F = \{1,2\}$, $F \setminus E = \{4,5\}$.

2. $E^c = \{4,5,6\}$, $F^c = \{1,2\}$.

3. $E \setminus F = \{1,2\} = E \cap F^c$.

Exercice 17. *Let $A = \{1,2\}$ and $B = \{a,b,c\}$.*

1. *Compute $A \times B$ and $B \times A$. what is conclusion?*
2. *Let $R \subseteq A \times B$ be defined by*

$$R = \{(1,a),(1,b),(2,c)\}.$$

Determine the domain and the image of R.

Solution. 1.

$$\begin{aligned} A \times B &= \{(x,y) \mid x \in A,\ y \in B\} \\ &= \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\}. \end{aligned}$$

$$\begin{aligned} B \times A &= \{(y,x) \mid y \in B,\ x \in A\} \\ &= \{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}. \end{aligned}$$

Conclusion: $A \times B \neq B \times A$.

2. *The relation is*

$$R = \{(1,a),(1,b),(2,c)\}.$$

- *The domain of R is the set of first components:* $\mathrm{Dom}(R) = \{1,2\}$.
- *The image of R is the set of second components:* $\mathrm{Im}(R) = \{a,b,c\}$.

Exercice 18. *Given three sets E, F, G, show the following identities:*

1. $E \setminus (F \cup G) = (E \setminus F) \cap (E \setminus G)$
2. $(E \setminus F) \cup (F \setminus G) = (E \cup F) \setminus (F \cap G)$.
3. $(E \cup F) \setminus G = (E \setminus G) \cup (F \setminus G)$
4. *If $E \subseteq F$, then $E \setminus G \subseteq F \setminus G$.*

Solution. 1. *Let x be an element.*

$$\begin{aligned} x \in E \setminus (F \cup G) &\iff x \in E \text{ and } x \notin F \cup G \\ &\iff x \in E \text{ and } (x \notin F \text{ and } x \notin G) \\ &\iff (x \in E \setminus F) \text{ and } (x \in E \setminus G) \\ &\iff x \in (E \setminus F) \cap (E \setminus G). \end{aligned}$$

2. *Let x be an element.*

$$\begin{aligned} x \in (E \setminus F) \cup (F \setminus G) &\iff (x \in E \text{ and } x \notin F) \text{ or } (x \in F \text{ and } x \notin G) \\ &\iff (x \in E \text{ or } x \in F) \text{ and } \neg(x \in F \text{ and } x \in G) \\ &\iff x \in E \cup F \text{ and } x \notin F \cap G \\ &\iff x \in (E \cup F) \setminus (F \cap G). \end{aligned}$$

3. *Let x be an element.*

$$\begin{aligned} x \in (E \cup F) \setminus G &\iff (x \in E \text{ or } x \in F) \text{ and } x \notin G \\ &\iff (x \in E \text{ and } x \notin G) \text{ or } (x \in F \text{ and } x \notin G) \\ &\iff x \in (E \setminus G) \cup (F \setminus G). \end{aligned}$$

4. *Assume $E \subseteq F$. Let $x \in E \setminus G$. Then $x \in E$ and $x \notin G$.*

   Since $E \subseteq F$, we have $x \in F$. Hence, $x \in F$ and $x \notin G$, which means $x \in F \setminus G$. Therefore, $E \setminus G \subseteq F \setminus G$.

Exercice 19. 1. *Prove that if $A \subseteq B$, then $A \cap C \subseteq B \cap C$ and $A \cup C \subseteq B \cup C$.*

2. *Give a counterexample to show that the converse is false.*

Solution. 1. *Assume that $A \subseteq B$.*

- *Proof that $A \cap C \subseteq B \cap C$:*

  Let $x \in A \cap C$. Then $x \in A$ and $x \in C$. Since $A \subseteq B$, we have $x \in B$. Hence, $x \in B$ and $x \in C$, which implies $x \in B \cap C$. Therefore, $A \cap C \subseteq B \cap C$.

- *Proof that $A \cup C \subseteq B \cup C$:*

  Let $x \in A \cup C$. Then $x \in A$ or $x \in C$. If $x \in A$, then $x \in B$ since $A \subseteq B$. Thus, in both cases, $x \in B \cup C$. Hence, $A \cup C \subseteq B \cup C$.

2. *The converse would state:*

   If $A \cap C \subseteq B \cap C$ and $A \cup C \subseteq B \cup C$, then $A \subseteq B$. *This is false.*

   Let $A = \{1\}, \quad B = \{2\}, \quad C = \{1,2\}$.

   Then: $A \cap C = \{1\}, \quad B \cap C = \{2\},$

   so $A \cap C \subseteq B \cap C$ *is false, but* $A \cup C = \{1,2\} = B \cup C$.

   Moreover,

   $$A \nsubseteq B.$$

   Thus, the converse does not hold in general.

Exercice 20. *Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 2x + 3$, and $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = x^2$.*

1. *Compute $g \circ f$ and $f \circ g$.*
2. *Are $g \circ f$ and $f \circ g$ equal?*
3. *Determine whether $g \circ f$ is injective.*

Solution. 1. *For all $x \in \mathbb{R}$, We have:*

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

2. *We have*

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

Since $4x^2 + 12x + 9 \neq 2x^2 + 3$ for all $x \in \mathbb{R}$, we conclude that $g \circ f \neq f \circ g$.

3. *Observe that, for example,*

$$(g \circ f)(0) = 9 \quad \textit{and} \quad (g \circ f)(-3) = 9, \textit{ with } 0 \neq -3.$$

Hence, $g \circ f$ is not injective. (Since g is not injective, $g \circ f$ is not injective.)

Exercice 21. *Let $f : \mathbb{R} \setminus \{-1\} \to \mathbb{R} \setminus \{1\}$ be defined by: $f(x) = \frac{x-1}{x+1}$.*

1. *Show that f is bijective.*
2. *Find the inverse f^{-1}.*
3. *Verify that $f^{-1} \circ f = f \circ f^{-1} = Id$.*

Solution. 1. •

$$\begin{aligned}
\forall x_1, x_2 \in \mathbb{R} \setminus \{-1\}; f(x_1) = f(x_2) &\implies \frac{x_1 - 1}{x_1 + 1} = \frac{x_2 - 1}{x_2 + 1}. \\
&\implies (x_1 - 1)(x_2 + 1) = (x_2 - 1)(x_1 + 1). \\
&\implies x_1x_2 + x_1 - x_2 - 1 = x_1x_2 + x_2 - x_1 - 1. \\
&\implies x_1 - x_2 = x_2 - x_1 \\
&\implies 2x_1 = 2x_2, \\
&\implies x_1 = x_2. \\
&\implies f \textit{ is injective.}
\end{aligned}$$

•

$$\begin{aligned}
\forall y \in \mathbb{R} \setminus \{1\} : \ f(x) = y &\implies y = \frac{x - 1}{x + 1} \\
&\implies y(x + 1) = x - 1 \\
&\implies yx - x = -1 - y \\
&\implies x(y - 1) = -(1 + y) \\
&\implies x = \frac{-(1 + y)}{y - 1}, \textit{ Since } y \neq 1 \\
&\implies x = \frac{1 + y}{1 - y} \in \mathbb{R} \setminus \{1\} \\
&\implies f \textit{ is surjective.}
\end{aligned}$$

Therefore, f is bijective.

2. *From the previous computation, we have*

$$\begin{array}{rccc} f^{-1}: & \mathbb{R}\setminus\{1\} & \longrightarrow & \mathbb{R}\setminus\{1\} \\ & x & \longmapsto & f^{-1}(x)=\frac{1+x}{1-x}. \end{array}$$

3. • $f^{-1}(f(x)) = f^{-1}\left(\frac{x-1}{x+1}\right) = \frac{1+\frac{x-1}{x+1}}{1-\frac{x-1}{x+1}} = \frac{\frac{2x}{x+1}}{\frac{2}{x+1}} = x$, *for all* $y \neq -1$.

   • $f(f^{-1}(y)) = f\left(\frac{1+y}{1-y}\right) = \frac{\frac{1+y}{1-y}-1}{\frac{1+y}{1-y}+1} = \frac{\frac{2y}{1-y}}{\frac{2}{1-y}} = y$, *for all* $x \neq -1$.

   Hence,

$$f^{-1}\circ f = f\circ f^{-1} = Id.$$

Exercice 22. *Let* $f:\mathbb{R}\to\mathbb{R}$ *be defined by* $f(x)=x^2+x-2$.

1. *Give the definition of* $f^{-1}(\{4\})$ *and calculate it.*
2. *Is the function* f *bijective?*
3. *Give the definition of* $f([-1,1])$ *and calculate it.*
4. *Give the definition of* $f^{-1}([-2,4])$ *and calculate it.*
5. *Show that the restriction* $g:]-3,+\infty[\longrightarrow]-3,+\infty$ *defined by* $g(x)=f(x)$ *is a bijection.*

Solution. 1. *By definition,* $f^{-1}(\{4\}) = \{x\in\mathbb{R} \mid f(x)=4\}$. *Solve*

$$x^2+x-2=4 \iff x^2+x-6=0.$$

Factor or use quadratic formula: $x=\frac{-1\pm\sqrt{1+24}}{2}=\frac{-1\pm5}{2}$.

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

2. • f *is not injective because* $f(-3)=4=f(2)$, *but* $-3\neq 2$.

   • f *is not surjective because a quadratic* x^2+x-2 *has a minimum at* $x=-\frac{1}{2}$:

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

   Thus $f(\mathbb{R})=[-9/4,+\infty)\subsetneq\mathbb{R}$.

   Conclusion: f *is not bijective.*

3. *By definition,* $f([-1,1])=\{f(x)\mid x\in[-1,1]\}$.

   • f *is continuous on* $[-1,1]$.

   • *Critical point:* $f'(x)=2x+1=0 \implies x=-\frac{1}{2}$.

- *Evaluate endpoints and critical point:*

$$f(-1) = (-1)^2 + (-1) - 2 = -2, \quad f(1) = 1 + 1 - 2 = 0, \quad f(-\tfrac{1}{2}) = \frac{1}{4} - \frac{1}{2} - 2 = -\frac{9}{4}.$$

- *Minimum:* $f(-\frac{1}{2}) = -9/4$, *Maximum:* $f(1) = 0$.

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

4. *By definition,* $f^{-1}([-2,4]) = \{x \in \mathbb{R} \mid -2 \leq f(x) \leq 4\}$.

- $f(x) \geq -2 \implies x^2 + x - 2 \geq -2 \implies x^2 + x \geq 0 \implies x(x+1) \geq 0$ *This gives* $x \leq -1$ *or* $x \geq 0$.
- $f(x) \leq 4 \implies x^2 + x - 2 \leq 4 \implies x^2 + x - 6 \leq 0$ *Solve* $x^2 + x - 6 = 0 \implies x = \frac{-1 \pm \sqrt{1+24}}{2} = -3$ *or* 2 *So* $x \in [-3,2]$.

Intersection of the two conditions ($x \leq -1$ *or* $x \geq 0$) *with* $[-3,2]$: $[-3,-1] \cup [0,2]$. *So,* $f^{-1}([-2,4]) = [-3,-1] \cup [0,2]$.

5. - *For all* $x > -3$, *we have* $f'(x) = 2x + 1 > 0$ *for* $x > -\frac{1}{2}$. *Thus,* g *is strictly increasing and therefore injective.*
   - *Moreover,*

$$\lim_{x \to -3^+} f(x) = 4, \qquad \lim_{x \to +\infty} f(x) = +\infty.$$

   Since g *is continuous and strictly increasing, its image is* $]-3, +\infty[$. *Hence,* g *is surjective.*

Therefore, g *is bijective.*

Exercice 23. *Let* $f : E \to F$, $g : F \to G$, *and define* $h(x) = g(f(x))$.

1. *Injectivity of* h *implies injectivity of* f; *surjectivity of* h *implies surjectivity of* g.
2. *If* h *is surjective and* g *is injective, then* f *is surjective.*
3. *If* h *is injective and* f *is surjective, then* g *is injective.*

Solution. 1. • If h is injective, then f is injective.

Assume that h *is injective. Let* $x_1, x_2 \in E$ *such that* $f(x_1) = f(x_2)$.

Applying g *to both sides, we obtain* $g(f(x_1)) = g(f(x_2))$, *that is,* $h(x_1) = h(x_2)$.

Since h *is injective, it follows that* $x_1 = x_2$. *Hence,* f *is injective.*

- If h is surjective, then g is surjective.

  Assume that h is surjective. Let $y \in G$. Since h is surjective, there exists $x \in E$ such that $h(x) = y$. Thus, $g(f(x)) = y$. Let $z = f(x) \in F$. Then $g(z) = y$. Hence, g is surjective.

2. *Assume that h is surjective and g is injective. Let $y \in F$. We must show that there exists $x \in E$ such that $f(x) = y$.*

   Since $g(y) \in G$ and h is surjective, there exists $x \in E$ such that $h(x) = g(y)$.

   That is, $g(f(x)) = g(y)$. Since g is injective, we conclude that $f(x) = y$. Therefore, f is surjective.

3. *Assume that h is injective and f is surjective. Let $y_1, y_2 \in F$ such that $g(y_1) = g(y_2)$.*

   Since f is surjective, there exist $x_1, x_2 \in E$ such that $f(x_1) = y_1 \quad and \quad f(x_2) = y_2$.

   Then, $h(x_1) = g(f(x_1)) = g(y_1), and h(x_2) = g(f(x_2)) = g(y_2)$.

   Thus, $h(x_1) = h(x_2)$. Since h is injective, we obtain $x_1 = x_2$, and consequently,

$$y_1 = f(x_1) = f(x_2) = y_2.$$

   Hence, g is injective.

Chapter 3

Binary relations on a set

A binary relations on a set is a subset of the Cartesian product of the set with itself, defining a relationship between pairs of elements. Binary relations are used to describe orderings, equivalences, and connections between elements and are fundamental in mathematics, computer science, and logic.

3.1 Basic definitions

Definition 3.1.1. *A **binary relation** $\mathcal{R}$ on a set E is a property concerning ordered pairs of elements of E. We write $x\mathcal{R}y$ or $\mathcal{R}(x,y)$ to express that the property holds for the pair $(x,y) \in E \times E$. It is then said that: "x is related to y by the relation $\mathcal{R}$".*

Example 3.1.2. *Let $\mathcal{P}(E)$ be all parts of a set E. The relationship $\mathcal{R}$ in $\mathcal{P}(E)$ is defined by:*

$$\forall A, B \in P(E) : A\mathcal{R}B \iff A \subset B.$$

Said:" For any two subsets A and B of E, A is related to B if and only if A is a subset of B".

Remark 3.1.3. *If $\mathcal{R}$ is a binary relation over E and it does not hold for the pair (x,y), then $\overline{x\mathcal{R}y}$, $\urcorner(x\mathcal{R}y)$ or $(x \not\mathcal{R}y)$. In other words, $(x,y) \notin \mathcal{R} \iff \overline{x\mathcal{R}y}$.*

Example 3.1.4. *Let$E = \{1,2,3\}$. On définit une relation binaire $\mathcal{R}$ sur E par :*

$$x\mathcal{R}y \iff x \leq y.$$

Considérons le couple $(3,1)$. Comme $3 \not\leq 1$, on a : $(3,1) \notin \mathcal{R}$.

Definition 3.1.5. *The representing* ***graph*** *of a relation in E is a graph $G \subseteq E \times E$ which consists of all the pairs (x,y) such that the relation between two elements x and y is true.*

$$G = \left\{(x,y) \in E^2;\ \ x\mathcal{R}y\right\}.$$

Example 3.1.6. *Let $A = \{1,2,3,4,5\}$. Define the relation $\mathcal{R}$ on A by:*

$$x\mathcal{R}y \iff x - y \text{ is even.}$$

We can compute all pairs (x,y) satisfying this condition:

$$G = \{(1,1),(1,3),(1,5),(2,2),(2,4),(3,1),(3,3),(3,5),(4,2),(4,4),(5,1),(5,3),(5,5)\}.$$

Thus, the relation $\mathcal{R}$ groups together all numbers that have the same parity (both even or both odd).

Example 3.1.7. *Let us consider the set $E = \{1,2,3,4\}$. We define a binary relation $\mathcal{R}$ on E by:*

$$\forall x,y \in E, \quad x\mathcal{R}y \iff x < y$$

The ordered pairs of the relation are: $G = \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$.

