Algebra 1

By Medjadj Imene

USTO-MB

2023/2024


UNIVERSITY OF SCIENCE AND TECHNOLOGY OF ORAN
FACULTY OF MATHEMATICS AND INFORMATICS

ALGEBRA I

BY

MEDJADJ IMENE

USTO-MB
2023/2024

Contents

1 Logic **4**
- 1.1 Operations . . . 4
  - 1.1.1 Negation $\ll (notP) \gg, \ll \overline{P} \gg$: . . . 4
  - 1.1.2 Conjunction $\ll and \gg, \ll \wedge \gg$ . . . 5
  - 1.1.3 Disjunction $\ll or \gg, \ll \vee \gg$ . . . 5
  - 1.1.4 Implication . . . 5
  - 1.1.5 Equivalence . . . 6
  - 1.1.6 Properties . . . 6
- 1.2 Quantifiers . . . 8
  - 1.2.1 The universal quantifier . . . 8
  - 1.2.2 The existential quantifier . . . 8
- 1.3 Proof Methods . . . 9
  - 1.3.1 Direct Proof . . . 9
  - 1.3.2 Proof by Contrapositive . . . 9
  - 1.3.3 Proof by Contradiction . . . 9
  - 1.3.4 Proof by giving counterexamples . . . 10
  - 1.3.5 Proof by Induction . . . 10
- 1.4 Solved Exercises . . . 11
  - 1.4.1 Exercises . . . 11
  - 1.4.2 Solutions . . . 13

2 Set Theory **19**
- 2.1 Basic definition and notation . . . 19
  - 2.1.1 Subsets . . . 19
  - 2.1.2 Equal Sets . . . 20
  - 2.1.3 Power sets . . . 20
- 2.2 Stets Operations . . . 20
  - 2.2.1 Union . . . 20
  - 2.2.2 Intersection . . . 20
  - 2.2.3 Set Difference . . . 20
  - 2.2.4 Symmetric difference . . . 21
- 2.3 Some properties . . . 21
- 2.4 Partition of a set . . . 22
- 2.5 Product Cartesian . . . 22
- 2.6 Cardinal . . . 22
- 2.7 Solved Exercises . . . 23
  - 2.7.1 Exercises . . . 23
  - 2.7.2 Solutions . . . 25

3 Relations and mapping **31**
- 3.1 RELATIONS . . . 31
  - 3.1.1 Definition . . . 31

3.2 Types of Relations . . . 31
3.3 An equivalence relation . . . 32
3.3.1 Equivalence class . . . 32
3.3.2 The quotient set $\mathbb{Z}/n\mathbb{Z}$ . . . 33
3.4 Order Relation . . . 33
3.4.1 Partial and total order . . . 33
3.4.2 Special Elements of Partially Ordered Sets . . . 34
3.4.3 Solved Exercises . . . 35
3.5 Mappings . . . 44
3.5.1 Definition . . . 44
3.5.2 Image and inverse image . . . 44
3.6 Injectivity, Surjectivity, Bijectivity . . . 45
3.7 Solved Exercises . . . 49
3.7.1 Exercises . . . 49
3.7.2 Solutions . . . 50

4 Algebraic Structures **55**
4.1 Binary Operations . . . 55
4.2 Groups . . . 57
4.2.1 Subgroup . . . 58
4.2.2 Group homomorphisms . . . 59
4.2.3 kernel and image . . . 59
4.3 Examples of groups . . . 60
4.3.1 The group $\mathbb{Z}/n\mathbb{Z}$ . . . 60
4.3.2 Permutation group $\mathscr{S}_n$ . . . 61
4.4 Ring . . . 63
4.4.1 Calculus rules of ring . . . 63
4.4.2 Subring . . . 63
4.4.3 Ring homomorphism . . . 64
4.4.4 An integral domain . . . 65
4.4.5 Ideals . . . 65
4.5 Field . . . 65
4.6 Solved Exercises . . . 66
4.6.1 Exercises . . . 66
4.6.2 Solutions . . . 68

5 Polynomial and Rational Functions **82**
5.1 Polynomials ring . . . 82
5.2 Operations on Polynomials . . . 82
5.2.1 Addition and product . . . 82
5.2.2 Composition . . . 83
5.2.3 Divisibility of polynomial over a field . . . 84
5.2.4 Euclidean division over a field . . . 85
5.2.5 Division according to the increasing degrees . . . 86
5.2.6 Derivative polynomial and Taylor's formula. . . . 88
5.3 Zeros of polynomials . . . 89
5.4 Rational functions . . . 90
5.4.1 Irreducible polynomials . . . 90
5.4.2 Rational Fractions . . . 91
5.5 Partial fractional decomposition . . . 92
5.6 Solved Exercises . . . 96
5.6.1 Exercises . . . 96
5.6.2 Solutions . . . 97

Introduction

The document Algebra I covers the algebra program of the first year of university. The reader will find a part of the course that has been taught and, at the end of each chapter, a part of corrected exercises, most of which have been proposed in the context of supervised work or have been the subject of knowledge control. It is mainly intended for first-year computer engineers and also L.M.D. students, as well as anyone needing basic algebra tools. We hope that this handout meets the expectations of the students and that it will help them succeed.

Chapter 1

Logic

Introduction:
The language used in mathematics is the same all over the world, we can say that it's a universal language. Logic is the science of thinking in the correct way.
Mathematical statements form the basis of logical reasoning in math. Mathematical statements are also called propositions.

Definition 1.0.1. *A proposition is a mathematical statement that is either true or false, but cannot be both true and false at the same time.*

Example 1.0.2.
1. *The number 2 is smaller or equal to 3, this proposition is true.*
2. $\sqrt{2} \notin \mathbb{Q}$, *this proposition is true.*
3. $x+1$ *is not a proposition. This is only a mathematical expression, it isn't an equation.*
4. *It's a beautiful day, this isn't a proposition, it's just someone's personal opinion.*

Definition 1.0.3.
A theorem is a proposition or statement that is demonstrated (for example Pythagoras' theorem, Thales's theorem...)

1.1 Operations

In this section, we are going to give a way to form new statements from old ones. For example, we have P, Q two abstract statements, using the English expression: "**and**", "**or**", "**not**", "**if**", "**then**", "**if and only if**", we will get a new statement like P and Q.

1.1.1 Negation $\ll (notP) \gg, \ll \overline{P} \gg$:

Let P be a proposition, the negation of P denoted by $\overline{P}$.
$\overline{P}$ is true when P is false.
Truth table :

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

Example 1.1.1.
1. $P : \sqrt{2} \notin \mathbb{Q}$, *then* $\overline{P} : \sqrt{2} \in \mathbb{Q}$.
2. P : *the function* f *is positive, then* $\overline{P}$: *the function* f *is not positive.*
3. $P : x+2=0$, *then* $\overline{P} : x+2 \neq 0$.

1.1.2 Conjunction $\ll and \gg, \ll \wedge \gg$

Let P, Q be propositions, The conjunction of P and Q, denoted $\ll \wedge \gg$.
$(P \wedge Q)$ is true if both of P and Q are true.

Truth table :

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

Example 1.1.2. *1.* 2 *is an even number* ***and*** 3 *is a prime number, this proposition is true.*

2. $3 \leq 2$ ***and*** $4 \geq 2$*, this proposition is false.*

1.1.3 Disjunction $\ll or \gg, \ll \vee \gg$

Let P, Q be propositions. The disjunction of P and Q, denoted by $\ll \vee \gg$.

$P \vee Q$ is true if at least one of P or Q is true.

Truth table :

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

Example 1.1.3. *1.* 2 *is an even number* ***or*** 3 *is a prime number, this proposition is true.*

2. $3 \leq 2$ ***or*** $4 \leq 2$*, this proposition is false.*

1.1.4 Implication

Let P, Q be propositions. The proposition "**if** P **then** Q," or "P**implies** Q," denoted by $P \Rightarrow Q$ is called implication or conditional statement.
$P \Rightarrow Q$ is false, if P is true and Q is false.

Truth table :

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

The statement P is called the hypothesis (or premise) of the conditional statement, and the statement Q is called the conclusion (consequence) of the conditional statement.

Example 1.1.4. *1.* $0 \leq x \leq 4 \Rightarrow \sqrt{x} \leq 2$*. True*

2. The car is out of gaze $\Rightarrow$ *the car won't run. True*

Converse

The converse of $(P \Rightarrow Q)$ is $(Q \Rightarrow P)$.

Example 1.1.5. 1. *The converse of:* $(0 \leq x \leq 4 \Rightarrow \sqrt{x} \leq 2)$,
is: $(\sqrt{x} \leq 2 \Rightarrow 0 \leq x \leq 4)$.

2. *The converse of: (The car is out of gaze ⇒ the car won't run),*
***is** : (The car won't run ⇒ the car is out of gaze).*

Contrapositive
The contrapositive of $(P \Rightarrow Q)$ is $(\overline{Q} \Rightarrow \overline{P})$.

Example 1.1.6. ***is** : (If I don't get a party then it isn't my birthday).*

1. *The contrapositive of : (The car is out of gaze ⇒ the car won't run),*
***is** : (The car will run ⇒ the car is not out of gaze).*

Inverse
The inverse of $(P \Rightarrow Q)$ is $(\overline{P} \Rightarrow \overline{Q})$.

Example 1.1.7. *The inverse of : (The car is out of gaze ⇒ the car won't run),*
***is** : (The car isn't out of gaze ⇒ the car will run).*

1.1.5 Equivalence

Let P, Q be propositions, the proposition "P **if and only if** Q, denoted by $P \Leftrightarrow Q$ is called equivalence or bi conditional statement.That means that the two propositions are equivalent if they always have the same truth values.
Truth table :

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

Theorem 1.1.8. *Let P, Q be propositions, we have :*

$$(P \Leftrightarrow Q) \Leftrightarrow (P \Rightarrow Q) \wedge (Q \Rightarrow P).$$

Proof.

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$	$P \Leftrightarrow Q$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	1	0	0	0
0	0	1	1	1	1

1.1.6 Properties

Let P, Q and R be propositions. Then we have

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

5. $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$.
6. $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$.
7. $P \vee P \Leftrightarrow P$.
8. $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$.
9. $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$.
10. $P \wedge (P \vee Q) \Leftrightarrow P$.
11. $P \vee (P \wedge Q) \Leftrightarrow P$.
12. $\overline{P \wedge Q} \Leftrightarrow \overline{P} \vee \overline{Q}$. De Morgan's Law
13. $\overline{P \vee Q} \Leftrightarrow \overline{P} \wedge \overline{Q}$. De Morgan's Law
14. $(P \Rightarrow Q) \Leftrightarrow (\overline{P} \vee Q)$.
15. $(Q \Rightarrow P) \Leftrightarrow (\overline{P} \Rightarrow \overline{Q})$.

Proof. (12)

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

(15)

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

Remark 1.1.9. *Let P, Q be propositions, then*

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

Example 1.1.10. *1. The negation of : $(0 \leq x \leq 4 \Rightarrow \sqrt{x} \leq 2)$ is : $(0 \leq x \leq 4 \wedge \sqrt{x} > 2)$*

2. The negation of : The car is out of gas $\Rightarrow$ the car won't run,
is: The car is out of gas $\wedge$ the car will run.

Definition 1.1.11.
A tautology is a statement that is always true.

Example 1.1.12. *Let P, Q be propositions :*
1. $P \vee \overline{P}$ is tautology.
Truth table :

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

2. $((P \Rightarrow Q) \wedge P) \Rightarrow Q$ is tautology.
Truth table :

P	Q	$P \Rightarrow Q$	$(P \Rightarrow Q) \wedge P$	$((P \Rightarrow Q) \wedge P) \Rightarrow Q$
1	*1*	*1*	*1*	*1*
1	*0*	*0*	*0*	*1*
0	*1*	*1*	*0*	*1*
0	*0*	*1*	*0*	*1*

Remark 1.1.13. *A contradiction is the statement that is always false, (it's the opposite of tautology). For example : $P \wedge \overline{P}$ is contradiction.*
Truth table :

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

1.2 Quantifiers

The statement $P(x)$ it's called a predicate it may be true or false depending on the value of variable x.

1.2.1 The universal quantifier

The universal quantifier is denoted $\forall$ and it reads "for all".
The statement: "$\forall x, P(x)$" is true if $P(x)$ is true for all values of x

1.2.2 The existential quantifier

The existential quantifier is denoted $\exists$ and it reads "there exists". The statement: "$\exists x, P(x)$" is true if $P(x)$ is true for at least one value of x.

Remark 1.2.1. *There exists a unique $x, P(x)$ is denoted by $\exists! x \in E, P(x)$.*

Example 1.2.2.

1. $P(x) : \forall x \in \mathbb{R}, f(x) = 0$, *it means that f is the zero function.*
2. $P(x) : \exists c \in \mathbb{R}$, *such that $f(c) = 0$, that means c is zero of f.*

We can also define predicates with multiple free variables such as $P(x, y)$, if we are using the same quantifier, then the ordering does not matter. But if we are using mixed quantifiers, then the ordering does matter.
For example: $\forall x, \exists y, P(x, y)$ and $\exists y, \forall x, P(x, y)$ are different, For the first y is dependent of x, but for the second y is independent of x.

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

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

Example 1.2.3.
1. *(a) All humans have a blood group. (True)*
2. *(b) All humans have the same blood group. (False)*
3. $(\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : x + y = 0)$. *(True)* $\forall x \in \mathbb{R}, \exists y = -x \in \mathbb{R}, x + (-x) = 0$.
4. $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, x^2 \geq y$. *(True)* $\exists y = 0, \forall x \in \mathbb{R}, x^2 \geq 0$.

Negation Rules:
When we negate a quantified statement, we negate all the quantifiers first,
from left to right (keeping the same order), and next we negative the statement. Let $P(x)$ be a proposition,

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

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

3. $\overline{\forall x \in E, \exists y \in F,\ P(x,y)} \Leftrightarrow \exists x \in E, \forall y \in F,\ \overline{P}(x,y)$.

4. $\overline{\exists x \in E, \forall y \in F,\ P(x,y)} \Leftrightarrow \forall x \in E, \exists y \in F,\ \overline{P}(x,y)$.

Example 1.2.4. *1.* $\overline{\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : x+y=0} \Leftrightarrow \exists x \in \mathbb{R}, \forall y \in \mathbb{R} : x+y \neq 0$.

2. $\overline{\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, x^2 \geq y} \Leftrightarrow \forall y \in \mathbb{R}, \exists x \in \mathbb{R}, x^2 < y$

3. $\overline{\forall \epsilon > 0, \exists q \in \mathbb{Q}^+, 0 < q < \epsilon} \Leftrightarrow \exists \epsilon > 0, \forall q \in \mathbb{Q}^+,\ q \leq 0 \vee q \geq \epsilon$

1.3 Proof Methods

1.3.1 Direct Proof

To prove an implication $P \Rightarrow Q$, we assume that the premise P is true and conclude that Q must be true.

Example 1.3.1. $\forall n \in \mathbb{N}$, *if* n *is even* $\Rightarrow n^2$ *is even. We assume that* n *is even, which means that,* $\exists k \in \mathbb{N}$, *such that* $n = 2k$, *hence,*

$$n.n = 2(2k^2) \Rightarrow n^2 = 2k',$$

where $k' = 2k^2 \in \mathbb{N}$. *Then* $\exists k' \in \mathbb{N}, n^2 = 2k'$, *thus* n^2 *is even.*

1.3.2 Proof by Contrapositive

We have that $(P \Rightarrow Q) \Leftrightarrow (\overline{Q} \Rightarrow \overline{P})$, therefore, instead of proving $P \Rightarrow Q$ we may prove its contrapositive $\overline{Q} \Rightarrow \overline{P}$, since it is an implication, we could use a direct proof: Assume $\overline{Q}$ is true and show that $\overline{P}$ is true.

Example 1.3.2. *For any* $n \in \mathbb{N}$, *if* $5n+3$ *is even then* n *is odd.*

By contrapositive, we must prove that: for any $n \in \mathbb{N}$, *if* n *is even then* $5n+3$ *is odd.*
We assume that n *is even, which means that,* $\exists k \in \mathbb{N}$, *such that* $n = 2k$, *hence*

$$5n+3 = 10k+3 = 10k+2+1 = 2(5k+1)+1 = 2k'+1,$$

where $k' = 5k+1$, *then* n *is odd.*

1.3.3 Proof by Contradiction

The idea of proof by contradiction is to suppose that the statement which we want to prove is false, that means, we suppose that $\overline{P}$ is true. Then we show that this assumption leads to a logical contradiction (to nonsense). Then we conclude that we were wrong to suppose the statement $\overline{P}$ is true, so the statement $\overline{\overline{P}} = P$ is true.

Now let us use the proof by contradiction, to prove the implication $P \Rightarrow Q$:
So we suppose that $\overline{(P \Rightarrow Q)} \Leftrightarrow P \wedge \overline{Q}$ is true, that assume that P is true and Q is false. Argue until we obtain a contradiction, which could be any result that we know is false.

Example 1.3.3. *1. Show that* $\sqrt{2}$ *is an irrational number.*

By contradiction: we suppose that $\sqrt{2} \in Q$, *then* $\exists a, b \in \mathbb{Z}, b \neq 0$ *such that* $\sqrt{2} = \frac{a}{b}$, *we assume that* $\frac{a}{b}$ *is irreducible (*a, b *are co-prime integers). Hence* $2 = \frac{a^2}{b^2}$ *this imply that* a^2 *is even then* a *is itself even,* $\exists k \in \mathbb{N}, a = 2k$, *we obtain that* $b^2 = 2k^2 \Rightarrow b$ *is even, this contradicts the fact that* $\frac{a}{b}$ *is irreducible . That is to say,* $\sqrt{2} \notin Q$.

2. *n is even $\Rightarrow n^2$is even, by contradiction: we suppose that n is even and n^2 is odd.*
   n is even, which means that, $\exists k \in \mathbb{N}$, such that $n = 2k$, hence,

$$n.n = 2(2k^2) \Rightarrow n^2 = 2k',$$

   thus $\exists k' = 2k^2 \in \mathbb{N}, n^2 = 2k'$, n^2 is even this contradicts the fact that n^2 is odd.

1.3.4 Proof by giving counterexamples

To show that a proposition P is false, we must find a counterexample which shows that the proposition P is false.

Example 1.3.4. *(n is even)$\Rightarrow$ (n^2+1 is even), this statement is false because for $n = 2, 4+1 = 5$ is odd, then this is a counterexample.*

Remark 1.3.5. *The proof by given example is invalid. For example:*
1. To show that :$\forall n \in \mathbb{N}$ if, n is even $\Rightarrow n^2$ is even.
We can not say for $n = 2$ is even $\Rightarrow n^2 = 4$ is even, so the statement is true, but we have to prove it for any $n \in \mathbb{N}$.
2. $\forall x \in \mathbb{R}, (x+1)^2 = x^2 + 1$, we can not say that is true because for $x = 0$ we have $1^2 = 1$, (we all know that this statement is false), but we can give a counterexample for $x = 1$ then $(1+1)^2 = 4 \neq 2$. It's show that statement is false.

1.3.5 Proof by Induction

Let $P(n)$ be statement for each $n \in \mathbb{N}$. The principle of mathematical induction states that $P(n)$: is true $\forall n \in \mathbb{N}, n \geq n_0, P_n(x)$ if :

1. $P(n_0)$ is true, and
2. Assume that the statement $P(n)$ is true.
3. Show that the statement $P(n+1)$ is true.

Example 1.3.6. *Show that $\forall n \in \mathbb{N}^* : 1+2+...+n = \frac{n(n+1)}{2}$*

1. *For $n = 1, P(1)$ it true. $1 = \frac{1(2)}{2}$.*
2. *Assume that $1+2+...+n = \frac{n(n+1)}{2}$ is true.*
3. *Show that $1+2+...+n+1 = \frac{(n+1)(n+2)}{2}$ is true,*
   $1+2+...+n+1 = 1+2+...+n+(n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}$.
   Then $P(n+1)$ is true.

1.4 Solved Exercises

1.4.1 Exercises

Exercise 1.4.1. *Let P, Q and R be propositions, using the truth table prove the following logical equivalence*

1. $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$.
2. $(P \wedge Q) \vee R \Leftrightarrow (P \Rightarrow \overline{Q}) \Rightarrow R$.
3. $\overline{(P \Leftrightarrow Q)} \Leftrightarrow (P \wedge \overline{Q}) \vee (Q \wedge \overline{P})$.

Exercise 1.4.2. *Let P, Q and R be propositions, using the truth table prove the following logical statements are tautologies:*

1. $(P \Rightarrow Q) \wedge (Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$.
2. $((\overline{P} \Rightarrow Q) \wedge (\overline{P} \Rightarrow \overline{Q})) \Rightarrow P$.

Exercise 1.4.3. *Let $f : \mathbb{R} \to \mathbb{R}$ be a function. Give the negation of the following propositions:*

1. $(x = 0) \vee (x \neq -1)$.
2. $0 \leq x \leq 1$.
3. $(3 \leq x \leq 4) \Rightarrow (x^2 = 1 \wedge x \geq 0)$.
4. *For all $\epsilon > 0$, there exist $q \in \mathbb{Q}^{*+}$ such that :* $0 < q < \epsilon$.
5. $\forall \epsilon > 0, \exists \eta > 0, \forall (x, y) \in \mathbb{R}^2, (|x - y| \leq \eta \Rightarrow |f(x) - f(y)| \leq \epsilon)$

Exercise 1.4.4. *Use quantifiers to express each of the following statements and prove them if they are true, or give a counterexample when they are false.*

1. *The product of two even numbers is always an even number.*
2. *The product of two odd numbers is always an odd number.*
3. *The product of an even number and an odd number is an even number.*
4. *An natural number is even if and only if its square is even pair.*
5. *The sum of rational and irrational number is irrational.*
6. *The sum of two irrationals number is irrational.*
7. *The product of rational and irrational number is irrational.*
8. *The product of two irrationals number is irrational.*

Exercise 1.4.5. *Find if the following propositions are true or false.*

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

6. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : y^2 = x + 1.$
7. $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}^*, x < y.$
8. $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}^*, x < y.$
9. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R} : (x + y < 0 \vee x + y = 0).$
10. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R} : (x + y < 0 \wedge x + y = 0).$

Exercise 1.4.6. *By using the proof by* ***contrapositive****, show that:*

1. $\forall x, y \in \mathbb{R}, xy \neq 0 \Rightarrow x \neq 0 \wedge y \neq 0.$
2. $\forall x, y \in \mathbb{R}, x \neq y \Rightarrow (x+1)(y-1) \neq (x-1)(y+1).$
3. $(\forall \epsilon > 0, |x| \leq \epsilon) \Rightarrow x = 0.$

Exercise 1.4.7. *By using the proof by* ***contradiction****, show that:*

1. $\forall n \in \mathbb{N}, n^2$ *is even* $\Rightarrow n$ *is even.*
2. $\sqrt{2} \notin \mathbb{Q}$, *deduce that* $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}.$
3. $\frac{\ln 2}{\ln 3} \notin \mathbb{Q}.$
4. $\forall x, y \in \mathbb{R}^+, \frac{x}{y+1} = \frac{y}{x+1} \Rightarrow x = y.$

Exercise 1.4.8. *By using the proof by* ***induction****, show that:*

1. $\forall n \in \mathbb{N} - \{0,1,2,3\}, n^2 \leq 2^n.$
2. $\forall n \in \mathbb{N}, \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$
3. $\forall n \geq 1$, 6 *divide* $7^n - 1.$
4. $\forall n \in \mathbb{N}^*$, $4^n + 6n - 1$ *is multiple of* 9.
5. $\forall n \geq 1, x > -1, (1+x)^n \geq 1 + nx.$

Exercise 1.4.9. *Show that:*

1. $\forall n \in \mathbb{N}, n(n+1)$ *is even.*
2. *Let* $n \in \mathbb{N}$, $n^2 - 1$ *isn't divisible by* $8 \Rightarrow n$ *is even.*
3. $\forall n \in \mathbb{N}, n^3 - n$ *is divisible by* 6.

Exercise 1.4.10. *Give a counterexample to the following statements:*

1. $\forall x, y \in \mathbb{R}$, $(x+y)^2 = x^2 + y^2.$
2. *Let* $n \in \mathbb{Z}$, *if* n^2 *is divisible by* 4, *then* n *is divisible by* 4.
3. *Let* $f : I \to \mathbb{R}$ *be a continuous function then* f *is derivable on* I. *(Where* I *is an interval of* $\mathbb{R}$. *)*
4. *Let* $f, g : \mathbb{R} \to \mathbb{R}$ *be two functions,* $f(x).g(x) = 0 \Rightarrow f(x) = 0 \vee g(x) = 0$
5. *Every bounded sequence is convergent.*

1.4.2 Solutions

Solution 1.4.11. 1. $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$.

Truth table :

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

2. $(P \wedge Q) \vee R \;\Leftrightarrow\; (P \Rightarrow \overline{Q}) \Rightarrow R$. ***Truth table :***

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

3. $\overline{(P \Leftrightarrow Q)} \Leftrightarrow (P \wedge \overline{Q}) \vee (Q \wedge \overline{P})$.

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

Solution 1.4.12. *1.* $H_1 : (P \Rightarrow Q) \wedge (Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$.

Truth table :

P	Q	R	$(P \Rightarrow Q)$	$(Q \Rightarrow R)$	$(P \Rightarrow Q) \wedge (Q \Rightarrow R)$	$P \Rightarrow R$	H_1
1	1	1	1	1	1	1	1
1	0	1	0	1	0	1	1
0	1	1	1	1	1	1	1
0	0	1	1	1	1	1	1
1	1	0	1	0	0	0	1
1	0	0	0	0	0	0	1
0	1	0	1	0	0	1	1
0	0	0	1	1	1	1	1

2.$H_2 : ((\overline{P} \Rightarrow Q) \wedge (\overline{P} \Rightarrow \overline{Q})) \Rightarrow P$ ***Truth table :***

P	Q	$\overline{P}$	$\overline{Q}$	$\overline{P} \Rightarrow Q$	$\overline{P} \Rightarrow \overline{Q}$	$(\overline{P} \Rightarrow Q) \wedge (\overline{P} \Rightarrow \overline{Q})$	H_2
1	1	0	0	1	1	1	1
1	0	0	1	1	1	1	1
0	1	1	0	1	0	0	1
0	0	1	1	0	1	0	1

Solution 1.4.13.

1. $\overline{P} : (x \neq 0) \wedge (x = -1)$.

2. $0 \leq x \leq 1 \Leftrightarrow (0 \leq x \wedge x \leq 1)$, *then:* $\overline{P} : (0 > x \vee x > 1)$.

3. $(3 \leq x \leq 4) \wedge (x^2 \neq 1 \vee x < 0)$.

4. *The negation is: there exists* $\epsilon > 0$, *for all* $q \in Q^{*+}$ *such that:* $0 \geq q \vee q \geq \epsilon$.

5. $\overline{P} : \exists \epsilon > 0, \forall \eta > 0, \exists (x, y) \in \mathbb{R}^2, (|x - y| \leq \eta \wedge |f(x) - f(y)| > \epsilon)$.

Solution 1.4.14.

1. *The product of two even numbers is always an even number*
   Let $\mathscr{P} = \{2k / k \in \mathbb{N}\}$ *be the set of even number, the proposition P is :*$\forall n, m \in \mathscr{P}, n \times m \in \mathscr{P}$, *P is true.*
   Let $n, m \in \mathscr{P}$, *so* $\exists k_1 \in \mathbb{N} / n = 2k_1, \exists k_2 \in \mathbb{N} / m = 2k_2$ *so* $n \times m = 2(2k_1 k_2) = 2k_3$, *then* $\exists k_3 = 2k_1 k_2 \in \mathbb{N} / n \times m = 2k_3 \Rightarrow n \times m \in \mathscr{P}$.

2. *The product of two odd numbers is always an odd number.*
   Let $I = \{2k + 1 / k \in \mathbb{N}\}$ *be the set of odd number. The proposition P is:* $\forall n, m \in I, n \times m \in I$, *P is true.*
   Let $n, m \in I$, *so* $\exists k_1 \in \mathbb{N} / n = 2k_1 + 1, \exists k_2 \in \mathbb{N} / m = 2k_2 + 1$ *so* $n \times m = 2(2k_1 k_2 + k_1 + k_2) + 1 = 2k_3 + 1$, *then* $\exists k_3 = 2k_1 k_2 + k_1 + k_2 \in \mathbb{N} / n \times m = 2k_3 + 1 \Rightarrow n \times m \in I$.

3. *The product of an even number and an odd number is an even number.*
   The proposition P is : $\forall n \in \mathscr{P}, m \in I, n \times m \in \mathscr{P}, n \times m \in I$, *P is true. Let* $n \in \mathscr{P}, m \in I$, *so* $\exists k_1 \in \mathbb{N} / n = 2k_1, \exists k_2 \in \mathbb{N} / m = 2k_2 + 1$ *so* $n \times m = 2(2k_1 k_2 + k_1) = 2k_3$, *then* $\exists k_3 = 2k_1 k_2 + k_1 \in \mathbb{N} / n \times m = 2k_3 \Rightarrow n \times m \in \mathscr{P}$.

4. *An natural number is even if and only if its square is even pair. The proposition P is:* $[\forall n \in \mathbb{N}, n$ *is even* $\Leftrightarrow n^2$ *is even], P is true. Now we are going to show that: if n is even* $\Rightarrow n^2$ *is even.*
   Let $n \in P$, *so* $\exists k_1 \in \mathbb{N} / n = 2k_1$, *so* $n^2 = n.n = 2(2k_1^2)$, *then* $\exists k_2 = 2k_1^2 \in \mathbb{N} / n^2 = 2k_2 \Rightarrow n^2$ *is even.*
   Now we are going to show that: if n^2 *even* $\Rightarrow n$ *is even.*
   By contrapositive, we must prove that n is odd $\Rightarrow n^2$ *is odd, it's true using the second question of the current exercise, then* n^2 *is even* $\Rightarrow n$ *is even and n is even* $\Rightarrow n^2$ *is even so we have* $\forall n \in \mathbb{N}, n$ *is even* $\Leftrightarrow n^2$ *is even.*

5. *The sum of rational and irrational numbers is irrational.*
   The proposition P is :$\forall m \in \mathbb{Q}, n \notin \mathbb{Q}, m + n \notin \mathbb{Q}$, *P is true*
   $\exists a, b \in \mathbb{Z}, b \neq 0, a \wedge b = 1, m = \frac{a}{b}$, *and* $n \notin \mathbb{Q}$, $b = 1$, *we suppose by contradiction that* $n + m \in \mathbb{Q}$ *so there exists* $c, d \in \mathbb{Z}, c \wedge d = 1$, $n + \frac{a}{b} = \frac{c}{d} \Rightarrow n = \frac{c}{d} - \frac{a}{b}$ *(you must know that the sum and difference between two rationales is rational) then we conclude that* $n \in \mathbb{Q}$ *but* $n \notin \mathbb{Q}$ *so contradiction then the supposition that* $n + m \in \mathbb{Q}$ *is false so* $n + m \notin \mathbb{Q}$.

6. *The sum of two irrational numbers is irrational.*
   The proposition P is: $\forall m, n \notin \mathbb{Q}, m + n \notin \mathbb{Q}$, *P is false.*
   $\exists n = \sqrt{2}, m = 1 - \sqrt{2}, n + m = 1 \in \mathbb{Q}$.

7. *The product of rational and irrational number is irrational.*
   The proposition P is: $\forall m \in \mathbb{Q}, n \notin \mathbb{Q}, m.n \notin \mathbb{Q}$, *P is true*
   $\exists a, b \in \mathbb{Z}^*, a \wedge b = 1, m = \frac{a}{b}$, *and* $n \notin \mathbb{Q}$, *we suppose by contradiction that* $n.m \in \mathbb{Q}$ *so there exists* $c, d \in \mathbb{Z}, c \wedge d = 1$, $n.\frac{a}{b} = \frac{c}{d} \Rightarrow n = \frac{c}{d}.\frac{b}{a}$ *(you must know that the product and division between two rationals is rational) then we conclude that* $n \in \mathbb{Q}$ *but* $n \notin \mathbb{Q}$ *so contradiction then the supposition that* $n.m \in \mathbb{Q}$ *is false so* $n.m \notin \mathbb{Q}$.

8. *The product of two irrational numbers is irrational.*
The proposition P is: $\forall m,n \notin \mathbb{Q}, m.n \notin \mathbb{Q}$, *P is false.*
$\exists n = \sqrt{2}, m = \sqrt{8}, n.m = 4 \in \mathbb{Q}$.

Solution 1.4.15.

1. $P : \exists x \in \mathbb{R}, \forall y \in \mathbb{R} : x + y > 0$, *is false because,* $\overline{P}$ *:* $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : x + y \leq 0$, *is true, in fact* $\forall x \in \mathbb{R}, \exists y = -x \in \mathbb{R}; x + y \leq 0$

2. $P : \forall x \in \mathbb{R}, \forall y \in \mathbb{R} : x + y > 0$, *is false because* $\overline{P} : \exists x \in \mathbb{R}, \exists y \in \mathbb{R} : x + y \leq 0$ *is true , in fact:* $\exists x = 0, \exists y = 0; 0 \leq 0$.

3. $\exists x \in \mathbb{R}, \exists y \in \mathbb{R} : x + y > 0$, *is true, in fact:* $\exists x = 0, \exists y = 1; 1 > 0$.

4. $\exists x \in \mathbb{R}, \forall y \in \mathbb{R} : y^2 > x$ *is true, in fact:* $\exists x = -1 \in \mathbb{R}, \forall y \in \mathbb{R} : y^2 > x$.

5. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : y = x^2 + 1$, *is true, in fact:* $\forall x \in \mathbb{R}$, $\exists y = x^2 + 1 \in \mathbb{R}$.

6. $P : \forall x \in \mathbb{R}, \exists y \in \mathbb{R} : y^2 = x + 1$, *is false because* $\overline{P}$ *is true:* $\bar{P} : \exists x = -2 \in \mathbb{R}, \forall y \in \mathbb{R}, y^2 \neq -1$.

7. $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}^*, x < y$ *is false because* $\overline{P}$ *is true:* $\overline{P} : \forall x \in \mathbb{R}, \exists y = -x^2 - 1 \in \mathbb{R}^*$,
$x \geq -x^2 - 1$.

8. $P : \exists y \in \mathbb{R}, \forall x \in \mathbb{R}^*, x < y$. *is false because* $\overline{P}$ *is true:* $\overline{P} : \forall y \in \mathbb{R}, \exists x = y^2 + 1 \in \mathbb{R}^*$,
$y^2 + 1 \geq y$.

9. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R} : (x + y < 0 \vee x + y = 0)$, *is false because* $\overline{P}$ *is true:*
$\exists x = 1, \exists y = 0, (1 + 0 \geq 0 \wedge 1 + 0 \neq 0)$.

10. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R} : (x + y < 0 \wedge x + y = 0)$ *is false because* $\bar{P}$ *is true:*
$\exists x = 1, \exists y = 0, (1 + 0 \geq 0 \vee 1 + 0 \neq 0)$.

Solution 1.4.16.

1. $\forall n \in \mathbb{N}, n^2$ *is odd* $\Rightarrow n$ *is odd.*

   The contrapositive is given by: n *is even* $\Rightarrow n^2$ *is even, it's true see the exercise 4.1). Then the proposition* $P \Rightarrow Q$ *is true because we have proved that contrapositve* $\overline{Q} \Rightarrow \overline{P}$ *is also true.*

2. *By contrapositive we are going to prove that* $\forall x, y \in \mathbb{R}, (x+1)(y-1) = (x-1)(y+1) \Rightarrow x = y$ *is true, in the fact :*

$$(x + 1)(y - 1) = (x - 1)(y + 1) \Rightarrow xy - x + y - 1 = xy + x - y - 1 \Rightarrow 2x = 2y \Rightarrow x = y.$$

3. *By contrapositive we are going to prove that:*
($x \neq 0 \Rightarrow (\exists \epsilon > 0, |x| > \epsilon)$*) is true. Let* $x \neq 0$*, there exist* $\epsilon = \frac{|x|}{2} > 0$ *such that* $|x| > \frac{|x|}{2}$ *because* $x \neq 0$.

Solution 1.4.17.

1. $\forall n \in \mathbb{N}, n^2$ *is even* $\Rightarrow n$ *is even. By contradiction, we are going to prove that :*
Let $n \in \mathbb{N}$ *by contradiction, we suppose that* n^2 *is even and* n *is odd, then* $\exists k \in \mathbb{N}$ *such that* $n = 2k + 1$ *so* $n^2 = 2(2k^2 + 2k) + 1 = 2k' + 1, k' = (2k^2 + 2k) \in \mathbb{N}, n^2$ *is odd, here the contradiction because* n^2 *is even. Then our supposition is false so* $\forall n \in \mathbb{N}$, n^2 *is even* $\Rightarrow n$ *is even, it's true.*

2. *By contradiction, we suppose that:* $\sqrt{2} \in \mathbb{Q}$ *, so* $\exists a, b \in \mathbb{N}, b \neq 0 \;\; a \wedge b = 1, /\sqrt{2} = \frac{a}{b} \Rightarrow \frac{a^2}{b^2} \Rightarrow 2b^2 = a^2$*, then* a *is even* $\exists k \in \mathbb{N} / n = 2k$*, so*

$$2b^2 = 4k^2 \Leftrightarrow b^2 = 2k^2,$$

we deduce that b *is even too or* $a \wedge b = 1$ *here the contradiction, Then our supposition is false so* $\sqrt{2} \notin \mathbb{Q}$.
By contradiction, we suppose that $\sqrt{2} + \sqrt{3} \in \mathbb{Q}$*, so* $\exists a, b \in \mathbb{N}^*, \;\; a \wedge b = 1, \; \sqrt{2} + \sqrt{3} = \frac{a}{b}$
then $\sqrt{3} = \frac{a}{b} - \sqrt{2} \Rightarrow 3 = (\frac{a^2}{b^2} + 2) - 2\frac{a}{b}\sqrt{2} \Rightarrow \sqrt{2} = [(\frac{a^2}{b^2} + 2) - 3]\frac{b}{2a}$*. So* $\sqrt{2} = \frac{a^2 - b^2}{2ab} \in \mathbb{Q}$ *contradiction with the* $\sqrt{2} \notin \mathbb{Q}$*. Then our supposition is false, so* $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$

3. *By contradiction we suppose that* $\frac{\ln 2}{\ln 3} \in \mathbb{Q}$*, :* $\exists a, b \in \mathbb{N}, b \neq 0 \;\; a \wedge b = 1, \frac{\ln 2}{\ln 3} = \frac{a}{b}$ *so* $b \ln 2 = a \ln 3 \Rightarrow 2^b = 3^a$ *the* 3^a *is even contradiction. Then our supposition is false so* $\frac{\ln 2}{\ln 3} \notin \mathbb{Q}$.

4. $\forall x, y \in \mathbb{R}^+$*, By contradiction we suppose that* $\frac{x}{y+1} = \frac{y}{x+1} \wedge x \neq y$*, so:*

$$\frac{x}{y+1} = \frac{y}{x+1} \Rightarrow x^2 + x = y^2 + y \Rightarrow x^2 - y^2 + x - y = 0$$

$$\Rightarrow (x - y)(x + y + 1) = 0 \Rightarrow x + y + 1 = 0 \Rightarrow x + y = -1.$$

such that $x, y \in \mathbb{R}^+$*. then the contradiction.*

Solution 1.4.18. *By induction we show that:*

1. $\forall n \in \mathbb{N} - \{0, 1, 2, 3\}, n^2 \leq 2^n$.

   (a) *For* $n = 4$ *we have:* $4^2 \leq 2^4$*,* $P(4)$ *is true.*

   (b) *We suppose that:* $n^2 \leq 2^n$*,* $P(n)$ *is true.*

   (c) *We prove that:* $(n+1)^2 \leq 2^{n+1}$*,* $P(n+1)$ *is true.*

   We have: $(n+1)^2 = n^2 + 2n + 1 \leq n^2 + n^2 \leq 2n^2 \leq 2.2^n \leq 2^{n+1}$.
   Since $n \geq 4 \Rightarrow 2n < n.n$*, then* $2n \leq n^2 - 1$.
   Or we can prove that $n^2 - 2n - 1 \geq 0, \forall n \geq 4$.
   Then $P(n+1)$ *is true, so* $\forall n \in \mathbb{N} - \{0, 1, 2, 3\}, n^2 \leq 2^n$.

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

   (a) *For* $n = 1, P(1)$ *it true.* $1 = \frac{1(2)(3)}{6}$.

   (b) *Assume that:* $1^2 + 2^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$ *is true.*

   (c) *Show that:* $1^2 + 2^2 + ... + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}$ *is true,*

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

   $\sum_{k=1}^{n+1} k^2 = \frac{(n+1)(n+2)(2n+3)}{6}$*, then* $P(n+1)$ *is true, so* $P(n)$ *is true.*

3. $\forall n \geq 1$, 6 *divide* $7^n - 1$.

   (a) *For* $n = 1$*,* $P(1)$ *it true.* $7 - 1 = 6 = 6.1$.

   (b) *Assume that:* 6 *divide* $7^n - 1$ *is true, so there* $\exists k \in \mathbb{Z}$ *such that* $7^n - 1 = 6k$.

(c) *Show that:* 6 *divide* $7^{n+1}-1$ *is true,*

$$7^{n+1}-1=7(7^n-1+1)-1=7.(6k)+7-1=6(7k+1)=6k', k'=6k+1\in\mathbb{Z}.$$

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

4. $\forall n\in\mathbb{N}^*$, 4^n+6n-1 *is multiple of* 9.

(a) *For* $n=1, P(1)$ *it true.* $4+6-1=9$.

(b) *Assume that:* 4^n+6n-1 *is multiple of* 9 *is true, so there* $\exists k\in\mathbb{Z}$ *such that* $4^n+6n-1=6k$.

(c) *Show that:* $4^{n+1}+6(n+1)-1$ *is multiple of* 9 *is true,*

$$4^{n+1}+6(n+1)-1=4[4^n+6n-1+(1-6n)]+6n+6-1$$

$$=4[9k]+4(1-6n)+6n+5=4[9k]-24n+4+6n+5=9[4k-3n+1]=9k'$$

Where $k'=4k-3n+1\in\mathbb{Z}$. *Then* $P(n+1)$ *is true, so* $P(n)$ *is true.*

5. $\forall n\geq 1, x>-1, (1+x)^n\geq 1+nx$..

(a) *For* $n=1, P(1)$ *it true.* $(1+x)\geq 1+x$.

