Algebra I Courses

with Corrected Exercises

Dr. Hamid BEDDANI

Preface

This handout is a work, mainly intended for first year Electrical and Energy Engineering students, but also for all first year students in technological and scientific fields, we address the first year algebra program. The courses are presented in a very clear way with many examples which allows the student the best understanding of the program. At the end of each course, exercises with detailed solutions are offered.

Contents

1 Logic, Set and Applications 5

1.1 Propositional logic **5**

1.1.1 Propositions (Assertions): 5

1.1.2 Quantifiers 8

1.1.3 Types of reasoning in mathematics 9

1.2 Set Language **10**

1.2.1 concepts 10

1.2.2 Operations on sets 10

1.3 Applications **12**

1.3.1 Concepts 12

1.3.2 Injections, surjections, bijections 13

1.3.3 Image and inverse image 15

1.3.4 **Exercises** 18

1.3.5 **Additional exercises** 24

2 Algebraic Structure 27

2.0.1 Internal composition law $(I.C.L)$ 27

2.0.2 Group Structure 29

2.0.3 Ring Structure 31

2.0.4 Field Structure 32

2.1 Exercises **32**

2.2 Additional exercises **36**

3 Rings of Polynomials 39

3.0.1 Concepts 39
3.0.2 Operations on $\mathbb{K}[X]$ 40
3.0.3 Polynomial Division 40
3.0.4 Reducibility 43
3.0.5 Greatest Common Divisor (g.c.d) 43
3.0.6 Factoring a polynomial into irreducible 45

4 Rational fractions 47

4.0.1 Roots and poles of a rational fraction 47
4.0.2 Decomposition into simple elements 47
4.0.3 Practical examples 49
4.0.4 Practical decomposition methods 52

4.1 Exercises solved 52

4.1.1 Additional exercises 60

4.2 Final exam. 62

4.2.1 Exam 1. 62
4.2.2 Exam 2. 67
4.2.3 Exam 3. 71
4.2.4 Exam 4. 74

1. Logic, Set and Applications

1.1 Propositional logic

1.1.1 Propositions (Assertions):

- In mathematics, the propositions are denoted by $P, Q, R, \cdots$, these are propsitions that can be judged as true (we denote by 1 or T) or false (we denote by 0 or F).

■ **Exemples 1.1** 1) "All even integers are divisible by two" is a true proposition.
2) "4 is an odd number" is a false proposition.

Définition 1.1.1 0 and 1 are called truth values.

Logical connectors

$\wedge$	Conjunction	$P \wedge Q$	P and Q.
$\vee$	Disjunction	$P \vee Q$	P or Q.
$-$	Negation	$\overline{P}$	not P.
$\Longrightarrow$	Implication (Conditional)	$P \Longrightarrow Q$	P implies Q
$\Longleftrightarrow$	Equivalence (Biconditional)	$P \Longleftrightarrow Q$	P if and only if (**iff**) Q. P is equivalent to Q.

■ **Exemples 1.2** P: The sine function is not one-to-one (Injective).
Q :The square root function is one-to-one correspondence (Bijective).
R :The absolute value function is not onto (Surjective).
The following symbols represent the indicated propositions:
$\overline{R}$: The absolute value function is onto.
$\overline{P} \vee \overline{Q}$: The sine function is one-to-one, **or** the square root function is not one-to-one correspondence.
$Q \Longrightarrow R$: **If** the square root function is one-to-one, **then** the absolute function is not onto.

$R \Longleftrightarrow P$: The absolute value function is not onto **if and only if** the sine function is not one-to-one.

$P \wedge Q$: The sine function is not one-to-one, **and** the square root function is one-to-one correspondence.

Valuations and Truth Tables

Propositions have truth values, but propositional forms do not. This is because every propositional form represents any one of infinitely many propositions. However, once a propositional form is identified with a proposition, there should be a process by which the truth value of the proposition is associated with the propositional form. This is done with a rule v called a valuation. The input of v is a propositional form, and its output is T or F.

Suppose that P is a propositional variable. If P has been assigned a proposition,

$$v(P) = \begin{cases} 1 & \text{if } P \text{ is true} \\ 0 & \text{if } P \text{ is false} \end{cases}.$$

For example, if $P := 2+3=5$, then $v(P)=1$, and if $P := 2+3=7$, then $v(P)=0$.

Définition 1.1.2 Let P and Q be propositional forms.

The truth value of the negation of a proposition is the opposite of the truth value of that proposition,

$$v(\overline{P}) = \begin{cases} 0 & \text{if } P \text{ is true} \quad (\text{or if } v(P)=1) \\ 1 & \text{if } P \text{ is false} \quad (\text{or if } v(P)=0) \end{cases}.$$

The conjunction is true when both of its conjuncts are true, and false otherwise.

$$v(P \wedge Q) = \begin{cases} 1 & \text{if } v(P)=1 \text{ and } v(Q)=1 \\ 0 & \text{if not (otherwise).} \end{cases}.$$

The disjunction is true when at least one disjunct is true, and false otherwise.

$$v(P \vee Q) = \begin{cases} 0 & \text{if } v(P)=0 \text{ and } v(Q)=0 \\ 1 & \text{if not (otherwise).} \end{cases}.$$

The implication $(P \Longrightarrow Q)$, (it reads also "if P then Q") is false only if P is true and Q is false, otherwise it is true

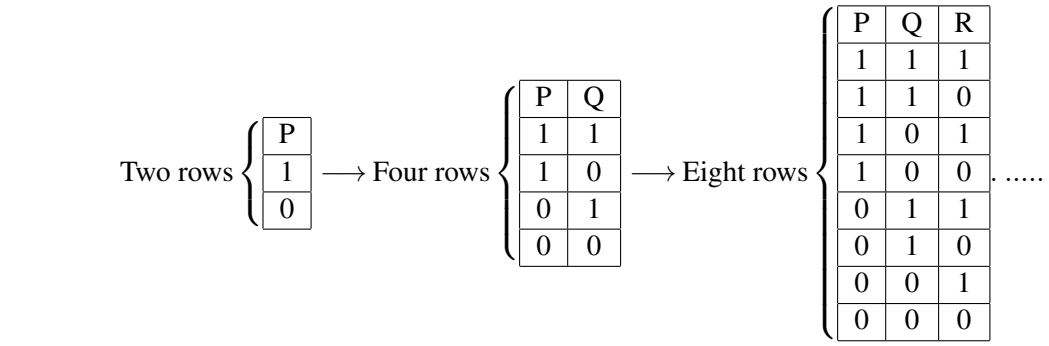
$$v(P \Longrightarrow Q) = \begin{cases} 0 & \text{if } v(P)=1 \text{ and } v(Q)=0 \\ 1 & \text{if not (otherwise).} \end{cases}.$$

The equivalence is true if P and Q have the same truth values

$$v(P \Longleftrightarrow Q)) = \begin{cases} 1 & \text{if } v(P)=v(Q) \\ 0 & \text{if not (otherwise).} \end{cases}.$$

- The following truth table summarizes the above definition

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



Properties:

Let P, Q and R be three propositions. Using truth tables, we can proof that the following propositions are true:

1 $[P \Longleftrightarrow Q] \Longleftrightarrow [\overline{P} \Longleftrightarrow \overline{Q}]$

2 $P \Longleftrightarrow Q \Longleftrightarrow (P \Longrightarrow Q) \wedge (Q \Longrightarrow P)$.

3 $[(P \Longrightarrow Q) \wedge (Q \Longrightarrow R)] \Longrightarrow [P \Longrightarrow R]$.

Distributive Laws

4 $P \wedge (Q \vee R) \Longleftrightarrow (P \wedge Q) \vee (P \wedge R)$.(the distribution of $\wedge$ on $\vee$),

5 $P \vee (Q \wedge R) \Longleftrightarrow (P \vee Q) \wedge (P \vee R)$.(the distribution of $\vee$ on $\wedge$),

De Morgan's Laws

6 $\overline{P \wedge Q} \Longleftrightarrow \overline{P} \vee \overline{Q}$.

8 $\overline{P \vee Q} \Longleftrightarrow \overline{P} \wedge \overline{Q}$.

9 $\overline{[P \Longrightarrow Q]} \Longleftrightarrow [P \wedge \overline{Q}]$.

Contrapositive Law

10 $P \Longrightarrow Q \Longleftrightarrow \overline{Q} \Longrightarrow \overline{P}$.

Proof:

- Truth table associated of De Morgan's Laws

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

We see that the logical propositions $(\overline{P \wedge Q})$ and $(\overline{P} \vee \overline{Q})$ have the same truth values, so they are equivalent. In the same way, we prove the other properties.

- Truth table associated of (9)

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

We see that the logical propositions $(\overline{P \Longrightarrow Q})$ and $(P \wedge \overline{Q})$ have the same truth values, so they are equivalent

- Truth table associated of (3)

P	1	1	1	1	0	0	0	0
Q	1	1	0	0	1	0	1	0
R	1	0	1	0	1	1	0	0
$P \Longrightarrow Q$	1	1	1	1	0	1	0	1
$Q \Longrightarrow R$	1	1	0	1	1	0	1	1
$P \Longrightarrow R$	1	1	1	1	0	0	1	1
$P \Longrightarrow Q \wedge Q \Longrightarrow R$	1	1	0	1	0	0	0	1
$[P \Longrightarrow Q \wedge Q \Longrightarrow R] \Longrightarrow [P \Longrightarrow R]$	1	1	1	1	1	1	1	1

We see that the logical propositions $[P \Longrightarrow Q \wedge Q \Longrightarrow R] \Longrightarrow [P \Longrightarrow R]$ always true. In the same way, we prove the other properties.

1.1.2 Quantifiers

In mathematics, there exists three logical quantifiers represented in the Table

Quantifiers	**Proposition**	**Description**
$\forall$: The universal quantifier " **for all**"	$\forall x \in \mathbb{E} : P(x)$	is true if $P(x)$ is true for all values of x in $\mathbb{E}$
$\exists$: The existential quantifier "there exists" or "there exists at least one"	$\exists x \in \mathbb{E} : P(x)$	is true if $P(x)$ is true for at least one value of x in $\mathbb{E}$
$\exists!$: There exists a unique	$\exists! \in \mathbb{E} : P(x)$	is true if there exists an x which is unique satisfying $P(x)$ It is false if this x does not exist or if there exist several x satisfying$P(x)$

■ **Exemples 1.3 :**

1. The quantified assertion « $\forall n \in \mathbb{N} : (4-n)n < 0$ » is false since there exists an element n in $\mathbb{N}$ (We take $n = 0, n = 1, n = 2$, or $n = 3$)« $(4-n)n < 0$ ».

2. The quantified assertion « $\exists x \in \mathbb{R} : x^4 = 81$ » is true because there exists at least one element in $\mathbb{R}$ which satisfies $x^4 = 81$. This is the case for the two real numbers -3 and 3..

- Following the expression "Who can do more, can do less", it is clear that the quantified assertion "$\exists x \in \mathbb{E} : P(x)$ " is automatically verified when the quantified assertion "$\forall x \in \mathbb{E} : P(x)$ » is. For example, the quantified assertion

« $\exists x \in [-3,3] : x^2 - 9 \leq 0$ » is true since the quantified assertion « $\forall x \in [-3,3] : x^2 - 9 \leq 0$ » is true.

Negation of a quantified proposition

1. $\overline{\forall x \in \mathbb{E} : P(x)} \Longleftrightarrow \exists x \in \mathbb{E} : \overline{P(x)}$
2. $\overline{\exists x \in \mathbb{E} : P(x)} \Longleftrightarrow \forall x \in \mathbb{E} : \overline{P(x)}$
3. $\overline{\exists! x \in \mathbb{E} : P(x)} \Longleftrightarrow \overline{\exists x \in \mathbb{E} : P(x) \wedge x \text{ is unique}} \Longleftrightarrow \overline{\exists x \in \mathbb{E} : P(x)} \vee \overline{x \text{ is unique}}$

Important rules

1. $\forall x \in \mathbb{E}, \forall y \in \mathbb{F} : P(x,y) \Longleftrightarrow \forall y \in \mathbb{F}, \forall x \in \mathbb{E} : P(x,y)$
2. $\exists x \in \mathbb{E}, \exists y \in \mathbb{F} : P(x,y) \Longleftrightarrow \exists y \in \mathbb{F}, \exists x \in \mathbb{E} : P(x,y)$
3. $\forall x \in \mathbb{E}, \exists y \in \mathbb{F} : P(x,y) \not\Leftrightarrow \exists y \in \mathbb{F}, \forall x \in \mathbb{E} : P(x,y)$

▪ **Exemples 1.4** : Let U and V be two sequences

1. $\forall n \in \mathbb{N} : U_n = V_n$. The negation of this proposition is $\exists n \in \mathbb{N} : U_n \neq V_n$.
2. $\exists! n \in \mathbb{N} : U_n = V_0$. The negation of this proposition is
   $\forall n \in \mathbb{N} : U_n \neq V_0$ or $\exists (n_1, n_2) \in \mathbb{N}^2 : U_{n_1} = V_0 \wedge U_{n_2} = V_0$
3. $\forall n \in \mathbb{N}, \exists m \in \mathbb{N} : U_n \leq V_m$. The negation of this proposition is: $\exists n \in \mathbb{N}, \forall m \in \mathbb{N} : U_n > V_m$

1.1.3 Types of reasoning in mathematics

Proof by Contrapositive

Since, for two propositions P and Q, we have

$$[P \Longrightarrow Q] \Longleftrightarrow \left[\overline{Q} \Longrightarrow \overline{P}\right]$$

So, for show that $P \Longrightarrow Q$, It is enough to show that $\overline{Q} \Longrightarrow \overline{P}$.

▪ **Exemples 1.5** : By using the proof by contrapositive, we prove the following proposition:

$$\forall n \in \mathbb{N} : n^2 \text{ is even number} \Longrightarrow n \text{ is even number.}$$

For that, proof that

$$\forall n \in \mathbb{N} : \overline{n \text{ is even number}} \Longrightarrow \overline{n^2 \text{ is even number}},$$

In other words

$$n \text{ is odd number} \Longrightarrow n^2 \text{ is odd number .}$$

Let $n \in \mathbb{N}$. Suppose n is odd number. This means that $\exists p \in \mathbb{N}$ such that $n = 2p+1$. Then we have:

$$n^2 = (2p+1)^2 = 2(2p^2+2p)+1 = 2q+1, q \in \mathbb{N}.$$

So n^2 is odd number. Then prove the proposition.

Proof by the absurd

For prove that a proposition P is true, we assume that $\overline{P}$ is true and we deduce a contradiction.

▪ **Exemples 1.6** :

1. Let $n \in \mathbb{N}^*$, proof that n^2+1 cannot be a square of $p \in \mathbb{N}$.
   By using the proof by the absurd, we assume that $\exists p \in \mathbb{N}$ such that $n^2+1 = p^2$.
   Which implies

$$p^2 - n^2 = 1 \Longleftrightarrow (p-n)(p+n) = 1,$$

As $n \in \mathbb{N}^*$, then we must take $p > 1$ so that $p-n$ is strictly positive (> 0). So

$$\begin{cases} n \geq 1 \\ and \\ p-n \geq 1 \end{cases} \Longrightarrow p+n = p-n+2n \geq 1+2 = 3,$$

then

$$(p-n)(p+n) \geq 1 \times 3 > 1,$$

hence the contradiction.

Direct Proof:

To prove that $P \Longrightarrow Q$ is true, we assume that P is true and show that Q is true.

- **Exemples 1.7 :**

  Proof that if $\forall a, b \in \mathbb{Q}$, then $a+b \in \mathbb{Q}$. Indeed, let $a, b \in \mathbb{Q}$, so :

$$\begin{cases} a = \frac{x}{y}, x \in \mathbb{Z}, y \in \mathbb{N}^* \\ b = \frac{s}{t}, s \in \mathbb{Z}, t \in \mathbb{N}^* \end{cases} \Longrightarrow a+b = \frac{xt+ys}{yt} \in \mathbb{Q}.$$

Hence the result.

1.2 Set Language

1.2.1 concepts

A set $\mathbb{E}$ is a collection of objects called elements.

We call $CardE$ the number of elements of the set $\mathbb{E}$.

We write $x \in \mathbb{E}$ to say that: x is an element of $\mathbb{E}$ (or that x belongs to $\mathbb{E}$).

We write $x \notin \mathbb{E}$ to say that: x does not belong to $\mathbb{E}$

We write $\mathbb{F} \subset \mathbb{E}$ to say that: $\mathbb{F}$ is a subset of $\mathbb{E}$, or $\mathbb{F}$ is a part of $\mathbb{E}$ or $\mathbb{F}$ is included in $\mathbb{E}$.

We note by $\varnothing$ the empty set which does not contain any element.

- **Exemples 1.8** $\mathbb{E} = \{1, t, 5, m, \sqrt{7}\}$,

$$Card\mathbb{E} = 5, \quad m \in \mathbb{E}, \quad \{1,5\} \subset \mathbb{E}, \quad s \notin \mathbb{E}, \quad \{0,t\} \not\subseteq \mathbb{E}.$$

1.2.2 Operations on sets

Let $\mathbb{E}$ and $\mathbb{F}$ be two sets, then we present the possible operations between $\mathbb{E}$ and $\mathbb{F}$.

$\mathbb{E} \subset \mathbb{F}$	$\mathbb{E}$ is included in $\mathbb{F}$	$\mathbb{E} \subset \mathbb{F} \Longleftrightarrow \forall x : x \in \mathbb{E} \Longrightarrow x \in \mathbb{F}$
$\mathbb{E} = \mathbb{F}$	$\mathbb{E}$ and $\mathbb{F}$ are two equal sets	$\mathbb{E} = \mathbb{F} \Longleftrightarrow (\mathbb{E} \subset \mathbb{F}) \wedge (\mathbb{F} \subset \mathbb{E})$
$\mathbb{E} \cup \mathbb{F}$	The union of $\mathbb{E}$ and $\mathbb{F}$	$x \in (\mathbb{E} \cup \mathbb{F}) \Leftrightarrow (x \in \mathbb{E}) \vee (x \in \mathbb{F})$, The set that contains all the elements of $\mathbb{E}$ and $\mathbb{F}$
$\mathbb{E} \cap \mathbb{F}$	The intersection of $\mathbb{E}$ and $\mathbb{F}$	$x \in (\mathbb{E} \cap \mathbb{F}) \Leftrightarrow (x \in \mathbb{E}) \wedge (x \in \mathbb{F})$, the set of elements which are both in $\mathbb{E}$ and in $\mathbb{F}$
$\mathbb{E} \backslash \mathbb{F} = \mathbb{E} - \mathbb{F}$ ($\mathbb{E}$ minus $\mathbb{F}$)	The difference between $\mathbb{E}$ and $\mathbb{F}$	$x \in (\mathbb{E} - \mathbb{F}) \Leftrightarrow (x \in \mathbb{E}) \wedge (x \notin \mathbb{F})$, the set of elements of $\mathbb{E}$ which are not in F
$A \subset \mathbb{E}$, $A^c = C_{\mathbb{E}}^A = \overline{A}$	The complement of A in $\mathbb{E}$	$A^c = \mathbb{E} \backslash A = \{x : x \in \mathbb{E} \wedge x \notin A\}$
$\mathbb{E} \triangle \mathbb{F}$	The symmetrical difference between $\mathbb{E}$ and $\mathbb{F}$	$\mathbb{E} \triangle \mathbb{F} = (\mathbb{E} \backslash \mathbb{F}) \cup (\mathbb{F} \backslash \mathbb{E}) = (\mathbb{E} \cup \mathbb{F}) - (\mathbb{F} \cap \mathbb{E})$.

Properties:

Let A, B and C be parts of a set $\mathbb{E}$, then:

- $\varnothing \cup A = A$.
- $\varnothing \cap A = \varnothing$.
- $\mathbb{E} \cap A = A$.
- $A \cup \mathbb{E} = \mathbb{E}$.
- $A \subset B \Longrightarrow A \cap B = A$, and $A \cup B = B$.
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, (The distribution of $\cap$ on $\cup$).
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, (the distribution of $\cup$ on $\cap$).
- $(A \cup B)^c = A^c \cap B^c$.
- $(A \cap B)^c = A^c \cup B^c$.
- $A^c \cap A = \varnothing$, and $A^c \cup A = \mathbb{E}$.
- $\varnothing \subset A, \forall A \subset \mathbb{E}$.

Set of parts:

$\mathbb{E}$ is a set, we denote $\mathscr{P}(\mathbb{E})$ the set which contains all the parts of $\mathbb{E}$ and we call it set of parts of $\mathbb{E}$.

$$\mathscr{P}(\mathbb{E}) = \{A, A \subset \mathbb{E}\}.$$

If $Card\mathbb{E} = n$, then $Card\,\mathscr{P}(\mathbb{E}) = 2^n$.

Cartesian product

Let $\mathbb{E}$ and $\mathbb{F}$ be two sets, the cartesian product, denoted $\mathbb{E} \times \mathbb{F}$, is the set of pairs (x, y) where $x \in \mathbb{E}$ and $y \in \mathbb{F}$, that is to say:

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

Examples: Let $A = \{1,2,3,4\}$ and $B = \{4,5\}$, then
$A \cap B = \{4\}$, $A \cup B = \{1,2,3,4,5\}$, $A \backslash B = A - B = \{1,2\}$, $C_B^A = \{5\}$
$A \times B = \{(1,4), (1,5), (2,4), (2,5), (3,4), (3,5), (4,4), (4,5)\}$.

1.3 Applications

1.3.1 Concepts

1- **An application (map)** $f : \mathbb{E} \to \mathbb{F}$ is a relation between a set $\mathbb{E}$ and a set $\mathbb{F}$ for which each element $x \in \mathbb{E}$ has a unique image $f(x) \in \mathbb{F}$. That is to say:

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

- $\mathbb{E}$ is called the starting set of the map.
- $\mathbb{F}$ is called the arrival set of the map.
- $(x, f(x)) \in \Gamma$, Γ is called the graph of the map.
- y is called image of x by the map.
- x is an antecedent of y by the map.

