الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIR

Ministère de l'Enseignement Supérieur de la Recherche Scientifique
Université 8 mai 1945 Guelma
Faculté des Mathématiques et de l'Informatique et des Sciences de la Matière
Département de Mathématiques

وزارة التعليم العالي و البحث العلمي
جامعة 8 ماي 1945 قالمة
كلية الرياضيات و الإعلام الآلي و علوم المادة
قسم الرياضيات

Course support for the module

ALGEBRA I

Intended for first-year LMD computer science & engineering students

Presented by: Dr. Badreddine MEFTAH

Academic year
2025

Semestre:1
Unité d'enseignement : UEF11
Matière : Analyse 1
Crédits : 6
Coefficient : 4
Objectif du cours:L'objectif de ce module est de familiariser les étudiants avec le vocabulaire ensembliste, de donner des différentes méthodes de convergence des suites réelles et les différents aspects de l'analyse des fonctions d'une variable réelle.
Connaissances préalables recommandées : Niveau terminale.
Contenu de la matière :
Chapitre 1 : Le Corps des Réels
$\mathbb{R}$ est un corps commutatif, $\mathbb{R}$ est un corps totalement ordonné, Raisonnement par récurrence, $\mathbb{R}$ est un corps valué, Intervalles, Bornes supérieure et inférieure d'un sous ensemble de $\mathbb{R}$, $\mathbb{R}$ est un corps archimédien, Caractérisation des bornes supérieure et inférieure, La fonction partie entière, Ensembles bornés, Prolongement de $\mathbb{R}$: Droite numérique achevée $\mathbb{R}$, Propriétés topologiques de $\mathbb{R}$, Parties ouvertes fermées.
Chapitre 2 : Le Corps des Nombres Complexes
Opérations algébriques sur les nombres complexes, Module d'un nombre complexe z, Représentation géométrique d'un nombre complexe, Forme trigonométrique d'un nombre complexe, Formules d'Euler, Forme exponentielle d'un nombre complexe, Racines n-ième d'un nombre complexe.
Chapitre 3 : Suites de Nombres réels
Suites bornées, suites convergentes, Propriétés des suites convergentes, Opérations arithmétiques sur les suites convergentes, Extensions aux limites infinies, Infiniment petit et infiniment grand, Suites monotones, Suites extraites, Suite de Cauchy, Généralisation de notion de la limite, Limite supérieure, Limite inférieure, Suites récurrentes.
Chapitre 4 : Fonctions réelles d'une variable réelle
Graphe d'une fonction réelle d'une variable réelle, Fonctions paires-impaires, Fonctions périodiques, Fonctions bornées, Fonctions monotones, Maximum local, Minimum local, Limite d'une fonction, Théorèmes sur les limites, Opérations sur les limites, Fonctions continues, Discontinuités de première et de seconde espèce, Continuité uniforme, Théorèmes sur les fonctions continues sur un intervalle fermé, Fonction réciproque continue, Ordre d'une variable-équivalence (Notation de Landau).
Chapitre 5: Fonctions dérivables
Dérivée à droite, dérivée à gauche, Interprétation géométrique de la dérivée, Opérations sur les fonctions dérivables, Différentielle-Fonctions différentiables, Théorème de Fermat, Théorème de Rolle, Théorème des accroissements finis, Dérivées d'ordre supérieur, Formule de Taylor, Extrémum local d'une fonction, Bornes d'une fonction sur un intervalle, Convexité d'une courbe. Point d'inflexion, Asymptote d'une courbe, Construction du graphe d'une fonction.
Chapitre 6 : Fonctions Élémentaires
Logarithme népérien, Exponentielle népérienne, Logarithme de base quelconque, Fonction puissance, Fonctions hyperboliques, Fonctions hyperboliques réciproques.
Mode d'évaluation : Examen (60%), contrôle continu (40%)
Références

1. J.-M. Monier, Analyse PCSI-PTSI, Dunod, Paris 23.
2. Y. Bougrov et S. Nikolski, Cours de Mathématiques Supérieures, Editions Mir, Moscou, 1983.
3. N. Piskounov, Calcul différentiel et intégral, Tome 1, Editions Mir, Moscou, 1980.
4. K. Allab, Eléments d'Analyse, OPU, Alger, 1984.
5. B. Calvo, J. Doyen, A. Calvo, F. Boschet, Cours d'analyse, Librairie Armand Colin, Paris, 1976.
6. J. Lelong-Ferrand et J. M. Arnaudiès, Cours de mathématiques, tome 2, Edition Dunod, 1978.

Contents

Introduction

The Algebra 1 course, which covers the first semester, is aimed at first-year undergraduate students in computer science (LMD) and engineering students. It can also be used by students at various levels.

As per the core curriculum, the course contains four chapters. A number of examples are given to enhance the information and guarantee that the ideas being covered are understood. A number of exercises with solutions are included at the conclusion of each chapter to help students solidify their comprehension.

The format of this course is as follows:

- Propositional logic is covered in the first chapter.
- Basic ideas related to set theory, binary relations, and applications are discussed in the second chapter.
- Group theory is presented in the third chapter.
- The idea of polynomials with indeterminacy, coefficients in a ring, and the method of decomposition into rational fractions are treated in the last chapter.

Chapter 1

Mathematical logic

Logic can be defined as the science of reasoning. It represents a non-empirical science like mathematics. Its objective is to discern between sound and flawed reasoning. Making inferences, or deriving conclusions from facts, data, and information.

The following elements must be present in every well-written mathematical theory.

Definition 1.1. *An axiom is a claim that is made without any effort to prove it and is taken for granted. Stated differently, a principle that serves as the foundation for a self-evident demonstration.*

Example 1.1. *Euclid's axioms for plane geometry*

- *There is always a line that passes through two points on the plane.*
- *Any segment can be extended along its direction into an (infinite) line.*
- *From a segment, there exists a circle whose center is one of the points on the segment and whose radius is the length of the segment.*
- *Every right angle is equal to every other right angle.*
- *There is only one line parallel to a line that passes through a point located outside that line.*

Example 1.2. *Peano's axioms for the construction of integers*

- *The element called zero and noted* 0 *is a natural number.*
- *Every natural number* n *has a unique successor, denoted* $s(n)$*, which is a natural number.*
- 0 *is not a successor of any natural integer.*
- *The successor's injectivity is* $\forall x, y \in \mathbb{N} : s(x) = s(y) \Rightarrow x = y$.

- *The set of natural numbers* $\mathbb{N}$ *is the only set that includes* 0 *and the successors of each of its elements.*

Definition 1.2. *A proposition is a statement that can be true or false, not both at the same time.*

Example 1.3. $\sqrt{4} = -2$ *is a false proposition.*

Example 1.4. $|-5| = 5$ *is a true proposition.*

Remark 1.1. *A propositional form is any mathematical expression containing a variable* x *that cannot be said to be true or false.*

Example 1.5. x *be a positive real number, is a propositional form, it becomes a proposition depending on the value assigned to* x*.*

Definition 1.3. *A definition is a statement in which we describe the particularities of a mathematical object.*

Example 1.6. *A set* A *is considered convex, if* $tx+(1-t)y$ *stays in* A *for any* x,y *in* A *and* t *in* $[0,1]$*.*

Definition 1.4. *A demonstration, also known as a proof, is the accomplishment of a procedure that enables one to proceed from presumptions to conclusions.*

Definition 1.5. *A lemma is a minor result or a known partial result used to prove a major result.*

Definition 1.6. *A theorem is a result of major importance.*

Definition 1.7. *A corollary is a consequence of a theorem.*

Definition 1.8. *A conjecture is a mathematical result that we believe to be true but cannot prove.*

Definition 1.9. *A proposition, denoted by the letters* P,Q,R*, etc., is a mathematical assertion that may or may not be true.*

There is a corresponding truth table for each proposition.

P		P
V	or	1
F	0	

For two propositions P and Q there correspond 2^2 possibilities of attribution of truth.

P	Q
1	1
1	0
0	1
0	0

In general, there are 2^n ways for attribution of the truth table for every n propositions.

i2	**i1**	S
0	0	
0	1	
1	0	
1	1	

inputs:2→rows:$4 = 2^2$

i3	**i2**	**i1**	S
0	0	0	
0	0	1	
0	1	0	
0	1	1	
1	0	0	
1	0	1	
1	1	0	
1	1	1	

inputs:3→rows:$8 = 2^3$

i4	**i3**	**i2**	**i1**	S
0	0	0	0	
0	0	0	1	
0	0	1	0	
0	0	1	1	
0	1	0	0	
0	1	0	1	
0	1	1	0	
0	1	1	1	
1	0	0	0	
1	0	0	1	
1	0	1	0	
1	0	1	1	
1	1	0	0	
1	1	0	1	
1	1	1	0	
1	1	1	1	

inputs:4→rows:$16 = 2^4$

1.1 Logic connectors

Logical connectors are tools for turning preexisting propositions and generating new ones.

1.1.1 Negation of a proposition

The negation of a proposition P is a proposition denoted $\overline{P}$ which is the opposite or contrary of the proposition P. It is defined from the following truth table.

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

Example 1.7. $P : x^2 + 1 \geq 0$ *its negation is* $\overline{P} : x^2 + 1 < 0$.

1.1.2 Conjunction

The logical connector $\wedge$, or conjunction, links the assertions P and Q to the statement $P \wedge Q$, which is true if P and Q are both true at the same time and false otherwise. The following truth table defines it.

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

Example 1.8. *Let P the assertion "This card is a queen", and Q the assertion "This card is a club". The proposition $P \wedge Q$ is true if the card drawn is the queen of clubs and false otherwise.*

1.1.3 Disjunction

The logical connector $\vee$, or disjunction, links the assertions P and Q to the statement $P \vee Q$, which is false if P and Q are both false at the same time and true otherwise. The following

truth table defines it.

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

1.1.4 Implication

The logical connector $\Rightarrow$, or implication, links the assertions P and Q to the statement $P \Rightarrow Q$, which is false if P is true and Q are is false and true otherwise. The following truth table defines it.

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

1.1.5 Equivalence

The logical connector $\Leftrightarrow$, or implication, links the assertions P and Q to the statement $P \Leftrightarrow Q$, which is true if P and Q are both false or true at the same time and false otherwise. The following truth table defines it.

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

1.2 Properties of logical connectors

Definition 1.10. *A tautology is an assertion that holds true regardless of the truth values of the propositions that make it up.*

Proposition 1.1. *The following propositions are tautology regardless the truth values of the propositions, P, Q and R.*

- $P \vee \overline{P}$,
- $\overline{\overline{P}} \Leftrightarrow P$,
- $P \wedge P \Leftrightarrow P$,
- $P \vee P \Leftrightarrow P$,
- $P \wedge Q \Leftrightarrow Q \wedge P$,
- $P \vee Q \Leftrightarrow Q \vee P$,
- $(P \wedge Q) \wedge R \Leftrightarrow Q \wedge (P \wedge R)$,
- $(P \vee Q) \vee R \Leftrightarrow Q \vee (P \vee R)$,
- $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$,
- $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$,
- $P \Rightarrow Q \Leftrightarrow \overline{P} \vee Q$,
- $P \Rightarrow Q \Leftrightarrow \overline{Q} \Rightarrow \overline{P}$,
- $\overline{P \wedge Q} \Leftrightarrow \overline{P} \vee \overline{Q}$,
- $\overline{P \vee Q} \Leftrightarrow \overline{P} \wedge \overline{Q}$,
- $(P \Rightarrow Q) \wedge (Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$,
- $(P \Leftrightarrow Q) \Leftrightarrow (P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

Proof. It is enough to draw up the truth table. □

1.3 Mathematical quantifiers

1.3.1 Propositional form

Definition 1.11. *A propositional form, is a mathematical assertion that contains one or more variables and is true for certain values assigned to these variables and false in other situations. They are generally represented as* $P(x)$ *or* $P(x_1,x_2,\ldots,x_n)$.

Example 1.9. *"*$x+1\geq 0$*", this proposition is true for* $x\geq -1$ *and false otherwise.*

From a propositional form $P(x)$ defined on a set E, we construct new propositions called quantified propositions using the universal quantifiers "$\forall$"whatever or existential "$\exists$"it exists at least.

1.3.2 Universal quantifier and existential quantifier

The quantifier "whatever", denoted $\forall$, allows us to define the proposition "$\forall x\in E,P(x)$", which is true for all elements $x\in E$.

The quantifier "there exists at least", denoted $\exists$, allows us to define the proposition "$\exists x\in E,P(x)$", which is true if we can find at least one element $x\in E$ that makes the proposition $P(x)$ is true.

Remark 1.2. *We write "*$\exists !x\in E,P(x)$*"if there is only one element* $x\in E$ *for which* $P(x)$ *is true.* $\exists !$ *reads there is a unique.*

Example 1.10. $\forall x\in\mathbb{N}:x(2x-3)>0$ *is a false proposition. Howevere* $\exists x\in\mathbb{N}:x(2x-3)>0$ *is a true proposition.*

1.3.3 Rules of negation

Consider the propositional form $P(x)$ on a set E.

- The negation of the proposition "$\forall x\in E,P(x)$"is "$\exists x\in E,\overline{P(x)}$".
- The negation of the proposition "$\exists x\in E,P(x)$"is "$\forall x\in E,\overline{P(x)}$".

Remark 1.3. *Quantifiers of various types can be combined as long as their ordering are respected and two separate quantifiers are not switched.*

1.4 Reasonings

1.4.1 Direct reasoning

To demonstrate that the statement "$P \Rightarrow Q$"is accurate. it suffices to assume that P to be true and we demonstrate that Q must likewise be true.

Example 1.11. *Let $n \in \mathbb{N}$. If n is odd then n^2 is too.*

Let n be an odd number. There exists a natural integer p such that $n = 2p+1$. Consequently, $n^2 = (2p+1)^2 = 4p^2+4p+1 = 2\left(2p^2+2p\right)+1$. Thus, n^2 is odd.

1.4.2 Disjunction reasoning

It is advisable to evaluate $P(x)$ based on the likely situations when there are several cases that emerge while validating an assertion $P(x)$ based on the various values of x selected from the set E. That is, looking at each of the possible cases separately. This is a case-by-case examination.

Example 1.12. *Let $a,b \in]-1,+1[$. Let us show that $|a+b| < 1+ab$.*

- *If $a+b<0$, then $|a+b| = -(a+b)$. Since $a > -1$ therefore $a+1>0$. Similarly, we have $b+1>0$.*

  So $(1+a)(1+b) = (1+a)(1+b) = 1+a+b+ab > 0$. Thus $-(a+b) < 1+ab$.

- *In the case where $a+b \geq 0$, we have $|a+b| = a+b$. Since $a<1$ and $b<1$, we deduce $a-1<0$ and $b-1<0$. So $(a-1)(b-1)>0$. Then $(a-1)(b-1) = ab-a-b+1>0$. Therefore, $a+b<1+ab$. Thus, the proposition is proven.*

1.4.3 Reasoning by contraposition

Reasoning by contraposition is based on the following equivalence: $P \Rightarrow Q \Leftrightarrow \overline{Q} \Rightarrow \overline{P}$.

Example 1.13. *Let $x \in \mathbb{R}$. Let us show that, if $x \neq 5 \wedge x \neq -5 \Rightarrow 2x^2-50 \neq 0$.*

Assume that $2x^2-50=0$, then $x^2=25$. So $|x|=5$. Therefore, $x=5$ or $x=-5$.

1.4.4 Reasoning by contradiction

The following idea underpins the reasoning by contradiction used to demonstrate "$P \Rightarrow Q$": we presume both that P and Q are true, and then we search for a contradiction. In other terms Q can't be true when P is true.

Example 1.14. *Prove that the number $\sqrt{2}$ is irrational.*

Assuming that $\sqrt{2}$ is a rational integer, we can find a and b such that $\sqrt{2} = \frac{a}{b}$ such that a and b are coprime with $b \neq 0$. Therefore, $2 = \frac{a^2}{b^2}$, therefore $2b^2 = a^2$. Since the above equation makes it clear that 2 divides a^2. Then a^2 is even. So, there exists k such that $a = 2k$, and $2b^2 = 4k^2 \Rightarrow b^2 = 2k^2$. So, 2 divides b^2, which implies b^2 is even, then b is even. We may then infer that $\gcd(a,b) = 2$. Given that a and b are coprime, this proves that $\sqrt{2}$ is irrational.

1.4.5 Reasoning by counterexample

Finding x in E such that $P(x)$ is false is sufficient to demonstrate that an assertion of the type "$\forall x \in E : P(x)$"is false (keep in mind that the negation of "$\forall x \in E : P(x)$"is "$\exists x \in E : \overline{P(x)}$"). To demonstrate that an assertion of this type is true, we must demonstrate that $P(x)$ is true for each x in E.

Example 1.15. *Show that for all $x \in \mathbb{R} : (x-1)^2 > 0$.*

Clearly, if we take $x = 1$, we find $0 > 0$. So the proposition is false.

1.4.6 Induction principle

We may demonstrate that an assertion $P(n)$, which depends on n, is true for every $n \in \mathbb{N}$ by using the induction principle.

Three phases make up the induction demonstration.

- Check whether the given statement is true for $n = 1$.
- Assume that given statement $P(n)$ is also true for $n = k$, where k is any positive integer.
- Show that for each positive integer k, the result is valid for $P(k+1)$.

Example 1.16. *Show that for all $n \in \mathbb{N} \setminus \{0\} : 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.*

- *Initialization : For* $n = 1$*, we have* $1 = 1$*. So, the property is true at rank* 1*.*

- *Inheritance: Assume the property* $P(n)$ *is true at rank* n*. Let's prove it for rank* $(n+1)$ *i.e.*

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

We have

$$\begin{aligned} P(n+1) =& 1+2+\ldots+n+(n+1) \\ =& P(n)+(n+1) \\ =& \frac{n(n+1)}{2}+(n+1) \\ =& \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Thus, $P(n)$ *is true for all* $n \in \mathbb{N}\setminus\{0\}$*.*

1.5 First Chapter's exercises

Exercise 1.1. *Which of the following statements are true, which are false, and why?*

- $(1<4)$ *and* $(2$ *divides* $4)$,
- $(3<8)$ *and* $(5$ *is a multiple of* $3)$,
- $(3<3)$ *or* $(5>2)$,
- $(\overline{2=4})$ *and* $(15$ *is a multiple of* $3)$,
- $(3\times 2=8)\Rightarrow(2+5=9)$,
- $(3\times 2=6)\Rightarrow(2+5=9)$.

Exercise 1.2. *Fill in the dotted lines with the correct logical connective:* $\Leftrightarrow,\Leftarrow,\Rightarrow$.

- $x\in\mathbb{R}:x^2=9\ldots x=3$.
- $x\in\mathbb{R}:x<2\ldots x<0$.
- $x\in\mathbb{R}:x>2\ldots x>0$.
- $x\in\mathbb{C}:x=\bar{x}\ldots x\in\mathbb{R}$.

Exercise 1.3. *Complete, where possible, with* $\forall,\exists$ *or* $\nexists$ *so that the following statements are true.*

- $\ldots x\in\mathbb{R}:(2-x)^2=x^2-4x+4$.
- $\ldots x\in\mathbb{R}:x^2-2x+3=0$.
- $\ldots x\in\mathbb{N}:x^2>8$.
- $\ldots x\in\mathbb{N}:x^2<6$.
- $\ldots x\in\mathbb{N}:x^2\geq 0$.

Exercise 1.4. *Let* $\mathscr{R}$ *and* $\mathscr{S}$ *be two propositions. Give their negations.*

- $\overline{\mathscr{R} \wedge \mathscr{S}}$.
- $\overline{\mathscr{R}} \vee \mathscr{S}$.
- $\mathscr{R} \Rightarrow \mathscr{S}$.

Exercise 1.5. *Give the negation and contraposition of the following propositions:*

- $\exists \varepsilon > 0, \forall N \in \mathbb{N}, \exists n \in \mathbb{N}, \exists p \in \mathbb{N}, n > N$ *and* $p \geq 0 \Rightarrow |u_{n+p} - u_n| < \varepsilon$.
- $\forall \varepsilon > 0, \exists \eta > 0, \forall x \in \mathbb{R} : |x - x_0| < \eta \Rightarrow |f(x) - f(x_0)| < \varepsilon$.

Exercise 1.6. *Using the truth table, show that*

- $(P \Rightarrow \mathscr{Q}) \Leftrightarrow (\overline{P} \vee \mathscr{Q})$.
- $(P \vee \mathscr{Q}) \Rightarrow \mathscr{R} \Leftrightarrow (P \Rightarrow \mathscr{R}) \wedge (\mathscr{Q} \Rightarrow \mathscr{R})$.

Exercise 1.7. *Are these statements true or false? Give their negations.*

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

Exercise 1.8. *Let* $(u_n)_{n \in \mathbb{N}}$ *be a sequence of numbers. What do the following statements mean in words.*

- $\forall n \in \mathbb{N}, \exists l \in \mathbb{C} : u_n = l$.
- $\exists l \in \mathbb{R}, \forall n \in \mathbb{N} : u_n = l$.

- $\forall l \in \mathbb{R}, \exists n \in \mathbb{N} : u_n = l$.

Exercise 1.9. *Consider the real functions f and g with real variables. Translate the following expressions into quantifiers:*

- *The function f never vanishes.*
- *The function f only intersects the (ox) axis once.*
- *The function g is odd.*
- *The function g is bounded below.*
- *The function f is greater than the function g.*

Exercise 1.10. *Show that*

- $n \in \mathbb{N} : n^2$ *is odd* $\Rightarrow n$ *is odd.*
- $n \in \mathbb{N} : n^2$ *is even* $\Rightarrow n$ *is even.*
- *Let a,b be two positive real numbers. If $\frac{a}{1+b} = \frac{b}{1+a}$ then $a = b$.*
- *Let a,b be two positive real numbers. If $a \leq b$ then $a \leq \frac{a+b}{2} \leq b$.*
- *Let a,b be two positive real numbers. If $a \leq b$ then $a \leq \sqrt{ab} \leq b$.*
- *Let a,b be two positive real numbers. If $a \leq b$ then $a \leq \frac{2ab}{a+b} \leq b$.*

Exercise 1.11. *Prove that*

- *Let a,b be two real numbers. If $a^2 + b^2 = 1$, then $|a+b| \leq 2$.*
- *For two real numbers a,b, we have $\min\{a,b\} = \frac{a+b-|a-b|}{2}$.*
- *For two real numbers a,b, we have $\max\{a,b\} = \frac{a+b+|a-b|}{2}$.*
- *For all $n \in \mathbb{N} : 2^n \geq n^2$.*
- *The equation: $x^4 + 2x^3 - 5x - 2 = 0$, has no integer solution.*

Exercise 1.12. *Show by induction that*

- $\forall n \in \mathbb{N} : n \geq 5 : 2^n \geq n^2$.
- $\forall n \in \mathbb{N}, 3^{2n+1} + 2^{n+2}$ *divides* 7.
- $\forall n \in \mathbb{N}, \sum_{p=0}^{p=n} (2p)^2 = \frac{2}{3} n (n+1) (2n+1)$.
- $\forall n \in \mathbb{N} \setminus \{0\}, 2 \times 6 \times \ldots (4n-2) = (n+1) (n+2) \ldots (2n)$.
- $\forall n \in \mathbb{N} \setminus \{0\}, \sum_{p=1}^{p=n} (2p-1)^2 = \frac{1}{3} n \left(4n^2 - 1\right)$.
- $\forall n \in \mathbb{N} \setminus \{0\}, 3 \times 5^{2n-1} + 2^{3n-2}$ *divides* 17.

1.6 Corrections of first chapter exercises

Correction of Exercise 1.1

- $(1 < 4)$ and (2 divides 4).

  The first proposition $(1 < 4)$ is true, the second proposition (2 divise 4) is true.

  So, the proposition is true.

  $P \wedge Q$ is true, since both propositions are true.

- $(3 < 8)$ and (5 is a multiple of 3).

  The first proposition $(3 < 8)$ is true, the second proposition (5 is a multiple of 3)

  is false. So, the proposition is false.

  $P \wedge Q$ is false, if at least one of the two propositions is false.

- $(3 < 3)$ or $(5 > 2)$.

  The first proposition $(3 < 3)$ is false, the second proposition $(5 > 2)$ is true.

  So, the proposition is true.

  $P \vee Q$ is true, if at least one of the two propositions is true.

- $(\overline{2 = 4}\ )$ and (15 is a multiple of 3).

  The first proposition $(\ \overline{2 = 4}) \Leftrightarrow (2 \neq 4)$ is true, the second proposition

  (15 is a multiple of 3) is true. So, the proposition is true.

- $(3 \times 2 = 8) \Rightarrow (2 + 5 = 9)$.

  The first proposition $(3 \times 2 = 8)$ is false, the second proposition $(2 + 5 = 9)$

  is false. So, the proposition is true.

  $P \Rightarrow Q$ is false, only if the first proposition is true and the second is false.

- $(3 \times 2 = 6) \Rightarrow (2 + 5 = 9)$, is false,

  since $(3 \times 2 = 6)$ is true and $(2 + 5 = 9)$ is false.

Correction of Exercise 1.2

- $$x \in \mathbb{R} : x^2 = 9 \Leftarrow x = 3.$$
- $$x \in \mathbb{C} : x = \bar{x} \Leftrightarrow x \in \mathbb{R}.$$
- $$x \in \mathbb{R} : x < 2 \Leftarrow x < 0.$$
- $$x \in \mathbb{R} : x > 2 \Rightarrow x > 0.$$

Correction of Exercise 1.3

- $$\forall x \in \mathbb{R} : (2-x)^2 = x^2 - 4x + 4.$$
- $$\nexists x \in \mathbb{R} : x^2 - 2x + 3 = 0.$$
- $$\exists x \in \mathbb{N} : x^2 > 8.$$
- $$\exists x \in \mathbb{N} : x^2 < 6.$$
- $$\forall x \in \mathbb{N} : x^2 \geq 0.$$

Correction of Exercise 1.4

- The negation of $\overline{\mathscr{R} \wedge \mathscr{S}}$ is
$$\overline{\overline{\mathscr{R} \wedge \mathscr{S}}} = \mathscr{R} \wedge \mathscr{S}.$$

- The negation of $\overline{\mathscr{R}} \wedge \mathscr{S}$ is

$$\overline{\overline{\mathscr{R}} \wedge \mathscr{S}} = \mathscr{R} \vee \overline{\mathscr{S}}.$$

- The negation of $\mathscr{R} \Rightarrow \mathscr{S}$ is

$$\overline{\mathscr{R} \Rightarrow \mathscr{S}} = \overline{\overline{\mathscr{R}} \vee \mathscr{S}} = \mathscr{R} \wedge \overline{\mathscr{S}}.$$

Correction of Exercise 1.5

- The negation is

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, \forall p \in \mathbb{N}, n > N \text{ and } p \geq 0 \text{ and } |u_{n+p} - u_n| \geq \varepsilon.$$

  The contrapositive is

$$\exists \varepsilon > 0, \forall N \in \mathbb{N}, \exists n \in \mathbb{N}, \exists p \in \mathbb{N}, |u_{n+p} - u_n| \geq \varepsilon \Rightarrow n < N \text{ and } p \leq 0.$$

- The negation is

$$\exists \varepsilon > 0, \forall \eta > 0, \exists x \in \mathbb{R} : |x - x_0| < \eta \text{ and } |f(x) - f(x_0)| \geq \varepsilon.$$

  The contrapositive is

$$\forall \varepsilon > 0, \exists \eta > 0, \forall x \in \mathbb{R} : |f(x) - f(x_0)| > \varepsilon \Rightarrow |x - x_0| > \eta.$$

Correction of Exercise 1.6 $(P \Rightarrow \mathscr{Q}) \Leftrightarrow (\overline{P} \vee \mathscr{Q})$.

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

$$\underbrace{(P \vee \mathscr{Q}) \Rightarrow \mathscr{R}}_{(1)} \Leftrightarrow \underbrace{(P \Rightarrow \mathscr{R}) \wedge (\mathscr{Q} \Rightarrow \mathscr{R})}_{(2)}$$

P	Q	R	$P \vee \mathscr{Q}$	(1)	$P \Rightarrow \mathscr{R}$	$\mathscr{Q} \Rightarrow \mathscr{R}$	(2)	(1) $\Leftrightarrow$ (2)
1	1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	0	1
1	0	1	1	1	1	1	1	1
1	0	0	1	0	0	1	0	1
0	1	1	1	1	1	1	1	1
0	1	0	1	0	1	0	0	1
0	0	1	0	1	1	1	1	1
0	0	0	0	1	1	1	1	1

Correction of Exercise 1.7

- $\forall x \in \mathbb{R} : x^2 > 0$ is false, just take $x = 0$.

  Its negation is:

  $$\exists x \in \mathbb{R} : x^2 \leq 0.$$

- $\exists x \in \mathbb{R} : x^2 > 0$ is true, for $x = 1$, hence the existence of at least one x.

  Its negation is:

  $$\forall x \in \mathbb{R} : x^2 \leq 0.$$

- $\exists x \in \mathbb{R}, \forall y \in \mathbb{R} : x + y > 0$ is false, just take $y = -x$.

  Its negation is:

  $$\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : x + y \leq 0.$$

- $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : x + y > 0$ is true, just take $y = x - 1$.

  Its negation is:

  $$\exists x \in \mathbb{R}, \forall y \in \mathbb{R} : x + y \leq 0.$$

- $\forall x \in \mathbb{R}, \forall y \in \mathbb{R} : x + y > 0$ is false, just take $y = x = 0$.

Its negation is:

$$\exists x \in \mathbb{R}, \exists y \in \mathbb{R} : x + y \leq 0.$$

- $\exists x \in \mathbb{R}, \exists y \in \mathbb{R} : x + y > 0$ is true, just take $y = x = 1$.

  Its negation is:

  $$\forall x \in \mathbb{R}, \forall y \in \mathbb{R} : x + y \leq 0.$$

- $\exists x \in \mathbb{C} : x^2 + 2x + 5 = 0$ is true, because any polynomial of degree n in $\mathbb{C}$ has n roots including their multiplicities.

  Its negation is:

  $$\forall x \in \mathbb{C} : x^2 + 2x + 5 \neq 0.$$

Correction of Exercise 1.8

- The sequence $(u_n)_{n\in\mathbb{N}}$ is a complex sequence.
- The sequence $(u_n)_{n\in\mathbb{N}}$ is a constant sequence.
- The sequence $(u_n)_{n\in\mathbb{N}}$ takes all integer values.