(b) *Assume that:* $(1+x)^n\geq 1+nx$ *is true.*

(c) *Show that:* $(1+x)^{n+1}\geq 1+(n+1)x$ *is true,*

$(1+x)^n\geq 1+nx\Rightarrow(1+x)^{n+1}\geq(1+x)(1+nx)$
Now we have to prove that $(1+x)(1+nx)\geq 1+(n+1)x\Rightarrow 1+nx+x+nx^2\geq 1+nx+1$, *which is true because* $nx^2\geq 0$. *Then* $P(n+1)$ *is true, so* $P(n)$ *is true.*

Solution 1.4.19.

1. $\forall n\in\mathbb{N}, n(n+1)$ *is even .*
If n *is even then* $n+1$ *is odd using the exercise 4) the product of even and odd numbers is an even number, then* $n(n+1)$ *is even.*
If else n *is odd then* $n+1$ *is even, with the same way we conclude that* $n(n+1)$ *is even.*

2. *By contrapositive we show that the proposition :(* n *is odd* $\Rightarrow(n^2-1)$ *is divide by* 8*) is true.*
Let n *be an odd number there* $\exists k\in\mathbb{N}$ *such that* $n=2k+1\Rightarrow n^2=4k^2+4k+1\Rightarrow n^2-1=4k^2+4k=4k(k+1)$, *Since* $k(k+1)$ *is even* $\exists k'\in\mathbb{N}/k(k+1)=2k'$, *so* $n^2-1=4(2k')=8k'\Rightarrow n^2-1$ *is divide by* 8.

3. *By induction, we are going to show that:* $\forall n\in\mathbb{N}, n^3-n$ *is divisible by* 6,

(a) *For* $n=0$ *we have:* 0^3-0 *is divisible by* 6, $P(0)$ *is true.*

(b) *Assume that:* n^3-n *is divisible by* 6, $P(n)$ *is true.*

(c) *Show that:* $(n+1)^3-n-1$ *is divisible by* 6, $P(n+1)$ *is true.*

$(n+1)^3-n-1=n^3+3n^2+3n+1-n-1=n^3-n+3n(n+1)$,
since $\exists k\in\mathbb{N}, n^3-n=6k, \exists k'\in\mathbb{N}, n(n+1)=2k$,
so $(n+1)^3-n-1=6k+3.2k'=6(k+k')=6k'', k''\in\mathbb{N}$.
Then $P(n+1)$ *is true, so* $P(n)$ *is true too.*

Solution 1.4.20.

1. $P:\forall x,y\in\mathbb{R}, (x+y)^2=x^2+y^2$, P *is false, because* $\exists x=1, y=2$ *such that* $(1+2)^2=9\neq 5=1^2+2^2$.

2. *Let* $n\in\mathbb{Z}$, P: *if* n^2 *is divisible by* 4, *then* n *is divisible by* 4, *the proposition is false, because for* $n=2$ *we have* $n^2=4$ *is divisible by* 4 *but* 2 *isn't.*

3. *Let* $f : I \to \mathbb{R}$ *be a continuous function, then* f *is derivable on* I*. (Where* I *is an interval of* $\mathbb{R}$*.) This proposition is false because for* $f(x) = |x|$ *a continuous function on* $\mathbb{R}$ *but* f *isn't derivable on* $\mathbb{R}$*, for* $x_0 = 0$*,* $f'(0)$ *doesn't exist.*

4. *Let* $f, g : \mathbb{R} \to \mathbb{R}$ *be two functions,* $f(x).g(x) = 0 \Rightarrow f(x) = 0 \vee g(x) = 0$ *. This proposition is false because for*

$$f(x) = \begin{cases} x, & \text{if } x \geq 0 \\ 0 & \text{if } x < 0. \end{cases}, g(x) = \begin{cases} 0, & \text{if } x \geq 0 \\ 1 + x & \text{if } x < 0. \end{cases}$$

We remark that $f(x)g(x) = 0$ *and* $f(x) \neq 0, g(x) \neq 0.$

5. *Every bounded sequence is convergent. This proposition is false because for* $x_n = (-1)^n$ *is bounded, but it doesn't converge (we know that if the limit exists it's unique) but the sequence admits two limit different, so the limit doesn't exist.*

Chapter 2

Set Theory

2.1 Basic definition and notation

Definition 2.1.1. *A set is a collection of objects called elements.*

Definition 2.1.2. *The emptyset is the set with no elements, denoted by* $\emptyset$.

We often use capital letters as A to denote sets, and lower letters as a to denote the elements.

Notation :

1. $a \in A$ (a is an element of A).
2. $a \notin A$ (a is not an element of A).
3. $\mathbb{N}$ is the set of all natural numbers.
4. $\mathbb{Z}$ is the set of all integers numbers.
5. $\mathbb{Q}$ is the set of all rational numbers.
6. $\mathbb{R}$ is the set of all real numbers.

Example 2.1.3. *1.* $A = \{a\}$ *is a singleton set is a set containing one element* a.

2. $E = \{2,4,6,8,...\}$ *is the set of all even numbers.*
3. $O = \{1,3,5,7,...\}$ *is the set of all odd numbers.*
4. $B = \{x \in \mathbb{Z}, x$ *is divisible by* $3\}$.

2.1.1 Subsets

Definition 2.1.4. *1. A set* B *is a subset of* A*, if every element of* B *is also an element of* A*. We denote this by* $B \subset A$ *: this means that*

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

Negation:

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

2.1.2 Equal Sets

We say that A equals B, if have the same elements. We denote this by $A = B$: this means that

$$A = B \Leftrightarrow ((A \subset B) \text{ and } (A \subset B)) \Leftrightarrow (\forall x, (x \in A \Leftrightarrow x \in B))$$

Example 2.1.5. *1.* $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

2. $A = \{0,1,2,3,5,8\}, B = \{8,1,5,0,3,2\}, C = \{0,1,2,5\}, D = \{1,2,3,4\}$ *then we have that :* $A = B, C \neq A$, $C \subset A$, $D \not\subset A, D \neq C$.

Remark 2.1.6. *The empty set $\emptyset$ is a subset of every set.*

2.1.3 Power sets

The set of all subsets of a set E is called the power set of E and denoted by $\mathscr{P}(E)$. $\mathscr{P}(E) = \{X / X \subset E\}$.

Remark 2.1.7. *The empty $\emptyset$ and E are elements of $\mathscr{P}(E)$.*

Example 2.1.8. $E = \{a\}, \mathscr{P}(E) = \{\emptyset, \{a\}\}, \mathscr{P}(\mathscr{P}(E)) = \{\emptyset, \{\emptyset, \{a\}\}, \{\emptyset\}, \{\{a\}\}$.

2.2 Stets Operations

Let A, B be any two sets.

2.2.1 Union

The **union** of A and B is the set of elements in either A, or B, it is denoted by $A \cup B$. This means that :

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

Negation:

$$x \notin A \cup B \Leftrightarrow (x \notin A \wedge x \notin B).$$

2.2.2 Intersection

The intersection of A and B is the set of elements in both A and B, it is denoted by $A \cap B$. This means that :

$$x \in A \cap B \Leftrightarrow (x \in A \wedge x \in B).$$

Negation :

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

Remark 2.2.1. *Two sets A, B are said disjoint if $A \cap B = \emptyset$.*

2.2.3 Set Difference

The set difference between A and B is the set of elements ib A but not in B, it is denoted by $A - B$ or $A \setminus B$. This means that :

$$A - B = \{x / x \in A \wedge x \notin B\}.$$

If $A \subset B$ then $B - A$ is called the complement of A (denoted by A^c or C_B^A). This means that :

$$C_B^A = \{x / x \in B \wedge x \notin A\}.$$

2.2.4 Symmetric difference

Let A,B be two subsets of E
The symmetric difference of A and B is the set$(A-B)\cup(B-A)$ denoted by $A\Delta B$. Hence

$$A\Delta B=(A-B)\cup(B-A)=(A\cap C_E^B)\cup(B\cap C_E^A)=(A\cup B)-(A\cap B).$$

$$x\in A\Delta B\Leftrightarrow\{x/x\in(A-B)\vee x\in(B-A)\}.$$

Example 2.2.2. *Let* $E=\{1,2,3,4,5,6,7,8\},A=\{1,2,3,4,5,6\},B=\{2,4,6,8\}$

1. $A\subset E,B\subset E$.
   $A\not\subset B$ *because* $1\in A\wedge 1\notin B$.
   $B\not\subset A$ *because* $8\in B\wedge 8\notin A$.
2. $A\cap B=\{2,4,6\},A\cup B=\{1,2,3,4,5,6,8\}$.
3. $A-B=\{1,3,5\},B-A=\{8\}$.
4. $A\Delta B=\{1,3,5,8\}$.

2.3 Some properties

Let A, B and C be subsets of a suitable universal set E, then

1. $A\cup A=A$, $A\cap A=A$.
2. $A\cap B=B\cap A$
3. $A\cup B=B\cup A$
4. $A\cap(B\cap C)=(A\cap B)\cap C$,
5. $A\cup(B\cup C)=(A\cup B)\cup C$.
6. $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$
7. $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.
8. $(A\cup B)^c=A^c\cap B^c$. De Morgan's Law
9. $(A\cap B)^c=A^c\cup B^c$. De Morgan's Law

Proof. Let us prove that: $(A\cup B)^c=A^c\cap B^c$, then we must show that:
$(A\cup B)^c\subset A^c\cap B^c$ and $A^c\cap B^c\subset(A\cup B)^c$.

$(A\cup B)^c\subset A^c\cap B^c$: let $x\in(A\cup B)^c$
$x\in(A\cup B)^c\Rightarrow x\notin(A\cup B)\Rightarrow x\notin A\wedge x\notin B\Rightarrow x\in A^c\wedge x\in B^c$, hence $x\in(A\cup B)^c\Rightarrow x\in(A^c\cap B^c)$, then $(A\cup B)^c\subset(A^c\cap B^c)$.

$A^c\cap B^c\subset(A\cup B)^c$: let $x\in(A^c\cap B^c)$
$x\in(A^c\cap B^c)\Rightarrow x\in A^c\wedge x\in B^c\Rightarrow x\notin A\wedge x\notin B\Rightarrow x\notin(A\cup B)$, hence $A^c\cap B^c\subset(A\cup B)^c$, then $(A\cup B)^c=A^c\cap B^c$.

2.4 Partition of a set

Let E be finite set and $A_i \in \mathscr{P}(E), i = 1,...,n$, then $\{A_1, A_2, ..., A_n\}$ is **a partition of** E if :

1. $A_1 \cup A_2 \cup ... \cup A_n = \bigcup_{i=1}^{n} A_i = E$.
2. $A_i \cap A_j = \emptyset$, for $i \neq j$.

Example 2.4.1. *Let* $E = \{0,1,2,3,4,5,6,7,8,9\}$, $A = \{0,1,3\}, B = \{2,4\}$, $C = \{5,7\}, D = \{6,8,9\}$, *since* $A \cup B \cup C \cup D = E$, *and* $A \cap B = B \cap C = \mathbb{C} \cap D = A \cap C = A \cap D = ... = \emptyset$. *Then* $\{A,B,C,D\}$ *is a partition of* E.

2.5 Product Cartesian

Let A and B be sets, $a \in A, b \in B$, we can form the ordered pair (a,b).
We denote by $A \times B$ **the Cartesian product** of A and B defined by :

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

Example 2.5.1. $A = \{1,2\}, B = \{1,2,3\}$

$$A \times B = \{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3)\},$$

$$B \times A = \{(1,1),(1,2),(2,1),(2,2),(3,1),(3,2)\},$$

$A \times B \neq B \times A$, *because* $(3,2) \in B \times A$, *and* $(3,2) \notin A \times B$.

2.6 Cardinal

Definition 2.6.1. *the Cardinal of a set* A *is the number of elements of* A. *We note the cardinal number by* $n(A)$, *or* $|A|$. *If* $n(A)$ *is finite, then* A *is said to be finite, Otherwise,* A *is said to be infinite.*

Remark 2.6.2. *1.* $n(\emptyset) = 0$, $n(\{\emptyset\}) = 1$.
2. Let $\mathscr{E}$ *be an nonempty set, then*

$$n(\mathscr{P}(\mathscr{E})) = 2^n.$$

Proposition 2.6.3. *Let* A,B *be finite sets then :*

1. $n(A \times B) = n(A) \times n(B)$.
2. $n(A \cup B) = n(A) + n(B) - n(A \cap B)$.

Example 2.6.4. *Let* $A = \{0,1,2\}, B = \{1,2,3,4\}$, *then :*
$n(\mathscr{P}(A)) = 2^3, n(\mathscr{P}(B)) = 2^4$.
$\mathscr{P}(A) = \{\emptyset,\{0\},\{1\},\{2\},\{0,1\},\{0,2\},\{1,2\},A\}$.
$\mathscr{P}(B) = \{\emptyset,\{1\},\{2\},\{3\},\{4\},\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\},\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\},B\}$.
$n(A \times B) = 12 = n(B \times A) = n(A)n(B)$.

$$A \times B = \{(0,1),(0,2),(0,3),(0,4),(1,1),(1,2),(1,3),(1,4),(2,1),(2,2),(2,3),(2,4)\},$$

$$B \times A = \{(1,0),(1,1),(1,2),(2,0),(2,1),(2,2),(3,0),(3,1),(3,2),(4,0),(4,1),(4,2)\},$$

$A \times B \neq B \times A$, *because* $(3,2) \in B \times A$, *and* $(3,2) \notin A \times B$.
$A \cup B = \{0,1,2,3,4\}, A \cap B = \{1,2\}, n(A \cup B) = n(A) + n(B) - n(A \cap B) = 3 + 4 - 2 = 5$.

2.7 Solved Exercises

2.7.1 Exercises

Exercise 2.7.1. *Let us consider the following sets:*
$A=\{1,2,3\}, B=\{\{1,2\},3\}, C=\{\{1,2,3\}\}, D=\{\emptyset,1,2,3\}$,
$E=\{3,1,2\}, F=\{\{1,3\},\{2\}\}, G=\{\{1,3\},\{2\},2,\{\emptyset\}\}, H=\{1,\{2\},\{3\}\}$.

1. *Find all equality and inclusion between these sets.*
2. *Find* $A\cap B$, $B\cap F$, $A\cap H$, $A\cup B$, $D\cup G$, $D-A$, $G-F$, $A\Delta B$, $G\Delta D$.
3. *Find the complement of* A *on* D, *and the complement of* A *on* G.
4. *Find* $\mathscr{P}(B), \mathscr{P}(G)$.

Exercise 2.7.2. *Let* A,B,C *and* D *be sets defined by :*

$$A=\{0,1,2\}, B=\{\{0,1\},2\}, C=\{0,\{0,1\},\{2\},\emptyset\}, D=\{0,1\}.$$

1) *Tell if the following propositions are true.*
$a) 0\in B, b)\{0,1\}\subset B, c)\emptyset\in C, d)\emptyset\subset C, e)\{\emptyset\}\subset C$.
2. Find : $A\cap B$, $A\cap C$, $A-B$, $C-B$, $A\times D$, $\mathscr{P}(A)$, $\mathscr{P}(\mathscr{P}(D))$.
3. Let E,F *be two sets. Prove that* $\mathscr{P}(E)=\mathscr{P}(F)\Rightarrow E=F$.

Exercise 2.7.3. *Let A, B and C be subsets of a suitable universal set* E,
a) Show that:

1. $(A\cap B)\cup B^c = A\cup B^c$.
2. $(A-B)-C = A-(B\cup C)$.
3. $(A\cup B)-C = (A-C)\cup(B-C)$
4. $(A\cap B)-C = (A-C)\cap B = (B-C)\cap A$.
5. $A-(B\cap C) = (A-B)\cup(A-C)$
6. $A^c - B^c = B-A$.

b) Simplify the following:
1. $\overline{(A\cup B)}\cap\overline{(C\cup\overline{A})}$.
2. $\overline{(A\cap B)}\cup(C\cap\overline{A})$.
3. $(A-C)\cup(B-C)\cup(A^c-B^c)\cup C$.
4. $(A-(B^c\cup C)\cup A^c\cup B^c\cup C$.

Exercise 2.7.4. *Let A, B and C be subsets of a suitable universal set* E, *show that*

1. $(A\cap B)\cup C = (A\cup C)\cap(B\cup C)$
2. $(A\cup B)\cap C = (A\cap C)\cup(B\cap C)$
3. $(A\cap B)-(A\cap C) = (A\cap B)\cap C^c$

Exercise 2.7.5. *Let A, B be subsets of a suitable universal set* E, *show that:*
$A\subset B\Rightarrow B^c\subset A^c$.
Deduce that :
1. $(A\cap B)^c = A^c\cup B^c$.
2. $(A\cup B)^c = A^c\cap B^c$.

Exercise 2.7.6. *Let A, B be subsets of a suitable universal set E, show that*

1. $\mathscr{C}_E A \Delta \mathscr{C}_E B = A \Delta B$.
2. $\mathscr{C}_E(A \Delta B) = \mathscr{C}_E A \Delta B = A \Delta \mathscr{C}_E B$.
3. *Evaluate :* $A \Delta A^c, B \Delta E, B \Delta \emptyset$.

Exercise 2.7.7. *Let A, B and C be subsets of a suitable universal set E, prove that:*

1. $A \cup B = A \cap C \Leftrightarrow B \subset A \subset C$.
2. $[(A \cup B \subset A \cup C) \wedge (A \cap B \subset A \cap C)] \Rightarrow B \subset C$.

Exercise 2.7.8. *Let A, B and C be subsets of a suitable universal set E, prove that:*

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

Exercise 2.7.9. *1. Let us consider the following sets:* $E = \{0,1,2,3,4,5\}$, *and* $A = \{(i,j) \in E^2 / i < j\}$, $B = \{(i,j) \in E^2 / i > j\}$, $C = \{(i,j) \in E^2 / i = j\}$. *Draw A,B et C, and prove that $\{A,B,C\}$ is a partition of $E \times E$.*
2. Let $a,b,c \in \mathbb{R}$, with $a \geq 0$. Find a condition for which the following subsets $]0,a[$, $]-\infty,b]$, and $[c,+\infty[$ form a partition of $\mathbb{R}$.

2.7.2 Solutions

Solution 2.7.10. *Let us consider the following sets:*
$A=\{1,2,3\}, B=\{\{1,2\},3\}, C=\{\{1,2,3\}\}, D=\{\emptyset,1,2,3\},$
$E=\{3,1,2\}, F=\{\{1,3\},\{2\}\}, G=\{\{1,3\},\{2\},2,\{\emptyset\}\}, H=\{1,\{2\},\{3\}\}.$

1. $A\subset D, A=E, F\subset G.$

2. $A\cap B=\{3\}, B\cap F=\emptyset, A\cap H=\{1\}, A\cup B=\{1,2,3,\{1,2\}\},$
   $D\cup G=\{\emptyset,1,2,3,\{2\},\{\emptyset\},\{1,3\}\}, D-A=\{\emptyset\}, G-F=\{2,\{\emptyset\}\},$
   $A\Delta B=(A-B)\cup(B-A)=\{1,2,\{1,2\}\},$
   $G\Delta D=(G-D)\cup(D-G)=\{\{1,3\},\{2\},\{\emptyset\},\emptyset,1,3\}.$

3. $A_D^c=\{\emptyset\}$, $A_G^c=\{\{1,3\},\{2\},\{\emptyset\}\}.$

4. *The set B has two elements that mean that* $Card(B)=2$, *then* $card(\mathscr{P}(B))=2^2=4$, *so* $\mathscr{P}(B)$ *has* 4 *elements, which are :* $\mathscr{P}(B)=\{\emptyset,\{\{1,2\}\},\{3\},B\}$,
   The set G has 4 *elements so* $Card(G)=4$, *then* $card(\mathscr{P}(G))=2^4=16$, *so* $\mathscr{P}(G)$ *has* 16 *elements, which are :*
   $\mathscr{P}(G)=\{\emptyset,\{\{1,3\}\},\{\{2\}\},\{2\},\{\{\emptyset\}\},\{\{1,3\},\{2\}\},\{\{1,3\},2\},\{\{1,3\},\{\emptyset\}\},$
   $\{\{2\},2\},\{\{2\},\{\emptyset\}\},\{2,\{\emptyset\}\},\{\{1,3\},\{2\},2\},\{\{1,3\},2,\{\emptyset\}\},\{\{1,3\},\{2\},\{\emptyset\}\},$
   $\{\{2\},2,\{\emptyset\}\},G\}.$

Solution 2.7.11. *Let* A,B,C *and* D *be sets defined by :*

$$A=\{0,1,2\}, B=\{\{0,1\},2\}, C=\{0,\{0,1\},\{2\},\emptyset\}, D=\{0,1\}.$$

1) $a)0\in B$, *true* .
$b)\{0,1\}\subset B$, *false because* $\{0,1\}\in B$.
$c)\emptyset\in C$, *true.*
$d)\emptyset\subset C$, *true because* $\emptyset$ *is part of any set.*
$e)\{\emptyset\}\subset C$, *true because* $\emptyset\in C$.
2. $A\cap B=\{2\}$, $A\cap C=\{0\}, A-B=\{0,1\}, C-B=\{0,\{2\},\emptyset\},$
$A\times D=\{(0,0),(0,1),(1,0),(1,1),(2,0),(2,1)\},$
The set D has two elements so $Card(A)=2$, *then* $card(\mathscr{P}(D))=2^2=4$, *so* $\mathscr{P}(D)$ *has* 4 *elements, which are :* $\mathscr{P}(D)=\{\emptyset,\{0\},\{1\},D\}$,
The set $\mathscr{P}(D)$ *has four elements so* $Card(\mathscr{P}(D))=4$, *then* $card(\mathscr{P}(\mathscr{P}(D)))=2^4=16$, *so* $\mathscr{P}(\mathscr{P}(D))$ *has* 16 *elements, which are :*
$\mathscr{P}(\mathscr{P}(D))=\{\emptyset,\{\emptyset\},\{\{0\}\},\{\{1\}\},\{D\},\{\emptyset,\{0\}\},\{\emptyset,\{1\}\},\{\emptyset,D\},\{\{0\},\{1\},$
$\{\{0\},D\},\{D,\{1\}\}\ \{\emptyset,\{0\},\{1\}\},\{\emptyset,\{0\},D\},\{\{0\},\{1\},D\},\{\emptyset,\{1\},D\},\mathscr{P}(D),\}.$
3. Let E,F *be two sets. Prove that* $\mathscr{P}(E)=\mathscr{P}(F)\Rightarrow E=F$.
At first time we are going to prove that $E\subset F$*:*
Let $x\in E$

$$x\in E\Rightarrow\{x\}\subset E\Rightarrow\{x\}\in\mathscr{P}(E)\Rightarrow\{x\}\in\mathscr{P}(F)\Rightarrow\{x\}\subset F\Rightarrow x\in F.$$

Now let us prove that $F\subset E$*:*

$$x\in F\Rightarrow\{x\}\subset F\Rightarrow\{x\}\in\mathscr{P}(F)\Rightarrow\{x\}\in\mathscr{P}(E)\Rightarrow\{x\}\subset E\Rightarrow x\in E.$$

Then $E=F$.

Solution 2.7.12. *Let A, B and C be subsets of a suitable universal set* E,
a) Show that :

1. $(A \cap B) \cup B^c = A \cup B^c$.

a) Let us prove that $(A \cap B) \cup B^c \subset A \cup B^c$

$$\begin{aligned} x \in (A \cap B) \cup B^c &\Rightarrow (x \in A \wedge x \in B) \vee (x \notin B) \\ &\Rightarrow (x \in A \vee x \notin B) \wedge (x \in B \vee x \notin B) \\ &\Rightarrow x \in (A \cup B^c) \wedge x \in (B \cup B^c) \\ &\Rightarrow x \in (A \cup B^c) \cap E \\ &\Rightarrow x \in A \cup B^c. \end{aligned}$$

Since $E = B^c \cup B$ *and* $A \cup B^c$ *is subset of* E.

b) Let us prove that $A \cup B^c \subset (A \cap B) \cup B^c$

$$\begin{aligned} x \in A \cup B^c &\Rightarrow (x \in A \wedge x \in B) \vee (x \notin B) \\ &\Rightarrow (x \in A \vee x \notin B) \wedge (x \in B \vee x \notin B) \\ &\Rightarrow x \in (A \cup B^c) \wedge x \in (B \cup B^c) \\ &\Rightarrow x \in (A \cup B^c) \cap E \\ &\Rightarrow x \in (A \cap B) \cup B^c. \end{aligned}$$

2. $(A - B) - C = A - (B \cup C)$.

$$\begin{aligned} x \in (A - B) - C &\Leftrightarrow (x \in A \wedge x \notin B) \wedge (x \notin C) \\ &\Leftrightarrow x \in A \wedge (x \notin B \wedge x \notin C) \\ &\Leftrightarrow x \in A \wedge (x \in B^c \wedge x \in C^c) \\ &\Leftrightarrow x \in A \wedge (x \in B^c \cap C^c) \\ &\Leftrightarrow x \in A \wedge x \notin (B \cup C), \\ &\Leftrightarrow x \in A - (B \cup C). \end{aligned}$$

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

$$\begin{aligned} x \in (A \cup B) - C &\Leftrightarrow (x \in A \vee x \in B) \wedge (x \notin C) \\ &\Leftrightarrow (x \in A \wedge x \notin C) \vee (x \in B \wedge x \notin C) \\ &\Leftrightarrow x \in (A - c) \vee x \in (B - C) \\ &\Leftrightarrow x \in (A - C) \cup (B - C) \end{aligned}$$

4. $(A \cap B) - C = (A - C) \cap B = (B - C) \cap A$.

a) Let us proof that $(A \cap B) - C = (A - C) \cap B$

$$\begin{aligned} x \in (A \cap B) - C &\Leftrightarrow (x \in A \wedge x \in B) \wedge (x \notin C) \\ &\Leftrightarrow x \in A \wedge (x \notin C \wedge x \in B) \\ &\Leftrightarrow (x \in A \wedge x \in C^c) \wedge x \in B \\ &\Leftrightarrow x \in (A - C) \cap B \end{aligned}$$

b) Now we are going to proof that : $(A - C) \cap B = (B - C) \cap A$

$$\begin{aligned} x \in (A - C) \cap B &\Leftrightarrow (x \in A \wedge x \notin C) \wedge (x \notin B) \\ &\Leftrightarrow x \in A \wedge (x \in B \wedge x \notin B) \\ &\Leftrightarrow x \in A \wedge x \in (B - C) \\ &\Leftrightarrow x \in (B - C) \cap A \end{aligned}$$

Then we have : $(A \cap B) - C = (A - C) \cap B = (B - C) \cap A$.

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

$$\begin{aligned} x\in A-(B\cap C) &\Leftrightarrow x\in A\wedge x\notin(B\cap C)\\ &\Leftrightarrow x\in A\wedge x\in(B^c\cup C^c)\\ &\&\Leftrightarrow x\in A\wedge(x\in B^c\vee C^c)\\ &\Leftrightarrow (x\in A\wedge x\in B^c)\vee(x\in A\wedge x\in C^c)\\ &\Leftrightarrow x\in(A-B)\cup(A-C). \end{aligned}$$

6. $A^c-B^c=B-A.$

$$\begin{aligned} x\in A^c-B^c &\Leftrightarrow x\in A^c\wedge x\notin B^c\\ &\Leftrightarrow x\notin A\wedge x\in B\\ &\Leftrightarrow x\in B\wedge x\notin A\\ &\Leftrightarrow x\in(A-B) \end{aligned}$$

b) Simplify:

$$1.\overline{(A\cup B)}\cap\overline{(C\cup\overline{A})}=(\overline{A}\cap\overline{B})\cap(\overline{C}\cap A)=(\overline{A}\cap A)\cap(\overline{B}\cap\overline{C})=\emptyset\cap(\overline{B}\cap\overline{C})=\emptyset.$$

$$2.\overline{(A\cap B)}\cup\overline{(C\cap\overline{A})}=(\overline{A}\cup\overline{B})\cup(\overline{C}\cup A)=(\overline{A}\cup A)\cup(\overline{B}\cup\overline{C})=E\cup(\overline{B}\cup\overline{C})=E.$$

3. $(A-C)\cup(B-C)\cup(A^c-B^c)\cup C.$

$$\begin{aligned} (A-C)\cup(B-C)\cup(A^c-B^c)\cup C &= [(A\cup B)-C](A\cup B)^c\cup C\\ &= [(A\cup B)\cap C^c]\cup(A\cup B)^c\cup C\\ &= [(A\cup B)\cup(A\cup B)^c]\cap[C^c\cup(A\cup B)^c]\cup C\\ &= E\cap[C^c\cup(A\cup B)^c]\cup C\\ &= [C^c\cup(A\cup B)^c]\cup C\\ &= C^c\cup C\cup(A\cup B)^c\\ &= E\cup(A\cup B)^c=E. \end{aligned}$$

4. $(A-(B^c\cup C)\cup A^c\cup B^c\cup C.$

$$\begin{aligned} (A-(B^c\cup C)\cup A^c\cup B^c\cup C &= (A\cap(B^c\cup C)^c\cup A^c\cup B^c\cup C\\ &= (A\cap(B^c\cup C)^c)\cup A^c\cup(B^c\cup C)\\ &= (A\cap(B^c\cap C)^c)\cup((A^c\cup(B^c\cup C))^c)^c\\ &= (A\cap(B\cap C^c))\cup(A\cap(B^c\cup C)^c)^c=E. \end{aligned}$$

Solution 2.7.13. *1.* $(A\cap B)\cup C=(A\cup C)\cap(B\cup C).$

$$\begin{aligned} x\in(A\cap B)\cup C &\Leftrightarrow x\in(A\cap B)\vee x\in C\\ &\Leftrightarrow (x\in A\wedge x\in B)\vee x\in C\\ &\Leftrightarrow (x\in A\vee x\in C)\wedge(x\in B\vee x\in C)\\ &\Leftrightarrow x\in(A\cup C)\wedge x\in(B\cup C)\\ &\Leftrightarrow x\in(A\cup C)\cap(B\cup C). \end{aligned}$$

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

$$\begin{aligned} x \in (A \cup B) \cap C &\Leftrightarrow x \in (A \cup B) \wedge x \in C \\ &\Leftrightarrow (x \in A \vee x \in B) \wedge x \in C \\ &\Leftrightarrow (x \in A \wedge x \in C) \vee (x \in B \wedge x \in C) \\ &\Leftrightarrow x \in (A \cap C) \vee x \in (B \cap C) \\ &\Leftrightarrow x \in (A \cap C) \cup (B \cap C). \end{aligned}$$

3. $(A \cap B) - (A \cap C) = (A \cap B) \cap C^c$.

$$\begin{aligned} x \in (A \cap B) - (A \cap C) &\Rightarrow x \in (A \cap B) \wedge x \notin (A \cap C) \\ &\Rightarrow x \in (A \cap B) \wedge x \in (A \cap C)^c \\ &\Rightarrow (x \in A \wedge x \in B) \wedge x \in (A^c \cup C^c) \\ &\Rightarrow [(x \in A \wedge x \in B)] \wedge [(x \in A^c \vee x \in C^c)] \\ &\Rightarrow [(x \in A \wedge x \in B) \wedge x \in A^c] \vee [(x \in A \wedge x \in B) \wedge x \in C^c] \\ &\Rightarrow x \in [(A \cap B) \cap A^c] \vee x \in [(A \cap B) \cap C^c] \\ &\Rightarrow [x \in \emptyset] \vee [(A \cap B) \cap C^c] \\ &\Rightarrow x \in [(A \cap B) \cap C^c]. \end{aligned}$$

Now the other side :

$$\begin{aligned} x \in [(A \cap B) \cap C^c] &\Rightarrow x \in [(A \cap B) \cap C^c] \cup \emptyset \\ &\Rightarrow x \in [(A \cap B) \cap C^c] \cup [(A \cap A^c) \cap B] \\ &\Rightarrow [x \in (A \cap B) \wedge x \in C^c] \vee [x \in (A \cap B) \wedge x \in A^c] \\ &\Rightarrow x \in (A \cap B) \wedge x \in (C^c \cup A^c) \\ &\Rightarrow x \in (A \cap B) \wedge x \in (C \cap A)^c \\ &\Rightarrow x \in (A \cap B) \wedge x \notin (A \cap C) \\ &\Rightarrow x \in (A \cap B) - (A \cap C). \end{aligned}$$

Solution 2.7.14. *We suppose that $A \subset B$, so $x \in B^c \Rightarrow x \notin B \Rightarrow x \notin A \Rightarrow x \in A^c$. Then $B^c \subset A^c$, deduce that:*

1. We have that $\begin{cases} (A \cap B) \subset A & \Rightarrow A^c \subset (A \cap B)^c \\ (A \cap B) \subset B & \Rightarrow B^c \subset (A \cap B)^c \end{cases}$ *, thus $A^c \cup B^c \subset (A \cap B)^c$ ..(1)*

Now $x \in (A \cap B)^c \Rightarrow x \notin (A \cap B) \Rightarrow x \notin A \vee x \notin B \Rightarrow x \in A^c \vee x \in B^c \Rightarrow x \in A^c \cup B^c$.
Then, $(A \cap B)^c \subset A^c \cup B^c$...(2).
By (1) and (2) we deduce that $A^c \cup B^c = (A \cap B)$.

2. We have that $\begin{cases} A \subset (A \cup B) & \Rightarrow (A \cup B)^c \subset A^c \\ B \subset (A \cup B) & \Rightarrow (A \cup B)^c \subset B^c \end{cases}$ *, thus $(A \cup B)^c \subset A^c \cap B^c$ ..(1)*

Now $x \in A^c \cap B^c \Rightarrow x \notin A \wedge x \notin B \Rightarrow x \notin (A \cup B) \Rightarrow x \in (A \cup B)^c$.
Then, $A^c \cap B^c \subset (A \cup B)^c$...(2).
By (1) and (2) we deduce that $(A \cup B)^c = A^c \cap B^c$.

Solution 2.7.15. *1. $\mathscr{C}_E A \Delta \mathscr{C}_E B = A \Delta B$.*

$$\begin{aligned} x \in \mathscr{C}_E A \Delta \mathscr{C}_E B &\Leftrightarrow (x \in \mathscr{C}_E A - \mathscr{C}_E B) \vee (x \in \mathscr{C}_E B - \mathscr{C}_E A) \\ &\Leftrightarrow (x \in \mathscr{C}_E A \wedge x \notin \mathscr{C}_E B) \vee (x \in \mathscr{C}_E B \wedge x \notin \mathscr{C}_E A) \\ &\Leftrightarrow (x \notin A \wedge x \in B) \vee (x \notin B \wedge x \in A) \\ &\Leftrightarrow (x \in B - A) \vee (x \in A - B) \Leftrightarrow x \in (B - A) \cup (A - B) \\ &\Leftrightarrow x \in A \Delta B. \end{aligned}$$

2. $\mathscr{C}_E(A\Delta B) = \mathscr{C}_E A\Delta B = A\Delta\mathscr{C}_E B$, *using the precedent question:* $\mathscr{C}_E A\Delta\mathscr{C}_E B = A\Delta B$ *then* $\mathscr{C}_E A\Delta B = A\Delta\mathscr{C}_E B$. *Now must to proof that:*

$$\begin{aligned}
x \in (A\Delta B)^c &\Leftrightarrow x \in [(A-B)\cup(B-A)]^c \\
&\Leftrightarrow x \in (A-B)^c \cap (B-A)^c \\
&\Leftrightarrow x \in (A\cap B^c)^c \wedge x \in (B\cap A^c)^c \\
&\Leftrightarrow x \in (A^c \cup B) \wedge x \in (B^c \cup A) \\
&\Leftrightarrow x \in (A^c \cap A) \vee x \in (A^c \cap B^c) \vee x \in (B\cap B^c) \vee x \in (B\cap A) \\
&\Leftrightarrow x \in (A^c \cap B^c) \vee x \in (B\cap A) \\
&\Leftrightarrow x \in (A^c - B) \vee x \in (B - A^c) \\
&\Leftrightarrow x \in (A^c - B) \cup (B - A^c) \\
&\Leftrightarrow x \in \mathscr{C}_E A\Delta B \Leftrightarrow A\Delta\mathscr{C}_E B.
\end{aligned}$$

3. *Evaluate:* $A\Delta A^c = (A-A^c)\cup(A^c-A) = A\cup A^c = E$,
$B\Delta E = (B-E)\cup(E-B) = \emptyset\cup B^c = B^c$,
$B\Delta\emptyset = (B-\emptyset)\cup(\emptyset-B) = B\cup\emptyset = B$.

Solution 2.7.16. *Let us show that:*

1. $A\cup B = A\cap C \Leftrightarrow B\subset A\subset C$.
(⇒) *We suppose that* $A\cup B = A\cap C$*:*

$$\text{let } x\in B \Rightarrow x\in A\cup B \Rightarrow x\in A\cap C \Rightarrow x\in A\wedge x\in C \Rightarrow x\in A, \text{ then } B\subset A,$$

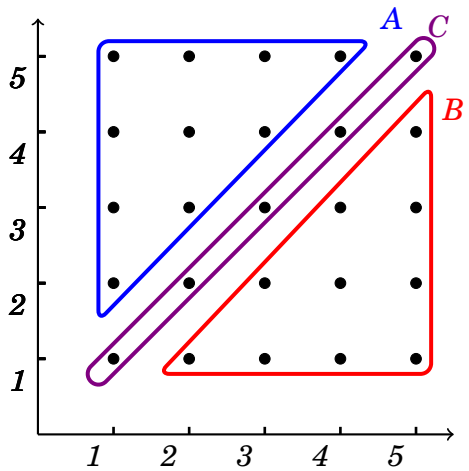
$$\text{let } x\in A \Rightarrow x\in A\cup B \Rightarrow x\in A\cap C \Rightarrow x\in A\wedge x\in C \Rightarrow x\in C, A\subset C,$$

so $B\subset A\subset C$.
(⇐) *We suppose that* $B\subset A\subset C$, *then* $A\cup B = A = A\cap C$.

2. $[(A\cup B\subset A\cup C)\wedge(A\cap B\subset A\cap C)]\Rightarrow B\subset C$.

$$\begin{aligned}
x\in B &\Rightarrow x\in(A\cup B) \\
&\Rightarrow x\in(A\cap C) \\
&\Rightarrow x\in A\vee x\in C
\end{aligned}$$

Case 1: if $x\in A$ *and* $x\in B$ *then* $x\in A\cap B\Rightarrow x\in A\cap C\Rightarrow x\in A\wedge x\in C\Rightarrow x\in C$ *so* $B\subset C$.
Case 2: if $x\in C$ *then* $B\subset C$.



Solution 2.7.17. *I.* $\{A,B,C\}$, *is a partition of* $E\times E$, *because :* $A\cap B = \emptyset, B\cap C = C\cap A$, $A\cup B\cup C = E$.

2. Let $a,b,c \in \mathbb{R}$, with $a \geq 0$. $\{]0,a[,]-\infty,b],[c,+\infty[\}$ form a partition of $\mathbb{R}$, if $b \geq 0, a \geq c$, then $]0,a[\cup]-\infty,b] \cup [c,+\infty[= \mathbb{R}$.
If $b \leq 0 \Rightarrow]0,a[\cap]-\infty,b] = \emptyset$, for $b < c \Rightarrow]-\infty,b] \cup [c,+\infty[= \emptyset$, and for $a < c$, $]0,a[\cup[c,+\infty[= \emptyset$.
Then $\{]0,a[,]-\infty,b],[c,+\infty[\}$ form a partition of $\mathbb{R}$, if $b = 0, a = c$.

Solution 2.7.18. *Let $A \times B = \{(x,y) \in R, x \in A, y \in B\}$.*

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

$$\begin{aligned}
(x,y) \in (A \times B) \cap (C \times D) &\Leftrightarrow (x,y) \in (A \times B) \wedge (x,y) \in (C \times D) \\
&\Leftrightarrow (x \in A \wedge y \in B) \wedge (x \in C \wedge y \in D) \\
&\Leftrightarrow (x \in A \wedge x \in C) \wedge (y \in B \wedge y \in D) \\
&\Leftrightarrow (x \in A \cap C) \wedge (y \in B \cap D) \\
&\Leftrightarrow (x,y) \in (A \cap C) \times (B \cap D).
\end{aligned}$$

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

$$(x,y) \in (A \times C) - (B \times C) \Rightarrow (x,y) \in (A \times C) \wedge (x,y) \notin (B \times C).$$

Note that $(x,y) \notin (B \times C)$ means that: $x \notin B \vee y \notin C$ but $y \in C$, thus $x \notin B$.

$$\begin{aligned}
(x,y) \in (A \times C) - (B \times C) &\Rightarrow (x,y) \in (A \times C) \wedge (x,y) \notin (B \times C) \\
&\Rightarrow (x \in A \wedge y \in C) \wedge (x \notin B \wedge y \in C) \\
&\Rightarrow (x \in A \wedge x \notin B) \wedge (y \in C) \\
&\Rightarrow (x \in (A - B) \wedge (y \in C) \\
&\Rightarrow (x,y) \in (A - B) \times C.
\end{aligned}$$

$$\begin{aligned}
(x,y) \in (A - B) \times C &\Rightarrow x \in (A - B) \wedge y \in C \\
&\Rightarrow (x \in A \wedge x \notin B) \wedge y \in C \\
&\Rightarrow (x \in A \wedge y \in C) \wedge (x \notin B \wedge y \in C) \\
&\Rightarrow (x,y) \in (A \times C) \wedge (x,y) \notin (B \times C) \\
&\Rightarrow (x,y) \in (A \times C) - (B \times C).
\end{aligned}$$

Chapter 3

Relations and mapping

In mathematics, we study relations between two sets of numbers, where members of one set are related to the other set by a rule. Relations are also described as mappings. When we map a set of numbers onto another set of numbers, we often express the rule for the mapping using mathematical relationships instead of words.

PARTE I : RELATIONS

3.1 RELATIONS

3.1.1 Definition

Definition 3.1.1. *A **Relation** $\mathscr{R}$ from a nonempty set E to a nonempty set F is a subset of the Cartesian product $E \times F$. Then $\mathscr{R}$ is a set of ordered pairs (x,y) where $x \in E, y \in F$. x is $\mathscr{R}$-related to y, written $x\mathscr{R}y$.*
If $E = F$ the relation $\mathscr{R}$ it called a binary relation.
The set of all first elements in a relation $\mathscr{R}$, is called the domain of the relation $\mathscr{R}$, and the set of all second elements called images, is called the range of $\mathscr{R}$.

Example 3.1.2.

