Foundations of Mathematics

Abdulqader O. Hamadameen

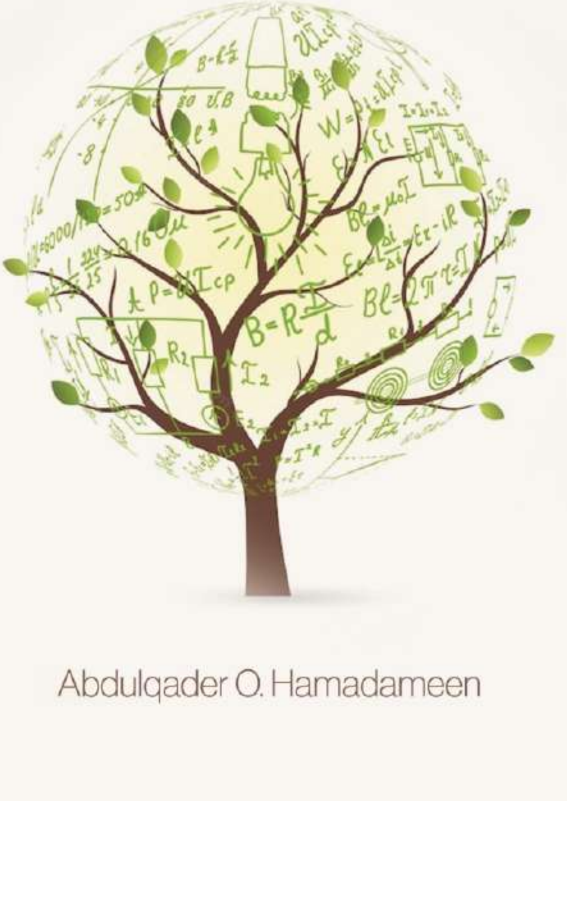
Foundations of Mathematics
Abdulqader O.Hamadameen
Foundations of Mathematics
Abdulqader O.Hamadameen
Mathematic Set

9 789922 924892

Foundations of Mathematics

Abdulqader O. Hamadameen

Foundations of Mathematics



Abdulqader O. Hamadameen

FOUNDATIONS OF MATHEMATICS

Abdulqader Othman

Department of Mathematics
Koya University

2022

List of Tables

List of Figures

Dedication

To my beloved wife and children

Preface

This book is based on lectures developed by the author to B.Sc and M.Sc. students at Koya University, Department of Mathematics. In addition, the book is also the product of the observations accumulated in the last two decades of teaching under, and graduate studies of the author.

The book takes into consideration, the necessity of the contents of this book for students to study mathematics as well as physics in both theoretical and practical branches in the faculties of science, education, engineering, and the statistics department in the faculties of administration and economics. In addition, even faculties of medicine, technical science, industrial mathematics, petrochemical departments, ...etc for their purposes to use the preliminaries of mathematics of some special functions as a tool to implement some tasks in the field of their professional applications in the field of mathematics practical work, such as; some functions related to transformations, statistical and probabilistic mappings, and what is related to applied field.

The academic goals of this book are;

(i) To help students to be fully familiar with the foundations of mathematics.

(ii) To help students to use mathematics logically in life to scientific thinking in order to solve problems.

(iii) To employ mathematics in other sciences to facilitate their tasks.

(iv) To help students to study problems from different scientific perspectives. And to find appropriate scenarios to state the algorithms for optimal solutions through logical reasoning and the rule of conditional proof associated with the deductive rules for those problems.

It is noteworthy that, most of the theorems, corollaries, and exercises in this book are adapted from the references (Albert, 1956; Bittinger, 1970; Bittinger, 1985; Birkhoff and Mac, 1962; Birkhoff and Mac, 2017; Cohen, 2008; Cohen and Ehrlich, 1969; Eves and Newsom, 1958; Fraenkel, 1969; Hafstrom, 2013; Hall, 2018; Halmos, 2017a; Halmos, 2017b; Herstein, 2006; Hu, 1965; Kamke, 1950; Kelley, 2017; Kelley, 1955; Monk, 1973a; Monk, 1973b; Pervin, 1964; Pervin, 2014; Pinter, 2014; Stoll, 1960; Stoll, 1979; Van der Waerden et al., 1950; Suppes, 1999; Wilder et al., 2012; Wilder, 1952; Zariski and Samuel, 1958; Zariski and Samuel, 2013; Zulauf, 1969b; Zulauf, 1969a; Nagornyi, 1971).

The contents of this book are organized as follows: chapter 1, dedicated to discussing to the mathematical logic and the basic concepts of it. Chapter 2, deals with the sets and operations on them. Chapter 3, deals with relations on sets. The mappings or functions from a set to another set based on the domain and the codomain took their place in chapter 4. Chapter 5, dealing with the potency of sets, equipotent sets, arithmetic on cardinal numbers, ordinal numbers, and paradoxes. Chapter 6, deals with the natural numbers, Peano's axioms, arithmetic of the natural numbers, and infinite sets. Chapter 7, considered binary operations and groups, subgroups, Lagrange theorem on groups, and homomorphism and isomorphism. Chapter 8, deals with integers, construction of integers, integers with two binary operations to creation integral domain, rings, and order on integers. Chapter 9, describes how to create rational numbers of integers. Moreover, proves that this collection of numbers with the addition and multiplication operations can be an incomplete Archimedean field. Chapter 10, collection the rational numbers with irrational numbers to create the real numbers. Finally, chapter 11, expands the real numbers to obtain the field of the complex numbers, and proves that this kind of the set is closed algebraically.

Theorems and their corollaries are printed in *italics.* While, the end of the proofs to theorems and corollaries are indicated by the symbol ♦.

Abdulqader Othman
Department of Mathematics, Faculty of Science & Health
Koya University
2022

1

Mathematical Logic

1.1 Introduction

Mathematics consists of three main branches; arithmetic and probability, algebra and what are related them, and geometry in all its branches. Logic is the only way to connect these branches directly or indirectly. All mathematicians agree that the mathematics generally is a connected and consistent unit, based on sets in its the mathematical structures or mathematical systems, basically formed on sets and the associated concepts.

The traditional mathematics focus on acquiring mathematical skills rather than mathematical concepts, while the modern mathematics balance between the acquiring mathematical skills and the mathematical concepts.

Since mathematics interference all the fields in the real life, because all modern sciences are structured based on the sets and the relationships on them, hence, the progress of the mathematics is closely related to the progress of the society and its intellectual and material prosperity.

1.2 Definition

We can define the concept of definition based on some researchers in literature (Eves and Newsom, 1958; Stoll, 1979; Ian, 1995; Kamke, 1950) as follows.

Definition 1.1 It consists of words, some of them are understandable and others need new definitions,... and so on.

1.3 The Initial Statement

Definition 1.2 The initial statement: Initial phrases: They cannot be proven, because they are not preceded (Stoll, 1979).

1.4 The Axiom

Definition 1.3 It is not necessary to satisfy your understanding and knowledge, provided that does not violate the laws of the logic (Stoll, 1979).

1.5 Sets

Definition 1.4 The set A is any collection of definite, distinguishable objects of our intuition or of our intellect to be conceived as a whole. The objects are called elements or members (Stoll, 1979).

.

1.5.1 Express of Sets

The express of sets can be in three different methods:

(i) Venn method (Diagrams). This is the simplest method to express of a sets, that used by Oiler and called Venn diagrams. Venn diagram is the is closed curve not intersected with itself. For example,

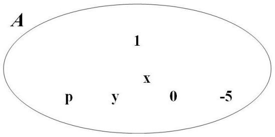


Figure 1.1: Venn Diagram of the Set A

(ii) Tabulation method. In this method the elements of the set can be written between braces and named. For example, (1). $A = \{1, p, y, x, 0, -5\}$. (2). the set of the integer numbers of $5, 6, 7$ can be written as $\{5, 6, 7\}$.

(iii) Rule method. This method can assigned a property owned by all the elements in the set, and not owned by others. $P(x)$ can be used as a sentence in the variable x. For example ($x \leq 5$, x is an odd integer), can be expressed as: $\{x|P(x)\} = \{5, 3, 1\}$. Or, can be defined as: $\{x|1 \leq x \leq 5\}$. It means, (the set of all odd integers such that, $1 \leq x \leq 5$). As well as the set of all integers that their square are greater than 3 can written as, $\{x|x^2 > 3, x \in \mathbb{Z}\}$.

1.5.2 Membership to Sets

The big letters denoted to the sets, while the small letters denoted to the members of the set. The membership of the set A specifies the status of membership of element $x \in A$. For example, let us recall $A = \{1, p, x, y, 0, -5\}$, it seen that $p \in A$, while $7 \notin A$, so as $m \notin A$. Furthermore, $30 \in \{x|x \in \mathbb{Z}, \text{and x is Complications of 5}\}$, while $13 \notin \{x|x \in \mathbb{Z}^+\}$.

1.5.3 Empty Set

Definition 1.5 A set that does not contains any element is called the empty set, and denoted it by ϕ or $\{\}$ (Conway and Guy, 1996; Mendelson, 2009b).

Example 1.1 (i) The set of natural numbers less than zero$= \phi$.

(ii) $\{x|x^2 = 13 \wedge x \in \mathbb{Z}^+\} = \phi$.

(iii) $\{x|x \neq x \wedge x \in \mathbb{C}\} = \phi$.

(iv) $\{x| - 5 < x < -4 \wedge x \in \mathbb{Z}^-\} = \phi$.

1.5.4 Subset

Definition 1.6 Let $A, B \neq \phi$, $A \subseteq B \Leftrightarrow a \in A \Rightarrow a \in B$(Stoll, 1979). And said A is subset of B, or B contain of A.

1.5.5 Proper Subset

Definition 1.7 Let $A, B \neq \phi$, $A \subset B \Leftrightarrow$ (1). $A \subseteq B$, and (2). $\exists b \in B \wedge b \notin A$ (Stoll, 1979).

Note: (1). $A \subseteq B$ means that A is subset or equal to B. (2). $A \subset B$ means that A is proper subset of B. (3). $A \nsubseteq B$ means that A is not equal or subset of B.

1.5.6 Universal Set

Definition 1.8 If all sets under consideration are subsets of fixed set, then the fixed set called universal set, and denoted by U(Mustafa et al., 1980; Stoll, 1979).

Example 1.2 (i) consider the sets, $A = \{1, 3, 5, 7\}, B = \{2, 4, 6, 8\}, C = \{2, 9, 10\}$, then the universal set according to A, B, C can be: $U = \{1, 2, , 7, 8, 3, 4, 5, 6, 9, 10\}$. Or, $U = \{x|1 \leq x \leq 10\}$, $U = \mathbb{N}$, $U = \mathbb{Z}$,...

(ii) $U = \{x|$ x is a branch of mathematical science$\}$, then U can takes all branches of the mathematical science.

1.6 Types of Set Numbers

(i) Natural numbers ($\mathbb{N}$)= $\{0, 1, 2, 3, ...\}$.

(ii) Integer numbers ($\mathbb{Z}$) = $\{..., -3, -2, -1, 0, 1, 2, 3, ...\}$.

(iii) Rational numbers ($\mathbb{Q}$) = $\left\{\frac{a}{b} \wedge b \neq 0, a, b \in \mathbb{Z}\right\}$.

(iv) Rear numbers $(\mathbb{R}) = \{x|x \text{ is real number}\}$.

(v) Complex numbers $(\mathbb{C})= \left\{x+iy| \wedge x, y \in \mathbb{R}, i=\sqrt{-1}\right\}$.

(vi) Positive integer numbers $(\mathbb{Z}^{+})= \{1, 2, 3, ...\}$.

(vii) Negative integer numbers $(\mathbb{Z}^{-})= \{-1, -2, -3, ...\}$.

(viii) Even integer numbers $(\mathbb{Z}_e) = \{x|x \text{ is even number}\}$
$= \{x|x = 2n \wedge n \in \mathbb{Z}\} = \{..., -6, -4, -2, 0, 2, 4, 6, ...\}$.

(ix) Odd integer numbers $(\mathbb{Z}_o)= \{x|x \text{ is odd number}\}$
$= \{x|x = 2n+1 \wedge n \in \mathbb{Z}\} = \{..., -5, -3, -1, 1, 3, 5, ...\}$.

(x) Positive Rational numbers $(\mathbb{Q}^{+})= \left\{\frac{a}{b} \wedge b \neq 0, a, b \in \mathbb{Z}^{+} \vee \mathbb{Z}^{-}\right\}$.

(xi) Negative Rational numbers $(\mathbb{Q}^{-})= \left\{\frac{a}{b} \wedge b \neq 0, a, b \notin \mathbb{Z}^{+} \wedge \mathbb{Z}^{-}\right\}$.

(xii) Positive Real numbers $(\mathbb{R}^{+})= \{x|x \text{ is positive real number}\}$.

(xiii) Negative Real numbers $(\mathbb{R}^{-})= \{x|x \text{ is negative real number}\}$.

(xiv) Prime numbers $(P)= \{x|\text{x is prime number}\} = \{2, 3, 5, 7, 11, ...\}$.
Or, The prime number is the integer number which has only four denominators namely are $\{\pm 1, \pm P\}$.

1.7 Sets in the Form of Intervals

(i) Open interval $= \{x|a < x < b\} = (a, b)$. Example $(2, 5)$.

(ii) Closed interval $= \{x|a \leq x \leq b\} = [a, b]$. Example $[-5, 5]$.

(iii) Half open interval from the left $= \{x|a < x \leq b\} = (a, b]$. Example $(-2, 5]$.

(iv) Half open interval from the right$= \{x|a \leq x < b\} = [a, b)$. Example $[-2, 5)$.

1.8 Equality

Definition 1.9 If both a, b are symbols to the same thing (object) then the statement $a = b$ means the same thing (Carolyn, 1981).

Note: If a is the symbol to an object, and b is the symbol to another different object then said a is not equal to b, and expressed by $a \neq b$.

Example 1.3 (i) 1 Km$= 10^3$ m.

(ii) $17 = 7 + 3 + 7$.

(iii) $\pi \neq \frac{22}{7}$.

1.8.1 Properties of Equality

There are four basic properties of the equality as follows:

(i) $a = a$.

(ii) If $a = b$ then $b = a$.

(iii) If $a = b$ and $b = c$ then $a = c$.

(iv) If $a = b$ each property achieved by a, is achieved by b and vice versa (Principle of substitution).

1.8.2 Equality of Sets

Definition 1.10 Consider the sets $A, B \neq \phi$, $A = B$ if and only if each of A, B are symbols to the same set. Or, $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$ (Ian, 1995; Ian and David, 2015).

Note: $A \neq B$ means A and B are not equals.

Example 1.4 (i) $\{1, -5\} = \{x | (x-1)(x+5) = 0 \wedge x \in \mathbb{Z}\}$.

(ii) $\{1, 3, 5\} = \{5, 3, 1\} = \{5, 5, 3, 1, 1\}$.

(iii) $\{x | x^2 = 4 \wedge x \in \mathbb{Z}\} = \{-2, 2\}$

1.9 Sentences

Depending on some reliable sources in literature (Eves and Newsom, 1958; Stoll, 1979; Stoll, 1960; Patrick, 1999; Wilder et al., 2012; Zulauf, 1969b; Zulauf, 1969a), we can define a sentence as follows;

Definition 1.11 A sentence is a linguistic expression of an idea, or certain ideas. A sentence could be informative or descriptive. In other words, a sentence is a group of words that makes complete sense, contains a main verb, and begins with a capital letter.

The mathematicians use a mathematical sentences in order to express of their ideas as follows;

(i) If $y = x^2$ then $\frac{dy}{dx} = 2x$.

(ii) In the field of Euclidean geometry, the total measurements of any triangle is 180^0.

1.9.1 Statements

Definition 1.12 A statement is an informative sentence, and could be true or false. It does not be true and false at the same time(Eves and Newsom, 1958; Stoll, 1979; Stoll, 1960; Patrick, 1999; Wilder et al., 2012; Zulauf, 1969b; Zulauf, 1969a).

Note: The statements can be denoted by symbols like; $p, q, r, \ldots.$
(1) Truth or false of the statement called the value of the statement.
(2) Paired with the true statement the symbol T, while paired with the false statement the symbol F.

Example 1.5 (i) The university is an advanced scientific center: true statement.

(ii) $9 = 7 - 2$: False statement.

(iii) Where are you going? This is the interrogative sentence not statement.

(iv) If $f(x) = \sec x$ then $f'(x) = \sec x \tan x$: true statement.

(v) My father is a mathematician: it is not statement.

(vi) $x + 3 = 0$: it is not statement.

1.9.2 Variables

Depending on the researchers in the literature (Eves and Newsom, 1958; Stoll, 1979; Stoll, 1960; Patrick, 1999; Wilder et al., 2012; Zulauf, 1969b), the variable can defined as follows;

Definition 1.13 A variable is a letter (symbol) which can represent any element of the universal set.

For example: (1) He is a good mathematicians. Note that "he" is the variable, and can take any one of the mathematicians group. (2) In the sentence $x - 1 = 0$, x is a variable ($x \in \mathbb{N} \vee x \in \mathbb{Z} \vee ...$).

Note: Any sentence can be converted to a statement by; (1) replacing the variable with a number, and (2) adding expressions"$\forall$" or "$\exists$" for each sentence.

Example 1.6 (i) $x < -5$ is not statement but $-6 < -5$ is a true statement.

(ii) $\forall x \in \mathbb{R}, x < -5$ is a false statement.

1.9.3 Parameters

Thomas et al. (2010) defined the parameter as follows;

Definition 1.14 The relation between two variables called parameter.

Example 1.7 Let $x = t^2$ and $t = y - 1, \forall t \in \mathbb{R}$. Then t is called the parameter between x and y, and that leads to $x = (y - 1)^2$ or $y = \sqrt{x} + 1$.

1.9.4 Open Sentences

Based on Cauman (1998), an open sentence can be defined as follows:

Definition 1.15 Let A be a nonempty set, and $P(x)$ an expression in x, the $P(x)$ is called an open sentence in x on A if and only if $P(a), \forall a \in A$ is a true or false statement.

Examples: (1). Let $\mathbb{R}$ and the expression $x < 3$ be an open sentence in x defined on $\mathbb{R}$. If we take $r \in \mathbb{R}$ then $r < 3$ become a true statement or a false statement. (2). Consider $\{0, 1, 2, 3, 4\}$, then $x + 1 < 4$ is the open sentence in x on A. Note that $0 + 1 < 4, 1 + 1 < 4, 1 + 2 < 4$ are true statements, while $1 + 3 < 4, 1 + 4 < 4$ are false statements.

1.9.5 Solution Sets

Definition 1.16 Let $P(x)$ be an open sentence in x defined on the set A, and let $a \in A$. If $P(a)$ is a true statement in a then a is a solution for the open sentence $P(x)$. The set of all solutions for $P(x)$ is called set solutions for the sentence, and denoted by T_P for $P(x)$. Or, $T_P = \{a \in A | P(a) \text{is a true statement}\}$ (Cauman, 1998).

Example 1.8 Let $A = \{0, 1, 2, 3\}$, and $x - 2 < 3$ is an open sentence in x on A then $T_P = \{0, 1, 2, 3\}$.

Note:

(i) The alternative selection for the variable must be in the universal set in which $P(x)$ has been defined on it.

(ii) $T_P \subseteq U, \forall\, T_P$.

1.10 Exercises

Solve the following questions:

Q1: Identify which of the following sentences is statement, and mention the reason.

(i) $x < 2$.

(ii) $x + y = y + x$.

(iii) $\exists x \in \mathbb{N}, s.t. x < 5$.

(iv) this is false statement.

(v) $\lim\limits_{x \to \infty} \frac{1}{n} = 0$.

(vi) If $x, y \in \mathbb{R}$ then $x + y = y + x$.

Q2: Identify the variables in each of the above sentences.
Q3: Find an T_P in the following sentences:

(i) $x - 2 < 5$ and $U = \{0, 1, 2, 3\}$.

(ii) $|x| + 1 < 3$ and $U = \{0, 1, 2, 3, 5\}$.

(iii) $(x - 1)(x + 2) = 0$ and $U = \{5, 6, 7\}$.

(iv) $2x^2 + 3x + 1 = 0$ and $U = \mathbb{Q}$.

(v) $x^2 + 1 = 0$ and $U = \mathbb{R}$.

Q4: Find the value of the truth from what comes where $x \in \mathbb{R}$ and f is a real valued function.

(i) $\forall x, x^2 = 0$.

(ii) If $f(x) = x^3$ then $f'(x) = 3x^2$.

(iii) If $x = 0 \vee x = 1$ then $x^2 = x$.

(iv) $\forall a \in \mathbb{N}, a^2 = a$.

(v) $\exists a \in \mathbb{N}, a^2 = a$.

(vi) If the function is continuous, then it is derivable.

(vii) $\exists b \in \mathbb{Q}, b < 2$.

1.11 Negation and Compound Statements

In this section we deal with negation of statements compound of them.

1.11.1 Negation

Definition 1.17 Let P be a statement, the statement not P is a negation of it and denoted by $\sim P$(Cauman, 1998).

Example: P: Mathematics is a Language of Science. The $\sim P$: Mathematics is not a Language of Science.

1.11.2 Axiom of Negation

The negation verifies the following essential axiom.

If P is true then $\sim P$ is false, and vice versa (Dalen, 1998; Troelstra and Dalen, 1988).

1.11.3 Truth Table

To illustrate the relationship between the statement and its negation, we can use the method named truth table where T is the truth value of P, and F is the false value of P as demonstrated in Table 1.1:

Table 1.1: Truth Table of P

P	$\sim P$
T	F
F	T

The first column in the table is the truth value of P while the second column is the truth value of $\sim P$.

Example 1.9 (i) If $P : a = b$ then $\sim P : a \neq b; \forall a, b \in \mathbb{R}$.

(ii) $P : a \in A$ then $\sim P : a \neq A$.

Note: $\sim\sim P = P$.

1.11.4 Compound Statements

It is possible to obtain the compound statement by associating more than one statement by on of connectives like; and, or, if.... then, and if and only if, ... etc. The obtained statement called compound statement, and the original statements of it called by their name of components. We delve into explaining in each of these connectives, based on some logical studies in the literature (Dalen, 1998; Troelstra and Dalen, 1988; Eves and Newsom, 1958; Stoll, 1979; Stoll, 1960; Patrick, 1999; Wilder et al., 2012; Zulauf, 1969b; Zulauf, 1969a), as follows;

(i) Conjunction statements

Definition 1.18 Let each of p, q be statements. The compound statement in p, q is true if and only if each of p, q is true, and denoted by $p \wedge q$ called p conjunction. q

As descried in the Table 1.2.

Table 1.2: Truth Table of $p \wedge q$

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Example 1.10 (a) Stephen is an English scientist: T. Einstein is a German scientist: T. Then Stephen is an English scientist and Einstein is a German scientist: T. Then.

(b) $(p : 6 + 2 = 9)$: F. $(q : 6 + 3 = 9)$: T. Then $(p \wedge q : 6 + 2 = 9 \wedge 6 + 3 = 9)$: F.

Note: $p \wedge q = q \wedge p$.

(ii) Disjunction statements

Definition 1.19 Let each of p, q be statements. The compound statement in p, q is false if and only if each of p, q is false, and denoted by $p \vee q$ called p disjunction q. As descried in the Table 1.3.

Table 1.3: Truth Table of $p \vee q$

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Example 1.11 (a) (p : Hawler is in Germany) is a false statement. (q :Berlin is in Kurdistan) is a false statement. Thus, the compound statement ($p \vee q$: Hawler in Germany or Berlin in Kurdistan) is a false statement.

(b) The compound statement ($p \vee \sim p$: Hawler is in Germany or Hawler is in Kurdistan) is a true statement. In general, If p is a statement then the compound statement ($p \vee \sim p$: is always a true statement, as illustrated in Table 1.4.

Table 1.4: Truth Table of $p \vee \sim p$

p	$\sim p$	$p \vee \sim p$
T	F	T
F	T	T

(c) The statement $5 > 20 \vee \sqrt{x^2} = |x|$ is a true statement $\forall x \in \mathbb{R}$.

(d) The statement $\pi > 0 \vee 3 + 4 = 7$ is a true statement.

Note: $p \vee q = q \vee p$.

(iii) Conditional statements

Definition 1.20 Let each of p, q be statements. The compound statement in $p \rightarrow q$ is false if and only if p is true and q is false, and denoted by $p \rightarrow q$ called a conditional statement. p is called hypothesis/ antecedent, and q is called consequent/ conclusion.

As descried in the Table 1.5.

Table 1.5: Truth Table of $p \rightarrow q$

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Conditional axiom: The statement $p \rightarrow q$ is always true except in the case if p is true and q is false. Let us illustrate the conditional axiom in the following conditional decision: The father said to his son if you pass the exam, I will buy you the bike.

(a) p is T: The son passed the exam, q is T: The father bought the bike.

(b) p is T: The son passed the exam, q is F: The father did not buy the bike.

(c) p is F: The son did not pass the exam, q is T: The father bought the bike.

(d) p is F: The son did not pass the exam, q is F: The father did not buy the bike.

Logically, the statement is false just in the second case.

Example 1.12 (a) If $2 = 3$ then $\sqrt{15} = 7$: T.

(b) If $\sqrt{x^2} = |x|$ then $8 - 3 = 4$: F.

Note: The following expressions have the same meaning:

(a) $p \to q$.

(b) If p then q.

(c) p lead to q. Or, p requires q.

(d) q if p (p only if q).

(e) p is sufficient condition to q.

(f) q is necessary condition to p.

(g) q is concluding from p.

Example 1.13 Express what that comes in the form of $p \leftrightarrow q$:

(a) The polygon has no diagonals only if it is triangular. Let p : The polygon has no diagonals. q :The polygon is a triangle. Thus, the considered sentence in the form of $p \leftrightarrow q$ becomes as. If the polygon has no diagonals it should be a triangular.

(b) The function f is continuous if it differentiable. Let p : The function is differentiable. q : The function is continuous. Thus, the considered sentence in the form of $p \leftrightarrow q$ becomes as. If the function is differentiable then it is continuous.

Note: $p \to q$ is not $q \to p$ as illustrated in Table 1.6.

Table 1.6: Truth Table of $p \to q$,$q \to p$

p	q	$p \to q$	$q \to p$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

(iv) Biconditional statements

Definition 1.21 Let each of p, q be statements. The compound statement in p, q is true if and only if the truth value of each of p, q are equal, and denoted by $p \leftrightarrow q$.

As descried in the Table 1.7.

Table 1.7: Truth Table of $p \leftrightarrow q$

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Note: The statement $p \leftrightarrow q$ means p if and only if q and this in its role leads to q if p and p if only q. Or, $p \rightarrow q \wedge q \rightarrow p$, as described in Table 1.8.

Table 1.8: Truth Table of $p \rightarrow q \wedge q \rightarrow p$

p	q	$p \rightarrow q$	$q \rightarrow p$	$p \rightarrow q \wedge q \rightarrow p$	$p \leftrightarrow q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

Note: The following expressions are the same;

(i) $p \rightarrow q$.

(ii) p is the necessary and sufficient to q.

(iii) q is the necessary and sufficient to p.

(iv) p if and only if q.

(v) q if and only if p.

(vi) If p then q, and vice versa.

(vii) If q then p, and vice versa.

(viii) $p \leftrightarrow q$ it means $p \to q \wedge q \to p$.

1.12 Exercises

Answer the following questions:

Q1: Find a truth value of;

(i) $e \in \mathbb{Q} \wedge \lim\limits_{x \to \infty} \frac{1}{n} = 1$.

(ii) $9 \neq 4 \wedge \sqrt{x^2} = |x|, \forall x \in \mathbb{R}$.

(iii) $\pi \in \mathbb{Q} \vee \mathbb{R}$.

(iv) $\sim (\pi$ is irrational number$)$.

(v) $2 = \sqrt{4} \to \int x^2 dx = x^4$.

(vi) $x \in \mathbb{Z} \leftrightarrow \frac{-1}{3} \in \mathbb{N}$.

(vii) (Steven is a great English scientist $\wedge\ |x| \geq 0, x \in \mathbb{R}$).

Q2: Expressed what comes in four different ways $p : 3 = 4, q :$ e is irrational number.

Q3: Express what comes without using the negation symbol;

(i) $\sim (x < y)$.

(ii) $\sim (x > y)$.

(iii) $\sim (4 \leq x)$.

(iv) $\sim (y^3 \geq 2 + x)$.

(v) $\sim (\sqrt{x^2} = |x|)$.

Q4: Write the following sentences in the form of (if p then q) and show the hypothesis and conclusion.

(i) There is no analysis to n as long as n is the prime number.

(ii) x is integer if x is natural number.

(iii) The integer number is the rational.

(iv) The square is a rectangle.

(v) $x = y$ because $3x = 3y$.

(vi) The squares are not triangles.

Q5: Write the following sentences in the form of $p \leftrightarrow q$.

(i) $ab = 0$ if and only if $a = 0$ or $b = 0$.

(ii) $2x - 1 = 0$ is equivalent to $x = \frac{1}{2}$.

(iii) The function f is continuous if and only if f is a drivable.

(iv) If the triangle is equilateral, it must have two equal ribs, and vice versa.

(v) $x = 4$ if and only if $3x = 12$.

1.13 The Compound Statements with More Than One Connective

In this section we are going to deal with the compound statements with more than one connective.

Example 1.14 (i) If p, q are numbers in $\mathbb{Z}$, and $q \neq 0$ then $\frac{p}{q}$ is a rational number. Let us express this statement via mathematical logic and by symbols as: $p \in \mathbb{Z} \wedge q \in \mathbb{Z} \wedge q \neq 0 \rightarrow \frac{p}{q} \in \mathbb{Q}$.

(ii) If a is integer number then a is even number or odd number. Mathematically, $a \in \mathbb{Z} \rightarrow (a \in \mathbb{Z}_e \vee a \in \mathbb{Z}_o)$.

Now, let us deal with some examples, to show that the truth table of statements in more than one connective.

Example 1.15 Write the truth table of $p \wedge \sim q$.

Solution See Table 1.9.

Table 1.9: Truth Table of $p \wedge \sim q$

p	q	$\sim q$	$p \wedge \sim q$
T	T	F	F
T	F	T	T
F	T	F	F
F	F	T	F

Example 1.16 Write the truth table of $(p \vee q) \rightarrow (p \wedge q)$.

Solution See Table 1.10.

Table 1.10: Truth Table of $(p \vee q) \rightarrow (p \wedge q)$

p	q	$p \vee q$	$p \wedge q$	$(p \vee q) \rightarrow (p \wedge q)$
T	T	T	T	T
T	F	T	F	F
F	T	T	F	F
F	F	F	F	T

1.14 Exercises

Solve the following questions:

Q1: Write the truth table for the following statements;

(i) $\sim p \vee q$.

(ii) $p \rightarrow \sim q$.

(iii) $(p \wedge q) \rightarrow (p \vee q)$.

(iv) $\sim (p \wedge q) \vee \sim (q \leftrightarrow p)$.

Table 1.11: Truth Table of $P \equiv Q$

p	q	$p \to q$	$\sim p$	$\sim p \vee q$
T	T	T	F	T
T	F	T	F	F
F	T	T	T	T
F	F	T	T	T

(v) $(p \to q) \vee \sim (p \leftrightarrow \sim q)$.

(vi) $(p \to p \wedge (\sim q \vee r)) \wedge \sim (q \vee (p \to r))$.

Q2: Express what comes by symbols $\to, \leftrightarrow, \sim, \wedge, \vee$.

(i) If p, q are integers and $q \neq 0$ then $\frac{p}{q}$ is a rational number.

(ii) If a^2 is integer the a is odd number or even number.

(iii) The function f is a derivable and the function g is a derivable if and only if $g \circ f$ is a derivable.

1.15 Logical Equivalence

Definition 1.22 Let each of p, q be statements. p is logical equivalence to q if and only if the truth table of p is the same as truth table of q and denoted by $p \equiv q$ (Sándor, 2008; Stoll, 1979; Patrick, 1999).

Example 1.17 Let $P : p \to q$ and $Q : \sim p \vee q$ then $P \equiv Q$.

Solution See Table 1.11.

It is noted that the third and fifth columns are identical, thus they are equivalence.

Example 1.18 For any statements p, q then, the logical equivalence held the following properties

(i) $p \equiv p$.

Table 1.12: Truth Table of $p \vee p$, $p \wedge p$

p	$p \vee p$	$p \wedge p$
T	T	T
F	F	F

Table 1.13: Truth Table of $p \vee \sim p$

p	$\sim p$	$p \vee \sim p$
T	F	T
F	T	T

(ii) $(p \leftrightarrow q) \equiv (p \to q) \wedge (q \to p)$.

(iii) $p \vee p \equiv p$ and $p \wedge p \equiv p$.

Solution For the case (i), see Table 1.12.

1.15.1 Tautology

Definition 1.23 If a compound statement is true regardless of the truth value of its components, it is called the tautology (Elliott, 2009; Stoll, 1979).

Tautology held the following two laws;

(i) Law of the excluded middle.

(1) $p \vee \sim p$, as illustrated in Table 1.13.

(2) Let P, Q be statements, then $P \equiv Q$ if and only if $P \leftrightarrow Q$ is tautology.

(ii) Law of syllogism.

Let P, Q, R be statements. The statement $((P \to Q) \wedge (Q \to R)) \to (P \to R)$ is tautology and it called law of syllogism. As described in Table 1.14.

Note that the eighth column contains of $\mathrm{T}^{'s}$ only.

Table 1.14: Truth Table of $((P \to Q) \wedge (Q \to R)) \to (P \to R)$

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
P	Q	R	$P \to Q$	$Q \to R$	$(4) \wedge (5)$	$P \to R$	$(6) \to (7)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

Table 1.15: Truth Table of $p \wedge \sim p$

p	$\sim p$	$p \wedge \sim p$
T	F	F
F	T	F

1.15.2 Contradiction

Definition 1.24 If a compound statement is false, regardless of the truth value of its components, it is called the contradiction(Elliott, 2009; Stoll, 1979).

Example 1.19 The statement $p \wedge \sim p$ is a contradiction, and called law of contradiction.

Solution The truth table of the statement $p \wedge \sim p$ described in Table 1.15.

Note that the last column contains of F's only.

Note: The statement P is contradiction if and only if $\sim P$ is tautology.

Note: $p \vee \sim p$ is tautology. Thus $\sim (p \vee \sim p)$ is a contradiction, and by using the truth table we can easily prove that $\sim (p \vee \sim p) \equiv$

Table 1.16: Truth Table of $\sim (p \vee \sim p) \equiv p \wedge \sim p$

p	$\sim p$	$p \wedge \sim p$	$p \vee \sim p$
T	F	F	T
F	T	F	T

Table 1.17: Truth Table of $P \wedge I$

P	I	$P \wedge I$
T	T	T
F	T	F

$p \wedge \sim p$. Thus, $p \wedge \sim p$ is contradiction as proved before in Tables (1.14, 1.15). Now we can combine both tables in Table 1.16.

Note: Assume that P is any statement, I is the symbol of tautology, and 0 is the symbol of contradiction, then;

(i) $P \wedge I \equiv P$.

(ii) $P \wedge 0 \equiv 0$.

(iii) $P \vee I \equiv I$.

(iv) $P \vee 0 \equiv P$.

Let us clarify the first and third case by truth table, and leave the second and fourth case as exercise to the reader, as shown in Tables (1.17, 1.18).

Table 1.18: Truth Table of $P \vee I$

P	I	$P \vee I$
T	T	T
F	T	T

1.16 Exercises

Solve the following questions:

Q1: Which of the following statements is tautology?

(i) $(P \wedge (P \to Q)) \to Q$.

(ii) $\sim (P \wedge Q) \leftrightarrow (\sim P \vee \sim Q)$.

(iii) $(P \to Q) \leftrightarrow (P \wedge \sim Q)$.

(iv) $(P \to Q) \to (Q \to P)$.

Q2: Verify the truth value of each of the following;

(i) $p \vee p \equiv p$.

(ii) $p \wedge p \equiv p$.

(iii) $(p \vee q) \vee r \equiv p \vee (q \vee r)$.

(iv) $p \wedge q \equiv q \wedge p$.

(v) $\sim (\sim p) \equiv p$.

(vi) $\sim (p \vee q) \equiv \sim p \wedge \sim q$.

(vii) $p \wedge t \equiv p$, where t is the symbol of true statement.

(viii) $P \vee f \equiv p$, where f is the symbol of false statement.

(ix) $(p \to \sim q) \equiv q \to \sim p$.

Q3: Verify that the statement $((P \to Q) \wedge P) \wedge \sim Q$ is a contradiction.

1.17 Logical Implication

Definition 1.25 Let P, Q be statements, It said the statement P implicates logically the statement Q. Or Q concluding logically from P, if and only if the statement $P \to Q$ is tautology. It expresses by the symbol $P \Rightarrow Q$ (Elliott, 2009; Stoll, 1979; Celia and Dietmar, 2002; Shan-Hwei et al., 1993).

Example 1.20 Let $P : ((p \to q) \wedge (q \to r))$, $Q : (p \to r)$, then $P \Rightarrow Q$.

Solution Since it is proved that $P \to Q$ is tautology, hence $P \Rightarrow Q$.

The next section explains the logical implication by a certain theorem which deals with tautology concept.

Mustafa et al. (1980) have proved the principle of the logical implication via the following theorem.

Theorem 1.1 *Let P, Q be statements then;*

(i) $P \Rightarrow Q$ *if and only if* $\sim P \vee Q$ *is a tautology.*

(ii) *If* $P \Rightarrow Q$ *and* $Q \Rightarrow P$*, then* $P \equiv Q$*.*

Proof

(i) Based on the definition of the logical implication $P \Rightarrow Q$ if and only if $P \to Q$ is a tautology. But $\sim P \vee Q \equiv P \to Q$. Thus, $P \Rightarrow Q$ if and only if $\sim P \vee Q$ is tautology.

(ii) $P \Rightarrow Q$ means $P \to Q$ is tautology. Thus, $Q \Rightarrow P$ means that $Q \to P$ is tautology. ♦

Definition 1.26 The statement $Q \to P$ is converse of the statement $P \to Q$. Note that the statement and its converse are not equivalences generally. Or, $(P \to Q) \not\equiv (Q \to P)$. Thus, $P \Rightarrow Q$ does not necessarily mean $Q \Rightarrow P$ (Elliott, 2009; Stoll, 1979; Celia and Dietmar, 2002; Shan-Hwei et al., 1993).

Definition 1.27 The statement $\sim Q \rightarrow \sim P$ is called the contrapositive of the statement $P \rightarrow Q$. Note that $(P \rightarrow Q) \equiv (\sim Q \rightarrow \sim P)$. Thus, $(P \Rightarrow Q)$ does mean $(\sim Q \Rightarrow \sim P)$ (Elliott, 2009; Stoll, 1979; Celia and Dietmar, 2002; Shan-Hwei et al., 1993).

Example 1.21 The statement equilateral triangle is a isosceles triangle is equivalent to the statement the triangle with not two equal sides is not three equal sides. Because the first statement is a kind of $P \rightarrow Q$, while the second one is a kind of $\sim Q \rightarrow \sim P$.

1.18 Exercises

Solve the following questions:

(i) Show by an example that $P \Rightarrow Q$ does not mean $Q \Rightarrow P$.

(ii) Prove that $P \Rightarrow Q$ if and only if $\sim Q \Rightarrow \sim P$.

(iii) Show that $P \Rightarrow Q$ if and only if $P \wedge \sim Q$ is contradiction.

(iv) Prove that if $P \Rightarrow Q$ and $Q \Rightarrow R$, then $P \Rightarrow R$.

(v) Put the statement" Every function is derivable at a certain point, it is continuous at that point" in the form of $P \rightarrow Q$, then write its converse and logical implication.

1.19 Algebra of Statements

Let P, Q, R be statements, and $0, I$ are symbols of contradiction and tautology respectively, then

(i) Idempotent Laws

(a) $P \vee P \equiv P$.

(b) $P \wedge P \equiv P$.

(ii) Associativity Laws

(a) $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$.

(b) $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$.

(iii) Commutativity Laws

(a) $P \vee Q \equiv Q \vee P$.

(b) $P \wedge Q \equiv Q \wedge P$.

(iv) Distributivity Laws

(a) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$.

(b) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$.

(v) Identity Laws

(a) $P \vee 0 \equiv P$.

(b) $P \wedge I \equiv P$.

(c) $P \vee I \equiv P$.

(d) $P \wedge 0 \equiv 0$.

(vi) Complementary Laws

(a) $P \vee \sim P \equiv I$.

(b) $P \wedge \sim P \equiv 0$.

(c) $\sim (\sim P) \equiv P$.

(d) $\sim I \equiv 0$, $\sim 0 \equiv I$.

(vii) De Morgan's Laws

(a) $\sim (P \wedge Q) \equiv \sim P \vee \sim Q$.

(b) $\sim (P \vee Q) \equiv \sim P \wedge \sim Q$.

Now, we will prove the distributive law, and leave others as an exercise to the reader, as described in Table 1.19. Thus, $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$. By using these laws, we can often dispense of truth tables.

Example 1.22 Simplify the statement $\sim (P \vee \sim Q)$.

Table 1.19: Truth Table of $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	(6) ∨ (7)	(5) ↔ (8)
T	T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T	T
T	F	T	T	T	F	T	T	T
T	F	F	F	F	F	F	F	T
F	T	T	T	F	F	F	F	T
F	T	F	T	F	F	F	F	T
F	F	T	T	F	F	F	F	T
F	F	F	F	F	F	F	F	T

Solution
$$\begin{aligned} \sim (P \vee \sim Q) &\equiv \sim P \wedge \sim (\sim Q) \quad \text{(De Morgan's Laws)} \\ &\equiv \sim P \wedge Q \quad \text{(Complementary Laws).} \end{aligned}$$

1.20 Exercises

Solve the following questions:

Q1: Prove that

(i) $\sim (p \to q) \equiv p \wedge \sim q$.

(ii) $\sim (p \to q) \equiv p \to \sim q$.

Q2: Simplify the statements

(i) $\sim (\sim p \leftrightarrow q)$.

(ii) $\sim (\sim p \to q)$.

(iii) $\sim (\sim p \to \sim q)$.

(iv) $(p \vee q) \vee (\sim p \wedge q)$.

(v) $(p \vee q) \wedge \sim p$

Q3: Show that

(i) $p \to (q \wedge r) \equiv (p \to q) \wedge (p \to r)$.

(ii) $p \to q \not\equiv (\sim p \to \sim q)$. [Hint: $(p \to q)$ is a converse of $(\sim p \to \sim q)$].

1.21 Quantifiers

The statements and their concepts expressed in wholly or partially. This section deals with existential quantifier and total quantifier.

1.21.1 Existential Quantifier

Definition 1.28 Let $P(x)$ be an open sentence in x on the set A. The statement, there exist $x \in A$ such that $P(x)$ is true, called existential quantifier and denoted by the symbol $\exists x \in A, P(x)$ (Dalen, 1998; Mustafa et al., 1980).

Note:

(i) The symbol $\exists$, read there exist.

(ii) The statement $\exists x \in A, P(x)$ is true if and only if its truth set is not empty. Or $T_P \neq \phi$.

1.21.2 Universal Quantifier

Based on Definition 1.28, we will define a universal quantifier as follows:

Definition 1.29 Let $P(x)$ be an open sentence in x on the set A. The statement, for all $x \in A$ such that $P(x)$ is true, called a universal quantifier and denoted by the symbol $\forall x \in A, P(x)$(Dalen, 1998; Mustafa et al., 1980).

Example 1.23 (i) The statement $(\exists n \in \mathbb{N}, 5n + 1 > 5)$ is a true statement. For example 2 is satisfies the statement.

(ii) The statement $(\exists x \in \mathbb{R}, x^2 + 1 = 0)$ is a false statement, because $(\nexists x \in \mathbb{R}, x^2 + 1 = 0)$.

(iii) The statement ($\forall n \in \mathbb{N}, n > -1$) is a true statement.

(iv) The statement ($\forall x \in \mathbb{Q}, x > 0$) is a false statement.

Note: The statement may contain more than one existential quantifier, and universal quantifier. As the form of

(i) $\forall x \in A, \forall y \in B, \forall z \in C, ..., P(x, y, z, ...)$.

(ii) $\exists x \in A, \exists y \in B, \exists z \in C, ..., P(x, y, z, ...)$.

(iii) $\forall x \in A, \exists y \in B, P(x, y)$.

Example 1.24 Consider $A = \{-2, -1, 0, 1, 2\}$. Then

(i) $\forall x \in A, \exists y \in A, x + y = 0$ is true.

(ii) $\exists y \in A, \forall x \in A, x + y = 0$ is false.

It concluded from the example that the truth
$\exists y \in A, \forall x \in A, P(x, y) \not\equiv \forall x \in A, \exists y \in A, P(x, y)$.
Generally
$\exists y \in A, \forall x \in A, \forall z \in A, ..., P(x, y, z, ...) \not\equiv \forall x \in A, \exists y \in A, \exists z \in A, ..., P(x, y, z, ...)$.

1.21.3 Negation of Quantifiers

Based on studies (Stoll, 1979; Stoll, 1960; Zulauf, 1969b; Zulauf, 1969a; Mustafa et al., 1980; Dalen, 1998) in the literature, the negation of quantities is reflected in the following theorem.

Theorem 1.2 *Let $P(x)$ be an open sentence in x on the set A. Then*

(i) $\sim (\forall x \in A, P(x)) \equiv \exists x \in A, \sim P(x)$.

(ii) $\sim (\exists x \in A, P(x)) \equiv \forall x \in A, \sim P(x)$.

Proof (i) We will prove that $\sim (\forall x \in A, P(x))$, and $\exists x \in A, \sim P(x)$ are equivalences, because their truth values are equal.

Suppose that $\sim (\forall x \in A, P(x))$ is true. Then $\forall x \in A, P(x)$ is false. Then, there is an alternative $b, b \in U$, such that if $P(b)$ is a true statement, the $\sim P(b)$ is a false statement. Thus, $\exists x \sim P(x)$ is a true statement.

Now, suppose that $sim(\forall x, P(x))$ is false, then $\forall x, P(x)$ it will be true.

Thus, for all alternative b, $P(b)$ is true, and for all alternative b, the statement $\sim P(b)$ is false. So that $\exists x, \sim P(x)$ will be false.

Thus,

$$\begin{aligned}\sim (\forall x \in A, P(x)) &\equiv \exists x \in A, \sim P(x)\\ \sim (\forall x \in A, P(x)) &\equiv \exists x \in A, \sim\sim P(x)\\ &\equiv \exists x \in A, P(x)\\ \forall x \in A, P(x) &\equiv \sim (\exists x \in A, P(x)).\end{aligned}$$

(ii) In the same way, we can prove this part. ♦

Example 1.25 Find $\sim (\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y = y)$.

Solution

$$\begin{aligned}&\sim (\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, x + y = y)\\ &\equiv \forall x \in \mathbb{R}, \sim (\forall y \in \mathbb{R}, x + y = y)\\ &\equiv \forall x \in \mathbb{R}, \exists y \in \mathbb{R}, \sim (x + y = y)\\ &\equiv \forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y \neq y\end{aligned}$$

Example 1.26 Find the Negation of the statement $\forall n \in \mathbb{N}, (2n + 3 > 7)$.

Solution $\sim (\forall n \in \mathbb{N}, (2n + 3 > 7)) \equiv \exists n \in \mathbb{N}, (2n + 3 \leq 7)$.

1.21.4 Hilbert Operator on an Open Sentence

Consider $P(x)$ an open sentence in x, and let $\exists x, P(x)$ be a true statement. According to David Hilbert (1862-1943) (Bell, 1993; Mustafa et al., 1980), there may be more than one value for x that satisfies $P(x)$. If we want to choose one of the values for $P(x)$, we will denoted by symbol $i_x P(x)$. Thus, if $i_x P(x) = c$, that means $P(c)$ is true statement. In other words $(P(x))$ is true while $x = c$. i_x is called Hilbert operator.

Example 1.27 Let $P(x)$, x means mathematician. Thus, x may be Laplace, because he was one of the greatest mathematicians.

1.22 Exercises

Solve the following questions:

(i) Express the following statements by using logical symbols

(a) There exists p, q such that $pq = 32$.

(b) For all x there exists y, such that $x < y$.

(c) There exists y, for all x, such that $x + 0 = y$.

(d) For all x, for all y, $x + y = y + x$.

(e) Each triangle is polygon.

(f) For each x, where x is natural number, then x is integer.

(g) For all natural number x, x is odd number or even number.

(h) There exists s, such that x is prime number or even number.

(i) There exists $x \in \mathbb{R}$, such that $x = \lim\limits_{n\to\infty} \frac{1}{n}$.

(j) There exists x where $n \leq x \leq 2$ and $\int_n^2 f(x)dx = (2-n)f(x)$.

(k) Each even number is not odd.

(ii) Are the following statements true?

(a) $\forall x \in A, \forall y \in A, x + y = y + x$, where $A = \{0, 1, 2\}$.

(b) $\forall x \in A, \exists y \in A, x + y = y + x$, where $A = \{0, 1, 2, 3, 4, ...\}$.

(iii) Is the following statement true?: $\forall x \exists y, p(x, y) \to\ x \exists y \forall x, p(x, y)$.

(iv) Find the negation of the following statements:

(a) $\forall x \forall y \exists z, x + y + z = 18$.

(b) Ther exist y such that for all x, $xy \leq 2$.

(c) $\exists x, (p(x) \rightarrow q(x))$.

(v) Explain the following statements by an illustrative example, or by another method.

(a) $(\forall x), [\Pi(x) \wedge P(x)] \equiv (\forall x), \Pi(x) \wedge (\forall x), P(x)$.

(b) $(\exists x), [\Pi(x) \vee P(x)] \equiv (\exists x), \Pi(x) \vee (\exists x), P(x)$.

(c) $(\exists x), [\Pi(x) \rightarrow P(x)] \equiv \exists x, \Pi(x) \rightarrow (\exists x), P(x)$.

(d) $(\forall x), [\Pi(x) \vee \forall x, P(x)] \Rightarrow \forall x[\Pi(x) \vee P(x)]$.

(e) $(\exists x), [\Pi(x) \wedge, P(x)] \Rightarrow \exists x, [\Pi(x) \vee \exists x, P(x)]$.

(f) $[\exists x, \Pi(x) \Rightarrow \forall x, P(x)] \Rightarrow \forall x, [\Pi(x) \Rightarrow P(x)]$.

(g) $\forall x[\Pi(x) \Rightarrow P(x)] \Rightarrow [\forall x, [\Pi(x) \Rightarrow \forall x, P(x)]$.

(vi) Let $P(x) : x + 2 > 3$, and $U = \{0, 1, 2, 3, 4, ...\}$. Find $i_x P(x)$.

1.23 Logical Reasoning

Definition 1.30 Let $\{S_i, i = 1, 2, ..., n\}$ be the set of statements, and let S be a statement can be concluded from $\{S_i, i = 1, 2, ..., n\}$. The statement ($S$ from $\{S_i, i = 1, 2, ..., n\}$) is called argument, $\{S_i, i = 1, 2, ..., n\}$ is premises, and S called conclusion, denoted as $\{S_i, i = 1, 2, ..., n\} \vdash S$(Henry, 1993; Walton, 1990).

Note:

(i) It seems from the definition the argument may be either valid or invalid (fallacy).

(ii) The argument $S_1, S_2, ..., S_n \vdash S$ will valid if and only if the statement $S_1 \wedge S_2 \wedge ... \wedge S_n \rightarrow S$ is tautology. Or, $S_1 \wedge S_2 \wedge ... \wedge S_n \Rightarrow S$.

Example 1.28 Premises; S_1 : Some of physicians are mathematicians. S_2 : Ali is a physician. Thus, conclusion (S : Ali is a mathematician). The argument $S_1, S_2 \vdash S$ is invalid because not all physicians are mathematicians.

1.24 Exercises

Solve the following questions:

Q1: Find the set of premises, such that the argument will be valid, and each premises is necessary to the conclusion: S_1 : The clever student his average is excellent. S_2 : Who he average is excellent will be a master candidate. S_3 : Ali is excellence. S :.... .

Q2: Are the following arguments valid?

(i) $p \to q, \sim p \vdash \sim q$.

(ii) $p \leftrightarrow q, q \vdash p$.

Q3: Prove this argument $p \to \sim q, r \to q, r \vdash \sim p$.

Q4: Is the argument, If Ali goes to the war, he will be killed. Ali does not go to the war. Thus, Ali will not be killed.

Q5: Check the validity of the following arguments:

(i) $(\forall x \in A)P(x), x_\circ \in A \vdash P(x_\circ)$.

(ii) $x_\circ \in A, P(x_\circ) \vdash (\exists x \in A)P(x)$.

1.25 Mathematical Proof

The evidence is a dialectical argument for a mathematical statement. In argument, and proofs, essential as preconfigured data can be used, such as theories. In principle, evidence can be traced to clear or presumed statements. In addition to accepted rules of reasoning. Evidence is a special case of inductive extrapolation. Evidence must prove that the statement is always true rather than counting many confirmed cases. The signs use logic but usually include some amount of natural language that usually recognizes some ambiguity. In fact, most proofs in written mathematics can be considered as applications of the logic. Proofs written in symbolic language rather than natural language are considered in the theory of evidence. The philosophy of mathematics is concerned with the role of language and logic in proofs, and mathematics as a language (Antonella, 2011; Eric, 2009).

In what follows, we are going to delve into the concept of pure definition of mathematical proof and the basic types of it based on produced studies in literature (Uri, 1983; Christoph et al., 2003; Daniel and Michael, 2002; Daniel, 2018; Artemov, 1994; Mustafa et al., 1980; Antonella, 2011; Eric, 2009).

Definition 1.31 Let $\{(S_i; i = 1, 2, ..., n), S\}$ be the set of statements, S concluded from S_i. If The argument $S_1, ..., S_n \vdash S$ is true, then it is called proof.

1.25.1 Proof of Sentences of Type $(P \to Q)$

There are two methods of $(P \to Q)$. Which are

(i) Rule of Conditional Proof.

To proof $P \to Q$, we assume first P is true, then by using P, theorems, and previous axioms Q can be concluded. Upon conclusion, Q in this case we proof of $P \to Q$.

In this method, we did not prove that Q is true, but we have proved that Q is true if and only if P is true. For illustrative, assume that $S_1, S_2, ..., S_n$ are axioms, and theorems have been proved in the past. So to prove $P \to Q$ its enough to prove that $S_1, S_2, ..., S_n, P \vdash Q$ its true argument. And this process is called deduction theorem although we have called it proof axiom.

Example 1.29 If a is even then a^2 is even too.

Proof Let a be an even number. Then $a = 2k, k \in \mathbb{Z}$. Thus, $a^2 = 4k^2$(Quadrature of two sides). Thus, $a^2 = 2(2k^2)$. Now, since $2k^2$ is integer, then a^2 is integer.

In this proof, we have used the tautology concept, as $[(P \to S_1) \wedge (S_1 \to S_2) \wedge ... \wedge (S_n \to Q)]$, where:

$P : a$ is even number
$S_1 : a = 2k$
$S_2 : a^2 = 4k^2$
$R : a^2$ is even number

(ii) Contrapositive.

It is possible to prove that $P \to Q$ by its contrapositive, whereas $\sim Q \to \sim P$, because $P \to Q \equiv \sim Q \to \sim P$.

Example 1.30 Prove that if a is even number, then a^2 is even number too.

Proof Let a be odd number, we have to prove a^2 is odd number.

Since a is odd number, thus, $a = 2k + 1; k \in \mathbb{Z}$. Now, by quadrature of two sides we get

$$a^2 = 4k^2 + 4k + 1$$
$$a^2 = 2(2k^2 + 2k) + 1$$

Thus, a^2 is odd number (Definition of odd number).

1.25.2 Proof of Sentences of Type $(P \leftrightarrow Q)$

This type of proof has three different cases as follows:

(i) $P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to P)$.

First, we prove that $P \to Q$, and then we have to prove $Q \to P$.

(ii) Contrapositive $(\sim Q \to \sim P)$.

(iii) $P \leftrightarrow Q \equiv (P \to Q_1) \wedge (Q_1 \to Q_2) \wedge ... \wedge (Q_{n-1} \to Q_n) \wedge (Q_n \to Q)$. Starting from P to Q through the series of equivalence statements. This method is supported by the tautology.

1.25.3 Proof of Sentences of Type $(\forall x, P(x))$

To prove the sentences in the kind of type $\forall x, P(x)$, we suppose that $x \in U$, and then we have to prove $P(x)$ is true for all x in the arbitrary universal set U.

1.25.4 Proof of Sentences of Type $(\exists x, P(x))$

To prove the sentences in the kind of type $\exists x, P(x)$, we suppose that $x \in U$, and then we have to prove $P(x)$ is true when there exists x in the arbitrary universal set U.

Example 1.31 Prove that $\exists f$ such that f is non-derivative and continuous.

Solution $f(x) = |x|$ is a function, continuous and non-derivative.

1.25.5 Proof of Sentences of Type $(P \vee R \rightarrow Q)$

To prove this kind of proof, we depend up on $[(P \rightarrow Q) \wedge (R \rightarrow Q)] \rightarrow [(P \vee Q) \rightarrow Q]$. Thus, we have to prove $P \rightarrow Q$ and $R \rightarrow Q$. That means Q can be concluded from P or from R.

Example 1.32 Prove that if $(a = 0 \vee b = 0) \rightarrow ab = 0$.

Solution

(i) $a = 0 \rightarrow ab = 0$. Suppose that, $a = 0$ then $ab = 0.b = 0$.

(ii) $b = 0 \rightarrow ab = 0$. Suppose that, $b = 0$ then $ab = a.0 = 0$.

1.25.6 Proof by Contradiction

The proof by contradiction is a kind of indirect proof. To prove the statement by contradiction, we suppose $\sim P$ and then we will try to find the statement of the kind $R \wedge \sim R$ where R is any statement consists of P, or, any previous proved theorem, or axiom that supports the following tautology statement, $[\sim P \wedge (R \wedge \sim R)] \rightarrow P$. And, by using contradiction, we can prove the statements of the type of; $P \rightarrow Q$, or $\exists x, P(x)$, or $\forall x, P(x)$.

Note: The contradiction is always false statement whatever the truth of its components, or, for all the statement R, the contradiction $R \wedge \sim R$ is false.

For proving the statement $P \rightarrow Q$ by contradiction, we follow the following algorithm;

(i) Let the statement of the kind of $\sim (P \rightarrow Q)$.

(ii) $\sim (P \rightarrow Q) \equiv \sim (\sim P \vee Q) \equiv P \wedge \sim Q$.

(iii) From the equivalence (i) and (ii), we suppose that P is true and $\sim Q$ is true. Then we will try to get contradiction, and then prove that the $\sim (P \rightarrow Q)$ is false. Or, $(P \rightarrow Q)$ is true.

Example 1.33 (i) For any set A, prove that $\phi \subseteq A$.

(ii) For any x, prove that $x \neq 0 \rightarrow x^{-1} \neq 0$.

Solution

(i) We have to prove $x \in \phi \rightarrow x \in A$. By contrapositive, prove that $x \notin A \rightarrow x \notin \phi$.

Obviously, $x \notin \phi$, because ϕ is the empty set not contains of any element. Thus, $x \notin A \rightarrow x \notin \phi$.

Or, $x \in \phi \rightarrow x \in A$. Thus, $\phi \subseteq A$.

(ii) Let $P : x \neq 0$. $Q : x^{-1} \neq 0$. The desired proof is $P \rightarrow Q$.

Suppose that $\sim (P \rightarrow Q)$ is true. Since, $\sim (P \rightarrow Q) \equiv P \wedge \sim Q$. Thus, $P \wedge \sim Q$ is true.

Or, $x \neq 0 \wedge x^{-1} = 0$.

As, $x.x^{-1} = 1$ and $x^{-1} = 0$. That implies to $x.x^{-1} = x.0 = 0$. Or, $1 = 0$.

This is contradiction because of $(1 \neq 0) \wedge (1 = 0)$.

Thus, $\sim (P \rightarrow Q)$ is the false statement. And $P \rightarrow Q$ is true.

So, $x \neq 0 \rightarrow x^{-1} \neq 0$.

1.26 Exercises

Solve the following questions:

Q1: Prove that all sentence of the kind of $\forall x, P(x) \rightarrow \exists x, P(x)$ is true.

Q2: Show why the statement $\forall x, P(x) \to \exists x, P(x)$ is true, when $\forall x, P(x)$ is false.

Q3: Prove that the statement of the kind of $\exists y \forall x, P(x, y) \to \forall x \exists y, P(x, y)$ is true.

Q4: Give a direct proof using the rule of conditional proof of the following questions;

(i) If each of a, b integer, then $a + b$ is even number.

(ii) If a is even, b is odd, then $a + b$ is odd number.

Q5: Use contrapositive method to prove;

(i) If a is perfect number, then a cannot be prime number (A perfect number is a positive integer that is equal to the sum of its proper positive divisors).

(ii) $[\forall \epsilon > 0, (|a| < \epsilon)] \to a = 0$.

Q6: When proof of the sentence $P \to (Q \wedge R)$, we will prove on $P \to Q$, and $P \to R$. Find a tautology that supports that method.

Q7: Prove what a, b are roots of the equation $x^2 + px + q = 0$ if and only if $ab = q$, $a + b = -p$. [Hint: Use the constitution of solving the second-order equation].

Q8: Prove that, every statement of the kind of $\forall x\ \forall y, P(x, y) \leftrightarrow \forall y\ \forall x, P(x, y)$ is true.

Q9: Prove that $a < b \leftrightarrow a + b < b + c$, where $a, b, c\ in \mathbb{R}$.

Q10: Prove that x is odd number if and only if $x+1$ is even number.

Q11: Prove that every sentences in the kind of $\forall x[P(x) \wedge Q(x)] \leftrightarrow [\forall x, P(x) \wedge \forall x, Q(x)]$ is true.

Q12: Prove that $\forall x$, x is even number if and only if x^2 is even number.

Q13: Consider $U = \mathbb{R}$ prove what that comes;

(i) $\exists x, (x^2 = x)$.

(ii) $\exists y\ \forall x, (x + y = x)$.

(iii) $\exists y\ \forall x, (xy = x)$.

Q14: Prove that the truth of $[\forall x, (x) \vee \forall x, Q(x)] \rightarrow [\forall x, P(x) \vee Q(x)]$.

Q15: Prove that if x rational number, and y is irrational number, then $x + y$ is irrational number.

Q16: Prove that if $f(x) = f(x + \alpha), \forall \alpha > 0$, then f must be constant mapping.

Q17: Prove that $\sqrt{3}$ is irrational number.

Q18: Prove that $\sqrt{x} < \sqrt{x + 2}, \forall x > 0$.

Q19: Prove that $\forall x > 0, x + \frac{1}{x} \geq 2,$.

2
Algebra of Sets

2.1 Introduction

When we deal with the system of numbers, we will use regular calculations, like additions and multiplications. But, when dealing with sets, the similar operations like union ($\cup$) and intersection ($\cap$) can be used.

Using these operations on sets generates the concept of the algebra of sets. The algebra of sets is similar of normal algebra. But broader and more complex in terms of operations, because the operations on sets give the student the following skills; applications and extensions of the algebra operations on non-numbers. And Helping the student discover the relationships between algebra and the other branches of mathematics.

There are some applications of algebra of sets in the real life fields which far away from mathematics in the first glance. For example, the applications in insurance companies that are specialized in a set of people of a certain ages, or, used by sociologists who care about a set of human characteristics, qualities, and properties.

The algebra of sets is a type of Boolean algebra. Symbols like, $\vee, \wedge, \sim$ which are operations on statements are just algebra of logic in the first chapter.

2.2 Union and Intersection of Sets

This chapter, based on available literature (Stoll, 1960; Stoll, 1979; Courant et al., 1996; Mustafa et al., 1980; Shen et al., 2002) attempts to delving into defining union and intersection. In addition, to insert some basic definitions and theorems supported by illustrative examples.

2.2.1 Union of Sets

Definition 2.1 Let A, B be nonempty sets. The union of A, B is the set of all elements in A or B or in both of them, and denoted by $A \cup B$. Or, $A \cup B = \{x | x \in A \vee x \in B\}$. i. e. $x \in A \cup B \leftrightarrow x \in A \vee x \in B$.

Example 2.1 $A = \{x|x \text{ is even natural number}\} = \{0, 2, 4, ...\}$. $B = \{x|x \text{ is odd natural number}\} = \{1, 3, 5, ...\}$. Then: $A \cup B = \mathbb{N} = \{0, 1, 2, 3, 4, 5, ...\}$.

Theorem 2.1 *Let A, B be sets, then*

(i) $A \subseteq A \cup B \wedge B \subseteq A \cup B$.

(ii) $A \subseteq B \leftrightarrow A \cup B = B$.

Proof

(i) To prove $A \subseteq A \cup B$, suppose that

$$\begin{aligned} x &\in A \\ \text{Now}, x \in A &\rightarrow x \in A \vee x \in B \\ &\rightarrow x \in A \cup B \\ \text{Thus}, A &\subseteq A \cup B. \end{aligned}$$

And similarly, $B \subseteq A \cup B$.

(ii) Let $A \subseteq B$, and $x \in A \cup B$

$$\begin{aligned} \text{Now}, x \in A \cup B &\rightarrow x \in A \vee x \in B \\ &x \in B \vee x \in B \\ &\rightarrow x \in B \\ \text{Thus}, A \cup B &\subseteq B \\ \text{Since} B &\subseteq A \cup B \\ \text{Thus}, A \cup B &= B. \end{aligned}$$

Similarly,

Suppose that$A \cup B = B$
From (i), $A \subseteq A \cup B$.
Thus, $A \subseteq B$. ♦

Theorem 2.2 *Let each of A, B, C be nonempty set. Then*

(i) *Idem Potent Law: $A \cup A = A$.*

(ii) *Commutative Law: $A \cup B = B \cup A$.*

(iii) *Associative Law: $A \cup (B \cup C) = (A \cup B) \cup C$.*

Proof

(i) It is left as an exercise for the reader.

(ii) $A \cup B = B \cup A \Leftrightarrow (A \cup B) \subseteq (B \cup A) \wedge (B \cup A) \subseteq (A \cup B)$.

$$\begin{aligned} &\text{Let}x \in A \cup B, \\ \text{Now}, x \in A \cup B &\rightarrow x \in A \vee x \in B \\ &\rightarrow x \in B \vee x \in A \\ &\rightarrow x \in B \cup A \\ \text{Thus}, &A \cup B \subseteq B \cup A ...(1). \end{aligned}$$

Similarly,

$$\begin{aligned} &\text{Let}y \in B \cup A, \\ \text{Now}, y \in B \cup A &\rightarrow y \in B \vee y \in B \\ &\rightarrow y \in A \vee y \in B \\ &\rightarrow y \in A \cup B \\ \text{Thus}, &B \cup A \subseteq A \cup B ...(2). \end{aligned}$$

Thus, from (1)&(2), $A \cup B = B \cup A$. ♦

(iii) Based on (i) & (ii), we can easily prove this part of the theorem.