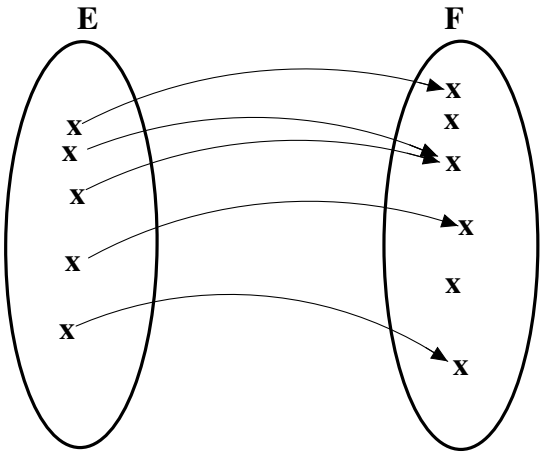


Figure 1.1: Application

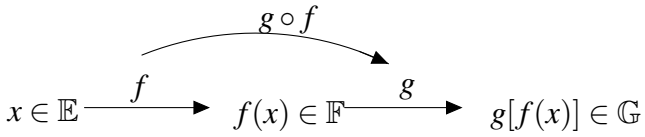
- **Notation:**

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

2- **Equality**: Let $f : \mathbb{E} \to \mathbb{F}$ and $g : \mathbb{E} \to \mathbb{F}$, we say that these two applications are equal if and only if (iff)

$$\forall x \in \mathbb{E}, : g(x) = f(x).$$

3- **Composition of applications**: Let $f : \mathbb{E} \to \mathbb{F}$ and $g : \mathbb{F} \to \mathbb{G}$, then



4- **Restriction, Extension:** Let $f : A \to \mathbb{F}$ and $g : B \to \mathbb{F}$. if $A \subset B$ and if, for all $x \in A$, we have $f(x) = g(x)$, we say that f is a restriction of g, or that g is an extension of f.

Examples:

1) Identity on a set $\mathbb{E}$ is an application defined as follows:

$$\begin{array}{rccc} Id_{\mathbb{E}} : & \mathbb{E} & \longrightarrow & \mathbb{E} \\ & x & \longmapsto & Id_{\mathbb{E}}(x) = x \end{array}$$

2)

$$f : \begin{array}{ccc} \mathbb{R}_+^* & \longrightarrow & \mathbb{R}_+^* \\ x & \longmapsto & f(x) = \frac{1}{x} \end{array} \quad \text{and} \quad g : \begin{array}{ccc} \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ x & \longmapsto & g(x) = \frac{x-1}{x+1} \end{array},$$

then

$$gof : \begin{array}{ccc} \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ x & \longmapsto & gof(x) = g(f(x)) = \frac{1-x}{1+x} \end{array}$$

1.3.2 Injections, surjections, bijections

Injective Application (one-to-one)

An application (map) f:$\mathbb{E} \to \mathbb{F}$ is injective if and anly if (1 or 2):

1.

$$\forall x, x' \in \mathbb{E} : x \neq x' \Longrightarrow f(x) \neq f(x')$$

2.

$$\forall x, x' \in \mathbb{E} : f(x) = f(x') \Longrightarrow x = x'$$

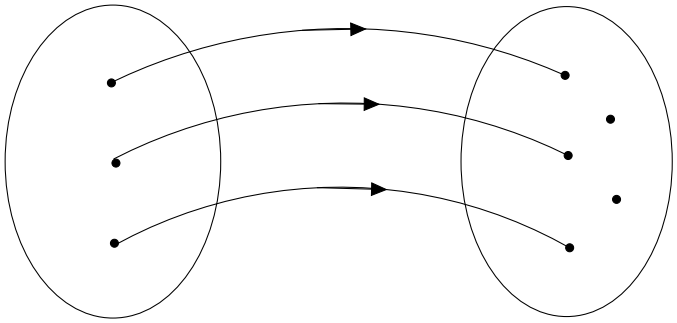


Figure 1.2: Injective

■ **Exemples 1.9 :**

- Id_E is injective.
- The map $f : \mathbb{R}_+ \longrightarrow \mathbb{R}$ and $f(x) = x^2$ is injective.
- $x \longmapsto \sin x$ is not injective on $\mathbb{R}$ because $\frac{\pi}{2} \neq \frac{5\pi}{2}$ but $\sin\frac{\pi}{2} = \sin\frac{5\pi}{2} = 1$
- $x \longmapsto x^2$ is not injective on $\mathbb{R}$ because $(1)^2 = (-1)^2$ but $-1 = 1$.
- $f :]-1, +\infty[\longrightarrow]-1, +\infty[$ and $f(x) = \frac{1}{x+1}$.

Let $x, x' \in]-1, +\infty[$, we have

$$f(x) = f(x') \Longleftrightarrow \frac{1}{x+1} = \frac{1}{x'+1} \Longleftrightarrow x+1 = x'+1 \Longleftrightarrow x = x'$$

then f is injective.

Surjective Application (onto)

A map f:$\mathbb{E} \to \mathbb{F}$ is surjective if every element y of $\mathbb{F}$ is the image of at least one element x of $\mathbb{E}$, i.e.:

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

In other words, $f(\mathbb{E}) = \mathbb{F}$.

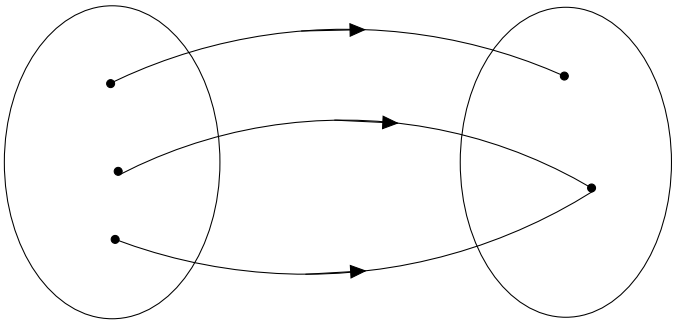


Figure 1.3: Surjective

■ **Exemples 1.10 :**

- $Id_{\mathbb{E}}$ is surjective.
- The map $f : \mathbb{R} \longrightarrow \mathbb{R}_+$ and $f(x) = x^2$ is surjective.
- $x \longmapsto \cos x$ is not surjective on $\mathbb{R}$ because 2 It has no antecedent
- $f :]-1, +\infty[\longrightarrow \mathbb{R}^*$ and $f(x) = \frac{1}{x+1}$

let $y \in \mathbb{R}^*$:

$$y = f(x) \Longleftrightarrow y = \frac{1}{x+1} \Longleftrightarrow x = \left(\frac{1}{y} - 1\right)$$

then $\forall y \in \mathbb{R}^*,\ \exists x = \left(\frac{1}{y} - 1\right) \in]-1, +\infty[:\ y = f(x)$

Then f is surjective.

Bijective Application (one-to-one correspondence)

The application f is a bijective, if and only if, it is both injective and surjective, i.e:

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

Existence: comes from surjectivity,
Uniqueness: comes from injectivity.
If f is not injective or is not surjective then it is not bijective.

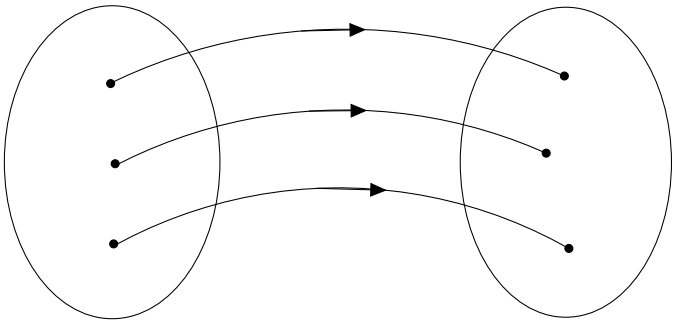


Figure 1.4: Bejection

■ **Exemples 1.11 :**

- 1) $Id_{\mathbb{E}}$ is bijective.
- The application $f : \mathbb{R}_+ \longrightarrow \mathbb{R}_+$ and $f(x) = x^2$ is bijective.
- $f : \mathbb{R} \longrightarrow]0, +\infty[$ and $f(x) = e^x$

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

$$f(x) = f(x') \Longleftrightarrow e^x = e^{x'} \Longleftrightarrow x = x'$$

Then f is injective, and let $y \in]0, +\infty[$:

$$y = f(x) \Longleftrightarrow y = e^x \Longleftrightarrow x = \ln y$$

Then f is surjective, so it is bijective.

Corollary 1.3.1 Let $\mathbb{E}$ and $\mathbb{F}$ two sets and $f : \mathbb{E} \to \mathbb{F}$ the application, then
f is bijective $\Longleftrightarrow$ there exists a unique application which we note $f^{-1} : \mathbb{F} \to \mathbb{E}$ such that

$$\begin{aligned} f \circ f^{-1} &= Id_{\mathbb{F}}, \text{ and } f^{-1} \circ f = Id_{\mathbb{E}} \\ x &= f^{-1}(y) \Longleftrightarrow y = f(x), \end{aligned}$$

Let f the application from $\mathbb{E}$ to $\mathbb{F}$, and g the application from $\mathbb{F}$ to $\mathbb{G}$. We have the following implications.

– If f and g are injectives, then $g \circ f$ is injective.
– If $g \circ f$ is injective, then f is injective.
– If f and g are surjectives, then $g \circ f$ is surjective.
– If $g \circ f$ is surjective, then g is surjective.
– If f and g are bijectives, then $g \circ f$ is bijective, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

1.3.3 Image and inverse image

Let $A \subset \mathbb{E}$ and $M \subset \mathbb{F}$.
1. We call image of A by f, the set of images of the elements of A noted:

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

$f(A)$ is a part of $\mathbb{F}$,
2. We call inverse image of M by f, the set of antecedents of the elements of M, denoted

$$f^{-1}(M) = \{x \in \mathbb{E}, f(x) \in M\} \subset \mathbb{E}$$

$f^{-1}(B)$ is a part of $\mathbb{E}$,
Formally we have:

$$\forall y \in \mathbb{F}, (y \in f(A) \Longleftrightarrow \exists x \in A, y = f(x))$$

$$\forall x \in \mathbb{E}, \left(x \in f^{-1}(M) \Longleftrightarrow f(x) \in M\right).$$

■ **Exemples 1.12 :**
$f : \mathbb{R} \longrightarrow \mathbb{R}$ and $f(x) = x^2$
1. $f([0,3]) = \{f(x), x \in [0,3]\} = \left\{x^2, x \in [0,3]\right\}$

$$\begin{array}{rcl} (x \in [0,3]) & \Longleftrightarrow & 0 \leq x \leq 3 \\ & \Longleftrightarrow & 0 \leq x \leq 3 \\ & \Longleftrightarrow & 0 \leq x^2 \leq 9 \ (f \text{ is increasing}) \\ & \Longrightarrow & f([0,3]) = [0,9] \end{array}$$

2. $f([0,3]) = \{f(x), x \in [-3,3]\} = \left\{x^2, x \in [-3,3]\right\}$

$$\begin{array}{rcl} (x \in [-3,3]) & \Longleftrightarrow & x \in [-3,0] \cup [0,3] \\ & \Longleftrightarrow & (-3 \leq x \leq 0) \vee (0 \leq x \leq 3) \\ & \Longleftrightarrow & \left(0 \leq x^2 \leq 9\right) \vee \left(0 \leq x^2 \leq 9\right). \\ & \Longrightarrow & f([-3,3]) = [0,9] \end{array}$$

3. $f^{-1}([1,4]) = \{x, f(x) \in [1,4]\} = \left\{x, x^2 \in [1,4]\right\}$

$$\begin{array}{rcl} \left(x^2 \in [1,4]\right) & \Longleftrightarrow & (1 \leq x \leq 2) \vee (-2 \leq x \leq -1) \\ & \Longleftrightarrow & x \in [-2,-1] \cup [1,2] \\ & \Longrightarrow & f^{-1}([1,4]) = [-2,-1] \cup [1,2] \end{array}$$

Proposition 1.3.2 Let $f : \mathbb{E} \longrightarrow \mathbb{F}$, $A, B \subset \mathbb{E}$ and $M, N \subset \mathbb{F}$, then
1 $A \subset B \Longrightarrow f(A) \subset f(B)$.
2 $N \subset M \Longrightarrow f^{-1}(N) \subset f^{-1}(M)$.
3 $f(A \cup B) = f(A) \cup f(B)$.
4 $f(A \cap B) \subset f(A) \cap f(B)$.

5 $f^{-1}(M \cup N) = f^{-1}(M) \cup f^{-1}(N)$.
6 $f^{-1}(M \cap N) = f^{-1}(M) \cap f^{-1}(N)$.
7 $f^{-1}\left(C_{\mathbb{F}}^{M}\right) = C_{\mathbb{E}}^{f^{-1}(M)}$.

Prove:
3. Let $y \in \mathbb{F}$, then

$$\begin{aligned}
[y \in f(A \cup B)] &\iff \exists x \in A \cup B; y = f(x) \\
&\iff \exists x [((x \in A) \vee (x \in B)) \wedge (y = f(x))] \\
&\iff \exists x [((x \in A) \wedge (y = f(x)) \vee ((x \in B) \wedge (y = f(x))] \\
&\iff [\exists x((x \in A) \wedge (y = f(x))] \vee [\exists x((x \in B) \wedge (y = f(x))] \\
&\iff (y \in f(A)) \vee (y \in f(B)) \\
&\iff y \in f(A) \cup f(B)
\end{aligned}$$

which shows that $f(A \cup B) = f(A) \cup f(B)$.
4. Let $y \in \mathbb{F}$, then

$$\begin{aligned}
[y \in f(A \cap B)] &\iff \exists x \in A \cap B; y = f(x) \\
&\iff \exists x [((x \in A) \wedge (x \in B)) \wedge y = f(x)] \\
&\iff \exists x [((x \in A) \wedge (y = f(x)) \wedge ((x \in B) \wedge (y = f(x))] \\
&\implies [\exists x((x \in A) \wedge (y = f(x))] \wedge [\exists x((x \in B) \wedge (y = f(x))] \\
&\implies (y \in f(A)) \wedge (y \in f(B)) \\
&\implies y \in f(A) \cup f(B)
\end{aligned}$$

which shows that $f(A \cap B) \subset f(A) \cap f(B)$.
5. Let $x \in \mathbb{E}$, then

$$\begin{aligned}
\left[x \in f^{-1}(N \cup M)\right] &\iff f(x) \in N \cup M \\
&\iff (f(x) \in N) \vee (f(x) \in M) \\
&\iff \left(x \in f^{-1}(M)\right) \vee \left(x \in f^{-1}(N)\right) \\
&\iff \left(x \in f^{-1}(M)\right) \vee \left(x \in f^{-1}(N)\right) \\
&\iff x \in f^{-1}(M) \cup f^{-1}(N)
\end{aligned}$$

which shows that $f^{-1}(M \cup N) = f^{-1}(M) \cup f^{-1}(N)$.
6. Let $x \in \mathbb{E}$, then

$$\begin{aligned}
\left[x \in f^{-1}(N \cap M)\right] &\iff f(x) \in N \cap M \\
&\iff (f(x) \in N) \wedge (f(x) \in M) \\
&\iff \left(x \in f^{-1}(M)\right) \wedge \left(x \in f^{-1}(N)\right) \\
&\iff \left(x \in f^{-1}(M)\right) \wedge \left(x \in f^{-1}(N)\right) \\
&\iff x \in f^{-1}(M) \cap f^{-1}(N)
\end{aligned}$$

which shows that $f^{-1}(M \cap N) = f^{-1}(M) \cap f^{-1}(N)$.

7. Let $x \in \mathbb{E}$, then

$$\begin{aligned} x \quad \in \quad & f^{-1}(C_{\mathbb{F}}^{M}) \Longleftrightarrow f(x) \in C_{\mathbb{F}}^{M} \\ \Longleftrightarrow \quad & (f(x) \in \mathbb{F}) \wedge (f(x) \notin M) \\ \Longleftrightarrow \quad & (x \in \mathbb{E}) \wedge \left(x \notin f^{-1}(M)\right) \\ \Longleftrightarrow \quad & x \in C_{\mathbb{E}}^{f^{-1}(M)} \end{aligned}$$

which shows that $f^{-1}\left(C_{\mathbb{F}}^{M}\right) = C_{\mathbb{E}}^{f^{-1}(M)}$.

Remark: The sets $C_{\mathbb{F}}^{f(A)}$ and $f\left(C_{\mathbb{E}}^{A}\right)$ are not always comparable.

1.3.4 Exercises

Exercise 1.3.1: Let P, Q and R be three logical propositions.

1. Prove that $\overline{P \wedge Q} \Longleftrightarrow \overline{P} \vee \overline{Q}$
2. Prove that $[(P \Longrightarrow Q)] \Longleftrightarrow \left(\overline{P} \vee Q\right)$. Conclude $\overline{P \Longrightarrow Q}$.
3. Prove that $[(P \Longrightarrow Q) \wedge (Q \Longrightarrow R)] \Longrightarrow (P \Longrightarrow R)$.

Solution:

1. Prove that $\overline{P \wedge Q} \Longleftrightarrow \overline{P} \vee \overline{Q}$: By using the truth table

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

We see that the logical propositions $(\overline{P \wedge Q})$ and $(\overline{P} \vee \overline{Q})$ have the same truth values, so they are equivalent.

2. a) Prove that $(P \Longrightarrow Q) \Longleftrightarrow \left(\overline{P} \vee Q\right)$: Using the truth table

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

We see that the logical propositions $(P \Rightarrow Q)$ and $(\overline{P} \vee \overline{Q})$ have the same truth values, so they are equivalent.

b) Conclusion of $\overline{P \Longrightarrow Q}$: Using negation to equivalent the previous, we find

$$\overline{(P \Longrightarrow Q)} \Longleftrightarrow \overline{\left(\overline{P} \vee Q\right)} \Longleftrightarrow P \wedge \overline{Q}.$$

3. Prove that $[(P \Longrightarrow Q) \wedge (Q \Longrightarrow R)] \Longrightarrow (P \Longrightarrow R)$: Using the truth table

P	Q	R	$P \Longrightarrow Q$	$Q \Longrightarrow R$	$(P \Longrightarrow Q) \wedge (Q \Longrightarrow R)$	$P \Longrightarrow R$	$.\Rightarrow.$
1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	1
1	0	1	0	1	0	1	1
1	0	0	0	1	0	0	1
0	1	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	0	1	1	1	1	1	1
0	0	0	1	1	1	1	1

We see that the logical propositions $((P \Longrightarrow Q) \wedge (Q \Longrightarrow R))$ and $(P \Longrightarrow R)$ have the same truth values, so they are equivalent.

Exercise 1.3.2: I) Are the following propositions true or false? and give their negation.

1. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R} : x^2 = y^2 \Longrightarrow x = y$.
2. $\forall x \in \mathbb{N}, \forall y \in \mathbb{N} : x^2 = y^2 \Longrightarrow x = y$.
3. $\exists x \in \mathbb{R}, \exists y \in \mathbb{R} : x = e^y$.
4. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : x = e^y$.
5. $\exists x \in \mathbb{R}, \forall y \in \mathbb{R} : x = e^y$.
6. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R} : x = e^y$.

II) Let f be a function of $f : I \to \mathbb{R}$: By using logical quantifiers, express the following propositions:

1. f is a bounded.
2. f is a continuous on I.

Solution:

Ia) True or false? and give their negation.

1. Is false ($(-x)^2 = x^2 \nRightarrow x = -x, \forall x \in \mathbb{R}$)
2. Is true ($x \geq 0$, and $y \geq 0$)
3. Is true (Easily, $\exists x = 1, \exists y = 0 : 1 = e^0$).
4. Is false (if $x \leq 0$, there is no y)
5. Is false (for example, $\exists x = 1$, and $y = 2 : 1 \neq e^2$).
6. Is false (Exponential function is always positive)

Ib) Negation the previous propositions

$\overline{1}$. $\exists x \in \mathbb{R}, \exists y \in \mathbb{R} : x^2 = y^2 \wedge x \neq y$.
$\overline{2}$. $\exists x \in \mathbb{N}, \exists y \in \mathbb{N} : x^2 = y^2 \wedge x \neq y$.
$\overline{3}$. $\forall x \in \mathbb{R}, \forall y \in \mathbb{R} : x \neq e^y$.
$\overline{4}$. $\exists x \in \mathbb{R}, \exists y \in \mathbb{R} : x \neq e^y$.
$\overline{5}$. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : x \neq e^y$.
$\overline{6}$. $\exists x \in \mathbb{R}, \exists y \in \mathbb{R} : x \neq e^y$.

II) Let f be a function of $f : I \to \mathbb{R}$: Using logical quantifiers:

1. f is a bounded $\Leftrightarrow (\exists m, M \in \mathbb{R}, \forall x \in I : m \leq f(x) \leq M)$.
2. f is a continuous on $I \Leftrightarrow (\forall \varepsilon > 0, \forall x, a \in I, \exists \delta > 0 : |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon)$.

Exercise 1.3.3: I) By contrapositive proof, show that:

$$(x \neq 2) \wedge (y \neq 2) \Longrightarrow xy - 2x - 2y + 4 \neq 0.$$

II) Let $x,y \in \mathbb{Q}$. Prove the following equivalence:

$$x + y.\sqrt{3} = 1 \Longleftrightarrow (x = 1 \text{ and } y = 0).$$

Solution:

I) By contrapositive proof, show that

$$(x \neq 2) \wedge (y \neq 2) \Longrightarrow xy - 2x - 2y + 4 \neq 0.$$

that's to say

$$xy - 2x - 2y + 4 = 0 \Longrightarrow (x = 2) \vee (y = 2).$$

We have

$$xy - 2x - 2y + 4 = (x - 2) \times (y - 2)$$

then

$$xy - 2x - 2y + 4 = (x - 2) \times (y = 2) = 0 \Longrightarrow (x = 2) \vee (y = 2).$$

So

$$(x \neq 2) \wedge (y \neq 2) \Longrightarrow xy - 2x - 2y + 4 \neq 0.$$

II) Let $x,y \in \mathbb{Q}$. Prove the following equivalence:

$$x + y.\sqrt{3} = 1 \Longleftrightarrow (x = 1 \text{ and } y = 0).$$

1. $(\Rightarrow)$:Using absurd proof: suppose that $x + y.\sqrt{3} = 1$ and $x \neq 1 \vee y \neq 0$, so we get $\sqrt{3} = \frac{1-x}{y} \in \mathbb{Q}$, this is contraduction. Then

$$x + y.\sqrt{3} = 1 \Rightarrow (x = 1 \text{ and } y = 0).$$

2. $(\Leftarrow) : (x = 1 \text{ and } y = 0) \Rightarrow x + y.\sqrt{3} = 1 + 0\sqrt{3} = 1$ (this is easy).

$$(x = 1 \text{ and } y = 0) \Rightarrow x + y.\sqrt{3} = 1.$$

Exercise 1.3.4:

1. Let $F = \{\{1,2\},\{3,4,5\},\{6,7,8\}\}$, Which of the following propositions are true:
   a) $\{1,2\} \subset F$; b) $7 \in F$; c) $\{6,7,8\} \in F$; d) $\{\{3,4,5\}\} \subset F$; e) $\varnothing \in F$; f) $\varnothing \subset F$.
2. Let $A;,B$ be two parts of a set E. Show that:
   a) $(A \cup B)^c = A^c \cap B^c$.
   b) $A \setminus (A \setminus B) = A \cap B$.