1. $\forall x, y \in \mathbb{R}, x\mathscr{R}y \Leftrightarrow x = y$.
2. $\forall x, y \in \mathbb{N}, x\mathscr{R}y \Leftrightarrow x \text{ divi } y$.
3. $\forall x, y \in \mathbb{R}, x\mathscr{R}y \Leftrightarrow x \geq y$.
4. $A \subset E, B \subset F, A\mathscr{R}B \Leftrightarrow A \subset B$.

3.2 Types of Relations

Let $\mathscr{R}$ be a relation on a nonempty set E.

1. **Reflexive Relation**: We say that $\mathscr{R}$ is **reflexive** if:
$$\forall x \in E, (x\mathscr{R}x).$$
2. **Symmetric Relation:** We say that $\mathscr{R}$ is **symmetric** if:
$$\forall x \in E, \forall y \in E, (x\mathscr{R}y \Rightarrow y\mathscr{R}x).$$
3. **Anti-symmetric Relation** We say that $\mathscr{R}$ is **anti-symmetric** if:
$$\forall x \in E, \forall y \in E, (x\mathscr{R}y \wedge y\mathscr{R}x) \Rightarrow (x = y).$$

4. **Transitive Relation:** We say that $\mathscr{R}$ is **Transitive** if:

$$\forall x,y,z \in E, (x\mathscr{R}y \wedge y\mathscr{R}z) \Rightarrow (x\mathscr{R}z).$$

Example 3.2.1. *1.* $\forall x,y \in \mathbb{R}, x\mathscr{R}y \Leftrightarrow x^2 = y^2$.
a) $\mathscr{R}$ *is reflexive :* $\forall x \in \mathbb{R}, x^2 = x^2$.
b) $\mathscr{R}$ *is symmetric :* $\forall x,y \in \mathbb{R}$, $x\mathscr{R}y \Leftrightarrow x^2 = y^2 \Leftrightarrow y^2 = x^2 \Leftrightarrow y\mathscr{R}x$.
c) $\mathscr{R}$ *is not anti-symmetric :* $\exists x = 1, y = 1$ *such that* $x\mathscr{R}y \Leftrightarrow x^2 = y^2$ *and* $y\mathscr{R}x$ *but* $x \neq y$.
d) $\mathscr{R}$ *is transitive :* $\forall x,y,z \in R$ $((x\mathscr{R}y) \wedge (y\mathscr{R}z)) \Rightarrow (x\mathscr{R}z)$, $x^2 = y^2 \wedge y^2 = z^2$ *implies* $x^2 = z^2$.

2. $\forall x,y \in \mathbb{R}, xTy \Leftrightarrow x \leq y$.
T is reflexive, anti-symmetric, transitive (it is simple to verify).
But T is not symmetric : $\exists x = 1, y = 2, 1\mathscr{R}2$ *because* $1 \leq 2$ *but it doesn't imply that* $2\mathscr{R}1$.

Remark 3.2.2. *1. If a relation* $\mathscr{R}$ *isn't symmetric it doesn't mean that it is anti-symmetric:*

Let be a relation defined on a nonempty set E, the negation for symmetric is : $\exists x,y \in E$ *such that* $x\mathscr{R}y$ *and y isn't* $\mathscr{R}$*-related to y this is completely different form the definition of anti-symmetric which is* $\forall x,y \in E, x\mathscr{R}y \wedge y\mathscr{R}x \Rightarrow x = y$.

2. A relation can be neither symmetric or anti-symmetric : For instance the relation $\mathscr{R}$ *defined on* $\mathbb{N}$ *by* $\frac{n+2m}{2} \in \mathbb{N}$.
$\mathscr{R}$ *isn't symmetric because there exists* $n = 2, m = 1$ *such that* $n\mathscr{R}m \Leftrightarrow \frac{2+2}{2} \in N$, *but* $\frac{m+2n}{2} = \frac{5}{2} \notin \mathbb{N}$. *And* $\mathscr{R}$ *isn't anti-symmetric because there exists* $n = 2, m = 4$ *such that* $n\mathscr{R}m \Leftrightarrow \frac{2+8}{2} = 4 \in N$, *and* $\frac{4+4}{2} = 4 \in \mathbb{N}$ *but* $n \neq m$.

3. A relation can be symmetric and anti-symmetric at the same time, for example the relation $\mathscr{R}$ *defined by* $x\mathscr{R}y \Leftrightarrow x = y$ *is symmetric and anti-symmetric simultaneously.*

3.3 An equivalence relation

Definition 3.3.1. *Let E be a nonempty set. A relation* $\mathscr{R}$ *defined on the set E is called* ***an equivalence relation*** *on E when* $\mathscr{R}$ *is : reflexive, symmetric and transitive.*

Example 3.3.2.
1. $\forall x,y \in \mathbb{N}, x\mathscr{R}y \Leftrightarrow x = y$ *is an equivalence relation on* $\mathbb{N}$.
2. $\forall x,y \in \mathbb{R}, x\mathscr{R}y \Leftrightarrow x^2 - x = y^2 - y, \mathscr{R}$ *is an equivalence relation. Indeed :*

a $\forall x \in \mathbb{R}, x^2 - x = x^2 - x \Leftrightarrow x\mathscr{R}x \Leftrightarrow \mathscr{R}$ *is reflexive.*

b $\forall x,y \in \mathbb{R}, x\mathscr{R}y \Leftrightarrow x^2 - x = y^2 - y \Leftrightarrow y^2 - y = x^2 - x \Leftrightarrow y\mathscr{R}x, \mathscr{R}$ *is symmetric.*

c $\forall x,y,z \in \mathbb{R}, x\mathscr{R}y \Leftrightarrow x^2 - x = y^2 - y \wedge y^2 - y = z^2 - z \Leftrightarrow x^2 - x = z^2 - z \Leftrightarrow z\mathscr{R}x, \mathscr{R}$ *is transitive.*

3.3.1 Equivalence class

Let $\mathscr{R}$ be an equivalence relation defined on the nonempty set E and let $x \in F$. The set of elements in E that are related to x is called **equivalence class of** x, or class of x **modulo** $\mathscr{R}$, and denoted by $\overline{x}$ or $\dot{x}$.

$$\overline{x} = C_x = \dot{x} = \{y \in E / x\mathscr{R}y\}$$

Definition 3.3.3. *The set of equivalence classes is called the* ***quotient*** *set of E* ***modulo*** $\mathscr{R}$, *denoted by* $E_{/\mathscr{R}}$,

$$E_{/\mathscr{R}} = \{\dot{x} / x \in E\},\ E_{/\mathscr{R}} \subset \mathscr{P}(E).$$

Proposition 3.3.4. *Let $\mathscr{R}$ be an equivalence relation on the nonempty set E. Then we have :*

1. $\forall x, y \in E, \overline{x} = \overline{y} \Leftrightarrow x \mathscr{R} y$.
2. $\forall x, y \in E, \overline{x} \neq \overline{y} \Leftrightarrow \overline{x} \cap \overline{y} = \emptyset$.

Example 3.3.5. $\forall x, y \in \mathbb{R}, x \mathscr{R} y \Leftrightarrow x^2 - x = y^2 - y, \mathscr{R}$ *is an equivalence relation.*
Let us determine: $C_0, \overline{1}, \dot{2}, C_{\frac{1}{2}}$.

1. $C_0 = \{y \in E / 0 \mathscr{R} y\}, 0 \mathscr{R} y \Leftrightarrow y^2 - y = 0$, *hence* $C_0 = \{0, 1\}$.
2. $\overline{1} = \{y \in E / 1 \mathscr{R} y\}, y^2 - y = 1 - 1 = 0$, *hence* $\overline{1} = \{0, 1\}$.
3. $\dot{2} = \{y \in E / 2 \mathscr{R} y\}, y^2 - y = 2$, *hence* $\dot{2} = \{-1, 2\}$.
4. $C_{\frac{1}{2}} = \{y \in E / \frac{1}{2} \mathscr{R} y\}, y^2 - y = \frac{1}{4} - \frac{1}{2} = -\frac{1}{4}$, *hence* $C_{\frac{1}{2}} = \{\frac{1}{2}\}$.

3.3.2 The quotient set $\mathbb{Z}/n\mathbb{Z}$

On $\mathbb{Z}$ we consider **the congruence relation modulo** n, which is an equivalence relation. When a is related to b, we write

$$a \equiv b[n] \Leftrightarrow \exists k \in \mathbb{Z}, a - b = nk.$$

And we read this as "a **is congruent to** b **modulo** n".
The quotient set is denoted by $\mathbb{Z}/n\mathbb{Z}$. Then, the quotient set is given by

$$\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dot{1}, ..., (n \dot{-} 1)\}.$$

Where : $\dot{0} = \{nk, k \in \mathbb{Z}\}, \dot{1} = \{nk + 1, k \in \mathbb{Z}\}$.....$(n \dot{-} 1) = \{nk + (n - 1), k \in \mathbb{Z}\}$

Example 3.3.6.
1. $\mathbb{Z}/2\mathbb{Z} = \{\dot{0}, \dot{1}\}, \dot{0}$: *set of the even numbers,* $\dot{1}$: *set of odd numbers.*
2. $\mathbb{Z}/4\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}\}$.

3.4 Order Relation

Definition 3.4.1. *Let E be a nonempty set. A relation $\mathscr{R}$ defined on the set E is called* ***an order relation*** *on E when $\mathscr{R}$ is: reflexive, anti-symmetric and transitive.*

Example 3.4.2. *1.* $\forall A, B \in \mathscr{P}(E), A \mathscr{R} B \Leftrightarrow A \subset B$ *is an order relation, Indeed:*

- *(a)* $\forall A \in \mathscr{P}(E), A \subset A \Leftrightarrow \mathscr{R}$ *is reflexive.*
- *(b)* $\forall A, B \in \mathscr{P}(E), ((A \subset B) \wedge (B \subset A)) \Rightarrow A = B \Leftrightarrow \mathscr{R}$ *is anti-symmetric.*
- *(c)* $\forall A, B, C \in \mathscr{P}(E), ((A \subset B) \wedge (B \subset C)) \Rightarrow A \subset C \Leftrightarrow \mathscr{R}$ *is transitive.*

2. $\forall x, y \in \mathbb{R}, x \mathscr{R} y \Leftrightarrow x \leq y$, *is an order relation.*

3.4.1 Partial and total order

Definition 3.4.3 (Total Order).
Let E be a nonempty set. And $\preceq$ be an order relation defined on E, $\preceq$ is ***a total order relation*** *if and only if $x, y \in E$, $x \preceq y$ ou $y \preceq x$. That means every pair of elements is comparable.*

Definition 3.4.4 (Partial Order).
When the order is not total, we say it is partial. That means there exist an elements $(x, y) \in E$, that may be incomparable. Neither $x \preceq y$ nor $y \preceq x$.

Example 3.4.5.

- $\forall x, y \in \mathbb{R}, x \mathscr{R} y \Leftrightarrow x \leq y$, *is an order relation.*

  1. $\mathscr{R}$ *is reflexive:* $\forall x \in \mathbb{R}, x \leq x \Leftrightarrow x \mathscr{R} x$.
  2. $\mathscr{R}$ *is anti-symmetric:* $\forall x, y \in \mathbb{R}, ((x \mathscr{R} y) \wedge (y \mathscr{R} x)) \Leftrightarrow ((x \leq y) \wedge (y \leq x)) \Rightarrow x = y$.
  3. $\mathscr{R}$ *is transitive :* $\forall x, y, z \in \mathbb{R}, ((x \mathscr{R} y) \wedge (y \mathscr{R} z)) \Leftrightarrow ((x \leq y) \wedge (y \leq z)) \Leftrightarrow y \leq z \Rightarrow x \leq z \Leftrightarrow x \mathscr{R} z$.
  4. $\mathscr{R}$ *is a total order relation, indeed :* $\forall x, y \in \mathbb{R}, x \leq \vee\ y \leq x$.

- $\forall A, B \in \mathscr{P}(E), A \mathscr{R} B \Leftrightarrow A \subset B$ *is partial order relation.*
  Indeed let $E = \{1,2,3,4,5\}$, $A = \{1,2\}, B = \{3,4,5\}$, *then we have* $A \not\subset B$ *and* $B \not\subset A$.

- $\forall (x, y), (x', y') \in \mathbb{R}^2; (x, y) \preceq (x', y') \Leftrightarrow (x \leq x') \wedge (y \leq y')$ *is partial order relation, indeed :*
  $\exists (1,2), (3,0) \in \mathbb{R}^2$, $(1,2) \not\preceq (3,0)$, *and* $(3,0) \not\preceq (1,2)$.

3.4.2 Special Elements of Partially Ordered Sets

Let E be a partially ordered set which respect to $\mathscr{R}$, and let A a subset of E.

Upper and Lower Bounds

Definition 3.4.6.
1. An element $M \in E$ *is called* ***an upper bound*** *(or* ***majorant****) of* A *if :* $\forall x \in A, x \mathscr{R} M$.
2. An element $m \in E$ *is called* ***a lower bound*** *(or* ***minorant****) of* A *if :* $\forall x \in A, m \mathscr{R} x$.

Least Upper and Greatest Lower Bounds

Definition 3.4.7.
1. ***The least upper bound of*** A *is called* ***supremum*** *of* A, *denoted by* $sup(A)$.
2. ***The greatest lower bound*** *of* A *is called* ***infimum*** *of* A, *denoted by* $in(A)$.
The least upper bound and the greatest lower bound do not always exist. However, if they exist, they are unique.

Maximal and Minimal

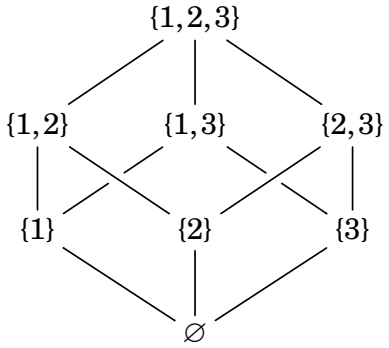
Definition 3.4.8.
1. The ***maximal*** *(****the greatest****) element of* A *is an upper bound of* A *which belongs to* A, *denoted by* $max(A)$.
2. The ***minimal****(****least****) element of* A *a lower bound of* A *which belongs to* A, *denoted by* $min(A)$.
The greatest and least elements are unique when they exist.

Example 3.4.9.

1. *Consider the usual (total) order* $\leq$ *on* $\mathbb{R}$.
   The subset $A =]a, b[$, *has many upper bounds (any real* $\geq b$.*)*
   A *has many lower bounds (any real* $\leq a$*). However, the element* a *is the greatest lower bound of* A, $inf(A)$. *And the element* b *is the least upper bound of* A, $sup(A) = b$.
   A *has neither a maximum nor minimum element, because* $a, b \notin A$. *However,* $B = [a, b]$ *has* $min(B) = a, max(B) = b$.

2. *Let* $E = \mathscr{P}(\{1,2,3\})$ *equipped with the order relation* " $\subset$ " *the maximal is* $\{1,2,3\}$, *and minimal*

is $\emptyset$



Let $A = \{\{1,2\},\{2,3\},\{1,3\},\{1\},\{2\},\{3\}\}$, *then* $sup(A) = \{1,2,3\}, inf(A) = \emptyset$, *but* $min(A), max(A)$ *doesn't exists.*

3.4.3 Solved Exercises

Exercises

Exercise 3.4.10. *1. Is the relation* $\mathscr{R}$ *defined on* $\mathbb{N}$ *by :* $n\mathscr{R}m \Leftrightarrow \frac{n+m}{2} \in \mathbb{N}$ *reflexive ? Is it anti-symmetric? Is it transitive?*

2. *Is the relation* $\mathscr{R}$ *defined on by:* $n\mathscr{R}m \Leftrightarrow \frac{n+m}{3}$ *is even, anti-symmetric?*
3. *Is the relation* $\mathscr{R}$ *defined on* $\mathbb{Z}$ *by:* $n\mathscr{R}m \Leftrightarrow n = -m$ *reflexive? Is it anti-symmetric?*
4. *Is the relation* $\mathscr{R}$ *defined on* $\mathbb{R}$ *by :* $x\mathscr{R}y \Leftrightarrow \sin^2(x) + \cos^2(y) = 1$ *reflexive? Is it symmetric? Is it anti-symmetric? Is it transitive ?*

Exercise 3.4.11. *Let* $E = \mathbb{R}$.

1. $\forall A,B \in \mathscr{P}(E), A\mathscr{R}B \Leftrightarrow A \subset B$. $\mathscr{R}$ *is it reflexive? Is it symmetric? Is it anti-symmetric? Is it transitive ?*
2. $\forall A,B \in \mathscr{P}(E), A\mathscr{R}B \Leftrightarrow A \cup B = \emptyset$. $\mathscr{R}$ *is it reflexive? Is it symmetric?*
3. $\forall A,B \in \mathscr{P}(E), A\mathscr{R}B \Leftrightarrow A \cap B \neq \emptyset$. $\mathscr{R}$ *is it reflexive? Is it symmetric?Is it anti-symmetric? Is it transitive ?*
4. $\forall A,B \in \mathscr{P}(E), A\mathscr{R}B \Leftrightarrow A \cap B = \emptyset$. $\mathscr{R}$ *is it reflexive? Is it symmetric?Is it anti-symmetric? Is it transitive ?*
5. $\forall A,B \in \mathscr{P}(E), A\mathscr{R}B \Leftrightarrow A\Delta B \neq \emptyset$. $\mathscr{R}$ *is it reflexive? Is it symmetric?Is it anti-symmetric? Is it transitive ?*

Exercise 3.4.12. *Let a relation* $\mathscr{R}$ *defined on* $\mathbb{R}$ *by :*

$$\forall x,y \in \mathbb{R},\ x\mathscr{R}y \Leftrightarrow x^3 - x = y^3 - y,$$

a) Show tha $\mathscr{R}$ *is an equivalence relation on* $\mathbb{R}$.
b) Determine the equivalent classes of 0, *and deduce the equivalent classes* 1.

Exercise 3.4.13. *Let a relation* $\mathscr{R}$ *defined on* $]1,+\infty[$ *by :*

$$x\mathscr{R}y \Leftrightarrow \frac{1}{1+x^2} \geq \frac{1}{1+y^2}$$

1. *Show that* $\mathscr{R}$ *is an order relation.*

2. *Is it a total order relation ?*

Exercise 3.4.14. *Let a relation $\mathscr{R}$ defined on $\mathbb{R}^2$ by:*

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

1. *Show that $\mathscr{R}$ is an equivalence relation.*
2. *Find the equivalence classes of $(0,0)$.*

Exercise 3.4.15. *Let a relation $\mathscr{R}$ defined on $\mathbb{R}^2$ by:* $(x_1,y_1)\mathscr{R}(x_2,y_2) \Leftrightarrow x_1^2+y_1^2=x_2^2+y_2^2$

1. *Show that $\mathscr{R}$ is an equivalence relation.*
2. *Find the equivalence classes of (a,b).*

Exercise 3.4.16. *Let a relation $\mathscr{R}$ defined on $\mathbb{R}$ by: $x\mathscr{R}y \Leftrightarrow xe^y=ye^x$.*
a) Show that $\mathscr{R}$ is an equivalence relation.
b) For $x\in\mathbb{R}$, determine the cardinal of equivalence classes of x.

Exercise 3.4.17. *Let a relation $\prec$ defined on $\mathbb{R}^2$ by:* $(x,y)\prec(x',y') \Leftrightarrow (x-x'\geq 0 \text{ et } y=y')$

1. *Show that $\prec$ is an order relation.*
2. *Is it a total order relation?*

Exercise 3.4.18. *Let a relation T defined on $\mathbb{R}^2$ by :*

$$(x,y)T(x',y') \Leftrightarrow |x-x'|\leq y'-y$$

1. *Show that T is an order relation.*
2. *Is it a total order relation ?*
3. *Let $(a,b)\in\mathbb{R}^2$, give a representation of the set $\{x,y)\in\mathbb{R}^2/(x,y)T(a,b)\}$.*

Exercise 3.4.19. *Let E be a set and $A,B\in\mathscr{P}(E)$, we define the relation $\mathscr{R}$ by :*
$A\mathscr{R}B \Leftrightarrow \exists X\in\mathscr{P}(E), X\cap A=X\cap B$

1. *Prove that $\mathscr{R}$ is an equivalence relation on E.*
2. *Determine the equivalence classes : $\dot{\emptyset},\dot{E}$.*

Exercise 3.4.20. *Let $\mathscr{R}$ a relation defined on $\mathbb{N}^*$, by: $n\mathscr{R}m \Leftrightarrow n$ divides m*

1. *Show that $\mathscr{R}$ is an order relation.*
2. *Is it a total order relation?*
3. *Let $A=\{1,2,3,4,6,12\}$. Determine the upper and lower bounds . Is there a maximum and minimum element ?*

Exercise 3.4.21. *Let $\mathscr{R}$ a relation defined on $\mathbb{N}^*$ defined by : $n\mathscr{R} \Leftrightarrow \exists k\in\mathbb{N}: n=m^k$*

1. *Show that $\mathscr{R}$ is an order relation.*
2. *Is it a total order relation?*
3. *Determine the least upper and greatest lower bounds of $A=\{2,4,8\}$, min(A), max(A) exists ?*

Solutions

Solution 3.4.22. *1. A relation $\mathscr{R}$ defined on $\mathbb{N}$ by : $n\mathscr{R}m \Leftrightarrow \dfrac{n+m}{2} \in \mathbb{N}$.*

a) $\forall n \in \mathbb{N}, \dfrac{n+n}{2} = n \in \mathbb{N}$, thus $\forall n \in \mathbb{N}, n\mathscr{R}n$, the $\mathscr{R}$ is reflexive.

b) $\mathscr{R}$ isn't anti-symmetric :$\exists n = 2, m = 4 \in \mathbb{N}$ such that $2\mathscr{R}4$ because $\frac{2+4}{2} = 3 \in \mathbb{N}$ and $4\mathscr{R}2$ because $\frac{4+2}{2} = 3 \in \mathbb{N}$ but $2 \neq 4$.

c) $\mathscr{R}$ is it transitive if and only if: $\forall n, m, l \in \mathbb{N}, n\mathscr{R}m \wedge m\mathscr{R}l \Rightarrow n\mathscr{R}l$ indeed:

$$\begin{cases} n\mathscr{R}m & \Leftrightarrow \dfrac{n+m}{2} \in \mathbb{N} \\ \wedge & \\ m\mathscr{R}l & \Leftrightarrow \dfrac{m+l}{2} \in \mathbb{N} \end{cases} \Rightarrow \frac{n+m}{2} + \frac{m+l}{2} \in \mathbb{N} \Rightarrow \frac{n+l}{2} + 2m \in \mathbb{N}$$

$\Rightarrow \dfrac{n+l}{2} \in \mathbb{N} \Leftrightarrow m\mathscr{R}l$, *because* $m \in \mathbb{N}$.

2. *Is the relation $\mathscr{R}$ defined on by: $n\mathscr{R}m \Leftrightarrow \dfrac{n+m}{3}$ is even.*

a) $\mathscr{R}$ isn't reflexive : $\exists n = 2$, and $\dfrac{2+2}{3}$ is not even.

b) $\mathscr{R}$ isn't anti-symmetric :$\exists n = 12, m = 6 \in \mathbb{N}$ such that $12\mathscr{R}6$ because $\frac{12+6}{2} = 6 = 2.3$ is even and $6\mathscr{R}12$ because $\frac{6+12}{3} = 6 = 2.3$ is even but $n = 12 \neq 6 = m$.

3. *$\mathscr{R}$ defined on $\mathbb{Z}$ by: $n\mathscr{R}m \Leftrightarrow n = -m$.*
a) $\mathscr{R}$ isn't reflexive : $\exists n = 1$, such that $1 \neq -1$. We have ($\forall n \in \mathbb{Z}, n \neq -n$.)
b) $\mathscr{R}$ isn't anti-symmetric : $\exists n = 1, m = -1/n\mathscr{R}m \Leftrightarrow n = -m \Leftrightarrow m = -n \Leftrightarrow m\mathscr{R}n$ but $n \neq m$.

4. *The relation $\mathscr{R}$ defined on $\mathbb{R}$ by: $x\mathscr{R}y \Leftrightarrow \sin^2(x) + \cos^2(y) = 1$.*
a) $\mathscr{R}$ reflexive if and only if: $\forall x \in \mathbb{R}, x\mathscr{R}x$ that is true because $\forall x \in \mathbb{R}, \cos^2(x) + \sin^2(x) = 1$. So $\mathscr{R}$ is reflexive
b) $\mathscr{R}$ is symmetric if and only if: $\forall x, y \in \mathbb{R}, x\mathscr{R}y \Rightarrow y\mathscr{R}x$.
As,

$$\forall x, y \in \mathbb{R}, \sin^2(x) + \cos^2(x) = 1 \wedge \sin^2(y) + \cos^2(y) = 1.$$

Then

$$\sin^2(x) + \cos^2(x) + \sin^2(y) + \cos^2(y) = 2$$

and $x\mathscr{R}y \Leftrightarrow \cos^2(x) + \sin^2(y) = 1$, so $\sin^2(y) + \cos^2(x) + 1 = 2 \Leftrightarrow \sin^2(y) + \cos^2(x) = 1 \Leftrightarrow y\mathscr{R}x$. i.e $\mathscr{R}$ is symmetric.
c) $\mathscr{R}$ is anti-symmetric isn't symmetric: $\exists x = 0, y = \pi \in \mathbb{R}, x\mathscr{R}y$ because $\sin^2(0) + \cos^2(0) = 1$ and $y\mathscr{R}x$ because $\sin^2(\pi) + \cos^2(\pi) = 1$ but $x = 0 \neq \pi = y$.

c) $\mathscr{R}$ is it transitive if and only if: $\forall x, y, z \in \mathbb{R}, x\mathscr{R}y \wedge y\mathscr{R}z \Rightarrow x\mathscr{R}z$. Indeed :

$$\begin{cases} x\mathscr{R}y & \Leftrightarrow \sin^2(x) + \cos^2(y) = 1 \\ \wedge & \\ y\mathscr{R}z & \Leftrightarrow \sin^2(y) + \cos^2(z) = 1 \end{cases}$$

$$\Rightarrow \sin^2(x) + \cos^2(y) + \sin^2(y) + \cos^2(z) = 2 \Rightarrow \sin^2(x) + \cos^2(z) = 1.$$

Then $x\mathscr{R}z$, thus $\mathscr{R}$ is transitive.

Solution 3.4.23. *1. $\forall A, B \in \mathscr{P}(E), A\mathscr{R}B \Leftrightarrow A \subset B$.*
a) $\mathscr{R}$ is reflexive if and only if: $\forall A \in \mathscr{P}(E), A\mathscr{R}A$ it's simple because $A \subset A$. Then $\mathscr{R}$ is reflexive.
b) $\mathscr{R}$ isn't symmetric indeed $\exists A = \emptyset, B = E, A\mathscr{R}B$ because $\emptyset \subset E$, but $A\not\mathscr{R}B$ because $E \not\subset \emptyset$.
c)$\mathscr{R}$ is anti-symmetric if and only if : $\forall A, B \in \mathscr{P}(E), A\mathscr{R}B \wedge B\mathscr{R}A \Rightarrow A = B$ it's simple because if $A \subset B \wedge B \subset A$ then $A = B$. So $\mathscr{R}$ is anti-symmetric.

d)$\mathscr{R}$ is transitive if and only if: $\forall A,B,C \in \mathscr{P}(E), A\mathscr{R}B \wedge B\mathscr{R}C \Rightarrow A\mathscr{R}C$ it's simple because $A \subset B \wedge B \subset C \Rightarrow A \subset C$. Then $\mathscr{R}$ is transitive.

2. $\forall A,B \in \mathscr{P}(E), A\mathscr{R}B \Leftrightarrow A \cup B = \emptyset$.
   a) $\mathscr{R}$ isn't reflexive because $\exists A = E \in \mathscr{P}(E)$ such that $A \cup A = A \neq \emptyset$, so $A\not\mathscr{R}A$.
   b) $\mathscr{R}$ is symmetric because $\cup$ is commutative indeed : $\forall A,B \in \mathscr{P}(E), A\mathscr{R}B \Leftrightarrow A \cup B = \emptyset \Rightarrow B \cup A = \emptyset \Leftrightarrow B\mathscr{R}A$. Then $\mathscr{R}$ is symmetric.

3. $\forall A,B \in \mathscr{P}(E), A\mathscr{R}B \Leftrightarrow A \cap B \neq \emptyset$.
   a) $\mathscr{R}$ isn't reflexive because $\exists A = \emptyset \in \mathscr{P}(E), A \cap A = \emptyset$.

   b) $\mathscr{R}$ is symmetric because $\forall A,B \in \mathscr{P}(E), A\mathscr{R}B \Leftrightarrow A \cap B \neq \emptyset \Rightarrow B \cap A \neq \emptyset \Leftrightarrow B\mathscr{R}A$.

   c) $\mathscr{R}$ isn't anti-symmetric because $\exists A = [0,1], B = [1,2] \in \mathscr{P}(E), A\mathscr{R}B \Leftrightarrow A \cap B = \{1\} \wedge B\mathscr{R}A \Leftrightarrow B \cap A = \{1\}$ but $A \neq B$.

   d) $\mathscr{R}$ isn't transitive :$\exists A = [0,1], B = [1,2], C = [2,3] \in \mathscr{P}(E)$, $A\mathscr{R}B \wedge B\mathscr{R}C \Rightarrow A\mathscr{R}C$, $A \cap B = \{1\} \neq \emptyset$ and $B \cap C = \{2\} \neq \emptyset$, but $A \cap C = \emptyset$, so $A\not\mathscr{R}C$.

4. $\forall A,B \in \mathscr{P}(E), A\mathscr{R}B \Leftrightarrow A \cap B = \emptyset$.
   a) $\mathscr{R}$ isn't reflexive because $\forall A \in \mathscr{P}(E)$, if$A \neq \emptyset$, then $A\not\mathscr{R}A$, it's simple indeed $A \cap A \neq \emptyset$.
   b) $\mathscr{R}$ is symmetric it's simple because $\forall A,B \in \mathscr{P}(E), A\mathscr{R}B \Leftrightarrow A \cap B = \emptyset \Rightarrow B \cap A = \emptyset \Leftrightarrow B\mathscr{R}A$.
   c) $\mathscr{R}$ isn't anti-symmetric because $\exists A = [0,1], B = [2,3] \in \mathscr{P}(E), A\mathscr{R}B \wedge B\mathscr{R}A$ but $A \neq B$
   d) $\mathscr{R}$ isn't transitive $\exists A = [0,1], B = [2,3], C = [-1,1] \in \mathscr{P}(E)$,

$$\begin{cases} A\mathscr{R}B & \Leftrightarrow A \cap B = \emptyset \\ \wedge & \\ B\mathscr{R}C & \Leftrightarrow B \cap C = \emptyset \end{cases}$$

   but $A \cap C = [0,1] \neq \emptyset$.

5. $\forall A,B \in \mathscr{P}(E), A\mathscr{R}B \Leftrightarrow A\Delta B \neq \emptyset$.
   a) $\mathscr{R}$ isn't reflexive $\forall A, A\not\mathscr{R}A = \emptyset$.
   b) $\mathscr{R}$ is symmetric $A\mathscr{R}B \Leftrightarrow (A \cup B) - (A \cap B) \neq \emptyset \Rightarrow (B \cup A) - (B \cap A) \neq \emptyset \Leftrightarrow B\mathscr{R}A$.
   c) $\mathscr{R}$ isn't anti-symmetric $\exists A = E, B = \emptyset, A\mathscr{R}B \wedge B\mathscr{R}A$, but $A \neq B$.
   d) $\mathscr{R}$ isn't transitive if $A = C$, indeed $A\mathscr{R}B \wedge B\mathscr{R}A$ but $A\not\mathscr{R}C$ because $A\Delta C = \emptyset$.

Solution 3.4.24. *1.$\forall x,y \in \mathbb{R}, x\mathscr{R}y \Leftrightarrow x^3 - x = y^3 - y, \mathscr{R}$ is an equivalence relation indeed :*

1. *$\forall x \in \mathbb{R}, x^3 - x = x^3 - x \Leftrightarrow x\mathscr{R}x \Leftrightarrow \mathscr{R}$ is reflexive.*
2. *$\forall x,y \in \mathbb{R}, x\mathscr{R}y \Leftrightarrow x^3 - x = y^3 - y \Leftrightarrow y^3 - y = x^3 - x \Leftrightarrow y\mathscr{R}x, \mathscr{R}$ is symmetric.*
3. *$\forall x,y,z \in \mathbb{R}, x\mathscr{R}y \Leftrightarrow x^3 - x = y^3 - y \wedge y^3 - y = z^3 - z \Leftrightarrow x^3 - x = z^3 - z \Leftrightarrow z\mathscr{R}x, \mathscr{R}$ is transitive.*

2. $C_0 = \{y \in E / \ 0\mathscr{R}y\}, 0\mathscr{R}y \Leftrightarrow y^3 - y = 0$, so $C_0 = \{0,1,-1\}$. We deduce $\overline{1} = \{0,1,-1\}$.

Solution 3.4.25. *a) $\mathscr{R}$ is reflexive* $\Leftrightarrow \forall x \in]1,+\infty[, x\mathscr{R}x, \quad x\mathscr{R}x \Leftrightarrow \dfrac{1}{1+x^2} \geq \dfrac{1}{1+x^2}$. *So $\mathscr{R}$ is reflexive*
b) $\mathscr{R}$ is anti-symmetric $\Leftrightarrow \forall x, y \in]1,+\infty[, x\mathscr{R}y \wedge y\mathscr{R}x \Rightarrow x = y$

$$x\mathscr{R}y \quad \wedge \quad y\mathscr{R}x \Rightarrow \begin{cases} \dfrac{1}{1+x^2} \geq \dfrac{1}{1+y^2} \\ \wedge \\ \dfrac{1}{1+y^2} \geq \dfrac{1}{1+x^2} \end{cases} \Rightarrow \frac{1}{1+y^2} = \frac{1}{1+x^2}$$

$$\Rightarrow |x| = |y| \Rightarrow x = y, \text{ because } x, y \in]1,+\infty[.$$

So $\mathscr{R}$ is anti-symmetric.
c) $\mathscr{R}$ is transitive $\Leftrightarrow \forall x, y, z \in]1,+\infty[, \; x\mathscr{R}y \wedge y\mathscr{R}z \Rightarrow x\mathscr{R}z$

$$x\mathscr{R}y \quad \wedge \quad y\mathscr{R}z \Rightarrow \begin{cases} \dfrac{1}{1+x^2} \geq \dfrac{1}{1+y^2} \\ \wedge \\ \dfrac{1}{1+y^2} \geq \dfrac{1}{1+z^2} \end{cases} \Rightarrow \frac{1}{1+x^2} \geq \frac{1}{1+z^2} \Leftrightarrow x\mathscr{R}z.$$

So $\mathscr{R}$ is transitive, then $\mathscr{R}$ is an order relation .
$\leq$ is a total order relation, then $\mathscr{R}$ is a total order relation $\Leftrightarrow x\mathscr{R}y \vee y\mathscr{R}x$, *Indeed:*
If $x \leq y \Rightarrow 1+x^2 \leq 1+y^2 \Rightarrow \dfrac{1}{1+x^2} \geq \dfrac{1}{1+y^2} \Rightarrow \dfrac{x}{1+x^2} \geq \dfrac{y}{1+y^2} \Rightarrow y\mathscr{R}x.$
Otherwise $x \geq y \Rightarrow x\mathscr{R}y$.

Solution 3.4.26. *$\mathscr{R}$ is an equivalence relation if and only if it is reflexive, symmetric and transitive.*

1. *a) $\mathscr{R}$ is reflexive if and only if:* $\forall (x,y) \in \mathbb{R}^2, (x,y)\mathscr{R}(x,y)$

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

   So $\mathscr{R}$ is reflexive.

2. *b) $\mathscr{R}$ is symmetric if and only if:*

   $$\forall (x,y),(x',y') \in \mathbb{R}^2, (x,y)\mathscr{R}(x',y') \Rightarrow (x',y')\mathscr{R}(x,y)$$

   $$\begin{aligned} (x,y)\mathscr{R}(x',y') &\Rightarrow x+y = x'+y' \\ &\Rightarrow x'+y' = x+y \\ &\Rightarrow (x',y')\mathscr{R}(x,y) \end{aligned}$$

   then $\mathscr{R}$ is symmetric.

3. *$\mathscr{R}$ is transitive if and only if:*
   $\forall (x,y),(x',y'),(x'',y'') \in \mathbb{R}^2, (x,y)\mathscr{R}(x',y') \wedge (x',y')\mathscr{R}(x'',y'') \Leftrightarrow (x,y)\mathscr{R}(x'',y'')$

   $$\begin{aligned} (x,y)\mathscr{R}(x',y') \wedge (x',y')\mathscr{R}(x'',y'') &\Rightarrow \begin{cases} x+y = x'+y' \\ \wedge \\ x'+y' = x''+y'' \end{cases} \\ &\Rightarrow x+y = x''+y'' \\ &\Leftrightarrow (x,y)\mathscr{R}(x'',y''). \end{aligned}$$

   Then $\mathscr{R}$ is transitive, so $\mathscr{R}$ is an equivalence relation.
   Let us determine the equivalent classes of $(0,0)$.

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

Solution 3.4.27. *$\mathscr{R}$ is an equivalence relation if and only if it is reflexive, symmetric and transitive.*

1. *a) $\mathscr{R}$ is reflexive if and only if:* $\forall (x,y) \in \mathbb{R}^2, (x,y)\mathscr{R}(x,y)$

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

So $\mathscr{R}$ is reflexive.
b) $\mathscr{R}$ is symmetric is and only if: $\forall (x,y),(x_1,y_1) \in \mathbb{R}^2, (x,y)\mathscr{R}(x_1,y_1) \Rightarrow (x_1,y_1)\mathscr{R}(x,y)$

$$\begin{aligned} (x,y)\mathscr{R}(x_1,y_1) &\Rightarrow x^2+y^2 = x_1^2+y_1^2 \\ &\Rightarrow x_1^2+y_1^2 = x^2+y^2 \\ &\Leftrightarrow (x_1,y_1)\mathscr{R}(x,y) \end{aligned}$$

So $\mathscr{R}$ is symmetric.
c) $\mathscr{R}$ is transitive if and only if: $\forall (x,y),(x_1,y_1),(x_2,y_2) \in \mathbb{R}^2$,
$(x,y)\mathscr{R}(x_1,y_1) \wedge (x_1,y_1)\mathscr{R}(x_2,y_2) \Rightarrow (x,y)\mathscr{R}(x_2,y_2)$

$$\begin{aligned} (x,y)\mathscr{R}(x_1,y_1) \quad &\wedge \quad (x_1,y_1)\mathscr{R}(x_2,y_2) \\ &\Rightarrow \begin{cases} x^2+y^2 = x_1^2+y_1^2 \\ \wedge \\ x_1^2+y_1^2 = x_2^2+y_2^2 \end{cases} \\ &\Rightarrow x_1^2+y_1^2 = x_2^2+y_2^2 \\ &\Leftrightarrow (x,y)\mathscr{R}(x_2,y_2) \end{aligned}$$

So $\mathscr{R}$ is transitive, then $\mathscr{R}$ is an equivalence relation.

2. *Determine equivalence of* (a,b).

$$\begin{aligned} C((a,b)) &= \{(x,y) \in \mathbb{R}^2 / (x,y)\mathscr{R}(a,b)\} \\ &= \{(x,y) \in \mathbb{R}^2 / x^2+y^2 = a^2+b^2\} \end{aligned}$$

If $a^2+b^2 = 0 \Rightarrow a = b = 0$ then $C(a,b) = \{(0,0)\}$ is the point $O = (0,0)$ the origin.
If else $a^2+b^2 \neq 0, C(a,b) = \{(x,y) \in \mathbb{R}^2 / x^2+y^2 = a^2+b^2\}$ is a circle with center $(0,0)$ and radius $\sqrt{(a^2+b^2)}$.

Solution 3.4.28. *On $\mathbb{R}$ is an equivalence relation $\mathscr{R}$ by: $x\mathscr{R}y \Leftrightarrow xe^y = ye^x$.*
a) $\mathscr{R}$ if and only if it is reflexive, symmetric and transitive.
1. $\mathscr{R}$ is reflexive if and only if: $\forall x \in \mathbb{R}, x\mathscr{R}x$
$x\mathscr{R}x \Leftrightarrow xe^x = xe^x$. *So $\mathscr{R}$ is reflexive.*
2. $\mathscr{R}$ is symmetric if and only if: $\forall x,y \in \mathbb{R}, x\mathscr{R}y \Rightarrow y\mathscr{R}x$

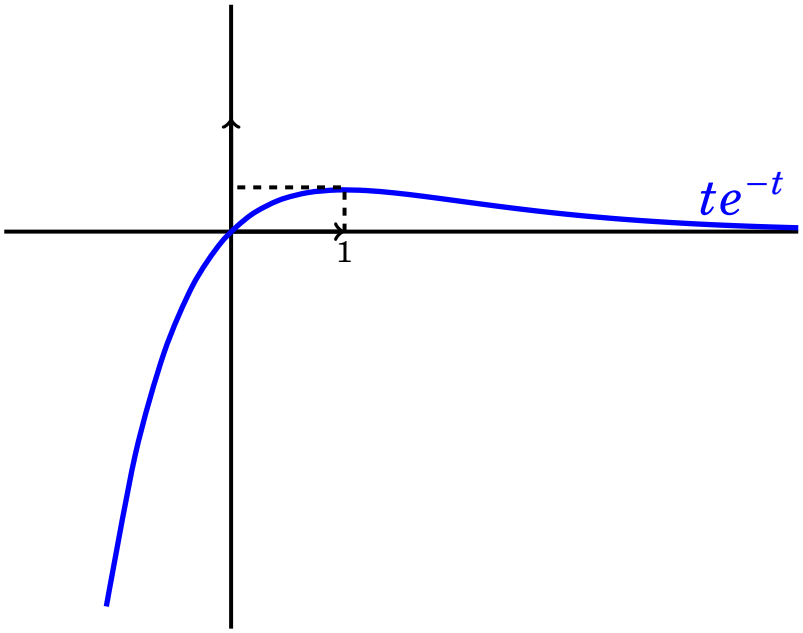
$$\begin{aligned} x\mathscr{R}y \quad &\Rightarrow xe^y = ye^x \\ &\Rightarrow \quad ye^x = xe^y \\ &\Leftrightarrow \quad y\mathscr{R}x \end{aligned}$$

So $\mathscr{R}$ is symmetric.
3. $\mathscr{R}$ is transitive if and only if: $\forall x,y,z \in \mathbb{R}, x\mathscr{R}y \wedge y\mathscr{R}z \Rightarrow x\mathscr{R}z$

$$\begin{cases} x\mathscr{R}y \\ \wedge \\ y\mathscr{R}x \end{cases} \Rightarrow \begin{cases} xe^y = ye^x \\ \wedge \\ ye^z = ze^y \end{cases} \Rightarrow \begin{cases} xe^{-x} = ye^{-y} \\ \wedge \\ ye^{-y} = ze^{-z} \end{cases} \Rightarrow xe^z = ze^x \Leftrightarrow x\mathscr{R}z.$$

SO $\mathscr{R}$ is transitive, so $\mathscr{R}$ is an equivalence relation.
b) For $x \in \mathbb{R}$, determiner le cardinal de an equivalence classes of x with respect relation $\mathscr{R}$:
$C_x = \{y \in \mathbb{R} / x\mathscr{R}y\} = \{y \in \mathbb{R} / ye^x = xe^y\}$. *So we get:* $ye^{-y} = xe^{-x}$.