Theorem 2.3 *Let A be nonempty set. Then*

(i) $A \cup \phi = A$.

(ii) $A \cup U = U$, *where U is a universal set.*

Proof

(i) Since $\phi \subseteq A, \forall A$. Thus from Theorem 2.1, we get $A \cup \phi = A$.

(ii) Since, $A \subseteq U, \forall A$. Thus from Theorem 2.1, we get $A \cup U = U$. ♦

2.2.2 Intersection of Sets

Definition 2.2 Let A, B be nonempty sets. The intersection of A, B is the set of all elements in A and B, and denoted by $A \cap B$. Or, $A \cap B = \{x|x \in A \wedge x \in B\}$. i. e. $x \in A \cap B \leftrightarrow x \in A \wedge x \in B$.

Example 2.2 (i) $A = \{x|x \leq 6\} = \{0, ..., 6\}$,
$B = \{x|, x \text{ prime number such that } x \leq 6\} = \{2, 3, 5\}$.
Then $A \cap B = \{2, 3, 5\}$.

(ii) Let $A = \{x|0 \leq x \leq 100\}$, $B = \left\{x|\frac{1}{9} \leq x \leq 100\frac{1}{33}\right\}$.
Then $A \cap B = \left\{\frac{1}{9} \leq x \leq 100\right\}$.

Definition 2.3 Let A, B be nonempty sets. A, B are called disjoint sets if and only if there are no common elements between them. Or, the intersection of them is empty set. i. e. A, B are disjoint $\Leftrightarrow A \cap B = \phi$.

Example 2.3 Let $A = \{x|x \leq 9\}, B = \{x|x > 9\}$. Then, A, B are disjoint sets because $A \cap B = \phi$.

Theorem 2.4 *Let A, B be nonempty sets, then*

(i) $A \cap B \subseteq A,\ A \cap B \subseteq B$.

(ii) $A \subseteq B \leftrightarrow A \cap B = A$.

Proof

(i) To prove $A \cap B \subseteq A$,

$$\begin{aligned} &\text{Let } x \in A \cap B. \\ \text{Now },\ &x \in A \cap B \rightarrow x \in A \wedge x \in B, \\ &\rightarrow x \in A, \\ &\text{which means } A \cap B \subseteq A. \end{aligned}$$

Similarly, $A \cap B \subseteq B$.

(ii) Suppose that $A \subseteq B$, and $x \in A$.

$$\begin{gathered}\text{Now}, x \in A,\\ \to x \in B,\\ \to x \in A \wedge \in B\\ \text{So}, x \in A \to x \in A \wedge x \in B,\\ \to x \in A \cap B.\\ \text{Thus}, A \subseteq A \cap B.\end{gathered}$$

$$\text{Since} A \cap B \subseteq A, \text{hence}, A \cap B = A....(1).$$

Conversely, let $A \cap B = A$. Since, $A \cap B \subseteq B$, thus $A \subseteq B$. ...(2).

From (1)& (2), $A \subseteq B \leftrightarrow A \cap B = A$. ♦

Theorem 2.5 *Let A, B, C be nonempty sets, then*

(i) *Idem Potent Law: $A \cap A = A$.*

(ii) *Commutative Law: $A \cap B = B \cap A$.*

(iii) *Associative Law: $A \cap (B \cap C) = (A \cap B) \cap C$.*

Proof

(i) It is left as an exercise for the reader (Similar to Theorem 2.2 (i)).

(ii) It is left as an exercise for the reader (Similar to Theorem 2.2 (ii)).

(iii) Let $x \in A \cap (B \cap C)$.

$$\begin{gathered}\text{Now}, x \in A \cap (B \cap C) \to x \in A \wedge x \in (B \cap C)\\ \to x \in A \wedge (x \in B \wedge x \in C)\\ \to (x \in A \wedge x \in B) \wedge x \in C)\\ \to x \in (A \cap B) \wedge x \in C)\\ \to x \in (A \cap B) \cap C\\ \text{Thus}, A \cap (B \cap C) \subseteq (A \cap B) \cap C....(1)\\ \text{Similaly}, y \in (A \cap B) \cap C,\\ \text{We prove that} y \in (A \cap B) \cap C \to y \in A \cap (B \cap C)\\ \text{Thus}, (A \cap B) \cap C \subseteq A \cap (B \cap C)....(2)\\ \text{From}(1)\&(2), \text{we get}, A \cap (B \cap C) = (A \cap B) \cap C. \ ♦\end{gathered}$$

Theorem 2.6 *Let $A \neq \phi$, then*

(i) $A \cap \phi = \phi$.

(ii) $A \cap U = A$.

Proof

(i) Since $\phi \subseteq A, \forall A$, and based on Theorem 2.4, we conclude that $A \cap \phi = \phi$.

(ii) Since $A \subseteq U, \forall A$, and based on Theorem (2.4), we conclude that $A \cap U = A$. $\blacklozenge$

The following theorem illustrates the relation between intersection and union.

Theorem 2.7 *Let A, B, C be nonempty sets, then the distributive Laws are;*

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

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

Proof

(i) Suppose that $x \in A \cap (B \cup C)$.

$$\begin{gathered}
\text{Now}, x \in A \cap (B \cup C) \rightarrow x \in A \wedge x \in (B \cup C) \\
\rightarrow x \in A \wedge (x \in B \vee x \in C) \\
\rightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \\
\rightarrow x \in (A \cap B) \vee x \in (A \cap C) \\
\rightarrow x \in (A \cap B) \cup (A \cap C) \\
\text{Thus}, A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cup C) ...(1) \\
\text{Similarly, suppose that } y \in (A \cap B) \cup (A \cap C) \\
\text{Now}, y \in (A \cap B) \cup (A \cap C) \rightarrow y \in (A \cap B) \vee y \in (A \cap C) \\
\rightarrow (y \in A \wedge y \in B) \vee (y \in A \wedge y \in C) \\
\rightarrow y \in A \wedge (y \in B \vee y \in C) \\
\rightarrow y \in A \wedge y \in (B \cup C) \\
\rightarrow y \in A \cap (B \cup C) \\
\text{Thus}, (A \cap B) \cup (A \cup C) \subseteq A \cap (B \cup C) ...(2) \\
\text{From}(1)\&(2), \text{we concluting that} A \cap (B \cup C) = (A \cap B) \cup (A \cap C).
\end{gathered}$$

(ii) Proof of this branch has been left as an exercise to the reader. ⧫

2.3 Exercises

Solve the following questions:

Q1: If $A \cup B = A, \forall A$, prove that $B = \phi$.

Q2: Describe the following set;
$\{x \in \mathbb{R} | x^2 > 2\} \cap \{x \in \mathbb{R} | \, |x-2| < |x+3|\}$.

Q3: Let A, B be nonempty sets, prove that $\phi \subseteq (A \cap B) \subseteq (A \cup B)$.

Q4: Let A, B, C be nonempty sets, prove that
$(A \cap B) \cup C = A \cap (B \cup C) \leftrightarrow C \subseteq A$.

Q5: Let A, B be nonempty sets, prove that
(1). $A \cup (A \cap B) = A$. (2). $A \cap (A \cup B) = A$.

Q6: Let A, B, C be nonempty sets, prove that
$A \cap C = \phi \Rightarrow A \cap (B \cup C) = A \cap B$.

Q7: Let A, B be sets, prove that
$A \cup B = \phi \Rightarrow A = \phi \wedge B = \phi$.

Q8: Let A, B, C be sets, when will be it $A \cup C = B \cup C$?

Q9: If $n(A)$ represents the number of A's elements, prove that
$n(A \cup B) = n(A) + n(B) - n(A \cap B)$.

Q10: If $C \subseteq A$, $C \subseteq B$, prove that $C \subseteq A \cap B$.

Q11: Let A', B' be any two arbitrary sets. If $A \subseteq A', B \subseteq B'$ then $A \cap B \subseteq A' \cap B'$.

2.4 Complement of a Set

Definition 2.4 Let A be any set, the complement of a set A is the set of all elements in U not in A, denoted by A^c. Mathematically, $A^c = \{x | x \in U \wedge x \notin A\}$. i.e., $A^c = \{x | x \notin A\}$(Devlin, 2012; Drake, 1980; Mustafa et al., 1980; Shen et al., 2002).

Example 2.4 (i) If $A = \{x | x \geq 5\}$, $U = \mathbb{N}$. Then
$A^c = \{4, 3, 2, 1, 0\}$.

(ii) Let $A = \mathbb{Z}_e$, $U = \mathbb{Z}$. Then $A^c = \mathbb{Z}_o$.

Theorem 2.8 *Let A, B be sets. If $A \subseteq B$ then $B^c \subseteq A^c$.*

Proof Since $A \subseteq B$, hence $x \in B \to x \in A$.
Thus, $x \notin B \to x \notin A$. $\therefore x \in B^c \to x \in A^c$.
Thus, $B^c \subseteq A^c$. ♦

Theorem 2.9 *Let A be a set, then $(A^c)^c = A$.*

Proof Suppose that $x \in (A^c)^c$.
Now, $x \in (A^c)^c \to x \notin A^c \to x \in A$. Or, $(A^c)^c \subseteq A ...(1)$.
Conversely, suppose $y \in A$.
Now, $y \in A \to y \notin A^c \to y \in (A^c)^c$. Or, $A \subseteq (A^c)^c ...(2)$.
From (1)&(2), we get that $(A^c)^c = A$. ♦

Definition 2.5 Let A, B be sets, the set that its elements belong to A, and not belong to B is called the difference of two sets A, B. And denoted by $A - B$. In the other statement, $A - B = A \cap B^c$. Or, $A - B = \{x | x \in A \wedge x \notin B\}$(Givant and Halmos, 2008; Dwinger, 1971; Drake, 1980; Mustafa et al., 1980; Wilder et al., 2012).

Note: If $A = U$, then: $A - B = B^c$.

Example 2.5 If $\mathbb{N} = U$, and $\mathbb{N}_o$, then $\mathbb{N} - \mathbb{N}_o = \{0, 2, 4, ..., 2n, n \in \mathbb{N}\}$.

Example 2.6 Prove that $A - B = B^c - A^c; \forall A, B$.

Proof Suppose that $x \in A - B$.

$$\begin{aligned} \text{Now}, x \in A - B &\to x \in A \wedge x \notin B \\ &\to x \notin A^c \wedge x \in B^c \\ &\to x \in B^c \wedge x \notin A^c \\ &\to x \in B^c - A^c \end{aligned}$$

$$\text{Thus}, A - B \subseteq B^c - A^c ...(1).$$

Similarly, we can prove that $B^c - A^c \subseteq A - B ...(2)$.

$$\text{From}(1)\&(2), \text{we get}, A - B = B^c - A^c.$$

Theorem 2.10 *Let A be a set, then*

(i) $U^c = \phi$.

(ii) $\phi^c = U$.

(iii) $A \cap A^c = \phi$.

(iv) $A \cup A^c = U$.

Proof

(i) According to the definition $U^c = \{x|x \in U \wedge x \notin U\}$. And this is contradiction, because there is any element like x belongs to U, and in the same time does not exists in U. Thus, $U^c = \phi$.

(ii) This part is left as an exercise for the reader.

(iii) According to the definition $A \cap A^c = \{x|x \in A \wedge x \notin A\}$. And this is contradiction, because is not exists any element like x belongs to A, and in the same time does not exists in A. Thus, $A \cap A^c = \phi$.

(iv) This part is left as an exercise for the reader. ⧫

Theorem 2.11 *De Morgan's Laws: Let A be a set, then*

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

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

Proof

(i) Let $x \in (A \cup B)^c$.

$$\begin{gathered}
\text{Now}, x \in (A \cup B)^c \rightarrow x \notin (A \cup B) \\
\rightarrow x \notin A \wedge x \notin B \\
\rightarrow x \in A^c \wedge x \in B^c \\
\rightarrow x \in (A^c \cap B^c) \\
\text{Thus}, (A \cup B)^c \subseteq (A^c \cap B^c)...(1). \\
\text{Conversely}, y \in A^c \cap B^c. \\
\text{Now}, y \in A^c \cap B^c \rightarrow y \in A^c \wedge y \in B^c \\
\rightarrow y \notin A \wedge y \notin B \\
\rightarrow y \notin A \cup B \rightarrow y \in (A \cup B)^c. \\
\text{Thus}, A^c \cap B^c \subset (A \cup B)^c...(2). \\
\text{From}(1)\&(2), \text{we get that}(A \cup B)^c = A^c \cap B^c.
\end{gathered}$$

(ii) This part is left, as an exercise for the reader. ⧫

2.5 Symmetric Difference

Definition 2.6 Let A, B be sets. The union of $A - B$ and $B - A$ are called the symmetric difference of A, B, and denoted by $A \triangle B$. Or, $A \triangle B = (A - B) \cup (B - A)$(Rotman, 2010; Givant and Halmos, 2008; Dwinger, 1971; Drake, 1980; Wilder et al., 2012).

Example 2.7 Let $A = \{1, 5, 9, 11, 13\}$. $B = \{2, 5, 11, 18, 19\}$. Then $A \triangle B = \{1, 9, 13, 2, 18, 19\}$.

The following theorem describes the properties of the symmetric difference.

Theorem 2.12 *Let A, B be sets, then*

(i) $A \triangle \phi = A$.

(ii) $A \triangle B = \phi \leftrightarrow A = B$.

Proof

(i) is left, as an exercise for the reader.

(ii) Suppose that $A \triangle B = \phi$.

Now, from the definition of the symmetric difference,

$$(A - B) \cup (B - A) = \phi,$$
$$\therefore A - B = \phi \wedge B - A = \phi$$
$$\text{And so on } A = B...(1)$$
$$\text{Conversely, suppose that } A = B.$$
$$\text{Now}, A = B, \text{implies that}, A - B = \phi.$$
$$\therefore B - A = \phi$$
$$\text{Or}, (A - B) \cup (B - A) = \phi$$
$$\therefore A \triangle B = \phi...(2)$$
$$\text{From(1)\&(2)}, A \triangle B = \phi \leftrightarrow A = B. \ \blacklozenge$$

Now, using the algebra's laws of sets in which proved previous, it is possible to investigated of all the properties of sets without recall the definitions of $\cap, \cup, \subseteq$. As as illustrative in the following examples.

Example 2.8 Prove the following

(i) $A \cup (A \cap B) = A$.

(ii) $A \cap (A \cup B) = A$.

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

(iv) $A \cup (A \cup B^c)^c = A \cup B$.

Proof

(i) Since $A \cap B \subseteq A$ (Theorem 2.4), hence, $A \cup A = A$.

(ii) Since $A \subseteq A \cup B$, hence, $A \cap A = A$.

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

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

2.6 Exercises

Solve the following questions:

Q1: Let P, Q be sets, prove the following:

(i) $P \subseteq Q \leftrightarrow P \cap Q^c = \phi$.

(ii) $P \subseteq Q \leftrightarrow P^c \cup Q = U$.

(iii) $P \subseteq Q \leftrightarrow (P \cap Q^c) \subset P^c$.

(iv) $P \subseteq Q \leftrightarrow (P \cap Q^c) \subset Q$.

Q2: Let A, B, C be sets, prove the following:

(i) $A \bigtriangleup \phi = A$.

(ii) $A \bigtriangleup B = B \bigtriangleup A$.

(iii) $A \bigtriangleup (B \bigtriangleup C) = (A \bigtriangleup B) \bigtriangleup C$.

(iv) $A \triangle (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

(v) $A \triangle A = \phi$.

(vi) $A \triangle C = B \triangle C \to A = B$.

Q3: Prove the equation $(A \cap X) \cup (B \cap X^c) = \phi$ has a solution if and only if $B \subseteq A^c$. In addition, for any set X satisfies the relation $B \subseteq X \subseteq A^c$ is a solution to the equation.

Q4: Prove that X can be expressed as $X = (B \cup T) \cap A^c$, where T is any set.

Q5: Prove that $(A \cap X) \cup (B \cap X^c) = (C \cap X) \cup (D \cap X^c)$ if and only if $B \triangle D \subseteq (A \triangle C^c)$. Then find all solutions.

Q6: Let A, B, C be sets, prove the following:

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

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

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

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

(v) $A \cup C = B \cup C$ if and only if $A \triangle B \subseteq C$.

(vi) $(A \cup C) \triangle (B \cup C) = (A \triangle B) - C$.

(vii) If $A \subseteq B$, and $C = B - A$, then $A = B - C$.

Q7: Prove that The De Morgan's Laws can be generated as following:

(i) $(A_1 \cup A_2 \cup ... \cup A_n)^c = A_1^c \cap A_2^c \cap ... \cap A_n^c$.

(ii) $(A_1 \cap A_2 \cap ... \cap A_n)^c = A_1^c \cup A_2^c \cup ... \cup A_n^c$.

2.7 Family of Sets

Definition 2.7 The set in which each element in it is a set called the family of sets (Padlewska, 1990; Trybulec, 1989; Bylinski, 1989b; Law, 1990b).

Example 2.9 (i) Consider $A = \{1,3\}, B = \{-1,5,8\}, C = \{0,2,4\}$. The family of sets of these sets is $\{A,B,C\}$.

(ii) Let $A = \{a,b,c\}$. The subsets of A are making the family of sets as follows: $\{\phi, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, A\}$. Each element is subset of A.

2.7.1 Power Sets

Definition 2.8 Let A be a set, The set of all subsets of A is called power set of A, and denoted by the symbol $P(A)$. Or, $P(A) = \{X|X \subseteq A\}$ (Devlin, 2012; Puntambekar, 2007; Sharma, 2006; Lane and Moerdijk, 1992; Maclane and Moerdijk, 2012).

Example 2.10 (i) (See, Example (i) in 2.7).

(ii) Let $A = \mathbb{N}$ then $P(A)$ is appear as $P(A) = \{X|X \subseteq \mathbb{N}\}$. Since $\mathbb{N}$ is indefinite, hence we cannot write all power sets of A.

Theorem 2.13 *Let A be a set if $n(A) = m$ then $n(P(A)) = 2^m, m \in \mathbb{N}$.*

Proof We will prove this theorem by using the mathematical induction. Suppose that $P(m)$ is represents the following statement $n(A) = m \to n(P(A)) = 2^m$.

(i) (a) $P(0)$ is true because where $m = 0$ then $n(A) = 2^0 = 1$. Or, the set A not contains any element, i. e. $A = \phi$. Thus, ϕ is the only subset of A. And so $n(A) = 0 \to n(P(A) = 2^0 = 1$. Thus, $P(A)$ is true.

(b) $P(1)$ is true because where $m = 1$ then $n(A) = 2^1 = 2$. Or, the set A contains of only one element. Let $A = \{a\}$. In this case, the power sets of A are $\{\phi, A\}$. i. e. $n(P(A)) = 2^1 = 2$. Thus, $P(A)$ is true.

(ii) Suppose that $P(k), \forall k \in \mathbb{N}$ is true. Or, $n(A) = k \to n(P(A) = 2^k$ is true.

(iii) Now we have to prove $n(A) = k + 1$. Or A contains of $k + 1$ of elements.

Suppose $A = \{a_1, a_2, ..., a_k, a_{k+1}\}$, and $B = \{a_1, a_2, ..., a_k\} \subseteq A$.

$\therefore n(B) = k$.

According to the axiom of the mathematical induction, we conclude that

$n(P(B)) = 2^k$.

Now, Let $W \subseteq A$, and there are two possibilities

(a) $a_{k+1} \notin W$, in this case $W \subseteq B$.

(b) $a_{k+1} \in W$, or $W = D \cup \{a_{k+1}\}$, where $D \subseteq B$. i.e. $W \subseteq A \to W \subseteq B \vee W = D \cup \{a_{k+1}\}, D \subseteq B$.

$\therefore n(P(A)) = 2^k + 2^k = 2.2^k = 2^{k+1}$. Thus, $P(k + 1)$ is true.

$\therefore P(m)$ is true $\forall m \in \mathbb{N}$. ♦

Theorem 2.14 *Let A, B be sets then*

(i) $A \subseteq B \leftrightarrow P(A) \subseteq P(B)$.

(ii) $P(A) \cap P(B) = P(A \cap B)$.

(iii) $P(A) \cup P(B) = P(A \cup B)$.

Proof

(i) Let $A \subseteq B, X \in P(A)$.

$$\text{Now}, X \in P(A) \to X \subseteq A$$
$$\to X \subseteq B$$
$$\to X \in P(B)$$
$$\text{Or, } X \in P(A) \to X \in P(B)$$
$$\therefore P(A) \subseteq P(B)$$

Conversully, suppose that $P(A) \subseteq P(B)$, we have to prove $A \subseteq B$

Suppose that $a \in A$

$$\therefore \{a\} \in A$$

Based on the difinition of the power set $\{a\} \in A$

$$\to \{a\} \in B$$
$$\therefore \{a\} \subseteq B. \text{ Or, } a \in B$$

Thus, we conclude that $a \in A \to a \in B$

$$\to A \subseteq B.$$

(ii) Suppose that

$$X \in P(A) \cap P(B)$$
$$\therefore X \in P(A) \wedge X \in P(B)$$

Based on the difinition of the power set, we find that

$$X \subseteq A \wedge X \subseteq B$$
$$\to X \subseteq A \cap B$$
$$\to X \in P(A \cap B)$$

We conclude that $X \in P(A) \cap P(B) \to X \in P(A \cap B)$

$$\to P(A) \cap P(B) \subseteq P(A \cap B) ...(1).$$

In the same manner, suppose that $Y \in P(A \cap B)$

$$\therefore Y \subseteq A \cap B$$
$$\to Y \subseteq A \wedge Y \subseteq B$$

Now, based on the definition of power sets, we obtain that

$$Y \in P(A) \wedge Y \in P(B)$$
$$\to Y \in P(A) \cap P(B)$$

We conclude that $Y \in P(A \cap B) \to Y \in P(A) \cap P(B)$

$$\therefore P(A \cap B) \subseteq P(A) \cap P(B) ...(2).$$

From, (1)&(2) $P(A \cap B) = P(A) \cap P(B)$.

(iii) It is left as an exercise for the reader. ♦

2.7.2 Index Family of Sets

Definition 2.9 Let F be a power set, and let I be a set. If $\forall i \in I, \exists! A_i \in F$. Then, I called indexed set, the element i is called the index for A_i, and F is called the power set related to the indexed set I, or index family of sets, and denoted by $\{A_i\}_{i\in I}$ (Halmos, 2017b; Warner, 1965; Blyth, 1975; Munkres, 2000).

Note: If the indexed set I is finite, then we have a finite family of sets, otherwise there is an infinite family of sets.

Example 2.11 (i) Let $I = \{1, 2, 3, 4, 5, 6\}, J = \{a, b, c, d, e\}$. Let $F = \{A_a, A_b, A_c, A_d, A_e\}, M = \{B_1, B_2, B_3, B_4, B_5, B_6\}$. Then F is an indexed family of sets related to the indexed set J, and can be written as $F = \{A_j\}_{j\in J}$. Also, M is an indexed family of sets related to the indexed set B, and can be written as $M = \{B_i\}_{i\in I}$.

(ii) Let $i \in \mathbb{N}$ and let $A_i = (i, \infty)$. Then $\{A_i\}_{i\in I}$ is an infinite index set, and the indexed set $\mathbb{N}$ is infinite set.

Note that $... \subset A_n \subset A_{n-1} \subset ... \subset A_3 \subset A_2 \subset A_1 \subset A_0$, where $A_0 = (0, \infty), A_1 = (1, \infty), A_2 = (2, \infty), ...$

2.7.3 Generalized Union and Intersection

Definition 2.10 Let $\{A_i\}_{i\in I}$ be an index family of sets. The union of sets A_i is the set contains of the all elements in which belong to at least one of A_i of power sets, and denoted by $\bigcup\limits_{i\in I} A_i$. Mathematically, $\bigcup\limits_{i\in I} A_i = \{x | \exists j \in I \ni x \in A_j\}$ (Itō, 1993; Mustafa et al., 1980).

Theorem 2.15 *Let $\{A_i\}_{i\in I}$ be any index family of sets*

(i) *If $A_i \subseteq B$ $\forall i \in I$, then* $\bigcup\limits_{i\in I} A_i \subseteq B$.

(ii) *If $B \subseteq A_i$ $\forall i \in I$, then* $B \subseteq \bigcap\limits_{i\in I} A_i$.

Proof

(i) Suppose that $A_i \subseteq B\ \forall i \in I$, and $x \in \bigcup\limits_{i\in I} A_i$.

$$\begin{aligned} &\therefore j \in I \ni x \in A_j \\ &\text{since } A_j \subseteq B, \\ &\therefore x \in B \\ &\text{Or, } A_i \subseteq B\ \forall i \in I. \end{aligned}$$

(ii) It is left as an exercise for the reader. ♦

Theorem 2.16 ***Generalized of the De Morgan's Laws:*** *Let* $\{A_i\}_{i\in I}$ *be an index family of sets, then*

(i) $(\bigcup\limits_{i\in I} A_i)^c = \bigcap\limits_{i\in I} A_i^c$.

(ii) $(\bigcap\limits_{i\in I} A_i)^c = \bigcup\limits_{i\in I} A_i^c$.

Proof

(i) Suppose that $x \in (\bigcup\limits_{i\in I} A_i)^c$.

$$\begin{aligned} \text{Now } x \in (\bigcup_{i\in I} A_i)^c &\rightarrow x \notin \bigcup_{i\in I} A_i \\ &\rightarrow x \notin A_i, \forall i \in I \\ &\rightarrow x \in A_i^c, \forall i \in I \\ &\rightarrow x \in \bigcap_{i\in I} A_i^c \\ \therefore (\bigcup_{i\in I} A_i)^c &\subseteq \bigcap_{i\in I} A_i^c ...(1) \end{aligned}$$

$$\begin{aligned} \text{Conversaly, suppose that } y &\in \bigcap_{i\in I} A_i^c \\ \therefore y &\in A_i^c \\ \text{Since } y \in A_i^c &\rightarrow y \notin A_i, \forall i \in I \\ &\rightarrow y \notin \bigcup_{i\in I} A_i \\ &\rightarrow y \in (\bigcup_{i\in I} A_i)^c \\ \therefore \bigcap_{i\in I} A_i^c &\subseteq (\bigcup_{i\in I} A_i)^c ...(2). \\ \text{From } (1)\&(2) (\bigcup_{i\in I} A_i)^c &= \bigcap_{i\in I} A_i^c. \end{aligned}$$

(ii) It is left as an exercise for the reader. ♦

Theorem 2.17 ***Generalized of the Distribution Law***

Let each of $\{A_i\}_{i\in I}, \{B_j\}_{j\in J}$ be index family of sets, then

(i) $(\bigcup\limits_{i\in I} A_i)\bigcap(\bigcup\limits_{j\in J} B_j) = \bigcup\limits_{(i,j)\in I\times J}(A_i\bigcap B_j)$.

(ii) $(\bigcap\limits_{i\in I} A_i)\bigcup(\bigcap\limits_{j\in J} B_j) = \bigcap\limits_{(i,j)\in I\times J}(A_i\bigcup B_j)$.

Proof

(i) Suppose that $x \in (\bigcup\limits_{i\in I} A_i)\bigcap(\bigcup\limits_{j\in J} B_j)$.

$$\text{Now } x \in (\bigcup_{i\in I} A_i)\bigcap(\bigcup_{j\in J} B_j)(\exists h \in I \ni x \in A_h) \wedge (\exists k \in J \ni x \in B_k)$$

$$\to \exists(h,k) \in I \times J \ni x \in A_h \bigcap B_k$$

$$\to x \in \bigcup_{(i,j)\in I\times J}(A_i\bigcap B_j)$$

$$\therefore (\bigcup_{i\in I} A_i)\bigcap(\bigcup_{j\in J} B_j) \subseteq \bigcup_{(i,j)\in I\times J}(A_i\bigcap B_j)...(1).$$

$$\text{Conversely, suppose that } y \in \bigcup_{(i,j)\in I\times J}(A_i\bigcap B_j)$$

$$\therefore \exists(s,t) \in I \times J \ni y \in A_s \bigcap B_t$$

$$\therefore (\exists s \in I \wedge t \in J) \ni (y \in A_s \wedge y \in B_t)$$

$$\text{Or } (\exists s \in I \ni y \in A_s) \wedge (\exists t \in J \ni y \in B_t)$$

$$\therefore y \in \bigcup_{i\in I} A_i \wedge y \in \bigcup_{j\in J} B_j$$

$$\to y \in \bigcup_{(i,j)\in I\times J}(A_i\bigcap B_j)$$

$$\therefore \bigcup_{(i,j)\in I\times J}(A_i\bigcap B_j) \subseteq (\bigcup_{i\in I} A_i)\bigcap(\bigcup_{j\in J} B_j)...(2).$$

$$\text{From (1)\&(2) } (\bigcup_{i\in I} A_i)\bigcap(\bigcup_{j\in J} B_j) = \bigcup_{(i,j)\in I\times J}(A_i\bigcap B_j).$$

(ii) It is left as an exercise for the reader. ♦

2.8 Exercises

Solve the following questions:

Q1: Let $\{A_i\}_{i\in I}, \{B_j\}_{j\in J}$ be two index family of sets. Prove

(i) $(\bigcup_{i\in I} A_i) - (\bigcup_{j\in J} B_j) = \bigcup_{i\in I}(\bigcap_{j\in J}(A_i - B_j))$.

(ii) $(\bigcap_{i\in I} A_i) - (\bigcap_{j\in J} B_j) = \bigcap_{i\in I}(\bigcup_{j\in J}(A_i - B_j))$.

Q2: The index family of sets $\{B_i\}_{i\in I}$ is said to be covering of A if $A \subseteq \bigcup_{i\in I} B_i$. Prove that if $\{B_i\}_{i\in I}, \{C_j\}_{j\in J}$ two different covering of A. Then the index family of sets $\{B_i \bigcap C_j\}_{(i,j)\in I\times J}$ is covering of A.

Q3: Let A, B be two sets. Prove that

(i) $A = B \leftrightarrow P(A) = P(B)$.

(ii) $P(A) \bigcup P(B) \subseteq P(A \bigcup B)$.

(iii) Give an example to show that $P(A) \bigcup P(B) \neq P(A \bigcup B)$.

(iv) $A \bigcap B = \phi \leftrightarrow P(A) \bigcap P(B) = \{\phi\}$.

Q4: Let $\Psi = \mathbb{Z}^+$, $A_\alpha = \{1, \frac{1}{2}, \frac{1}{3}, ..., \frac{1}{\alpha}\}$, and let $\mathcal{X} = \{P \in \mathbb{R} | 0 \leq P \leq 1\}$, then find each of the following;

(i) $\bigcap\{A_\alpha | \alpha \in \Psi\}$.

(ii) $\bigcup\{A_\alpha | \alpha \in \Psi\}$.

(iii) $\bigcup\{\mathcal{X} - A_\alpha | \alpha \in \Psi\}$.

(iv) $\bigcap\{\mathcal{X} - A_\alpha | \alpha \in \Psi\}$.

Q5: If $\{A_\alpha | \alpha \in \Psi\}$ is an index family of sets of $\mathcal{X}$, in which $\bigcap\{A_\alpha | \alpha \in \Psi\} = \phi$, then prove that $\bigcup\{\mathcal{X} - A_\alpha | \alpha \in \Psi\} = \mathcal{X}$.

Q6: Consider $U = \{7, 8, 9, 10, 11, 12, 13\}, A = \{11, 12, 13\}, B = \{7, 8\}$. Find the following;

(i) $A \cup B$.

(ii) $(A \cup B)'$.

(iii) A'.

(iv) B'.

(v) $A' \cap B'$.

(vi) $A \cap B$.

(vii) $(A \cap B)'$.

(viii) $A' \cup B'$.

(ix) What do you notice?

3

Relations

3.1 Introduction

Social relation, in social science, is any social interaction between two or more individuals. International relation is studying interconnections of politics, economics and law on a global level. Public relation is managing the spread of information to the public. Interpersonal relationship is association or acquaintance between two or more people. . . etc.

In mathematics, there are many kinds of relations like, binary relation, or dyadic relation or two place relation. Heterogeneous relation is relations between distinct sets, relations with a finite number of places. And relation algebra is an algebraic structure inspired by algebraic logic.

Mathematical science deals with a special kinds of sets called relations. Let the set A consists of two things x, y. In many cases or situations it is necessary to deal with these two things. For example,

- The bigger (smaller) relation, if $x, y \in \mathbb{Z}$.
- The longer (shorter) relation, if $x, y \in S; S =$ the set of persons.
- The parallel relation, if $x, y \in S; S =$

the set of straight lines in the tesesian plane.

- The divisibility on relation, if $x, y \in \mathbb{Z}$.
- The humanity relation, if $x, y \in \mathbb{H}; \mathbb{H} =$ human society.

Before dealing with the definition of relation and what related it, we have to know what is ordered pairs and Cartesian product? The next section provides logically convincing answers.

3.2 Ordered Pairs

Definition 3.1 Let $A = \{a, b\}$. The set $\{a, \{a, b\}\}$ is called ordered pairs a, b, $\forall a, b \in A$ (Quine, 1969; Quine, 2013).

Theorem 3.1 *If* $\{a, \{a, b\}\} = \{c, \{c, d\}\}$*then* $a = c$*, and* $b = d$.

Proof Based on the Definition 3.1, we easily get the proof. ⧫

Note: If $a \neq b$ then $\{a, \{a, b\}\} \neq \{b, \{a, b\}\}$ then, we can denote to the set $\{a, \{a, b\}\}$ by the symbol (a, b), and called the ordered pairs a, b. Thus, the Theorem 3.1 can be reformulated as the following theorem.

Theorem 3.2 $(a, b) = (c, d) \leftrightarrow a = c \wedge b = d.$

Definition 3.2 The set X is called ordered pairs, if there is object(thing)s $a, b \in X \ni X = (a, b)$. a is called the first projection of the X, while b is the second projection of X. (Mustafa et al., 1980; Quine, 1969; Quine, 2013).

Note: It is possible to the generalized the ordered pairs on a set consisting of n of elements where $1 \leq n \in \mathbb{Z}^+$. For example, any set consists of three elements a, b, c the triple tuple (a, b, c) can be defined as follows $(a, b, c) = ((a, b), c)$. In general if the set consists of n pairs $a_1, a_2, ..., a_n$ then $n-$tuples $(a_1, a_2, ..., a_n)$ can be defined as $(a_1, a_2, ..., a_n) = ((a_1, a_2, ..., a_{n-1}), a_n)$.

3.2.1 Cartesian Product

If there are two sets A, B then it is possible to generate another set from A, B by using the concept of the ordered pairs.

Definition 3.3 Let each of A, B be a set. The Cartesian product of A, B is a set of all elements (a, b) in which $a \in A \wedge b \in B$, and denoted by $A \times B$. Or, $A \times B = \{(a, b) | a \in A \wedge b \in B\}$(Warner, 1965; Warner, 1990).

Example 3.1 (i) Let $A = \{1, 3, 5\}, B = \{0, -2, -4\}$ then

$A \times B = \{(1, 0), (1, -2), (1, -4), (3, 0), (3, -2), (3, -4), (5, 0), (5, -2), (5, -4)\}$

Also,

$B \times A = \{(0, 1), (0, 3), (0, 5), (-2, 1), (-2, 3), (-2, 5), (-4, 1), (-4, 3), (-4, 5)\}$

It noted that $A \times B \neq B \times A$.

(ii) Let $A = \mathbb{R}$, then $\mathbb{R} \times \mathbb{R} = \{(a, b) | a \in \mathbb{R} \wedge b \in \mathbb{R}\}$.

Or, $\mathbb{R} \times \mathbb{R} = \{(a, b) | a, b \in \mathbb{R}\}$.

Note:

(i) If A Containing n elements, and B Containing m elements then $A \times B = n \times m$ of ordered pairs.

(ii) If A, B are infinite sets then $A \times B$ is infinite set too.

(iii) If A, B are empty sets then $A \times B$ is empty set too.

Theorem 3.3 *Let $A, B \neq \phi$. $A \times B = B \times A \leftrightarrow A = B$.*

Proof Suppose that $A = B$. Obviously, $A \times A = A \times A$. $\because A = B$, $\therefore A \times B = B \times A$ ...(1).

Conversely, suppose that $A \times B = B \times A$, and let $a \in A$.

$$\begin{gathered}\text{Now, } a \in A \rightarrow \forall b \in B \ni (a,b) \in A \times B\\ \rightarrow (a,b) \in B \times A\\ \therefore (a,b) \in B \times A \rightarrow a \in A \wedge b \in B\\ \because a \in A \rightarrow a \in B\\ \therefore A \subseteq B\\ \text{Through the same method, we can prove that } B \subseteq A\\ \therefore A = B...(2).\\ \text{From, }(1)\&(2), A \times B = B \times A \leftrightarrow A = B. \ \blacklozenge\end{gathered}$$

Theorem 3.4 *If each of A, B, C, D is a set, then*

(i) $A \times (B \bigcap C) = (A \times B) \bigcap (A \times C)$.

(ii) $A \times (B \bigcup C) = (A \times B) \bigcup (A \times C)$.

(iii) $(A \times B) \bigcap (C \times D) = (A \bigcap C) \times (B \bigcap D)$.

Proof

(i) Let, $(x,y) \in A \times (B \bigcap C)$

$$\begin{gathered}\text{Now, } (x,y) \in A \times (B \bigcap C) \rightarrow x \in A \wedge y \in (B \bigcap C)\\ \rightarrow x \in A \wedge (y \in B \wedge y \in C)\\ \rightarrow (x \in A \wedge y \in B) \wedge (x \in A \wedge y \in C)\\ \rightarrow (x,y) \in (A \times B) \wedge (x,y) \in (A \times C)\\ \rightarrow (x,y) \in (A \times B) \bigcap (A \times C)...(1).\\ \text{Conversely, suppose that } (a,b) \in (A \times B) \bigcap (A \times C)\\ \text{Now, } (a,b) \in (A \times B) \bigcap (A \times C)\\ \rightarrow (a,b) \in (A \times B) \wedge (a,b) \in (A \times C)\\ \rightarrow (a \in A \wedge b \in B) \wedge (a \in A \wedge b \in C)\\ \rightarrow a \in A \wedge (b \in B \wedge b \in C)\\ \rightarrow a \in A \wedge (b \in B \bigcap C)\\ \rightarrow (a,b) \in A \times (B \bigcap C)\\ \therefore (A \times B) \bigcap (A \times C) \subseteq A \times (B \bigcap C)...(2).\\ \text{From }(1)\&(2) A \times (B \bigcap C) = (A \times B) \bigcap (A \times C).\end{gathered}$$

(ii) It is left as an exercise to the reader.

(iii) Suppose that $(x, y) \in (A \times B) \bigcap (C \times D)$.

$$\begin{gathered}
\text{Now, } (x, y) \in (A \times B) \bigcap (C \times D) \\
\to (x, y) \in (A \times B) \wedge (x, y) \in (C \times D) \\
\to (x \in A \wedge y \in B) \wedge (x \in C \wedge y \in D) \\
\to (x \in A \wedge x \in C) \wedge (y \in B \wedge y \in D) \\
\to x \in (A \bigcap C) \wedge y \in (B \bigcap D) \\
\to (x, y) \in (A \bigcap C) \times (B \bigcap D) \\
\to (A \times B) \bigcap (C \times D) \subseteq (A \bigcap C) \times (B \bigcap D) ...(1). \\
\text{Conversely, suppose that } (a, b) \in (A \bigcap C) \times (B \bigcap D) \\
\text{Now, } (a, b) \in (A \bigcap C) \times (B \bigcap D) \\
\to a \in (A \bigcap C) \wedge b \in (B \bigcap D) \\
\to (a \in A \wedge a \in C) \wedge (b \in B \wedge b \in D) \\
\to (a \in A \wedge b \in B) \wedge (a \in C \wedge b \in D) \\
\to (a, b) \in (A \times B) \wedge (a, b) \in (C \times D) \\
\to (a, b) \in (A \times B) \bigcap (C \times D) \\
\to (A \bigcap C) \times (B \bigcap D) \subseteq (A \times B) \bigcap (C \times D) ...(2) \\
\text{From, } (1)\&(2) (A \bigcap C) \times (B \bigcap D) = (A \times B) \bigcap (C \times D). \ \blacklozenge
\end{gathered}$$

3.2.2 Co-ordinate Diagram

To explain the relationships between the Cartesian product of sets, we use the horizontal and vertical axes in the Cartesian coordinates and in the first quarter only. The line segment of the horizontal axis represents A, while the line segment of the vertical axis represents the set B. The rectangle in the first quarter represents the set of $A \times B$, as shown in the Figure 3.1.

Example 3.2 If A, B, C, D are sets then the $(A \times B) \bigcap (C \times D)$ is as shown in the Figure 3.2. Where, $R = (A \times B) \bigcap (C \times D)$, $A = [a_1, b_1], B = [c_1, d_1], C = [a_2, b_2], D = [c_2, d_2]$.

3.2.3 Generalization of Cartesian Product

Definition 3.4 Let each of A, B, C be a set. The set of Cartesian product of A, B, C is the set of all elements (a, b, c) in which $a \in A, b \in B, c \in C$, and denoted by $A \times B \times C$.

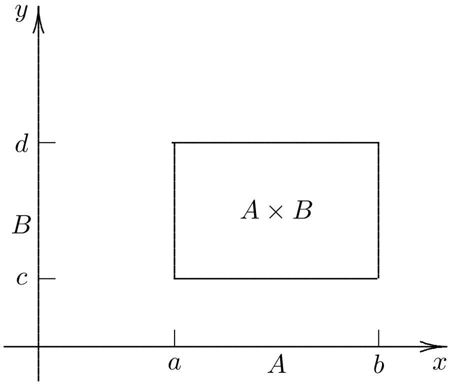


Figure 3.1: The Cartesian Product Region $A \times B$

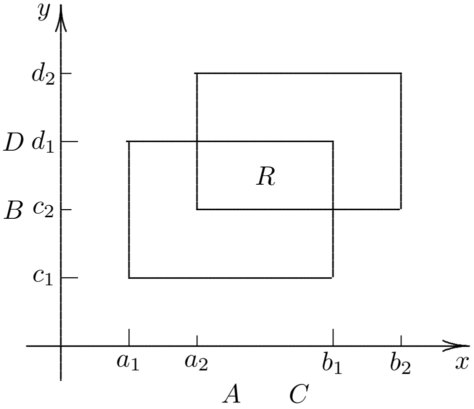


Figure 3.2: The Cartesian Product Region R

In other words $A \times B \times C = \{(a,b,c)|a \in A \wedge b \in B \wedge c \in C\}$ (D'angelo and West, 1997; Vander Waerden, 1949; Wilder et al., 2012).

It is defined as the following;

Definition 3.5 Let $A_1, A_2, ..., A_n$ be sets. The Cartesian product of the sets $A_i; i = 1, 2, ..., n$ is the set in which all $n-tuples(a_1, a_2, ..., a-n)$ in which $a_i \in A_i; 1 \leq i \leq n$, and denoted by the symbol $A_1 \times A_2 \times ... \times A_n$.

Or, $\prod_{i=1}^{n} A_i = \{(a_1, a_2, ..., a_n)|a_i \in A_i, 1 \leq i \leq n\}$.

Example 3.3 Let us consider $A_i = \mathbb{R}; 1 \leq i \leq n$, then: $\prod_{i=1}^{n} A_i = \{(a_1, a_2, ..., a_n)|a_i \in \mathbb{R}, 1 \leq i \leq n\} = \mathbb{R}^n$.

3.3 Exercises

Solve the following questions:

Q1: If $(a-b, 2a-7b) = (a+b, 3a+5b)$ then find a value of a, b.

Q2: If $(u, v, w) = (x, y, z)$ then prove that $u = x, v = y, w = z$.

Q3: If $A = \{1, 3, 5, 7\}, B = \{-2, -9, 6\}, C = \{x, y, z\}$, find each of: (1) $(A \bigcup B) \times C$. (2) $(A \times C) \bigcup (B \times C)$. (3) $(A \bigcup B) \times (B \bigcup C)$.

Q4: Let A, B, C, D be sets. Prove the following statements:

(i) $(A \times A) \bigcap (B \times C) = (A \bigcap B) \times (A \bigcap C)$.

(ii) $(A \times B) - (C \times C) = [(A - C) \times B] \bigcup [A \times (B - C)]$.

(iii) $(A \times A) - (B \times C) = [(A - B) \times A] \bigcup [A \times (A - C)]$.

(iv) $A \times (B - D) = (A \times B) - (A \times D)$.

(v) $(A \times B) \bigcap (C \times D) = (A \times D) \bigcap (C \times B)$.

Q5: If each of A, B, C be set such that $A \neq \phi, B \neq \phi$, and if $(A \times B) \bigcup (B \times A) = C \times C$, then prove that $A = B = C$.

Q6: If A, B, C are sets, and $A \subseteq B$ then prove that $A \times C \subseteq B \times C$.

Q7: Prove that

$\{s_1, s_2, ..., s_n\} \times A = (\{s_1\} \times A) \bigcup (\{s_2\} \times A) \bigcup ... \bigcup (\{s_n\} \times A)$.

Q8: Give an example for A, B, C to show that $A \bigcup (B \times C) \neq (A \bigcup B) \times (A \bigcup C)$.

Q9: If $A \times A = B \times B$ then $A = B$.

Q10: If $A \times Y = A \times Z$, $A \neq \phi$ then $B = C$.

Q11: Let $A, C \neq \phi$ and $A \subseteq B \wedge C \subseteq D \leftrightarrow A \times C \subseteq B \times D$.

Q12: Consider a nonempty sets A, B, C, D. Prove that $A \times B = C \times D \leftrightarrow A = C \wedge B = D$.

3.4 Binary Relation

Definition 3.6 Let each of A, B be a set, and $P(x, y)$ be an open sentence defined on the Cartesian product $A \times B$. The ordered triple (3-tuple) $A, B, P(x, y)$ is called a relation from A to B, and the truth set according to $P(x, y)$ is called graph of the relation and denoted by G.

Or, $G = \{(x, y) \in A \times B | P(x, y) \text{ is true}\}$ (Itō, 1993; Mustafa et al., 1980; Suppes, 1960; Suppes, 1972; Smullyan, 1996; Levy, 2002).

Note: It will be noted that $G \subseteq A \times B$. If we consider $T \subseteq A \times B$ then a relation from A to B can be defined as follows;

Let $P(x, y)$ be a statement on $A \times B$, it means $(x, y) \in T$. The ordered triple $(A, B, P(x, y))$ is a relation and T is the truth set, or T is a graph of the relation. It means there is a correspondance between A to B and the subsets $A \times B$.

Definition 3.7 Let each of A, B be a set. Any subset of $A \times B$ is a relation from A to B(Itō, 1993; Mustafa et al., 1980; Suppes, 1960; Suppes, 1972; Smullyan, 1996; Levy, 2002).

Note: According to the definition, if we suppose R is a relation from A to B, then $R \subseteq A \times B$.

3.5 Expression of the Relation

We will express the relation as a set by one of the following methods;

(i) Write its elements (ordered pairs, ordered triple, ..., $n-$tuple) between braces. This method called tabulation method (See 1.5.1(ii)).

(ii) Rule method or, writing the relation by its own property. As $R = \{(x,y)|x \in A \wedge y \in B, P(x,y)\}$, where $P(x,y)$ is the characteristic of R (See 1.5.1(iii)).

Note: If $(x,y) \in R$, then we will express in this membership by xRy, and read x is related with y via the relation R. And if $(x,y) \notin R$, it can be written $x \not R\, y$, and read x does not related with y.

Definition 3.8 If R is a relation from A to A, then $R \subseteq A \times A$ and called R is a relation on A (Itō, 1993; Mustafa et al., 1980; Suppes, 1960; Suppes, 1972; Smullyan, 1996; Levy, 2002).

Note:

(i) Any subset of A is a single relation on A.

(ii) Any subset of $A \times B \times C$ is called a triple relation on A, B, C.

(iii) Any subset of $A_1 \times A_2 \times .... \times A_n$ is called $n-$ relation on $A_i; i = 1, 2, ..., n$.

Note: The study for this book will focus on the binary relation.

Example 3.4 Let $A = \{1,3,5\}, B = \{0,2,4,6\}$ then:

(i) The set $R_1 = \{(x,y) \in A \times B|x < y\}$
$= \{(1,2),(1,4),(1,5),(1,6),(3,4),(3,6),(5,6)\}$.

(ii) The set $R_2 = \{(x,y)) \in A \times B|x > y\}$
$= \{(1,0),(3,0),(3,2),(5,0),(5,2),(5,4)\}$.

(iii) The set $R_3 = \{(x,y)) \in A \times B|x = y\} = \phi$.

(iv) The set $R_4 = \{(x,y)) \in B \times A|x > y\}$
$= \{(2,1),(4,1),(4,3),(6,1),(6,3),(6,5)\}$.

Example 3.5 Let A the set of all straight lines in the plane, then

(i) The set $R_1 = \{(x, y) \in \mathbb{R} \times \mathbb{R} | x \parallel y\}$ is the relation on A such that xRy and x is parallels to y.

(ii) The set $R_2 = \{(x, y) \in \mathbb{R} \times \mathbb{R} | x \perp y\}$ is the relation on A such that xRy and x, y are orthogonal.

Example 3.6 Let X by any set, the set
$R = \{(A, B) \in P(x) \times P(X) | A \subseteq B\}$ is the relation on the power set $P(X)$ provided the first ordered pair is subset of the second ordered pair.

Note: Since the relation from a set to another set is a set, then all the algebra relations on sets are hold in relations too. For example let R, Q be relations from A to B. Or, $R \subseteq A \times B, Q \subseteq A \times B$ then

(i) Union of the relations
$R \bigcup Q = \{(x, y) \in A \times B | (x, y) \in R \vee (x, y) \in Q\}$ is a relation from A to B.

(ii) Intersection of the relations
$R \bigcap Q = \{(x, y) \in A \times B | (x, y) \in R \wedge (x, y) \in Q\}$ is a relation from A to B.

(iii) The difference of the relations
$R - Q = \{(x, y) \in A \times B | (x, y) \in R \wedge (x, y) \in Q^c\}$ is a relation from A to B.

Example 3.7 Let $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} | x^2 + y^2 = 4\}$,
$Q = \{(x, y) \in \mathbb{R} \times \mathbb{R} | 3x - 5y = 7\}$. Then:

(i) $R \bigcup Q = \{(x, y) \in \mathbb{R} \times \mathbb{R} | x^2 + y^2 = 4 \vee 3x - 5y = 7\}$.

(ii) $R \bigcap Q = \{(x, y) \in \mathbb{R} \times \mathbb{R} | x^2 + y^2 = 4 \wedge 3x - 5y = 7\}$.

(iii) $R - Q = \{(x, y) \in \mathbb{R} \times \mathbb{R} | x^2 + y^2 = 4 \wedge 3x - 5y \neq 7\}$.

3.6 Basic Concepts of Relations

3.6.1 Identity Relation

Definition 3.9 Let A be any set, the set whose its ordered pairs $(x, y) \in A \times A$ where $x = y$ is called identity relation on A, and denoted by the symbol I_A. Or, $I_A = \{(x, y) \in A \times A | x = y\}$(Hafstrom, 2013; Herstein, 1975; Wilder et al., 2012; Zulauf, 1969b; Zulauf, 1969a).

Example 3.8 (i) Let $A = \{a, b, c, d\}$.

The $I_A = \{(a, a), (b, b), (c, c), (d, d)\}$.

(ii) If $A = \mathbb{Z}$.

The $I_A = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | x = y\}$

$= \{..., (-2, -2), (-1, -1), (0, 0), (1, 1), (2, 2), ...\}$.

(iii) If $A = \mathbb{N}$.

The $I_A = \{(x, y) \in \mathbb{N} \times \mathbb{N} | x = y\} = \{(0, 0), (1, 1), (2, 2), ...\}$.

3.6.2 Inverse Relation

Definition 3.10 Let R be a relation from the set A to the set B. The relation from B to A whose its ordered pairs are (y, x) such that $(x, y) \in R$ is called inverse relation, and denoted by R^{-1}. Or, $R^{-1} = \{(y, x) | (x, y) \in R\}$(Itō, 1993; Mustafa et al., 1980; Wilder et al., 2012; Suppes, 1960; Suppes, 1972; Smullyan, 1996; Levy, 2002).

Note: $(x, y) \in R \leftrightarrow (y, x) \in R^{-1}$.

Theorem 3.5 *If R is a relation on A, then $(R^{-1})^{-1} = R$.*

Proof Suppose that, $(x, y) \in (R^{-1})^{-1}$.

$$\begin{gathered}
\text{Now, } (x,y) \in (R^{-1})^{-1} \\
\to (x,y) \in (y,x) \in R^{-1} \\
\to (x,y) \in R. \therefore (R^{-1})^{-1} \subseteq R...(1). \\
\text{Conversely, suppose that} (x,y) \in R \\
\text{Now,} (x,y) \in R \to (y,x) \in R^{-1} \\
\to (x,y) \in (R^{-1})^{-1} \\
\to R \subseteq (R^{-1})^{-1}...(2). \\
\text{Thus, from(1)\&(2), } (R^{-1})^{-1} = R. \ \blacklozenge
\end{gathered}$$

Example 3.9 (i) Consider $A = \{a, b, c\}$, $B = \{x, y\}$. If $R = \{(a, x), (c, y), (b, y)\}$ is a relation from A to B. Then, $R^{-1} = \{(x, a), (y, c), (y, b)\}$ is the inverse relation from B to A.

(ii) Let ψ be a relation on $\mathbb{Z}^+$ as $\psi = \{(x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+ | y = 5\} = \{(1, 5), (2, 5), (3, 5), ...\}$. The $\psi^{-1} = \{(y, x) \in \mathbb{Z}^+ \times \mathbb{Z}^+ | x = 5\} = \{(5, 1), (5, 2), (5, 3), ...\}$ is the inverse relation on $\mathbb{Z}^+$.

(iii) Let Γ be a relation on $\mathbb{R}$ as: $\Gamma = \{(x, y) \in \mathbb{R} \times \mathbb{R} | y = \sqrt{x}\}$. Thus, $\Gamma^{-1} = \left\{(y, x) \in \mathbb{R} \times \mathbb{R} | x = \sqrt{y}\right\}$ is the inverse relation on $\mathbb{R}$.

3.6.3 Domain and Range of a Relation

Definition 3.11 Let R be a relation from the set A to the set B. Then:

(i) The first elements of the ordered pairs in R is called domain of R, denoted by *dom* R. Or, *dom* $R = \{x | \exists y \in B \ni (x, y) \in R\}$.

(ii) The second elements of the ordered pairs in R is called range of R, denoted by *ran* R. Or, *ran* $R = \{y | \exists x \in A \ni (x, y) \in R\}$ (Paley and Weichsel, 1966; Wilder et al., 2012; Warner, 1965; Warner, 1990).

Note: (1) *dom* $R \subseteq A$. (2) *ran* $R \subseteq B$.

Example 3.10 (i) Let $A = \{7, 11, 13\}, B = \{0, 2, 4\}$, and let $R = \{(7, 0), (7, 0), (13, 2)\}$ be a relation from A to B. Then, *dom* $R = \{7, 13\}$, *ran* $R = \{0, 2\}$.

(ii) Let Ψ be a relation on $\mathbb{R}$ defined as $\Psi = \{(x, y) \in \mathbb{R} \times \mathbb{R} | y = x^2\}$. Then $dom\ \Psi = \{x|\exists y \in \mathbb{R} \ni (x, y) \in \Psi\} = \{x|\exists y \in \mathbb{R} \ni y = x^2\}$. Thus, $dom\ \Psi = \mathbb{R}$. $ran\ \Psi = \{y|\exists x \in \mathbb{R} \ni (x, y) \in \Psi\} = \{y|\exists x \in \mathbb{R} \ni y = x^2\}$. Thus, $ran\ \Psi = \{y|y \geq 0\} = \mathbb{R}^+$.

Theorem 3.6 *If R is a relation from the set A to the set B. Then*

(i) $dom\ R = ran\ R^{-1}$.

(ii) $ran\ R = dom\ R^{-1}$.

Proof

(i) Suppose that $x \in dom\ R$.

$$\begin{gathered}
\text{Now } x \in dom\ R \rightarrow \exists y \in B \ni (x, y) \in R \\
\rightarrow \exists y \in B \ni (y, x) \in R^{-1} \\
\rightarrow x \in ran\ R^{-1} \\
\therefore dom\ R \subseteq ranR^{-1}...(1). \\
\text{Converaly, suppose that } y \in ran\ R^{-1} \\
\text{Now } y \in ran\ R^{-1} \rightarrow \exists x \in B \ni (x, y) \in R^{-1} \\
\rightarrow \exists x \in B \ni (y, x) \in R \\
\rightarrow y \in dom\ R \\
\therefore ran\ R^{-1} \subseteq dom\ R...(2). \\
\text{From}(1)\&(2), dom\ R = ran\ R^{-1}.
\end{gathered}$$

(ii) It is left as an exercise for the reader. ⧫

3.6.4 Restriction of a Relation

Definition 3.12 Let R be a relation from the set A to the set B, and let $C \subseteq A, D \subseteq B$. The set $R \bigcap (C \times D)$ is called restriction of a relation R from C to D (Stoll, 1960).

Note: If $A = B, C = D$ then R becomes a relation on A. Then, $R \bigcap (C \times D)$ is called restriction of a relation R on C, and denoted by R/C.

Example 3.11 (i) Consider $A = \{x|x \in \mathbb{Z}_e^-\}$, $B = \{x|x \in \mathbb{Z}_o^-\}$, and let $C = \{-6, -12, -18\}$, $D = \{-3, -5, -9\}$. If R is a relation from A to B, and defined as

$R = \{(x, y) \in A \times B|$ x is dividable on y$\}$. The restriction of R from C to D is the set

$R \bigcap (C \times D) = \{(-6, -3), (-12, -3), (-18, -3), (-18, -9)\}$.

(ii) Let $A = \{x|x \in \mathbb{Z} \ni -20 \leq x \leq 20\}$, $B = \{x|x \in \mathbb{N} \ni x \leq 20\}$. If R defined on A as $R = \{(x, y) \in A \times A|y = x^2 + 1\}$ then $R/B = \{(0, 1), (1, 2), (2, 5), (3, 10), (4, 17)\}$.

3.6.5 Composition of Relations

Definition 3.13 If R is a relation from A to B, and S is a relation from Y to Z. A composition of the relation R and S denoted by $S \circ R$ defined as

$S \circ R = \{(x, z) \in X \times Z|\exists y \in Y \ni (x, y) \in R \wedge (y, z) \in S\}$(Jónsson, 1984).

Theorem 3.7 *If R be a relation on A then $I_A \circ R = R \circ I_A = R$.*

Proof First, we prove that $I_A \circ R = R$.

$$\text{Let, } (x, y) \in I_A \circ R$$
$$\therefore \exists z \in A \ni (x, z) \in R \wedge (z, y) \in I_A$$
$$\because (z, y) \in I_A \to z = y$$
$$(x, z) \in R \to (x, y) \in R$$
$$\therefore I_A \circ R \subseteq R...(1).$$
$$\text{Suppose that} (x, y) \in R$$
$$\because (x, y) \in R \wedge (y, y) \in I_A$$
$$\therefore (x, y) \in I_A \circ R$$
$$\therefore R \subseteq I_A \circ R...(2).$$
$$\text{From}(1)\&(2) I_A \circ R = R.$$

Through the same method, $R \circ I_A = R$. ⧫

Theorem 3.8 *Let the given relations R, S, T on A. Then*

(i) $(T \circ S) \circ R = T \circ (S \circ R)$*: Association property for the composition of relations.*

(ii) $(S \bigcup T) \circ R = (S \circ R) \bigcup (T \circ R)$*: Distribution the union of relations over the composition of relations.*

(iii) $(S \bigcap T) \circ R \subseteq (S \circ R) \bigcap (T \circ R)$*: The intersection of relations does not distributes over the composition of relations.*

(iv) *If* $R \subseteq S$ *then*

(a) $T \circ R \subseteq T \circ S$.

(b) $R \circ T \subseteq S \circ T$*: The composition of the relations keeps the containment of relations.*

(v) $(S \circ R) \bigcap T = \phi \leftrightarrow (T \circ R^{-1}) \bigcap S = \phi$.

(vi) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Proof

(i) Suppose that $(x, w) \in (T \circ S) \circ R$.

$$\therefore [\exists y \ni (x,y) \in R \wedge (y,w) \in T \circ S] \wedge [\exists z \ni (y,z) \in S \wedge (z,w) \in T]$$
$$\because (x,y) \in R \wedge (y,z) \in S \to (x,z) \in S \circ R$$
$$\because (x,z) \in S \circ R \wedge (z,w) \in T \to (x,w) \in T \circ (S \circ R)$$
$$\therefore (T \circ S) \circ R \subseteq T \circ (S \circ R) ...(1).$$

By the same method, we can prove that $T \circ (S \circ R) \subseteq (T \circ S) \circ R ...(2)$

$$\text{From}(1)\&(2)(T \circ S) \circ R = T \circ (S \circ R).$$

(ii) It is left as an exercises for the reader.

(iii) It is left as an exercises for the reader.

(iv) Suppose that $(S \circ R) \bigcap T \neq \phi$.

$$\exists(x,y) \ni (x,y) \in (S \circ R) \bigcap T$$
$$\to (x,y) \in S \circ R \wedge (x,y) \in T$$
$$\because (x,y) \in S \circ R \to \exists z \ni (x,z) \in R \wedge (z,y) \in S$$
$$\text{But } (x,z) \in R \to (z,x) \in R^{-1}$$
$$[(z,x) \in R^{-1} \wedge (x,y) \in T] \to (z,y) \in T \circ R^{-1}$$
$$\text{But } (z,y) \in S$$
$$\therefore (z,y) \in (T \circ R^{-1}) \bigcap S$$
$$\to (T \circ R^{-1}) \bigcap S \neq \phi ...(1).$$
$$\text{In the same way } (T \circ R^{-1}) \bigcap S \neq \phi \to (S \circ R) \bigcap T \neq \phi ...(2).$$
$$\text{From(1)\&(2)}, (S \circ R) \bigcap T = \phi \leftrightarrow (T \circ R^{-1}) \bigcap S = \phi.$$

(v) It is left as an exercises for the reader. ♦

Example 3.12 Consider $X = \{1,2,3\}, Y = \{4,5,6,7\}, Z = \{x,y\}$. R is a relation from X to Y and denoted as $R = \{(1,4),(1,5),(2,6)\}$. And, S is a relation from Y to Z denoted as $S = \{(4,y),(5,x)\}$. Then, $S \circ R = \{(1,y),(1,x)\}$ is a relation from X to Z.

Example 3.13 Consider X, Y, Z, R as in previous example, and let $Q = \{(1,4),(2,6)\}$. Note that $Q \subseteq R$, thus, $S \circ Q = \{(1,y)\}$. In the previous example, $S \circ R = \{(1,y),(1,x)\}$ that means $S \circ Q \subseteq S \circ R$.

3.7 Exercises

Answer the following questions:

Q1: Given $X = \{a,b,c,d\}, Y = \{1,2,0\}$. Write down all possible relations from

(i) X to Y.

(ii) Y to X.

Q2: How many relations are there on a set contains of n-elements?

Q3: Given S, T relations from X to Y. Prove that

(i) $(S \bigcap T)^{-1} = S^{-1} \bigcap T^{-1}$.

(ii) $(S \bigcup T)^{-1} = S^{-1} \bigcup T^{-1}$.

Q4: Consider each of R, S be a relation on a set A. Give an example to show that $S \circ R \neq R \circ S$.

Q5: Let $\psi : X \to Y$, and $\varphi : Y \to Z$ be relations, prove that

(i) $dom(\psi \circ \varphi) \subseteq dom\ \varphi$.

(ii) $ran(\psi \circ \varphi) \subseteq ran\ \psi$.

(iii) If $ran\ \varphi \subseteq dom\ \psi$ then, $dom\ (\psi \circ \varphi) = dom\ \varphi$

Q6: Let G, H, J, K relations on a set A. Prove that

(i) $G \subseteq H \wedge J \subseteq K \to G \circ J \subseteq H \circ K$.

(ii) $G \subseteq H \leftrightarrow G^{-1} \subseteq H^{-1}$.

Q7: Given ζ, η relations on A. Prove that

(i) $dom\ (\zeta \bigcup \eta) = (dom\ \zeta) \bigcup (dom\ \eta)$.

(ii) $run\ (\zeta \bigcup \eta) = (run\ \zeta) \bigcup (run\ \eta)$.

Q8: Consider R a relation on A, and $B \subseteq A, C \subseteq A$. Prove that

(i) $R/(A \bigcap C) = (R/B) \bigcap (R/C)$.

(ii) $R/(A \bigcup C) = (R/B) \bigcup (R/C)$.

3.8 Types of Relations

In this section, we deal with the various types of relations and their mathematical definitions, and insert the illustrative examples for each kind of them in order to bring and attract the mind of the reader or the student to the concept of these definitions in a scientific and practical manner.

In addition, we will try to find out the common concepts among the similar relations in terms of definitions. Furthermore, the differences among those relations in what related to their terms, definitions and concepts.

3.8.1 Reflexive Relation

Definition 3.14 Let R be a relation defined on A. R is called reflexive relation if $(x, x) \in R, \forall x \in A$ (Hinman, 2005; Levy, 2002; Schmidt, 2010).

Note: If R is reflexive on A then $I_A \subseteq R$.

Example 3.14 (i) If $A = \{1, 2, 3, 4\}$, and R is a relation on A in which $R = \{(1, 1), (1, 3), (2, 2), (2, 4), (3, 3), (3, 4), (4, 4)\}$. This relation is reflexive because $(1, 1), (2, 2), (3, 3), (4, 4) \in R$. While if T is a relation on A, and defined as $T = \{(1, 1), (1, 3), (2, 4), (3, 3), (4, 4)\}$ is not reflexive, because $(2, 2) \notin T$ while $2 \in A$.

(ii) Let $A = \mathbb{N}$

(a) $R_1 = \{(x, y) \in \mathbb{N} \times \mathbb{N} | x < y\}$ not reflexive because $x \nless x, \forall x \in \mathbb{N}$.

(b) $R_2 = \{(x, y) \in \mathbb{N} \times \mathbb{N} | x \leq y\}$ is a reflexive relation because $x \leq x, \forall x \in \mathbb{N}$.

(c) $R_3 = \{(x, y) \in \mathbb{N} \times \mathbb{N} | x \text{ is divisible by } y; y \neq 0\}$ is reflexive relation because $x$is divisible by $x; x \neq 0$.