Remark 3.1.8. *Two relations $\mathcal{R}$ and $\mathcal{R}'$ are* ***equal*** *if and only if their graphs are equal:*

$$\mathcal{R} = \mathcal{R}' \iff G_{\mathcal{R}} = G_{\mathcal{R}'}.$$

3.1.1 Reflexive, symmetric, antisymmetric, transitive relation

Definition 3.1.9. *Let $\mathcal{R}$ be a relation on a set E. For all $x,y,z \in E$.*

1. *$\mathcal{R}$ is* ***Reflexive*** *iff $\forall x \in E$: $x\mathcal{R}x$.*
2. *$\mathcal{R}$ is* ***Symmetric*** *iff $\forall x,y \in E$: $x\mathcal{R}y \Rightarrow y\mathcal{R}x$.*
3. *$\mathcal{R}$ is* ***Transitive*** *iff $\forall x,y,z \in E$: $(x\mathcal{R}y$ and $y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.*
4. *$\mathcal{R}$ is* ***Antisymmetric*** *iff $\forall x,y \in E$: $(x\mathcal{R}y$ and $y\mathcal{R}x) \Rightarrow x = y$.*

Example 3.1.10. *Let the relation $\mathcal{R}$ be defined on $\mathbb{Z}$ by:*

$$x\mathcal{R}y \iff x \text{ divides } y.$$

1. ***Reflexivity:*** *Let $x \in \mathbb{Z}$. We have x divides x (even 0 divides 0). Hence, for all $x \in \mathbb{Z}$, $x\mathcal{R}x$. Therefore, $\mathcal{R}$ is reflexive.*

2. ***Symmetric:*** *Let $x, y \in \mathbb{Z}$. If $x\mathcal{R}y$, then x divides y. But y does not necessarily divide x. For example, 1 divides 4 but 4 does not divide 1. Thus, there exist $x, y \in \mathbb{Z}$ such that $x\mathcal{R}y$ and not $y\mathcal{R}x$. Therefore, $\mathcal{R}$ is not symmetric.*

3. ***Antisymmetric:*** *Let $x, y \in \mathbb{Z}$.*

$$\begin{aligned}(x\mathcal{R}y \text{ and } y\mathcal{R}x) &\implies (x \text{divides} y) \text{ and } (y \text{ divides} x)\\ &\implies (y = x) \text{ or } (y = -x)\\ &\implies \text{is antisymmetric}\end{aligned}$$

4. ***Transitive:*** *Let $x, y, z \in \mathbb{Z}$,*

$$\begin{aligned}(x\mathcal{R}y \text{ and } y\mathcal{R}z) &\implies (x \text{dividesy}) \text{ and } (y \text{ dividesz})\\ &\implies x \text{ divides } z\\ &\implies \text{is transitive.}\end{aligned}$$

Remark 3.1.11. *A relation may be neither symmetric nor antisymmetric.*

3.2 Order Relation

Definition 3.2.1. *A binary relation $\mathcal{R}$ on a set E is called an **order relation** (or **ordering**) if and only if it is reflexive, antisymmetric and transitive. We then say that $(E, \mathcal{R})$ is an ordered set.*

Example 3.2.2. *Let $\mathbb{R}$ be the binary relation on E defined by:*

$$A\mathcal{R}B \iff A \subseteq B, \quad \text{for all } A, B \in \mathcal{P}(E).$$

Let us show that $\mathbb{R}$ is an order relation.

1. ***Reflexive:*** *For all $A \in \mathcal{P}(E)$, we have $A \subseteq A$. Hence, $A\mathcal{R}A$. Therefores, $\mathcal{R}$ is reflexive.*

2. ***Antisymmetric:*** *For all* $A, B \in \mathcal{P}(E)$,

$$\begin{aligned}(A\mathcal{R}B) \text{ and } (B\mathcal{R}A) &\Longrightarrow A \subseteq B \text{ and } B \subseteq A \\ &\Longrightarrow A = B. \\ &\Longrightarrow \mathcal{R} \text{ is antisymmetric.}\end{aligned}$$

3. ***Transitive:*** *For all* $A, B, C \in \mathcal{P}(E)$,

$$\begin{aligned}(A\mathcal{R}B) \text{ and } (B\mathcal{R}C) &\Longrightarrow A \subseteq B \text{ and } B \subseteq C \\ &\Longrightarrow A \subseteq C \\ &\Longrightarrow A\mathcal{R}C. \\ &\Longrightarrow \mathcal{R} \text{ is transitive.}\end{aligned}$$

Therefore, $\mathbb{R}$ *is an order relation.*

3.2.1 Total order and Partial order

Definition 3.2.3. *Let* $\mathcal{R}$ *be an order relation on* E*, any two element* x *and* y *are said to be* ***comparable*** *if* $(x\mathcal{R}y)$ *or* $(y\mathcal{R}x)$.

Definition 3.2.4. *Let* $\mathcal{R}$ *be an order relation on a set* E.

1. *If any two elements* x *and* y *in* E *are always comparable, then* $\mathcal{R}$ *is called a* ***total (or linear) order****, and the set* E *is said to be* ***totally ordered****.*
2. *If there exist at least two elements* x *and* y *in* E *that are not comparable, then* $\mathcal{R}$ *is called a* ***partial order****, and the set* E *is called a* ***partially ordered set*** *(or* ***poset****).*

Example 3.2.5. *Let* $\mathcal{R}$ *be the binary relation on* $\mathbb{R}$ *defined by:*

$$x\mathcal{R}y \Longleftrightarrow x \leq y.$$

Let us show that $\mathcal{R}$ *is a total order relation.*
Before a total order relation, we prove $\mathcal{R}$ *is a order relation:*

1. • ***Reflexive:*** *For all* $x \in \mathbb{R}$*, we have* $x \leq x$*. Hence,* $x\mathcal{R}x$*. Therefores,* $\mathcal{R}$ *is reflexive.*

- ***Antisymmetric:*** *For all* $x,y \in \mathbb{R}$,

$$\begin{aligned}(x\mathcal{R}y) \text{ and } (y\mathcal{R}x) &\Longrightarrow x \leq y \text{ and } y \leq x\\ &\Longrightarrow x = y.\\ &\Longrightarrow \mathcal{R} \text{ is antisymmetric.}\end{aligned}$$

- ***Transitive:*** *For all* $x,y,z \in \mathbb{R}$,

$$\begin{aligned}(x\mathcal{R}y) \text{ and } (y\mathcal{R}z) &\Longrightarrow x \leq y \text{ and } y \leq z\\ &\Longrightarrow x = z.\\ &\Longrightarrow x\mathcal{R}z.\\ &\Longrightarrow \mathcal{R} \text{ is transitive.}\end{aligned}$$

2. *For all* $x,y \in \mathbb{R}$, *either* $x \leq y$ *or* $y \leq x$.

   Therefore, $\mathcal{R}$ *is a total order relation.*

Exercice 24. *Let* $A = \{1,2,3,4,6,12\}$ *define the relation* $\mathcal{R}$ *on* A *by*

$$x\mathcal{R}y \Longleftrightarrow x \mid y.$$

1. *Prove* $\mathcal{R}$ *is an order relation on* A.
2. *Is* $\mathcal{R}$ *a total or partial order?*

Solution. 1. • *Reflexivity: For every* $x \in A$, *we have* $x \mid x$ *since* $x = 1 \cdot x$. *Hence,* $\forall x \in A,\ x\mathcal{R}x$. *It is reflexive.*

- *Antisymmetry: For all* $x,y \in A$,

$$\begin{aligned}(x\mathcal{R}y) \text{ and } (y\mathcal{R}x) &\Longrightarrow (x \mid y) \text{and } (y \mid x)\\ &\Longrightarrow \exists (k,\ell) \in \mathbb{Z} :\ y = kx \quad \text{and} \quad x = \ell y.\\ &\Longrightarrow \exists (k,\ell) \in \mathbb{Z} :\ x = \ell k x\\ &\Longrightarrow \exists (k,\ell) \in \mathbb{Z} :\ \ell k = 1\\ &\Longrightarrow x = y\\ &\Longrightarrow \mathcal{R} \text{ is antisymmetric.}\end{aligned}$$

- Transitivity: *For all* $(x,y,z) \in A^3$,

$$\begin{aligned}(x\mathcal{R}y) \text{ and } (y\mathcal{R}z) &\implies (x \mid y)_a nd\ (y \mid z)\\ &\implies \exists (k,\ell) \in \mathbb{Z} :\ y = kx \quad \text{and} \quad z = \ell y.\\ &\implies \exists (k,\ell) \in \mathbb{Z} :\ z = \ell kx\\ &\implies x \mid z.\\ &\implies x\mathcal{R}z.\\ &\implies \mathcal{R} \text{ is transitive.}\end{aligned}$$

It is an order relation *on* A.

2. *A relation is total if every pair of elements is comparable. Consider* $2,3 \in A$*:*

$$2 \nmid 3 \quad \text{and} \quad 3 \nmid 2.$$

Thus, neither $2\mathcal{R}3$ *nor* $3\mathcal{R}2$ *holds. Therefore,* $\mathcal{R}$ *is not a total order.*

The relation $\mathcal{R}$ *is a partial order on* A.

Definition 3.2.6. *Let* $\mathcal{R}$ *be an order relation on a set* E*, and let* $X \subseteq E$.

1. *An element* $a \in E$ *is called a* ***lower bound*** *of* X *if:* $\forall x \in X, \quad a\,\mathcal{R}\,x$.
2. *An element* $b \in E$ *is called an* ***upper bound*** *of* X *if:* $\forall x \in X, \quad x\,\mathcal{R}\,b$.

Proposition 13. 1. *If* X *has a lower bound, then it has infinitely many lower bounds. Indeed, if* a *is a lower bound, any* $a' \in E$ *such that* $a'\,\mathcal{R}\,a$ *is also a lower bound.*

2. *Similarly, if* X *has an upper bound, then it has infinitely many upper bounds. Indeed, if* b *is an upper bound, any* $b' \in E$ *such that* $b\,\mathcal{R}\,b'$ *is also an upper bound.*

Definition 3.2.7. ***(Minimum and Maximum)*** *Let* $X \subseteq E$.

- *If a lower bound* a *belongs to* X*, it is called the* ***least element*** *or* ***minimum*** *of* X*, denoted* $\min(X)$.
- *If an upper bound* b *belongs to* X*, it is called the* ***greatest element*** *or* ***maximum*** *of* X*, denoted* $\max(X)$.

Remark 3.2.8. *A set* X *may have lower or upper bounds without having a minimum or maximum. Similarly, a set may have a minimum but no maximum, or vice versa.*

3.3 Equivalence Relation Sets

3.3.1 Equivalence Relation

Definition 3.3.1. *A binary relation $\mathcal{R}$ on a set E is called an **equivalence relation** if a relation that is reflexive, symmetric and transitive.*
*When $\mathcal{R}$ is an equivalence relation on E, we say that two elements x and y are **equivalent** and we write $x \sim y$.*

Exercice 25. *Let $\mathcal{R}$ be a binary relation on $\mathbb{R}$ defined by:*

$$x\mathcal{R}y \iff x^2 - 1 = y^2 - 1$$

Show that $\mathcal{R}$ is an equivalence relation.

Solution. 1. *Reflexive: $\mathcal{R}$ is reflexive since for all x, $x^2 - 1 = x^2 - 1$, hence $x\mathcal{R}x$. Therefore, $\mathcal{R}$ is reflexive.*

2. *Symmetric: For any $(x,y) \in \mathbb{Z}^2$,*

$$\begin{aligned} x\mathcal{R}y &\implies x^2 - 1 = y^2 - 1 \\ &\implies y^2 - 1 = x^2 - 1 \\ &\implies y\mathcal{R}x. \\ &\implies \mathcal{R} \text{ is symmetric.} \end{aligned}$$

3. *Transitive: For all $(x,y,z) \in \mathbb{Z}^3$,*

$$\begin{aligned} (x\mathcal{R}y) \text{ and } (y\mathcal{R}z) &\implies x^2 - 1 = y^2 - 1 \text{ and } y^2 - 1 = z^2 - 1, \\ &\implies x^2 - 1 = z^2 - 1 \\ &\implies x\mathcal{R}z. \\ &\implies \mathcal{R} \text{ is transitive.} \end{aligned}$$

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

3.3.2 Equivalence Classes

Definition 3.3.2. *If $\mathcal{R}$ is an equivalence relation on a set E, then for any element $x \in E$, the* ***equivalence class of*** *x is defined by:*

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

That is, $[x]$ is the set of all elements of E that are related to x by $\mathcal{R}$. Denoted by $\dot{x}$, C_x or $C(x)$.

Exercice 26. *Let $\mathcal{R}$ be the binary relation on $\mathbb{Z}$ defined by: $x\mathcal{R}y \iff x+y$ is even.*

1. *Show that $\mathcal{R}$ is an equivalence relation.*
2. *Calculate equivalence classes of $[0]$ and $[1]$.*

Solution. 1.

- ***Reflexive:*** *Let $x \in \mathbb{Z}$, $x\mathcal{R}x \Longrightarrow x+x$ is even. Since $x+x = 2x$, and $2x$ is divisible by 2 (because x is an integer). Therefore. Hence, $\mathcal{R}$ is reflexive.*
- ***Symmetric:*** *Let $x, y \in \mathbb{Z}$.*

$$\begin{aligned} x\mathcal{R}y &\Longrightarrow x+y \text{ is even.} \\ &\Longrightarrow \exists k \in \mathbb{Z},\ x+y = 2k. \\ &\Longrightarrow \exists k \in \mathbb{Z},\ y+x = 2k. \\ &\Longrightarrow y+x \text{ is even.} \\ &\Longrightarrow y\mathcal{R}x. \\ &\Longrightarrow \mathcal{R} \text{ is symmetric.} \end{aligned}$$

- ***Transitive:*** *Let $x, y, z \in \mathbb{Z}$.*

$$\begin{aligned} (x\mathcal{R}y \text{ and } y\mathcal{R}z) &\Longrightarrow \exists (k_1,k_2) \in \mathbb{Z}^2,\ y+x = 2k_1 \text{and } y+z = 2k_2. \\ &\Longrightarrow \exists (k_1,k_2) \in \mathbb{Z}^2,\ (x+y)+(y+z) = 2k_1+2k_2. \\ &\Longrightarrow \exists (k_1,k_2) \in \mathbb{Z}^2,\ x+z+2y = 2(k_1+k_2). \\ &\Longrightarrow x+z = 2(k_1+k_2-y). \end{aligned}$$

The right-hand side is twice an integer (since $k_1, k_2, y \in \mathbb{Z}$), so $x+z$ is even. Hence, $x\mathcal{R}z$. Therefore, $\mathcal{R}$ is transitive.

We conclude that $\mathcal{R}$ is an equivalence relation on $\mathbb{Z}$.

2. *Find the Equivalence Class* $[0]$ *and* $[1]$*:*

- $$\begin{aligned}[0] &= \{y \in \mathbb{Z} \mid 0\mathcal{R}y\} \\ &= \{y \in \mathbb{Z} \mid 0 + y \text{ is even}\} \\ &= 2\mathbb{Z} \\ &= \{\ldots, -4, -2, 0, 2, 4, \ldots\}.\end{aligned}$$

- $$\begin{aligned}[1] &= \{y \in \mathbb{Z} \mid 1\mathcal{R}y\} \\ &= \{y \in \mathbb{Z} \mid 1 + y \text{ is even}\} \\ &= \{y \in \mathbb{Z} \mid y \text{ is odd}\} \\ &= 2\mathbb{Z} + 1 \\ &= \{\ldots, -3, -1, 1, 3, 5, \ldots\}.\end{aligned}$$

3.3.3 Quotient set

Definition 3.3.3. *The set of all equivalence classes of elements of* E *is called the* ***quotient set*** *of* E *by* $\mathcal{R}$*, and is denoted by* $E_{/\mathcal{R}}$*:*

$$E_{/\mathcal{R}} = \{[x] \mid x \in E\}.$$

Where $[x]$ *equivalence class.*

Exercice 27. *Let* $\mathcal{R}$ *be the binary relation on* $\mathbb{R}$ *defined by:*

$$x\mathcal{R}y \Longleftrightarrow x^2 - x = y^2 - y.$$

1. *Show that* $\mathcal{R}$ *is an equivalence relation?*
2. *Determine the following equivalence classes:* C_0, C_1, C_2*, and* $C_{\frac{1}{2}}$*.*
3. *Detrmine quotient set* $\mathbb{R}/\mathcal{R}$*.*

Solution. 1. • ***Reflexive:*** *For all* $x \in \mathbb{R}$*, we have* $x^2 - x = x^2 - x$*, hence* $x\mathcal{R}x$*. Therefore,* $\mathcal{R}$ *is reflexive.*

- ***Symmetric:*** *For all* $x, y \in \mathbb{R}$,

$$\begin{aligned} x\mathcal{R}y &\implies x^2 - x = y^2 - y \\ &\implies y^2 - y = x^2 - x \\ &\implies y\mathcal{R}x. \\ &\implies \mathcal{R} \text{ is symmetric.} \end{aligned}$$

- ***Transitive:*** *For all* $x, y, z \in \mathbb{R}$,

$$\begin{aligned} (x\mathcal{R}y \text{ and } y\mathcal{R}z) &\implies x^2 - x = y^2 - y \quad \text{and} \quad y^2 - y = z^2 - z \\ &\implies x^2 - x = z^2 - z. \\ &\implies x\mathcal{R}z. \\ &\implies \mathcal{R} \text{ is transitive.} \end{aligned}$$

Thus, R *is an equivalence relation.*

2. *Calculte equivalence class of* x*:*

$$\begin{aligned} [x] &= \{y \in E \mid x\mathcal{R}y\} \\ &\implies x^2 - x = y^2 - y. \\ &\implies y^2 - y - x^2 + x = 0. \\ &\implies (y - x)(y + x - 1) = 0. \\ &\implies y = x \quad \text{or} \quad y = 1 - x. \end{aligned}$$

So the equivalence class of x *is* $C_x = [x] = \{x, 1 - x\}$*. Hence:*

$$\begin{aligned} C_0 &= \{0, 1\}, \\ C_1 &= \{0, 1\}, \\ C_2 &= \{2, -1\}, \\ C_{\frac{1}{2}} &= \{\frac{1}{2}\}, \end{aligned}$$

3. *The quotient set is* $\mathbb{R}/\mathcal{R} = \left\{\{x, 1 - x\} \mid x \in \mathbb{R}, x \neq \frac{1}{2}\right\} \cup \left\{\left\{\frac{1}{2}\right\}\right\}$.

.

Theorem 3.3.4. *If $\mathcal{R}$ is an equivalence relation on E, then the set of all equivalence classes of $\mathcal{R}$ forms a* ***partition*** *of E. Conversely, if P is a partition of E, then the relation defined by*

$$x\mathcal{R}y \iff \exists S \in P \text{ such that } x,y \in S$$

is an equivalence relation.

Example 3.3.5. *Let $E = \mathbb{Z}$ (the integers), and define: $x\mathcal{R}y \iff x+y$ is even. Hence, the integers are parttioned into two disjoint class: the even numbers and odd numbers.*

3.4 Exercises with solutions

Exercice 28. *Let R be the relation defined on $\mathbb{Z}$ by*

$$aRb \iff \forall (a,b) \in \mathbb{Z}^2 \ (a-b) \text{ is odd.}$$

is it reflexive, symmetric, antisymmetric or transitive?

Solution.