Correction of Exercise 1.9

- The function f never vanishes $\Leftrightarrow$

  $$\forall x \in \mathbb{R} : f(x) \neq 0.$$

- The function f only intersects the (ox) axis once $\Leftrightarrow$

  $$\exists! x \in \mathbb{R} : f(x) = 0.$$

- The function g is odd $\Leftrightarrow$

  $$\forall x \in \mathbb{R}, -x \in \mathbb{R} : g(-x) = -g(x).$$

- The function g is bounded below $\Leftrightarrow$

$$\exists m \in \mathbb{R}, \forall x \in \mathbb{R} : g(x) \geq m.$$

- The function f is greater than the function $g \Leftrightarrow$

$$\forall x \in \mathbb{R} : f(x) \geq g(x).$$

Correction of Exercise 1.10 1 - We use contrapositive reasoning.

n^2 is odd $\Rightarrow$ n is odd $\Leftrightarrow$ n is even $\Rightarrow$ n^2 is even

Since n is even $\Rightarrow \exists k \in \mathbb{N} : n = 2k$. So,

$$n^2 = (2k)^2 = 4k^2 = 2\left(\underbrace{2k}_{p}\right) = 2p.$$

Thus, n^2 is even.

2 - We use a contrapositive reasoning.

n^2 is even $\Rightarrow$ n is even $\Leftrightarrow$ n is odd $\Rightarrow$ n^2 is odd

Since n is odd $\Rightarrow \exists k \in \mathbb{N} : n = 2k+1$. So,

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2\left(\underbrace{2k^2 + 2k}_{p}\right) + 1 = 2p + 1.$$

Thus, n^2 is odd.

3 - We use a contradiction reasoning.

We have $a, b > 0$, $\frac{a}{1+b} = \frac{b}{1+a}$ and suppose that $a \neq b$

$$\begin{aligned}
\frac{a}{1+b} &= \frac{b}{1+a} \\
&\Leftrightarrow a(1+a) = b(1+b) \\
&\Leftrightarrow a + a^2 - b - b^2 = 0 \\
&\Leftrightarrow (a-b) + (a-b)(a+b) = 0
\end{aligned}$$

$$\Leftrightarrow (a-b)(1+a+b)=0.$$

Since $a \neq b$, then $a-b \neq 0$. So $1+a+b=0 \Rightarrow a+b=-1$,

which is a contradiction with the fact that $a,b>0$.

So, our assumption is false. Thus $a=b$.

4- Since $a \leq b$, we have

$$a \leq b \Rightarrow a+a \leq a+b \Rightarrow 2a \leq a+b \Rightarrow a \leq \tfrac{a+b}{2}.$$

Hence, the first inequality is proven.

On the other hand, we have

$$a \leq b \Rightarrow a+b \leq b+b \Rightarrow a+b \leq 2b \Rightarrow \tfrac{a+b}{2} \leq b.$$

The second inequality is thus proven. Thus, the desired result is obtained.

5- Since $a \leq b$ and $a>0$, we have

$$a \times a \leq a \times b \Rightarrow a^2 \leq ab \Rightarrow \sqrt{a^2}=a \leq \sqrt{ab}. \tag{1.1}$$

Hence, the first inequality is proven.

On the other hand, we have $a \leq b$ and $b>0 \Rightarrow$

$$a \times b \leq b \times b \Rightarrow ab \leq b^2 \Rightarrow \sqrt{ab} \leq \sqrt{b^2}=b. \tag{1.2}$$

The second inequality is thus proven. The desired result follows from (1.1) and (1.2).

6- Since $a \leq b$ and $a>0$, we have

$$\begin{aligned} a \times a \leq & a \times b \Rightarrow a^2 \leq ab \\ & \Rightarrow a^2+ab \leq ab+ab=2ab \\ & \Rightarrow a(a+b) \leq 2ab \Rightarrow a \leq \tfrac{2ab}{a+b}, \end{aligned} \tag{1.3}$$

Hence, the first inequality is proven.

On the other hand, we have $a \leq b$ and $b > 0 \Rightarrow$

$$\begin{aligned} a \times b \leq & b \times b \Rightarrow ab \leq b^2 \\ \Rightarrow & 2ab \leq b^2 + ab = b(a+b) \\ \Rightarrow & \tfrac{2ab}{a+b} \leq b. \end{aligned} \tag{1.4}$$

The second inequality is thus proven. The desired result follows from (1.3) and (1.4).

Correction of Exercise 1.11 1- We will apply direct reasoning.

According to the hypothesis, we have: $a^2 + b^2 = 1$. So, we can write

$$a^2 = 1 - b^2,$$

which implies that

$$1 - b^2 \geq 0.$$

Hence,

$$b^2 \leq 1.$$

Thus, we conclude

$$|b| \leq 1 \Leftrightarrow -1 \leq b \leq 1. \tag{1.5}$$

Likewise,

$$b^2 = 1 - a^2,$$

which implies that

$$1 - a^2 \geq 0.$$

Hence,

$$a^2 \leq 1.$$

Thus, we conclude

$$|a| \leq 1 \Leftrightarrow -1 \leq a \leq 1. \tag{1.6}$$

Summing (1.5) and (1.6) gives

$$-2 \leq a+b \leq 2 \Rightarrow |a+b| \leq 2,$$

which is the desired result.

2 - Two cases arise: either $a < b$ or $b < a$.

If $a < b$, then $\min\{a,b\} = a$, it yields

$$|a-b| = b-a.$$

So,

$$\frac{a+b-|a-b|}{2} = \frac{a+b-(b-a)}{2} = \frac{2a}{2} = a = \min\{a,b\}.$$

If $b < a$, then $\min\{a,b\} = b$, which implies

$$|a-b| = a-b.$$

and

$$\frac{a+b-|a-b|}{2} = \frac{a+b-(a-b)}{2} = \frac{2b}{2} = b = \min\{a,b\}.$$

Thus, $\min\{a,b\} = \frac{a+b-|a-b|}{2}$ holds for all real values a,b.

3 - We distinguish two cases: either $a \leq b$ or $b \leq a$

If $a \leq b$, then $\max\{a,b\} = b$, it yields

$$|a-b| = b-a.$$

So,

$$\frac{a+b+|a-b|}{2} = \frac{a+b+b-a}{2} = \frac{2b}{2} = b = \max\{a,b\}. \tag{1.7}$$

In the case where $b \leq a$, we have $\max\{a,b\} = a$. Hence

$$|a-b| = a-b,$$

and

$$\frac{a+b+|a-b|}{2} = \frac{a+b+a-b}{2} = \frac{2a}{2} = a = \max\{a,b\}. \tag{1.8}$$

The desired result follows from (1.7) and (1.8).

4 - We will apply a counterexample argument.

For $n=3$, we have $2^3 = 8 \geq 3^2 = 9$, which is false.

Therefore, $2^n \geq n^2$ is not true for all natural numbers.

5 - We use the contradiction reasoning.

We assume that the equation $x^4+2x^3-5x-2=0$ has an integer solution.

So, $x^4+2x^3-5x=2 \Rightarrow x\left(x^3+2x^2-5\right)=2 \Rightarrow x \backslash 2 \Rightarrow x \in \{-2,-1,1,2\}$.

If $x=-2$, it follows that $(-2)^4+2(-2)^3-5(-2)-2=16-16+10-2=8\neq 0$

$\Rightarrow -2$ is not a solution.

If $x=-1$, it follows that $(-1)^4+2(-1)^3-5(-1)-2=1-2+5-2=2\neq 0$

$\Rightarrow -1$ is not a solution.

If $x=1$, it follows that $(1)^4+2(1)^3-5(1)-2=1+2-5-2=-4\neq 0$

$\Rightarrow 1$ is not a solution.

If $x=2$, it follows that $(2)^4+2(2)^3-5(2)-2=16+16-10-2=20\neq 0$

$\Rightarrow 2$ is not a solution.

Thus, the equation $x^4+2x^3-5x-2=0$ has no integer solutions.

Correction of Exercise 1.12 1- Initialization: For $n=5$, we have $2^5 = 32 \geq 5^2 = 25$,

the property is true at rank 0.

Inheritance: Assume the property is true at rank n. We therefore have $2^n \geq n^2$.

We therefore have $2^n \geq n^2$ jusqu'au rang n. Let us prove it for rank $(n+1)$, i.e.

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

According to the induction hypothesis, we have

$$2^n \geq n^2 \Rightarrow 2^{n+1} \geq 2n^2. \tag{1.9}$$

On the other hand, we have

$$
\begin{aligned}
&\begin{cases} n \geq 5 \geq 1-\sqrt{2} \Rightarrow n-\left(1-\sqrt{2}\right) \geq 0 \\ n \geq 5 \geq 1+\sqrt{2} \Rightarrow n-\left(1+\sqrt{2}\right) \geq 0 \end{cases} \\
&\Rightarrow \left(n-\left(1-\sqrt{2}\right)\right)\left(n-\left(1+\sqrt{2}\right)\right) \geq 0 \\
&\Rightarrow n^2-2n-1 \geq 0 \\
&\Rightarrow n^2 \geq 2n+1 \\
&\Rightarrow 2n^2 \geq n^2+2n+1=(n+1)^2 . \qquad (1.10)
\end{aligned}
$$

Thus, from (1.9) and (1.10), we have $2^{n+1} \geq (n+1)^2$. So, $\forall n \geq 5 : 2^n \geq n^2$ is true.

2- $\forall n \in \mathbb{N} : 3^{2n+1}+2^{n+2}$ divides $7 \Leftrightarrow \mathscr{P}(n) : \exists k \in \mathbb{N} : 3^{2n+1}+2^{n+2}=7k$.

Initialization: For $n=0$, we have $\mathscr{P}(0) : 3^{2\times 0+1}+2^{0+2}=3+4=7=7\times 1$ " $k=1$", the property is true at rank 0.

Inheritance: Assume the property $\mathscr{P}(n)$ is true at rank n.

Let us prove it for rank $(n+1)$ i.e.

$$\mathscr{P}(n+1) : \exists k' \in \mathbb{N} : 3^{2(n+1)+1}+2^{(n+1)+2}=7k'.$$

We have

$$
\begin{aligned}
&3^{2(n+1)+1}+2^{(n+1)+2} \\
=&3^{2n+2+1}+2^{n+1+2}=3^2\times 3^{2n+1}+2^1\times 2^{n+2} \\
=&9\times 3^{2n+1}+2^1\times 2^{n+2}=(7+2)\times 3^{2n+1}+2\times 2^{n+2} \\
=&7\times 3^{2n+1}+2\times 3^{2n+1}+2\times 2^{n+2} \\
=&7\times 3^{2n+1}+2\times \left(\underbrace{3^{2n+1}+2^{n+2}}_{\mathscr{P}(n)=7k}\right)=7\times 3^{2n+1}+2\times 7k.
\end{aligned}
$$

So,

$$3^{2(n+1)+1}+2^{(n+1)+2}=7\times\left(\underbrace{3^{2n+1}+2\times k}_{=k'\in\mathbb{N}}\right)=7k'.$$

Thus, $\mathscr{P}(n)$ is true for all $n \in \mathbb{N}$.

3- Initialization: For $n=0$, we have $\mathscr{P}(n): \underbrace{\sum_{p=0}^{p=0}(2p)^2}_{(2\times 0)^2=0} = \frac{2}{3}0(0+1)(2\times 0+1)$

$\Rightarrow 0=0$, the property is true at rank 0.

Inheritance: Assume the property $\mathscr{P}(n)$ is true at rank n.

Let's prove it for rank $(n+1)$ i.e.

$$\sum_{p=0}^{p=n+1}(2p)^2 \stackrel{?}{=} \frac{2}{3}(n+1)(n+2)(2n+3).$$

According to the induction hypothesis, we have:

$$\sum_{p=0}^{p=n}(2p)^2 = \frac{2}{3}n(n+1)(2n+1).$$

So,

$$\begin{aligned}
\sum_{p=0}^{p=n}(2p)^2+(2(n+1))^2 =& \frac{2}{3}n(n+1)(2n+1)+(2(n+1))^2\\
=& \sum_{p=0}^{p=n+1}(2p)^2 = \frac{2}{3}n(n+1)(2n+1)+4(n+1)^2\\
=& \frac{2}{3}n(n+1)(2n+1)+\frac{2}{3}\times 4\times\frac{3}{2}(n+1)^2\\
=& \frac{2}{3}(n+1)\left(n(2n+1)+4\times\frac{3}{2}(n+1)\right)\\
=& \frac{2}{3}(n+1)\left(2n^2+7n+6\right).
\end{aligned}$$

It is clear that $2n^2+7n+6=0$ for $n_1=\frac{-7-1}{4}=-2$ or $n_2=\frac{-7+1}{4}=-\frac{3}{2}$.

So,

$$\begin{aligned}
2n^2+7n+6 =& 2(n-n_1)(n-n_2) = 2(n+2)\left(n+\frac{3}{2}\right)\\
=& (n+2)(2n+3).
\end{aligned}$$

Thus, $\sum_{p=0}^{p=n+1}(2p)^2 = \frac{2}{3}(n+1)\left(2n^2+7n+6\right) = \frac{2}{3}(n+1)(n+2)(2n+3)$,
is true for all $n\in\mathbb{N}$.

4- Initialization: For $n=1$, we have $2=2$, the property is true at rank 0.

Inheritance: Assume the property $\mathscr{P}(n)$ is true at rank n.

Let's prove it for rank $(n+1)$ i.e.

$$\begin{aligned}2\times 6\times \ldots (4n-2)(4n+2) &= ((n+1)+1)((n+1)+2)\ldots (2(n+1))\\ &= (n+2)(n+3)\ldots (2n+2).\end{aligned}$$

We have

$$\begin{aligned}2\times 6\times \ldots (4n-2)(4n+2) =& \underbrace{2\times 6\times \ldots (4n-2)}_{(n+1)(n+2)\ldots (2n)}(4n+2)\\ =& (n+1)(n+2)\ldots (2n)(4n+2)\\ =& (n+1)(n+2)\ldots (2n)\,2\,(2n+1)\\ =& 2(n+1)(n+2)\ldots (2n)(2n+1)\\ =& (2n+2)(n+2)\ldots (2n)(2n+1)\\ =& (n+2)\ldots (2n)(2n+1)(2n+2).\end{aligned}$$

Thus, $2\times 6\times \ldots (4n-2)=(n+1)(n+2)\ldots (2n)$, is true for all $n\in \mathbb{N}\setminus\{0\}$.

5- Initialization: For $n=1$, we have $\mathscr{P}(n)$: $\underbrace{\sum_{p=1}^{p=1}(2p-1)^2}_{(2\times 1-1)^2=1} = \frac{1}{3}1\left(4\times 1^2-1\right)=\frac{1}{3}3$

$\Rightarrow 1=1$, the property is true at rank 0.

Inheritance: Assume the property $\mathscr{P}(n)$ is true at rank n.

Let us prove it for rank $(n+1)$ i.e.

$$\begin{aligned}\sum_{p=1}^{p=n+1}(2p-1)^2 &\overset{?}{=} \frac{1}{3}(n+1)\left(4(n+1)^2-1\right)\\ = & \underbrace{\frac{1}{3}(n+1)\left(4n^2+8n+3\right)}_{\frac{1}{3}(4n^3+8n^2+3n+4n^2+8n+3)=\frac{1}{3}(4n^3+12n^2+11n+3)}.\end{aligned}$$

According to the induction hypothesis, we have:

$$\sum_{p=1}^{p=n}(2p-1)^2=\frac{1}{3}n\left(4n^2-1\right).$$

So,

$$\begin{aligned}
&\sum_{p=1}^{p=n}(2p-1)^2+\left(2(n+1)^2-1\right)^2\\
=&\frac{1}{3}(n+1)\left(4n^2-1\right)+(2(n+1)-1)^2\\
=&\sum_{p=1}^{p=n+1}(2p-1)^2=\frac{1}{3}n\left(4n^2-1\right)+(2n+1)^2\\
=&\frac{1}{3}n\left(4n^2-1\right)+(2n+1)^2\\
=&\frac{1}{3}\left(4n^3-n\right)+\frac{1}{3}\times 3\left(4n^2+4n+1\right)\\
=&\frac{1}{3}\left(4n^3-n\right)+\frac{1}{3}\left(12n^2+12n+3\right)\\
=&\frac{1}{3}\left(4n^3-n+12n^2+12n+3\right)\\
=&\frac{1}{3}\left(4n^3+12n^2+11n+3\right).
\end{aligned}$$

Thus, $\mathscr{P}(n)$ is true for all $n\in\mathbb{N}\setminus\{0\}$.

6- Initialization:

For $n=1$, we have $\mathscr{P}(n):3\times 5^{2-1}+2^{3-2}=3\times 5+2=17=17\times 1$ " $k=1$",

the property is true at rank 0.

Inheritance: Assume the property $\mathscr{P}(n)$ is true at rank n.

Let's prove it for rank $(n+1)$ i.e.

$$\mathscr{P}(n+1):\exists k'\in\mathbb{N}:3\times 5^{2(n+1)-1}+2^{3(n+1)-2}=17k'.$$

We have

$$\begin{aligned}
3\times 5^{2(n+1)-1}+2^{3(n+1)-2}=&3\times 5^{2n+2-1}+2^{3n+3-2}\\
=&3\times 5^2\times 5^{2n-1}+2^3\times 2^{3n-2}\\
=&25\left(3\times 5^{2n-1}\right)+8\times 2^{3n-2}
\end{aligned}$$

$$
\begin{aligned}
&= (17+8)\left(3\times 5^{2n-1}\right) + 8\times 2^{3n-2} \\
&= 17\times 3\times 5^{2n-1} + 8\times 3\times 5^{2n-1} + 8\times 2^{3n-2} \\
&= 17\times 3\times 5^{2n-1} + 8\times \left(\underbrace{3\times 5^{2n-1}+2^{3n-2}}_{\mathscr{P}(n)=17k}\right) \\
&= 17\times 3\times 5^{2n-1} + 8\times 17k \\
&= 17\times \left(\underbrace{3\times 5^{2n-1}+8k}_{=k'\in\mathbb{N}\setminus\{0\}}\right) = 17k'.
\end{aligned}
$$

Thus, $\mathscr{P}(n)$ is true for all $n \in \mathbb{N}\setminus\{0\}$.

Chapter 2

Sets, Relations and Applications

Definition 2.1. *A group of items (elements) with one or more characteristics is called a set.*

Example 2.1. *The set of natural numbers* $\mathbb{N}$.

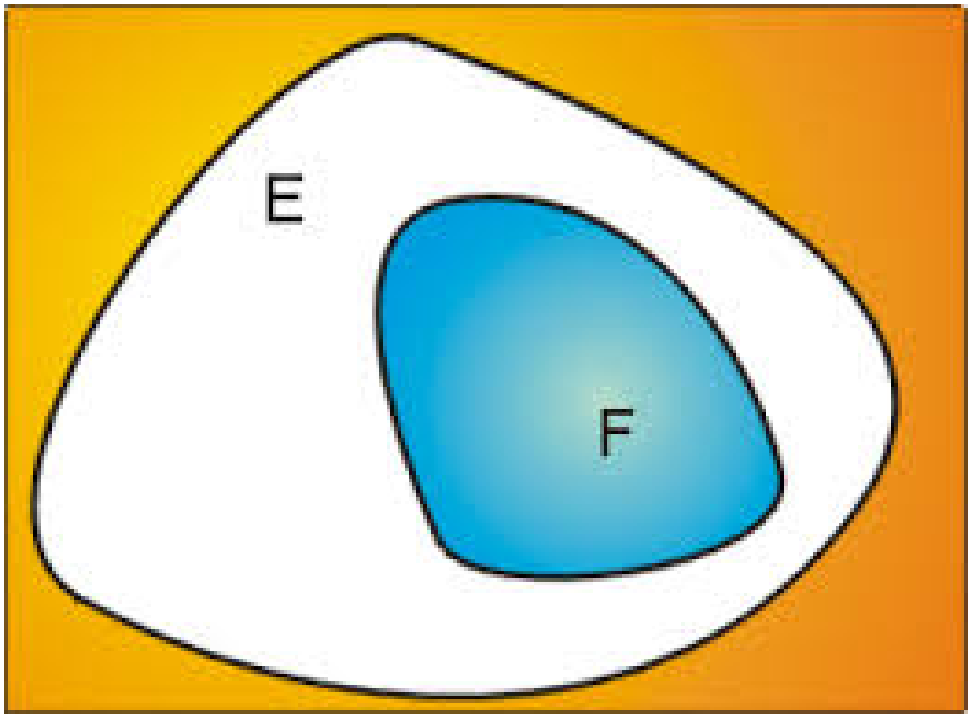
Remark 2.1. *An empty set, represented by the notation* $\phi = \{x : x \neq x\}$, *is a set that has no elements.*

Remark 2.2. *A singleton is a set that has just one element in it.*

Example 2.2. $A = \{1\}, B = \left\{y \in \mathbb{R} : y = \sqrt{-x^2}\right\}$, *are a segleton sets.*

Definition 2.2. *Let* F *and* E *be two subsets of* Ω. *When each element of* F *is also an element of* E, *we say that* F *is a subset of* E *or components of* E. *We frequently state that* F *is a part of* E, *which we express formally as* $F \subset E$.

$$F \subset E \Leftrightarrow \forall x \in E : x \in F \Rightarrow x \in E.$$



Example 2.3. *Consider the sets* $A = \{2,3\}$ *and* $B = \{1,2,3,4,5\}$. *Clearly* $A \subset B$.

Definition 2.3. *If two sets,* A *and* B*, have the same items, then they are considered equal.*

$$A = B \Leftrightarrow \forall x : x \in A \Leftrightarrow x \in B,$$

or

$$A = B \Leftrightarrow (A \subset B) \wedge (B \subset A).$$

Example 2.4. *Consider the sets* $A = [-1,5]$ *and* $B = \{x \in \mathbb{R} : |x-2| \leq 3\}$. *Clearly* $A = B$.

Remark 2.3. *The set of all parts of a set* E *constitutes a new set denoted* $\mathscr{P}(E)$.

Example 2.5. *Consider the set* $A = \{1,2,3\}$.

We have $\mathscr{P}(A) = \{\phi, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, A\}$.

2.1 Operations on sets

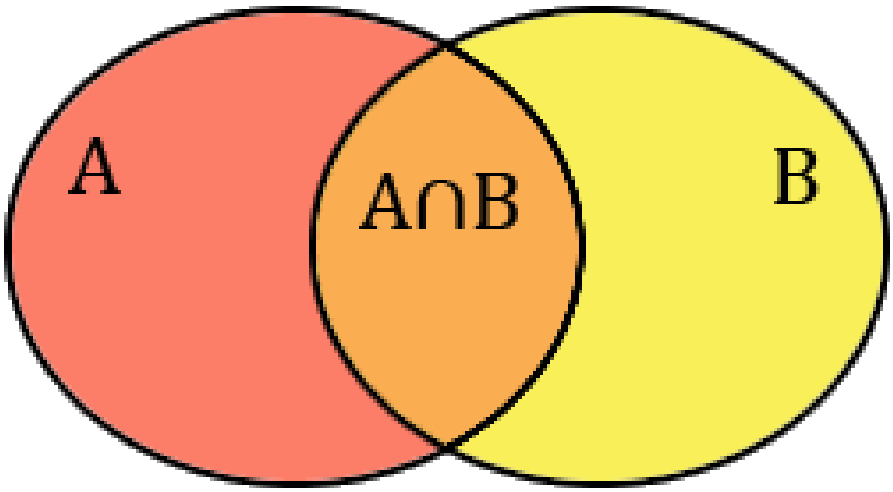
Intersection

Definition 2.4. *Let* E *be a set with two components,* A *and* B*. The set of items that belong to both* A *and* B *is the intersection of the sets* A *and* B*, and it is represented by the symbol* $A \cap B$*, as shown in the diagram in the figure below.*

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

or

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



Example 2.6. *Consider the sets* $A = \{1,2,3,5,9\}$ *and* $B = \{1,2,7,6,8\}$.

Clearly $A \cap B = \{1,2\}$.

Remark 2.4. *If two sets have an empty intersection, they are disjoint.*

i.e A *and* B *disjoint* $\Rightarrow A \cap B = \phi$.

Example 2.7. *Let* $A = \{1,2,3,5,9\}$ *and* $B = \{7,6,8\}$. *Clearly, we have* $A \cap B = \phi$.

Example 2.8. *Consider the sets* $A = \{x \in \mathbb{R} : |x-1| \leq 2\}$ *and* $B = \{x \in \mathbb{R} : |x+3| < 2\}$. *Clearly, we have* $A \cap B = \phi$.

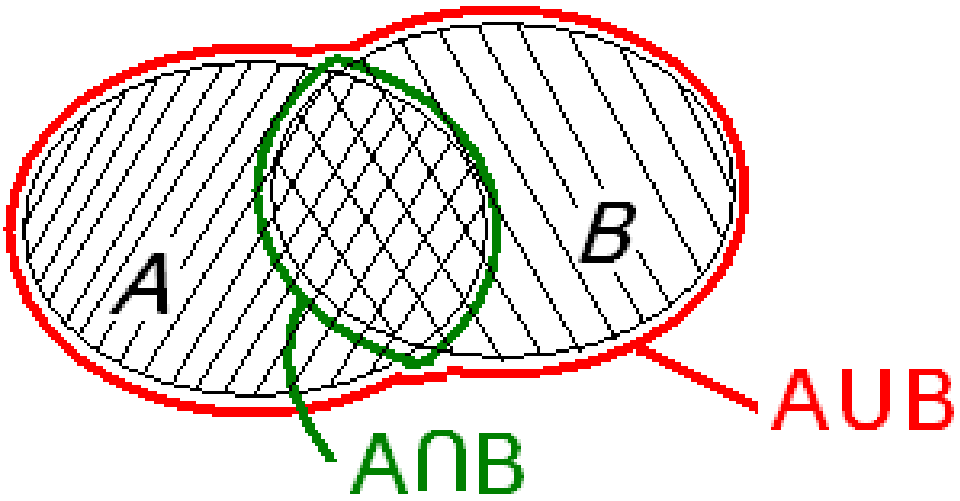
Union

Definition 2.5. *Let* E *be a set with two components,* A *and* B. *The union of the sets* A *and* B *is considered the set of items which belong to at least one of the two sets* A *or* B *and is denoted* $A \cup B$, *see the figure below.*

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

or

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



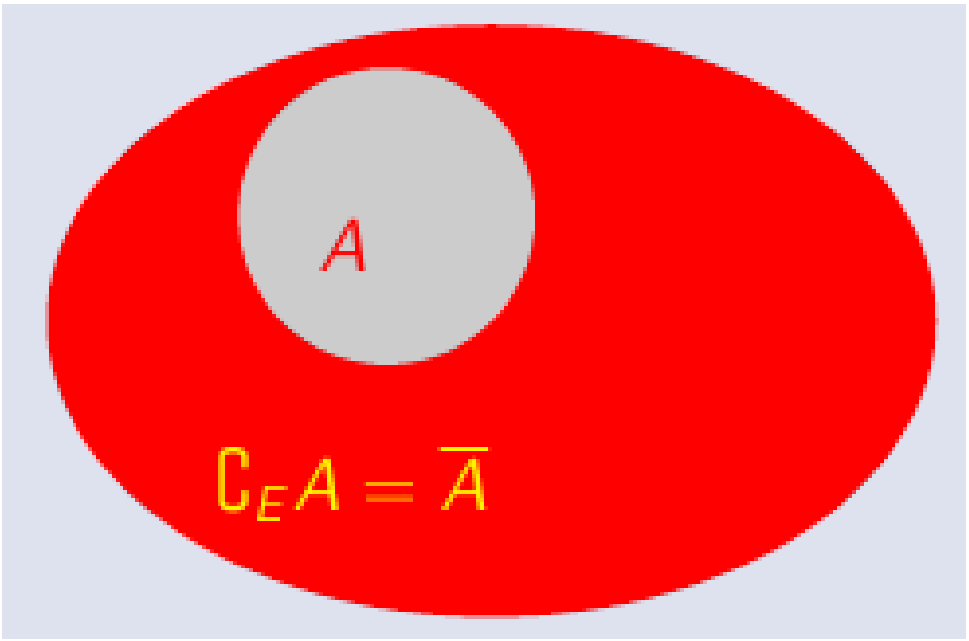
Example 2.9. *Consider the sets* $A = \{1,2,3,5,9\}$ *and* $B = \{1,2,7,6,8\}$. *We have* $A \cup B = \{1,2,3,5,6,7,8,9\}$.

Example 2.10. *Consider the sets* $A = \{x \in \mathbb{R} : |x-1| \leq 2\}$ *and* $B = \{x \in \mathbb{R} : |x+3| < 2\}$. *We have* $A \cup B =]-5,1]$.

Complementary

Definition 2.6. *Consider* A *to be a subset of* E. *The complement of* A *is the collection of items of* E *that are not part of* A. *It is represented by* $\overline{A}$ *or* $C_E A$.

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



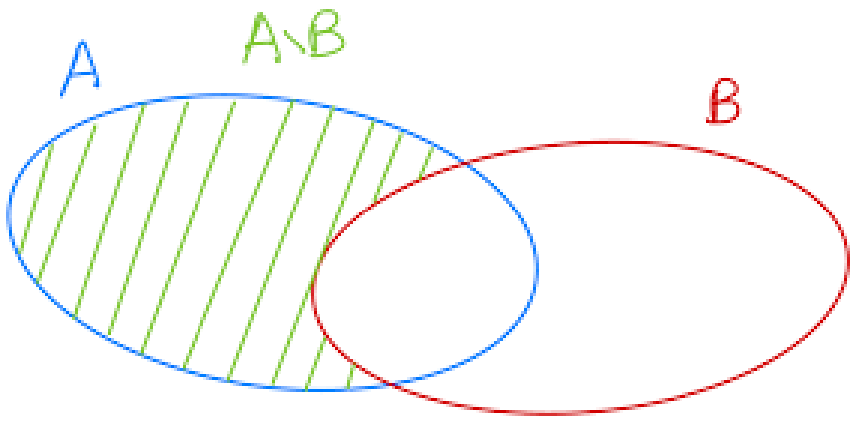
Example 2.11. *Consider the sets* $A = \{2,3\}$ *and* $B = \{1,2,3,4,5\}$.