(d) $R_4 = \{(x, y) \in \mathbb{N} \times \mathbb{N} | x \times y = 8\}$ is not reflexive relation because $x \times x \neq 8, \forall x \in \mathbb{N}$.

(iii) Let X be any arbitrary set, and $P(X)$ be a power set of X, then

(a) $R_1 = \{(A, B) \in P(X) \times P(X) | A \subseteq B\}$ is a reflexive relation because $A \subseteq A, \forall A \in P(X)$.

(b) $R_2 = \{(A, B) \in P(X) \times P(X) | A \bigcap B = \phi\}$ is not reflexive relation because if we consider $A \in P(X), A \neq \phi$, then $A \bigcap A = A \neq \phi$. Thus, $(A, A) \notin R_2$.

3.8.2 Symmetric Relation

Definition 3.15 Let R be relation on A. R is called symmetric relation on A if $\forall x, y \in A, (x, y) \in R \rightarrow (y, x) \in R$ (Eves, 1992; Eves and Newsom, 1958; Quine, 1969; Mustafa et al., 1980; Hafstrom, 2013; Nešetřil, 1972).

Example 3.15 (i) Consider $A = \mathbb{N}$, and R is a relation on A in which $R = \{(x, y)|x + y = 5, x, y \in A\}$. R is a symmetric relation on A because $x + y = 5 \Rightarrow y + x = 5$. Or, $R = \{(0, 5), (5, 0), (1, 4), (4, 1), (2, 3), (3, 2)\}$.

(ii) Consider $A = \mathbb{N}$, and R is a relation on A in which $R = \{(x, y)|\text{x is a divisor of y}\}$. R is not symmetric as $3R9$ does not imply $9R3$ for 3 divides 9, but 9 does not divide 3.

Note: From the first part of the Example 3.15, $R^{-1} = \{(5, 0), (0, 5), (4, 1), (1, 4), (3, 2), (2, 3)\} = R$. Thus R is symmetric if and only if it equals to its inverse as empathized in the following theorem.

Theorem 3.9 *Let R be a relation on A, R is symmetric relation on A if and only if $R = R^{-1}$.*

Proof Suppose that R is a symmetric relation on A, and let $(x, y) \in R$

$$(x, y) \in R \leftrightarrow (y, x) \in R$$
$$\leftrightarrow (x, y) \in R^{-1}$$
$$\therefore R = R^{-1} ...(1).$$

Conversally if we suppose that $R = R^{-1}$, and let $(x, y) \in R$

$$(x, y) \in R \rightarrow (x, y) \in R^{-1}$$
$$\rightarrow (y, x) \in R$$
$$\therefore R \text{ is symmteric relation}...(2).$$

From (1)&(2), R is symmetric relation on A if and only if $R = R^{-1}$. ♦

Example 3.16 (i) Let R be a relation on $A = \{a, -1, x, 0\}$, and $R = \{(a, x), (0, -1), (-1, 0), (x, a)\}$.
Since $R^{-1} = \{(x, a), (-1, 0), (0, -1), (a, x)\} = R$, thus according to the Theorem 3.9 R is symmetric.

(ii) Let each of R, S, T be a relation on $A = \mathbb{Z}^+$ as follows

(a) $R = \{(x, y) \in A \times A|y \text{ is divisible on } x\}$.
The relation R is not symmetric because $(3, 6) \in R$, but $(6, 3) \notin R$.

(b) $S = \{(x, y) \in A \times A | x + y = 7\}$.
The relation S is a symmetric because $x + y = 7 \wedge y + x = 7$, or $(x, y) \in S \to (y, x) \in S$.

(c) $T = \{(x, y) \in A \times A | 3x + 2y = 7\}$.
The relation T is not a symmetric because if $x = 1, y = 2$, then $3x + 2y = 3(1) + 2(2) = 7, 3y + 2x = 3(2) + 2(1) = 8 \neq 7$. Thus, $(x, y) \in T$, but $(y, x) \notin T$.

(iii) Let X be any set, and ν, σ are relations on $P(X)$, denoted as

(a) $\nu = \{(A, B) \in P(X) \times P(X) | A \subset B\}$.
Then, ν is not symmetric relation on $P(X)$ because if $A \subset B \to B \not\subset A$. Or, if $(A, B) \in \nu \to (B, A) \notin \nu$.

(b) $\sigma = \{(A, B) \in P(X) \times P(X) | A = X - B\}$.
Then, σ is a symmetric relation on $P(X)$ because if $(A, B) \in \sigma \to (A = X - B) \equiv (B = X - A) \to (B, A) \in \sigma$.

(iv) If ν, σ be symmetric relations on any set then $\nu \bigcap \sigma$ is a symmetric relation on the same set.

Proof Suppose that $(x, y) \in \nu \bigcap \sigma$.
Now $(x, y) \in \nu \bigcap \sigma \to (x, y) \in \nu \wedge (x, y) \in \sigma$,
$\because$ each of ν, σ are a symmetric,
$\therefore (y, x) \in \nu \wedge (y, x) \in \sigma \to (y, x) \in \nu \bigcap \sigma$.
Thus, $\nu \bigcap \sigma$ is a symmetric relation.

3.8.3 Transitive Relation

Definition 3.16 Let R be a relation on A. R is called a transitive relation on A, if $(x, y) \in R \wedge (y, z) \in R \to (x, z) \in R, \forall x, y, z \in A$ (Eggen et al., 2006; Flaška et al., 2007; Mustafa et al., 1980).

Note:

(i) The empty relation on any non-empty set is transitive because the conditional defining a transitive relation is logically true.

(ii) A relation R which only contains one ordered pair which is transitive for the same reason. Mathematically, if R is a relation on A, then $(x, y) \in R \wedge (y, z) \notin R \nrightarrow (x, z) \in R, \forall x, y, z \in A$. In other words, if $(x, y) \in R$, but $(y, z) \notin R$, then it does not need $(x, z) \in R$.

Example 3.17 (i) Let $A = \mathbb{N}$, and let R, S be relations on A, in which defined as

(a) $R = \{(x, y) \in A \times A | x < y\}$. This relation is transitive because if we assume that x, y, z are natural numbers, and $x < y, y < z \rightarrow x < z$. Or, if $(x, y) \in R \wedge (y, z) \in R \rightarrow (x, z) \in R$.

(b) $S = \{(x, y) \in A \times A | x + 2y = 10\}$. This relation is not transitive because if we take $x = 2, y = 4, z = 3$, then $2 + 2(4) = 10, 4 + 2(3) = 10$, but $2 + 2(3) \neq 10$. Or, $(2, 4) \in S \wedge (4, 3) \in S \nrightarrow (2, 3) \notin S$.

(ii) Consider $A = \{a, b, c\}$, and $R_i; i = 1, 2, 3$ is a relation on A, defined as

(a) $R_1 = \{(a, b), (b, b)\}$ is a transitive because $(a, b) \in R_1 \wedge (b, b) \in R_1 \rightarrow (a, b) \in R_1$.

(b) $R_2 = \{(a, a)\}$ is transitive because $(a, a) \in R_2 \wedge (a, a) \in R_2 \rightarrow (a, a) \in R_2$.

(c) $R_3 = \{(a, b), (b, c), (a, c), (b, a)(a, a)\}$ is not transitive since $(b, a) \in R_3 \wedge (a, b) \in R_3$, while $(b, b) \notin R_3$.

Note: Reflexive relation $\subseteq$ symmetric relation $\subseteq$ transitive relation. For example let $A = \{1, 2, 3\}$, and R is a relation on A defined as $R = \{(1, 1), (2, 2), (3, 3)\}$. R is reflexive, symmetric and transitive synchronously.

3.8.4 Anti-symmetric Relation

Definition 3.17 Let R be a relation on A. R is called anti-symmetric on A, if $(x, y) \in R \wedge (y, x) \in R \rightarrow x = y$ (Lipschutz and Lipson, 1992; Nešetřil, 1972).

Note: There should not be confusion between the concepts symmetric and anti-symmetric. The statement R is not symmetric relations does not means that it is antisymmetric.

Theorem 3.10 *If R is a relation on A. R is anti-symmetric if and only if $R \bigcap R^{-1} \subseteq I_A$.*

Proof Suppose that R is anti-symmetric, and $(x, y) \in R \bigcap R^{-1}$.
Now, $(x, y) \in R \bigcap R^{-1} \rightarrow (x, y) \in R \wedge (x, y) \in R^{-1}$,
$\rightarrow (x, y) \in R \wedge (y, x) \in R$
$\because R$ is anti-symmetric
$\therefore (x, y) \in R \wedge (y, x) \in R \rightarrow x = y$
Thus, $(x, y) \in I_A$
$\therefore R \bigcap R^{-1} \subseteq I_A$...(1).
Conversally, suppose that $R \bigcap R^{-1} \subseteq I_A$
To prove that R is anti-symmetric, suppose$(x, y) \in R \wedge (y, x) \in R$
Now, $(x, y) \in R \wedge (y, x) \in R \rightarrow (x, y) \in R \wedge (x, y) \in R^{-1}$
$\rightarrow (x, y) \in R \bigcap R^{-1}$
From (1)$(x, y) \in I_A$
$\rightarrow x = y$
$\therefore R$ is anti-symmetric...(2).
From (1)& (2) the proof is completed. ⧫

3.9 Exercises

Answer the following questions:

Q1: Let η be a relation on A, then, prove that

(i) η is transitive if and only if $\eta \circ \eta \subset \eta$.

(ii) If η is reflexive and transitive, then $\eta \circ \eta = \eta$. Is the vice versa true?

Q2: ζ, β are transitive relations on the set X. Is $\zeta \bigcap \beta$ transitive?

Q3: Consider the following relations on the set $A = \{0, 1, ..., 17\}$. Check out the relation if they are reflexive, symmetric, anti-symmetric, and transitive.

(i) $\sigma_1 = \{(x,y)|y - x \in A\}$.

(ii) $\sigma_2 = \{(x,y)|y - x \in A \wedge y - x = 0\}$.

(iii) $\sigma_3 = \{(x,y)|1 < x - y\}$.

(iv) $\sigma_4 = \{(x,y)|y - x = 1\}$.

Q4: Consider R is a relation on X, prove that

(i) $R \bigcup R^{-1}$ is the smallest symmetric relation contains of R.

(ii) $R \bigcap R^{-1}$ is the greatest symmetric relation in R.

Q5: Let R_1, R_2 be relations on A. If R_1 is reflexive and R_2 is reflexive and transitive, then $R_1 \subseteq R_2 \leftrightarrow R_1 \circ R_2 = R_2$.

Q6: Consider R_1 is a reflexive relation on A, and R_2 be any arbitrary relation on A. Prove that

(i) $R_2 \subseteq R_1 \circ R_2$.

(ii) $R_2 \subseteq R_2 \circ R_1$.

Q7: Consider φ is a reflexive relation on A, and χ be any relation on A. Prove that $\varphi \bigcup \chi$ is a reflexive.

Q8: Consider φ, χ be relations on the set A. Show that the following statements are false;

(i) If φ, χ are anti-symmetric relations, then $\varphi \bigcup \chi$ is anti-symmetric too.

(ii) If φ, χ are transitive relations, then $\varphi \bigcup \chi$ is transitive too.

3.10 Equivalence Relations and Partition

3.10.1 Equivalence Relation

Definition 3.18 Let R be a relation on the set A, R is called an equivalence relation if it reflexive, symmetric, and transitive relation (Wilder et al., 2012; Wallace, 2012; Dummit and Foote, 2004a; Hrbacek and Jech, 1999).

Example 3.18 Let R, S be relations on $A = \mathbb{R}$ as follows;

(i) $R = \{(x, y) \in A \times A | x = y\}$ is the equivalence relation because (1) $\forall x \in A, x = x$. Or, $\forall x \in A, (x, x) \in R$. (2) $\forall x, y \in A, x = y \rightarrow y = x$. Or $\forall x, y \in A; (x, y) \in R \rightarrow (y, x) \in R$. (3) $\forall x, y, z \in A; x = y \wedge y = z \rightarrow x = z$. Or $\forall x, y, z \in A; (x, y) \in R \wedge (y, z) \in R \rightarrow (x, z) \in R$. Thus, R is the equivalence relation because it is reflexive, symmetric, and transitive relation.

(ii) $S = \{(x, y) \in A \times A | x < y\}$ is not equivalence relation because it is not reflexive, and symmetric, $\forall x \in A, x \nless x$. Or, $\forall x \in A; (x, x) \notin S$.

Note: To prove that the relation is not equivalence, it is adequate to prove it is not reflexive, or not symmetric, or not transitive.

Example 3.19 Let X be any set, and let ψ, ϕ be relations defined on $P(X)$ as follows;

(i) $\psi = \{(A, B) \in P(X) \times P(X) | A = B\}$.
The ψ is equivalence relation because it satisfies the following;

(a) $\forall A \in P(X), A = A$.
Or, $\forall A \in P(X), (A, A) \in \psi$. Thus, ψ is a reflexive relation.

(b) $\forall A, B \in P(X), A = B \rightarrow B = A$.
Or, $\forall A, B \in P(X), (A, B) \in \psi \rightarrow (B, A) \in \psi$. Thus, ψ is a symmetric relation.

(c) $\forall A, B, C \in P(X), A = B \wedge B = C \rightarrow A = C$.
Or, $\forall A, B, C \in P(X), (A, B) \in \psi \wedge (B, C) \in \psi \rightarrow (A, C) \in \psi$. Thus, ψ is a transitive relation. Based on the definition, ψ is the equivalence relation.

(ii) $\phi = \{(A, B) \in P(X) \times P(X) | A \subseteq B\}$.
This relation is not equivalence because it is not symmetric.

Example 3.20 Let A be a set of straight lines in the Cartesian plane, and σ_1, σ_2 be relations on A in which defined as;

(i) $\sigma_1 = \{(x, y) \in A \times A | x \parallel y\}$. This relation is equivalence for the following reasons;

 (a) Since each straight line is parallels to itself, hence, $\forall x \in A, (x, x) \in \sigma_1$. Thus, the relation is reflexive.

 (b) As $x \parallel y \to y \parallel s$. Or, $\forall x, y \in A; (x, y) \in \sigma_1 \to (y, x) \in \sigma_1$. So, the relation is symmetric.

 (c) if $x \parallel y \wedge y \parallel z \to x \parallel z$. Or, $\forall x, y, z \in A; (x, y) \in \sigma_1 \wedge (y, z) \in \sigma_1 \to (x, z) \in \sigma_1$. Therefore, the relation is transitive. So on, and based on the definition, the relation is the equivalence relation.

(ii) $\sigma_2 = \{(x, y) \in A \times A | x \perp y\}$. Since this relation is not reflexive, neither transitive hence, it is not equivalence relation.

Example 3.21 Let $A = \mathbb{R} \times \mathbb{R}$, Υ is a relation on A and defined as follows; $\Upsilon = \{((a, b), (c, d) \in A \times A | a + b = c + d)\}$.

Prove that the relation is equivalence.

Proof

(i) If $(a, b) \in A \to a + b = b + a$. Or, $\forall (a, b) \in A, ((a, b), (a, b)) \in \Upsilon$. Thus, Υ is reflexive.

(ii) If $((a, b), (c, d)) \in A$, and if $((a, b), (c, d)) \in \Upsilon \to a + b = c + d \to c + d = a + b$. Thus, $(c, d), (a, b) \in \Upsilon$, and so on, Υ is symmetric relation.

(iii) If $(a, b), (c, d), (e, f) \in A$, $((a, b), (c, d)) \in \Upsilon \wedge ((c, d), (e, f)) \in \Upsilon$, then $a + b = c + d \wedge c + d = e + f \to a + b = e + f$.
Thus, $((a, b), (e, f)) \in \Upsilon$, and so on Υ is transitive relation. From (i), (ii), and (iii), we conclude that Υ is the equivalence relation on A.

Theorem 3.11 *If R_1, R_2 are equivalence relations on A, then $R_1 \bigcap R_2$ is an equivalence relation on A.*

Proof

(i) Since each of R_1, R_2 is a reflexive relation, hence, $\forall x \in A, (x,x) \in R_1 \wedge (x,x) \in R_2$. Or, $\forall x \in A, (x,x) \in R_1 \bigcap R_2$. Thus, $R_1 \bigcap R_2$ is the reflexive relation.

(ii) Let$\forall x, y \in A, (x,y) \in R_1 \bigcap R_2$.
Now, $(x,y) \in R_1 \bigcap R_2 \to (x,y) \in R_1 \wedge (x,y) \in R_2$.
$\because R_1, R_2$ are symmetric relations,
$\therefore (y,x) \in R_1 \wedge (y,x) \in R_2 \to (y,x) \in R_1 \bigcap R_2$.
Accordingly, the $R_1 \bigcap R_2$ is symmetric.

(iii) Let$\forall x, y, z \in A, (x,y) \in R_1 \bigcap R_2 \wedge (y,z) \in R_1 \bigcap R_2$.
$((x,y) \in R_1) \wedge (x,y) \in R_2) \wedge ((y,z) \in R_1) \wedge (y,z) \in R_2)$.
$((x,y) \in R_1) \wedge (y,z) \in R_1) \wedge ((x,y) \in R_2) \wedge (y,z) \in R_2)$.
$\because R_1, R_2$ are transitive relations,
$\therefore (x,z) \in R_1 \wedge (x,z) \in R_2 \to (x,z) \in R_1 \bigcap R_2$.
Based on (i), (ii), and (iii), $R_1 \bigcap R_2$ is equivalence relation. ♦

Theorem 3.12 *If R is an equivalence relation on A then $R \circ R = R$.*

Proof Suppose that$\forall x, z \in A, (x,z) \in R \circ R$,
$\therefore \exists y \in A \ni (x,y) \in R \wedge (y,z) \in R$.
$\because R$ is transitive,$\therefore (x,y) \in R \wedge (y,z) \in R \to (x,z) \in R$
Accordingly, the$R \circ R \subseteq R$...(1).
Converserlly, let $(x,y) \in R$.
$\because R$ is reflexive,$\therefore (x,x) \in R$.
$\exists x \in A \ni (x,x) \in A \wedge (x,y) \in R$.
Based on the definition of composite relation, we obtain $(x,y) \in R \circ R$.
$R \circ R \subseteq R$...(2).
From, (1)& (2), we get that $R \circ R = R$. ♦

3.10.2 Equivalence Classes

Definition 3.19 Let R be an equivalence relation on nonempty set A, and $a \in A$. The set that all elements in A in which related with a through R is called equivalence class consists of a denoted by A_a, or $[a]$. Mathematically, $A_a = [a] = \{x \in A|(x, a) \in R\}$ (Devlin, 2003; Avelsgaard, 1990).

Example 3.22 Let $A = \{a, b, c, d\}$, R is a relation on A defined as $R = \{(a, a), (b, b), (c, c), (d, d), (a, c), (c, a)\}$.
R is the equivalence relation because $\forall l \in A; l = a, b, c, d$: (1) $(l, l) \in R$. (2) $\forall m \in A; m = a, b, c, d|(l, m) \in R \rightarrow (m, l) \in R$. (3). $\forall n \in A, n = a, b, c|(l, m) \in R \wedge (m, n) \in R \rightarrow (l, n) \in R$.
$[a] = \{x \in A|(x, a) \in R\} = \{a, c\}$.
$[b] = \{x \in A|(x, b) \in R\} = \{b\}$.
$[c] = \{x \in A|(x, c) \in R\} = \{c, a\}$.
$[d] = \{x \in A|(x, d) \in R\} = \{d\}$.
Since $[a] = [c]$ hence, the equivalence classes are $[a], [b], [d]$.

3.10.3 Properties of Equivalence Classes

The following theory illustrates us the most important properties of equivalence classes.

Theorem 3.13 *Consider R a relation on a nonempty set A, and $a, b \in A$ then:*

(i) $a \in [a]$.

(ii) *If* $b \in [a]$ *then* $[a] = [b]$.

(iii) $[a] = [b]$ *if and only if* $(a, b) \in R$.

(iv) *If* $[a] \wedge [b] \neq \phi$ *then* $[a] = [b]$.

Proof

(i) According of the definition of equivalence class;
$[a] = \{x \in A|(x, a) \in R\}$ ...(1).
Since R is reflexive, hence $\forall a \in A, (a, a) \in R$ ...(2).
From (1)& (2), we conclude that $a \in [a]$.

(ii) Suppose that $b \in [a]$.
To prove that $[a] = [b]$, suppose that $x \in [b]$.
From the definition of equivalence class $(x, b) \in R$.
Since $b \in [a]$, it concluded from the definition $(b, a) \in R$.
Since R is transitive, thus $(x, b) \in R \wedge (b, a) \in R \rightarrow (x, a) \in R$.
According of the definition of equivalence class:
$(x, a) \in R \rightarrow x \in [a]$.
Thus, $[b] = [a]$ ...(1).
To prove $[a] \subseteq [b]$, suppose that $y \in [a]$.
Now $y \in [a] \rightarrow (y, a) \in R$. Also, $b \in [a] \rightarrow (b, a) \in R$.
Since, R is symmetric, so that $(a, b) \in R$. Again, R is transitive.
So that $(y, a) \in R \wedge (a, b) \in R \rightarrow (y, b) \in R$. Or, $y \in [b]$.
$[a] \subseteq [b]$ ...(2).
From (1)& (2), we get that $[a] = [b]$.

(iii) Suppose that $[a] = [b]$.
From (i), $a \in [a] \rightarrow a \in [b]$.
Based on the definition of the equivalence classes, it is concluded that
$a \in [b] \rightarrow (a, b) \in R$.
Conversely, let $(a, b) \in R$, to prove that $[a] = [b]$, suppose that $x \in [a]$.
Thus, from the definition of equivalence classes.
$x \in [a] \rightarrow (x, a) \in R$.
Since R is transitive, thus
$(x, a) \in R \wedge (a, b) \in R \rightarrow (x, b) \in R$.
Or, $x \in [b]$
Thus, $[a] \subseteq [b]$ ...(1).
In the same way, let $y \in [b]$.
From the definition of the equivalence classes, $y \in [b] \rightarrow (y, b) \in R$.
Since, R is symmetric hence, $(a, b) \in R \rightarrow (b, a) \in R$.
Since, R is transitive hence, $(y, b) \in R \wedge (b, a) \in R \rightarrow (y, b) \in R$.
Thus, $y \in [a]$ ...(2).
From (1)& (2), $[a] = [b]$.

(iv) Let, $[a] \wedge [b] \neq \phi$, and let $x \in [a] \bigcap [b]$.

Thus, $x \in [a] \bigcap [b] \to x \in [a] \wedge x \in [b]$.
$\to (x, a) \in R \wedge (x, b) \in R$.
$\to (x, b) \in R \wedge (x, a) \in R$.
Since R is symmetric, hence $(b, x) \in R \wedge (x, a) \in R$.
Since R is transitive, so that $(b, x) \in R \wedge (x, a) \in R \to (b, a) \in R$.
Since R is symmetric, that why $(a, b) \in R$.
From (iii), $(a, b) \in R \to [a] = [b]$. ♦

3.10.4 Partition

Definition 3.20 Let $\{A_i\}_{i \in I}$ family of sets of the nonempty set A. The $\{A_i\}_{i \in I}$ it said to be partition for A, if:

(i) $\forall i, j \in I, A_i \bigcap A_j = \phi \vee A_i = A_j$.

(ii) $A = \bigcup\limits_{i \in I} A_i$(Halmos, 2017b; Lucas, 1990; Brualdi, 1992).

Example 3.23 Let $A = \mathbb{Z}, X = \mathbb{Z}^e, Y = \mathbb{Z}^o$. We note that, each of X, Y is subset of A, $X \bigcap Y = \phi$, and $X \bigcup Y = A$. And so on $\{X, Y\}$ is a partition for A.

Theorem 3.14 *Let R be an equivalence relation on a nonempty set A, and $\bigcup\limits_{a \in A} A_a$ all equivalence classes according to R, then $\bigcup\limits_{a \in A} A_a$ is a partition of A.*

Proof It is clear that, $A_a \subseteq A, \forall a \in A$.

Since R is reflexive, hence $(a, a) \in R$.

From the Theorem 3.12, it concluded that: $A_a \neq \phi, \forall a \in A$. Now, we have to prove the necessary conditions of the definition of the partition.

(i). Suppose that $\exists a, b \in A \ni A_a \bigcap A_b \neq \phi$.
From, Theorem 3.12, it concluded that $A_a = A_b$.
Thus, we conclude that: $\forall a, b \in A$; either $A_a \bigcap A_b = \phi$, or, $A_a = A_b$.
(ii). To prove that $A \subseteq \bigcup\limits_{a \in A} A_a$, suppose that $x \in A$.
From the Theorem 3.13, $x \in A_x$.
$\therefore x \in \bigcup\limits_{a \in A} A_a \to A \subseteq \bigcup\limits_{a \in A} A_a$ ...(1).

To prove, $\bigcup\limits_{a\in A} A_a \subseteq A$, we note that $A_a \subseteq A, \forall a \in A$.
From the Theorem 2.15 $\bigcup\limits_{a\in A} A_a \subseteq A$ ...(2).
From (1)& (2), $A = \bigcup\limits_{a\in A} A_a$.
Thus, from (i)& (ii) we conclude that, $\{A_a\}_{a\in A}$ is a partition of A.
♦

Theorem 3.15 *Consider a nonempty set A, if $\{A_i\}_{i\in I}$ is a partition of A, then there exists an equivalence relation on A such that an equivalence classes relative to this relation is $\{A_i\}_{i\in I}$ itself.*

Proof Suppose that R will be a relation on A, defined as follows:
$R = \{(x, y) \in A \times A | \exists A_i \ni x, y \in A_i\}$.
Now, we have to prove R is the equivalence relation.

(i) Suppose, that $x \in A$,
$\because \{A_i\}_{i\in I}$ is the partition of A,
$\therefore A = \bigcup\limits_{i\in I} A_i$.
Thus, $\exists A_i \ni x \in A_i$.
$\therefore x \in A_i \wedge x \in A_i \to (x, x) \in R$.
Or, R is reflexive.

(ii) Suppose, that $(x, y) \in R$,
$\therefore \exists A_i \ni x \in A_i \wedge y \in A_i$.
Or, $\exists A_i \ni y \in A_i \wedge x \in A_i$.
From the definition of R, we conclude that $(y, x) \in R$.
Or, R is symmetric.

(iii) Suppose, that $(x, y) \in R \wedge (y, x) \in R$,
$\therefore \exists A_i, A_j \ni x, y \in A_i \wedge y, z \in A_j$.
Note that $y \in A_i \bigcap A_j$.
Or, $A_i \bigcap A_j \neq \phi$.
Since, $\{A_i\}_{i\in I}$ is a partition of A, hence, $A_i = A_j$.
Thus, $\exists A_i \ni x \in A_i \wedge z \in A_i$.
From the definition of R, we obtain that, $(x, z) \in R$.
Or, $(x, y) \in R \wedge (y, z) \in R \to (x, z) \in R$.

Thus, R is transitive.

From, (i)& (ii)& (iii), R is equivalence relation.

Now, we are going to prove each subset A_i within the partition $\{A_i\}_{i\in I}$ is an equivalence class with respect to the relation R.
$\because A_i \neq \phi, \forall i \in I$,
$\therefore A_i$ is contains at least one element like x, and A_x will be equivalence class with respect to the relation R.
Let us, claim that $A_i = A_x$. To prove the claim,
Suppose that $y \in A_x$.
From the definition of the equivalence class, we have $(y, x) \in R$.
$\because x \in A_i$,
$\therefore$ from the definition of R, also, $y \in A_i$.
Or, $y \in A_x \to y \in A_i$.
$\therefore z \in A_i \wedge x \in A_i \to (z, x) \in R$.
By the same way, suppose that $z \in A_i$.
That why, $z \in A_i \wedge x \in A_i \to (z, x) \in R$.
And from the definition of the equivalence class, we conclude that, $z \in A_x$.
$\therefore z \in A_i \to z \in A_x$.
Or, $A_i \subseteq A_x$.
Thus, $A_i = A_x$. ♦

Example 3.24 Let $A = \{1, 3, 5, 7, 9\}, X = \{1, 3\}, Y = \{5, 7\}, Z = \{9\}$. According to the definition, there exists, equivalence classes, the partition; $\{X, Y, Z\}$, in respect to the relation: $I_A \bigcup \{(1, 3), (3, 1), (5, 7), (7, 5)\}$.

We can easily prove that:

(i) The set X, Y, Z is a partition to A.

(ii) The relation R is equivalence on A. And the equivalence classes are; $[1] = [3], [5] = [7], [9]$. Note that; $X = [1] = [3]$, $Y = [5], [7]$, $Z = [9]$.

Example 3.25 Let, $A = \mathbb{Z}$, $X = \mathbb{Z}_e)$, $Y = \mathbb{Z}_o)$. The set X, Y is the partition of A. Now, if we consider the relation $R = \{(x, y) \in A \times A | x - y \text{ even number}\}$. R is the equivalence relation on A, and the equivalence classes are: $[0], [1]$, where $X = [0], Y = [1]$.

3.10.5 Quotient Set

Definition 3.21 Let R be an equivalence relation on a nonempty set A, the set of all equivalence classes with respect to R is called quotient set (Mustafa et al., 1980; Halmos, 2017b; Lucas, 1990; Brualdi, 1992).

Example 3.26 Let R be a relation on $\mathbb{N}$, and defined as follows:
$R = \{(x, y) \in \mathbb{N} \times \mathbb{N} | x - y$ divisible on $3\}$. Then, $\mathbb{N}/R = \{[0], [1], [2]\}$ is the the quotient set.

Example 3.27 Consider $A = \{1, 3, 5, 7, 9\}$, and R, S are definitions on A, where:
$R = I_A \bigcup \{(1, 3), (3, 1), (5, 7), (7, 5)\}$.
$S = I_A \bigcup \{(1, 3), (3, 1), (5, 7), (5, 9), (9, 5), (7, 9), (9, 7)\}$. We can easily prove that both of R, S are equivalence relations, and:
$A/R = \{[1], [5], [9]\}$, $A/S = \{[1], [5]\}$ are the quotient sets.

Theorem 3.16 *Let R be a relation on $A \neq \phi$. R is an equivalence relation, if and only if there exists the set P in which its elements are disjoint sets such that:*
$R = \{(x, y) \in A \times A | \exists B \in P \ni (x, y) \in B \times B\}$.

Proof Let us consider R is the equivalence relation on A, and P is a quotient set A/R. Obviously, A/R is a set its elements are disjoint sets. We are going to proof that:

$R = \{(x, y) \in A \times A | \exists B \in A/R \ni (x, y) \in B \times B\}$.

If we symbolize the right side of this equation by D, then we have to proof that $R = D$.

(i) Let $(x, y) \in R$
$\therefore ((x, y) \in A \times A) \wedge (x, y) \in [x]$
Or, $[x] \in A/R \ni (x, y) \in [x] \times [x]$
$\because (x, y) \in A \times A | \exists [x] \in A/R \ni (x, y) \in [x] \times [x]$
$\rightarrow (x, y) \in D$
$\rightarrow R \subseteq D$ ...(1).

(ii) Let $(x, y) \in D$
$\therefore (x, y) \in A \times A | \exists B \in A/R \ni (x, y) \in B \times B$.

Suppose that $B = [z]; z \in A$
$\therefore x, y \in [z]$.

From the definition of the equivalence classes, we get that, $(x, z) \in R \wedge (y, z) \in R$.

Since R is symmetric, hence $(z, y) \in R$.

Again, since R is transitive, hence $(x, z) \in R \wedge (z, y) \in R \rightarrow (x, y) \in R$.

$\rightarrow D \subseteq R$ ...(2).

From (1)& (2), we conclude that $R = D$.

The conversely proof of the theorem is left to the reader. ♦

3.11 Exercises

Answer the following questions:

Q1: Let Γ is the set of all equivalence relations on the set A. Prove that $\bigcap \Gamma$ is equivalence relation.

Q2: Consider γ_1 is the equivalence relation on the set X, and γ_2 is the equivalence relation on the set Y. The defined relation χ on the set $X \times Y$ as follows:

$(x_1, y_1)\chi(x_2, y_2) \leftrightarrow (x_1, y_1) \in \gamma_1 \wedge (x_2, y_2) \in \gamma_2$. Prove that χ is the equivalence relation on $X \times Y$.

Q3: Let each of H, G is an equivalence relation on A. Prove that $G \circ H$ is an equivalence relation on A if and only if $G \circ H = H \circ G$.

Q4: Let each of H, G is an equivalence relation on A. when $G \bigcup H$ will be an equivalence relation on A?

Q5: Let $\{A_i\}_{i \in I}$ is a partition of the set A, $\{B_j\}_{j \in J}$ is a partition of the set B. Prove that $\{A_i \times B_j\}_{(i,j) \in I \times J}$ is a partition of the set $A \times B$.

3.12 Ordered Relations

The order relations we are going to study here are an abstraction of those relations. The properties common to orders we see in our daily lives have been extracted and are used to characterize the concepts of order.

Here we are going to learn some types of order: partial order, strict order, partially ordered sets, totally ordered sets, and well ordered sets.

3.12.1 Partial Ordered Relations

Definition 3.22 Let R be a relation on the set A, then R is a partial order set on A if it is (1). reflexive, (2). anti-symmetric, and (3). transitive (Simovici and Djeraba, 2008; Schröder, 2003).

Note:

(i) The symbol $\preceq$, indicates of the partial ordered relation on the set A. Each ordered pair (x, y) in the relation is written in the form $x \preceq y$, it means: x is precedes y, or y is follows x.

(ii) The symbol $x \prec y$, indicates that $x \preceq y, x \neq y$.

(iii) In the case not using $\preceq$ or $\prec$, it ought to written the relation in addition to its symbol.

Example 3.28 Let each of R_1, R_2 is a relation on $\mathbb{Z}$ and defined as:
$R_1 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | x \leq y\}$.
$R_2 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | x - y$ divisible over $3\}$.

It is easy to prove that R_1 is partial ordered relation, but R_2 is not partial ordered relation because it is not anti symmetric relation, hence $(2, 8) \in R_2 \wedge (8, 2) \in R_2$, but $2 \neq 8$.

Example 3.29 Let $X \neq \phi$, R be a relation on the power set $P(X)$ and defined as: $R = \{(A, B) \in P(X) \times P(X) | A \subseteq B\}$.

It is clear that R is a partial ordered relation on $P(X)$.

Definition 3.23 Let R be a relation on the set A. The relation R is called strict order relation if R is: (1). Irreflexive, or $(a, a) \notin R, \forall a \in A$, (2). Antisymmetric, and (3). Transitive (Simovici and Djeraba, 2008; Mustafa et al., 1980).

Example 3.30 Consider $\mathbb{R}$ the set of all real numbers. Then $R = \{(x, y) | x < y; x, y \in \mathbb{R}\}$ is a strict order relation on $\mathbb{R}$.

Theorem 3.17 *If R is a partial ordered relation on A then R^{-1} is a partial ordered relation too.*

Proof (1). We have to prove R^{-1} is reflexive. $\because$ R is partial ordered relation on A, $\therefore$ $(a,a) \in R, \forall a \in A$. From the definition of R^{-1}, $(a,a) \in R \to (a,a) \in R^{-1}$. Or, R^{-1} is reflexive.

(2). We are going to prove R^{-1} is anti-symmetric. From the definition of R^{-1} we have, $(a,b) \in R^{-1} \wedge (b,a) \in R^{-1}$

$\to (b,a) \in R \wedge (a,b) \in R.$

Since R is anti-symmetric, hence $a = b$

$\to R^{-1}$ is anti-symmetric.

(3). To prove R^{-1} is transitive. Again, from the definition of R^{-1}.

$(a,b) \in R^{-1} \wedge (b,c) \in R^{-1} \to (b,a) \in R \wedge (c,b) \in R,$

$\to (c,b) \in R \wedge (b,a) \in R,$

$\to (c,a) \in R$, because R is transitive.

$(a,c) \in R^{-1}$, from the definition of R^{-1}.

$\therefore R^{-1}$ is transitive.

From (1), (2)& (3), R^{-1} is partial ordered relation. ♦

Theorem 3.18 *Let R be a relation on $A \neq \phi$. R is partial ordered relation on A if and only if $R \bigcap R^{-1} = I_A \wedge R \circ R = R$.*

Proof Suppose that $R \bigcap R^{-1} = I_A \wedge R \circ R = R.$

We are going to prove R is a partial ordered relation on A.

(1) From the identity relation we have:

$\forall a \in A, (a,a) \in I_A$

$\to \forall a \in A, (a,a) \in R \bigcap R^{-1}$

$\to \forall a \in A, (a,a) \in R$

$\therefore R$ is reflexive. (2) Suppose that $(a,b) \in R \wedge (b,a) \in R$

From the definition of the symmetric relation $(a,b) \in R \to (b,a) \in R^{-1}$

$\therefore (b,a) \in I_A$

$\to (b,a) \in R \circ R^{-1}$

From the definition of the identity relation $a = b$

$R$is amti-symmetric relation.

(3) Suppose that$(a,b) \in R \wedge (b,c) \in R$

$\because R \circ R = R$

$(a,b) \in R \circ R \wedge (b,c) \in R \circ R$

From the definition of composition of relations, we conclude that:

$\exists x \in A \ni (a,x) \in R \wedge (x,b) \in R$
$\exists y \in A \ni (b,y) \in R \wedge (y,c) \in R$
$(x,b) \in R \wedge (b,y) \in R \rightarrow (a,y) \in R \circ R$
$(a,y) \in R(a,y) \in R \wedge (y,c) \in R \rightarrow (a,c) \in R \circ R$
$\rightarrow (a,c) \in R$
$\therefore (a,b) \in R \wedge (b,c) \in R \rightarrow (a,c) \in R$
$\therefore R$ is a transitive relation
From $(1), (2)\&(3), R$ is transitive.
The conversely direction of the proof has been left to the reader, as an exercise.

3.12.2 Hasse Diagram

Definition 3.24 Let A be partial ordered set by the relation R, and let $a, b \in R$ such that, then aRb can be expressed by one of these methods, where a, b represents initial and final points in the arrow respectively, as shown in Figure 3.3 (Di and Tamassia, 1988; Freese, 2004; Nicos, 1975).

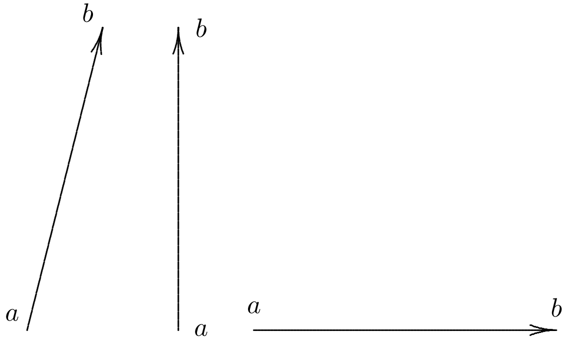


Figure 3.3: Hasse Diagram

Example 3.31 Let $A = \{1, 3, 5, 12\}, \mathbb{R} = \{(x, y) \in A \times A | x \leq y\}$. The Hasse diagram for $(A, \mathbb{R})$ is as shown in Figure 3.4.

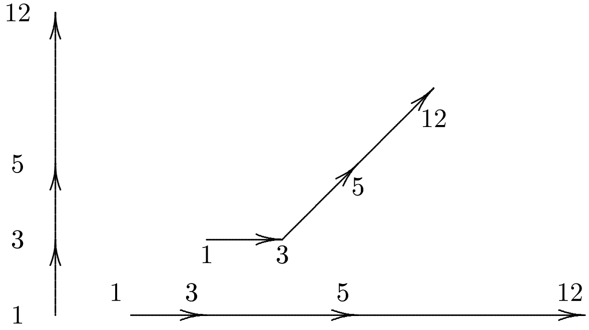


Figure 3.4: The Hasse diagram for $(A, \mathbb{R})$

Example 3.32 Let $B = \{2, 6, 20, 15\}$, and

$\mathbb{R} = \{(x, y) \in A \times A |$y is divided by x$\}$. The Hasse diagram for $(B, \mathbb{R})$ is as shown in Figure 3.5.

3.12.3 Initial Segment

Definition 3.25 Let A be partial ordered by the relation $\leq$, and let $a \in A$. The initial segment and limited by a is the subset S_a defined as: $S_a = \{x \in A | x < a\}$(Rubin, 1967; Dauben, 1990; Moore, 2012).

Note:

Let $(A, \mathbb{R})$ be a partial ordered set. If P is an initial segment of A, and Q is an initial segment of P then Q will be an initial segment of A.

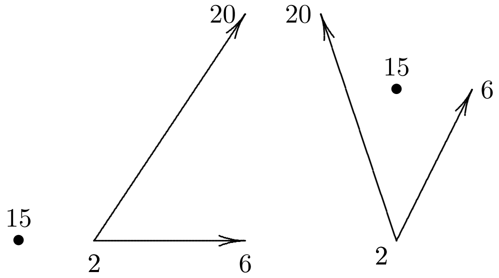


Figure 3.5: The Hasse Diagram for $(B, \mathbb{R})$

Example 3.33 The following sketch in Figure 3.6 represents the partially ordered set A and will consist of six elements:
$S_e = \{b, c, f\} = \{x \in A | x < e\}$.

If each of A, B is partially ordered set, there are many ways to define a partially ordered relation $A \times B$. We will mention one of these ways.

Definition 3.26 Let each of $(A, R_1), (B, R_2)$ be a partial ordered set. The Lexicographic ordering is expressed of R on $A \times B$ as follows: If $(a_1, b_1) \in A \times B, (a_2, b_2) \in A \times B$ then $(a_1, b_1) R (a_2, b_2)$ will be;
(1). $a_1 R a_2$ or, (2). $a_1 = a_1 \ \wedge b_1 R b_2$(Harzheim, 2006; Baader and Nipkow, 1999).

Example 3.34 Let $A = \{1, 3, 5\}, B = \{2, 4\}$, and let R_1 is a relation defined on A as: $x R_1 y \leftrightarrow x \leq y$. And Let R_2 is a relation on B, defined as: $x R_2 y \leftrightarrow$ y is divisible by x. It can be prove that R_1, R_2 are partial ordered relation on A, B respectively. Assume that R is lexicographic ordering relation on the set $A \times B = \{(1, 2), (1, 4), (3, 2), (3, 4), (5, 2), (4, 5)\}$ is a partially ordered by the

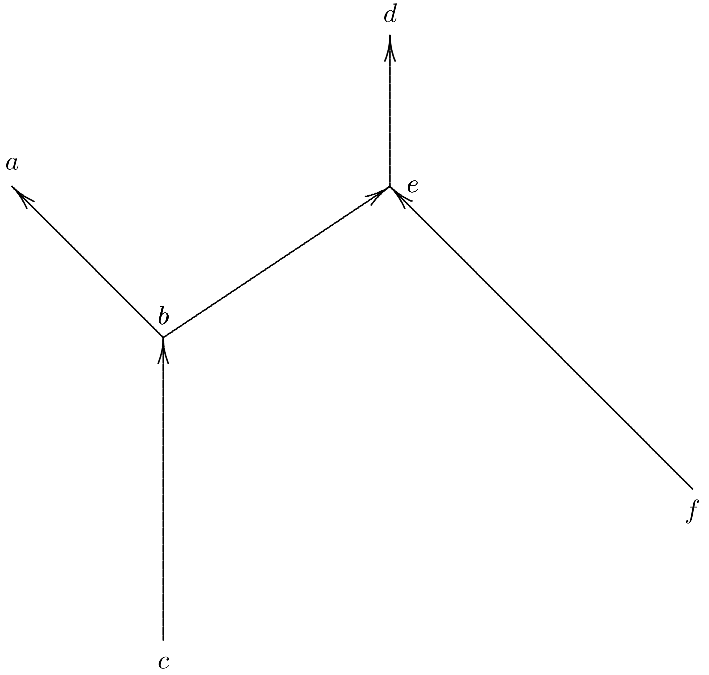


Figure 3.6: A is a Partially Ordered Set

relation R. Note that, $(1,2)R(1,4)$ because $a_1 = a_2 = 1$, and 4 is divided on 2, where $b_1 = 2, b_2 = 4$. Also, note that $(1,2)R(3,2)$ because $1 < 3$, where $a_1 = 1, a_2 = 3$. And so on with respect to the remind elements of R.

Definition 3.27 Let $(A, R_1), (B, R_2)$ be partial ordered sets. The anti lexicographic ordering is represents of a partial ordered relation R on the set $A \times B$ as: if $(a_1, b_1) \in A \times B, (a_2, b_2) \in A \times B$ then $(a_1, b_1)R(a_2, b_2) \leftrightarrow$ (1). $b_1 R_2 b_2$, or (2). $b_1 = b_2 \wedge a_1 R_1 a_2$ (Mustafa et al., 1980).

Example 3.35 Let $A = \{1, 3, 5\}, B = \{2, 4\}$, and consider the same relations R_1, R_2 in the previous example. Let us assume that R is the anti lexicographic relation, then the set: $A \times B = \{(1,2),(3,2),(5,2),(1,4),(3,4),(5,4)\}$ as a partial ordered set by the anti lexicographic relation R. Note that $(1,2)R(3,2)$, $b_1 = b_2 = 2, a_1 < a_2$, where $a_1 = 1, a_2 = 3$. Also, note that, $(3,2)R(3,4)$, because b_2 is divisible on b_1, where $b_1 = 2, b_2 = 4$.

Definition 3.28 Let $(A_1, R_1), (A_2, R_2), ..., (A_n, R_n)$ be n of partial ordered sets. We define R on the Cartesian product $A = \sum_{i=1}^{n} A_i$ as follows: Let $a, b \in A$, where $a = (a_1, a_2, ..., a_n), b = (b_1, b_2, ..., b_n), aRb \leftrightarrow a_i R_i b_i; \forall i (1 \leq i \leq n)$ (Mustafa et al., 1980).

Example 3.36 Let $A = \{1,3,5\}, B = \{2,4\}, R_1 = \{(x,y) \in A \times A | x \leq y\}, R_2 = \{(x,y) \in B \times B |$y is divisiable by x$\}$. The following sketch is represents $(A \times B, R_1 \times R_2)$.

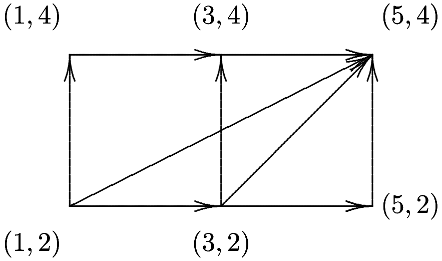


Figure 3.7: $(A \times B, R_1 \times R_2)$

Definition 3.29 Let A be a partial ordered set by a relation R. The element $b \in A$ said to be a least element of A according to R if $bRx, \forall x \in A$(Davey and Priestley, 2002; Armstrong, 1997).

Example 3.37 Let $A = \{3, 6, 9, 12, 15\}$, and let R_1, R_2, R_3 relations defined on A as follows:

$R_1 = \{(x, y) \in A \times A | x \leq y\}$, $R_2 = \{(x, y) \in A \times A | x \geq y\}$, and $R_3 = \{(x, y) \in A \times A | \text{y is divisiable by x}\}$. All R_1, R_2, R_3 are the partial ordered relations on A.

The number 3 is a least element in A with respect to R_1, because $3 \leq x, \forall x \in A$, where 15 is a greatest element in A with respect to R_2, because $15 \geq x, \forall x \in A$. Also, 3 is a least element in A with respect to R_3, because each element in A is divided by 3.

Example 3.38 Consider a relation R on the set $A = \mathbb{N}$ and R, defined as: $R = \{(x, y) \in A \times A | x \leq y\}$. R is a partial ordered relation on A, and 0 is a least element in A with respect to R, because $0 \leq x, \forall x \in A$. It noted that there dose not a greatest element for A with respect to the relation.

Example 3.39 Let R be a relation on $P(X)$ defined as: $R = \{(A, B) \in P(X) \times P(X) | A \subseteq B\}$. The empty set is a least element in $P(X)$ with respect to R, because $\phi \subseteq A, \forall A \in P(X)$.

Theorem 3.19 *Let A be a partial ordered set by the relation R. If A has a least element it will be a unique.*

Proof Suppose that each of a, a' is a least element of A.

From the definition of least element, we conclude that:

$aRa' \wedge a'Ra$.

$\because R$ is anti-symmetric, $\therefore aRa' \wedge a'Ra \to a = a'$.

Thus, there is a unique least element. ♦

Definition 3.30 Let A be a partial ordered set by a relation R. The element $m \in A$ said to be a greatest element of A according to R if there does not any element $x \in A$ such that $mRx \wedge m \neq x, \forall x \in A$(Davey and Priestley, 2002; Armstrong, 1997).

Example 3.40 Consider $A = \{3, 5, 6, 9, 10, 12, 13\}$. Let R_1, R_2, R_3 relations on A defined as:

$R_1 = \{(x, y) \in A \times A | x \leq y\}$, $R_2 = \{(x, y) \in A \times A | x \geq y\}$, and $R_3 = \{(x, y) \in A \times A | y \text{ is divisible by } x\}$.

Each of R_1, R_2, R_3 is a partial ordered relation on A.

The number 3 is a greatest element in A with respect to R_1, because it does not element $x \in A$ such that $3 \geq x \wedge 3 \neq x$. And the number 18 is the greatest element with respect to R_2 because there does not $x \in A$ such that $18 \leq x \wedge 18 \neq x$. The number 7 is the greatest element with respect to R_3 because there does not $x \in A$ divided by 7 and $x \neq 7$ in the same time. And for the same reasonable the numbers $12, 13, 15, 18$ are greatest elements with respect to R_3.

Example 3.41 Let each of,
$X = \{1, 3, 5, 6, 7\}, E = \{\{1, 3\}, \{5, 7\}, \{1, 3, 5\}, \{1, 3, 7\}, X\}$.
Also, let R_1, R_2 be relations on E, defined as:
$R_1 = \{(A, B) \in E \times E | A \subseteq B\}$
$R_2 = \{(A, B) \in E \times E | A \supseteq B\}$.

Each of R_1, R_2 is partial ordered relation on E. The element X is the greatest element with respect to R_1 because there does not any element in E with respect to R_1, there does not element $B \in E$ such that $X \subseteq X \wedge B \neq X$. But, the set $\{5, 7\}$ is the greatest element with respect to R_2.

Note: All greatest element is maximal, but maximal element need not be greatest.

Definition 3.31 Let A be a partial ordered set by the relation R. The element $n \in A$ is called minimal element in the set with respect to the relation R, if there does not element $x \in A$, such that $xRn \wedge x \neq n$ (Richmond and Richmond, 2004; Scott, 2012).

Example 3.42 Let $A = \{3, 5, 9\}$, and $R_i, i = 1, 2, 3$ is a relation on A defined as follows:
$R_1 = \{(x, y) \in A \times A | x \leq y\}$,
$R_2 = \{(x, y) \in A \times A | x \geq y\}$, and
$R_3 = \{(x, y) \in A \times A | y$ is divisiable by $x\}$.

Each of $R_i; i = 1, 2, 3$ is a partial ordered relation on A. The number 3 is the minimal with respect to R_1, because there does not element $x \in A \ni x \leq 3 \wedge x \neq 3$. The number 9 is the minimal with respect to R_2, because there does not element $x \in A \ni x \geq 3 \wedge x \neq 9$. The number 3 is the minimal with respect to R_3, because there does not element $x \in A$, such that 3 divisible on x and $x \neq 3$. And that why 5 will be a minimal element in A with respect to R_3. Or, each of $3, 5$ is a minimal element with respect to R_3.

Example 3.43 Consider $X = \{a, b, c, d\}$
, $E = \{\{a, b\}, \{b, d\}, \{a, b, c\}, X\}$. And R_1, R_2 relations on E defined as:

$R_1 = \{(A, B) \in E \times E | A \subseteq B\}$, $R_2 = \{(A, B) \in E \times E | A \supseteq B\}$.

Each of R_1, R_2 is a partial ordered relation on E.

The set $\{a, b\}$ is the minimal element in E with respect to R_1, because there does not a set $A \in E$ such that $A \subseteq \{a, b\} \wedge A \neq \{a, b\}$. And for the same reason $\{b, d\}$ is the minimal element in E with respect to R_1.

The set $X \in E$ is the minimal element with respect to the relation R_2, because of there dose not a set $A \in E$ such that $A \supseteq X \wedge A \neq X$.

Notes:

(i) Least element is a minimal element, but the vice versa is not true.

(ii) Each finite partial ordered set has at least maximal element and minimal element.

(iii) If R is a partial ordered relation on A, then $x \leq y$ in the set $(A, R) \leftrightarrow x \geq y$ in the set (A, R^{-1}). And, $a \in A$ is a maximal element in A, R if and only if a is a minimal element in (A, R^{-1}). Conversely, a is a maximal element in (A, R) if and only if a is a maximal element in (A, R^{-1}).

Definition 3.32 Let $(A, \preceq)$ be a partial ordered set, and $B \subseteq A$. The element $a \in A$ is called:

- Upper bound of B in A if $xRa, \forall x \in B$. Or, $a \geq x, \forall x \in B$. In this case, we say that B is bounded above.

- Lower bound of B in A if $aRx, \forall x \in B$. Or, $a \leq x, \forall x \in B$. In this case, we say that B is bounded below.

(Saunders and Birkhoff, 1999).

Example 3.44 (i) Consider $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} | x \leq y\}$, and let $B = [2, 3]$. The number $5 \in \mathbb{R}$ is the upper bound to B, and $1 \in \mathbb{R}$ is the lower bound to B.

(ii) Let $A = \{5, 3, 12, 10, 30\}$, $R = \{(x, y) \in A \times A | y \text{ divided is by } x\}$, and $B = \{5, 10\}$. The number $30 \in A$ is the upper bound to B, while $5 \in A$ is the lower bound to B.

Definition 3.33 Let A be a partial ordered set, and $B \subseteq A$. The element $x \in A$ is called least upper bound to the set B in A if:

- x is un upper bound to B.
- $x \leq y$ for all upper bound y to B.

In other words; x is upper bound and it is a minimal element for the set of all elements with are upper bound for A, and denoted by $lubB$, or $supA$ (Bartle and Sherbert, 2011; Bressoud, 2007; Browder, 2012; Rudin et al., 1976; Willard, 2004).

Definition 3.34 Let A be a partial ordered set, and $B \subseteq A$. The element $x \in A$ is called greatest lower bound to the set B in A if:

- x is a lower bound to B.
- $x \geq y$ for all lower bound y to B.

In other words; x is lower bound and it is a maximal element for the set of all elements with are lower bound for A, and denoted by $glbB$, or $infA$ (Bartle and Sherbert, 2011; Bressoud, 2007; Browder, 2012; Rudin et al., 1976; Willard, 2004).

Example 3.45 Let $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} | x \leq y\}$, and let $B = [-1, 5]$. Then, $supB = 5, infB = -1$.

Notes: Let $(A, \leq)$ be a partial ordered set, and $B \subseteq A$ then:

(i) If $supB$ exists then it is a unique. As well as for $infB$.

(ii) b will be upper bound for the set B in $(A, \leq)$ if and only if b is lower bound for the set B in $(A, \geq)$.

(iii) $b = supB$ in $(A, \leq)$ if and only if $b = infB$ in $(A, \geq)$.

Definition 3.35 Let (A, R) be a partial ordered set. The set (A, R) called complete, if and only if each $B \subseteq A$ bounded above. Or, *supB* is existed. This, equivalency mean, each $B \subseteq A$ is bounded below. (Abramsky et al., 1992; Burris and Sankappanavar, 2006; Markowsky, 1976)

Example 3.46 (1) Let $A = \mathbb{R}$, then $(A, \leq)$ is a complete. (How?)

(2) Let $A = \mathbb{Q}$, then $(A, \leq)$ is not complete. (How?)

Definition 3.36 Let (A, R) be partil ordered set. A said to be lattice if and only if the binary $\{x, y\}$ has *sup*, and *inf*. The $sup\{x, y\}$ denoted by $x \vee y$, and $inf\{x, y\}$ denoted by $x \wedge y$(Grätzer, 2011; Birkhoff, 1940; Birkhoff, 1967; Birkhoff and Mac, 2017).

3.12.4 Totally Ordered Sets

Definition 3.37 Let $(A, \leq)$ be a partially ordered set. the binary elements x, y in A are called comparable if $x \leq y$ or $y \leq x$, otherwise they are incomparable(Trotter, 1992; Gilmore and Hoffman, 2003).

Example 3.47 (1) Let $A = \mathbb{Z}^+$, and R be a relation defined on A as: $R = \{(x, y) \in A \times A | x \text{ divisable on } y\}$. A will be partial ordered set by R. It should be noted that no binary elements in A comparable. Foe example, $3, 4$ are incomparable, because 3 is not divisible by 5, and vise versa. Thus, A is not totally ordered set by R.

(2) Consider $X = \{1, 3, 5\}$. Let us consider, the partial ordered set $(P(X), \subset)$. Again, it should be noted that, no binary elements in $P(X)$ are comparable, because if we take any two elements $A = \{1\}, B = \{3\}$ in $P(X)$ it is not necessary $A \subseteq B$, or $B \subseteq A$. Thus, $A \nsubseteq B$, also $B \nsubseteq A$.

(3) Assume that the partial ordered set $(\mathbb{Z}, \leq)$. Note that each binary elements x, y in $\mathbb{Z}$ are comparable. Thus, $x \leq y$, or $y \leq x$. Thus, $\mathbb{Z}$ is totally ordered set by the relation $\leq$.

Definition 3.38 Let A be totally ordered set, and let B be a subset of A. If each binary elements in B is comparable then B is called totally ordered subset. Sometimes, B is called chain in A, and if each binary elements is comparable then A is called totally ordered set (Markowsky, 1976; Mustafa et al., 1980).

Example 3.48 (1) The binary $(\mathbb{Z}, \leq)$ is a totally ordered set, because it satisfies; (i) $(\mathbb{Z}, \leq)$ is partially ordered set, and (ii) each binary elements in it is comparable.

(2) Consider the sets, $A = \{a | a \in \mathbb{N} \wedge 1 \leq a \leq 9\}$, $B = \{2, 4, 8\}$, $R = \{(x, y) \in A \times A | x \text{ divisable by } y\}$.

It should be noted that not each binary elements in A are comparable, while each binary elements are comparable in B.

Thus, the set (A, R) is not totally ordered set, while the set $(B, R/B)$ is totally ordered set.

Note: All subset of a totally ordered set is a totally ordered set.

Theorem 3.20 *Let each of $(A, R_1), (B, R_2)$ be a totally ordered set. The $(A \times B, R)$ is a totally ordered set by the lexicographic ordering relation R on $A \times B$.*

Proof Consider $x = (a, b), y = (a', b')$ are elements in $A \times B$.

There are two possible cases:

(1) $a = a'$, but $b \neq b'$.

Since, B is totally ordered set, hence $aR_1a' \vee a'R_1a$. Thus, $xRy \vee yRx$. Thus, $A \times B$ is a totally ordered set by the relation R.

(2) $b = b'$, but $a \neq a'$.

By the same way $A \times B$ is a totally ordered set by the relation R . ♦

Theorem 3.21 *Let (A, R) be a totally ordered set. There exists at most one minimum element, and it is a minimal element. Furthermore, there exists at most one maximum element, and it is a maximal element.*

Proof Let a_1, a_2 be minimum elements, and $a_1 \neq a_2$.

there does not exists $x \in A$ such that; $a_1 \not R\, x$.

Also there does not $x \in A$ such that; $xRa_2 \wedge x \neq a_2$.

But, A is ordered set by the relation R, thus $a_1Ra_2 \vee a_2Ra_1$. And this is contradiction, there for $a_1 = a_2$.

Now, we have to prove that a_1 is a minimal element. Or, $a_1Rx, \forall x \in A$.

Let us consider $x \in A, a_1Rx$. Since A is totally ordered set, this implies that xRa_1. This is contradiction, because a_1 is minimum element.

By the same way the rest of the theorem can be proved. ⧫

3.12.5 Well Ordered Sets

Definition 3.39 Let R be a partial ordered relation on the set A. A is said to be well ordered set if and only if, the following condition is satisfied: For all nonempty subset of A has least element (Cantor, 1883b; Hausdorff, 1914b; Aleksandrov, 1967; Nicolas, 1968; Kuratowski and Mostowski, 1976; Levy, 2002).

Theorem 3.22 *Every well ordered set is a totally ordered set.*

Proof Let A be well ordered set, and $(x, y) \in A$. Let $B = \{x, y\} \subseteq A$. Thus, B has least element which is either x or y. Therefor, in the set A each binary element will be comparable, and this implies A be totally ordered set. ⧫

Example 3.49 (1) Let,

$A = \{2, 3, 4, 5, 6\}$, $R = \{(x, y) \in A \times A | x \leq y\}$. The set is well ordered set over the R.

(2) Let $\mathbb{N} = \{0, 1, 2, ...\}, R = \{(x, y) \in \mathbb{N} \times \mathbb{N} | x \leq y\}$.

The set $(\mathbb{N}, R$ is well defined set.

(3) The set $\mathbb{Z}$ does not well defined, because if we consider the set $A = \{..., -3, -2, -1, 0\} \subseteq \mathbb{Z}$ has no least element.

Theorem 3.23 *Consider the well ordered set A, then for all $a \in A$ except the greatest element immediate successor.*

Proof Note that the following set: $T = \{y \in A | y > a\}$ is nonempty subset of A. Therefor, T has a least element, which will be immediate successor of a. ♦

Definition 3.40 Let A be partial ordered set, the section of A is a subset B or $B \subseteq A$ has the following property: $\forall x \in A\ [(y \in B \wedge x \leq y) \rightarrow x \in B]$ (Mustafa et al., 1980).

Theorem 3.24 *Let A be well ordered set, and $B \subseteq A$. The set B is a section of A if and only if $B = A$, or B is an initial segment of A.*

Proof If $B = A$, or an initial segment of A then B will be a section of A.

Now, let us go on another path to prove the theorem.

Assume that B is a section of A, and then there are two possibilities:

- $B = A$, the proof has been over.
- $B \neq A$, or $A - B \neq \phi$. Therefor, the set $A - B$ has a least element, and let us denote it by m.

  Now, we are going to prove that $B = \{x | x < m\} = S_m$; where S_m is an initial segment determined by the element m.

  Now, if $x \in S_m, x < m \rightarrow x \in B$.

  Conversely, if $x \in B \rightarrow x < m$, because if $m \leq x \rightarrow m \in B$.

  And this is contradiction, based on the definition of the section, because $x \in A - B$.

  Thus, $x \in B \rightarrow x < m \rightarrow x \in S_m$.

  Therefore, $B = S_m$. ♦

In what follows, we are introduce a theorem, has been know as: Principle of transfinite induction

Theorem 3.25 *Let A be well ordered set, and $P(x)$ be an open sentence in x on the set A. And assume that the following condition provided: [If $P(y)$ is true statement for all $y < x$ then $P(x)$ is true]. Then $P(x)$ is true for all $x \in A$.*

Proof Assume that $P(x)$ is not true $\forall x \in A$.

Now, let us define the set T as following:

$T = \{y \in A | P(y) \text{is a false}\}$. Now, $T \subseteq A$

Therefore, the set T has a least element, let named it m. Since $P(x)$ is true for all $x < m$, hence $P(m)$ will be true according to the given condition. But, based on the selection m, $P(m)$ is a false, because m is a least element leads $P(m)$ to be false, and this contradiction.

Thus, $P(x)$ should be true $\forall x \in A$. ⧫

Let us complete this chapter, by the well ordering theorem which is important th the next chapter in the functions and mappings.

Now, we are ready to submit the following theorem and going to prove it in the next chapter.

Theorem 3.26 *Every set A, can be ordered as a well ordering set.*

3.13 Exercises

Solve the following questions:

Q1: Write all possible partial ordered relations on the set $A = \{0, 1, 2\}$, and show that the totally ordered relations.

Q2: Show that if ϕ can be partially ordered relation?

Q3: Consider δ is a subset of of partial ordered relations on A. Prove that $\cap\delta$ is a partial ordered relation.

Q4: If S is a partial ordered relation on the set X, and $A \subseteq X$. Prove that $S \cap (A \times A)$ is a partial ordered relation. And, prove that if S is totally ordered relation then $S \cap (A \times A)$ is totally ordered relation on A.

Q5: Let S be a partial ordered relation on X. Prove that $S - I_X$ is a strict order relation.

Q6: Let S be strict order relation on X. Prove that $S \cup I_X$ is partial order relation.

Q7: Give an example on a set X and on a set δ of partial order relations on X to show that $\cup\delta$ is not partial order relation on X.

Q8: Draw Hasse Diagram for the ordered sets (X, S), $X = \{a, b, c, d, e\}$, $S = \{(a, d), (a, c), (a, b), (a, e), (b, e), (c, e), (d, e)\} \cup I_X$

Q9: Let (X, S) be a subset where, $X = \{a, b, c, d\}$, $S = \{(c, d)\} \cup I_X$. Determined least element, maximum element, minimal element, and maximal element.

Q10: Prove that, if X is a partial ordered set, and has two minimum elements then it has no minimal element.

Q11: Consider the partial order set (X, R), and let $A \subseteq X$, where X is a finite and totally ordered set, let $a = supA$. Prove that a is a maximal element for A. Furthermore, give an example, to show that if A is not totally order set the the previous conclusion is false.

Q12: Let S be a anti-symmetric on X. Give an example to prove that: There does not a partial order relation T on X such that $S \subset T$. In other words, not all anti-symmetric relation can be extend to a partial order relation.

Q13: Let $\{S_i\}_{i \in I}$ be a family of nonempty equivalence relations on the totally ordered set X by the containment relations. Prove that $\cup_{i \in I} S_i$ is an equivalence relation on X.

Q14: Prove that each subset of well ordered set is a well ordered set.

Q15: Let (X, R) be a well ordered set. The set (X, R^{-1}) is a well ordered set if and only if X is a finite set.

Q16: Prove that the set X is a finite if and only if any totally ordered relation on X is well ordered relation.

Q17: Consider the well ordered sets: $(A_1, R_1), ..., (A_n, R_n)$. Prove that $(\prod_{i=1}^{n} A_i, R)$ will be well ordered set, where R is a lexicographic ordering relation on $\prod_{i=1}^{n} A_i$.

Q18: Let each of $(A, R_1), (B, R_2)$ be an partial order subset. Prove that:

(i) Let $A \times B$ be ordered by the lexicographic ordering relation R. Prove that if (a, b) is a maximal element in $A \times B$ then a is a maximum element in A.

(ii) Let $A \times B$ be ordered set by the anti-lexicographic ordering relation. Prove that if (a, b) is a maximal element in $A \times B$ then b is a maximal element in B.

4
Mapping

4.1 Introduction

A mapping (function) is a relation that uniquely associates members of one set with members of another set. A function from is an object such that every is uniquely associated with an object. More formally, it is therefore a many-to-one (or sometimes one-to-one) relation.