1. *Reflexivity: Let $a \in \mathbb{Z}$. We have $a - a = 0$, which is even, not odd. For example, $1 - 1 = 0$ is not odd. Therefore, aRa is false for all $a \in \mathbb{Z}$; hence R is not reflexive.*

2. *Symmetry. Let $a,b \in \mathbb{Z}$. Suppose aRb, that is, $a - b$ is odd. Then $b - a = -(a-b)$ is also odd, since the negative of an odd integer remains odd. Hence bRa. Therefore, R is symmetric.*

3. *Non-antisymmetry. Let $a,b \in \mathbb{Z}$ such that aRb and bRa. That means both $a - b$ and $b - a$ are odd, but this does not imply $a = b$. For example:*

$$6 - 1 = 5 \text{ (odd)}, \qquad 1 - 6 = -5 \text{ (odd)}, \quad \text{but } 6 \neq 1.$$

   Therefore, R is not antisymmetric.

4. *Transitive. Let $a,b,c \in \mathbb{Z}$ such that aRb and bRc. Then $a - b$ and $b - c$ are odd. The sum of two odd integers is even, hence*

$$a - c = (a - b) + (b - c)$$

is even, not odd. Thus aRc is false. Therefore, R is not transitive.

it is symmetric, but neither reflexive, antisymmetric, nor transitive.

Exercice 29. *Let $\mathcal{R}$ be an order relation on $\mathbb{R}^3$ defined by*

$$\forall (a,b,c),(x,y,z) \in \mathbb{R}^3,\ (a,b,c)\mathcal{R}(x,y,z) \Longleftrightarrow (\mid x-a \mid \leq b-y \text{ and } z=c).$$

1. *Show that $\mathcal{R}$ is an order relation on $\mathbb{R}^3$.*
2. *Is the order total on $\mathbb{R}^3$?*

Solution. 1. • *Reflexivity: For any $(a,b,c) \in \mathbb{R}^3$, we have*
$|a-a| = 0 \leq b-b = 0$ *and* $c=c$. *Hence, $(a,b,c)\mathcal{R}(a,b,c)$. It is reflexive.*

- Antisymmetry: *For all $(a,b,c) \in \mathbb{R}^3$ and $(x,y,z) \in \mathbb{R}^3$*
$(a,b,c)\mathcal{R}(x,y,z)$ *and* $(x,y,z)\mathcal{R}(a,b,c)$

$$\Longrightarrow \begin{cases} |x-a| \leq b-y, & |a-x| \leq y-b, \\ z=c \quad \text{and} \quad c=z. \end{cases}$$

Since $|x-a| = |a-x|$, adding the inequalities gives $2|x-a| \leq 0$,
which implies $x=a$. Substituting back yields $b=y$, and from above $c=z$. Thus,
$(a,b,c)=(x,y,z)$, so $\mathcal{R}$ is antisymmetric.

- Transitivity: *For all $(a,b,c) \in \mathbb{R}^3$; $(x,y,z) \in \mathbb{R}^3$ and $(u,v,w) \in \mathbb{R}^3$,*
$(a,b,c)\mathcal{R}(x,y,z)$ *and* $(x,y,z)\mathcal{R}(u,v,w)$.

$$\Longrightarrow \begin{cases} |x-a| \leq b-y, & |u-x| \leq y-v, \\ z=c \quad \text{and} \quad w=z. \end{cases}$$

By the triangle inequality, $|u-a| \leq |u-x| + |x-a| \leq (y-v)+(b-y) = b-v$.
Moreover, $w=c$. Hence, $(a,b,c)\mathcal{R}(u,v,w)$.

Therefore, $\mathcal{R}$ is reflexive, antisymmetric, and transitive, and thus an order relation *on $\mathbb{R}^3$.*

2. *A total order requires that any two elements be comparable. Consider, for example, $(0,0,0)$ and $(1,0,1)$. Since the third coordinates are different, neither $(0,0,0)\mathcal{R}(1,0,1)$ nor $(1,0,1)\mathcal{R}(0,0,0)$ holds.*

Hence, the order is not total. The relation $\mathcal{R}$ is a partial order on $\mathbb{R}^3$.

Exercice 30. *Let $\mathbb{N}^* = \{1,2,3,\dots\}$ and define a relation $\ll$ on $\mathbb{N}^*$ by:*

$$k \ll l \iff \exists n \in \mathbb{N}^* \text{ such that } l = k^n, \quad \forall (k,l) \in \mathbb{N}^* \times \mathbb{N}^*.$$

1. *Prove that $\ll$ is a partial order relation on $\mathbb{N}^*$.*
2. *Consider the set $A = \{2,4,16\}$, ordered by $\ll$. Determine: the smallest element and greatest element of A.*

Solution. 1. • Reflexive: $\forall k \in \mathbb{N}^*$, $k \ll k$. *Indeed, for any $k \in \mathbb{N}^*$, take $n = 1$. Then $k = k^1$, so $k \ll k$. Hence $\ll$ is reflexive.*

• Antisymmetric: *Then there exist $m,n \in \mathbb{N}^*$ such that*

$$\begin{aligned} k \ll l \text{ and } l \ll k &\implies l = k^n \quad \text{and} \quad k = l^m. \\ &\implies k = (k^n)^m \\ &\implies nm = 1 \\ &\implies n = 1 \ \text{ and } \ m = 1 \\ &\implies l = k \end{aligned}$$

Hence $\ll$ is antisymmetric.

• Transitive: *$k \ll l$ and $l \ll p \Rightarrow k \ll p$. There exist $n_1, n_2 \in \mathbb{N}^*$ such that*

$$\begin{aligned} k \ll l \text{ and } l \ll p \Rightarrow k \ll p &\implies l = k^{n_1} \quad \text{and} \quad p = l^{n_2} \\ &\implies p = (k^{n_1})^{n_2} \end{aligned}$$

Since $n_1 n_2 \in \mathbb{N}^*$, it follows that $k \ll p$. Hence $\ll$ is transitive.

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

2. *Let $A = \{2,4,16\}$ in $(\mathbb{N}^*, \ll)$. We compute the relation $\ll$ among the elements of A:*

• *The **smallest element** of A is 2, because $2 \ll 4$ and $2 \ll 16$.*

• *The **greatest element** of A is 16, because $2 \ll 16$ and $4 \ll 16$.*

Exercice 31. *Let $\mathcal{R}$ be the relation on $\mathbb{Z}$ defined by: $x \mathcal{R} y \iff x - y$ is divisible by 4.*

1. *Prove that $\mathcal{R}$ is an equivalence relation on $\mathbb{Z}$.*
2. *Determine the equivalence classes of $0,1,2,3$.*

3. *How many distinct equivalence classes exist?*

Solution. 1. • *Reflexive: For any* $x \in \mathbb{Z}$, $x - x = 0$ *is divisible by* 4. *Thus* $x\mathcal{R}x$.

• *Symmetric: For any* $(x,y) \in \mathbb{Z}^2$,

$$\begin{aligned} x\mathcal{R}y &\implies \exists k \in \mathbb{Z},\ x - y = 4k \\ &\implies k \in \mathbb{Z},\ y - x = -4k \\ &\implies y\mathcal{R}x. \\ &\implies \mathcal{R} \text{ is symmetric.} \end{aligned}$$

• *Transitive: For all* $(x,y,z) \in \mathbb{Z}^3$,

$$\begin{aligned} (x\mathcal{R}y) \text{ and } (y\mathcal{R}z) &\implies \exists (k,k') \in \mathbb{Z}^2,\ x\mathcal{R}y \text{ and } y\mathcal{R}z \\ &\implies \exists (k,k') \in \mathbb{Z}^2,\ x - y = 4k \text{ and } y - z = 4k' \\ &\implies \exists (k,k') \in \mathbb{Z}^2,\ x - z = 4(k + k') \\ &\implies x\mathcal{R}z. \\ &\implies \mathcal{R} \text{ is transitive.} \end{aligned}$$

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

2. *The equivalence class of* a *is* $[a] = \{x \in \mathbb{Z} \mid x - a \equiv 0 \pmod 4\}$.

$$[0] = \{\dots,-8,-4,0,4,8,\dots\}, \qquad [1] = \{\dots,-7,-3,1,5,9,\dots\},$$

$$[2] = \{\dots,-6,-2,2,6,10,\dots\}, \qquad [3] = \{\dots,-5,-1,3,7,11,\dots\}.$$

3. *There are exactly* 4 *distinct classes, corresponding to residues* $0,1,2,3 \pmod 4$.

Exercice 32. *Let* $\mathcal{R}$ *be the binary relation on* $\mathbb{R}$ *defined by*

$$x\mathcal{R}y \iff x^4 - y^4 = x^2 - y^2.$$

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

2. *Determine the equivalence class of* 0, *and deduce the equivalence class of* 1.

3. *Detrmine quotient set* $\mathbb{R}/\mathcal{R}$

Solution. 1. • *Reflexive: For every* $x \in \mathbb{R}$, $x^4 - x^4 = 0 = x^2 - x^2$, *so* $x\mathcal{R}x$. *Therefore,* $\mathcal{R}$ *is reflexive.*

- *Symmetric: For any* $(x,y) \in \mathbb{R}^2$,

$$\begin{aligned} x\mathcal{R}y &\implies x^4 - y^4 = x^2 - y^2 \\ &\implies y^4 - x^4 = y^2 - x^2 \\ &\implies y\mathcal{R}x. \\ &\implies \mathcal{R} \text{ is symmetric.} \end{aligned}$$

- *Transitive: For all* $(x,y,z) \in \mathbb{R}^3$,

$$\begin{aligned} (x\mathcal{R}y) \text{ and } (y\mathcal{R}z) &\implies x^4 - y^4 = x^2 - y^2 \quad \text{and} \quad y^4 - z^4 = y^2 - z^2. \\ &\implies x^4 - z^4 = x^2 - z^2, \\ &\implies x\mathcal{R}z. \\ &\implies \mathcal{R} \text{ is transitive.} \end{aligned}$$

Thus R is reflexive, symmetric and transitive, i.e. an equivalence relation on $\mathbb{R}$.

2. *Equivalence classes of* 0 *and* 1.

- *Compute the class of* 0*:*

$$\dot{0} = \{y \in \mathbb{R} \mid 0Ry\} = \{y \in \mathbb{R} \mid -y^4 = -y^2\} = \{y \in \mathbb{R} \mid y^4 = y^2\}.$$

Thus $y^2(y^2 - 1) = 0$, *so* $y \in \{-1,0,1\}$. *Therefore,* $\dot{0} = \{-1,0,1\}$.

- *Similarly for* 1*:*

$$\dot{1} = \{y \in \mathbb{R} \mid 1^4 - y^4 = 1^2 - y^2\} = \{y \in \mathbb{R} \mid y^4 = y^2\} = \{-1,0,1\}.$$

3. *From the characterization, we have:* $x\mathcal{R}y \iff x^2 = y^2 \quad or \quad x^2 + y^2 = 1$, *we deduce that each equivalence class is of the form* $[x] = \{\, y \in \mathbb{R} \mid y^2 = x^2 \text{ or } x^2 + y^2 = 1 \,\}$.

In particular:

- *If* $x^2 \neq 0$ *and* $x^2 \neq 1$, *then:* $[x] = \{\, x, -x, \sqrt{1 - x^2}, -\sqrt{1 - x^2} \,\}$.
- *For* $x = 0$ *or* $x = \pm 1$, $[x] = \{-1,0,1\}$.

Chapter 4

Agebraic structures

An algebraic structures is a set equipped with one or more operations that satisfy specific properties. Such structures form the foundation of modern algebra and are widely used in number theory.

4.1 Internal Composition Laws

4.1.1 Definition

Definition 4.1.1. *Let E be a non-empty set. A **law of internal composition** (or **internal binary operation**) on E is a function from $E \times E$ to E associating every pair (x,y) in $E \times E$ with an element of E, denoted as $x * y$:*

$$\begin{array}{rcl} * : E \times E & \longrightarrow & E \\ (x,y) & \longmapsto & *(x,y) = x * y \end{array}.$$

Remark 4.1.2. *The internal composition law can be noted by $*$, $\star$, $+$, $\times$, $\circ$, $\perp$, $\top$,$\diamond$,..., or other symbols.*

Example 4.1.3.

1. *Intersection and union constitute internal composition laws on the power set of the set E.*
2. *If $E = \mathbb{R}$: Addition*

$$\begin{array}{rcl} + : \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & x + y \end{array}.$$

3. *And, if $E = \mathbb{R}$: Multiplication*

$$\begin{array}{rcl} \times : \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ (x,y) & \longmapsto & x \times y \end{array}.$$

It is an internal composition law.

4. *On $\mathbb{N}$, subtraction $(x,y) \mapsto x - y$ is* not *an internal law, since $x - y$ may not belong to $\mathbb{N}$.*

4.1.2 Properties of Internal Composition Laws

Let $(E,*)$ and $(E,\top)$ are two internal composition laws on E. We study several important properties that this law may satisfy:

Definition 4.1.4. *(**Commutativity**) We say that $*$ is commutative if and only if:*

$$x * y = y * x, \quad \forall (x,y) \in E^2.$$

Example 4.1.5. *We define on $\mathbb{R}$ the internal composition law by :*

$$t * s = t + s + 1,$$

we have:

$$\begin{array}{rcl} t * s & = & t + s + 1 \\ & = & s + t + 1 \\ & = & s * t. \end{array}$$

Thus, $*$ is commutative.

Definition 4.1.6. *(**Associativity**) We say that $*$ is Associative if and only if:*

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

Example 4.1.7. *We define on $\mathbb{R}$ the internal composition law by:*

$$t * s = t + s + 1$$

we have:

$$\begin{aligned}(t*s)\star r &= (t+s+1)+r+1\\ &= t+s+r+2.....(1)\end{aligned}$$

$$\begin{aligned}t*(s*r) &= t+(s+r+1)+1\\ &= t+s+r+2.....(2)\end{aligned}$$

When (1) *and* (2). *Hence, the operation* $*$ *is associative.*

Definition 4.1.8. *(**Identity element**) We say that* $*$ *is identity element if and only if:*

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

The element e *is called the* ***neutral element*** *of* $(E,*)$.

Remark 4.1.9. *The neutral element, if it exists, is unique. Indeed let* e' *be another neutral element for* $*$*,then*

$$e' = e'*e = e*e' = e.$$

Example 4.1.10. *We define on* $\mathbb{R}$ *the internal composition law by*

$$t*s = t+s+1$$

Let e *be the neutral element such that* $t*e = t$.

$$t+e+1 = t \quad \Rightarrow \quad e = -1.$$

Therefore, the neutral element is $e = -1$.

Definition 4.1.11. *(**Inverse element**) We assume that E has a neutral element* e *for* $*$. *We say that* $*$ *is inverse element (or* ***symmetric element****) if and only if:*

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

The element x' *is called the* inverse *of* x, *denoted* x^{-1}.

Example 4.1.12. *We define on $\mathbb{R}$ the internal composition law by*

$$t * s = t + s + 1.$$

The symmetric element of t with respect to $*$ is t' such that $t * t' = e = -1$.

$$t + t' + 1 = -1 \quad \Rightarrow \quad t' = -2 - t.$$

Hence, the symmetric element of t is $t' = -2 - t$.

Definition 4.1.13. *Let $*$ and $\top$ be two binary operations (**laws of internal composition**) defined on a set E.*

- *The operation $\top$ is said to be **left distributive** with respect to $*$ if*

$$\forall (a,b,c) \in E^3, \quad a \top (b * c) = (a \top b) * (a \top c).$$

- *The operation $\top$ is said to be **right distributive** with respect to $*$ if*

$$\forall (a,b,c) \in E^3, \quad (b * c) \top a = (b \top a) * (c \top a).$$

*The operation $\top$ is said to be **distributive** with respect to $\star$ if it is both left and right distributive with respect to $\star$.*

Example 4.1.14. *Let $E = \mathbb{R}$. Define two binary operations on E by*

$$t \top s = t + s + 1 \quad \text{and} \quad t * s = t + s.$$

We examine whether the operation $\top$ is distributive with respect to $*$.

- *Left distributivity. We test whether: $a \top (b * c) = (a \top b) * (a \top c)$.*

$$a \top (b * c) \quad = \quad a \top (b + c) = a + b + c + 1, \ldots\ldots (1).$$

$$\begin{aligned} (a \top b) * (a \top c) &= a(a + b + 1) + (a + c + 1) \\ &= 2a + b + c + 2 \ldots\ldots\ldots\ldots\ldots (2). \end{aligned}$$

Since $(1) \neq (2)$, the operation $\top$ is not left distributive with respect to $*$.

- *Right distributivity. We test whether:* $(b*c)\top a = (b\top a)*(c\top a)$.

$$(b+c)\top a = b+c+a+1, \ldots\ldots\ldots\ldots\ldots\ldots(1).$$

$$\begin{aligned}(b\top a)*(c\top a) &= (b+a+1)+(c+a+1)\\ &= 2a+b+c+2\ldots\ldots\ldots\ldots\ldots(2).\end{aligned}$$

Since $(1)\neq(2)$*, the operation* $\top$ *is not right distributive with respect to* $*$.

Example 4.1.15. *Let* $E=\mathbb{R}$*. Define two binary operations on* E *by*

$$a*b=a+b \quad \text{and} \quad a\top b=a\times b.$$

We show that the operation $\top$ *is distributive with respect to* $*$.

- *Left distributivity. For all* $a,b,c\in\mathbb{R}$,

$$\begin{aligned}a\top(b*c) &= a\times(b+c)\\ &= (a\times b)+(a\times c)\\ &= (a\top b)*(a\top c).\end{aligned}$$

- *Right distributivity. For all* $a,b,c\in\mathbb{R}$,

$$\begin{aligned}(b*c)\top a &= (b+c)\times a\\ &= (b\times a)+(c\times a)\\ &= (b\top a)*(c\top a).\end{aligned}$$

The operation $\top$ *(multiplication) is both left and right distributive with respect to* $*$ *(addition). Hence,* $\top$ *is distributive with respect to* $*$.