Let the function $f:\mathbb{R}\to\mathbb{R}$ be defined by $f(t)=te^{-t}\Rightarrow f'(t)=(1-t)e^{-t}$. f strictly increasing function on $]-\infty,1]$ and strictly decreasing function on $[1,+\infty[$.



Following the graph we deduce that:
for $x\in]0,1[\cup]1,+\infty[$ then $f\in]0,e^{-1}[$ and f has two antecedents, $Card(C_x)=2$.
For $x\in]-\infty,0[\cup\{1\}$ then $f\in]-\infty,0]\cup\{e^{-1}\}$ and f has one antecedent, $Card(C_x)=1$.

Solution 3.4.29. *a) $\prec$ is reflexive if and only if: $\forall(x,y)\in\mathbb{R}^2,(x,y)\prec(x,y)$*
$(x,y)\prec(x,y)\Leftrightarrow x-x\geq 0\wedge y=y$. *Then $\prec$ is reflexive.*
b) $\prec$ is anti-symmetric if and only if: $\forall(x,y),(x',y')\in\mathbb{R}^2,((x,y)\prec(x',y'))\wedge((x',y')\prec(x,y))\Rightarrow(x,y)=(x',y')$

$$\begin{cases}(x,y)\prec(x',y')\\ \wedge\\ (x',y')\prec(x,y)\end{cases}\Rightarrow\begin{cases}x-x'\geq 0\wedge y'=y\\ \wedge\\ x'-x\geq 0\wedge y=y'\end{cases}$$
$$\Rightarrow\quad x=x',y=y'.$$

So $(x,y)=(x',y')$, then $\prec$ is anti-symmetric.
c) $\prec$ is transitive if and only if: $\forall(x,y),(x',y'),(x'',y'')\in\mathbb{R}^2$,
$((x,y)\prec(x',y'))\wedge((x',y')\prec(x'',y''))\Leftrightarrow(x,y)\prec(x'',y'')$

$$\begin{cases}(x,y)\prec(x',y')\\ \wedge\\ (x',y')\prec(x'',y'')\end{cases}\Rightarrow\begin{cases}x-x'\geq 0\wedge y'=y\\ \wedge\\ x'-x''\geq 0\wedge y''=y'\end{cases}$$
$$\Rightarrow\quad x-x''\geq 0\wedge y''=y$$
$$\Leftrightarrow\quad (x,y)\prec(x'',y'')$$

So $\prec$ is transitive, then $\prec$ is an order relation.
the order isn't a total order because $\exists(x,y)=(2,5)$ and $(x',y')=(4,3)$ such that $(x,y)\not\prec(x',y')$, because $2-4\geq 0\wedge 3=5$ it is false and $(x',y')\not\prec(x,y)$ because $4-2\geq 0\wedge 5=3$ is false too.

Solution 3.4.30. *On $\mathbb{R}^2$ we define a relation T by*

$$(x,y)T(x',y')\Leftrightarrow|x-x'|\leq y'-y$$

1. T is an order relation if and only if T is reflexive, anti-symmetric and transitive.
a) $\mathscr{R}$ is reflexive if and only if: $\forall(x,y)\in\mathbb{R}^2,(x,y)\mathscr{R}(x,y)$
$(x,y)\mathscr{R}(x,y)\Leftrightarrow|x-x|\leq y-y\Rightarrow 0\leq 0$.
So T is reflexive.

b) T is anti-symmetric if and only if:
$\forall (x,y),(x',y') \in \mathbb{R}^2, ((x,y)T(x',y')) \wedge ((x',y')T(x,y)) \Rightarrow (x,y) = (x',y')$

$$\begin{aligned}
(x,y)T(x',y') \wedge (x',y')T(x,y) &\Rightarrow \begin{cases} |x-x'| \leq y'-y \\ \wedge \\ |x'-x| \leq y-y' \end{cases} \\
&\Rightarrow 2|x-x'| \leq 0 \\
&\Rightarrow |x-x'| = 0 \\
&\Rightarrow x = x' \\
&\Rightarrow y'-y \geq 0 \wedge y-y' \geq 0 \\
&\Rightarrow y'-y \geq 0 \wedge y'-y \leq 0 \\
&\Rightarrow y'-y = 0 \Rightarrow y = y'.
\end{aligned}$$

So $(x,y) = (x',y')$, the T is anti-symmetric.
c) T is transitive if and only if:

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

$$\begin{aligned}
(x,y)T(x',y') \wedge (x',y')T(x'',y'') &\Rightarrow \begin{cases} |x-x'| \leq y'-y \\ \wedge \\ |x'-x''| \leq y''-y' \end{cases} \\
&\Rightarrow \begin{cases} -y'+y \leq x-x' \leq y'-y \\ \wedge \\ -y''+y' \leq x'-x'' \leq y''-y' \end{cases} \\
&\Rightarrow -y''+y \leq x'-x'' \leq y''-y \\
&\Rightarrow |x-x''| \leq y''-y \\
&\Leftrightarrow (x,y)T(x'',y'')
\end{aligned}$$

So T is transitive, then is an order relation.
2. the order isn't total order, indeed : $\exists (x,y) = (2,3)$ and $(x',y') = (4,3)$ such that $(x,y) \not T (x',y')$, because $|2-4| \leq 0$ it is false and $(x',y') \not T (x,y)$ because $|4-2| \leq 0$ it is false too.
3. Let $(a,b) \in \mathbb{R}^2$, let us determine the following set $\{(x,y) \in \mathbb{R}^2 / (x,y)T(a,b)\}$.

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

We get:
D_{p_1} : is a closed half-plane of equation $(x-y-a+b) \geq 0$.
D_{p_2} : is an open half-plane of equation $(x+y-a-b) < 0$.
D_{p_3} : is an open half-plane of equation $(x-y-a+b) < 0$.
D_{p_4} : a closed half-plane of equation $(x+y-a-b) \geq 0$.
So

$$(a,b) = \{(x,y) \in \mathbb{R}^2 / (x,y)T(a,b)\} = (D_{p_1} \cap D_{p_2}) \cup (D_{p_3} \cap D_{p_4})$$

Solution 3.4.31. *Let E be a set and $A,B \in \mathcal{P}(E)$, we define the relation $\mathcal{R}$ by :*
$A \mathcal{R} B \Leftrightarrow \exists X \in \mathcal{P}(E), X \cap A = X \cap B$

1. *Prove that $\mathscr{R}$ is an equivalence relation on E $\mathscr{R}$ if and only if it is reflexive, symmetric and transitive.*
   a) $\mathscr{R}$ is reflexive if and only if: $\forall A \in \mathscr{P}(E), A\mathscr{R}A$
   $A\mathscr{R}A \Leftrightarrow \exists X = E \in \mathscr{P}(E), X \cap A = X \cap A$. *So $\mathscr{R}$ is reflexive.*
   b) $\mathscr{R}$ is symmetric if and only if: $\forall A, B \in \mathscr{P}(E), A\mathscr{R}B \Rightarrow B\mathscr{R}A$
   $A\mathscr{R}B \Rightarrow \exists X \in \mathscr{P}(E), X \cap A = X \cap B \Rightarrow \exists X \in \mathscr{P}(E), X \cap B = X \cap A \Rightarrow B\mathscr{R}A$ *So $\mathscr{R}$ is symmetric.*
   c) $\mathscr{R}$ is transitive if and only if $\forall A, B, C \in \mathscr{P}(E), A\mathscr{R}B \wedge B\mathscr{R}C \Rightarrow A\mathscr{R}C$
   $$A\mathscr{R}B \wedge B\mathscr{R}C \Rightarrow \begin{cases} \exists X \in \mathscr{P}(E),\ X \cap A = X \cap B \\ \wedge \\ \exists X' \in \mathscr{P}(E),\ X' \cap B = X' \cap C \end{cases}$$
   $\Rightarrow (X' \cap X) \cap A = X' \cap (X \cap A) = X' \cap (X \cap B) = X \cap (X' \cap B) = X \cap (X' \cap C) = (X \cap X') \cap C$
   $\exists X'' = X \cap X' / X'' \cap A = X'' \cap C \Leftrightarrow A\mathscr{R}C$. *So $\mathscr{R}$ is transitive, thus $\mathscr{R}$ is an equivalence relation.*

2. *Determine the equivalence classes : $\dot{\phi}, \dot{E}$:*
   $(i)\dot{\phi} = \{Y \in \mathscr{P}(E) / Y\mathscr{R}\phi\}$, *so* $Y\mathscr{R}\phi \Leftrightarrow \exists X \in \mathscr{P}(E),\ X \cap \phi = X \cap Y \Rightarrow \phi = X \cap Y \Rightarrow Y \subset X^c$ *then* $\dot{\phi} = \{Y \in \mathscr{P}(E) / Y \subset X^c\}$.
   $(ii)\dot{E} = \{Y \in \mathscr{P}(E) / Y\mathscr{R}E\}$, *so* $Y\mathscr{R}E \Leftrightarrow \exists X \in \mathscr{P}(E),\ X \cap Y = X \cap E \Rightarrow X \cap Y = X \Rightarrow X \subset Y$ *then* $\dot{E} = \{Y \in \mathscr{P}(E) / X \subset Y\}$.

Solution 3.4.32. *On $\mathbb{N}^*$, we define a relation $\mathscr{R}$ by : $n\mathscr{R}m \Leftrightarrow n$ divides m.*
$\mathscr{R}$ is an order relation if and only if $\mathscr{R}$ is reflexive, anti-symmetric and transitive.

1. *$\mathscr{R}$ is reflexive if and only if:* $\forall n \in \mathbb{N}^*, n\mathscr{R}n$
   $n\mathscr{R}n \Leftrightarrow n$ *divides* n, *because* $n = 1 \times n$. *So $\mathscr{R}$ is reflexive.*
   2. *$\mathscr{R}$ is anti-symmetric if and only if :* $\forall n, m \in \mathbb{N}^*, n\mathscr{R}m \wedge m\mathscr{R}n \Rightarrow n = m$
   $$n\mathscr{R}m \Leftrightarrow \exists k \in \mathbb{N}^* m = kn$$
   $$m\mathscr{R}n \Leftrightarrow \exists k' \in \mathbb{N}^* n = k'm$$
   $$\Rightarrow m = kn = kk'm \Rightarrow kk' = 1 \Rightarrow k = k' = 1 \quad \Rightarrow n = m.$$
   So $\mathscr{R}$ is anti-symmetric.
   Then $\mathscr{R}$ is an order relation.
   2. *$\mathscr{R}$ is transitive if and only if :* $\forall n, m, h \in \mathbb{N}^*, n\mathscr{R}m \wedge m\mathscr{R}h \Rightarrow n\mathscr{R}h$
   $$\begin{cases} n\mathscr{R}m \Leftrightarrow \exists k \in \mathbb{N}^* m = kn \\ \wedge \\ m\mathscr{R}l \Leftrightarrow \exists k' \in \mathbb{N}^* l = k'm \end{cases} \Rightarrow l = k'm = kk'n \Rightarrow l = k''n \Rightarrow n\mathscr{R}l, k'' \in \mathbb{N}^*.$$
   So $\mathscr{R}$ is transitive.

2. *the order isn't total order it's partial order because* $\exists 3, 5$ *which aren't comparable.*

3. *Let set* $A = \{1, 2, 3, 4, 6, 12\}$.
   $m = 1$ *lower bound with respect the relation $\mathscr{R}$ because* $\forall n \in A, \exists k = n \in \mathbb{N}^*, n = k \times 1$.
   The possible upper bound is 12 *because* $\forall n \in A, n$ *divides* 12. *So* $min(A) = 1 = inf(A), sup(A) = 12 = max(A)$.

Solution 3.4.33. *Let $\mathscr{R}$ a relation defined on $\mathbb{N}^*$ defined by :* $n\mathscr{R} \Leftrightarrow \exists k \in \mathbb{N} : n = m^k$
1. $\mathscr{R}$ is an order relation if and only if $\mathscr{R}$ is reflexive, anti-symmetric and transitive.
a)$\mathscr{R}$ is reflexive if and only if: $\forall n \in \mathbb{N}^*, n\mathscr{R}n$
$n\mathscr{R}n \Leftrightarrow n = n^1$, *so $\mathscr{R}$ is reflexive.*
b) $\mathscr{R}$ is anti-symmetric if and only if : $\forall n, m \in \mathbb{N}^*, n\mathscr{R}m \wedge m\mathscr{R}n \Rightarrow n = m$
$$n\mathscr{R}m \Leftrightarrow \exists k \in \mathbb{N}^* m = n^k$$
$$m\mathscr{R}n \Leftrightarrow \exists k' \in \mathbb{N}^* n = m^{k'}$$
$$\Rightarrow m = n^k = m^{kk'} \Rightarrow kk' = 1 \Rightarrow k = k' = 1 \quad \Rightarrow n = m.$$

So $\mathscr{R}$ is anti-symmetric.
c) $\mathscr{R}$ is transitive if and only if : $\forall n,m,h \in \mathbb{N}^*, n\mathscr{R}m \wedge m\mathscr{R}h \Rightarrow n\mathscr{R}h$

$$\begin{cases} n\mathscr{R}m \Leftrightarrow \exists k \in \mathbb{N}^* \, m = n^k \\ \wedge \\ m\mathscr{R}l \Leftrightarrow \exists k' \in \mathbb{N}^* \, l = m^{k'} \end{cases} \Rightarrow l = m^{k'} = n^{kk'} \Rightarrow l = n^{k''} \Rightarrow n\mathscr{R}l, k'' = kk' \in \mathbb{N}^*.$$

So $\mathscr{R}$ is transitive.
Then $\mathscr{R}$ is an order relation.
Show that $\mathscr{R}$ is an order relation.
2. The order is partial because $\exists n = 2, m = 3$ such that $2\mathscr{R}3 \wedge 3\mathscr{R}2$.
3. Let set $A = \{2,4,8\}$,
$m = 2$ lower bounds with respect the relation $\mathscr{R}$ because $\forall n \in A$, $2\mathscr{R}n$, indeed $\forall n \in A, \exists k \in \mathbb{N}, n = 2^k, 2 = 2^1, 4 = 2^2, 8 = 2^3$.
$M = 8$ is a upper bounds because $\forall n \in A, n\mathscr{R}M$, indeed $\forall n \in A, \exists k \in \mathbb{N}, 8 = 2^3 = 4^2$. So $min(A) = 2 = inf(A), sup(A) = 8 = max(A)$.

PARTE II : Mapping

3.5 Mappings

3.5.1 Definition

Definition 3.5.1. *A relation f from a set E to a set F is said to be mapping or function if every element of set E has one and only one image in set F.*

In other words, a function f is a relation such that no two pairs in the relation has the same first element.

E is called the domain of f and F is called the co-domain of f.

Example 3.5.2. $f_1 : \begin{array}{l} \mathbb{N} \to \mathbb{N} \\ n \to 4n+2. \end{array}$, $f_2 : \begin{array}{l} \mathbb{R} \to \mathbb{R} \\ x \to 5x+3. \end{array}$

3.5.2 Image and inverse image

a) Image

Let $f : E \longmapsto F$ and $A \subset E$, **the image** of A is:

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

b) Inverse image

Let $f : E \longmapsto F$ and $B \subset F$, the inverse image of B is

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

Example 3.5.3. *1. Let f a mapping defined by*

$$f : [0,3] \to [0,4]$$

$$x \to f(x) = 2x + 1$$

Then $f([0,1]) = \{f(x) / x \in [0,1]\} = \{2x + 1 / 0 \le x \le 1\}$, we have:
$0 \le x \le 1 \Rightarrow 0 \le 2x \le 2 \Rightarrow 1 \le 2x + 1 \le 3$, hence $f([0,1]) = [1,3] \subset [0,4]$.

2. Let f a mapping defined by

$$g : [0,2] \to [0,4]$$

$$x \to f(x) = (2x-1)^2.$$

Then :
$f^{-1}(\{0\}) = \{x \in [0,2] / f(x) \in \{0\}\} = \{x \in [0,2] / f(x) = 0\} = \{x \in [0,2] / (2x-1)^2 = 0\} = \{\frac{1}{2}\}$.

$$f^{-1}(]0,1[) = \{x \in [0,2] / f(x) \in]0,1[\} = \{x \in [0,2] / 0 < (2x-1)^2 < 1\}.$$

Since $(2x-1)^2 > 0$ *is true* $\forall x \in \mathbb{R} - \{\frac{1}{2}\}, x \in [0,2]$.
Let us pass to :

$$(2x-1)^2 < 1 \Rightarrow |2x-1| < 1 \Rightarrow -1 < 2x-1 < 1 \Rightarrow 0 < x < 1,$$

hence $x \in]0,1[$, *thus*

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

3.6 Injectivity, Surjectivity, Bijectivity

1) Surjection

Definition 3.6.1. *The mapping* $f : E \to F$ *is called surjective (or onto mapping) if :* $\forall y \in F, \exists x \in E / f(x) = y$. *Equivalently if and only if (iff)* $f(E) = F$.

Example 3.6.2. *The following maps are they surjectives?*

1. $f_1 : \mathbb{N} \to \mathbb{N}$
   $n \to 4n+2$.
   f_1 *is not surjective. If we suppose that* f *is surjective :* $\forall y \in \mathbb{N}, \exists n \in \mathbb{N} / 4n+1 = y \Longrightarrow n = \frac{y-1}{4}$, *or* $n = \frac{y-1}{4} \notin \mathbb{N}$ *contradiction* f_1 *isn't surjective.*

2. $f_2 : \mathbb{R} \to \mathbb{R}$
   $x \to 5x+3$.
   f_2 *is surjective indeed:* $\forall y \in \mathbb{R}, \exists x \in \mathbb{R} / 5x+3 = y \Longrightarrow x = \frac{y-3}{5} \in \mathbb{R}$.

2) Injection

Definition 3.6.3. *The mapping* $f : E \to F$ *is called injective (or one-one mapping) if :*
$\forall x_1, x_2 \in E, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, *or we can use the contrapositive*

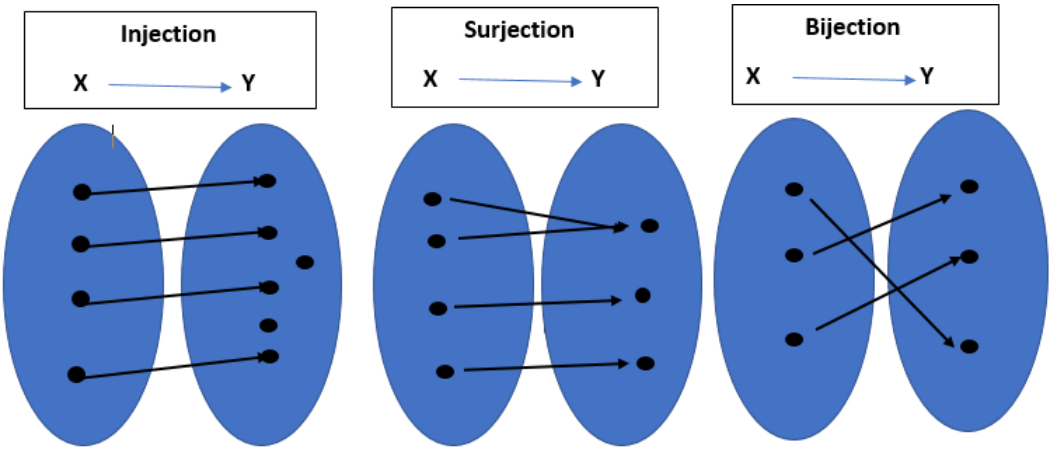
$$f \text{ is injective } \Leftrightarrow \forall x_1, x_2 \in E, f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

Example 3.6.4. *The following maps are they injectives ?*

1. $f_1 : \mathbb{N} \to \mathbb{N}$
   $n \to 4n+2$.
   f_1 *is injective indeed:*$\forall n_1, n_2 \in \mathbb{N}, f(n_1) = f(n_2) \Rightarrow 4n_1+2 = 4x_2+2 \Rightarrow 4n_1 = 4n_2 \Rightarrow n_1 = n_2$.

2. $f_2 : \mathbb{R} \to \mathbb{R}$
   $n \to 5x+3$.
   f_2 *is injective(one to one) indeed:*$\forall n_1, n_2 \in \mathbb{N}, f(x_1) = f(x_2) \Rightarrow 5x_1+3 = 5x_2+3 \Rightarrow 5x_1 = 5x_2 \Rightarrow x_1 = x_2$.

3. $f_3 : \mathbb{R} \to \mathbb{R}$
   $x \to x^2+3$.
   f_2 *is not injective. If we suppose that* f_2 *is injective :*$\forall x_1, x_2 \in \mathbb{R}$,
   $f(x_1) = f(x_2) \Rightarrow x_1^2+3 = x_2^2+3 \Rightarrow |x_1| = |x_2|$. *Then* $\exists x_1 = 1, x_2 = -1$, *such that* $f(-1) = f(1)$ *but* $x_1 \neq x_2$.



3) Bijection

A function that is both injective (one to one) and surjective(onto) is said to be bijective(one-to-one correspondence) if and only if:

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

Example 3.6.5. *1. f_1, f_3 are not bijectives.*

2. f_2 is bijective.

Remark 3.6.6. *When a mapping f is bijective we conclude that f^{-1} exists. f^{-1} is bijective too form F to E and $(f^{-1})^{-1} = f$.*

Example 3.6.7. *f_2 is bijective and the inverse mapping is given by:*

$$f_2^{-1} : \mathbb{R} \to \mathbb{R}$$

$$y \to \frac{y-3}{5}.$$

4) Composition

Let E, F, G be sets and f, g be mappings such that :

$$f : E \to F, \ g : F \to G$$

$$x \to f(x) = y \ , y \to g(y) = z$$

We define the mapping

$$g \circ f : E \to G$$

$$x \to g \circ f(x) = z.$$

Example 3.6.8. *1. Identity, $id_E : E \to E$ is defined by $id(x) = x$.*

2. if $f :]0, +\infty[\to]0, \infty[, g :]0, +\infty[\to]0, +\infty[,$

$$x \to \frac{1}{x} \qquad x \to x + \frac{1}{x},$$

then $g \circ f(x) = \frac{1}{x} + \frac{1}{\frac{1}{x}} = g(x), \quad f \circ g(x) = \frac{1}{x + \frac{1}{x}} = \frac{x}{1+x^2}.$

Proposition 3.6.9. *1. If f and g are injectives $\Rightarrow g \circ f$ is injective.*

2. If f and g are surjectives $\Rightarrow g \circ f$ is surjective.

Proof. 1. We suppose that f and g are injectives, we are going to show that $g \circ f$ is injective: $\forall x_1, x_2 \in E, g \circ f(x_1) = g \circ f(x_2)$, hence g is injective we have:

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

and f is injective. Then:

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

$g \circ f$ is injective.

2. We suppose that f and g are surjectives : $f(E) = F$, $g(F) = G$, we are going to prove that $g \circ f$ is surjective:

$$g \circ f(E) = g(f(E)) = g(F) = G$$

.

Remark 3.6.10. *Let $f : E \longmapsto F$ be bijective mapping, then $f^{-1} \circ f = Id_E, f \circ f^{-1} = Id_F$.*

c) Proprieties of Mappings

I. Let $f : E \longmapsto F$, and $A, B \in \mathscr{P}(E), C, D \in \mathscr{P}(F)$ we have:

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

II. Let I be a nonempty set and let $(A_i)_{i \in I}$ be a family of sets indexed by I, $A_i \subset E$, and let $(B_j)_{j \in J}$ be a family of sets indexed by J, $B_j \subset F$, and $f : E \to F$ we have :

1. $f(\bigcup_{i \in I} A_i) = \bigcup_{i \in I} f(A_i)$,
2. $f(\bigcap_{i \in I} A_i) \subset \bigcap_{i \in I} f(A_i)$.
3. $f^{-1}(\bigcup_{j \in J} B_j) = \bigcup_{j \in J} f^{-1}(B_j)$,
4. $f^{-1}(\bigcap_{j \in J} B_j) = \bigcap_{j \in J} f^{-1}(B_j)$.

Proof. I.1. Let $y \in f(A)$ then $\exists x \in A / f(x) = y$, or $A \subset B \Rightarrow x \in B$ hence $y = f(x) \in f(B)$ so $f(A) \subset f(B)$.

2. Let

$$\begin{aligned} y \in f(A \cup B) &\Leftrightarrow \exists x \in A \cup B / f(x) = y \\ &\Leftrightarrow \exists x \in A / f(x) = y \vee \exists x \in B / f(x) = y \\ &\Leftrightarrow y \in f(A) \vee y \in f(B) \\ &\Leftrightarrow y \in f(A) \cup f(B), \end{aligned}$$

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

3. Let

$$\begin{aligned} y \in f(A \cap B) &\Rightarrow \exists x \in A \cap B / f(x) = y \\ &\Rightarrow \exists x \in A / f(x) = y \wedge \exists x \in B / f(x) = y \\ &\Rightarrow y \in f(A) \wedge y \in f(B) \\ &\Rightarrow y \in f(A) \cap f(B), \end{aligned}$$

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

5. Let $x \in f^{-1}(C)$ hence, $\exists y \in C / y = f(x)$ or $C \subset D \Rightarrow y = f(x) \in D$ Hence $x \in f^{-1}(D)$ the $f^{-1}(C) \subset f^{-1}(D)$.

6. Let

$$\begin{aligned} x \in f^{-1}(C \cup D) &\Leftrightarrow f(x) \in C \cup D \\ &\Leftrightarrow f(x) \in C \vee f(x) \in D \\ &\Leftrightarrow x \in f^{-1}(C) \vee x \in f^{-1}(D) \\ &\Leftrightarrow x \in f^{-1}(C) \cup f^{-1}(D), \end{aligned}$$

Hence $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.

7. Let

$$\begin{aligned} x \in f^{-1}(C \cap D) &\Leftrightarrow f(x) \in C \cap D \\ &\Leftrightarrow f(x) \in C \wedge f(x) \in D \\ &\Leftrightarrow x \in f^{-1}(C) \wedge x \in f^{-1}(D) \\ &\Leftrightarrow x \in f^{-1}(C) \cap f^{-1}(D), \end{aligned}$$

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

II.1

$$\begin{aligned} y \in f(\bigcup_{i \in I} A_i) &\Leftrightarrow \exists x \in \bigcup_{i \in I} A_i / y = f(x) \\ &\Leftrightarrow \exists i \in I, \exists x \in A_i / y = f(x) \\ &\Leftrightarrow \exists i \in I, y \in f(A_i) \\ &\Leftrightarrow y \in \bigcup_{i \in I} f(A_i). \end{aligned}$$

Hence $f(\bigcup_{i \in I} A_i) = \bigcup_{i \in I} f(A_i)$.

II.2

$$\begin{aligned} y \in f(\bigcap_{i \in I} A_i) &\Leftrightarrow \exists x \in \bigcap_{i \in I} A_i / y = f(x) \\ &\Rightarrow \forall i \in I, \exists x \in A_i / y = f(x) \\ &\Rightarrow \forall i \in I, y \in f(A_i) \\ &\Rightarrow y \in \bigcap_{i \in I} f(A_i). \end{aligned}$$

Hence $f(\bigcap_{i \in I} A_i) \subset \bigcap_{i \in I} f(A_i)$.

Example 3.6.11.

$f(x) = x^2, A = [-1, 0], B = [0, 1], A \cap B = \{0\}, f(A) = [0, 1], f(B) = [0, 1],$

$$f(A) \cap f(B) = [0, 1],\ f(A \cap B) = f(\{0\}) = \{0\} \neq [0, 1] = f(A) \cap f(B).$$

The equality :$f(A \cap B) = f(A) \cap f(B)$ holds when f is injective.

Proposition 3.6.12. *Let $f : E \longmapsto F$, $g : F \longmapsto G$ we have:*

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

Proof. 1. Let $x_1, x_2 \in E / f(x_1) = f(x_2)$, then :
$g(f(x_1)) = g(f(x_2))$ since $g \circ f$ is injective hence $x_1 = x_2$ in conclusion, f is injective.

2. $f(E) \subset F \Rightarrow g \circ f(E) \subset g(F) \subset G$, since $g \circ f$ is surjective , then $g \circ f(E) = G$, hence $G \subset g(F)$ then $G = g(F), g$ is surjective.

3.7 Solved Exercises

3.7.1 Exercises

Exercise 3.7.1. *The followings mappings are they injectives? Are they surjectives? Are they bijectives?*

1. $f_1 : \mathbb{R} \to \mathbb{Z}, x \to f_1(x) = [x]$.
2. $f_2 : \mathbb{R}^2 \to \mathbb{R}^2, (x, y) \to f_2(x, y) = (x + y, x - y)$.
3. $f_3 : \mathbb{R} - \{-1\} \to \mathbb{R}, x \to f_3(x) = \dfrac{2x + 1}{x + 1}$.
4. $f_4 : \mathbb{Z}^2 \to \mathbb{Z}, (n, m) \to f_4(n, m) = nm^2$.

Exercise 3.7.2. *Let $f : \mathbb{R} \to \mathbb{R}$, a map defined by $f(x) = x^2 + 1$. and $A = [-2, 1], B = [0, 3]$ two parts of $\mathbb{R}$*

1. *Compare $f(A) \cap f(B)$ with $f(A \cap B)$.*
2. *For which condition do we have: $f(A) \cap f(B) = f(A \cap B)$.*
3. *f is-it surjective ?*
4. *Give the restriction g of f such that g will be bijective and give its bijection.*

Exercise 3.7.3. *Let $f : [0, 2[\cup]2, +\infty[\to]-\infty, 0] \cup]1, +\infty[$, a map defined by : $f(x) = \dfrac{x^2}{x^2 - 4}$*
1) f is it injective? Is it surjective? What can we deduce.
2) Determine the following sets : $f^{-1}(\{2\}), f^{-1}([\frac{1}{2}, 1]), f([0, 2[\cup]2, +\infty[)$.

Exercise 3.7.4. *Let $f : [0, 1] \to [0, 1]$ a map defined by : $\begin{cases} x & \text{if } x \in [0, 1] \cap \mathbb{Q} \\ 1 - x & \text{if} \end{cases}$. Show that $f \circ f = id$.*

Exercise 3.7.5. *Let $E = [0, 1], F = [-1, 1]$, et $G = [0, 2]$ be tree parts of $\mathbb{R}$. and f be a map form E to G defined by:*

$$f(x) = 2 - x,$$

and g a map from F to G defined by:

$$g(x) = x^2 + 1$$

1. *Determine $f(\{1/2\}), f^{-1}(\{0\}), g([-1, 1]), g^{-1}[0, 2])$.*

2. *f is it bijective?*

3. *g is it bijective?*

Exercise 3.7.6. *Let* $f:\mathbb{R}\to\mathbb{R}$ *be a map defined by*

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

1) f is it injective? f is it surjective?
2) Determine the following sets : $f(\{0\}), f^{-1}(\{0\}), f^{-1}(\{\frac{2}{\sqrt{2}}\})$.

Exercise 3.7.7. *Let* $f:\mathbb{R}\to\mathbb{R}, g:\mathbb{R}\to\mathbb{R}$ *are two maps defined by*

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

1. f is it injective ? Evaluate $f^{-1}(\{-1\})$. *What can you deduce ?*
2. g is it injective ? is it surjective ? If g isn't bijective so give injective restriction h_1 *of g, a surjective restriction* h_2 *of g and a bijective restriction* h_3 *of g.*

Exercise 3.7.8. *I. Let* $f:\mathbb{R}\to\mathbb{R}$ *be a map defined by* $f(x)=\dfrac{1}{1+x^2}$

1. *a) f is it injective ? b) f is it surjective?*

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

II. On $\mathbb{R}$ *we define a relation* $\mathscr{R}$ *by :* $x\mathscr{R}y \Leftrightarrow f(x)=f(y)$.

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

2. *Evaluate the equivalence classes of* 0.

3. *For which condition on f,* $\mathscr{R}$ *becomes an order relation.*

Exercise 3.7.9. *Let* $f:E\to F$, *be a map, let* $A\subset E, B\subset F$. *Show that:*

1. $f(f^{-1}(B))\subset B$, *Do we have equality ?*

2. $A\subset f^{-1}(f(A))$, *Do we have equality ?*

3.7.2 Solutions

Solution 3.7.10. 1. $f_1:\mathbb{R}\to\mathbb{Z}, x\to f_1(x)=[x]$,
(f_1*ins't injective because*) $\Leftrightarrow (\exists x_1=0, x_2=0.5\in\mathbb{R}, f(x_1)=f(x_2))=0\wedge x_1\neq x_2)$,
f_1 *is surjective because* $\forall y\in\mathbb{Z}, \exists x=y\in\mathbb{Z}/y=[x]$.

2. $f_2:\mathbb{R}^2\to\mathbb{R}^2, (x,y)\to f_2(x,y)=(x+y,x-y)$,
(f_2*is injective*) $\Leftrightarrow (\forall (x_1,y_1),(x_2,y_2)\in\mathbb{R}, f_2(x_1,y_1)=f_2(x_2,y_2)\Rightarrow (x_1,y_1)=(x_2,y_2)$.
$f_2(x_1,y_1)=f_2(x_2,y_2)\Rightarrow (x_1+y_1,x_1-y_1)=(x_2+y_2,x_2-y_2)\Rightarrow \begin{cases} x_1+y_1=x_2+y_2 \\ \wedge \\ x_1-y_1=x_2-y_2 \end{cases} \Rightarrow x_1=x_2\Rightarrow$
$y_1=y_2$.
f_2 *is surjective* $\forall (X,Y)\in\mathbb{R}^2, \exists (x,y)\in\mathbb{R}^2/f_2(x,y)=(X,Y)$.
$f_2(x,y)=(x+y,x-y)=(X,Y)\Rightarrow \begin{cases} x+y=X \\ \wedge \\ x-y=Y \end{cases} \Rightarrow \begin{cases} x=\dfrac{X+Y}{2} \\ \wedge \\ y=\dfrac{X-Y}{2} \end{cases}$

3. $f_3 : \mathbb{R}-\{-1\} \to \mathbb{R}, x \to f_3(x) = \dfrac{2x+1}{x+1}$. *$f_3$ is injective* $\Leftrightarrow f_3(x_1) = f_3(x_2) \Rightarrow x_1 = x_2$.
$f_3(x_1) = f_3(x_2) \Rightarrow \dfrac{2x_1+1}{x_1+1} = \dfrac{2x_2+1}{x_2+1} \Rightarrow 2x_1x_2 + x_2 + 2x_1 + 1 = 2x_1x_2 + x_1 + 1 + 2x_2 \Rightarrow x_1 = x_2$.
f_3 is surjective $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}-\{-1\}/, f_3(x) = y$.
$y = \dfrac{2x+1}{x+1} \Rightarrow xy + y = 2x + 1 \Rightarrow x(y-2) = 1 - y \Rightarrow x = \dfrac{1-y}{y-2}$, *$x$ isn't defined for $y = 2$. So f_3 isn't surjective.*

1. $f_4 : \mathbb{Z}^2 \to \mathbb{Z}, (n,m) \to f_4(n,m) = nm^2$. *$f_4$ isn't injective* $\exists (n,m) = (1,-1), (n',m') = (1,1)/f(n,m) = f(n',m')$ *but* $(n,m) \neq (n',m')$.
f is surjective $\forall y = k \in \mathbb{Z}, \exists (n,m) = (k,1)$ *such that* $y = k = nm^2$.

Solution 3.7.11. *I. Let* $f : \mathbb{R} \to \mathbb{R}$, *be a map defined by* $f(x) = x^2 + 1$.
$A = [-2,1], B = [0,3]$

$$\begin{aligned} 1. f(A) &= \{f(x), x \in A\} \\ &= [1,5] \cup [1,2] = [1,5], \\ f(B) &= \{f(x)/x \in [0,3]\} = [1,10] \\ &\quad A \cap B = [0,1] \Rightarrow f(A \cap B) = [1,2] \\ &\quad f(A \cap B) \subset f(A) \cap f(B) \\ &= [1,5] \cap [1,10] = [1,5]. \end{aligned}$$

2. We have: $f(A \cap B) \subset f(A) \cap f(B)$.
Let $y \in f(A) \cap f(B) \Rightarrow y \in f(A) \wedge y \in f(B) \Rightarrow \exists x_1 \in A/y = f(x_1) \wedge \exists x_2 \in A/y = f(x_2)$
$\Rightarrow y = f(x_1) = f(x_2) \Rightarrow^{?} x_1 = x_2 \in A \wedge x_1 = x_2 \in B$
$x_1 \in A \cap B$, *so* $f(A) \cap f(B) \subset f(A \cap B)$. *$f$ must be injective.*
3. F is surjective : $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}/y = f(x)$.
$x = \pm\sqrt{y-1}$, *for* $y = -1, x$ *doesn't exist* $f^{-1}(\{-1\}) = \emptyset$, $y = -1$ *hasn't antecedent. Thus f isn't surjective.*
4. Let $g : [0, +\infty] \to [1, +\infty[$ *be a restriction of f, its bijection is given by* $g^{-1}(y) = \sqrt{y-1}$.

Solution 3.7.12. *Let* $f : [0,2[\cup]2,+\infty[\to]-\infty,0] \cup]1,+\infty[$, $f(x) = \frac{x^2}{x^2-4}$

$$1) f \text{ is injective } \Leftrightarrow \forall x_1, x_2 \in E, f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

Let $x_1, x_2 \in E$ *such that,* $f(x_1) = f(x_2)$ *we have that:*

$$\begin{aligned} f(x_1) = f(x_2) &\Rightarrow \frac{x_1^2}{x_1^2-4} = \frac{x_2^2}{x_2^2-4} \Rightarrow x_1^2 = x_2^2 \\ &\Rightarrow |x_1| = |x_2| \Rightarrow x_1 = x_2, x_1, x_2 \geq 0. \end{aligned}$$

$$2) f \text{ is surjective } \Leftrightarrow \forall y \in F, \exists x \in E/f(x) = y.$$

Let $y \in]-\infty,0] \cup]1,+\infty[/y = f(x)$

$$y = \frac{x^2}{x^2-4} \Rightarrow x^2 = \frac{4y}{y-1}, \quad with \quad y \neq 1.$$

Moreover $4y(y-1) \geq 0$, $F =]-\infty,0] \cup]1,+\infty[$, *so* $x = \sqrt{\dfrac{4y}{y-1}}$, *thus f is surjective.*

Conclusion : f is bijective.
2) Determine the following sets : $f^{-1}(\{2\}), f^{-1}([\frac{1}{2},1]), f([0,2[\cup]2,+\infty[)$.

$$f^{-1}(\{2\}) = \{x \in [0,2[\cup]2,+\infty[, y = 2\} = \{2\sqrt{2}\}.$$

Or f is bijective $f^{-1}(2)=\sqrt{\dfrac{4.2}{2-1}}=\{2\sqrt{2}\}$.

$$f^{-1}([\frac{1}{2},1])=\{x\in[0,2[\cup]2,+\infty[,y\in[\frac{1}{2},1]\}=\emptyset,$$

because $[\frac{1}{2},1]\not\subseteq]-\infty,0]\cup]1,+\infty[$

$$f([0,2[\cup]2,+\infty[)=f(E)=F=]-\infty,0]\cup]1,+\infty[$$

Hence f is surjective.
Other to prove it : $f([0,2[\cup]2,+\infty[)=f([0,2[)\cup f(]2,+\infty[)$ *with f is decreasing* ($f'(x)=\dfrac{-8x}{(x^2+4)^2}$ *and f is bijective*

$$f([0,2[)=]\lim_{x\to 2^-}f(x),f(0)[=]-\infty,0],$$

$$f(]2,+\infty[)=]\lim_{x\to+\infty}f(x),\lim_{x\to 2^-}f(x)[=]1,+\infty],$$

so

$$f([0,2[\cup]2,+\infty[)=]-\infty,0]\cup]1,+\infty[$$

Solution 3.7.13. *Let* $f:[0,1]\to[0,1]$ *such that* $\begin{cases} x & if\ x\in[0,1]\cap\mathbb{Q} \\ 1-x & if \end{cases}$.

Let us evaluate $f\circ f: f(f(x))=\begin{cases} f(x) & if\ x\in[0,1]\cap\mathbb{Q} \\ f(1-x) & if \end{cases}=\begin{cases} f(x)=x & if\ x\in[0,1]\cap\mathbb{Q} \\ f(1-x) & if \end{cases}$.
Moreover $1-x\notin[0,1]\cap\mathbb{Q}$, *because if* $1-x=m\in\mathbb{Q}\Rightarrow x=1-m\in\mathbb{Q}$ *it's a contradiction, so* $f(1-x)=1-(1-x)=x$. *Then* $f\circ f(x)=Id(x)$.

Solution 3.7.14. *1. (a)* $f(\{1/2\})=\{f(x)\in[0,2]/x=1/2\}$,
$f(1/2)=3/2\in[0,2]$, *so :* $f(\{1/2\})=\{3/2\}$.

(b) $f^{-1}(\{0\})=\{x\in[0,1]/f(x)=0\}$.
we have $f(x)=2-x=0\Rightarrow x=2\notin[0,1]$, *so:* $f^{-1}(\{0\})=\emptyset$.