Mapping is one of the important basic mathematical concepts. It enters almost any mathematical discussion, and in all areas of the real life.

Consider the sets A, B. The mapping from A to B is a rule of correspondence, such that for all $x \in A$ corresponds a unique element $y \in B$, and denoted by: $x \to y$, where y is called image of x.

The concepts mapping and function are synonyms, the function from A to B it means mapping from A to B. In other words, mapping from A on a subset C in B. The set A is called domain of the mapping, while the se B is called codomain, and C is a range of the mapping.

Mapping ought to be distinguished between $f, f(x)$, the f is the function from A to B, while $f(x)$ is the element $y \in B$ corresponds to the element $x \in A$. The express $y = f(x)$ is read y is a function of x.

The graph of a function is a mapping from A to B, the graph of

f is the set of all ordered pairs $(x, y) \in A \times B$, such that $y = f(x)$. Thus, f is essentially is the graph of the function, and no need to be distinguished between them, they are same, and the function is special case of the relation. Based on what came previously we can set the definition of the mapping.

4.2 Mapping

Definition 4.1 Let each of A, B be a set. The mapping from A to B is an ordered triple (f, A, B) where f is a subset of $A \times B$ provides: (1) $\forall x \in A, \exists y \in B \mid (x, y) \in f$. (2) If $(x, y_1) \in f, (x, y_2) \in f \to y_1 = y_2$ (Halmos, 2017b; Saunders and Birkhoff, 1967).

In the definition, the second condition is a functional relation. The expression of the function in the form of $f : A \to B$ instead of (f, A, B) is more convenient. Furthermore, the conditions in the definition can be combined in a unique condition as; $\forall x \in A \exists !\ y \in B \ni (x, y) \in f$. x is called independent variable, and y is called dependent variable.

4.3 The Basic Definitions

Definition 4.2 Let each of A, B be a set. The relation $R : A \to B$ is called a functional relation if provided the following condition: $(x, y_1) \in R \wedge (x, y_2) \in R \to y_1 = y_2$ (Halmos, 2017b; Mustafa et al., 1980).

Example 4.1 (1) Let $A = B = \mathbb{R}, R = A \to B$, and consider the relation $R = \{(x, y) \in A \times B | y = x^2\}$. If $(x, y_1) \in R \wedge (x, y_2) \in R$, or $y_1 = x^2 \wedge y_2 = x^2 \to y_1 = y_2$. Thus, R is a functional relation from A to B. (2) Let $A = \{0, 3, 4, 7\}, B = \{20, 6, 41, 11\}$, and $R = \{(0, 41), (4, 20), (3, 20), (7, 6), (7, 11)\}$. R is not functional relation because $(7, 6) \in R \wedge (7, 11) \in R$, but $6 \neq 11$.

Definition 4.3 Let each of A, B be a set, and $f : A \to B$ be a relation. The triple (f, A, B) is called a mapping from A to B, if the following conditions are provided: (1). $\forall x \in A, \exists y \in B \ni (x, y) \in f$. (2). f is a functional relation(Halmos, 2017b; Wilder et al., 2012).

Example 4.2 Consider each of $A = \{a, b, c, d\}, B = \{x, y, z\}$, and let $f : A \to B$ be a relation defined as $f = \{(a, x), (b, y), (c, x), (d, z)\}$. The triple (f, A, B) is a mapping from A to B because each element of A has been connected by a unique element in B, and f is a functional relation.

Example 4.3 Let $A = \{0, 2, 4, 6\}, B = \{0, 1, 2, 3, 5, -1, -3, , 9, 20\}$, and let $f = \{(x, y) \in A \times B | y = 2x - 3\}$.

Since all element in A connected with just one element in B, hence (f, A, B) is a mapping from A to B. Note that if $x = 0 \to y = -3$, $x = 2 \to y = 1$, $x = 4 \to y = 5$, and $x = 6 \to y = 9$.

Example 4.4 Let $A = [-1, 2), B = [2, 4]$, and let
$f = \left\{(x, f(x)) | f(x) = \begin{Bmatrix} 1 - 2x; x \in A \\ x; x \in B \end{Bmatrix}\right\}$.

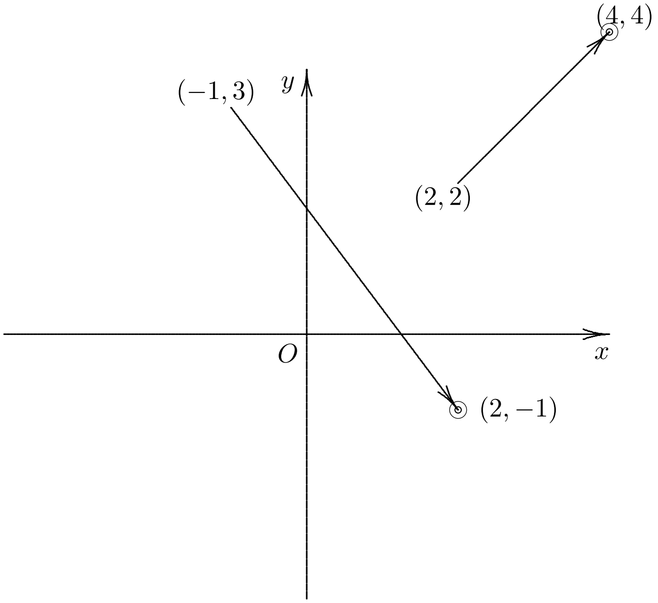


Figure 4.1: $y = f(x)$

The triple (f, A, B) is a mapping from A to B. By observing the graph of the function from the Figure 4.1 it can be inferred that $(2, -1) \notin f$.

Definition 4.4 If (f, A, B) is a mapping, then

(1) The set A is called domain. (2) The set B is called codomain. (3) If $(x, y) \in f$, then y is the image of x, and x is called preimage of y, and denoted by $y = f(x)$(Eccles, 1997; Forster, 2003; Scott, 1967).

Note: Vinn diagrams is on of methods to express of mapping as shown in Figure 4.2.

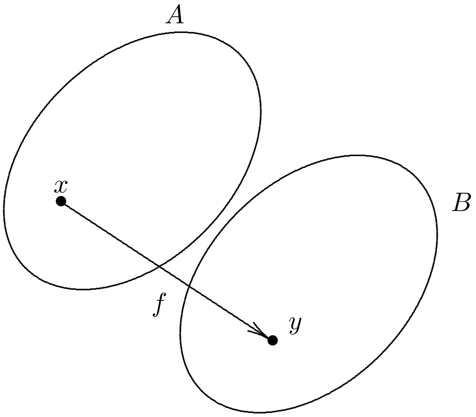


Figure 4.2: Vinn Diagram as a Function

Example 4.5 Let $A = \{a, b, c\}, B = \{x, y, z\}$.

The function f is illustrated by Vinn diagram in Figure 4.3.

Definition 4.5 Consider the function (f, A, B). The set of all elements which are images of all elements of A is called range of mapping, and denoted by *ran* f. Or, *ran* $f = \{y \in B | \exists x \in A \ni y = f(x)\}$ (Childs, 2009; Dummit and Foote, 2004a; Rudin, 1991).

Note: Consider the mapping (f, A, B), then: (1). *dom* $f = A$. (2). *ran* $f \subseteq B$.

Example 4.6 (1) Let $A = B = \mathbb{R}, f = \left\{(x, y) \in A \times B | y = \sqrt{x^2}\right\}$. The relation $f : A \to B$ is mapping, because $y = \sqrt{x^2} = |x| = \begin{cases} x; \forall x \geq 0 \\ -x; \forall x \leq 0 \end{cases}$

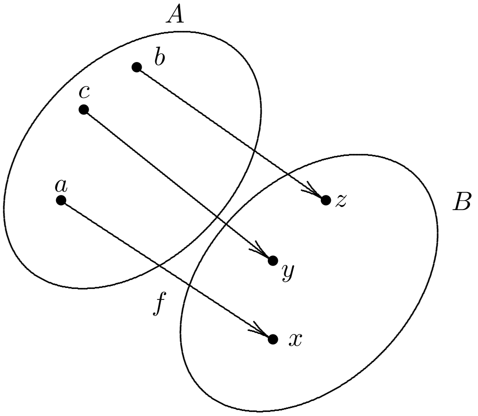


Figure 4.3: Graph of f

$dom\ f = \mathbb{R}, ran\ f = \mathbb{R}^+$.

(2) Let $A = \left\{0, \frac{1}{3}, \frac{1}{5}, -1, -2, 4, 9, \frac{-1}{5}\right\}, B = \mathbb{R}$, and $f = \left\{(x,y) \in A \times B \ni y = \left\{\begin{array}{c} x^4; \forall x \in \mathbb{Z} \\ \frac{-1}{4}x; \forall x \notin \mathbb{Z} \end{array}\right\}\right\}$.

The triple (f, A, B) is a mapping.
$dom\ f = A$, $ran\ f = \left\{0, -\frac{1}{12}, -\frac{1}{20}, \frac{1}{20}, 1, 16, 256, 6561\right\}$.

4.4 Graph of the Mapping

Definition 4.6 Consider the mapping (f, A, B). The set of all ordered pairs $(x, y) \in A \times B$ is called Graph of the mapping f, and denoted by G. Or, $G = \{(x, y) \in A \times B | y = f(x)\}$(Pinter, 1976; Pinter, 2014; Bridges et al., 1998).

Note: Consider the function $f : A \to B$. Then (1) $G \subseteq A \times B$. (2) $G = f$.

Example 4.7 (1) Let $(f, \mathbb{R}, \mathbb{R})$ be a function such that: $f(x) = -x^2$. The graph of the function will be $G = \{(x, y) \in \mathbb{R} \times \mathbb{R} | y = -x^2\} = \{(0, 0), (1, -1), (-1, -1), (2, -4), (-2, -4), ...\}$.

(2) Let $A = \{0, 2, 4, 6, 8\}, B = \{1, 3, 5, 10, 11, 15, 17, 21, 23, 25, 29\}$. Let (f, A, B) be a mapping where $f(x) = 3x + 5$. The

graph of the function is $G = \{(x,y) \in A \times B | y = 3x+5\} = \{(0,5),(2,11),(3,17),(6,23),(8,29)\}$.

Note that the set $\mathtt{L} = \{(0,1),(2,5),(3,17),(6,23),(8,29)\}$ is not the graph of the function $f : A \to B$, because $\mathtt{L} \neq G$.

Note: Consider the sets A, B. The set of all mappings from A to B denoted by B^A.

Theorem 4.1 *If the set A contains m of elements, and the set B contains n of elements then the set B^A contains n^m of elements.*

Proof Suppose that $A = \{a_1, a_2, ..., a_m\}, B = \{b_1, b_2, ..., b_n\}$. The element a_1 may be connected by any element of B. Since, $n(B) = n$, hence, a_1 could connects by any element of B which these elements are n. So, as to the element a_2 can be connected by any element of B by n of ways. Thus, the number of connections of elements of A by the elements of B as follows: $\underbrace{n.n...n}_{m-\text{times}} = n^m$. ♦

4.5 Surjective Mapping

Definition 4.7 The function $f : A \to B$ is surjective (onto) if and only if $ranf = B$. Or, $\forall y \in B, \exists x \in A \ni y = f(x)$ (Bourbaki, 2004).

Example 4.8 Let $A = B = \mathbb{R}, f : A \to B$, such that f is defined as; $f = \{(x,y) \in A \times B | y = 3x - 1\}$. The function f is surjective. Suppose that $y \in B \exists x \in A | x = \frac{y+1}{3}$. Since, $f(x) = 3x - 1 = 3(\frac{y+1}{3}) - 1 = y$. Thus, $\forall y \in B \exists x \in A \ni y = f(x)$. Note that $ranf = B$. That why $f : A \to B$ is surjective.

Example 4.9 Let $A = \{-1,0,1,3,5,7,9\}, B = \{0,1\}$, and $f = \{(-1,0),(0,0),(1,0),(3,0),(5,0),(7,1),(9,1)\}$. Since, $ranf = B$, hence f is surjective.

Example 4.10 Let $A = x \in \mathbb{R} | x \geq -1, B = \mathbb{R}$. Define $f : A \to B$ as; $f = \left\{(x,y) \in A \times B | y = x^2 - \frac{1}{2}\right\}$. The function (f, A, B) is not surjective, because $ranf = \left\{y \in B | y \geq \frac{-1}{2}\right\} \neq B$.

4.6 Injective Mapping

Definition 4.8 The function $f : A \to B$ is called injection function if and only if $f(x_1) = f(x_2) \to x_1 = x_2, \forall x_1, x_2 \in A$. Or, $\forall x_1, x_2 \in A \wedge x_1 \neq x_2 \to f(x_1) \neq f(x_2)$(Bartle et al., 1976; Halmos, 2017b).

Example 4.11 Let $A = \{-1, -3, 7, 9\}, B = \{2, 0, 1, 3, 5, 7\}$. Both of f, g are mapping from A to B, such that;
$f = \{(-1, 2), (-3, 0), (7, 5), (9, 3)\}, g = \{(-1, 5), (-3, 7), (7, 0), (9, 0)\}$. f is the injection function because the different elements in A have different images in B. g is not injective function because 0 is the image for two different elements $7, 9$.

Note: If $x_1 \neq x_2 \to f(x_1) \neq f(x_2), \forall x_1, x_2 \in A$.

Example 4.12 Let $A = [-2, 5] \subseteq \mathbb{R}, B = \mathbb{R}$. Let each of f, g be a function from A to B, such that; $f = \{(x, y) \in A \times B | y = x^3)\}, g = \left\{(x, y) \in A \times B | y = 3x^2 + \frac{1}{2}\right\}$. f is the injection function because if we assume that $f(x_1) = f(x_2) \to x_1^3 = x_2^3 \to x_1 = x_2$. Or, the different elements in A have different images in B. g is not injective function, because $-2 \neq 2$, while $f(-2) = f(2) = \frac{25}{2}$. Or, the value $\frac{25}{2}$ is the same image for two different elements $-2, 2$ in A.

4.7 Bijective Mapping

Definition 4.9 The function (f, A, B) is called bijective if and only if it is injective and surjective(Mustafa et al., 1980; Bourbaki, 2004; Bartle et al., 1976; Halmos, 2017b).

Note: The bijective function called one- one correspondence function because (1) $\forall x \in A\ \exists! y \in B \ni y = f(x)$. (2) $\forall y \in B \exists! x \in A \ni x = f^{-1}(y)$.

Example 4.13 Consider $A = \{1, 3, 5, 7, 9, ...2n + 1\}$, and $B = \{2, 4, 6, 8, 10, ...2n\}; \forall n \in \mathbb{N}$. Let f, g be functions from A to B such that $f = \{(x, y) \in A \times B | y = 2x\}$, $g = \{(x, y) \in A \times B | y = x + 1\}$. f is not bijective function because, $4 \in B, x \notin A \ni 4 = f(x)$. g is bijective function because it is both injective and surjective.

Example 4.14 Let $A = B = \mathbb{R}$, and (f, A, B) be a function, where $f = \{(x, y) \in A \times B | y = -2x^3 - 7\}$. f is bijective function because it is both injective and surjective.

4.8 Equality of Mapping

Definition 4.10 Let each of $(f_1, A_1, B_1), (f_2, A_2, B_2)$ be function. The two functions are equal, if and only if $A_1 = A_2, B_1 = B_2, f_1 = f_2$ (Rosser, 2008; Hamilton, 1988; Kleene, 2002; Ebbinghaus et al., 2013).

Example 4.15 (1) Let $f : \mathbb{R} \to \mathbb{R}, g : \mathbb{R} \to \mathbb{R}$ where $f = \frac{x^2-5x+6}{x^2-6x+8}$, $g(x) = \frac{x-2}{x-4}$. $f = \frac{(x-3)(x-2)}{(x-3)(x-4)} = \frac{x-2}{x-4} = g(x)$. Thus, $f(x) = g(x)$ with the same domains and codomains.

(2) Let each of f, g defined on $\mathbb{R}$ as follows

$f = \{(x, y) \in \mathbb{R} \times \mathbb{R}|\ y = |x|\}$, $g = \left\{(x, y) \in \mathbb{R} \times \mathbb{R}|\ y = \sqrt{x^2}\right\}$.

Each of $(f, \mathbb{R}, \mathbb{R}), (g, \mathbb{R}, \mathbb{R})$ is mapping, and since $f = g$, hence they are equal.

Example 4.16 Let $f : \mathbb{R} \to \mathbb{R}$ where $f = \{(x, y) \in \mathbb{R} \times \mathbb{R}|\ y = |x|\}$. And, $g : \mathbb{N} \to \mathbb{Z}$ where $f = \{(x, y) \in \mathbb{N} \times \mathbb{Z}|\ y = |x|\}$. $f \neq g$ because $\mathbb{R} \neq \mathbb{N}$, and $\mathbb{R} \neq \mathbb{Z}$.

Theorem 4.2 *Let each of $(f, A, B), (g, A, B)$ be a mapping. $f = g \leftrightarrow f(x) = g(x), \forall x \in A$.*

Proof Suppose that $f = g$, and $x \in A$.

$\because f(x)$ is image of x in B under the application of the mapping f. And $g(x)$ is also image of x in B under the application of the mapping g.

Let $f(x) = y$.

Now $f(x) = y \leftrightarrow (x, y) \in f \leftrightarrow (x, y) \in f; (f = g)$

Thus, $g(x) = y \leftrightarrow f(x) = g(x), \forall x \in A$.

Conversely, let $f(x) = g(x), \forall x \in A$.

To prove $f = g$, let $(x, y) \in f$.

Now, $(x, y) \in f \to y = f(x) \to y = g(x) \to (x, y) \in g$.

Or, $f \subseteq g$.

In the same method, if we suppose $(x, y) \in g \to (x, y) \in f$.
Or, $g \subseteq f$.
Thus, $f = g$. ♦

4.9 Types of Mappings

4.9.1 Identity Mapping

The function $f : A \to A$ is called identity mapping on A if and only if $f(x) = x; \forall x \in A$, and denoted by I_A(Knapp, 2007; Mapa, 2003; Anton et al., 2005).

Note:

(i) An I_A also called an identity relation or identity map or identity transformation.

(ii) An I_A is bijective function.

Example 4.17 Let $A = \{a, b, c, 0, 1, 5\}$.

(1) $f = \{(a, a), (b, b), (c, c), (0, 0), (1, 1), (5, 5)\}$. f is identity function because $(x, x) \in f; \forall x \in A$.

(2) $g = \{(a, a), (b, b), (c, c), (1, 1), (5, 5)\}$. Since $0 \in A$, but $(0, 0) \notin g$, hence g is not identity function.

4.9.2 Constant Mapping

Definition 4.11 The function $f : A \to B$ is called constant mapping if and only if $\exists c \in B$, and $\forall x \in A \ni f(x) = c$ (Tanton, 2005; Weisstein, 1999a).

Note: Let (f, A, B) be a constant mapping.

(i) If A consists of more than one element, then f is not injective.

(ii) If B consists of more than one element, then f is not surjective.

Example 4.18 Let $f : \mathbb{R} \to \mathbb{R}$ be a function such that $f = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} | y = -\frac{1}{3}\right\}$. Since $f(x) = -\frac{1}{3}; \forall x \in \mathbb{R}$. Thus, $f : \mathbb{R} \to \mathbb{R}$ is a constant mapping.

4.9.3 Inclusion Mapping

Definition 4.12 Let $\phi \neq A \subseteq B$, the mapping $f : A \to B$ is called inclusion mapping if and only if $f(x) = x, \forall x \in A$ (MacLane and Birkhoff, 1999).

Note: Inclusion mapping called inclusion function, insertion, or canonical injection.

Example 4.19 Let $f : \mathbb{R} \to \mathbb{C}$, and defined as:
$f = \{(x, y) \in \mathbb{R} \times \mathbb{C} | y = x\}$. Since $\mathbb{R} \subseteq \mathbb{C}$, and $f(x) = x, \forall x \in \mathbb{R}$, hence $f : \mathbb{R} \to \mathbb{C}$ is inclusion mapping.

Example 4.20 Let $A = \{x \in \mathbb{R} | -10 \leq x \leq 10\}, B = \mathbb{R}$, $f : A \to B$, and defined as $f = \{(x, y) \in A \times B | y = x\}$. Since $A \subseteq B$, and $f(x) = x, \forall x \in A$, hence $f : A \to B$ is inclusion mapping.

Note: Consider $f : A \to B$ be an inclusion mapping then:
(1) If $A = B$ then $f = I_A$. (2) The inclusion mapping is injection function. (3) If $A \subseteq B$ the inclusion mapping is not surjective function.

4.9.4 Characteristic Mapping

Definition 4.13 Let $B \subseteq A$, $C = \{0, 1\}$, and $f : A \to C$ be mapping defined as
$f(x) = \begin{cases} 0; \forall x \in B \\ 1; \forall x \in A - B \end{cases}$. The function $f : A \to C$ is called the characteristic mapping to B in A (Mustafa et al., 1980).

4.9.5 Restriction of Mapping

Definition 4.14 Let $f : A \to B$ be a mapping, and $C \subseteq A$. The mapping $g : C \to B$, defined as $g(x) = f(x), \forall x \in C$ is called restriction mapping f on C denoted by $g = f/C = (f/C, C, B)$(Borgers, 1960; Halmos, 2017b; Munkres, 2000; Adams and Franzosa, 2008).

Example 4.21 Let $(f, \mathbb{Z}, \mathbb{Z})$ where $f = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | f(x) = x^2\}$. And let $(g, \mathbb{N}, \mathbb{Z})$ where $g = \{(x, y) \in \mathbb{N} \times \mathbb{Z} | g(x) = x^2\}$. Since $\mathbb{N} \subseteq \mathbb{Z}$ and $f(x) = g(x), \forall x \in \mathbb{N}$, hence $G : \mathbb{N} \to \mathbb{Z}$ is restriction mapping f on $\mathbb{N}$.

4.9.6 Extension of Mapping

Definition 4.15 Let $f : A \to B$ be a mapping, and $A \subseteq D$. The mapping $g : D \to B$ defined as $g(x) = f(x), \forall x \in A$ is called extension mapping g on A denoted by $g/A = f = (g/D, D, B)$(Halmos, 2017b; Adams and Franzosa, 2008; Mendelson, 2009b; Warner, 1965; Dean, 1967; Kelley, 2017).

Example 4.22 In the example 4.21, f is the extension mapping in g.

4.9.7 Numerical Mapping

Definition 4.16 The mapping $f : A \to B$ is a numerical mapping if B is numerical set. Or, if the codomain of the mapping is numerical set (Mustafa et al., 1980).

4.9.8 Absolute Value Function

Definition 4.17 Let $f : \mathbb{R} \to \mathbb{R}$ be a mapping and defined as $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} | y = |x|\}$. Or, $y = |x| = \begin{cases} x; \forall x \geq 0 \\ -x; \forall x < 0 \end{cases}$. The function $f : \mathbb{R} \to \mathbb{R}$ is called absolute value function(Hass et al., 2019; Stewart, 2009).

4.9.9 Sequence

Definition 4.18 Let A ba any arbitrary set. The mapping $f : \mathbb{N} \to A$ is called sequences in A, and denoted by $\{f_n\}$. Or, $f_1, f_2, f_3, ..., f_n; n \in \mathbb{N}$, where $f_n = f(n); n \in \mathbb{N}$(Ramsey, 1926; Gaughan, 2009b; Wilder et al., 2012).

Note: If $A = \mathbb{R}$ then, the sequence is called sequence of real numbers. And if $A = \mathbb{C}$, then the sequence is called sequence of complex numbers.

Example 4.23 Each of $\{(-1)^n\}, \left\{\frac{-n}{3(2^n)}\right\}$ is sequence of real numbers.

4.9.10 Permutation

Definition 4.19 Let $\phi \neq A$. The bijection function $f : A \to A$ is called permutation (McCoy, 1968).

Example 4.24 (1) Let $A = \{a, b, c\}$, and the mapping $f : A \to A$ defined on Aas: $f(a) = b, f(b) = c, f(c) = a$. Since $f : A \to A$ is bijection, hence it is permutation on A. (2) Consider $A = \{1, 2, 3\}$, and the mapping $f : A \to A$ defined on Aas: $f(1) = 2, f(2) = 3, f(3) = 1$. Since $f : A \to A$ is bijection, hence $f : A \to A$ is permutation on A.

4.9.11 Canonical Mapping

Definition 4.20 Let A be any arbitrary set, and R be an equivalence relation on A. The mapping $f : A \to A/R$ denoted by $f(x) = [x]$ is called canonical mapping (Mustafa et al., 1980; Wilder et al., 2012).

Example 4.25 Let $A = \mathbb{Z}$, and let R be a relation defined on $\mathbb{Z}$ as follows: $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | (y - x) \text{ is even number}\}$.

Obviously, R is equivalence relation on $\mathbb{Z}$, and $\mathbb{Z}/R = \{[0], [1]\}$. The mapping $f : \mathbb{Z} \to \mathbb{Z}/R$ which defined $f(n) = \{[n]\}$ is a canonical mapping. And $f(2) = [0] = [2]$, $f(5) = [1] = [5]$. It is noted that $f : \mathbb{Z} \to \mathbb{Z}/R$ is surjective but not injective.

4.9.12 Mapping of Several Variables

Definition 4.21 A real valued function of n real variables is a function that takes as input n real numbers, commonly represented by the variables $x_1, x_2, ..., x_n$, for producing another real number, the value of the function, commonly denoted $f(x_1, x_2, ..., x_n)$. Or, $f : A_1 \times ... \times A_n \to A$, where $f = \{(x_1, y_1), ..., (x_n, y_n) \in A_1 \times A, ..., A_n \times A | y = f(x_1, x_2, ..., x_n)\}$ (Moskowitz and Paliogiannis, 2011; Fleming, 2012).

Example 4.26 (1) Let $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ be a mapping defined as: $f(x, y) = \frac{3}{4}\pi x^3 \sqrt{y}, \forall (x, y) \in \mathbb{R} \times \mathbb{R}$. f is a function of two variables, its domain is $\mathbb{R} \times \mathbb{R}$. (2) $f : \mathbb{R}^4 \to \mathbb{R}^2$, where $f(x_1, x_2, x_3, x_4) = (3x_1 +$

$x_2, 4x_3 + 5x_4)$ is a mapping in four variables its domain and codomain is $\mathbb{R}^4, \mathbb{R}^2$ respectively.

4.9.13 Distance Mapping

Definition 4.22 Let A be an arbitrary set, and $\mathbb{R}^* = \{x \in \mathbb{R} | x \geq 0\}$. The mapping $d : A \times A \to \mathbb{R}^*$ is called distance mapping if and only if provides the following conditions $\forall a, b, c \in A$ then; (1) $a = b \leftrightarrow d(a, b) = 0$. (2) $d(a, b) = d(b, a)$. (3) $d(a, b) \leq d(a, c) + d(c, b)$, where d is a metric on A(Grossman, 1994; Anton and Rorres, 1994).

Note: If $d : A \times A \to \mathbb{R}^*$ is a distance mapping on $\mathbb{R}$, then $d(a, b) = |a - b|$ is a distance function.

Example 4.27 Let A be any set, and $d : A \times A \to \mathbb{R}^*$ be a relation defined as follows $d(a, b) = \begin{cases} 1; \forall a \neq b \\ 0; \forall a = b \end{cases}$. Then, $d : A \times A \to \mathbb{R}^*$ is a distance mapping on A.

4.9.14 Projections

Definition 4.23 Let each of A_1, A_2 be a set. The mapping $P_i : A_1 \times A_2 \to A_i; i = 1, 2$ denoted by $P_i(a_1, a_2) = a_i; i = 1, 2$. It is called the projection of the $A_1 \times A_2$ on $A_i; i = 1, 2$ (Halmos, 2017b; Mustafa et al., 1980).

Note:

(i) If $i = 1$ The projection will be $P_i : A_1 \times A_2 \to A_1$ such that $P_1(a_1, a_2) = a_1$.

(ii) If $i = 2$ The projection will be $P_i : A_1 \times A_2 \to A_2$ such that $P_1(a_1, a_2) = a_2$.

(iii) The application of mapping $P_i : A_1 \times A_2 \to A_i; i = 1, 2$ is surjective but not injective.

(iv) The generation of Definition 4.22 can be as follows: Let $A_1, A_2, ..., A_n$ be sets, and the mapping $P_i : A_1 \times A_2 \times ... \times A_n \to$

$A_i; i = 1, 2, ..., n$, such that $P_i(a_1, a_2, ..., a_n) = a_i; i = 1, 2, ..., n$. It is called the projection of the $A_1 \times A_2 \times ... \times A_n$ on $A_i; i = 1, 2, ..., n$.

Example 4.28 $P_i : \mathbb{R}^3 \to \mathbb{R}$, such that $P_i(x_1, x_2, x_3) = x_i; i = 1, 2, 3$. It is the projection of the $\mathbb{R}^3$ on $\mathbb{R}$.

Theorem 4.3 *Let each of $f_1 : B \to A, f_2 : C \to A$ be a mapping, provided that $B \cap C \neq \phi$. If $f = f_1 \cup f_2$ then (1) $f : B \cup C \to A$ is a mapping. (2) $f_1 = f/B, f_2 = f/C$.*

Proof To prove this theorem, we have to prove the following two mathematical relations: (3) $(x, y) \in f \wedge x \in B \leftrightarrow (x, y) \in f_1$. (4) $(x, y) \in f \wedge x \in C \leftrightarrow (x, y) \in f_2$.

Proof (3) Suppose that $(x, y) \in f \wedge x \in$

$\therefore (x, y \in f) \to (x, y) \in f_1 \vee (x, y) \in f_2$

If, $(x, y) \in f_2 \to x \in C$.

As, $x \in B \wedge x \in C \to x \in B \cap C$. Or, $B \cap C \neq \phi$, and this is contradiction because $B \cap C = \phi$.

Thus, $(x, y) \notin f_2 \to (x, y) \in f_1$.

Conversely, suppose that $(x, y) \in f_1$, and since $f_1 : B \to C$ is a mapping.

$\therefore x \in B$.

Since $f = f_1 \cup f_2 \therefore (x, y) \in f$. Or, $(x, y) \in f_1 \to (x, y) \in f \wedge x \in B$.

Proof (4) In the same method of proof (3), we can prove (4).

Now, we come back to prove the theorem.

(1) Suppose that $x \in B \cup C$.

$x \in B \cup C \to x \in B \vee x \in C$.

Suppose that $x \in B$, As, $f_1 : B \to C$ is mapping, $\exists y \in A \ni (x, y) \in f_1$.

As $f_1 \subseteq f$, $\therefore (x, y) \in f$. Or, $\exists y \in A \ni (x, y) \in f ...(1)$.

Now, suppose that $x \in C$. As, $f_2 : C \to A$ is mapping, $\exists w \in A \ni (x, w) \in f_2$.

As $f_2 \subseteq f$, $\therefore (x, y) \in f$. Or, $\exists w \in A \ni (x, w) \in f ...(2)$.

From (1)&(2), we conclude that $\forall x \in B \cup C, \exists z \in A \ni (x, z) \in f$, where z represents y, w in $(1), (2)$ respectively.

Now, we are going to prove that f is a functional relation.

Suppose that $(x, y_1) \in f \wedge (x, y_2) \in f$.
From definition of the mapping, $x \in B \cup C \to x \in B \vee x \in C$.
Let us assume that $x \in B$.
From (3), we have,
$(x, y_1) \in f \wedge x \in B \to (x, y_1) \in f_1$.
So as $(x, y_2) \in f \wedge x \in B \to (x, y_2) \in f_1$.
As $f_1 : B \to A$ is a mapping, $\therefore y_1 = y_2$.
let us assume that $x \in C$.
Also, from (4), we have,
$(x, y_1) \in f \wedge x \in C \to (x, y_1) \in_2 f$.
So as $(x, y_2) \in f \wedge x \in B \to (x, y_2) \in f_2$.
As $f_2 : C \to A$ is a mapping, $\therefore y_1 = y_2$.
So, in any case we get that $y_1 = y_2$.
Thus, $f : B \cup C \to A$ is a mapping.
Through the similar method we can prove (2). ♦

4.10 Exercises

Solve the following questions:

Q1: Let $f : [1, \infty) \to \mathbb{R}$ be a mapping defined as:
(1) $f(x) = \sqrt{4x - 1}$. Find range of the mapping.
(2) $f(x) = (4x - 1)^{(\frac{1}{3})}$.
Find domain, codomain, and range of the domain.

Q2: Draw the graph of the following relationships:
(1) $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} | 3x - y = 4\}$.
(2) $g = \{(x, y) \in \mathbb{R} \times \mathbb{R} | y = x^2 - 4\}$.
(3) $h = \left\{ (x, y) \in \mathbb{R} \times \mathbb{R} | y = \left\{ \begin{array}{c} 2x; x \in (-2, 4) \\ \frac{3x+1}{2}; x \in (-4, -2) \end{array} \right\} \right.$.

Q3: Discuss the following statements:
(1) The value of the sphere is a function for its radius.
(2) Radius of the sphere is a function of its value.
(3) The value of the gas is a function of the pressure.

Q4: If $f(n)$ represents the prime numbers which is less than or equal the positive integer number n. Find $f(5), f(79)$.

Q5: Let $f : A \to B$ be an injective function, and let $C \subseteq A$. Prove that $f/C : C \to B$ is an injective function.

Q6: Let each of $f : A \to B, g : C \to D$ be a function. Multiplication of f, g is defined as $(f \times g)(x, y) = (f(x), g(y)); \forall (x, y) \in A \times C$. Prove that:

(1) $f \times g : A \times C \to B \times D$ is a mapping.

(2) If each of f, g is injective then $f \times g$ is injective.

(3) If each of f, g is surjective then $f \times g$ is surjective.

Q7: Let each of $f : A \to B, g : A \to B$ is a mapping. Prove that if $f \subseteq g$ then $f = g$.

Q8: Let $G : A \to B$ be a relation. Prove that G is a graph of the mapping $f : A \to B$ if and only if there exist relations;

$H : A \to B, J : A \to B$, such that $(H \cap J) \bullet G = (H \bullet G) \cap (J \bullet G)$.

4.11 Composite Mapping and Inverse

4.11.1 Composite mappings

Definition 4.24 Let $f : A \to B, g : B \to C$ be functions then the function $h : g \circ f : A \to C$ is a composition function(Velleman, 2006; Wilder et al., 2012).

Note: $g \circ f : A \to C$ defined by $g(f(x)) \forall x \in A$. The notation $g \circ f$ is read as “g circle f”, “g round f”, “ g composed with f”, “g after f”, “g following f”, “g of f”, “g on f”. Intuitively, composing two functions is a chaining process in which the output of the inner function becomes the input of the outer function.

Theorem 4.4 *If $f : A \to B$, and $g : B \to C$ be a mapping, then $g \circ f : A \to C$ is a mapping.*

Proof (1) Suppose that $x \in A$.

$\because f : A \to B$ is a mapping,

$\therefore \exists y \in b \ni (x, y) \in f$

$\because g : B \to C$ is a mapping,

$\therefore \exists z \in C \ni (y, z) \in g$

Or, $y \in B \ni (x, y) \in f \wedge (y, z) \in g$

From the definition of the composite mapping, $(x, z) \in g \circ f$,

Thus, $\forall x \in A, \exists z \in C \ni (x, z) \in g \circ f$.

(2) Suppose that $(x, z_1) \in g \circ f \wedge (x, z_2) \in g \circ f$
From the definition of the composite function, we have:
$(x, z_1) \in g \circ f \to \exists y_1 \in B \ni (x, y_1) \in f \wedge (y_1, z_1) \in g$
$(x, z_2) \in g \circ f \to \exists y_2 \in B \ni (x, y_2) \in f \wedge (y_2, z_2) \in g$
$\because f : A \to B,$
$\therefore (x, y_1) \in f \wedge (x, y_2) \in f \to y_1 = y_2.$
$\because g : B \to C,$
$\therefore (y_1, z_1) \in g \wedge (y_1, z_2) \in g \to z_1 = z_2.$
Thus, we find that:
$(x, z_1) \in g \circ f \wedge (x, z_2) \in g \circ f \to z_1 = z_2.$
From (1)&(2), we conclude that, $g \circ f : A \to C$ is a function.
Figure 4.4 illustrates $g \circ f$ of the theorem. ♦

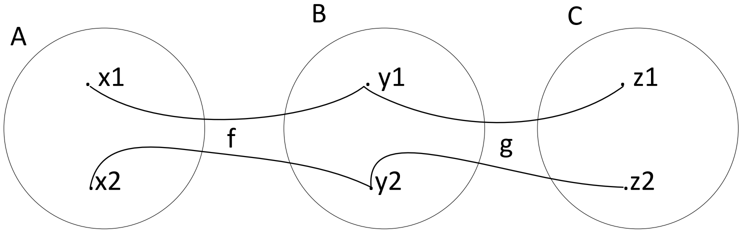


Figure 4.4: $g \circ f$

Corollary *If $f : A \to B$, and $g : B \to C$ be a mapping, then $\forall x \in A, (g \circ f)(x) = g(f(x))$.*

Proof Let $z = (g \circ f)(x)$.
$\because z = (g \circ f)(x) \to (x, z) \in g \circ f.$
From the definition of composite functions,
$\exists y \in B \ni (x, y) \in f \wedge (y, z) \in g.$
On the other hand, $(x, y) \in f \leftrightarrow y = f(x), (y, z) \in f \leftrightarrow z = g(y).$
$\therefore z = g(y) = g(f(x))$. Thus, $(g \circ f)(x) = g(f(x))$. ♦

Example 4.29 Consider $f = \left\{(x,y) \in \mathbb{C} \times \mathbb{C} | y = \sqrt{3x^2} + 1\right\}$, and $g = \{(x,y) \in \mathbb{C} \times \mathbb{C} | y = 3x^2 + 2x + 1\}$.

(1) $(g \circ f)(x) = g(f(x)) = g(\sqrt{3x^2} + 1) = 3(\sqrt{3x^2} + 1)^2 + 2(\sqrt{3x^2} + 1) + 5 = 9x^2 + 8(\sqrt{3x^2} + 1) = 9x^2 + 8(\sqrt{3}\,|x| + 1)$.

(2) $(f \circ g)(x) = f(g(x)) = f(3x^2 + 2x + 1) = \sqrt{3(3x^2 + 2x + 1)^2} + 1 = \sqrt{3}\,|3x^2 + 2x + 1| + 1$.

Note: Let each of f, g be a function, then $g \circ f \neq f \circ g, \forall f, g$.

Theorem 4.5 *Let each of $f : A \to B, g : B \to C$ be a mapping.*

(i) *If each of f, g is injection mapping, then $g \circ f$ is injection mapping too.*

(ii) *If each of f, g is surjection mapping, then $g \circ f$ is surjection mapping too.*

(iii) *If each of f, g is bijective mapping, then $g \circ f$ is bijection mapping too.*

Proof (i) Suppose that $x_1, x_2 \in A \ni (g \circ f)(x_1) = (g \circ f)(x_2)$.

$\because (g \circ f)(x_1) = (g \circ f)(x_2) \to g(f(x_1)) = g(f(x_1))$, [From the definition of composite functions].

As g is injection, $\therefore g(f(x_1)) = g(f(x_1)) \to f(x_1) = f(x_2)$

As f is injection, $\therefore f(x_1) = f(x_1) \to x_1 = x_2$.

$\therefore g \circ f$ is injective.

(ii) Suppose that $z \in C$.

Now, $z \in C$,

$\because g$ is surjective function $\exists y \in B \ni g(y) = z$, as f is surjective function $\exists x \in A \ni f(x) = y$.

Or, $\exists x \in A \ni z = g(y) = g(f(x)) = (g \circ f)(x)$.

Thus, $(g \circ f)(x)$ is surjective function.

(iii) Based on (1)& (2), $(g \circ f)(x)$ is bijective function. ♦

Theorem 4.6 *Let each of $f : A \to B, g : B \to C$ be a mapping.*

(i) *If the mapping $g \circ f$ is injective then f is injective.*

(ii) *If the mapping $g \circ f$ is surjective then g is surjective.*

Proof (i) Suppose that $x_1, x_2 \in A \ni f(x_1) = f(x_2)$

$\because f(x_1) = f(x_2) \to g(f(x_1)) = g(f(x_2))$

From the definition of the composite mapping we have $(g \circ f)(x_1) = (g \circ f)(x_2)$

As $g \circ f$ is injective $\to x_1 = x_2$

Thus f is injective.

(ii) Suppose that $z \in C$,

Now, $z \in C$, as $g \circ f$ is surjective,

$\therefore \exists x \in A \ni (g \circ f)(x) = z$.

Or $\exists x \in A \ni g(f(x)) = z$.

As $f(x) \in B$,

$\therefore g$ is surjective. ♦

Corollary *Let each of $f : A \to B, g : B \to C$ be a mapping. If the mapping $g \circ f$ is bijective, then f is injective, and g is surjective.*

Proof $\because g \circ f$ is bijective $\to g \circ f$ is injective and surjective [From the definition of bijective function].

As $g \circ f$ is injective $\to f$ is injective [From Theorem 4.6 (i)].

As $g \circ f$ is surjective $\to g$ is surjective [From Theorem 4.6 (ii)]. ♦

Note: The opposite of the corollary is not necessary would be always true. Or if f is injective function, and g is surjective function, then $g \circ f$ is bijective mapping. The following example illustrates that clam.

Example 4.30 Consider $f : \mathbb{R} \to \mathbb{R} | f(x) = x$, and $: \mathbb{R} \to \mathbb{R}^+ | g(x) = x^2$.

The mapping $g \circ f : \mathbb{R} \to \mathbb{R}^+ | (g \circ f)(x) = x^2$.

It is crucial to note that f is injective, and g is surjective while the mapping $g \circ f$ is not injective. If we take $x_1 = -5 \neq 5 = x_2 \to (g \circ f)(-5) = (g \circ f)(5) = 25$. Thus, the mapping $g \circ f$ is not injective.

4.11.2 Inverse Mapping

If $f : A \to B$ be a mapping. The inverse relation $f^{-1} : B \to A$ may be verified the requirements of mapping or not verified. On the other hand, if $f^{-1} : B \to A$ be a mapping, it is not necessary the relation $f : A \to B$ be a mapping.

Definition 4.25 Let $f : A \to B$ be a function. Then f is invertible if there exists a function $g = f^{-1} : B \to A$, with the property $f(x) = y \Leftrightarrow g(y) = f^{-1}(y) = x$, and $f^{-1} : B \to A$ is called inverse mapping(Scheinerman, 2000; Scheinerman, 2012; Thomas et al., 2010).

Example 4.31 Let $A = \{1, 3, 5\}, B = \{a, b\}$.

The $f = \{(1, a), (3, a), (5, b)\}$, $f^{-1} = \{(a, 1), (a, 3), (b, 5)\}$. It is clear that $f : A \to B$ is a mapping, while $f^{-1} : B \to A$ is not a mapping.

Example 4.32 Let $A = \{x, y\}, B = \{a, b, c, d\}$.

The $f = \{(x, a), (x, b), (x, c), (y, d)\}$,

$f^{-1} = \{(a, x), (b, x), (c, x), (d, y)\}$.

It is clear that $f : A \to B$ is not a mapping, while $f^{-1} : B \to A$ is a mapping.

Example 4.33 (1) Let $f : \mathbb{R} \to \mathbb{R}|y = x^3$, $\therefore f^{-1} : \mathbb{R} \to \mathbb{R}|x = y^3$.

Since $f^{-1} : \mathbb{R} \to \mathbb{R}|x = y^3$ is a mapping hence $f : \mathbb{R} \to \mathbb{R}|y = x^3$ is invertible.

(2) Let $h : \mathbb{R} \to \mathbb{R}|y = x^4$, $\therefore h^{-1} : \mathbb{R} \to \mathbb{R}|x = y^4$.

Since $f^{-1} : \mathbb{R} \to \mathbb{R}|x = y^4$ is not a mapping, hence $f : \mathbb{R} \to \mathbb{R}|y = x^4$ is not invertible.

Because if we take $y_1 = \frac{-1}{2}, y_2 = \frac{1}{2} \to x = \frac{1}{16}$.

Thus, $(\frac{1}{16}, \frac{-1}{2}) \in h^{-1} \wedge (\frac{1}{16}, \frac{1}{2}) \in h^{-1}$, but $\frac{-1}{2} \neq \frac{1}{2}$.

The necessary and sufficient conditions meet in the following theorem in order for the mapping to be invertible.

Theorem 4.7 *The function $f : A \to B$ is invertible if and only if it bijective.*

Proof Suppose that $f : A \to B$ is invertible. We have to prove that the function is bijective. Or, we have to prove that f is injective and surjective.

Let each of $x_1, x_2 \in A \ni f(x_1) = f(x_2)$.

Let $f(x_1) = f(x_2) = y \to (x_1, y) \in f \wedge (x_2, y) \in f$.

From the definition of the inverse relation,

$(y, x_1) \in f^{-1} \wedge (y, x_2) \in f^{-1}$.

$\because f^{-1}$ is a functional relation,

$\therefore (x_1, y) \in f \wedge (x_2, y) \in f \rightarrow x_1 = x_2$.

$\therefore f : A \rightarrow B$ is bijective function ...(1).

Now, we have to prove that $f : A \rightarrow B$ is surjective function.

Let $y \in B$, $\because f^{-1} : B \rightarrow A$ is a mapping,

$\therefore \exists x \in A \ni (y, x) \in f^{-1}$.

Or, $\exists x \in A \ni (x, y) \in f \rightarrow \exists x \in A \ni y = f(x)$ ...(2).

Thus, from (1)& (2), $f : A \rightarrow B$ is bijective.

Conversely, suppose that $f : A \rightarrow B$ is bijective.

We have to prove the mapping $f : A \rightarrow B$ is invertible.

Or, it ought to be proved that $f^{-1} : B \rightarrow A$ is a mapping.

Suppose that $y \in B$. As, $f : A \rightarrow B$ is surjective,

$\therefore \exists x \in A \ni f(x) = y \rightarrow \exists x \in A \ni (x, y) \in f$.

But $(x, y) \in f \rightarrow (y, x) \in f^{-1}$.

Thus, $\exists x \in A \ni (y, x) \in f^{-1}$.

Or, $domf^{-1} = B$ ...(3).

In order to prove $f^{-1} : B \rightarrow A$ is a functional relation, suppose that $(y, x_1) \in f^{-1} \wedge (y, x_2) \in f^{-1}$.

$\therefore (x_1, y) \in f \wedge (x_2, y) \in f$.

Or, $f(x_1) = y \wedge f(x_2) = y \rightarrow f(x_1) = f(x_2)$.

As $f : A \rightarrow B$ is injective, $\therefore x_1 = x_2$.

Or, $(y, x_1) \in f^{-1} \wedge (y, x_2) \in f^{-1} \rightarrow x_1 = x_2$.

$\therefore f^{-1}$ is functional relation ...(4).

From (3)& (4) $f^{-1} : B \rightarrow A$ is a mapping. ♦

Theorem 4.8 *If the mapping $f : A \rightarrow B$ is invertible, then $f^{-1} : B \rightarrow A$ is a bijective.*

Proof Let $f : A \rightarrow B$ be an invertible mapping.

From the definition, the relation $f^{-1} : B \rightarrow A$ is a mapping.

Now, we have to prove $f^{-1} : B \rightarrow A$ is a bijective.

Let each of $y_1, y_2 \in B \ni f^{-1}(y_1) = f^{-1}(y_2)$.

Suppose that $f^{-1}(y_1) = f^{-1}(y_2) = x$,

$\therefore (y_1, x) \in f^{-1} \wedge (y_2, x) \in f^{-1}$.

From the definition of the inverse relation, we conclude that:

$(x, y_1) \in f \wedge (x, y_2) \in f$

Or, $y_1 = f(x) \wedge y_2 = f(x) \to y_1 = y_2$
$\therefore f^{-1} : B \to A$ is injective (1).
Suppose that $x \in A$
As $f : A \to B$ is a mapping, $\exists y \in B \ni (x, y) \in f$
From definition of the inverse mapping $(y, x) \in f^{-1}$.
Or, $\exists y \in B \ni (y, x) \in f^{-1} \to \exists y \in B \ni f^{-1}(y) = x$
$\therefore f^{-1} : B \to A$ is surjective (2).
From (1)& (2) $f^{-1} : B \to A$ is bijective. ♦

Theorem 4.9 *If $f : A \to B$ is invertible mapping then:*

(i) $f^{-1} \circ f = I_A$.

(ii) $f \circ f^{-1} = I_B$.

Proof (i) As $f : A \to B$ is invertible mapping,
$\therefore f^{-1} : B \to A$ is a mapping.
The $f^{-1} \circ f : A \to A$ will be a mapping.
Let $x \in A \ni y = f(x) \to (f^{-1} \circ f)(x) = f^{-1}(f(x))$.
$\therefore (f^{-1} \circ f)(x) = f^{-1}(y) = x$.
As $I_A : A \to A$ is a mapping,
$\therefore I_A(x) = x$.
Or, $\forall x \in A, (f^{-1} \circ f)(x) = I_A(x)$
$\therefore f^{-1} \circ f = I_A$ (Theorem 4.2).
(ii) In the same way, we can prove that $f \circ f^{-1} = I_B$. ♦

4.12 Exercises

Solve the following questions:

Q1: Let each of $f : X \to Y, g : Y \to X$ be a mapping, and let $g \circ f = I_X$. Prove that $f : X \to Y$ is an injection mapping, then $g : Y \to X$ will be surjective.

Q2: Let each of $f : X \to Y, g : Y \to X$ be a mapping, and let $g \circ f = I_X, f \circ g = I_Y$. Prove that each of (1) f, g is a bijective. (2) $g = f^{-1}$.

Q3: Let $f : A \to B$ be a mapping, and let $C \subseteq A$. Prove that $f/C = f \circ E_C$, where $E_C : C \to A$ is the inclusion mapping.

Q4: Let each of $f : A \to B, g : B \to C, h : B \to C$ be a mapping. Suppose that $g \circ f = h \circ f$. Prove that $g = h$.

Q5: Let $f : A \to B$. Prove that $f : A \to B$ injective if and only if there exists a mapping $g : B \to$ such that $g \circ f = I_A$.

Q6: Prove that the mapping $f : A \to B$ invertible if and only if there exists a mapping $g : B \to A$, such that $f \circ g = I_A, g \circ f = I_B$.

4.13 Direct Images and Inverse Images Under Mapping

4.13.1 Direct Images Under Mapping

Definition 4.26 Let $f : A \to B$ be a mapping, and $C \subseteq A$. The set of all elements in B, in which every element in it, is the image of at least one element of A, it called direct image of C under $f : A \to B$, and denoted by $f(C)$. In other words, $f(C) = \{y \in B | \exists x \in C \ni y = f(x)\}$ (Pinter, 1976; Pinter, 2014).

Example 4.34 (1) Let $f : \mathbb{Z}_o \to \mathbb{Q}^+$, such that $\forall x \in \mathbb{Z}_o, f(x) = \frac{x^2}{2} + 3$, and let $C = \{-5, -3, -1, 1, 3, 5\}$, then $f(C) = \left\{\frac{31}{2}, \frac{15}{2}, \frac{7}{2}\right\}$.

(2) Let $f : \mathbb{R} \to \mathbb{R}$, such that $\forall x \in \mathbb{R}, f(x) = \sqrt{1 - x^2}$, and let that $C = [-1, 1]$, then $f(C) = [0, 1]$.

(3) Let $f : \mathbb{R} \to \mathbb{R}$, such that $\forall x \in \mathbb{R}, f(x) = \sqrt{4 - x}$, and let that $C = [-\infty, 4]$, then $f(C) = [0, \infty)$.

(4) Let $f : \mathbb{R} - \{0\} \to \mathbb{R}$, such that $\forall x \in \mathbb{R} - \{0\}, f(x) = \frac{1}{x}$, and let $C = (0, 1]$, then $f(C) = [1, \infty) = \{y \in B | 1 \leq y < \infty\}$.

Theorem 4.10 *Let $f : X \to Y$ be a mapping, and $A, B \in X$. If $A = B$, then $f(A) = f(B)$.*

Proof Suppose that $A = B$, and $y \in f(A)$.

From the definition of the direct images, we have, $\exists x \in A \ni y = f(x)$.

$\because A = B, \therefore x \in B \to f(x) \in f(B)$.

$\therefore y \in f(B)$.

Thus, $y \in f(A) \to y \in f(B)$.

Thus, $f(A) \subseteq f(B)$ (1).

In the same way, $f(B) \subseteq f(A)$ (2).

From, (1)& (2), we conclude that $f(A) = f(B)$. ♦

Note: If $f(A) = f(B)$, it is not necessary that $A = B$, as shown below:

Consider $f : \mathbb{Z} \to \mathbb{Z}^+$ be a mapping, such that $y = f(x) = x^2$. And let $A = \{1, 0, 2\}, B = \{-1, 0, -2\}$.

$f(A) = \{1, 0, 4\}, f(B) = \{1, 0, 4\}$. Note that $f(A) = f(B)$, but $A \neq B$.

Theorem 4.11 *Let, each of X, Y be a set, and $f : X \to Y$ be a mapping, and $f^* : P(X) \to P(Y)$ be a relation denoted as $f^* = \{(A, B) \in P(A) \times P(B|f(A) = B\}$, then $f^* : P(X) \to P(Y)$ is a mapping.*

Proof Suppose that $A \in P(X)$

Now, $A \in P(X) \to A \subseteq X$.

From definition of the direct images $f(A) \subseteq Y$

$\therefore f(A) \in P(Y)$.

Let $f(A) = B$

$\therefore \forall A \in P(X), \exists B \in P(Y) \ni (A, B) \in f^*$ (1).

Suppose that $(A, B_1) \in f^* \wedge (A, B_2) \in f^*$

$\to B_1 = f(A) \wedge B_2 = f(A)$

From Theorem 4.10 $f(A)$ should be a unique image, or, $\forall A; A \subseteq X$ the $f(A)$ is a unique set.

Thus, $B_1 = B_2$ (2).

From (1)& (2), $f^* : P(X) \to P(Y)$ is a mapping. ♦

Theorem 4.12 *If $f : A \to B$ is a mapping, and each of $C, D \subseteq A$, then:*

(i) $f(C \cup D) = f(C) \cup f(D)$.

(ii) $f(C \cap D) \subseteq f(C) \cap f(D)$.

(iii) $f(C - D) \supseteq f(C) - f(D)$.

Proof (i) Suppose that $y \in f(C \cup D)$.

Now, $y \in f(C \cup D) \rightarrow \exists x \in C \cup D \ni y = f(x)$
$\rightarrow \exists x \in C \vee \exists x \in D \ni y = f(x)$
$\rightarrow (\exists x \in C \ni y = f(x)) \vee (\exists x \in D \ni y = f(x))$
$\rightarrow f(x) \in f(C) \vee f(x) \in f(D)$
$\rightarrow y \in f(C) \vee y \in f(D)$
$\rightarrow y \in f(C) \cup f(D)$
$\rightarrow y \in (f(C) \cup f(D))$
$\therefore f(C \cup D) \subseteq f(C) \cup f(D)$ (1).

Conversely, suppose that $y \in f(C) \cup f(D)$
Now, $y \in f(C) \cup f(D) \rightarrow y \in f(C) \vee y \in f(D)$
$\rightarrow (\exists x_1 \in C \ni y = f(x_1)) \vee (\exists x_2 \in C \ni y = f(x_2))$
$\rightarrow (\exists x_1 \in C \cup D \ni y = f(x_1)) \vee (\exists x_2 \in C \cup D \ni y = f(x_2))$
$\rightarrow y \in f(C \cup D)$
$\therefore f(C) \cup f(D) \subseteq f(C \cup D)$ (2).

Thus, from (1)& (2), we conclude that $f(C \cup D) = f(C) \cup f(D)$.

(ii) Is leftas an exercise to the reader.

(iii) Suppose that $y \in f(C) - f(D)$.
Now, $y \in f(C) - f(D) \rightarrow y \in f(C) \wedge f \notin f(D)$
As $y \in f(C)$, $\therefore \exists x \in C \ni y = f(x)$.
As $y \notin f(D)$, $\therefore f(x) \notin f(D) \rightarrow x \notin D$.
Or, $\exists x \in C \wedge x \notin D \ni y = f(x)$
In other words $\exists x \in C - D \ni y = f(x)$
$\therefore y \in f(C - D)$
Or, $y \in f(C) - f(D) \rightarrow y \in f(C - D)$
$\therefore f(C) - f(D) \subseteq f(C - D)$. ♦

Example 4.35 This example illustrates the second part of Theorem 4.12. Or, $f(C) \cap f(D) \nsubseteq f(C \cap D)$.

Let $A = \{1, 3\}, B = \{0\}$ and $f : A \rightarrow B$ be a constant mapping.

Suppose that $C = \{1\}, D = \{3\}$. The $f(C \cap D) = f(\phi) = \phi$. On the other hand $f(C) = f(\{1\}) = 0$, and $f(D) = f(\{3\}) = 0 \rightarrow f(C) \cap f(D) = \{0\}$.

Thus, $f(C) \cap f(D) \neq f(C \cap D) \equiv f(C) \cap f(D) \subseteq f(C \cap D) \wedge f(C \cap D) \subseteq f(C) \cap f(D)$

$\therefore f(C) \cap f(D) \subseteq f(C \cap D)$.

4.13.2 Inverse Images Under Mapping

Definition 4.27 Let $f : A \to B$ be a mapping, and $D \subseteq B$. The set of all elements in A in which every element in it is the image of D, it called the inverse image of D under $f : A \to B$, and denoted by $f^{-1}(D)$. In other words $f^{-1}(D) = \{x \in A | f(x) \in D\}$ (Pinter, 1976; Pinter, 2014).

Note: If $f : A \to B$ is a mapping, $D \subseteq B$, and $\exists! b \in D$, or $D = \{b\}$, then $f^{-1}(b)$ can be used instead of $f^{-1}(\{b\})$ for convenient.

Example 4.36 Let $f : \mathbb{C} \to \mathbb{C}$, such that $f(x) = x^2 - 1, \forall x \in \mathbb{C}$.
(1) $f^{-1}(24) = \{x \in \mathbb{C} | f(x) = 24\} = \{x \in \mathbb{C} | x^2 - 1 = 24\}$
$= \{-5, 5\}$.
(2) $f^{-1}(\{5, 9\}) = \{x \in \mathbb{C} | f(x) \in \{5, 9\}\}$
$= \{x \in \mathbb{C} | x^2 - 1 = 5 \vee x^2 - 1 = 9\} = \left\{\mp\sqrt{6}, \mp\sqrt{10}\right\}$.

Theorem 4.13 *Let $f : X \to Y$, and $C, D \subseteq Y$. If $C = D$ then $f^{-1}(C) = f^{-1}(D)$.*

Proof Suppose that $C = D$, and $x \in f^{-1}(C)$.

From definition of the inverse images under mapping, $f(x) \in C$.

As, $C = D \to f(x) \in D$.

Again from definition of the inverse images under mapping, $x \in f^{-1}(D)$.

$\therefore x \in f^{-1}(C) \to x \in f^{-1}(D)$.

Or, $f^{-1}(C) \subseteq f^{-1}(D)$ ...(1).

In the same way, $f^{-1}(D) \subseteq f^{-1}(C)$ ...(2).

From (1)& (2), we conclude that $f^{-1}(C) = f^{-1}(D)$. ♦

Note: If $f^{-1}(C) = f^{-1}(D)$, it is not necessary $C = D$. Or, the vice versa of Theorem 4.13 is not true, as illustrated in the following example.

Example 4.37 Consider the mapping $f : \mathbb{R} \to \mathbb{R}$, such that $f(x) = |x|$. Let $C, D \subseteq \mathbb{R}$, where $C = (0, 1), D = (-1, 0)$.

Consequently $f^{-1}(0, 1) = (-1, 1) \wedge f^{-1}(-1, 0) = (-1, 1) \to f^{-1}(0, 1) = f^{-1}(-1, 0)$, but $(-1, 0) \neq (0, 1)$.

Theorem 4.14 *Let $f : X \to Y$ be a mapping. If the relation $f' : P(Y) \to P(X)$ denoted as $f' : \{(A, B) \in P(Y) \times P(X) | B = f(A)\}$, then $f' : P(Y) \to P(X)$ is a mapping.*

Proof The proof Is leftas an exercise to the reader. ⧫

Theorem 4.15 *If $f : A \to B$ be a mapping, and each of $C, D \subseteq B$, then:*

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

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

(iii) $f^{-1}(C - D) = f^{-1}(C) - f^{-1}(D)$.

Proof (i) Is leftas an exercise to the reader.

(ii) Suppose that $x \in f^{-1}(C \cap D)$.

Now, $x \in f^{-1}(C \cap D) \to f(x) \in C \cap D$ [From definition of the inverse images under mapping].

Again, now $f(x) \in C \cap D \to f(x) \in C \wedge f(x) \in D$
$\to x \in f^{-1}(C) \wedge x \in f^{-1}(D)$
$\to x \in f^{-1}(C) \cap f^{-1}(D)$
$\therefore f^{-1}(C \cap D) \subseteq f^{-1}(C) \cap f^{-1}(D)$ (1).
Similarly, suppose that $y \in f^{-1}(C) \cap f^{-1}(D)$.
Now, $y \in f^{-1}(C) \cap f^{-1}(D) \to y \in f^{-1}(C) \wedge y \in f^{-1}(D)$
$f(y) \in C \wedge f(y) \in D$
$f(y) \in C \cap D$
$y \in f^{-1}(C \cap D)$
$\therefore f^{-1}(C) \cap f^{-1}(D) \subseteq f^{-1}(C \cap D)$ (2).
From (1)& (2), we conclude that, $f^{-1}(C) \cap f^{-1}(D) = f^{-1}(C \cap D)$.
(iii) Is leftas an exercise to the reader. ⧫

4.14 exercises

Solve the following questions:

Q1: Let $X = \{x_1, x_2, x_3, x_4\}, Y = \{y_1, y_2, y_3, y_4\}$, and let $f : X \to Y$ be a mapping defined as $f(x_1) = y_1, f(x_2) = y_2, f(x_3) = y_3, f(x_4) = y_4$.

(1) Find the images of the sets $\{x_1, x_2\}, \{x_2, x_3\}, \{x_3\}, \{x_3, x_4\}$.

(2) Find the inverse images of the sets $\{y_1\}, \{y_1, y_2\}, \{y_1, y_2, y_3\}$, $\{y_3\}$.

Q2: Find the inverse image for each of the following sets, analytically and geometrically:

(i) $A = \{x \in \mathbb{R}| - 1 < y < 1\}$; $f : x \to y \ni f(x) = \frac{x}{2} - 1$.

(ii) $B = \{t \in \mathbb{R}|0 < s < 2\}$; $g : t \to s \ni g(t) = 2t^2 - 1$.

(iii) $k : m \to n \ni k(m) = \begin{cases} (m-1); m \geq 2 \\ (2m+1); m < 2 \end{cases}$.

(iv) $\psi = \{1 < l < 3\}$.

Q3: Consider the mapping $f : x \to f(x) = x^2 - 6x + 9; x \in \mathbb{R}$.

(i) Find and sketch the direct images of the intervals $[0, 1), (0, 3), [2, 4)$.

(ii) Find and sketch the direct inverse images of the intervals $[0, 1), (1, 3), [-2, 0)$.

Q4: If $f : A \to B$ is a mapping, and let $C \subseteq A, D \subseteq B$, then prove that:

(i) $C \subseteq f^{-1}[f(C)]$.

(ii) $f[f^{-1}(D)] \subseteq D$.

(iii) $C = f^{-1}[f(C)]$, if f is injective.

(iv) $f[f^{-1}(D)] = D$, if f is surjective.

Q5: Let each of $f : A \to B, f' : P(A) \to P(B), f'' : P(B) \to P(A)$ be a mapping.

(i) If f is injective, then f' is injective.

(ii) If f is surjective, then f'' is surjective.

(iii) If f is bijective, then f' is a bijective.

4.15 Order Preserving Mappings and Isomorphism

4.15.1 Increasing Mapping

Definition 4.28 Let each of A, B be a partial ordered sets. The mapping $f : A \to B$ is called an increasing mapping, or a conservative mapping, if and only if $x \leq y \leftrightarrow f(x) \leq f(y), \forall x, y \in A$(Jeffreys et al., 1999).

Example 4.38 Let each of $A = \{a, b, c, d\}, B = \{x, y, z, w\}$ be a partial ordered sets, as illustrated in Figure 4.5. If $f : A \to B$ be a mapping, where $d < b < c < a$, $w < z < y < x$, and $f(d) = w, f(b) = z, f(c) = y, f(a) = x$. Obviously, f is conservative mapping, or increasing mapping.

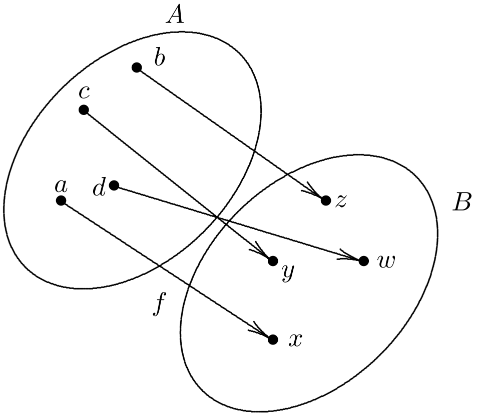


Figure 4.5: Graph of Increasing Mapping f

Example 4.39 Consider $\mathbb{Z}_o, \mathbb{Z}_e$ the set of odd integers, and even integers respectively. Let each of $\mathbb{Z}_o, \mathbb{Z}_e$ be a partial ordered set under the relation $\leq$. And, $f : \mathbb{Z}_o \to \mathbb{Z}_e$ be a mapping defind as $f(x) = x + 1, \forall x \in \mathbb{Z}_o$.

Clearly, $x \leq y \to x + 1 \leq y + 1, \forall x, y \in \mathbb{Z}_o$. $\therefore x \leq y \to f(x) \leq f(y), \forall x, y \in \mathbb{Z}_o$. Thus, $f : \mathbb{Z}_o \to \mathbb{Z}_e$ is a conservative mapping.

Example 4.40 Consider the partial ordered set $\mathbb{Z}_e$ under a relation $\leq$, defined as $x \leq y \leftrightarrow x \leq y$, and the partial ordered set $\mathbb{Z}_o$ under a relation $\leq$, defined as $x \leq y \leftrightarrow \frac{x}{y} \in \mathbb{Z}_o$. Let $f : \mathbb{Z}_e \to \mathbb{Z}_o$ where $f(x) = x + 3, \forall x \in \mathbb{Z}_e$.

It should be noted that f is not conservative mapping because if we take $2, 4$, then $f(2) = 5, f(4) = 7$. Thus, $2 \leq 4 \to \frac{5}{7} \notin \mathbb{Z}_o$.