Solution:

1. $F = \{\{1,2\},\{3,4,5\},\{6,7,8\}\}$.
   - $\{1,2\} \subset F$ is false, because $\{1,2\}$ is not a part of F.
   - $7 \in F$, is false, because 7 is not an element of F.
   - $\{6,7,8\} \in F$, is true, because $\{6,7,8\}$ is an element of F.
   - $\{\{3,4,5\}\} \subset F$, is true, because $\{6,7,8\}$ is a part of F.
   - $\varnothing \in F$, is false, because $\varnothing$ is not an element of F.
   - $\varnothing \subset F$, is true, because $\varnothing$ is a part of F.
2. Let $A;,B$ be two parts of a set E.
   a) Show that: $(A \cup B)^c = A^c \cap B^c$. Let $x \in (A \cup B)^c$, then
   $$\begin{aligned}
   [x \in (A \cup B)^c] &\Leftrightarrow x \notin (A \cup B) \\
   &\Leftrightarrow x \notin A \wedge x \notin B \\
   &\Leftrightarrow x \in A^c \wedge x \in B^c \\
   &\Leftrightarrow x \in A^c \cap B^c.
   \end{aligned}$$
   b) Show that: $A \setminus (A \setminus B) = A \cap B$. Let $x \in A \setminus (A \setminus B)$, then
   $$\begin{aligned}
   [x \in A \setminus (A \setminus B)] &\Leftrightarrow (x \in A) \wedge (x \notin (A \setminus B)) \\
   &\Leftrightarrow (x \in A) \wedge \overline{(x \in (A \setminus B))} \\
   &\Leftrightarrow (x \in A) \wedge \overline{(x \in A) \wedge (x \notin B)} \\
   &\Leftrightarrow (x \in A) \wedge [(x \notin A) \vee (x \in B)] \\
   &\Leftrightarrow [(x \in A) \wedge (x \notin A)] \vee [(x \in A) \wedge (x \in B)] \\
   &\Leftrightarrow [x \in \varnothing] \vee [x \in A \cap B] \\
   &\Leftrightarrow x \in \varnothing \cup (A \cap B) \\
   &\Leftrightarrow x \in (A \cap B).
   \end{aligned}$$

Exercise 1.3.5: I) Let A, B two sets

$$A = \left\{(x,y) \in \mathbb{R}^2 : 4x - y = 1\right\},$$

and

$$B = \left\{(t+1, 4t+3),\ t \in \mathbb{R}\right\}.$$

Prove that $A = B$.
II) Let A, B and C three sets given, show that

$$B \subset A \subset C \Longleftrightarrow A \cup B = A \cap C.$$

Solution:

I) Prove that $A = B$.

1. $A \subset B$: Let $(x,y) \in A$, with $4x - y = 1$, then $(x,y) = (x, 4x-1)$. Replacing X by $t+1$ we find

$$(x,y) = (x, 4x-1) = (t+1, 4t+3) \in B.$$

2. $B \subset A$: Let $(x,y) \in B$, then there exists $t \in \mathbb{R}$ such that $x = t+1$ and $y = 4t+3$. So

$$4x - y = 4(t+1) - (4t+3) = 1 \Rightarrow (x,y) \in A.$$

II) Let A, B and C three sets given, show that

$$B \subset A \subset C \Longleftrightarrow A \cup B = A \cap C.$$

1. $(\Rightarrow)$: We have

$$\begin{array}{rcl} B & \subset & A \Rightarrow A \cup B = A \\ & & \textit{and} \\ A & \subset & C \Longleftrightarrow A = A \cap C, \end{array}$$

then

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

2. $(\Longleftarrow)$: We have

$$\begin{array}{rcl} A & \subset & A \cup B \Rightarrow A \subset A \cap C \Rightarrow A \subset C \\ & & \textit{and} \\ B & \subset & A \cup B \Rightarrow B \subset A \cap C \Rightarrow B \subset A \wedge B \subset C \end{array}$$

then

$$B \subset A \subset C.$$

Exercise 1.3.6: Let the map(application) $f:\mathbb{R}\to\mathbb{R}$ be defined by:

$$f(x)=\begin{cases}\frac{1}{2} & if \quad x\leq 0\\ x+\frac{1}{2} & if \quad x>0\end{cases}$$

1. Draw the graph of f.
2. Determine $f([-1,1]);f^{-1}(\{0\});f^{-1}(\{\frac{1}{2}\});f^{-1}(]-\infty,1[)$.
3. The map f is it injective (one-to-one) ? is it surjective (onto)?, is it bijective (one-to-one correspondence)?
4. Find the interval for which the map f is bijective, then determine the reciprocal map f^{-1} in this interval.

Solution:

1. Determine
   - $f([-1,1])=f([-1,0])\cup f(]0,1])=\{\frac{1}{2}\}\cup]\frac{1}{2},\frac{3}{2}]=[\frac{1}{2},\frac{3}{2}]$.
   - $f^{-1}(\{0\})=\{x:f(x)=0\}=\varnothing$.
   - $f^{-1}(\{\frac{1}{2}\}=\{x:f(x)=\frac{1}{2}\}=]-\infty,0]$.
   - $f^{-1}(]-\infty,1[)=\{x:f(x)<1\}=]-\infty,\frac{1}{2}[$.
2. Injectivity, surjectivity and bijectivity.
   - The map f is not injective because $f(-3)=f(-2)$, but $-2\neq -3$. or $f(]-\infty,0])=\{\frac{1}{2}\}$.
   - The map f is not surjective because $f(x)=0$, does not accept solutions.
   - Finally f is not bijective.
3. Find the interval for which the map f is bijective.
   i) f it is injective if and anly if $x\in[0,+\infty[$.
   2i) f it is surjective if and anly if $y\in[\frac{1}{2},+\infty[$.
   3i) Then f is bijective if and anly if $x\in[0,+\infty[$ and $f(x)\in[\frac{1}{2},+\infty[$.
4. Determine the reciprocal map f^{-1} in this interval.

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

then

$$x=f^{-1}(y)\Leftrightarrow y=f(x)=x+\frac{1}{2}\Leftrightarrow x=y-\frac{1}{2}.$$

So

$$f^{-1}(y)=y-\frac{1}{2}.$$

Exercise 1.3.7: Let the following two maps $f:\mathbb{R}^2\to\mathbb{R}$ and $g:\mathbb{R}\to\mathbb{R}^2$ be defined by:

$$f(x,y)=xy, \text{ and } g(x)=\left(x^2,x\right).$$

1. Study the injectivity, surjectivity and bijectivity of f and g.
2. Find $f\circ g$ and $g\circ f$.

Solution:

1. Study the injectivity, surjectivity and bijectivity of f and g.
   - Injectivity of f: We have $f(2,5)=f(5,2)=10$, but $(2,5)\neq(5,2)$, then f is not injective.
   - Surjectivity of f: We have $\forall z\in\mathbb{R},\exists\,(x,y)\in\mathbb{R}^2 : z=xy$, take, for example $x=1,y=z$. Then f is surjective.
     Finally f is not bijective.
   - Surjectivity of g: The equation $(x^2,x)=(1,3)$ (For example), does not accept solutions in $\mathbb{R}$ then g is not surjective.
   - Injectivity of g: Let $a,b\in\mathbb{R}$ then
     $$\begin{aligned}[g(a)=g(b)] &\Rightarrow \left(a^2,a\right)=\left(b^2,b\right)\\ &\Rightarrow (a=b)\wedge\left(a^2=b^2\right)\\ &\Rightarrow (a=b)\wedge(a=b\vee a=-b)\\ &\Rightarrow [(a=b)\wedge(a=b)]\vee[(a=b)\wedge(a=-b)]\\ &\Rightarrow a=b.\end{aligned}$$
     Then g is injective.
     Finally g is not bijective.
2. Find $f\circ g$ and $g\circ f$.
   i) $g\circ f$:

   $$\mathbb{R}^2 \xrightarrow{f} \mathbb{R} \xrightarrow{g} \mathbb{R}, \quad g\circ f$$

   and $\forall\,(x,y)\in\mathbb{R}^2, g\circ f(x,y)=g\left[f(x,y)\right]=g(xy)=\left(x^2y^2,xy\right)$.
   ii) $f\circ g$:

   $$\mathbb{R} \xrightarrow{g} \mathbb{R}^2 \xrightarrow{f} \mathbb{R}, \quad f\circ g$$

   and $\forall x\in\mathbb{R}, f\circ g(x)=f\left[g(x)\right]=f(x^2,x)=x^3$.

1.3.5 Additional exercises

Exercise 1.3.8: Let $A;,B,C$ be three parts of a set E. Prove that:
a) $P(A\cap B)=P(A)\cap P(B)$.
b) $(A\cup B)\times C=(A\times C)\cup(B\times C)$.
c) $B\subset A\subset C\Longleftrightarrow A\cup B=A\cap C$.

Exercise 1.3.9: Let the map (application) $f : \mathbb{R}^2 \to \mathbb{R}^2$ be defined by

$$f(x,y) = (x+y, xy)$$

1. Show that $f(x,y) = f(y,x)$.
2. Find the inverse image (preimage) of the set $\{(0,1)\}$.
3. f is it injective (one-to-one) ?, surjective (onto)?

Exercise 1.3.10: PARTIE I: Let the function f be defined from $\mathbb{R}$ to $\mathbb{R}$ by:

$$\forall x \in \mathbb{R}, f(x) = \frac{x-1}{x^2+1}.$$

1. Prove that $f(a) = f\left(\frac{a+1}{a-1}\right)$ for all $a \neq 1$.
2. f is it injective? is it bijective (one-to-one correspondence)? Justify?

PARTIE II: Let h be the restriction of f on the interval $I = \left]-\infty, \left(1-\sqrt{2}\right)\right]$.

Exercise 1.3.11:

1. Prove that the equation $h(x) = m$ doesn't admit solutions if $m \in \mathbb{R}\backslash J$, where the interval $J = \left[\frac{-1}{2(\sqrt{2}-1)}, 0\right[$.
2. Prove that h is a bijection from I to the interval J.

2. Algebraic Structure

2.0.1 Internal composition law $(I.C.L)$

We say that the composition law $\star$ is an internal composition law $(I.C.L)$ of a set $\mathbb{E}$ if and only if

$$\forall (x,y) \in \mathbb{E} \times \mathbb{E} : (x \star y) \in \mathbb{E}.$$

■ **Exemples 2.1 :**

1.The law $\cap$ is an internal composition law of the set $\mathscr{P}(\mathbb{E})$ (set of parts of $\mathbb{E}$), because

$$\forall (A,B) \in \mathscr{P}(\mathbb{E}) \times \mathscr{P}(\mathbb{E}) : A \cap B \in \mathscr{P}(\mathbb{E}).$$

2. We define on $\mathbb{N}$ the law $\star$ by $n \star m = n + e^m$, then $\star$ is not a law of internal composition because $e^m \notin \mathbb{N}$.

Definitions

Let $\star$ and $\intercal$ be two internal composition laws of $\mathbb{E}$, then:

- The law $\star$ is associative if:

$$\forall (x,y,z) \in \mathbb{E} \times \mathbb{E} \times \mathbb{E}, \quad (x \star y) \star z = x \star (y \star z).$$

- The law $\star$ is commutative if:

$$\forall (x,y) \in \mathbb{E} \times \mathbb{E}, \quad x \star y = y \star x.$$

- We say that e is a neutral (an identity) element of the law $\star$ if:

$$\exists e \in \mathbb{E}, \ \forall x \in \mathbb{E}, \quad x \star e = e \star x = x.$$

- An element x is invertible in $\mathbb{E}$, if there exists $x' \in \mathbb{E}$ (called the inverse of x) such that:

$$\forall x \in \mathbb{E},\ \exists x' \in \mathbb{E} : x' \star x = x \star x' = e$$

We say that $\star$ is distributive with recpect to $\intercal$, if: $\forall (x,y,z) \in \mathbb{E} \times \mathbb{E} \times \mathbb{E}$,

$$x \star (y \intercal z) = (x \star y) \intercal (x \star z) \quad \text{and} \quad (y \intercal z) \star x = (x \star y) \intercal (x \star z).$$

■ **Exemples 2.2 :**

1. Let E a set. we provide $\mathscr{P}(\mathbb{E})$ by the internal composition law $\cap$:
-The law $\cap$ is associative $(A \cap B) \cap C = A \cap (B \cap C)$.
-The law $\cap$ is commutative $A \cap B = B \cap A$.
-The law $\cap$ accept a neutral element E: $A \cap E = E \cap A = A$
-The law $\cap$ does not accept an inverse element.
2. We define on $\mathbb{Z}$ the law of internal composition $\intercal$ by $n \intercal m = n + m - 3$
-$\intercal$ is associative
$(n \intercal m) \intercal p = (n + m - 3) \intercal p = n + m - 3 + p - 3 = n + m + p - 6$,
$n \intercal (m \intercal p) = n \intercal (m + p - 3) = n + m + p - 3 - 3 = n + m + p - 6$.
-$\intercal$ is a commutative $n \intercal m = n + m - 3 = m + n - 3 = m \intercal n$
-$\intercal$ accept a neutral element $e = 3 : n + e - 3 = n \Longrightarrow e = 3$
- An inverse element of n with recpect to $\intercal$ is $n' = 6 - n : n + n' - 3 = 3 \Longrightarrow n' = 6 - n$

Proposition 2.0.1 Let $\star$ be an internal composition law in $\mathbb{E}$, then following properties hold:

- The neutral element is unique;
- The inverse of any element $x \in \mathbb{E}$ is unique (i.e., x has only one inverse, i.e., if x has 2 inverses then they are equal);
- For every $x \in \mathbb{E}$, $\left(x^{-1}\right)^{-1} = x$.
- For every $x, y \in \mathbb{E}$, $(x \star y)^{-1} = y^{-1} \star x^{-1}$.

Proof.

- The neutral element is unique: Let e and s be two neutral elements, then by the definition we have

$$e = e \star e' = e' \star e, \text{ and } e' = e \star e' = e' \star e,$$

so

$$e = e'.$$

- The inverse of any element $x \in \mathbb{E}$ is unique: By Definition, let x_1^{-1}, x_2^{-1} be two inverses of x, which means that $x \star x_1^{-1} = x_1^{-1} \star x = e$.and $x \star x_2^{-1} = x_2^{-1} \star x = e$. Computing $x_1^{-1} \star x \star x_2^{-1}$ we obtain:

$$x_1^{-1} \star x \star x_2^{-1} = e \star x_2^{-1} = x_2^{-1} \text{ (using that } x_1^{-1} \star x = e \text{)},$$

and

$$x_1^{-1} \star x \star x_2^{-1} = x_1^{-1} \star e = x_1^{-1} \text{ (using that } x \star x_2^{-1} = e \text{)}.$$

So

$$x_1^{-1} = x_2^{-1}.$$

- For every $x \in \mathbb{E}$, $\left(x^{-1}\right)^{-1} = x$: We want to show that the inverse of x^{-1} is equal to x, then

$$e = \left(x^{-1}\right)^{-1} \star x^{-1} \Leftrightarrow x \star x^{-1} = \left(x^{-1}\right)^{-1} \star x^{-1}$$

and

$$e = x^{-1} \star \left(x^{-1}\right)^{-1} \Leftrightarrow x \star x^{-1} = x^{-1} \star \left(x^{-1}\right)^{-1}.$$

So

$$\left(x^{-1}\right)^{-1} = x.$$

- For every $x, y \in \mathbb{E}$, $(x \star y)^{-1} = y^{-1} \star x^{-1}$:

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

In the same way we show that

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

then we deduce that $(x \star y)$ is invertible and that

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

■

2.0.2 Group Structure

Groups

Définition 2.0.1 We call a group any group provided with an I.C.L which we note "$\star$", such that

1. $\star$ is associative,
2. $\star$ has a neutral element,
3. Every element of $\mathbb{G}$ has an inverse with recpect to $\star$.

We denote $(\mathbb{G}, \star)$ group. If, $\star$ is commutative, then $(\mathbb{G}, \star)$ is called a **commutative group** or **abelian group**.

▪ **Exemples 2.3 :**

$(\mathbb{R}, +), (\mathbb{Z}+), (\mathbb{C}, +)$ and $(\mathbb{Q}^*, .)$ are groups.

Subgroups

Let $(\mathbb{G}, \star)$ be a group, of the neutral element e and let $\mathbb{H} \subset \mathbb{G}$ with $\mathbb{H} \neq \varnothing$. We say that $(\mathbb{H}, \star)$ is a subgroup of $(\mathbb{G}, \star)$, if and only if

$$\begin{cases} 1).e \in \mathbb{H}, \\ 2).\forall a, b \in \mathbb{H}, \ a \star b \in \mathbb{H}, \\ 3).\forall a \in \mathbb{G}, \quad a \in \mathbb{H} \Longrightarrow a^{-1} \in \mathbb{H}. \end{cases}$$

▪ **Exemples 2.4 :**

$(\mathbb{G}, \star), (\{e\}, \star)$ are subgroups.

Proposition 2.0.2 Let $(\mathbb{G},\star)$ be a group and $\mathbb{H}\subset\mathbb{G}$, then

$$\mathbb{H} \text{ is a subgroup of } \mathbb{G} \Longleftrightarrow \begin{cases} \mathbb{H}\neq\varnothing \\ \forall a,b\in\mathbb{H},\ \ a\star b^{-1}\in\mathbb{H}. \end{cases}$$

Proof. **1.** Let $\mathbb{H}$ be a subgroup of $(\mathbb{G},\star)$, then :

i) e an neutral element in $\mathbb{H}$, then $\mathbb{H}\neq\varnothing$.

ii) Let $a,b\in\mathbb{H}$, since $\mathbb{H}$ provided with the law $\star$ is a group then b^{-1} exists in $\mathbb{H}$ and since $\mathbb{H}$ is stable with recpect to $\star$ we deduce that $a\star b^{-1}\in\mathbb{H}$.

2. Conversely, let $\mathbb{H}$ be a subset of $\mathbb{G}$ such that $\begin{cases} \mathbb{H}\neq\varnothing \\ \forall a,b\in\mathbb{H},\ \ a\star b^{-1}\in\mathbb{H}. \end{cases}$

Show that $(\mathbb{H},\star)$ is a group.

i) As $\mathbb{H}\neq\varnothing$ then $\exists a\in\mathbb{H}$ and according to the second hypothesis

$$e=a\star a^{-1}\in\mathbb{H},$$

which shows that the law $\star$ accept a neutral element e in $\mathbb{H}$.

ii) Let $x\in\mathbb{H}$, since $e\in\mathbb{H}$ then according to the second hypothesis we will have $x^{-1}=e\star x^{-1}\in\mathbb{H}$

which shows that for every element x in $\mathbb{H}$ is invertible in $\mathbb{H}$ with recpect to the law $\star$ to $\mathbb{H}$.

iii) The law $\star$ in $\mathbb{H}$ is an internal composition law, because for all x and y in $\mathbb{H}$, according to **ii)** we have $y^{-1}\in\mathbb{H}$ and using the second hypothesis we deduce that $x\star y=x\star(y^{-1})^{-1}\in\mathbb{H}$.

iv) The law $\star$ in $\mathbb{H}$ is associative, because $\star$ is associative in $\mathbb{G}$. ■

R From i) the prove of the previous proposition, we see that: If e is the neutral element of a group $\mathbb{G}$, then every subgroup of $\mathbb{G}$ contains e and we deduce the following corollary.

Corollary 2.0.3 Let $(\mathbb{G},\star)$ is a group and $\mathbb{H}\subset\mathbb{G}$, then

$$\mathbb{H} \text{ is a subgroup of } \mathbb{G} \Longleftrightarrow \begin{cases} e\in\mathbb{H} \\ \forall a,b\in\mathbb{H},\ \ a\star b^{-1}\in\mathbb{H}. \end{cases}$$

■ **Exemples 2.5** : Let $(\mathbb{G},\star)$ be a group and $H=\{a\in\mathbb{G};a\star x=x\star a,\forall y\in\mathbb{G}\}$, then $\mathbb{H}$ is a subgroup of $\mathbb{G}$. Indeed,

i) If e is a identity element of $\star$, then $e\in\mathbb{H}$ because : $\forall x\in\mathbb{G},\ \ e\star x=x\star e=x$

ii) Let $a,b \in \mathbb{H}, c \in \mathbb{G}$ $\left(a \star b^{-1} \overset{?}{\in} \mathbb{H}\right)$, then

$$\begin{aligned}
\left(a \star b^{-1}\right) \star c &= \left(a \star b^{-1}\right) \star \left(c^{-1}\right)^{-1} \\
&= a \star \left(b^{-1} \star \left(c^{-1}\right)^{-1}\right) \quad \text{because } \star \text{is associative,} \\
&= a \star \left(c^{-1} \star b\right)^{-1} \\
&= a \star \left(b \star c^{-1}\right)^{-1} \quad \text{because } b \in \mathbb{H} \\
&= a \star \left((b^{-1})^{-1} \star c^{-1}\right)^{-1} \\
&= a \star (c \star b^{-1}) \\
&= (a \star c) \star b^{-1} \quad \text{because } \star \text{is associative} \\
&= (c \star a) \star b^{-1} \quad \text{because } a \in \mathbb{H} \\
&= c \star (a \star b^{-1}) \quad \text{because } \star \text{is associative}
\end{aligned}$$

hence shows that $a \star b^{-1} \in \mathbb{H}$.
From i) and ii) we deduce that $\mathbb{H}$ is a subgroup of $\mathbb{G}$

2.0.3 Ring Structure

Rings

Définition 2.0.2 Let the set $\mathbb{A}$ provided with two internal composition laws $\star$.and $\intercal$ We say that $(\mathbb{A}, \star, \intercal)$ is a ring if and only if

1. $(\mathbb{A}, \star)$ is commutative group,
2. $\intercal$ is an associative,
3. $\intercal$ is a distributive on $\star$,
4. $\intercal$ accept a neutral element.