(c) $g([-1,1])=\{g(x)\in[0,2]/x\in[-1,1]\}$, *we have* $x\in[-1,0]\cup]0,1]$.

$$\begin{aligned} x\in[-1,0] &\Rightarrow -1\le x\le 0 \\ &\Rightarrow 0\le x^2\le 1 \\ &\Rightarrow 1\le x^2+1\le 2 \\ &\Rightarrow g(x)\in[1,2]\subset[0,2] \end{aligned}$$

so $g([-1,0])=[1,2]$

$$\begin{aligned} x\in]0,1] &\Rightarrow 0<x\le 1 \\ &\Rightarrow 0<x^2\le 1 \\ &\Rightarrow 1<x^2+1\le 2 \\ &\Rightarrow g(x)\in]1,2]\subset[0,2] \end{aligned}$$

so $g(]0,1])=]1,2], g([-1,1])=[1,2]$.

(d) $g^{-1}([0,2])=\{x\in[-1,1]/g(x)\in[0,2]\}$, *we have*

$$\begin{aligned} g(x)\in[0,2] &\Rightarrow 0\le x^2+1\le 2 \\ &\Rightarrow -1\le x^2\le 1 \\ &\Rightarrow (-1\le x^2<0)\vee(0\le x^2\le 1) \end{aligned}$$

This inequality $(-1 \le x^2 < 0)$ *doesn't have a solutions.*

$$0 \le x^2 \le 1 \Leftrightarrow 0 \le |x| \le 1 \Leftrightarrow -1 \le x \le 1.$$

So

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

2. *Since* $f^{-1}(\{0\}) = \emptyset$ *that means that* $0 \in [0,2]$ *hasn't antecedent with respect* f *on* $[-1,1]$*, then* f *isn't surjective so isn't bijective.*

3. g *is even map so* $g(-1) = g(1)$ *or* $-1 \neq 1$ *then* g *isn't injective so* g *isn't bijective, moreover* $g([-1,1]) = [1,2] \neq [0,2]$ *so* g *isn't surjective, hence isn't bijective.*

Solution 3.7.15. *Let* f *be a map defined by* $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \frac{2}{\sqrt{x^2+1}}$
1) f *is it injective? Is it surjective?*
a) f*is injective* $\Leftrightarrow \forall x, y \in \mathbb{R}, f(x) = f(y) \Rightarrow x = y$ *Let* $x, y \in E$ *such that* $f(x) = f(y)$ *we have:*

$$f(x) = f(y) \Rightarrow \frac{2}{\sqrt{x^2+1}} = \frac{2}{\sqrt{y^2+1}}) \Rightarrow \sqrt{x^2+1} = \sqrt{y^2+1} \Rightarrow x^2 = y^2 \Rightarrow |x| = |y|.$$

Hence, f *isn't injective on* $\mathbb{R}$ *because* $\exists x = -1 \neq y = 1/f(1) = f(-1)$.
f*is surjective* $\Leftrightarrow \forall y \in \mathbb{R}, \exists x \in \mathbb{R}/f(x) = y$ *Let* $y \in \mathbb{R}/y = f(x)$*:*

$$y = \frac{2}{\sqrt{x^2+1}} \Rightarrow \frac{2}{y} = \sqrt{x^2+1} \Rightarrow \frac{4}{y^2} = x^2 + 1$$

so f *isn't surjective because* x *isn't defined for* $y = 0$

2) $f(\{0\}) = \{f(x) \in \mathbb{R}, x = 0\}$, $f(\{0\}) = \{\frac{2}{\sqrt{x^2+1}} \in \mathbb{R}, x = 0\} = \{2\}$
$f^{-1}(\{0\}) = \{x \in \mathbb{R}, y = 0\}$, $f^{-1}(\{0\} = \{x \in \mathbb{R}, \frac{2}{\sqrt{x^2+1}} = 0\} = \emptyset$
$f^{-1}(\{2/\sqrt{2}\}) = \{x \in \mathbb{R}, y = \frac{2}{\sqrt{2}}\}, f^{-1}(\{2/\sqrt{2}\}) = \{x \in \mathbb{R}, \frac{2}{\sqrt{x^2+1}} = \frac{2}{\sqrt{2}}\}$, *so*
$\sqrt{x^2+1} = \sqrt{2} \Rightarrow x^2 = 1. \Rightarrow f^{-1}(\{2/\sqrt{2}\}) = \{1, -1\}.$

Solution 3.7.16. *Let* $f : \mathbb{R} \to \mathbb{R}, g : \mathbb{R} \to \mathbb{R}$ *are two maps defined by* $f(x) = x^2 + x, g(x) = x^2 + x + 1$.
1. a)f *isn't injective indeed* $\exists x_1 = 0, x_2 = -1$ *such that* $f(x_1) = f(x_2) = 0$*, but* $x_1 \neq x_2$.
b)$f(\{-1\}) = \emptyset$ *because* $\exists y = -1, \forall x \in \mathbb{R}, f(x) \neq -1$*, so* f *isn't sujective, the* f *isn't bijective.*
2. a) g *isn't injective indeed* $\exists x_1 = 0, x_2 = -1$ *such that* $g(x_1) = g(x_2) = 1$*, but* $x_1 \neq x_2$.
b)g *isn't sujective because* $\exists y = 0, \forall x \in \mathbb{R}, f(x) \neq 0$.
Now let us determine a restrictions of g*:*
(i) $h_1 : [-\frac{1}{2}, +\infty) \to \mathbb{R}$ *or* $h_1 :]-\infty, -\frac{1}{2}] \to \mathbb{R}$. *Indeed* h_1 *is injective* $\Leftrightarrow \forall x_1, x_2 \in [-\frac{1}{2}, +\infty), f(x_1) = f(x_2) \Rightarrow$
$x_1^2 + x_1 + 1 = x_2^2 + x_1 + 1 \Rightarrow (x_1 + \frac{1}{2})^2 + \frac{3}{4} = (x_2 + \frac{1}{2})^2 + \frac{3}{4} \Rightarrow x_1 = x_2$.
(ii) $h_2 : \mathbb{R} \to [\frac{3}{4}, +\infty[$. *Indeed* h_2 *is surjective* $\Leftrightarrow \forall y \in [\frac{3}{4}, +\infty[, \exists x \in \mathbb{R}/y = f(x) \Rightarrow (x_1 + \frac{1}{2})^2 + \frac{3}{4} = y \Rightarrow x =$
$\pm\sqrt{y - \frac{3}{4}} - \frac{1}{2}$.
At least $h_3 : [-\frac{1}{2}, +\infty) \to [\frac{3}{4}, +\infty[$ *is bijective.*

Solution 3.7.17. *I.Let* $f : \mathbb{R} \to \mathbb{R}$ *be a map defined by* $f(x) = \dfrac{1}{1+x^2}$

1. *a)* f *is injective if and only if:* $\forall x, x' \in \mathbb{R}, f(x) = f(x') \Rightarrow x = x'$
   f *isn't injective because* $\exists x = 1 \neq x' = -1 \in \mathbb{R}, f(1) = f(-1) = 1/2$.
   b) f *is surjective if and only if:* $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}, y = f(x)$:
   f *isn't surjective because* $\exists y = 0$*, such that* x *isn't defined*

2. $f([-1,1]) = \{f(x) \in \mathbb{R} \; x \in [-1,1]\}$, *so :*

$$-1 \leq x \leq 1 \Rightarrow \begin{cases} 0 \leq x \leq 1 \\ -1 \leq x \leq 0 \end{cases} \Rightarrow 0 \leq x^2 \leq 1 \Rightarrow f([-1,1]) = [\frac{1}{2}, 1]$$

$f^{-1}(\{0\}) = \{x \in \mathbb{R} / f(x) = 0\} = \emptyset$.

II. On $\mathbb{R}$ *we define a relation* $\mathscr{R}$ *by :* $x\mathscr{R}y \Leftrightarrow f(x) = f(y)$.

1. $\mathscr{R}$ *is reflexive if and only if:* $\forall x \in \mathbb{R}, x\mathscr{R}x \quad x\mathscr{R}x \Leftrightarrow f(x) = f(x)$ *it's clear.*

2. $\mathscr{R}$ *is symmetric if and only if:* $\forall x, y \in \mathbb{R}, x\mathscr{R}y \Rightarrow y\mathscr{R}x$ *:*

$$x\mathscr{R}y \Leftrightarrow f(x) = f(y) \Rightarrow f(y) = f(x) \Leftrightarrow y\mathscr{R}x$$

3. $\mathscr{R}$ *is transitive if and only if:* $\forall x, y, z \in \mathbb{R}, x\mathscr{R}y \wedge y\mathscr{R}z \Rightarrow x\mathscr{R}z$
$\begin{cases} x\mathscr{R}y \Leftrightarrow f(x) = f(y) \\ y\mathscr{R}z \Leftrightarrow f(y) = f(z) \end{cases} \Rightarrow f(x) = f(z) \Leftrightarrow x\mathscr{R}z.$

2. $\dot{0} = \{y \in \mathbb{R} / 0\mathscr{R}y\}$

$$0\mathscr{R}y \Leftrightarrow f(0) = f(y) \Rightarrow 1 = \frac{1}{1+y^2} \Rightarrow y = 0, \dot{0} = \{0\}.$$

3. $\mathscr{R}$ *is an order relation if it is anti-symmetric:* $\forall x, y \in \mathbb{R}, x\mathscr{R}y \wedge y\mathscr{R}x \Rightarrow x = y$*, then*
$\begin{cases} x\mathscr{R}y \Leftrightarrow f(x) = f(y) \\ y\mathscr{R}x \Leftrightarrow f(y) = f(x) \end{cases} \Rightarrow x = y.$ *So* f *must be injective.*

Solution 3.7.18. *Let* $f : E \to F$*, be a map, let* $A \subset E, B \subset F$*. Show that :*

1. $f(f^{-1}(B)) \subset B$*, let* $y \in f(f^{-1}(B)) \Rightarrow \exists x \in f^{-1}(B)$ *such* $y = f(x)$*, on the other hand* $x \in f^{-1}(B) \Rightarrow \exists y \in B / y = f(x) \in B$.
We don't have the equality, here the counterexample :
let $f : \mathbb{R} \to \mathbb{R}$ *be a map, defined by* $f(x) = x^2$*, and let* $B = \{-1\}, f^{-1}(\{-1\}) = \{x \in \mathbb{R} / x^2 = -1\} = \emptyset, f(f^{-1}(\{-1\})) = f(\emptyset) = \emptyset$.
Moreover $B = \{-1\} \not\subset \emptyset = f(f^{-1}(B))$.
Another counterexample: *let* $f : \{0,1\} \to \{0,1,2\}$ *be a map such that* $f(0) = 1, f(1) = 2$, $B = \{0\}, f^{-1}(\{0\}) = \{x \in \mathbb{R} / f(x) = 0\} = \emptyset$, $f(f^{-1}(\{0\})) = f(\emptyset) = \emptyset$.
Moreover $B = \{0\} \not\subset \emptyset = f(f^{-1}(B))$.
Remark : $B = f(f^{-1}(B))$ *if* f *is surjective.*

2. $A \subset f^{-1}(f(A))$*, let* $x \in A$*; we have* $f(x) \in f(A) \Rightarrow x \in f^{-1}(f(A))$.
We don't have the equality, here the counterexample :
Let $f : \mathbb{R} \to \mathbb{R}$ *be a map, defined by* $f(x) = x^2$*, let* $A = \{1\}, f(\{1\}) = \{f(x) \in \mathbb{R} / x = 1\} = \{1\}$, $f^{-1}(f(\{1\})) = \{x \in \mathbb{R} / x^2 = 1\} = \{-1, 1\}$.
Moreover $f^{-1}(f(A)) = \{-1, 1\} \not\subset \{1\} = A$.
Another counterexample: *let* $f : \{0,1\} \to \{0,1,2\}$ *be a map such that* $f(0) = 1, f(1) = 1$, $A = \{1\}, f(\{1\}) = \{f(x) \in \mathbb{R} / x = 1\} = \{1\}$, $f^{-1}(f(\{1\})) = \{x \in \{0,1\} / y = 1\}$
Moreover $f^{-1}(f(A)) = \{0,1\} \not\subset \{1\} = A$.
Remark: $f^{-1}(f(A)) = A$*, if* f *injective.*

Chapter 4

Algebraic Structures

4.1 Binary Operations

Definition 4.1.1. *Let G be a nonempty set. Any map $\star$ form $G\times G$ into G is called **binary operation** on G or **binary composition** in G.*

Example 4.1.2. *1. Addition is binary operation on $\mathbb{R}$*

$$+ : \mathbb{R}\times\mathbb{R}\to\mathbb{R}$$

$$(a,b)\to a+b.$$

2. The map

$$\star : \mathbb{R}-\{\frac{1}{2}\}\times\mathbb{R}-\{\frac{1}{2}\}\longmapsto\mathbb{R}-\{\frac{1}{2}\}$$
$$(a,b)\longmapsto a+b-2ab$$

is binary operation on $\mathbb{R}-\{\frac{1}{2}\}$.
$\forall a,b\in\mathbb{R}-\{\frac{1}{2}\}$, we have to show that $a+b-2ab\in\mathbb{R}-\{\frac{1}{2}\}$ more precisely that $a+b-2ab\neq\frac{1}{2}$, because $a+b-2ab\in\mathbb{R}$, we are going to use the proof by contradiction, we suppose that $a+b-2ab=\frac{1}{2}$, with $a\neq\frac{1}{2}$, et $b\neq\frac{1}{2}$:

$$a+b-2ab=\frac{1}{2}\Rightarrow a(1-2b)+(b-\frac{1}{2})=0\Rightarrow(\frac{1}{2}-b)(2a-1)=0\Rightarrow a=\frac{1}{2}\vee b=\frac{1}{2}$$

contradiction then $a+b-2ab\neq\frac{1}{2}$, so $a\star b\in\mathbb{R}-\{\frac{1}{2}\}$, $\star$ is binary operation .

3. The map

$$\clubsuit :]-1,1[\times]-1,1[\to]-1,1[$$
$$(x,y)\to\frac{x+y}{1+xy},$$

is binary operation on $]-1,1[$.

Definition 4.1.3. *Let G be a set and $\star$ binary operation.*

*1. $\star$ is called **commutative** if and only if :*

$$\forall x,y\in G, x\star y=y\star x.$$

*2. $\star$ is called **associative** if and only if :*

$$\forall x,y,z\in G, x\star(y\star z)=(x\star y)\star z.$$

3. $\star$ ***has a neutral element*** *if and only if :*

$$\exists e \in G, \forall x \in G, x \star e = e \star x = x.$$

(The element e is also called the identity element of G.)

4. *For any element $x \in G$, there is an element $x' \in G$ est satisfying : $x \star x' = x' \star x = e$, where $e \in G$. (We denote this element x' by x^{-1}, and call it the inverse of x.)*

Example 4.1.4. *a) the law*

$$\star : \mathbb{R} - \{\frac{1}{2}\} \times \mathbb{R} - \{\frac{1}{2}\} \longmapsto \mathbb{R} - \{\frac{1}{2}\}$$
$$(a,b) \longmapsto a + b - 2ab.$$

1. $\star$ *is commutative :*
$\forall a, b \in \mathbb{R} - \{\frac{1}{2}\}, a \star b = b \star a$, *because the sum and product are commutative.*

2. $\star$ *is associative:*
$\forall a, b, c \in \mathbb{R} - \{\frac{1}{2}\}, a \star (b \star c) = (a \star b) \star c,$

$$a \star (b \star c) = a \star (b + c - 2cb) = a + b + c - 2cb - 2ab - 2ac + 4abc ...(1)$$

$$(a \star b) \star c = (a + b - 2ab) \star c = c + a + b - 2ab - 2ac - 2cb + 4abc ...(2)$$

$(2) = (1)$.

3. $\star$ *has a neutral element :*
$\exists e \in \mathbb{R} - \{\frac{1}{2}\}, \forall a \in \mathbb{R} - \{\frac{1}{2}\}, a \star e = e \star a = a$, *however $\star$ is commutative then let us resolve just this equation:*
$a \star e = a + e - 2ae = a \Rightarrow e(1 - 2a) = 0 \Rightarrow e = 0 \in \mathbb{R} - \{\frac{1}{2}\}$.

4. *for any element $a \in \mathbb{R} - \{\frac{1}{2}\}$ there exists an element $a' \in \mathbb{R} - \{\frac{1}{2}\}$ such that $a \star a' = a' \star a = e = 0$,*
$a \star a' = a + a' - 2aa' = 0 \Rightarrow a' = \dfrac{-a}{1 - 2a}$, *now we are going to prove $a' \in \mathbb{R} - \{\frac{1}{2}\}$ that means $a' \neq \frac{1}{2}$, by contradiction $a' = \frac{1}{2} \Rightarrow 1 = 0$, contradiction, then $a' \in \mathbb{R} - \{\frac{1}{2}\}$.*

b)

$$\clubsuit :]-1,1[\times]-1,1[\to]-1,1[$$
$$(x,y) \to \frac{x+y}{1+xy}$$

1. $\clubsuit$ *is commutative if and only if :*
$\forall x, y \in]-1,1[, x \clubsuit y = y \clubsuit x$, *however the sum and product are commutative.*

2. $\clubsuit$ *is associative if and only if:*
$\forall x, y, z \in]-1,1[, x \clubsuit (y \clubsuit z) = (x \clubsuit y) \clubsuit z,$

$$x \clubsuit (y \clubsuit z) = x \clubsuit (\frac{y+z}{1+yz}) = \frac{x + \dfrac{y+z}{1+yz}}{1 + \dfrac{xy+zx}{1+yz}} = \frac{x + xyz + y + z}{1 + yz + xy + zx} ...(1)$$

$$(x \clubsuit y) \star z = \frac{x+y}{1+xy} \clubsuit z = \frac{z + \dfrac{x+y}{1+xy}}{1 + \dfrac{zx+zy}{1+xy}} = \frac{z + xyz + x + y}{1 + xz + zx + zy} ...(2)$$

$(2) = (1)$

3. *Existence of neutral element:*
   $\exists e \in]-1,1[, \forall x \in]-1,1[, e\clubsuit x = e\clubsuit x = x$,
   since $\clubsuit$ *is commutative then let us resolve just this equation :*
   $x\clubsuit e = \dfrac{x+e}{1+xe} = x \Rightarrow x+e = x+x^2e \Rightarrow e(1-x^2) = 0 \Rightarrow e = 0 \in]-1,1[$.

4. *Existence of inverses :*
   For any element $x \in]-1,1[$ *there exist an element* $x' \in]-1,1[$ *such that :*
   $x\clubsuit x' = x'\clubsuit x = e = 0$,
   $x\clubsuit x' = \dfrac{x+x'}{1+xx'} = 0 \Rightarrow x' = -x \in]-1,1[$

Remark 4.1.5. *i) The neutral element if it exists is unique.*
ii) The neutral element is always invertible, and we have $e^{-1} \star e = e \star e^{-1} = e$.

Proposition 4.1.6. *Let* G *be a set and* $\star$ *binary operation which is associative and has a neutral element* e, *let* $x, y \in G$ *two invertible element under* $\star$, *then* $x \star y$ *is invertible under* $\star$, *and* $(x \star y)^{-1} = y^{-1} \star x^{-1}$.

Proof.

$$(y^{-1} \star x^{-1}) \star (x \star y) = (y^{-1} \star (x^{-1}) \star x) \star y = (y^{-1} \star e) \star y = y^{-1} \star y = e.$$
$$(x \star y) \star (y^{-1} \star x^{-1}) = (x \star (y \star y^{-1})) \star x^{-1} = (x \star e) \star x^{-1} = x \star x^{-1} = e.$$

4.2 Groups

Definition 4.2.1. *Let* G *be a set and* $\star$ *be a binary operation.* G *is called a group if and only if :*

1. $\star$ *is associative.*
2. $\star$ *has a neutral element.*
3. *Every element of* G *has an inverse in* G.

If $\star$ *est commutative, then* $(G, \star)$ *in called commutative or Abelian group.*

Example 4.2.2. 1. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+)$ *and* $(\mathbb{C},+)$ *are commutative groups.*

2. $(\mathbb{R},\times)$ *is not a group because the element* 0 *does not have an inverse element.*
3. $(\mathbb{R}_+^*,\times)$ *is a commutative group.*
4. *Let* $\star$ *be binary operation defined by :*

$$\star : \mathbb{R} - \{\frac{1}{2}\} \times \mathbb{R} - \{\frac{1}{2}\} \to \mathbb{R} - \{\frac{1}{2}\}$$
$$(a,b) \to a + b - 2ab,$$

   $G = \mathbb{R} - \{\frac{1}{2}\}$, *so* $(G, \star)$ *is an Abelian group.*

5. $(]-1,1[,\clubsuit)$ *is commutative group, with*

$$\clubsuit :]-1,1[\times]-1,1[\to]-1,1[$$
$$(x,y) \to \frac{x+y}{1+xy}$$

6. $(\mathbb{Z}/n\mathbb{Z},+)$ *is Abelian group, with* $\mathbb{Z}/n\mathbb{Z} = \{\bar{0},\bar{1},\bar{2},...,\overline{n-1}\}, n \geq 1$. $\bar{a} = \bar{b} \Leftrightarrow a \equiv b[n]$, *or* $\exists k \in \mathbb{Z}, a = b + kn$. *We define the addition in* $\mathbb{Z}/n\mathbb{Z}$ *by* $\bar{a} + \bar{b} = \overline{a+b}$.

4.2.1 Subgroup

Definition 4.2.3. *Let $(G,\star)$ be a group, and H be a part of G. We say that $(H,\star)$ is a subgroup of $(G,\star)$ if $(H,\star)$ is a group.*

Definition 4.2.4. *$H \subset G$ is a subgroup of G if :*

1. $e \in H$.
2. *For all* $x,y \in H$, $x \star y \in H$.
3. *For each* $x \in H$, $x^{-1} \in H$.
   Where e neutral element G, x^{-1} is an inverse element of x on G.

Proposition 4.2.5. *Let H be a part of a group $(G,\star)$, then :*

$$(H,\star) \text{ is subgroup of } (G,\star) \Leftrightarrow \begin{cases} e \in H \\ \forall x,y \in H : x \star y^{-1} \in H \end{cases}$$

Example 4.2.6.

1. *$(\mathbb{Z},+)$ is a subgroup of $(\mathbb{Q},+)$, indeed:*
$$0 \in \mathbb{Z}, \forall x,y \in \mathbb{Z}, x+(-y) \in \mathbb{Z}.$$
2. *$(\mathbb{Q},+)$ is subgroup of $(\mathbb{R},+)$.*
3. *$(\mathbb{R}^{*+},\times)$ is a subgroup of $(\mathbb{R}^{*},\times)$ indeed :*
$$1 \in \mathbb{R}^{*+}, \forall x,y \in \mathbb{R}^{*+}, x \times \frac{1}{y} \in \mathbb{R}^{*+}.$$
4. *the subgroups of $(\mathbb{Z},+)$ are $n\mathbb{Z}$, for $n \in Z$, where $n\mathbb{Z} = \{k.n/k \in \mathbb{Z}\}$.*

Proposition 4.2.7. *Let G be a group, and $(H_i)_{i\in I}$ be a family of subgroups of G, so $\bigcap_{i\in I} H_i$ is a subgroup of G.*

Proof. Let $(H_i)_{i\in I}$ be a family of sets indexed by I, $\bigcap_{i\in I} H_i$, so $e \in H$, because $\forall i \in I, e \in H_i$, $\forall x,y \in H, \forall i \in I, x \in H_i, y \in H_i$, thus $xy^{-1} \in H_i \Rightarrow xy^{-1} \in H$. Then $\bigcap_{i\in I} H_i$ is a subgroup of G.

Remark 4.2.8. *We deduce from the precedent result that the intersection of two subgroups $H,K \subset G$ of a group G is a subgroup of G. But the union of subgroups of G is not necessarily a subgroup of G.*

Generated subgroups

Let $(G,\star)$ be a group and $A \subset G$ be a subset of G. The subgroup generate by A is the smallest subgroup of G containing A, denoted $< A >$ or $gr(A)$.
The subgroup generate denoted $\{a\}$, denoted by $< a >$.

Example 4.2.9.

1. *If A is subgroup of G then $< A >= A$.*
2. *On $(\mathbb{Z},+)$, $< 2 >= \{...,-4,-2,0,2,4,6,...\} = 2\mathbb{Z}, < \{3,5\} >= \mathbb{Z}$.*
3. *On $(G,.)$, if $a \in G$, so $< a >= \{...,a^{-2},a^{-1},1,a,a^2,...\} = \{a^n, n \in \mathbb{Z}\}$.*

Cyclic group

Definition 4.2.10. *A cyclic group G is a group that can be generated by a single element $a \in G$ that mean $< a >= G = \{a^n, n \in \mathbb{Z}\}$.*
(For addition $G = \{na,\ n \in \mathbb{Z}\}$.)

Example 4.2.11.

The group $\mathbb{Z}$ under addition is a cyclic group and $\mathbb{Z} =< 1 >=< -1 >$.

The group $2\mathbb{Z}$ under addition is a cyclic group and $2\mathbb{Z} =< 2 >=< -2 >$.

Remark 4.2.12. *Any cyclic group can be generated by more than one generator.*

4.2.2 Group homomorphisms

Definition 4.2.13. *Let $(G,\star),(G',\diamond)$ be two groups, and $f:G\to G'$ is a map, we say that f is group homomorphism if :*

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

If f is bijective, so f is called an isomorphism .
If $G=G'$, f became an endomorphism of G, and if plus f is bijective, so f is called an automorphism.

Example 4.2.14. *1. The map $f_1:\mathbb{R}\to\mathbb{R}^{+*}$, defined by $f_1(x)=e^x$ is an isomorphism from group $(\mathbb{R},+)$ to the group $(\mathbb{R}^{+*},\times)$.*
Indeed :

$$f_1(x+y)=e^{x+y}=e^xe^y=f_1(x)\times f_1(y).$$

2. The map $f_2:\mathbb{R}^{+*}\to\mathbb{R}$, defined by $f_2(x)=\ln(x)$ is an isomorphism from group $(\mathbb{R}^{+*},\times)$ to the group $(\mathbb{R},+)$.
Indeed :

$$f_2(x\times y)=\ln(xy)=\ln(x)+\ln(y)=f_2(x)+f_2(y).$$

Proposition 4.2.15. *Let a map $f:G\to G'$ be a group homomorphism from group $(G,\star)$ to a group $(G',\diamond)$, so :*

1. $f(e)=e'$.
2. $\forall x\in G,(f(x))^{-1}=f(x^{-1})$.

Where e,(resp e') is the neutral element of G(resp G').

Proof. 1. $f(e)=f(e\star e)=f(e)\diamond f(e)\Rightarrow f(e)\diamond(f(e))^{-1}=f(e)\diamond f(e)\diamond(f(e))^{-1}\Rightarrow e'=f(e)$.

2. $f(x)\diamond f(x^{-1})=f(x\star x^{-1})=f(e)=e'$, and $f(x^{-1})\diamond f(x)=f(x^{-1}\star x)=f(e)=e'$, so $(f(x))^{-1}=f(x^{-1})$.

Proposition 4.2.16. 1. *Let $f:G\to G'$ et $g:G'\to G''$ be two groups homomorphism.*
Then $g\circ f:G\to G''$ is group homomorphism

2. *IF $f:G\to G'$ is a bijective homomorphism, then $f^{-1}:G'\to G$ is a group homomorphism too.*

4.2.3 kernel and image

Let $(G,\star),(G',\diamond)$ be two groups, and $f:G\to G'$ be a group homomorphism.

Definition 4.2.17. 1. *The kernel of f, denoted by* $\ker(f)$*:*

$$\ker(f)=\{x\in G/f(x)=e'\}=f^{-1}(\{e'\}).$$

Where e', is the neutral element of $(G',\diamond)$.

2. *the image of f, denoted by $Im(f)$:*

$$Im(f)=\{f(x)/x\in G\}.$$

Proposition 4.2.18. *Let $f:G\to G'$ a group homomorphism, then*

1. $\ker(f)$ *is a subgroup of G.*
2. *$Im(f)$ is a subgroup of G'.*

Proof. 1. Let us show that $\ker(f)$ is a subgroup of G:

i) $f(e)=e'$, so $e'\in\ker(f)$.

ii) Let $x,x'\in\ker(f)$, $f(x\star x')=f(x)\diamond f(x')=e'\diamond e'=e'$, then $x\star x'\in\ker(f)$.

iii) Let $x \in \ker(f)$, so $f(x^{-1}) = (f(x))^{-1} = e'^{-1} = e'$, then $x^{-1} \in \ker(f)$.

2. Let us show that $Im(f)$ is a subgroup of G':

   i) $f(e) = e'$, so $e' \in Im(f)$.

   ii) Let $y, y' \in Im(f)$, so $\exists x, x' \in G$ such that $f(x) = y, f(x') = y'$, Moreover $y \diamond y' = f(x) \diamond f(x') = f(x \star x')$, then $y \diamond y' \in Im(f)$.

   iii) Let $y \in Im(f), x \in G / y = f(x)$, so $y^{-1} = f(x)^{-1} = f(x^{-1}) \in Im(f)$.

Proposition 4.2.19. *Let $f : G \to G'$ be a group homomorphism, then :*
1. f is injective (one-to-one) if and only if $\ker(f) = \{e\}$.
2. f is surjective (onto) if and only if $Im(f) = G'$.

Definition 4.2.20. *A group $(G, \star)$ is isomorphic to a group $(G', \diamond)$ if and only if there exist an isomorphism from $(G, \star)$, to $(G', \diamond)$.*

Example 4.2.21. *$(\mathbb{R}^{+*}, \times)$ is isomorphic to $(\mathbb{R}, +)$ because there exist an isomorphism : $\ln : \mathbb{R}_+^* \to \mathbb{R}$.*

Definition 4.2.22. *We say $(G, \star)$ is a finite group, if the cardinal of G is finite.*

Group Tables :
we can represent a finite group $(G, \star)$ where $G = \{a_1, ..., a_n\}$ set using a table, called group table (of dimension $n \times n$) composed of $a_i \star a_i$, for $i, j = 1, .., n$.

Definition 4.2.23. *Let $(G, \star)$ be a finite group. The cardinal of G is called the order of the group and it's denoted by $ord(G)$, or $|G|$.*
The second notion of order, for a group element $a \in G$, the least (positive) integer such that $x^k = e$, k is called the order of the element a. We write it $|x|$.

Theorem 4.2.24. *(Lagrange's Theorem) Let H be a subgroup of a finite group $(G, \star)$ Then the order of H divides the order of G.*

4.3 Examples of groups

4.3.1 The group $\mathbb{Z}/n\mathbb{Z}$

Let $n \in \mathbb{Z}^+$, let $\equiv$ be an equivalence relation on $\mathbb{Z}$, defined by :

$$\forall a, b \in \mathbb{Z} \Leftrightarrow a \equiv b[n] \Leftrightarrow \exists k \in \mathbb{N} / a - b = nk.$$

Read as a is congruent to b modulo n. The set of equivalence classes of integers modulo n is called the integer modulo n. We denote it $\mathbb{Z}_n$ the quotient set, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$.

Example 4.3.1. $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}, \mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{3}\}$.

We define the addition and multiplication operation on $\mathbb{Z}/n\mathbb{Z}$ by :

1. The addition is given by : $\forall a, b \in \mathbb{Z}/n\mathbb{Z}, \overline{a} + \overline{a} = \overline{a + b}$.

2. The multiplication is given by: $\forall a, b \in \mathbb{Z}/n\mathbb{Z}, \overline{a} \times \overline{a} = \overline{a \times b}$.

Example 4.3.2. *Let us give the table of addition and multiplication, on $\mathbb{Z}/3\mathbb{Z}$,*
$\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{3}\}$

+	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

×	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Proposition 4.3.3. *The set $(\mathbb{Z}/n\mathbb{Z}, +)$ is a commutative group.*

4.3.2 Permutation group $\mathscr{S}_n$

Definition 4.3.4. *Let E be a nonempty set. A permutation of E is a map $f : E \to E$ that is bijective(one to one and onto).*
A permutation group of E denoted by $\mathscr{S}_E$ is a group under map composition.
$\mathscr{S}_E$ is called the symmetric group on E.

Definition 4.3.5. *For any $n \geq 1$, if E has n elements, $E = \{1,...,n\}$. We denote by $\mathscr{S}_n$ the symmetric group corresponding to E.*

Proposition 4.3.6. *$(\mathscr{S}_n, \circ)$ is non-commutative group, where $\circ$ is the map composition law, with $e = Id_E$ the identity element.*

Proposition 4.3.7. *$\mathscr{S}_n$ is a finite group and $|\mathscr{S}_n| = n!$.*

Notation and examples

A permutation $\sigma : \{1,2,...,n\} \to \{1,2,...,n\}$ maps the elements
$1,...,n$ to $\sigma(1),...,\sigma(n)$, defined by:

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}.$$

For example on $\mathscr{S}_4$ we give the following permutation:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

σ it's bijection from $\{1,2,3,4\}$to $\{1,2,3,4\}$ defined by :

$$\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 2.$$

Neutral element of a group $\mathscr{S}_n$ is the identity id, given by :

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix}.$$

The composition of two permutations σ_1, σ_2 it's the composition of maps $\sigma_2 \circ \sigma_1(n) = \sigma_2(\sigma_1(n))$.
For example :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}.$$

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \\ 4 & 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}.$$

Observe that $\sigma_2 \circ \sigma_1 \neq \sigma_1 \circ \sigma_2$.

Inverse element of σ denoted by σ^{-1} can be found just by reading σ upside-down or by doing a permutation of the two lines.
For example :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \sigma^{-1} = \begin{pmatrix} 1 & 3 & 4 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Proposition 4.3.8. *Let $\sigma_1,...,\sigma_n, \gamma, \tau \in \mathscr{S}_n$. Then*

1. $(\sigma\gamma)\tau = \sigma(\gamma\tau)$ *(Associativity).*
2. $Id\sigma = \sigma Id = \sigma$.
3. $(\sigma_1,...,\sigma_n)^{-1} = \sigma_n^{-1}...\sigma_2^{-1}\sigma_1^{-1}$.
4. $\sigma\gamma = \sigma\tau \Rightarrow \gamma = \tau$.
5. $\gamma\sigma = \tau\sigma \Rightarrow \gamma = \tau$.

Definition 4.3.9. *1. The transposition is a permutation that swaps two elements and leaves everything else fixed.*
For example, (i,j) is the transposition that swaps i and j given by :

$$\tau_{ij} = \begin{pmatrix} 1 & 2 & ... & i & ... & j & ... & n \\ 1 & 2 & ... & j & ... & i & ... & n \end{pmatrix} = (i,j), 1 \leq i, \leq j \leq n.$$

2. The cycle is a permutation which maps a finite subset $\{1,2,3,...,n\}$ by

$$1 \to 2 \to 3 \to ... \to (n-1) \to n \to 1.$$

The cycle is denoted by $(1,2,3,...,n)$.
The cycle $(1,2,3,...,n)$ has length n.
For example, the cycle $(1,2,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$ of length 3.
And $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (1,2,3)(4,5)$ is a product of a cycle of length 3 and another of length 2.

Note that a cycle of length n has order n as an element of $\mathcal{S}_n$.

Remark 4.3.10. *The transposition is a cycle of length 2.*

Example 4.3.11. *Let us give the six elements of $(\mathcal{S}_3,\circ)$, $\mathcal{S}_3$ has $3! = 6$ elements :*

$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \mathcal{S}_3 = \{id, \tau_1, \tau_2, \tau_3, \sigma_1, \sigma_2\}.$$

$\tau_1 \circ \tau_2, \tau_2 \circ \tau_1$ are given by :

$$\tau_1 \circ \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_1 \neq \tau_2 \circ \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_2.$$

The cycle $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3)$ has length 3.

Theorem 4.3.12. *All permutations of $\mathcal{S}_n$ may be written as a product of disjoint cycles.*

Example 4.3.13. *1. Let $f = (12) \circ (234), g = (234) \circ (12)$*

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1,2,3,4)$$

$$f \neq g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1,3,4,2)$$

2. Let $f = (12) \circ (34), g = (34) \circ (12)$,

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = g$$

4.4 Ring

Definition 4.4.1. *Let R be a nonempty set equipped with two binary operation $\star,\delta$, we say that $(R,\star,\delta)$ is a ring if:*

1. *$(R,\star)$ is commutative group.*
2. *$\forall x,y,z\in R,\ x\delta(y\star z)=(x\delta y)\star(x\delta z) and (x\star y)\delta z=(x\delta z)\star(y\delta z)$.*
3. *δ is associative.*

If δ is commutative, then $(R,\star,\delta)$ is commutative ring.
If δ has neutral element, then $(R,\star,\delta)$ is ring with unity.

Example 4.4.2. *1.$(\mathbb{Z},+,\cdot)$ is commutative ring with unity.*
2. Let I be an interval of $\mathbb{R}$, we denote by $C(I,\mathbb{R})$ the set of continuous functions $f:I\to\mathbb{R}$ equipped with the addition and product between functions, so $(C(I,\mathbb{R}),+,\times)$ is a commutative ring with unity.
3. $(\mathbb{Z}/n\mathbb{Z},+,\times)$ is a commutative ring with unity.

4.4.1 Calculus rules of ring

Let $(R,+,\cdot)$be a ring. Where 0 is a neutral element of the addition, and $-x$ is the symmetric element of $x\in R$ and $+$, $1=1_R$ is the neutral element of the product, the following hold:

1. $\forall x\in R, 0.x=x.0=0$.
2. $\forall x,y\in R,(-y).x=(-x).y=-xy$
3. $\forall x,y,z\in R,(x-y)z=xz-yz$.
4. $\forall x,y,z\in R,z(x-y)=zx-zy$.

Proof. 1. Let $x\in R$:

$$x.0=x(0+0)=x.0+[x.0+(-(0.x))]=x(0+0)+(-(0x))=x.0+(-(0.x))=0.$$

2. Let $x,y\in R$,using 1):

$$(-y)x+xy=((-y)+y)x=0.x=0,(-x)y+xy=((-x)+x)y=0.$$

3. Let $x,y,z\in R$, using 2):
$(x-y)z=(x+(-y))z=xz+(-y)z=xz-xz, z(x-y)=z(x+(-y))=zx+z(-y)=zx-zy.$

□

4.4.2 Subring

Let $(R,+,.)$ be a ring, $B\in\mathscr{P}(R)$. B is called a subring of A if and only if :

1. B is subgroup of $(R,+)$.
2. For each $x,y\in B$, we have $xy\in B$.
3. $1_R\in B$.

Proposition 4.4.3. *Let $(R,+,.)$ be a ring , $B\in\mathscr{P}(R)$. B is called a subring of A if and only if :*

1. *$\forall x,y\in B, x-y\in B$.*
2. *For each $x,y\in B$, we have $xy\in B$.*
3. *$0_R,1_R\in B$.*

Example 4.4.4. *$\mathbb{Z}$ is a subring of $\mathbb{Q}$ which is a subring of R.*

4.4.3 Ring homomorphism

Let $(R,+,.),(R',+,.)$ be two rings with unity, let $f:R\to R'$ be a map. f is called ring homomoprhism if and only if :

1. $\forall x,y\in R, f(x+y)=f(x)+f(y)$.
2. $\forall x,y\in R, f(x.y)=f(x).f(y)$.
3. $f(1_R)=1_{R'}$.

The notions of isomorphism, endomorphism, and automorphism are the same as those to a group.

Proposition 4.4.5. *If $f:R\to R'$ et $g:R'\to R''$ are two rings homomorphisms, then $g\circ f$ is ring homomorphism.*

Example 4.4.6. *Let* $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}/(a,b)\in\mathbb{Z}^2\}$

1. $\mathbb{Z}[\sqrt{2}]$ *is a subring of* $(\mathbb{R},+,.)$ *indeed:*

   (a) $\forall x,y\in\mathbb{Z}[\sqrt{2}],\ x-y\in\mathbb{Z}[\sqrt{2}]$:
   $x,y\in\mathbb{Z}[\sqrt{2}],\ \exists a,b,a',b'\in\mathbb{Z},\ x=a+b\sqrt{2}$ *and* $y=a'+b'\sqrt{2}$, *so:*

   $$x-y=a+b\sqrt{2}-a'-b'\sqrt{2}=(a-a')+(b-b')\sqrt{2}\in\mathbb{Z}[\sqrt{2}].$$

   (b) *For each* $x,y\in\mathbb{Z}[\sqrt{2}]$, *we have* $xy\in\mathbb{Z}[\sqrt{2}]$.
   $x,y\in\mathbb{Z}[\sqrt{2}],\ \exists a,b,a',b'\in\mathbb{Z},\ x=a+b\sqrt{2}$ *and* $y=a'+b'\sqrt{2}$, *so :*

   $$x.y=(a+b\sqrt{2})(a'+b'\sqrt{2})=(aa'+bb')+(ab'+a'b)\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$$

   (c) $0,1\in\mathbb{Z}[\sqrt{2}]$:
   It's simple since : $0=0+0\sqrt{2}\in\mathbb{Z}[\sqrt{2}],\ 1=1+0\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$.
   Then, $(\mathbb{Z}[\sqrt{2}],+,.)$ *is a subring of* $(\mathbb{R},+,.)$.

2. *Let f be a map defined by* $f:\mathbb{Z}[\sqrt{2}]\to\mathbb{Z}[\sqrt{2}]$ $f(a+b\sqrt{2})=a-b\sqrt{2}$.
   f is ring automorphism $(\mathbb{Z}[\sqrt{2}],+,.)$ *if f is ring homomorphism and f is bijective.*
   f is ring homomorphism $\mathbb{Z}[\sqrt{2}]$ *if and only if :*

   (a) $\forall x,y\in\mathbb{Z}[\sqrt{2}],\ f(x+y)=f(x)+f(y)$:
   $f(x+y)=f(a+b\sqrt{2}+a'+b'\sqrt{2})=(a+a')-(b+b')\sqrt{2}=f(a+b\sqrt{2})+f(a'+b'\sqrt{2})$.

   (b) $\forall x,y\in\mathbb{Z}[\sqrt{2}], f(x.y)=f(x).f(y)$:

   $$f(xy)=f((a+b\sqrt{2})(a+'b'\sqrt{2}))=f((aa'+bb')+(a'b+ab')\sqrt{2})$$

   $$=(aa'+bb')-(a'b+ab')\sqrt{2}=f(a+b\sqrt{2})f(a'+b'\sqrt{2}).$$

   (c) $f(1)=1$.

   f is bijective because for each $a+b\sqrt{2}$ there exist a unique $a-b\sqrt{2}$.
   Then f is a ring automorphism $(\mathbb{Z}[\sqrt{2}],+,.)$.