Definition 4.1.16. ***(Idempotence)****. Let* E *be a set and let* $*$ *be a binary operation on* E*. The operation* $*$ *is said to be* ***idempotent*** *if* $\forall x\in E, \quad x*x=x$.

Example 4.1.17. *Let* $E=\mathbb{R}$ *and define* $x*y=\max(x,y)$.
Then, for all $x\in\mathbb{R}$, $x*x=\max(x,x)=x$.
Hence, the operation $*$ *is idempotent.*

4.1.3 Stable part

Definition 4.1.18. *Let E be a set equipped with a binary operation $*$. A subset $F \subseteq E$ is said to be **stable** (or **closed**) under the operation $*$ if and only if*

$$\forall a, b \in F, \quad a * b \in F.$$

Example 4.1.19. *The set $\mathbb{N}$ is a subset of $\mathbb{R}$ that is stable under the internal operations $+$ and $\times$, since the sum and the product of two natural numbers are again natural numbers.*

4.2 Group Structure

4.2.1 Definition

Definition 4.2.1. *Let $*$ be an internal composition law on a non-empty set E.*
*We say that $(E, *)$ is a **group** if and only if:*

1. *$*$ is a **law of internal composition** on E.*
2. *$*$ is **associative**,*
3. *$*$ admits a **neutral element**,*
4. *Every element of E is **invertible** with respect to $*$.*

*It is also said that the set E has a **group structure for the law** $*$.*

Remark 4.2.2. *If $*$ is commutative, the group is called **Abelian** or **(Commutative)**.*

Example 4.2.3.

1. *The structures $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are commutative groups.*
2. *The structures $(\mathbb{Q}, \times)$, $(\mathbb{R}, \times)$ and $(\mathbb{C}, \times)$ are not groups, since 0 has no inverse for the usual multiplication.*
3. *The structure $(\mathbb{Z}, *)$ defined by $n * m = n - m$ is not a group.*

4.2.2 Subgroup

Definition 4.2.4. *Let $(E,*)$ be a group and let H be a subset of E, that is, $H \subseteq E$. The set H is called a* ***subgroup*** *of $(E,*)$ if and only if H is nonempty, is stable under the operation $*$, and, when endowed with the operation induced by $*$, forms a group.*

Definition 4.2.5. *Let $(E,*)$ be a group and let H be a nonempty subset of E. We say that $(H,\star)$ is a* ***subgroup*** *of $(E,*)$ if and only if:*

1. *$e \in H$;*
2. *for all $x,y \in H$, we have $x * y \in H$;*
3. *for all $x \in H$, the inverse element $x^{-1} \in H$.*

Proposition 14. *(**Characterization of a Subgroup**). Let H be a subset of a group $(E,*)$. The subset H is a subgroup of E if and only if :*

$$e \in H \quad \textit{and} \quad \forall x,y \in H,\ x * y^{-1} \in H$$

Proof. **(⇒)** Assume that H is a subgroup of $(E,*)$. Since H is a subgroup, it contains the identity element e of E.
Moreover, since H is stable under the group operation and taking inverses, for all $x,y \in H$, we have $y^{-1} \in H$ and therefore $x * y^{-1} \in H$. Thus the stated conditions are satisfied.

(⇐) Conversely, assume that $e \in H$ and that $\forall x,y \in H,\ x * y^{-1} \in H$.

1. Let $x \in H$. Taking $y = x$ in the condition, we obtain $x * x^{-1} = e \in H$, which is already satisfied. Now, taking $x = e$ and $y = x$, we get: $e * x^{-1} = x^{-1} \in H$.
2. Let $x,y \in H$. Since $y^{-1} \in H$ by Step 1, applying the given condition yields

$$x * (y^{-1})^{-1} = x * y \in H.$$

   Thus H is closed under the group operation.

Since H contains the identity, is closed under inverses, and is closed under the operation, H is a subgroup of $(E,*)$. ■

Example 4.2.6. .

1. *$2\mathbb{Z}$ is a subgroup of $(\mathbb{Z},+)$. Indeed, $0 \in 2\mathbb{Z}$; if $2a, 2b \in 2\mathbb{Z}$ then $2a+2b = 2(a+b) \in 2\mathbb{Z}$; and the inverse of $2a$ is $-2a = 2(-a) \in 2\mathbb{Z}$.*

2. *$\{\pm 1\}$ is a subgroup of $(\mathbb{R}^*,\times)$. The neutral element 1 belongs to $\{\pm 1\}$; products of ± 1 lie in $\{\pm 1\}$; and each element is its own inverse.*

3. *The unit circle $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ is a subgroup of $(\mathbb{C}^*,\times)$. We have $1 \in S^1$; if $|z| = |w| = 1$ then $|zw| = 1$ so closure holds; and $z^{-1} = \overline{z}$ with $|\overline{z}| = 1$.*

Exercice 33. *Let $(\mathbb{R}^2,+)$ be the additive group and define by:*

$$H = \{(x,y) \in \mathbb{R}^2 \mid 2x + y = 0\}.$$

We show that H is a subgroup of $(\mathbb{R}^2,+)$.

Proof.

1. Identity: $(0,0) \in \mathbb{R}^2$ and $2 \cdot 0 + 0 = 0$, hence $(0,0) \in H$.

2. Closure under addition: If $(x_1,y_1),(x_2,y_2) \in H$, then

$$2(x_1 + x_2) + (y_1 + y_2) = (2x_1 + y_1) + (2x_2 + y_2) = 0 + 0 = 0,$$

   so $(x_1 + x_2, y_1 + y_2) \in H$.

3. Inverses: If $(x,y) \in H$, then $2x + y = 0$ and $2(-x) + (-y) = -(2x + y) = 0$,

   thus $(-x,-y) \in H$.

Since H is nonempty and closed under addition and inverses, H is a subgroup of $(\mathbb{R}^2,+)$.

■

Remark 4.2.7. 1. *The intersection of two subgroups of a group is itself a subgroup.*

2. *In general, the union of two subgroups of a group is not a subgroup.*

3. *For any group E, the singleton set $\{e\}$, where e denotes the identity element, and the group E itself are subgroups of E.*

4.2.3 Group Homomorphism

Definition 4.2.8. *et $(E,*)$ and $(E,\top)$ be two groups, and let f be a map from $(E,*)$ to $(E,\top)$. The map f is called a **group homomorphism** if:*

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

Example 4.2.9. *Let*

$$\begin{array}{rccc} f: & (\mathbb{R},+) & \longrightarrow & (\mathbb{R}^{*,+},\times) \\ & x & \longmapsto & f(x)=e^x. \end{array}$$

Then

$$\begin{aligned} f(x+y) &= e^{x+y} \\ &= e^x \times e^y \\ &= f(x) \times f(y) \end{aligned}$$

So f is an homomorphism.

Theorem 4.2.10. *Let f be a homomorphism from the group $(E,*)$ to the group $(E',\top)$, with neutral elements $e \in E$ and $e' \in E'$. Then:*

1. *$f(e) = e'$,*
2. *for every $x \in E$, $\big(f(x)\big)^{-1} = f(x^{-1})$.*

Proof.

1. Since f is a homomorphism, $f(e) = f(e*e) = f(e) \top f(e)$.

   Multiplying on the right by $\big(f(e)\big)^{-1}$ yields $f(e) = e'$.

2. For any $x \in E$ we have

   $$f(x) \top f(x^{-1}) = f(x * x^{-1}) = f(e) = e',$$

   and likewise $f(x^{-1}) \top f(x) = e'$. Hence $f(x^{-1})$ is the inverse of $f(x)$, so $\big(f(x)\big)^{-1} = f(x^{-1})$.

■

Definition 4.2.11. *Let $f : (E,*) \to (E',\top)$ be a group homomorphism, where e and e' denote the identity elements of E and E', respectively.*

- *The **kernel** of f is defined by*

$$\mathrm{Ker}(f) = \{\, x \in E \mid f(x) = e' \,\}.$$

- *The **image** of f is defined by*

$$\mathrm{Im}(f) = \{\, f(x) \in E' \mid x \in E \,\}.$$

Proposition 15. *Let $f : (E,*) \to (E',\top)$ be a group homomorphism, with identity elements $e \in E$ and $e' \in E'$. Then:*

1. *The image of f is a subgroup of E'.*
2. *The kernel of f is a subgroup of E.*
3. *The homomorphism f is injective if and only if $\mathrm{Ker}(f) = \{e\}$.*
4. *The homomorphism f is surjective if and only if $\mathrm{Im}(f) = E'$.*

Proof.

1. Recall that: $\mathrm{Im}\, f = \{f(x) \mid x \in E\}$.
   - Since $f(e) = e'$, we have $e' \in \mathrm{Im}\, f$.
   - Let $y, y' \in \mathrm{Im}\, f$. There exist $x, x' \in E$ such that $y = f(x)$ and $y' = f(x')$. Then

$$y \top y' = f(x) \top f(x') = f(x * x') \in \mathrm{Im}\, f.$$

   - Let $y \in \mathrm{Im}\, f$. There exists $x \in E$ such that $y = f(x)$. Then

$$y^{-1} = f(x)^{-1} = f(x^{-1}) \in \mathrm{Im}\, f.$$

   Thus, $\mathrm{Im}\, f$ is a subgroup of E'.

2. Recall that $\ker f = \{x \in E \mid f(x) = e'\}$.
   - Since f is a homomorphism, we have $f(e) = e'$, hence $e \in \ker f$.

- Let $x, x' \in \ker f$. Then

$$f(x * x') = f(x) \top f(x') = e' \top e' = e',$$

so $x * x' \in \ker f$.

- Let $x \in \ker f$. Then

$$f(x^{-1}) = f(x)^{-1} = e'^{-1} = e',$$

hence $x^{-1} \in \ker f$.

Therefore, $\ker f$ is a subgroup of E.

3. **(⇒)** Assume that f is injective. Let $x \in \mathrm{Ker}(f)$. Then

$$f(x) = e' = f(e).$$

Since f is injective, it follows that $x = e$. Hence, $\mathrm{Ker}(f) = \{e\}$.

(⇐) Assume that $\mathrm{Ker}(f) = \{e\}$. Let $x, y \in E$ such that $f(x) = f(y)$. Then

$$f(x) \top f(y)^{-1} = e',$$

which implies

$$f(x * y^{-1}) = e'.$$

Thus $x * y^{-1} \in \mathrm{Ker}(f)$. Since the kernel is trivial, we have $x * y^{-1} = e$, and therefore $x = y$. Hence, f is injective.

4. **(⇒)** Assume that f is surjective. By definition of surjectivity, for every $y \in E'$ there exists $x \in E$ such that

$$f(x) = y.$$

Hence every element of E' belongs to the image of f, and therefore $\mathrm{Im}(f) = E'$.

(⇐) Assume that $\mathrm{Im}(f) = E'$. Then for every $y \in E'$ there exists $x \in E$ such that

$$y = f(x).$$

This is precisely the definition of surjectivity. Hence f is surjective.

■

Example 4.2.12. *(Reduction modulo n). Let*

$$\begin{array}{rccc} f: & (\mathbb{Z},+) & \longrightarrow & (\mathbb{Z}_n,+) \\ & k & \longmapsto & f(k)=k \pmod{n}. \end{array}$$

We have

$$f(a+b)\equiv a+b\equiv f(a)+f(b) \pmod{n}.$$

$\ker f = n\mathbb{Z}$, $\operatorname{Im} f = \mathbb{Z}_n$.

4.2.4 Group isomorphism

Definition 4.2.13. ***(Types of Homomorphisms)*** *Let $f: E \to E'$ be a group homomorphism. Then:*

- *f is a **monomorphism** if it is injective (one-to-one).*
- *f is an **epimorphism** if it is surjective (onto).*
- *f is an **isomorphism** if it is bijective; in this case, the groups E and E' are said to be* isomorphic, *denoted $E \simeq E'$.*
- *f is an **endomorphism** if it is a homomorphism from E to itself, i.e., $f: E \to E$.*
- *f is an **automorphism** if it is a bijective endomorphism, i.e., $f: E \to E$ is bijective.*

Example 4.2.14. *Consider the function*

$$\begin{array}{rccc} f: & (\mathbb{R},+) & \longrightarrow & (\mathbb{R}^{*,+},\times) \\ & x & \longmapsto & f(x)=e^x. \end{array}$$

Then f is a group isomorphism.
Indeed:

- *f is an homomorphism.*
- *f is bijective, since the exponential function is strictly increasing and its image is $\mathbb{R}_+^*$.*

Hence, f is an isomorphism of groups.

4.2.5 Finite $\mathbb{Z}/n\mathbb{Z}$ Groups

Definition 4.2.15. *Let $n \geq 1$ be a fixed integer. Recall that*

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

where each element $\overline{p}$ (or noted $[p]$) represents the equivalence class of the integer p modulo n. That is, for any $p, q \in \mathbb{Z}$,

$$\overline{p} = \overline{q} \iff p \equiv q \pmod{n} \iff \exists k \in \mathbb{Z} : p - q = kn.$$

Definition 4.2.16. *We define **addition** on $\mathbb{Z}/n\mathbb{Z}$ by:*

$$\overline{p} + \overline{q} = \overline{p+q},$$

*and **multiplication** by:*

$$\overline{p} \times \overline{q} = \overline{p.q}$$

Example 4.2.17. *In the group $\mathbb{Z}/12\mathbb{Z}$*

1. *Addition modulo 12*

$$\overline{10} + \overline{5} \equiv \overline{15} \equiv \overline{3} \pmod{12}, \quad \overline{7} + \overline{5} \equiv \overline{12} \equiv \overline{0} \pmod{12}.$$

2. *Multiplication modulo 12*

$$\overline{10 \cdot 5} \equiv \overline{50} \equiv \overline{2} \pmod{12}, \quad \overline{7 \cdot 5} \equiv \overline{35} \equiv \overline{11} \pmod{12}.$$

Proposition 16. *The set $\mathbb{Z}/n\mathbb{Z}$ equipped with this addition forms a group $(\mathbb{Z}/n\mathbb{Z}, +)$. Moreover, this group is abelian.*

Proof.

1. Closure: For any $\overline{p}, \overline{q} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{p} + \overline{q} = \overline{p+q} \in \mathbb{Z}/n\mathbb{Z}$.

2. Associativity: For any $\overline{p}, \overline{q}, \overline{r} \in \mathbb{Z}/n\mathbb{Z}$,

$$(\overline{p} + \overline{q}) + \overline{r} = \overline{p+q} + \overline{r} = \overline{(p+q)+r} = \overline{p+(q+r)} = \overline{p} + (\overline{q} + \overline{r}).$$

3. Identity: $\overline{0}$ is the identity element since $\overline{p}+\overline{0}=\overline{p+0}=\overline{p}$.

4. Inverse: For each $\overline{p}$, the class $\overline{n-p}$ is the additive inverse, because $\overline{p}+\overline{n-p}=\overline{n}=\overline{0}$.

5. Commutativity: For all $\overline{p},\overline{q}$,

$$\overline{p}+\overline{q}=\overline{p+q}=\overline{q+p}=\overline{q}+\overline{p}.$$

So group $(\mathbb{Z}/n\mathbb{Z},+)$ is group abelian. ■

Example 4.2.18. *Let* $\mathbb{Z}/5\mathbb{Z}=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\}$.

- ***The addition table*** *is given below:*

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

- ***The multiplication table*** *is given below:*

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

4.2.6 Group of Permutations $\mathcal{S}_3$

Definition 4.2.19. *Let* $n\geq 1$ *be an integer, and consider the set* $X=\{1,2,\ldots,n\}$. *The set of all bijections from* X *to itself, equipped with the composition of functions, forms a group, denoted by* $(\mathcal{S}_n,\circ)$.
A bijection $f:X\to X$ *is called a* ***permutation*** *of* X. *The group* $(\mathcal{S}_n,\circ)$ *is called the* ***symmetric group*** *(or the* ***group of permutations****) of degree* n.

Definition 4.2.20. *Let $n \geq 1$ be an integer, and let $X = \{1,2,\ldots,n\}$. A **permutation** of X is a bijective function*

$$f : X \longrightarrow X.$$

The set of all permutations of X, equipped with the composition of functions, forms the symmetric group $\mathcal{S}_n$. A permutation can be represented in two-line notation as

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}.$$

Proposition 17. ***(Properties of Permutations)** Let $f, g \in \mathcal{S}_n$ be permutations of $X = \{1,2,\ldots,n\}$. Then:*

1. ***Closure:** The composition $g \circ f \in \mathcal{S}_n$.*
2. ***Identity:** The identity permutation*

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$$

   is the neutral element in $\mathcal{S}_n$.
3. ***Inverse:** Every permutation $f \in \mathcal{S}_n$ has a unique inverse $f^{-1} \in S_n$ such that*

$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}.$$

4. ***Non-commutativity:** For $n \geq 3$, there exist permutations $f, g \in \mathcal{S}_n$ such that*

$$f \circ g \neq g \circ f.$$

Example 4.2.21. *Consider $\mathcal{S}_7$ and the permutation*

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 6 & 1 & 2 \end{pmatrix}.$$

1. ***Composition:** Let*

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 1 & 7 & 5 & 6 \end{pmatrix}.$$

Then the composition $g \circ f$ is obtained by applying f first, then g:

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 7 & 1 & 5 & 4 & 3 \end{pmatrix}.$$

2. ***Inverse:*** *The inverse of f is obtained by swapping rows and reordering columns to match the top row:*

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 1 & 4 & 3 & 5 & 2 \end{pmatrix}.$$

Proposition 18. *Let $\mathcal{S}_n$ be the symmetric group of degree n, i.e., the group of all permutations of the set $\{1,2,\ldots,n\}$. Then the **cardinality** of $\mathcal{S}_n$ is $|\mathcal{S}_n| = n!$.*

Proof. A permutation of n elements is a bijection from the set $\{1,2,\ldots,n\}$ to itself.