Clearly, we have $C_B A = \{3,4,5\}$.

Difference

Definition 2.7. *Let* E *be a set with two components,* A *and* B. *We call the difference of* A *and* B *in this order the set of elements of* E *belonging to* A *but not to* B *and is denoted* $A\backslash B$.

$$A\backslash B = \{x \in E : (x \in A) \wedge (x \notin B)\}.$$



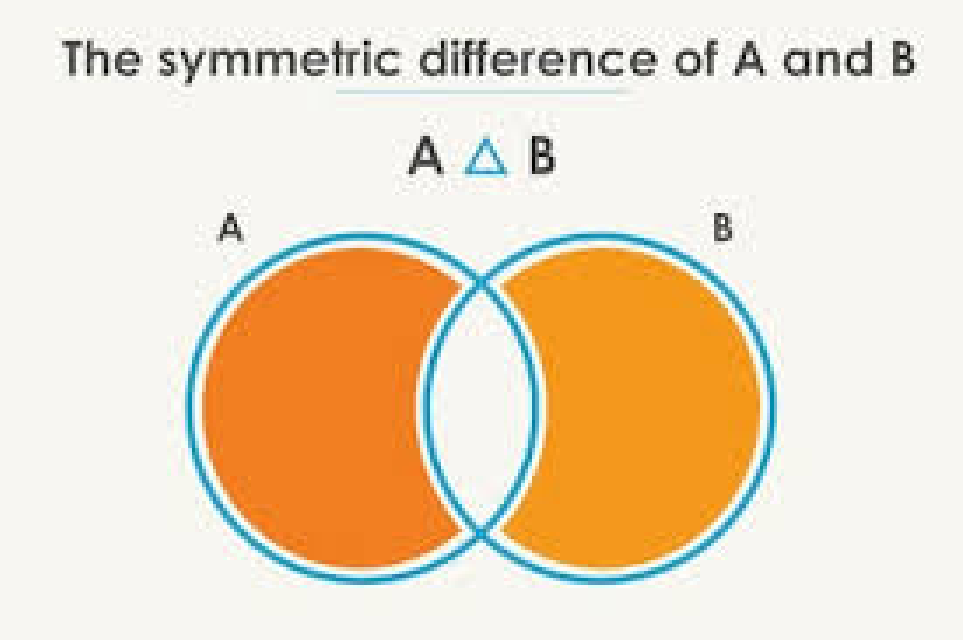
Example 2.12. *Consider the sets* $A = \{1,2,3,5,9\}$ *and* $B = \{1,2,7,6,8\}$.

Clearly, we have $A\backslash B = \{3,5,9\}$ *and* $B\backslash A = \{7,6,8\}$.

Symmetrical difference

Definition 2.8. *Let* E *be a set with two components,* A *and* B. *The set of components of* E *that belong to either* A *or* B *exclusively is known as the symmetric difference of* A *and* B, *and it is represented by* $A\Delta B$.

$$A\Delta B = \{x \in E : [(x \in A) \wedge (x \notin B)] \vee [(x \in B) \wedge (x \notin A)]\}.$$



Remark 2.5. *In addition, we may write* $A\Delta B = A\backslash B \cup B\backslash A = (A \cup B) \setminus (A \cap B)$.

Example 2.13. *Consider the sets* $A = \{1,2,3,5,9\}$ *and* $B = \{1,2,7,6,8\}$.

We have $A\Delta B = \{3,5,,6,7,8,9\}$.

Properties of operations on sets Let A, B and C be three subsets of a set E. The properties listed below are met.

- Commutativity

$$A \cap B = B \cap A \text{ and } A \cup B = B \cup A.$$

- Associativity

$$A\cap(B\cap C)=(A\cap B)\cap C \text{ and } A\cup(B\cup C)=(A\cup B)\cup C.$$

- Distributivity

$$A\cap(B\cup C)=(A\cap B)\cup(A\cap C) \text{ and } A\cup(B\cap C)=(A\cup B)\cap(A\cup C).$$

- De Morgan's laws

$$\overline{A\cap B}=\overline{A}\cup\overline{B} \text{ and } \overline{A\cup B}=\overline{A}\cap\overline{B}.$$

Partition Consider a set E and a family $\{A_i\}_{i=\overline{1,n}}$ of subsets of E.

Definition 2.9. *We say that the $\{A_i\}_{i=\overline{1,n}}$ form a partition of E, if all of the following criteria holds*

1/ $A_i\neq\phi$ for all $i\in\{1,2,\ldots,n\}$.

2/ $A_i\cap A_j=\phi$ for all $i,j\in\{1,2,\ldots,n\}$ with $i\neq j$.

3/ $\bigcup_{i=1}^{n}A_i=E$.

Example 2.14. *Consider the following sets $E=\{x\in\mathbb{R}:|x-2|\leq 2\}$, $A=\{x\in\mathbb{R}:|x-1|<1\}$, $B=\{x\in\mathbb{R}:|x-3|<1\}$ and $C=\{0,2,4\}$. It is clear that A,B and C form a partition of E, because they satisfy the 3 conditions listed above.*

Cartesian product

Definition 2.10. *The Cartesian product of the sets $\{A_i\}_{i=\overline{1,n}}$ is the set comprising the elements of the form $(a_1,a_2,\ldots,a_n)$ such that $a_1\in A_1$ and is denoted $A_1\times A_2\times\ldots\times A_n$ or $\prod_{i=1}^{n}A_i$.*

$$A_1\times A_2\times\ldots\times A_n=\prod_{i=1}^{n}A_i=\left\{(a_1,a_2,\ldots,a_n):a_i\in A_i \text{ for all } i=\overline{1,n}\right\}.$$

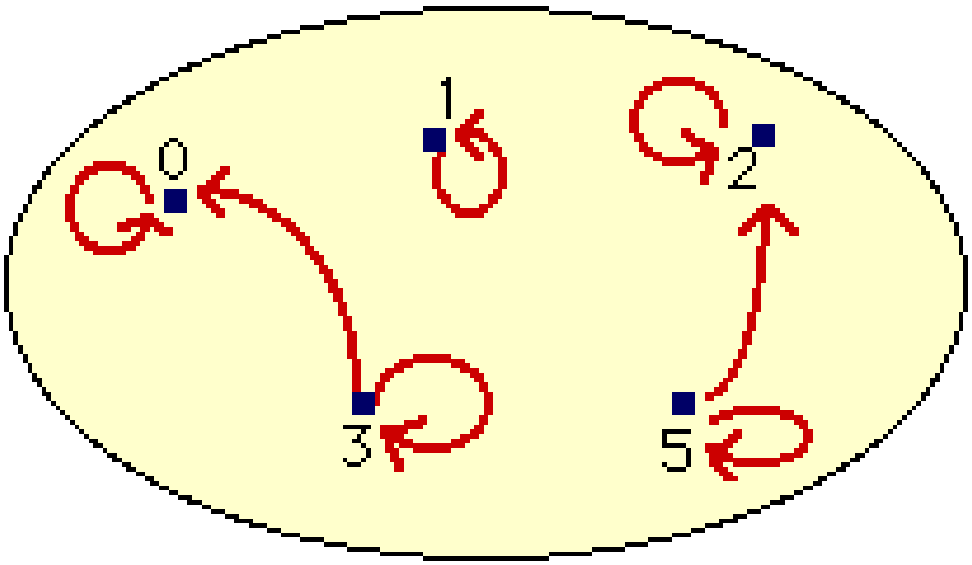
Example 2.15. *Consider the sets $A=\{1,2,3\}$ and $B=\{\alpha,\beta\}$, we have*

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

2.2 Binary relation

Definition 2.11. *A collection of couples of the Cartesian product $E \times F$, whose components are connected by a commonly recognized proposition, constitutes a relation from a set E to a set F and is denoted $\mathscr{R}$.*

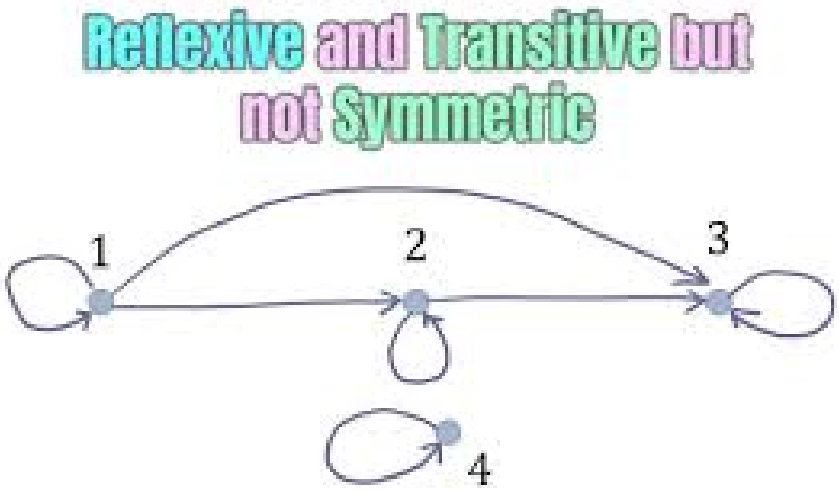
Remark 2.6. *The relation $\mathscr{R}$ is referred to as a binary relation in E when $F = E$.*



Definition 2.12. *$\Gamma = \{(x,y) \in E \times E : x\mathscr{R}y\}$ is a common notation for the graph of a binary relation on the set E, which shows that the pairings $(x,y) \in E \times E$ are in relation, i.e. $x\mathscr{R}y$.*

Properties of binary relations in a set Consider a set E and $\mathscr{R}$ a relation defined in E.

Definition 2.13. *The relation $\mathscr{R}$ is considered reflexive, if $\forall x \in E : x\mathscr{R}x$ holds.*



Remark 2.7. *For a relation to be reflexive, all couples of the type* (x,x) *must belong to the graph* Γ *for every* $x \in \Omega$*, if the relation* $\mathscr{R}$ *on a set* Ω *is represented by its graph* Γ*.*

Example 2.16. *Let us consider the binary relation* $\mathscr{R}$ *on set* $\mathbb{R}^2$ *as follows*

$\forall (x,y),(x',y') \in \mathbb{R}^2 : (x,y)\mathscr{R}(x',y') \Leftrightarrow x = x'.$

Prove that the relation $\mathscr{R}$ *is reflexive.*

Clearly $\forall (x,y) \in \mathbb{R}^2 : (x,y)\mathscr{R}(x,y)$ *because* $x = x$*. Consequently,* $\mathscr{R}$ *is a reflexive relation.*

Example 2.17. *Consider the set* $\Omega = \{1,2,3,4\}$ *and the graphs of the relations* $\mathscr{R}_1$ *and* $\mathscr{R}_2$ *are*

$\Gamma_1 = \{(1,1),(1,3),(2,2),(2.3),(3,4),(4,4)\}$

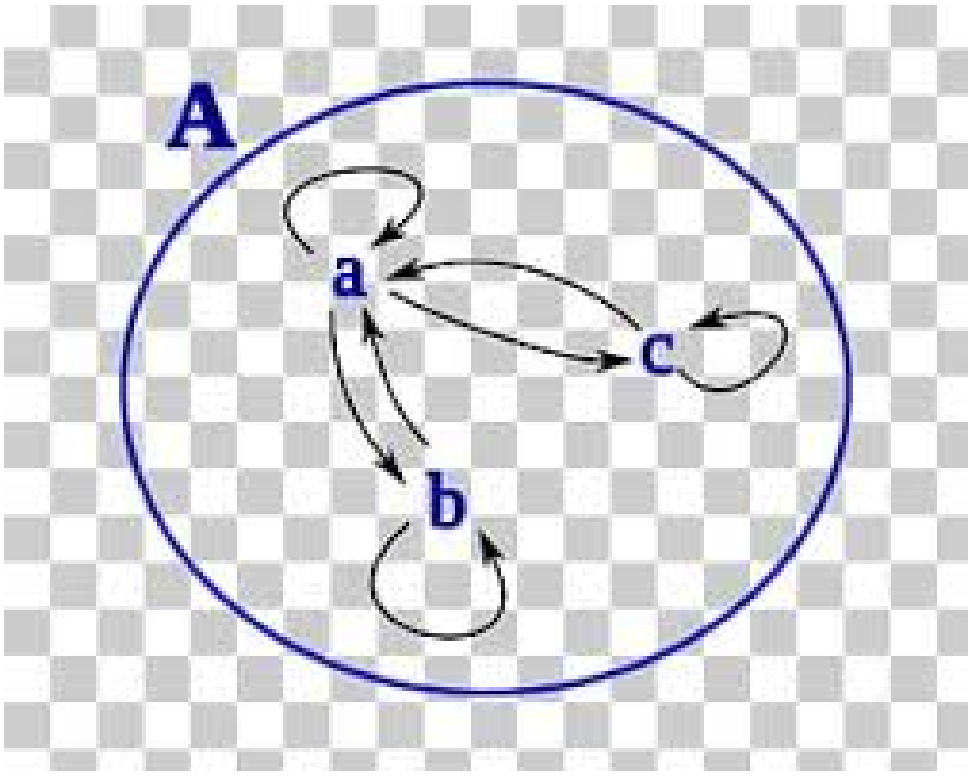
and $\Gamma_2 = \{(1,1),(1,3),(2,2),(3.3),(3,4),(4,2),(4,4)\}$*, respectively.*

Are the relations $\mathscr{R}_1$ *and* $\mathscr{R}_2$ *reflexive?*

Since $(3,3) \notin \Gamma_1$*, then* $\mathscr{R}_1$ *is not a reflexive relation.*

Since $(1,1),(2,2),(3.3),(4,4) \in \Gamma_2$ *that is to say* $\forall x \in \Omega$ *the pair* $(x,x) \in \Gamma_2$*. Consequently,* $\mathscr{R}_2$ *is a reflexive relation.*

Definition 2.14. *The relation* $\mathscr{R}$ *is considered symmetric, if* $\forall x,y \in E : x\mathscr{R}y \Rightarrow y\mathscr{R}x$ *holds.*



Remark 2.8. *For a relation to be symmetric, the following condition must be satisfied. If* $(x,y) \in \Gamma$ *then* (y,x) *also belong to the graph* Γ*, if the relation* $\mathscr{R}$ *on a set* Ω *is represented by its graph* Γ*.*

Example 2.18. *Let us consider the binary relation* $\mathscr{R}$ *on set* $\mathbb{R}^2$ *as follows*

$\forall (x,y),(x',y') \in \mathbb{R}^2 : (x,y)\mathscr{R}(x',y') \Leftrightarrow x = x'$.

Prove that the relation $\mathscr{R}$ *is symmetric.*

Clearly $\forall (x,y) \in \mathbb{R}^2 : (x,y)\mathscr{R}(x',y') \Leftrightarrow x = x' \Leftrightarrow (x',y')\mathscr{R}(x,y)$ *because* $x = x'$*. Consequently,* $\mathscr{R}$ *is a symmetric relation.*

Example 2.19. *Consider the set* $\Omega = \{1,2,3,4\}$ *and the graphs of the relations* $\mathscr{R}_1$ *and* $\mathscr{R}_2$ *are*

$\Gamma_1 = \{(1,1),(1,3),(2,2),(3.1),(3,4),(4,4)\}$

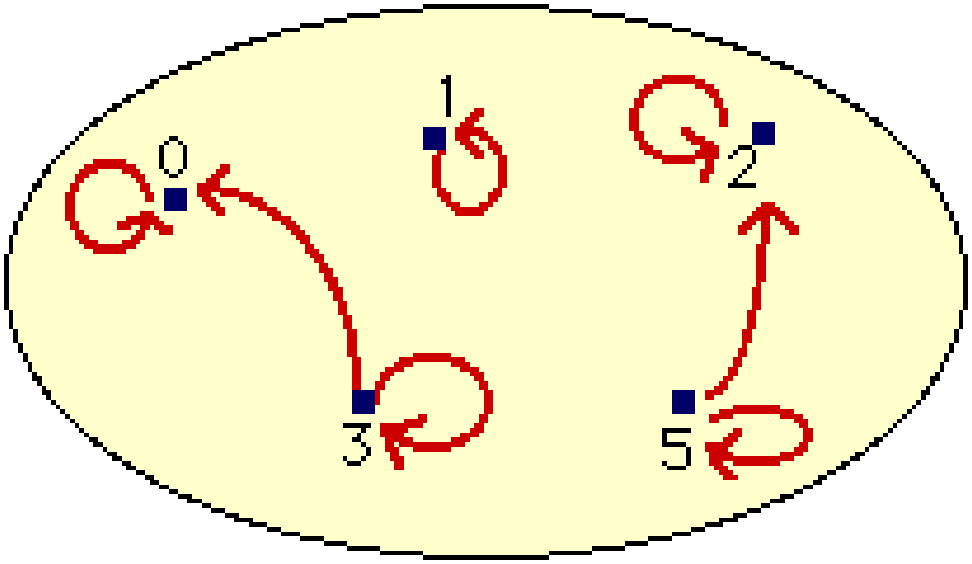
and $\Gamma_2 = \{(1,1),(1,3),(2,2),(3,1),(3.3),(3,4),(4,3),(4,4)\}$*, respectively.*

Are the relations $\mathscr{R}_1$ *and* $\mathscr{R}_2$ *symmetric?*

Since $(3,4) \in \Gamma_1$ *and* $(4,3) \notin \Gamma_1$*, then* $\mathscr{R}_1$ *is not a symmetric relation.*

Since $(1,3),(3,1),(3.4),(4,3) \in \Gamma_2$ *that is to say* $\forall x,y \in \Omega$ *the pair* $(x,y),(y,x) \in \Gamma_2$*. Consequently,* $\mathscr{R}_2$ *is a symmetric relation.*

Definition 2.15. *The relation $\mathscr{R}$ is considered antisymmetric, if $\forall x,y \in E : x\mathscr{R}y \wedge y\mathscr{R}x \Rightarrow x = y$ holds.*



Remark 2.9. *For a relation to be an antisymmetric, the following condition must be satisfied. If $(x,y) \in \Gamma$ then (y,x) does not belong to the graph Γ, if the relation $\mathscr{R}$ on a set Ω is represented by its graph Γ.*

Example 2.20. *Let us consider the binary relation $\mathscr{R}$ on set $\mathbb{R}$ as follows*

$\forall x,x' \in \mathbb{R} : x\mathscr{R}x' \Leftrightarrow x \leq x'$.

Prove that the relation $\mathscr{R}$ is antisymmetric.

Assume that $x\mathscr{R}x'$ and $x'\mathscr{R}x$, then we obtain $x \leq x' \leq x$. So $x = x'$. Consequently, $\mathscr{R}$ is an antisymmetric relation.

Example 2.21. *Consider the set $\Omega = \{1,2,3,4\}$ and the graphs of the relations $\mathscr{R}_1$ and $\mathscr{R}_2$ are*

$\Gamma_1 = \{(1,1),(1,3),(2,2),(3,2),(3,4),(4,4)\}$

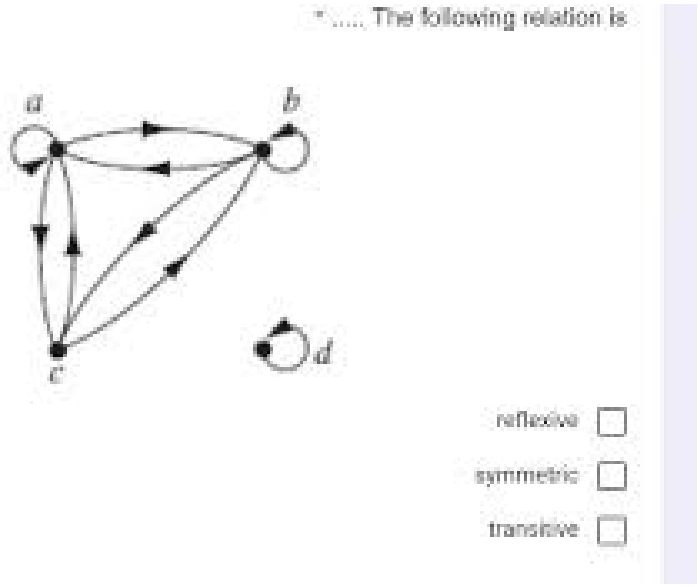
and $\Gamma_2 = \{(1,1),(1,3),(2,2),(3,1),(3,3),(4,3),(4,4)\}$, respectively.

Are the relations $\mathscr{R}_1$ and $\mathscr{R}_2$ antisymmetric?

Since $(1,3),(3,2),(3,4) \in \Gamma_1$ and $(3,1),(2,3),(4,3) \notin \Gamma_1$, then $\mathscr{R}_1$ is an antisymmetric relation.

Since both $(1,3),(3,1) \in \Gamma_2$, then $\mathscr{R}_2$ is not an antisymmetric relation.

Definition 2.16. *The relation $\mathscr{R}$ is considered transitive, if $\forall x,y,z \in E : x\mathscr{R}y \wedge y\mathscr{R}z \Rightarrow x\mathscr{R}z$ holds.*



Remark 2.10. *For a relation to be transitive, the following condition must be satisfied. If* $(x,y),(y,z)\in\Gamma$ *then* (x,z) *must be belong to the graph* Γ*, if the relation* $\mathscr{R}$ *on a set* Ω *is represented by its graph* Γ*.*

Example 2.22. *Let us consider the binary relation* $\mathscr{R}$ *on set* $\mathbb{R}^2$ *as follows*

$\forall(x,y),(x',y')\in\mathbb{R}^2:(x,y)\mathscr{R}(x',y')\Leftrightarrow x=x'.$

Prove that the relation $\mathscr{R}$ *is transitive.*

Assume that $(x,y)\mathscr{R}(x',y')$ *and* $(x',y')\mathscr{R}(x'',y'')$*, then we get* $x=x'$ *and* $x'=x''$*. So,* $(x,y)\mathscr{R}(x'',y'')$*. Therefore,* $\mathscr{R}$ *is transitive relation.*

Example 2.23. *Consider the set* $\Omega=\{1,2,3,4\}$ *and the graphs of the relations* $\mathscr{R}_1$ *and* $\mathscr{R}_2$ *are*

$\Gamma_1=\{(1,1),(1,3),(2,2),(3,2),(3,4),(1,4)\}$

and $\Gamma_2=\{(1,1),(1,3),(1,4),(2,2),(3,1),(3,3),(3,4),(4,4)\}$*, respectively.*

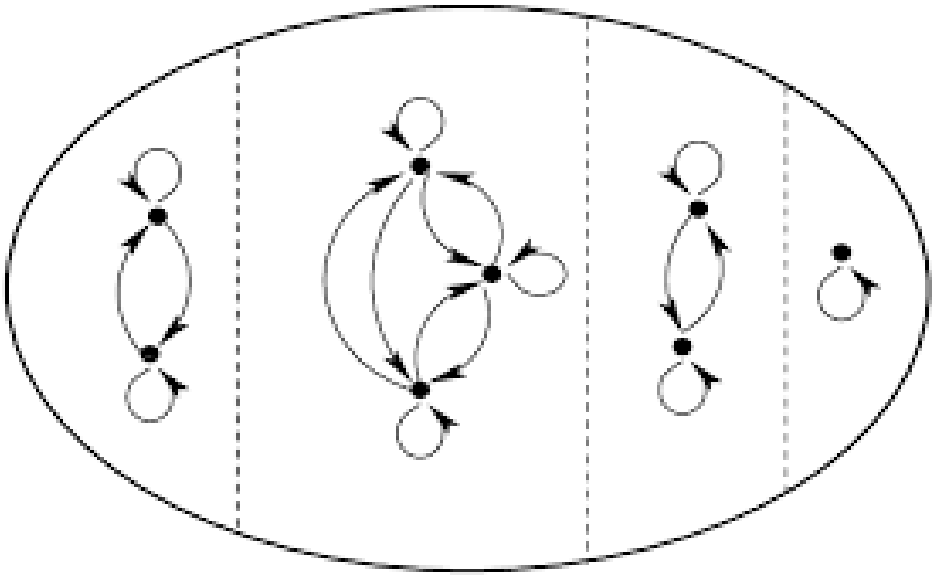
Are the relations $\mathscr{R}_1$ *and* $\mathscr{R}_2$ *transitive?*

Since $(1,3),(3,2)\in\Gamma_1$ *but* $(1,2)\notin\Gamma_1$*, then* $\mathscr{R}_1$ *is not a transitive relation.*

Since $(1,3),(3,4),(1,4)\in\Gamma_2$*. Therefore,* $\mathscr{R}_2$ *is a transitive relation.*

Remark 2.11. *Do not confuse a transitive relation with a circular relation. Because a circular relation must verify* $\forall x,y,z\in E:x\mathscr{R}y\wedge y\mathscr{R}z\Rightarrow z\mathscr{R}x$*. The desired result is* $z\mathscr{R}x$ *not* $x\mathscr{R}z$ *as in the transitive relation i.e. If* $(x,y),(y,z)\in\Gamma$ *then* (z,x) *must be belong to the graph* Γ*.*

Definition 2.17. *An equivalent relation is defined as a relation $\mathscr{R}$ on a set E that is reflexive, symmetric, and transitive.*



Example 2.24. *Let us consider the binary relation $\mathscr{R}$ on set $\mathbb{R}^2$ as follows*

$\forall (x,y),(x',y') \in \mathbb{R}^2 : (x,y)\mathscr{R}(x',y') \Leftrightarrow x = x'$.

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

From Example 2.16,Example 2.18 and Example 2.22 The relation $\mathscr{R}$ is reflexive, symmetric, and transitive. Consequently $\mathscr{R}$ is an equivalence relation.

Definition 2.18. *Let $\mathscr{R}$ be an equivalence relation on E. The subset of E of items related to x by $\mathscr{R}$ is referred to as the equivalence class of x, and the subset is denoted $\dot{x}$ or $\bar{x}$*

$$\dot{x} = \{y \in E : x\mathscr{R}y\}.$$

Example 2.25. *Let us consider the equivalence relation $\mathscr{R}$ on set $\mathbb{R}^2$ as follows*

$\forall (x,y),(x',y') \in \mathbb{R}^2 : (x,y)\mathscr{R}(x',y') \Leftrightarrow x = x'$.

Find the equivalence class $\dot{\overline{(x,y)}}$ of certain (x,y)

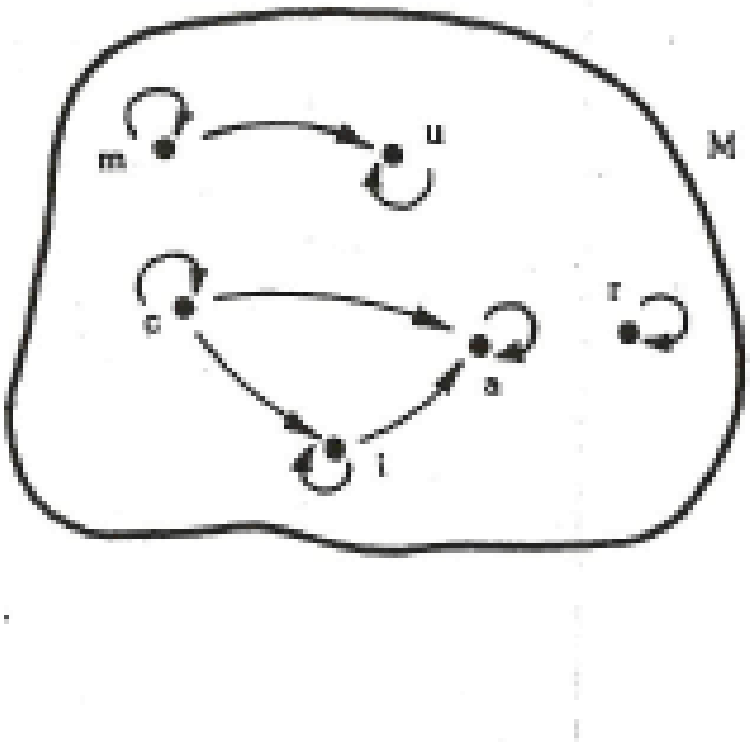
$$\begin{aligned}\dot{\overline{(x,y)}} &= \left\{\left(x',y'\right) \in \mathbb{R}^2 : (x,y)\mathscr{R}\left(x',y'\right)\right\} \\ &= \left\{\left(x',y'\right) \in \mathbb{R}^2 : x' = x, \forall y' \in \mathbb{R}\right\} \\ &= \{x\} \times \mathbb{R}.\end{aligned}$$

Remark 2.12. *Two equivalence classes are either identical or disjoint.*

Definition 2.19. *The quotient set of E by $\mathscr{R}$, represented by the symbol $E/\mathscr{R}$, is the collection of all equivalence classes.*

Remark 2.13. *The set of all equivalence classes of E forms a partition of E.*

Definition 2.20. *An order relation is defined as a relation $\mathscr{R}$ on a set E that is reflexive, antisymmetric, and transitive.*



Example 2.26. *Let us consider the binary relation $\mathscr{R}$ on set $\mathbb{R}$ as follows*

$\forall x,x' \in \mathbb{R} : x\mathscr{R}x' \Leftrightarrow x \leq x'$.

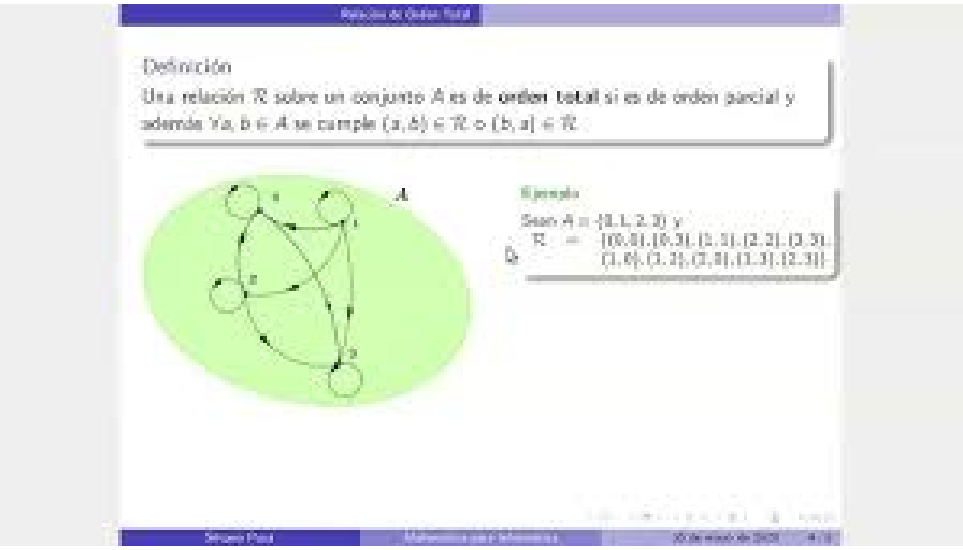
Prove that the $\mathscr{R}$ is an order relation.