4.4.4 An integral domain

Definition 4.4.7. *Let R be a commutative ring with unity, $r \in R$.*
r is called a zero divisor in R if and only if :

$$r \neq 0, \exists a \in R, (b \neq 0 \ \ and \ \ ra = 0).$$

Example 4.4.8. *1. $\mathbb{Z}$ hasn't a zero divisor.*

2. On $\mathbb{Z}/6\mathbb{Z}$, the zero divisor are : $\dot{2}, \dot{3}, \dot{4}$.

Definition 4.4.9. *A commutative ring with unity R is an integral domain if and only if it doesn't have non-zero divisors.*

Example 4.4.10. *$(\mathbb{Z}, +, .)$ is an integral domain.*

Proposition 4.4.11. *[The cancellation law] If R is an integral domain and $a, b, c \in R$ such that $a \neq 0$ and $a.b = a.c$ then $b = c$.*

Definition 4.4.12. *Let R be a ring. A nilpotent element of R is an element r, such that there exists an $n \in \mathbb{N}$ such that $r^n = 0$. Note that 0 is allowed to be nilpotent.*

Proposition 4.4.13. *Let R be a ring and let $r \in R$ be nilpotent. Then r is a zero divisor.*

Proposition 4.4.14. *For $n > 1$, $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is prime.*

4.4.5 Ideals

Let R be a commutative ring.

Definition 4.4.15. *A subring I of a ring R is an ideal if $\forall r \in R, \forall x \in I, rx \in I$.*

Definition 4.4.16. *1. $\forall n \in \mathbb{N}, n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.*
2. $\mathbb{Z}$ isn't an ideal of $\mathbb{R}$, because $\exists 1 \in \mathbb{Z}, \sqrt{2} \in \mathbb{R}, \sqrt{2} \notin \mathbb{Z}$.

Proposition 4.4.17. *A nonempty set I of a ring R is an ideal if and only if, the following properties hold:*

1. *$O_R \in I$.*
2. *If $x, y \in I$, the $x - y \in I$.*
3. *If $r \in R$ and $x \in I$, then $rx \in I$.*

4.5 Field

Definition 4.5.1. *Let F be a nonempty set equipped by two binary operations $\star, \delta$, $(\mathbb{K}, \star, \delta)$ is called a field if :*

1. *$(\mathbb{K}, \star, \delta)$ is ring with unity.*
2. *$(\mathbb{K} - \{e\}, \delta)$ is a group , where e is a neutral element of $\star$.*

If δ is commutative, $(\mathbb{K}, \star, \delta)$ is called a commutative field.

Example 4.5.2. *$(\mathbb{R}, +, \cdot)$ is a commutative field.*

Proposition 4.5.3. *Any finite integral domain is a field.*

Definition 4.5.4. *Let $(K, +, .)$ be a field, $L \in \mathscr{P}(K)$. L is called a sub-field*

1. *L is a sub-ring K*

2. $\forall x \in L - \{0\}, x^{-1} \in L$.

Example 4.5.5. $(\mathbb{Q}, +, .)$ *is a sub-field of* $(\mathbb{R}, +, .)$ *which is a sub-field of* $(\mathbb{C}, +, .)$

Proposition 4.5.6. $\mathbb{Z}/n\mathbb{Z}$ *is a field if* n *is prime* .

4.6 Solved Exercises

4.6.1 Exercises

Exercise 4.6.1. *1. On* $\mathbb{R}$ *we define the binary operation* $\star$ *by :*

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

$\star$ *is it associative? Does it have a neutral element ?*
2. On $\mathbb{R}^{+*}$ *we define the binary operation* $\star$ *by :*

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

$\star$ *has it a neutral element ?*
The inverse element exist ?
On $\mathbb{R}$ *we define the binary operation* $\star$ *by :*

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

$\star$ *is it commutative, associative ? Does it have a neutral element ?*

Exercise 4.6.2. *On* $G = \mathbb{R}^* \times \mathbb{R}$ *we define the binary operation* $\star$ *by :*

$$\forall (x, y), (x', y') \in G, (x, y) \star (x', y') = (xx', xy' + y).$$

1. *Show that* $(G, \star)$ *is non-commutative group.*
2. *Show that* $\mathbb{R}^{+*} \times \mathbb{R}$ *is a sub-group of* G.

Exercise 4.6.3. *Are the following sets subgroups of* $(G, +)$*:*

1. $H_1 = \{(x, y, z) \in \mathbb{R}^3 / x + 2y + 3z = 0 \wedge 2x - y + z = 0\}, G = \mathbb{R}^3$.
2. $H_2 = \{(x, y, z) \in \mathbb{R}^3 / x + y = 0 \vee x - y + z = 0\}, G = \mathbb{R}^3$.
3. $H_3 = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} / (a, b) \in \mathbb{Z}^2\}, G = \mathbb{R}$.

Exercise 4.6.4. *Let* $(G, \star)$ *be group and* $(H, \star), (K, \star)$ *two subgroups of* $(G, \star)$.

1. *Show that* $K \cap H$ *is a subgroup*
2. *Show that* $K \cup H$ *is a subgroup if and only if* $K \subset H$ *or* $K \subset H$.

Exercise 4.6.5. *On* $G = \mathbb{R}^2$ *we define the binary operation* $*$ *by:*

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

1. Show that $(G, *)$ *is a commutative group.*
2. Show that $H = (\mathbb{Q}^2, *)$ *is a subgroup of* G.
3. Show that

$$f : (\mathbb{Z}^2, *) \to (\mathbb{Z}^2, *)$$
$$(x, y) \to (x, y)$$

is group homomorphism.

Exercise 4.6.6. *On $G = \mathbb{R} \times \mathbb{R}^*$ we define the binary operation $*$ by:*

$$\forall (x,y),(x',y') \in G, (x,y) * (x',y') = (x + x', yy')$$

1. *Show that $(G,*)$ is commutative group.*
2. *Show that $H = \{(x,1)/x \in \mathbb{Z}\}$ is a subgroup of G.*

Exercise 4.6.7. *On $\mathbb{R} - \{1\}$ we define the binary operation $*$ by:*

$$\forall x, y \in \mathbb{R} - \{1\}, x * y = x + y - xy.$$

1. *Show that $*$ is binary operation.*
2. *Show that $(\mathbb{R} - \{1\}, *)$ is an commutative group.*
3. *We define the map f by:*

$$f : (\mathbb{R}^*, \times) \to (\mathbb{R} - \{1\}, *)$$
$$x \to 1 - \frac{1}{x}.$$

a) Show that f is an isomorphism.
b) Determine le $Ker(f)$.

Exercise 4.6.8. *On $\mathbb{R} - \{1\}$ we define an operation $*$ by:*

$$\forall x, y \in \mathbb{R} - \{1\}, x * y = xy - x - y + 2.$$

1. *Show that $*$ is binary operation.*
2. *Show that $(\mathbb{R} - \{1\}, *)$ is commutative group.*

Exercise 4.6.9. *On $\mathbb{R}$ we define the binary operation $\star$ by :*

$$\forall x, y \in \mathbb{R}, x \star y = \sqrt[3]{x^3 + y^3}.$$

1. *Show that $(\mathbb{R}, \star)$ is a commutative group.*
2. *$H = \{-3,-2,-1,0,1,2,3\}$ is a subgroup of $(\mathbb{R}, \star)$?*
3. *Let f be a map define from $\mathbb{R}$ to $\mathbb{R}$ by $f(x) = \sqrt[3]{x}$.*
   Show that f is an isomorphism from $f(\mathbb{R}, +)$, to $f(\mathbb{R}, \star)$.
4. *Show that $(\mathbb{R}, \star)$, is isomorphic to $(\mathbb{R}, +)$,.*

Exercise 4.6.10. *Let G be a group :*

1. *A map $f : (G,.) \to (G,.)$ defined by $f(x) = x^{-1}$ is a group homomorphism if and only if G is commutative.*
2. *Let $a \in G$ show that the map $f : (G,.) \to (G,.)$ defined by : $f(x) = axa^{-1}$ is an automorphism. Determiner $Ker(f)$.*
3. *Let a map $f : (\mathbb{R}, +) \to (\mathbb{R}^*, .)$ defined by : $f(x) = 2^x$ show that f is group homomorphism. Determiner its kernel.*

Exercise 4.6.11. *1. Determine the elements of $(\mathcal{S}_3, \circ)$, and its group table.*
2. Determine the inverse of $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.
3. Determine the generated group of σ.

Exercise 4.6.12. *On $\mathbb{Z}^2$ we define two binary operations $\oplus, \odot$ by:*

$$\forall (x,y),(x',y') \in \mathbb{Z}^2, (x,y) \oplus (x',y') = (x+x', y+y'),$$

$$\forall (x,y),(x',y') \in \mathbb{Z}^2, (x,y) \odot (x',y') = (xx', xy'+yx').$$

1. Show that $(\mathbb{Z}^2, \oplus, \odot)$ is a commutative ring.
2. Show that $A = \{(a,0)/a \in \mathbb{Z}\}$ is a subring of $(\mathbb{Z}^2, \oplus, \odot)$.

Exercise 4.6.13. *Let a set $\mathbb{Z}[\sqrt{5}]$ defined by $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5}/(a,b) \in \mathbb{Z}^2\}$*

1. *Show that $\mathbb{Z}[\sqrt{5}]$ is a subring of $(\mathbb{R}, +, .)$*
2. *Let $f : \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}[\sqrt{5}]$ be a map defined by $f(a + b\sqrt{5}) = a - b\sqrt{5}$.*
   Show that f is an automorphism of the ring $(\mathbb{Z}[\sqrt{5}], +, .)$

Exercise 4.6.14. *I. $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$ are they fields ?*
II. a) Determine the elements of $\mathbb{Z}/8\mathbb{Z}$ and the invertible elements of $\mathbb{Z}/8\mathbb{Z}$.
b) Determine the zero divisors of $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$ is it a field ?
III. $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}$ are they fields?
IV. a) Determine the elements of $\mathbb{Z}/10\mathbb{Z}$ and the invertible elements of $\mathbb{Z}/10\mathbb{Z}$.
b)Determine the zero divisors of $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/10\mathbb{Z}$ is it a field ?

Exercise 4.6.15. *Any finite integral domain is a field.*

Exercise 4.6.16. *Let $x, y \in \mathbb{R}$, we define the binary operations $T, \star$ by :*

$$xTy = x + y - 1, x \star y = xy - x - y + 2.$$

Show that $(\mathbb{R}, T, \star)$ is a field.

4.6.2 Solutions

Solution 4.6.17. *1. On $\mathbb{R}$ we define the binary operation $\star$ by :*

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

$\star$ is associative if and only if:

$$\forall x, y, z \in \mathbb{R},\ (x \star y) \star z = x \star (y \star z)$$

$$\begin{aligned}
(x \star y)\star &= (xy + (x^2-1)(y^2-1)) \star z \\
&= xyz + z(x^2-1)(y^2-1) + [(xy + (x^2-1)(y^2-1))^2 - 1](z^2-1).....(1), \\
x \star (y \star z) &= x \star (yz + (y^2-1)(z^2-1)) \\
&= xyz + x(y^2-1)(z^2-1) + (x^2-1)[(yz + (y^2-1)(z^2-1))^2 - 1].....(2).
\end{aligned}$$

$(1) \neq (2)$ so $\star$ isn't associative.
$\star$ has a neutral element if and only if :

$$\exists e \in \mathbb{R}, \forall x \in \mathbb{R}, x \star e = e \star x = x.$$

$$\begin{cases} x \star e = x \\ e \star x = x \end{cases} \Rightarrow \begin{array}{l} xe + (x^2-1)(e^2-1) = x \\ ex + (e^2-1)(x^2-1) = x \end{array} \Rightarrow ex + (e^2-1)(x^2-1) = x$$

$$\begin{cases} \forall x \in \mathbb{R} & (1+e)x^2 + x - (1+e) = 0 \\ \vee e - 1 = 0 & \Rightarrow e = 1 \end{cases} \Rightarrow e = 1 \in R.$$

Indeed : $(1+e)x^2+x-(1+e)\neq 0,\ \forall x\in\mathbb{R}$ *it's different from zero polynomial :* $P=0=(0x^2+0x+0)$ *where all coefficients are zero, the coefficient of* x *is equal to* $1\neq 0$.
2. On $\mathbb{R}^{+*}$ *we define the binary operation* $\star$ *by :*

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

$\star$ *has a neutral element if and only if:*

$$\exists e\in\mathbb{R}^{+*},\forall x\in\mathbb{R}^{+*}, x\star e=e\star x=x.$$

$$\begin{cases} x\star e=x \\ e\star x=x \end{cases} \Rightarrow \begin{matrix}\sqrt{x^2+e^2}=x \\ \sqrt{e^2+x^2}=x\end{matrix} \Rightarrow \sqrt{x^2+e^2}=x\Rightarrow e=0\notin\mathbb{R}^{+*}.$$

So $\star$ *hasn't a neutral element, the, the inverse element also doesn't exist.*
3. On $\mathbb{R}$ *we define the binary operation* $\star$ *by :*

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

$\star$ *isn't commutative because* $\exists x=2,y=3$ *and* $x\star y=2+3+(2^2\times 3)=17\neq 3+2+(3^2\times 2)=y\star x$.
$\star$ *is associative si if and only if:*

$$\forall x,y,z\in\mathbb{R},\ (x\star y)\star z=x\star(y\star z)$$

$$\begin{aligned} (x\star y)\star &= (x+y+x^2y)\star z \\ &= x+y+x^2y+z+z(x+y+x^2y)^2.....(1), \\ x\star(y\star z) &= x\star(y+z+y^2z) \\ &= x+y+z+y^2z+x(y+z+y^2z)^2.....(2). \end{aligned}$$

$(1)\neq(2)$ *so* $\star$ *isn't associative.*
$\star$ *has a neutral element if and only if:*

$$\exists e\in\mathbb{R},\forall x\in\mathbb{R}, x\star e=e\star x=x.$$

$$\begin{cases} x\star e=x \\ e\star x=x \end{cases} \Rightarrow \begin{matrix}x+e+x^2e=x \\ e+x+e^2x=x\end{matrix} \Rightarrow \begin{matrix}e(1+x^2)=0 \\ e(1+ex)=\end{matrix} \Rightarrow e=0\in\mathbb{R}$$

$e=0$ *is a neutral element .*

Solution 4.6.18. $(G,*)$ *is a group if and only if:*

$$\begin{cases} *\text{is associative} \\ *\text{has a neutral element} \\ \text{Every element of} G \text{ has its inverse element of } G \end{cases}$$

1. $*$ *is associative if and only if:* $\forall(x,y),(x',y'),(x'',y'')\in G$,
$[(x,y)*(x',y')]*(x'',y'')=(x,y)*[(x',y')*(x'',y'')]$

$$\begin{aligned} [(x,y)*(x',y')]*(x'',y'') &= (xx',xy'+y)*(x'',y'') \\ &= (xx'x'',xx'y''+xy'+y).....(1), \\ (x,y)*[(x',y')*(x'',y'')] &= (x,y)*(x'x'',x'y''+y') \\ &= (xx'x'',xx'y''+xy'+y).....(2). \end{aligned}$$

$(1)=(2)$, *so* $*$ *is associative.*

2. $*$ *has a neutral element* G *if and only if:*

$$\exists (e,e') \in G,\ \forall (x,y) \in G, (x,y)*(e,e') = (e,e')*(x,y) = (x,y)$$

$$\begin{cases} (x,y)*(e,e') = (x,y) \\ (e,e')*(x,y) = (x,y) \end{cases} \Rightarrow \begin{cases} (xe, xe'+y) = (x,y) \\ (ex, ey+e') = (x,y) \end{cases}$$

$$\Rightarrow \begin{cases} xe = x \\ xe' + y = y \\ ex = x \\ ey + e' = y \end{cases}$$

$$\Rightarrow \begin{cases} e = 1 \in \mathbb{R}^*, & x \neq 0 \\ e' = 0 \in \mathbb{R}, \end{cases}$$

So $(e,e') = (1,0) \in G$ *is the neutral element.*

3. $\forall (x,y) \in G, \exists (x',y') \in G,\ (x,y)*(x',y') = (x',y')*(x,y) = (e,e') = (1,0).$

$$\begin{cases} (x,y)*(x',y') = (1,0) \\ (x',y')*(x,y) = (1,0) \end{cases} \Rightarrow \begin{cases} (xx', xy'+y) = (1,0) \\ (x'x, x'y+y') = (1,0) \end{cases}$$

$$\Rightarrow \begin{cases} xx' = 1 \\ xy' + y = 0 \\ x'x = 1 \\ x'y + y' = 0 \end{cases}$$

$$\Rightarrow \begin{cases} x' = 1/x \in \mathbb{R}^*, & x \neq 0 \\ y' = -y/x \in \mathbb{R}, & x \neq 0 \end{cases}$$

So the inverse of $(x,y) \in G$ *is* $(x',y') = (1/x, -y/x) \in G$, *Then* $(G,*)$ *is a group.*

4. $*$ *isn't commutative because :*

$$\exists (x,y) = (2,0) \in G, \exists (x',y') = (1,1) \in G,\ (x,y)*(x',y') \neq (x',y')*(x,y).$$

$$\begin{cases} (2,0)*(1,1) = (2,2) & ...(1) \\ (1,1)*(2,0) = (2,1) & ...(2) \end{cases}$$

we remark that $(1) \neq (2)$, *so* $(G,*)$ *is non-commutative group.*

2. $\mathbb{R}^{+*} \times \mathbb{R} = H$ *is a subgroup if and only if :*

$$\begin{cases} (1,0) \in H \\ \forall (x,y),(x',y') \in H, (x,y) \star (x',y')^{-1} \in H \end{cases}$$

1. $(1,0) \in \mathbb{R}^{+*} \times \mathbb{R} = H$ *is satisfied.*
2. $\forall (x,y),(x',y') \in H,$

$$(x,y) \star (x',y')^{-1} = (x,y) \star (\frac{1}{x'}, -\frac{y'}{x'}) = (\frac{x}{x'}, -\frac{xy'}{x'} + y) \in \mathbb{R}^{+*} \times \mathbb{R}.$$

So $\mathbb{R}^{+*} \times \mathbb{R} = H$ *is a subgroup of* $\mathbb{R}^+ \times \mathbb{R}$.

Solution 4.6.19. 1. $H_1 = \{(x,y,z) \in \mathbb{R}, x + 2y + 3z = 0 \wedge 2x - y + z = 0\},\ G = \mathbb{R}^3.$

i) $(0,0,0) \in H_1 \Rightarrow H_1 \neq \emptyset.$

ii) *Let* $X=(x,y,z)\in H_1, Y=(x',y',z')\in H_1, X-Y\in H_1$
Where $X-Y=(x-x',y-y',z-z')$ *we have that:*

$$\begin{cases} (x-x')+2(y-y')+3(z-z')=E_1 \quad , \\ \wedge \\ 2(x-x')-(y-y')+(z-z')=E_2 \end{cases}$$

$$\Rightarrow \begin{cases} E_1=x+2y+3z-(x'+2y'+3z')=0-0=0 \quad , \\ \wedge \\ E_2=2x-y+z-(2x'-y'+z')=0-0=0 \end{cases}$$

$\Rightarrow X-Y\in H_1$, H_1 *is a subgroup of* $(\mathbb{R}^3,+)$.

2. $H_2=\{(x,y,z)\in\mathbb{R}, x+y=0\vee x-y+z=0\}, G=\mathbb{R}^3$.

   i) $(0,0,0)\in H_1\Rightarrow H_2\neq\emptyset$.

   ii) H_2 *isn't a subgroup of* $(\mathbb{R}^3,+)$, $\exists X=(1,0,-1)\in H_2, \exists Y=(-1,1,0)\in H_1$, *and* $X-Y=(2,-1,-1)\notin H_2$.

3. $H_3=\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}/(a,b)\in\mathbb{Z}^2\}, G=\mathbb{R}$.

   i) $0\in H_3$, *because* $\exists a=0,b=0\in\mathbb{Z}, 0=0+0\sqrt{2}\Rightarrow H_3\neq\emptyset$.

   ii) *Let* $x\in H_3, y\in H_3, x-y\in H_3$
   $\exists(a,b),(a',b')\in\mathbb{Z}$ *such that* $x=a+b\sqrt{2}$ *and* $y=a'+b'\sqrt{2}$, *so:*

$$x-y=(a-a')+(b-b')\sqrt{2}.$$

   Thus $\exists a''=a-a'\in Z, \exists b''=b-b'\in Z, x-y=a''+b''\sqrt{2}\Rightarrow x-y\in H_3$.
   Then H_3 *is a subgroup of* $(\mathbb{R},+)$.

Solution 4.6.20. *Let* G *be a group and* H,K *are two subgroups of* G.

1. *Sow that* $K\cap H$ *is a subgroup:*
   i) $e_G\in H\wedge e_G\in K$, *so* $e_G\in H\cap K\Rightarrow H\cap K\neq\emptyset$.
   ii) Let $x,y\in H\cap G\Rightarrow x,y\in H$ *et* $x,y\in G$, *so using the fact that they are subgroups of* G, *hence* $x\star y^{-1}\in H$, *et* $x\star y^{-1}\in G$, *then* $x\star y^{-1}\in H\cap K$, *that means that* $H\cap K$ *is a subgroup of* $(G,\star)$.

2. *When* $K\subset H$ *or* $H\subset K$, *let us show that* $K\cup H$ *is a subgroup:*
   We observe that when $K\subset H$, *so* $K\cup K=H$ *which is a subgroup, as same for* $H\subset K$, *then* $K\cup K=K$ *which is a subgroup too.*
   Now let us suppose that $K\cup H$ *is a subgroup and* H *isn't a subset of* K *and* H *isn't a subset of* H *so :*
   There exists $x\in H$ *but* $x\notin K$, *and there exists* $y\in K$ *but* $y\notin H$, *then* $x,y\in H\cup K, x\star y\in H\cup K$, *otherwise*

$$\begin{cases} \text{If } x\star y\in H & \Rightarrow x^{-1}\star(x\star y)=y\in H \text{ contradiction}, \\ \vee \\ \text{If else } x\star y\in K & \Rightarrow (x*y)\star y^{-1}=x\in K \text{ contradiction}. \end{cases}$$

   Then we have that $H\subset K$ *or* $K\subset H$.

Solution 4.6.21. $(G,*)$ *is a group if and only if:*

$$\begin{cases} *\text{is associative} \\ *\text{has a neutral element} \\ \text{Every element of } G \text{ has an inverse of } G \end{cases}$$

$*$ *is commutative if and only if:*

$$\forall(x,y),(x',y')\in G,\ (x,y)*(x',y')=(x,y)*(x',y')$$

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

then the result.
$*$ *is associative if and only if:*

$$\forall (x,y),(x',y'),(x'',y'')\in G,\ [(x,y)*(x',y')]*(x'',y'')=(x,y)*[(x',y')*(x'',y'')]$$

$$\begin{aligned}[(x,y)*(x',y')]*(x'',y'') &= (x+x',y'+y)*(x'',y'')\\ &= (x+x'+x'',y+y'+y'').....(1),\\ (x,y)*[(x',y')*(x'',y'')] &= (x,y)*(x'+x'',y'+y'')\\ &= (x+x'+x'',y+y'+y'').....(2).\end{aligned}$$

$(1)=(2)$ *then the result.*
$*$ *has a neutral element of* G *if and only if:*

$$\exists (e,e')\in G,\forall (x,y)\in G,(x,y)*(e,e')=(e,e')*(x,y)=(x,y)$$

We observe that $*$ *is commutative, so we are going to resolve just the following equation:*

$$(x,y)*(e,e')=(x+e,y+e')=(x,y)\Rightarrow (x+e=x)\wedge (y+e'=y)\Rightarrow e=0,e'=0.$$

so $(e,e')=(0,0)\in G$ *is a identity element (neutral element).*
$\forall (x,y)\in G,\exists (x',y')\in G,\ (x,y)*(x',y')=(x',y')*(x,y)=(e,e')=(0,0).$
We observe that $*$ *is commutative, so we are going to resolve just the following equation:*

$$(x,y)*(x',y')=(0,0)\Rightarrow (x+x',y+y')=(0,0)\Rightarrow x'=-x\wedge y'=-y.$$

Then the inverse of $(x,y)\in G$ *is* $(x',y')=(-x,-y)\in G$.
Thus $(G,*)$ *is a commutative group.*
$H=\mathbb{Q}^2$ *is a subgroup of* G *if :*

$$\begin{cases}(0,0)\in \mathbb{Q}^2\\ \forall X,Y\in H,\ X\star Y\in H\\ \forall X\in H,\ X^{-1}\in H\end{cases}$$

Where $X=(x,y),Y=(x',y')\in \mathbb{Q}^2$.
i) $(0,0)\in \mathbb{Q}^2$ *it's clear.*
ii) $\forall (x,y),(x',y')\in \mathbb{Q}^2,\ (x,y)\star (x',y')=(x+x',y+y')\in \mathbb{Q}^2$.
iii) $\forall (x,y)\in H,(x,y)^{-1}=(-x,-y)\in \mathbb{Q}^2$.
Then $(\mathbb{Q}^2,*)$ *is a subgroup of* $(\mathbb{R}^2,*)$.

$$f:(\mathbb{Z}^2,*)\to (\mathbb{Z}^2,*)$$

$$(x,y)\to (x,y)$$

group homomorphism if and only if :

$$\forall X=(x,y),Y=(x',y')\in \mathbb{Z}^2,f(X*Y)=f(X)*f(Y)$$

$$f(X*Y)=f(x+x',y+y')=(x+x',y+y')=(x,y)*(x',y')=f(X)*f(Y).$$

Solution 4.6.22. $*$ *is commutative if and only if:*

$$\forall (x,y),(x',y')\in G,\ (x,y)*(x',y')=(x,y)*(x',y')$$

$$(x,y)*(x',y')=(x+x',yy')=(x'+x,y'y)=(x,y)*(x',y').$$

$*$ ***is associative*** *if and only if:*

$$\forall (x,y),(x',y'),(x'',y'') \in G,\ [(x,y)*(x',y')]*(x'',y'') = (x,y)*[(x',y')*(x'',y'')]$$

$$\begin{aligned} [(x,y)*(x',y')]*(x'',y'') &= (xx',y'y)*(x'',y'') \\ &= (x+x'+x'',yy'y'').....(1), \\ (x,y)*[(x',y')*(x'',y'')] &= (x,y)*(x'+x'',y'y'') \\ &= (x+x'+x'',yy'y'').....(2). \end{aligned}$$

$(1)=(2)$*, thus* $*$ *is associative.*
$*$ *has a neutral element of* G *if and only if:*

$$\exists (e,e') \in G, \forall (x,y) \in G, (x,y)*(e,e') = (e,e')*(x,y) = (x,y).$$

We observe that $*$ *is commutative, so we are going to resolve just the following equation:*

$$(x,y)*(e,e') = (x+e,ye') = (x,y) \Rightarrow (x+e=x) \wedge (ye'=y) \Rightarrow e=0, e'=1.$$

so $(e,e') = (0,1) \in G$ *is the neutral element.*
$\forall (x,y) \in G, \exists (x',y') \in G,\ (x,y)*(x',y') = (x',y')*(x,y) = (e,e') = (0,1).$
We observe that $*$ *is commutative, so we are going to resolve just the following equation:*

$$(x,y)*(x',y') = (1,0) \Rightarrow (x+x',yy') = (0,1) \Rightarrow x' = -x \wedge y' = 1/y.$$

Then the inverse element of $(x,y) \in G$ *is* $(x',y') = (-x,1/y) \in G$*, so* $(G,*)$ *is a commutative group.*
$H = \{(x,1)/x \in \mathbb{Z}\}$ *is a subgroup of* G *if :*

$$\begin{cases} (0,1) \in H \\ \forall X,Y \in H,\ X \star Y \in H \\ \forall X \in H,\ X^{-1} \in H \end{cases}$$

Where $X=(x,1), Y=(x',1) \in H, x,x' \in \mathbb{Z}.$
1. $(0,1) \in H$*, it's simple.*
2. $\forall (x,1),(x',1) \in H,\ (x,y) \star (x',y') = (x+x',1) \in H.$
3. $\forall (x,1) \in H, (x,1)^{-1} = (-x,1) \in H.$
Hence, H *is a subgroup of* $\mathbb{R} \times \mathbb{R}^*$.

Solution 4.6.23. *1. Let us show that* $x*y \in \mathbb{R}-\{1\}$*, By contradiction:*
we suppose that $x+y-xy=1,\ x \neq 1,\ y \neq 1$*:*

$$x+y-xy=1 \Rightarrow y(1-x)+x-1=0$$

$$\Rightarrow (1-x)(y-1)=0 \Rightarrow x=1 \vee y=1$$

contradiction, so $x+y-xy \neq 1$*, then* $x*y \in \mathbb{R}-\{1\}$*,* $*$ *is a binary operation.*
$*$ *is commutative if and only if :* $\forall x,y \in \mathbb{R}-\{1\}, x*y=y*x$*, since the addition and the product are commutative operations.*
$*$ *is associative if and only if:* $\forall x,y,z \in \mathbb{R}-\{1\}, (x*y)*z = x*(y*z)$

$$(x*y)*z = (x+y-xy)*z = x+y-xy+z-xz-yz+xyz$$

$$(x*y)*z = x+y+z-xy-xz-yz+xyz...(1)$$

$$x*(y*z) = x*(y+z-yz) = x+y+z-yz-xy-xz+xyz$$

$$x*(y*z) = x+y-xy+z-xz-yz+xyz...(2)$$

$(2) = (1)$, *thus* $*$ *is associative.*
$*$ *has a neutral element if and only if:* $\exists e \in \mathbb{R} - \{1\}, \forall x \in \mathbb{R} - \{1\}, x * e = e * x = x.$
We observe that $*$ *is commutative, so we are going to resolve just the following equation:*

$$x * e = x + e - xe = x \Rightarrow e(1 - x) = 0.$$

Since $x \neq 1$, *so* $e = 0 \in \mathbb{R} - \{1\}$, *is a neutral element.*
Every element has an inverse element $\Leftrightarrow \forall x \in \mathbb{R} - \{1\}$, $\exists x' \in \mathbb{R} - \{1\}$ *such that* $x * x' = x' * x = e = 0.$
We observe that $*$ *is commutative, so we are going to resolve just the following equation :*

$$x * x' = x + x' - xx' = 0 \Rightarrow x' = \frac{-x}{1 - x}.$$

Show that $x' \in \mathbb{R} - \{1\}$ *then* $x' \neq 1$, *by contradiction we suppose that* $x' = 1 \Rightarrow 1 = 0$, *so* $x' \in \mathbb{R} - \{1\}.$
Then $(\mathbb{R} - \{1\}, *)$ *is commutative group.*
f *is an isomorphism if and only if* :
1.f *is a group homomorphism :*

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

$$f(xy) = 1 - \frac{1}{xy} ...(i).$$

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

$$f(x) * f(y) = 2 + 1 - \frac{1}{x} - 1 - \frac{1}{y} - 1 + \frac{1}{x} + \frac{1}{y} - \frac{1}{xy}$$

$$f(x) * f(y) = 1 - \frac{1}{xy} ...(ii).$$

$(i) = (ii)$ *then* f *is a group homomorphism.*
f *is bijective if and only if:* f *is injective (one to one) and surjective(onto):*
f *is one to one :* $\forall x, x' \in \mathbb{R}^*$, $f(x) = f(x') \Rightarrow x = x'.$

$$f(x) = f(x') \Rightarrow 1 - \frac{1}{x} = 1 - \frac{1}{x'} \Rightarrow x = x'.$$

f *is onto* $\forall y \in \mathbb{R} - \{1\}, \exists x \in \mathbb{R}^*, y = f(x).$

$$y = 1 - \frac{1}{x} \Rightarrow y - 1 = -\frac{1}{x} \Rightarrow x = \frac{1}{1 - y}.$$

So f *is bijective, then* f *is an isomorphisme.*
b) $f : E \to F$ *where* $E = \mathbb{R}^*, F = \mathbb{R} - \{1\}$, $Ker(f) = \{x \in \mathbb{R}^* / f(x) = e_F = 0\}$,

$$1 - \frac{1}{x} = 0 \Rightarrow \frac{x - 1}{x} \Rightarrow x = 1, \ Ker(f) = \{1\}.$$

Solution 4.6.24. *1. Show that* $x * y \in \mathbb{R} - \{1\}$ *by contraction :*
we suppose that $xy - x - y + 2 = 1$, *where* $x \neq 1$, *and* $y \neq 1$:

$$xy - x - y + 2 = 1 \Rightarrow x(y - 1) - y + 1 = 0$$

$$\Rightarrow (x - 1)(y - 1) = 0 \Rightarrow x = 1 \vee y = 1$$

contradiction, so $xy - x - y + 2 \neq 1$, *then* $x * y \in \mathbb{R} - \{1\}$, $*$ *is binary operation.*
$*$ *is commutative if and only if:* $\forall x, y \in \mathbb{R} - \{1\}, x * y = y * x$, *because addition and the product are*

commutative operations.
$*$ *is associative if and only if:* $\forall x,y,z \in \mathbb{R}-\{1\}, (x*y)*z = x*(y*z)$.

$$(x*y)*z = (xy-x-y+2)*z = xyz-xz-yz+2z+xy+x+y-2-z+2$$

$$(x*y)*z = xyz-xz-yz-xy+x+y+z \ldots (1)$$

$$x*(y*z) = x*(yz-y-z+2) = xyz-xy-xz+2x-yz+y+z-2-x+2$$

$$x*(y*z) = xyz-xz-yz-xy+x+y+z \ldots (2)$$

$(2) = (1)$, *thus* $*$ *is associative .*
$*$ *has a neutral element if and only if :* $\exists e \in \mathbb{R}-\{1\}, \forall x \in \mathbb{R}-\{1\},\ x*e = e*x = x$.
We observe that $*$ *is commutative, so we are going the resolve just the following equation:*

$$x*e = xe-x-e+2 = x \Rightarrow x(e-2)-(e-2) = 0 \Rightarrow (e-2)(x-1) = 0$$

Since $x \neq 1$, *so* $e = 2 \in \mathbb{R}-\{1\}$, *is a neutral element.*
Every element has an inverse element if and only if: $\forall x \in \mathbb{R}-\{1\}\ \exists x' \in \mathbb{R}-\{1\}$ *such that* $x*x' = x'*x = e = 2$ *We observe that* $*$ *is commutative, so we are going to resolve just the following equation:*

$$x*x' = xx'-x-x'+2 = 2 \Rightarrow x' = \frac{x}{x-1}.$$

Let us show that $x' \in \mathbb{R}-\{1\}$ *that mean* $x' \neq 1$, *by contraction, we suppose that* $x' = 1 \Rightarrow -1 = 0$, *then* $x' \in \mathbb{R}-\{1\}$.
Then $(\mathbb{R}-\{1\}, *)$ *is commutative group.*

Solution 4.6.25. *On* $\mathbb{R}$ *we define the binary operation* $\star$ *by :*

$$f\ \forall x,y \in \mathbb{R}, x \star y = \sqrt[3]{x^3+y^3}.$$

1. $(\mathbb{R}, \star)$ *is a commutative group* $\begin{cases} \star \text{is commutative} \\ \star \text{is associative} \\ \star \text{Existence of neutral element} \\ \text{Existence of en inverse element} \end{cases}$

$\star$ *is commutative if and only if:* $\forall x,y \in \mathbb{R}, x \star y = y \star x$.

$$x \star y = \sqrt[3]{x^3+y^3} = \sqrt[3]{y^3+x^3} = y \star x.$$

So $\star$ *is commutative.*
$\star$ *is associative if and only if :* $\forall x,y,z \in \mathbb{R}, (x \star y) \star z = x \star (y \star z)$.

$$\begin{aligned} (x \star y) \star z &= \left(\sqrt[3]{x^3+y^3}\right) \star z \\ &= \sqrt{(\sqrt[3]{x^3+y^3})^3+z^3} = \sqrt[3]{x^3+y^3+z^3} \ldots (1) \\ x \star (y \star z) &= x \star \left(\sqrt[3]{y^3+z^3}\right) \\ &= \sqrt[3]{x^3+(\sqrt[3]{y^3+z^3})^3} = \sqrt[3]{x^3+y^3+z^3} \ldots (2) \end{aligned}$$

$(1) = (2)$, *thus* $\star$ *is associative.*
$\star$ *has a neutral element if and only if:* $\exists e \in \mathbb{R},\ \forall x \in \mathbb{R},\ x \star e = e \star x = x$.
As $\star$ *is commutative we are going to resolve just the following equation :*

$$x \star e = \sqrt[3]{x^3+e^3} = x \Rightarrow x^3+e^3 = x^3 \Rightarrow e = 0 \in \mathbb{R}.$$

Every element has its symmetric element : $\forall x \in \mathbb{R}, \exists x^{-1} \in \mathbb{R} : x \star x^{-1} = x^{-1} \star x = e = 0$.
We observe that $*$ *is commutative, so we are going the resolve just to following equation :*

$$x \star x^{-1} = \sqrt[3]{x^3+(x^{-1})^3} = 0 \Rightarrow (x^{-1})^3 = -x^3 \Rightarrow x^{-1} = -x \in \mathbb{R}.$$

2. $H=\{-3,-2,-1,0,1,2,3\}$ *is a subgroup of* $(\mathbb{R},\star)$ *if and only if :* $\begin{cases} e=0\in H \\ \forall x,y\in H, x\star y\in H \\ \forall x\in H, x^{-1}\in H \end{cases}$

   Moreover : $0\in H, \forall x\in H, x^{-1}\in H$,
   $\exists x=1, y=3, x\star y=\sqrt[3]{1^3+3^3}\notin H$. *Then* H *isn't a subgroup of* $(\mathbb{R},\star)$.

3. f *is a map from* $\mathbb{R}$ *to* $\mathbb{R}$ *given by* $f f(x)=\sqrt[3]{x}$.
   f *is a group isomorphism from* $(\mathbb{R},+)$, *to* $(\mathbb{R},\star)$ *if and only if* f *is a group homomorphism and bijective:*
   f *a group homomorphism if and only if :*

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

$$f(x+y)=\sqrt[3]{x+y}.$$

$$f(x)\star f(y)=(\sqrt[3]{x})\star(\sqrt[3]{y})=\sqrt[3]{(\sqrt[3]{x})^3+(\sqrt[3]{y})^3}=\sqrt[3]{x+y}=f(x+y).$$

   f *is bijective if and only if* f *is injective and surjective:*
   f ***is injective*** *if and only if :* $\forall x,x'\in\mathbb{R}, f(x)=f(x')\Rightarrow x=x'$.

$$f(x)=f(x')\Rightarrow\sqrt[3]{x}=\sqrt[3]{x'}\Rightarrow x=x'.$$

   f ***is surjective*** *if and only if:* $\forall y\in\mathbb{R},\exists x\in\mathbb{R}, y=f(x)$.

$$y=\sqrt[3]{x}\Rightarrow x=y^3.$$

   Then f *is bijective, so* f *is an isomorphism.*

4. $\left[\text{Since } f \text{ is an isomorphism from the group } (\mathbb{R},+), \text{ to } (\mathbb{R},\star), \text{ and its bijection } f^{-1} \text{ is an isomorphism too from } (\mathbb{R},\star), \text{ to } (\mathbb{R},+)\right]$, $f^{-1}(y)=y^3$. *Then* $(\mathbb{R},\star)$ *is isomorphic to* $(\mathbb{R},+)$

Solution 4.6.26. *Let* G *be a group :*

1. *A map* $f:(G,.)\to(G,.)$ *given by :* $f(x)=x^{-1}$ *is a group homomorphism if and only if* G *is commutative.*
   a) We suppose that f *is a group homomorphism, so :*

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

$$\forall x,y\in G, xy=((xy)^{-1})^{-1}=(x^{-1}y^{-1})^{-1}=(y^{-1})^{-1}(x^{-1})^{-1}=yx.$$

   Because $(ab)^{-1}=b^{-1}a^{-1}$. *Then* G *is commutative.*
   We suppose that $(G,.)$ *is commutative, let us prove that* f *is homomorphism :*

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

2. *Let* $a\in G$ *show that the map* $f:(G,.)\to(G,.)$ *given by :* $f(x)=axa^{-1}$ *is an automorphism .*

$$f(xy)=axya^{-1}=axa^{-1}aya^{-1}=f(x)f(y), aa^{-1}=e$$

   Then f *is a homomorphism,* f *is bijective:*
   $\forall y\in G,\exists! x\in G : y=f(x)=axa^{-1}$, *since* $x=a^{-1}ya$ *is unique.*
   Other way:
   f *is injective(one to one)* $\forall x,x'\in G, f(x)=f(x')\Rightarrow x=x'$:
   $f(x)=f(x')\Rightarrow axa^{-1}=ax'a^{-1}\Rightarrow a^{-1}axa^{-1}=a^{-1}ax'a^{-1}a\Rightarrow x=x'$.
   f *is surjective(onto)* $\forall y\in G\exists x\in G : y=f(x)=axa^{-1}$, *Indeed,* $x=a^{-1}ya\in G$, *because* $(G,.)$ *is a group.*
   The kernel: $ker(f)=\{x\in G/f(x)=e_G\}=\{x\in G/axa^{-1}=e\}$, *so*

$$a^{-1}axa^{-1}a=a^{-1}ea\Rightarrow x=a^{-1}ea=a^{-1}ea=a^{-1}a=e$$

   $ker(f)=\{e\}$.
   Another way : since f *is bijective, then* $ker(f)=\{e'_G=e_G=e\}$.

3. *f is homomorphism if and only if :* $\forall x, y \in \mathbb{R}, f(x+y) = f(x).f(y)$.

$$f(x+y) = 2^{x+y} = 2^x.2^y = f(x)f(y).$$

$$Ker(f) = \{x \in \mathbb{R} / f(x) = 1\} = \{0\}.$$

so f is one to one because $Ker(f) = \{0\}$.

Solution 4.6.27. *Let us give the six elements of $(\mathscr{S}_3, \circ)$, the group table, $\mathscr{S}_3$ has $3! = 6$ elements :*

$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \mathscr{S}_3 = \{id, \tau_1, \tau_2, \tau_3, \sigma_1, \sigma_2\}.$$

$\tau_1 \circ \tau_2, \tau_2 \circ \tau_1$:

$$\tau_1 \circ \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_1 \neq \tau_2 \circ \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_2.$$

The group table is : $\mathscr{S}_3$:

$\circ$	id	τ_1	τ_2	τ_3	σ_1	σ_2
id	id	τ_1	τ_2	τ_3	σ_1	σ_2
τ_1	τ_1	id	σ_1	σ_2	τ_2	τ_3
τ_2	τ_2	σ_2	id	σ_1	τ_3	τ_1
τ_3	τ_3	σ_1	σ_2	id	τ_1	τ_2
σ_1	σ_1	τ_3	τ_1	τ_2	σ_2	id
σ_2	σ_2	τ_2	τ_3	τ_1	id	σ_1

Le cycle $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3)$ *has length* 3.