If $\intercal$ is a commutative, then $(\mathbb{A}, \star, \intercal)$ is called a commutative ring.

- Let $(\mathbb{A}, \star)$ be a group, then x has an inverse we denote $-x$.
- If $\intercal$ has a neutral element, we note it 1 or $1_{\mathbb{A}}$ and we say that the ring $(\mathbb{A}, \star, \intercal)$ is unitary
- For all $x \in \mathbb{A}$, it is invertiblewith recpect to the second law $\intercal$ The inverse of an element $x \in \mathbb{A}$ is denoted x^{-1}.
- Let $(\mathbb{A}, \star, \intercal)$ be a commutative ring. We say that $y \in \mathbb{A} - \{0_{\mathbb{A}}\}$ is a divisor of x, if

$$\exists z \in \mathbb{A} - \{0_{\mathbb{A}}\}, \quad x = y \intercal z.$$

- If 0_A does not have a divisor in $\mathbb{A}$, we say that $(\mathbb{A}, \star, \intercal)$ is an integrity ring.

■ **Exemples 2.6 :**

1. $(\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are rings.
2. Let $\mathbb{E}$ be a non-empty set. $(\mathscr{P}(\mathbb{E}), \cap, \cup)$ is not a ring.

Sub-Rings

Définition 2.0.3 Let $(\mathbb{A}, \star, \intercal)$ be a ring with $0_{\mathbb{A}}$ is the neutral element of $\star$ and 1_A is the neutral element of $\intercal$. Let $\mathbb{H}$ be a subset of $\mathbb{A}$. We say that $(\mathbb{H}, \star, \intercal)$ is a subring of $((\mathbb{A}, \star, \intercal)$ if and only if

1. $(\mathbb{H}, \star)$ is a subgroup of $(\mathbb{A}, \star)$,

2. $\forall x,y \in \mathbb{H},\ x \intercal y \in \mathbb{H}$,
3. $1_A \in \mathbb{H}$

■ **Exemples 2.7 :**

1. $(\mathbb{Q},+,\times)$ is a subring of $(\mathbb{R},+,\times)$.
2. $(\mathbb{Z},+,\times)$ is a subring of $(\mathbb{Q},+,\times)$.

Proposition 2.0.4 A subset $\mathbb{H}$ of $\mathbb{A}$ is a subring if and only if:

1. $\mathbb{H} \neq \varnothing$,
2. $\forall x,y \in \mathbb{H},\ (x \star y^{-1}) \in \mathbb{H}$
3. $\forall x,y \in \mathbb{H},\ (x \intercal y) \in \mathbb{H}$.

Proof. We know that $\mathbb{H}$ is a subgroup of $(\mathbb{A},*)$ if and only if

$$(\mathbb{H} \neq \varnothing) \wedge (\forall x,y \in \mathbb{H},\ (x \star y^{-1}) \in \mathbb{H}),$$

so for $\mathbb{H}$ to be a subring of $\mathbb{A}$, it suffices to see if the restriction of the second law $\intercal$ is internal in $\mathbb{H}$, It's enough to show that $(\forall x,y \in \mathbb{H},\ (x \intercal y) \in \mathbb{H})$, which completes the proof of our proposition. ■

2.0.4 Field Structure

Fields

Définition 2.0.4 Let the set $\mathbb{K}$ provided with two internal composition laws $\star$.and $\intercal$ We say that $(\mathbb{K},\star,\intercal)$ is a field if and only if

1. $(\mathbb{K},\star,\intercal)$ is a ring,
2. $\intercal$ accept an identity element $1_{\mathbb{K}}$,
3. For every element in $\mathbb{K}-\{e_\star\}$ has an inverse in $\mathbb{K}$ with respect to $\intercal$. (Where $e_\star$ is an identity element of $\star$)

If $\intercal$ is commutative, then $(\mathbb{K},\star,\intercal)$ is called a **commutative field.**

■ **Exemples 2.8 :**

1. $(\mathbb{R},+,\times),(\mathbb{Q},+,\times)$ and $(\mathbb{C},+,\times)$ are fields.
2. Let $\mathbb{E}$ be a non-empty set. $(\mathscr{P}(E),\cap,\cup)$ is not a field.

Proposition 2.0.5 Every body is an integral ring.

Subfield

Définition 2.0.5 We call subfield, of a body $(\mathbb{K},\star,\intercal)$, any subset $\mathbb{K}'$ of $\mathbb{K}$ such that, provided with the restrictions of the laws $\star$ and $\intercal$, is a body. $\mathbb{K}' \subset \mathbb{K}$ is a subfield of $(\mathbb{K},\star,\intercal)$ if and only if

1. $\mathbb{K}' \neq \varnothing$,
2. $\forall x,y \in \mathbb{K}',\ (x \star y),(x \intercal y) \in \mathbb{K}'$.

2.1 Exercises

Exercise 2.1.1: Study the properties (ICL, Commutativity, Associativity, Neutral element, Inverse element) on $\mathbb{E}$, for the following composition laws $\star$:

1. $\mathbb{E} = \mathbb{R}$ and $x \star y = x + y - 1$.
2. $\mathbb{E} = \mathbb{Z}$ and $x \star y = x + y - x^2 y$.

$(\mathbb{E},\star)$ is it a commutative group?

Solution:

1. For the first law:
   - i) ICL: $\star$ is an internal composition law in $\mathbb{R}$, because: $\forall (x,y) \in \mathbb{R}\times\mathbb{R}, x+y-1 \in \mathbb{R}$.
   - 2i) Commutativity: $\star$ is a commutative, because: $\forall (x,y) \in \mathbb{R}\times\mathbb{R}, x\star y = x+y-1 = y+x-1 = y\star x$.
   - 3i) Associativity: $\star$ is an associative, because: $\forall (x,y) \in \mathbb{R}\times\mathbb{R}$:

$$\begin{cases} (x\star y)\star z = (x+y-1)\star z = (x+y-1)+z-1 = x+y+z-2, \\ \text{and} \\ x\star(y\star z) = x+(y\star z)-1 = x+(y+z-1)-1 = x+y+z-2 \end{cases}$$

   - 4i) Neutral element: $\exists^? e \in \mathbb{R}, \forall x \in \mathbb{R}; x\star e = e\star x = x$,

$$x\star e = x+e-1 = x \Longrightarrow e = 1.$$

   - 5i) Invese element: $\forall x \in \mathbb{R}, \exists^? x' \in \mathbb{R}; x\star x' = x'\star x = 1$,

$$x\star x' = x+x'-1 = 1 \Longrightarrow x' = 2-x \in \mathbb{R}.$$

   Then, $(\mathbb{R},\star)$ is a commutative group.

2. For the second law:
   - i) ICL: $\star$ is an internal composition law in $\mathbb{Z}$, because: $\forall (x,y) \in \mathbb{Z}\times\mathbb{Z}, x+y-x^2y \in \mathbb{Z}$.
   - 2i) Commutativity: $\star$ is not a commutative, because: $\forall (x,y) \in \mathbb{Z}\times\mathbb{Z}, x\star y = x+y-x^2y \neq x+y-y^2x = y\star x$.
   - 3i) Associativity: $\star$ is not an associative, because: $\forall (x,y) \in \mathbb{Z}\times\mathbb{Z}$:

$$\begin{cases} (x\star y)\star z = (x\star y)+z-(x\star y)^2 z = \left(x+y-x^2y\right)+z-\left(x+y-x^2y\right)^2 z \\ \text{and} \\ x\star(y\star z) = x+(y\star z)-x^2\,(y\star z) = x+\left(y+z-y^2z\right)-x^2\left(y+z-y^2z\right). \end{cases}$$

   Then $(x\star y)\star z \neq x\star(y\star z)$.
   - 4i) Neutral element: $\exists^? e \in \mathbb{Z}, \forall x \in \mathbb{Z}; x\star e = e\star x = x$,

$$x\star e = x+e-x^2e = x \Longrightarrow e(1-x^2) = 0 \Longrightarrow e = 0, \quad \text{(to the right)}$$

   and

$$e\star x = e+x-e^2x = x \Longrightarrow e(1-ex^2) = 0 \Longrightarrow e = 0. \quad \text{(to the left)}$$

   Then $e = 0$.

5i) Invese element: $\forall x \in \mathbb{Z}, \exists^{?} x' \in \mathbb{Z}; x \star x' = x' \star x = 0,$

$$x \star x' = x + x' - x^2 x' = 0 \Longrightarrow x' = \frac{x}{x^2 - 1} \notin \mathbb{Z}. \text{ (in general)}$$

For example for $x = \pm 1$ or $x = 2$, does not exist x' in $\mathbb{Z}$ such that $\pm 1 \star x = 0$ or $2 \star x = 0$.
So x does not accept an inverse on $\mathbb{Z}$. Then $(\mathbb{Z}, \star)$ does not form a group.

Exercise 2.1.2: We define the composition law $\star$ on $\mathbb{E} = \mathbb{R}^* \times \mathbb{R}$, by:

$$\forall (a,b), (c,d) \in \mathbb{E} : (a,b) \star (c,d) = (ac, ad + b).$$

Show that $(\mathbb{E}, \star)$ is a non-commutative group.

Solution:

1) ICL: $\star$ is an internal composition law in $\mathbb{R}^* \times \mathbb{R}$, because: $\forall (a,b), (c,d) \in \mathbb{R}^* \times \mathbb{R} : ac \in \mathbb{R}^*$, and $ad + b \in \mathbb{R}$.
2) Commutativity: $\star$ is not a commutative, because: $\forall (a,b), (c,d) \in \mathbb{R}^* \times \mathbb{R} : ad + b \neq ca + d$.
3) Associativity: $\star$ is an associative, because: $\forall (a,b), (c,d), (x,y) \in \mathbb{R}^* \times \mathbb{R}$:

$$\begin{cases} \{(a,b) \star (c,d)\} \star (x,y) = (acx, acy + ad + b), \\ \text{and} \\ (a,b) \star \{(c,d) \star (x,y)\} = (acx, acy + ad + b). \end{cases}$$

4) Neutral element: $\exists^{?} (e,f) \in \mathbb{R}^* \times \mathbb{R}, \forall (a,b) \in \mathbb{R}^* \times \mathbb{R}; (a,b) \star (e,f) \overset{1}{=} (a,b) \overset{2}{=} (e,f) \star (a,b)$,
   $\overset{1}{=})$: $(a,b) \star (e,f) = (a,b) \Longrightarrow (ae, af + b) = (a,b) \Rightarrow \{e = 1$ and $f = 0$,
   and
   $\overset{2}{=})$: $(e,f) \star (a,b) = (a,b) \Longrightarrow (ea, eb + f) = (a,b) \Rightarrow \{e = 1$ and $f = 0$,
   then $(e,f) = (1,0)$.
5) Invese element: $\forall (a,b) \in \mathbb{R}^* \times \mathbb{R}, \exists^{?} (a',b') \in \mathbb{R}^* \times \mathbb{R}; (a,b) \star (a',b') \overset{1}{=} (1,0) \overset{2}{=} (a',b') \star (a,b)$,
   $\overset{1}{=})$: $(a,b) \star (a',b') = (1,0) \Longrightarrow (aa', ab' + b) = (1,0) \Rightarrow \left\{ a' = \frac{1}{a} \text{ and } b' = \frac{-b}{a}, \right.$
   and
   $\overset{2}{=})$: $(a',b') \star (a,b) = (1,0) \Longrightarrow (a'a, a'b + b') = (1,0) \Rightarrow \left\{ a' = \frac{1}{a} \text{ and } b' = \frac{-b}{a}, \right.$
   then $(a',b') = \left(\frac{1}{a}, \frac{-b}{a}\right)$.
   Then, $(\mathbb{E}, \star)$ is a non-commutative group.

Exercise 2.1.3:

1. Let $(\mathbb{G},\star)$ be a non-commutative group. Show that the center
$$C(\mathbb{G}) = \{a \in \mathbb{G}; x\star a = a\star x, \forall x \in \mathbb{G}\},$$
is a subgroup of $(\mathbb{G},\star)$.
2. Show that the center $\mathbb{A} = \{(a,0); a \in \mathbb{Z}\}$ is a subgroup of $\left(\mathbb{Z}^2,+\right)$.

Solution:

1) Show that the center $C(\mathbb{G}) = \{a \in \mathbb{G}; x\star a = a\star x, \forall x \in \mathbb{G}\}$ is a subgroup of $(\mathbb{G},\star)$. (let e be a neutral element)
   (a) $C(\mathbb{G}) \neq \varnothing$, because $\forall x \in \mathbb{G} : x\star e = e\star x \Rightarrow e \in C(\mathbb{G})$.
   (b) Let $a \in C(\mathbb{G}) : a^{-1} \overset{?}{\in} C(\mathbb{G})$, then let $x \in \mathbb{G}$:
$$\begin{aligned} x\star a^{-1} &= e\star x\star a^{-1} \\ &= a^{-1}\star a\star x\star a^{-1} \\ &= a^{-1}\star x\star a\star a^{-1} \\ &= a^{-1}\star x\star e = a^{-1}\star x, \end{aligned}$$
   then $a^{-1} \in C(\mathbb{G})$.
   (a) Let $a,b \in C(\mathbb{G}) : a\star b \overset{?}{\in} C(\mathbb{G})$, then let $x \in \mathbb{G}$:
$$x\star a\star b = a\star x\star b = a\star b\star x,$$
   so $a\star b \in C(\mathbb{G})$, and finally $C(\mathbb{G})$ is a subgroup of $(\mathbb{G},\star)$.
2) Show that the center $\mathbb{A} = \{(a,0); a \in \mathbb{Z}\}$ is a subgroup of $\left(\mathbb{Z}^2,+\right)$. (**Remark** $(0,0)$ is a neutral element of $\left(\mathbb{Z}^2,+\right)$ and $(-a,-b)$ is an inverse element of (a,b)).
   (a) $\mathbb{A} \neq \varnothing$, because $(0,0) \in \mathbb{A}$.
   (b) For all $(a,0) \in C(\mathbb{G}) : (-a,0) \in \mathbb{A}$, because $-a \in \mathbb{Z}$
   (c) For all $(a,0),(b,0) \in \mathbb{A} : (a,0)+(b,0) = (a+b,0) \in \mathbb{A}$, because $a+b \in \mathbb{Z}$
   Finally $\mathbb{A}$ is a subgroup of $\left(\mathbb{Z}^2,+\right)$.

Exercise 2.1.4: We consider on $\mathbb{R}$ the following two internals composition laws:
$$x\oplus y = x+y-1, \quad \text{and} \quad x\otimes y = x+y-xy.$$

1. Show that $\otimes$ is an associative and a commutative.
2. $(\mathbb{R},\oplus,\otimes)$ is it a commutative ring?
3. $(\mathbb{R},\oplus,\otimes)$ is it a field?

Solution:

1 Show that $\otimes$ is an associative and a commutative. So, let $x,y,z \in \mathbb{R}$, then
$$x\otimes y = x+y-xy = y+x-yx = y\otimes x,$$
and therefore $\otimes$ is a commutative. And for the asociativity, show that $x\otimes$

$(y\otimes z)=(x\otimes y)\otimes z$

$$\begin{aligned}(x\otimes y)\otimes z &= (x\otimes y)+z-(x\otimes y)z\\ &= x+y+z-xy-xz-yz+xyz\end{aligned}$$

and

$$\begin{aligned}x\otimes(y\otimes z) &= x+(y\otimes z)-x(y\otimes z)\\ &= x+y+z-xy-xz-yz+xyz.\end{aligned}$$

Hence the associativity

2 $(\mathbb{R},\oplus,\otimes)$ is it a commutative ring?

(a) $(\mathbb{R},\oplus)$ it is a commutative group (See exercise 1) ii) $\otimes$ is an associative and a commutative.(Question 1)

(b) $\otimes$ accept a neutral element (so be it e'): show that $\exists e'\in\mathbb{R},\forall x\in\mathbb{R}; x\otimes e'=e'\otimes x=x$.

$$e'\otimes x=x\otimes e'=x+e'-xe'=x\Leftrightarrow e'(1-x)=0\Leftrightarrow e'=0,$$

Then $e'=0$.

(c) $\otimes$ is distributive on $\oplus$. So, let $x,y,z\in\mathbb{R}$, it is enough to verify that

1) : $(x\oplus y)\otimes z=(x\otimes z)\oplus(y\otimes z)$

and

2) : $x\otimes(y\oplus z)=(x\otimes y)\oplus(x\otimes z)$

and sinse $\otimes$ is a commutative, so it is enough to verify 1) or 2), then

$$\begin{aligned}(x\oplus y)\otimes z &= (x\oplus y)+z-(x\oplus y)z\\ &= (x+y-1)+z-(x+y-1)z=x+y+2z-xz-yz-1\end{aligned}$$

and

$$\begin{aligned}(x\otimes z)\oplus(y\otimes z) &= (x\otimes z)+(y\otimes z)-1\\ &= x+z-xz+y+z-yz-1=x+y+2z-xz-yz-1\end{aligned}$$

Hence $\otimes$ is distributive on $\oplus$.

Conclusion: $(\mathbb{R},\oplus,\otimes)$ is a commutative ring.

3 $(\mathbb{R},\oplus,\otimes)$ is it a field

It is enough to verify that there exist an inverse element for all $x\in\mathbb{R}-\{e=1\}$ with recpect to the law $\otimes$. So let $x\in\mathbb{R},\exists^{?}x'\in\mathbb{R}$, such that $x\otimes x'=x'\otimes x=0$,

$$x\otimes x'=x'\otimes x=0\Longrightarrow x+x'-xx'=0\Longrightarrow x'=\frac{x}{1-x}.$$

Then for all $x\in\mathbb{R}-\{1\}$, accept an inverse element $x'=\frac{x}{1-x}\in\mathbb{R}$.
Finallywe conclude that $(\mathbb{R},\oplus,\otimes)$ is a commutative ring.

2.2 Additional exercises

Exercise 2.2.1: We define the internal composition law $\triangle$ on $\mathbb{Q}$, by:

$$\forall\alpha,\beta\in\mathbb{Q}:\alpha\triangle\beta=(\alpha-1)(\beta-1)+1.$$

$(\mathbb{Q},\triangle)$ is it a commutative group?

Exercise 2.2.2: We consider on $\mathbb{R}$ the following two internals composition laws:

$$x \oplus y = x + y - 2, \quad \text{and} \quad x \otimes y = xy - 2x - 2y + 6.$$

1. Show that $(\mathbb{R}, \oplus)$ is a commutative group.
2. Show that $\otimes$ is associative and that it accept a neutral element.
3. $(\mathbb{R}, \oplus, \otimes)$ is it a commutative ring?
4. $(\mathbb{R}, \oplus, \otimes)$ is it a body?

Exercise 2.2.3: Let $(\mathbb{R}, \star)$ be a commutative group, and e it is neutral element.
PART I: Let $H = \{x \in \mathbb{R} : x \star x = e\}$ a subset of $\mathbb{R}$.
- Prove that $(H, \star)$ is a subgroup of $(\mathbb{R}, \star)$.
PART II: Let the law $\star$ defined by:

$$\forall x, y \in \mathbb{R}; \quad x \star y = x + y - 2.$$

And for all $n \in \mathbb{N}^*$, we pose $x^{(1)} = x$ and $x^{(n+1)} = x^{(n)} \star x$

(a) Calculate $x^{(2)}$, $x^{(3)}$ and $x^{(4)}$.
(b) Prove that $\forall n \in \mathbb{N}^* : x^{(n)} = nx - 2(n-1)$.

3. Rings of Polynomials

3.0.1 Concepts

In the following, $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$

- A polynomial P, is an expression of the form

$$P = \sum_{i=n}^{i=0} a_i X^i = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

  where $n \in \mathbb{N}$, and the coefficients $a_i, i \in \{0, ..., n\}$, are elements of $\mathbb{K}$.
- The set of all polynomials with coefficients in $\mathbb{K}$ is denoted by $\mathbb{K}[X]$.

$$\mathbb{K}[X] = \{ \text{ the polynomials with coefficients in } \mathbb{K}\}.$$

- A polynomial $P \in \mathbb{K}[X]$ is said to be zero polynomial if all the coefficients a_n are zero, i.e

$$P = 0 \Longleftrightarrow a_n = a_{n-1} = \cdots = a_1 = a_0 = 0$$

- If $a_n \neq 0$ then the degree of P is n, and we note $\deg P = n$, so

$$\deg P \leq n \Longleftrightarrow P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

- By convention the degree of the zero polynomial is $-\infty$ ($\deg(0) = -\infty$.)
- If $a_n = 1$, we say that P is the **monic (unitary)** polynomial.

■ **Exemples 3.1** 1) $P_1 = X^6 - X + 8$, is a polynomial in $\mathbb{R}[X]$
2) $P_2(X) = X^4 + 5X^2 - iX$ is a polynomial in $\mathbb{C}[X]$
3) $Q_1 = X^6 - \sqrt{X} + 8$, $Q_2(X) = X^4 + 5\sin\left(X^2\right) - \frac{X}{X^2+1}$ are not polynomials
4) $P_3 = X^7 - 8X^4 + 13$ is monic polynomail and $\deg P_3 = 7$.