Clearly, $x\mathscr{R}x$ and $x'\mathscr{R}x$, since $x \leq x$. So, $\mathscr{R}$ is a reflexive relation.

From Example 2.20, $\mathscr{R}$ is an antisymmetric relation.

Assume that $\forall x,x',x'' \in \mathbb{R} : x\mathscr{R}x' \wedge x'\mathscr{R}x''$. Then $x \leq x' \wedge x' \leq x'' \Rightarrow x \leq x''$. Consequently, $x\mathscr{R}x''$. So, $\mathscr{R}$ is a transitive relation. Therefore, is an an order relation.

Definition 2.21. *The order relation is said to be of total order if any two elements of E are comparable, in other terms, there is relation between any two elements i.e. $\forall x,y \in E$, we have $x\mathscr{R}y$ or $y\mathscr{R}x$, otherwise the order is said to be partial.*



Example 2.27. *Let us consider the order relation $\mathscr{R}$ on set $\mathbb{R}$ as follows*

$\forall x,x' \in \mathbb{R} : x\mathscr{R}x' \Leftrightarrow x \leq x'$.

Is the relation of total order?

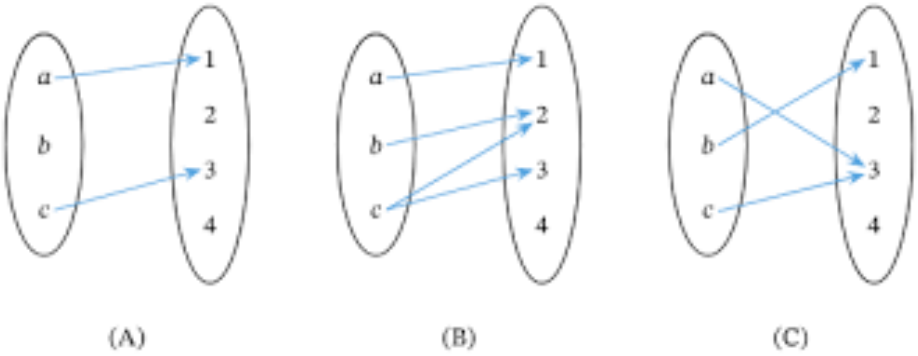
Let x and y be any two real numbers, we always have either $x \leq y$ or $y \leq x$. Consequently, $\mathscr{R}$ is a total order relation.

2.3 Applications

Let E and F be two non-empty sets, and let f be a correspondence ($f : E \to F$) between their elements.

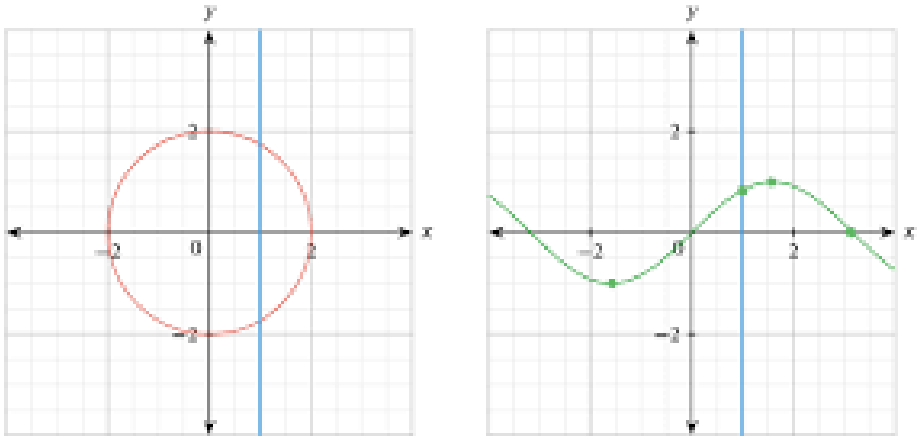
Definition 2.22. *A function is a connection that relates any element of an initial set E corresponds to at most one element of set F, named the codomain or set of destination.*

Example 2.28. *Consider $f : \{a,b,c\} \to \{1,2,3,4\}$, as shown by the graphs below.*



(A) and (C) are functions, but (B) is not because the element c has two different images, i.e. $f(c) = 2$ *and* $f(c) = 3$.

Example 2.29. *Consider the graphs represented by the following figures*



- *The graph in Figure 1 is not of function because in the region* $x \in]-2,2[$, *the lines parallel to* $(0y)$ *intersect the graph at more than one point.*
- *The graph in Figure 2 is of function because the lines parallel to* $(0y)$ *intersect the graph at most at one point.*

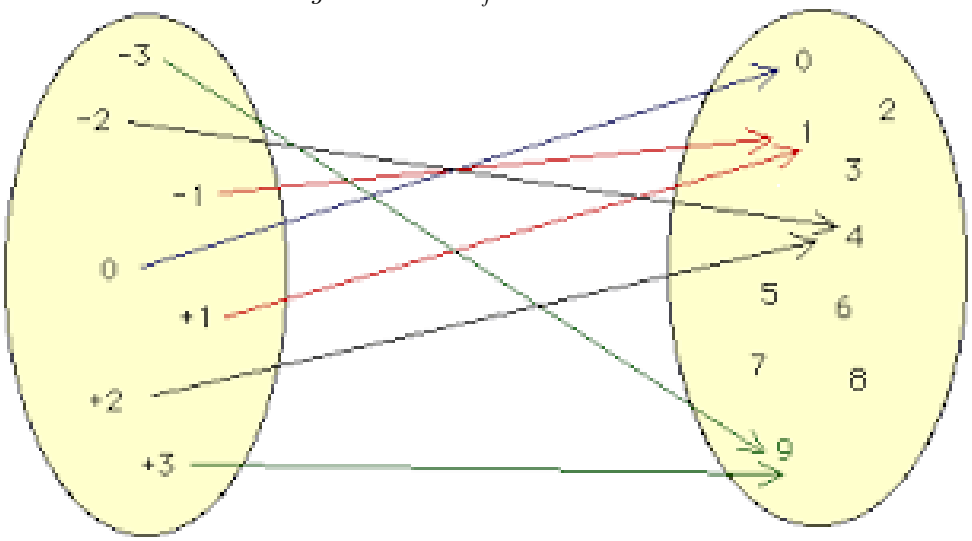
Definition 2.23. *An antecedent is any element of the starting set (source set). The elements of the arrival set (target set) are called "direct images"or just "images".*

Definition 2.24. *The subset of E that only includes elements that permit images is known as the domain of definition of f, and it is represented by the notation* D_f.

Definition 2.25. *The graph of a function f is denoted*

$$\Gamma_f = \{(x,y) \in E \times F : y = f(x)\}.$$

Definition 2.26. *An application is a function which associates to any element of the starting set E an element of an arrival set F. In other terms, there is no element of the starting set which does not have an image i.e. $E = D_f$.*



Definition 2.27. *Two applications f and g are equal if they have the same starting set and the same arrival set i.e. $f,g : E \to F$, moreover they must satisfy the following condition, $\forall x \in E : f(x) = g(x)$.*

Definition 2.28. *Let $f : E \to F$ be an application and $A \subseteq E$. The direct image of A by f is the subset of F that consists of elements of A by f i.e. $f(A) = \{f(x) \in F : x \in A\}$.*

Definition 2.29. *Let $f : E \to F$ be an application and $B \subseteq F$. We call the inverse image of B by f the subset of E which constitutes antecedents of the elements of B by f i.e. $f^{-1}(B) = \{x \in E : f(x) \in B\}$.*

Remark 2.14. *f^{-1} is just a symbol. Moreover f^{-1} does not equal to $\frac{1}{f}$ and f is not necessary invertible.*

Some properties of direct and reciprocal images Consider the application $f : E \to F$. The following claims hold true when $A,B \subset E$ and $C,D \subset F$.

- $A \subset B \Rightarrow f(A) \subset f(B)$,
- $f(A \cup B) = f(A) \cup f(B)$,
- $f(A \cap B) \subset f(A) \cap f(B)$,
- $M \subset N \Rightarrow f^{-1}(M) \subset f^{-1}(N)$,
- $f^{-1}(M \cup N) = f^{-1}(M) \cup f^{-1}(N)$,
- $f^{-1}(M \cap N) = f^{-1}(M) \cap f^{-1}(N)$.

Composition of the two applications Consider the two maps $f : E \to F$ and $g : F \to K$.

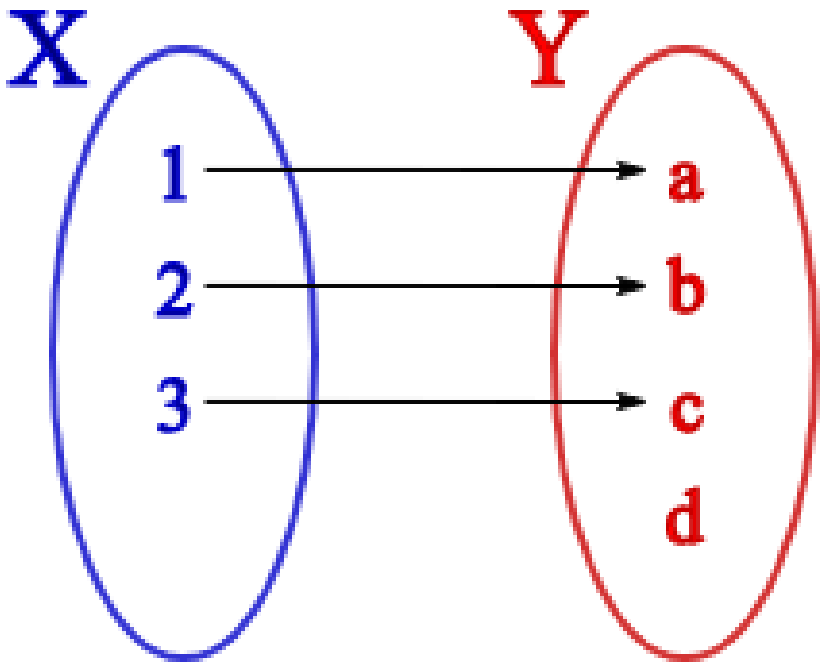
Definition 2.30. *The new application created from maps f and g is what we refer to as the composition of two applications f and g. It is defined as follows $g \circ f : E \xrightarrow{f} F \xrightarrow{g} K$ where $(g \circ f)(x) = g(f(x))$. More specifically $(g \circ f)(x) \neq (f \circ g)(x)$.*

Definition 2.31. *f is said to be injective if every element y of F has at most one antecedent in E i.e.*

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

or

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



Example 2.30. *Consider the function* $f :]1,+\infty[\to]1,+\infty[$ *given by* $f(x) = \frac{x+1}{x-1}$. *Show that* f *is injective.*

$\forall x_1, x_2 \in]1,+\infty[: f(x_1) = f(x_2) \Rightarrow \frac{x_1+1}{x_1-1} = \frac{x_2+1}{x_2-1}$

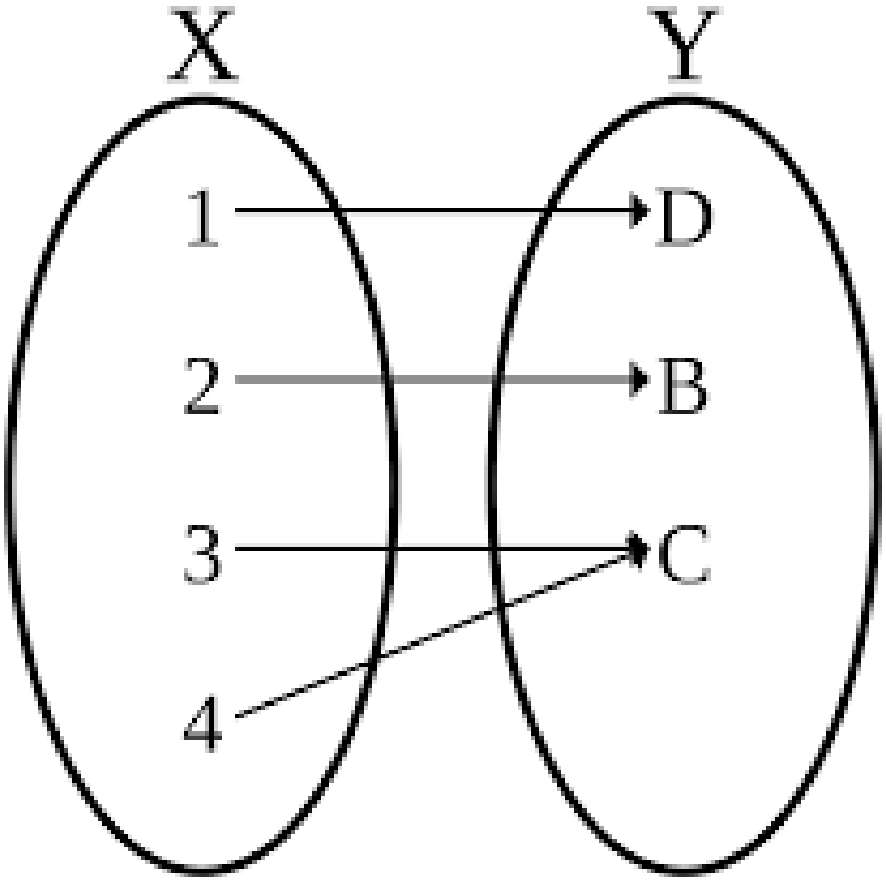
$\Rightarrow (x_1+1)(x_2-1) = (x_1-1)(x_2+1)$

$\Rightarrow x_1x_2 - x_1 + x_2 - 1 = x_1x_2 + x_1 - x_2 - 1 \Rightarrow -x_1 + x_2 = x_1 - x_2$

$\Rightarrow -2x_1 = -2x_2 \Rightarrow -x_1 = -x_2$. *So,* f *is injective.*

Definition 2.32. f *is said to be surjective if every element* y *of* F *has at least one antecedent in* E *i.e.*

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



Example 2.31. *Consider the function* $f :]1,+\infty[\to]1,+\infty[$ *given by* $f(x) = \frac{x+1}{x-1}$. *Show that* f *is surjective.*

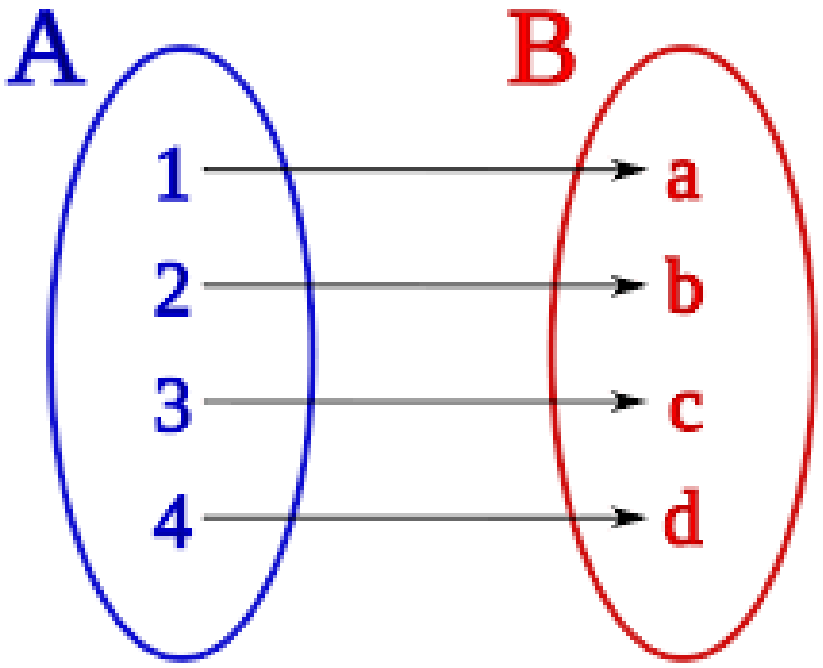
$\forall y \in]1,+\infty[, \exists x \in]1,+\infty[: y = f(x) = \frac{x+1}{x-1} \Rightarrow y(x-1) = x+1$

$\Rightarrow yx - y - x - 1 = 0 \Rightarrow (y-1)x = 1+y$ *because* $y \neq 1$.

Then $y-1 \neq 0$. *So,* $x = \frac{1+y}{y-1}$ *for every* y *in the set* $]1,+\infty[$. *Hence the existence of* x. *Thus* f *is surjective.*

Definition 2.33. f *is said to be bijective if and only if it is both surjective and injective i.e.*

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



Example 2.32. *Consider the function* $f :]1,+\infty[\to]1,+\infty[$ *given by* $f(x) = \frac{x+1}{x-1}$. *Show that* f *is bijective.*

From Example 2.30, f *is injective, and from Example 2.31,* f *is surjective. So,* f *is bijection.*

Definition 2.34. *If* f *performs a bijection from* E *into* F, *then, there exists a unique definite bijection from* F *into* E *which is associated with the image of its antecedent. This map is called a reciprocal or inverse application and is denoted by* f^{-1}.

Remark 2.15. *If* $f : E \to F$ *is bijective and there exists a mapping* $g : F \to E$ *satisfying* $f \circ g = Id_F$ *and* $g \circ f = Id_E$, *then* $g = f^{-1}$ *where* Id_K *is the identity mapping on the set* K *verifying* $Id_K(\alpha) = \alpha$ *for all* $\alpha \in K$.

Remark 2.16. *If* $f \circ g$ *is a bijective application, then, we have* $(f \circ g)^{-1}(x) = \left(g^{-1} \circ f^{-1}\right)(x)$.

Remark 2.17. *Do not confuse reciprocal image and inverse application.*

2.4 Second Chapter's exercises

Exercise 2.1. *Demonstrate by using contradiction reasoning that the set*

$$\mathscr{C} = \left\{(x,y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\right\}$$

cannot be expressed as a Cartesian product of two $\mathbb{R}$ *sections.*

Exercise 2.2. *Let* E *be a non-empty set,* $A,B,C \in \mathscr{P}(E)$*. Show the following assertions.*

- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
- $C_E(A \cup B) = C_E A \cap C_E B$;
- $C_A(A \cap B) = A \backslash B$.

Exercise 2.3. *We define the relation* $\mathscr{R}$ *on* $\mathbb{R}^2$ *by*

$$\forall (x,y), \left(x',y'\right) \in \mathbb{R}^2, (x,y)\,\mathscr{R}\left(x',y'\right) \Leftrightarrow x + y = x' + y'.$$

- *Prove that* $\mathscr{R}$ *is an equivalence relation.*
- *Find the equivalence class of the pair* $(0,0)$*.*

Exercise 2.4. *We define the relation* $\mathscr{R}$ *on* $\mathbb{R}^2$ *by*

$$\forall (x,y), \left(x',y'\right) \in \mathbb{R}^2, \quad (x,y)\,\mathscr{R}\left(x',y'\right) \Leftrightarrow \left|x - x'\right| \leq y' - y.$$

- *Prove that* $\mathscr{R}$ *is an order relation.*
- *Is the order total?*

Exercise 2.5. *We define a binary relation* $\mathscr{R}$ *on the set* $\mathbb{N}\backslash\{0\} \times \mathbb{N}\backslash\{0\}$ *by*

$$\forall (x,y), \left(x',y'\right) \in \mathbb{N}\backslash\{0\} \times \mathbb{N}\backslash\{0\}, \quad (x,y)\mathscr{R}(z,w) \Longleftrightarrow x^w = z^y.$$

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

Exercise 2.6. *We define a binary relation $\mathscr{R}$ on the set $\mathbb{R}$ by*

$$\forall x, y \in \mathbb{R},\ x \mathscr{R} y \Longleftrightarrow \cos^2 x + \sin^2 y = 1.$$

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

Exercise 2.7. *We define a binary relation $\mathscr{R}$ on the set $\mathbb{N}$ by*

$$\forall x, y \in \mathbb{N},\quad x \mathscr{R} y \Longleftrightarrow \exists p, q \in \mathbb{N} \setminus \{0,1\} : y = p x^q.$$

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

Exercise 2.8. *Let E be a set and $\mathscr{P}(E)$ the set of parts of E. We define a binary relation $\mathscr{R}$ on the set $\mathscr{P}(E)$ by*

$$\forall A, B \in \mathscr{P}(E),\quad A \mathscr{R} B \Longleftrightarrow A = B \text{ or } A = \overline{B}.$$

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

Exercise 2.9. *A relation $\mathscr{R}$ is said to be circular if it satisfies $a \mathscr{R} b \wedge b \mathscr{R} c \Rightarrow c \mathscr{R} a$. Demonstrate that $\mathscr{R}$ is an equivalence relation $\Leftrightarrow$ $\mathscr{R}$ is reflexive and $\mathscr{R}$ is circular.*

Exercise 2.10. *Prove that the following functions are applications? Are they injective, surjective or bijective?*

$$\begin{array}{ccc} f_1 : \mathbb{N} \to \mathbb{N} & f_2 : \mathbb{R} \to \mathbb{R} & f_3 : \mathbb{N} \to \mathbb{N} \\ x \mapsto x^2 & x \mapsto \exp\left(-x^2\right) & x \mapsto \ln x \end{array}$$

$$\begin{array}{cc} f_4 : [-2,2] \to [0,2] & f_5 : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{2\} \\ x \mapsto \sqrt{4 - x^2} & x \mapsto \frac{2x+1}{x}. \end{array}$$

Exercise 2.11. *Let $f : \mathbb{R} \setminus \{\alpha\} \to \mathbb{R} \setminus \{\beta\}$ defined by $f(x) = \frac{3x-1}{4x+2}$. To make f bijective, find α and β, then provide its inverse.*

2.5 Corrections of second chapter exercises

Correction of Exercise 2.1 Let us assume that $\mathscr{C} = \{(x,y) \in \mathbb{R}^2 : x^2+y^2 \leq 1\} = E \times F \subset \mathbb{R} \times \mathbb{R}$.

Clearly, $(1,0) \in \mathscr{C}$ because $1^2+0^2 = 1 \leq 1 \Rightarrow 1 \in E$.

Also, we have $(0,1) \in \mathscr{C}$ because $0^2+1^2 = 1 \leq 1 \Rightarrow 1 \in F$.

Therefore, $(1,1) \in E \times F = \mathscr{C}$. But $1^2+1^2 = 2$ is not less than 1, which is a contradiction. Therefore, the hypothesis that $\mathscr{C} = E \times F \subset \mathbb{R} \times \mathbb{R}$ is false.

Correction of Exercise 2.2

- Let x be any element of $A \cup (B \cap C)$, we have

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

  So, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

- Let x be any element of $A \cap (B \cup C)$, we have

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

  So, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

- Let x be any element of $C_E(A \cup B)$, we have

$$x \in C_E(A \cup B) \Leftrightarrow x \in E \wedge x \notin (A \cup B)$$

$$\begin{aligned}
&\Leftrightarrow x \in E \wedge (x \notin A \wedge x \notin B) \\
&\Leftrightarrow (x \in E \wedge x \notin A) \wedge (x \in E \wedge x \notin B) \\
&\Leftrightarrow (x \in C_E A) \wedge (x \in C_E B) \\
&\Leftrightarrow x \in (C_E A \cap C_E B).
\end{aligned}$$

So, $C_E(A \cup B) = C_E A \cap C_E B$.

4/ $C_A(A \cap B) = A \backslash B$

- Let x be any element of $C_E(A \cap B)$, we have

$$\begin{aligned}
x \in C_A(A \cap B) &\Leftrightarrow x \in A \wedge x \notin (A \cap B) \\
&\Leftrightarrow x \in A \wedge (x \notin A \vee x \notin B) \\
&\Leftrightarrow (x \in A \wedge x \notin A) \vee (x \in A \wedge x \notin B) \\
&\Leftrightarrow (x \in \phi) \vee (x \in AA \backslash B) \\
&\Leftrightarrow x \in (\phi \cup A \backslash B) \\
&\Leftrightarrow x \in A \backslash B.
\end{aligned}$$

So, $C_A(A \cap B) = A \backslash B$.

Correction of Exercise 2.3 $\forall (x,y) \in \mathbb{R}^2, (x,y) \mathscr{R} (x,y)$, we have

$$x + y = x + y.$$

So, $(x,y) \mathscr{R} (x,y)$. Thus, $\mathscr{R}$ is a reflexive relation.
$\forall (x,y), (x',y') \in \mathbb{R}^2, (x,y) \mathscr{R} (x',y') \Rightarrow (x',y') \mathscr{R} (x,y)$, we have

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

So, $\mathscr{R}$ is a symmetric relation.
$\forall (x,y), (x',y'), (x'',y'') \in \mathbb{R}^2, (x,y) \mathscr{R} (x',y') \wedge (x',y') \mathscr{R} (x'',y'') \Rightarrow (x,y) \mathscr{R} (x'',y'')$.

We have

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

Summarizing, we get

$$x+y+x'+y'=x'+y'+x''+y'' \Rightarrow x+y=x''+y''.$$

So, $(x,y)\mathscr{R}(x'',y'')$. So, $\mathscr{R}$ is a transitive relation. Hence, $\mathscr{R}$ is an equivalence relation.

The equivalence class of the pair $(0,0)$ is

$$\begin{aligned} \dot{\overline{(0,0)}} &= \left\{(x,y) \in \mathbb{R}^2 : (0,0)\mathscr{R}(x,y)\right\} \\ &= \left\{(x,y) \in \mathbb{R}^2 : x+y=0\right\}, \end{aligned}$$

which represents the line $y=-x$ (the second bisector).

Correction of Exercise 2.4 $\forall (x,y) \in \mathbb{R}^2, (x,y)\mathscr{R}(x,y)$, we have

$$|x-x| \leq y-y=0.$$

So, $\mathscr{R}$ is a reflexive relation.

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

$$\begin{cases} (x,y)\mathscr{R}(x',y') \Leftrightarrow |x-x'| \leq y'-y \\ (x',y')\mathscr{R}(x,y) \Leftrightarrow |x'-x| \leq y-y'. \end{cases}$$

Summarizing, we get

$$\left|x-x'\right| + \left|x'-x\right| = 2\left|x-x'\right| \leq 0 \Rightarrow x=x'.$$

Consequently, we have

$$\begin{cases} 0 \leq y'-y \\ 0 \leq y-y' \end{cases} \Rightarrow \begin{cases} y' \leq y \\ y \leq y' \end{cases} \Rightarrow y \leq y' \leq y \Rightarrow y=y'.$$

So, $\mathscr{R}$ is an antisymmetric relation.

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

We have

$$\begin{cases} (x,y)\mathscr{R}(x',y') \Leftrightarrow |x-x'| \leq y'-y \\ (x',y')\mathscr{R}(x'',y'') \Leftrightarrow |x'-x''| \leq y''-y'. \end{cases}$$

Summarizing, we get

$$\left|x-x'\right| + \left|x'-x''\right| \leq y'-y+y''-y' = y''-y.$$

However, the triangular inequality guarantees that

$$\left|x-x''\right| \leq \left|x-x'\right| + \left|x'-x''\right|.$$

So, we find

$$\left|x-x''\right| \leq y''-y.$$

In other terms $(x,y)\mathscr{R}(x'',y'')$. So, $\mathscr{R}$ is a transitive relation. Hence, $\mathscr{R}$ is an order relation. The order is partial, just consider $(x',y') = (x+1,y)$, which are two incomparable items.

Correction of Exercise 2.5 $\forall (x,y) \in \mathbb{N}\setminus\{0\} \times \mathbb{N}\setminus\{0\} : (x,y)\mathscr{R}(x,y)$

$$(x,y)\mathscr{R}(x,y) \Longleftrightarrow x^y = x^y.$$

So, $\mathscr{R}$ is a reflexive relation.

$\forall (x,y),(z,w) \in \mathbb{N}\setminus\{0\} \times \mathbb{N}\setminus\{0\} : (x,y)\mathscr{R}(z,w) \stackrel{?}{\Rightarrow} (z,w)\mathscr{R}(x,y)$

$$(x,y)\mathscr{R}(z,w) \Longleftrightarrow x^w = z^y \Longleftrightarrow z^y = x^w \Longleftrightarrow (z,w)\mathscr{R}(x,y).$$

So, $\mathscr{R}$ is a symmetric relation.

$\forall (x,y),(z,w),(k,l) \in \mathbb{N}\setminus\{0\} \times \mathbb{N}\setminus\{0\} : (x,y)\mathscr{R}(z,w) \wedge (z,w)\mathscr{R}(k,l) \stackrel{?}{\Rightarrow} (x,y)\mathscr{R}(k,l)$

$$(x,y)\mathscr{R}(z,w) \Longleftrightarrow x^w = z^y \Rightarrow w\ln x = y\ln z \tag{2.1}$$

and

$$(z,w)\mathscr{R}(k,l) \Longleftrightarrow z^l = k^w \Rightarrow l\ln z = w\ln k. \tag{2.2}$$

Multiplying (2.1) by (2.2), we get

$$w\ln x \times l\ln z = y\ln z \times w\ln k \Rightarrow \ln x \times l = y \times \ln k$$
$$\Rightarrow \ln x^l = \ln k^y \Rightarrow x^l = k^y.$$

Hence, $(x,y)\mathscr{R}(k,l)$. So, $\mathscr{R}$ is a transitive relation. Thus, $\mathscr{R}$ is an equivalence relation.

Correction of Exercise 2.6 As for all $x \in \mathbb{R}$, we have

$$\cos^2 x + \sin^2 x = 1 \Rightarrow x\mathscr{R}x.$$

So, $\mathscr{R}$ is a reflexive relation.

$\forall x, y \in \mathbb{R} : x\mathscr{R}y \Rightarrow y\mathscr{R}x$?

Clearly,

$$\cos^2 x = 1 - \sin^2 x \text{ and } \sin^2 y = 1 - \cos^2 y,$$

as well as

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

Then

$$1 - \sin^2 x + 1 - \cos^2 y = 1.$$

From which, we get

$$2 - \sin^2 x - \cos^2 y = 1.$$

Therefore,

$$-\sin^2 x - \cos^2 y = -1.$$

Hence,

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

So, $\mathscr{R}$ is a symmetric relation.