4.15.2 Strictly Increasing Mapping

Definition 4.29 Let each of A, B be a partial ordered set. The mapping $f : A \to B$ is called strictly increasing mapping if and only if $x < y \to f(x) < f(y), \forall x, y \in A$(Jeffreys et al., 1999; Thomas et al., 2010; Varberg and Purcell, 1992).

Example 4.41 Let each of $A = \{a, b, c, d\}, B = \{x, y, z\}$ be partial ordered sets, as illustrated in Figure 4.6. If $f : A \to B$ be a mapping, where $b < c < d$, $b < c < a$, where a, d are not comparable, $z < y < x$, and $f(b) = z, f(c) = y, f(a) = f(d) = x$. Obviously, f is strictly increasing mapping.

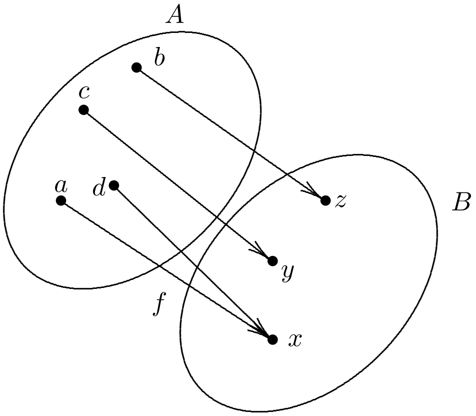


Figure 4.6: Graph of Strict Increasing Mapping f

Example 4.42 Consider each of $\mathbb{Z}^+, \mathbb{R}$ partial ordered sets by the relation $\leq$. Let $f : \mathbb{Z}^+ \to \mathbb{R}$ be a function defined as $f(x) = 5x^3 + \frac{3}{5}, \forall x \in \mathbb{Z}^+$. The function f is strictly increasing function because if $x < y \to 5x^3 + \frac{3}{5} < 5y^3 + \frac{3}{5}, \forall x, y \in \mathbb{Z}^+$. Or, $x < y \to f(x) < f(y), \forall x, y \in \mathbb{Z}^+$.

4.15.3 Isomorphism

Definition 4.30 If each of A, B are partial ordered sets. The mapping $f : A \to B$ is an isomorphism if and only if (1) $f : A \to B$ is bijective function. (2) $x \leq y \to f(x) \leq f(y), \forall x, y \in A$(Awodey, 2010; Vinberg, 2003).

Example 4.43 Let $\mathbb{N}$ be a partial ordered numbers under the relation $\leq$, and $\mathbb{Z}_o^-$ be a partial ordered numbers under the relation. Consider the mapping $f : \mathbb{N} \to \mathbb{Z}_o^-$, defined by $f(n) = -(2n+1), \forall n \in \mathbb{N}$.

(1) We can easily prove that f is bijective function.

(2) Since $n_1 \leq n_2 \leftrightarrow -(2n_1+1) \geq -(2n_2+1), \forall n_1, n_2 \in \mathbb{N}$.

$\therefore n_1 \leq n_2 \leftrightarrow f(n_1) \geq f(n_2), \forall n_1, n_2 \in \mathbb{N}$, hence f is isomorphism.

Example 4.44 Let $A = \{a, c, d, b\}$, where $a \leq d, a \leq c \leq b$, and d, c are not comparable. On the other hand, $B = \{u, v, s, w\}$ where $u \leq s \leq w, u \leq v \leq w$, and s, v are not comparable. Consider $f : A \to B$ be a mapping such that $f(a) = u, f(c) = v, f(b) = w, f(d) = s$.

(1) Clearly, f is bijective, because $x \leq y \to f(x) \leq f(y)$.

(2) but, $s \leq w \nrightarrow d \leq b$. Thus, $f : A \to B$ is not isomorphism.

Example 4.45 Let $A = \{a, b, c\}$ be partial ordered set under $\leq$ as $c \leq a, c \leq b$, and a, b are not comparable. Let $B = \{u, v, w\}$ be partial ordered set under $\leq$ as $w \leq u, w \leq v$, and u, v are not comparable. Consider the mapping $f : A \to B$, defined as $f(a) = v, f(b) = u, f(c) = w$.

(1) $f : A \to B$ is a bijective mapping.

(2) $x \leq y \to f(x) \leq f(y), \forall x, y \in A$. Thus, $f : A \to B$ is the isomorphism function.

Theorem 4.16 *If each of A, B be an ordered set, and $f : A \to B$ be an isomorphism function, then, $x < y \to f(x) < f(y)$.*

Proof Suppose that $x < y$.

$\therefore x \leq y \wedge x \neq y$.

$\because f : A \to B$ is isomorphism,

$\therefore x \leq y \to f(x) \leq f(y) \wedge x \neq y \to f(x) \neq f(y)$.

$\therefore [f(x) \leq f(y) \wedge f(x) \neq f(y)] \rightarrow f(x) < f(y)$.

Thus, $x < y \rightarrow f(x) < f(y)$. ♦

Theorem 4.17 *Let each set of A, B be a partial ordered sets, and $f : A \rightarrow B$ be a bijective function. $f : A \rightarrow B$ is isomorphism if and only if $f : A \rightarrow B$, and $f^{-1} : B \rightarrow A$ are increasing mappings.*

Proof Suppose that $f : A \rightarrow B$ is isomorphism.

$\therefore f : A \rightarrow B$ is increasing.

To prove $f^{-1} : B \rightarrow A$ is increasing, suppose that $z, w \in B, z \leq w$.

$\because f : A \rightarrow B$ is bijective,

$\exists x, y \in A \ni f(x) = z, f(y) = w$,

$\therefore f(x) \leq f(y)$.

$\because f : A \rightarrow B$ is isomorphism,

$\therefore f(x) \leq f(y) \rightarrow x \leq y$.

$\because f : A \rightarrow B$ is bijective,

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

Or, $x = f^{-1}(z), y = f^{-1}(w)$.

$\therefore f(x) \leq f(y) \rightarrow f^{-1}(f(x)) \leq f^{-1}(f(y))$.

Or, $z \leq w \rightarrow f^{-1}(z) \leq f^{-1}(w)$.

$\therefore f^{-1} : B \rightarrow A$ is increasing mapping.

Conversely, suppose that each of $f : A \rightarrow B$, and $f^{-1} : B \rightarrow A$ are increasing mappings. Now, we have to prove $f : A \rightarrow B$ is isomorphism.

(1) From state of the theorem, $f : A \rightarrow B$ is bijective.

(2) Let $x, y \in A \ni x \leq y$.

$\because f : A \rightarrow B$ is increasing,

$\therefore x \leq y \rightarrow f(x) \leq f(y)$ ...(i).

For the inverse function, let us suppose that $x, y \in A \ni f(x) \leq f(y)$.

$\because f^{-1} : B \rightarrow A$ is increasing,

$\therefore f(x) \leq f(y) \rightarrow f^{-1}(f(x)) \leq f^{-1}(f(y))$.

$\because f : A \rightarrow B$ is bijective,

$\therefore f^{-1}(f(x)) = x, f^{-1}(f(y)) = y$,

$\therefore f(x)) \leq f(y) \rightarrow x \leq y$ ...(ii).

From (i) & (ii), it is concluded that $\forall x, y \in A, f : A \rightarrow B$ is isomorphism. ♦

Theorem 4.18 *Let each of A, B, C be a partial ordered set, then:*

(i) *The identity function, $I_A : A \to A$ is isomorphism.*

(ii) *If the mapping $f : A \to B$ is isomorphism, then it's inverse mapping, $f^{-1} : B \to A$ is isomorphism.*

(iii) *If each of the mapping $f : A \to B, g : B \to C$ is isomorphism, then $g \circ f : A \to C$ is isomorphism.*

Proof (i) $\because I_A : A \to A$ is a bijective function,
$\therefore \forall x, y \in A, x \leq y \to I_A(x) \leq I_A(y)$,
$\therefore I_A : A \to A$ is isomorphisim.
(ii) $\because f : A \to B$ is isomorphism,
$\therefore f : A \to B$ is bijective, based on Theorem 4.17.
$\therefore f^{-1} : B \to A$ is increasing function.
Now suppose that, $x, y \in B \ni f^{-1}(x) \leq f^{-1}(y)$.
$\because f : A \to B$ is isomorphism,
$\therefore f^{-1}(x) \leq f^{-1}(y) \to f[f^{-1}(x) \leq f[f^{-1}(y)]$
$\to x \leq y$.
$\therefore f^{-1} : B \to A$ is isomorphism.
(iii) It is left as an exercise for the reader. ♦

4.15.4 Isomorphism of Sets

Definition 4.31 Let each of A, B be partial ordered sets, A is isomorphic with B, if there exists isomorphic mapping $f : A \to B$, and denoted by $A \cong B$(Awodey, 2010; Vinberg, 2003).

Example 4.46 Let $A = \{x, y, z\}, B = \{x', y', z'\}$, where $y < x, y < z$ and x, z are not comparable, $y' < x', y' < z'$ and x', z'. Let $f : A \to B$ defined as $f(y) = y', f(x) = x', f(z) = z'$. It should be noted that $A \cong B$ because $f : A \to B$ is isomorphic function.

Theorem 4.19 *Let W be a set of all partial ordered sets, and let R be a relation defined on W as $R : A \to B, \forall A, B \subseteq W$. If $A \cong B$, then R is an equivalence relation.*

Proof It is left as an exercise for a reader. ♦

Theorem 4.20 *Consider a mapping $f : A \to B$, where A, B are totally and partially ordered sets respectively. If $f : A \to B$ is bijective and increasing function, then it is isomorphic function.*

Proof Suppose that, $x, y \in A \ni f(x) \leq f(y)$.
$\because A$ is totally ordered set,
$\therefore x, y$ are comparable.
Or, $x \leq y \vee y < x$.
Let us consider $y < x \to y \neq x \wedge y \leq x$.
$\because f : A \to B$ is increasing,
$\therefore y \leq x \to f(y) \leq f(x)$.
If, $f(y) = f(x) \to y = x$, then f is injective.
This is contradiction, because $y \neq x$.
Thus, $f(y) \neq f(x)$.
Or, $f(y) \leq f(x) \wedge f(y) \neq f(x) \to f(y) \leq f(x)$.
This contradicts our hypothesis. Thus, $x \leq y$.
$\because f : A \to B$ is bijective, and $\forall x, y \in A$,
$\therefore f$ is isomorphic function. ♦

Theorem 4.21 *If A be a well ordered set, and f be an isomorphic mapping from A to a subset of A, then $x \leq f(x), \forall x \in A$.*

Proof Suppose that $P = \{x \in A | f(x)\ x\} \neq \phi$
$\because A$ is well ordered set, and $\phi \neq P \subseteq A$,
$\therefore P$ has a least element.
Let us assume that $a \in P$ is a least element.
$\because a \in P \to f(a) < a$,
$\because f$ is isomorphic, from A to a subset of A,
$\therefore f(a) < a \to f(f(a)) < f(a)$.
$\because f(a) \in A$, and a is a least element,
$\therefore a \leq f(a)$.
This is contradiction because we have assumed that $f(a) < a$.
$\therefore P = \phi$.
Thus, $x \leq f(x), \forall x \in A$. ♦

Theorem 4.22 *If A be a well ordered set, then there is no isomorphic mapping from A to an initial segment of a subset of A.*

Proof Suppose that f is an isomorphic mapping from A to an initial segment S_a of a subset of A such that $S_a = \{x \in A | x < a\}, \forall a \in A$.

Based on Theorem 4.21, we have $a \leq f(a)$,

$\therefore f(a) \notin S_a$.

This in impossible because $f(a) \in ranf \subseteq S_a$.

Thus, there is not such isomorphic mapping. ♦

Corollary *There is no isomorphism between well ordered set and its initial segment.*

Proof It is left as an exercise for a reader. ♦

Theorem 4.23 *Let each of A, B be well ordered sets. If A is isomorphic with an initial segment of B, then B is not isomorphic with any subset of A.*

Proof Suppose that $f : A \to S_b$ is an isomorphism from A to an initial segment S_b of B, and also suppose an isomorphism $g : B \to C, C \subseteq A$.

It should be noted that $g : B \to C$ is a mapping. And, it should also be noted that both of $f : A \to S_b, g : B \to C$ are injective and increasing mapping.

$\therefore f \circ g : B \to S_b$ is injective and increasing.

$\therefore f \circ g : B \to S_b$ is isomorphic from B to $ran(f \circ g)$ based on Theorem 4.20 where $ran(f \circ g) \subseteq S_b$.

But, this is impossible according to Theorem 4.22.

Thus, our assumed isomorphic g is not exists. And therefore, there is not an isomorphism from B to any subset of A. ♦

Theorem 4.24 *Let X be an well ordered set, and let $S_x, S_y \subseteq X$. If $x < y$, then $S_x \subseteq S_y$.*

Proof $\because x < y \to S_x \subseteq S_y$, that is $[a \in S_x \to a < x \to a < y \to a \in S_y]$.

In the same way $S_y \subseteq S_x$.

Thus, depending on Theorem 4.23, $S_x = S_y$, or S_x is an initial segment of S_y.

But, $x \neq y \to S_x \neq S_y$.

Thus, S_x is an initial segment of S_y. ♦

4.15.5 Cantor's Theorem

The chapter concludes with a new theorem as a collection of the contents of theorems (4.22-4.24), based on the concept of a well-ordered set, isomorphism of sets, and initial segment os a set in which introduced by Cantor (1883b).

Theorem 4.25 *If each of A, B be well ordered sets, then one and only one of the following statements is true.*

(i) *A is isomorphic with B.*

(ii) *A is isomorphic with an initial segment of B.*

(iii) *B is isomorphic with an initial segment of A.*

Proof Suppose that each of A, B are well ordered sets, and

$C = \{x \in A | \exists r \in B \ni S_x \cong S_r\}$.

It should be noted that, if $x \in C$, there is just one element $r \in B$, such that $S_x \cong S_r$.

Let us assume that there exists another element $t \in B$, such that

$S_x \cong S_r \wedge S_x \cong S_t, r \neq t, r < t$.

Now, based on Theorem 4.24, S_r will be an initial segment to S_t.

But as assumed before, $S_r \cong S_x \cong S_t$.

This is impossible, based on the corollary of Theorem 4.22.

$\therefore \forall x \in C\ \exists!\ r \in B \ni S_x \cong S_r$.

Now, we define the relation $F : C \to B$, in which $F(x) = r$.

Suppose that $ranF = D$.

$\therefore F : C \to B$ will be a mapping.

Now, we have to prove that $F : C \to B$ is isomorphism.

(a) Obviously, the mapping $F : C \to D$ is surjective.

To prove that the mapping is injective, suppose that $u, v \in C$ such that $F(u) = F(v) = r$.

$\therefore S_u \cong S_r \cong S_v$.

Suppose that $u \neq v$, let $u < v$, based on Theorem 4.24, S_u become initial segment of S_v, and this impossible according to the corollary of Theorem 4.22.

$\therefore u = v$,

$\therefore F : C \to D$ is injective.

Thus, the mapping $F : C \to D$ is bijective.

(b) Now, we have to prove that the mapping $F : C \to D$ is increasing.

Let $u, v \in C$ such that $u \leq v$, and suppose that, $F(u) = r, F(v) = t$.

$\therefore S_u \cong S_r \wedge S_r \cong S_t$.

Suppose $t < r$.

$\therefore S_t$ will be an initial segment of S_r according to Theorem 4.24.

Or, $S_u \subseteq S_v$. Thus,

(1) S_v is isomorphic with the initial segment S_r.

(2) S_r is isomorphic with subset of S_v. And that is impossible according to Theorem 4.23.

$\therefore r \leq t$. Or, $F(u) \leq F(v)$.

$\therefore u \leq v \to F(u) \leq F(v)$.

$\therefore F : C \to D$ is increasing.

Thus, $F : C \to D$ is isomorphism.

(c) Now, we are going to prove that C is segment of A.

Suppose $c \in C, x < c$, and we have to prove $x \in C$.

If $F(c) = r$, then $S_c \cong S_r$.

$\therefore \exists g : S_c \to S_r$.

It should be noted that the mapping $g/S_x : S_x \to S_{g(x)}$ will be isomorphism.

$\therefore S_x \cong S_{g(x)}$.

$\therefore x \in C$.

Through the same method, we can prove that D is a segment of B.

Now, we are going to prove that C is not initial segment of A or D is not initial segment of B.

Let us assume the opposite, assuming that C is an initial segmentof A, and D is an initial segment of B.

Or, $C = S_x \wedge D = S_r$.

As, $F : C \to D$ is isomorphism,

$\therefore C \cong D$.

$\therefore S_x \cong S_r$.

But, since $x \in C$, hence, $x \in S_x$.

And this is a contradiction. Thus, one of the statements (1), (2), (3) is satisfied. On the other hand, and based on Theorems (4.22, 4.23), it concludes that it can not obtain more than one claim. Thus, just one of the statements (a), (b), (c) hold true. ♦

4.16 exercises

Answer the following questions:

Q1: Let A be a well ordered set. Prove that any subset of A will be isomorphic with A, or with a initial segment with A.

Q2: Let A, B be well ordered sets. Prove that there is at most one isomorphism, $f : A \to B$.

Q3: Let A, B be well ordered sets. Prove that if A is isomorphic with B and B is isomorphic with a subset of A there is at most one isomorphism, then A is isomorphic with B.

Q4: Let A be well ordered set. Prove that I_A is a unique isomorphism from A to A.

Q5: Let A, B be well ordered sets. If each of $f : A \to B, g : B \to A$ isomorphic, then $g = f^{-1}$.

Q6: Let A, B be well ordered sets. Consider that A does not contains on a greatest, and assume that all elements in B (except of least element) have an immediate predecessor. And, prove that B is isomorphic with an initial segment of A.

Q7: Consider a bijective function $f : A \to B$. If the set A is partially ordered set or totally ordered set or well ordered set, then it is possible to define on B, a partially ordered relation or totally ordered relation or well ordered relation via f to make f isomorphism.

4.17 Axiom of Choice

The scientist Zermelo (1904) explained that there is a hypothesis used implicitly in many fields of mathematics, and this hypothesis is not derived from any hypotheses known previously in mathematics or logic. Therefore, he was considered as a new axiom and called an axiom of choices. In what follows, Axiom of choices will be explained.

Definition 4.32 Let $\{A_i\}_{i\in I} \neq \phi$ be a nonempty family of sets. It can be selected an element x_i from A_i, for all $i \in I$. Or, there exists a mapping $f : I \to \bigcup_{i\in I} A_i \ni f(i) \in A_i, \forall i \in I$ (Zermelo, 1904; Mendelson, 2009b; Jech, 1977).

Note: Obviously, if I is a finite set, then it can be selected $x_1 \in A_1, ..., x_n \in A_n$. But, if I is an infinite set, then the selection is uncertainty.

Definition 4.33 Consider a set A, and $P'(A) = P(A) - \{\phi\}$. The defined mapping $f : P'(A) \to A | f(B) \in B, \forall B \in P'(A)$ is called a choice mapping. Or, f_B instead of $f(B)$(Zermelo, 1904; Smith, 1975).

Example 4.47 Let $A = \{a, b\}$. Let us apply a choice function on A, is a function $f : P'(A) \to A$ defined as follows in Table 4.1:

Table 4.1: Choice Mapping

B	$f(B)$
$\{a, b\}$	a
$\{a\}$	a
$\{b\}$	b

According to the definition 4.32, the problem can be states as:

Consider a set A. Is there always a choice mapping for A? In fact, based on the axiom of choice, every element has a choice mapping, but do not specify how to choose it. The axiom of choice can not de derived from any hypotheses known previously in mathematics or logic. Furthermore, it also does not contradict those hypotheses known previously.

The position of the axiom of choice, as a Euclid's fifth hypothesis (Eves, 1963; Eves, 1992): *From the point outside of the certain line, it can draw just one parallel for that line.*

The three inserted statements are equivalent to the axiom of choice as follows;

(i) Every set has a choice mapping.

(ii) Let A be a set, its elements are nonempty sets and separated. There exists a set C contains one element of $A \in \mathcal{A}, \forall A$. Or, $\{\exists! c | c\} = C \subseteq A \in \mathcal{A}, \forall A$.

(iii) Let $\{A_i\}_{i \in I}$ be a family of sets. If I is a nonempty set and for all A_i be a nonempty set, then $\prod_{i \in I} A_i$ is nonempty. Or, if $I, A_i \neq \phi, \forall A_i$, then $\prod_{i \in I} A_i \neq \phi$.

In what follows, we are going to deal with a theorem has an equivalent statements(Zermelo, 1904; Jech, 2008; Renteln and Dundes, 2005; Harper et al., 1976; Moore, 2012).

Theorem 4.26 *The following statements are equivalent.*

(i) *If $U = \{X_\alpha\}_{\alpha \in I}$ is a family of sets, and for any subset family U_1 is a totally ordered with respect to inclusion mapping $\bigcup \{X | X \in U_1\}$ is belong to the family of sets U, then U contains a maximal element with respect to an inclusion mapping (Zermelo, 1904; Mendelson, 2009b; Jech, 1977; MacLane and Birkhoff, 1999).*

(ii) *Tukey's lemma (Jech, 2008): If $U = \{X_\alpha\}_{\alpha \in I}$ is a family of sets with finite property, then U contains a maximum element with respect to inclusion mapping. Finite property means;*

(a) *Each set of the finite family subsets in any element of the family belongs to the family of sets.*

(b) *If all finite subsets of X belongs to the family of sets, then X itself belongs to the family of sets.*

(iii) *Zorn's lemma (Moore, 2012): Let $A \neq \phi$ be a partially ordered set. If all subsets of A be totally ordered sets and bounded above, then A contains of greatest element.*

(iv) *Axiom of choice (Zermelo, 1904): If $\{X_\alpha\}_{\alpha \in I} \neq \phi$ is a family of sets, then there exists a mapping $f : I \to \bigcup_{\alpha \in I} Y_\alpha | f(x) \in Y_\alpha, \forall \alpha \in I$.*

(v) *Zermelo's theorem: Well ordering theorem (Zermelo, 1904): Every set A can be arranged as a well ordered set.*

(vi) *Hausdorff Maximal Principle (Kelley, 1955; Kelley, 2017; Moore, 2012; Harper et al., 1976): If A is a partial ordered set, let B be a nonempty totally ordered subset of A, then there exists a subset B^* in A, such that it will be totally ordered and has a greatest element among all totally ordered sets and contain the set A.*

Proof It is left as an exercise for the reader.

4.18 Exercises

Solve the following questions:

Q1: Consider a set A, and a mapping $f : A \to A$. The mapping $f : A \to A$ is surjective if and only if there exists a mapping $g : B \to A$, such that $f \circ g = I_B$.

Q2: Consider a sets A, B, and a mapping $f : A \to B$. There exists a set $C \subseteq A, g \subset f$, such that $g : C \to B$ is injective function, and $ranf = rang$.

Q3: Prove that the following hypothesis is equivalent to the axiom of choice. If E be a set, and assume that $G \subseteq E \times E$ and $A = domG, B = ranG$, then there exists a mapping $f : A \to B$, such that $f \subseteq G$.

Q4: Let $R : A \to B$ be a relation such that $domR = A$. There exists a subset $R^* \subset R$ such that $R^* : A \to B$ be a mapping.

Q5: Consider a sets A, B, C. Let $f : B \to C, g : A \to C$ be mappings. Assume that $ranf \subseteq g$. Prove that there exists a mapping $g \circ h = f$ where $h : B \to A$.

Q6: Consider this quote from Bertrand Russell (18 May 1872 - 2 February 1970) “The Axiom of Choice is necessary to select a set from an infinite number of pairs of socks, but not an infinite number of pairs of shoes.” Do you think that explanation makes sense for the quote?

The observation here is that one can define a function to select from an infinite number of pairs of shoes, for example by choosing the left shoe from each pair. Without the axiom of choice, one cannot assert that such a function exists for pairs of socks, because left and right socks are (presumably) indistinguishable.

5

Potency of Sets

5.1 Introduction

Consider a finite sets A, B. Now, let us ask the following question, Are the contents of the sets of the same number have same elements? We can answer this question by one of the following methods;

(i) We begin to account elements for each set separately. But we can not generalize this method in the case of infinite sets because it is impractical.

(ii) We will try to finite a bijective mapping between A and B. If we found such mapping, then we conclude that the sets consist of the same number of elements and the vice versa. This method can be generalized although the sets consist of infinite elements.

Thus, $A \sim B$ if and only if there exists a bijective mapping between A and B. The relation $\sim$ is an equivalence relation, and each equivalence class relates to an element called cardinal number.

It should be noted that the cardinal numbers is a general case of natural numbers ($\mathbb{N} = \{0, 1, 2, 3, ...\}$), provided that the cardinal numbers do not care of ordering sets. There are kind of numbers that are called ordinal numbers, in which they are the most used than the cardinal numbers. In the case of dealing with the finite sets, the concept of the ordinal number matches with the concept of the cardinal number.

5.2 Equipotent Sets

Definition 5.1 Let each of A, B be a set. A is equipotent to B if and only if there exists a bijective function $f : A \to B$, and denoted by $A \sim B$ (Weisstein, 2019).

Notation: It is clear from the definition, if there is not exist any bijection between A, B, then A is not equipotent to B, denoted by $A \nsim B$.

Notes:

(i) The relation $\sim$ among sets is an equivalent relation. Or,

(a) $A \sim A, \forall A$.

(b) If $(A \sim B) \to (B \sim A), \forall A, B$.

(c) If $((A \sim B) \wedge (B \sim C)) \to (A \sim C), \forall A, B, C$.

Thus, any collections of sets divided into equivalence classes.

(ii) It should be noted that the definition shows that how can the equipotent of sets, not what mean by equipotent of sets. The concept of the equipotent of sets is an abstract concept, especially if the set is infinite. Thus, it would be said that the equipotent of a set is the amount of the elements of it.

(iii) The concept of cardinal number used to refer to the property of equipotent sets. Based on (ii) the cardinal numbers will be a criterion of a number of elements in the sets.

Thus, we have connected with any set A, a new mathematical concept named a cardinal number of the set A. As mentioned by Cantor (1845-1918) (Dauben, 1990; Dauben, 1977; Guinness, 1971; Guinness, 2000), the cardinal number of a set is a concept which is strongly aware of abstraction and connects with the set, ignoring the nature of its elements and their order.

Notation: If A be a set, the cardinal number of it denoted by $\#(A)$ as the expression of the number of elements of A. Thus, the essential property of the cardinal numbers is as follows:
$(A \sim B) \to \#(A) = \#(B)$.

Definition 5.2 α is a cardinal number if exists a set A such that $\alpha = \#(A)$(Sierpiński, 1958).

Notation: The cardinal number of:
$\#(\phi) = 0$, $\#(\{\phi\}) = 1$, $\#(\{\phi, \{\phi\}\}) = 2$, ..., $\#(\{0, 1, ..., n-1\}) = n$.

Example 5.1 Consider $A = \{2, 4, 6, 8\}$, $B = \{x, y, p, q\}$. We define the mapping $f : A \to B$, as follows; $f(2) = x, f(4) = y, f(6) = p, f(8) = q$.

Obviously, $f : A \to B$ is bijective, so $A \sim B$. Thus, $\#(A) = \#(B) = 4$.

Example 5.2 Consider $A = \{x, y, z\}$, $B = \{1, 2\}$. It is clear cannot be found any bijective between A and B is $A \nsim B$.

Example 5.3 Let $A = [0, 1] \subset \mathbb{R}, B = [2, 5] \subset \mathbb{R}$, and consider the mapping $f : A \to B \ni f(x) = 3x + 2, \forall x \in A$, as illustrated in Figure 5.1. Since $f : A \to B$ is bijective, hence $A \sim B$.

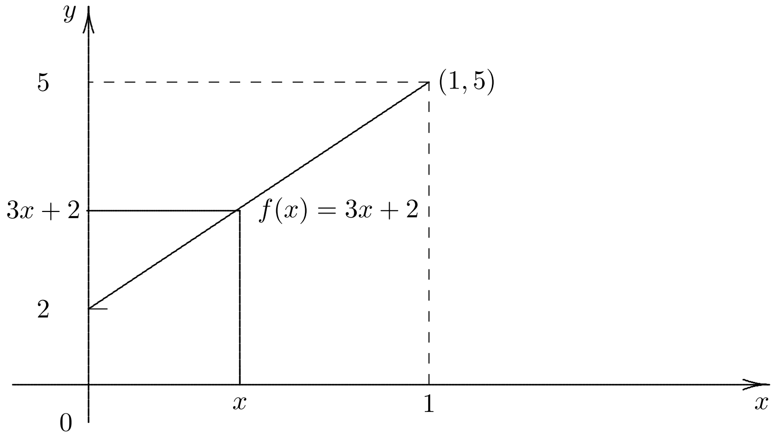


Figure 5.1: $f(x) = 3x + 2$

Definition 5.3 Let A be a set. A said to be a finite if and only if it equipotent with a set of $\mathbb{N}$ with the property $\{0, 1, 2, ..., n-1\}, n \in \mathbb{N}$, otherwise A is infinite set(Apostol, 1974; Cohn and Cohn, 1981; Dedekind, 1963).

Definition 5.4 If A is equipment with a set of $\{0, 1, 2, ..., n-1\}, n \in \mathbb{N}$, then the cardinal number of A is n (Mustafa et al., 1980; Sierpiński, 1958).

Note:

(i) The cardinal number for the finite sets is the number of elements for that set.

(ii) The set A is finite if there is not any subset of A in which equipment with it except A itself. Thus, the infinite set could be defined as follows: The set A is infinite if and only if A is equipotent with the proper subset of it.

(iii) The number α is a finite number if it is the cardinal number for a finite number, otherwise, it is called infinite number. In addition, the finite cardinal number is also called a natural number. Furthermore, the finite cardinal number is called transfinite number(Levy, 2002; Rubin, 1967; Rucker, 2013; Suppes, 1960).

(iv) The set A is a finite if and only if $\#(A) \neq \#(A) + 1$. Thus, if $\alpha = \#(A)$, A is finite, then $\alpha \neq \alpha + 1$.

(v) There exists a unique natural number ($\mathbb{N}$), where this set is infinte and denoted for its cardinal numbers by the symbol N_o.

5.3 The Ordering on the Cardinal Numbers

Definition 5.5 Let each of α, β be a cardinal number. It said $\alpha \leq \beta$ if and only if there exists sets A, B such that $\alpha\#(A), \beta\#(B)$. And A is equipment with a subset of B, and this means there exists an injective function $f : A \to B$ (Dauben, 1990; Rubin, 1967; Suppes, 1960).

Note:

(i) The relation $\leq$ on the potent of sets (the cardinal numbers) is a partial ordered relation because:

  (a) The relation $\leq$ is a reflexive. Or, $\alpha \leq \alpha, \forall\alpha$.

  (b) The relation $\leq$ is a transitive. Or, $(\alpha \leq \beta) \wedge (\beta \leq \gamma) \rightarrow (\alpha \leq \gamma)\forall\alpha, \beta, \gamma$.

  (c) Based on Schroeder-Bernstein (Bernstein, 1905), the relation $\leq$ is an anti-symmetric.

(ii) The expression $\beta \geq \alpha$, implies that $\alpha \leq \beta$.

(iii) The relation $\leq$ on the cardinal numbers is a totally ordered relation. Or, any two cardinal numbers are comparable.

Example 5.4 If n denoted to finite cardinal number, then $n \leq \mathbb{N}_o$, where $\mathbb{N}_o$ is a finite cardinal number for the natural numbers.

5.3.1 Preliminary Theorem

Theorem 5.1 *Let A be a subset of B. Consider the bijective function $f : B \rightarrow A$, and for all X from $B - A$, there exists a bijective $f : B \rightarrow (A \cup X)$.*

Proof Let $f_1 : X \rightarrow X$ be a mapping, such that $f_1(X) = X$.

Let $f_2 : X \rightarrow A$, such that $f_2(X) = f(f_1(X))$. Generally, we define a mapping $f_{i+1} : X \rightarrow A$, such that $f_{i+1} = f(f_i(X)); i = 1, 2, ..., n$.

Let $G = \bigcup_{i=1}^{\infty} f_i(X)$. Obviously, $G = f(C) \bigcup X$.

Now, we define $f_0 : B \rightarrow A \bigcup X$, such that;

$$f_0 = \begin{cases} b, \forall b \in C \\ f(b), \forall b \in B - C \end{cases}$$

The mapping $f_0 : B \rightarrow A \bigcup X$ is surjective because;

$f_0(B) = f_0(C \bigcup (B - C)) = f_0(C) \bigcup f_0(B - C) = C \bigcup f(B - C) = X \bigcup f(C) \bigcup f(B - C) = X \bigcup f(B) = X \bigcup A$.

As well as the mapping $f_0 : B \rightarrow A \bigcup X$ is injective because f_0/C is injective, therefore $f_0/B - C$ is injective. And, $f_0(C) \bigcap f_0(B - C) = \phi$.

Since $f_0 : B \rightarrow A \bigcup X$ is injective and surjective, hence it is bijective. ⧫

5.3.2 Schroeder-Bernstein Theorem

The Schroeder-Bernstein Theorem (Remmel, 1981; Hinkis, 2013; Gwynne, 2009) is a result from set theory(Suppes, 1960), named for Ernst Schroeder and Felix Bernstein(Crow, 1993). Informally, it implies that if two cardinalities are both less than or equal to each other, then they are equal.

Theorem 5.2 *Let each of A, B be a set. If A is equipotent with a subset of B, and B is equipotent with a subset of A, then A is equipotent with B.*

Proof Let $g : A \to B_1$ be a bijective mapping, where $B_1 \subseteq B$. And $h : B \to A_1$ be a bijective mapping, where $A_1 \subseteq A$.

The mapping $(g \circ h) : B \to (g \circ h)(B)$ is a bijective between the sets B and $(g \circ h)(B)$.

Let $S = B_1 - (g \circ h)(B)$. Now, based on Theorem 5.1, a bijective between B and B_1, such that $B_1 = (g \circ h)(B) \bigcup S$.

Or, $B \sim B_1$. But, $B_1 \sim A$

$\therefore A \sim B$ (By substitution). ⧫

Corollary *Let each of α, β be cardinal number. If $\alpha \leq \beta \wedge \beta \leq \alpha$, then $\alpha = \beta$.*

Proof The proof is been left as an exercise to the reader. ⧫

Definition 5.6 Let A be a set, it is called that A has a power of the continuum, if it bijective with the set of points of the closed interval $[0, 1]$(Gödel, 1947).

Notation: $\#[0, 1] = C$

Note:

(i) $\mathbb{R} \sim [0, 1]$. The mapping $f : (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$, where $f(x) = tanx$ is a bijective.

$\therefore \#(\mathbb{R}) = \#(-\frac{\pi}{2}, \frac{\pi}{2}) = \#(0, 1) = \#[0, 1]$ Thus, $\#(\mathbb{R}) = C$.

(ii) If $x \in [0,1]$, then $x = \sum_{i\geq 1} \frac{a_i}{2^i}$, where $a_i = \begin{cases} 1 \\ 0 \end{cases} \forall i \in \mathbb{N}, x = (a_1, a_2, ...)$.

5.3.3 Cantor's Theorem

Theorem 5.3 *Consider a set B, then $\#(B) < \#(P(B))$(Hausdorff, 1914b; Hausdorff, 1914a; Hinkis, 2013; Cantor, 1878).*

Proof Let us denote for the mapping from B to $P(B)$ by g, in which translate b to $\{b\}$.

The mapping $g : B \to P(B)$ is injective.

Suppose that there existed a bijective mapping $f : B \to P(B)$, and let denote to the set $\{x \in B | x \notin f(x)\}$ by the symbol A.

Obviously, $A \subseteq B \to A \in P(B)$.

$\forall f : B \to P(B)$ is surjective mapping.

$\therefore \exists b \in B \ni f(b) = A$.

Now, there are two possibilities:

(i) $b \in A$, in this case $b \notin f(b)$. Or, $b \notin A$.

(ii) $b \notin A$, that means that $b \in f(b) = A$.

In both cases, there is a contradiction. That means there is not bijective between B and $P(B)$.

Or, $\#B \neq \#(P(B)) \to \#B < \#(P(B))$. ♦

5.3.4 Continuum Hypothesis

One of the unsolved problems in the set theory is the following problem:

Is there a cardinal number α such that $\mathbb{N}_o < \alpha < C$. (Continuum hypothesis states that there is not a cardinal number α such that $\mathbb{N}_o < \alpha < C$ (Cantor, 1883b; Cantor, 1878; Gödel, 1947)).

Gödel (1947) proved that if the axioms of the set theory are consistent then there is no contradiction when adding the Continuum hypothesis to those axioms. Furthermore, Cohen (1964) proved the independence of Continuum hypothesis. Or, the axiom or its negation can be added into the system of the mathematical axiom without any perturbation (Cohen, 2008; Cohen, 1964).

5.4 Exercises

Answer the following questions:

Q1: Prove that:

(i) $(0,1) \sim [0,1]$.

(ii) $(-\frac{\pi}{2}, \frac{\pi}{2}) \sim (0,1)$.

Q2: Let each of A, B be a set, prove that $A \times B \sim B \times A$.

Q3: Let each of A, B, C be a set, prove that $(A \times B) \times C \sim A \times (B \times C)$.

Q4: Let each of B, C be a set, such that $\#(B - C) = \#(C - B)$, prove that $\#(B) = \#(C)$.

Q5: Let each of A, B, C, D be a set, such that $\#(A) = \#(B), \#(C) = \#(D)$, prove that it is not necessary $\#(C \cap A) = \#(D \cap B)$.

Q6: Let A be an infinite set, and B be a subset of it, such that $A - B$ be a finite set, prove that $\#(A) = \#(B)$.

Q7: Prove that any undefined group can be expressed through a combination of two subgroups of it, where these two groups are not infinite and not intersected.

Q8: Prove that for any set A will be finite if and only if any totally ordered relation on it will be well ordered relation.

5.5 Arithmetic on Cardinal Numbers

5.5.1 Addition of the Cardinal Numbers

We are going to define additional on the cardinal numbers by a method as a generation of the addition on the finite cadinal numbers (The natural numbers).

Definition 5.7 Let us assume each of m, n a cardinal number, we obtain the cardinal number $m + n$ by selecting M contains of m of elements, and N contains of n of elements, such that $M \cap W = \phi$, then we account a number of $M \cup W$. Similarly, let each of α, β a cardinal number, then the cardinal number $\alpha + \beta$ of the set $A \cup B$, provided;

(i) $\#(A) = \alpha$.

(ii) $\#(B) = \beta$.

(iii) $A \cap B = \phi$. (Deiser, 2010; Enderton, 1977).

Theorem 5.4 *All cardinal numbers are well defined.*

Proof Let $A^* \sim A, B^* \sim B$, such that $A \cap B = \phi, A^* \cap B^* = \phi$.
$\therefore (A^* \cup B^*) \sim (A \cup B) \rightarrow \#(A \cup B) = \#(A^* \cup B^*)$.
$\therefore \alpha + \beta$ well defined such that $\alpha = \#(A), \beta = \#(B)$. ♦

Note: Might happen $\alpha = \#(A), \beta = \#(B)$, but $A \cap B \neq \phi$. In that case, the following standard substitution theorem used to find $\alpha + \beta$.

Theorem 5.5 *Let* $\{A_\alpha\}_{\alpha \in I}$ *be a family of sets, there exists a family of sets* $\{A^*_\alpha\}_{\alpha \in I}$ *such that:*

(i) $A^*_\alpha \sim A_\alpha, \forall \alpha \in I$.

(ii) $\alpha \neq \beta \rightarrow A^*_\alpha \bigcap A^*_\beta = \phi$.

Proof Assume that $A^*_\alpha = \{(a, \alpha) | a \in A_\alpha\}$.
Obviously, $A^*_\alpha \sim A_\alpha$, and $A^*_\alpha \bigcap A^*_\gamma = \phi$.
If $\alpha \neq \gamma$ then $\{A^*_\alpha\}_{\alpha \in I}$ is disjoint and an intersection of a family of sets. ♦

Example 5.5 This example illustrated of the standard substitution theorem.

Let each of α_1, α_2 be a cardinal number, and each of A_1, A_2 be a set, such that;

$\#(A_1) = \alpha_1, \#(A_2) = \alpha_2, A_1 \cap A_2 \neq \phi$.

$\therefore \alpha_1 + \alpha_2 = \#(A^*_1 + A^*_2)$, where $\alpha_1 = \#(A^*_1) = \#(A_1 \times \{1\})$, $\alpha_2 = \#(A^*_2) = \#(A_2 \times \{2\})$.

Where each of A^*_1, A^*_2 substituted by $A_1 \times \{1\}, A_2 \times \{2\}$, respectively.

It is clear that $A^*_1 \bigcap A^*_2 = \phi$.

Example 5.6 Let $A = \{1, 3, 5, ...\}, B = \{0, 2, 4, 6, ...\}$.

Note that, $\#(A) = \mathbb{N}_o, \#(B) = \mathbb{N}_e$, and $A \cap B = \phi$.

Thus, $\mathbb{N}_o + \mathbb{N}_e = \#(A \cup B) = \#(\mathbb{N})$.

Example 5.7 Let $S = [0, 1) \subseteq \mathbb{R}, T = [1, 2) \subseteq \mathbb{R}$.

Note that $\#(S) = \#(T) = C$, and $T \cap S = \phi$.

Thus, $C + C = \#(T + S) = \#([0, 2)) = C$.

Generally, $C + C + ... = C$.

Since all the sets of the type $F_n = [n, n + 1), n = 1, 2, ...$ are separated, and $\#(F_n), \forall n = 1, 2, ...$ hence, $C + C + ... = \#(\bigcup_{n=1}^{\infty} F_n) = \# \{x|x \geq 1\} = C$.

Note: It should be noted, from the previous example, the subtract operation on the cardinal numbers cannot be defined because there is not inverse of the addition operation. So, the equation $C + x = C$ has the solution as follows:

(i) x any finite cardinal number.

(ii) $x = \mathbb{N}_o$.

(iii) $x = C$.

Theorem 5.6 *Consider the cardinal numbers α, β, γ, the following properties holds;*

(i) *The associated property for the addition $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.*

(ii) *The commutative property for the addition $\alpha + \beta = \beta + \alpha$.*

Proof (i) Let A, B, C be separated sets.

$\therefore, \alpha = \#(A), \beta = \#(B), \gamma = \#(C)$.

$(\alpha + \beta) + \gamma = \#(A \bigcup B) + \#(C) = \#((A \bigcup B) \bigcup C) = \#(A \bigcup (B \bigcup C)) = \#(A) + \#(B \bigcup C) = \alpha + (\beta + \gamma)$.

(ii) $\alpha + \beta = \#(A \bigcup B) = \#(B \bigcup A) = \beta + \alpha$. ⧫

Note: It should be noted, the cancellation law does not hold in the addition of the cardinal numbers, for example;

$\mathbb{N}_o + \mathbb{N}_o = \mathbb{N}_o = 1 + \mathbb{N}_o$. While $\mathbb{N}_o \neq 1$.

5.5.2 Multiplication of the Cardinal Numbers

We are going to define the multiplication of the cardinal numbers in such way as a generalization of the multiplication operation on the finite cardinal numbers (the natural numbers).

Definition 5.8 Let each of m, n be a natural numbers, we obtain on mn to choose the set M in which it contains of m of elements, and W contains of n of elements, then we account the ordered pairs of $M \times W$. Similarly, if each of α, β is a cardinal number, then the multiplication of them written $\alpha\beta$ is a cardinal number to $A \times B$ where $\#(A) = \alpha, \#(B) = \beta$ (Deiser, 2010; Enderton, 1977).

Note: Based on the definition, the above multiplication will be;
$\because A^* \sim A, B^* \sim B, \therefore (A^* \times B^*) \sim (A \times B) \to (A^* \times B^*) = \#(A \times B)$.

Theorem 5.7 *Let α, β, γ be cardinal numbers, the following properties are hold;*

(i) *The associate property $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.*

(ii) *The commutative property $\alpha\beta = \beta)\alpha$.*

(iii) *The multiplication distributed on the addition $(\beta + \gamma)\alpha = \beta\alpha + \gamma\alpha, \alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.*

Proof (i), (ii) are left to the reader.

(iii) Let A, B, C be disjoint sets, such that: $\#(A) = \alpha, \#(B) = \beta, \#(C) = \gamma$.

Now, $\alpha(\beta + \gamma) = \#(A)\#(B \bigcup C) = \#(A \times (B \bigcup C)) = \#((A \times B) \bigcup (A \times C))$.

$\because (A \times B) \bigcup (A \times C) = \phi$

$\therefore \alpha(\beta + \gamma) = \#(A \times B) + \#(A \times C) = \alpha\beta + \alpha\gamma$. ♦

Note: Multiplication of the Cardinal Numbers could be generated to any family of the cardinal numbers. For example, $\alpha_1, \alpha_2, ..., \alpha_n = \#(\prod_{i=1}^{n} A_i)$, where $\#(A_i) = \alpha_i; \forall i = 1, 2, .., n$.

Theorem 5.8 *If $\mathbb{N}_o = \#(\mathbb{N}), C = \#([0, 1))$, then:*

(i) $\mathbb{N}_o\ \mathbb{N}_o = \mathbb{N}_o$.

(ii) $\mathbb{N}_o\ C = C$.

(iii) $C\ C = C$.

Proof (i) $\mathbb{N}_o\ \mathbb{N}_o = \#\{\mathbb{N} \times \mathbb{N}\}$

We can express of elements of $\mathbb{N} \times \mathbb{N}$ as follows;

$$\begin{array}{ccccc}
(0,0) & (0,1) & (0,2) & (0,3) & ... \\
(1,0) & (1,1) & (1,2) & (1,3) & ... \\
(2,0) & (2,1) & (2,2) & (2,3) & ... \\
(3,0) & (3,1) & (3,2) & (3,3) & ... \\
. & . & . & . & \\
. & . & . & . & \\
. & . & . & . &
\end{array}$$

Then arranged in an infinite sequence:

$\{(0,0),(1,0),(0,1),(2,0),(1,1),(0,2),...\}$.

$\therefore \#(\mathbb{N} \times \mathbb{N}) = \mathbb{N}_o \Rightarrow \mathbb{N}_o\ \mathbb{N}_o = \mathbb{N}_o$.

(ii) $\mathbb{N}_o\ C = \#\{\mathbb{N} \times [0,1)\}$.

Now, let us define a mapping $f : \mathbb{N} \times [0,1) \rightarrow [0,\infty)$, such that $f((x,y)) = x + y$.

It is clear that $f : \mathbb{N} \times [0,1) \rightarrow [0,\infty)$ is a surjective , and injective mapping.

$\therefore f : \mathbb{N} \times [0,1) \rightarrow [0,\infty)$ is bijective.

$\because \#([0,\infty)) = C$,

$\therefore \mathbb{N}_o\ C = C$.

(iii) $C\ C = \#\{(x,y)|x,y \in [0,1)\}$.

We will express of x, y as an infinite decimal fraction (this expression is unique).

$\therefore (x,y) = (0.x_1x_2x_3...,0.y_1y_2y_3...)$.

Note that $z = 0.x_1y_1x_2y_2...$ is an infinite decimal fraction.

$\therefore$ z is represents a certain number on [0, 1). Thus, we have defined injective function $f : [0,1) \times [0,1) \rightarrow [0,1)$.

Also, we can define an injective function $g : [0,1) \rightarrow [0,1) \times [0,1)$.

Now, according to Schroeder-Bernstein theorem (Bernstein, 1905), it will be $[0,1) \times [0,1) \sim [0,1)$.

$\therefore C\ C = C$. ⧫

Corollary *If the set B has the power of continuum, then the set $B \times B$ has a power of continuum too.*

Proof The proof is left to the reader. ♦

Note:

(i) It should be noted, cannot be defining the division of the cardinal numbers because the inverse of the multiplication does not exist. For example, the equation $C\ X = C$ has the following solutions;

(a) x any finite cardinal number.

(b) $x = \mathbb{N}_o$.

(c) $x = C$.

(ii) The deletion rule is not verified for the multiplication. For example, $\mathbb{N}_o\ \mathbb{N}_o = \mathbb{N}_o = 1.\mathbb{N}_o$. But $\mathbb{N}_o \neq 1$. Also, $C\ C = C\ \mathbb{N}_o$, while $C \neq \mathbb{N}_o$.

Theorem 5.9 *If $\{A_\alpha\}_{x \in I}$ be a family of sets, where $\#(A_\alpha) = C, \forall \alpha \in I$ and $\#(I) = C$, then the set $\bigcup_{\alpha \in A} A_\alpha$ has a power of continuum.*

Proof Assume that $I = \mathbb{R}, \forall \alpha \in I$.

Let L_α be a straight line $x = \alpha$, as shown in Figure 5.2.

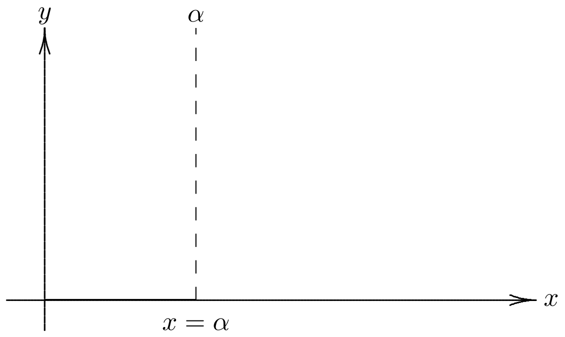


Figure 5.2: $x = \alpha$

$\therefore A_\alpha \sim L_\alpha$ Then $\bigcup_\alpha A_\alpha \sim B \subseteq \bigcup_\alpha L_\alpha$

But, $\bigcup_\alpha L_\alpha = \mathbb{R} \times \mathbb{R}$
$\therefore \#(\bigcup_\alpha L_\alpha) = C\ C = C$.
Thus, $\#(\bigcup_\alpha A_\alpha) = \#B \leq C$ ...(1)
But, $A_\alpha \subseteq \bigcup_\alpha A_\alpha$
$\therefore \#(A_\alpha) \leq \#(\bigcup_\alpha A_\alpha)$
Thus, $C \leq \#(\bigcup_\alpha A_\alpha)$ ...(2)
From (1)& (2) and by utilizing Schroeder-Bernstein theorem, we conclude that $\#(\bigcup_\alpha A_\alpha) = C$. ⧫

5.5.3 Power of the Cardinal Numbers

Definition 5.9 Let each of m, n be finite cardinal numbers, then $(m \times m \times ... \times m)$ n-times (Mustafa et al., 1980; Deiser, 2010; Enderton, 1977; Halmos, 2017b)

Definition 5.10 Let each of α, β be an arbitrary cardinal number, then $\alpha^\beta = \#(\prod A_\gamma | \gamma \in B)$, where $\#(A_\gamma) = \alpha \forall \gamma \in B, \#(B) = \beta$ (Mustafa et al., 1980; Deiser, 2010; Enderton, 1977; Halmos, 2017b).

We can assume that $A_\gamma = A \forall \gamma \in B$
$\therefore \alpha^\beta = \#(\prod A_\gamma | \gamma \in B)$
$\therefore \alpha^\beta = \# \left\{ A^B \right\}$.
Or, $\therefore \alpha^\beta = \# \{ f | f : B \to A \}$, such that $f : B \to A$ is a mapping, and $\#(A) = \alpha, \#(B) = \beta$.

Note: The above operation is well defined.

Theorem 5.10 *For any cardinal numbers α, β, γ the following power rules are hold;*

(i) $\alpha^\beta \alpha^\gamma = \alpha^{\beta+\gamma}$.

(ii) $(\alpha^\beta)^\gamma = \alpha^{\beta\gamma}$.

(iii) $\alpha^\gamma \beta^\gamma = (\alpha\beta)^\gamma$.

Proof (i) Let A, B, C be sets, such that $C \cap B = \phi$, and $\alpha = \#(A), \beta = \#(B), \gamma = \#(C)$.

Now, $\alpha^{\beta+\gamma} = \#(A^{B \cup C}), \alpha^{\beta}.\alpha^{\gamma} = \#(A^B \times A^C)$.

The set $A^{B \cup C}$ consists of all mappings in which their domains and codomains are $B \cup C$ and A respectively.

Let $f \in A^{B \cup C}$, and $f|B$ is a restriction of a mapping on the set B, and $f|C$ is a restriction of a mapping on the set C.

Now, we define the mapping $F : A^{B \cup C} \to A^B \times A^B$, such that $F(f) = (f|B, f|C)$.

We are going to prove that F is bijective.

(1) F is surjective mapping:

Let $(g_1, g_2) \in A^B \times A^C$, such that each of $g_1 : B \to A, g_2 : CB \to A$.

Let us define a mapping $f : (B \cup C) \to A$, such that:

$$f(x) = \begin{cases} g_1(x) & \text{if } x \in B \\ g_2(x) & \text{if } x \in C \end{cases}$$

$\therefore (f|B, f|C) = (g_1, g_2)$.

(2) F is an injective mapping.

$F(f_1) = F(f_2) \to (f_1|B, f_1|C) = (f_2|B, f_2|C)$.

$\therefore f_1|B = f_2|B, f_1|C = f_2|C$,

$\because C \cap B = \phi$,

$\therefore f_1 = f_2$.

Or, F is bijective, thus $A^{B \cup C} \sim A^B \times A^C \Rightarrow \alpha^{\beta+\gamma} = \alpha^{\beta}.\alpha^{\gamma}$.

(ii) & (iii) are left as exercises to the reader. ♦

Example 5.8 Suppose that $A = \{x, y, z\}, B = \{a, b\}$.

$\#(A) = 3, \#(B) = 2$.

Since the set B^A is consists of eight mappings, thus, $B^A = 2^3 = 8$.

Theorem 5.11 *Consider the set A, if $\#(A) = \alpha$, then $\#(P(A)) = 2^{\alpha}$.*

Proof It is proved previously, there is a bijective between $P(A)$ and 2^A; where 2 is a symbol for a set consists of two elements.

$\therefore \#(P(A)) = \#(2^A) = 2^{\alpha}$. ♦

Note:

(i) If A is a finite set and consists of n of elements, then $P(A)$ consists of 2^n of elements. Theory 5.11 is the generalization of this case.

(ii) The Cantor theorem (Cantor, 1883b) states that $2^{\alpha} > \alpha$ for all cardinal number α.

(iii) $2^{\mathbb{N}_o} > \mathbb{N}_o$.

Theorem 5.12 $2^{\mathbb{N}_o} = C$.

Proof Based on the definition of the cardinal number, $2^{\mathbb{N}_o}$ is a cardinal number.

Now, for the set $2^{\mathbb{N}}$ where $2^{\mathbb{N}} = \{f | f : \mathbb{N} \to \{0, 1\}\}$.

Let $f : \mathbb{N} \to \{0, 1\}$ be a mapping.

We can express $f(n) = f_n \ni (f_n = 0 \vee f_n = 1)$.

For all mapping f_i determined by $\{f_1, f_2, ...\}$ where $f_1 = (0 \vee 1)$

Each sequence associated with a real number $\sum_n \frac{f_n}{2^n}$.

Or, the real number its binary expansion is $0.f_1.f_2.f_3.....$

Now, there exists an infinite uniqueness binary expansion for every real number in the interval $(0, 1]$ in which just a countable set has a finite binary expansion.

$\therefore 2^{\mathbb{N}_o} = C + \mathbb{N}_o = C$. ♦

Note:

(i) If n is a finite cardinal number, then $n^{\mathbb{N}_o} = C$.

(ii) The Continuum Hypothesis (Cantor, 1883b; Cantor, 1878; Gödel, 1947) states that there is not a cardinal number α such that $\mathbb{N}_o < \alpha < 2^{\mathbb{N}_o}$.

(iii) The generalization of the Continuum Hypothesis (Gödel, 1938; Shelah, 2000) states that there dose not exists a cardinal number β such that $\alpha < \beta < 2^{\alpha}$.

5.6 Exercises

Answer the following questions:

Q1: Prove that $\mathbb{N}_o + \alpha = \alpha$, for all the cardinal number α.

Q2: Consider a cardinal numbers α, β, such that $\alpha \leq \beta$. For any cardinal number γ prove that;

(i) $\alpha^{\gamma} \leq \beta^{\gamma}$.

(ii) $\gamma^{\alpha} \leq \gamma^{\beta}$.

(iii) $\alpha + \gamma \leq \beta + \gamma$.

(iv) $\alpha\gamma \leq \beta\gamma$.

Q3: Prove that $\#(T) = C$, where T is the set of transcendental real numbers.

Q4: Let each of α, β, γ be a cardinal number. Prove that

(i) $\alpha\beta = 0 \leftrightarrow \alpha = 0 \vee \beta = 0$.

(ii) $\alpha\beta = 1 \leftrightarrow \alpha = 1 \wedge \beta = 1$.

Q5: For each of a cardinal number α, β, prove that $\alpha \leq \beta \leftrightarrow \exists \gamma \ni \beta = \alpha + \gamma$.

Q6: Consider the cardinal numbers $\alpha, \beta, \gamma, \delta$, such that $\alpha \leq \gamma, \beta \leq \delta$. Prove that

(i) $\alpha + \beta \leq \gamma + \delta$.

(ii) $\alpha\beta \leq \gamma\delta$.

(iii) $\alpha^{\beta} \leq \gamma^{\delta}$.

Q7: If α be an infinite cardinal number, then $\alpha\alpha = \alpha$.

Q8: Consider a cardinal numbers α, β, γ, prove that

(i) $\alpha\beta < \alpha\gamma \rightarrow \beta < \gamma$.

(ii) $\alpha + \beta \leq \alpha + \gamma \rightarrow \beta < \gamma$.

(iii) $\alpha + \alpha = \alpha + \beta \rightarrow \alpha \geq \beta$.

(iv) $\alpha \leq \beta \rightarrow \alpha^{\beta} = 2^{\beta}$.

Q9: Evaluate $\mathbb{N}_o! = 1.2.3....\mathbb{N}_o$.

Q10: Prove the Konig's theorem (Rubin and Rubin, 1985; Holz et al., 2010; König, 1905) If $\alpha_\lambda < \alpha_\lambda, \forall \lambda$, then $\sum_\lambda \alpha_\lambda < \prod_\lambda \beta_\lambda$.

Q11: Find $C^{\mathbb{N}_o}$.

Q12: Let each of α, β be an infinite cardinal number, prove that $\alpha + \beta = \alpha\beta \max\{\alpha, \beta\}$.

5.7 Ordinal Numbers

When dealing with ordered sets, the concept of the potency of sets is insufficient because it depends on the sets only and has nothing to do with their order.

In this section, we will discuss and deal with the ordinal numbers that refer to the order of elements of the sets. These numbers have an important role in topology.

Definition 5.11 Let each of A, B be a partial ordered set, A, B said to be similar if and only if there exists isomorphism mapping $f : A \to B$, and expressed by the symbol $A \simeq B$, and f is called similarity (Awodey, 2010; Vinberg, 2003).

Note:

(i) The expression $A \not\simeq B$ means that the set A is not similarity to the set B.

(ii) The relation $\simeq$ is an equivalence of the partial ordered sets. Accordingly, the gathering of the partially ordered sets divided into equivalence classes.

Definition 5.12 The totally ordered sets in the same equivalence classes are said to have the same order type (Ciesielski et al., 1997; Dauben, 1990).

Note:

(i) The similarity sets are potency sets. The order type sets are the cardinal numbers, but vice versa is not true.

(ii) It is clear from the above definition that the order type set is totally ordered set, which is just an abstract concept. We denote to the type order set A by the symbol $\prod(A)$.

(iii) Assume that the sets A, B are totally finite ordered then: $\#(A) = \#(B) \leftrightarrow \prod(A) = \prod(B)$.

Example 5.9 Assume that $M = \{1, 2, 3, ...\}, M^\star = \{..., 3, 2, 1\}$. It should be noted that $M \sim M^\star$, but $M \simeq M^\star$ because the set M has the first element, but the set $M^\star$ has no the first element.

Notation:

(i) The order type of $\mathbb{N}$ associated with its usual ordering denoted by the symbol W which is the order type for $\mathbb{N}$. The $\mathbb{Q}$ with its usual order denoted by η. The $\mathbb{R}$ with its usual order denoted by λ.

(ii) With respect to the finite sets, the concepts of the potency and the similarity have the same meaning. Thus, ordering of a set consists of n elements, denoted by the symbol n.

(iii) Let A be an ordered set of α shape. The $\alpha^\star$ is denoted to ordered shape $A^\star$, where $A^\star$ is the same A with the inverse order.

5.7.1 Ordinal on the Ordinal Patterns

Definition 5.13 Let each of α, β be an ordinal patterns, it said that $\alpha \leq \beta$ if and only if $A \simeq B_1$, where $B_1 \subseteq B$, α is a pattern to A and β is a pattern to B (Hamilton, 1982; Conway and Guy, 2012).

Note: The relation $\leq$ is a partial ordered relation, but it is not totally ordered relation on set of the ordinal patterns.

5.7.2 Addition on the Ordinal Patterns

Definition 5.14 Let each of α, β be an ordinal patterns, the summation $\alpha + \beta$ is the ordinal pattern for the set $\{A, B\}$, such that $A \cap B = \phi$, and ϕ is the ordinal pattern to A and β is the ordinal pattern to B. And $\{A, B\}$ is the set $A \cup B$ in which ordered based on that all element in A is precedes an element in B, provides that elements in A or in B are ordered according to their order in A or in B On symmetrically. (Hamilton, 1982; Conway and Guy, 2012; Mustafa et al., 1980).

Note: If $\prod(A) = \alpha, \prod(B) = \beta, A \cap B = \phi$. Thus, based on theorem of the standard substitution theorem, we can substitute each of A, B by $A^{\star}, B^{\star}$ respectively, such that $\alpha + \beta = \prod \{A^{\star}, B^{\star}\}$.

Example 5.10 $1 + W$ is the ordinal pattern for the set $\mathbb{N} = \{-1, 0, 1, 2, 3, ...\}$. $\therefore 1 + W = W$. While $W + 1$ is the ordinal pattern for the set $T = \{0, 1, 2, 3, ..., -1\}$.

Note that $T \not\simeq \mathbb{N} \rightarrow W + 1 \neq W$
$\therefore 1 + W \neq W + 1$.

(i) The addition operation is not a commutative. For example, $W + 1 \neq 1 + W$.

(ii) The association property for the addition operation is hold. Or, $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma)$, where α, β, γ are ordinal patterns.

(iii) Generally, $n + W = W$. But, $W + n \neq W$ because if $T = \{n + 1, n + 2, ..., 1, 2, 3, ..., n\}$, then $T \simeq W$ where n is a finite cardinal number.

(iv) The ordinal pattern of the open interval (a, b) is equal to the ordinal pattern of $\mathbb{R}$(or equal to λ).

(v) The half-closed interval $[a, b)$ has ordinal pattern equal to $1 + \lambda$, while the closed interval $[a, b]$ has ordinal pattern equal to $1+\lambda+1$.

5.7.3 Multiplication on the Ordinal Patterns

Definition 5.15 Let each of α, β be an ordinal patterns, the multiplication of them $\alpha\beta$ is the ordinal pattern for the set $B \times A$ in addition to lexicographic ordering, α is the ordinal pattern for the set A and β is the ordinal pattern for the set B. The lexicographic ordering is $(x_1, x_2) \leq (y_1, y_2)$ if and only if $x_1 < y_1$, or $x_1 = y_1 \wedge x_2 \leq y_2$. Knowing that $\alpha\beta$ is the ordered pattern for the ordered set $A \times B$, in addition to anti-lexicographic ordering. (Ciesielski et al., 1997; Dauben, 1990; Moore, 2012; Rubin, 1967; Suppes, 1960).

Example 5.11 $2W$ is the ordinal pattern for the set $S = \{(0,a),(0,b),(1,a),(1,b),(2,a),(2,b);...\}$ where W is the ordinal pattern for $\mathbb{N}$, and 2 is the ordinal pattern for the set $\{a,b\}$. While $W2$ is the ordinal pattern $H = \{(a,o),(a,1),(a,2),...;(b,o),(b,1),(b,2),\}$. It should be noted that the set H has ordinal pattern $W+W$, or $W2 = W+W$, but $2W = W$.

Note:

(i) The multiplication operation is not a commutative. For example, $W2 \neq 2W$.

(ii) Generally, $\alpha 2 = \alpha + \alpha$ for any ordinal pattern α.

(iii) The association property for the multiplication operation is hold. Or, $\alpha(\beta\gamma) = (\alpha\beta)\gamma)$ where α, β, γ are ordinal patterns.

(iv) The left distribution law is valid. Or, $\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$ for any ordinal pattern α, β, γ. But, the right distribution law is not valid. Or, $(\alpha+\beta)\gamma \neq \alpha\gamma + \beta\gamma$. For example,

$$\begin{aligned}(W+1)2 &= (W+1)+(W+1)\\ &= W+(1+W)+1\\ &= W+W+1\\ &= W2+1\\ &\neq W2+2.\end{aligned}$$

(v) $W^2 = W.W = W+W+W+...$ where W^2 is the ordinal pattern for $K = \left\{1,2,3,...;\frac{1}{2},\frac{3}{2},\frac{5}{2},...;\frac{1}{3},\frac{2}{3},\frac{4}{3},...;...;...\right\}$. It should be noted that $K = \mathbb{Q}^+$.

Definition 5.16 The ordinal pattern of a well ordered set is called ordinal number, and the ordinal number for the totally ordered set A denoted by the symbol $Ord(A)$ (Bancerek, 1989; Kleene, 1938; Mustafa et al., 1980).

Note:

(i) Let each of A, B be well ordered sets, The sets $\{A, B\}$, $B \times A$ are well ordered sets too. Thus, the addition and multiplication of the ordered sets are well ordered sets.

(ii) Any ordinal pattern set of type W_n(n is a finite number) will be well ordered set. But, the sets of the ordinal pattern $W^\star, n, \lambda$ will be not totally ordered set.

(iii) Let each of α, β be an ordinal number, $\alpha < \beta$ if and only if the set A similarities to an initial segment of B. Where A is a well ordered set with an ordinal number α, and Where B is a well ordered set with an ordinal number β.

Theorem 5.13 *The set of ordinal numbers is totally ordered by the relation* $\leq$.

Proof Let each of α, β be ordinal numbers. We need to prove that either $\alpha \leq \beta$ or $\beta \leq \alpha$.

Let each of A, B be well ordered set, such that $Ord(A) = \alpha, Ord(B) = \beta$. Now, based on Cantor's theorem:

Either A is similarity to B, or A is similarity to an initial segment of B, or B is similarity to an initial segment of A.

That means that $\alpha = \beta \vee \alpha < \beta \vee \beta < \alpha$.

Thus, $\alpha \leq \beta \vee \beta \leq \alpha$. ⧫

Corollary *Every set of the ordinal numbers is well ordered.*

Proof Assume that T is set of the ordinal numbers in which not totally well ordered.

Therefore, there is a subset of T has no least element.