3.0.2 Operations on $\mathbb{K}[X]$

On $\mathbb{K}[X]$ we define the following laws, if $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0, Q = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0$, then:

1. $P = Q \iff a_i = b_i \ \ \forall i \in \{0,1,\ldots,n\}$
2. $P \pm Q = \sum_{i=\max(n,m)}^{i=0} (a_i \pm b_i) X^i$, and $\deg(P \pm Q) = \max(\deg P, \deg Q)$.
3. $\lambda P = \sum_{i=n}^{i=0} \lambda a_i X^i$, with $\lambda \in \mathbb{K}$, and $\deg(\lambda P) = \deg P$.
4. $PQ = \sum_{k=n+m}^{k=0} c_k X^k$ such that $c_k = \sum_{i=k}^{i=0} a_i b_{k-i}$.$(a_k = 0, \forall k \geq n+1,\ b_k = 0, \forall k \geq m+1)$, and $\deg(PQ) = \deg P + \deg Q$.
5. $\mathbb{K}[X]$ is stable for these laws, we say that it is an algebra

▪ **Exemples 3.2** $P = X^3 + 1$, $Q = X^5 - X$, then

$$2P - 3Q = -3X^5 + 2X^3 + 3X + 2, \text{ and } \deg(2P - 3Q) = \deg g = 5.$$

and

$$\begin{aligned} PQ &= \sum_{k=8}^{k=0} c_k X^k = X^8 + X^5 - X^4 - X, \text{and } \deg(PQ) = \deg P + \deg Q = 8. \\ c_8 &= c_5 = 1, c_7 = c_6 = c_3 = c_2 = c_0 = 0, \text{and } c_1 = -1. \end{aligned}$$

Associated polynomials

We say that A and B are associated if, and only if:

$$\exists k \in \mathbb{K} \ \ A = kB \ \text{ or } \ B = kA.$$

▪ **Exemples 3.3** The polynomials $X - \frac{1}{2}, 2X - 1, -2X + 1$ are associated.

3.0.3 Polynomial Division

Theorem 3.0.1 Euclidean division $\forall A, B \in \mathbb{K}[X]$such that $B \neq 0$, $\exists Q, R \in \mathbb{K}[X]$ unique such that $A = BQ + R$ with $\deg R < \deg B$, or $R = 0$. Q is called the quotient of the Euclidean division of A by B and R the remainder The rest).

Proof. • **Existence**: Let $B = b_0 + b_1X + \ldots + b_pX^p \in \mathbb{K}[X]$ be a fixed. The reasoning is then done by induction on the degree of the polynomial A. The hypothesis of recurrence at rank n, $\mathscr{P}(n)$ is:

$$\forall A \in \mathbb{K}[X] \quad \deg(A) \leq n, \ \ \exists (Q,R) \in \mathbb{K}[X] \quad A = BQ + R \ \ et \ \ \deg(R) < \deg(B).$$

We notice if $n < p$, then $\mathscr{P}(n)$ is true: $A = B.0 + A$. Let $n \geq p$ and assume the recurrence hypothes is true for all $k \leq n-1$ and show that then $\mathscr{P}(n)$ is true. The polynomial A is written

$$A = a_0 + a_1X + \cdots + a_nX^n, \text{ where } a_n \neq 0.$$

Let us then consider the polynomial $C = A - \frac{a_n}{b_p}X^{n-p}B$. The degree of $\deg C \leq n-1$. By induction hypothesis we then know that there exists a pair of polynomials (Q,R)

such that: $C = BQ+R$ and $\deg(R) < \deg(B)$. It follows that $A = B(Q+\frac{a_n}{b_p}X^{n-p})+R$, with $\text{ddeg}(R) < \deg(B)$.

- **Uniqueness :** Suppose that $A = BQ+R = BQ'+R'$ with $\deg R < \deg B$ et $\deg R' < \deg B$ Then $\deg(R-R') \leq \max(\deg R, \deg R') < \deg B$ or $R-R' = B(Q'-Q)$. Hence

$$\deg(Q'-Q) < 0 \Rightarrow Q'-Q = 0.$$

We deduce $Q = Q'$ and $R = R'$.
B divides A if and only if the rest of the Euclidean division of A by B is zero polynomail.

■

■ **Exemples 3.4** 1. Let $P = X^5 - X + 2, Q = X^3 + 1$ be two polynomail in $\mathbb{K}[X]$. Let us divide Q by P

$$\begin{array}{r|l} x^5 \quad -x+2 & x^3+1 \\ \cline{2-2} -x^5-x^2 & x^2 \\ \cline{1-1} -x^2-x+2 & \end{array}$$

Therefore,

$$\frac{X^5-X+2}{X^3+1} = X^2 + \frac{-X^2-X+2}{X^3+1}$$

or equivalently,

$$X^5 - X + 2 = X^2\left(X^3+1\right) + \left(-X^2-X+2\right).$$

That is $A = BQ+R$ where $Q = X^2$, and $R = -X^2-X+2$.

2.

$$\begin{array}{r|l} 2X^4 \; -X^3 \; +X^2 \; +X-1 & 2X^2-3X \\ \cline{2-2} -2X^4+3X^3 & X^2+X+2 \\ \cline{1-1} \quad 2X^3 \; +X^2 & \\ \quad -2X^3+3X^2 & \\ \cline{1-1} \quad\quad 4X^2 \; +X & \\ \quad\quad -4X^2+6X & \\ \cline{1-1} \quad\quad\quad 7X-1 & \end{array}$$

then $2X^4 - X^3 + X^2 + X - 1 = \left(2X^2-3X\right)\left(X^2+X+2\right) + (7X-1)$.

3.

$$\begin{array}{r|l} 2X^3+5X^2+7X+8 & X^2+X+2 \\ \cline{2-2} -2X^3-2X^2-4X & 2X+3 \\ \cline{1-1} \quad 3X^2+3X+8 & \\ \quad -3X^2-3X-6 & \\ \cline{1-1} \quad\quad 2 & \end{array}$$

$2X^3 + 5X^2 + 7X + 8 = \left(X^2+X+2\right)(2X+3) + 2.$

Euclidean divisions

Définition 3.0.1 Let A and B two be polynomials in $\mathbb{K}[X]$. We say that A is a **divisor** of B, if and only if $\exists! Q \in \mathbb{K}[X]$ such that $B = AQ$, we note $B \backslash A$. If, moreover, B is not a zero polynomial, then Q is unique.

▪ **Exemples 3.5**
1. The polynomial X is a divisor of $X^3 + X$.
2. The polynomials $X + i, X - i, X + 1$ are a divisors of $X^3 + X$.
3. Every polynomial is a divisor of zero polynomial.

Proposition 3.0.2 Let A, B and C be three polynomials in $\mathbb{K}[X]$, then we have
1. $A \backslash B \Longrightarrow \deg A \leq \deg B$.
2. $A \backslash B \wedge B \backslash C \Longrightarrow A \backslash C$.
3. $A \backslash B \wedge B \backslash A \Longrightarrow \exists \lambda \in \mathbb{K}$,such that $A = \lambda B$

Proof.
1. $A \backslash B \Longrightarrow \exists Q \in \mathbb{K}[X]$, such that $B = QA$, then $\deg(B) = \deg(AQ) = \deg A + \deg Q$, since $\deg A \leq \deg B$.
2. $A \backslash B \wedge B \backslash C \Longrightarrow \exists Q_1, Q_2 \in \mathbb{K}[X]$, such that $B = Q_1 A$ and $C = Q_2 B$ then $C = Q_2 Q_1 A = QA$, since $A \backslash C$.
3. $A \backslash B \wedge B \backslash A \Longrightarrow \deg(A) \leq \deg(B)$ and $\deg(B) \leq \deg(A)$, since $\deg A = \deg B$. And
   - $A \backslash B \wedge B \backslash A \Longrightarrow \exists Q_1, Q_2 \in \mathbb{K}[X]$, such that $B = Q_1 A$ and $A = Q_2 B$ then $\deg Q_2 = \deg Q_1 = 0$, since Q_2, Q_1 are constants.

■

Division according to increasing powers

Theorem 3.0.3 Let A and B be two polynomails in $\mathbb{K}[X]$ and $k \in \mathbb{N}^*$. Then, there exists unique $Q, R \in \mathbb{K}[X]$ such that

$$A = BQ + X^{k+1} R$$

with, $\deg Q \leq k$, if $Q \neq 0$.
1. $52X + 3X^2 - X^3 = (1 + 2X - X^3)(2X - X^2 + 3X^2 + X^4) + X^{4+1}(-4 - X)$.
2. $-1 + X + X^2 = (-2 + X)\left(\frac{1}{2} - \frac{1}{4}X - \frac{5}{8}X^2\right) + X^{2+1}\left(\frac{5}{8}\right)$.

Roots of a polynomial

Définition 3.0.2 Let P be a polynomial in $\mathbb{K}[X]$ and $\alpha \in \mathbb{K}$. We say that α is a root (zero) of P if $P(\alpha) = 0$.
α is the root of order k (with $k \in \mathbb{N}^*$),(or of multiplicity k), if there exists $Q \in \mathbb{K}[X]$ such that $P = (X - \alpha)^k Q$ with $Q(\alpha) \neq 0$.

▪ **Exemples 3.6** $X^4 - 1$ accept two real roots $1, -1$ and accept four roots in $\mathbb{C}$ $1, -1, i$ and $-i$.

Proposition 3.0.4 Let $P \in \mathbb{K}[X]$ and $\alpha \in \mathbb{K}$: α is a root of P if and only $X - \alpha$ divides P.

Proof. Let us carry out the Euclidean division of P by $X - \alpha$: $P = (X - \alpha)Q + R$ where the $\deg R < \deg(X - \alpha)$. Therefore the polynomial R is the zero polynomial or the constant polynomial, but $P(\alpha) = 0$, then $P(\alpha) = (\alpha - \alpha)Q + R(\alpha) = R = 0$. We deduce the proposition. ■

Theorem 3.0.5 (D'Alembert-Gauss Theorem) Every non-constant polynomial of $\mathbb{C}[X]$ accept at least one root in $\mathbb{C}$.

Corollary 3.0.6 A non-zero polynomial of degree $n \in \mathbb{N}$ admits at most n roots.

3.0.4 Reducibility

Définition 3.0.3 We say that a polynomial $P\,(\deg P \geq 1)$ is irreducible if all the divisors of P are constant polynomials.

Définition 3.0.4 We say that a polynomial $P\,(\deg P \geq 1)$ is reducible if there exists $Q, R \in \mathbb{K}[X]$ such that $\deg Q \geq 1, \deg R \geq 1$ and $P = QR$.

Theorem 3.0.7 The only irreducible polynomials of $\mathbb{R}[X]$ are:

- The polynomials of degree 1.
- The polynomials of degree 2 with the discriminant strictly negative .($\Delta = b^2 - 4ac < 0$).

Corollary 3.0.8 The irreducible polynomials of $\mathbb{C}[X]$ are exactly of degree 1.

R A polynomail is irreducible of $\mathbb{R}[X]$, it can be reducible to $\mathbb{C}[X]$. Then, it is clear that if a polynomial is reducible from $\mathbb{R}[X]$, then it is necessarily reducible from $\mathbb{C}[X]$.

■ **Exemples 3.7**

- All polynomials of degree "1" are irreducible in $\mathbb{R}[X]$ and in $\mathbb{C}[X]$.
- The polynomials $X^3 - 1$, $X^2 - 3$ and $X^3 + 1$ are irreducible in $\mathbb{R}[X]$ and in $\mathbb{C}[X]$. Actually,
  $X^3 - 1 = (X-1)(X^2 + X + 1)$, and $X^2 - 3 = \left(X - \sqrt{3}\right)\left(X - \sqrt{3}\right)$.
- The polynomial $X^2 + 1$ is irreducible in $\mathbb{R}[X]$, but it is reducible in $\mathbb{C}[X]$, because

$$X^2 + 1 = (X - i)(X + i).$$

3.0.5 Greatest Common Divisor (g.c.d)

Définition 3.0.5 $(g.c.d)$ Let A and B be two polynomials in $\mathbb{K}[X]$ both non-zero, then there exists a unique unitary polynomial D (not both zero) of greatest degree which divides both A and B. This polynomial is called the greatest common divisor of A and B and we note $gcd(A;B) = D$.

■ **Exemples 3.8**

$$gcd\left(X^3 + 3X^2 + 3X + 1, X^3 + 2X^2 + 2X + 1\right) = X + 1$$

Définition 3.0.6 Two polynomials are said to be coprime if their GCD is 1

Euclid's algorithm

Let A and B be two non-zero polynomials such that $\deg A \geq \deg B$. So, Euclid's algorithm consists of performing Euclidean divisions until obtaining a zero remainder, as follows

$$A = BQ_1 + R_1,$$

then, we divide B on R_1, we have

$$B = R_1 Q_2 + R_2.$$

Now, we divide R_1 on R_2, we have

$$R_1 = R_2Q_3 + R_3,$$

We continue the divisions: R_2 on R_3, R_3 on R_4 $\cdots$ until we obtain a zero remainder, as follows

$$R_{k-1} = R_kQ_{k+1} + R_{k+1};\ \text{and}\ R_k = R_{k+1}Q_{k+2}.$$

The $g.c.d$ of A and B is R_{k+1}, that is to say the last non-zero remainder.
As the $g.c.d$ is unique and monic, we take the monic polynomial associated with the last non-zero remainder of Euclid's algorithm.

■ **Exemples 3.9** $A = 2X^4 - X^3 + X^2 + X - 1$ and $B = 2X^2 - 3X$.

$$\begin{array}{rrrr|l}
2X^4 & -X^3 & +X^2 & +X-1 & 2X^2-3X \\
\cline{5-5}
-2X^4 & +3X^3 & & & X^2+X+2 \\
\cline{1-2}
 & 2X^3 & +X^2 & & \\
 & -2X^3 & +3X^2 & & \\
\cline{2-3}
 & & 4X^2 & +X & \\
 & & -4X^2 & +6X & \\
\cline{3-4}
 & & & 7X-1 &
\end{array}$$

$$\underbrace{2X^4 - X^3 + X^2 + X - 1}_{A} = \underbrace{(2X^2 - 3X)}_{B}\underbrace{(X^2 + X + 2)}_{Q_1} + \underbrace{(7X - 1)}_{R_1},$$

and

$$\begin{array}{rrr|l}
2X^2 & -3X & & 7X-1 \\
\cline{4-4}
-2X^2 & +\frac{2}{7}X & & \frac{2}{7}X-\frac{19}{49} \\
\cline{1-2}
 & -\frac{19}{7}X & & \\
 & \frac{19}{7}X & -\frac{19}{49} & \\
\cline{2-3}
 & & -\frac{19}{49} &
\end{array}$$

$$\underbrace{(2X^2 - 3X)}_{B} = \underbrace{(7X - 1)}_{R_1}\underbrace{\left(\frac{2}{7}X + 2\right)}_{Q_2} + \underbrace{\left(\frac{-19}{49}\right)}_{R_2},$$

and

$$\begin{array}{rr|l}
7X & -1 & -\frac{19}{49} \\
\cline{3-3}
-7X & & -\frac{343}{19}X+\frac{49}{19} \\
\cline{1-1}
 & -1 & \\
 & 1 & \\
\cline{2-2}
 & 0 &
\end{array}$$

$$\underbrace{(7X-1)}_{R_1} = \underbrace{\left(\frac{-19}{49}\right)\left(\frac{-343}{19}X+\frac{49}{19}\right)}_{Q_3} + 0$$

Then $\gcd(A,B) = \frac{-49}{19}R_2 = 1$

Theorem 3.0.9 (1^{st} Bézout's Theorem) Let A and B be two non-zero polynomials in $\mathbb{K}[X]$. If $D = pgcd(A,B)$, then there exist two polynomials $U, V \in \mathbb{K}[X]$ such that $AU + BV = D$.

■ **Exemples 3.10** Find a Bézout relation from the example presented previously:

$$\begin{aligned} B &= R_1Q_2 + R_2 \iff B - R_1Q_2 = R_2 \\ &\iff B - (A - BQ_1)Q_2 = R_2 \\ &\iff -Q_2A + (1 + Q_1Q_2)B = R_2 = D, \end{aligned}$$

that is to say

$$U = -Q_2 = -X - 2, \text{ et } V = (1 + Q_1Q_2) = 1 + (X-2)(X+2) = X^2 - 3$$

Coprime polynomails

Theorem 3.0.10 (2^{nd} Bézout's Theorem)

Two polynomials A and B are coprime if and only if there exist two polynomials U and V such that $AU + BV = 1$.

Theorem 3.0.11 (Gauss's Theorem)

If a polynomial divides a product of two polynomials and it is prime with one of the factors, it divides the other.

$$(A \backslash BC \quad \text{and} \quad A \wedge B = 1) \Longrightarrow A \backslash C$$

3.0.6 Factoring a polynomial into irreducible

Theorem 3.0.12 Let $P \in \mathbb{K}[X]$ be a non-constant polynomial, then there exist $k \in \mathbb{N}^*$ and irreducible polynomials $P_1, P_2, \cdots, P_k$ of $\mathbb{K}[X]$, such that

$$P = \beta P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_k^{\alpha_k},$$

where, $\beta \in \mathbb{K}^*$ and $\alpha_1, \alpha_2, \cdots, \alpha_k \in \mathbb{N}^*$. The polynomials $P_1, P_2, \cdots, P_k$ are unique up to permutation.

■ **Exemples 3.11** 1. Decompose $P = X^8 + X^4 + 1$ into irreducible factors in $\mathbb{R}[X]$, in $\mathbb{C}[X]$.

a In $\mathbb{R}[X]$, we have

$$X^8 + X^4 + 1 = (X^4+1)^2 - X^4 = (X^4 + 1 + X^2)(X^4 + 1 - X^2)$$

also

$$\begin{aligned} (X^4 + 1 + X^2) &= (X^2+1)^2 - X^2 = (X^2 + 1 + X)(X^2 + 1 - X) \\ &\textit{and} \\ X^4 - X^2 + 1 &= (X^2+1)^2 - 3X^2 = (X^2 + 1 + \sqrt{3}X)(X^2 + 1 - \sqrt{3}X), \end{aligned}$$

Then

$$P = (X^2+X+1)(X^2-X+1)(X^2+\sqrt{3}X+1)(X^2-\sqrt{3}X+1).$$

b In $\mathbb{C}[X]$,we can search for the roots of P in $\mathbb{C}[X]$, we have

$$\begin{aligned}
X^2+1+X &= \left(X+\frac{1+i\sqrt{3}}{2}\right)\left(X+\frac{1-i\sqrt{3}}{2}\right),\\
X^2+1-X &= \left(X-\frac{1+i\sqrt{3}}{2}\right)\left(X-\frac{1-i\sqrt{3}}{2}\right),\\
X^2+1+\sqrt{3}X &= \left(X+\frac{\sqrt{3}-i}{2}\right)\left(X+\frac{\sqrt{3}+i}{2}\right),\\
X^2+1-\sqrt{3}X &= \left(X-\frac{\sqrt{3}-i}{2}\right)\left(X-\frac{\sqrt{3}+i}{2}\right).
\end{aligned}$$

Then

$$\begin{aligned}
P &= \left(X+\frac{1+i\sqrt{3}}{2}\right)\left(X+\frac{1-i\sqrt{3}}{2}\right)\left(X-\frac{1+i\sqrt{3}}{2}\right)\left(X-\frac{1-i\sqrt{3}}{2}\right)\\
&\quad\times\left(X+\frac{\sqrt{3}-i}{2}\right)\left(X+\frac{\sqrt{3}+i}{2}\right)\left(X-\frac{\sqrt{3}-i}{2}\right)\left(X-\frac{\sqrt{3}+i}{2}\right).
\end{aligned}$$

2. Decompose $P = X^5+1$ into irreducible factors in $\mathbb{R}[X]$ and in $\mathbb{C}[X]$.
   a In $\mathbb{C}[X]$. We will search for the complex roots of the form $e^{i\theta}$, as follows

$$\left(e^{i\theta}\right)^5+1=0 \Longleftrightarrow e^{i5\theta}=-1=e^{i(2k+1)\pi}, k\in\mathbb{Z}.$$

We can choose

$$5\theta=(2k+1)\,\pi, k\in\mathbb{Z} \Longleftrightarrow \theta=\frac{\pi}{5}+\frac{2k\pi}{5}.$$

Which implies,

$$\alpha_1=e^{i\frac{\pi}{5}},\ \ \alpha_2=e^{i\frac{3\pi}{5}},\ \ \alpha_3=e^{i\frac{5\pi}{5}}=-1,\ \ \alpha_4=e^{i\frac{7\pi}{5}},\ \ \alpha_5=e^{i\frac{9\pi}{5}}.$$

So, the factorization of X^5+1 is

$$X^5+1=(X+1)\left(X-e^{i\frac{\pi}{5}}\right)\left(X-e^{i\frac{3\pi}{5}}\right)\left(X-e^{i\frac{7\pi}{5}}\right)\left(X-e^{i\frac{9\pi}{5}}\right).$$

b In $\mathbb{R}[X]$: According to the previous method on $\mathbb{C}$, we have

$$\alpha_1=\overline{\alpha_5},\ \ \alpha_2=\overline{\alpha_4},\ \ \alpha_3=e^{i\pi}=-1,$$

then

$$\begin{aligned}
X^5+1 &= (X+1)\,(X-\overline{\alpha_5})\,(X-\alpha_5)\,(X-\overline{\alpha_4})\,(X-\alpha_4)\\
&= (X+1)\left(X^2-[\alpha_5+\overline{\alpha_5}]X+\overline{\alpha_5}\alpha_5\right)\left(X^2-[\alpha_4+\overline{\alpha_4}]X+\overline{\alpha_4}\alpha_4\right)\\
&= (X+1)\left(X^2-2\cos\left(\frac{\pi}{5}\right)X-1\right)\left(X^2-2\cos\left(\frac{3\pi}{5}\right)X-1\right).
\end{aligned}$$

Then X^5+1 is reducible in $\mathbb{R}$

4. Rational fractions

- A rational fraction in $\mathbb{K}$ is written $F = \frac{P}{Q}$, where P and Q are polynomials in $\mathbb{K}$, with $Q \neq 0$.
- We say that the representative $\frac{P}{Q}$ of F is irreducible, if the polynomials P and Q are coprime.
- Every rational fraction has a unique irreducible representative

■ **Exemples 4.1 :**

1. $F = \frac{X^5 - X^4 + 5}{X^3 - 3X + 2}$.
2. The rational fraction $F = \frac{X^4 - X^2}{X^2 - 3X + 2}$, accept an irreducible form $F = \frac{X^2(X+1)}{X-2}$

4.0.1 Roots and poles of a rational fraction

- We call roots (zeros) of the rational fraction $F = \frac{P}{Q}$ (supposed to be irreducible) the roots of the numerator P, and poles the roots of the denominator Q.
- We call degree of the rational fraction $F = \frac{P}{Q}$ the relative integer:

$$\deg\left(\frac{P}{Q}\right) = \deg P - \deg Q$$

■ **Exemples 4.2** The rational fraction $F = \frac{X^4 - X^2}{X^2 - 3X + 2}$, accept the roots $0, 1, -1$ and accept the poles $1, 2$.