- There are n choices for the image of the first element.
- There are $n-1$ remaining choices for the image of the second element.
- Continuing in this way, there are $n-2, n-3, \ldots, 1$ choices for the subsequent elements.

By the multiplication principle, the total number of permutations is

$$n \times (n-1) \times \cdots \times 2 \times 1 = n!.$$

Hence, $|\mathcal{S}_n| = n!$. ■

Group of $\mathcal{S}_3$

Definition 4.2.22. *Let $X = \{1,2,3\}$. The set of all bijections from X to itself, equipped with the composition of functions, forms a group called the **symmetric group of degree** 3, denoted by $\mathcal{S}_3$:*

$$\mathcal{S}_3 = \{f : X \to X \mid f \text{ is bijective}\}.$$

The symmetric group $\mathcal{S}_3$, consisting of all permutations of $\{1,2,3\}$, has $3! = 6$ elements, which we enumerate as follows:

$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ *(the identity permutation),*

$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ *(a transposition)*,

$\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ *(a second transposition)*,

$\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ *(a third transposition)*,

$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *(a 3-cycle)*,

$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ *(the inverse of the 3-cycle)*.

Hence, we have:

$$\mathcal{S}_3 = \{\mathrm{id}, \tau_1, \tau_2, \tau_3, \sigma, \sigma^{-1}\}.$$

The group operation is the composition of permutations. The Cayley table of $\mathcal{S}_3$ is given below, where the entry in row g and column f is $g \circ f$.

$\circ$	id	τ_1	τ_2	τ_3	σ	σ^{-1}
id	id	τ_1	τ_2	τ_3	σ	σ^{-1}
τ_1	τ_1	id	σ	σ^{-1}	τ_2	τ_3
τ_2	τ_2	σ^{-1}	id	σ	τ_3	τ_1
τ_3	τ_3	σ	σ^{-1}	id	τ_1	τ_2
σ	σ	τ_3	τ_1	τ_2	σ^{-1}	id
σ^{-1}	σ^{-1}	τ_2	τ_3	τ_1	id	σ

Remark 4.2.23. *This table shows explicitly that the group $\mathcal{S}_3$ is not commutative, since in general*

$$g \circ f \neq f \circ g.$$

Example 4.2.24. *Let us compute $\tau_1 \circ \sigma$ and $\sigma \circ \tau_1$.*

Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Computation of $\tau_1 \circ \sigma$ and $\sigma \circ \tau_1$.

$$\tau_1 \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau_2, \qquad \sigma \circ \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \tau_3.$$

Since

$$\tau_1 \circ \sigma \neq \sigma \circ \tau_1,$$

the group $\mathcal{S}_3$ is not commutative.
More generally, the symmetric group $\mathcal{S}_n$ is not commutative for all $n \geq 3$.

Proposition 19. *The symmetric group $\mathcal{S}_3$ has the following subgroups:*

- *The trivial subgroup $\{\mathrm{id}\}$ and the whole group $\mathcal{S}_3$ itself.*
- *The subgroups of order 2: $\{\mathrm{id}, \tau_i\}$ for $i = 1,2,3$, where τ_i are the transpositions.*
- *The cyclic subgroup of order 3: $\{\mathrm{id}, \sigma, \sigma^{-1}\}$, generated by the 3-cycle σ.*

4.3 Rings Structure

4.3.1 Definition

Definition 4.3.1. *Let A be a non-empty set containing at least two elements, equipped with two internal composition laws (denoted $+$ and $\times$). Then $(A, +, \times)$ is called a **ring** if:*

1. *$(A, +)$ is a commutative group with identity 0_A.*
2. *$\times$ is associative.*
3. *$\times$ is distributive with respect to $+$.*

Remark 4.3.2.

- *If $\times$ is commutative, the ring is said to be **commutative**.*
- *if $\times$ has an identity element 1_A, the ring is said to be **unitary**.*

Example 4.3.3.

- *$(\mathbb{R}, +, \times)$ is a commutative rings.*
- *$(\mathbb{R}^2, +, \times)$ is a commutative rings.*
- *$(\mathbb{Z}, +, \times)$ is a commutative rings.*

4.3.2 Calculation Rules in a Ring

Let $(A,+,\times)$ be a ring and let $a,b \in A$. Then the following properties hold:

1. **Multiplication by zero:** $a \times 0_A = 0_A \times a = 0_A$.
2. **Compatibility with integers:** For all $n \in \mathbb{Z}$, $n(ab) = (na)b = a(nb)$.
3. **Product of opposites:** $(-a)(-b) = ab$.

Proposition 20. *(**Binomial Formulas**) Let $(A,+,\times)$ be a ring and let $x,y \in A$ such that $xy = yx$. Then, for all $n \in \mathbb{N}$, the following formulas hold:*

1. ***Binomial theorem:***
$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$
2. ***Difference of powers:***
$$x^n - y^n = (x-y) \sum_{k=0}^{n-1} x^k y^{n-1-k}.$$

Remark 4.3.4. *The commutativity condition $xy = yx$ is essential for the validity of the binomial formulas. In particular, these formulas hold in any commutative ring.*

Example 4.3.5. *In the ring $(\mathbb{Z},+,\times)$ and take $x = 5$, $y = 2$, and $n = 3$. Then:*

1. *In Binomial theorem:*
$$(2+3)^3 = 5^3 = 125,$$
and
$$\sum_{k=0}^{3} \binom{3}{k} 2^k 3^{3-k} = 27 + 54 + 36 + 8 = 125.$$
2. *In Difference of powers:*
$$x^3 - y^3 = 5^3 - 2^3 = 125 - 8 = 117.$$
Using the formula:
$$(x-y) \sum_{k=0}^{2} x^k y^{2-k} 3(4+10+25) = 3 \times 39 = 117.$$

Thus, the identity is verified in the ring $\mathbb{Z}$.

4.3.3 Sub-Rings

Definition 4.3.6. *Let $(A,+,\times)$ be a ring and B a subset of A ($B \subseteq A$). We say that $(B,+,\times)$ is a **subring** of $(A,+,\times)$ if and only if the following conditions hold:*

1. *$(B,+)$ is a subgroup of $(A,+)$;*
2. *B is closed under multiplication, i.e. $\forall x,y \in B, \quad x \times y \in B$;*
3. *The multiplicative identity of A belongs to B, that is, $1_A \in B$.*

Remark 4.3.7.

- *Every subring of a commutative ring is itself commutative.*
- *Unlike subgroups, a subring is not required to contain the multiplicative identity of the ring, unless this is explicitly stated.*

Example 4.3.8.

1. *The set $\mathbb{Z}$ is a subring of $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.*
2. *The set $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ is a subring of $\mathbb{Z}$.*
3. *The set of all polynomials with integer coefficients $\mathbb{Z}[X]$ is a subring of $\mathbb{R}[X]$.*

Exercice 34. *Show that $\mathbb{Z}$ is a subring of $\mathbb{Q}$?*

Solution. *Let $H = \mathbb{Z} \subset \mathbb{Q}$. We verify the subring conditions.*

1. *The multiplicative identity of $\mathbb{Q}$ is 1, and $1 \in \mathbb{Z}$.*
2. *We have $0 \in \mathbb{Z}$, the sum of two integers is an integer, and the additive inverse of any integer is also an integer. Hence $(\mathbb{Z},+)$ is a subgroup of $(\mathbb{Q},+)$.*
3. *If $a,b \in \mathbb{Z}$, then $a \times b \in \mathbb{Z}$.*

Therefore, $(\mathbb{Z},+,\times)$ is a subring of $(\mathbb{Q},+,\times)$.

Proposition 21. ***(Unital Subring Criterion).*** *Let $(A,+,\times)$ be a ring with identity 1_A and let $B \subseteq A$. Then B is a **unitary (or unital) subring** of A (i.e., a subring containing the same identity as A) if and only if:*

1. *$1_A \in B$,*
2. *$\forall x,y \in B,\ x - y \in B$,*
3. *$\forall x,y \in B,\ x \times y \in B$.*

Remark 4.3.9. *The intersection of any family of subrings of a ring A is again a subring of A.*

4.3.4 Invertible Elements and Zero Divisors

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

Definition 4.3.10. *(**Invertible Elements**). An element $x \in A$ is called **invertible** (or a **unit**) if there exists $y \in A$ such that*

$$x \times y = y \times x = 1_A,$$

*where 1_A is the multiplicative identity of A. The element y is called the **inverse** of x and is denoted by x^{-1}.*
The set of all invertible elements of A is denoted by $A^\times$ and forms a group under multiplication.

Example 4.3.11. .

1. *In the ring $\mathbb{Z}$, the only invertible elements are 1 and -1.*
2. *In $\mathbb{Q}$, every nonzero element is invertible.*

Definition 4.3.12. *(**Zero Divisors**). Let $(A, +, \times)$ be a ring. An element $x \in A \setminus \{0\}$ is called a **zero divisor** if there exists $y \in A \setminus \{0\}$ such that*

$$x \times y = 0 \quad \text{or} \quad y \times x = 0.$$

- *If $x \times y = 0$, then x is called a **left zero divisor**.*
- *If $y \times x = 0$, then x is called a **right zero divisor**.*

*If both hold, x is a **two-sided zero divisor** (or simply a **zero divisor**).*

Example 4.3.13. *In the ring $\mathbb{Z}/6\mathbb{Z}$, we have:*

$$\overline{2} \times \overline{3} = \overline{0}, \ \text{but} \ \overline{2} \neq \overline{0} \ \text{and} \ \overline{3} \neq \overline{0}.$$

Therefore, $\overline{2}$ and $\overline{3}$ are zero divisors.

Remark 4.3.14.

1. *No invertible element can be a zero divisor. Indeed, if x is invertible in a ring A with inverse x^{-1}, and $x \times y = 0$, then multiplying both sides by x^{-1} gives*

$$x^{-1} \times (x \times y) = (x^{-1} \times x) \times y = 1 \times y = y = 0.$$

   Hence $y = 0$, which shows that x cannot be a zero divisor.

2. *A ring with no zero divisors (i.e., $x \times y = 0 \implies x = 0$ or $y = 0$) is called an **integral domain**.*

4.3.5 Ring Homomorphism

Let $(A,+,\times)$ and $(A',\oplus,\odot)$ be two rings.

Definition 4.3.15. *A function*

$$f : A \longrightarrow A'$$

is called a ***ring homomorphism*** *if for all $x,y \in A$, the following conditions hold:*

1. $f(x+y) = f(x) \oplus f(y)$ ***(preserves addition)***,
2. $f(x \times y) = f(x) \odot f(y)$ ***(preserves multiplication)***,
3. $f(1_A) = 1_A$ ***(preserves the multiplicative identity)***, *if the rings are* ***unital***.

Example 4.3.16. *The map $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ defined by $\varphi(a) = [a]_n$ is a ring homomorphism, where $[a]_n$ means the equivalence class of the integer a modulo n.*

Definition 4.3.17. *Let $f : A \longrightarrow A'$ be a ring homomorphism.*

- *The* ***kernel*** *of f is* $\ker(f) = \{x \in A \mid f(x) = 0_{A'}\}$.
- *The* ***image*** *of f is* $\mathrm{Im}(f) = \{\varphi(x) \mid x \in A\}$.

Proposition 22. 1. $\ker(\varphi)$ *is an ideal of E.*

2. $\mathrm{Im}(\varphi)$ *is a subring of F.*

4.3.6 Ideal

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

Definition 4.3.18. *A nonempty subset $I \subseteq A$ is called a* ***left ideal*** *of A if:*

1. $(I,+)$ *is a subgroup of* $(A,+)$,
2. $\forall a \in A, \forall x \in I, \quad a \times x \in I$.

Similarly, I is a ***right ideal*** *if:* $\forall a \in E, \forall x \in I, \quad x \times a \in I$.
If I is both a left and right ideal, it is called a ***two-sided ideal*** *(or simply an* ***ideal****) of E.*

Example 4.3.19. 1. *In the ring $\mathbb{Z}$, the set $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ is an ideal for any integer n.*

2. *In the ring of* 2×2 *matrices* $M_2(\mathbb{R})$*, the set of matrices with zero in the second row*

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a,b \in \mathbb{R} \right\}$$

is a left ideal but not a right ideal.

Proposition 23. *Let* I *be an ideal of* A*.*

1. $0_A \in I$*.*
2. *For all* $x,y \in I$*,* $x - y \in I$*.*
3. *If* $x \in I$ *and* $a \in A$*, then* $a \times x$*;* $x \times a \in I$*.*

Remark 4.3.20. *Ideals are important because they allow the construction of quotient rings: if* I *is a two-sided ideal of* A*, the set*

$$A/I = \{x + I \mid x \in E\}$$

forms a ring called the ***quotient ring*** *of* A *modulo* I*.*

4.4 Fields Structure

4.4.1 Definition

Definition 4.4.1. *A ring* $(F,+,\times)$ *with* $1_F \neq 0$ *is called a* ***field*** *if every nonzero element of* F *is invertible.*

Example 4.4.2. .

1. *The set of rational numbers* $\mathbb{Q}$ *with the usual addition and multiplication is a field.*
2. *The set of integers* $\mathbb{Z}$ *is not a field since most nonzero elements are not invertible in* $\mathbb{Z}$*.*

Proposition 24. *Every field is an* ***integral domain****, that is, it has no zero divisors.*

Proof. Let F be a field and suppose $x, y \in F$ with $x \cdot y = 0$ and $x \neq 0$. Since x is invertible, multiply both sides by x^{-1}:

$$x^{-1} \cdot (x \cdot y) = (x^{-1} \cdot x) \cdot y = 1 \cdot y = y = 0.$$

Hence $y = 0$, which shows that F has no zero divisors. ■

Remark 4.4.3.

- *Every field is a commutative ring with unity.*
- *In a field, the additive identity* 0 *and the multiplicative identity* 1 *are distinct.*
- *Every nonzero element of a field is invertible with respect to multiplication.*

4.4.2 Finite fields: the example of $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number

Theorem 4.4.4. *The ring* $\mathbb{Z}/p\mathbb{Z}$ *is a field if and only if* p *is prime.*

Proof. If p is prime, then for every $\overline{a} \neq \overline{0}$, there exist integers u, v such that $au + pv = 1$. Reducing modulo p, we obtain

$$\overline{a}\,\overline{u} = \overline{1},$$

hence $\overline{a}$ is invertible.
Conversely, if p is not prime, then $p = ab$ with $1 < a, b < p$, and

$$\overline{a}\,\overline{b} = \overline{0},$$

which shows the existence of zero divisors. Therefore, $\mathbb{Z}/p\mathbb{Z}$ cannot be a field. ■

Example 4.4.5. *In* $\mathbb{Z}/5\mathbb{Z}$*, the inverse of* $\overline{2}$ *is* $\overline{3}$*, since*

$$\overline{2} \times \overline{3} = \overline{6} = \overline{1}.$$

Thus, $\mathbb{Z}/5\mathbb{Z}$ *is a finite field with five elements.*

More generally, every finite field has p^n elements for some prime p and integer $n \geq 1$.

4.4.3 The field of $\mathbb{R}$

Definition 4.4.6. *The set $\mathbb{R}$ of real numbers, equipped with the usual addition and multiplication, is called the* field of real numbers.
The field $\mathbb{R}$ is infinite, and every nonzero real number admits a multiplicative inverse. Moreover, $\mathbb{R}$ is an *ordered field*, meaning that it is endowed with a total order compatible with addition and multiplication. It is also *complete*: every Cauchy sequence converges in $\mathbb{R}$.

Example 4.4.7. *The real number 2 is invertible in $\mathbb{R}$, and its inverse is $1/2$ since $2 \times \frac{1}{2} = 1$.*

However, $\mathbb{R}$ is not algebraically closed. For instance, the equation $x^2 + 1 = 0$ has no solution in $\mathbb{R}$.

4.4.4 The field of $\mathbb{C}$

Definition 4.4.8. *The field of complex numbers is defined as $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R},\ i^2 = -1\}$.*
With the usual addition and multiplication, $\mathbb{C}$ is an infinite field containing $\mathbb{R}$ as a subfield. Every nonzero complex number has a multiplicative inverse.

Example 4.4.9. *The inverse of the complex number $1 + i$ is $\frac{1-i}{2}$, since $(1+i)\left(\frac{1-i}{2}\right) = 1$.*

Unlike $\mathbb{R}$, the field $\mathbb{C}$ is not ordered. Its fundamental property is that it is *algebraically closed*.

Theorem 4.4.10. *(Fundamental Theorem of Algebra) Every nonconstant polynomial with coefficients in $\mathbb{C}$ has at least one root in $\mathbb{C}$.*

4.5 Exercises with solutions

Exercice 35. *Let $E = \mathbb{R} \setminus \{-5\}$ be equipped with the binary operation $*$ defined by*

$$\forall (a,b) \in E^2, \qquad a * b = ab + 5(a + b + 4).$$

1. *Verify that $*$ is an internal composition law on E.*

2. *Show that $(E,*)$ is a commutative group.*

3. *Let*

$$\begin{array}{rccc} f: & (\mathbb{R}^*,\cdot) & \longrightarrow & (E,*) \\ & x & \longmapsto & f(x)=x-5. \end{array}$$

Show that f is a group homomorphism, where $\cdot$ denotes the usual multiplication.

Solution. 1. *For all $a,b\in E$, we compute:*

$$a*b=ab+5a+5b+20=(a+5)(b+5)-5.$$

Suppose that $a*b=-5$. Then

$$(a+5)(b+5)-5=-5 \quad\Longrightarrow\quad (a+5)(b+5)=0.$$

Thus $a=-5$ or $b=-5$, which is impossible since $a,b\in E$.

Hence $a*b\neq -5$, and therefore $a*b\in E$. So $*$ is an internal law on E.

2. *Group structure*

- Associativity: *For all $a,b,c\in E$,*

$$\begin{array}{rcl} (a*b)*c & = & (a+5)(b+5)(c+5)-5 \\ & = & a*(b*c). \end{array}$$

- Neutral element: *We look for $e\in E$ such that $a*e=a$ for all $a\in E$:*

$$\begin{array}{rcl} (a+5)(e+5)-5=a & \Longrightarrow & e+5=1 \\ & \Longrightarrow & e=-4. \end{array}$$

Thus, the neutral element is $e=-4$.