Since, T is totally ordered set, so we can form a sequence of ordinal numbers $\{\alpha_n\}_{n\in\mathbb{N}}$, such that $\alpha_1 > \alpha_2 > \alpha_3 > ....$

Let A be totally ordered and its ordinal number be α_1.

Therefore, there are initial segments of A:

$Sa_2, Sa_3, Sa_4, ...,$ where their ordinal numbers are $\alpha_2, \alpha_3, \alpha_4, ...,$ respectively.

That means $a_2 > a_3 > a_4 > ....$

Or, the subset $K = \{..., a_4, a_3, a_2\} \subseteq A$ has no least element, and this is contradiction because A is totally ordered set.

Thus, T is totally ordered set. ♦

Notation: The symbol W denoted to the set of ordinal numbers in which less than the ordinal number α.

Theorem 5.14 *Every ordinal number α is the ordinal pattern for the set W_α.*

Proof Let A be a set that has the ordinal number α.

For all ordinal number $\beta, \beta < \alpha$ corresponded by an initial segment S_b of A.

On the other hand, $\forall b \in A$ means an initial segment S_b in which has ordinal number $\beta, \beta < \alpha$.

$\therefore$ there is a corresponding between W_α, A.

The corresponding is an isomorphism because;

$\alpha_1 \leq \alpha_2 \leftrightarrow S_{b1} \subseteq S_{b2}$.

$\therefore A \simeq W_\alpha$. ♦

Theorem 5.15 *For all cardinal numbers a, b, either $a \leq b$, or $b \leq a$.*

Proof Associating with every ordinal number α, connecting an certain cardinal number (The cardinal number of W_α).

According to the well ordered theorem, connected with every cardinal number a nonempty set consists of the ordinal numbers in which have that cardinal number.

Since all the ordinal numbers in which well ordered, there is a unique first ordinal number. Thus, we have connected with all cardinal number a a unique ordinal number, and called initial ordinal of a.

So as, with all cardinal number b connected an initial ordinal number $\alpha(b)$.

Let each of A, B be well ordered sets, such that;

The ordinal number of A is $\alpha(a)$, and the ordinal number of B is $\alpha(b)$.

$\therefore \#(A) = a, \#(B) = b$.

Now, it should be noted that the well ordered sets are comparable. Or, anyone of them is similar for a subset of others. But the similar sets are the potency sets.

Therefore, A is equipotent set with a subset of B, or B is equipotent set with a subset of A.

Thus, either $a \leq b$, or $b \leq a$. ♦

5.8 Exercises

Answer the following questions:

Q1: Consider the ordinal patterns α, β, γ, then;

(i) $(\alpha + \beta)^\star = \beta^\star + \alpha^\star$.

(ii) $(\alpha.\beta)^\star = \beta^\star.\alpha^\star$.

Q2: Prove all that comes;

(i) $n^\star = n, \lambda^\star = \lambda$.

(ii) $n + n = n$.

(iii) $\lambda + \lambda \neq \lambda$.

(iv) $n + 1 + n = n$.

(v) $\lambda + 1 + \lambda = \lambda$.

Q3: If $m \neq n$, then prove that;

(i) $W + m \neq W + n$.

(ii) $m + W^\star \neq n + W^\star$.

Q4: Prove that; $(1 + \lambda)W = 1 + \lambda$.

Q5: Prove that all infinite well ordered set contains a subset with W of ordinal numbers.

Q6: Prove that the set A is well ordered if and only if it does not contains any subset with ordinal pattern $W^\star$.

Q6: Prove that if σ is ordinal number, then $\sigma < \sigma + 1$.

5.9 Paradoxes

There are negatives and disadvantages in the intuitive set theory in which in which they lead to contradictions. It is crucial to note that, we assumed that any collection of things may be called a set. For example, we expect there is a so-called set of all cardinal numbers or the ordinal numbers, but this leads to the following contradictions.

5.9.1 Bovali-Forti Paradox

Let X be the set of all the ordinal numbers, so X is totally ordered, and its ordinal pattern (say α) ordinal number. Thus, $\alpha \in X$.

In fact, α ia an ordinal pattern for $W_\alpha = S_\alpha \subseteq X$, where $S_\alpha = \{\beta | \beta < \alpha\}$. So, α will be ordinal pattern for the sets X, S_α, and this is a clear paradox, because the well ordered set is not a similar to any its initial segment (Burali-Forti, 1897; Copi, 1958; Moore and Garciadiego, 1981; Rosser, 1942).

Note: The paradox above is not the only one of its kind, especially if we are exposed to the concepts of the Theory of Intuitive Sets. Russell (1980) is the first who pointed out the paradox, where he explained that we get paradox when talking to the set of all sets.

Definition 5.17 A set that is an element in itself is called an abnormal set. Mathematically, let A be a set, then A is an abnormal set if and only if $A \in A$. That is A is an element of itself. Otherwise, it is called a normal set (Simmons and Hammitt, 1963).

5.9.2 Russell Paradox

Let $\mathcal{U} = \{B_\alpha | \alpha \in \gamma, B_\alpha \in B_\alpha\}$. The set $\mathcal{U}$ is either a normal or abnormal set.

(i) If it is abnormal set, then $\mathcal{U} \in \mathcal{U}$. But, based on the definition of $\mathcal{U}, \mathcal{U} \notin \mathcal{U}$, we get on paradox.

(ii) Assume that $\mathcal{U}$ is normal set, then $\mathcal{U} \notin \mathcal{U}$. But, $\mathcal{U}$ is a set of all the natural sets. Thus, $\mathcal{U}$ (considering out of the set $\mathcal{U}$) should be abnormal set, and a gain we get on paradox (Russell, 1980; Simmons and Hammitt, 1963)

5.9.3 Cantor Paradox

If A be a set, then $\#(P(A)) > \#(A)$. We denote a set of all sets in nature by the symbol $\mathcal{Y}$. Now, $P(\mathcal{Y}) \subseteq \mathcal{Y}$, it implies that $\#(P(\mathcal{Y})) \leq \#(\mathcal{Y})$. And, this is a paradox (Cantor, 1883b; Cantor, 1883a; Cantor, 1899; Broad, 1916; Menzel, 1984).

Note: Gödel (1938) proved that there is no paradox or contradiction in the different axioms in the set theory. Later, in the mid of 1960s, Cohen (1964) proved the independence of those axioms.

6

The Natural Numbers

6.1 Introduction

Number is a fundamental concept in mathematics and it is an effective tool in scientific and practical studies. There is a difference between the numerical sense and the number itself. The numerical sense is a common property among organisms while operations on numbers involve complex mental processes. Thus, operations on numbers are related to humans exclusively.

Comparison of sets is the primitive and optimal method to determine the elements of sets in which someone takes and specifies a typical set to compares it to other sets to determine their elements. The matter becomes easier if we add the ordinal property of sets, where we arrange sets ordinally and sequentially where the first set does not contain any element, the second contains just one element, the third contains two elements and so on. In other words, every set is a subset of the next set that has one extra element.

It should be given names and symbols to such sets and typical sets, for example, zero, one, two, three, ... and so on, in which denoted by symbols $0, 1, 2, 3, ...$

It should be noted the natural numbers ($\mathbb{N}$) consists of the ideas cardinal number and ordinal number. For example the set consists of 5 numbers, its cardinal numbers is 5, while its ordinal numbers are first, second, third, fourth, and fifth. Or, the number that is determined relative to others in the series of the natural numbers.

The mathematical accuracy drives us to insert axiom of infinity which states of a successor set. Or the set contains on $X \cup \{X\}$ whenever contains of X. The intersection of all the successor sets is the set of the natural numbers ($\mathbb{N}$). In what follows we are going to the state of Peano's axioms and proof of them. In addition to the addition and multiplication operations on $\mathbb{N}$, and defining on the ordinal relation on it.

6.2 Natural Numbers and Peano's Axioms

In the 19th century, Italian mathematician Giuseppe Peano (Peano, 1967) presented axioms in mathematical logic, known as Peano axioms, or the Dedekind–Peano axioms or the Peano postulates. These axioms including research into fundamental questions of whether number theory is consistent and complete.

In the 1860s, Grassmann (1861) proved that many facts in arithmetic could be derived from more basic facts about the successor operation and induction. And a year later, Peirce (1881) provided an axiomatization of natural-number arithmetic. In 1888 Richard Dedekind (Ferreirós, 2005) proposed another axiomatization of natural number arithmetic. Finally, in 1889 Peano (1967) published a simplified version collection of axioms on natural numbers.

Definition 6.1 Based on some researchers (Tarski and Givant, 1987; Patrick, 1960; Kroon, 1986), we can define the following definition.

Let $0 = \phi$. Now, we define that 1 is the set that contains of just one element. Thus it can be expressed as:

$1 = \{0\}$

And in the same manner we can define:

$2 = \{0, 1\}$

$3 = \{0, 1, 2\}$

$4 = \{0, 1, 2, 3\}$

.

.

.

Thus, $0 = \phi$, $1 = \{\phi\}$, $2 = \{\phi, \{\phi\}\}$, $3 = \{\phi, \{\phi\}, \{\phi, \{\phi\}\}\}$... etc.

Definition 6.2 Consider a set A. The successor of A defined $A^+ = A \cup \{A\}$, where A^+ is the successor of A (Halmos, 2017b; Takeuti and Zaring, 2013).

Note: We can define the numbers $0, 1, 2, 3, ...$ via successor in more precisely concept, as follows

$0 = \phi$

$1 = \{0\} = \{\phi\} = \{\phi\} \cup \phi = \phi^+ = 0^+$.

$2 = \{0, 1\} = \{0\} \cup \{1\} = 1 \cup \{1\} = 1^+$.

$3 = 2^+$.

$4 = 3^+$.

.

.

.

etc.

6.2.1 Axiom of Infinity

The axiom of infinity is one of the axioms of Zermelo–Fraenkel set theory (Zermelo, 1908; Zermelo, 1930a; Zermelo, 1930b). It emphasizes that the existence of at least one infinite set namely a set containing the natural numbers. It was first published by Zermelo (1908) as part of his set theory in 1908. The axiom states:

There exists a successor set.

Before proceeding to the definition of the set of natural numbers, we must understand these two facts:

(i) The family of all successor sets is nonempty.

(ii) The intersection of any nonempty successor sets is a successor set.

Definition 6.3 The intesection of all successor sets is called the set of natural numbers denoted by $\mathbb{N}$, and any element belongs to it, called a number of $\mathbb{N}$ (Carothers, 2000; Bancerek, 1990; Grassmann, 1861).

Note: Based on the axiom of extension, we conclude that there is a unique successor set of another successor set (Halmos, 2017b).

6.2.2 Peano's Axioms

Here, we are going to prove the natural numbers satisfy five properties, called Peano axioms (Grassmann, 1861; Peirce, 1881; Van, 1967; Peano, 1967). Or, the natural numbers could defined based on these axioms. In other words, these axioms could be utilized to define the natural numbers.

The Peano's axioms for the natural numbers states as follows

$$
\begin{aligned}
&P_1 : 0 \in \mathbb{N}, \\
&P_2 : n \in \mathbb{N} \to n^+ \in \mathbb{N}, \\
&P_3 : n^+ \neq 0, \forall n \in \mathbb{N}, \\
&P_4 : \text{If } X \subseteq \mathbb{N} \text{ and } X \text{ is a successor set then } X = \mathbb{N}, \\
&P_5 : [(n, m \in \mathbb{N}) \wedge (n^+ = m^+)] \to n = m.
\end{aligned}
$$

Note:

(1) The statement P_4 called the mathematical induction (Bather, 1994).

(2) By assuming the infinity axiom, Peano's axioms converted to theorems, and could be proved (Kapur et al., 1986), as in the following section.

6.2.3 Proof of Peano's Axioms

Proof We are going to prove Peano's axioms based on the scientific contributions of Peano (1889) and some other eminent scholars (Zermelo, 1908; Zermelo, 1930a; Zermelo, 1930b; Carothers, 2000; Bancerek, 1990; Grassmann, 1861; Halmos, 2017b; Peirce, 1881; Van, 1967; Peano, 1967; Bather, 1994; Kapur et al., 1986), as mentioned them before.

P_1, P_2 can be proved from the definition of $\mathbb{N}$ directly. Now, we have to prove P_3.

From the definition, we have;

$n^+ = n \cup \{n\}$, thus, $n \in n^+, \forall n$.

Assume that 0 is a ϕ implies that $0 \neq n^+, \forall n$ [If $0 = n^+ \to n \in 0$ and this is contraction].

To prove P_4, we have to put the following two conditions:

(i) $0 \in X$,

(ii) $n \in X \to n^+ \in X$. Or, X is a successor set.

But, from the definition of $\mathbb{N}$, it is noted that $\mathbb{N}$ is a subset of all successor set.

$\therefore \mathbb{N} \subseteq X$.

But, $X \subseteq \mathbb{N}$ [From the definition of $\mathbb{N}$].

$\therefore X = \mathbb{N}$.

6.2.4 Introductory Theorem

Theorem 6.1 *For all $n \in \mathbb{N}$, if $x \in n$ then $x \subseteq n$.*

Proof Let us assume the following set:

$X = \{n \in \mathbb{N} | \forall x(x \in n \to x \subseteq n)\}$. now, it should be noted that:

(i) $0 \in X$ because if $0 \notin X$ that means $\exists y \in 0 \ni y \nsubseteq 0$. But this is contradiction because $0 = \phi$.

(ii) $n \in X \to n^+ \in X$.

Because if $m \in n^+$ where $n^+ = n \cup \{n\}$. $\therefore (m = n) \vee (m \in n)$.

If $m \in n$ then $m \subseteq n$, because $n \in X$ as assumed before.

On the other hand, we have $n \subseteq n^+$ and it implies $m \subseteq n^+$.

If $m = n \to m \in n^+$ because $n \in n^=$.

Thus, from (i) & (ii), we obtain $m \in n \to n^+$.

$\therefore n^+ \in X$.

Now, by utilizing P_4 we get $X = \mathbb{N}$. Or, for all $n \in X$, then $x \in n \to x \subseteq n$ (Peano, 1967) ♦.

6.2.5 Proof of Fifth Axiom of Peano's Axioms

In this section, we use the proofs of 6.1.4 in addition to 6.1.5 to proof P_5.

Assume that $n^+ = m^+$.

Now, $n^+ = m^+ \wedge n \in n^+ \to n \in m^+$.

Thus, $(n \in m) \vee (n = m)$.

If $n = m$ then the axiom is proved.

Now, assume that $(m \in n) \wedge (n \in m)$, and by using the Introductory theorem in 6.1.4, we get $(m \subseteq n) \wedge (n \subseteq m)$.

$\therefore n = m$.

Thus, we proved that the set $\mathbb{N}$ satisfies Peano's Axioms.

6.3 Exercises

Answer the following questions:

Q1: Assume that each of A and B are sets. Prove that if $A = B \to A^{\#} = B^{\#}$.

Q2: For all $n \in \mathbb{N}$, prove that $n \notin n$.

Q3: Use the mathematical induction to prove;

(1) $(A \in n) \wedge (n \in \mathbb{N}) \to A \in \mathbb{N}$. (2) $n \in \mathbb{N} \to (n = 0) \vee (n = m^+), m \in \mathbb{N}$.

Q4: Prove that if $A^+ \in \mathbb{N} \to A \in \mathbb{N}$

6.4 Arithmetic of $\mathbb{N}$

Before defining addition and multiplying of $\mathbb{N}$. We need to state and proof Recursion theorem (Kjos-Hanssen et al., 2011; Rogers, 1987; Kirby and Paris, 1982) as follows:

Theorem 6.2 *Let $a \in X$, and consider a mapping $f : X \to X$. Then, there is a unique function $\alpha : \mathbb{N} \to X$, such that; $\alpha(n^+) = f(\alpha(n)), \alpha(0) = a, \forall n \in \mathbb{N}$.*

Proof Let $\{F = A \subseteq \mathbb{N} \times X | (0, a) \in A \wedge (n_1, x) \in A \rightarrow (n^+, f(x)) \in A\}$
Since $\mathbb{N} \times X \in F$ thereby $F \neq \phi$.
Thus, $\alpha = \bigcap_{A \in F} A$.
Obviously, $\alpha \in F$. Now, we have to prove $\alpha : \mathbb{N} \rightarrow X$ is a mapping.

(i) We prove by mathematical induction.

$((n, x) \in \alpha \wedge (n, y) \in \alpha) \rightarrow x = y$

Assume that $S = \{n \in \mathbb{N} | ((n, x) \in \alpha \wedge (n, y) \in \alpha) \rightarrow x = y\}$.

(a) $0 \in S$, because if $0 \notin S \rightarrow (0, b) \in \alpha \ni b \neq a$.
Let $\beta = \alpha - \{(0, b)\}$. It is noted that $\beta \in F$ and this is contradiction because α is a smallest set in F.
$\therefore 0 \in S$.

(b) Assume that $n \in S$
$\therefore \exists!\ x \in X \ni (n, x) \in \alpha$.
$\therefore (n^+, f(x)) \in \alpha$.
If $n^+ \notin S$ then $(n^+, y) \in \alpha \ni y \neq f(x)$.
Assume that $\gamma = \alpha - \{(n^+, y)\}$.
It is noted that, $(0, a) \in \gamma$, because $n^+ \neq 0$.
Also, $(m, t) \in \gamma \rightarrow (m^+, f(t)) \in \gamma$
$\therefore \gamma \in F$, and this is contradiction because α is the smallest set in F.
$\therefore n^+ \in S$.
Thus, $\mathbb{N} = S$.

(ii) By mathematical induction, We prove that $dom\ \alpha = \mathbb{N}$

(a) Since $(0, a) \in \alpha \rightarrow 0 \in dom\ \alpha$.

(b) Suppose that $n \in dom\ \alpha$.
$\therefore \exists x \in X \ni (n, x) \in \alpha$
$\therefore (n^+, f(x)) \in \alpha \rightarrow n^+ \in dom\ \alpha$.
$\therefore dom\ \alpha = \mathbb{N}$.

Thus, we have proved that $\alpha : \mathbb{N} \to X$ is a mapping. The prove of that this mapping is a unique has been left for a reader as an exercise. ♦

Example 6.1 (1) Let $C \neq 1$, and $f : \mathbb{R} \to \mathbb{R}$ be a mapping such that $f(x) = xC \ \forall x \in \mathbb{R}$.

We define $\alpha : \mathbb{N} \to \mathbb{R}$, such that $\alpha(n) = C^n$.

Note that $\alpha(0) = C^0 = 1$, and $\alpha(n^+) = f(\alpha(n)) = f(C^n) = C^nC$.

Or, $C^{n+1} = C^nC, \forall n \in \mathbb{N}$. And this is the definition of the mathematical induction.

(2) Consider the mapping $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x^2$. Defining $\alpha : \mathbb{N} \to \mathbb{R}$ in which;

(i). $\alpha(0) = 2$. (ii). $\alpha(n+1) = f(\alpha(n)) = (\alpha(n))^2$.

It is clear that from the induction definition;

$\alpha(1)) = (\alpha(0))^2 = 2^2 = 2^{2^1}$,

$\alpha(2)) = (\alpha(1))^2 = (2^2)^2 = 2^{2^2}$,

$\alpha(3)) = (\alpha(2))^2 = 2^{2^2} = 2^{2^3}$,

.

.

. ect.

Thus, we saw how the mathematical induction employed as a method of proof.

6.4.1 Addition of $\mathbb{N}$

Definition 6.4 For all $m \in \mathbb{N}$, and based on Recursion Theorem (Theorem 6.2), there existed a unique mapping as follows:

$\beta_m : \mathbb{N} \to \mathbb{N}$, such that

(1) $\beta_m(0) = m$. (2). $\beta_m(n^+) = (\beta_m(n))^+$.

The addition of $\mathbb{N}$ can be defined as follows;

$m + n = \beta_m(n), \forall m, n \in \mathbb{N}$.

Or, (1) $m + 0 = m$. (2) $m + n^+ = (m + n)^+$.

We list some addition properties of $\mathbb{N}$ in the next sections.

Theorem 6.3 $n^+ = 1 + n, \forall n \in \mathbb{N}$, *where* $0^+ = 1$ *by definition.*

Proof We will prove this theorem by mathematical induction on n.

(i) If $n = 0 \to 0^+ = 1 = 1 + 0$. Thereby the theorem is true for $n = 0$.

(ii) Assume that the theorem is true for n.

(iii) Now, we have to prove it is true for n^+.

now, $(1 + n)^+ = 1 + n^+ = (n^+)$[By induction axiom].

$\therefore$ the theorem is trur for n^+.

Thus, the theorem is true $\forall n \in \mathbb{N}$. ♦

Theorem 6.4 $n = 0 + n, \forall n \in \mathbb{N}$.

Proof Assume that $X = \{n \in \mathbb{N} |\ 0 + n = n\}$

(i). Now, $0 + 0 = 0 \to 0 \in X$.

(ii). Suppose that $n \in X$

$\therefore 0 + n = n$

Thereby $0 + n^+ = (0 + n)^+ = n^+$.

$\therefore n^+ \in X$.

According of P_4 we conclude that $X = \mathbb{N}$.

Or, $0 + n = n\ \forall n \in \mathbb{N}$. ♦

Theorem 6.5 (Associative Property)

$m + (n + k) = (m + n) + k, \forall\ m, n, k \in \mathbb{N}$.

Proof Let $L_m = \{n \in \mathbb{N} | m + n = n + m\}$.

Now, (i). $0 \in L_m$. (ii). Suppose that $n \in L_m$.

$\therefore m + n = n + m$.

Now, $m+n^+ = (m+n)^+ = (n+m)^+ = 1+(n+m) = (1+n)+m = n^+ + m$

$\therefore n^+ \in L_m$.

According on P_4, we get $L_m = \mathbb{N}$.

Or, $n + m = m + n, \forall m, n \in \mathbb{N}$. ♦

6.4.2 Multiplication of $\mathbb{N}$

Definition 6.5 If $m \in \mathbb{N}$, according of the Recursion Theorem (Theorem 6.2), there is a unique mapping as follows;

$\gamma_m : \mathbb{N} \to \mathbb{N}$, such that:

(1) $\gamma_m(0) = 0$. (2) $\gamma_m(n^+) = \gamma_m(n) + m, \forall m, n \in \mathbb{N}$.
The multiplication on $\mathbb{N}$ can be defined as follows:
$\gamma_m(n) = mn, \forall m, n \in \mathbb{N}$.
Or, (1) $m0 = 0$. (2) $mn^+ = mn + m$.

We list some multiplication properties of $\mathbb{N}$ in the next sections.

Theorem 6.6 $0n = 0, \forall n \in \mathbb{N}$.

Proof Assume that $M = \{n \in \mathbb{N} | 0n = 0\}$.
Now, (i) $0 \in \mathbb{M}$ because $00 = 0$.
(ii) Assume that $n \in M$
$\therefore 0n = 0$.
Now, $0n^+ = 0n + 0 = 0n = 0$.
Thereby $n^+ \in \mathbb{N}$.
According of P_4, we conclude that $M = \mathbb{N}$.
Or, $0n = 0, \forall n \in \mathbb{N}$. ⧫

Theorem 6.7 $1n = n, \forall n \in \mathbb{N}$.

Proof Assume that $T = \{n \in \mathbb{N} | 1n = n\}$.
Now, (i) $0 \in \mathbb{T}$, because $10 = 0$.
(ii) Assume that $n \in T$
$\therefore 1n = n$.
Now, $1n^+ = 1n + 1 = n + 1 = 1 + n = n^+$.
Thereby $n^+ \in T$.
We conclude that $T = \mathbb{N}$.
Or, $1n = n, \forall n \in \mathbb{N}$. ⧫

Theorem 6.8 (Distribution Laws)
(1) $m(n + k) = mn + mk$.
(2) $(n + k)m = nm + nk$. $\forall m, n, k \in \mathbb{N}$.

Proof (1) It is left as an exercise.

(2) Assume that $L_{kn} = \{m \in \mathbb{N} | (n+k)m = nm + kn\}$.

(i) $0 \in L_{kn}$, because $(n+k)0 = n0 + k0 = 0 + 0 = 0$.

(ii) Let $m \in L_{kn}$

$\therefore (n+k)m = nm + km$.

Now, $(n+k)m^{+} = (n+k)m+n+k = nm+km+n+k = nm^{+}+km^{+}$.

$\therefore m^{+} \in L_{kn}$.

Now, according of P_4, we conclude that $L_{kn} = \mathbb{N}$.

Or, $(n+k)m = nm + km, \forall m, n, k \in \mathbb{N}$. ♦

Theorem 6.9 (Associative and Commutative Lows for Multiplication)

(1) $(mn)k = m(nk)$ (Associative Law for Multiplication).

(2) $mn = nm$ (Commutative Law for Multiplication). $\forall m, n, k \in \mathbb{N}$.

Proof (1) It is left as an exercise.

(2) Assume that $L_m = \{n \in \mathbb{N} | mn = nm\}$.

(i) $0 \in L_m$, because $m0 = 0m = 0$.

(2) Let $n \in L_m$

$\therefore mn = nm$.

Now, $mn^{+} = mn + m = nm + m = (n+1)m = n^{+}m$.

$\therefore n^{+} \in L_m$.

Now, according of P_4, we conclude that $L_m = \mathbb{N}$.

Or, $mn = nm, \forall m, n \in \mathbb{N}$. ♦

6.5 Exercises

Solve the following Questions:

Q1: Consider a set A, let $C \in A$, and let $f : A \to A$ be an injective mapping such that $C \notin ranf$. Prove that, there exists a unique injective function $\gamma : \mathbb{N} \to A$ such that

(a) $\gamma(0) = C$. (b) $\gamma(n^{+}) = f(\gamma(n)), \forall n \in \mathbb{N}$.

Q2: Consider a set A, and let $f : A \to B$ be an injective mapping such that $B \subset A$. Prove that A contained of a subset D, such that there is a corresponding between D and $\mathbb{N}$.

Q3: Let A be a set that does not contains of big elements. Prove that there exists a strictly increasing sequences of A. Or, there exists a mapping $\gamma : \mathbb{N} \to A$, in which $\gamma(0) < \gamma(1) < \gamma(2) < ....$

Q4: For all $m, n, k \in \mathbb{N}$. Prove that

(a). If $m = n \to m + k = n + k$. (b). If $m = n \to mk = nk$.

Q5: Give an induction definition for m^n similarity to the definition of addition and multiplication of natural numbers satisfying the Recursion theorem. Then, prove that

(a) $m^{n+k} = m^n m^k$. (2) $(mn)^k = m^k n^k$. (3) $(m^n)^k = m^{nk}$.

6.6 Order on $\mathbb{N}$

In review of the $\mathbb{N}$s, researchers noted that the most important property, which is the order of it (Shilnikov, 1967; Schmidt, 1993; Davey and Priestley, 2002). It is noted that the natural number n is just a prenumbers of it in which $n = \{0, 1, ..., n-1\}$. Based on this we can say n is precedes m if n is an element of the set m. Thereby we set the following definition.

Definition 6.6 Let $m, n \in \mathbb{N}$, it is said that $m \leq n$ if and only if $m \in n \vee m = n$ (Feferman, 1964; Hamilton, 1982; Sierpiński, 1958).

Theorem 6.10 *The relation $\leq$ is a partial order relation on $\mathbb{N}$.*

Proof (1) $\forall m \in \mathbb{N}, m = m$.

$\therefore m \leq m$.

Thereby $\leq$ is the reflex relation on $\mathbb{N}$.

(2) Assume that $m \leq n \wedge n \leq m$.

$\therefore m = n \vee ((m \in n) \wedge (n \in m))$.

Or, $(m \subseteq n) \wedge (n \subseteq m)$.

Or, $n = m$.

Thus, $m = n$.

Thereby $\leq$ is the symmetric relation on $\mathbb{N}$.

(3) Assume that $m \leq n \wedge n \leq p$.

There are four cases;

(i) $m \in n \wedge n \in p$.

That means $m \in n \wedge mn \subseteq p$.

$\therefore m \in p$.

Or, $m \leq p$.

(ii) $m \in n \wedge m = p$.

$m \in p$.

Or, $m \leq p$.

(iii) $m = n \; wedgen \in p$.

$\therefore m \in p$.

Or, $m \leq p$.

(iv) $m = n \wedge n = p$. $\therefore m = p$.

Or, $m \leq p$.

$\therefore$ frome (i), (ii), (iii) & (iv) we conclude that $\leq$ is the transitive relation on $\mathbb{N}$.

From (1), (2) & (3) $\leq$ is the partial ordered relation on $\mathbb{N}$. ♦

Theorem 6.11 (Well Ordered Set)

$(\mathbb{N}, \leq)$ *is well ordered ($\mathbb{N}$ is well ordered set).*

Proof Before proving this theorem, we need to demonstrate the following facts:

(1) $0 \leq m, \forall m \in \mathbb{N}$.

Assume that $L = \{m \in \mathbb{N} | 0 \leq m\}$.

Obviously, $0 \in L$.

Let $m \in L$, this implies that $0 \leq m$.

$\forall m \in m^+$, or $m \leq m^+$.

$\therefore 0 \in m^+$, or $m^+ \in L$.

Thereby $m \in L \rightarrow m^+ \in L$.

Thus, according to P_4, we get that $L = \mathbb{N}$.

(2) If $n \leq m \rightarrow n^+ \leq m$.

Let $L_n = \{m \in \mathbb{N} | n \leq m \rightarrow n^+ \leq m\}$.

Obviously, $0 \in L_n$.

Assume that $m \in L_n$.

$\therefore n \leq m \rightarrow n^+ \leq m$.

Let $n < m^+ \rightarrow n \in m^+$.

This means that $n \in m^+ \vee n = m$.

If $n = m \rightarrow n^+ = m^+$. Thereby, $n^+ = m^+$.

If $n \in m \to n \leq m$.

now, based on the induction axiom we have $n^+ \leq m$, but $m < m^+$.

$\therefore n^+ \leq m^+$.

$\therefore n < m^+ \to n^+ \leq m^+$.

Or, $n^+ \in L_n$.

Thus, by P_4, $n < m \to n^+ \leq m, \forall n, m \in \mathbb{N}$.

Or, $L_n = \mathbb{N}$.

Now, we are ready to begin proving the theorem of the well ordered set.

Let $\phi \neq A \subseteq \mathbb{N}$, and assume that the set A does not consists of a least element.

Let $T = \{n \in \mathbb{N} | n \leq m, \forall m \in A\}$.

Based on (1) we conclude that $0 \in T$.

Now, assume that $n \in T$.

$\therefore n \leq m, \forall m \in A$, because if $n = a \ni a \in A \to a \leq m, \forall m \in A$.

Or, a is the least element in A, and we get contradiction.

$\therefore n < m, \forall m \in A$.

According of (2), we have $n^+ \leq m, \forall n \in A$.

Or, $n^+ \in T$.

Thereby, $n \in T \to n^+ T$.

Thus, based on P_4 we conclude that $T = \mathbb{N}$.

$\therefore T \cap A = \mathbb{N} \cap A = A$.

But, $T \cap A = \phi$, because A does not consistent of a least element.

$\therefore A = \phi$ and this is contradiction since $A \neq \phi$.

$\therefore A$ has a least element.

Or, $\mathbb{N}$ is well ordered set. ♦

Corollary

(i) **(Trichotomy Law)** $(\mathbb{N}, \leq)$ *totally ordered.*

(ii) **(Second Principle of Mathematical Induction)** *Let* $S \subset \mathbb{N}$ *such that* $(\{m | m \in \mathbb{N}, m < n\} \subseteq S) \to n \in S, \forall n \in \mathbb{N}$ *then* $S = \mathbb{N}$.

Proof

(i) If $m, n \in \mathbb{N} \to (n \leq m) \vee (m \leq n)$.

Or, $\forall m, n \in \mathbb{N} \to (m = n) \vee (m < n) \vee (n < m)$.

It is clear that just one of these relationships could be satisfied, and this is called Trichotomy Law.

(ii) Let $T = \{t | t \in \mathbb{N} - S\}$

Assume that $T \neq \phi$.

$\therefore T$ consistent of an least element n.

Let $m \in \mathbb{N} \ni m < n$.

$\therefore m \in S$.

Thereby, $\{m | m \in \mathbb{N}, m < n\} \subseteq S$.

Thus, and based on the axiom on S, we conclude that $n \in S$.

And this contradiction, because $n \in T$.

Thus, $T = \phi$. Or, $S = \mathbb{N}$. ♦

Theorem 6.12 *Let* $m, n \in \mathbb{N}$ *then* $m \leq n \to \exists p \in \mathbb{N} \ni m + p = n$

Proof It is left as an exercise . ♦

6.6.1 System of $\mathbb{N}$

Definition 6.7 The set $\mathbb{N}$ with the two operations addition and multiplication and the relation $\leq$ is called the algebraic system of the natural numbers, and denoted by $(\mathbb{N}, +, ., \leq)$ (Eves and Newsom, 1958; Eves, 1992; Ian and David, 2015; Wilder et al., 2012; Jech, 1977; Mustafa et al., 1980).

6.6.2 Weaknesses of $\mathbb{N}$

The system $(\mathbb{N}, +, ., \leq)$ has weaknesses, for example, the following system;

$\left.\begin{matrix} m+x=n \\ mx=n \end{matrix}\right\}$ $\forall m,n\in\mathbb{N}$ has no solution in the $\mathbb{N}$ in general. That why we are forced to extension the system $(\mathbb{N},+,.,\leq)$ to $(\mathbb{Z},+,.,\leq)$ to find solutions of the kind of $m+x=n$ in the next chapter.

6.7 Exercises

Solve the following questions:

Q1: Prove that $m<1\rightarrow m=0,\forall m\in\mathbb{N}$.

Q2: Prove that there is not a natural number k such that satisfies $m<k<m^+, m\in\mathbb{N}$.

Q3: prove that $n<k\rightarrow m+n<m+k, m,n,k\in\mathbb{N}$.

Q4: Prove that $m+n=m+k\rightarrow n=k, m,n,k\in\mathbb{N}$.

Q5: Consider $m,n,k\in\mathbb{N}$, show that (i) $((m<n)\wedge(k\neq 0))\rightarrow mk<nk$. (ii) $((mk=nk)\wedge(k\neq 0))\rightarrow m=n$.

Q6: Consider $m,n,k\in\mathbb{N}$, show that $m+k<n+k\rightarrow m<n$.

Q7: Prove that $((p=mn)\wedge m\neq 1)\rightarrow p>n,\forall p,m,n\in\mathbb{N}$.

6.8 Infinite Sets

Definition 6.8 A set A called a finite if it capable with a subset of $\mathbb{N}$ in the pattern of $\{0,1,2,...,m\}$,$\forall m\in\mathbb{N}$, in in this case $\#(A)=m$. Otherwise it called infinite set (Weisstein, 2000; Weisstein, 2002d; Cohen, 1964; Cohen, 2008; Quine, 1969; Monk, 1973a; Stoll, 1979).

Example 6.2 (1) $A=\{x,y,z,w\}$ is a finite set.

(2) $B=\{0,2,4,6,...\}$ is infinite set.

(3) $\mathbb{N},\mathbb{Z},\mathbb{R},\mathbb{Q},\mathbb{Z}_o,...$ are infinite sets.

Definition 6.9 The set A is countable if it is capable with $\mathbb{N}$. Also, we say that the set at mos countable if is countable or finite (Lang, 1993c; Rubin, 1967; Kamke, 1950).

Definition 6.10 The set A is discountable if it is at most not countable (Mustafa et al., 1980).

Example 6.3 The following are countable sets; (1) $\mathbb{N}_o$. (2) $\mathbb{Q}$. (1) Let the mapping $g : \mathbb{N} \to \mathbb{N}_o$, defined as: $g(n) = 2n + 1$.

Its easy to prove that g is bijective. thereby, from the definition of the countable set, we can confirm that the set $\mathbb{N}_o$ is countable. Similarly, we can prove that the set $\mathbb{N}_e$ is countable too.

(2) We prove this problem in the chapter of the rational numbers.

Theorem 6.13 (Introductory Theorem) *If A is the countable set, and let $x \in A$ then the set $A - \{x\}$.*

Proof $\because A$ is countable, $\therefore \ \exists f : \mathbb{N} \to A$.

Assume that $f(n) = x; n \in \mathbb{N}$.

Now, define the mapping $g : \mathbb{N} \to A$ as follows:

$$g(m) = \begin{cases} f(m); m < n \\ f(m+1); m \geq n \end{cases}$$

It is clear that $g : \mathbb{N} \to A - \{x\}$ is a bijective mapping.

Thereby, $A - \{x\}$ is a countable set. ♦

Theorem 6.14 *A set A is countable if and only if can numbering its elements by the natural numbers. Or, can express of A as a sequence of elements $A = (a_i, i \in \mathbb{N})$.*

Proof Assume that A is a countable set.

$\therefore \ \exists f : \mathbb{N} \to A$, provided that f is bijective mapping.

Now, $A = f(\mathbb{N} = \{f(0), f(1), ...\}$.

Let $f(0) = a_0, f(1) = a_1, ..., f(n) = a_n$.

$\therefore A = \{a_0, a_1, ...\}$.

Now, if we define the mapping $f : \mathbb{N} \to A$, such that $f(n) = a_n, n \in \mathbb{N}$.

Obviously, f is a bijective, thereby A is a countable set ...(1).

Conversely, suppose that $A = (a_i, i \in \mathbb{N})$.

$\therefore \exists f : \mathbb{N} \to A \ni f(n) = a_n, n \in \mathbb{N}$.

$\because A = \{a_i, i \in \mathbb{N}\}$.

$\therefore f(0) = a_0, f(1) = a_1, ...$

It is clear that f is bijective.

$\therefore A$ is countable ...(2).

From (1)& (2), we get the prove of the theorem . ♦

Theorem 6.15 (Introductory Theorem) *Let $n \in \mathbb{N}$, if n does not consists of a subset then it will be a countable.*

Proof (1) If $n = 0$, it will be clear that n does not consists of any element. Thereby, it will be a countable.

(2) Assume that the statement is true for n. Let n^+ consists of a countable subset, say S.

Now, if $n \notin S \rightarrow S \subset n$.

$\because n = \{0, 1, 2, ..., n-1\}$, and this is contradicts a hypothesis on n.

$\therefore n \notin S$. Thereby, $n \in S$.

Or, $S - \{n\} \subseteq n$ But, $S - \{n\}$ is a countable subset.

Again, we get contradiction on the hypothesis on n.

$\therefore n^+$ does not consists of a countable subset.

Thus, the statement is true of n^+.

Or, we proved that $\forall n \in \mathbb{N}$, n not consists of a countable subset.

♦

Theorem 6.16 *A set is infinite if and only if consists of a countable subset.*

Proof We prove the necessary condition by contrapositive. Or, if the set does not consists of a countable set it will be a finite.

Based on Zermelo (1904) in Chapter 3, the set A, can be arranged as a well ordered set. On the other hand, and based on Cantor (1883b) in Chapter 4, a unique case could be satisfied in the following situations;

(1) $\mathbb{N}$ is isomorphic with A.

(2) $\mathbb{N}$ is isomorphic with an initial segment of A.

(3) A is isomorphic with an initial segment of $\mathbb{N}$.

Since A does not contain a countable subset, hence (1) & (2) cannot be satisfied. Thereby, (3) could be investigated.

Or, A is equipotent with an initial segment of $\mathbb{N}$, and could be expressed as follows:

$S_n = \{m | m < n\} = \{0, 1, ..., n-1\} = n$.

Thus, A is a finite set ...(1).

Now, we have to prove the sufficient condition of the theorem.

Assume that A is contains of a countable subset, say B.

We prove this part by contradiction.

$\because A$ is a finite set, $\therefore A \sim n$.

But, $B \sim \mathbb{N} \wedge B \subseteq A$.

$\therefore$ we have the conditional mapping: $\mathbb{N} \to B \to A \to n$.

$\therefore$ we got an injective mapping from the above composite mappings: $g : \mathbb{N} \to n$.

$\therefore$ n is contains of a countable subset, and this is contradiction up on of Theorem 6.15 ...(2).

$\therefore$ from (1)& (2), A should be infinite set. ♦

Corollary

(i) *For all infinite cardinal number α, it will be $\mathbb{N}_o \leq \alpha$.*

(ii) *Any set consisted of an infinite subset is infinite.*

(iii) *Any subset of infinite set is infinite set.*

Proof (i) It is left as an exercise.

(ii) Let $B \subseteq A$, assume that B is infinite set.

Now, according to Theorem 6.14, B, it contains of a countable subset, say W.

Or, $W \subseteq B \subseteq A$.

Thus, A contains of a countable subset, and based on Theorem 6.14 A will be infinite set.

(iii) Let $B \subseteq A$, where A is finite set.

Now, if B is finite then A is infinite set.

Thus, based on (ii), we conclude that B is infinite. ♦

Theorem 6.17 *A set is infinite if and only if it is equipotent with its proper subset.*

Proof Suppose that A is an infinite set, thereby it contains of a subset B, such that $B = \{a_0, a_1, ...\}$.

Now, define a mapping $f : A \to A$, such that

$$f(x) = \begin{cases} x; x \in A - B \\ a_{m+1}; x = a_m, \forall m \in \mathbb{N} \end{cases}$$

Obviously, f is bijective between the set A and the proper subset of it $A - \{a_0\}$.

$\therefore A \sim A - \{a_0\}$

Assume that $g : A \to B, B \subset A$.

Let $C \in A - B$.

Now, and based on the Recursion Theorem, there exists a mapping:

$\gamma : \mathbb{N} \to A$, provided that

(1). $\gamma(0) = C$. (2). $\gamma(n^+) = g(\gamma(n))$.

Now, $C \in A - B, ran(g) = B$, thereby $C \notin ran(g)$.

We have to prove that γ is an injective function.

Or, $\gamma(m) = \gamma(n) \to m = n$.

We prove by mathematical induction on m.

(i) If $m = 0$.

If $n = 0$, the proof is covered, but if $n \neq 0 \to n = k^+, k \in \mathbb{N}$.

Thus, $C = \gamma(0) = \gamma(m) = \gamma(n) = \gamma(k^+) = g(\gamma(k))$.

But, this is impossible because $C \notin ran(g)$.

$\therefore n = 0 = m$.

(ii). Suppose that the statement is true for m, and assume that $\gamma(m^+) = \gamma(n)$.

If $n = 0 \to C = \gamma(0) = \gamma(m^+) = g(\gamma(m))$.

Again, impossible.

Thereby, $n \neq 0 \to n = k^+, k \in \mathbb{N}$.

Now, $\gamma(m^+) = \gamma(k^+)$.

Or, $g(\gamma(m)) = g(\gamma(k))$.

But, g is bijective, thereby $\gamma(m) = \gamma(k)$.

According to induction axiom, we get $m = k$.

Or, $m^+ = k^+n$.

Thus, we proved that γ is injective.

Now, $ran(g) \subseteq A$. It is clear $ran(g)$ is a countable subset.

Thus, based on Theorem 6.16, A should be infinite set. ♦

Theorem 6.18 *Every subset of a countable set is a finite or a countable (It is almost a countable).*

Proof Assume that A is a countable set.

$\therefore A = \{a_0, a_1, ...\}$.

Let $B \subseteq A$.

Now, there are two cases:

(i) If $B \neq \phi$ then B is a finite set. (ii) If $B \neq \phi$ then assume that a_{n_1} is the first element of the sequence $a_0, a_1, ... \ni a_{n_1} \in B$.

Again, assume that a_{n_2} is the first element after a_{n_1} of the sequence $a_0, a_1, ... \ni a_{n_2} \in B$.

Now, let us consider $B = \{a_{n_1}, a_{n_2}, ...\}$.

If the set $B^* = \{n_1, n_2, ...\}$ is bounded then the set B will be finite. And, if B^* is unbounded then B will be a countable. $\blacklozenge$

Theorem 6.19 $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

Proof elements of $\mathbb{N} \times \mathbb{N}$ can be arranged as a matrix as follows;

$$\begin{array}{ccccc}
\downarrow (0,0) & (0,1) & (0,2) & (0,3) & ... \\
(1,0) & (1,1) & (1,2) & (1,3) & ... \\
(2,0) & (2,1) & (2,2) & (2,3) & ... \\
(3,0) & (3,1) & (3,2) & (3,3) & ... \\
. & . & . & . & . \\
. & . & . & . & . \\
. & . & . & . & .
\end{array}$$

Or, $\mathbb{N} \times \mathbb{N} = \left\{ \begin{array}{c} (0,0), (1,0), (0,1), (2,0), (1,1), (0,2), \\ (3,0), (2,1), (1,2), (0,3), (4,0), (3,1), ... \end{array} \right\}$

$= \{a_0, a_1, a_2, a_3, ...\}$, where $a_1 = (0,0), a_1 = (1,0), a_2 = (0,1)$, $a_3 = (2,0), ...$

Or, the elements of $\mathbb{N} \times \mathbb{N}$ is enumerable.

Thereby, $\mathbb{N} \times \mathbb{N}$ is a countable.

Thus, $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$. $\blacklozenge$

Theorem 6.20 *If a countable family of sets* $\{A_n\}_{n \in \mathbb{N}}$ *of a countable set, then* $A = \bigcup_{n \in \mathbb{N}} A_n$ *is a countable set.*

Proof $\forall n \in \mathbb{N}, \exists$ a bijective mapping $f : A \to A_n$.

Let us define a mapping $\sigma : \mathbb{N} \times \mathbb{N} \to A \ni \sigma(k, m) = fk(m)$.

(i) σ is a surjective function because $\forall x \in A, \exists n \in \mathbb{N} \ni x \in A_n$.

But $f_n : \mathbb{N} \to A_n$ is bijective.

$\therefore \exists m \in \mathbb{N} \ni x = f_n(m) = \sigma(n, m)$.

(ii) As $\mathbb{N} \sim \mathbb{N} \times \mathbb{N}$, $\exists$ a bijective mapping $\psi : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$.
Thereby, the mapping $\sigma \circ \psi : \mathbb{N} \to A$ is surjective mapping.
$\therefore$ there exists an injective mapping $g : A \to \mathbb{N}$.
Thereby, $A \sim g(A) \subseteq \mathbb{N}$.
Or, A is finite subset or it is a countable.
But, $A_n \subseteq A$, and A_n is infinite set.
Thereby, A should be infinite set.
Thus, A is a countable. ◆

Corollary *If A, B are a countable sets then $A \cup B$ is a countable.*

Proof $A \subseteq A \cup B \subseteq A \bigcup_{i=1}^{\infty} B_i$ where $B = B_i, i = 1, 2, ...$
So, $\mathbb{N}_o \leq \#(A \cup B) \leq \mathbb{N}_o$.
$\therefore \#(A \cup B) = \mathbb{N}_o$.
Thus, $A \cup B$ is a countable. ◆

Theorem 6.21 *Let $f : A \to B$ be a mapping. If A almost a countable set then the range of f is almost a countable.*

Proof We have to prove that: (i) $A \subseteq \mathbb{N}$. (ii) f is surjective. Then we can decide that B is almost a countable.
Let $C = \{x \in A | (y \in A \wedge y < x) \to f(x) \neq f(y)\}$.
Or, C is consisting of the smallest element of each set $f^{-1}(y), y \in B$.
$\therefore f/C : C \to B$.
But $C \subseteq A$ is almost a countable.
$\therefore B$ is almost a countable set. ◆

6.9 Exercises

Solve the following questions:

Q1: If A be infinite set, and $B \neq \phi$ then each of $A \times B, B \times A$ is infinite.

Q2: Let A be a finite set, and $B \subset A$, where B infinite. Prove that $A - B$ is infinite.

Q3: Prove that A is an infinite set if and only if $\forall n \in \mathbb{N}$, $\exists B \subset A$ such that $B \sim n$.

Q4: Let A be infinite set, $B \subset A$. Prove that $A \sim (A \cup B)$.

Q5: Let $x \in A$. Prove that A is infinite set if and only if $A \sim A - \{x\}$.

Q6: Let A is a countable set. Prove that it can find a countable subset B of A such that $A - B$ be a countable.

Q7: Prove that $\mathbb{N}^n \sim \mathbb{N}, n \in \mathbb{N}$.

Q8: Prove $A = \mathbb{N} \cup \mathbb{N}^2 \cup \mathbb{N}^3 \cup ...$ It is lefta countable set.

Q9: Consider a finite set $A \neq \phi$, B is a countable set. Prove that $A \times B$ is a countable set.

Q10: Prove that the set of algebraic numbers will be a countable.

[Hint: The real number x is called algebraic number if and only if the equation $x^n + a_1 x^{n-1} + ... + a_n = 0$ is a solvable, $a_1, a_2, ..., a_n \in \mathbb{R}$.]

Q11: Prove that a set of all infinite subsets of $\mathbb{N}$ is an equipotent with $2^{\mathbb{N}}$.

Q12: If a power set $\{A_i\}_{i \in I}$ is almost a countable then the set $A = \bigcup_{i \in \mathbb{N}} A_i$ is almost a countable.

Q13: Let $\{A_i\}_{i \in I} \neq \phi$ is almost a countable of a unaccountable sets. Is $A = \bigcup_{i \in \mathbb{N}} A_i$ a unaccountable?

Q14: If $\{A_1, A_2, ..., A_n\}$ is a finite countable power of sets then $\prod_{i=1}^{n} A_i$ almost a countable set.

Q15: Distinguish countable sets from non-countable sets in the following example;

(i) Let $X = \{1, 2, 3, ..., x\}, Y = \{2, 4, 6, ..., 2x\}$, $f : X \to Y$ is a mapping such that $f = \{(x, 2x) | x \in X, 2x \in Y\}$.

(ii) Consider a mapping $f : \mathbb{N} \to \mathbb{N}$, where $f = \{(n, 2n), \forall n \in \mathbb{N}\}$

(iii) Let $X = \{1, 2, 3, ..., x, ...\}, Y = \{2, 4, 6, ..., 2x, ...\}$, $f : X \to Y$ is a mapping such that $f = \{(x, 2x) | x \in X, 2x \in Y\}$.

(iv) $(0, 1)$.

(v) $(0, 1]$.

(vi) $[0, 1)$.

(vii) $[0, 1]$.

(viii) The set $S = \left\{\frac{1}{n}, \forall n \in \mathbb{N}\right\}$.

(ix) The set $L = \{(-1)^n, \forall n \in \mathbb{N}\}$.

7
Binary Operations and Groups

7.1 Introduction

We will dive into this chapter to the binary operations on sets in details. The binary operation on the set A is a mapping from $A \times A$ to A. Or its domain is $A \times A$, and its codomain is A. Thereby, the binary operation is an algebraic operation to connect two elements of the set to get the third element in the same set. Also, there are mono and triple operations and... etc.

Then, we define the mathematical system, which is a set A with one or more than an operation on A. The most important system with the mono operation is a group in which the group is the fundamental subject of abstract algebra. The next sections deals with rings, vector spaces, and fields.

Although various types of groups were dealt with during the 18th and 19th centuries, however the concept of the abstract group did not appear until the end of the 19th century.

Group theory is the most important algebraic theory and has wide contributions and applications in mathematics, physics, chemistry, electrical engineering, computers,...and so on.

Many scientists and researchers contributed to the development of the group theory (Taton, 1972; Wussing, 2007; Hunter et al., 1977;

Jacobson, 2012; Cohn, 2012; Knapp, 2007).

Gårding and Skau (1994) utilized group theory to prove that there is not specific solution method for equation that have a degree of five or more. On the other hand, Galois (Tignol, 2015) proved that there is not a specific method to solve equation of the fifth degree or more. Moreover, he have defined quotient group, and right and left cosets (Tignol, 2015; Bruno and Baker, 1999; Stewart, 2015).

klein (O'Connor and Robertson, 2001; Gillispie et al., 2008; Grattan-Guinness, 2009) was the first to apply group theory in the natural and applied sciences in which linked between geometry and group theory as emphasized in his program (Klein, 1974).

The idea of symmetry is described via group theory (Miller, 1973). Poincaré (1898b) proved that the Euclidean geometry is constructed essentially by group theory (Poincaré, 1898a).

In the previous literature of the group, it is clear that groups have their role and effective in our lives, and they are considered one of the basic concepts in mathematics and applied sciences.

7.2 Binary Operations

Definition 7.1 Let a set $A \neq \phi$, the mapping: $f : A \times A \to A$ is called binary operation on A (Rotman, 1973; Hardy et al., 2011; Fraleigh, 2003).

Note:

(1) Generally, we denote to the binary operation on A by the symbol $*$. Or, $* : A \times A \to A$.

(2) The ordered pair $(a, b) \in A \times A$ has the image in A, and expressed by $a * b$ instead of $*((a, b))$. Or, $*((a, b)) = a * b$.

(3) If $*$ is a binary operation on A, then A is a closed set with respect of $*$, if and only if $a * b \in A, \forall a, b \in A$.

Example 7.1 (1) Let $A = \mathbb{N}$, and let $* = +$. Or, $\forall (a, b) \in \mathbb{N} \times \mathbb{N}$, then $a * b = (a + b) \in \mathbb{N}$. It should be noted that $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Thus, $+$ is a mapping from the domain $\mathbb{N} \times \mathbb{N}$ to the range of $\mathbb{N}$, and $\mathbb{N}$ is the closed set on the $+$.

(2) Also, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are closed sets on the $+$.

(3) It is not necessary every set is closed on $+$. For example, $A = \{-3, -2, -1, 0, 1, 2, 3\}$. The $+$ is not binary operation on A because $2 + 3 = 5 \notin A$. Thus, $\forall a, b \in A, \exists c \notin A \ni a + b = c$.

(4) Let $X \neq \phi$, the mapping $* : P(X) \times P(X) \to P(X)$ defined as $A * B = A \cup B, \forall A, B \in P(X)$ is the binary operation on $P(X)$. Or, the union is the binary operation on $P(X)$. So as $A \cap B$ is a binary operation on $P(X)$.

(5) Sometimes it can be utilize a table to assignment or determine a binary operation on a set. Let $S = \{1, 2, 3\}$, the binary operation defined on S as follows;

$1 * 1 = 1 \quad , 1 * 2 = 2 \quad , 1 * 3 = 3$
$2 * 1 = 3 \quad , 2 * 2 = 1 \quad , 2 * 3 = 2.$
$3 * 1 = 2 \quad , 3 * 2 = 3 \quad 3 * 3 = 1$

The multiplication table of the binary operation is shown in Table 7.1:

Table 7.1: Binary Operation Table

$*$	1	2	3
1	1	2	3
2	3	1	2
3	2	3	1

(6) Let $X \neq \phi$, S is the set of all mappings $f : X \to X$. $*$ is defined on S as follows:

$f * g = g \circ f, \forall f, g \in S.$

Since $f : X \to X \wedge g : X \to X$ are mapping then $g \circ f : X \to X$ is a mapping (See Theorem 4.4). Thereby, $g \circ f \in S$, and $*$ is a binary operation on S.

(7) Let $X \neq \phi$, T is the set of all mappings $f : X \to \mathbb{R}$. $*$ is defined on T as follows:

$f * g = f + g | (f + g)(x) = f(x) + g(x), \forall x \in X, \forall f, g \in T.$

Or, $f + g : X \to \mathbb{R}$ is a mapping.

$\therefore f + g \in T.$

Thereby, $*$ is a binary operation on T.

(8) # on T, defined as

$f\#g = (f - g)(x) = f(x) - g(x)$ is also binary operation on T.

(9) $\cdot$ on T, defined as:

$f \cdot g = (f \cdot g)(x) = f(x) \cdot g(x)$ is also binary operation on T.

(10) $\otimes$ is a binary operation on T'. Let $D = \{x \in X | g(x) = 0\}$, let $T' : X - D \to \mathbb{R} | f \otimes g = \frac{f}{g}$, in which $(\frac{f}{g})(x) = \frac{f(x)}{g(x)}$.

Definition 7.2 Let A be a set, $B \subseteq A$, and $*$ be a binary operation on A. B is called a closed subset with respect to $*$ if and only if $a * b \in B, \forall a, b \in B$ (Birkhoff, 1967).

7.3 Properties of Binary Operations

7.3.1 Commutative Property

Definition 7.3 Let $*$ be a binary operation on a set $A \neq \phi$, $*$ is called a commutative if and only if $a * b = b * a, \forall a, b \in A$(Flood et al., 2011; Axler, 1997; Gallian, 2006; Goodman, 1998).

Example 7.2 Consider the following cases;

(1) Addition and multiplication operations commutative on $\mathbb{R}$, as $a + b = b + a$ and $a.b = b.a, \forall a, b \in \mathbb{R}$.

But, subtraction and division operations not commutative on $\mathbb{R}$, as $1 - 2 \neq 2 - 1$ and $\frac{1}{2} \neq \frac{2}{1}$.

(2) Let X be a set contains of more than two elements, and let $S = \{f | f : X \to X\}$, where $f : X \to X$ is a mapping, and $*$ is a binary operation on S in which defined as follows: $f * g = g \circ f, \forall f, g \in S$.

Since $g \circ f \neq f \circ g$, and

$\because f * g \neq g * f$.

Thereby, $\circ$ is nor commutative binary operation.

Now, let $X = \{a, b, c\}$ contains of more than two elements, and a, b, c are different elements.

If the mapping $f : X \to X$ defined as: $f(a) = f(b) = c, f(c) = a$. And, the mapping $g : X \to X$ defined as: $g(a) = a, g(b) = g(c) = b$.

Then, $(f * g)(a) = (g \circ f)(a) = g(f(a)) = g(c) = b$.

While, $(g * f)(a) = (f \circ g)(a) = f(g(a)) = f(a) = c$.

$\because b \neq c$ by assumed.

$\therefore (f * g)(a) \neq (g * f)(a)$.

Thus, $f * g \neq g * f$.

7.3.2 Associative Property

Definition 7.4 Let $*$ be a binary operation on $a \neq \phi$, $*$ is called associative binary operation if and only if $a*b*c = a*(b*c) = b*(a*c) = c*(a*c) \forall a, b, c \in A$(Hungerford, 1974; Durbin, 1992a; Durbin, 1992b).

Example 7.3 (1) Addition and multiplication operations associative on $\mathbb{R}$, as follows; $(a+b)+c = a+(b+c)$ and $(ab)c = a(bc), \forall a, b \in \mathbb{R}$.

But, subtraction and division operations are not associative on $\mathbb{R}$, as follows;

$1-2-3 \neq (1-2)-3 \neq 1-(2-3)$ and $(\frac{2}{3})/(4) \neq 2/(\frac{3}{4})$.

(2) Let $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ such that $a * b = a + 3b, \forall a, b \in \mathbb{R}$.

The $(a * b) * c = (a + 3b) * c = a + 3b + 3c$. And $a * (b * c) = a * (b + 3c) = a + 3(b + 3c) = a + 3b + 9c$.

Thereby, $(a * b) * c \neq a * (b * c)$. Thus $*$ is not associative on $\mathbb{R}$.

(3) Let $X \neq \phi$, and $S = \{f | f : X \to X\}$. Since $f \circ (g \circ h) = (f \circ g) \circ h$ hence $\circ$ is associative binary operation.

(4) $\cup, \cap$ are associative on $P(X)$.

7.3.3 Distributive Property

Definition 7.5 Let $*, \#$ be binary operations on $A \neq \phi$. $\#$ distributive over $*$ if and only if; (1) $a\#(b * c) = (a\#b) * (a\#c)$. (2) $(b*c)\# = (b\#a)*(c\#a)$ (Bylinski, 1989a; Mendelson, 2009b; Mendelson, 2009a; Mendelson, 1964; Tarski, 1941).

Example 7.4 (1) Consider the set of real numbers $\mathbb{R}$, $*$ be the additional operation on R, and $\#$ be the multiplication operation on R. Then:

$a * b = a + b, \forall a, b \in \mathbb{R}$.

$a\#b = a.b, \forall a, b \in \mathbb{R}$.

$a\#(b*c) = a.(b+c) = (a.b)+(a.c) = (a\#b)+(a\#c) = (a\#b)*(a\#c)$.

also, $(b * c)\#a = (b + c).a = (b.a) + (c.a) = (b\#a) + (c\#a) = (b\#a) * (c\#a)$.

Thus, the multiplication operation distributive over the additional operation.

(2) The additional operation does not distributive over the multiplication operation. Foe example, $3 + (4.5) \neq (3 + 4).(3 + 5)$.

(3) Let $X \neq \phi$, $\#$ be a union operation on $P(X)$, and $*$ is an intersection on $P(X)$.

Then:

(i) $A \cup (B \cap C) = (A \cap B) \cup (a \cap c)$[$\cup$ distributives over $\cap$].

(ii) $(B \cap C) \cup (B \cup A) \cap (C \cup A), \forall A, B, C \in P(X)$[$\cap$ distributive over $\cup$].

7.4 Mathematical System

Definition 7.6 A mathematical system is a set with one or more binary operations on the set (Deskins, 1995).

Note: The set A with a binary operation $*$ on it denoted by $(A, *)$ called mathematical system with a mono operation. If another binary operation $\#$ on A then $(A, *, \#)$ called a mathematical system with two binary operations, and so on.

Definition 7.7 An algebraic system is a mathematical system consisting of a set called the domain and one or more operations on the domain(Deskins, 1995; Cohn and Cohn, 1981; Grätzer, 1979; Birkhoff, 1935; Plotkin and Plotkin, 1972).

Example 7.5 Consider the following cases;

(1) $(\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ are mathematical systems with one binary operation $+$, while $(\mathbb{N}, -), (\mathbb{N}, \div)$ are not mathematical system, because $-, \div$ are not binary operations on $\mathbb{N}$.

(2) Let $X \neq \phi$, and the mapping $\delta : X \to X$, then $(S, \circ)$ is a mathematical system where $\circ$ is denoted to a composite of mappings.

(3) If $X \neq \phi$ then $(P(X), \cup, \cap)$ is a mathematical system with two binary operations.

Definition 7.8 The mathematical system $(A, *)$ is a commutative if and only if $*$ is a commutative binary operation on A.

Or, $a * b = b * a, \forall a, b \in A$ (Bylinski, 1989a; Durbin, 1992a).

Example 7.6 Consider the following cases;

(1) Each of the following mathematical systems are commutative mathematical systems:

$(\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{N}, .), (\mathbb{Z}, .), (\mathbb{Q}, .), (\mathbb{R}, .)$.

(2) Each of the following mathematical systems is not a commutative mathematical system:

$(\mathbb{N}, -), (\mathbb{Z}, -), (\mathbb{Q}, -), (\mathbb{R}, -), (\mathbb{N} - \{0\}, \div), (\mathbb{Z} - \{0\}, \div), (\mathbb{Q} - \{0\}, \div), (\mathbb{R} - \{0\}, \div)$.

(3) Consider the set $A = \{x, y\}$, $*$ a binary operation on A, and defined as shown in Table 7.2:

Table 7.2: Binary Operation $*$ on A

*	x	y
x	x	y
y	y	x

The mathematical system $(A, *)$ is commutative because

$a * b = b * a, \forall a, b \in A$.

Let $a = x, b = y \rightarrow a * b = x * x = x; b * a = x * x = x$.

Let $a = x, b = y \rightarrow a * b = x * y = y; b * a = y * x = y$.

Let $a = y, b = x \rightarrow a * b = y * x = y; b * a = x * y = y$.

Let $a = y, b = y \rightarrow a * b = y * y = x; b * a = y * y = x$.

(4) If $X \neq \phi$ then each of $(P(X), \cup), (P(X), \cap), (P(X), \Delta)$ are commutative because $\forall A, B \in P(A)$ then

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

Definition 7.9 The mathematical system $(A, *)$ is an associative if and only if $*$ is an associative binary operation on A.

Or, $a * b * c = a * (b * c) = b * (a * c) = c * (a * b), \forall a, b, c \in A$ (Hungerford, 1974; Bylinski, 1989a; Durbin, 1992a).

Example 7.7 (1) Each of the following mathematical systems are the associative mathematical systems:

$(\mathbb{N},+),(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{N},.),(\mathbb{Z},.),(\mathbb{Q},.),(\mathbb{R},.)$.

(2) Each of the following mathematical systems are not associative mathematical systems:

$(\mathbb{N},-),(\mathbb{Z},-),(\mathbb{Q},-),(\mathbb{R},-),(\mathbb{N}-\{0\},\div),(\mathbb{Z}-\{0\},\div),(\mathbb{Q}-\{0\},\div),(\mathbb{R}-\{0\},\div)$.

(3) If $X \neq \phi$ then each of $(P(X),\cup),(P(X),\cap),(P(X),\Delta)$ are associative mathematical systems.

(4) If $X \neq \phi$, and $S : X \to X$ be a set of all mappings, then $(S,\circ)$ is associative mathematical system.

Definition 7.10 The mathematical system $(A,*,\#)$ called number system if and only if:

(1) Both of $*,\#$ are commutative and associative.

(2) Each binary operation is a distributive over the other binary operation (Smith and Karpinski, 1911; Chowdhury, 1970).

Note: For all numerical system $(A,*,\#)$, the elements of A called numbers.

Definition 7.11 Let $(A,*)$ be a mathematical system, the identity element of the system denoted by e with respect to $*$ if and only if $a*e=e*a=a, \forall a \in A$ (Weisstein, 2002e; Weisstein, 2002f).

Example 7.8 (1) 0 is the identity element for the mathematical system $(\mathbb{N},+)$, since $a+0=0+a=a, \forall a \in \ltimes$.

(2) 1 is the identity element for the mathematical system $(\mathbb{N},.)$, since $a.1=1.a=a, \forall a \in \ltimes$.

(3) The system $(\mathbb{Z}^{+},+)$ has no identity element.

(4) Let $X \neq \phi$, and $P(X)$ be a power set of X. ϕ is the identity element for the system $(P(X),\cup)$, since $A\cup\phi=\phi\cup A=A, \forall A \in P(X)$.

(5) Let $X \neq \phi$, and $P(X)$ be a power set of X. X is the identity element for the system $(P(X),\cap)$, since $A\cap X=X\cap A=A, \forall A \in P(X)$.

(6) Let $X \neq \phi$, and $P(X)$ be a power set of X. The system $(P(X),-)$ has no identity element, where $-$ is denoted to the difference between any two sets of $P(X)$.

Theorem 7.1 *The mathematical system* $(A, *)$ *has a unique identity element.*

Proof Suppose that $(A, *)$ has two identity elements e, e'.

$\because e$ is the identity element,

$\therefore e' * e = e * e' = e'$ ...(1).

And, for the same reason

$e * e' = e' * e = e$ ...(2).

From (1)& (2), we get $e = e'$.

Thus, the system has a unique identity element. ♦

Definition 7.12 Let $(A, *)$ be a mathematical system, $a \in A$, and e be the identity element for it. If there is $b \in A \ni a * b = b * a = e$, then b is called inverse of a, and denoted by a^{-1}(Howie, 1995; Nordahl and Scheiblich, 1978; Wilder et al., 2012).