4.0.2 Decomposition into simple elements

Définition 4.0.1 We say that $\frac{P}{Q}$ with $P \times Q \neq 0$ is a simple element iff $\deg P < \deg Q$, $\gcd(P, Q) = 1$, Q is an irreducible polynomial.

Simple element in $\mathbb{C}$:
A simple element in $\mathbb{C}$ is a fraction of the form $\frac{b}{(X-\alpha)^n}$, where $a \in \mathbb{C}^*, b \in \mathbb{C}$ and $n \in \mathbb{N}^*$.

Simple element in $\mathbb{R}$:

A simple element in $\mathbb{R}$ is a fraction which can have one of the following forms:

1. $\frac{b}{(X-\alpha)^n}$, where $a \in \mathbb{R}^*, b \in \mathbb{R}$ and $n \in \mathbb{N}$.
2. $\frac{aX+b}{(X^2+\alpha X+\beta)^n}$ where $a,b,\alpha,\beta \in \mathbb{R}$ and $\alpha^2-4\beta<0$, and a,b non-zero at the same time.

■ **Exemples 4.3**

1. $\frac{5-i}{(X-2)^3}$, $\frac{i}{X+3i}$ are simple elements in $\mathbb{C}$
2. $\frac{7}{(X+2)^3}$, $\frac{5}{X+3}$ are simple elements in $\mathbb{C}$ and in $\mathbb{R}$.
3. $\frac{2X}{(X^2+X+5)^6}$, $\frac{4}{(X^2-4X+7)^2}$, $\frac{X-3}{X^2+3X+5}$ are simple elements in $\mathbb{R}$.

General method of decomposition

- A rational fraction, of irreducible form $F=\frac{P}{Q}$, with $\deg P \geq \deg Q$, is written uniquely, in the form:

$$F = E + \frac{R}{Q} \text{ with } \deg R < \deg Q.$$

E is the integer part and $\frac{R}{Q}$ the fractional part of F.

■ **Exemples 4.4 :**

$$\frac{X^3+X^2+1}{X^2+1} = X+1+\frac{-X}{X^2+1}.$$

Theorem 4.0.1 Let $\frac{R}{Q}$ with $\deg R < \deg Q$ a rational fraction. Suppose $Q = Q_1Q_2$ with $\gcd(Q_1,Q_2)=1$. There exists a unique pair (R_1,R_2) of polynomials such that:

$$\frac{R}{Q} = \frac{R_1}{Q_1}+\frac{R_2}{Q_2}, \text{ with } \deg R_1 < \deg Q_1 \text{ and } \deg R_2 < \deg Q_2.$$

■ **Exemples 4.5** $F(X) = \frac{X}{(X-1)(X-2)} = \frac{-1}{X-1}+\frac{2}{X-2}.(\text{in } \mathbb{R}[X])$

Corollary 4.0.2 Any rational fraction $\frac{R}{Q}$ with $\deg R < \deg Q$, acceptting a pole of order m is uniquely decomposed into:

$$\frac{R}{Q} = \frac{R}{(X-\alpha)^m Q_2} = \frac{R_1}{(X-\alpha)^m}+\frac{R_2}{Q_2}, \text{ with } \deg R_1 < m \text{ and } \deg R_2 < \deg Q_2.$$

The term $\frac{R_1}{(X-\alpha)^m}$ is called the **polar part** of $\frac{R}{Q}$ relative to the pole α

■ **Exemples 4.6** $F(X) = \frac{2X^3+3X^2+2X}{(X+1)^2(X^2+X+1)} = \frac{X}{(X+1)^2}+\frac{X}{X^2+X+1}.(\text{in } \mathbb{R}[X])$

Theorem 4.0.3 Let $\frac{R}{(X-\alpha)^m}$, with $\deg R < m$, a polar part of a pole α. There are unique constants $(c_1,c_2,\cdots,c_m)$ such that:

$$\frac{R}{(X-\alpha)^m} = \sum_{k=1}^{m} \frac{c_k}{(X-\alpha)^k}.$$

■ **Exemples 4.7** $F(X) = \frac{7X-4}{(X-1)^2} = \frac{7}{X-1}+\frac{3}{(X-1)^2}.(\text{in } \mathbb{R}[X])$

Corollary 4.0.4 Let $Q = \prod_{i=1}^{p} (X-\alpha_i)^{m_i}$ a polynomail. Any rational fraction with denominator Q and strictly negative degree is uniquely decomposed into:

$$\frac{R}{Q} = \sum_{i=1}^{p} \frac{R_i}{(X-\alpha_i)^{m_i}} \quad \text{with } \forall i \in \overline{1,P} \quad \deg R_i < m_i.$$

4.0.3 Practical examples

■ **Exemples 4.8 :**

Research for the polar parts of the rational fraction:

$$F = \frac{X\left(X^2+1\right)^2}{\left(X^2-1\right)^2}$$

Extract the entire part:

$$\frac{X\left(X^2+1\right)^2}{\left(X^2-1\right)^2} = X + \frac{4X^3}{\left(X^2-1\right)^2} = X + \frac{4X^3}{(X+1)^2(X-1)^2}. \tag{4.1}$$

Decomposition the fraction $G(X) = \frac{4X^3}{\left(X^2-1\right)^2}$ into simple elements,

1. 1^{st} Method: We have

$$\frac{4X^3}{\left(X^2-1\right)^2} = \frac{4X^3}{(X+1)^2(X-1)^2}.$$

Applying Euclid's algorithm to polynomials $(X+1)^2$ and $(X-1)^2$:

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

then

$$1 = (X-1)^2\frac{X+2}{4} - (X+1)^2\frac{X-2}{4}.$$

We deduce

$$\frac{1}{\left(X^2-1\right)^2} = \frac{X+2}{4(X+1)^2} - \frac{X-2}{4(X-1)^2}.$$

Then

$$\frac{4X^3}{\left(X^2-1\right)^2} = \frac{X^4+2X^3}{(X+1)^2} - \frac{X^4-2X^3}{(X-1)^2}.$$

Calculating the integer part of the two terms:

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

So:

$$F = X + \frac{2X-1}{(X-1)^2} + \frac{2X+1}{(X+1)^2}.$$

Decomposition of the polar parts found in the previous example:

$$2X+1 = 2(X+1)-1; \text{ hence } \frac{2X+1}{(X+1)^2} = \frac{2}{X+1} + \frac{-1}{(X+1)^2},$$

and

$$2X-1 = 2(X-1)+1; \text{ hence } \frac{2X-1}{(X-1)^2} = \frac{2}{X-1} + \frac{1}{(X-1)^2}.$$

Finally

$$F = X + \frac{2}{X-1} + \frac{1}{(X-1)^2} + \frac{2}{X+1} + \frac{-1}{(X+1)^2}.$$

2. 2^{nd} Method:
The fraction G accepts a decomposition of the form:

$$G(X) = \frac{a}{X+1} + \frac{b}{(X+1)^2} + \frac{c}{X-1} + \frac{d}{(X-1)^2}$$

- Note that G is odd and compare the decompositions of $G(-X)$ and $-G(X)$:

$$\begin{aligned}
G(-X) &= \frac{-a}{X-1} + \frac{b}{(X-1)^2} + \frac{-c}{X+1} + \frac{d}{(X+1)^2} \\
-G(X) &= \frac{-a}{X+1} + \frac{-b}{(X+1)^2} + \frac{-c}{X-1} + \frac{-d}{(X-1)^2}
\end{aligned}$$

Then

$$G(-X) = -G(X) \Rightarrow \left\{ \begin{array}{c} a = c \\ b = -d \end{array} \right. .$$

- For find b, we multiply G by $(X+1)^2$

$$(X+1)^2G = \frac{4X^3}{(X-1)^2} = a(X+1)+b+\frac{c(X+1)^2}{X-1}+\frac{d(X+1)^2}{(X-1)^2}.$$

By replacing X with -1, we obtain $b=-1$, then $d=1$.
This method makes it possible to find the coefficient of the highest degree term of each polar part.

- For find the coefficients a and c, we multiply G by X:

$$XG(X) = \frac{4X^4}{(X-1)^2} = \frac{aX}{X+1}+\frac{bX}{(X+1)^2}+\frac{cX}{X-1}+\frac{dX}{(X-1)^2}.$$

By research for the limit of $XG(X)$ in $+\infty$, we obtain:

$$\lim_{x\to+\infty} xG(x) = 4 = a+c, \text{ then } a=c=2.$$

This method makes it possible to find the sum of the lowest degree coefficients of all the polar parts. Eventually,, we obtain:$(a,b,c,d)=(2,-1,2,1)$.

$$G = \frac{2}{X-1}+\frac{1}{(X-1)^2}+\frac{2}{X+1}+\frac{-1}{(X+1)^2}.$$

■ **Exemples 4.9 :**

Decomposition into simple elements

$$F = \frac{X^3+1}{(X-2)^4}.$$

By divide successively on $X-2$:

$$\begin{aligned} X^3+1 &= (X-2)(X^2+2X+4)+9 \\ &\Rightarrow \frac{X^3+1}{(X-2)^4} = \frac{X^2+2X+4}{(X-2)^3}+\frac{9}{(X-2)^4}, \end{aligned}$$

and

$$\begin{aligned} X^2+2X+4 &= (X-2)(X+4)+12 \\ &\Rightarrow \frac{X^2+2X+4}{(X-2)^3} = \frac{X+4}{(X-2)^2}+\frac{12}{(X-2)^3}, \end{aligned}$$

and

$$X+4=(X-2)+6 \quad \frac{X+4}{(X-2)^2} = \frac{1}{(X-2}+\frac{6}{(X-2)^3}.$$

Finally,

$$F = \frac{1}{X-2}+\frac{6}{(X-2)^3}+\frac{12}{(X-2)^3}+\frac{9}{(X-2)^4}.$$

■ **Exemples 4.10** : In $\mathbb{C}[X]$.

$$F = \frac{3X+1}{X^2+1} = \frac{a}{X-i} + \frac{b}{X+i}$$

Multiply both sides of the equality by $(X-i)$ and replacing X by i, we obtain $a = \frac{3-i}{2}$.
Multiply both sides of the equality by $(X+i)$ and replacing X by -i, we obtain $b = \frac{3+i}{2}$.
We conclude,

$$F = \frac{3X+1}{X^2+1} = \frac{3-i}{2(X+i)} + \frac{3+i}{2(X-i)}$$

4.0.4 Practical decomposition methods

Study plan:

a We put $F = \frac{P}{Q}$ in irreducible form by simplifying by the *GCD* of the numerator P and the denominator Q.
b We obtain E and R using the Euclidean division of P by Q.
c We factor B into irreducible polynomials.
d We write the literal form of the decomposition into simple elements of F, or of $\frac{P}{Q}$.
e We determine the coefficients using various methods.

4.1 Exercises solved

Exercise 4.1.1:

1. Find the polynomials P of degree 3, such that

$$P(0) = 1, P(1) = -1, P(-1) = 3, P(2) = 5.$$

2. Under what condition on $a,b,c \in \mathbb{R}$, the polynomial $X^4 + aX^2 + bX + c$ is divisible by $X^2 + X - 2$?
3. Find the polynomials of degree 2 such that P' divides P.
4. (**TP**) Find the polynomials P of degree 3, such that

$$P(0) = 0 \text{ and } P(X+1) - P(X) = X^2.$$

5. The following statements are true or false:
   (a) A polynomial of degree 3 is always reducible in $\mathbb{R}[X]$.
   (b) P is irreducible in $R[X]$, if and anly if $\deg P = 1$.
   (c) A polynomial $P \in \mathbb{R}[X]$ of degree 5 accept at least one real root.

Solution:

1.
2. $P = aX^3 + bX^2 + cX + d$ where a,b,c and d satisfy the following equations:

$$\begin{cases} d = 1 \\ a+b+c+d = -1 \\ -a+b-c+d = 3 \\ 8a+4b+2c+d = 5 \end{cases}$$

then,

$$P = \frac{4}{3}X^3 - \frac{10}{3}X + 1.$$

3. The rest of the division of $X^4 + aX^2 + bX + c$ by $X^2 + X - 2$ is

$$R = (b - a - 5)X + 2a + c + 6.$$

For it to be zero it is necessary that

$$b = a + 5 \text{ and } c = -2a - 6.$$

4. The rest of the division of $P = aX^2 + bX + c$ by $P' = 2aX + b$ is

$$R = c - \frac{b^2}{4a}.$$

So the condition is

$$4ac = b^2.$$

5. (**TP**) $P = \frac{1}{3}\left(X^3 - 2X^2 + X\right)$.
6. True or False
   (a) Is true, because the degree of P is odd number.
   (b) $(\deg P = 1) \Rightarrow (P$ is irreducible in $\mathbb{R}[X])$, is true. And (P is irreducible in $\mathbb{R}[X]) \Rightarrow (\deg P = 1)$, is false.
   (c) Is true. because the graph of polynomail of degree odd always pass by the axis (Ox).

Exercise 4.1.2: Let the polynomial $P(X) = X^8 + X^4 + 1$
1. Show that P does not admit real roots.
2. P is it an irreducible polynomial of $\mathbb{R}[X]$.

Solution:

1. We consider the function

$$X \longmapsto P(X) = X^8 + X^4 + 1.$$

So, we have

$$P'(X) = 8X^7 + 4X^3 = X^3\left(8X^4 + 4\right),$$

then,

$$P'(X) = 0 \Leftrightarrow X^3\left(8X^4 + 4\right) = 0 \Longrightarrow X = 0.$$

Since, $P(0) = 1 > 0$, then graph of $P(X)$ does not pass by the axis (Ox).

2. As P does not accept any real root but it is of degree 8, then it is the product of polynomials of degree 2, therefore it is reducible from $\mathbb{R}[X]$.

Exercise 4.1.3: (gcd of polynomials)

1. Determine the $D = \gcd$ the following polynomials:
   (a) $A = X^3 - X^2 - X - 2$ and $B = X^5 - 2X^4 + X^2 - X - 2$,
   (b) $A = X^5 + 3X^4 + X^3 + X^2 + 3X + 1$ and $B = X^4 + 2X^3 + X + 2$.
2. Find U and V of the previous D, such that $AU + BV = D$.

Solution:

1. The gcd of polynomials:
   (a) $\gcd(A,B) = X - 2$,
   (b) $\gcd(A,B) = X^3 + 1$.
2. Determination of U and V such that $AU + BV = D$:
   (a) $A\left(-\frac{2}{3}X - \frac{1}{3}\right) + B\left(\frac{2}{3}X^3 - \frac{1}{3}X^2 - \frac{1}{3}X + \frac{4}{3}\right) = X - 2$,
   (b) $A(-1) + B(X+1) = X^3 + 1$.

Exercise 4.1.4:

1. Are the following polynomials irreducible in $\mathbb{R}[X]$ or in $\mathbb{C}[X]$?

$$P(X) = X^8 + X^4 + 1, \quad Q(X) = X^5 + 1.$$

2. Factor these polynomials on $\mathbb{R}[X]$, on $\mathbb{C}[X]$.

Solution:

1. The polynomials P and Q are irreducibles in $\mathbb{R}[X]$ and in $\mathbb{C}[X]$, See the exercices 1 and 2
2. Decompose $P = X^8 + X^4 + 1$ into irreducible factors in $\mathbb{R}[X]$, in $\mathbb{C}[X]$.
   a) In $\mathbb{R}[X]$, we have

$$X^8 + X^4 + 1 = (X^4+1)^2 - X^4 = (X^4 + 1 + X^2)(X^4 + 1 - X^2)$$

also

$$\begin{aligned} (X^4 + 1 + X^2) &= (X^2+1)^2 - X^2 = (X^2 + 1 + X)(X^2 + 1 - X) \\ &\text{and} \\ X^4 - X^2 + 1 &= (X^2+1)^2 - 3X^2 = (X^2 + 1 + \sqrt{3}X)(X^2 + 1 - \sqrt{3}X), \end{aligned}$$

Then

$$P = (X^2 + X + 1)(X^2 - X + 1)(X^2 + \sqrt{3}X + 1)(X^2 - \sqrt{3}X + 1).$$

b) In $\mathbb{C}[X]$,we can search for the roots of P in $\mathbb{C}[X]$, we have

$$\begin{aligned}
X^2+1+X &= \left(X+\frac{1+i\sqrt{3}}{2}\right)\left(X+\frac{1-i\sqrt{3}}{2}\right),\\
X^2+1-X &= \left(X-\frac{1+i\sqrt{3}}{2}\right)\left(X-\frac{1-i\sqrt{3}}{2}\right),\\
X^2+1+\sqrt{3}X &= \left(X+\frac{\sqrt{3}-i}{2}\right)\left(X+\frac{\sqrt{3}+i}{2}\right),\\
X^2+1-\sqrt{3}X &= \left(X-\frac{\sqrt{3}-i}{2}\right)\left(X-\frac{\sqrt{3}+i}{2}\right).
\end{aligned}$$

Then

$$\begin{aligned}
P &= \left(X+\frac{1+i\sqrt{3}}{2}\right)\left(X+\frac{1-i\sqrt{3}}{2}\right)\left(X-\frac{1+i\sqrt{3}}{2}\right)\left(X-\frac{1-i\sqrt{3}}{2}\right)\\
&\quad\times\left(X+\frac{\sqrt{3}-i}{2}\right)\left(X+\frac{\sqrt{3}+i}{2}\right)\left(X-\frac{\sqrt{3}-i}{2}\right)\left(X-\frac{\sqrt{3}+i}{2}\right).
\end{aligned}$$

3. Decompose $Q=X^5+1$ into irreducible factors in $\mathbb{R}[X]$ and in $\mathbb{C}[X]$.

a) In $\mathbb{C}[X]$. We will search for the complex roots of the form $e^{i\theta}$, as follows

$$\left(e^{i\theta}\right)^5+1=0\Longleftrightarrow e^{i5\theta}=-1=e^{i(2k+1)\pi},k\in\mathbb{Z}.$$

We can choose

$$5\theta=(2k+1)\,\pi,k\in\mathbb{Z}\Longleftrightarrow\theta=\frac{\pi}{5}+\frac{2k\pi}{5}.$$

Which implies,

$$\alpha_1=e^{i\frac{\pi}{5}},\ \ \alpha_2=e^{i\frac{3\pi}{5}},\quad \alpha_3=e^{i\frac{5\pi}{5}}=-1,\ \ \alpha_4=e^{i\frac{7\pi}{5}},\ \ \alpha_5=e^{i\frac{9\pi}{5}}.$$

So, the factorization of X^5+1 is

$$X^5+1=(X+1)\left(X-e^{i\frac{\pi}{5}}\right)\left(X-e^{i\frac{3\pi}{5}}\right)\left(X-e^{i\frac{7\pi}{5}}\right)\left(X-e^{i\frac{9\pi}{5}}\right).$$

b) In $\mathbb{R}[X]$: According to the previous method on $\mathbb{C}$, we have

$$\alpha_1=\overline{\alpha_5},\ \ \alpha_2=\overline{\alpha_4},\ \ \alpha_3=e^{i\pi}=-1,$$

then

$$\begin{aligned}
X^5+1 &= (X+1)\,(X-\overline{\alpha_5})\,(X-\alpha_5)\,(X-\overline{\alpha_4})\,(X-\alpha_4)\\
&= (X+1)\left(X^2-[\alpha_5+\overline{\alpha_5}]\,X+\overline{\alpha_5}\alpha_5\right)\left(X^2-[\alpha_4+\overline{\alpha_4}]\,X+\overline{\alpha_4}\alpha_4\right)\\
&= (X+1)\left(X^2-2\cos\left(\frac{\pi}{5}\right)X-1\right)\left(X^2-2\cos\left(\frac{3\pi}{5}\right)X-1\right).
\end{aligned}$$

Then X^5+1 is reducible in $\mathbb{R}[X]$.

$$X^5+1=(X+1)\left(X^2-2\cos\left(\frac{\pi}{5}\right)X-1\right)\left(X^2-2\cos\left(\frac{3\pi}{5}\right)X-1\right).$$

Exercise 4.1.5: Let A and B be t wo polynomails such that :

$$A(X)=X^5+X^4-3X^3-3X^2+2X+2 \text{ and } B(X)=X^3+1.$$

1. Show that $(X+1)$ divides $A(X)$.
2. Factor A and B on $\mathbb{R}[X]$, on $\mathbb{C}[X]$.
3. Determine the $D=\gcd(A,B)$

Solution:

1. Show that $(X+1)$ divise $A(X)$.

$$(X+1) \text{ divise } A(X) \Longleftrightarrow (-1) \text{ is a root of } A(X) \Longleftrightarrow A(-1)=0.$$

Then $A(-1)=(-1)^5+(-1)^4-3(-1)^3-3(-1)^2+2(-1)+2=0$, so $(X+1)$ divise $A(X)$.