- Inverse element: *For $a\in E$, we seek $b\in E$ such that $a*b=-4$:*

$$(a+5)(b+5)-5=-4 \quad\Longrightarrow\quad (a+5)(b+5)=1.$$

Hence, $b=\frac{1}{a+5}-5$. So every element has an inverse in E.

- Commutativity:

$$\begin{aligned} a * b &= (a+5)(b+5) - 5 \\ &= (b+5)(a+5) - 5 \\ &= b * a. \end{aligned}$$

Therefore, $(E, *)$ is a commutative group.

3. *Let $x, y \in \mathbb{R}^*$. Then: $f(xy) = xy - 5$.*

   On the other hand,

$$\begin{aligned} f(x) * f(y) &= (x-5) * (y-5) \\ &= ((x-5)+5)((y-5)+5) - 5 \\ &= xy - 5 \\ &= f(xy) \end{aligned}$$

Hence, f is a group homomorphism.

Exercice 36. *Let $E = \{0,1,2\}$ and define the operation $*$ by:*

$$x * y = (x + 2y) \bmod 3$$

1. *Verify that $*$ is an internal composition law.*
2. *Determine whether $*$ is associative.*
3. *Determine whether $*$ is commutative.*

Solution. 1. *$* : E \times E \to E$ because for all $x, y \in \{0,1,2\}$, $(x + 2y) \bmod 3 \in E$. Thus, $*$ is internal.*

2. *Check associativity:*

$$(x * y) * z = ((x + 2y) + 2z) \bmod 3 = (x + 2y + 2z) \bmod 3$$

$$x * (y * z) = (x + 2(y + 2z)) \bmod 3 = (x + 2y + 4z) \bmod 3 = (x + 2y + z) \bmod 3$$

Since $(x + 2y + 2z) \neq (x + 2y + z) \bmod 3$ in general, $*$ is not associative.

3. *Check commutativity:*

$$x * y = (x + 2y) \bmod 3, \quad y * x = (y + 2x) \bmod 3$$

Generally $x + 2y \neq y + 2x \bmod 3$, *e.g.* $x = 1, y = 2$ *gives* $1 + 4 = 5 \equiv 2 \bmod 3$ *and* $2 + 2 = 4 \equiv 1 \bmod 3$. *Therefore,* $*$ *is not commutative.*

Exercice 37. *Let* $E = \{0,1,2\}$ *with* $x * y = (x + y) \bmod 3$.

1. *Find the neutral element of* $*$.
2. *Find the inverse of each element in* E.
3. *Verify that* $(E,*)$ *forms a group abelian.*

Solution. 1. *An element* $e \in E$ *is neutral if*

$$x * e = e * x = x \quad \forall x \in E.$$

We check: $x * 0 = (x + 0) \bmod 3 = x, \qquad 0 * x = (0 + x) \bmod 3 = x.$

Hence, the neutral element is 0.

2. *The inverse of* $x \in E$ *is an element* $y \in E$ *such that:* $x * y = 0$.

$$\begin{aligned} 0 * 0 = 0 &\Rightarrow 0^{-1} = 0, \\ 1 * 2 = (1 + 2) \bmod 3 = 0 &\Rightarrow 1^{-1} = 2, \\ 2 * 1 = (2 + 1) \bmod 3 = 0 &\Rightarrow 2^{-1} = 1. \end{aligned}$$

3. *Group structure*

- Closure*: For all* $x, y \in E$, $(x + y) \bmod 3 \in E$.
- Associativity*: Addition modulo* 3 *is associative.*
- Identity*:* 0 *is the neutral element.*
- Inverse*: Every element of* E *has an inverse.*
- Commutativity*:*

$$x * y = (x + y) \bmod 3 = (y + x) \bmod 3 = y * x.$$

$(E,*)$ *is an abelian group. (In fact, this group is exactly the cyclic group* $\mathbb{Z}/3\mathbb{Z}$*.)*

Exercice 38. *Show that*

$$H = \{\, x + y\sqrt{3}\,;\ x \in \mathbb{N},\ y \in \mathbb{Z},\ x^2 - 3y^2 = 1 \,\}$$

is a subgroup of $(\mathbb{R}^+, \times)$.

Solution. 1. $H \subset \mathbb{R}^+$ *Let* $x + y\sqrt{3} \in H$. *Since* $x^2 - 3y^2 = 1$, *we must have* $x \geq 1$. *Therefore,* $x + y\sqrt{3} > 0$, *so* $H \subset \mathbb{R}^+$.

2. *The identity element of* $(\mathbb{R}^+, \times)$ *is* 1. *We have*

$$1 = 1 + 0\sqrt{3}, \quad 1^2 - 3 \cdot 0^2 = 1.$$

Thus $1 \in H$.

3. *Let* $a = x_1 + y_1\sqrt{3}$ *and* $b = x_2 + y_2\sqrt{3}$ *be elements of* H. *Then*

$$ab = (x_1x_2 + 3y_1y_2) + (x_1y_2 + x_2y_1)\sqrt{3}.$$

Set $x = x_1x_2 + 3y_1y_2, \quad y = x_1y_2 + x_2y_1$.

We compute:

$$x^2 - 3y^2 = (x_1^2 - 3y_1^2)(x_2^2 - 3y_2^2) = 1 \cdot 1 = 1.$$

Thus $ab = x + y\sqrt{3} \in H$, *so* H *is closed under multiplication.*

4. *Let* $a = x + y\sqrt{3} \in H$. *Then* $a^{-1} = x - y\sqrt{3}$, *because*

$$(x + y\sqrt{3})(x - y\sqrt{3}) = x^2 - 3y^2 = 1.$$

Moreover, $x \in \mathbb{N}$, $-y \in \mathbb{Z}$, *and* $x^2 - 3(-y)^2 = 1$, *so* $a^{-1} \in H$.

Since H *contains the identity, is closed under multiplication, and contains inverses, we have* H *is a subgroup of* $(\mathbb{R}^+, \times)$.

Exercice 39. *Let* $E = \{0,1,2,3\}$ *and define the operation* $*$ *by:*

$$x * y = (x + 3y) \bmod 4$$

1. *Verify that* $*$ *is an internal composition law on* E.

2. *Determine if* $*$ *is associative.*

3. *Determine if $*$ is commutative.*

4. *Find a neutral element if it exists.*

5. *Find inverses of elements if they exist.*

6. *Conclude whether $(E,*)$ forms a group or not.*

Solution. 1. *For all $x,y \in E$, we have $x+3y \in \mathbb{Z}$, hence*

$$(x+3y) \bmod 4 \in \{0,1,2,3\} = E.$$

Thus, $*$ is an internal law on E.

2. *We test associativity:*

$$(x*y)*z = \big((x+3y) \bmod 4 + 3z\big) \bmod 4 = (x+3y+3z) \bmod 4.$$

On the other hand,

$$x*(y*z) = \big(x+3(y+3z)\big) \bmod 4 = (x+3y+9z) \bmod 4.$$

Since $9z \equiv z \pmod 4$, we obtain

$$x*(y*z) = (x+3y+z) \bmod 4.$$

Therefore,

$$(x*y)*z \neq x*(y*z)$$

in general. Hence, $*$ is not associative.

3. *We compare:*

$$x*y = (x+3y) \bmod 4, \qquad y*x = (y+3x) \bmod 4.$$

In general, $x+3y \not\equiv y+3x \pmod 4$. For example, $1*0=1$ but $0*1=3$.

Thus, $*$ is not commutative.

4. *Let $e \in E$ be neutral. Then for all $x \in E$, $x*e = x$.*

This implies $(x+3e) \bmod 4 = x \implies 3e \equiv 0 \pmod 4$.

Since $\gcd(3,4)=1$, we obtain $e \equiv 0 \pmod 4$. Thus, the neutral element is 0.

5. *An element $y \in E$ is an inverse of x if $x * y = 0$, that is, $x + 3y \equiv 0 \pmod 4$.*

   Since $3^{-1} \equiv 3 \pmod 4$, we have $y \equiv -3x \pmod 4$.

   Hence, the inverses are:

x	x^{-1}
0	0
1	1
2	2
3	3

6. *Although the operation is internal, has a neutral element, and every element has an inverse, the operation $*$ is not associative. So $(E,*)$ is not a group.*

Exercice 40. *Let $E = \mathbb{Z}_6 = \{0,1,2,3,4,5\}$ with operations:*

$$x + y = (x + y) \bmod 6, \quad x \times y = (x \times y) \bmod 6$$

1. *Verify that $(E,+)$ is an Abelian group.*
2. *Verify distributivity of $\times$ over $+$.*
3. *Determine if $(E,+,\times)$ forms a ring.*
4. *Determine if $(E,+,\times)$ forms a field.*

Solution. 1. *Verification that $(E,+)$ is an Abelian group*

- Closure*: For all $x,y \in E$, $(x + y) \bmod 6 \in E$.*
- Associativity*: Addition of integers is associative, and taking modulo 6 preserves associativity:*

$$(x + y) + z \equiv x + (y + z) \pmod 6.$$

- Neutral element*: 0 satisfies*

$$x + 0 = 0 + x = x \quad \forall x \in E.$$

- Inverse element*: For each $x \in E$, there exists $y \in E$ such that*

$$x + y \equiv 0 \pmod 6.$$

The inverses are:

x	$-x$
0	0
1	5
2	4
3	3
4	2
5	1

- Commutativity*: Since integer addition is commutative,*

$$x + y \equiv y + x \pmod 6.$$

Thus, $(E,+)$ is an Abelian group.

2. *For all $x,y,z \in E$,*

$$\begin{aligned} x \times (y+z) &= x(y+z) \bmod 6 \\ &= (xy + xz) \bmod 6 \\ &= (xy) \bmod 6 + (xz) \bmod 6 \\ &= (x \times y) + (x \times z). \end{aligned}$$

Similarly,

$$(y+z) \times x = (y \times x) + (z \times x).$$

Hence, multiplication is distributive over addition.

3. *We know that:*

   - *$(E,+)$ is an Abelian group,*
   - *multiplication $\times$ is associative,*
   - *multiplication is distributive over addition.*

   Therefore, $(E,+,\times)$ is a (commutative) ring.

4. *A field requires that every nonzero element has a multiplicative inverse.*

   In $\mathbb{Z}_6$, we observe:

$$2 \times 3 \equiv 0 \pmod 6,$$

so 2 and 3 are zero divisors.

Hence, elements such as 2,3,4 do not have multiplicative inverses.

Hence, $(E,+,\times)$ is not a field.

Exercice 41. *Let p be a prime number. Define*

$$\mathbb{Z}_p = \left\{ x = \frac{m}{n} \; ; \; m \in \mathbb{Z},\ n \in \mathbb{N},\ \gcd(n,p) = 1 \right\} \subset \mathbb{Q}.$$

1. *Show that $\mathbb{Z}_p$ is a subring of $(\mathbb{Q},+,\cdot)$.*
2. *Let $k \geq 0$ and define*
$$J_{p^k} = \left\{ \frac{m}{n} \in \mathbb{Z}_p \; ; \; p^k \mid m \right\}.$$
Show that J_{p^k} is an ideal of $\mathbb{Z}_p$.

Solution. 1. *We verify the subring criteria:*

- Closure under addition: *Let $x = \frac{m_1}{n_1}$ and $y = \frac{m_2}{n_2}$ be in $\mathbb{Z}_p$, with $\gcd(n_1,p) = \gcd(n_2,p) = 1$. Then*
$$x + y = \frac{m_1 n_2 + m_2 n_1}{n_1 n_2}.$$
Since $\gcd(n_1 n_2, p) = 1$, it follows that $x + y \in \mathbb{Z}_p$.
- Closure under multiplication:
$$x \cdot y = \frac{m_1 m_2}{n_1 n_2}.$$
Again, $\gcd(n_1 n_2, p) = 1$, so $xy \in \mathbb{Z}_p$.
- Contains 0 and 1: *$0 = 0/1$ and $1 = 1/1$ are in $\mathbb{Z}_p$.*
- Additive inverses: *If $x = m/n \in \mathbb{Z}_p$, then $-x = -m/n \in \mathbb{Z}_p$.*

Therefore, $\mathbb{Z}_p$ is a subring of $\mathbb{Q}$.

2. *We check the ideal properties:*

- Nonempty and additive subgroup: *If $x = m_1/n$ and $y = m_2/n \in J_{p^k}$, then $p^k \mid m_1$ and $p^k \mid m_2$, so*
$$x - y = \frac{m_1 - m_2}{n} \in J_{p^k}.$$
Thus J_{p^k} is an additive subgroup of $\mathbb{Z}_p$.

- Absorption property: *Let* $x = m/n \in J_{p^k}$ *and* $z = a/b \in \mathbb{Z}_p$. *Then*

$$z \cdot x = \frac{a}{b} \cdot \frac{m}{n} = \frac{am}{bn}.$$

Since $p^k \mid m$ *and* $\gcd(bn, p) = 1$, *it follows that* $p^k \mid am$. *Hence,* $z \cdot x \in J_{p^k}$.

Therefore, J_{p^k} *is an ideal of* $\mathbb{Z}_p$.

Chapter 5

Rings of polynomials

A ring of polynomials is consisting of polynomials with coefficients in a given ring, equipped with addition and multiplication. It extends the arithmetic of the coefficient ring to polynomials and allows operations such as divisibility, Euclidean division, gcd, lcm, factorization, and the study of roots and their multiplicities.

Throughout this chapter, $\mathbb{K}$ denotes either of the fields $\mathbb{R}$ or $\mathbb{C}$.

5.1 Polynomial and degree

Definition 5.1.1. *A **polynomial** with coefficients in $\mathbb{K}$ is an expression of the form*

$$\begin{aligned} P(X) &= a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \\ &= \sum_{k=0}^{n} a_k X^k. \end{aligned}$$

where $n \in \mathbb{N}$ and $a_0, a_1, \ldots, a_n \in \mathbb{K}$. The set of all polynomials is denoted $\mathbb{K}[X]$.

- *The a_n are called the **leading coefficients** of P. Denote by $\mathrm{lc}(P)$.*
- *If all $a_i = 0$, then P is the **zero polynomial**, denoted 0.*
- *A polynomial of the form $P = a_0$ with $a_0 \in \mathbb{K}$ is called a **constant polynomial**.*
- *The term $a_n X^n$ is the leading term or it is called a **monomial**.*
- *If $a_n = 1$, then P is said to be **monic**.*

Example 5.1.2. 1. *$P(x) = 5 + 2x - 2x^3 + 3x^4$ is a polynomial with real coefficients, i.e., $P(x) \in \mathbb{R}[x]$.*

2. *$Q(x) = 1 + (2i - 19)x + (6 + 2i)x^2 - 2ix^4$ is a polynomial with complex coefficients, i.e., $Q(x) \in \mathbb{C}[x]$.*

Definition 5.1.3. *Let P be a non-zero polynomial. The **degree of** P is the greatest exponent of the variable whose coefficient is non-zero. It is denoted by $\deg P$. If $P = a_n X^n + ... + a_1 X + a_0$ with $a_n \neq 0$, then $\deg P = n$. By convention, $\deg 0 = -\infty$.*

Example 5.1.4. 1. *$P(x) = 5x^4 - 3x^2 + 2$. Degree: 4, Leading coefficient: 5.*

2. *$Q(x) = x^3 + 4x - 1$. Degree: 3, Leading coefficient: 1.*

3. *$R(x) = -7$. Degree: 0, Leading coefficient: -7.*

Example 5.1.5. *Let $P(X) = (X-1)(X^n + X^{n-1} + \cdots + X + 1)$. Expanding gives: $P(X) = (X^{n+1} + X^n + \cdots + X^2 + X) - (X^n + X^{n-1} + \cdots + X + 1) = X^{n+1} - 1$. Hence P is monic of degree $n+1$ and the sum of two monomials X^{n+1} and -1.*

Definition 5.1.6. *Let $P(x)$ be a polynomial in $\mathbb{K}[X]$. We say that $P(x)$ is a **unit** in the polynomial ring $K[x]$ if it is a non-zero constant polynomial.*
*Equivalently, $P(x)$ is a **unit** if and only if $\deg(P) = 0$ and its constant coefficient $a_0 \neq 0$.*
In particular, the units of $\mathbb{K}[x]$ are exactly the elements of $\mathbb{K}^*$.

Example 5.1.7. 1. *$P(x) = 5 + 3x - 2x^2 + x^3$.*

The degree of P is 3 and its leading coefficient is 1. Hence, $P(x)$ is a monic *polynomial. Since $\deg(P) \neq 0$, it is* not a unit *in $\mathbb{R}[x]$.*

2. *$Q(x) = 7 + (2i + 9)x + (6 - i)x^3 - 8ix^5$.*

The degree of Q is 5 and its leading coefficient is $-8i$. Since the leading coefficient is not equal to 1, $Q(x)$ is not monic. *As $\deg(Q) \neq 0$, it is* not a unit *in $\mathbb{C}[x]$.*

5.2 Construction of the ring of polynomials

We will equip $(\mathbb{K}, +, \cdot)$ be a commutative ring.

5.2.1 Equality of Two Polynomials

Definition 5.2.1. *Let $P = a_nX^n + ... + a_1X + a_0$ and $Q = b_nX^n + ... + b_1X + b_0$ be two polynomials in $\mathbb{K}[X]$ with $n \in \mathbb{N}$. We say that P and Q are **equal** as follows:*

$$P = Q \iff a_i = b_i,\ \forall i \in \{1,2,...,n\}.$$

Example 5.2.2. *Consider the two polynomials*

$$P(X) = (X-1)^2 \qquad \text{and} \qquad Q(X) = X^2 - 2X + 1.$$

Then $P = Q$ in $K[X]$, since they have the same coefficients after expansion.