Example 7.9 (1) Consider the mathematical system $(\mathbb{N}, +)$.

It should be noted the inverse of the identity element 0 is 0 itself, because $0 + 0 = 0$.

(2) Let the system $(\mathbb{N} - \{0\}, +)$. This system has no inverse element because if $a \in \mathbb{N} - \{0\} \nexists b \in \mathbb{N} - \{0\} \ni a + b = 0$. Or, there is not inverse for all elements of $\mathbb{N} - \{0\}$.

(3) Consider the system $(\mathbb{Z}, +)$. If $a \in \mathbb{Z}\ \exists a^{-} \in \mathbb{Z} \ni a + (-a) = -a + a = 0$. Or, $-a$ is inverse element with respect to the additional operation.

Theorem 7.2 *Consider a mathematical system* $(A, *)$ *has an identity element, then the inverse of the identity element is the identity element itself.*

Proof Suppose that e is the identity element for $(A, *)$.

Now, since e is the identity element for the system hence

$a * e = e, \forall a \in A$.

$\therefore e^{-1} = e$.

$\therefore a^{-1} = e$. ♦

Theorem 7.3 *If $(A, *)$ be the associative mathematical system has the identity element, then every element of A has a unique inverse.*

Proof Suppose that e is the identity element with respect to the binary operation $*$, and consider the element $a \in A$ with two inverse elements $b, b' \in A$.

Now, $\because$ b is the inverse of a,

$\therefore b * a = e$.

$\therefore (b * a) * b' = e * b' = b'$.

Or, $(b * a) * b' = b'$.

$\because$ b' is the inverse of a,

$\therefore b' * a = e$.

$\therefore b * (a * b') = b * e = b$.

Or, $b * (a * b') = b$.

$\because$ $*$ is associative,

$\therefore (b * a) * b' = b * (a * b')$.

Thus, $b' = b$. ♦

Definition 7.13 The mathematical system $(A, *)$ is called semigroup if and only if it is an associative mathematical system (Martino and Martino, 2014; Liapin, 1968; Wallace, 2012; Scott, 2012; Cohn, 2012; Rotman, 1973; Hall, 2018; Hall, 1962; Hall, 1967; Howie, 1995; Nordahl and Scheiblich, 1978).

Example 7.10 (1) Each of the examples we have previously given to the associative mathematical systems represents a semigroup.

(2) Let $*$ be a binary operation defined on $\mathbb{R}$, such that

$a * b = max\{a, b\}, \forall a, b \in \mathbb{R}$. Or, the result of $a * b$ is the great of a, b, or any of them in case if $a = b$.

$*$ is the associative on $\mathbb{R}$, that is because

$a * (b * c) = max\{a, , b, c\}$.

$(a * b) * c = max\{a, , b, c\}$.

Or, $a * (b * c) = (a * b) * c$.

Thus, we conclude that $(\mathbb{R}, *)$ is semigroup.

(3) Let $A = \{a, b\}$, and $*$ defined on A as shown in Table 7.3:

$*$ is associative on A, that is because

Table 7.3: Binary Operation $*$ on A

$*$	x	y
x	x	y
y	y	x

$a * (b * c) = (a * b) * c, \forall a, b, c \in A.$
(i) If $a = x, b = x, c = x$ then
$a * (b * c) = x * (x * x) = x * x = x$
$(a * b) * c = (x * x) * x = x * x = x.$
(ii) If $a = x, b = x, c = y$ then
$a * (b * c) = x * (x * y) = x * y = y$
$(a * b) * c = (x * x) * y = x * y = y.$
(iii) If $a = x, b = y, c = x$ then
$a * (b * c) = x * (y * x) = x * y = y$
$(a * b) * c = (x * y) * x = y * x = y.$
(iv) If $a = x, b = y, c = y$ then
$a * (b * c) = x * (y * y) = x * x = x$
$(a * b) * c = (x * y) * y = y * y = x.$
(v) If $a = y, b = x, c = x$ then
$a * (b * c) = y * (x * x) = y * x = y$
$(a * b) * c = (y * x) * x = y * x = y.$
(vi) If $a = y, b = x, c = y$ then
$a * (b * c) = y * (x * y) = y * y = x$
$(a * b) * c = (y * x) * y = y * y = y.$
(vii) If $a = y, b = y, c = x$ then
$a * (b * c) = y * (y * x) = y * y = x$
$(a * b) * c = (y * y) * x = x * x = x.$
(viii) If $a = y, b = y, c = y$ then
$a * (b * c) = y * (y * y) = y * x = y$
$(a * b) * c = (y * y) * y = x * y = y.$
Thus, we conclude that $(A, *)$ is semigroup.

(4) The mathematical system $(\mathbb{Z}, -)$ is not a semigroup, because $-$ is not associative binary operation.

Definition 7.14 The mathematical system $(A, *)$ is a monoid if and only if provides these two conditions:

(1) $*$ is associative binary operation.

(2) There is an identity element for $*$ (Fountain, 1997; Jacobson, 1951; Jacobson, 2009a).

Example 7.11 (1) The semigrou $(\mathbb{N}, +)$ is a monoid.

(2) The system $(\mathbb{Z}^+, +)$ is a semigroup but not monoid. From this example, we conclude the following note.

Note: Every monoid system is a semigroup while a semigroup is not necessary to be a monoid.

7.5 Exercises

Solve the following questions:

Q1: Let $S = \left\{a + b\sqrt{3} | a, b \in \mathbb{Z}\right\}$, and $*$ be The multiplication operation on S.

(1) Prove that S closed on $*$.

(2) Prove that $(S, *)$ ia a commutative semigroup with an identity element.

Q2: Let $\mathbb{R}^* = \mathbb{R} - \{0\}, T = \{(a, b) \in \mathbb{R} \times \mathbb{R}^*\}$. Define $*$ on T as follows;

$(a, b) * (c, d) = (ac, bd)$. Prove that the system $(T, *)$ is the commutative semigroup has the identity element.

Q3: Give an example of noncommutative but associative mathematical system.

Hint: Let $X \neq \phi, S = \{f | f : X \to X\}$, then $(S, \circ)$ is a noncommutative but associative mathematical system .

Q4: Give an example of a commutative but not associative a mathematical system.

Hint: Let $A \neq \phi, a * b = a + b - ab, \forall a, b \in A$, then $(A, *)$ is a a commutative but not associative mathematical system because $*$ is a commutative but not associative binary operation.

Q5: Distinguish the commutative binary operation from the associative binary operation on $\mathbb{Q}$ of the following binary operations;

(1) $a * b = b$. (2) $a * b = a + b - 2$.

Q6: Let $(S, *)$ be a mathematical system that has its own identity element, and let $(a * b) * (c * d) = (a * c) * (b * d), \forall a, b, c, d \in S$. Prove that $*$ is a commutative and associative.

Q7: Consider $S = \{1, ..., 6\}$. Define $*$ on S as follows;

$a * b = gcd\, \{a, b\}$. Prove that $(S, *)$ is semigroup.

Q8: Let the binary operation $*$ defined on $\mathbb{Q}$ as follows;

$a * b = a + b - ab$.

(1) Find the identity element. (2) Is each element of $\mathbb{Q}$ has inverse?

Q9: Define $*$ on $\mathbb{N}$ as $a * b = a + b^2, \forall a, b \in \mathbb{N}$. Does the identity element exist?

Q10: Consider the binary operation $*$ on $\mathbb{Q}$, and defined as;

$a * b = \frac{a+b}{2}, \forall a, b \in \mathbb{Q}$. Dose $*$ a commutative on $\mathbb{Q}$?

Q11: Prove that the system $(\mathbb{Q}, +, .)$ is a number system.

Q12: Consider the set pf all mappings $S : \mathbb{R} \rightarrow \mathbb{R}$. Is $(S, +, .)$ a numerical system?

7.6 Groups

Definition 7.15 The mathematical system $(G, *)$ is called a group if and only if the following three conditions are met;

(1) The binary operation $*$ is associative on G. Or, $a * b * c = a * (b * c) = b * (a * c) = c * (a * b), \forall a, b, c \in G$.

(2) There is an identity element. Or, $\exists e \in G \ni a * e = e * a = a, \forall a \in G$.

(3) Every element is invertible. Or, $\forall a \in G, \exists a^{-1} \in G \ni a * a^{-1} = a^{-1} * a = e$ (Hall, 2018; Hall, 1962; Ledermann, 1973; Robinson, 2012; Hall, 1967).

Definition 7.16 The group $(G, *)$ is called commutative group if and only if $*$ is a commutative operation (Szmielew, 1959; Jacobson, 2012; Jacobson, 1951; Jacobson, 2009a; Jacobson, 2009b; Rotman, 2010; Rotman, 1973; Rotman, 2012).

Example 7.12 (1) The mathematical system $(\mathbb{N}, +)$ is not a group because there is not inverse elements for some elements in $\mathbb{N}$.

(2) The mathematical system $(\mathbb{Z}, +)$ is a commutative group with the identity element 0.

(3) The mathematical system $(\mathbb{Z}, .)$ is not a group because there is not inverse elements for some elements in $\mathbb{Z}$. For example, $3.\frac{1}{3} = 1$, but $\frac{1}{3} \notin \mathbb{Z}$.

(4) The mathematical system $(\mathbb{Z}, -)$ is not a group because $-$ is not associative on $\mathbb{Z}$.

(5) Each of $(\mathbb{Q}, +), (\mathbb{R}, +)$ are groups.

(6) Each of $(\mathbb{Q}, .), (\mathbb{R}, .)$ are not groups.

(7) Each of $(\mathbb{Q} - \{0\}\}, .), (\mathbb{R} - \{0\}\}, .)$ are commutative groups.

(8) Let $X \neq \phi$, each of $(P(X), \cup), (P(X), \cap)$ are not groups.

(9) Let $X \neq \phi$, $(P(X), \Delta)$ is a group.

Example 7.13 Prove that $(\mathbb{Z}, *)$ is a commutative group where $a*b = a+b+1, \forall a, b \in \mathbb{Z}$.

Solution (1) $*$ is associative.

$a * (b * c) = a * (b + c + 1) = a + (b + c + 1) + 1 = a + b + c + 2.$

$(a * b) * c = (a + b + 1) * c = (a + b + 1) + c + 1 = a + b + c + 2.$

$\therefore a * (b * c) = (a * b) * c, \forall a, b, c \in \mathbb{Z}.$

(2) Identity element. If e is the identity element, it ought to be

$a * e = a$, and $e * a = a, \forall a \in \mathbb{Z}$.

Or, $a + e = a + e + 1 = a$, and $e + a = e + a + 1 = a$.

Thereby, $e = -1$ to satisfy,

$a * (-1) = a + (-1) + 1 = a$, and $(-1) + a = (-1) + a + 1 = a$.

(3) Inverse element. If b is the inverse element for $a \in \mathbb{Z}$ then,

$a * b = e = (-1)$, and $b * a = e = (-1)$.

$\therefore a + b + 1 = (-1)$, and $b + a + 1 = (-1)$.

$\therefore b = -(a + 2)$.

Thus, the inverse of $a = -(a + 2) \in \mathbb{Z}$ to satisfy,

$a * (-2 - a) = a + (-2 - a) + 1 = (-1)$, and $(-2 - a) * a = (-2 - a) + a + 1 = (-1)$.

$a * b = a + b + 1 = b + a + 1 = b * a$.

$\therefore (\mathbb{Z}, *)$ is a commutative group.

Example 7.14 Consider $G = \{(a, b) \in \mathbb{R} \times \mathbb{R} | a \neq 0\}$, and the binary operation $*$ defined on G as $(a, b) * (c, d) = (ac, bc + d)$. Prove that $(G, *)$ is uncommunicative group.

Solution: (1) $*$ is associative

$(a, b) * (c, d) * (e, f) = (ac, bc + d) * (e, f) = (ace, (bc + d)e + f) = (ace, bce + de + f)$, and

$(a, b) * (c, d) * (e, f) = (a, b) * (ce, de + f) = (ace, bce + de + f)$.

$\therefore [(a, b) * (c, d)] * (e, f) = (a, b) * [(c, d) * (e, f)], \forall (a, b), (c, d), (e, f) \in \mathbb{R}$

(2) Identity element. If (x, y) is the identity element for G.

$(a, b) * (x, y) = (a, b)$, and $(x, y) * (a, b) = (a, b)$.

Or, $\forall a, b \in G$, then $(ax, bx + y) = (a, b)$,

$\therefore ax = a \wedge bx + y = b \Rightarrow x = 1 \wedge y = 0$.

$\therefore (1, 0) \in G$ is the identity element.

(3) Inverse element. Let (x, y) is an inverse element for $(a, b) \in G$.

$(a, b) * (x, y) = e = (1, 0)$, and $(x, y) * (a, b) = e = (1, 0)$.

Or, $(ax, bx + y) = (1, 0)$, and $(xa, ya + b) = (1, 0)$.

$\therefore ax = 1 \wedge bx + y = 0 \Rightarrow x = \frac{1}{a}, y = -\frac{b}{a}$.

$\therefore (\frac{1}{a}, -\frac{b}{a}) \in G, a \neq 0$ is the inverse element for (a, b).

Thus, $(G, *)$ is a group.

Now, let $(1, 3), (5, 7)\ inG$.

$(1, 3) * (5, 7) = (5, 15 + 7) = (5, 22)$, while $(5, 7) * (1, 3) = (5, 7 + 3) = (5, 10)$.

Since $(1, 3) * (5, 7) \neq (5, 7) * (1, 3)$, hence $*$ is uncommutative, it implies that $(G, *)$ is uncommutative group.

7.6.1 Finite Groups

Definition 7.17 The group $(G, *)$ is called finite if and only if the set G is finite, otherwise the group $(G, *)$ is infinite group (Aschbacher, 2004; Jacobson, 2012; Humphreys et al., 1996).

Definition 7.18 Let $(G, *)$ be a finite group, the number of elements of $(G, *)$ is called the order of the group, and denoted by $O(G)$. If the group $(G, *)$ is infinite then it is said that the group is of infinite order (Dummit and Foote, 2004a; Burnside, 1911).

Example 7.15 (1) Consider $G = \{-1, 1\}$, then $(G, *)$ is a finite group, and $O(G) = 2$.

(2) Consider $G = \{-1, 1, -i, i\}, i = sqr{-}1$, then $(G, *)$ is a finite group, and $O(G) = 4$.

(3) $\mathbb{Z}, 0$ is infinite group, since $\mathbb{Z}$ is infinite set.

Theorem 7.4 *Any group $(G, *)$ has;*

(1) A unique identity element. (2) A unique inverse element of any element of it.

Proof Since $(G, *)$ is a mathematical system, hence:

(1) Based on Theorem 7.1, the identity element is a unique.

(2) Based on Theorem 7.3, the inverse element is a unique. ♦

7.6.2 Cancellation Law

Theorem 7.5 *Let $(G, *)$ be a group. If,*

(1) $a * b = a * c$, or

(2) $b * a = c * a$, then $b = c \; \forall a, b, c \in G$.

Proof (1) Let $a * b = a * c$.

As a is the element in the group $(G, *)$,

$\therefore \exists a^{-1} \neq a * a^{-1} = e$.

$\therefore a^{-1} * (a * b) = a^{-1} * (a * c)$.

$\because *$ ia associative,

$\therefore e * b = e * c$.

$\therefore b = c$.

(2) Through the same method $b = c$. ♦

Theorem 7.6 *In the group $(G, *)$. Each of the equations;*

(i) $a * x = b$.

(ii) $y^* \; a = b$.

Has a unique solution, $\forall a, b \in G$, is $b * a^{-1}, b * a^{-1}$ respectively.

Proof (i) $\because a \in G$,

$\therefore a^{-1} \in G$.

$\therefore a^{-1} * b \in G$.

$\therefore a^{-1} * b$ is a solution for the equation $a * x = b$, and it satisfies as followings;

$a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$.

$\therefore$ there exists at least one solution satisfies the equation.

Now, to prove a solution is a unique.

Suppose that x' is another solution for $a * x = b$.

$\therefore a * x' = b$.

$\because a * (a^{-1} * b) = b$.

$\therefore a * x' = a * (a^{-1} * b)$.

Thus, and based on the cancellation law, we get that $x' = a^{-1} * b$.

Or, the solution is a unique.

(ii) It is left as an exercise. ⧫

Theorem 7.7 *Let $(G, *)$ be a group, and $\forall a, b \in G$, then*

(i) $(a^{-1})^{-1} = a$.

(ii) $(a * b)^{-1} = b^{-1} * a^{-1}$.

Proof (i) $\because a^{-1}$ is inverse of a,

$\therefore a^{-1} * a = e$ ...(1).

$\because (a^{-1})^{-1}$ is inverse of a^{-1},

$\therefore a^{-1} * (a^{-1})^{-1} = e$ ...(2).

$\therefore$ from (1)& (2), we get $a^{-1} * a = a^{-1} * (a^{-1})^{-1}$.

By canceling a^{-1} from both sides, it concluded that

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

(ii) $\because a^{-1}$ is inverse of a,

$\therefore a * a^{-1} = e$.

$\because b^{-1}$ is inverse of b,

$\therefore b * b^{-1} = e$.

$\because *$ is associative,

$\therefore (a * b) * (b^{-1} * a^{-1}) = [(a * b) * b^{-1}] * a^{-1} = [a * (b * b^{-1})] * a^{-1} = (a * e) * a^{-1} = a * a^{-1} = e$.

Or, $(a * b) * (b^{-1} * a^{-1}) = e$ ...(1).

In the same way, we get that $(b^{-1} * a^{-1}) * (a * b) = e$ ...(2).

From (1)& (2) it is concluded that $(a*b)*(b^{-1}*a^{-1}) = (b^{-1}*a^{-1})* (a * b) = e$.

From the definition of the inverse, we conclude that $b^{-1} * a^{-}$ is the inverse of $a * b$.

Or, $(a * b)^{-1} = b^{-1} * a^{-1}$. ♦

Note: Consider the group $(G, *)$, and let $a_1, ..., a_n \in G$, then
$(a_1 * ... * a_n)^{-1} = a_n^{-1} * ... * a_1 - 1$.

Definition 7.19 Let $(G, *)$ be a group, and $a \in G, k \in \mathbb{Z}^+$. We define $a^k = a.a....a(k - factors)$. $a^0 = e, a^{-k} = (a^{-1})^k = a^{-1} * a^{-1} * ... * a^{-1}(k - times)$ (Dummit and Foote, 2004a; Herstein, 1975; McCoy, 1968; Gilbert, 2014).

Example 7.16 Consider the group $(\mathbb{Z}, +)$, and let $a = 5, k = 4$.
$\therefore a^k = 5^4 = 5 + 5 + 5 + 5 = 20$
$5^0 = e = 0$
$5^{-4} = (5^{-1})^4 = (-5) + (-5) + (-5) + (-5) = -20$.

Theorem 7.8 *Let $(\mathbb{Z}, +)$ be a group, and $a \in G, m, n \in \mathbb{Z}$. Then*

(i) $a^n * a^m = a^{n+m} = a^m * a^n$.

(ii) $(a^n)^m = a^{nm} = (a^m)^n$.

Proof The proof has been left as an exercise for the reader. ♦

7.6.3 Symmetric Group

Definition 7.20 Let S be a set, G be the set of all bijective mappings from S to itself, and $*$ be a composition of mappings then the grou $(G, *)$ is called symmetric group and denoted by $A(S)$ (Jacobson, 2012; Jacobson, 1951; Jacobson, 2009a; Jacobson, 2009b; Grillet, 2007).

Theorem 7.9 *Let S be a set, G is the set of all bijective functions on S, and $*$ be a composition of mappings. Or, $f * g = g \circ f, \forall f, g \in G$ then $(G, *)$ is a group on S, and namely called Symmetric group.*

Proof (1) Associative property. Let $f, g, h \in G$, then $g \circ (f \circ h) = (g \circ f) \circ h$.

So, $\forall x \in S$, then $(g \circ (f \circ h))(x) = g(f \circ h)(x) = g(f(h(x)))$.

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

Or, $(g \circ (f \circ h))(x) = (g \circ (f \circ h))(x), \forall x \in S$.

$\therefore g \circ (f \circ h) = (g \circ f) \circ h, \forall f, g, h \in G$.

$\therefore$ the associative property is achieved.

(2) Identity element.

Let the identity mapping $I_S : S \to S$ be the identity element in G, where $f \circ I_S = I_S \circ f = f$.

$\therefore I_S$ is the identity element for G.

(3) Inverse element.

Let $f \in G$.

$\because f$ is bijective,

$\therefore \exists f^{-1} : S \to S$.

$\therefore f^{-1} \in G \ni f \circ f^{-1} = f^{-1} \circ f = I_S$.

$\therefore \forall f \in G \; \exists f^{-1} \in G$.

$\therefore (G, \circ)$ is a group. ♦

Theorem 7.10 *If $O(S) > 2$, then there are two elements $\alpha, \beta \in A(S) \ni \alpha \circ \beta \neq \beta \circ \alpha$.*

Proof Let $s_1, s_2, s_3 \in S$. We define $\alpha : S \to S \ni \alpha(x_1) = x_2, \alpha(x_2) = x_3, \alpha(x_3) = x_1; \alpha(s) = S, \forall s \in S$.

The α can expressed as follows;

$\alpha = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}$.

Again, we define $\beta : S \to S \ni \beta(x_2) = x_3, \beta(x_3) = x_2; \beta(s) = S, \forall s \in S - \{x_2, x_3\}$.

The β can be expressed as follows;

$\beta = \begin{pmatrix} x_2 & x_3 \\ x_3 & x_2 \end{pmatrix}$.

Obviously, $\alpha, \beta \in A(S)$.

Now, we have:

$(\alpha \circ \beta)(x_1) = \alpha(\beta(x_1)) = \alpha(x_1) = x_2$.

$(\beta \circ \alpha)(x_1) = \beta(\alpha(x_1)) = \beta(x_2) = x_3$.

$\because x_2 \neq x_3$,
$\therefore \alpha \circ \beta \neq \beta \circ \alpha$. ♦

Corollary *If $O(S = n)$ then $O(A(S)) = n!$.*

Proof The proof is left as an exercise. ♦

Definition 7.21 If $O(S) = n$, then $A(S)$ denoted by S_n, and it is called symmetric group of degree n(Jacobson, 2012; Jacobson, 1951; Jacobson, 2009a; Jacobson, 2009b; Grillet, 2007).

Example 7.17 If $O(S_3) = 3!$. Or, S_3 contains of six elements which can be expressed as;

$S = \{x_1, x_2, x_3\}$. The six elements are as follows:

$f_0 = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix}$,

$f_1 = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix}$,

$f_2 = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}$,

$f_3 = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix}$,

$f_4 = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_2 & x_1 \end{pmatrix}$,

$f_5 = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix}$.

It should be noted that:

$f_1^2 = f_1 \circ f_1 = f_0$, $f_2^2 = f_2 \circ f_2 = f_0$, and $f_2 \circ f_1 = f_4 \neq f_5 = f_1 \circ f_2$.

7.6.4 Groups of Integers mod n

Definition 7.22 Let $n \in \mathbb{Z}^+, a, b \in \mathbb{Z}$. It is said that a congruent to b module n if and only if;

$a - b$ divided by n and expressed by the symbol $(mod\, n)$, $a \equiv b \vee a \equiv_n b$.

Or, $a \equiv b\ mod\ n) \Leftrightarrow a - b = kn, k \in \mathbb{Z}$ (Vinogradov, 2016; Gauss, 1966; Gauss, 2006).

Example 7.18 If $n = 5$ then
$3 \equiv 13(mod\ 5)$,
$-5 \equiv 10(mod\ 5)$,
$-20 \equiv -30(mod\ 5)$.

Note:

If $a - b$ not divisible over n then it said a not equivalent b *mod* n. Or, $a \not\equiv b\ mod\ n)$, or, $a \not\equiv_n b$.

Theorem 7.11 *If $n \in \mathbb{Z}^+$ then $\equiv_n$ is equivalence relation on $\mathbb{Z}^+$.*

Proof (1) Reflexive.
Since $a \equiv a(mod\ n), \forall a \in \mathbb{Z}$,
$\therefore aRa, \forall a \in \mathbb{Z}$.
$\therefore R$ is reflexive relation.
(2) Symmetric.
Since $aRb \to a \equiv b(mod\ n)$.
Or, $a - b = kn$.
$\therefore b - a = (-k)n$.
Or, $b \equiv a(mod\ n)$.
Thereby, $bRa, \forall a, b \in \mathbb{Z}$.
$\therefore R$is symmetric relation.
(3) Transitive.
Since $aRb \wedge bRc \to a \equiv b(mod\ n) \wedge b \equiv c(mod\ n)$.
Thereby, $a - b = k_1 n, k_1 \in \mathbb{Z} \wedge b - c = k_2 n, k_2 \in \mathbb{Z}$.
$\therefore a - c = (a - b) + (b - c) = (k_1 + k_2)n = k_3 n, k_3 \in \mathbb{Z}$.
$\therefore a \equiv c(mod\ n)$.
$\therefore aRc, \forall a, b, c \in \mathbb{Z}$.
$\therefore R$ is transitive relation.
Thus, from (1), (2)& (3) R is equivalence relation. ♦

It should be noted that there is a relation between *modn* $, \forall n \in \mathbb{Z}^+$, and equivalence classes as verified by researchers (Palagallo, 1991; Devlin, 2003; Maddox, 2002; Morash, 1987; Wolf, 1998). The relation is stated in the following corollary.

Corollary *If $n \in \mathbb{Z}^+$ then $\mathbb{Z}$ divided by equivalence relation (mod n $\equiv$) to equivalence classes.*

Proof The proof is left for the reader. ⧫

Note: The class contains on a denoted by $[a]$ called the congruence class *mod* n, and a is called the class representative. Mathematically, if $n \in \mathbb{Z}^+, a \in \mathbb{Z}$, then $[a] = \{x \in \mathbb{Z} | x \equiv a \ (mod \ n)\}$.

Or, $[a] = \{x \in \mathbb{Z} | x = a + kn, k \in \mathbb{Z}\}$.

Example 7.19 Let $n = 3$, then
$[0] = \{x \in \mathbb{Z} | x = 0 + 3k, k \in \mathbb{Z}\}$
$= \{x \in \mathbb{Z} | x = 2k, k \in \mathbb{Z}\}$
$= \{..., -6, -3, 0, 3, 6, ...\}$.
$[1] = \{x \in \mathbb{Z} | x = 1 + 3k, k \in \mathbb{Z}\}$
$= \{..., -5, -2, 1, 4, 7, ...\}$.
$[2] = \{x \in \mathbb{Z} | x = 2 + 3k, k \in \mathbb{Z}\}$
$= \{..., -4, -1, 2, 5, 8, ...\}$.

It should be noted that every integer number lies in one of the classes $[0], [1], [2]$. The integer numbers lie in the same congruence class are identities *mod* 3, while the integer numbers lie in different congruence class are not identities *mod* 3. On the other hand, $..., [-1] = [2], [5], [8], [11], [14]$. But, we always select the least positive integer number, in this case $[2]$ is representatives the equivalence class.

7.6.5 Division Algorithm

Definition 7.23 If $a, b \in \mathbb{Z}, b \neq 0$ then $\exists r, t \in \mathbb{Z} \ni a = bt + r, 0 \leq r < b$, t is called quotient and r is remainder (McCann and Pippenger, 2005; Obermann and Flynn, 1995; Goldschmidt, 1964; Hasselström, 2003).

Example 7.20 (1) Let $a = 15, b = 4$, then $15 = 4.3 + 3$. Or, $t = 3, r = 3$.

(2) Let $a = 19, b = 6$, then $19 = 6.3 + 1$. Or, $t = 3, r = 1$.

Theorem 7.12 *Let $n \in \mathbb{Z}^*$, R is the relation $\equiv_n$. There are n of congruence classes* $[0], [1], ..., [n-1]$.

Proof Let $a \in \mathbb{Z}$.

Now, based on division algorithm, we have $a = qn + r \ni q, r \in \mathbb{Z}, 0 \leq r < n$.

$\therefore a - r = qn$.
$\therefore [a] = [r]$.
$\because r = 0, 1, ..., n-1$,
$\therefore [a] = [0] \vee [1] \vee ... \vee [n-1]$.
Thus there are n of equivalence classes. ♦

Note: If $n \in \mathbb{Z}^+$ then $Z_n = \{[0], [1], ..., [n-1]\}$.

Example 7.21 $Z_3 = \{[0], [1], [2]\}$.

7.6.6 Addition Modulo n

Definition 7.24 The operator $*$ denoted by $+_n$ can be defined Z_n as follows;

$[a] * [b] = [a+b], [a], [b] \in Z_n$, and called addition modulo n (Mustafa et al., 1980).

Theorem 7.13 *If* $[a'] = [a] \wedge [b'] = [b]$ *then* $[a'] +_n [b'] = [a] +_n [b]$.

Proof We have to prove that $[a' + b'] = [a + b]$.

Now, $a' \equiv a(mod\ n) \wedge b' \equiv b(mod\ n)$.
$\therefore a' + b' \equiv a + b(mod\ n)$.
$\therefore [a' + b'] = [a + b]$. ♦

Corollary $+_n$ *is a binary operation on* Z_n.

Proof The proof is left as an exercise for the reader. ♦

Example 7.22 $[3] +_7 [6] = [3 + 6] = [9] = [2] \in Z_7$.

Theorem 7.14 $(Z_n\ , +_n)$ *is a commutative group.*

Proof (1) The operation $+_n$ is associative.

$[a] +_n ([b] + n[c]) = [a] +_n ([b + c]) = [a + (b + c)] = [(a + b) + c] = [a + b] +_n [c] = ([a] +_n [b]) +_n [c]$.

(2) $[0]$ is the identity element. $[0] +_n [a] = [0 + a] = [a] = [a + 0] = [a] +_n [0], \forall [a] \in Z_n$.

(3). If $[a] \in Z_n$ then $[n-a] \in Z_n$. Furthermore, $[a] +_n [n-a] = [a+(n-a)] = [n] = [0]$. Or, $[a]^{-1} = [n-a]$.

(4) $[a] +_n [b] = [a+b] = [b+a] = [b] +_n [a], \forall [a], [b] \in Z_n$.

$\therefore +_n$ is a commutative operation.

$\therefore (Z_n, +_n)$ is a commutative group. . ♦

7.6.7 Integer Group mod n

Definition 7.25 $(Z_n, +_n)$ called integer group mod n (Mustafa et al., 1980).

Note: For all $n \in \mathbb{Z}^+$, there exist at least one commutative group G such that $O(G) = n$.

Example 7.23 Let $n = 3$, then $Z_3, +_3$ is illustrated in Table 7.4

Table 7.4: Operation $+_3$ on Z_3

$+_3$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

For convenience, Z_3 can be written as in Table 7.5.

Table 7.5: Operation $+_3$ on Z_3

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Thus, $Z_3 = \{0, 1, 2\}$. Generally, $Z_n = \{0, 1, 2, ..., n-1\}$.

7.7 Exercises

Solve the following questions:

Q1: Consider $G = \{a_0, a_1, ..., a_6\}$, and let $*$ defined as a binary operation on G as follows;

$$\begin{cases} a_i * a_j = a_{i+j}; \text{if } i+j < 7 \\ a_i * a_j = a_{i+j-7}; \text{if } i+j \geq 7 \end{cases}$$

Is $G, *$ a group? Give logical reasons.

Q2: Let $(G, *)$ be a commutative group. Prove that

$(a * b)^n = a^n * b^n, \forall a, b \in G, n \in \mathbb{Z}$.

Q3: If $(G, *)$ is a group, such that $(a*b)^2 = a^2*b^2, \forall a, b \in G$. Prove that $(G, *)$ is a commutative group.

Q4: Give an example in the group S_3 with two elements x, y such that

$(x \circ y)^2 \neq x^2 \circ y^2$.

Q5: Consider $(G, *)$ such that $O(G) = 3$. Prove that $(G, *)$ is a commutative group.

Q6: Let $(G, *)$ be a group such that $O(G) = 2k, k \in \mathbb{Z}^+$. Prove that $\exists a \neq e \ni a^2 = e$, where e is the identity element.

Q7: Prove that a mathematical system $(G, *)$ is a group if

(i) $*$ is associative. (ii) Cancellation law is verified in G.

Q8: Let $n > 2$ and be an integer number. Create a noncommutative group such that its order is equal to Z_n.

Q9: Let $n \in \mathbb{Z}^*$. Define the operation δ_n on $\mathbb{Z}^*$ as follows: $[a]\delta_n[b] = [ab]$. Prove that:

(i) δ_n is a binary operation on Z_n. (ii) Is the mathematical system (Z_n, δ_n) is a group? Explain your answer logically.

Q10: Prove that any noncommutative group has at least six elements.

Q11: Let $a \equiv b(mod\ n)$. Prove that $ca \equiv cb(mod\ cn)$.

Q12: If $x \in [0, 15)$ then solve the equation $3x \equiv 6(mod\ 15)$.

Q13: Prove that $6^n \equiv 6(mod\ 10), \forall n \in \mathbb{Z}^+$.

Q14: Prove that the ordered pair $(\{0, 4, 8, 12\}, +16)$ is a group.

Q15: Prove that the integer number n is divisible on q if and only if its summation of numbers is divisible on q.

7.8 Subgroups

Definition 7.26 Let $\phi \neq H \subseteq G$, and $(G, *)$ be a group. The binary $(H, */H)$ is a subgoup of $(G, *)$ if and only if $(H, */H)$ is a group, and $*/H$ is a restriction binary operation on $H \times H$(Hungerford, 1974; Dummit and Foote, 2004a).

Note: For convenience, we use $(H, *)$ instead of $(H, */H)$.

Example 7.24 (1) If $H = G$, then $(H, *)$ is a subgroup of $(G, *)$.

(2) Consider $H = \{e\}$, where e is an identity of the group $(G, *)$. $(\{e\}, *)$ is a subgroup of $(G, *)$.

(3) Consider the group $(\mathbb{R}, +)$. Each of $(\mathbb{Q}, +), (\mathbb{Z}_e, +), (\mathbb{Z}, +)$ are subgroups, while $(\mathbb{N}, +)$ is not a subgroup og $(G, +)$.

(4) Let $G = \{\pm 1, \pm i\}; i^2 = \sqrt{-1}$, and let $*$ be the ordinary multiplying operation. Or, $a * b = a.b, \forall a, b \in G$. Let $H = \{-1, 1\}$ then $(G, *)$ is a group, and $(H, *)$ is a subgroup of $(G, *)$.

(5) Consider $G = \mathbb{R} - \{0\}$ with the ordinary multiplying operation, and let $H = \mathbb{Q}^{+}$. Then, $(\mathbb{Q}^{+}, .)$ is a subset of $(G, .)$

Definition 7.27 Let $(H, *)$ be a subgroup of the group $(G, *)$. If $H \neq \{e\} \vee G$ then $(H, *)$ is called nontrivial subgroup of $(G, *)$ (Fraleigh, 2003).

Note: If $H = \{e\} \vee G$ then $(H, *)$ is called trivial subgroup of $(G, *)$.

Example 7.25 Consider the group $(\mathbb{Z}, *)$. and let H be a set of all multiples of the number 3 then $(H, *)$ is a nontrivial subgroup of $(\mathbb{Z}, *)$.

Theorem 7.15 *Let $\phi \neq H \subseteq G$, The $(H, *)$ is subgroup of the group $(G, *)$ if and only if*

(i) $a, b \in H \rightarrow a * b \in H$.

(ii) $a \in H \rightarrow a^{-1} \in H$.

Proof Suppose that $(H, *)$ is a subgroup of $(G, *)$.

(i) $\because (H, *)$ is a subgroup,

$\therefore a * b \in H$.

(ii) Suppose that $a \in H$.

$\because (H, *)$ is a subgroup,

$\therefore a^{-1} \in H$.

Conversely, suppose that $\phi \neq H \subseteq G$.

It should be noted that $a, b \in H \to a * b \in H$.

$\therefore *$ is a binary operation on H.

$\because *$ is an associated on G, and $H \subseteq G$,

$\therefore *$ is a binary operation on H.

From (ii), we get that $\forall a \in H \exists a^{-1} \in H$.

From (i), we have $a, a^{-1} \to a * a^{-1} \in H$.

But, $a * a^{-1} = e \in H$.

$\therefore H$ contains of an identity element.

$\therefore (H, *)$ is a group.

Thus, $(H, *)$ is a subgroup of $(G, *)$. ♦

Theorem 7.16 *Let $\phi \neq H \subseteq G$, and $(G, *)$ be a group. $(H, *)$ is a subgroup of $(G, *)$ if and only if $a, b \in H \to a * b^{-1} \in H, \forall a, b \in H$.*

Proof Suppose that $(H, *)$ is a subgroup of the group $(G, *)$, and let $a, b \in H$.

$\because b \in H \to \exists b^{-1} \in H$.

$\because *$ is a binary operation,

$\therefore a, b^{-1} \in H \to a * b^{-1} \in H$.

Conversely, suppose that $H \subseteq G$, in which, $a, b \in H \to a * b^{-1} \in H$ ...(1).

Now, we have to prove $(H, *)$ is a subgroup of $(G, *)$.

$\because H \neq \phi$,

$\therefore$ there is at least one element like $a \in H$.

From (1), we get that $a * a^{-1} = e \in H$.

Or, H contains of the identity element.

Again, from (1), $e * a^{-1} = a^{-1} \in H$.

Or, $\forall a \in H \to \exists a^{-1} \in H$.

$\therefore (H, *)$ is a group.

Now, we have to prove that $*$ is closed binary operation on H.

Let $a, b \in H$.

$\because b \in H \to b^{-1} \in H$.

From (1), we get that $a * (b^{-1})^{-1} \in H$.

But, $a * (b^{-1})^{-1} = a * b \in H$.

Thus, $(H, *)$ is a subgroup of $(G, *)$. ♦

Example 7.26 Consider the group $(\mathbb{Z}, +)$, $n \in \mathbb{Z}^{+}$, and let $H = \{na | a \in \mathbb{Z}\}$.

It possible to prove that $(H, *)$ is a subgroup of the group $(G, *)$ as follows:

Let $x, y \in H$.

$\because x, y \in H$,

$\therefore x = na, y = nb \ni a, b \in \mathbb{Z}$.

$\because y \in \mathbb{Z} \to \exists y^{-1} \in \mathbb{Z}$.

$\therefore y^{-1} = (nb)^{-1} = -nb$.

For instant $x * y^{-1} = x + y^{-1} = (na) + (-nb) = n(a - b)$.

$\because a - b \in \mathbb{Z}$,

$\therefore n(a - b) \in H$.

Thereby $x + y^{-1} \in H$, and implies that $(H, +)$ is a subgroup of the group $(\mathbb{Z}, +)$.

Theorem 7.17 *Let $\phi \neq H \subset G$, and be finite. Let $(G, *)$ be a group. If H be a closed set on the binary operation $*$ then $(H, *)$ is a subgroup of $(G, *)$.*

Proof Let $a \in H$.

$\because H$ is closed on $*$,

$\therefore a^2 = a * a \in H, a^3 = a^2 * a \in H, ...$ and so on.

In general, $a^m \in H, m \in \mathbb{Z}^{+}$.

Let, $S = \{a, a^2, ...\}$.

Note that each element in S is an element in H.

Thereby, the set is nonempty infinite, S is a subset of the finite set, and this is contradiction.

So, there is a repetition of elements of S. Or there are integer numbers like $r, s, r > s > 0 \wedge a^r = a^s$.

But, $a^s * a^{r-s} = a^s$.
$\because a^r = a^r * e = a^s * e$,
$\therefore a^s * a^{r-s} = a^s * e$,
Thereby, according on cancellation law in G, we get $a^{r-s} = e$.
$\because r - s > 0$,
$\therefore a^{r-s} \in H$.
$\therefore e \in H$.
$\because r - s > 0 \rightarrow r - s - 1 \geq 0$,
$\therefore a^{r-s-1} \in H$.
It should be noted that, $a * a^{r-s-1} = a^{r-s} = e$.
Or, $a * a^{r-s-1} = e$.
$\therefore a^{-1} = a^{r-s-1}$ is the inverse for a.
Thereby, we have proved that $a \in H \rightarrow a^{-1} \in H$.
Thus, $(H, *)$ is a subgroup of the group $(G, *)$. ⧫

Note: The opposite of the theorem is incorrect. Or, consider a group $(G, *)$, and infinite $\phi \neq H \subset G$. If H is closed set on $*$, it is not necessary $(H, *)$ be a subgroup of the group $(G, *)$, as shown in the following example.

Example 7.27 Consider the group $(G, *)$, and the set of $\mathbb{N}$.

Although $\mathbb{N}$ is closed on the ordinary addition, but $(\mathbb{N}, +)$ is not subgroup of $(\mathbb{N}, +)$.

Theorem 7.18 *Let $(G, *)$ be a group. If each of $(H_1, *), (H_2, *)$ be a subgroup of $(G, *)$ then $(H_1 \cap H_2, *)$ is a subgroup of $(G, *)$.*

Proof $\because e \in H_1 \wedge e \in H_2$,
$\therefore H_1 \cap H_2 \neq \phi$.
Suppose that $a, b \in H_1 \cap H_2$.
$\therefore a, b \in H_\wedge a, b \in H_2$.
$\therefore a * b^{-1} \in H_1$ (According on Theorem 7.16).
In the same way $\therefore a * b^{-1} \in H_2$ (According on Theorem 7.16).
$\therefore a * b^{-1} \in H_\cap H_2$.
Thereby, $a, b \in H_1 \cap H_2 \rightarrow a * b^{-1} \in H_1 \cap H_2$.
Thus, $(H_1 \cap H_2, *)$ is a subgroup of $(G, *)$. ⧫

Note: The opposite of the theorem is incorrect. Or, if each of $(H_1, *), (H_2, *)$ are subgroups on the group $(G, *)$ then in general

$(H_1, \cup H_2, *)$ not a subgroup of $(G, *)$. As shown in the following example.

Example 7.28 Consider the group $(\mathbb{Z}, +)$, and the sets

$H_1 = \{..., -4, -2, 0, 2, 4, ...\}, H_2 = \{..., -6, -3, 0, 3, 6, ...\}$.

Each of $(H_1, +), (H_2, +)$ are subgroups of the group $(\mathbb{Z}, +)$, while $(H_1 \cup H_2, +)$ is not a subgroup of $(\mathbb{Z}, +)$. For example, $2, 3 \in H_1 \cup H_2$ but $2 + 3 = 5 \notin H_1 \cup H_2$.

Theorem 7.19 *Let each of $(H_1, *), (H_2, *)$ be a subgroup of $(G, *)$. The $(H_1 \cup H_2, *)$ is a subgroup of $(G, *)$ if and only if $H_1 \subseteq H_2 \vee H_2 \subseteq H_1$.*

Proof Suppose that $H_1 \subseteq H_2$.

Obviously, $H_1 \cup H_2 = H_2$.

$\because (H_2, *)$ is a group,

$\therefore (H_1 \cup H_2, *)$ is a subgroup of $(G, *)$.

In the same way, if we suppose that $H_2 \subseteq H_1$, we get that $(H_1 \cup H_2, *)$ is a subgroup of $(G, *)$.

Conversely, suppose that $(H_1 \cup H_2, *)$ is a subgroup of $(G, *)$.

Suppose that $\sim (H_1 \subseteq H_2 \vee H_2 \subset H_1) \equiv H_1 \nsubseteq H_2 \wedge H_2 \nsubseteq H_1$.

Now, $\because H_1 \nsubseteq H_2$,

$\therefore \exists a \ni a \in H_1 \wedge a \notin H_2$.

$\because H_2 \nsubseteq H_1$,

$\therefore \exists b \ni b \in H_2 \wedge b \notin H_1$.

$\therefore a, b \in H_1 \cup H_2$.

$\because (H_1 \cup H_2, *)$ is a subgroup,

$\therefore a * b \in H_1 \cup H_2 \rightarrow a * b \in H_1 \vee a * b \in H_2$.

Suppose that $a * b \in H_1$.

$\because a \in H_1 \rightarrow \exists a^{-1} \in H_1$.

$\therefore a^{-1} * (a * b) \in H_1$.

But, $a^{-1} * (a * b) = (a^{-1} * a) * b = e * b = b \rightarrow b \in H_1$.

This is contradiction because $b \notin H_1$.

In the same way $a \in H_2$, and we get contradiction because $a \notin H_2$.

$\therefore H_1 \subseteq H_2 \vee H_2 \subseteq H_1$. ♦

7.8.1 Cyclic Groups

Before diving into the detail of a cyclic group, let us start with this introductory theorem below. Which it appears as a definition of the cyclic subgroup, and then we focus on definitions and deal with some theorems, and examples for the cyclic groups.

Theorem 7.20 *Let* $(G, *)$ *be a group, and let* $a \in G$. *If* $H = \{a^n | n \in \mathbb{Z}\}$ *then* $(H, *)$ *will be a subgroup of* $(G, *)$.

Proof Let $h_1, h_2 \in H$.
$\therefore h_1 = a^r, h_2 = a^s, r, s \in \mathbb{Z}$.
$\because h_1 * h_2^{-1} = a^r * (a^s)^{-1} = a^r * a^{-s} = a^{r-s} \in H$.
$\therefore (H, *)$ is a subgroup of $(G, *)$ (Theorem 7.16). ♦
Note: To convenience, we denote $\{a^n | n \in \mathbb{Z}\}$ by (a).

Definition 7.28 Let $(G, *)$ be a group, and $a \in G$. $((a), *)$ is called cyclic subgroup generated by a, and a is called generator (Lajoie and Mura, 2000; Balakrishnan and Ramabhadran, 1986; Herstein, 1996).

Definition 7.29 Let $(G, *)$ be a group, If there is an element $a \in G \ni (a) = G$ then $(G, *)$ is called cyclic group generated by a (Lajoie and Mura, 2000; Balakrishnan and Ramabhadran, 1986; Herstein, 1996).

Example 7.29 (1) $(\mathbb{Z}, +)$ is infinite cyclic group generated by 1. Because, $(1) = \{1^n | n \in \mathbb{Z}\} = \{n.1 | n \in \mathbb{Z}\} = \mathbb{Z}$.

(2) The group $(Z_3, +_3)$ is a finite cyclic group generated by [1] equivalence of one because
$[1]^1 = [1]$.
$[1]^2 = [1] +_3 [1] = [2]$.
$[1]^3 = [1] +_3 [1] +_3 [1] = [3] = [0]$.
$\therefore [1] = \{[1]^n | n\mathbb{Z}\} = \{[0], [1], [2]\}$
$\therefore ([1]) = Z_3$.

Note: The generator of a cyclic group is often not alone as demonstrated in the next example.

Example 7.30 (1) The cyclic group $\mathbb{Z}, +$ generated by each of (-1) and (1).

(2) The cyclic group $(\{e, a, a^2\}, *)$ generated by
$(a) = \{a^n | n \in \mathbb{Z}\} = \{a, a^2, a^3 = e\}$.
$(a^2) = \{(a^2)^n | n \in \mathbb{Z}\} = \{a^2, a^4 = a, a^6 = e\}$.

Theorem 7.21 *If $((a), *)$ is a finite cyclic group with the rank n then $(a) = \{e, a, a^2, ..., a^{n-1}\}$.*

Proof Since the set (a) is a finite, thereby the powers of it can not be differentiated.

$\therefore \exists i, j \in \mathbb{Z} \ni a^i = a^j, 0 < i < j$.
$\therefore a^i * a^{-i} = a^j * a^{-j}$
$\therefore a^0 = a^{j-i} \to e = a^{j-i}$.
Let us suppose that $W = \left\{k \in \mathbb{Z}^+ | a^k = e\right\}$
$\because a^{j-i} \ni j - i > 0 \to W \neq \phi$.
$\therefore W$ is well ordered set, implies W has a minimal element.
Suppose that m is a minimal element for W.
Or, $a^m = e$.
Since $a^k \neq e, 0 < k < m$.
Let $S = \{e, a, a^2, ..., a^{m-1}\}$,
Thereby, the elements of S are differentiated, and $\therefore S \subseteq (a)$ ...(1).
Because if $a^r = a^s \ni 0 \leq r < s \leq m - 1 \to a^{s-r} = e$.
But, $s - r < m$, and this is contradiction, thus S is differentiated.
Now, we have to prove, $(a) \subseteq S$.
Suppose that $b \in (a)$.
$\therefore b = a^1 \ni 1 \in \mathbb{Z}$.
Now, based on division algorithm, we have $1 = qm + r \ni q, r \in \mathbb{Z}, 0 \leq r < m$.
Thereby, $a^1 = a^{mq+r} = a^{mq} * a^r = (a^m)^q * a^r = e^q * a^r = e * a^r = a^r$
$\therefore a^1 = a^r$.
$\because a^r \in S$,
$\therefore b \in S$.
$\therefore (a) \subseteq S$ ...(2).
Thus, from (1)&(2), $(a) = S$.
Or, $(a) = \{e, a, a^2, ..., a^{m-1}\} \to m = n$.

$\therefore \{e, a, a^2, ..., a^{n-1}\}$. ♦

Definition 7.30 Let $(G, *)$ be a group, and $a \in G$. If $n \in \mathbb{Z}^+$ be the smallest number satisfied $a^n = e$ then n is called order of a, and denoted by $O(a)$. If does not exists n satisfied $a^n = e$ then it is said that a has infinite order (Dummit and Foote, 2004a; Artin, 1991).

Example 7.31 Let $(G, *)$ be a group, in which $G = \{1, -1, i, -1\}, i = \sqrt{-1}$, and $*$ is the ordinary multiplication operation.

It should be noted that 1 is the identity element, and $1^1 = 1, (-1)^2 = 1, (i)^4 = 1, (-i)^4 = 1$.

$\therefore O(1) = 1, O(-1) = 2, O(i) = 4, O(-i) = 4$.

(2) Consider the cyclic group $(G, *)$ with order of r, generated by $a \in G$. Or, $G = \{e, a, a^2, ..., a^5\}$.

It should be noted that $a^6 = e, (a^2)^3 = a^6 = e, (a^3)^2 = a^6 = e, (a^4)^3 = a^{12} = e, (a^5)^6 = a^{30} = e$.

$\therefore O(6) = 6, O(a^2) = 3, O(a^3) = 2, O(a^4) = 3, O(a^5) = 6$.

Definition 7.31 Let $(G, *)$ be a group, and $\phi \neq A, B \subset G$. The product of A, B defined as follows;

$AB = \{x \in G | x = a * b, a \in A, b \in B\}$(Ballester-Bolinches et al., 2010; Nicholson, 2012; Ledermann, 1973).

Example 7.32 Consider the group $(\mathbb{Z}, +)$, and $A = \{1, 3\}, B = \{2, 4\}$. The product of $AB = \{1+2, 1+4, 3+2, 3+4\} = \{3, 5, 5, 7\} = \{3, 5, 7\}$.

Note: If $(H, *), (K, *)$ are subgroups of $(G, *)$ then it is not necessary $(HK, *)$ will be a subgroup of $(G, *)$.

Example 7.33 Let S_3 be a group of permutation of degree 3. If $H = \{e, \psi\}$, where e= the identity element, and $\psi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix}$,

$K\{e, \chi\}$, where e= the identity element, and $\chi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_2 & x_1 \end{pmatrix}$.

Obviously, each of ψ, χ is a subgroup of S_3.

Now, let $HK = \{e, \psi, \chi, \psi\chi\}$, where $\psi\chi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix}$.

$\because$ it does not inverse of $\psi\chi$ in HK,
$\therefore \psi\chi$ it is not a subgroup of S_3.

Theorem 7.22 *If $(H, *)$ is a subgroup of the group $(G, *)$ then $HH = H$.*

Proof Let $x \in HH \rightarrow x = h_1 * h_2, h_1, h_2 \in H$.
$\because h_1, h_2 \in H \rightarrow h_* h_2 \in H$.
$\therefore x \in H$.
$\therefore HH \subseteq H ...(1)$.
Conversely, let $y \in H \rightarrow y * e \in HH$.
$\because e \in H$
$\because y * e = y$,
$\therefore y \in HH...(2)$.
From (1)&(2), $HH = H$. ♦

7.8.2 Right and Left Cosets of Subgroups

Definition 7.32 Let $(H, *)$ be a subgroup of the group $(G, *)$, and $a \in G$. The set $H * a = \{h * a | h \in H\}$ is called right coset of H in G. And, the set $a * H = \{a * h | h \in H\}$ is called left coset of H in G (Rotman, 2000; Rotman, 2013; Joshi, 1989).

Example 7.34 (1) Let $(H, *)$ be a subgroup of the group $(G, *)$. H will be a right coset and left coset for itself because
$H * e = \{h * e | h \in H\} = \{h | h \in H\} = H$.
$\therefore H * e = H$.
Also, $e * H = \{e * h | h \in H\} = \{h | h \in H\} = H$.
$\therefore e * H = H$.
(2) Let $H = \{..., -6, -3, 0, 3, 6, ...\}$. The following sets are right cosets of H in G:
$H + 0 = \{h + 0 | h \in H\} = H$.
$H + 1 = \{h + 1 | h \in H\} = \{..., -5, -2, 1, 4, 7, ...\}$.
$H + 2 = \{h + 2 | h \in H\} = \{..., -4, -1, 2, 5, 8, ...\}$.
.
.
.

Also,
$0 + H = \{0 + h|h \in H\} = H$.
$1 + H = \{1 + h|h \in H\} = \{..., -5, -2, 1, 4, 7, ...\}$.
$2 + H = \{2 + h|h \in H\} = \{..., -4, -1, 2, 5, 8, ...\}$.
.
.
.

Theorem 7.23 *If $(H, *)$ be a subgroup of the group $(G, *)$, and $a \in G$ then*

(i) $a * H = H \leftrightarrow a \in H$.

(ii) $H * a = H \leftrightarrow a \in H$.

Proof (i) Let $a \in H$, we have to prove that $a * H = H$.
Suppose that $x \in a * H$.
$\because x \in a * H$,
$\therefore h \in H \ni x = a * h$.
$\because a, b \in H$, and $(H, *)$ is a subgroup,
$\therefore a * h \in H \to x \in H$.
$\therefore a * H \subseteq H$ ...(1).
Now, let $y \in H$.
$\because y \in H$,
$\therefore y = e * y$.
$\because a * a^{-1} = e$,
$\therefore y = (a * a^{-1}) * y = a * (a^{-1} * y)$.
$\because a^{-1}, y \in H$,
$\therefore a^{-1} * y \in H$,
Thereby, $a * (a^{-1} * y) \in a * H$.
Or, $y \in a * H$.
$\therefore H \subseteq a * H$ ...(2).
From (1)&(2), we conclude that $a * H = H$.
Conversely, suppose that $a * H = H$.
$\because e \in H$,
$\therefore a * e \in a * H$.
But, $a * e = a$,

$\therefore a \in a * H$.

Thus, $a \in H$.

(ii) It can be proved in the same way. ♦

Theorem 7.24 *If $(H, *)$ be a subgroup of the group $(G, *)$, and $a, b \in G$ then*

(i) $H * a = H * b \leftrightarrow a * b^{-1} \in H$.

(ii) $a * H = b * H \leftrightarrow b^{-1} * a \in H$.

Proof (i) Suppose that $H * a = H * b$.

Now, $H * a = H * b$,

$\therefore H * (a * b^{-1}) = H * (b * b^{-1}) = H * e = H$.

$\therefore H * (a * b^{-1}) = H$.

Thereby, based on Theorem 7.23, we get that $a * b^{-1} \in H$.

Conversely, let $a * b^{-1}$.

Now, $\because a * b^{-1} \in H$, thereby based on Theorem 7.23, we conclude that $H * (a * b^{-1}) = H$.

$\therefore H * [(a * b^{-1}) * b] = H * b$,

$\therefore H * [a * (b^{-1} * b)] = H * b$,

$\therefore H * (a * e) = H * b$,

$\therefore H * a = H * b$.

(ii) Can be proved in the same method. ♦

Corollary

(i) *If $(H, *)$ be a subgroup of the group $(G, *)$, and $a, b \in G$ then*

(a) $H * a \cap H * b = \phi \vee H * a = H * b$.

(b) $a * H \cap b * H = \phi \vee a * H = b * H$.

(ii) *If $(H, *)$ is a subgroup of the group $(G, *)$ then the set of all right(left) cosets of H in G will be a partition of G.*

Proof (i) (a) Suppose that c is a common element between the right coset $H * a$ and the left coset $H * b$.

$\because c \in H * a,$

$\therefore \exists h_1 \in H \ni c = h_1 * a.$

$\because c \in H * b,$

$\therefore \exists h_2 \in H \ni c = h_2 * b.$

Thereby, $h_1 * a = h_2 * b.$

$\therefore h_2^{-1} * (h_1 * a) = h_2^{-1} * (h_2 * b)$

$(h_2^{-1} * h_1) * a = (h_2^{-1} * h_2) * b = e * b = b.$

$\therefore (h_2^{-1} * h_1) * a = b.$

Also, $[(h_2^{-1} * h_1) * a] * a^{-1} = b * a^{-1},$

$\therefore (h_2^{-1} * h_1) * (a * a^{-1}) = b * a^{-1},$

$\therefore (h_2^{-1} * h_1) * e = b * a^{-1}.$

$\therefore h_2^{-1} * h_1 = b * a^{-1}.$

$\because h_2^{-1}, h_1 \in H,$

$\therefore h_2^{-1} * h_1 \in H.$

$\therefore b * a^{-1} \in H.$

$\therefore H * b = H * a.$

Thus, we conclude that if there is a common element between the right coset $H * a$ and the right coset $H * b$ then the cosets will be equal. In addition, if there is no common element between them, then they are separate.

(b) In the same way, we can proof it.

(ii) The proof is left as an exercise to the reader. , ♦

Theorem 7.25 *If $(H, *)$ is a subgroup of the group $(G, *)$, and $a, b \in G$ then there exists a bijective between the right coset $H * a$ and the right coset $H * b$.*

Proof Let us define a mapping $f : H * a \to H * b | f(h * a) = h * b.$

Now, we have to prove the mapping is injective.

Suppose that $x, y \in H * a \ni f(x) = f(y).$

$\because x \in H * a,$

$\exists h_1 \in H \ni x = h_* a.$

$\because y \in H *,$

$\exists h_2 \in H \ni y = h_2 * a.$

Now, from the definition of the mapping

$f(x) = f(h_1 * a) = h_1 * b$.

$f(y) = f(h_2 * a) = h_2 * b$.

$\because f(x) = f(y)$,

$\therefore h_1 * b = h_2 * b \rightarrow h_1 = h_2$ (canceling b from both sides).

$\therefore h_1 * a = h_2 * a$.

$\therefore x = y$.

Thus, the mapping $f : H * a \rightarrow H * b$ is injective ...(1).

The mapping is surjective, because

For all $h*b \in h*b, h \in H$, there exists $h*a \in H*a \ni f(h*a) = h*b$ ...(2).

From (1)&(2), we get that the mapping $f : H * a \rightarrow H * b$. ♦

7.9 Lagrange's Theorem

This section talks about Lagrange's theorem (Birkhoff, 1935; Birkhoff and Mac, 1962; Birkhoff and Mac, 2017; Roth, 2001) which is concerned with groups and subgroups. To dealing with depth throughout the relation between groups and their subgroups, and to give some theorems and definitions on the relation between the order of groups and the order of subgroups.

Theorem 7.26 *If $(H, *)$ be a subgroup of the finite group $(G, *)$, then $O(H)$ divides $O(G)$ i. e. $\frac{O(H)}{O(G)}$.*

Proof Suppose that $O(G) = n, O(H) = m$.

$\because (H, *)$ is a subgroup of the group $(G, *)$,

$\therefore$ there is a partition for $(G, *)$ based on Theorem 7.24: Corollary 1, in which elements of the partition are the set of all right cosets of H in G.

$\because (G, *)$ is the finite group,

$\therefore$ the number of the right cosets is a finite say k.

$\therefore G = (H, e) \cup (H, a_1), ..., (H, a_{k-1})$.

Now, based on Theorem 7.25 there is a bijective between $H * e = H$ and $H * a_i, \forall i = 1, 2, ..., k - 1$.

$\because O(H) = m$,

$\therefore O(H * a_i) = n, \forall i = 1, 2, ..., k-1.$

$\therefore O(G) = \underbrace{m + m + ...m}_{k-\text{times}}.$

$\therefore n = km, k \in \mathbb{Z}^+.$

$\therefore O(H)$ divides $O(G)$.

Thus, $\frac{O(H)}{O(G)}$. ♦

Definition 7.33 Let $(H, *)$ be a subgroup of the group $(G, *)$. The index of $(H, *)$ in $(G, *)$ is a numbers of the different right cosets of H in G, and denoted by $i_G(H)$ (Fraleigh, 2003; Joshi, 1989; Rotman, 2013; Miller, 2012; Scott, 2012; Scott, 1987).

Note: If $(G, *)$ is the finite group, then $i_G(H) = \frac{O(G)}{O(H)}$.

Example 7.35 Consider the $(\mathbb{Z}, +)$, and $H = (3)$. The $(H, +)$ is subset of the group $(\mathbb{Z}, +)$. The different right cosets of H in G are

$H + 0 = H, H + 1, H + 2.$

Thus, $i_G(H) = 3$.

Corollary

(i) *If $(G, *)$ be a finite group, $a \in G$, then the number $O(a)$ divides $O(G)$.*

(ii) *If $(G, *)$ be a finite group, and $a \in G$, then $a^{O(G)} = e$.*

Proof (i) Suppose that $H = (a)$.

$\because H = (a),$

$\therefore (H, *)$ will be a subgroup of the group $(G, *)$.

As a knowledge $H = \{e, a, a^2\}$, and let $O(a) = m$.

$\therefore a^m = e.$

Thus, H contains at most m of elements.

Now, we have to prove that H is contains at least m of elements. Because if the number of elements of H is leas than m, then there exist i, j of integer numbers in which $0 \leq i \leq j < m$.

$\because a^i = a^j,$

$\therefore a^{j-i} = e.$

But, this is construction because $j-i<m$, where m is the smallest integer in which $a^m=e$.

Thereby, H contains at least m of elements in which $O(H)=m$.

Thus, based on Lagrange's theorem (Theorem 7.26), m divides $O(G)$. Or, $\frac{O(a)}{O(G)}$.

(ii) Based on Corollary 1, we have $\frac{O(a)}{O(G)}$.

$\therefore O(G)=kO(a), k\in\mathbb{Z}$.

$\therefore a^{O(G)}=a^{kO(a)}=(a^{O(a)})^k=e^k=e.$ ♦

7.9.1 Normal Subgroups

Definition 7.34 Let $(H,*)$ be a subgroup of the group $(G,*)$. The $(H,*)$ is a normal subgroup of The group $(G,*)$ if and only if $a*h*a^{-1}\in H,\forall h\in H, a\in G$, and denoted by $H\lhd G$(Cantrell, 2000; Dummit and Foote, 2004a; Dummit and Foote, 2004b; Fraleigh, 2003; Hall, 2018; Robinson, 2012).

Note: Let $(H,*)$ be subgroup of the group $(G,*)$. The $(H,*)$ will be normal subgroup of $(G,*)$ if and only if $a*H*a^{-1}\subseteq H,\forall a\in G$.

Example 7.36 (1) Consider the group $(\mathbb{R},+)$, then $(\mathbb{Z},+)$ will be a normal subgroup of $(\mathbb{R},+)$ because

(a) $(\mathbb{Z},+)$ is subgroup of $(\mathbb{R},+)$.

(b) $\forall a\in\mathbb{R}, h\in\mathbb{Z}|a+h-a=h\in\mathbb{Z}$.

In general, every subgroup of a commutative group is a normal subgroup.

(2) Consider $S_3, H=\{e,\psi\}$, where $\psi=\begin{pmatrix}x_1 & x_2 & x_3\\ x_2 & x_1 & x_3\end{pmatrix}$ It should be noted that H is a nonnormal subgroup.

While $\Gamma=\{e,\lambda,\lambda^2\}$, where $\lambda=\begin{pmatrix}x_1 & x_2 & x_3\\ x_2 & x_3 & x_1\end{pmatrix}$ is a normal subgroup.

Theorem 7.27 *If $(H,*)$ is a subgroup of the $(G,*)$ then $(H,*)$ is a normal subgroup of $(G,*)$ if and only if $a*H*a^{-1}=H,\forall a\in G$.*

Proof Suppose that $a * H * a^{-1} = H, \forall a \in G$.

$\therefore a * H * a^{-1} \subseteq H, \forall a \in G$.

Thereby, $(H, *)$ is a normal subgroup of $(G, *)$.

Conversely, Suppose that $(H, *)$ is a normal subgroup of $(G, *)$.

Now, from the definition of the normal subgroup, we have

$a * H * a^{-1}, \forall a \in G$ ...(1).

$\because a^{-1} \in G$,

$\therefore$ from the Definition 7.33, we have $a^{-1} * H * (a^{-1})^{-1} \subseteq H$.

Or, $a^{-1} * H * a \subseteq H$.

$\therefore a * (a^{-1} * H * a) * a^{-1} \subseteq a * H * a^{-1}$.

$\therefore H \subseteq a * H * a^{-1}$ ...(2).

Thus, from (1)&(2), we get that $H = a * H * a^{-1}$. ♦

Theorem 7.28 *If $(H, *)$ be a subgroup of the group $(G, *)$ then $(H, *)$ is a normal subgroup if and only if each right coset, it is also a left coset.*

Proof Suppose that $(H, *)$ is a normal subgroup of the group $(G, *)$.

So, based on the Theorem 7. 27, $a * H * a^{-1} = H, \forall a \in G$.

$\therefore (a * H * a^{-1}) * a = H * a$,

$\therefore a * H = H * a$.

Thus, every right coset, it is also a left coset.

Conversely, suppose that every right coset, it is also a left coset, and let $a \in G$.

So, $H * a = \{h * a | h \in H\}$ is a right coset.

$\because e \in H$,

$\therefore e * a \in H * a$.

$\because e * a = a$,

$\therefore a \in H * a$.

Now, it should be noted that if left coset equal to the right coset $(H * a)$ has to contain of a. Suppose that L is represents to left coset, and contains of a.

$\because a * H$ is also contains of a.

$\therefore a \in L \wedge a \in a * H$.

$\therefore$ according to the Corollary of Theorem 7.24, $L = a * H$.

$\therefore a * H$ is a unique left coset equal to $H * a$.

Now, we have $H * a = a * H$.

$\therefore H * a * a^{-1} = a * H * a^{-1}$,

$\therefore H = a * H * a^{-1}, \forall a \in G$.

Thus, $(H, *)$ is a normal subgroup of the $(G, *)$. ♦

Theorem 7.29 *If $(H, *)$ be a subgroup of the group $(G, *)$ then $(H, *)$ is a normal subgroup if and only if a product of any right cosets of H in G is also a right coset of H in G.*

Proof Suppose that $(H, *)$ is a normal subgroup of $(G, *)$.