$\forall x,y,z \in \mathbb{R} : x\mathscr{R}y \wedge y\mathscr{R}z \Rightarrow x\mathscr{R}z$. Since

$$\begin{cases} x\mathscr{R}y \Rightarrow \cos^2 x + \sin^2 y = 1, \\ y\mathscr{R}z \Rightarrow \cos^2 y + \sin^2 z = 1. \end{cases}$$

Summarizing, we get

$$\cos^2 x + \underbrace{\sin^2 y + \cos^2 y}_{=1} + \sin^2 z = 1 + 1.$$

Therefore,

$$\cos^2 x + 1 + \sin^2 z = 2.$$

Thus,

$$\cos^2 x + \sin^2 z = 1 \Rightarrow x\mathscr{R}z.$$

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

Correction of Exercise 2.7 $\forall x \in \mathbb{N} : x\mathscr{R}x \iff \exists p,q \in \mathbb{N}\setminus\{0\} : x = px^q$, it suffices to take $p = q = 1$.

So, $\mathscr{R}$ is a reflexive relation.

$\forall x,y \in \mathbb{N}, x\mathscr{R}y$ and $y\mathscr{R}x \stackrel{?}{\Rightarrow} x = y$.

On one hand, we have

$$x\mathscr{R}y \iff \exists p,q \in \mathbb{N}\setminus\{0\} : y = px^q \Rightarrow y \geq x. \tag{2.3}$$

On the other hand, we have

$$y\mathscr{R}x \iff \exists \alpha,\beta \in \mathbb{N}\setminus\{0\} : x = \alpha y^\beta \Rightarrow x \geq y. \tag{2.4}$$

From (2.3) and (2.4), we conclude that $y \leq x \leq y$. Hence, $x = y$.

So, $\mathscr{R}$ is an antisymmetric relation.

$\forall x,y,z \in \mathbb{N}, x\mathscr{R}y \wedge y\mathscr{R}z \stackrel{?}{\Rightarrow} x\mathscr{R}z$.

We have

$$\begin{cases} x\mathscr{R}y \iff \exists p,q \in \mathbb{N}\setminus\{0\} : y = px^q, \\ y\mathscr{R}z \iff \exists \alpha,\beta \in \mathbb{N}\setminus\{0\} : z = \alpha y^\beta. \end{cases}$$

Therefore,

$$z=\alpha\left(px^{q}\right)^{\beta}=\underbrace{\alpha p^{\beta}}_{k\in\mathbb{N}\setminus\{0\}}x^{\overbrace{q\beta}^{l\in\mathbb{N}-\{0\}}}=kx^{l}\Rightarrow x\mathscr{R}z.$$

So, $\mathscr{R}$ is a transitive relation. Thus, $\mathscr{R}$ is an order relation.

Correction of Exercise 2.8 Clearly, we have $\forall A\in\mathscr{P}(E):A=A\Rightarrow A\mathscr{R}A$. So, $\mathscr{R}$ is a reflexive relation.

$\forall A,B\in\mathscr{P}(E):A\mathscr{R}B\Longleftrightarrow A=B$ or $A=\overline{B}$. If $A=\overline{B}\Leftrightarrow\overline{A}=\overline{\overline{B}}\Leftrightarrow\overline{A}=B$.

Thus, $B=A$ or $B=\overline{A}\Rightarrow B\mathscr{R}A$.

$\forall A,B,C\in\mathscr{P}(E):A\mathscr{R}B\wedge B\mathscr{R}C\Rightarrow A\mathscr{R}C$

$A\mathscr{R}B\Longleftrightarrow A=B$ or $A=\overline{B}\wedge B\mathscr{R}C\Longleftrightarrow B=C$ or $B=\overline{C}$.

a/ If $A=B\wedge B=C\Rightarrow A=C$.

b/ If $A=B\wedge B=\overline{C}\Rightarrow A=\overline{C}$.

c/ If $A=\overline{B}\wedge B=C\Rightarrow A=\overline{C}$.

d/ If $A=\overline{B}\wedge B=\overline{C}\Rightarrow A=\overline{\overline{C}}=C$.

So in all cases, we have either $A=C$ or $A=\overline{C}\Rightarrow A\mathscr{R}C$.

Consequently, $\mathscr{R}$ is a transitive relation. Thus, $\mathscr{R}$ is an equivalence relation.

Correction of Exercise 2.9 Let us show that if $\mathscr{R}$ is an equivalence relation $\Rightarrow\mathscr{R}$ is a reflexive and circular relation.

$$\mathscr{R}\text{ is an equivalence relation}\Rightarrow\begin{cases}\mathscr{R}\text{ is reflexive,}\\ \mathscr{R}\text{ is symmetric,}\\ \mathscr{R}\text{ is transitive.}\end{cases}$$

Since $\mathscr{R}$ is a reflexive relation, it remains to be proven that it is a circular relation.

From transitivity, we have

$$a\mathscr{R}b\wedge b\mathscr{R}c\Rightarrow a\mathscr{R}c. \tag{2.5}$$

From symmetricity, we have:

$$a\mathscr{R}c\Rightarrow c\mathscr{R}a. \tag{2.6}$$

Hence, (2.5) and (2.6), we have

$$a\mathscr{R}b \wedge b\mathscr{R}c \Rightarrow c\mathscr{R}a.$$

So, $\mathscr{R}$ is circular relation.

Let us now show that if $\mathscr{R}$ is a reflexive and circular relation, then $\mathscr{R}$ is an equivalence relation.

It suffices to show that $\mathscr{R}$ is a symmetric and transitive relation, because it is a reflexive relation.

Let us assume that $a\mathscr{R}b$, as

$$a\mathscr{R}b \wedge b\mathscr{R}c \Rightarrow c\mathscr{R}a$$

is satisfied for all $a,b,c \in E$.

The relation's still true, if we take $c = b$.

Since $\mathscr{R}$ is a reflexive relation, we have $a\mathscr{R}b \wedge b\mathscr{R}b \Rightarrow b\mathscr{R}a$.

Thus, we have $a\mathscr{R}b \Rightarrow b\mathscr{R}a$. So, $\mathscr{R}$ is a symmetric relation.

Now, by the assumption that $\mathscr{R}$ is a circular relation, and additionally, it is symmetric, we have $a\mathscr{R}b \wedge b\mathscr{R}c \Rightarrow c\mathscr{R}a \Rightarrow a\mathscr{R}c$, which ensures that $\mathscr{R}$ is a transitive relation. Thus, $\mathscr{R}$ is an equivalence relation.

Correction of Exercise 2.10 1/

- f_1 is injective.
- f_1 is not surjective (because integers that are not perfect squares have no antecedents).
- Since f_1 is not surjective, then it cannot be bijective.

2/

- f_2 is not injective (because $f_2(-1) = f_2(1)$, but $-1 \neq 1$).
- f_2 is not injective (because real numbers that are strictly greater than 1 have no antecedents).
- Since f_2 is neither injective nor surjective. Consequently, it is not bijective.

3/ Zero has no image. So, f_3 is not an application. Consequently, it is not injective, surjective, or bijective.

4/

- f_4 is not injective (because $f_2(-2) = f_2(2)$, but $-2 \neq 2$).
- f_4 is surjective.
- Since f_4 is not injective, then it cannot be bijective.

5/

- f_5 is injective.
- f_5 is surjective.
- Since f_5 is both injective and surjective. Consequently, it is bijective.

Correction of Exercise 2.11 $f : \mathbb{R}\setminus\{\alpha\} \to \mathbb{R}\setminus\{\beta\}$ defined as $f(x) = \frac{3x-1}{4x+2}$.

For f to be a map, it must be defined, for this, it must be that $4x+2 \neq 0 \Rightarrow 4x+2 \neq -\frac{1}{2}$.

So, we take $\alpha = -\frac{1}{2}$. Therefore, $f : \mathbb{R}\setminus\left\{-\frac{1}{2}\right\} \to \mathbb{R}\setminus\{\beta\}$.

f injective $\Leftrightarrow \forall x_1, x_2 \in E : f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. We have

$$\begin{aligned} f(x_1) =& f(x_2) \\ \Rightarrow& \frac{3x_1-1}{4x_1+2} = \frac{3x_2-1}{4x_2+2} \\ \Rightarrow& (3x_1-1)(4x_2+2) = (4x_1+2)(3x_2-1) \\ \Rightarrow& 12x_1x_2 - 4x_2 + 6x_1 - 2 = 12x_1x_2 + 6x_2 - 4x_1 - 2 \\ \Rightarrow& -4x_2 + 6x_1 = 6x_2 - 4x_1 \Rightarrow 10x_1 = 10x_2 \Rightarrow x_1 = x_2. \end{aligned}$$

Thus, f is an injective map.

f surjective $\Leftrightarrow \forall y \in F, \exists x \in E : y = f(x)$. We have

$$\begin{aligned} y =& f(x) = \frac{3x-1}{4x+2} \\ \Rightarrow& y(4x+2) = 3x-1 \end{aligned}$$

$$\Rightarrow 3x - 4xy = 2y + 1$$

$$\Rightarrow x(3 - 4y) = 2y + 1.$$

For $3 - 4y \neq 0 \Rightarrow y \neq \frac{3}{4}$ any image will admit an antecedent, and we have $x = \frac{2y+1}{3-4y}$.

So, let's take $\beta = \frac{3}{4}$. Thus, $f : \mathbb{R} \setminus \left\{-\frac{1}{2}\right\} \to \mathbb{R} \setminus \left\{\frac{3}{4}\right\}$ is a bijective mapping.

The inverse mapping is $f^{-1} : \mathbb{R} \setminus \left\{\frac{3}{4}\right\} \to \mathbb{R} \setminus \left\{-\frac{1}{2}\right\}$ and is defined as

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

Chapter 3

Algebraic structures

3.1 General notions

Consider the non-empty set $\mathscr{G}$.

Definition 3.1. *Any application $* : \mathscr{G} \times \mathscr{G} \to \mathscr{G}$ that connects the element $x * y$ of $\mathscr{G}$ to any pair of elements (x, y) of $\mathscr{G} \times \mathscr{G}$ is referred to as an internal composition law. Stated otherwise, the composite of two $\mathscr{G}$ components stays in $\mathscr{G}$, and we write*

$$\forall x, y \in \mathscr{G}, x * y \in \mathscr{G}.$$

We also say that the law $*$ is stable in $\mathscr{G}$.

Example 3.1. *Let $\mathscr{G} =]0,1[$, We define the law $*$ by*

$$\forall x, y \in \mathscr{G} : x * y = x^y.$$

- *Is the law $*$ an internal composition law?*

  Assume that $x, y \in \mathscr{G}$, we have

$$0 < x < 1 \Rightarrow \ln x < 0.$$

Since $y \in \mathscr{G} \Rightarrow y > 0$. So

$$y \ln x < 0.$$

On the other hand, we have

$$y \ln x = \ln x^y < 0 \Rightarrow 0 < x^y < 1.$$

Thus $*$ is an internal composition law.

Example 3.2. *Let $\mathscr{G} = [0,1]$, We define the law $*$ by*

$$\forall x, y \in \mathscr{G} : x * y = x + y - 1.$$

- *Is the law $*$ an internal composition law?*

Taking $x, y \in \left]0, \frac{1}{2}\right[\subset \mathscr{G}$. Clearly,

$$x + y < 1 \Rightarrow x + y - 1 < 0.$$

So, $x * y \notin \mathscr{G}$. Therefore, $*$ is not an internal composition law.

For the remainder of the chapter, we assume that $*$ and Δ are two internal composition rules on the non-empty set $\mathscr{G}$.

Definition 3.2. *An internal composition law $*$ is said to be commutative, if and only if:*

$$\forall x, y \in \mathscr{G}, x * y = y * x.$$

Example 3.3. *Let $\mathscr{G} = \mathbb{R}$, We define the law $*$ by*

$$\forall x, y \in \mathscr{G} : x * y = x + y + xy.$$

- *Is the law $*$ a commutative law?*

Clearly, we have $\forall x, y \in \mathscr{G}$

$$x * y = x + y + xy = y + x + yx = y * x.$$

So, $*$ is a commutative law.

Example 3.4. *Let $\mathscr{G} = \mathbb{R}$, We define the law $*$ by*

$$\forall x, y \in \mathscr{G} : x * y = 2x + 3y.$$

- *Is the law $*$ a commutative law?*

Clearly, we have $\forall x, y \in \mathscr{G}$

$$x * y = 2x + 3y.$$

On the other hand, we have

$$y * x = 2y + 3x.$$

As x, y *are chosen arbitrarily, if we take* $x \neq y$*, then, we have*

$$x * y - y * x = y - x \neq 0.$$

So, $x * y \neq y * x$*. Therefore* $*$ *is not a commutative law.*

Definition 3.3. *An internal composition law* $*$ *is said to be associative, if and only if*

$$\forall x, y, z \in \mathscr{G}, x * (y * z) = (x * y) * z.$$

Example 3.5. *Let* $\mathscr{G} = \mathbb{R}$*, We define the law* $*$ *by*

$$\forall x, y \in \mathscr{G} : x * y = x + y + xy.$$

- *Is the law* $*$ *an associative law?*

Clearly, we have $\forall x, y, z \in \mathscr{G}$

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

On the other hand, we have

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

Obviously, from the equalities above, we have $(x*y)*z = x*(y*z)$. *So,* $*$ *is an associative law.*

Example 3.6. *Let* $\mathscr{G} = \mathbb{R}$, *We define the law* $*$ *by*

$$\forall x, y \in \mathscr{G} : x*y = 2x+3y.$$

- *Is the law* $*$ *an associative law?*

Clearly, we have $\forall x, y, z \in \mathscr{G}$

$$\begin{aligned}(x*y)*z &= (2x+3y)*z \\ &= 2(2x+3y)+3z \\ &= 4x+6y+3z.\end{aligned}$$

On the other hand, we have

$$\begin{aligned}x*(y*z) &= x*(2y+3z) \\ &= 2x+3(2y+3z) \\ &= 2x+6y+9z.\end{aligned}$$

From the above equalities, we conclude that $(x*y)*z \neq x*(y*z)$. *Therefore* $*$ *is not an associative law.*

Definition 3.4. *An internal composition law* $*$ *is said to be left-distributive with respect to* Δ *in* $\mathscr{G}$, *if*

$$\forall x, y, z \in \mathscr{G}, x*(y\Delta z) = (x*y)\Delta(x*z).$$

An internal composition law $*$ *is said to be right-distributive with respect to* Δ *in* $\mathscr{G}$, *if*

$$\forall x, y, z \in \mathscr{G}, (y\Delta z)*x = (y*x)\Delta(z*x).$$

Remark 3.1. *If* $*$ *is distributive to the left and to the right with respect to* Δ *on* $\mathscr{G}$, *we say that it is distributive.*

Example 3.7. *We define the internal composition law $*$ and $\top$ in $\mathbb{R}^2$ by*

$$\forall (x,y),(x',y') \in \mathbb{R}^2, (x,y) * (x',y') = (x+x',y+y'),$$
$$(x,y) \top (x',y') = (xx',xy'+x'y).$$

- *Show that $\top$ is distributive with respect to $*$ in $\mathbb{R}^2$.*

For all $(x,y),(x',y'),(x'',y'')$ in $\mathbb{R}^2$, we have

$$\begin{aligned}
[(x,y) * (x',y')] \top (x'',y'') &= (x+x',y+y') \top (x'',y'') \\
&= ((x+x')x'', (x+x')y'' + x''(y+y')) \\
&= (xx'' + x'x'', xy'' + x'y'' + x''y + x''y') \\
&= (xx'', xy'' + x''y) + (x'x'', x'y'' + x''y') \\
&= [(x,y) \top (x'',y'')] * [(x',y') \top (x'',y'')].
\end{aligned}$$

So, $\top$ is right-distributive with respect to $*$ in $\mathbb{R}^2$, and since $\top$ is a commutative law in $\mathbb{R}^2$. Therefore, $\top$ is distributive with respect to $*$ in $\mathbb{R}^2$.

Definition 3.5. *The element e of $\mathscr{G}$ is said to be left-neutral with respect to $*$ in $\mathscr{G}$, if*

$$\exists e \in \mathscr{G}, \forall x \in \mathscr{G} : e * x = x,$$

The element e of $\mathscr{G}$ is said to be right-neutral with respect to $*$ in $\mathscr{G}$, if

$$\exists e \in \mathscr{G}, \forall x \in \mathscr{G} : x * e = x.$$

Definition 3.6. *e is called a neutral element, if it is both a left and a right neutral element.*

Remark 3.2. *It will be adequate to demonstrate only one of the two aforementioned relations in the event that $*$ is a commutative law.*

Example 3.8. *Let $\mathscr{G} = \mathbb{R} \setminus \{-1\}$, We define the law $*$ by*

$$\forall x,y \in \mathscr{G} : x * y = x + y + xy.$$

- *Does $\mathscr{G}$ admit a neutral element with respect to the law $*$?*

$\exists e \in \mathscr{G}, \forall x \in \mathscr{G} : x * e = e * x = x$

$$x * e = x + e + xe = x \Rightarrow (1+x)e = 0$$
$$\Rightarrow e = 0 \text{ since } x \neq -1$$

As $0 \in \mathscr{G}$, then it isright-neutral. Since $*$ is a comutative law, we conclude that 0 is a neutral element.

Example 3.9. *Let $\mathscr{G} = \mathbb{R}$, We define the law $*$ by*

$$\forall x, y \in \mathscr{G} : x * y = 2x + 3y.$$

- *Does $\mathscr{G}$ admit a neutral element with respect to the law $*$?*

$\exists e \in \mathscr{G}, \forall x \in \mathscr{G} : x * e = e * x = x$

$$x * e = 2x + 3e = x \Rightarrow e = -\frac{x}{3}.$$

Since e depends on x, so it is not unique. Therefore $\mathscr{G}$ does not admit a neutral element with respect to the law $*$

Definition 3.7. *The element x' of $\mathscr{G}$ is said to be a left-symmetric element of x with respect to $*$ in $\mathscr{G}$, if*

$$\forall x \in \mathscr{G}, \exists x' \in \mathscr{G} : x' * x = e,$$

The element x' of $\mathscr{G}$ is said to be a right-symmetric element of x with respect to $*$ in $\mathscr{G}$, if

$$\exists e \in \mathscr{G}, \forall x \in \mathscr{G}, x * x' = e,$$

where e is the neutral element with respect to $*$ in $\mathscr{G}$.

Definition 3.8. *x' is called symmetric element of x, if it is both a left and right symmetric element of x.*

Remark 3.3. *The symmetric element is commonly said to be the inverse of x and is denoted x^{-1}.*

Remark 3.4. *It will be adequate to demonstrate only one of the two aforementioned relations in the event that $*$ is a commutative rule.*

Example 3.10. *Let $\mathcal{G} = \mathbb{R}\setminus\{-1\}$, We define the law $*$ by $\forall x,y \in \mathcal{G} : x*y = x+y+xy$.*

- *does every element of $\mathcal{G}$ admit an symmetric element in $\mathcal{G}$ with respect to $*$?*

$\forall x \in \mathcal{G}, \forall x' \in \mathcal{G} : x*x' = x'*x = e$

$$\begin{aligned} x*x' =& x+x'+xx' = 0 \\ \Rightarrow& (1+x)x' = -x \\ \Rightarrow& x' = -\frac{x}{1+x} \quad \text{because } x \neq -1. \end{aligned}$$

$x' \neq -1$ *since there is no solution to* $-\frac{x}{1+x} = -1$. *Additionally, the law $*$ is commutative. Therefore, every element of $\mathcal{G}$ admits an inverse element in $\mathcal{G}$ with respect to $*$.*

Example 3.11. *Let $\mathcal{G} = \mathbb{R}$, We define the law $*$ by $\forall x,y \in \mathcal{G} : x*y = 2x+3y$.*

- *Does $\mathcal{G}$ admit a neutral element with respect to the law $*$?*

Since $\mathcal{G}$ does not admit a neutral element, we will not be able to find a symmetric element.

3.2 Group

Definition 3.9. *A group is defined as any set $\mathcal{G} \neq \phi$ equipped with an internal composition law $*$ that satisfies*

- *$*$ is an associative law.*
- *$\mathcal{G}$ has a neutral element with respect to $*$.*
- *Every element $x \in \mathcal{G}$ has a symmetric element (an inverse) $x^{-1} \in \mathcal{G}$.*

Definition 3.10. *If $(\mathcal{G},*)$ is a group and $*$ is commutative, we say that $(\mathcal{G},*)$ is an abelian or commutative group.*

Example 3.12. *Let $\mathscr{G} = \{-1, 1, -i, i\}$ with $i^2 = -1$, we define the law $*$ by*

$$\forall x, y \in \mathscr{G} : x * y = xy.$$

- *Is $(\mathscr{G}, *)$ a group?*

Clearly $*$ is an internal composition law, since we have

$-1 \times -1 = 1 \in \mathscr{G}$, $-1 \times 1 = -1 \in \mathscr{G}$, $-1 \times i = -i \in \mathscr{G}$, $-1 \times -i = i \in \mathscr{G}$,

$1 \times -1 = -1 \in \mathscr{G}$, $1 \times 1 = 1 \in \mathscr{G}$, $1 \times -i = -i \in \mathscr{G}$, $1 \times i = i \in \mathscr{G}$,

$-i \times -1 = i \in \mathscr{G}$, $-i \times 1 = -i \in \mathscr{G}$, $-i \times -i = -1 \in \mathscr{G}$, $-i \times i = 1 \in \mathscr{G}$,

$i \times -1 = -i \in \mathscr{G}$, $i \times 1 = i \in \mathscr{G}$, $i \times -i = 1 \in \mathscr{G}$, $i \times i = -1 \in \mathscr{G}$.

So $\forall x, y \in \mathscr{G} : x * y \in \mathscr{G}$. Obviously $\forall x, y, z \in \mathscr{G}$, we have $x * y = y * x$. Therefore $*$ is commutative. Also, we have $(x * y) * z = x * (y * z)$, then $*$ is an associative law. 1 is the neutral element in $\mathscr{G}$ with respect to $*$. It is evident that, the symmetric element of -1 is -1, and that of $-i$ is i and vice versa.

Remark 3.5. *The following special sets can be found in various works.*

- *Any set $\mathscr{G} \neq \phi$ equipped with an internal composition law $*$ is known as magma.*
- *Any set $\mathscr{G} \neq \phi$ equipped with an internal composition law $*$ that is associative is known as monoid.*
- *Any set $\mathscr{G} \neq \phi$ equipped with an internal composition law $*$ that is associative and commutative is known as commutative monoid.*

3.2.1 Subgroup

Let $(\mathscr{G}, *)$ be a group and let $\mathscr{H}$ be a non-empty subset of $\mathscr{G}$.

Definition 3.11. *We say that the non-empty subset $\mathscr{H}$ of $\mathscr{G}$ is a subgroup of $\mathscr{G}$, if $(\mathscr{H}, *)$ is a group for the law $*$ restricted to $\mathscr{H}$ and we denote $(\mathscr{H}, *) < (\mathscr{G}, *)$.*

Proposition 3.1. *Let $(\mathscr{G},*)$ be a group whose e is the neutral element and $\mathscr{H} \subset \mathscr{G}$.*

$$(\mathscr{H},*) < (\mathscr{G},*) \Leftrightarrow \begin{cases} \mathscr{H} \neq \phi \text{ i.e. } e \in \mathscr{H}, \\ \forall x,y \in \mathscr{H} : x*y \in \mathscr{H}, \\ \forall x \in \mathscr{H} : x^{-1} \in \mathscr{H}. \end{cases} \tag{3.1}$$

Remark 3.6. *The following statements are equivalent*

$$\begin{cases} \mathscr{H} \neq \phi \text{ i.e. } e \in \mathscr{H}, \\ \forall x,y \in \mathscr{H} : x*y \in \mathscr{H}, \\ \forall x \in \mathscr{H} : x^{-1} \in \mathscr{H}, \end{cases} \Leftrightarrow \begin{cases} \mathscr{H} \neq \phi \text{ i.e. } e \in \mathscr{H}, \\ \forall x,y \in \mathscr{H} : x*y^{-1} \in \mathscr{H}, \end{cases}$$

where y^{-1} is the symmetric element of y in $\mathscr{H}$.

Remark 3.7. *$\mathscr{G}$ and $\{e\}$ are the trivial subgroups of $\mathscr{G}$.*

Definition 3.12. *Let $(\mathscr{G},*)$ be a group and $\mathscr{H} \subset \mathscr{G}$ a subset of $\mathscr{G}$. The subgroup $\mathscr{K}$ generated by $\mathscr{H}$ is the smallest subgroup of $\mathscr{G}$ containing $\mathscr{H}$.*

Example 3.13. *Let $\mathscr{G} = \{z \in \mathbb{C} : |z| = 1\}$*

- *Show that $(\mathscr{G},\times)$ is a subgroup of $(\mathbb{C},\times)$.*

Clearly, $1 \in \mathscr{G}$ since $|1| = 1 \Rightarrow \mathscr{G} \neq \phi$.
Let $z_1, z_2 \in \mathscr{G}$, does $z_1 \times z_2^{-1} \in \mathscr{G}$? We have

$$z_1 \times z_2^{-1} = \frac{z_1}{z_2} \Rightarrow \left|z_1 \times z_2^{-1}\right| = \left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|} = 1,$$

since $z_1, z_2 \in \mathscr{G}$, then $|z_1| = 1$ and $|z_2| = 1$. So $z_1 \times z_2^{-1} \in \mathscr{G}$. Therefore, $(\mathscr{G},\times)$ is a subgroup of $(\mathbb{C},\times)$.

3.3 Group morphisms

Definition 3.13. *Let $(\mathscr{G},*)$ and $(\mathscr{H},\top)$ be two groups. An application $f : (\mathscr{G},*) \to (\mathscr{H},\top)$ is called a group morphism, if*

$$f(x*y) = f(x) \top f(y)$$

holds every x, y in $\mathscr{G}$.

Example 3.14. *Let $k \in \mathbb{Z}$ and let $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ defined by : $f(x) = kx$.*

- *Is f a group morphism?*

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

$$f(x+y) = k(x+y) = kx+ky = f(x)+f(y).$$

Therefore, f is a group morphism.

Proposition 3.2. *Let $f : (\mathscr{G}, *) \to (\mathscr{H}, \top)$ be a group morphism, we have*

- $f(e_{\mathscr{G}}) = e_{\mathscr{H}}$.
- $\forall x \in \mathscr{G} : f\left(x^{-1}\right) = (f(x))^{-1}$.

Definition 3.14. *Let $f : (\mathscr{G}, *) \to (\mathscr{H}, \top)$ be a group morphism, if f is bijective, then, f is said to be an isomorphism.*

3.3.1 Kernel and image

Definition 3.15. *The subset of $\mathscr{G}$ that we refer to as the kernel of f is denoted by*

$$\ker f = \{x \in \mathscr{G} : f(x) = e_{\mathscr{H}}\}.$$

Definition 3.16. *The subset of $\mathscr{H}$ that we refer to as the image of f is denoted by*

$$\mathrm{Im} f = \{f(x) \in \mathscr{H} : x \in \mathscr{G}\}.$$

Proposition 3.3. *Let $f : (\mathscr{G}, *) \to (\mathscr{H}, \top)$ be a group morphism.*

- $(\ker f, *)$ *is a subgroup of* $(\mathscr{G}, *)$.
- $(\mathscr{H}, \top)$ *is a subgroup of* $(\mathscr{H}, \top)$.
- *The map f is injective, if and only if* $\ker f = \{e_{\mathscr{G}}\}$.

- *The map f is surjective, if and only if* $\mathrm{Im} f = \mathscr{H}$.

Proposition 3.4. *Let $f : (\mathscr{G}, *) \to (\mathscr{H}, \top)$ be a group morphism. If* $\dim \mathscr{G} < \infty$*, then*

$$f \text{ is injective} \Longleftrightarrow f \text{ is surjective} \Longleftrightarrow f \text{ is bijective.}$$

3.4 Rings

Consider a set $\mathscr{A}$ equipped with two internal composition laws $*$ and $\top$.

Definition 3.17. *We say that $(\mathscr{A}, *, \top)$ is a ring, if*

- $(\mathscr{A}, *)$ *is a commutative group.*
- $\top$ *is associative law.*
- $\top$ *is distributive with respect to* $*$.

Definition 3.18. *$(\mathscr{A}, *, \top)$ is said to be a commutative ring, if $(\mathscr{A}, *, \top)$ is a ring and $\top$ is commutative.*

Definition 3.19. *$(\mathscr{A}, *, \top)$ is said to be a unitary ring, if $(\mathscr{A}, *, \top)$ is a ring and $\top$ admits a neutral element.*

3.4.1 Sub-rings

Definition 3.20. *Let $(\mathscr{A}, *, \top)$ be a ring and $\phi \neq \mathscr{H} \subset \mathscr{A}$. $(\mathscr{H}, *, \top)$ is said to be a subring, if $(\mathscr{H}, *, \top)$ is itself a ring.*

Definition 3.21. *Let $(\mathscr{A}, *, \top)$ be a ring and $\phi \neq \mathscr{H} \subset \mathscr{A}$. $(\mathscr{H}, *, \top)$ is said to be a subring, if $(\mathscr{H}, *) < (\mathscr{A}, *)$ and $\forall x, y \in \mathscr{H}$, $x \top y \in \mathscr{H}$.*

Example 3.15. *We define the internal composition law $*$ and $\top$ on $\mathbb{R}^2$ by*

$$\begin{aligned} \forall (x,y), (x',y') \in \mathbb{R}_0^2, (x,y) * (x',y') &= (x+x', y+y'), \\ (x,y) \top (x',y') &= (xx', xy' + x'y). \end{aligned}$$

Show that $\left(\mathbb{R}^2, *, \top\right)$ *be a commutative ring.*

Clearly, $\left(\mathbb{R}^2, *\right)$ *is a commutative group, whose neutral element is* $(0,0)$ *and* $(-x,-y)$ *the inverse element of* (x,y)*. From Example 3.7, the distributivity of* $\top$ *with respect to* $*$ *in* $\mathbb{R}^2$ *follows. Also it is obvious that* $\top$ *is commutative law. It remains to prove that* $\top$ *is an associative law.*

We have for all $(x,y), (x',y'), (x'',y'') \in \mathbb{R}^2$

$$\begin{aligned}
\left[(x,y) \top \left(x',y'\right)\right] \top \left(x'',y''\right) &= \left(xx', xy' + x'y\right) \top \left(x'',y''\right) \\
&= \left(\left(xx'\right)x'', \left(xx'\right)y'' + x''\left(xy' + x'y\right)\right) \\
&= \left(xx'x'', xx'y'' + x''xy' + x''x'y\right) \\
&= \left(x\left(x'x''\right), x\left(x'y'' + x''y'\right) + \left(x''x'\right)y\right) \\
&= (x,y) \top \left[\left(x',y'\right) \top \left(x'',y''\right)\right].
\end{aligned}$$

So, $\top$ *is an associative law. Thus* $\left(\mathbb{R}^2, *, \top\right)$ *is a commutative ring.*

3.4.2 Integrated rings

Let $+, \times$ be two laws without reducing the general meaning and let $(\mathscr{A}, +, \times)$ be a ring such that 0 is the neutral element of the $+$ law and 1 is the neutral element of the $\times$ law, and let $a \in \mathscr{A}$ be such that $a \neq 0$.