The inverse of $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *is* $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

The subgroup generated by σ is given by $H = \{id, \sigma, \sigma^{-1}\}$.

Solution 4.6.28. *$(\mathbb{Z}^2, \oplus, \odot)$ is a commutative ring if and only if :*

$$\begin{cases} (\mathbb{Z}^2, \oplus) & \text{is a commutative} \\ \odot & \text{is associative and distributive .} \\ \odot & \text{is commutative} \end{cases}$$

1. *$(\mathbb{Z}^2, \oplus)$ is commutative group:*

   a *$\oplus$ is commutative:*
   $\forall (x,y), (x',y') \in \mathbb{R}^2$,

   $$(x,y) \oplus (x',y') = (x+x', y+y') = (x'+x, y'+y) = (x',y') \oplus (x,y).$$

   b *$\oplus$ is associative:*
   $\forall (x,y), (x',y'), (x'',y'') \in \mathbb{R}^2$,
   $[(x,y) \oplus (x',y')] \oplus (x'',y'') = (x+x', y+y') \oplus (x'',y'') = (x+x'+x'', y+y'+y'')...(1)$
   $(x,y) \oplus [(x',y') \oplus (x'',y'')] = (x,y) \oplus (x'+x'', y'+y'') = (x+x'+x'', y+y'+y'')...(2).$
   $(1) = (2)$*, thus $\oplus$ is associative.*

   c *$\exists e = (e_1, e_2) \in \mathbb{Z}^2$ such that:*

   $$(e_1,e_2) \oplus (x,y) = (x,y) \oplus (e_1,e_2) = (x,y)$$

   We observe that $\oplus$ is commutative, so we are going to resolve just the following equation:

$$(x,y)\oplus(e_1,e_2)=(x,y)\Longrightarrow(x+e_1,y+e_2)=(x,y)$$

$$so\begin{cases}x+e_1=&x\\y+e_2=&y\end{cases}\Longrightarrow\begin{cases}e_1=&0\\e_2=&0\end{cases}\quad e=(0,0)\in\mathbb{Z}^2\ is\ the\ neutral\ element\ of\ \oplus.$$

d *Every element* $\mathbb{Z}^2$ *has its inverse element on* $\mathbb{Z}^2$, $\forall(x,y)\in\mathbb{Z}^2,\exists(x',y')\in\mathbb{Z}^2$:

$$(x,y)\oplus(x',y')=(0,0),(x',y')\oplus(x,y)=(0,0),$$

then $x'=-x,y'=-y$ *so* $(-x,-y)\in\mathbb{Z}^2$ *is the inverse element* $(x,y)\in\mathbb{Z}^2$.
Using ***a,b,c,d*** *we deduce that* $(\mathbb{Z}^2,\oplus)$ *is a commutative group.*

2.

- $\odot$ *is associative :* $\forall(x,y),(x',y'),(x",y")\in\mathbb{R}^2$,
  $[(x,y)\odot(x',y')]\odot(x",y")=(xx',xy'+yx')\odot(x",y")=(xx'x",xx'y"+xy'x"+yx'x")...(1)$
  $(x,y)\odot[(x',y')\odot(x",y")]=(x,y)\odot(x'x",x'y"+y'x")=(xx'x",xx'y"+xx"y'+yx'x")...(2).$*çç* $(1)=(2)$*, thus* $\odot$ *is associative.*
- $\odot$ *is distributive :* $\forall(x,y),(x',y'),(x",y")\in\mathbb{R}^2$,

$$(x,y)\odot[(x',y')\oplus(x",y")]=[(x,y)\odot(x',y')]\oplus[(x,y)\odot(x",y"],$$
$$[(x,y)\oplus(x',y')]\odot(x",y")=[(x,y)\odot(x",y")]\oplus[(x',y')\odot(x",y")].$$

Let us show that :

$$(x,y)\odot[(x',y')\oplus(x",y")]=[(x,y)\odot(x',y')]\oplus[(x,y)\odot(x",y"],$$

We have :

$$(x,y)\odot[(x',y')\oplus(x",y")]=(x,y)\odot[x'+x",y'+y"]$$

So

$$(x,y)\odot[(x',y')\oplus(x",y")]=(xx'+xx",xy'+xy"+yx'+yx")...(3)$$

$$[(x,y)\odot(x',y')]\oplus[(x,y)\odot(x",y"]=(xx',xy'+yx')\oplus(xx",xy"+yx").$$

Moreover

$$[(x,y)\odot(x',y')]\oplus[(x,y)\odot(x",y"]=(xx'+xx",xy'+yx'+xy"+yx")...(4)$$

Then $(3)=(4)$.
Let us show that :

$$[(x,y)\oplus(x',y')]\odot(x",y")=[(x,y)\odot(x",y")]\oplus[(x',y')\odot(x",y")].$$

We have that: $[(x,y)\oplus(x',y')]\odot(x",y")=(x+x',y+y')\odot(x",y")=(xx"+x'x,xy"+x'y"+yx"+y'x")...(5)$
$[(x,y)\odot(x",y")]\oplus[(x',y')\odot(x",y")]=(xx",xy"+yx")\oplus(x'x",x'y"+y'x"),\ [(x,y)\odot(x",y")]\oplus[(x',y')\odot(x",y")]=(xx"+x'x",xy"+yx"+x'y"+y'x")...(6).$
So $(5)=(6)$.

3. $\odot$ *is commutative:* $\forall(x,y),(x',y')\in\mathbb{R}^2$,

$$(x,y)\odot(x',y')=(xx',xy'+yx')...(7)$$

$$(x',y')\odot(x,y)=(x'x,x'y+y'x)=(xx',xy'+yx')..(8)=(7).$$

$(\mathbb{Z}^2,\oplus,\odot)$ *is a commutative ring.*
A is a sub-ring of $(\mathbb{Z}^2,\oplus,\odot)$ *if and only if :*

1. $\forall X,Y \in A, X \oplus Y^{-1} \in A$:
   $X,Y \in A, \exists a,a' \in \mathbb{Z}, X=(a,0), Y=(a',0)$, *so :*

$$X \oplus Y = X - Y = (a-a',0) \in A, \ \ because \ \ a-a' \in \mathbb{Z}.$$

2. $\forall X,Y \in A, X \odot Y \in A$:
   $X,Y \in A, \exists a,a' \in \mathbb{Z}, X=(a,0), Y=(a',0)$, *so :*

$$X \odot Y = XY = (aa',0) \in A, \ \ because \ \ aa' \in \mathbb{Z}.$$

3. $e_{\mathbb{Z}^2} = (0,0) \in A$ *It's clear that :* $0 \in \mathbb{Z}$,
   the neutral element of (a,b) *with respect the operation* $\odot$*:*
   $\exists (a,b) \in \mathbb{Z}^2, \forall (x,y) \in \mathbb{Z}^2, (x,y) \odot (a,b) = (a,b) \odot (x,y) = (x,y)$.
   $\begin{cases} xa = & x \\ xb + ya = & y \end{cases} \Longrightarrow \begin{cases} a = 1 \\ b = 0 \end{cases} \Rightarrow (a,b) = (1,0) \in \mathbb{Z}^2$. *We observe* $(1,0) \in A$.
   Then, $(A, \oplus, \odot)$ *is a sub-ring of* $(\mathbb{Z}^2, \oplus, \odot)$.

Solution 4.6.29. *Let* $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} / (a,b) \in \mathbb{Z}^2\}$

1. $\mathbb{Z}[\sqrt{5}]$ *is a sub-ring of* $(\mathbb{R}, +, .)$ *if and only if :*

   (a) $\forall x,y \in \mathbb{Z}[\sqrt{5}], x-y \in \mathbb{Z}[\sqrt{5}]$:
   $x,y \in \mathbb{Z}[\sqrt{5}], \exists a,b,a',b' \in \mathbb{Z}, x = a + b\sqrt{5}$ *et* $y = a' + b'\sqrt{5}$, *so :*

$$x - y = a + b\sqrt{5} - a' - b'\sqrt{5} = (a-a') + (b-b')\sqrt{5} \in \mathbb{Z}[\sqrt{5}].$$

   (b) *For each* $x,y \in \mathbb{Z}[\sqrt{5}]$, *we have* $xy \in \mathbb{Z}[\sqrt{5}]$.
   $x,y \in \mathbb{Z}[\sqrt{5}], \exists a,b,a',b' \in \mathbb{Z}, x = a + b\sqrt{5}$ *et* $y = a' + b'\sqrt{5}$, *so :*

$$x.y = (a + b\sqrt{5})(a' + b'\sqrt{5}) = (aa' + bb') + (ab' + a'b)\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$$

   (c) $0,1 \in \mathbb{Z}[\sqrt{5}]$:
   It's clear that : $0 = 0 + 0\sqrt{5} \in \mathbb{Z}[\sqrt{5}], 1 = 1 + 0\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$. *Then,* $(\mathbb{Z}[\sqrt{5}], +, .)$ *is a sub-ring of* $(\mathbb{R}, +, .)$.

2. *Let* $f : \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}[\sqrt{5}]$ *be a map defined by* $f(a + b\sqrt{5}) = a - b\sqrt{5}$. f *is an automorphisme de l'anneau* $(\mathbb{Z}[\sqrt{5}], +, .)$ *is* f *a ring homomorphisme and* f *is bijective:*
   f *is a ring homomorphism* $\mathbb{Z}[\sqrt{5}]$ *if and only if :*

   (a) $\forall x,y \in \mathbb{Z}[\sqrt{5}], f(x+y) = f(x) + f(y)$:

$$f(x+y) = f(a + b\sqrt{5} + a' + b'\sqrt{5}) = (a+a') - (b+b')\sqrt{5} = f(a + b\sqrt{5}) + f(a' + b'\sqrt{5}).$$

   (b) $\forall x,y \in, f(x.y) = f(x).f(y)$:

$$f(xy) = f((a + b\sqrt{5})(a +' b'\sqrt{5})) = f((aa' + bb') + (a'b + ab')\sqrt{5})$$

$$= (aa' + bb') - (a'b + ab')\sqrt{5} = f(a + b\sqrt{5}) f(a' + b'\sqrt{5}).$$

   (c) $f(1) = 1$.

   f *is bjective because for all* $a + b\sqrt{5}$ *thee exist* $a - b\sqrt{5}$. *So* f *is an automorphisme .*

Solution 4.6.30. 13 :
I. $\mathbb{Z}/2\mathbb{Z}, Z/5\mathbb{Z}$ *are fields because* $2,5$ *are prime numbers.*
II. a) $\mathbb{Z}/8\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}, \dot{6}, \dot{7}\}$

The inverse elements of $\mathbb{Z}/8\mathbb{Z}$ *are the element* k *such that* $k \wedge 8 = 1$ *then:*
$\dot{1}, \dot{3}, \dot{5}, \dot{7}.$
b)The zero divisors of $\mathbb{Z}/8\mathbb{Z}$ *are :* $\dot{2}, \dot{4}, \dot{6}$*, because*

$$\dot{4} \times \dot{2} = 0 = \dot{2} \times \dot{4} = \dot{0} = \dot{6} \times \dot{4}.$$

then $\mathbb{Z}/8\mathbb{Z}$ *isn't a field.*
III.$\mathbb{Z}/3\mathbb{Z}$ *is a field because* 3 *is a prime number ,* $Z/6\mathbb{Z}$ *isn't a field* 6 *isn't a prime number.*
IV.a)$\mathbb{Z}/10\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}, \dot{6}, \dot{7}, \dot{8}, \dot{9}\}$
The inverse elements of de $\mathbb{Z}/10\mathbb{Z}$ *are :* $\dot{1}, \dot{3}, \dot{7}, \dot{9}.$
b)The zero divisors of $\mathbb{Z}/10Z$ *are :* $\dot{2}, \dot{4}, \dot{5}, \dot{6}, \dot{8}$*, because*

$$\dot{2} \times \dot{5} = 0 = \dot{5} \times \dot{4} = \dot{0} = \dot{6} \times \dot{5} = 0 = \dot{8} \times \dot{5}.$$

Then $\mathbb{Z}/10\mathbb{Z}$ *isn't a field.*

Solution 4.6.31. *A finite integral domain is a field if it doesn't have a zero divisor, so:*
Let $a \in A - \{0_A\}$ *we define a group homomorphism* $f : (A, +) \to (A, +)$ *by* $= f(x) = ax$ *which is one to one because* $\ker(f) = \{0_A\}$*, since* A *is finite so* f *is bijective, then* 1_A *there exist an antecedent* $x \in A$ *such that* $ax = 1_A$ *by commutativity of* A, $xa = 1_A$, *so* a *admits an inverse, then* A *is a field.*

Solution 4.6.32. *1. Let us show that* $(\mathbb{R}, T)$ *is a commutative group:*
T *is commutative if and only if :*

$$\forall x, y \in \mathbb{R}, xTy = yTx,$$

since the addition is commutative operation.
T *is associative if and only if:*

$$\forall x, y, z \in \mathbb{R}, (xTy)Tz = xT(yTz)$$

$$(xTy)Tz = (x + y - 1)Tz = x + y - 1 + z - 1 = x + y + z - 2 ...(1)$$

$$xT(yTz) = xT(y + z - 1) = x + y + z - 1 - 1 = x + y + z - 2 ...(2)$$

$(2) = (1)$*, thus* T *is associative.*
T *has a neutral element if and only if:*

$$\exists e \in \mathbb{R}, \forall x \in \mathbb{R}, xTe = eTx = x.$$

Since T *is commutative so we are going to resolve just the following equation :*
$xTe = x + e - 1 = x \Rightarrow e = 1$ *is the neutral element.*
Every element has its inverse if and only if:

$$\forall x \in, \ \exists x' \in \mathbb{R}, \ xTx' = x'Tx = e = 1.$$

Since T *is commutative so we are going to resolve just the following equation :*
$xTx' = x + x' - 1 = 1 \Rightarrow x' = 2 - x \in \mathbb{R}$ *is the inverse element of* x.
2. Distributivity: $\forall x, y, z \in \mathbb{R}$, $x \star (yTz) = (x \star y)T(x \star z)$ *and* $(xTy) \star z = (x \star z)T(y \star z)$,

$$\begin{aligned} x \star (yTz) &= x \star (y + z - 1) = xy + xz - x - x - y - z + 1 + 2 + 1 - 1 \\ &= (xy - x - y + 2) + (xz - x - z + 2) - 1 = (xy - x - y + 2)T(xz - x - z + 2) \\ &= (x \star y)T(x \star z) \end{aligned}$$

$$\begin{aligned}(xTy)\star z &= (x+y-1)\star z = xz+yz-z-x-y+1-z+2+1-1\\ &= (xz-x-z+2)+(yz-z-y+2)-1\\ &= (x\star z)T(y\star z)\end{aligned}$$

3. Let us show that $(\mathbb{R}-\{1\},\star)$ *is group.*
$\star$ *is associative if and only if:*

$$\forall x,y,z\in\mathbb{R}-\{1\},(x\star y)\star z = x\star(y\star z)$$

$$\begin{aligned}(x\star y)\star z &= (xy-x-y+2)\star z\\ &= xyz-xz+yz-2z-xy+x+y-2-z+2\\ &= xyz-xy-xz-yz+x+y+z...(1)\\ x\star(y\star z) &= x\star(yz-y-zz+2)\\ &= xyz-xy-xz+2x-yz+y+z-2-x-2\\ &= xyz-xy-xz-yz+x+y+z...(2).\end{aligned}$$

$(2)=(1)$*, thus* $\star$ *is associative.*
$\star$ *is commutative if and only if :*

$$\forall x,y\in\mathbb{R}-\{1\},x\star y = y\star x,$$

since the addition is commutative operation.

$\star$ *has a neutral element if and only if:*

$$\exists e\in\mathbb{R}-\{1\},\forall x\in\mathbb{R}-\{1\},x\star e = e\star x = x$$

$$x\star e = xe-x-e+2 = e\star x = x\Rightarrow e(x-1)+2(1-x)=0\Rightarrow=0$$

Where $x\neq 1$*, so* $e=2\in\mathbb{R}-\{1\}$*, is a neutral element.*
Every element ha its inverse element if and only if: $\forall x\in\mathbb{R}-\{1\}\ \exists x'\in\mathbb{R}-\{1\}$ *such that*

$$x\star x' = x'\star x = e = 0$$

Since $\star$ *is commutative, we are going to resolve just the following equation :*
$x\star x' = xx'-x-x'+2 = 2\Rightarrow x' = \dfrac{x}{x-1}$ *, now let us prove that* $x'\in\mathbb{R}-\{1\}$ *that means* $x'\neq 1$*, by contradiction we suppose that* $x'=1\Rightarrow -1=0$*, then* $x'\in\mathbb{R}-\{1\}$ *.*
Then $(\mathbb{R}-\{1\},\star)$ *is a group.*
Since $\star$ *is commutative, so* $(\mathbb{R},T,\star)$ *is a commutative field.*

Chapter 5

Polynomial and Rational Functions

5.1 Polynomials ring

Let R be a commutative ring with unity it can be $\mathbb{R}$ or $\mathbb{C}$, X be an indeterminate.

Definition 5.1.1. *A polynomial in X over a ring R is an expression of the form :*

$$P(X) = \sum_{i=0}^{n} a_i x_i = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n.$$

Where $n \in \mathbb{N}, a_0, a_1, ..., a_n \in R$ they are called coefficients of P.
We denote by $R[X]$, the set of all polynomials in the indeterminate X with coefficients in R.
If $a_n \neq 0$ then the degree of P is n, we write $deg(P) = n$.
***A zero polynomial** is given by $P = 0 = 0 + 0.x + x.x^2 + ... + 0x^n, a_n = 0 \forall n$, the degree of P is undefined, but for convenience we say that $deg(0) = -\infty$.*
***A constant polynomial** is a polynomial with a single term $P = a_0 \in R$, $deg(P) = 0$.*
***A monic polynomial** or **unitary polynomial** of order n is a polynomial $P = x^n + a_(n-1)x^{n-1} + ... + a_1 x + a_0$ in which the coefficient of the highest order term is 1.*

Example 5.1.2. *1.* $P(X) = X3 + 2X - \sqrt{2}X + 1, R = \mathbb{R}$, $deg(P) = 3$.

2. $Q(X) = X^2 + iX + 1, R = \mathbb{C}$, $deg(P) = 2$.

3. $P(X) = 1, R = \mathbb{R}$, $deg(P) = 0$.

Two polynomials $P, Q \in A[X]$, $P(X) = a_0 + a_1 X + a_2 X + ... + a_n X^n, Q(X) = b_0 + b_1 X + b_2 X + ... + bnX^n$, are said to be equal if $\forall i, a_i = b_i$

5.2 Operations on Polynomials

5.2.1 Addition and product

Consider polynomials $P(X) = a_0 + a_1 X + a_2 X + ... + a_n X^n + ..., Q(X) = b_0 + b_1 X + b_2 X + ... + b_m X^m + ...$, over the ring R.
The sum $P + Q \in R[X]$ is defined by :

$$p(X) + Q(X) = (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + ... + (a_i + b_i)X^i + ...$$

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

Proposition 5.2.1. *$(R[X], +)$ is a commutative group.*

Let $P,Q \in R[X]$ such that:
$P(X) = a_0 + a_1X + a_2X + ... + a_nX^n, Q(X) = b_0 + b_1X + b_2X + ... + b_mX^m$.
The product $P.Q$ is defined by :

$$P(X) \times Q(X) = c_0 + c_1X + c_2X^2 + ... + c_{n+m}X^{n+m},$$

where $c_k = \sum_{i+j=k} a_ib_j, \forall k \in \{0,1,...,n+m\}$.
For example : $c_0 = \sum_{i+j=0} a_ib_j = a_0b_0, c_1 = \sum_{i+j=1} a_ib_j = a_0b_1 + a_1b_0,$
$c_2 = \sum_{i+j=2} a_ib_j = a_0b_2 + a_1b_1 + b_0a_2.$
Le $deg(P.Q) = deg(P) + deg(Q)$.

Let $\lambda \in A$, $\lambda P(X)$ is defined by:

$$\lambda P(X) = \lambda a_0 + \lambda a_1X + \lambda a_2X + ... + \lambda a_nX^n.$$

Example 5.2.2. *Let* $P(X) = X^2 + 2X - 5, Q(x) = 2X^3 + 5X^2 - 4X - 1$, *let us evaluate:* $P + Q, \frac{1}{2}P, PQ$.

$$P(X) + Q(X) = 2X^3 + 6X^2 - 2X - 6, \quad \frac{1}{2}P(X) = \frac{1}{2}X^2 + x - \frac{5}{2}$$

$$P(X)Q(X) = 2X^5 + (5+4)X^4 + (-4+10-10)X^3 + (-1-8-25)X^2 + (-2+20)X + 5$$
$$P(X)Q(X) = 2X^5 + 9X^4 - 4X^3 - 34X^2 + 18X + 5$$

5.2.2 Composition

Let $P,Q \in A[X]$:
1. If $P = 0$, then $P \circ Q = 0$.
2. If $P \neq 0, n \in \mathbb{N}, P(X) = a_0 + a_1X + a_2 + ... + a_nX^n$. Then

$$P \circ Q = a_0Q^0 + a_1Q + a_2Q^2 + ... + a_nQ^n, deg(P \circ Q) = deg(P)deg(Q).$$

Example 5.2.3. *Let* $P(X) = 2X^3 + X^2 + 2X - 5, Q(X) = 4X - 1$, *then*

$$(P \circ Q)(X) = P(Q(X)) = 2(4X-1)^3 + (4X-1)^2 + 2(4X-1) - 5.$$

Proposition 5.2.4. $(R[X], +, .)$ *is commutative ring with unity.*

Proof. 1. $(R[X], +)$ is a group:

a) The addition is a binary operation on $R[X]$, and it's associative and commutative.

b) 0 is a neutral element of $R[X]$.

c) Every $P \in R[X]$ has an inverse element $-P$ on $R[X]$.

2. The product is a binary operation on $R[X]$, and it's commutative and associative:

$$\forall P,Q,R \in R[X], (PQ)R = P(QR)$$

where $P(X)=a_0+a_1X+a_2X+...+a_nX^n, Q(X)=b_0+b_1X+b_2X+...+bmX^m$,

$$R(X)=c_0+c_1X+c_2X+...+c_rX^r$$

$$P(X)Q(X)=d_0+d_1X+d_2X^2+...+d_{n+m}X^{n+m},$$

$d_k=\sum_{i+j=k} a_ib_j, \forall k\in\{0,1,...,n+m\}$,

$$(P(X)Q(x))R(x)=f_0+f_1X+f_2X^2+...+f_{n+m+r}X^{n+m+r}, f_k=\sum_{i+j+l=k} a_ib_jd_l,$$

$\forall k\in\{0,1,...,n+m+r\}$

$$Q(X)R(X)=e_0+e_1X+e_2X^2+...+e_{n+m}X^{m+r},$$

$e_k=\sum_{j+l=k} b_jc_l, \forall k\in\{0,1,...,m+r\}$,

$$P(X)(Q(X)R(X))=h_0+h_1X+h_2X^2+...+h_{n+m+r},$$

$$h_k=\sum_{i+j+l=k} a_ib_jd_l, \forall k\in\{0,1,...,n+m+r\}$$

$(P(X)Q(X))R(X)=P(X)(Q(X)R(X))$ they have the same coefficients .

3. The distributive law is satisfied as well.
4. The ring R is with unity $e_R=1$. Then $(R[X],+,.)$ is a commutative ring with unity.

Proposition 5.2.5. *If R is an integral domain, then $(R[X],+,.)$ is an integral domain.*

Proof. :
If $P\neq 0$, and $Q\neq 0$, then $deg(PQ)=deq(P)+deg(Q)\neq -\infty$, so $PQ\neq 0$.

We denote by $\mathbb{K}$ the field $\mathbb{R}$ or $\mathbb{C}$.

5.2.3 Divisibility of polynomial over a field

Let $P,Q\in\mathbb{K}[X]$, we say that Q divides P or Q is divisor (factor) of P, if there exist $B\in A[X]$ such that $P=BQ$. Denoted by Q/P.

Example 5.2.6.

1. *Every element $a\in\mathbb{K}$ divides every polynomial P of $\mathbb{K}[X]$.*
2. *All polynomial divides a zero polynomial.*
3. *$x+1$ divides X^2-1.*
4. *$x-i$ divides X^2+1.*

Proposition 5.2.7. *Let P,Q and R are polynomials in $\mathbb{K}[X]$, the following proprieties hold:*

1. *$\forall P\in\mathbb{K}[X], P/P$.*
2. *P/Q, so $deg(P)\leq deg(Q)$.*
3. *If P/Q and Q/P so $\exists\alpha\in\mathbb{K}-\{0\}, P=\alpha Q$.*
4. *If P/Q and Q/R so P/R.*

Proof. 1. It's simple.

2. P/Q, so $\exists B \in \mathbb{K}[X]$ such that $Q = PB, deg(Q) = deg(P) + deg(B)$, so $deg(P) \leq deg(Q)$.

3. If P/Q, so $\exists B \in \mathbb{K}[X]$ such that $Q = PB$, and Q/P so $\exists B' \in \mathbb{K}[X]$ such that $P = B'Q$, then $P = B'BP$.
   If $P = 0$ so $Q = 0$. If else $P \neq 0$ so $B'B = 1$ then $deg(B) = deg(B') = 1$, Hence there exist $\alpha \in \mathbb{K} - \{0\}, P = \alpha Q$.

4. If P/Q then $\exists B \in \mathbb{K}[X]$ such that $Q = PB$, and Q/R so $\exists B' \in \mathbb{K}[X]$ such that $R = B'Q$, then $R = BB'P \Rightarrow P/R$.

Proposition 5.2.8. *Let P, Q and R, T are polynomials in $\mathbb{K}[X]$, the following proprieties hold:*

1. $\forall P \in A[X], P/Q \Rightarrow P/QR$
2. $P/Q \wedge P/R$, *then* $P/Q + R$.
3. *if* P/Q *and* R/T *then* PR/QT.
4. $\forall n \in \mathbb{N}^*$, P/Q *then* P^n/Q^n

5.2.4 Euclidean division over a field

Theorem 5.2.9. *Let $A \in \mathbb{K}[X], B \in \mathbb{K}[x] - \{0\}$, there exist $(Q, R) \in (R[X])^2$ such that :*

$$\begin{cases} A = BQ + R \\ deg(R) < deg(B) \end{cases}$$

The polynomial Q is called the quotient, the polynomial R is called the remainder.
When $R = 0$ that means B/A.

Example 5.2.10. *1.*

$$\begin{array}{rl|l} x^3 - x^2 - 4x + 4 & & x - 1 \\ \cline{3-3} -x^3 + x^2 & & x^2 - 4 \\ \cline{1-1} \quad -4x + 4 & & \\ \quad 4x - 4 & & \\ \cline{1-1} \quad 0 & & \end{array}$$

2.

$$\begin{array}{rl|l} x^4 + 2x^3 + 5x^2 + 3x + 1 & & x^2 + x + 1 \\ \cline{3-3} -x^4 - x^3 - x^2 & & x^2 + x + 3 \\ \cline{1-1} \quad x^3 + 4x^2 + 3x & & \\ \quad -x^3 - x^2 - x & & \\ \cline{1-1} \quad 3x^2 + 2x + 1 & & \\ \quad -3x^2 - 3x - 3 & & \\ \cline{1-1} \quad -x - 2 & & \end{array}$$

3.

$$\begin{array}{rr|l} x^4 & -1 & x-1 \\ \cline{3-3} -x^4+x^3 & & x^3+x^2+x+1 \\ \cline{1-1} x^3 & & \\ -x^3+x^2 & & \\ \cline{1-1} x^2 & & \\ -x^2+x & & \\ \cline{1-1} x-1 & & \\ -x+1 & & \\ \cline{1-1} 0 & & \end{array}$$

4.

$$\begin{array}{rr|l} x^2 & +4i & x+i \\ \cline{3-3} -x^2-ix & & x-i \\ \cline{1-1} -ix & +4i & \\ ix & +i^2 & \\ \cline{1-2} & (1i^2+4i) & \end{array}$$

obtained by the division according to the increasing degrees to order n of the polynomial

5.2.5 Division according to the increasing degrees

Theorem 5.2.11. *Let $\mathbb{K}$ be a commutative field, A et B be two polynomials of $\mathbb{K}[X]$ and $n \geq 0$ fixed integer. We suppose that $B(0) \neq 0$. Then there exist a unique (Q,S) satisfying the following condition :*

$A = BQ + X^{n+1}S$ and $\deg Q \leq n$.

The division according to the increasing degrees to order n of the polynomial A by the polynomial B. The method consist of writing the polynomials A,B to write the polynomials in increasing order, from the smallest order to the largest, then proceed with the division until you obtain the order requested, because this division does not stop.

Example 5.2.12. *1. We stop to the order 3:*

$$\begin{array}{r|l} 1+X & 1-X \\ \cline{2-2} -1+X & 1+2X+2X^2+2X^3 \\ \cline{1-1} 2X & \\ -2X+2X^2 & \\ \cline{1-1} 2X^2 & \\ -2X^2+2X^3 & \\ \cline{1-1} 2X^3 & \\ -2X^3+2X^4 & \\ \cline{1-1} 2X^4 & \end{array}$$

2. We stop to the order 2:

$$\begin{array}{r|l} 1+X^2+3X^3+X^4 & 1+X+X^2 \\ \cline{2-2} -1-X-X^2 & 1-X+X^2 \\ \cline{1-1} -X+3X^3+X^4 & \\ X+X^2+X^3 & \\ \cline{1-1} X^2+4X^3+X^4 & \\ -X^2-X^3-X^4 & \\ \cline{1-1} 3X^3 & \end{array}$$

GCD, LCM

Now we consider $\mathbb{K}$ as a commutative field.

Definition 5.2.13. ***GCD***
*Let $A,B \in \mathbb{K}[X]$, be two polynomials with $A \neq 0$ or $B \neq 0$. The greatest common divisor called **GCD** of two polynomials is a polynomial, of the highest possible degree, that is a factor of both the two polynomials A,B. This polynomial is unique and denoted by $gcd(A,B)$.*

Definition 5.2.14. ***LCM***
*Let $A,B \in \mathbb{K}[X]-\{0\}$, The least common multiple called **LCM** of two polynomials which is a multiple of A and B. This polynomial is unique and denoted by $lcm(A,B)=M$.*

Example 5.2.15.

1. $\boldsymbol{gcd}(X^2+3X+2, X^2-1) = pgcd((X+1)(X+2),(X-1)(X+1)) = X+1.$
2. $\boldsymbol{gcd}(X^2+X+1, X^2+2X+1) = 1.$
3. $\boldsymbol{lcm}(X(X+1)(X+2)^2,(X+1)^2(X^2+1)) = X(X+1)^2(X+2)^2(X^2+1).$
4. $\boldsymbol{lcm}(X^2+1, X^2-1) = X^4-1.$

Euclidean algorithm

Let $A,B \in \mathbb{K}[X], B \neq 0$. Repeated Euclidean division gives:

$$A = BQ_1 + R_1, deg(R_1) < deg(B)$$
$$B = R_1Q_2 + R_2, deg(R_2) < deg(R_1)$$
$$R_1 = R_2Q_3 + R_3, deg(R_3) < deg(R_2)$$
$$\dots$$
$$R_{k-2} = R_{k-1}Q_k + R_k, deg(R_k) < deg(R_{k-1}).$$
$$R_{k-1} = R_kQ_{k+1} + R_{k+} = R_kQ_{k+1}, R_{k+1} = 0.$$

We stop when the remainder is equal to zero R_{k+1}. Then the gcd is the last non-zero remainder: $gcd(A,B) = R_k$. Using the iterative division we can find U,V such that $pgcd(AB) = AU + BV$.

Example 5.2.16. 1. *Let $A = X^2+3X+2, B = X^2-1$ we have :*

$$X^2+3X+2 = (X^2-1)\underbrace{1}_{Q_1} + \underbrace{3X+3}_{R_1},$$
$$X^2-1 = (3x+3)\underbrace{\frac{1}{3}x}_{Q_2} + \underbrace{0}_{R_2}.$$

So the $gcd(A,B) = \frac{1}{3}R_1 = \frac{1}{3}(3X+3) = X+1$. The GCD is unitary polynomial.

2. *Let $A = X^2+X+1, B = X^2+2X+1$ we have :*

$$X^2+X+1 = (X^2+2X+1)\underbrace{1}_{Q_1} + \underbrace{(-X)}_{R_1},$$
$$X^2+2X+1 = (-X)\underbrace{(-X-2)}_{Q_2} + \underbrace{1}_{R_2}.$$
$$-X = 1.\underbrace{(-X)}_{Q_3} + \underbrace{0}_{R_3}.$$

So the $gcd(A,B) = R_2 = 1$.

3. *Let* $A = X^5 + X^4 - X^3 + X^2 + 4, B = X^3 + X^2 + 1$ *we have :*

$$\begin{aligned} X^5 + X^4 - X^3 + X^2 + 4 &= (X^3 + X^2 + 1) \cdot (X^2 - 1) + (X^2 + 5) \\ X^3 + X^2 + 1 &= (X^2 + 5) \cdot (X + 1) + (-5X - 4) \\ X^2 + 5 &= (-5X - 4) \cdot (-\tfrac{1}{5}X + \tfrac{4}{25}) + \tfrac{141}{25} \\ -5X - 4 &= \tfrac{141}{25} \cdot (-\tfrac{125}{141}X - \tfrac{100}{141}) + 0 \end{aligned}$$

So the $gcd(A,B) = \frac{25}{141}R_3 = 1$.

4. *Let* $A = 2X^4 - 3X^3 + 4X^2 - 3X + 2, B = X^3 + X^2 + X + 1$ *we have :*

$$\begin{aligned} 2X^4 - 3X^3 + 4X^2 - 3X + 2 &= (X^3 + X^2 + X + 1) \cdot (2X - 5) + (7X^2 + 7). \\ X^3 + X^2 + X + 1 &= (7X^2 + 7) \cdot (\tfrac{1}{7}X + \tfrac{1}{7}) + 0 \end{aligned}$$

So the $pgcd(A,B) = \frac{1}{7}R_1 = 1 + X^2$.

Prime polynomial

Definition 5.2.17. *Let* $A, B \in \mathbb{K}[X]$. *We say that* A *and* B ***are coprime*** *if* $gcd(A,B) = 1$.
We write $A \wedge B = 1$.

Theorem 5.2.18. *(**Bezout theorem**)*
Let $A, B \in \mathbb{K}[X]$ *two polynomials* $A \neq 0$ *or* $B \neq 0$. $D = gcd(A,B)$. *there exist* $U, V \in \mathbb{K}[X]$ *such that :* $AU + BV = D$

Example 5.2.19. *Let* $A = X^2 + 3X + 2, B = X^2 - 1$ *we have :*

$$\exists (U,V) = (\frac{1}{3}, -\frac{1}{3}) \ / \ A\frac{1}{3} + (-\frac{1}{3})B = X + 1.$$

Theorem 5.2.20. *Let* $A, B \in \mathbb{K}[X]$. A *and* B *are coprime if and only if there exist* $U, V \in \mathbb{K}[X]$ *such that:* $AU + BV = 1$.

Theorem 5.2.21. *Let* $A = X^2 + X + 1, B = X^2 + 2X + 1$ *so :*

$$\exists (U,V) = (X + 2, -X - 1) \ / \ A(X + 2) + B(-X - 1) = 1.$$

Corollary 5.2.22. *Let* $A, B, C \in \mathbb{K}[X]$ *with* $A \neq 0 \vee B \neq 0$.
If C/A *and* C/B *then* $C/pgcd(A,B)$.

Corollary 5.2.23. *Let* $A, B \in \mathbb{K}[X]$ *be non-zero and* $M = lcm(A,B)$. *If* $C \in \mathbb{K}[X]$ *satisfy* A/C *and* B/C, *then* M/C.

Lemma 5.2.24. *(**Gauss Lemma**)*
Let $A, B, C \in \mathbb{K}[X] - \{0\}$. *If* A/BC *and* $gcd(A,B) = 1$ *then* A/C.

5.2.6 Derivative polynomial and Taylor's formula.

Definition 5.2.25. *Let* $P \in R[X]$, *we denote by* P' *the derivative polynomial of* P *it's defined by :*

$$P'(X) = (a_0 + a_1X + a_2X^2 + ... + a_nX^n)' = a_1 + 2a_2X + ... + nX^{n-1}.$$

Proposition 5.2.26. *Let* $P, Q \in R[X], \lambda \in R$ *we have :*

1. $(P + \lambda Q)' = P' + \lambda Q'$.
2. $(PQ)' = P'Q + Q'P, (P^n)' = nP'P^{n-1}, n \in N^*$.
3. $(P \circ Q) = Q'(P \circ Q)'$.

Definition 5.2.27. *(**polynomial function**)*
For all $P = \sum_{n=0}^{N} a_n X^n \in \mathbb{K}[X]$, *we associated the function* $\tilde{P} : \mathbb{K} \to \mathbb{K}$ *defined by :*

$$\tilde{P}(x) = \sum_{n=0}^{N} a_n x^n.$$

$\tilde{P}$ *it is called a polynomial function.*

Proposition 5.2.28. *(**Leibniz's formula**)*
For every $P, Q \in \mathbb{K}[X], n \in \mathbb{N}$, *:*

$$(PQ)^{(n)} = \sum_{k=0}^{n} C_k^n P^{(k)} Q^{(n-k)}.$$

Proposition 5.2.29. *(**Taylor's formula**)*
For each $n \in \mathbb{N}, P \in \mathbb{K}[X], deg(P) \leq n, a \in \mathbb{K}$, *:*

$$P(X) = \sum_{k=0}^{n} \frac{\tilde{P}^{(k)}(a)}{n!}(x-a)^k.$$

5.3 Zeros of polynomials

Definition 5.3.1. *Let* $P \in \mathbb{K}[X], \alpha \in \mathbb{K}$. *We called* α *a zero (or root) of polynomial* P *if and only if* $p(\alpha) = 0$

Proposition 5.3.2.

$$P(\alpha) = 0 \Leftrightarrow (X - \alpha)/P.$$

Definition 5.3.3. *Let* $P \in \mathbb{K}[X] - \{0\}, \alpha$ *is a zero of* P *there exist* $n \in \mathbb{N}^n$ *such that* $(X-a)^n/P$. n *is called multiplicity of* α.
If $n = 1$, P *has a root of multiplicity* 1, *or a simple root.*
Si $n = 2$, P *has a root of multiplicity* 2
Si $n = 3$, P *has a root of multiplicity* 2

Proposition 5.3.4. *Let* $\alpha_0, \alpha_1, ..., \alpha_m$ *a distinct root of* $P \in \mathbb{K}[X]$ *and* $n_0, n_1, ..., n_m$, *their multiplicities respectively, then*

$$(X - \alpha_0)^{n_0}(X - \alpha_1)^{n_1}...(X - \alpha_m)^{a_m}/P.$$

Example 5.3.5.

1. $1, -1$ *are simple roots of the polynomial* $X^2 - 1$.
2. $i, -i$, *are simple roots of the polynomial* $X^2 + 1$.
3. 1 *is a root of multiplicity* 2 *of the polynomial* $X^2 - 2X + 1$.
4. 1 *is a root of multiplicity* 3 *of the polynomial* $X^3 + 3X^2 + 3X + 1$.

Theorem 5.3.6. *(**Alembert-Gauss**) Every non-constant polynomial with complex coefficients has at least one complex root.* $\mathbb{C}$ *an algebraically closed field.*

Definition 5.3.7. *(**Split polynomial**) A polynomial* $P \in \mathbb{K}[P]$ *is a split polynomial in* $\mathbb{K}$ *if and only if* $\lambda \in \mathbb{K} - \{0\}, n \in \mathbb{N}^*, a_1, .., a_n \in \mathbb{K}$ *such that :*

$$P = \lambda \Pi_{i=1}^{n}(X - a_i).$$

Proposition 5.3.8. *Every non-constant polynomial in* $\mathbb{C}[X]$ *is split in* $\mathbb{C}$.

5.4 Rational functions

5.4.1 Irreducible polynomials

Definition 5.4.1. *A non-constant polynomial $P \in \mathbb{K}[X]$ is irreducible over a field if P cannot be expressed as a product of two polynomials A and B in $\mathbb{K}[X]$, where the degrees of A and B are both smaller than the degree of P.*

Example 5.4.2.

1. *On $\mathbb{K} = \mathbb{C} : P(X) = X - 1$ is irreducible.*
2. *On $\mathbb{K} = \mathbb{R} : P(X) = X^2 + 1$ is irreducible.*
3. *On $\mathbb{K} = \mathbb{R} : P(x) = X^2 - X + 1$ is irreducible.*

Lemma 5.4.3. *Met $P \in \mathbb{K}[X]$ be an irreducible polynomial and $A, B \in \mathbb{K}[X]$. If P/AB then P/A or P/B..*

Theorem 5.4.4. *Every non-constant polynomial $A \in \mathbb{K}[X]$ can write as the product of monic and irreducible polynomials :*

$$A = \lambda P_1^{k_1} P_2^{k_2} ... P_r^{k_r}.$$

where $\lambda \in \mathbb{K}^*, r \in \mathbb{N}^*, k_i \in \mathbb{N}^*$ and P_i are distinct irreducible polynomials.

Theorem 5.4.5. *The irreducible polynomials in $\mathbb{C}[X]$ are polynomials of degree 1. Then $P \in \mathbb{C}[X]$ of degree $n > 1$ is given by :*

$$P = \lambda (X - \alpha_1)^{k_1} (X - \alpha_2)^{k_2} .... (X - \alpha_r)^{k_r}$$

Where $\alpha_1, ..., \alpha_r$ are distinct root of P and $k_1, ..., k_r$ are their multiplicities respectively.

Example 5.4.6.