2. Factor A and B on $\mathbb{R}[X]$, on $\mathbb{C}[X]$.

(a) Factorization of $A(X)$:
A is divisible by $(X+1)$ then by Euclidean division of A on $(X+1)$ we obtain the quotient $Q(X)=X^4-3X^2+2$.
we assume $Y=X^2$, then $Q(Y)=Y^2-3Y+2$.
Calculation: Δ: $\Delta=1$, then the roots of $Q(Y)$ are $Y_1=1$ and $Y_2=2$. so $Q_1(Y)=(Y-1)(Y-2)$.
Donc $Q(X)=\left(X^2-1\right)\left(X^2-2\right)$.
Also

$$X^2-1=(X-1)(X+1) \text{ and } X^2-2=\left(X-\sqrt{2}\right)\left(X+\sqrt{2}\right).$$

Finally the factorization of A on $\mathbb{R}[X]$ and $\mathbb{C}[X]$ is:

$$A(X)=(X+1)^2(X-1)\left(X-\sqrt{2}\right)\left(X+\sqrt{2}\right).$$

(b) Factorization of $B(X)$:

We note (-1) is a root of $B(X)$, then by Euclidean division of B on $(X+1)$ we obtain the quotient $K(X)=X^2-X+1$.
Calculation: Δ: $\Delta=-3$, then the roots of $K(X)$ in $\mathbb{C}[X]$ are $X_1=\frac{1+i\sqrt{3}}{2}$ and $X_2=\frac{1-i\sqrt{3}}{2}$. So $K(X)=\left(X-\frac{1+i\sqrt{3}}{2}\right)\left(X-\frac{1-i\sqrt{3}}{2}\right)$.

Finally the factorization of B on $\mathbb{C}[X]$ is

$$B(X) = (X+1)\left(X - \frac{1+i\sqrt{3}}{2}\right)\left(X - \frac{1-i\sqrt{3}}{2}\right).$$

And the factorization of B on $\mathbb{R}[X]$ is

$$B(X) = (X+1)\left(X^2 - X + 1\right).$$

3. Determine the $D = \gcd(A,B)$:
   According to the factorizations of A and B:

$$A(X) = A(X) = (X+1)^2(X-1)\left(X - \sqrt{2}\right)\left(X + \sqrt{2}\right).$$

$$B(X) = (X+1)\left(X^2 - X + 1\right).$$

We obtain

$$D = \gcd(A,B) = X + 1.$$

Exercise 4.1.6:

1. Decompose the following fractions into simple elements in $\mathbb{R}[X]$, and in $\mathbb{C}[X]$.

$$\begin{aligned} F_0(X) &= \frac{X^2+X+1}{(X-1)^3}, \\ F_1(X) &= \frac{3X^3+X^2+X+1}{X^2-3X+2}, \\ F_2(X) &= \frac{2X^4+1}{X(X-1)^3(X^2+X+1)}, \\ F_3(X) &= \frac{X^2+1}{X^4+1}. \text{ (TP)} \end{aligned}$$

2. Calculate the following integral

$$\int_3^4 F_1(X)\,dx.$$

Solution:

1. Decompose $F_0(X)$ into simple elements in $\mathbb{R}[X]$, and in $\mathbb{C}[X]$.

$$F_0(X) = \frac{X^2+X+1}{(X-1)^3}.$$

(1^{st}). Decomposition: Determine a, b, and c of the real numbers such that

$$\frac{X^2+X+1}{(X-1)^3} = \frac{a}{X-1} + \frac{b}{(X-1)^2} + \frac{c}{(X-1)^3}$$

then

$$\begin{aligned}(X-1)^3 F_0(X) &= X^2+X+1 \\ &= a(X-1)^2+b(X-1)+c \overset{\text{For } X=1}{\Longrightarrow} c=3,\end{aligned}$$

and

$$\frac{X^2+X+1}{(X-1)^3}=\frac{aX^2+(b-2a)X+a-b+3}{(X-1)^3} \Rightarrow \begin{cases} a=1 \\ b=3 \end{cases}.$$

Finally,

$$\frac{X^2+X+1}{(X-1)^3}=\frac{1}{X-1}+\frac{3}{(X-1)^2}+\frac{3}{(X-1)^3}.$$

2. Decompose $F_1(X)$ into simple elements in $\mathbb{R}[X]$, and in $\mathbb{C}[X]$.

$$F_1(X)=\frac{3X^3+X^2+X+1}{X^2-3X+2}.$$

(1^{st}). Determination of the integer part: by using Euclidean division of $3X^3+X^2+X+1$ by X^2+X+1 by X^2-3X+2, we obtain

$$\frac{3X^3+X^2+X+1}{X^2-3X+2}=2X+7+\frac{16X-13}{X^2-3X+2}.$$

$\left(2^{nd}\right)$. Denominator factorization: Factor the polynomial X^2-3X+2 in $\mathbb{R}$

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

$\left(3^{rd}\right)$. Decomposition: Determine a and b of the real numbers such that

$$\frac{16X-13}{X^2-3X+2}=\frac{a}{X-1}+\frac{b}{X-2}.$$

Multiply both sides of the equality by $(X-1)$, we have

$$\frac{16X-13}{X-2}=a+\frac{b(X-1)}{X-2},$$

for $X=1$, we obtain $a=-3$. And also,

$$(X-2)\frac{16X-13}{X^2-3X+2}=\frac{16X-13}{X-1}=\frac{a(X-2)}{X-1}+b,$$

for $X=2$, we obtain $b=19$. Finally,

$$\frac{3X^3+X^2+X+1}{X^2-3X+2}=2X+7+\frac{-3}{X-1}+\frac{19}{X-2}. \tag{4.2}$$

3. Decompose $F_2(X)$ into simple elements in $\mathbb{R}[X]$, and in $\mathbb{C}[X]$.

(a) In $\mathbb{R}[X]$:

$$F_2(X) = \frac{2X^4+1}{X(X-1)^3(X^2+X+1)}.$$

(1^{st}) Decomposition: Determine a, c and b of the real numbers such that

$$F_2(X) = \frac{a}{X} + \frac{b}{(X-1)^3} + \frac{cX+d}{X^2+X+1},$$

then

$$\begin{aligned}
XF_2(X) &= \frac{2X^4+1}{(X-1)^3(X^2+X+1)} \\
&= a + \frac{bX}{(X-1)^3} + \frac{cX^2+dX}{X^2+X+1} \overset{\text{For } X=0}{\Longrightarrow} a = 1, \\
(X-1)^3 F_2(X) &= \frac{2X^4+1}{X(X^2+X+1)} \\
&= \frac{(X-1)^3}{X} + b + \frac{(cX+d)(X-1)^3}{X^2+X+1} \overset{\text{For } X=1}{\Longrightarrow} b = 1, \\
\left(X^2+X+1\right) F_2(X) &= \frac{2X^4+1}{X(X-1)^3} \\
&= \frac{\left(X^2+X+1\right)}{X} + \frac{\left(X^2+X+1\right)}{(X-1)^3} + cX + d \overset{\substack{\text{For } X=-1 \\ \text{and } X=2}}{\Longrightarrow} \begin{cases} c = \frac{3}{2}, \\ d = 3 \end{cases}.
\end{aligned}$$

Finally,

$$F_2(X) = \frac{1}{X} + \frac{1}{(X-1)^3} + \frac{\frac{3}{2}X+3}{(X^2+X+1)}.$$

(b) In $\mathbb{C}[X]$: We have

$$X^2+X+1 = \left(X + \frac{1+i\sqrt{3}}{2}\right)\left(X + \frac{1-i\sqrt{3}}{2}\right).$$

(1^{st}) Decomposition: Determine d,and e of the real numbers such that

$$\begin{aligned}
\frac{\frac{3}{2}X+3}{X^2+X+1} &= \frac{d}{X+\frac{1+i\sqrt{3}}{2}} + \frac{e}{X+\frac{1-i\sqrt{3}}{2}} \\
&= \frac{(d+e)X + \frac{1}{2}\left(d+e+(e-d)i\sqrt{3}\right)}{X^2+X+1},
\end{aligned}$$

By identification we find

$$e+d = \frac{3}{2}, \text{ and } e-d = \frac{-3\sqrt{3}}{2}i,$$

then

$$d = \frac{3}{4}\left(1+i\sqrt{3}\right), \text{ and } e = \frac{3}{4}\left(1-i\sqrt{3}\right).$$

We conclude,

$$\frac{\frac{3}{2}X+3}{X^2+X+1} = \frac{3\left(1+i\sqrt{3}\right)}{4X+2(1+i\sqrt{3})} + \frac{3\left(1-i\sqrt{3}\right)}{4X+2(1-i\sqrt{3})}.$$

Finally

$$F_2(X) = \frac{1}{X} + \frac{1}{(X-1)^3} + \frac{3\left(1+i\sqrt{3}\right)}{4X+2(1+i\sqrt{3})} + \frac{3\left(1-i\sqrt{3}\right)}{4X+2(1-i\sqrt{3})}.$$

4. Calculate the integral

$$\int_2^3 F_1(X)\,dx = \int_3^4 \frac{3X^3+X^2+X+1}{X^2-3X+2}dx,$$

according to (4.2) we find

$$\begin{aligned}\int_3^4 F_1(X)\,dx &= \int_3^4 \left(2X+7+\frac{-3}{X-1}+\frac{19}{X-2}\right)dx \\ &= \left[X^2+7X-3\ln(X-1)+19\ln(X-2)\right]_3^4 \\ &= 14+\ln\left(\frac{2^{22}}{27}\right).\end{aligned}$$

4.1.1 Additional exercises

Exercise 4.1.7: Let A and B be t wo polynomails such that:

$$A(X) = X^5+X^4-X^3-3X^2+2X+2 \text{ and } B(X) = X^3+1.$$

1. Show that $(X+1)$ divides $A(X)$.
2. Factor A and B on $\mathbb{R}[X]$, on $\mathbb{C}[X]$.
3. Determine the $D = \gcd(A,B)$

Exercise 4.1.8: Are the following polynomials irreducible in $\mathbb{R}[X]$ or in $\mathbb{C}[X]$?

$$P(X) = X^6+1,\ Q(X) = X^{12}-1,\ R(X) = X^8-X^4+1$$

Factor these polynomials on $\mathbb{R}[X]$, on $\mathbb{C}[X]$.

Exercise 4.1.9: For $n \in \mathbb{N}$, show that the polynomial

$$P(X) = nX^{n+1} - (n+1)X^n,$$

is divisible by $(1-X)^2$.

Exercise 4.1.10: (gcd of polynomials)

- Determine the $D = \gcd$ the following polynomials:
  1. $A = X^5 + X^3 + X + 1$ and $B = X^4 + X^2 + 1$,
  2. $A = X^6 + X^4 - X^2 - 1$ and $B = X^3 - 4X + 1$.
- Find U and V of the previous D, such that $AU + BV = D$.

4.2 Final exam.

4.2.1 Exam 1.

Exercise 4.2.1: (**05pts**) Let p, q and r be three propositions mathematics.

1. Determine all cases for which the following proposition is false, and find its negation.

$$(p \Rightarrow q) \Rightarrow (r \Rightarrow p).$$

2. Choose the proof method, and prove the following statement:

$$\forall n \in \mathbb{Z}, n \neq 0 \Rightarrow 2^n + 3 \neq 4.$$

Solution:

Let p, q and r be three propositions mathematics.

- Find all cases for which the proposition $(p \Rightarrow q) \Rightarrow (r \Rightarrow p)$ is false, using the associated truth table

p	q	r	$p \Rightarrow q$	$r \Rightarrow p$	$(p \Rightarrow q) \Rightarrow (r \Rightarrow p)$
1	1	1	1	1	1
1	1	0	1	1	1
1	0	1	0	1	1
1	0	0	0	1	1
0	1	1	1	0	0
0	1	0	1	1	1
0	0	1	1	0	0
0	0	0	1	1	1

  So the proposition $(p \Rightarrow q) \Rightarrow (r \Rightarrow p)$ is false in both cases:
  - 1^{st} : p is false, q is false and r is true. **(01)**
  - 2^{nd} : p is false, q is true and r is true. **(01)**
- Negation of the previous statement.

$$\begin{aligned} \overline{(p \Rightarrow q) \Rightarrow (r \Rightarrow p)} &\Leftrightarrow (p \Rightarrow q) \wedge \overline{(r \Rightarrow p)} \\ &\Leftrightarrow (p \Rightarrow q) \wedge (r \wedge \overline{p}). \textbf{(01)} \end{aligned}$$

- The appropriate proof method and Prove
  - The appropriate proof method is contrapositive proof.**(0.5)**
  - **Prove** : **(01.5)**

$$\forall n \in \mathbb{Z}, n \neq 0 \Rightarrow 2^n + 3 \neq 4.$$

Using contrapositive proof, we prove

$$(2^n + 3 = 4) \Rightarrow \exists n \in \mathbb{Z}, n = 0.$$

Then, let $n \in \mathbb{Z}$

$$\begin{aligned}(2^n+3=4) &\Rightarrow 2^n=1\\ &\Rightarrow \ln 2^n=\ln 1\\ &\Rightarrow n\ln 2=0\\ &\Rightarrow n=0.\end{aligned}$$

Finally

$$\forall n\in\mathbb{Z}, n\neq 0 \Rightarrow 2^n+3\neq 4.$$

Exercise 4.2.2: **(04pts)**
Let the application f be defined by

$$\begin{array}{rccc} f: & \mathbb{N}\times\mathbb{R}-\{-1\} & \to & \mathbb{R} \\ & (n,x) & \longmapsto & f(n,x)=\frac{n}{x+1}. \end{array}$$

1. Calculate $f(\{1,2\}\times[0,2])$ and $f^{-1}(\{1\})$.
2. Study the injectivity and the surjectivity of f.

Solution:

- Calculate $f(\{1,2\}\times[0,2])$ et $f^{-1}(\{1\})$.
  1. $f(\{1,2\}\times[0,2])$. **(01)**
  $$\begin{aligned} f(\{1,2\}\times[0,2]) &= \{f(n,x):(n,x)\in\{1,2\}\times[0,2]\}\\ &= \{f(1,x):x\in[0,2]\}\cup\{f(2,x):x\in[0,2]\},\end{aligned}$$
  so for $n\in\{1,2\}$
  $$x\in[0,2]\Rightarrow \frac{n}{x+1}\in\left[\frac{n}{3},n\right].$$
  Then
  $$f(\{1,2\}\times[0,2])=\left[\frac{1}{3},1\right]\cup\left[\frac{2}{3},2\right]=\left[\frac{1}{3},2\right].$$
  2. $f^{-1}(\{1\})$. **(01)**
  $$\begin{aligned} f^{-1}(\{1\}) &= \left\{(n,x):\frac{n}{x+1}=1\right\}\\ &= \{(n,x):x=n-1\}\\ &= \{(n,n-1):n\in\mathbb{N}^*\}.\end{aligned}$$
- Study the injectivity and surjectivity of f.
  1. Injectivity: we have for example $f(0,0)=f(0,1)$, but $(0,0)\neq(0,1)$, then f is not injective. **(01)**
  2. Surjectivity: let $y\in\mathbb{R}$, then
     (a) If $y=0$, then $\exists n=0$, and $x\in\mathbb{R}\setminus\{-1\}$ such that $0=\frac{0}{x+1}$.
     (b) If $y\neq 0$, then $\exists n\in\mathbb{N}^*$ and $\exists x\in\mathbb{R}$, for example $n=|[y]|+1\in\mathbb{N}^*$, and $x=\frac{|[y]|+1}{y}-1\in\mathbb{R}\setminus\{-1\}$ such that $y=\frac{n}{x+1}$.
     where $[.]$: is the integer part function. Then f is surjective. **(01)**

Exercise 4.2.3: (04 pts)

1. Let $(\mathbb{G},\star)$ be a commutative group and e its neutral element. Show that the set
$$\mathbb{H}=\{a\in\mathbb{G}:\ a\star a\star a=a\},$$
is a subgroup of $(\mathbb{G},\star)$.
2. Solve in $\mathbb{H}$ the following equation $x^{2024}=e$, where $x^n=\underbrace{x\star x\star\ldots\star x}_{n\text{ times}}$.

Solution:

I Show that the set $\mathbb{H}=\{a\in\mathbb{G}:\ a\star a=a\}$ is a subgroup of $(\mathbb{G},\star)$.

i) $\mathbb{H}\neq\varnothing$, because $e\star e\star e=e\star e=e\Rightarrow e\in\mathbb{H}$. **(0.5)**

2i) Let $a\in\mathbb{H}:a^{-1}\overset{?}{\in}\mathbb{H}$, then let $a\in\mathbb{G}$:

$$a^{-1}\star a^{-1}\star a^{-1}=(a\star a)^{-1}\star a^{-1}=(a\star a\star a)^{-1}=a^{-1}.$$

So $a^{-1}\in\mathbb{H}$. **(01)**

3i) Let $a,b\in\mathbb{H}:a\star b\overset{?}{\in}\mathbb{H}$, then

$$\begin{aligned}&a\star b\star a\star b\star a\star b\overset{\star:\text{ commutative}}{=}a\star a\star b\star a\star b\star b\\ =\ &a\star a\star a\star b\star b\star b=a\star\star b.\end{aligned}$$

So $a\star b\in\mathbb{H}$, and finally $\mathbb{H}$ is a subgroup of $(\mathbb{G},\star)$. **(01)**

II Solve in $\mathbb{H}$ the following equation $x^{2024}=e$, we have

$$\begin{aligned}x^{2024}&=\underbrace{x\star x\star\ldots\star x}_{2024\text{ times}}=\underbrace{x\star\ldots\star x}_{674\times3\text{ times}}\star x\star x=\underbrace{x\star\ldots\star x}_{675\text{ times}}\star x\\&=\underbrace{x\star\ldots\star x}_{225\times3\text{ times}}\star x=\underbrace{x\star\ldots\star x}_{225\text{ times}}\star x=\underbrace{x\star\ldots\star x}_{75\times3\text{ times}}\star x=\underbrace{x\star\ldots\star x}_{75\text{ times}}\star x\\&=\underbrace{x\star\ldots\star x}_{25\times3\text{ times}}\star x=\underbrace{x\star\ldots\star x}_{25\text{ times}}\star x=\underbrace{x\star\ldots\star x}_{8\times3\text{ times}}\star x\star x\\&=\underbrace{x\star\ldots\star x\star x}_{9\text{ times}}\star x=x\star x\star x\star x=x\star x.\end{aligned}$$

Then

$$x\star x=e\Rightarrow x=x^{-1},$$

hence the set of solutions is $\mathbb{S}=\left\{x\in\mathbb{H}:\ x=x^{-1}\right\}$. **(01.5)**

Exercise 4.2.4: (07 pts)

- What is the value of a such that the polynomail

$$P_a = X^4 + X^2 + a$$

does not accept roots in $\mathbb{R}$. In this case what do you conclude?
- Factor the polynomail P_1 in $\mathbb{R}[X]$.
- Find the $D = \gcd(P_1, Q)$, where $Q = X^5 + X^4 + 2X^3 + X^2 + X$.
  1. Deduce the factorization of Q in $\mathbb{R}[X]$.
  2. Find A and B of the previous D, such that $AP_1 + BQ = D$.
  3. Decompose the fraction $\frac{Q}{P_1}$ into simple elements in $\mathbb{R}[X]$.

Solution:

- – The value of a such that the polynomail P_a does not accept the roots in $\mathbb{R}$. We consider the function

$$X \longmapsto P_a(X) = X^4 + X^2 + a.$$

So, we have

$$P_a'(X) = 4X^3 + 2X = 2X\left(2X^2 + 1\right),$$

then,

$$P_a'(X) = 0 \Longrightarrow X = 0,$$

since, $P_a(0) = a$, then graph of $P(X)$ pass by the axis (Ox) if $a \leq 0$.
Then the polynomail P_a does not accept the roots in $\mathbb{R}$ if $a \in]0, +\infty[$. **(01)**
$xP_a'(x)P_a\infty 0\infty\infty P_a(0)\infty$
  – Conclusion: The polynomail P_a does not accept the roots in $\mathbb{R}$, but it is of degree 4, so it is the product of polynomials of degree 2, **(0.5)**
- Factor the polynomail P_1 in $\mathbb{R}[X]$: we have $a = 1$ so P it is the product of polynomials of degree 2. Then **(01)**

$$\begin{aligned} X^4 + X^2 + 1 &= \left(X^2 + 1\right)^2 - X^2 \\ &= \left(X^2 + X + 1\right)\left(X^2 - X + 1\right). \end{aligned}$$

- Find the $D = \gcd(P_1, Q)$, where $Q = X^5 + X^4 + 2X^3 + X^2 + X$. Using Euclidean division we find

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

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

$$\begin{array}{rr|l} X^3 & -1 & X^2+X+1 \\ \cline{3-3} -X^3-X^2-X & & X-1 \\ \cline{1-1} -X^2-X-1 & & \\ X^2+X+1 & & \\ \cline{1-1} 0 & & \end{array}$$

then $D = \gcd(P_1, Q) = X^2+X+1$. **(02)**

1. Deduce the factorization of Q in $\mathbb{R}[X]$. Factorization of Q in $\mathbb{R}[X]$, from the above, we get Q divisible by$D = X^2+X+1$, then

$$\begin{array}{rr|l} X^5+X^4+2X^3+X^2+X & & X^2+X+1 \\ \cline{3-3} -X^5-X^4 & -X^3 & X^3+X \\ \cline{1-2} & X^3+X^2+X & \\ & -X^3-X^2-X & \\ \cline{2-2} & 0 & \end{array}$$

   And from it we find **(0.5)**

$$X^5+X^4+2X^3+X^2+X = X(X^2+1)(X^2+X+1).$$

2. Find A and B of the previous D, such that $AP_1+BQ = D$: According to the euclidean division, we obtain

$$Q = (X+1)P_1+(X^3-1), \quad \text{and} \quad P_1 = X(X^3-1)+D.$$

   Then

$$D = P_1 - X(Q-(X+1)P_1) = (-X)Q+(X^2+X+1)P_1.$$

   So **(01)**

$$A = (X^2+X+1), B = (-X).$$

3. Decompose the fraction $\frac{Q}{P_1}$ into simple elements in $\mathbb{R}[X]$.

$$\frac{Q}{P_1} = \frac{(X^3+X)D}{(X^2-X+1)D} = \frac{X^3+X}{X^2-X+1}$$

and

$$\begin{array}{rr|l} X^3 & +X & X^2-X+1 \\ \cline{3-3} -X^3+X^2-X & & X+1 \\ \cline{1-1} X^2 & & \\ -X^2+X-1 & & \\ \cline{1-1} X-1 & & \end{array}$$

Finally **(01)**

$$\frac{Q}{P_1}=\frac{X^3+X}{X^2-X+1}=X+1+\frac{X-1}{X^2-X+1}.$$

4.2.2 Exam 2.

Exercise 4.2.5: **(04pts)**

1. Let A and B two parts of a set $\mathbb{E}$, show that: $(A\cap B)\cup B^c = A\cup B^c$.
2. By contrapositive proof, show that: If (n^2-1) is not divisible by 8, so n is even.