Definition 3.22. *a is said to be a left divisor of zero in* $\mathscr{A}$*, if there exists* $x \in \mathscr{A}$ *with* $x \neq 0$*, such that* $a \times x = 0$*.*

Definition 3.23. *a is said to be a right divisor of zero in* $\mathscr{A}$*, if there exists* $x \in \mathscr{A}$ *with* $x \neq 0$*, such that* $x \times a = 0$*.*

Definition 3.24. *a is said to be a zero divisor in* $\mathscr{A}$*, if it is a zero divisor on the left and on the right simultaneously.*

Definition 3.25. *A ring* $(\mathscr{A}, +, \times)$ *is said to be integral if it does not admit any divisors of zero.*

3.4.3 Homomorphism-Isomorphism of rings

Let $(\mathscr{A}, *, \top)$ and $(\mathscr{B}, \nabla, \perp)$ be two rings, and let $f : \mathscr{A} \to \mathscr{B}$.

Definition 3.26. *We say that f is a ring homomorphism, if it verifies*

- $\forall x, y \in \mathscr{A}, f(x * y) = f(x) \nabla f(y)$.
- $\forall x, y \in \mathscr{A}, f(x \top y) = f(x) \perp f(y)$.

Definition 3.27. *We say that f is a ring isomorphism, if f is a bijective homomorphism.*

Definition 3.28. *We say that f is a ring endomorphism, if f is a homomorphism and $\mathscr{A} = \mathscr{B}$.*

Definition 3.29. *We say that f is a ring automorphism, if f is a bijective endomorphism.*

3.4.4 Ideals

Let $(\mathscr{A}, *, \top)$ be a ring and $\mathscr{I} \subset \mathscr{A}$.

Definition 3.30. *We say that $\mathscr{I}$ is a left ideal of $\mathscr{A}$, if*

- $(\mathscr{I}, *)$ *is a subgroup of* $(\mathscr{A}, *)$.
- $\forall x \in \mathscr{A}, \forall y \in \mathscr{I}$, $y \top x \in \mathscr{I}$.

Definition 3.31. *We say that $\mathscr{I}$ is a right ideal of $\mathscr{A}$, if*

- $(\mathscr{I}, *)$ *is a subgroup of* $(\mathscr{A}, *)$.
- $\forall x \in \mathscr{A}, \forall y \in \mathscr{I}$, $x \top y \in \mathscr{I}$.

Definition 3.32. *If $\mathscr{I}$ is simultaneously a left and right ideal of $\mathscr{A}$, we refer to it as a two-sided ideal.*

Remark 3.8. *If $(\mathscr{A}, *, \top)$ is a commutative ring, then every ideal is two-sided.*

3.5 Fields

Definition 3.33. $(\mathscr{A}, *, \top)$ *is called a field, if*

- $(\mathscr{A}, *)$ *is a commutative group.*
- $(\mathscr{A} \setminus \{e\}, \top)$ *is a group.*

- $\top$ *is distributive with respect to* $*$.

The following definition is equivalent to Definition 3.33.

Definition 3.34. $(\mathscr{A}, *, \top)$ *is called a field, if*

- $(\mathscr{A}, *, \top)$ *is a unit ring.*
- *Every element of* $\mathscr{A} - \{e\}$ *admits a symmetry where* e *is the neutral element of the law* $*$.

Definition 3.35. $(\mathscr{A}, *, \top)$ *is said to be a commutative field, if* $(\mathscr{A}, *, \top)$ *has a field structure and* $\top$ *is commutative.*

Proposition 3.5. *Every field* $(\mathscr{A}, *, \top)$ *is an integral ring.*

3.6 Third Chapter's exercises

Exercise 3.1. *Let $\mathscr{G} =]-1,1[$. We define the law $*$ by*

$$\forall x,y \in \mathscr{G} : x*y = \frac{x+y}{1+xy}.$$

- *Prove that $*$ is an internal composition.*
- *Show that $(\mathscr{G},*)$ is an abelian group.*

Exercise 3.2. *Prove that $\left(\mathbb{R}^2,\top\right)$ is an abelian group, where $\top$ is defined as follows*

$$\forall (x,y),\left(x',y'\right) \in \mathbb{R}^2 : (x,y) \top \left(x',y'\right) = \left(x+x', ye^{x'} + y'e^{x}\right).$$

Exercise 3.3. *Let $(\mathscr{G},*)$ be a group with neutral element e, such that $*$ satisfies*

$$\forall x \in \mathscr{G} : x*x = e.$$

- *Prove that $(x*y)^{-1} = y^{-1}*x^{-1}$ where z^{-1} is the symmetric element of z.*
- *Prove that $(\mathscr{G},*)$ is an abelian group.*

Exercise 3.4. *Let $(H,\triangledown)$ and $(G,\triangle)$ be two subgroups of $\mathbb{R}$. Consider the map $\varphi : (H,\triangledown) \to (G,\triangle)$.*

Check if φ is a group homomorphism in the instances listed below:

- $\varphi : (\mathbb{R},+) \to (\mathbb{R}\setminus\{0\},\times)$, *where* $\varphi(x) = e^x$.
- $\varphi : (\mathbb{R}^+,\times) \to (\mathbb{R}^+,\times)$, *where* $\varphi(x) = \sqrt{x}$.
- $\varphi : (]0,+\infty[,\times) \to (\mathbb{R},+)$, *where* $\varphi(x) = \ln x$.

Exercise 3.5. *Let $\mathscr{A} = \left\{x = a+b\sqrt{2} : a,b \in \mathbb{Z}\right\}$.*

- *Prove that $(\mathscr{A},+,.)$ is a ring.*
- *We denote by $\varphi\left(a+b\sqrt{2}\right) = a^2-2b^2$. Prove that $\forall x,y \in \mathscr{A}$, we have $\varphi(xy) = \varphi(x)\varphi(y)$.*

- *Deduce that the invertible elements x of $\mathscr{A}$ verify $\varphi(x) = \pm 1$.*

Exercise 3.6. *Let $\mathscr{A} = \mathbb{R}^2$. We define the internal composition laws $+$ and $\times$ by*

$$\forall (x,y), (x',y') \in \mathscr{A}, (x,y) + (x',y') = (x+x', y+y')$$
$$(x,y) \times (x',y') = (xx'-yy', xy'+x'y).$$

- *Show that $(\mathscr{A}, +, \times)$ is a ring.*
- *Is $(\mathscr{A}, +, \times)$ a field?*

Exercise 3.7. *Let $(\mathscr{A}, +, .)$ be a ring, and assume $\forall x \in \mathscr{A}$, $x^2 = x$.*

- *Show that $\forall x \in \mathscr{A}$, $2x = 0$.*
- *Prove that $(\mathscr{A}, +, .)$ is a commutative ring.*

Exercise 3.8. *We define the law $*$ on $]2, +\infty[$ by $x * y = (x-2)(y-2)+2$.*

- *a/ Show that $*$ is an internal composition distribution on $]2, +\infty[$.*

Lett $f :]0, +\infty[\to]2, +\infty[$ such that $f(x) = \frac{2x+1}{x}$.

- *b/ Show that f is an isomorphism from $(]0, +\infty[, \times)$ to $(]2, +\infty[, *)$.*

Exercise 3.9. *We define the law $*$ on $]3, +\infty[$ by $x * y = xy - 3x - 3y + 12$.*

- *Calculate $x * y - 3$.*
- *Show that $*$ is an internal composition law on $]3, +\infty[$.*
- *Does $*$ admit a neutral element?*
- *Does every element of $]3, +\infty[$ admit a symmetric element with respect to $*$.*

Exercise 3.10. *We define the internal composition law $*$ on $\mathbb{R}\setminus\{0\} \times \mathbb{R}\setminus\{0\}$ by*

$$\forall (x,y), (x',y') \in \mathbb{R}\setminus\{0\} \times \mathbb{R}\setminus\{0\}, (x,y) * (x',y') = (xx', xy'+x'y).$$

Show that $(\mathbb{R}\setminus\{0\} \times \mathbb{R}\setminus\{0\}, *)$ is a commutative group.

Exercise 3.11. *We define the internal composition law $*$ on $\mathbb{R}$ by*

$$\forall a, b \in \mathbb{R} : a * b = a + b + 3.$$

Consider the map f, where

$$f : (\mathbb{R}, *) \to (\mathbb{R}, +)$$

$$x \mapsto \alpha x + \beta$$

- *Show that $(\mathbb{R}, *)$ is a commutative group.*
- *Find a relation between α and β so that f is a group morphism.*

3.7 Corrections of third chapter exercises

Correction of Exercise 3.1 1/ $\forall x,y \in \mathscr{G} : x*y \in \mathscr{G}$

Since $x,y \in \mathscr{G}$, we have

$$\begin{cases} x<1 \\ y<1 \end{cases} \Rightarrow \begin{cases} x-1<0 \\ y-1<0 \end{cases} \Rightarrow (x-1)(y-1)>0$$

$$\Rightarrow xy-x-y+1>0 \Rightarrow xy+1>x+y. \tag{3.2}$$

However, we also have

$$\begin{cases} -1<x<1 \\ -1<y<1 \end{cases} \Rightarrow \begin{cases} |x|<1 \\ |y|<1 \end{cases} \Rightarrow |x|\,|y| = |xy| < 1$$

$$\Rightarrow -1<xy<1 \Rightarrow 0<1+xy<2. \tag{3.3}$$

Hence, $1+xy>0$. Thus, from (3.2) and (3.3), we conclude that

$$xy+1>x+y \Rightarrow \frac{x+y}{1+xy} < \frac{1+xy}{1+xy} = 1. \tag{3.4}$$

On the other hand, we have

$$\begin{cases} -1<x \\ -1<y \end{cases} \Rightarrow \begin{cases} x+1>0 \\ y+1>0 \end{cases} \Rightarrow (x+1)(y+1)>0$$

$$\Rightarrow xy+x+y+1>0 \Rightarrow xy+1>-(x+y). \tag{3.5}$$

Since $1+xy>0$, then

$$-\left(\frac{x+y}{1+xy}\right) < \frac{xy+1}{1+xy} = 1 \Rightarrow -1 < \frac{x+y}{1+xy}. \tag{3.6}$$

From (3.4) and (3.6), we get

$$-1 < \frac{x+y}{1+xy} = x*y < 1.$$

Therefore, $x*y \in \mathscr{G}$. So $*$ is an internal composition law.

$$2/\ (\mathscr{G},*) \text{ is an abelian group} \Longleftrightarrow \begin{cases} * \text{ is commutative,} \\ * \text{ is associative,} \\ \text{existence of a neutral element,} \\ \text{every element admits a symmetry.} \end{cases}$$

$*$ is commutative $\Leftrightarrow \forall x,y \in \mathscr{G} : x*y = y*x$. We have

$$x*y = \frac{x+y}{1+xy} = \frac{y+x}{1+yx} = y*x,$$

because addition and multiplication are commutative in $\mathbb{R}$.

$*$ is associative $\Leftrightarrow \forall x,y,z \in \mathscr{G} : (x*y)*z = x*(y*z)$. We have

$$\begin{aligned} (x*y)*z = \left(\frac{x+y}{1+xy}\right)*z = \frac{\frac{x+y}{1+xy}+z}{1+\frac{x+y}{1+xy}z} \\ = \frac{\frac{x+y+z(1+xy)}{1+xy}}{1+\frac{xz+yz}{1+xy}} = \frac{\frac{x+y+z+xyz}{1+xy}}{\frac{1+xy+xz+yz}{1+xy}} = \frac{x+y+z+xyz}{1+xy+xz+yz} \end{aligned} \tag{3.7}$$

and

$$\begin{aligned} x*(y*z) = x*\left(\frac{y+z}{1+yz}\right) = \frac{x+\frac{y+z}{1+yz}}{1+x\frac{y+z}{1+yz}} \\ = \frac{\frac{x(1+yz)+y+z}{1+yz}}{\frac{1+yz+xy+xz}{1+yz}} = \frac{\frac{x+xyz+y+z}{1+yz}}{\frac{1+yz+xy+xz}{1+yz}} = \frac{x+xyz+y+z}{1+yz+xy+xz}. \end{aligned} \tag{3.8}$$

Since (3.7) = (3.8) $\Leftrightarrow *$ is associative.

The existence of a neutral element in $\mathscr{G}$ with respect to $*$

$\Leftrightarrow \exists e \in \mathscr{G}, \forall x \in \mathscr{G} : x*e = e*x = x$.

Since $*$ is commutative, it suffices to prove $x*e = x$. We have

$$\begin{aligned} x*e = \frac{x+e}{1+xe} = x \Rightarrow x+e = x(1+xe) \\ \Rightarrow x+e = x+x^2e \\ \Rightarrow e-x^2e = 0 \Rightarrow \left(1-x^2\right)e = 0. \end{aligned}$$

Since $x \neq \pm 1$ $(x \in \mathscr{G})$ the unique solution is that $e = 0 \in \mathscr{G}$.

The existence of a symmetric element in $\mathscr{G}$ with respect to $*$

$\Leftrightarrow \forall x \in \mathscr{G}, \exists x' \in \mathscr{G} : x * x' = x' * x = e$.

Since $*$ is commutative, it suffices to prove $x * x' = e$. We have

$$x * x' = \frac{x + x'}{1 + xx'} = e = 0 \Rightarrow x + x' = 0 \Rightarrow x' = -x.$$

Since $-1 < x < 1 \Rightarrow 1 > -x > -1 \Rightarrow x' \in \mathscr{G}$.

So, $(\mathscr{G}, *)$ is an abelian group.

Correction of Exercise 3.2 $\forall (x,y),(x',y') \in \mathbb{R}^2 : (x,y) \top (x',y') = \left(x + x', ye^{x'} + y'e^{x}\right)$

$\top$ is an internal composition law because $\forall (x,y),(x',y') \in \mathbb{R}^2 : (x,y) \top (x',y') \in \mathbb{R}^2$.

for every $x, y, x', y' \in \mathbb{R}$, we have

$$\begin{cases} x + x' \in \mathbb{R} \\ e^{x}, e^{x'} \in \mathbb{R} \end{cases} \Rightarrow ye^{x'}, y'e^{x} \in \mathbb{R} \Rightarrow ye^{x'} + y'e^{x} \in \mathbb{R}.$$

$\top$ commutative $\Leftrightarrow$

$\forall (x,y),(x',y') \in \mathbb{R}^2 : (x,y) \top (x',y') = (x',y') \top (x,y)$. We have

$$(x,y) \top (x',y') = \left(x + x', ye^{x'} + y'e^{x}\right) = \left(x' + x, y'e^{x} + ye^{x'}\right) = (x',y') \top (x,y),$$

because addition and multiplication are commutative in $\mathbb{R}$.

$\top$ associative $\Leftrightarrow \forall (x,y),(x',y'),(x'',y'') \in \mathbb{R}^2 :$

$[(x,y) \top (x',y')] \top (x'',y'') = (x,y) \top [(x',y') \top (x'',y'')]$. We have

$$\begin{aligned} \left[(x,y) \top (x',y')\right] \top (x'',y'') &= \left(x + x', ye^{x'} + y'e^{x}\right) \top (x'',y'') \\ &= \left(x + x' + x'', \left(ye^{x'} + y'e^{x}\right)e^{x''} + y''e^{x+x'}\right) \\ &= \left(x + x' + x'', ye^{x'}e^{x''} + y'e^{x}e^{x''} + y''e^{x+x'}\right) \\ &= \left(x + x' + x'', ye^{x'+x''} + y'e^{x+x''} + y''e^{x+x'}\right) \end{aligned} \tag{3.9}$$

and

$$\begin{aligned}(x,y)\top\left(x'+x'',y'e^{x''}+y''e^{x'}\right)&=\left(x+x'+x'',ye^{x'+x''}+\left(y'e^{x''}+y''e^{x'}\right)e^{x}\right)\\&=\left(x+x'+x'',ye^{x'+x''}+y'e^{x''}e^{x}+y''e^{x'}e^{x}\right)\\&=\left(x+x'+x'',ye^{x'+x''}+y'e^{x''+x}+y''e^{x'+x}\right)\end{aligned}\tag{3.10}$$

Since (3.9) = (3.10) $\Leftrightarrow \top$ is associative.

The existence of a neutral element in $\mathbb{R}^2$ with respect to $\top$

$\Leftrightarrow \exists (p,q)\in\mathbb{R}^2, \forall (x,y)\in\mathbb{R}^2 : (x,y)\top(p,q)=(p,q)\top(x,y)=(x,y)$.

Since $\top$ is commutative, it suffices to prove $(x,y)\top(p,q)=(x,y)$. On a :

$$(x,y)\top(p,q)=(x+p,ye^{p}+qe^{x})=(x,y)$$

$$\Leftrightarrow\begin{cases}x+p=x\Rightarrow p=0\\ ye^{p}+qe^{x}=y\Rightarrow ye^{0}+qe^{x}=y\Rightarrow qe^{x}=0\Rightarrow q=0, \text{ car } e^{x}\neq 0.\end{cases}$$

So, $(0,0)$ is the neutral element of $\mathbb{R}^2$ with respect t $\top$.

The existence of a symmetric element in $\mathbb{R}^2$ with respect to $\top$

$\Leftrightarrow \forall (x,y)\in\mathbb{R}^2, \exists (x',y')\in\mathbb{R}^2 : (x,y)\top(x',y')=(x',y')\top(x,y)=(p,q)=(0,0)$.

Since $\top$ is commutative, it suffices to prove $(x,y)\top(x',y')=(0,0)$. On a :

$$(x,y)\top\left(x',y'\right)=\left(x+x',ye^{x'}+y'e^{x}\right)=(0,0)$$

$$\Leftrightarrow\begin{cases}x+x'=0\Rightarrow x'=-x\\ ye^{x'}+y'e^{x}=0\Rightarrow y'e^{x}=-ye^{x'}=-ye^{-x}\Rightarrow y'e^{x}e^{-x}=-ye^{-x}e^{-x}\Rightarrow y'=-ye^{-2x}.\end{cases}$$

So, $\left(-x,-ye^{-2x}\right)$ is the symmetric element of (x,y) in $\mathbb{R}^2$ with respect to $\top$.

Thus, $\left(\mathbb{R}^2,\top\right)$ is an abelian group.

Correction of Exercise 3.3 Since $(\mathscr{G},*)$ is a group with neutral element e, hence

$*$ is an internal composition law $\Rightarrow \forall x,y \in \mathscr{G}$, the element $x*y \in \mathscr{G}$

and admits a symmetric element in $\mathscr{G}$. So, we have

$$\begin{aligned} x*y*(x*y)^{-1} =& e \\ \Rightarrow& \underbrace{x^{-1}*x}_{e}*y*(x*y)^{-1} = x^{-1}*e \\ \Rightarrow& y*(x*y)^{-1} = x^{-1} \\ \Rightarrow& \underbrace{y^{-1}*y}_{e}*(x*y)^{-1} \\ =& y^{-1}*x^{-1} \Rightarrow (x*y)^{-1} = y^{-1}*x^{-1}. \end{aligned}$$

Let us now show that $\forall x,y \in \mathscr{G}$, we have: $x*y = y*x$.

According to the hypotheses, we have

$$(x*y)*(x*y) = e \Rightarrow x*(x*y)*(x*y) = x*e$$

$$\overset{\text{the associativity of } *}{\Rightarrow} \left(\underbrace{x*x}_{e}\right)*y*(x*y) = x$$

$$\begin{aligned} \Rightarrow& y*(x*y) = x \\ \Rightarrow& y*y*(x*y) = y*x \\ \Rightarrow& \left(\underbrace{y*y}_{e}\right)*(x*y) = y*x. \end{aligned}$$

Hence $*$ is commutative. Thus $(\mathscr{G},*)$ is a commutative group.

Correction of Exercise 3.4 Let $(H,\triangledown)$ and $(G,\triangle)$ be two subgroups of $\mathbb{R}$. Consider the map $\varphi:(H,\triangledown)\to(G,\triangle)$. Recall that φ is a group momorphism, iff

$$\forall x,y\in H:\varphi(x\triangledown y)=\varphi(x)\triangle\varphi(y).$$

1/ $\varphi:(\mathbb{R},+)\to(\mathbb{R}\setminus\{0\},\times)$, where $\varphi(x)=e^x$.

$\forall x,y\in\mathbb{R}$:

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

$\Rightarrow\varphi$ is a group momorphism.

2/ $\varphi:(\mathbb{R}^+,\times)\to(\mathbb{R}^+,\times)$, where $\varphi(x)=\sqrt{x}$.

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

$$\varphi(x\times y)=\sqrt{x\times y}=\sqrt{x}\times\sqrt{y}=\varphi(x)\times\varphi(y),$$

because $x,y\geq 0\Rightarrow\varphi$ is a group momorphism.

3/ $\varphi:]0,+\infty[,\times)\to(\mathbb{R},+)$, where $\varphi(x)=\ln x$.

$\forall x,y\in]0,+\infty[$:

$$\varphi(x\times y)=\ln(x\times y)=\ln x+\ln y=\varphi(x)+\varphi(y).$$

$\Rightarrow\varphi$ is a group momorphism.

Correction of Exercise 3.5 Let $\mathscr{A}=\left\{x=a+b\sqrt{2}:a,b\in\mathbb{Z}\right\}$.

1/ Let us first show that "+" and "." are internal composition laws in $\mathscr{A}$.

$\forall x,y\in\mathscr{A},x+y\overset{?}{\in}\mathscr{A}$ and $x.y\overset{?}{\in}\mathscr{A}$

$x,y\in\mathscr{A}\Rightarrow\exists a,b,\alpha,\beta\in\mathbb{Z}:x=a+b\sqrt{2}$ and $y=\alpha+\beta\sqrt{2}$. We have

$$x+y=a+b\sqrt{2}+\alpha+\beta\sqrt{2}=\left(\underbrace{a+\beta}_{\in\mathbb{Z}}\right)+\left(\underbrace{b+\beta}_{\in\mathbb{Z}}\right)\sqrt{2}\in\mathscr{A}\Rightarrow x+y\in\mathscr{A}.$$

$$x.y=\left(a+b\sqrt{2}\right).\left(\alpha+\beta\sqrt{2}\right)=a\left(\alpha+\beta\sqrt{2}\right)+b\sqrt{2}\left(\alpha+\beta\sqrt{2}\right)$$

$$=a\alpha+a\beta\sqrt{2}+\alpha b\sqrt{2}+2b\beta=\left(\underbrace{a\alpha+2b\beta}_{\in\mathbb{Z}}\right)+\left(\underbrace{a\beta+\alpha b}_{\in\mathbb{Z}}\right)\sqrt{2}\in\mathscr{A}\Rightarrow x.y\in\mathscr{A}.$$

Thus the laws are of internal composition in $\mathscr{A}$.

Let us show that $(\mathscr{A},+)$ is a commutative group.

$\forall x,y\in\mathscr{A},:x+y=y+x$. Since $x,y\in\mathscr{A}\Rightarrow\exists a,b,\alpha,\beta\in\mathbb{Z}:x=a+b\sqrt{2}$

and $y=\alpha+\beta\sqrt{2}$, we have

$$x+y=a+b\sqrt{2}+\alpha+\beta\sqrt{2}=\alpha+\beta\sqrt{2}+a+b\sqrt{2}=y+x,$$

because addition is commutative in $\mathbb{Z}$.

$\forall x,y,z\in\mathscr{A},\ (x+y)+z=x+(y+z)$. Since $x,y,z\in\mathscr{A}$

$\Rightarrow \exists a,b,\alpha,\beta,c,d\in\mathbb{Z}: x=a+b\sqrt{2}$ and $y=\alpha+\beta\sqrt{2}$ and $z=c+d\sqrt{2}$, we have

$$\begin{aligned}(x+y)+z=&\left(a+b\sqrt{2}+\alpha+\beta\sqrt{2}\right)+c+d\sqrt{2}\\ =&a+b\sqrt{2}+\left(\alpha+\beta\sqrt{2}+c+d\sqrt{2}\right)=x+(y+z),\end{aligned}$$

because addition is associative in $\mathbb{Z}$.

The neutral element: $\exists e\in\mathscr{A},\forall x\in\mathscr{A}: x+e=e+x=x$.

Since $+$ is commutative in $\mathscr{A}$, it suffices to prove that $x+e=x$.

Since $x,e\in\mathscr{A}\Rightarrow\exists a,b,\alpha,\beta\in\mathbb{Z}: x=a+b\sqrt{2}$ and $e=\alpha+\beta\sqrt{2}$, we have

$$\begin{aligned}x+e=x&\Rightarrow a+b\sqrt{2}+\alpha+\beta\sqrt{2}=a+b\sqrt{2}\\ &\Rightarrow(a+\alpha)+(b+\beta)\sqrt{2}=a+b\sqrt{2}\\ &\Rightarrow\begin{cases}a+\alpha=a\\ b+\beta=b\end{cases}\Rightarrow\begin{cases}\alpha=0\\ \beta=0.\end{cases}\end{aligned}$$

So, $0=0+0\sqrt{2}\in\mathscr{A}$ is neutral element.

The symmetric element: $\forall x\in\mathscr{A},\exists x'\in\mathscr{A}: x+x'=x'+x=e=0$.

Since $+$ is commutative in $\mathscr{A}$, it suffices to prove that $x+x'=0$.

Since $x,x'\in\mathscr{A}\Rightarrow\exists a,b,a',b'\in\mathbb{Z}: x=a+b\sqrt{2}$ and $x'=a'+b'\sqrt{2}$

$$\begin{aligned}x+x'=x&\Rightarrow a+b\sqrt{2}+a'+b'\sqrt{2}=a+b\sqrt{2}\\ &\Rightarrow\left(a+a'\right)+\left(b+b'\right)\sqrt{2}=0\\ &\Rightarrow\begin{cases}a+a'=0\\ b+b'=0\end{cases}\Rightarrow\begin{cases}a'=-a\\ b'=-b.\end{cases}\end{aligned}$$

So, $-a-b\sqrt{2}\in\mathscr{A}$ is the symmetric element of $a+b\sqrt{2}$.

Thus, $(\mathscr{A},+)$ is a commutative group.

Let us show that "." is distributive with respect to "+"

$\forall x,y,z\in\mathscr{A},\ (x+y).z=x.z+y.z$ and $\forall x,y,z\in\mathscr{A},\ z.(x+y)=z.x+z.y$.

Indeed $a,b,a',b',a'',b''\in\mathbb{Z}: x=a+b\sqrt{2}$ and $y=a'+b'\sqrt{2}$ and $z=a''+b''\sqrt{2}$, we have

$$\begin{aligned}
(x+y).z &= \left(a+b\sqrt{2}+a'+b'\sqrt{2}\right).\left(a''+b''\sqrt{2}\right)\\
&= \left(\left(a+a'\right)+\left(b+b'\right)\sqrt{2}\right).\left(a''+b''\sqrt{2}\right)\\
&= \left(\left(a+a'\right)\left(a''+b''\sqrt{2}\right)+\left(b+b'\right)\sqrt{2}\left(a''+b''\sqrt{2}\right)\right)\\
&= \left(\left(a+a'\right)a''+\left(a+a'\right)b''\sqrt{2}+\left(b+b'\right)\sqrt{2}a''+\left(b+b'\right)\sqrt{2}b''\sqrt{2}\right)\\
&= a''\left(a+a'\right)+b''\sqrt{2}\left(a+a'\right)+a''\left(b+b'\right)\sqrt{2}+b''\sqrt{2}\left(b+b'\right)\sqrt{2}\\
&= a''a+a''a'+ab''\sqrt{2}+b''\sqrt{2}a'+a''b\sqrt{2}+a''b'\sqrt{2}+2bb''+2b'b''\\
&= \left(a''a+ab''\sqrt{2}+a''b\sqrt{2}+2bb''\right)+\left(a''a'+b''\sqrt{2}a'+a''b'\sqrt{2}+2b'b''\right)\\
&= \left(a\left(a''+b''\sqrt{2}\right)+b\sqrt{2}\left(a''+\sqrt{2}b''\right)\right)+\left(a'\left(a''+b''\sqrt{2}\right)+b'\sqrt{2}\left(a''+\sqrt{2}b''\right)\right)\\
&= \left(\left(a+b\sqrt{2}\right)\left(a''+\sqrt{2}b''\right)\right)+\left(\left(a'+b'\sqrt{2}\right)\left(a''+\sqrt{2}b''\right)\right)=x.z+y.z.
\end{aligned}$$

Similarly, we demonstrate that $z.(x+y)=z.x+z.y$.

So, "." is distributive with respect to "+". Therefore $(\mathscr{A},+,.)$ is a ring.