1. $P(X) = X^2 + 1 = (X - i)(X + i)$ *here* $(X - i), (X + i)$ *are irreducible polynomials.*
2. $P(X) = X^3 + 2X^2 + 4X + 3 = (X + 1)\left(X + \frac{1 + i\sqrt{11}}{2}\right)\left(X + \frac{1 - i\sqrt{11}}{2}\right)$, *here* $(X + 1), \left(X + \frac{1 + i\sqrt{11}}{2}\right), \left(X + \frac{1 - i\sqrt{11}}{2}\right)$ *are irreducible polynomials.*
3. $P(X) = X^4 + 3X^3 + 4X^2 + 3X + 1 = (X + 1)^2\left(X + \frac{1 + i\sqrt{3}}{2}\right)\left(X + \frac{1 - i\sqrt{3}}{2}\right)$, *here* $(X + 1)^2, \left(X + \frac{1 + i\sqrt{3}}{2}\right), \left(X + \frac{1 - i\sqrt{3}}{2}\right)$ *are irreducible polynomials.*
4. $X^4 - 1 = (X^2 - 1)(X^2 + 1) = (X^2 - 1)(X^2 + 1) = (X - 1)(X + 1)(X + i)(X - i)$, *here* $(X - 1), (X + 1), (X + i), (X - i)$ *are irreducible polynomials.*

Theorem 5.4.7. *The irreducible polynomials in $\mathbb{R}[X]$ are polynomials of degree 1, and polynomials of degree 2 that haven't roots ($\Delta < 0$). Then $P \in \mathbb{R}[X]$ of degree $n > 1$ is given*

$$P = \lambda (X - \alpha_1)^{k_1} (X - \alpha_2)^{k_2} .... (X - \alpha_r)^{k_r} Q_1^{l_1} ... Q_s^{l_s}.$$

Where $\alpha_1, ..., \alpha_r$ are real distinct roots of P and $k_1, ..., k_r$ are their multiplicities, respectively, Q_i are polynomials of degree 2 with $\delta < 0$.

Example 5.4.8.

1. $P(X) = X^2 + 3X + 2 = (X + 2)(X + 1)$.
2. $Q(X) = X^2 + 2X + 1 = (X + 1)^2$.
3. $P(X) = X^2 + 1$

4. $P(X) = X^4 + 3X^3 + 4X^2 + 3X + 1 = (X+1)^2(X^2+X+1)$

5. $X^4 - 1 = (X^2-1)(X^2+1) = (X^2-1)(X^2+1) = (X-1)(X+1)(X^2+1)$

5.4.2 Rational Fractions

Definition 5.4.9. *A rational fraction with coefficient on $\mathbb{K}$ is expression given by :*

$$F = \frac{P}{Q}, \text{ où } P, Q \in \mathbb{K}[X],\ \mathbb{Q} \neq 0.$$

Example 5.4.10.

$$\frac{X+1}{X^2+3X+1}$$

Rational fraction operations:
Let $(P,Q),(R,S) \in K[X] \times \mathbb{K}[X] - \{0\}, \lambda \in \mathbb{K}$, then we have :

1. $\lambda \frac{P}{Q} = \frac{\lambda P}{Q}$.
2. $\frac{P}{Q} + \frac{R}{S} = \frac{PS+RQ}{QS}$.
3. $\frac{P}{Q}.\frac{R}{S} = \frac{PR}{QS}$.
4. $F = \frac{P}{Q}$, then $F' = \frac{P'Q - Q'P}{Q^2}$.

Definition 5.4.11. *(**Degree**)*
Let $(P,Q) \in \mathbb{K}[X] \times \mathbb{K}[X] - \{0\}, F = \frac{P}{Q}$, the degree of F is defined by :

$$deg(F) = deg(P) - deg(Q).$$

Lemma 5.4.12. *Let $(P,Q) \in \mathbb{K}[X] \times \mathbb{K}[X] - \{0\}, F = \frac{P}{Q}$ on $\mathbb{K}[X]$, so $\exists!(E,R) \in (\mathbb{K}[X])^2$ such that*

$$F = E + \frac{R}{Q}, deg(R) < deg(Q).$$

If $P \wedge Q = 1$, then $R \wedge Q = 1$.

Remark 5.4.13. *If $E = 0$ then $deg(P) < deg(Q.)$*

Example 5.4.14. *1.*

$$\frac{X^3 - X^2 - 4X + 4}{X-1} = X^2 - 4 + \frac{0}{X-1}.$$

2.

$$\frac{X^4 + 2X^3 + 5X^2 + 3X + 1}{X^2+X+1} = X^2 + X + 3 + \frac{-X-2}{X^2+X+1}.$$

3.

$$\frac{X^4-1}{X^5-1} = 0 + \frac{X^4-1}{X^5-1}.$$

5.5 Partial fractional decomposition

Theorem 5.5.1. *(**Partial fractional decomposition over** $\mathbb{R}$).*
Let $F = \frac{P}{Q}$ *be a rational fraction with* $P, Q \in \mathbb{R}[X], pgcd(P,Q) = 1$. *Then* F *is given by the unique expression as :*

$$P = E(X) + \frac{a_i}{(X-\alpha_i)^{k_i}} + \frac{b_i X + ci}{(X^2+bX+c)^{h_i}}.$$

Where $X - \alpha_i$ *and* $X^2 + bX + c$ *are irreducible factors of* $Q(X)$ *and exponents* k_i, h_i *are the multiplicities.*

Example 5.5.2. *1.* $F_1 = \frac{1}{X^2 - X - 2} = \frac{1}{(X+1)(X-2)}, \Delta \geq 0.$

The partial fraction decomposition is given by :

$$\frac{1}{(X+1)(X-2)} = \frac{a}{X+1} + \frac{b}{X-2}.$$

Now let us determine a, b *:*
To find $\boldsymbol{a}$, *we multiply each side by* $(X+1)$, *so we get :*

$$\frac{1}{(X-2)} = a + \frac{b(X+1)}{X-2}.$$

we tend $x \to -1$ *so*

$$\frac{-1}{3} = a.$$

To get the valued of $\boldsymbol{b}$, *we multiply each side by* $(X-2)$, *so we get :*

$$\frac{1}{(X+1)} = \frac{a(X-2)}{X+1} + b.$$

We tend $x \to 2$ *so*

$$\frac{1}{3} = b.$$

(Or by identification)

$$\frac{1}{(X+1)(X-2)} = \frac{a}{X+1} + \frac{b}{x-2} = \frac{X(a+b)+b-2a}{(X+1)(X-2)}.$$

$$\begin{cases} a+b=0, \\ b-2a=1 \end{cases} \Rightarrow 3a = -1, a = -1/3, b = 1/3.$$

$$F_1 = \frac{\frac{-1}{3}}{X+1} + \frac{\frac{1}{3}}{X-2},$$

2. $F_2 = \frac{X^2 - 2X - 5}{X^3 + 2X^2 - X - 2}$, *we observe that* 1 *is a root denominator, using Euclidean division we get :*

$$\begin{array}{r|l} X^3+2X^2-X-2 & X-1 \\ \cline{2-2} -X^3+X^2 & X^2+3X+2 \\ \cline{1-1} 3X^2-X & \\ -3X^2+3X & \\ \cline{1-1} 2X-2 & \\ -2X+2 & \\ \cline{1-1} 0 & \end{array}.$$

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

Then the partial fraction decomposition of F_2 is given by : :

$$\frac{X^2-2X-5}{(X+1)(X-1)(X+2)}=\frac{a}{X+1}+\frac{b}{X-1}+\frac{c}{X+2}.$$

Let us determine a,b,c :

$$a=\lim_{X\to -1}\frac{X^2-2X-5}{(X-1)(X+2)}=1$$

$$b=\lim_{X\to 1}\frac{X^2-2X-5}{(X+1)(X+2)}=-1$$

$$c=\lim_{X\to -2}\frac{X^2-2X-5}{(X+1)(X-1)}=1$$

$$F_2=\frac{X^2-2X-5}{(X+1)(X-1)(X+2)}=\frac{-1}{X+1}+\frac{1}{X-1}+\frac{1}{X+2}.$$

3. $F_3=\dfrac{1}{(X+1)^2(X-1)}$. *The partial fraction decomposition is given by :*

$$\frac{1}{(X+1)^2(X-1)}=\frac{a}{(X+1)}+\frac{b}{(X+1)^2}+\frac{c}{(X-1)}$$

Let us determine b,c using the limit method:

$$c=\lim_{X\to 1}\frac{1}{(X+1)^2},b=\lim_{X\to -1}\frac{1}{1-X},$$

But it does not work for finding $\boldsymbol{a}$*, so we select* $X=0$*, we obtained:*

$$-1=a+b-c\Rightarrow a=-1-b+c=-1+\frac{1}{2}+\frac{1}{4}$$

$$a=-\frac{1}{4},b=-\frac{1}{2},c=\frac{1}{4}.$$

$$F_3=\frac{1}{(X+1)^2(X-1)}=\frac{-\frac{1}{4}}{(X+1)}+\frac{-\frac{1}{2}}{(X+1)^2}+\frac{\frac{1}{4}}{(X-1)}.$$

4. $F_4=\dfrac{X^4+1}{X^3+X}$. *The Euclidean division give :* $X^4+1=X(X^3+X)+(1-X^2)$, *so* $F_4=X+\underbrace{\dfrac{1-X^2}{X^3+X}}_{F}$.

Since $\Delta<0, x^2+1$. *The partial fraction decomposition of F is given by :*

$$F=\frac{1-X^2}{X(X^2+1)}=\frac{a}{X}+\frac{bX+c}{X^2+1}.$$

Let us determine a,b,c :

$a=\lim_{x\to 0}\dfrac{1-X^2}{(X^2+1)}=1.$

For b,c *we set two valued of x such that* $F(x)$ *is well-defined*

$$\begin{cases}\text{For } x=1, \text{ we get}: & 0=1+\frac{b+c}{2}\\ \wedge & \\ \text{For } x=-1, \text{ we get}: & 0=-1+\frac{-b+c}{2}\end{cases}\Rightarrow b=-2,c=0.$$

$$F_4=X+\frac{1}{X}-\frac{2}{X^2+1}.$$

5. $F_5 = \dfrac{1}{X(X^2+X+1)}$, *the partial fraction decomposition of* F_5 *is given by :*

$$F_5 = \frac{1}{X(X^2+X+1)} = \frac{a}{X} + \frac{bX+c}{X^2+X+1}.$$

$a = \lim_{x\to 0} \dfrac{1}{X^2+X+1} = 1.$

To determine $\boldsymbol{b}$, *we multiply each side by* X, *we get*

$$\frac{X}{X^2+X+1} = a + \frac{X(bX+c)}{X^2+X+1}.$$

We tend $X \to \infty$, *then* $b = -a = -1$.

To determine $\boldsymbol{c}$ *we set* $X = 1$ *so* $c = -1$.

$$F_5 = \frac{1}{X} - \frac{X+1}{X^2+X+1}$$

Theorem 5.5.3. ***(Partial fractional decomposition over*** $\mathbb{C}$*).*
Let $F = \dfrac{P}{Q}$ *be a rational fraction* $P, Q \in \mathbb{C}[X], gcd(P,Q) = 1$. *Let* $\alpha_1, \alpha_2, ..., \alpha_p \in \mathbb{C}$ *are roots of* Q, *and* $k_1, k_2, ..., k_p$, *are their multiplicities respectively,* $Q = (X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}...(X-\alpha_p)^{k_p}$. *Then* F *is given by unique expression as :*

$$F = E + \frac{a_1}{X-\alpha_1} + \frac{a_2}{(X-\alpha_1)^2} + ... + \frac{a_k}{(X-\alpha_1)^{k_1}} + \frac{b_1}{X-\alpha_2} + \frac{b_2}{(X-\alpha_2)^2} + ... + \frac{a_1}{(X-\alpha_2)^{k_2}}$$
$$+ ... + \frac{z_1}{X-\alpha_p} + \frac{z_2}{(X-\alpha_p)^2} + ... + \frac{z_k}{(X-\alpha_p)^{k_p}}.$$

Example 5.5.4.

1. $F_1 = \dfrac{X^3+X^2+X+2}{X^2+1}$, *we start by Euclidean division, and we get :*

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

so

$$F_1 = 1 + X + \frac{1}{1+X^2} = 1 + X + \frac{1}{(X+i)(X-i)}$$

The partial fractional decomposition is given by:

$$F = \frac{1}{(X+i)(X-i)} = \frac{a}{X+i} + \frac{b}{X-i}$$

We use the same method to determine the constant a, b *:*

$$a = \lim_{x\to -i} \frac{1}{X-i} = \frac{i}{2}, b = \lim_{x\to i} \frac{1}{X+i} = -\frac{i}{2}.$$

$$F = \frac{\frac{i}{2}}{X+i} + \frac{\frac{-i}{2}}{X-i}.$$

$$F_1 = 1 + X + \frac{\frac{i}{2}}{X+i} + \frac{\frac{-i}{2}}{X-i}.$$

2.
$$F_2 = \frac{1}{X(X^2+X+1)} = \frac{1}{X\left(X+\frac{1+i\sqrt{3}}{2}\right)\left(X+\frac{1-i\sqrt{3}}{2}\right)}.$$

The partial fractional decomposition is given by :

$$F_2 = \frac{1}{X\left(X+\frac{1+i\sqrt{3}}{2}\right)\left(X+\frac{1-i\sqrt{3}}{2}\right)} = \frac{a}{X} + \frac{b}{X+\frac{1+i\sqrt{3}}{2}} + \frac{c}{X+\frac{1-i\sqrt{3}}{2}}$$

$$F_2 = \frac{1}{X\left(X+\frac{1+i\sqrt{3}}{2}\right)\left(X+\frac{1-i\sqrt{3}}{2}\right)} = \frac{1}{X} + \frac{\frac{-3+i\sqrt{3}}{2}}{X+\frac{1+i\sqrt{3}}{2}} + \frac{\frac{-3-i\sqrt{3}}{2}}{X+\frac{1-i\sqrt{3}}{2}}$$

3.
$$F_3 = \frac{4X^2+4X+4}{(X^2+1)^2} = \frac{4X^2+4X+4}{(X+i)^2(X-i)^2}.$$

The partial fractional decomposition is given by:

$$F_3 = \frac{4X^2+4X+4}{(X+i)^2(X-i)^2} = \frac{a}{X+i} + \frac{b}{(X+i)^2} + \frac{c}{X-i} + \frac{d}{(X-i)^2}.$$

$$F_3 = \frac{4X^2+4X+4}{(X+i)^2(X-i)^2} = \frac{2i}{X+i} + \frac{i}{(X+i)^2} - \frac{2i}{X-i} - \frac{i}{(X-i)^2}.$$

4. $A_1 = \dfrac{X}{X^4+1} = \dfrac{X}{(X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)},$

On $\mathbb{R}$ the partial fractional decomposition is given by:

$$A_1 = \frac{aX+b}{(X^2+\sqrt{2}X+1)} + \frac{cX+d}{(X^2-\sqrt{2}X+1)}$$

$$A_1 = \frac{\frac{-\sqrt{2}}{4}}{(X^2+\sqrt{2}X+1)} + \frac{\frac{\sqrt{2}}{4}}{(X^2-\sqrt{2}X+1)}$$

On $\mathbb{C}$ the partial fractional decomposition is given by:

$$A_1 = \frac{a}{X-\frac{\sqrt{2}(1+i)}{2}} + \frac{b}{X-\frac{\sqrt{2}(1-i)}{2}} + \frac{c}{X+\frac{\sqrt{2}(1+i)}{2}} + \frac{d}{X+\frac{\sqrt{2}(1-i)}{2}}.$$

We have also :

$$A_1 = \frac{X}{X^4+1} = \frac{a}{X-e^{\frac{i\pi}{4}}} + \frac{b}{X-e^{\frac{3i\pi}{4}}} + \frac{c}{X-e^{\frac{i5\pi}{4}}} + \frac{d}{X-e^{\frac{i7\pi}{4}}}.$$

Since $e^{\frac{i5\pi}{4}} = e^{-\frac{i\pi}{4}}, e^{\frac{i7\pi}{4}} = e^{-\frac{i3\pi}{4}}$. *Then*

$$A_1 = \frac{X}{X^4+1} = \frac{-i\frac{1}{4}}{X-e^{\frac{i\pi}{4}}} + \frac{i\frac{1}{4}}{X-e^{\frac{3i\pi}{4}}} + \frac{-i\frac{1}{4}}{X-e^{-\frac{i\pi}{4}}} + \frac{i\frac{1}{4}}{X-e^{-\frac{i3\pi}{4}}}.$$

5.6 Solved Exercises

5.6.1 Exercises

Exercise 5.6.1. *Find the quotient and the remainder of the following divisions using Euclidean division, Divide A by B:*

1. $A = X^5 + X^3 - X + 1$, $B = X^2 - X - 2$.
2. $A = X^3 + 4X^2 + 5X + 2$, $B = X^2 + 2X + 1$.
3. $A = X^3 + X^2 + X + 1$,$B = X + 1$.
4. $A = X^9 + X^6 + X^3 + 1$, $B = X^3 + 1$.

Exercise 5.6.2. *Find the quotient and the remainder of the following divisions according to the increasing degrees :*

1. $A = X^3 - X + 1$, $B = X^2 + X + 1$ *stop to degree* 2.
2. $A = X^2 + 1$, $B = X + 1$ *stop to degree* 3.

Exercise 5.6.3. *Determine the gcd=D, and find U and V such that* $AU + BV = D$.

1. $A = X^3 - X^2 - X + 1$, $B = X^2 - 3X + 2$.
2. $A = X^4 + 2X^3 + 2X^2 + 2X + 1$, $B = 2X^3 + 3X^2 + 2X + 2$.
3. $A = X^6 + 1$, $B = X^2 + 1$.
4. $A = X^6 - 1$, $B = X^2 - 1$.

Exercise 5.6.4. *For which values of* $a \in \mathbb{R}$ *the polynomial* $(X+1)^7 - X^7 - a$ *admits a real root of multiplicity* 2*?*

Exercise 5.6.5. *Let* $P = X^4 + 2X^3 + 2X^2 + 2X + 1$.
a) Determine $GCD(P, P')$.
b) Factorize P over $\mathbb{R}[X]$.

Exercise 5.6.6. *Factorize the following polynomials over* $\mathbb{R}[X]$ *and* $\mathbb{C}[X]$ *:*

1. $X^3 + X^2 + X + 1$.
2. $X^4 - 1$.
3. $X^4 + 1$.
4. $X^6 - 1$.
5. $X^6 + 1$.
6. $X^9 + X^6 + X^3 + 1$.

Exercise 5.6.7. *Decompose the following rational fraction over* $\mathbb{R}[X]$ *:*

1. $\dfrac{1}{X^2-X-2}$.
2. $\dfrac{X^2+1}{X^3+4X^2+5X+2}$.
3. $\dfrac{X^2+1}{(X^2-3X+2)(X+2)}$.
4. $\dfrac{X^2+X+1}{X^2(X+1)^2}$.

Exercise 5.6.8. *Decompose the following rational fraction over* $\mathbb{R}[X], \mathbb{C}[X]$ *:*

1. $\dfrac{X+2}{X^4-1}$.
2. $\dfrac{6}{(X^2+1)(X^2+4)}$.
3. $\dfrac{-4}{X^4+1}$.
4. $\dfrac{1+2X^2}{(X+1)(X^2+1)^2}$.

Exercise 5.6.9. *Let* $P(x)=x^4+6x^3+13x^2+12x+4, Q(x)=x^3+3x^2+3x+1$.

1. *Determine* $GCD(P,Q)$.
2. *Factorize* $P(x)$.
3. *Decompose* $F=\dfrac{2x+3}{(x+1)^2(x+2)^2}$ *over* $\mathbb{R}$.

5.6.2 Solutions

Solution 5.6.10. 1.

$$\begin{array}{rrrrr|l}
X^5 & & +X^3 & -X & +1 & X^2-X-2 \\
\cline{6-6}
-X^5 & +X^4 & +2X^3 & & & X^3+X^2+4X+6 \\
\cline{1-3}
 & X^4 & +3X^3 & & & \\
 & -X^4 & +X^3 & +2X^2 & & \\
\cline{2-4}
 & & 4X^3 & +2X^2 & -X & \\
 & & -4X^3 & +4X^2 & +8X & \\
\cline{3-5}
 & & & 6X^2 & +7X & +1 \\
 & & & -6X^2 & +6X & +12 \\
\cline{4-5}
 & & & & 13X & +13
\end{array}$$

$$X^5+X^3-X+1=(X^3+X^2+4X+6)(X^2-X-2)+13(X+1).$$

2.

$$\begin{array}{rrrr|l}
X^3 & +4X^2 & +5X & +2 & X^2+2X+1 \\
\cline{5-5}
-X^3 & -2X^2 & -X & & X+2 \\
\cline{1-3}
 & 2X^2 & +4X & +2 & \\
 & -2X^2 & -4X & -2 & \\
\cline{2-4}
 & & 0 & &
\end{array}$$

$$X^3+4X^2+5X+2=(X+2)(X^2+2X+1).$$

3. $X^3+X^2+X+1 \mid X+1$
$-X^3-X^2 \quad\quad\quad\quad \mid X^2+1$
$X+1$
$-X-1$
0

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

4. $X^9+X^6+X^3+1 \mid X^3+1$
$-X^9-X^6 \quad\quad\quad\quad \mid X^6+1$
X^3+1
$-X^3-1$
0

$$X^9+X^6+X^3+1=(X^3+1)(X^6+1)$$

Solution 5.6.11.

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

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

Solution 5.6.12.

1. $gcd(X^3-X^2-X+1, X^2-3X+2)$:
$A=X^3-X^2-X+1=(X^2-3X+2)\underbrace{(X+2)}_{Q_1}+\underbrace{(3x-3)}_{R_1}.$
$B=X^2-3X+2=(3x-3)\underbrace{(\frac{1}{3}X-\frac{2}{3})}_{Q_2}+\underbrace{0}_{R_2}.$
Then the $gcd(A,B)=\frac{1}{3}R_1=\frac{1}{3}(3X-3)=X-1$. *Since* $A=BQ_1+3D \Rightarrow D=\frac{1}{3}A-\frac{1}{3}BQ_1$, *so*

$$U=\frac{1}{3}, V=\frac{1}{3}X-\frac{2}{3}.$$

2. $gcd(X^4+2X^3+2X^2+2X+1, 2X^3+3X^2+2X+2)$:
$A=X^4+2X^3+2X^2+2X+1$
$A=(2X^3+3X^2+2X+2)\underbrace{(\frac{1}{2}X+\frac{1}{4})}_{Q_1}+\underbrace{(\frac{1}{4}X^2+\frac{1}{2}X+\frac{1}{2})}_{R_1}.$
$B=2X^3+3X^2+2X+2=(\frac{1}{4}X^2+\frac{1}{2}X+\frac{1}{2})\underbrace{(8X-4)}_{Q_2}+\underbrace{4}_{R_2}.$

$$R_1=(\frac{1}{4}X^2+\frac{1}{2}X+\frac{1}{2})(\frac{1}{16}X^2+\frac{1}{8}X+\frac{1}{8})+0.$$

Then the $gcd(A,B) = \frac{1}{4}R_2 = 1$. *Since*

$$A = BQ_1 + R_1 \Rightarrow Q_2A = BQ_1Q_2 + Q_2R_1$$

$\Rightarrow Q_2A = BQ_1Q_2 + B - R_2 \Rightarrow R_2 = 4 = -Q_2A - (Q_1Q_2 + 1)$ *so*

$$U = \frac{1}{4}Q_2 = -2X + 1, V = X^2.$$

3. $A = B(X^4 - X^2 + 1) + 0$, *then* $gcd(X^6 + 1, X^2 + 1) = X^2 + 1$, $U = 0, V = 1$.
4. $A = B(X^4 + X^2 + 1) + 0$, *then* $gcd(X^6 - 1, X^2 - 1) = X^2 - 1$, $U = 0, V = 1$.

Solution 5.6.13. *Let* $P(X) = (X+1)^7 - X^7 - a$ *has a root* $x \in \mathbb{R}$ *of multiplicity* 2, *if and only if* $P(X) = 0$ *and* $P'(X) = 0$ *:*

$$P(X) = P'(X) = 0 \Rightarrow \begin{cases} (X+1)^7 - X^7 - a = 0 \\ 7(X+1)^6 - 7X^6 = 0 \end{cases} \Rightarrow \begin{cases} (X+1)^6 - X^7 - a = 0 \\ (X+1)^6 = X^6 \end{cases}$$

So

$$\begin{cases} (X+1-X)X^6 - a = 0 \\ (X+1)^3 = \pm X^3 \end{cases} \Rightarrow \begin{cases} X^6 = a \\ X+1 = \pm X \end{cases}.$$

Then P *admits a zero* $X = -\frac{1}{2}$, *of multiplicity* 2 *for* $a = \frac{1}{(-2)^6}$.

Solution 5.6.14. *Let* $P = X^4 + 2X^3 + 2X^2 + 2X + 1$.
a) Determine $GCD(P, P')$*:* $P = P'(\frac{1}{4}X + \frac{1}{8}) + \frac{1}{4}X^2 + X + \frac{3}{4}$.

$$P' = R_1(16X - 40) + (32X + 32).$$

$R_1 = R_2(\frac{1}{128}X + \frac{3}{128}) + 0$. *Then* $gcd(P, P') = \frac{1}{32}R_1 = X + 1$.
b) Factorize P *over* $\mathbb{R}[X]$ *: since* $gcd(P, P') = x + 1$ *then* $x = -1$ *a zero of multiplicity* 2, *by Euclidean division we get :*

$$\begin{array}{rr|l} X^4 + 2X^3 + 2X^2 + 2X + 1 & & X^2 + 2X + 1 \\ \cline{3-3} -X^4 - 2X^3 \quad -X^2 & & X^2 + 1 \\ \cline{1-1} X^2 + 2X + 1 & & \\ -X^2 - 2X - 1 & & \\ \cline{1-1} 0 & & \end{array}$$

Then the factorization is given by : $P(X) = (X+1)^2(X^2+1)$.

Solution 5.6.15.

1. *Over* $\mathbb{R}[X]$ *we get :* $P(X) = X^3 + X^2 + X + 1 = (X+1)(X^2+1)$ *using ex01 c)*
   Over $\mathbb{C}[X]$ *we get :* $P(X) = (X+1)(X+i)(X-i)$.
2. *Over* $\mathbb{R}[X]$ *we get :* $X^4 - 1 = (X^2-1)(X^2+1) = (X+1)(X-1)(X^2+1)$.
   Over $\mathbb{C}$ *we get :* $X^4 - 1 = (X+1)(X-1)(X+i)(X-i)$.
3. $\mathbb{C}[X]$ *we get :* $X^4 = -1$ *let us express* $z = -1$ *if polar form :*

$$-1 = r(\cos(\theta) + i\sin(\theta)) = 1.(\cos(\pi) + i\sin(\pi)).$$

Here, r *is the modulus (magnitude) of* $z = -1$, *and* θ *is its argument (angle).*
Then $X^4 = z = \cos(\pi)$.
Remark :

To find the $n-th$ complex root of z, solve the equation:
$z^n = w$ where w is the desired complex root.
The solutions for w are given by:

$$w_k = r^{1/n} e^{i(\frac{\theta}{n} + \frac{2k\pi}{n})} \text{ where } 0 \leq k < n-1.$$

So $x_1 = e^{\frac{i\pi}{4}}, x_2 = e^{\frac{3i\pi}{4}}, x_3 = e^{\frac{5i\pi}{4}}, x_4 = e^{\frac{7i\pi}{4}}$. Then here the algebraic form :

$$X^4+1 = (X - \frac{\sqrt{2}(1+i)}{2})(X - \frac{\sqrt{2}(1-i)}{2})(X + \frac{\sqrt{2}(1+i)}{2})(X + \frac{\sqrt{2}(1-i)}{2}).$$

We can also write it as :

$$X^4+1 = (X - e^{\frac{i\pi}{4}})(X - e^{\frac{3i\pi}{4}})(X - e^{\frac{i5\pi}{4}})(X - e^{\frac{i7\pi}{4}}).$$

We have that $e^{\frac{i5\pi}{4}} = e^{-\frac{i\pi}{4}}, e^{\frac{i7\pi}{4}} = e^{-\frac{i3\pi}{4}}$.

Over $\mathbb{R}[X]$: Let us find $a,b,c,a',b,c'' \in \mathbb{R}$: such that :
$X^4+1 = (aX^2+bX+c)(a'X^2+b'X+c')$ or let us find $b,b' \in \mathbb{R}$ such that

$$X^4+1 = (X^2+bX+1)(X^2+b'X+1) = X^4+1+X^2(bb'+2)+X(b+b')$$

Then $\begin{cases} bb'+2=0 & \Rightarrow bb' = -2 \\ b+b'=0 & \Rightarrow b = -b' \end{cases} \Rightarrow \begin{cases} bb'+2=0 & \Rightarrow -b^2 = -2 \\ b+b'=0 & \Rightarrow b = -b' \end{cases}$
$\Rightarrow b = \sqrt{2}, b' = -2\sqrt{2}$

$$X^4+1 = (X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1).$$

4. *Over $\mathbb{R}[X]$: $X^6-1 = (X^3-1)(X^3+1)$ moreover*

$$\begin{array}{r|l} X^3 + 1 & X+1 \\ \hline -X^3-X^2 & X^2-X+1 \\ \hline -X^2 & \\ X^2+X & \\ \hline X+1 & \\ -X-1 & \\ \hline 0 & \end{array}$$

$$\begin{array}{r|l} X^3 - 1 & X-1 \\ \hline -X^3+X^2 & X^2+X+1 \\ \hline X^2 & \\ -X^2+X & \\ \hline X-1 & \\ -X+1 & \\ \hline 0 & \end{array}$$

So

$$X^6-1 = (X+1)(X-1)(X^2-X+1)(X^2+X+1).$$

Over $\mathbb{C}[X]$:
$X^6-1 = (X+1)(X-1)(X - \frac{1+\sqrt{3}i}{2})(X - \frac{1-\sqrt{3}i}{2})(X - \frac{-1+\sqrt{3}i}{2})(X - \frac{-1-\sqrt{3}i}{2})$.

5. *Over $\mathbb{R}[X]$: we observe that $i, -i$ are roots of X^6+1, by Euclidean division we get :*

$$X^6+1 = (X^2+1)(X^4-X^2+1) = (X^2+1)(X^2+\sqrt{3}X+1)(X^2-\sqrt{3}X+1).$$

Over $\mathbb{C}[X]$: let us find 6−th complex root of $z=-1$, they are given by the formula :

$$x_k = r^{1/6} e^{i(\theta/6+2k\pi/6)}, 0 \le k < 5$$

here $r=1, \theta=\pi$, so $x_1 = e^{\frac{i\pi}{6}}, x_2 = e^{\frac{3i\pi}{6}}, x_3 = e^{\frac{5i\pi}{6}}, x_4 = e^{\frac{7i\pi}{6}} x_5 = e^{\frac{9i\pi}{6}} x_6 = e^{\frac{11i\pi}{6}}$. Then :

$$X^6+1 = (X-e^{\frac{i\pi}{6}})(X-e^{\frac{i\pi}{2}})(X-e^{\frac{5i\pi}{6}})(X-e^{\frac{7i\pi}{6}})(X-e^{3\frac{i\pi}{2}})(X-e^{\frac{11i\pi}{6}}).$$

6. *Over $\mathbb{R}[X]$: we get using ex01 4) and the precedent problem*

$$P(X) = X^9+X^6+X^3+1 = (X^3+1)(X^6+1)$$

$$X^9+X^6+X^3+1 = (X+1)(X^2-X+1)(X^2+1)(X^2+\sqrt{3}X+1)(X^2-\sqrt{3}X+1).$$

Over $\mathbb{C}[X]$ we get :

$$P(X) = (X+1)(X-e^{\frac{i\pi}{3}})(X-e^{\frac{5i\pi}{3}})(X-e^{\frac{i\pi}{6}})(X-e^{\frac{i\pi}{2}})(X-e^{\frac{5i\pi}{6}})(X-e^{\frac{7i\pi}{6}})(X-e^{3\frac{i\pi}{2}})(X-e^{\frac{11i\pi}{6}}).$$

The algebraic form est given by :

$$X^9+X^6+X^3+1 = (X+1)(X-\frac{1+\sqrt{3}i}{2})(X-\frac{1-\sqrt{3}i}{2})(X-i)(X+i)$$

$$\times(X-\frac{-\sqrt{3}+i}{2})(X-\frac{-\sqrt{3}-i}{2})(X-\frac{\sqrt{3}+i}{2})(X-\frac{\sqrt{3}-i}{2}).$$

Solution 5.6.16.

1. *The decomposition is given by:*

$$\frac{1}{X^2-X-2} = \frac{a}{X-2}+\frac{b}{X+1}.$$

Let us find a, b:

$$\frac{1}{(X+1)(X-2)} = \frac{a}{X+1}+\frac{b}{X-2}.$$

*To find **a**, we multiply each side by $(X+1)$, we get*

$$\frac{1}{(X-2)} = a+\frac{b(X+1)}{X-2}$$

on tend $X \to -1$ Then

$$\frac{-1}{3} = a.$$

*To find **b**,we multiply each side by $(X-2)$, we get*

$$\frac{1}{(X+1)} = \frac{a(X-2)}{X+1}+b$$

we tend $X \to 2$ so

$$\frac{1}{3} = b.$$

(we can use identification too)

$$\frac{1}{(X+1)(X-2)} = \frac{a}{X+1}+\frac{b}{X-2} = \frac{X(a+b)+b-2a}{(X+1)(X-2)}.$$

$$\begin{cases} a+b=0, \\ b-2a=1 \end{cases} \Rightarrow 3a=-1, a=-1/3, b=1/3$$

$$F_1 = \frac{\frac{-1}{3}}{X+1}+\frac{\frac{1}{3}}{X-2},$$

2. $\dfrac{X^2+1}{X^3+4X^2+5X+2} = \dfrac{X^2+1}{(X+1)^2(X+2)}$.
The decomposition is given by:

$$\frac{X^2+1}{(X+1)^2(X+2)} = \frac{a}{X+2} + \frac{b}{X+1} + \frac{c}{(X+1)^2}.$$

Let us determine a,b,c:

$$a = \lim_{X\to -2} \frac{X^2+1}{(X+1)^2} = 5, c = \lim_{X\to -1} \frac{X^2+1}{X+2} = 2,$$

*To find **b** we select $X=0$ we get:*

$$\frac{1}{2} = \frac{a}{2} + b + c \Rightarrow b = -4$$

$$\frac{X^2+1}{(X+1)^2(X+2)} = \frac{5}{X+2} + \frac{-4}{X+1} + \frac{2}{(X+1)^2}.$$

3. $\dfrac{X^2+1}{(X^2-3X+2)(X+2)} = \dfrac{X^2+1}{(X-1)(X-2)(X+2)}$
The decomposition is given by:

$$\frac{X^2+1}{(X+1)(X-2)(X+2)} = \frac{a}{X+1} + \frac{b}{X-2} + \frac{c}{X+2}.$$

Let us determine a,b,c:

$$a = \lim_{X\to -1} \frac{X^2+1}{(X-2)(X+2)} = -\frac{2}{3}, b = \lim_{X\to 2} \frac{X^2+1}{(X+1)(X+2)} = \frac{5}{12},$$

$$c = \lim_{X\to -2} \frac{X^2+1}{(X+1)(X-2)} = \frac{5}{4},$$

4. *The decomposition* $\dfrac{X^2+X+1}{X^2(X+1)^2}$ *is given by*

$$\frac{X^2+X+1}{X^2(X+1)^2} = \frac{a}{X} + \frac{b}{X^2} + \frac{c}{X+1} + \frac{d}{(X+1)^2}$$

Let us determine a,b,c,d:

$$b = \lim_{X\to 0} \frac{X^2+X+1}{(X+1)^2} = 1, d = \lim_{X\to -1} \frac{X^2+X+1}{X^2} = 1,$$

We multiply each side by X and we tend ∞, we set $X=1$ then we get the following equations :

$$\begin{cases} 1 = a + c \\ \frac{3}{4} = a + 1 + \frac{c}{2} + \frac{1}{4} \end{cases} \Rightarrow \begin{cases} 1 = a + c \\ 3 = 4a + 4 + 2c + 1 \end{cases} \Rightarrow \begin{cases} a = -2 \\ c = 3 \end{cases}$$

Solution 5.6.17.

1. *Over* $\mathbb{R}[X]$:
the decomposition of $\frac{X+2}{X^4-1} = \frac{X+2}{(X+1)(X-1)(X^2+1)}$ *is given by:*

$$\frac{X+2}{(X+1)(X-1)(X^2+1)} = \frac{a}{(X+1)} + \frac{b}{(X-1)} + \frac{cX+d}{X^2+1}$$

$a = \lim_{X\to -1} \frac{X+2}{(X-1)(X^2+1)} = \frac{3}{4}, b = \lim_{X\to +1} \frac{X+2}{(X+1)(X^2+1)} = -\frac{1}{4}.$
Let us find c?:
$$\frac{X(X+2)}{(X-1)(X+1)(X^2+1)} = \frac{aX}{(X+1)} + \frac{bX}{(X-1)} + \frac{cX^2+dX}{X^2+1},$$
we tend $X \to \infty$ *so* $c = -\frac{1}{2}$.
Let us find d?: we set $X = 0$, *then :*

$$-\frac{1}{2} = a - b + d \Rightarrow d = -1.$$

Over $\mathbb{C}[X]$:
the decomposition of $\frac{X+2}{X^4-1} = \frac{X+2}{(X+1)(X-1)(X+i)(X-i)}$ *is given by:*

$$\frac{X+2}{(X+1)(X-1)(X^2+1)} = \frac{a}{(X+1)} + \frac{b}{(X-1)} + \frac{C}{X+i} + \frac{C}{X-i}$$

$$a = \frac{3}{4}, b = -\frac{1}{4},$$

$$C = \lim_{X\to -i} \frac{X+2}{(X^2-1)(X-i)} = \frac{1}{2}(1+2i), D = \lim_{X\to i} \frac{X+2}{(X^2-1)(X+i)} = \frac{1}{2}(1-2i).$$

2. *Over* $\mathbb{R}[X]$: *the decomposition of* $\frac{6}{(X^2+1)(X^2+4)}$ *is given by :*

$$\frac{6}{(X^2+1)(X^2+4)} = \frac{ax+b}{X^2+1} + \frac{cx+d}{X^2+4} = \frac{2}{X^2+1} - \frac{2}{X^2+4}$$

Over $\mathbb{C}[X]$: *the decomposition of* $\frac{6}{(X^2+1)(X^2+4)}$ *is given by*

$$\frac{6}{(X+i)(X-i)(X+2i)(X-2i)} = \frac{a}{X+i} + \frac{b}{X-i} + \frac{c}{X+2i} + \frac{d}{(X-2i)}.$$

$$\frac{6}{(X+i)(X-i)(X+2i)(X-2i)} = \frac{i}{X+i} + \frac{-i}{X-i} + \frac{\frac{-i}{2}}{X+2i} + \frac{\frac{i}{2}}{(X-2i)}.$$

3. *Over* $\mathbb{R}[X]$: *the decomposition of* $F = \frac{-4}{X^4+1}$ *is given by*

$$F = \frac{-4}{(X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)} = \frac{aX+b}{X^2+\sqrt{2}X+1} + \frac{cX+d}{X^2-\sqrt{2}X+1}$$

$$F = \frac{-4}{(X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)} = \frac{\sqrt{2}}{X^2+\sqrt{2}X+1} + \frac{-\sqrt{2}}{X^2-\sqrt{2}X+1}.$$

Over $\mathbb{C}[X]$: the decomposition of F is given by :

$$F = \frac{-4}{(X-e^{\frac{i\pi}{4}})(X-e^{\frac{3i\pi}{4}})(X+e^{\frac{i\pi}{4}})(X+e^{\frac{3i\pi}{4}})},$$

$$F = \frac{a}{X-e^{\frac{i\pi}{4}}} + \frac{b}{X-e^{\frac{3i\pi}{4}}} + \frac{c}{X+e^{\frac{i\pi}{4}}} + \frac{a}{X+e^{\frac{3i\pi}{4}}}$$

$$F = \frac{1}{X-e^{\frac{i\pi}{4}}} + \frac{-1}{X-e^{\frac{3i\pi}{4}}} + \frac{1}{X+e^{\frac{i\pi}{4}}} + \frac{-1}{X+e^{\frac{3i\pi}{4}}}$$

4. *Over $\mathbb{R}[X]$: the decomposition of $G = \frac{1+2X^2}{X(X^2+1)^2}$ is give by :*

$$G = \frac{a}{X} + \frac{bX+c}{X^2+1} + \frac{dX+e}{(X^2+1)^2}.$$

$$G = \frac{1}{X} + \frac{-X}{X^2+1} - \frac{X}{(X^2+1)^2}.$$

Over $\mathbb{C}[X]$: the decomposition of $G = \frac{1+2X^2}{X(X^2+1)^2}$ is give by :

$$G = \frac{a}{X} + \frac{b}{X+i} + \frac{c}{X-i} + \frac{d}{(X+i)^2} + \frac{e}{(X-i)^2}.$$

$$G = \frac{1}{X} + \frac{1/2}{X+i} + \frac{1/2}{X-i} + \frac{-i/4}{(X+i)^2} + \frac{-i/4}{(X-i)^2}.$$

Solution 5.6.18. *Let $P(x) = X^3+5X^2+7X+3$*

1. $P(x) = P'(x)(\frac{1}{3}(3X+5)) - \frac{8}{9}(X+1)$,
   $P'(x) = R_1(\frac{27}{8}X + \frac{117}{8}) + 20$.
   $R_1 = R_2(\frac{2}{45}X - \frac{2}{45}) + 0$, *Then* $GCD(P,P') = (X+1)$

2. *Since $PGCD(P,P') = (X+1)$, then $X=1$ is a root with multiplicity 2, so $(x+1)^2$ divides $P(x)$,*
   $P(X) = (X+1)^2(X+3)$.

3. *Decomposition is given by :*
   $$F = \frac{X^2+1}{(X+1)^2(X+3)} = \frac{a}{X+1} + \frac{b}{(X+1)^2} + \frac{c}{X+3}.$$
   $$c = \frac{5}{2}, b = 1, a = 1-c = -\frac{3}{2}.$$

References

1. E. Azouly, J. Avignant, G. Auliac, Problèmes Corrigés de mathématiques , DEUG MIAS/SM, Ediscience(Dunod pour la nouvelle édition) Paris 2002.

2. E. Azouly, J. Avignant, G. Auliac, les mathématiques en Licence, 1ère. Tome 1 : Cours+ exos, MIAS.MASS.SM, Ediscience(Dunod pour la nouvelle édition) Paris 2003.

3. R. Godement Cours d'algèbre. Hermann, 1966.

4. J.K. Goyal and K.P. Gupta, Advanced course in modern algebra. Paragati prakashan (Educational publisher) 1971.

5. M. H. Mortad, Basic Abstract Algebra: Exercises and Solutions, World Scientific Publishing Co,2022

6. M. Queysanne, Algèbre, collection U, Armand Colin, 1971.