5.2.2 Addition of Two Polynomials

Definition 5.2.3. *Let $P = a_nX^n + ... + a_1X + a_0$ and $Q = b_nX^n + ... + b_1X + b_0$ be two polynomials in $\mathbb{K}[X]$ with $n \in \mathbb{N}$. We define the polynomial $P + Q$ as follows:*

$$\begin{aligned} P+Q &= (a_n+b_n)X^n + ... + (a_1+b_1)X + (a_0+b_0) \\ &= \sum_{k=0}^{n} (a_k+b_k)X^k. \end{aligned}$$

Example 5.2.4. *Let $P(x) = 5x^2 - 3x + 4$ and $Q(x) = 2x^2 + x - 1$, we have:*

1. $(P-Q)(x) = 3x^2 - 4x + 5.$
2. $(P+Q)(x) = 5x^2 - 3x + 4.$

Proposition 25. *For polynomials P, Q, R, are non-zero polynomials in $\mathbb{K}[X]$, then:*

1. $0 + P = P,$
2. $P + Q = Q + P,$
3. $(P+Q) + R = P + (Q+R).$
4. $\deg(P+Q) \leq \max(\deg P, \deg Q).$

5.2.3 Multiplication of Two Polynomials

Definition 5.2.5. *Let $P = a_n X^n + ... + a_1 X + a_0$ and $Q = b_m X^m + ... + b_1 X + b_0$ be two polynomials in $\mathbb{K}[X]$ with $(n,m) \in \mathbb{N}^2$. We define the polynomial $P \times Q$ as follows:*

$$\begin{aligned} P \times Q &= \sum_{k=0}^{n+m} c_k X^k \\ &= (a_0 b_0) + (a_0 b_1 + a_1 b_0) X + (a_0 b_2 + a_1 b_1 + a_2 b_0) X^2 + \dots \\ &+ (a_{n-1} b_m + a_n b_{m-1}) X^{n+m-1} + (a_n b_m) X^{n+m}. \end{aligned}$$

where $c_k = \sum_{j=0}^{k} a_j b_{k-j}$.

Example 5.2.6. *Let $P(x) = 2x + 3$ and $Q(x) = x + 4$*
$P(x) \times Q(x) = (2x+3)(x+4) = 2x^2 + 11x + 12.$

Proposition 26. *For polynomials P, Q, R, are non-zero polynomials $\in \mathbb{K}[X]$, then:*

1. $P \times Q = Q \times P$,
2. $(P \times Q) \times R = P \times (Q \times R)$,
3. $P \times (Q + R) = P \times Q + P \times R$,
4. $\deg(PQ) = \deg P + \deg Q$.

Proposition 27. *Let P, Q, be two polynomials. Then: $PQ = 0 \implies P = 0$ or $Q = 0$.*

Proposition 28. *A polynomial P is **invertible** $\in \mathbb{K}[X]$ (i.e., there exists $Q \in \mathbb{K}[X]$ such that $PQ = 1$) if and only if P is a **non-zero constant polynomial**.*

5.2.4 Scalar Multiplication of Polynomials

Definition 5.2.7. *Let $P = a_n X^n + ... + a_1 X + a_0$ be polynomials in $\mathbb{K}[X]$ with $n \in \mathbb{N}$. We define the polynomial λP for $\lambda \in \mathbb{K}$ as follows:*

$$\begin{aligned} \lambda P &= \lambda a_n X^n + ... + \lambda a_1 X + \lambda a_0 \\ &= \sum_{i=0}^{n} \lambda a_i X^i. \end{aligned}$$

Example 5.2.8. 1. *Let* $P(x) = 2x^3 - x + 4$ *and* $\lambda = -3$. *Then:* $\lambda P(x) = -6x^3 + 3x - 12$.

2. *Let* $Q(x) = (1+i)x^2 - 3ix + 2$ *and* $\lambda = 2 - i$. *Then:*
   $\lambda Q(x) = (3+i)x^2 - (6+3i)x + 4 - 2i$.

Proposition 29. *For polynomials* P *is non-zero polynomial, then:*

1. $1 \times P = P$.
2. $\deg P \geq 0$.
3. *If* $\lambda \neq 0$, *then* $\deg(\lambda P) = \lambda \deg P$.

5.2.5 Composition of Two Polynomials

Let P and Q be two polynomials in $\mathbb{K}[X]$. The **composition** of P and Q, denoted $P \circ Q$, is defined by:

$$(P \circ Q)(X) = P(Q(X)).$$

This means that we replace every occurrence of X in $P(X)$ by the polynomial $Q(X)$.

Example 5.2.9. *Let* $P(X) = 2X + 3, \quad Q(X) = X^2 - 1$. *Then:*

$$(P \circ Q)(X) = P(Q(X)) = 2(X^2 - 1) + 3 = 2X^2 + 1$$

Remark 5.2.10. *The composition of polynomials is generally* ***not commutative****, i.e.,*

$$P \circ Q \neq Q \circ P$$

in most cases.

Proposition 30. *For polynomials* P, Q, R, *are non-zero polynomials, then:*

1. $P \circ (Q \circ R) = (P \circ Q) \circ R$.
2. *Let* $I(X) = X$ *(The* ***identity polynomial****). Then:*

$$P \circ I = I \circ P = P.$$

3. $\deg(P \circ Q) = (\deg P) \times (\deg Q)$.

5.3 Arithmetic of Polynomials

5.3.1 Divisibility of a polynomial

Definition 5.3.1. *Let A, B be two polynomials in $\mathbb{K}[X]$. We say that polynomial A is **divisible** by polynomial B, written $B \mid A$ and say that A is a **multiple** of B (or that B is a **divisor** of A) if:*

1. *B is not zero*
2. *there exists $Q \in \mathbb{K}[X]$ with $A = BQ$.*

The polynomial Q is sometimes denoted as A/B or $\frac{A}{B}$.

Proposition 31. *For $A, B, C \in \mathbb{K}[X]$:*

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

5.3.2 Euclidean Division

Theorem 5.3.2. ***(Existence and Uniqueness of Euclidean Division)***
*Let A and B be two polynomials in $K[X]$, with $B \neq 0$. Then there exists a **unique pair** of polynomials $(Q, R) \in K[X]^2$ such that:*

$$A(X) = B(X)Q(X) + R(X) \quad \text{and} \quad \deg(R) < \deg(B).$$

*The polynomial Q is called the **quotient** and R the **remainder** of the Euclidean division of A by B.*

Euclidean Division (Descending powers)

Definition 5.3.3. *Let A and B be two polynomials arranged in **descending powers**. Then there exists a **unique pair** of polynomials $(Q,R) \in K[X]^2$ such that:*

$$A(X) = B(X)Q(X) + R(X) \quad \textit{with} \quad \deg(R) < \deg(B).$$

Remark 5.3.4. *If $R = 0$ if and only if $B|A$.*

Theorem 5.3.5. *Let $\deg A = n$ and $\deg B = m$.*

- *If $m > n$, then: $A = B \cdot 0 + R$, that is, the quotient is $Q = 0$ and the remainder is $R = A$.*
- *If $n \geq m$, then the first term of the quotient is: $Q_1(x) = \frac{p_n}{q_m} x^{n-m}$, where p_n and q_m are the leading coefficients of A and B.*

Example 5.3.6. *Compute the remainder of the Euclidean division of:*
$A(x) = 2X^4 - X^3 - 2X^2 + 3X - 1$ *by* $B(x) = X^2 - X + 1$. *We obtain:*
$A(x) = (X^2 - X + 1)(2X^2 + X - 3) + (-X + 2) = B(x)Q(x) + R(x)$. *Then:*
$Q(x) = 2X^2 + X - 3, \quad R(x) = -X + 2.$

Example 5.3.7. *Compute the remainder of the Euclidean division of:*
$A(x) = X^4 - 3X^3 + X + 1$ *by* $B(x) = X^2 + 2$. *We obtain:*
$A(x) = (X^2 + 2)(X^2 - 3X - 2) + (7X + 5) = B(x)Q(x) + R(x)$. *Then:*
$Q(x) = X^2 - 3X - 2, \quad R(x) = 7X + 5.$

Euclidean Division (Ascending powers)

Theorem 5.3.8. *Let A, B have degrees n, p and $h \in \mathbb{N}^*$. There exists a unique pair $(Q,R) \in K[X]^2$ such that:*

$$A(X) = B(X)Q(X) + X^{h+1}R(X) \quad \textit{with} \quad \deg Q \leq h \quad \textit{if} \quad Q \neq 0.$$

Example 5.3.9. *Compute the remainder of the Euclidean division of:*
$A(x) = 1 \quad$ *by* $\quad B(x) = 1 - x$ *for* $h = 3$.

If we apply the formula: $A(X) = B(X)Q(X) + x^{h+1}R(X)$, *we obtain:*

$$1 = (1-x)(1+x+x^2+\cdots+x^k) + x^{h+1},$$

Hence, $\frac{1-x^{h+1}}{1-x} = 1+x+x^2+\cdots+x^h$. *For* $h = 3$.
We have: $A(x) = (1-x)(1+x+x^2+x^3) + x^4 = B(x)(1+x+x^2+x^3) + x^4$.
with remainder $R(x) = 1$.

Example 5.3.10. *Compute the remainder of the Euclidean division of:*
$A(x) = 2 - 3X + 4X^2 - 5X^3$ *by* $B(x) = 1 - X - X^2$ *for* $h = 3$.
If we apply the formula: $A(X) = B(X)Q(X) + x^{h+1}R(X)$. *We have:*
$A(x) = B(x)(2 - X + 5X^2 - X^3) + X^4(4 - X)$, *with remainder* $R(x) = 4 - X$.

5.3.3 Greatest Common Divisor (GCD) of Two Polynomials

Definition 5.3.11. *Let* A, B *be two polynomials in* $\mathbb{K}[X]$. *The* ***greatest common divisor (GCD)*** *of* A *and* B *is a polynomial* D *that divides both* A *and* B, *denoted by* $\gcd(A,B) = D$.

Proposition 32. *Let* A, B *be two nonzero polynomials in* $\mathbb{K}[X]$. *There exists a unique* monic *polynomial of greatest degree dividing both* A *and* B, *called the* greatest common divisor $\gcd(A,B)$.

Proposition 33. *Let* A, B *be two nonzero polynomials in* $\mathbb{K}[X]$, *with* $\deg A \geq \deg B$. *The* ***GCD*** *of* A *and* B *can be calculated using* ***Euclid's algorithm*** *as follows:*

1. *Perform the Euclidean division of* A *by* B:

$$A = BQ_1 + R_1, \quad \deg R_1 < \deg B.$$

2. *Divide* B *by* R_1:

$$B = R_1Q_2 + R_2, \quad \deg R_2 < \deg R_1.$$

3. *Divide* R_1 *by* R_2:

$$R_1 = R_2Q_3 + R_3, \quad \deg R_3 < \deg R_2.$$

4. *Continue the divisions:*

$$\begin{aligned} R_2 &= R_3Q_4 + R_4, \quad \deg R_4 < \deg R_3. \\ &\vdots \\ R_k &= R_{k+1}Q_{k+2} + 0. \end{aligned}$$

until the remainder is zero. Then the last nonzero remainder R_{k+1} is the GCD of P and Q.

Remark 5.3.12. *The GCD is unique up to multiplication by a unit (typically chosen monic if desired).*

Example 5.3.13. *Consider two polynomials $A(X) = X^3 - 2X^2 + X - 2$ and $B(X) = X^2 - 1$ in $\mathbb{R}[X]$. We compute $\gcd(A, B)$ using Euclid's algorithm.*

1. *Divide A by B:*

   $A(X) = B(X)(X - 2) + R_1(X)$. *So* $R_1(X) = X - 2$.

2. *Divide B by R_1:*

   $B(X) = R_1(X)(X + 2) + R_2(X)$. *So* $R_2(X) = 0$.

The last nonzero remainder is $R_1(X) = X - 2$, so the GCD of P and Q is: $\gcd(P, Q) = X - 2$.

Remark 5.3.14. *This shows that the Euclid's algorithm gives the GCD as the last nonzero remainder. The GCD is unique up to multiplication by a nonzero constant.*

Proposition 34. *Let $A(x)$ and $B(x)$ be two nonzero polynomials in $\mathbb{K}[X]$. Then there exists a unique monic polynomial $\gcd(A, B)$ such that:*

1. $\gcd(A, B) \mid A \quad$ *and* $\quad \gcd(A, B) \mid B$,

2. *For any polynomial P such that $P \mid A$ and $P \mid B$, we have $P \mid \gcd(A, B)$.*

Proposition 35. *If A and B be two nonzero polynomials in $\mathbb{K}[X]$ and C is a unitary polynomial in $\mathbb{K}[X]$, then*

$$\gcd(AC, BC) = C \cdot \gcd(A, B).$$

5.3.4 Coprime Polynomials

Definition 5.3.15. *Let A, B be two nonzero polynomials in $\mathbb{K}[X]$. Polynomials A and B are said to be* ***coprime*** *or* ***relatively prime*** *if* $\gcd(A,B) = 1$.

Theorem 5.3.16. ***(Bézout's Theorem)***. *Let A and B be two non-zero polynomials in $\mathbb{K}[X]$. Let $D(X) = \gcd(A,B)$. Then there exist two polynomials $U(X), V(X) \in \mathbb{K}[X]$ such that:*

$$A(X)U(X) + B(X)V(X) = D(X).$$

Proposition 36. ***(Bézout's Theorem for Two Coprime Polynomials)***. *Let A and B be two non-zero polynomials in $\mathbb{K}[X]$. The polynomials A and B are said to be* ***coprime*** *if and only if there exist two polynomials $U(X)$ and $V(X)$ such that:*

$$A(X)U(X) + B(X)V(X) = 1.$$

Remark 5.3.17. *As in the case of integers, a Bézout relation is obtained by working backwards through the Euclidean algorithm.*

Example 5.3.18. *Let $A(X) = X^4 + 1, \quad B(X) = X^3 + 1$. Applying the Euclidean algorithm:*

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

The last non-zero remainder is a constant polynomial, hence: $\gcd(A,B) = 1$.
Working backwards, we can express 1 *as a linear combination of $A(X)$ and $B(X)$:*
$1 = A(X)U(X) + B(X)V(X)$, *for suitable polynomials $U(X)$ and $V(X)$.*
We now work backwards to express 1 *as follows:*

$$1 = \frac{1}{2}(X^3 + 1) - \frac{1}{2}(-X + 1)(-X^2 - X - 1).$$

Using the relation

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

we substitute and obtain:

$$\begin{aligned}1 &= \frac{1}{2}(X^3+1) - \frac{1}{2}\left[(X^4+1) - X(X^3+1)\right](-X^2-X-1)\\ &= (X^4+1)\left(\tfrac{1}{2}X^2+\tfrac{1}{2}X+\frac{1}{2}\right) + (X^3+1)\left(\frac{1}{2}-\tfrac{1}{2}X^3-\tfrac{1}{2}X^2-\tfrac{1}{2}X\right).\end{aligned}$$

Thus,

$$(X^4+1)U(X) + (X^3+1)V(X) = 1,$$

with

$$U(X) = \tfrac{1}{2}X^2+\tfrac{1}{2}X+\frac{1}{2}, \quad V(X) = \frac{1}{2}-\tfrac{1}{2}X^3-\tfrac{1}{2}X^2-\tfrac{1}{2}X.$$

5.3.5 Least Common Multiple (LCM) of Two Polynomials

Definition 5.3.19. *Let $A, B \in \mathbb{K}[X]$ be two nonzero polynomials. A polynomial $P \in \mathbb{K}[X]$ is called a* ***least common multiple*** *of A and B if:*

1. *$A \mid P$ and $B \mid P$,*
2. *for every polynomial $M \in \mathbb{K}[X]$ such that $A \mid M$ and $B \mid M$, we have $P \mid M$.*

The least common multiple of A and B is denoted by $\operatorname{lcm}(A,B)$.

Proposition 37. ***(Characterization of the Least Common Multiple).*** *Let $A, B \in \mathbb{K}[X]$ be two nonzero polynomials. Then:*

1. *If $Q \in \mathbb{K}[X]$ is a polynomial that is a multiple of both A and B, then Q is a multiple of $\operatorname{lcm}(A,B)$.*
2. *Moreover, if $M \in \mathbb{K}[X]$ is a* monic *polynomial such that every common multiple of A and B is divisible by M, then $M = \operatorname{lcm}(A,B)$.*

Proposition 38. ***(LCM of Coprime Polynomials)*** *Let $A, B \in \mathbb{K}[X]$ be two nonzero polynomials with leading coefficients $\operatorname{lc}(A)$ and $\operatorname{lc}(B)$, respectively. If A and B are* coprime, *then*

$$\operatorname{lcm}(A,B) = \frac{1}{\operatorname{lc}(A)\operatorname{lc}(B)}\,AB.$$

Corollary 5.3.20. ***(LCM and GCD Formula)*** *Let $A, B \in \mathbb{K}[X]$ be two nonzero polynomials. Then*

$$\operatorname{lcm}(A,B)\gcd(A,B) = \frac{1}{\operatorname{lc}(A)\operatorname{lc}(B)}\,AB.$$

5.3.6 Decomposition into a Product of Irreducible Factors

Definition 5.3.21. *A polynomial $P(X) \in \mathbb{K}[X]$ is called* ***irreducible Polynomial*** *$\mathbb{K}$ if:*

1. $\deg P \geq 1$ *(that is, P is non-constant).*
2. *The only divisors of $P(X)$ in $\mathbb{K}[X]$ are the units of $\mathbb{K}[X]$ and the associates of $P(X)$ that is polynomials of the form α and $\alpha P(X)$ with $\alpha \in \mathbb{K}^*$.*

Remark 5.3.22. *A polynomial $P \in \mathbb{K}[X]$ is said to be* ***reducible*** *over $\mathbb{K}$ if there exist polynomials $Q, R \in \mathbb{K}[X]$ such that $P = QR$, with $\deg Q \geq 1$ and $\deg R \geq 1$.*

Proposition 39. ***(Degree-1 polynomials are irreducible).*** *Let $a, b \in \mathbb{K}$ with $a \neq 0$. The polynomial $aX + b$ is irreducible in $\mathbb{K}[X]$. Indeed, a polynomial of degree 1 cannot be written as a product of two non-constant polynomials.*

Example 5.3.23.