$2/\ \forall x,y\in\mathscr{A}\Rightarrow\exists a,b,a',b'\in\mathbb{Z}: x=a+b\sqrt{2}$ et $x'=a'+b'\sqrt{2}$

$$\begin{aligned}
\varphi(xy) &= \varphi\left(\left(a+b\sqrt{2}\right)\left(a'+b'\sqrt{2}\right)\right)\\
&= \varphi\left(aa'+ab'\sqrt{2}+a'b\sqrt{2}+2bb'\right)\\
&= \varphi\left(\left(aa'+2bb'\right)+\left(ab'+a'b\right)\sqrt{2}\right)\\
&= \left(aa'+2bb'\right)^2-2\left(ab'+a'b\right)^2\\
&= \left(\left(aa'\right)^2+4aa'bb'+4\left(bb'\right)^2\right)-2\left(\left(ab'\right)^2+2ab'a'b+\left(a'b\right)^2\right)\\
&= \left(aa'\right)^2+4aa'bb'+4\left(bb'\right)^2-2\left(ab'\right)^2-4ab'a'b-2\left(a'b\right)^2\\
&= a^2a'^2-2a^2b'^2+4b^2b'^2-2a'^2b^2
\end{aligned}$$

$$\begin{aligned}
&= a^2\left(a'^2-2b'^2\right)+2b^2\left(2b'^2-a'^2\right)\\
&= a^2\left(a'^2-2b'^2\right)-2b^2\left(a'^2-2b'^2\right)\\
&= \left(a^2-2b^2\right)\left(a'^2-2b'^2\right)\\
&= \varphi(x)\,\varphi(y).
\end{aligned}$$

3/ First, note that for any element $m \in \mathscr{A}$, we have $\varphi(m) \in \mathbb{Z}$.

Suppose $x \in \mathscr{A}$ is invertible in $\mathscr{A} \Rightarrow \exists y \in \mathscr{A} : xy = 1$.

So, $\varphi(xy) = \varphi(y)\,\varphi(x) = \varphi(1) = 1 \Rightarrow \varphi(y) = \frac{1}{\varphi(x)}$.

$x, y \in \mathscr{A}$, we have $\varphi(x), \varphi(y) \in \mathbb{Z}$. As $\varphi(y) = \frac{1}{\varphi(x)}$ with $\varphi(x) \in \mathbb{Z}$.

However, the only relative integers in the inverse are 1 and -1.

So $\varphi(x) = \pm 1$.

Correction of Exercise 3.6 It is clear that "+" and "×" are commutative, because

$\forall (x,y),(x',y') \in \mathscr{A}$,

$$\begin{aligned}
(x,y)+\left(x',y'\right) &= \left(x+x',y+y'\right)\\
&= \left(x'+x,y'+y\right) = \left(x',y'\right)+(x,y).
\end{aligned}$$

$\forall (x,y),(x',y') \in \mathscr{A}$,

$$\begin{aligned}
(x,y).\left(x',y'\right) &= \left(xx'-yy',xy'+x'y\right)\\
&= \left(x'x-y'y,x'y+xy'\right) = \left(x',y'\right)\times(x,y).
\end{aligned}$$

$+$ is associative, because $\forall (x,y),(x',y'),(x'',y'') \in \mathscr{A}$,

$$\begin{aligned}
\left((x,y)+\left(x',y'\right)\right)+\left(x'',y''\right) &= \left(x+x',y+y'\right)+\left(x'',y''\right)\\
&= \left(x+x'+x'',y+y'+y''\right)\\
&= (x,y)+\left(x'+x'',y'+y''\right)\\
&= (x,y)+\left(\left(x',y'\right)+\left(x'',y''\right)\right).
\end{aligned}$$

$\exists (e,e') \in \mathscr{A}, \forall (x,y) \in \mathscr{A} : (x,y)+(e,e') = (e,e')+(x,y) = (x,y)$.

Since $+$ is commutative, it is enough to prove that $(x,y)+(e,e') = (x,y)$. We have

$$(x,y)+\left(e,e'\right) = \left(x+e,y+e'\right) = (x,y) \Rightarrow e = e' = 0.$$

From where $(0,0)$ is the neutral element.

$\forall (x,y) \in \mathscr{A}, \exists (x',y') \in \mathscr{A} : (x,y)+(x',y') = (x',y')+(x,y) = (e,e') = (0,0)$.

Since $+$ is commutative, it is enough to prove that

$$(x,y)+\left(x',y'\right) = \left(x+x',y+y'\right) = (0,0)\,.$$

Hence $x' = -x \in \mathbb{R}$ and $y' = y \in \mathbb{R}$.

Therefore $(-x,-y)$ is the symmetric element of (x,y) in $\mathscr{A}$ with respect to $+$.

Thus $(\mathscr{A},+)$ is a commutative group.

Let us show that $\forall (x,y),(x',y'),(x'',y'') \in \mathscr{A}$:

$$\left((x,y)+\left(x',y'\right)\right).\left(x'',y''\right) = (x,y).\left(x'',y''\right)+\left(x',y'\right).\left(x'',y''\right)$$

because "$\times$" is commutative. We have:

$$\begin{aligned}\left((x,y)+\left(x',y'\right)\right)\times\left(x'',y''\right) &= \left(x+x',y+y'\right)\times\left(x'',y''\right)\\ &= \left(\left(x+x'\right)x''-\left(y+y'\right)y'',\left(x+x'\right)y''+x''\left(y+y'\right)\right)\\ &= \left(xx''+x'x''-yy''-y'y'',xy''+x'y''+x''y+x''y'\right). \qquad (3.11)\end{aligned}$$

and

$$\begin{aligned}(x,y)\times\left(x'',y''\right)+\left(x',y'\right)\times\left(x'',y''\right) &= \left(xx''-yy'',xy''+x''y\right)+\left(x'x''-y'y'',x'y''+x''y'\right)\\ &= \left(xx''-yy''+x'x''-y'y'',xy''+x''y+x'y''+x''y'\right). \qquad (3.12)\end{aligned}$$

Since (3.11) = (3.12), therefore "$\times$" is distributive with respect to "$+$".

Let us now show that "$\times$" is associative

$\forall (x,y),(x',y'),(x'',y'') \in \mathscr{A}, ((x,y)\times(x',y'))\times(x'',y'') = (x,y)\times((x',y')\times(x'',y''))$.

Indeed:

$$\begin{aligned}((x,y)\times(x',y'))\times(x'',y'') &= (xx'-yy',xy'+x'y)\times(x'',y'')\\ &= ((xx'-yy')x''-(xy'+x'y)y'',(xx'-yy')y''+x''(xy'+x'y))\\ &= (xx'x''-yy'x''-xy'y''-x'yy'',xx'y''-yy'y''+x''xy'+x''x'y) \qquad (3.13)\end{aligned}$$

and

$$\begin{aligned}(x,y)\times((x',y')\times(x'',y'')) &= (x,y)\times(x'x''-y'y'',x'y''+x''y')\\ &= (x(x'x''-y'y'')-y(x'y''+x''y'),x(x'y''+x''y')+(x'x''-y'y'')y)\\ &= (xx'x''-xy'y''-yx'y''-yx''y',xx'y''+xx''y'+x'x''y-y'y''y). \qquad (3.14)\end{aligned}$$

Since (3.13) = (3.14), therefore "×" is associative. Thus, $(\mathscr{A},+,\times)$ is a ring.

For $(\mathscr{A},+,\times)$ to be a field, it will be necessary to show that "×" has a neutral element and that any point different from the neutral element of the "+" distribution is invertible.

$\exists (e_1,e_2)\in \mathscr{A}\setminus\{(0,0)\}, \forall (x,y)\in \mathscr{A}\setminus\{(0,0)\}$:

$$(x,y)\times(e_1,e_2) = (e_1,e_2)\times(x,y) = (x,y).$$

Since "×" is commutative, it suffices to prove that $(x,y)\times(e_1,e_2) = (x,y)$. Indeed

$$\begin{aligned}(x,y)\times(e_1,e_2) &= (xe_1-ye_2,xe_2+e_1y) = (x,y)\\ &\Rightarrow \begin{cases} xe_1-ye_2 = x \\ ye_1+xe_2 = y \end{cases} \Rightarrow \begin{cases} x^2e_1-xye_2 = x^2 \\ y^2e_1+yxe_2 = y^2 \end{cases}\end{aligned}$$

$$\begin{aligned}\overset{\text{by summation}}{\Rightarrow}\quad x^2e_1-xye_2+y^2e_1+yxe_2 &= x^2+y^2\\ \Rightarrow (x^2+y^2)e_1 &= x^2+y^2.\end{aligned}$$

As $(x,y) \in \mathscr{A} \setminus \{(0,0)\} \Rightarrow x^2+y^2 \neq 0$, we obtain $e_1 = 1$.

Replacing the value of e_1 in $xe_1 - ye_2 = x$, we get

$$x - ye_2 = x \Rightarrow -ye_2 = 0 \Rightarrow e_2 = 0.$$

Since $(1,0) \in \mathscr{A} \setminus \{(0,0)\}$, So, $(1,0)$ is the neutral element.

$\forall (x,y) \in \mathscr{A} \setminus \{(0,0)\}, \exists (x',y') \in \mathscr{A} \setminus \{(0,0)\}$:

$$(x,y) \times (x',y') = (x',y') \times (x,y) = (1,0).$$

Since "$\times$" is commutative, it suffices to prove that $(x,y) \times (x',y') = (1,0)$. Indeed

$$\begin{aligned}(x,y) \times (x',y') = (xx'-yy', xy'+x'y) &= (1,0) \\ \Rightarrow \begin{cases} xx'-yy' = 1 \\ x'y+xy' = 0 \end{cases} &\Rightarrow \begin{cases} x^2x'-xyy' = x \\ x'y^2+yxy' = 0. \end{cases}\end{aligned}$$

By summation, we have

$$\begin{aligned}x^2x'-xyy'+x'y^2+yxy' = x+0 &\Rightarrow (x^2+y^2)x' = x \\ &\Rightarrow x' = \frac{x}{x^2+y^2},\end{aligned}$$

because $x^2+y^2 \neq 0$. Similarly, we get

$$\begin{cases} xx'-yy' = 1 \\ x'y+xy' = 0 \end{cases} \Rightarrow \begin{cases} yxx'-y^2y' = y \\ xx'y+x^2y' = 0. \end{cases}$$

By subtraction we find

$$\begin{aligned}xx'y+x^2y'-(yxx'-y^2y') &= 0-y \\ \Rightarrow xx'y+x^2y'-yxx'+y^2y' &= -y \\ \Rightarrow (x^2+y^2)y' &= -y\end{aligned}$$

$$\Rightarrow y' = -\frac{y}{x^2+y^2},$$

because $x^2+y^2 \neq 0$. Thus, every element of $\mathscr{A}\setminus\{(0,0)\}$ is invertible. Therefore, $(\mathscr{A},+,\times)$ is a field.

Correction of Exercise 3.7 Clearly $2x = (x+x)$, according to the hypothesis, we have

$$\begin{aligned}(x+x)^2 = (x+x) &\Rightarrow (x+x)(x+x) = (x+x)\\ &\Rightarrow x(x+x)+x(x+x) = (x+x)\\ &\Rightarrow x^2+x^2+x^2+x^2 = (x+x)\\ &\Rightarrow x+x+x+x = (x+x),\end{aligned}$$

because $x^2 = x$. So, for simplification, we must add the symmetrical of x
with respect to "+" which we denote by $-x$, we obtain

$$\begin{aligned}\underbrace{-x+x}_{=0}+x+x+x = \underbrace{-x+x}_{=0}+x &\\ \Rightarrow x+x+x = x &\\ \Rightarrow \underbrace{-x+x}_{=0}+x+x = \underbrace{-x+x}_{=0} &\\ \Rightarrow x+x = 0 &\\ \Rightarrow 2x = 0.&\end{aligned}$$

So, the "0" is the neutral element of "+".
Since $(\mathscr{A},+,.)$ is a ring, it remains to prove that "." is a commutative law
"." is commutative $\Leftrightarrow \forall x,y \in \mathscr{A}, x.y = y.x$, according to the hypothesis, we have:

$$\begin{aligned}(x+y)^2 = (x+y) &\Rightarrow (x+y)(x+y) = (x+y)\\ &\Rightarrow xx+xy+yx+yy = (x+y)\\ &\Rightarrow x+xy+yx+y = (x+y)\\ &\Rightarrow -x+x+xy+yx+y = -x+x+y\end{aligned}$$

$$\begin{aligned}
&\Rightarrow xy+yx+y=y\\
&\Rightarrow xy+yx+y-y=y-y\\
&\Rightarrow xy+yx=0\\
&\Rightarrow xy+xy+yx=xy+0\\
&\Rightarrow \underbrace{2xy}_{=0 \text{ from question 1.}}+yx=xy\\
&\Rightarrow yx=xy.
\end{aligned}$$

So, $(\mathscr{A},+,.)$ is a commutative ring.

Correction of Exercise 3.8 4/ Let us show that $*$ is an internal composition law.

$$\begin{cases} x\in]2,+\infty[\Rightarrow x>2 \Rightarrow x-2>0\\ y\in]2,+\infty[\Rightarrow y>2 \Rightarrow y-2>0 \end{cases}$$
$$\Rightarrow (x-2)(y-2)>0 \Rightarrow \underbrace{(x-2)(y-2)+2}_{x*y}>2.$$

So, $*$ is an internal composition law on $]2,+\infty[$.

Let $f:]0,+\infty[\to]2,+\infty[$ such that $f(x)=\frac{2x+1}{x}$

Let us show that f is an isomorphism from $(]0,+\infty[,\times)$ to $(]2,+\infty[,*)$.

Assume $\forall x_1,x_2\in]0,+\infty[$, we have

$$\begin{aligned}
f(x_1)=f(x_2) &\Rightarrow \frac{2x_1+1}{x_1}=\frac{2x_2+1}{x_2} \Rightarrow (2x_1+1)x_2=(2x_2+1)x_1\\
&\Rightarrow 2x_1x_2+x_2=2x_2x_1+x_1 \Rightarrow x_1=x_2.
\end{aligned}$$

So, f is injective.

Let us prove that $\forall y\in]2,+\infty[,\exists x\in]0,+\infty[: y=f(x)$, we have

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

As $y\in]2,+\infty[\Rightarrow y-2\neq 0$, Therefore, $x=\frac{1}{y-2}$, hence the surjectivity of f.

So, f is bijective.

Let us show that $f(x\times y)=f(x)*f(y)$. Let's calculate $f(x)*f(y)$, we have

$$\begin{aligned}
f(x)*f(y) &= (f(x)-2)(f(y)-2)+2\\
&= \left(\frac{2x+1}{x}-2\right)\left(\frac{2y+1}{y}-2\right)+2\\
&= \left(\frac{2x+1-2x}{x}\right)\left(\frac{2y+1-2y}{y}\right)+2\\
&= \left(\frac{1}{x}\right)\left(\frac{1}{y}\right)+2\\
&= \frac{1}{xy}+2\\
&= \frac{1+2xy}{xy}\\
&= \frac{2xy+1}{xy}\\
&= f(x\times y).
\end{aligned}$$

So, f is a homomorphism and since it is bijective. Therefore, f is an isomorphism.

Correction of Exercise 3.9 $\forall x,y\in\,]3,+\infty[$, we have

$$\begin{cases} x>3\Rightarrow x-3>0\\ y>3\Rightarrow y-3>0 \end{cases} \Rightarrow (x-3)(y-3)>0. \tag{3.15}$$

Since

$$\begin{aligned}
(x-3)(y-3) &= x(y-3)-3(y-3)\\
&= xy-3x-3y+9\\
&= xy-3x-3y+12-3\\
&= x*y-3.
\end{aligned} \tag{3.16}$$

So, $x*y-3>0\Rightarrow x*y>3$. Thus $*$ is an internal composition law on $]3,+\infty[$.

$\exists e\in\,]3,+\infty[\,,\forall x\in\,]3,+\infty[\,: x*e=e*x=x$

$$x*e=x\Rightarrow xe-3x-3e+12=x$$

$$\Rightarrow (x-3)\,e = 4x-12$$
$$\Rightarrow (x-3)\,e = 4\,(x-3)\,. \tag{3.17}$$

As $x-3\neq 0 \Rightarrow e=\frac{4(x-3)}{x-3}=4\in\,]3,+\infty[$.

$$e*x = x \Rightarrow ex-3e-3x+12 = x$$
$$\Rightarrow e\,(x-3) = 4x-12.$$

Since $x-3\neq 0 \Rightarrow e=\frac{4(x-3)}{x-3}=4\in\,]3,+\infty[$.

from (3.16) and (3.17) we conclude that $e=4$ is the neutral element with respect to $*$.

Does every element of $]3,+\infty[$ have a symmetric element with respect to $*$?

$\forall x\in\,]3,+\infty[\,,\exists x'\in\,]3,+\infty[\,: x*x'=x'*x=e=4$

$$x*x' = 4 \Rightarrow xx'-3x-3x'+12 = 4 \Rightarrow (x-3)\,x' = 3x-8.$$

Since $x-3\neq 0 \Rightarrow x'=\frac{3x-8}{x-3}$. On the other hand, we have

$$\frac{3x-8}{x-3} = \frac{3x-9+1}{x-3} = \frac{3\,(x-3)}{x-3}+\frac{1}{x-3} = 3+\frac{1}{x-3} > 3.$$

Because $x>3$. So, $\frac{1}{x-3}>0$. Thus, $x'\in\,]3,+\infty[$.

$$x'*x = 4 \Rightarrow x'x-3x'-3x+12 = 4 \Rightarrow x'\,(x-3) = 3x-8$$
$$\Rightarrow x' = \frac{3x-8}{x-3}\in\,]3,+\infty[\,.$$

Due to $x\neq 3$ and $\frac{3x-8}{x-3}>3$. So, every element admits a symmetrical element $x'=\frac{3x-8}{x-3}$ with respect to $*$.

Correction of Exercise 3.10 a/ $\forall (x,y),(x',y')\in(\mathbb{R}\setminus\{0\})^2, (x,y)*(x',y')\overset{?}{=}(x',y')*(x,y)$

$$(x,y)*(x',y') = (xx',xy'+x'y) = (x'x,x'y+xy') = (x',y')*(x,y)\,.$$

So, $*$ is commutative.

b/ $\forall (x,y),(x',y'),(x'',y'')\in(\mathbb{R}\setminus\{0\})^2, [(x,y)*(x',y')]*(x'',y'')\overset{?}{=}(x,y)*[(x',y')*(x'',y'')]$

$$\begin{aligned}\left[(x,y)*(x',y')\right]*(x'',y'') &= (xx',xy'+x'y)*(x'',y'')\\ &= \left(xx'x'',xx'y''+x''(xy'+x'y)\right)\\ &= (xx'x'',xx'y''+x''xy'+x''x'y). \end{aligned} \tag{3.18}$$

On the other hand, we have

$$\begin{aligned}(x,y)*\left[(x',y')*(x'',y'')\right] &= (x,y)*(x'x'',x'y''+x''y')\\ &= (xx'x'',x(x'y''+x''y')+x'x''y)\\ &= (xx'x'',xx'y''+xx''y'+x'x''y). \end{aligned} \tag{3.19}$$

Since (3.18) = (3.19), Then $*$ is associative.

c/ $\exists (e,e')\in \mathbb{R}\setminus\{0\}\times\mathbb{R}\setminus\{0\}, \forall (x,y)\in \mathbb{R}\setminus\{0\}\times\mathbb{R}\setminus\{0\} : (x,y)*(e,e') = (e,e')*(x,y) = (x,y)$.

As $*$ is commutative, it suffices to prove that $(x,y)*(e,e') = (x,y)$, we have

$$(x,y)*(e,e') = (xe,xe'+ey) = (x,y)$$

$$\Rightarrow \begin{cases} xe = x \\ \text{and} \\ xe'+ey = y \end{cases}$$

$$\Rightarrow \begin{cases} xe-x = 0 \\ \text{and} \\ xe'+ey-y = 0 \end{cases}$$

$$\Rightarrow \begin{cases} x(e-1) = 0 \\ \text{and} \\ xe'+(e-1)y = 0 \end{cases}$$

$x(e-1)=0 \Rightarrow x=0$ or $e=1$. Since $x\in\mathbb{R}\setminus\{0\} \Rightarrow x\neq 0 \Rightarrow e=1\in\mathbb{R}\setminus\{0\}$.

$xe'+(e-1)y=0 \Rightarrow xe'=0 \Rightarrow e'=0\notin\mathbb{R}\setminus\{0\}$.

So $*$ does not admit a neutral element on $\mathbb{R}\setminus\{0\}\times\mathbb{R}\setminus\{0\}$.

Therefore, $(\mathbb{R}\setminus\{0\}\times\mathbb{R}\setminus\{0\},*)$ cannot have a group structure.

Correction of Exercise 3.11 $*$ commutative $\Leftrightarrow \forall a,b\in\mathbb{R}: a*b=b*a$

$$a*b=a+b+3=b+a+3=b*a.$$

$*$ associative $\Leftrightarrow \forall a,b,c\in\mathbb{R}: (a*b)*c=a*(b*c)$

$$(a*b)*c=(a+b+3)*c=(a+b+3)+c+3=a+b+c+6$$

and

$$a*(b*c)=a*(b+c+3)=a+(b+c+3)+3=a+b+c+6.$$

So, $*$ is associative.

Existence of neutral element $\Leftrightarrow \exists e\in\mathbb{R}\forall a\in\mathbb{R}: a*e=e*a=a$

Since $*$ is commutative, it suffices to prove that $a*e=a$, we have

$$a*e=a\Rightarrow a+e+3=a\Rightarrow e=-3\in\mathbb{R}.$$

Existence of symmetrical element $\Leftrightarrow \forall a\in\mathbb{R},\exists a'\in\mathbb{R}: a*a'=a'*a=e=-3$.

Since $*$ is commutative, it suffices to prove that $a*a'=-3$, we have

$$a*a'=a\Rightarrow a+a'+3=-3\Rightarrow a'=-a-6\in\mathbb{R}.$$

Thus $(\mathbb{R},*)$ is a commutative group.

2/ In order for f to be a morphism, we would need to $f(a*b)=f(a)+f(b)$, hence

$$\begin{aligned} f(a*b)=&f(a)+f(b)\Rightarrow f(a+b+3)=f(a)+f(b)\\ &\Rightarrow\alpha(a+b+3)+\beta=\alpha a+\beta+\alpha b+\beta\\ &\Rightarrow\alpha(a+b)+3\alpha+\beta=\alpha(a+b)+2\beta\\ &\Rightarrow 3\alpha=\beta. \end{aligned}$$

Chapter 4

Concepts of a polynomials with an indeterminate and coefficients in a ring

Let $\mathbb{K}$ be a field ($\mathbb{K}=\mathbb{Q}$ or $\mathbb{K}=\mathbb{R}$ or $\mathbb{K}=\mathbb{C}$).

Definition 4.1. *A polynomial with coefficients in $\mathbb{K}$ is an expression of the form*

$$P(X)=a_nX^n+X_{n-1}X^{n-1}+\ldots+a_1X+a_0,$$

where $n\in\mathbb{N}$ and $\{a_i\}_{i=1,2,\ldots,n}\in\mathbb{K}$ are called coefficients of the polynomial.

Remark 4.1. *The set of polynomials over the field $\mathbb{K}$ is denoted $\mathbb{K}[X]$.*

Definition 4.2. *Let $0\neq P(X)\in\mathbb{K}[X]$. We call the degree of $P(X)$ the largest integer n such that $a_n\neq 0$, we denote it $\deg(P)$, and the element $a_{\deg(P)}$ is called the dominant coefficient of P.*

Remark 4.2. *Conventionally, the degree of the zero polynomial is $a_{\deg(P=0)}=-\infty$.*

Definition 4.3. *Let $0\neq P(X)\in\mathbb{K}[X]$. We say that P is unitary (normalized), if and only if $a_{\deg(P)}=1$.*

Definition 4.4. *A polynomial with an indeterminate value with coefficients in $\mathbb{K}[X]$ is any polynomial whose coefficients are zero from a certain rank.*

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

Consider the two polynomials $P(X)=a_nX^n+X_{n-1}X^{n-1}+\ldots+a_1X+a_0=\sum_{i=0}^{n}a_iX^i$ and

$Q(X)=b_nX^n+b_{n-1}X^{n-1}+\ldots+b_1X+b_0=\sum_{l=0}^{n}b_jX^j$.

The following is how we define addition, polynomial product, and multiplication by a scalar $\lambda \in \mathbb{K}$.

- $(P+Q)(X) = \sum_{i=0}^{n} c_i X^i$ where $c_i = a_i + b_i$.
- $(PQ)(X) = \sum_{k=0}^{2n} v_k X^k$ where $v_k = \sum_{k=0}^{n} a_k b_{n-k}$.
- $(\lambda P)(X) = \sum_{i=0}^{n} \lambda a_i X^i$.
- $P(X) = Q(X) \Leftrightarrow \forall i \in \mathbb{N}, a_i = b_i$.

Definition 4.5. *The addition and multiplication previously described define internal composition laws on the set of polynomials with one indeterminate and coefficients in* $\mathbb{K}$.

Definition 4.6. *The set of one-indeterminate polynomials with coefficients in* $\mathbb{K}$ *equipped with addition and multiplication defines a commutative ring structure that we denote by* $\mathbb{K}[X]$.

4.2 Arithmetic of polynomials

Definition 4.7. *Let* P *and* Q *be two polynomials of* $\mathbb{K}[X]$. *We say that the polynomial* P *is divisible by the polynomial* Q *if there exists a polynomial* A *such that* $P = QA$ *and we denote* $Q \backslash P$ *and we say that* P *is a multiple of* Q *(or* Q *is a divisor of* P*).*

Proposition 4.1. *Let* $P, Q, R \in \mathbb{K}[X]$. *We have*

- $P \backslash Q$ *and* $Q \backslash P \Rightarrow \exists \lambda \in \mathbb{K} : P = \lambda Q$.
- $P \backslash Q$ *and* $Q \backslash R \Rightarrow P \backslash R$.
- $P \backslash Q$ *and* $P \backslash R \Rightarrow P \backslash (\lambda Q + \mu R)$ *where* $\lambda, \mu \in \mathbb{K}$.
- $P \backslash P, 1 \backslash P$ *and* $P \backslash 0$. *But* $0 \backslash P$ *is never true.*

4.2.1 Euclidian division on $\mathbb{K}[X]$

Let P and Q be two polynomials of $\mathbb{K}[X]$ and $Q \neq 0$, then there exists a unique pair (D, R) ofe $\mathbb{K}[X] \times \mathbb{K}[X]$ shuch that

$$P = DQ + R \text{ with } 0 \leq \deg(R) < \deg(Q).$$

Greatest Common Divisor (gcd)

Definition 4.8. *Let $P,Q \in \mathbb{K}[X]$, with $P \neq 0$ or $Q \neq 0$. There exists a unique unitary polynomial that divides both P and Q. This polynomial is called the* gcd *and is denoted* $\gcd(P,Q)$.

Proposition 4.2. *Let $P,Q \in \mathbb{K}[X]$, with $P \neq 0$ or $Q \neq 0$. Then*

- $A \backslash P$ *and* $A \backslash Q \Rightarrow A \backslash \gcd(P,Q)$.
- $\gcd(\alpha P, \alpha Q) = \alpha \gcd(P,Q)$.

Definition 4.9. *Let $P,Q \in \mathbb{K}[X]$. We say that P and Q are coprime if and only if* $\gcd(P,Q) = 1$.

Theorem 4.1. *[Bézout's Theorem] Let $P,Q \in \mathbb{K}[X]$ be polynomials with $P \neq 0$ or $Q \neq 0$ and $D = \gcd(P,Q)$. There exist two polynomials $\varphi, \xi \in \mathbb{K}[X]$ shuch that $\varphi P + \xi Q = D$.*

Root of a polynomial - Factorization

Definition 4.10. *Let $P \in \mathbb{K}[X]$ and $\alpha \in \mathbb{K}$. We say that α is a root of P, if $P(\alpha) = 0$.*

Theorem 4.2. *[d'Alembert-Gauss Theorem] Any polynomial with complex coefficients of degree $m \geq 1$ has m roots, including their multiplicities, at least one of which is in $\mathbb{C}$.*

Proposition 4.3. $P(\alpha) = 0 \Leftrightarrow (x-\alpha) \backslash P$.

Definition 4.11. *Let $m \in \mathbb{N} \backslash \{0\}$. We say that α is a root of multiplicity m of P if $(X-\alpha)^m \backslash P$ while $(X-\alpha)^{m+1}$ does not divide P.*

Remark 4.3. *When $m = 1$, α is said to be a simple root. If $m > 1$, α is said to be a root of order m.*

Proposition 4.4. *Let $P \in \mathbb{K}[X]$ and $\alpha \in \mathbb{K}$ be such that α is a root of order $m \in \mathbb{N} \backslash \{0,1\}$, the following assertions are equivalent*

- $\exists Q \in \mathbb{K}[X] : P = (X-\alpha)^m Q$ *with* $Q(\alpha) \neq 0$.
- $P(\alpha) = 0, P'(\alpha) = 0, \ldots, P^{(m-1)}(\alpha) = 0$ *and* $P^{(m)}(\alpha) \neq 0$ *where $P^{(i)}$ is the i^{th} order derivative of P.*

4.3 Concept of a rational fraction with an indeterminate

We denote by $\mathbb{K}[X]^*$ the set of non-zero polynomials i.e. $\mathbb{K}[X]^* = \mathbb{K}[X] \setminus \{0_{\mathbb{K}[X]}\}$ and we consider the equivalence relation $\mathscr{R}$ on $\mathbb{K}[X] \times \mathbb{K}[X]^*$, defined as follows

$$\forall (P,Q),(A,B) \in \mathbb{K}[X] \times \mathbb{K}[X]^*, (P,Q)\mathscr{R}(A,B) \Leftrightarrow P \times B = Q \times A.$$

Definition 4.12. *The equivalence class of* $(P,Q) \in \mathbb{K}[X] \times \mathbb{K}[X]^*$ *is called a rational fraction over* $\mathbb{K}$*, and is denoted* P/Q *or* $\frac{P}{Q}$ *i.e.*

$$\frac{P}{Q} = \left\{(A,B) \in \mathbb{K}[X] \times \mathbb{K}[X]^* : P \times B = Q \times A\right\}.$$

Remark 4.4. *We note by* $\mathbb{K}(X) = \mathbb{K}[X] \times \mathbb{K}[X]^* / \mathscr{R} = \left\{\frac{A}{B} : (A,B) \in \mathbb{K}[X] \times \mathbb{K}[X]^*\right\}$.

Definition 4.13. *We call irreducible form of a non-zero rational fraction* P *of* $\mathbb{K}(X)$ *any pair* $(A,B) \in \mathbb{K}[X]^* \times \mathbb{K}[X]^*$ *such that* $\gcd(A,B) = 1_{\mathbb{K}[X]}$.