Solution:

1. Show that: $(A\cap B)\cup B^c = A\cup B^c$. **(02)**

$$\begin{aligned} \text{Let } x \quad \in \quad & (A\cap B)\cup B^c \iff x\in(A\cap B)\vee x\in B^c \\ \iff \quad & (x\in A\wedge x\in B)\vee(x\in B^c) \\ \iff \quad & (x\in A\vee x\in B^c)\wedge(x\in B\vee x\in B^c) \\ \iff \quad & (x\in A\cup B^c)\wedge(x\in B\cup B^c) \\ \iff \quad & (x\in A\cup B^c)\wedge(x\in \mathbb{E}) \\ \iff \quad & x\in(A\cup B^c)\cap\mathbb{E} \\ \iff \quad & x\in A\cup B^c. \end{aligned}$$

2. By contrapositive proof, show that: If (n^2-1) is not divisible by 8, so n is even. **(02)**

Let n be odd then $\exists k\in\mathbb{Z}$ such that $n=2k+1$, so

$$n^2=4k^2+4k+1 \Leftrightarrow n^2-1=4k(k+1)$$

it suffices to show that $k(k+1)$ is even, we have two cases:
If k is even then $k+1$ is odd so the product of an even number and an odd number is even.
If k is odd, then $k+1$ is even so the product is even it is the same reasoning, (you should know that the product of two consecutive numbers is always even).
Thus $k(k+1)$ is even $\exists k'\in\mathbb{Z} : k(k+1)=2k'$, hence

$$n^2-1=8k'$$

So n^2-1 is divisible by 8.

Exercise 4.2.6: (**06pts**) Let the composition low $\star$ be defined in $\mathbb{E}=\mathbb{R}-\left\{\frac{1}{2}\right\}$ by

$$\begin{array}{rccc}\star: & \mathbb{E}\times\mathbb{E} & \longrightarrow & \mathbb{E} \\ & (a,b) & \longmapsto & a\star b=a+b-2ab\end{array}.$$

1. Show that $\star$ is an internal composition law.
2. Show that $(\mathbb{E},\star)$ is a commutative group.
3. Show that $\mathbb{H}=\left\{0,2,\frac{2}{3}\right\}$ is a subgroup of $\mathbb{E}$.

Solution:

1. Show that $\star$ is an internal law in $\mathbb{E}$ **(01)**,
   indeed: $\forall a,b\in\mathbb{E}$, $a+b-2ab\overset{??}{\in}\mathbb{E}$. (that's to say $\forall a,b\in\mathbb{E}: a+b-2ab\neq\frac{1}{2}$).
   we show by the absurd we suppose that $a+b-2ab=\frac{1}{2}$, knowing that $a\neq\frac{1}{2}$, and $b\neq\frac{1}{2}$
   $$\begin{aligned}a+b-2ab &= \frac{1}{2}\Rightarrow(2a-1)\left(b-\frac{1}{2}\right)=0\\ &\Rightarrow a=\frac{1}{2}\text{ or }b=\frac{1}{2}.\end{aligned}$$
   contradiction, so $a+b-2ab=\frac{1}{2}$ is false, that is to say $a+b-2ab\neq\frac{1}{2}$, and from it $a\star b\in\mathbb{E}$, $\star$ is an internal law.
2. Show that $(\mathbb{E},\star)$ is a commutative group.
   (a) Commutativity **(0.5)**: Let $a,b\in\mathbb{E}$, then $a\star b=a+b-2ab=b+a-2ba=b\star a$, so $\star$ is a commutative.
   (b) Associativity **(01)**: Let $\forall a,b,c\in\mathbb{E}$, then
   $$\begin{aligned}(a\star b)\star c &= a\star b+c-2(a\star b)c\\ &= b+a-2ab+c-2(b+a-2ba)c\\ &= b+a+c-2ab-2bc-2ac+4bac\end{aligned}$$
   and
   $$\begin{aligned}a\star(b\star c) &= a\star(b+c-2bc)\\ &= a+(b+c-2bc)-2a(b+c-2bc)\\ &= b+a+c-2bc-2ab-2ac+4bac\\ &= (a\star b)\star c\end{aligned}$$
   so $\star$ is a associative.
   (c) Identity element **(01)**: $\overset{?}{\exists}e\in\mathbb{E}$, $\forall a\in\mathbb{E}: a\star e=e\star a=a$,
   $$\begin{aligned}a\star e &= a\Longrightarrow a+e-2ea=a\\ &\Longrightarrow e(1-2a)=0\\ &\Longrightarrow e=0.\end{aligned}$$
   so the identity element is $e=0$.
   (d) Inverse element **(01)** : $\forall a\in\mathbb{E},\overset{?}{\exists}a^{-1}\in\mathbb{E},: a\star a^{-1}=a^{-1}\star a=0$,
   $$\begin{aligned}a\star a^{-1} &= 0\Longrightarrow a+a^{-1}-2aa^{-1}=0\\ &\Longrightarrow a^{-1}=\frac{a}{2a-1}\end{aligned}$$

so for all a in $\mathbb{E}$, there exist an inverse element $a^{-1}=\frac{a}{2a-1}\in\mathbb{E}$.
Finailly $(\mathbb{E},\star)$ is a commutative group.

3. Show that $\mathbb{H}=\left\{0,2,\frac{2}{3}\right\}$ is a subgroup of $\mathbb{E}$.
   (a) $e=0\in\mathbb{H}$. **(0.5)**
   (b) **(0.5)**

$$\begin{cases} 0\star 2=2\in\mathbb{H} \\ 0\star\frac{2}{3}=\frac{2}{3}\in\mathbb{H} \\ 2\star\frac{2}{3}=0\in\mathbb{H} \end{cases}$$

   (c) **(0.5)**

$$\begin{cases} 0^{-1}=0\in\mathbb{H} \\ \left(\frac{2}{3}\right)^{-1}=2\in\mathbb{H} \\ (2)^{-1}=\frac{2}{3}\in\mathbb{H} \end{cases}$$

So $\mathbb{H}=\left\{0,2,\frac{2}{3}\right\}$ is a subgroup of $\mathbb{E}$.

Exercise 4.2.7: **(04pts)**
Let the application g be defined by

$$\begin{array}{rccc} g: & \mathbb{N}\times\mathbb{N} & \to & \mathbb{N}\cup\{-3,-2,-1\} \\ & (n,m) & \longmapsto & g(n,m)=n+m-3. \end{array}$$

1. Calculate $g(\{(1,2),(2,3)\})$ and $g^{-1}(\{2\})$.
2. Study the injectivity and the surjectivity of g.

Solution:

- $g(\{(1,2),(2,3)\})$ and $g^{-1}(\{2\})$.
  1. $g(\{(1,2),(2,3)\})$. **(01)**

$$\begin{aligned} g(\{(1,2),(2,3)\}) &= \{g(n,m):(n,m)\in\{(1,2),(2,3)\}\} \\ &= \{g(1,2),g(2,3)\} \\ &= \{0,2\} \end{aligned}$$

  2. $g^{-1}(\{2\})$. **(01)**

$$\begin{aligned} g^{-1}(\{2\}) &= \{(n,m):n+m-3=2\} \\ &= \{(n,m):m+n=5,n,m\in\mathbb{N}\} \\ &= \{(0,5),(1,4),(2,3),(3,2),(4,1),(5,0)\} \end{aligned}$$

- Study the injectivity and surjectivity of g.
  1. Injectivity: we have for example $g(0,5)=g(1,4)$, but $(0,5)\neq(1,4)$, then g is not injective. **(01)**
  2. Surjectivity: we have $\forall s\in\mathbb{N}\cup\{-3,-2,-1\}$, $\exists(n,m)\in\mathbb{N}:n+m-3=s$.(For example $n=0,m=s+3$)
     Then g is surjective. **(01)**

Exercise 4.2.8: **(06pts)**
Let P and Q be two polynomials such that:
$P(X) = X^4 + 2X^3 - X - 2$, and $Q(X) = X^5 + 2X^4 - X^3 - 2X^2 + X + 2$.
1. Find the $D = \gcd(P, Q)$.
2. Find the polynomials A and B such that $D = AP + BQ$.
3. Factor the polynomails P and Q into a product of irreducible factors in $\mathbb{R}[X]$.

Solution:

1. Find the $D = \gcd(P, Q)$.
   (a) 1^{st}: We divide Q by P, we obtain
   $$R_1(X) = -X^3 - X^2 + 3X + 2, \text{ and } Q_1(X) = X.$$
   (b) 2^{nd}: We divide P by R_1, we obtain
   $$R_2(X) = 2X^2 + 4X, \text{ and } Q_2(X) = -(X+1).$$
   (c) 3^{rd}: We divide R_1 by R_2, we obtain
   $$R_3(X) = X + 2, \text{ and } Q_3(X) = -\frac{1}{2}(X-1).$$
   (d) 4^{th}: We divide R_2 by R_3, we obtain
   $$R_4(X) = 0, \text{ and } Q_4(X) = 2X.$$
   So $D = \gcd(P, Q) = R_3(X) = X + 2$. **(02)**
2. Find the polynomials A and B such that $D = AP + BQ$.
   we have
   $$\begin{cases} Q = Q_1 P + R_1 \\ P = R_1 Q_2 + R_2 \\ R_1 = R_2 Q_3 + D \end{cases} \Longrightarrow \begin{cases} R_1 = Q - Q_1 P \\ R_2 = P - R_1 Q_2 \\ D = R_1 - R_2 Q_3 \end{cases}$$
   $$\Longrightarrow D = (1 + Q_2 Q_3) Q + (-Q_1 - Q_3 - Q_1 Q_2 Q_3) P$$
   so
   $$A = -Q_1 - Q_3 - Q_1 Q_2 Q_3 = -\frac{1}{2}\left(X^3 + 1\right). \textbf{(0.5)}$$
   $$B = 1 + Q_2 Q_3 = \frac{1}{2}\left(X^2 + 1\right). \textbf{(0.5)}$$
3. Factor the polynomails P and Q into a product of irreducible factors in $\mathbb{R}[X]$.
   (a) **(01.5)**
   $$\begin{aligned} Q(X) &= X^5 + 2X^4 - X^3 - 2X^2 + X + 2 \\ &= (X+2)\left(X^4 - X^2 + 1\right) \\ &= (X+2)\left(X^4 + 2X^2 + 1 - 3X^2\right) \\ &= (X+2)\left(\left(X^2+1\right)^2 - \left(\sqrt{3}X\right)^2\right) \\ &= (X+2)\left(X^2 + \sqrt{3}X + 1\right)\left(X^2 - \sqrt{3}X + 1\right). \end{aligned}$$

(b) **(01.5)**

$$\begin{aligned} P(X) &= X^4+2X^3-X-2 \\ &= (X+2)\left(X^3-1\right) \\ &= (X+2)(X-1)\left(X^2+X+1\right). \end{aligned}$$

4.2.3 Exam 3.

Exercise 4.2.9: **(08pts)** Let the composition low $\otimes$ be defined in $\mathbb{G}=\mathbb{R}-\left\{\frac{-1}{3}\right\}$ by

$$\begin{array}{rccc} \otimes: & \mathbb{G}\times\mathbb{G} & \longrightarrow & \mathbb{G} \\ & (x,y) & \longmapsto & x\otimes y = x+y+3xy \end{array}.$$

1. Show that $\otimes$ is an internal composition law.
2. Show that $(\mathbb{G},\otimes)$ is a commutative group.
3. Show that $\mathbb{H}=\left\{0,1,\frac{-1}{4}\right\}$ is a subgroup of $\mathbb{G}$.

Solution:

1. Show that $\otimes$ is an internal law in $\mathbb{G}$ **(01.5)**,
   indeed: $\forall a,b\in\mathbb{E}$, $a+b+3ab\overset{??}{\in}\mathbb{G}$. (that's to say $\forall a,b\in\mathbb{G}: a+b+3ab\neq\frac{-1}{3}$).
   we show by the absurd we suppose that $a+b+3ab=\frac{-1}{3}$, knowing that $a\neq\frac{-1}{3}$, and $b\neq\frac{-1}{3}$

$$\begin{aligned} a+b+3ab &= \frac{-1}{3} \Rightarrow (3a+1)\left(b+\frac{1}{3}\right)=0 \\ &\Rightarrow a=\frac{-1}{3} \text{ or } b=\frac{-1}{3}. \end{aligned}$$

   contradiction, so $a+b+3ab=\frac{-1}{3}$ is false, that is to say $a+b+3ab\neq\frac{-1}{3}$, and from it $a\otimes b\in\mathbb{G}$, $\otimes$ is an internal law.
2. Show that $(\mathbb{G},\otimes)$ is a commutative group.
   (a) Commutativity **(01)**: Let $a,b\in\mathbb{G}$, then $a\otimes b=a+b+3ab=b+a+3ba=b\otimes a$, so $\otimes$ is a commutative.
   (b) Associativity **(02)**: Let $\forall a,b,c\in\mathbb{G}$, then

$$\begin{aligned} (a\otimes b)\otimes c &= a\otimes b+c+3(a\otimes b)c \\ &= b+a+3ab+c+3(b+a+3ba)c \\ &= b+a+c+3ab+3bc+3ac+9bac \end{aligned}$$

   and

$$\begin{aligned} a\otimes(b\otimes c) &= a\otimes(b+c+3bc) \\ &= a+(b+c+3bc)+3a(b+c+3bc) \\ &= b+a+c+3bc+3ab+3ac+9bac \\ &= (a\otimes b)\otimes c \end{aligned}$$

   so $\otimes$ is a associative.

(c) Identity element **(01)**: $\overset{?}{\exists} e \in \mathbb{G}, \forall a \in \mathbb{G} : a \otimes e = e \otimes a = a$,

$$\begin{aligned} a \otimes e &= a \Longrightarrow a + e + 3ea = a \\ &\Longrightarrow e(1+3a) = 0 \\ &\Longrightarrow e = 0. \end{aligned}$$

so the identity element is $e = 0$.

(d) Inverse element **(01)** : $\forall a \in \mathbb{G}, \overset{?}{\exists} a^{-1} \in \mathbb{E}, : a \otimes a^{-1} = a^{-1} \otimes a = 0$,

$$\begin{aligned} a \otimes a^{-1} &= 0 \Longrightarrow a + a^{-1} + 3aa^{-1} = 0 \\ &\Longrightarrow a^{-1} = \frac{-a}{3a+1} \end{aligned}$$

so for all a in $\mathbb{G}$, there exist an inverse element $a^{-1} = \frac{-a}{3a+1} \in \mathbb{G}$.

Finaily $(\mathbb{G}, \otimes)$ is a commutative group.

3. Show that $\mathbb{H} = \left\{0, 1, \frac{-1}{4}\right\}$ is a subgroup of $\mathbb{G}$.
   (a) $e = 0 \in \mathbb{H}$. **(0.5)**
   (b) **(0.5)**

$$\begin{cases} 0 \otimes 1 = 1 \in \mathbb{H} \\ 0 \otimes \left(\frac{-1}{4}\right) = \frac{-1}{4} \in \mathbb{H} \\ 1 \otimes \left(\frac{-1}{4}\right) = 0 \in \mathbb{H} \end{cases}$$

   (c) **(0.5)**

$$\begin{cases} 0^{-1} = 0 \in \mathbb{H} \\ (1)^{-1} = \frac{-1}{4} \in \mathbb{H} \\ \left(\frac{-1}{4}\right)^{-1} = 1 \in \mathbb{H} \end{cases}$$

So $\mathbb{H} = \left\{0, 1, \frac{-1}{4}\right\}$ is a subgroup of $\mathbb{G}$.

Exercise 4.2.10: **(06pts)**
Let the application h be defined by

$$\begin{array}{rccc} h: & \mathbb{N} \times \mathbb{N} \times \mathbb{N} & \to & \mathbb{N} \cup \{-1\} \\ & (n,m,p) & \longmapsto & h(n,m,p) = n+m+p-1. \end{array}$$

1. Calculate $h(\{(0,1,2),(2,0,3)\})$ and $h^{-1}(\{1\})$.
2. Study the injectivity and the surjectivity of h.

Solution:

- $h(\{(0,1,2),(2,0,3)\})$ and $h^{-1}(\{1\})$.
  1. $h(\{(0,1,2),(2,0,3)\})$. **(01)**

$$\begin{aligned} h(\{(0,1,2),(2,0,3)\}) &= \{h(n,m,p) : (n,m,p) \in \{(0,1,2),(2,0,3)\}\} \\ &= \{h(0,1,2), h(2,0,3)\} \\ &= \{2,4\} \end{aligned}$$

2. $h^{-1}(\{1\})$. **(01)**

$$\begin{aligned} h^{-1}(\{1\}) &= \{(n,m,p) : n+m+p-1=1\} \\ &= \{(n,m,p) : m+n+p=2, n,m \in \mathbb{N}\} \\ &= \{(0,0,2),(0,2,0),(2,0,0),(1,1,0),(1,0,1),(0,1,1)\} \end{aligned}$$

- Study the injectivity and surjectivity of h.
  1. Injectivity: we have for example $h(0,0,2) = h(2,0,0)$, but $(0,0,2) \neq (2,0,0)$, then h is not injective. **(01)**
  2. Surjectivity: we have $\forall s \in \mathbb{N} \cup \{-1\}, \exists (n,m,p) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N} : n+m+p-1 = s$.(For example $n = 0, m = s+1, p = 0$)
     Then h is surjective. **(01)**

Exercise 4.2.11: **(06pts)**
Let A and B be two polynomials such that:
$A = X^4 + 2X^3 - X - 2$, and $B = X^6 + 2X^5 - X^4 - 2X^3 + X^2 + 2X$.

1. Find the $D = \gcd(A,B)$.
2. Factor the polynomails A and B into a product of irreducible factors in $\mathbb{R}[X]$.

Solution:

1. Find the $D = \gcd(A,B)$.
   (a) 1^{st}: We divide B by A, we obtain

$$R_1(X) = X^3 + 3X^2 + X - 2, \text{ and } Q_1(X) = X^2 - 1.$$

   (b) 2^{nd}: We divide P by R_1, we obtain

$$R_2(X) = 2X^2 + 2X - 4, \text{ and } Q_2(X) = X - 1.$$

   (c) 3^{rd}: We divide R_1 by R_2, we obtain

$$R_3(X) = X + 2, \text{ and } Q_3(X) = \frac{1}{2}X + 1.$$

   (d) 4^{th}: We divide R_2 by R_3, we obtain

$$R_4(X) = 0, \text{ and } Q_4(X) = 2X.$$

   So $D = \gcd(A,B) = R_3(X) = X + 2$.**(03)**
2. Factor the polynomails A and B into a product of irreducible factors in $\mathbb{R}[X]$.
   (a) **(01.5)**

$$\begin{aligned} B(X) &= X^6 + 2X^5 - X^4 - 2X^3 + X^2 + 2X \\ &= X(X+2)(X^4 - X^2 + 1) \\ &= X(X+2)(X^4 + 2X^2 + 1 - 3X^2) \\ &= X(X+2)\left((X^2+1)^2 - \left(\sqrt{3}X\right)^2\right) \\ &= X(X+2)\left(X^2 + \sqrt{3}X + 1\right)\left(X^2 - \sqrt{3}X + 1\right). \end{aligned}$$

(b) **(01.5)**

$$\begin{aligned} A(X) &= X^4+2X^3-X-2 \\ &= (X+2)\left(X^3-1\right) \\ &= (X+2)(X-1)\left(X^2+X+1\right). \end{aligned}$$

4.2.4 Exam 4.

Exercise 4.2.12: **(06pts)**

1. Let p and r be two propositions mathematics, show that the following equivalence:

$$(p \Rightarrow r) \Leftrightarrow (p \Rightarrow p \wedge r).$$

2. Choose the proof method, and prove the following statement:

$$\forall n,m \in \mathbb{Z}, n \neq m \Rightarrow 2^n + 2^m \neq 32.$$

Exercise 4.2.13: **(06pts)**

Let the application f be defined by

$$\begin{array}{rccc} f: & \mathbb{R} & \to & \mathbb{Z}\times\mathbb{R} \\ & x & \longmapsto & f(x) = ([x],x). \end{array}$$

where $[.]$: is the integer part function.

1. Calculate $f(\{\frac{11}{5}, \frac{-11}{3}\})$ and $f^{-1}(\{(0,3)\})$.
2. Study the injectivity and the surjectivity of f.

Exercise 4.2.14: **(08pts)**

1. Let P and Q be two polynomails

$$P = X^4 - X^2 + 1,$$

$$Q = X^5 + \sqrt{3}X^4 + 2X^3 + \sqrt{3}X^2 + X.$$

2. Factor the polynomail P in $\mathbb{R}[X]$.
3. Find the $D = \gcd(P,Q)$, where
   (a) Deduce the factorization of Q in $\mathbb{R}[X]$.
   (b) Decompose the fraction $\frac{Q}{P}$ into simple elements in $\mathbb{R}[X]$.

Bibliography

Bibliography

[1] **Stéphane BALAC, Frédéric STURM**. Algèbre et Analyse Cours de mathématiques de première année avec exercices corrigés. 2^e édition revue et augmentée (2009)

[2] **J.M.Arnaudiès, H.Fraysse**. Cours de mathématiques-1 Algèbre Classes préparatoires 1^{er}cycle universitaire (Dunod université 1992)

[3] **J.QUINET** Cours élémentaire de mathématiques supérieues-1 Algèbre 6^e édition Dunod (1976)

[4] **Marie ALLANO6CHEVALIER.** MATHS MPSI 1^{RE} ANNÉE Cours et exercices avec solutions.

[5] **Daniel FREDON et Myriam MAUMY-BERTRAND** . Mathématiques Algèbre et géométrie en 30 fiches. Dunod, Paris, 2009

[6] **A. Bodin, B. Boutin, P. Romon**. Algèbre : Cours de Mathématiques première année Ex07.