- $X^2 + 1 = (X - i)(X + i)$ *is reducible in $\mathbb{C}[X]$ but irreducible in $\mathbb{R}[X]$.*
- $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ *is reducible in $\mathbb{R}[X]$ but irreducible in $\mathbb{Q}[X]$.*
- $X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$ *is reducible in $\mathbb{R}[X]$ but irreducible in $\mathbb{Q}[X]$.*
- $X^2 + 4 = (X - 2i)(X + 2i)$ *is reducible in $\mathbb{C}[X]$ but irreducible in $\mathbb{R}[X]$.*
- $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$ *is reducible in $\mathbb{R}[X]$ but irreducible in $\mathbb{Q}[X]$.*

Proposition 40. ***(Every polynomial of degree ≥ 1 has an irreducible divisor).*** *If P is a polynomial in $\mathbb{K}[X]$ with $\deg(P) \geq 1$, then there exists an irreducible polynomial in $\mathbb{K}[X]$ that divides P in $\mathbb{K}[X]$.*

Proof.

1. **Base case ($\deg(P) = 1$):** Any polynomial of degree 1 is irreducible, so it has an irreducible divisor (itself).
2. **Inductive step ($\deg(P) = n \geq 2$):**
   - If P is irreducible, we are done.
   - If P is reducible, write $P = QR$ with $\deg(Q), \deg(R) \geq 1$. By induction, Q or R has an irreducible divisor, hence so does P.

■

Lemme 5.3.24. ***(Gauss's Lemma)***. *Let $P, A, B \in \mathbb{K}[X]$ with P irreducible. If $\gcd(P, A) = 1$ and P divides the product AB, then P divides B.*

Proof. Since P and A are coprime, there exist polynomials $U, V \in \mathbb{K}[X]$ such that

$$UP + VA = 1.$$

Multiplying both sides by B, we get

$$UBP + VAB = B.$$

Now, P divides AB by assumption, and obviously P divides UBP. Hence, P divides $UBP + VAB = B$. ■

Example 5.3.25. *Let $P(X) = X + 1$, $A(X) = X^2 + X + 1$, $B(X) = X^3 - 1$ in $\mathbb{Q}[X]$. Since P and A are coprime, and P divides $AB = (X^2 + X + 1)(X^3 - 1)$, Gauss's Lemma implies that P divides $B(X) = X^3 - 1$.*

Theorem 5.3.26. *If A is a polynomial in $\mathbb{K}[X]$ of degree greater than or equal to 1, then there exist an integer $r \in \mathbb{N}$, monic and irreducible polynomials $P_1, \ldots, P_r$ in $\mathbb{K}[X]$, integers $m_1, \ldots, m_r \in \mathbb{N}^*$, and a constant $c \in \mathbb{K}$ such that*

$$A(X) = c\, P_1(X)^{m_1} P_2(X)^{m_2} \cdots P_r(X)^{m_r}.$$

Moreover, such a factorization is unique up to the order of the factors.

Theorem 5.3.27. *The irreducible polynomials in $\mathbb{C}[X]$ are exactly the polynomials of degree 1. Consequently, for any polynomial $P \in \mathbb{C}[X]$ of degree $n \geq 1$, the factorization of P can be written as*

$$P(X) = (X - \alpha_1)^{k_1} (X - \alpha_2)^{k_2} \cdots (X - \alpha_r)^{k_r},$$

where $\alpha_1, \alpha_2, \ldots, \alpha_r$ are the distinct roots of P, and $k_1, k_2, \ldots, k_r$ are their respective multiplicities.

Theorem 5.3.28. *The irreducible polynomials in $\mathbb{R}[X]$ are:*

- *all polynomials of degree 1, and*
- *all polynomials of degree 2 with negative discriminant ($\Delta < 0$).*

Let $P \in \mathbb{R}[X]$ be a polynomial of degree $n \geq 1$. Then P can be factorized as

$$P(X) = (X - \alpha_1)^{k_1} (X - \alpha_2)^{k_2} \cdots (X - \alpha_r)^{k_r} Q_1^{l_1} Q_2^{l_2} \cdots Q_s^{l_s},$$

where:

- $\alpha_1, \alpha_2, \ldots, \alpha_r$ *are the distinct real roots of* P*, with multiplicities* $k_1, k_2, \ldots, k_r$*,*
- $Q_1, \ldots, Q_s$ *are irreducible quadratic polynomials in* $\mathbb{R}[X]$ *with negative discriminant, i.e.,* $Q_i(X) = X^2 + b_i X + c_i$ *with* $\Delta_i = b_i^2 - 4c_i < 0$*, and* $l_1, \ldots, l_s$ *are their multiplicities.*

5.4 Roots of a Polynomial

5.4.1 Roots and degree

Definition 5.4.1. *Let* P *be a polynomial in* $\mathbb{K}[X]$*. An element* $\alpha \in \mathbb{K}$ *is called a* ***root*** *(or* ***zero****)* *of* P *if* $P(\alpha) = 0$*.*

Example 5.4.2.

1. *In* $\mathbb{R}$*,* $P(X) = X^2 - 1$ *has roots* 1 *and* -1*.*
2. *In* $\mathbb{C}$*,* $P(X) = X^2 + 1$ *has roots* i *and* $-i$*.*
3. *In* $\mathbb{Z}$*,* $P(X) = X^2 + 1$ *has no root.*

Proposition 41. *If* α *is a root of* P*, then* $(X - \alpha)$ *divides* $P(X)$ *in* $\mathbb{K}[X]$*; that is,*

$$P(X) = (X - \alpha)\, Q(X)$$

for some $Q(X) \in \mathbb{K}[X]$*.*

5.4.2 Roots of a multiplicity

Definition 5.4.3. *Let* $k \in \mathbb{N}$*. We say that* $\alpha \in \mathbb{K}$ *is a* ***root of multiplicity*** k *of a polynomial* $P \in \mathbb{K}[X]$*, if* $(X - \alpha)^k$ *divides* P *but* $(X - \alpha)^{k+1}$ *does not divide* P*. When* $k = 1$*,* α *is called a* ***simple root****; when* $k = 2$*,* α *is a* ***double root****, and so on. We also say that* α *is a* ***root of order*** k*.*

Proposition 42. *Let* $P \in \mathbb{K}[X]$ *and* $\alpha \in \mathbb{K}$*. The following statements are equivalent:*

1. α *is a root of multiplicity* k *of* P*.*
2. *There exists* $Q \in \mathbb{K}[X]$ *such that* $P(X) = (X - \alpha)^k Q(X) \quad$ *with* $\quad Q(\alpha) \neq 0$*.*

3. $P(\alpha) = P'(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0 \quad \text{and} \quad P^{(k)}(\alpha) \neq 0.$

Definition 5.4.4. *Let $P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ be a polynomial. The **derivative** of the polynomial P, denoted by P', is defined by*

$$P'(X) = a_1 + 2a_2X + \cdots + (n-1)a_{n-1}X^{n-2} + na_nX^{n-1}.$$

Theorem 5.4.5. ***(D'Alembert-Gauss)*** *Every non-constant polynomial with complex coefficients of degree $n \geq 1$ has at least one root in $\mathbb{C}$. Counting multiplicities, a polynomial of degree n has exactly n roots in $\mathbb{C}$.*

Example 5.4.6. ***(Quadratic polynomial with real coefficients)***. *Let*

$$P(X) = aX^2 + bX + c, \quad a,b,c \in \mathbb{R},\ a \neq 0.$$

- *If $\Delta = b^2 - 4ac > 0$, P has 2 distinct real roots: $\frac{-b \pm \sqrt{\Delta}}{2a}$.*
- *If $\Delta < 0$, P has 2 distinct complex roots: $\frac{-b \pm i\sqrt{-\Delta}}{2a}$.*
- *If $\Delta = 0$, P has a double real root: $\frac{-b}{2a}$.*

In all cases, counting multiplicities, P has exactly 2 roots.

Example 5.4.7. *Consider $P(X) = 3X^3 - 2X^2 + 6X - 4$.*

- *In $\mathbb{R}$, P has only one simple root: $\alpha = \frac{2}{3}$, $\quad P(X) = 3\left(X - \frac{2}{3}\right)(X^2 + 2)$.*
- *In $\mathbb{C}$, P factorizes as: $P(X) = 3\left(X - \frac{2}{3}\right)(X - i\sqrt{2})(X + i\sqrt{2})$, giving 3 simple roots.*

5.5 Exercises with solutions

Exercice 42. *Let $P(X) = X^4 + 2X^3 - 3X^2 - 4X + 4$.*

1. *Calculate $P(1)$.*
2. *Find $\gcd(P(X), P'(X))$?*
3. *Find all real roots of $P(X)$?*

Solution. *Let $P(X) = X^4 + 2X^3 - 3X^2 - 4X + 4$.*

1. $P(1) = 1^4 + 2 \cdot 1^3 - 3 \cdot 1^2 - 4 \cdot 1 + 4 = 1 + 2 - 3 - 4 + 4 = 0$. *So* $X = 1$ *is a root of* $P(X)$.

2. *Compute the derivative:*

$$P'(X) = 4X^3 + 6X^2 - 6X - 4 = 2(2X^3 + 3X^2 - 3X - 2)$$

Check $X - 1$ *as a common factor:* $P'(1) = 4 + 6 - 6 - 4 = 0$. *Factor* $X - 1$*:*

$$P(X) = (X - 1)(X^3 + 3X^2 - 4), \quad P'(X) = (X - 1)(4X^2 + 10X + 4)$$

Thus, $\gcd(P, P') = X - 1$.

3. *Solve* $X^3 + 3X^2 - 4 = 0$ *using Rational Root Theorem:* $X = 1, \quad X = -2$

So the complete factorization: $P(X) = (X - 1)^2(X + 2)^2$

Real roots: $X = 1$ *(double root),* $\quad X = -2$ *(double root).*

Exercice 43. *Calculate the quotient and the remainder of the Euclidean division of:*

1. $A(X) = X^4 + X^3 + X^2$ *by* $B(X) = X^2 + 2X + 4$.

2. $A(X) = 3X^5 + 2X^4 + X^2 + 1$ *by* $B(X) = X^3 + X + 2$.

3. $A(X) = 3X^5 + 4X^2 + 1$ *by* $B(X) = X^2 + 2X + 3$.

4. $A(X) = X^4 + 6X^3 + 10X^2 + 3X + 6$ *by* $B(X) = X^2 + 3X$.

Solution. 1. *Applying the Euclidean division, we have:*

$$A(X) = (X^2 - X - 1)(X^2 + 2X + 4) + (6X + 4)$$

So, quotient: $Q(X) = X^2 - X - 1$ *and remainder:* $R(X) = 6X + 4$

2. *We have*

$$A(X) = (X^3 + X + 2)(3X^2 + 2X - 3) + (-7X^2 - X + 7).$$

So, quotient: $Q(X) = 3X^2 + 2X - 3$ *and remainder:* $R(X) = -7X^2 - X + 7$

3. *We have*

$$A(X) = (X^2 + 2X + 3)(3X^3 - 6X^2 + 3X + 16) + (-41X - 47)$$

So, quotient: $Q(X) = 3X^3 - 6X^2 + 3X + 16$ *and remainder:* $R(X) = -41X - 47$.

4. *We have*

$$A(X) = B(X)(X^2 + 3X + 1) + 6.$$

So, quotient: $Q(X) = X^2 + 3X + 1$ *and and remainder:* $R(X) = 6$.

Exercice 44. *Consider the polynomials over* $\mathbb{R}$*:*

$$P(X) = X^4 - 1, \qquad Q(X) = X^3 - 1.$$

1. *Factor* $P(X)$ *and* $Q(X)$ *into irreducible polynomials over* $\mathbb{R}[X]$ *and over* $\mathbb{C}[X]$.
2. *Determine the greatest common divisor* $\gcd(P,Q)$ *over* $\mathbb{R}[X]$ *and over* $\mathbb{C}[X]$.
3. *Determine the least common multiple* $\operatorname{lcm}(P,Q)$ *over* $\mathbb{R}[X]$ *and over* $\mathbb{C}[X]$.
4. *Verify the relation:* $\operatorname{lcm}(P,Q) \cdot \gcd(P,Q) = P \cdot Q$.

Solution. 1. • $P(X) = X^4 - 1 = (X^2 - 1)(X^2 + 1) = (X - 1)(X + 1)(X^2 + 1)$ *over* $\mathbb{R}[X]$.

$$P(X) = (X - 1)(X + 1)(X - i)(X + i) \quad \text{over } \mathbb{C}[X].$$

• $Q(X) = X^3 - 1 = (X - 1)(X^2 + X + 1)$ *over* $\mathbb{R}[X]$.

$$Q(X) = (X - 1)\left(X - \frac{-1 + i\sqrt{3}}{2}\right)\left(X - \frac{-1 - i\sqrt{3}}{2}\right) \quad \text{over } \mathbb{C}[X].$$

2. *In* $\mathbb{R}[X]$ *or* $\mathbb{C}[X]$*, the common factor is* $X - 1$*. So,* $\gcd(P,Q) = X - 1$.

3. • *Over* $\mathbb{R}[X]$*:*
$\operatorname{lcm}(P,Q) = (X - 1)(X + 1)(X^2 + 1)(X^2 + X + 1)$

• *Over* $\mathbb{C}[X]$*:*
$\operatorname{lcm}(P,Q) = (X - 1)(X + 1)(X - i)(X + i)\left(X - \frac{-1+i\sqrt{3}}{2}\right)\left(X - \frac{-1-i\sqrt{3}}{2}\right)$

4. $\operatorname{lcm}(P,Q) \cdot \gcd(P,Q) = (X - 1)(X + 1)(X^2 + 1)(X^2 + X + 1) \cdot (X - 1) = P \cdot Q$.

Exercice 45. *Let define two polynome in* $\mathbb{R}$ *by:*
$A(X) = X^5 + 3X^4 + 2X^3 - X^2 - 3X - 2, \quad B(X) = X^4 + 2X^3 + 2X^2 + 7X + 6.$

1. *Calculate (GCD) of the polynomials* A *and* B.
2. *Find polynomials* U *and* V *such that* $D = AU + BV$.

Solution. 1. *We evaluate both polynomials at* $X = -1$: $A(-1) = 0, \quad B(-1) = 0$. *Hence,* $X + 1$ *is a common divisor of* A *and* B.

Dividing, we obtain:

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

$$B(X) = (X+1)(X^3 + X^2 + X + 6).$$

The remaining factors have no common root, hence: $D = \gcd(A, B) = X + 1$.

2. *For Since* $D = gcd(A, B) = X + 1$, *there exist polynomials* $U, V \in \mathbb{R}[X]$ *such that:*

$$X + 1 = A(X)U(X) + B(X)V(X).$$

One possible choice is: $U = 1, \qquad V = -X$, *which satisfies:*

$$A(X) - XB(X) = X + 1.$$

Exercice 46. *For* $n \in \mathbb{N}^*$, *determine the multiplicity (order) of the root* 2 *of the polynomial*

$$P_n(X) = nX^{n+2} - (4n+1)X^{n+1} + 4(n+1)X^n - 4X^{n-1}.$$

Solution. *We factor:* $P_n(X) = X^{n-1}\Big(nX^3 - (4n+1)X^2 + 4(n+1)X - 4\Big)$.
Since $2 \neq 0$, *the multiplicity of the root* 2 *depends on*

$$Q(X) = nX^3 - (4n+1)X^2 + 4(n+1)X - 4.$$

We compute: $Q(2) = 0$, *so* 2 *is a root. The derivative is*

$$Q'(X) = 3nX^2 - 2(4n+1)X + 4(n+1),$$

and $Q'(2) = 0$. *Thus the multiplicity is at least* 2. *The second derivative is*

$$Q''(X) = 6nX - 2(4n+1),$$

and $Q''(2) \neq 0 \quad (n \geq 1)$.
Therefore, the root 2 *has multiplicity exactly* 2.

Bibliography

[1] Adhikari, M. R., Adhikari, A. (2014). Basic modern algebra with applications. Springer India.

[2] Aluffi, P. (2009). Algebra: chapter 0 (Vol. 104). American Mathematical Soc.

[3] Cohen, C. (2012). Formalized algebraic numbers: construction and first-order theory (Doctoral dissertation, Ecole Polytechnique X).

[4] Enderton, H. B. (2001). A mathematical introduction to logic. Elsevier.

[5] Faccanoni, G. Recueil d'exercices corrigés et aide-mémoire.

[6] Fredon, D., MAUMY-BERTRAND, M., BERTRAND, F. (2010). Mathématiques. Analyse en, 30.

[7] Fuhrmann, P. A. (2013). A Polynomial Approach to Linear Algebra 2nd edition..

[8] Galbraith, S. D. (2012). Mathematics of public key cryptography. Cambridge University Press.

[9] Judson, T. W. (2020). Abstract algebra: theory and applications.

[10] McKenzie, R. N., McNulty, G. F., Taylor, W. F. (2018). Algebras, lattices, varieties: volume I (Vol. 383). American Mathematical Society.

[11] Milne, J. S. (2020, July). Algebraic number theory.

[12] Ramis, J. P., Warusfel, A. (2007). Mathématiques. Tout-en-un pour la licence, niveau L, 1.

[13] Reinert, B. (2009). On Groebner Basis in Monoid and Group Rings. arXiv preprint arXiv:0903.5044.

[14] Rotman, J. J. (2012). An introduction to the theory of groups (Vol. 148). Springer Science Business Media.

[15] Shoup, V. (2009). A computational introduction to number theory and algebra. Cambridge university press.

[16] Stein, W. (2005). Elementary Number Theory.