4.3.1 Operations on $\mathbb{K}(X)$

The set $\mathbb{K}(X)$ equipped with the following two internal composition laws:

$\forall \frac{P}{Q}, \frac{A}{B} \in \mathbb{K}(X), \frac{P}{Q} + \frac{A}{B} = \frac{P \times B + Q \times A}{Q \times B}$ and $\frac{P}{Q} \times \frac{A}{B} = \frac{P \times A}{Q \times B}$ has a commutative field structure.

Canonical Injection of $\mathbb{K}[X]$ into $\mathbb{K}(X)$

Examine the map $\mathscr{J} : \mathbb{K}[X] \to \mathbb{K}(X)$, which links each polynomial $\frac{P}{1_{\mathbb{K}[X]}}$ to the rational fraction P of $\mathbb{K}[X]$. The injective nature of $\mathscr{J}$ is readily demonstrated. $\mathbb{K}[X] \subset \mathbb{K}(X)$ is the result of identifying the elements of $\mathbb{K}[X]$ with the elements of $\mathbb{K}(X)$.

Remark 4.5. $\mathscr{J}$ *is called canonical injection.*

Roots and poles of a rational fraction

Definition 4.14. *Consider the irreducible rational fraction* $\mathscr{F} = \frac{P}{Q} \in \mathbb{K}(X)^*$.

- *The roots of* $\mathscr{F}$ *are the zeros of* P *in* $\mathbb{K}[X]$.

- *The order of multiplicity of the root α of $\mathscr{F}$ is the same when considering it as a root of P in $\mathbb{K}[X]$.*
- *The poles of $\mathscr{F}$ are the zeros of Q in $\mathbb{K}[X]$.*
- *The order of multiplicity of the pole α of $\mathscr{F}$ is the same when considering it as a root of Q in $\mathbb{K}[X]$.*

Definition 4.15. *Let $\mathscr{F} = \frac{P}{Q} \in \mathbb{K}(X)$ be a rational fraction. Any function $\widetilde{\mathscr{F}} : \mathbb{K} \to \mathbb{K}$ defined for any x differing from the poles of $\mathscr{F}$ is referred to as a function associated with $\mathscr{F}$. For example, the application $\widetilde{\mathscr{F}}(x) = \frac{\widetilde{P}(x)}{\widetilde{Q}(x)}$.*

4.3.2 Decomposition of a rational fraction

Consider the irreducible rational fraction $\mathscr{F} = \frac{P}{Q} \in \mathbb{K}(X)$. By means of Euclidean division in $\mathbb{K}[X]$, we have the existence and uniqueness of two polynomials D and R in $\mathbb{K}[X]$ such that

$$P = D \times Q + R \text{ with } \deg(R) < \deg(Q).$$

And by injecting rational fractions into the field $\mathbb{K}(X)$, we get

$$\frac{P}{Q} = \frac{D}{1_{\mathbb{K}[X]}} + \frac{R}{Q}.$$

Remark 4.6. *D is said to be the integer part of the rational fraction $\frac{P}{Q}$ and is equal to zero if $\deg(P) < \deg(Q)$.*

Simple elemental factorization on $\mathbb{K}$

Lemma 4.1. *Consider the rational fraction $\mathscr{F} = \frac{P}{Q} = \frac{D}{1_{\mathbb{K}[X]}} + \frac{R}{Q}$ where $\frac{R}{Q}$ is irreducible and $\deg(R) < \deg(Q)$, Let us also assume that Q is decomposable into prime factors of $\mathbb{K}[X]$ i.e. $Q = Q_1^{n_1} \times Q_2^{n_2} \times \ldots \times Q_k^{n_k}$. Then there exist k polynomials $L_1, L_2, \ldots, L_k \in \mathbb{K}[X]$ shuch that*

$$\frac{R}{Q} = \frac{L_1}{Q_1^{n_1}} + \frac{L_2}{Q_2^{n_2}} + \ldots + \frac{L_k}{Q_k^{n_k}} \text{ with } \deg(L_i) < \deg(Q_i), \text{ for } i = 1 \text{ to } k.$$

This decomposition is unique.

Lemma 4.2. *Consider the irreducible rational fraction* $\mathscr{F} = \frac{L}{Q^n}$ *with* $\deg(L) < \deg(Q^n)$. *Then there exist* n *polynomials* $S_1, S_2, \ldots, S_n \in \mathbb{K}[X]$:

$$\frac{L}{Q^n} = \frac{S_1}{Q} + \frac{S_2}{Q^2} + \ldots + \frac{S_n}{Q^n} \text{ with } \deg(S_i) < \deg(Q) \text{ for } i = 1, 2, \ldots, n.$$

This decomposition is unique.

Remark 4.7. *In the general framework, the two previous lemmas can be combined when decomposing any rational fraction if necessary.*

Remark 4.8. *The part* $\frac{S_1}{Q} + \frac{S_2}{Q^2} + \ldots + \frac{S_n}{Q^n}$ *is called the relative part of the polynomial* L.

Remark 4.9. *In the case where* $Q = X - \alpha$, *the partial sum is called the polar part relative to* α.

Remark 4.10. *In the case where* $Q = X - \alpha$, *we speak of the decomposition into a simple element of the first kind. On the other hand, if* $Q = aX^2 + bX + c$, *we speak of the decomposition into a simple element of the second kind.*

4.4 Fourth Chapter's exercises

Exercise 4.1. *Factorize X^4-1, then X^8-1 into a product of irreducible polynomials in $\mathbb{R}[X]$, and then in $\mathbb{C}[X]$.*

Exercise 4.2. *Consider the fraction $\frac{P}{Q}$, where*

$$P(X)=3X^4+5X^3+11X^2+5X+3 \text{ and } Q(X)=\left(X^2+X+1\right)^2(X-1).$$

- *Decompose $\frac{P}{Q}$ into simple elements in $\mathbb{R}[X]$.*
- *Decompose $\frac{P}{Q}$ into simple elements in $\mathbb{C}[X]$.*

Exercise 4.3. *Let $P\in\mathbb{R}[X]$. If $\alpha\in\mathbb{C}$ is a root of P of order m, then $\overline{\alpha}\in\mathbb{C}$ is also a root of P of order m.*

Exercise 4.4. *Consider the following polynomials*

$$P(X)=X^5+3X^4+2X^3-X^2-3X-2 \text{ and } Q(X)=X^4+2X^3+2X^2+7X+6.$$

- *Calculate $D=\gcd(P,Q)$.*
- *Find polynomials U and V such that $D=UP+VQ$.*

Exercise 4.5. *Consider the two polynomials*

$$P(X)=X^5-2X^3+4X^2-8X+11 \text{ and } Q(X)=X^3-3X+2.$$

- *Determine a greatest common divisor of P and Q.*
- *Are P and Q relatively prime?*
- *Show that 1 is a double root of Q.*
- *Decompose the fraction $\frac{P}{Q}$ in $\mathbb{R}[X]$.*

Exercise 4.6. *Consider the polynomial*

$$P(X)=X^5-2X^4-6X^3+20X^2-19X+6.$$

- *Show that* 2 *is a root of* $P(X)$.
- *Show that* 1 *is a triple root of* $P(X)$.
- *Factor the polynomial* P *into a product of irreducible polynomials in* $\mathbb{R}[X]$.

Exercise 4.7. *Consider the two polynomials*

$$P(X) = X^5 - 3X^4 + X^3 + X^2 + 5 \text{ and } Q(X) = X^3 - 3X^2 + 4.$$

- *Determine the greatest common divisor of* P *and* Q.
- *Are* P *and* Q *relatively prime?*
- *Show that* 2 *is a double root of* Q.
- *Decompose the fraction* $\frac{P(X)+1}{Q(X)}$ *in* $\mathbb{R}[X]$.

4.5 Corrections of fourth chapter exercises

Correction of Exercise 4.1 In $\mathbb{R}[X]$

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

$$\begin{aligned} X^8-1 &= \left(X^4-1\right)\left(X^4+1\right) \\ &= (X-1)(X+1)\left(X^2+1\right)\left(X^4+1\right) \\ &= (X-1)(X+1)\left(X^2+1\right)\left(X^2+\sqrt{2}X+1\right)\left(X^2-\sqrt{2}X+1\right), \end{aligned}$$

where we have used the fact that

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

In $\mathbb{C}[X]$

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

$$\begin{aligned} X^8-1 &= \left(X^4-1\right)\left(X^4+1\right) \\ &= (X-1)(X+1)(X-i)(X+i)\left(X^4+1\right). \end{aligned}$$

We have $X^4+1=0 \Rightarrow X^4=-1 \overset{Euler}{\Rightarrow} X^4=e^{i\pi+2k\pi} \Rightarrow X=e^{i\frac{\pi}{4}+\frac{k\pi}{2}}$ where $k=0$ to 3

$$\begin{aligned} X^8-1 =& (X-1)(X+1)(X-i)(X+i) \\ &\times\left(X-e^{i\frac{\pi}{4}}\right)\left(X-e^{i\frac{\pi}{4}+\frac{\pi}{2}}\right)\left(X-e^{i\frac{\pi}{4}+\pi}\right)\left(X-e^{i\frac{\pi}{4}+\frac{3\pi}{2}}\right) \\ =& (X-1)(X+1)(X-i)(X+i)\left(X-\tfrac{\sqrt{2}}{2}-i\tfrac{\sqrt{2}}{2}\right) \end{aligned}$$

$$\times \left(X+\tfrac{\sqrt{2}}{2}-i\tfrac{\sqrt{2}}{2}\right)\left(X+\tfrac{\sqrt{2}}{2}+i\tfrac{\sqrt{2}}{2}\right)\left(X-\tfrac{\sqrt{2}}{2}+i\tfrac{\sqrt{2}}{2}\right).$$

Correction of Exercise 4.2

$$\frac{P}{Q}=\frac{3X^4+5X^3+11X^2+5X+3}{(X^2+X+1)^2(X-1)}$$

Since the degree of Q is greater than the degree of P, we bypass the Euclidean division and go straight to the decomposition.

Consequently, the decomposition into simple components in $\mathbb{R}[X]$ is

$$\frac{3X^4+5X^3+11X^2+5X+3}{(X^2+X+1)^2(X-1)}=\frac{a}{(X-1)}+\frac{\alpha X+\beta}{(X^2+X+1)}+\frac{\gamma X+\delta}{(X^2+X+1)^2} \tag{4.1}$$

Multiplying both sides of (4.1) by $(X-1)$, then replacing X by 1 in the resulting equation, we find $a=\frac{27}{9}=3$.

Multiplying both sides of (4.1) by X, and then making X tend towards ∞ in the resulting equation, we find $3=a+\alpha \Rightarrow \alpha=0$.

Replacing X by 0 in (4.1), we get $-3=-a+\beta+\delta \Rightarrow \beta+\delta=0 \Rightarrow \beta=-\delta$. Therefore, (4.1) becomes

$$\frac{3X^4+5X^3+11X^2+5X+3}{(X^2+X+1)^2(X-1)}=\frac{3}{(X-1)}-\frac{\delta}{(X^2+X+1)}+\frac{\gamma X+\delta}{(X^2+X+1)^2} \tag{4.2}$$

Replacing X by -1 in (4.2), we get $-\frac{7}{2}=-\frac{3}{2}-\gamma \Rightarrow \gamma=\frac{7}{2}-\frac{3}{2} \Rightarrow \gamma=2$.

Replacing X by 2 in (4.2), we get $\frac{145}{49}=3-\frac{\delta}{7}+\frac{4+\delta}{49} \Rightarrow 145=147-7\delta+4+\delta \Rightarrow -6=-6\delta \Rightarrow \delta=1$.

Thus, we obtain

$$\frac{3X^4+5X^3+11X^2+5X+3}{(X^2+X+1)^2(X-1)}=\frac{3}{X-1}-\frac{1}{X^2+X+1}+\frac{2X+1}{(X^2+X+1)^2}. \tag{4.3}$$

Concerning the decomposition in $\mathbb{C}[X]$ we must first factorize the polynomial X^2+X+1, we get

$$X^2+X+1=\left(X+\tfrac{1}{2}-i\tfrac{\sqrt{3}}{2}\right)\left(X+\tfrac{1}{2}+i\tfrac{\sqrt{3}}{2}\right). \tag{4.4}$$

Substituting (4.4) into (4.3), we obtain

$$\frac{3X^4+5X^3+11X^2+5X+3}{(X^2+X+1)^2(X-1)} = \frac{3}{X-1} - \frac{1}{\left(X+\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)\left(X+\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)} + \frac{2X+1}{\left(X+\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)^2\left(X+\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)^2}. \tag{4.5}$$

So,

$$\begin{aligned}\frac{3X^4+5X^3+11X^2+5X+3}{(X^2+X+1)^2(X-1)} =& \frac{3}{X-1} + \frac{k}{\left(X+\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)} + \frac{v}{\left(X+\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)^2} \\ &+ \frac{u}{\left(X+\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)} + \frac{w}{\left(X+\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)^2}.\end{aligned}$$

Therefore,

$$\frac{X-X^2}{\left(X+\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)^2\left(X+\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)^2} = \frac{k}{\left(X+\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)} + \frac{v}{\left(X+\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)^2} + \frac{u}{\left(X+\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)} + \frac{w}{\left(X+\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)^2}. \tag{4.6}$$

Multiplying both sides of (4.6) by $\left(X+\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)^2$, and then replacing X by $\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)$ in the resulting equation,

we find $v=-\frac{i\sqrt{3}}{3}$.

Multiplying both sides of (4.6) by $\left(X+\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)^2$, and then replacing X by $\left(-\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)$ in the resulting equation,

we find $w=\frac{i\sqrt{3}}{3}$.

Multiplying both sides of (4.6) by $\left(X+\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)$, and then making X tend towards ∞ in the resulting equation, we find

$k+u=0 \Rightarrow u=-k$

Replacing X by 0 in (4.6), we get $k\left(\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)+u\left(\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)=-1 \Rightarrow k=-\frac{1}{i\sqrt{3}} \Rightarrow k=\frac{i\sqrt{3}}{3} \Rightarrow u=-\frac{i\sqrt{3}}{3}$.

Thus, we obtain

$$\frac{3X^4+5X^3+11X^2+5X+3}{(X^2+X+1)^2(X-1)} = \frac{3}{X-1} + \frac{\frac{i\sqrt{3}}{3}}{X+\frac{1}{2}-i\frac{\sqrt{3}}{2}} - \frac{\frac{i\sqrt{3}}{3}}{\left(X+\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)^2} - \frac{\frac{i\sqrt{3}}{3}}{X+\frac{1}{2}+i\frac{\sqrt{3}}{2}} + \frac{\frac{i\sqrt{3}}{3}}{\left(X+\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)^2}.$$

Correction of Exercise 4.3 $P \in \mathbb{R}[X] \Rightarrow \exists a_i \in \mathbb{R} : P(X) = \sum_{i\geq 0} a_i X^i$. It is clear that the successive derivatives of P are

$$\begin{cases} P(X) = \sum_{i\geq 0} a_i X^i \\ P'(X) = \sum_{i\geq 1} i a_i X^{i-1} \\ \vdots \\ P^{(m)}(X) = \sum_{i\geq m} i(i-1)\cdots(x-m+1)\, a_i X^{i-m} \\ P^{(m+1)}(X) = \sum_{i\geq m+1} i(i-1)\cdots(x-m)\, a_i X^{i-m-1} \end{cases}.$$

As $\xi \in \mathbb{C}$ is a root of order of multiplicity m of P, we have

$$\begin{cases} P(\xi) = \sum_{i\geq 0} a_i^i \xi = 0 \\ P'(\xi) = \sum_{i\geq 1} i a_i^{i-1} \xi = 0 \\ \vdots \\ P^{(m)}(\xi) = \sum_{i\geq m} i(i-1)\cdots(x-m+1)\, a_i \xi^{i-m} = 0 \\ P^{(m+1)}(\xi) = \sum_{i\geq m+1} i(i-1)\cdots(x-m)\, a_i \xi^{i-m-1} \neq 0. \end{cases}$$

According to the properties of the conjugate and the preceding system and taking into account the fact that the $a_i \in \mathbb{R}$ i.e. $\overline{a_i} = a_i$, we get

$$\begin{cases} \overline{\sum_{i\geq 0} a_i \xi^i} = \sum_{i\geq 0} \overline{a_i} \left(\overline{\xi}\right)^i = \underbrace{\sum_{i\geq 0} a_i \left(\overline{\xi}\right)^i}_{} = P\left(\overline{\xi}\right) = 0 \\ \sum_{i\geq 1} i\overline{a_i} \left(\overline{\xi}\right)^{i-1} = \sum_{i\geq 1} i a_i \underbrace{\left(\overline{\xi}\right)^{i-1}}_{} = P'\left(\overline{\xi}\right) = 0 \\ \vdots \\ \sum_{i\geq m} i(i-1)\cdots(x-m+1)\,\overline{a_i} \left(\overline{\xi}\right)^{i-m} = \sum_{i\geq m} i(i-1)\cdots(x-m+1)\, a_i \left(\overline{\xi}\right)^{i-m} = P^{(m)}\left(\overline{\xi}\right) = 0 \\ \sum_{i\geq m+1} i(i-1)\cdots(x-m)\,\overline{a_i} \left(\overline{\xi}\right)^{i-m-1} = \sum_{i\geq m+1} i(i-1)\cdots(x-m)\, a_i \left(\overline{\xi}\right)^{i-m-1} = P^{(m+1)}\left(\overline{\xi}\right) \neq 0. \end{cases}$$

Thus, $\overline{\xi} \in \mathbb{C}$ is also a root of order of multiplicity m of P.

Correction of Exercise 4.4

$$X^5+3X^4+2X^3-X^2-3X-2 = \left(X^4+2X^3+2X^2+7X+6\right)\cdot\left(X+1\right)+\left(-2X^3-10X^2-16X-8\right)$$
$$X^4+2X^3+2X^2+7X+6 = \left(-2X^3-10X^2-16X-8\right)\cdot\left(-\tfrac{1}{2}X+\tfrac{3}{2}\right)+\left(9X^2+27X+18\right)$$
$$-2X^3-10X^2-16X-8 = \left(9X^2+27X+18\right)\cdot\left(-\tfrac{2}{9}X-\tfrac{4}{9}\right)+0$$

So, $\gcd(P,Q) = 9X^2+27X+18$.

$$X^4+2X^3+2X^2+7X+6 = \left(-2X^3-10X^2-16X-8\right)\left(-\tfrac{1}{2}X+\tfrac{3}{2}\right)+\left(9X^2+27X+18\right)$$
$$X^5+3X^4+2X^3-X^2-3X-2 = \left(X^4+2X^3+2X^2+7X+6\right)(X+1)+\left(-2X^3-10X^2-16X-8\right)$$

$$\begin{cases} X^4+2X^3+2X^2+7X+6 \\ = \left(-2X^3-10X^2-16X-8\right)\left(-\tfrac{1}{2}X+\tfrac{3}{2}\right)+\left(9X^2+27X+18\right), \\ X^5+3X^4+2X^3-X^2-3X-2 \\ = \left(X^4+2X^3+2X^2+7X+6\right)(X+1)+\left(-2X^3-10X^2-16X-8\right), \end{cases} \Rightarrow$$

$$\begin{cases} 9X^2+27X+18 \\ = \left(X^4+2X^3+{}^2+7X+6\right)-\left(-2X^3-10X^2-16X-8\right)\left(-\tfrac{1}{2}X+\tfrac{3}{2}\right), \\ \left(-2X^3-10X^2-16X-8\right) \\ = \left(X^5+3X^4+2X^3-X^2-3X-2\right)-\left(X^4+2X^3+2X^2+7X+6\right)(X+1), \end{cases} \Rightarrow$$

$$\begin{cases} 9X^2+27X+18 \\ = \left(X^5+3X^4+2X^3-X^2-3X-2\right)\left(\tfrac{1}{2}X-\tfrac{3}{2}\right) \\ +\left(X^4+2X^3+2X^2+7X+6\right)\left(-\tfrac{1}{2}X^2+X+\tfrac{5}{2}\right), \\ -2X^3-10X^2-16X-8 \\ = \left(X^5+3X^4+2X^3-X^2-3X-2\right)-\left(X^4+2X^3+2X^2+7X+6\right)(X+1). \end{cases}$$

Thus, $D = \left(\tfrac{1}{2}X-\tfrac{3}{2}\right)P+\left(-\tfrac{1}{2}X^2+X+\tfrac{5}{2}\right)Q \Rightarrow U = \left(\tfrac{1}{2}X-\tfrac{3}{2}\right)$ and $V = \left(-\tfrac{1}{2}X^2+X+\tfrac{5}{2}\right)$.

Correction of Exercise 4.5

$$
\begin{aligned}
X^5-2X^3+4X^2-8X+11 &= \left(X^3-3X+2\right)\cdot\left(X^2+1\right)+\left(2X^2-5X+9\right),\\
X^3-3X+2 &= \left(2X^2-5X+9\right)\cdot\left(\tfrac{1}{2}X+\tfrac{5}{4}\right)+\left(-\tfrac{5}{4}X-\tfrac{37}{4}\right)\\
2X^2-5X+9 &= \left(-\tfrac{5}{4}X-\tfrac{37}{4}\right)\cdot\left(-\tfrac{8}{5}X+\tfrac{396}{25}\right)+\tfrac{3888}{25}\\
-\tfrac{5}{4}X-\tfrac{37}{4} &= \tfrac{3888}{25}\cdot\left(-\tfrac{125}{15552}X-\tfrac{925}{15552}\right)+0
\end{aligned}
$$

where the Euclidian division was done as follows

$$
\begin{array}{rl}
 & X^2 \quad +1\\
\hline
X^3-3X+2) & X^5-2X^3+4X^2-8X+11\\
 & -X^5+3X^3-2X^2\\
\hline
 & X^3+2X^2-8X+11\\
 & -X^3 \quad +3X \quad -2\\
\hline
 & 2X^2-5X \quad +9
\end{array}
$$

$$
\begin{array}{rl}
 & \tfrac{1}{2}X \quad +\tfrac{5}{4}\\
\hline
2X^2-5X+9) & X^3 \quad -3X \quad +2\\
 & -X^3+\tfrac{5}{2}X^2 \quad -\tfrac{9}{2}X\\
\hline
 & \tfrac{5}{2}X^2-\tfrac{15}{2}X \quad +2\\
 & -\tfrac{5}{2}X^2+\tfrac{25}{4}X-\tfrac{45}{4}\\
\hline
 & -\tfrac{5}{4}X-\tfrac{37}{4}
\end{array}
$$

$$
\begin{array}{rl}
 & -\tfrac{8}{5}X \quad +\tfrac{396}{25}\\
\hline
-\tfrac{5}{4}X-\tfrac{37}{4}) & 2X^2 \quad -5X \quad +9\\
 & -2X^2-\tfrac{74}{5}X\\
\hline
 & -\tfrac{99}{5}X \quad +9\\
 & \tfrac{99}{5}X+\tfrac{3663}{25}\\
\hline
 & \tfrac{3888}{25}
\end{array}
$$

$$
\begin{array}{r|l}
 & -\frac{125}{15552}X-\frac{925}{15552} \\
\hline
\frac{3888}{25}) \quad -\frac{5}{4}X \quad -\frac{37}{4} & \\
\underline{\quad \frac{5}{4}X \quad\quad} & \\
 & -\frac{37}{4} \\
 & \underline{\quad \frac{37}{4} \quad} \\
 & 0
\end{array}
$$

So, $\gcd(P,Q) = cte \Rightarrow P$ and Q are coprime.

$Q(1) = 1^3 - 3\times 1 + 2 = 0$. Moreover

$Q'(X) = 3X^2 - 3 \Rightarrow Q'(1) = 3 - 3 = 0$ and $Q''(X) = 6X \Rightarrow Q''(1) = 6 \neq 0$.

Since 1 cancels Q and Q', however, it does not cancel Q'', therefore $X = 1$ is a double root.

$$
\begin{aligned}
\frac{P}{Q} =& \frac{X^5 - 2X^3 + 4X^2 - 8X + 11}{X^3 - 3X + 2} \\
=& \frac{\left(X^3 - 3X + 2\right)\left(X^2 + 1\right) + 2X^2 - 5X + 9}{X^3 - 3X + 2} \\
=& X^2 + 1 + \frac{2X^2 - 5X + 9}{X^3 - 3X + 2} \\
=& X^2 + 1 + \frac{2X^2 - 5X + 9}{(X-1)^2(X+2)},
\end{aligned} \tag{4.7}
$$

because $X = 1$ is a double root of $Q(X)$ which is a polynomial of degree 3, and since the product of its roots $= -2$, therefore the third root $= 3$. On the other hand, we have

$$
\frac{2X^2 - 5X + 9}{(X-1)^2(X+2)} = \frac{a}{X-1} + \frac{b}{(X-1)^2} + \frac{c}{X+2}. \tag{4.8}
$$

Multiplying both sides of (4.2) by $(X-1)^2$ and then replacing X by 1 in the resulting equation, we find $b = 2$.

Multiplying both sides of (4.2) by $(X+2)$ and then replacing X by -2 in the resulting equation, we find $c = 3$.

Now, multiplying both sides of (4.2) by $(X-1)$ and then letting X tend to ∞ in the resulting equation, we find $2 = a + c = a + 3 \Rightarrow a = -1$.

Thus, we obtain

$$\frac{2X^2-5X+9}{(X-1)^2(X+2)} = -\frac{1}{X-1}+\frac{2}{(X-1)^2}+\frac{3}{X+2}. \tag{4.9}$$

Substituting (4.3) into (4.1), we get

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

Correction of Exercise 4.6 1/ $P(2) = 2^5-2(2)^4-6(2)^3+20(2)^2-19(2)+6 = 32-32-48+80-38+6 = 0$.

2/ $P(1) = 1^5-2(1)^4-6(1)^3+20(1)^2-19(1)+6 = 1-2-6+20-19+6 = 0$,

$P'(X) = 5X^4-8X^3-18X^2+40X-19$

$\Rightarrow P'(1) = 5(1)^4-8(1)^3-18(1)^2+40(1)-19 = 0$.

$P''(X) = 20X^3-24X^2-36X+40 \Rightarrow P''(1) = 20(1)^3-24(1)^2-36(1)+40 = 0$.

$P'''(X) = 60X^2-48X-36 \Rightarrow P'''(1) = 60(1)^2-48(1)-36 = -24 \neq 0$.

Since 1 cancels P, P', P'' and does not cancel P''', therefore 1 is a triple root of P.

3/ Since P is a polynomial of order 5, it admits at most 5 roots including their multiplicities, since 1 is a triple root and 2 is another root, so we still need to determine a final root. Since the product of the roots is equal to $(-1)\frac{a_5}{a_0}$, then $2X_5 = -6$. Hence $X_5 = -3$, because $X_1 = X_2 = X_3 = 1$ and $X_4 = 2$. So, we have

$$P(X) = X^5-2X^4-6X^3+20X^2-19X+6 = (X-1)^3(X-2)(X+3).$$

Correction of Exercise 4.7

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

$Q(X) = (X+1)\left(X^2-4\right)+1$.

So, the $\gcd(P,Q) = 1$. Thus P and Q are coprime.

$Q(2) = (2)^3 - 3(2)^2 + 4 = 8 - 12 + 4 = 0 \Rightarrow 2$ is root of $Q(X)$.

We have $Q'(X) = 3X^2 - 6X \Rightarrow Q'(2) = 3(2)^2 - 6(2) = 0$.

Moreover, $Q''(X) = 6X - 6 \Rightarrow Q''(2) = 6 \times 2 - 6 = 6 \neq 0$.

So, 2 is the double root of $Q(X)$.

Hence, $Q(X) = (X+1)(X-2)^2$.

Thus,

$$\begin{aligned}\frac{P+1}{Q} =& \frac{Q(X) \times \left(X^2+1\right)+2}{Q(X)} = X^2 + 1 + \frac{2}{Q(X)} \\ =& X^2 + 1 + \frac{2}{X^3 - 3X^2 + 4} \\ =& X^2 + 1 + \frac{2}{(X+1)(X-2)^2}. \end{aligned} \tag{4.10}$$

On the other hand, we want to rewrite (4.10) in the form

$$\frac{2}{(X+1)(X-2)^2} = \frac{a}{X+1} + \frac{b}{X-2} + \frac{c}{(X-2)^2}. \tag{4.11}$$

Multiplying both sides of (4.11) by $(X+1)$, then replacing X by -1, we find $a = \frac{2}{9}$.

Multiplying both sides of (4.11) by $(X-2)^2$, then replacing X by 2, we find $c = -2$.

Multiplying both sides of (4.11) by $(X-2)$, then making X tend towards ∞,

we obtain $\underbrace{\lim_{x\to\infty} \frac{2}{(X+1)(X-2)}}_{0} = \underbrace{\lim_{x\to\infty} \left(\frac{a(X-2)}{X+1} + b + \frac{c}{(X-2)} \right)}_{a+b} \Rightarrow b = -a.$

So, we get

$$\frac{P+1}{Q} = X^2 + 1 + \frac{1}{9(X+1)} - \frac{1}{9(X-2)} - \frac{2}{(X-2)^2}.$$

Bibliography

[1] F. Ayres and R. J. Lloyd, Theory and problems of abstract algebra. Schaum's outline, 2^{nd} Edition. The McGraw-Hill. (2004).

[2] É. Azoulay and J. Avignant, Mathématiques. 4 Algèbre. MacGraw-Hill. (1984).

[3] C. Baba-Hamed and K. Benhabib, Algèbre I Rappels de Cours et Exercices avec Solutions, Office des publications universitaires, E. (1988).

[4] S. Balac and F. Sturm, Algèbre et analyse: cours de mathématiques de première année avec exercices corrigés. EPFL Press. (2003).

[5] B. Calvo, J. Doyen , A. Calvo and F. Boschet, Exercices d'algèbre, 1er cycle scientifique, 1er année préparation aux grandes écoles. Librairie Armand Colin, Paris 1971.

[6] X. Gourdon, Les Maths en tête: mathématiques pour M': algèbre. Ellipses-Marketing. (2009).

[7] J. P. Marco and L. Lazzarini, Mathématiques L1: Cours complet avec 1 000 tests et exercices corrigés. Pearson Education France. (2012).