$\therefore H * a = a * H, \forall a \in G$ ...(1).

Suppose $a, b \in G$,

$\therefore a * b \in G$, and each of $H * (a * b), H * a, H * b$ is a right coset of H in G.

It should be noted that $(H * a)(H * b) = H(a * H) * b$.

From (1), $(H*a)(H*b) = H(a*H)*b = H(H*a)*b = HH*(a*b) = H * (a * b)$, from Theorem 7.22.

$\because H * (a * b)$ is a right coset of H in G,

$\therefore (H * a)(H * b)$ is a right coset of H in G.

Conversely, suppose that a product of any two right cosets of H in G is also a right coset of H in G.

Now, we have to prove that $(H, *)$ is a ormal subgroup of the group $(G, *)$.

Suppose that $a \in G \to a^{-1} \in G$.

$\therefore H * a, H * a^{-1}$ are right cosets of H in G.

$\because e \in H$,

$\therefore e * a \in H * a, e * a^{-1} \in H * a^{-1}$.

Thereby, $(e * a) * (e * a^{-1}) \in (H * a)()H * a^{-1}$.

$\because (e * a) * (e * a^{-1}) = e \to e \in (H * a)(H * a^{-1})$.

$\because (H * a)(H * a^{-1})$ is a right coset of H in G,

$\therefore (H * a)(H * a^{-1})$ contains of e.

$\because H = H * e$ is a right coset contains of e.

Thereby, and based on Corollary of Theorem 7.24, we get that
$(H * a)(H * a^{-1}) = H, \forall a, a^{-1} \in G$.

$\therefore (h_1 * a)(h * a^{-1}) = H, \forall h_1, h \in H \land a, a^{-1} \in G$.

It should be noted that $h_1^{-1} * [(h_1 * a) * (h * a^{-1})] \in h_1^{-1}H$.

$\because h_1^{-1} \in H$,
$\therefore h_1^{-1}H = H$.
$\because h_1^{-1} * [(h_1 * a) * (h * a^{-1})] = a * h * a^{-1}$,
$\therefore a * h * a^{-1} \in H$.
Thus, $(H, *)$ is a normal subgroup of the group $(G, *)$. ♦

7.9.2 Quotient Groups

Definition 7.35 If $(H, *)$ is a normal subgroup of the group $(G, *)$ then $G/H = \{H * a | a \in G\}$ is called a quotient group (factor group)(Dummit and Foote, 2004a; Herstein, 1975).

Note: (1) G/H is denoted to all cosets of H in G in which right cosets of H in G are equal to left cosets of H in G, and denoted for convenient by $H * a$.

(2) $\odot$ is a restricted of a product for all subsets of the group $(G, *)$, and called production of the cosets of H in G.

(3) $\odot$ is a binary operation on the set G/H, and $(G/H, \odot)$ is a mathematical system.

(4) If $X, Y \in G/H$ then XY denote that $X \odot Y$.

Theorem 7.30 *If $(H, *)$ is a normal subgroup of the group $(G, *)$ then the mathematical system $(G/H, \odot)$ is a group, and it is called quotient group G over H.*

Proof (1) $\odot$ is association binary operation.
Suppose that $X, Y, Z \in G/H$.
So, $X = H * a, Y = H * b, Z = H * c, \forall a, b, c \in G$.
It should be noted that
$X(YZ) = (H*a)[(H*b)(H*c)] = H*a[H*(b*c)] = H*[a*(b*c)] = H * [(a * b) * c]$.
$\therefore X(YZ) = [H * (a * b)](H * c) = [(H * a)(H * b)](H * c) = (XY)Z$.
$\therefore \odot$ is associated binary operation.
(2) Existence of the identity element.
We are going to prove that $H = H * e$ is the identity element.
Suppose that $X \in G/H$.
$\therefore X = H * a$.

It should be noted that

$XH = (H * a)(H * e) = H * (a * e) = H * a = X$.

Also, $HX = (H * e)(H * a) = H * (e * a) = H * a = X$.

Thereby, $HX = XH = X$.

Thus, $H = H * e$ is the identity element.

(3) Existence of inverse of the element.

Suppose that $X \in G/H$.

$\therefore X = H * a, \forall a \in G$.

Now, we have to prove that $H * a^{-1}$ is inverse of $H * a$.

$\because a^{-1} \in G$,

$\therefore H * a^{-1}$ is a coset of H in G.

$\because (H * a)(H * a^{-1}) = H * (a * a^{-1}) = H * e = H$.

Also, $(H * a^{-1})(H * a) = H * (a^{-1} * a) = H * e = H$.

$\therefore (H * a)(H * a^{-1}) = (H * a^{-1})(H * a) = H$.

$\therefore H * a^{-1}$ is the inverse of $H * a$.

From (1), (2) & (3) we conclude that $(G/H, \odot)$ is a group. ♦

Corollary *(1) If $(G, *)$ is a commutative group then $(G/H, \odot)$ is a commutative group.*

(2) If $(G, *)$ is a finite group then $O(G/H) = \frac{O(G)}{O(H)}$.

Proof (1) Let $X, Y \in G/H$.

$\therefore X = H * a, Y = H * b, \forall a, b \in G$.

$\because XY = (H * a)(H * b) = H * (a * b)$.

$\because (G, *)$ is a commutative group,

$\therefore a * b = b * a$.

$\therefore H * (a * b) = H * (b * a)$.

$\therefore XY = H * (a * b) = H * (b * a) = YX$.

Thus, $XY = YX$.

(2) Let $O(G) = n, O(H) = m$, and let the number of cosets of H in $G = k$.

$\therefore O(G/H) = k$.

$\therefore$ based on Lagrange theorem (Theorem 7.26), we have $n = mk$.

$\therefore k = \frac{n}{m}$.

Thus, $O(G/H) = \frac{O(G)}{O(H)}$. ♦

Example 7.37 Let G be a group of the integer numbers with addition operation, and $\mathbb{N}$ be the set of all multiples of 5.

Let $a \in G$, and based on the division algorithm, we have
$a = 5b + c, b \in G, c = 0, 1, 2, 3, 4.$
$\therefore \mathbb{N} + a = \mathbb{N} + 5b + c = (\mathbb{N} + 5b) + c = \mathbb{N} + c.$
$\therefore \mathbb{N}, \mathbb{N} + 1, \mathbb{N} + 2, \mathbb{N} + 3, \mathbb{N} + 4$ are the right cosets of $\mathbb{N}$ in G.
It should be noted that $(\mathbb{N} + 3) + (\mathbb{N} + 3+ = \mathbb{N} + 1$

7.10 exercises

Solve the following questions:

Q1: Let G be a group, and $W \subseteq G$. Consider (W) the set of all elements of G in which represented as a multiply finite sets of W to the power integer number. Prove that (W) is a subgroup of G *[Hint: (W) is a subset of G generated by W].*

Q2: If G is a group, and $O(G) = P$, and P is a prime number. Prove that G is a cyclic group.

Q3: If each of H, K are subgroups of the group G. Prove that HK is a subgroup of G if and only if $HK = KH$.

Q4: If each of H, K are subgroups of the commutative group G. Prove that HK is a subgroup of G.

Q5: Consider a finite group G in which $O(G) = Pq$, P, q are prime numbers and $P > q$. Prove that G has at most a unique subgroup in order P.

Q6: If each of H, K are subgroups of the commutative group G, in which $O(H) = n, O(K) = m$. Prove that G has a subgroup L where $O(L) = [n, m]$ *[Hint: $[n, m]$ is the simple common multiple of the numbers $[n, m]$.*

Q7: Let $a \in G$, and define $N(a) = \{x \in G | Xa = aX\}$. Prove that $N(a)$ is a subgroup of G *[Hint: $N(a)$ is called a normalizer of a in G].*

Q8: Let G be a group, and define $Z_G = \{z \in G | zx = xz, \forall x \in G\}$. Prove that Z_G is a subgroup of G *[Hint: Z_G is called a center of G].*

Q9 Prove that any subgroup of a cyclic group is a cyclic group.

Q10: Let G be a cyclic group in order n. How many generators have G? Prove your answer.

Q11: Let G be a group, and $a \in G$. If $a^m = e, \forall m \in \mathbb{Z}$ prove that $O(a)/m$ ($O(a)$ divisible over m).

Q12: Let H be a subgroup of the group G, in which $i(H) = 2$. Prove that H is a normal subgroup of G.

Q13: If each of K, L are normal subgroups of the group G then KL is a normal subgroup of G.

Q14: If each of K, L are normal subgroups of the group G then $K \cap L$ is a normal subgroup of G.

Q15: If each of K, L are normal subgroups of the group G then $K \cap L$ is a normal subgroup of K.

Q16: Give an example of a commutative group in which all its subgroups are normal.

Q17: If each of K, L are normal subgroups of the group G then KL is a normal subgroup of G.

Q18: Give an example on groups G, K, L in which L be a normal subgroup of K, and K be a normal subgroup of G, but L is not a normal subgroup of G.

7.11 Homomorphism and Isomorphism

7.11.1 Homomorphism

Definition 7.36 If each of $(G, *), (G', \circ)$ be groups and $f : G \to G'$ be a mapping from G to G' then $f : G \to G'$ is called a homomorphism from $(G, *)$ to $(G', \circ)$ if and only if $f(a * b) = f(a) \circ f(b), \forall a, b \in G$ (Dummit and Foote, 2004a; Lang, 2002b).

Example 7.38 Consider the groups $(G, *), (G', \circ)$, and the mapping $f : G \to G'$, defined as $f(a) = \bar{e}, \forall a \in G$ where $\bar{e}$ is the identity element in G'.

The mapping $f : G \to G'$ is a homomorphism from $(G, *)$ to $(G', \circ)$, because $\forall a, b \in G$

$f(a * b) = \bar{e}, f(a) = \bar{e}, f(b) = \bar{e}$.

On the other hand, $f(a) \circ f(b) = \bar{e} \circ \bar{e} = \bar{e}$.

$\therefore f(a * b) = f(a) \circ f(b) = \bar{e}$.

Example 7.39 Consider the groups $(\mathbb{R}, +), \mathbb{R} - \{0\}$, and the mapping $f : (\mathbb{R} \to \mathbb{R} - \{0\}$ defined as $f(a) = 2^a, \forall a \in \mathbb{R}$.

The mapping f is homomorphism, because $\forall a, b \in \mathbb{R}$, we have
$f(a+b) = a^{a+b}, f(a) = 2^a, f(b) = 2^b$.
But, $f(a+b) = 2^{a+b} = 2^a.2^b = f(a).f(b)$.
Or, $f(a+b) = 2^{a+b} = f(a).f(b)$.
$\therefore f : (\mathbb{R} \to \mathbb{R} - \{0\}$ is a Homomorphism.

Theorem 7.31 *If $f : G \to G'$ is a homomorphism from the group $(G, *)$ to the group $(G', \circ)$, then*
(a) $f(e) = \bar{e}$, where $e, \bar{e}$ are identity elements of G, G' respectively.
(b) $f(a^{-1}) = f(a)^{-1}, \forall a \in G$.

Proof (a) Let $a \in G$.
$\because a \in G, \therefore f(a) \in G'$.
$\because \bar{e}$ is the identity element of G',
$\therefore f(a) \circ \bar{e} = f(a)...(1)$.
$\because a * e = e$,
$\therefore f(a) = f(a * e)$.
$\because f : G \to G'$ is a homomorphism,
$\therefore f(a * e) = f(a) \circ f(e)$.
$\therefore f(a) \circ f(e) = f(a)...(2)$.
It results from (1)& (2) $f(a) \circ f(e) = f(a) \circ \bar{e}$.
$\because (G', \circ)$ is a group,
$\therefore$ by canceling $f(a)$ of both sides, it results that $f(e) = \bar{e}$.
(b) Suppose that $\forall a \in G, \exists a^{-1} \in G \ni a * a^{-1} = a^{-1} * a = e$.
$\therefore f(a * a^{-1}) = f(e)$.
$\because f : G \to G'$ is a homomorphism,
$\therefore f(a * a^{-1}) = f(a) \circ f(a^{-1})$.
From (a), we have $f(e) = \bar{e}$,
$\therefore f(a) \circ f(a^{-1}) = \bar{e}$.
In the same way, $f(a^{-1}) \circ f(a) = \bar{e}$.
$\therefore f(a) \circ f(a^{-1}) = f(a^{-1}) \circ f(a) = \bar{e}$.
Thereby, $f(a^{-1})$ is the inverse of $f(a)$ in the group $(G', \circ)$.
Thus, $[f(a)]^{-1} = f(a^{-1})$. ⧫

Theorem 7.32 *If $f : G \to G'$ be a mapping from the group $(G, *)$ to the group $(G', \circ)$, then*

(a) For all subgroup $(H, *)$ of $(G, *)$, the ordered pair $(f(H), \circ)$ will be subgroup of $(G', \circ)$.

(b) For all subgroup $(H', \circ)$ of $(G', \circ)$, the ordered pair $(f^{-1}(H'), *)$ will be subgroup of $(G, *)$.

Proof (a) Suppose that $a, b \in f(H)$.

$\because a, b \in f(H)$,

$\exists h, k \in H \ni f(h) = a, f(k = b)$.

$\because (H, *)$ is a group,

$\therefore h * k^{-1} \in H$.

$\therefore f(h * k^{-1}) \in f(H)$.

$\because f : G \to G'$ is homomorphism,

$\therefore f(h * k^{-1}) = f(h) \circ f(k^{-1})$, and based on Theorem 7.31, it is concluded that

$[f(k)]^{-1} = f(k^{-1})$.

$\therefore f(h * k^{-1}) = f(h) \circ [f(k)]^{-1} = a \circ b^{-1}$.

Thereby, $a \circ b^{-1} \in f(H)$.

Or, $a, b \in f(H) \to a \circ b^{-1} \in f(H)$.

Thus, $(f(H), \circ)$ is a subgroup of $(G', \circ)$.

(b) Let $a, b \in f^{-1}(H')$, in which $f^{-1}(H') = \{x \in G | f(x) \in H^{-1}\}$.

$\therefore f(a) \in H^{-1}, f(ba) \in H^{-1}$.

$\because (H', \circ)$ is a subgroup of $(G', \circ)$,

$\therefore f(a) \circ [f(b)]^{-1} \in H'$.

$\because f : G \to G'$ is homomorphism,

$\therefore [f(b)]^{-1} = f(b^{-1})$.

$\therefore f(a) \circ [f(b)]^{-1} = f(a) \circ f(b^{-1}) = f(a * b^{-1})$.

$\therefore f(a * b^{-1}) \in H \to a * b^{-1} \in f^{-1}(H')$.

Thereby, $a, b \in f^{-1}(H') \to a * b^{-1} \in f^{-1}(H')$.

Thus, $(f^{-1}(H'), *)$ is a subgroup of $(G, *)$. ♦

Definition 7.37 Let $f : G \to G'$ be a homomorphism from the group $(G, *)$ to the group $(G', \circ)$, and $\bar{e}$ be the identity element in $(G', \circ)$. The set of all elements of the $(G, *)$ in which their images is $\bar{e}$ is called kernal of f, and denoted by $ker(f) = \{a \in G | f(a) = \bar{e}\}$(Dummit and Foote, 2004a; Lang, 2002b; Axler, 2015; Lay, 2005).

Example 7.40 Let $(G, *) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a group of all real matrices 2×2, in which $a.d - b.c \neq 0$. Let $G' = (\mathbb{R} - \{0\})$.

Define a mapping $f : G \to G'$, where $f(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = ad - bc$.

(1) f is a homomorphism mapping from G to G' (How?).

(2) $kerf = \{x \in G | f(x) = 1\} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G | ad - bc = 1 \right\}$. For Example, $\begin{bmatrix} \frac{1}{5} & 2 \\ 0 & 5 \end{bmatrix} \in kerf$.

Theorem 7.33 *If $f : G \to G'$ is a homomorphism from the group $(G, *)$ to the group $G', \circ$ then the ordered pair $(kerf, *)$ will be a normal subgroup of $(G, *)$.*

Proof $\because f(e) = \bar{e}$,

$\therefore e \in ker(f) \to ker(f) \neq \phi$.

Now, to prove that $(ket(f), *)$ is a subgroup of $(G, *)$, suppose that $a, b \in ker(f)$.

$\because a, b \in ker(f)$,

$\therefore f(a) = \bar{e}, f(b) = \bar{e}$.

$\because f$ is a homomorphism,

$\therefore f(a * b^{-1}) = f(a) \circ f(b^{-1}) = f(a) \circ [f(b)]^{-1} = \bar{e} \circ (\bar{e})^{-1} = \bar{e} \circ \bar{e} = \bar{e}$.

$\therefore f(a * b^{-1}) = \bar{e}$.

$\therefore a * b^{-1} \in ker(f)$.

Or, $a, b \in ker(f) \to a * b^{-1} \in ker(f)$.

Thus, $(ker(f), *)$ is a subgroup of $(G, *)$.

To prove that, $(ker(f), *)$ is a normal subgroup of $(G, *)$, suppose that $a \in G, n \in ker(f)$.

$\because a \in G, n \in ker(f)$,

$\therefore f(n) = \bar{e}$.

$\because f : G \to G'$ is a homomorphism,

$\therefore f(a * n * a^{-1}) = f(a) \circ f(n) \circ f(n^{-1}) = f(a) \circ \bar{e} \circ [f(a)]^{-1} = f(a) \circ [f(a)]^{-1} = \bar{e}$.

$\therefore f(a * n * a^{-1}) = \bar{e} \to a * n * a^{-1} \in ker(f)$.

Thus, $(ker(f), *) \lhd (G, *)$. ♦

Theorem 7.34 *If $f : G \to G'$ be a homomorphism from the group $(G, *)$ to the group $(G', \circ)$ then the mapping f will be injective if and only if $ker(f) = \{e\}$.*

Proof Suppose that $f : G \to G'$ is the injective, and let $a \in ker(f)$.

$\because a \in ker(f)$,

$\therefore f(a) = \bar{e}$.

$\because f(e) = \bar{e}$,

$\therefore f(a) = f(e)$.

$\because f : G \to G'$ is the injective, it means $ker(f)$ contains only of the identity element e.

$\therefore ker(f) = \{e\}$.

Conversely, suppose that $ker(f) = \{e\}$.

To prove that the mapping $f : G \to G'$ is injective, suppose that $a, b \in G \ni f(a) = f(b)$.

$\because f : G \to G'$ is the injective mapping,

$\therefore f(a * b^{-1}) = f(a) \circ f(b^{-1}) = f(a) \circ [f(b)]^{-1} = e^{-1}$.

$\therefore f(a * b^{-1}) = e^{-1}$.

$\therefore a * b^{-1} \in ker(f)$.

$\because ker(f) = e$,

$\therefore a * b^{-1} = e$.

Thereby, $(a * b^{-1}) * b = e * b, a * b^{-1} = e$.

Thus, $a = b$. ♦

Theorem 7.35 *Let $(\mathbb{N}, *) \lhd (G, *)$. The canonical mapping $i_{\mathbb{N}} : G \to G/\mathbb{N}$ defined by $i_{\mathbb{N}}(x) = \mathbb{N} * x$ will be homomorphism, surjective and $ker(i_{\mathbb{N}}) = \mathbb{N}$.*

Proof To prove that the mapping $i_{\mathbb{N}} : G \to G/\mathbb{N}$ is homomorphism, suppose that $a, b \in G$.

$\because a, b \in G$,

$\therefore i_{\mathbb{N}}(a) = \mathbb{N} * a, i_{\mathbb{N}}(b) = \mathbb{N} * b$.

$\because a, b \in G$,

$\therefore i_{\mathbb{N}}(a * b) = \mathbb{N} * (a * b)$.

$\because (\mathbb{N}, *) \lhd (G, *)$,

$\therefore$ according Theorem 7.29, $\mathbb{N} * (a * b) = (\mathbb{N} * a)(\mathbb{N} * b)$.

$\therefore i_{\mathbb{N}}(a * b) = (\mathbb{N} * a)(\mathbb{N} * b) = i_{\mathbb{N}}(a) i_{\mathbb{N}}(b)$.

Thus, the mapping is homomorphism.

To prove that the mapping is surjective, let $Y \in G/\mathbb{N}$.

$\because Y \in G/\mathbb{N}$,

$\therefore Y = \mathbb{N} * a, \forall a \in G$.

Let $i_{\mathbb{N}}(a) = \mathbb{N} * a$.

$\therefore \forall \mathbb{N} * a \in G/\mathbb{N} \exists a \in G | i_{\mathbb{N}}(a) = \mathbb{N} * a$.

$\therefore i_{\mathbb{N}} : G \to G/\mathbb{N}$.

Now, we have to prove that $ker(i_{\mathbb{N}}) = \mathbb{N}$.

It should be noted that $ker(i_{\mathbb{N}}) = \{a \in G | i_{\mathbb{N}}(a) = \mathbb{N}\} = \{a \in G | \mathbb{N} * a = \mathbb{N}\} = \{a \in G | a \in \mathbb{N}\} = \mathbb{N}$.

$\therefore ker i_{\mathbb{N}} = \mathbb{N}$. ♦

7.11.2 Isomorphism

Definition 7.38 If $(G, *), (G', \circ)$ are groups, and $f : G \to G'$ be a mapping then f is an isomorphism if and only if it is a homomorphism and injective mapping (Dummit and Foote, 2004a; Lang, 2002b).

Example 7.41 (1) Let $G = (\mathbb{R}, +), G' = (\mathbb{R} - \{0\}, .)$, and the mapping $f : G \to G'$, in which $f(a) = 2^a$.

(a) f is a homomorphism. (b) f is an injective function because $f(a) = f(b) \leftrightarrow 2^a = 2^b$,

$2^a = 2^b \leftrightarrow a = b, \forall a, b \in G$.

$\therefore f : G \to G'$ is an isomorphic mapping.

It should be noted that f is not surjective function. Thereby f is called isomorphic embedding.

(2) Let $G = (\mathbb{Z}, +), G'_n = (\mathbb{Z}_n, +_n)$, and $f : G \to G'_n$ be a mapping in which $f(x) = [x], \forall x \in G$.

For illustrating, let $n = 6$, we find that

$f(20) = [20] = [2]$, and note that $f(26) = [26] = [2]$.

$\therefore f$ is not injective.

Thus, f is not isomorphic mapping from G to G'_n.

Definition 7.39 It is said that the two groups $(G, *), (G', \circ)$ are isomorphic if and only if there is a complete isomorphic between them, and denoted by $(G, *) \approx (G', \circ)$ (Dummit and Foote, 2004a; Lang, 2002b; Herstein, 1975; Herstein, 1996; Herstein, 2006).

Note:

(i) (a) $G \approx G$.

(b) $G \approx G' \to G' \approx G$.

(c) $(G \approx G') \wedge (G' \approx G'') \to (G \approx G'')$.

(ii) Let $f : G \to G'$ be a homomorphism mapping, then

(a) f is a surjective.

(b) $ker(f) = (0)$.

Example 7.42 (1) $(\mathbb{Z}_n, +_4) \approx (\{\mp 1, \mp i\}, .)$.

(2) $(\mathbb{Z}, +) \not\approx (\mathbb{Q} - \{0\}, .)$.

Because if $(\mathbb{Z}, +) \approx (\mathbb{Q} - \{0\}, .)$, it should be surjective homomorphism and injective mapping between them, $f : \mathbb{Z} \to \mathbb{Q} - \{0\}$, and we get a contradiction. For illustration, suppose that $x \in \mathbb{Z}$, in which $f(x) = -1$.

$\therefore f(x + x) = f(x).f(x) = (-1).(-1) = 1$.

$\because ker(f) = (0)$,

$\therefore 2x = 0 \to x = 0 \to f(0) = -1$.

$\because f(0) = 1$.

Thus, we get the contradiction.

Theorem 7.36 *If $\varphi : G \to G'$ be a homomorphism and surjective mapping in which $ker\varphi = W$, then $\frac{G}{W} \approx G'$.*

Proof Consider the Figure 7.1, where $\rho(g) = wg$, and $\rho : G \to G/W$ is the canonical mapping.

The aim is to complete the figure into Figure 7.2, where $\psi : G/W \to G'$ is a mapping and defined as follows

$X \in G/W$ in which $X = WG, \forall g \in G$.

Now, we define $\psi(wg) = \varphi(g)$. The defined function is

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, "\rho"'] & G' \\
G/W &
\end{tikzcd}$$

Figure 7.1: Isomorphic Mapping

(a) Well defined.
Suppose $X = Wg = Wg', \forall g, g' \in G$.
Currently, $\psi(X) = \varphi(g), \psi(X) = \varphi(g')$.
Currently, $Wg = Wg' \ni g = rg', r \in W$.
$\therefore \varphi(g) = \varphi(rg') = \varphi(r)\varphi(g') = e\varphi(g') = \varphi(g')$.
Thereby, φ is a well defined mapping.
(b) ψ is surjective.
Suppose that $\bar{x} \in \bar{G}$.
$\because \bar{x} \in \bar{G}\exists g \in G|\bar{x} = \varphi(g)$ because φ is surjective.
Thereby $\bar{x} = \varphi(g) = \psi(g)$.
(c) ψ is isomorphism.
Suppose that $X \in G/W$.
$\because X \in G/W$,
$\therefore X = Wg, Y = Wf, \forall g, f \in G$.
Now, $\psi(XY) = \psi(WgWf) = \psi(Wgf) = \varphi(gf) = \varphi(g)\varphi(f) = \psi(X)\psi(Y)$.
(d) $ker\psi = W(\psi$ is injective homomorphism).
Let $\psi(Wg) = \bar{e}$.

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, "\rho"'] & G' \\
G/W \arrow[ur, "\psi"'] &
\end{tikzcd}$$

Figure 7.2: Complete Isomorphic Mapping

$\because \psi(Wg) = \psi(g),$

$\therefore \psi(g) = \bar{e}.$

Thereby, $g \in ker\varphi = W \to Wg = W.$

$\therefore Wg \in ker\varphi \to Wg = W.$

$\therefore ker\varphi = W.$

Thereby, ψ is surjective homomorphism and injective from G/W to G'.

Thus, $\frac{G}{W} \approx G'$. ♦

7.12 Exercises

Solve the following questions:

Q1: Verify a homomorphism of the following mapping if they are isomorphic mapping then find kernel of them.

(a) $\phi : (\mathbb{R} - \{0\}, .) \to G'$, where $\phi(x) = x^2, \forall x \in G.$

(b) $\phi : (\mathbb{R}, +) \to G'$, where $\phi(x) = x + 1, \forall x \in G.$

(c) Let G be a commutative group, and $\phi : G \to G'$, where $\phi(x) = x^5, \forall x \in G.$

Q2: Consider the group G, and $f : G \to G$, where $f(x) = gxg^{-1}, \forall g \in G$. Prove that f is isomorphic on G (f is Automorphism).

Q3: Let $U = \left\{xyx^{-1}y^{-1|x,y \in G}\right\}$, and let $G' = (U)$. Or, G' is a generator (U), and G' is called the commutative subgroup in G.

(a) Prove that G' is a normal subgroup of G.

(b) Prove that $\frac{G}{G'}$ is a commutative.

(c) If $\frac{G'}{\mathbb{N}}$ is a commutative, then prove that $G' \subseteq \mathbb{N}$.

Q4: If each of L, P be normal subgroups of G, then $\frac{NM}{M} \approx \frac{N}{N \cap M}$.

Q5: Prove that every group on order q is a commutative group.

Q6: If G be a non commutative group such that $O(G) = 6$, then $G \approx S_3$.

Q7: Let G be a finite group, and $\Gamma : G \to G$ be an isomorphic mapping on G (Automorphism), where $\Gamma(x) = x \leftrightarrow x = e$, in addition $\Gamma^2 = I$ in which $I : G \to G$ is a mapping. Prove that G is a commutative group.

Q8: Let $\mathbb{R}^+$ be the multiplicative group of positive real numbers, and let $\mathbb{R}$ be the additive group of real numbers. Assign homomorphism and isomorphism from the functions;

(i) $Log : \mathbb{R}^+ \to \mathbb{R}$.

(ii) $Exp : \mathbb{R} \to \mathbb{R}^+$.

Q9: Consider the group $(\mathbb{Z}_6, +)$, the integers from 0 to 5 with addition modulo 6. Also consider the group $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$, the ordered pairs where the $x-$ coordinates can be 0 or 1, and the $y-$ coordinates can be 0, 1, or 2, where addition in the $x-$coordinate is modulo 2 and addition in the $y-$coordinate is modulo 3.

Are these structures isomorphic under addition, under the following scheme?

$$(0,0) \to 0$$
$$(1,1) \to 1$$
$$(0,1) \to 2$$
$$(1,0) \to 3$$
$$(0,1) \to 4$$
$$(1,2) \to 5$$

In general $(a, b) \to (3a + 4b)\ mod\ 6$

Q10: If one object consists of a set X with a binary relation R and the other object consists of a set Y with a binary relation S then an isomorphism from X to Y is a bijective function;

$f : X \to Y$ such that $S(f(u), f(v)) \leftrightarrow R(u, v)$.

8
The Integer Numbers

8.1 Introduction

Let each of $n, m \in \mathbb{N}$, and let us try to solve the equation $m + x = n, \forall x \in \mathbb{N}$. We will see that, we often fail to solve this equation, because we do not find an additive inverse for every element in $\mathbb{N}$. This imposes us to recourse another system than $\mathbb{N}$ to recover this drawback. Of course, a new system should contains $\mathbb{N}$ in order not to lose the advantages of this system in dealing with other situations, and we call the new system the integer numbers $\mathbb{Z}$.

There are two methods to creating $\mathbb{N}$:

(i) Construction of $\mathbb{N} \times \mathbb{N}$, and defining equivalence classes on it. The resulting set of equivalence classes will be $\mathbb{Z}$ exactly.

(ii) We define the ring and the system of $\mathbb{Z}$ as a ring containing of $\mathbb{N}$, and does not contains of a subring contains of $\mathbb{N}$ except of $\mathbb{N}$ itself.

We adopted the first case, and through it we resulting the second case as a theorem.

8.2 Construction of $\mathbb{Z}$

Definition 8.1 If $(m,n),(p,q) \in \mathbb{N}\times\mathbb{N}$ then $(m,n)R(p,q)$ if and only if $m+q=p+n$, and it is called relation (R) on the set $\mathbb{N}\times\mathbb{N}$ (Mendelson, 1973; Frobisher, 1999; Campbell, 1970).

Example 8.1 It should be noted that $(3,5)R(6,8) \leftrightarrow 3+8=6+5$. While $(2,3) \not R(1,4)$, because $2+4\neq 1+3$.

Theorem 8.1 *The relation R on $\mathbb{N}\times\mathbb{N}$ is equivalence relation.*

Proof (1) If $(m,n)\in\mathbb{N}\times\mathbb{N}$ then $m+n=m+n$.
$\therefore (m,n)R(m,n), \forall (m,n)\in\mathbb{N}\times\mathbb{N}$.
Thus, the relation R is reflexive.
(2) If $(p,q),(m,n)\in\mathbb{N}\times\mathbb{N}$, in which $(m,n)R(p,q)$.
$\because (m,n)R(p,q)\to m+q=p+n\to p+n=m+q$.
$\therefore (p,q)R(m,n)$.
Thus, the relation R is symmetric.
(3) If $(m,n),(p,q),(r,s)\in\mathbb{N}\times\mathbb{N}$, where $(m,n)R(p,q),(p,q)R(r,s)$.
$\because (m,n)R(p,q),(p,q)R(r,s)$,
$\therefore m+q=p+n, p+s=r+q$.
$\therefore (m+q)+s=(p+n)+s=(p+s)+n$.
But, $(p+s)+n=(r+q)+n$,
$\therefore (m+q)+s=(r+q)+n$.
$\therefore q+(m+s)=q+(r+n)$.
The cancellation low in $\mathbb{N}$ is $a+b=a+c\to b=c, \forall a,b,c\in\mathbb{N}$.
$\therefore m+s=r+n\to(m,n)R(r,s)$. Thus, the relation R transitive on $\mathbb{N}\times\mathbb{N}$.

Thus, from (1) &(2) $(3), R is equivalence relation on $\mathbb{N}\times\mathbb{N}$. ♦

Note: It will written $(m,n)\sim(p,q)$ to denote that $(m,n)R(p,q)$, and read it (m,n) equivalence to (p,q).

Definition 8.2 Equivalence class the ordered pair (m,n) is called integer and denoted by $[m,n]$. Or, Mathematically,$[m,n] = \{(p,q)\in\mathbb{N}\times\mathbb{N} | (p,q)\sim(m,n)\}$ (Campbell, 1970; Mendelson, 1973).

Note: The set of all equivalence classes is called set of integers and denoted by $\mathbb{Z}=\mathbb{N}\times\mathbb{N}$.

Example 8.2 Consider the following intervals:

(1)

$$\begin{aligned}[0,0] &= \{(p,q) \in \mathbb{N} \times \mathbb{N} | (p,q) \sim (0,0)\} \\ &= \{(p,q) \in \mathbb{N} \times \mathbb{N} | p + 0 = 0 + q\} \\ &= \{(0,0),(1,1),(2,2),...\}.\end{aligned}$$

(2)

$$\begin{aligned}[1,2] &= \{(p,q) \in \mathbb{N} \times \mathbb{N} | (p,q) \sim (1,2)\} \\ &= \{(p,q) \in \mathbb{N} \times \mathbb{N} | p + 2 = 1 + q\} \\ &= \{(p,q) \in \mathbb{N} \times \mathbb{N} | p + 1 = q\} \\ &= \{(0,1),(1,2),(2,3),...\}\end{aligned}$$

8.3 The Addition and Multiplication of $\mathbb{Z}$

Before we begin to define the operations of addition and multiplication, it is useful to take the following introductory theorem:

Theorem 8.2 (Introductory Theorem)
If $(m,n) \sim (m',n')$ and $(p,q) \sim (p',q')$, then
(a) $(m+p, n+q) \sim (m'+p', n'+q')$.
(b) $(mp+nq, mq+np) \sim (m'p'+n'q', m'q'+n'p')$.

Proof (a) Since $(m,n) \sim (m',n')$, and $(p,q) \sim (p',q')$ then
(1) $m+n' = m'+n$, (2) $p+q' = p'+q$.
From the additional properties on the set $\mathbb{N}$, we note that
$(m+p)+(n'+q') = (m+n')+(p+q')$.
From (1)& (2), we obtain $(m+p)+(n'+q') = (m'+n)+(p'+q)$, and this means $(m+p)+(n'+q') = (m'+p')+(n+q)$.
$\therefore (m+p, n+q) \sim (m'+p', n'+q')$.
(b) We are going to prove that
(1) $(mp+nq, mq+np) \sim (m'p+n'q, m'q+n'p)$,
(2) $(m'p+n'q, m'q+n'q) \sim (m'p'+n'q', m'q'+n'p')$.
$\because$ $\sim$ is a transitive relation,
$\therefore (mp+nq, mq+np) \sim (m'p'+n'q', m'q'+n'p')$.
To prove (1), from the assumption (given), $m+n' = m'+n$. And, from properties of addition, and multiplication on $\mathbb{N}$, we have

$(mp+nq)+(m'q+n'p)=(mp+n'p)+(nq+m'q)=(m+n')p+(n+m')q$.

$\because m+n'=m'+n$,

$\therefore (mp+nq)+(m'q+n'p)=(m+n')p+(m+n')q=(m+n')(p+q)$.

It should be noted that

$(m'p+n'q)+(mq+np)=(m'p+np)+(n'q+mq)=(m'+n)p+(n'+m)q$.

$\because m+n'=m'+n$,

$\therefore (m'p+n'q)+(mq+np)=(m+n')p+(m+n')q=(m+n')(p+q)$.

$\therefore (mp+nq)+(m'q+n'p)=(m'p+n'q)+(mq+np)$.

Or, $(mp+nq,mq+np)\sim(m'p+n'q,m'q+n'p)$.

In the same way, we can prove (2). ♦

Theorem 8.3 *The binary operations F,G on $\mathbb{Z}$. If $\forall(m,n)\in a,(p,q)\in b$, then*

(1) $F(a,b)=[m+p,n+q]$. (2) $G(a,b)=[mp+nq,mq+np]$.

Proof $\because F=\{((a,b),[m+p,n+q])|(m,n)\in a,(p,q)\in b,a,b\in\mathbb{Z}\}\subseteq(\mathbb{Z}\times\mathbb{Z})\times\mathbb{Z}$.

$\therefore F:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ is a relation.

$\therefore \forall(a,b)\in\mathbb{Z}\times\mathbb{Z}\ \exists(m,n)\in a,(p,q)\in b\ni c=[m+p,n+q]$ such that $((a,b),c)\in F$.

$\therefore dom\ F=\mathbb{Z}\times\mathbb{Z}$.

If $(m',n')\in a,p',q')\in b$, then $c'=[m'+p',n'+q']$.

$\therefore (m,n)\sim(m',n')$ and $(p,q)\sim(p',q')$.

Now, by using Theorem 8.2, we get

$(m+p,n+q)\sim(m'+p',n'+q')$.

Or, $[m+p,n+q]=[m'+p',n'+q']$.

$\therefore c=c'$.

$\therefore F$ is a functional relation.

$\therefore F:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$.

$\therefore F$ is a binary operation on $\mathbb{Z}$.

In the same way, G is a binary operation on $\mathbb{Z}$. ♦

Definition 8.3 Let $a,b\in\mathbb{Z},\ni(m,n)\in a,(p,q)\in b$. The binary operation F on $\mathbb{Z}$ defined as $F(a,b)=[m+p,n+q]$ is called addition on $\mathbb{Z}$, and expressed as $a+_z b=F(a,b),\forall a,b\in\mathbb{Z}$.

And, the binary operation G on $\mathbb{Z}$ defined as $G(a, b) = [mp + nq, mq + np]$ is called multiplication on $\mathbb{Z}$, and expressed as $a \cdot_z b = G(a, b), \forall a, b \in \mathbb{Z}$(Cameron, 2008; Warner, 1990; Mustafa et al., 1980; Mendelson, 1973).

Note: For convenient, we write $a + b, a \cdot b$ instead of $a +_z b, a \cdot_z b$, respectively.

Example 8.3 (1) If $a = (2, 3), b = (4, 5)$, then $a + b = [2, 3] + [4, 5] = [2+4, 3+5] = [6, 8]$, and $a \cdot b = [2, 3] \cdot [4, 5] = [2 \cdot 4 + 3 \cdot 5, 2 \cdot 5 + 3 \cdot 4] = [23, 22]$.

(2) If $a = (-3, 0)], b = (7, -4)$, then $a + b = [4, -4], a \cdot b = [-21, 12]$.

Theorem 8.4 *The mathematical system* $(\mathbb{Z}, +)$ *is a commutative group.*

Proof (1) The addition + should be associative.

Let $a = [m, n], b = [p, q], c = [r, t], \forall m, n, p, q, r, t \in \mathbb{Z}$.

$a + (b + c) = [m, n] + ([p, q] + [r, t]) = [m, n] + [p + r, q + t] = [m+(p+r), n+(q+t)] = [(m+p)+r, (n+q)+t] = [m+p, n+q]+[r, t] = ([m, n] + [p, q]) + [r, t] = (a + b) + c$.

(2) The identity element. $[0, 0]$ is the identity element for $\mathbb{Z}$ with respect to the addition operation.

Let $a = [m, n] \in \mathbb{Z}$.

$a + [0, 0] = [m, n] + [0, 0] = [m + 0, n + 0] = [m, n]$.

In the same way, $[0, 0] + a = a$.

Thus, $[0, 0]$ is the identity element of $\mathbb{Z}$ with respect to the addition operation. In addition, based on Theorem 7.1 it is a unique element.

(3) Inverse element. If $a = [m, n] \in \mathbb{Z}$, then $a' = [n, m]$ is the inverse element of $\mathbb{Z}$.

$a + a' = [m, n] + [n, m] = [m + n, n + m] = [0, 0]$ $([m + n, n + m] \sim [0, 0])$.

$\therefore a + a' = [0, 0]$.

In the same way, $a' + a = [0, 0]$.

Thus, $a + a' = a' + a = [0, 0]$. Or, $a' = [n, m]$ is the inverse of $a = [m, n]$. And, according of Theorem 7.3 is the unique element of $\mathbb{Z}$ with respect to addition operation.

(4) Commutative property of the addition

Let $a, b \in \mathbb{Z} \ni a = [m, n], b = [p, q], \forall m, n, p, q \in \mathbb{Z}$.
$a + b = [m, n] + [p, q] = [m + p, n + q] = [p + m, q + n]$
$= [p, q] + [m, n] = b + a$.
$\therefore a + b = b + a$.

From (1), (2), (3) & (4), the mathematical system $(\mathbb{Z}, +)$ is a commutative group. ♦

Notation:

(1) We express $[0, 0]$ as the identity element for the + on $\mathbb{Z}$.

(2) If $[m, n] = a \in \mathbb{Z}$, the $[n, m] = -a \in \mathbb{Z}$ as the inverse for the + on $\mathbb{Z}$.

Note:

The mathematical system $(\mathbb{N}, +)$ is the semigroup, because there is not an inverse of $n, \forall n \in \mathbb{N}$. That why the system $(\mathbb{N}, +)$ is extended to the system $(\mathbb{Z}, +)$, and it is a group based on Theorem 8.4.

Corollary *For all $a, b, c \in \mathbb{Z}$ then*
(1) $\forall a, b \in \mathbb{Z}, \exists!\ c \ni a = b + c$. (2) If $a + c = b + c \to a = b$.

Proof The proof is left to the reader as an exercise. ♦

Notation: For all $a, b, c! \in \mathbb{Z}$, the expression $a - b = c \ni a = b + c$.

Note: If $\forall a, b, c \in \mathbb{Z}$, then

(i) $-(-a) = a$.

(ii) $a + (-b) = a - b$.

(iii) $-(a + b) = (-a) + (-b)$.

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

(v) $-(a - b) = b - a$.

Theorem 8.5 *The mathematical system $(\mathbb{Z}, \cdot)$ is a commutative semigroup with an identity element.*

Proof (1) Association property.

Let $a, be, c \in \mathbb{Z}$, if $a = [m,n], b = [p,q], c = [r,t]$, then $a \cdot (b \cdot c)$

$= [m,n]. \cdot ([p,q] \cdot [r,t])$

$= [m,n] \cdot ([p \cdot t + q \cdot t, p \cdot t + q \cdot r])$

$= [m \cdot (p \cdot r + q \cdot t) + n \cdot (p \cdot t + q \cdot r), m \cdot (p \cdot t + q \cdot r) + n \cdot (p \cdot r + q \cdot t)]$

$= [m \cdot p \cdot r + m \cdot q \cdot t + n \cdot p \cdot t + n \cdot q \cdot r, m \cdot p \cdot t + m \cdot q \cdot r + n \cdot p \cdot r + n \cdot q \cdot t]$

$= [(m \cdot p + n \cdot q) \cdot r + (m \cdot q + n \cdot p) \cdot t, (m \cdot p + n \cdot q) \cdot t + (m \cdot q + n \cdot p) \cdot r]$

$= [m \cdot p + n \cdot q, m \cdot q + n \cdot p] \cdot (r,t)$

$= ([m,n] \cdot [p,q]) \cdot [r,t]$

$= (a \cdot b) \cdot c.$

(2) Identity element.

The element $[1,0]$ is the identity element of $\mathbb{Z}$ with respect to the multiplication operation because if $[m,n] = a \in \mathbb{Z}$, then

$a \cdot [1,0] = [m,n] \cdot [1,0] = [m \cdot 1 + n \cdot 0, m \cdot 0, n \cdot 1] = [m + 0, 0 + n] = [m,n] = a.$

In the same way, $[1,0] \cdot a = a$.

$\therefore a \cdot [1,0] = [1,0] \cdot a = a.$

$\therefore [1,0]$ is the identity element of $\mathbb{Z}$ with respect to $\cdot$ operation. And according to Theorem 7.1 is a unique element.

(3) Commutative property. It is left to the reader.

From (1, (2) & (3), the system $(\mathbb{Z}, \cdot)$ is a semigroup with the identity element. ♦

Notation: We expressed $[1,0]$ with respect to $\cdot$ operation by $1_{\mathbb{Z}}$, and for convenient write it 1.

Note: Since $\forall a \in \mathbb{Z}$ has no inverse with respect to $\cdot$ operation, hence the mathematical system $(\mathbb{Z}, \cdot)$ will be extended into the system $(\mathbb{Z}, +, \cdot)$ of the field $\mathbb{Q}$ in the next chapter.

Definition 8.4 If $x, y \in \mathbb{Z}, y \neq 0$. The division x on y, written $x \div y$ is a unique integer number b (positive) where $x = yb$ (Weisstein, 2002b; Mustafa et al., 1980).

Theorem 8.6 *The $\cdot$ operation is distributive over the $+_z$ operation.*

Proof If $a = [m,n], b = [p,q], c = [r,t]$, then $a \cdot (b + c)$

$= [m,n] \cdot ([p,q] + [r,t])$

$= [m, n] \cdot [p + r, q + t]$
$= [m \cdot (p + r) + n \cdot (q + t), m \cdot (q + t) + n \cdot (p + r)]$
$= [(m \cdot p + m \cdot r) + (n \cdot q + n \cdot t), (m \cdot q + m \cdot t) + (n \cdot p + n \cdot t)]$
$= (m \cdot p + n \cdot q) + (m \cdot r + n \cdot t), (m \cdot q + n \cdot p) + (n \cdot t + n \cdot r)$
$= [(m \cdot p + n \cdot q, m \cdot q + n \cdot p)] + [m \cdot r + n \cdot t, m \cdot t + n \cdot r]$
$= [m, n] \cdot [p, q] + [m, n] \cdot [r, t]$
$= a \cdot b + a \cdot c$
similarly, $(b + c) \cdot a = b \cdot a + c \cdot a$. ♦

8.4 Rings

Definition 8.5 If $A \neq \phi$, and $*, \#$ are binary operations on A then the ordered triple $(A, *, \#)$ is a ring if

(i) $(A, *)$ is a commutative group,

(ii) $(A, \#)$ is a semigroup, and

(iii) the operation # distributive on the operation $*$

(Bourbaki, 1989a; Saunders and Birkhoff, 1999; Saunders and Birkhoff, 1967; Saunders and Garrett, 1967; Lang, 2002a).

Definition 8.6 The ring $(A, *, \#)$ called the commutative ring if the operation $*$ is commutative, and it is called the ring with an identity if there exists an identity element with to # (Atiyah and Macdonald, 1969; Balcerzyk and Józefiak, 1989; Poonen, 2019).

Notation: (1) We will call the binary operations $*, \#$ addition and multiplication respectively, and denote them by $+, \cdot$, respectively. This does not mean that the operations are a usual addition and multiplication.

(2) For convenient, we write $(A, +, \cdot)$ instead of $(A, *, \#)$, and denote to the identity element in the $(A, *)$ by 0_A.

Theorem 8.7 *The ordered triple* $(\mathbb{Z}, +, \cdot)$ *is a commutative ring with an identity element.*

Proof (1) According to the Theorem 8.4, the mathematical system $(\mathbb{Z}, +$ is the commutative group.

(2) According to the Theorem 8.5, the mathematical system $(\mathbb{Z}, \cdot)$ is the semigroup with the identity element.

(3) According to the Theorem 8.6 the $\cdot$ operation is distributive over the $+$ operation.

Thus, from (1), (2), and (3), the system $(\mathbb{Z}, +, \cdot)$ is the commutative ring with the identity element. ♦

Example 8.4 (1) Let $A = \{x, y\}$, and $+, \cdot$ be operations defined on A as shown in Tables(8.1 & 8.2):

Table 8.1: The Result of $x + y$

$+$	x	y
x	x	x
y	x	y

Table 8.2: The Result of $x \cdot y$

$\cdot$	x	y
x	x	y
y	y	x

The system $(A, +, \cdot)$ is the commutative ring with the identity element y.

(2) Let $A = \mathbb{Z} \times \mathbb{Z}$, and consider the system $(A, *, \#)$. If $*, \#$ defined on A respectively as

$(a, b)*(c, d) = (a+c, b+d), (a, b)\#(c, d) = (ac, bd), \forall (a, b), (c, d) \in A$. Then the system is is a commutative ring with the identity element $(1, 1)$.

Theorem 8.8 *If $(A, +, \cdot)$ is a ring and $a, b, c \in A$ then*

(i) $a \cdot 0_A = 0_A \cdot 0 = 0_A$.

(ii) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.

(iii) $(-a) \cdot (-b) = a.b$.

(iv) $a \cdot (b - c) = a \cdot b - a \cdot c$.

(v) $(a - b) \cdot c = a \cdot c - b \cdot c$.

Proof (i) $\because 0_A$ is the identity element with respect to $+$,
$\therefore 0_A + 0_A = 0_A$.
$\therefore a \cdot) 0_A = a \cdot (0_A + 0_A) = a \cdot 0_A + a \cdot 0_A$.
$\therefore a \cdot 0_A + a \cdot 0_A = 0_A$.
In the same way, $0_A \cdot a = 0_A$.
(ii) $\because -a$ is the inverse of a,
$\therefore a + (-a) = 0_A$.
Based on (i), $0_A = 0_A \cdot b$,
$\therefore 0_A = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$.
$\therefore (-a) \cdot b$ is the inverse for $a \cdot b$ with respect to $+$.
$\because$ the inverse is a unique,
$\therefore (-a) \cdot b = -(a \cdot b)$.
In the same way, we can proof that $a \cdot (-b) = -(a \cdot b)$.
(iv) $\because b - c = b + (-c)$,
$\therefore a \cdot (b - c) = a \cdot (b + (-c)) = a \cdot b + a \cdot (-c)$.
Based on (ii), $a \cdot (-c) = -(a \cdot c)$.
$\therefore a \cdot (b - c) = a \cdot b + (-(a \cdot c)) = a \cdot b - a \cdot c$.
(iii)& (v) They are left as exercises for the reader. ♦

Theorem 8.9 *If* $(A, +, \cdot)$ *is a ring with an identity element* $A = \{0_A\}$, *then* $0_A \neq 1_A$.

Proof Suppose that $0_A = 1_A$.
$\because A \neq \{0_A\}$,
$\therefore \exists a \in A \ni a \neq 0_A$.
$\because 1_A$ is the identity element with respect to $\cdot$,
$\therefore a \cdot 1_A = a$.
$\therefore a \cdot 0_A = a$.
But, based on Theorem 8.8, $a \cdot 0_A = 0_A$.

$\therefore a = 0_A$.

This is contradiction, thereby $0_A \neq 1_A$. ♦

Example 8.5 Let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}_{2\times 2}$ be the set of all matrices where $a, b, c, d \in \mathbb{Z}$.

The binary operation $\odot$ defined on M as follows;

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \odot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$.

The binary operation $\oplus$ defined on M as follows;

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \oplus \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$.

The mathematical system $(M, \oplus, \odot)$ is noncommutative ring with identity element $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Example 8.6 To illustrate, noncommutative ring, if

$x = \begin{bmatrix} 3 & 4 \\ 5 & -1 \end{bmatrix}, y = \begin{bmatrix} 0 & 2 \\ -9 & 9 \end{bmatrix}$, then $xy = \begin{bmatrix} 36 & 10 \\ 9 & 1 \end{bmatrix}$, while

$yx = \begin{bmatrix} 10 & -2 \\ 32 & 35 \end{bmatrix}$.

Example 8.7 It should be noted that $A \neq 0, B \neq 0$, but $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$, as shown below;

$A = \begin{bmatrix} 0 & 5 \\ 0 & 13 \end{bmatrix}, B = \begin{bmatrix} 6 & 7 \\ 0 & 0 \end{bmatrix}$, while $BA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Definition 8.7 If R be a commutative ring, then $0 \neq a \in A$ is called zero divisor if $\exists 0 \neq b \in R \ni ab = 0$ (Bourbaki, 1989b; Lanski, 2005).

Example 8.8 In the previous example $A = A = \begin{bmatrix} 0 & 5 \\ 0 & 13 \end{bmatrix}$ is the zero divisor for the matrix $B = \begin{bmatrix} 6 & 7 \\ 0 & 0 \end{bmatrix}$.

Definition 8.8 If $(A, +, \cdot)$ is a commutative ring with the identity element in which $I_A \neq 0_A$ then it is called integral domain If it does not have the zero divisor. Or, $ab = 0 \to a = 0 \vee b = 0$ (Bourbaki, 1989b; Dummit and Foote, 2004a).

Example 8.9 The mathematical system $(\mathbb{Z}_7, +_7, \cdot_7)$ is the integral domain because it does not have a zero divisor. While the mathematical system $(\mathbb{Z}_6, +_6, \cdot_6)$ is not integral domain since it has the zero divisor. For example, $[2] \in \mathbb{Z}_6$ is a zero divisor, since $[2] \cdot [3] = [6] = [0]$.

Note: The mathematical system $(\mathbb{Z}_p, +_p, \cdot_p)$ is the integral domain if and only if p is a primal number.

8.5 Homomorphism

Definition 8.9 The mapping $\psi : A \to A'$ from a ring A to a ring A' is called a homomorphism if $\forall a, b \in A$, then (1) $\psi(a + b) = \psi(a) + \psi(b)$. (2) $\psi(a \cdot b) = \psi(a) \cdot \psi(b)$ (Artin, 1991; Hazewinkel et al., 2004; Bourbaki, 1989b).

Note: (i) The binary operations $+, \cdot$ on the left of (1), (2) are defined on the ring A. (ii) The binary operations $+, \cdot$ on the right of (1), (2) are defined on the ring A'.

Theorem 8.10 (Introductory Theorem) *If $\psi : A \to A'$ from a ring A to a ring A' be a homomorphism, then*

(1) $\psi(0) = 0$. (2) $\psi(-a) = -\psi(a), \forall\ 0, a \in A$.

Proof The proof is left for the reader. ⧫

Definition 8.10 If $\psi : A \to A'$ be a homomorphism, then Kernel ψ denoted by $ker\ \psi = \{a \in A |\ \psi(a) = 0'\}$, where $0'$ is a zero element in A', or $0'$ is the identity element with respect to $+$ (Artin, 1991; Hazewinkel et al., 2004; Bourbaki, 1989b; Jacobson, 2012).

Theorem 8.11 (Introductory Theorem) *If $\psi : A \to A'$ be a homomorphism, then*

(1) $ker\psi$ is a subgroup of A with respect to $+$. (2) $((a \in ker\psi) \wedge (b \in A)) \to (a \cdot b \wedge b \cdot a) \in ker\psi$.

Proof (1) It is left for the reader.

(2) $\psi(ab) = \psi(a)\psi(b) = 0\psi(a) = 0$.

$\therefore ab = ker\psi$.

In the same way $ba = ker\psi$. ♦

Example 8.10 (1) If $\gamma : A \to A'$ be a mapping, where $\gamma(a) = 0, \forall a \in A$, then $ker\ \gamma = A$, and γ is a zero homomorphism.

(2) Let $\gamma : A \to A'$ be a mapping from the ring A to the ring A', such that $\gamma(x) = x, \forall x \in A$. It should be noted that

$\gamma(x + y) = x + y = \gamma(x) + \gamma(y)$,

$\gamma(xy) = xy = \gamma(x)\gamma(y)$.

Thereby, γ is a homomorphism, and ker$(\gamma) = (0)$. γ is an identity homomorphism.

(3) Let $\gamma : \mathbb{Z} \to \mathbb{Z}_n$ be a mapping from the ring of the integer numbers to the ring of the integer numbers mod n, such that $\gamma(a) = [a], \forall a \in \mathbb{Z}$.

It should be noted that

$\gamma(a + b) = [a + b] = [a] +_n [b] = \gamma(a) +_n \gamma(b)$. In the same way, $\gamma(ab) = \gamma(a) \cdot_n \gamma(b)$. Thereby, γ is a homomorphism.

It should be remembered, γ is a surjective homomorphism because if $x \in \mathbb{Z}_n$, then $x = [a]; 0 \leq a < n$.

Thereby, $\gamma(a) = [a] = x$.

Now, let $y \in ker\gamma$,

$\therefore \gamma(y) = [0]$.

$\therefore [y] = [0]$.

$\therefore y = 0_n$.

$\therefore y$ is multiples of n.

$\therefore ker\ \gamma = (n), (n)$ is the set of all multiples of n.

Definition 8.11 The homomorphism $\psi : A \to A'$ is called isomorphism if the mapping ψ is injective (Vinberg, 2003).

Example 8.11 If $\mathbb{Z}(\sqrt{5}) = \left\{a + b\sqrt{5} | a, b \in \mathbb{Z}\right\}$, then $\mathbb{Z}(\sqrt{5})$ will be a ring with normal operations addition and multiplication. Let us define the following ψ mapping as

$\psi : \mathbb{Z}(\sqrt{5}) \to \mathbb{Z}(\sqrt{5})$, where $\psi : (a + b\sqrt{5}) = a - b\sqrt{5}$.

The homomorphism mapping ψ is Automorphism because

(1) If $x, y \in \mathbb{Z}\sqrt{5}$, then $x = a_1 + b_1\sqrt{5} \wedge y = a_2 + b_2\sqrt{5}$.

$\because \psi(x + y) = \psi(a_1 + a_2) + (b_1 + b_2)\sqrt{5} = a_1 + a_2 + (b_1 - b_2)\sqrt{5} = (a_1 - b_1\sqrt{5}) + (a_2 - b_2\sqrt{5}) = \psi(a) + \psi(b)$.

In the same way, we can get $\psi(xy) = \psi(a)\psi(b)$.

$\therefore \psi$ is a homomorphism.

(2) We have to prove that ψ is injective homomorphism.

If $\psi(x) = \psi(y)$, then $a_1 + b_1\sqrt{5} = a_2 + b_2\sqrt{5}$.

$\therefore a_1 = a_2, b_1 = b_2$,

$\therefore x = y$.

(3) ψ is a surjective homomorphism.

Thus, from (1), (2), and (3), ψ is Automorphism.

Definition 8.12 The ring A is isomorphic with the ring A' if there is an isomorphic mapping $f : A \to A'$, such that f is a surjective function, and denoted by $A \approx A'$(Vinberg, 2003; Artin, 1991; Bourbaki, 1989b; Jacobson, 2012).

Notes:

(1) The mapping $f : A \to A'$ is isomorphism if and only if $ker f = (0)$.

(2) The relation is equivalence.

Example 8.12 The ring $(\mathbb{Z}, +, \cdot) \not\approx (\mathbb{Z}_n, +_n, \cdot_n)$, because does not one to one correspondence between $\mathbb{Z}$ and $\mathbb{Z}_n$. For convenient, there is $\mathbb{Z} \not\approx \mathbb{Z}_n$.

Example 8.13 Consider the ring $(A, \oplus, \odot)$ with the identity element 1. Define the operations $\oplus, \odot$ on A as follows;

$x \oplus y = x + y + 1$, $x \odot y = xy + x + y, \forall x, y \in A$.

The ring $(A, +, \cdot) \approx (A, \oplus, \odot)$, because if we have a mapping $\psi : A \to A$, such that $\psi(x) = x - 1$, we have;

(1) The mapping is isomorphic

$\psi(x + y) = x + y - 1 = x - 1 + y - 1 + 1 = \psi(x) + \psi(y) + 1 = \psi(x) \oplus psi(y)$.

In the same way $\psi(xy) = \psi(x) \odot \psi(y)$.

(2) The mapping is surjective

$y \in A \to y = x + 1 \in A$.

$\therefore \psi(y) = y - 1 = x + 1 - 1 = x.$
(3) The mapping is injective
$\psi(x) = \psi(y) \rightarrow x - 1 = y - 1 \rightarrow x = y.$
From (1), (2) & (3), we get $\psi : A \rightarrow A$ is isomorphic.
Thus, $(A, +, \cdot) \approx (A, \oplus, \odot)$.
It should be noted that
(1) -1 is the identity element with respect to $\oplus$ such that
$x \oplus (-1) = a + (-1) + 1 = a.$
(2) 0 is the identity element with respect to $\odot$ such that
$a \odot 0 = a \cdot 0 + a + 0 = a.$

8.6 Quotient Rings

Definition 8.13 Consider a ring $(A, +, \cdot)$. If $\phi \neq U \subseteq A$, then U is called an ideal in A if and only if

(1) $(U, +)$ is a subgroup of $(A, +)$.

(2) $\forall a \in A, u \in U \rightarrow au \in u, ua \in U$(Hazewinkel et al., 2004; Mustafa et al., 1980; Milnor et al., 1971).

Definition 8.14 Let $(A, +, \cdot)$ be a ring, and $\phi \neq U \subseteq A$. U is a subgroup of A if and only if $(U, +', \cdot')$ is a ring where $+', \cdot'$ are restricted on U (Jacobson, 2012; Hungerford, 1974; Artin, 1991; Dummit and Foote, 2004a).

Note: Every ideal is a sub ring, but the opposite is not true.

Example 8.14 Consider $(\mathbb{Z}, +, \cdot)$ if $U = (5)$ all multiples of 5 then U is the ideal.

It should be noted that $((5), +)$ is a subgroup of $(\mathbb{Z}, +)$.
Let $u \in (5), n \in \mathbb{Z}$.
$\therefore u = 5k, k \in \mathbb{Z},$
$\therefore nu = n.5k = 5nk.$
Let $k_1 = nk \in \mathbb{Z},$
$\therefore nu = 5k_1 \in (5).$
In the same way $un \in (5)$.
$\therefore U = (5)$ is an ideal.
Consider $(\mathbb{Z}, +, \cdot)$ sub ring of $(\mathbb{Q}, +, \cdot)$ (Need proof).

The ring $(\mathbb{Z}, +, \cdot)$ is not ideal in $(\mathbb{Q}, +, \cdot)$ because $5 \in \mathbb{Z}, \frac{1}{6} \in \mathbb{Q}$ but $5.\frac{1}{6} \notin \mathbb{Z}$.

Definition 8.15 Let U be an ideal in the ring $(A, +, \cdot)$, and let the set $\frac{A}{U} = \{a + U | a \in A\}$. Define the binary operations $\oplus, \odot$ on $\frac{A}{U}$ as follows;

$(a + U) \oplus (b + U) = (a + b) + U$,

$(a + U) \odot (b + U) = ab + U$, (Mustafa et al., 1980; Jacobson, 2012; Hungerford, 1974; Artin, 1991; Dummit and Foote, 2004a).

Theorem 8.12 (Introductory Theorem)

Each of the binary operation $\oplus, \odot$ is well defined.

Proof We have to prove that the binary operation $\odot$ is completely defined.

Suppose that $a + U = a' + U, b + U = b' + U$,

$\therefore a = a' + u_1, b = b' + u_2, \forall u_1, u_2 \in U$.

$\therefore ab = (a' + u_1) + (b' + u_2) = a'b' + u_1b' + a'u_2 + u_1u_2$,

$\because U$ is the ideal in A,

$\therefore u_1b', a'u_2, u_1u_2 \in U$.

Let $u_3 = u_1b' + a'u_2 + u_1u_2$,

$\therefore u_3 \in U$.

Thereby, $ab = a'b' + u_3$.

Thus, $ab + U = a'b' + U$. ♦

Theorem 8.13 *The mathematical system $(\frac{A}{U}, \oplus, \odot)$ is a ring.*

Proof The system $(\frac{A}{U}, \oplus)$ is a commutative group (The proof is left).

Let, $X = a + U \in \frac{A}{U}, Y = b + U \in \frac{A}{U}, Z = c + U \in \frac{A}{U}, \forall a, b, c \in A$.

Now, $X \odot (Y \odot Z) = (a+U) \odot ((b+U) \odot (c+U)) = (a+U) \odot (bc+U) = a(bc)+U = (ab)c+U = (ab+U) \odot (c+U) = ((a+U) \odot (b+U)) \odot (c+U) = (X \odot Y) \odot Z$.

Thus $(\frac{A}{U}, \odot)$ is a semigroup.

Again, $(X \oplus Y) \odot Z = ((a + U) \oplus (b + U)) \odot (c + U) = ((a + b) + U) \odot (c + U) = (a + b)c + U = (ac + bc) + U = (ac + U) \oplus (bc + U) = ((a + U) \odot (c + U)) \oplus ((b + U) \odot (c + U)) = (X \odot Z) \oplus (Y \odot Z)$.

In the same way, we can prove that $Z\odot(X\oplus Y) = (Z\odot X)\oplus(Z\odot Y)$.
Thereby, the distributive rules are satisfied.
Thus, the system $(\frac{A}{U}, \oplus, \odot)$ is a ring. ♦

Definition 8.16 The ring $(\frac{A}{U}, +, \cdot)$ is called quotient ring of A by U(Jacobson, 1984; Dummit and Foote, 2004a; Lang, 2002a).

Note: If A is a commutative ring then $\frac{A}{U}$ is a ring too. If A is a ring with an identity element then $\frac{A}{U}$ with an identity element and its identity element is $1+U$ where 1 is the identity element for the ring A.

Theorem 8.14 *If $\tau : A \to \frac{A}{U}$ be a mapping from the ring A to the ring $\frac{A}{U}$ such that $\tau(a) = a+U, \forall a \in A$, then*
(1) τ is homomorphism and surjective.
(2) $ker\tau = U$.

Proof (1) $\tau(a+b) = (a+b)+U = (a+U)\oplus(b+U) = \tau(a)+\tau(b)$.
In the same way $\tau(ab) = \tau(a)\odot\tau(b)$.
$\therefore \tau$ is homomorphism.
Now, let $x \in \frac{A}{U}$.
$\therefore X = a+U, a \in A$,
$\therefore \tau(a) = a+U = X$.
Thereby, τ is surjective.
Thus, τ is surjective homomorphism.
(2) $ker\ \tau = U$, is left for the reader. ♦

Definition 8.17 The mapping, $\tau : A \to \frac{A}{U}$ from the ring A to the ring $\frac{A}{U}$, such that $\tau(a) = a+U, \forall a \in A$ is called the canonical homomorphism (Wilder, 1952; Wilder et al., 2012; Mustafa et al., 1980).

Example 8.15 Consider the ring $(\mathbb{Z}, +, \cdot)$, and let $U = (7)$, then $\frac{F}{U} = \{a+U|a \in \mathbb{Z}\}$.
Assume that $a = 7b+r, b \in \mathbb{Z}, 0 \leq r < 7$.
$\therefore a+U = (7b+r)+U = r+U$.
Now, let us define that
$\frac{\mathbb{Z}}{(7)} = \{0+U = U, 1+U, 2+U, ..., 6+U\}$,
$\tau : \frac{\mathbb{Z}}{(7)} \to \mathbb{Z}_7 \ni \tau(a+(7)) = a$.

So that $\tau : \frac{\mathbb{Z}}{(7)} \to \mathbb{Z}_7$ will be isomorphism.
Thereby, $\frac{\mathbb{Z}}{(7)} \approx \mathbb{Z}_7$.

Note: Generally, $\frac{\mathbb{Z}}{(n)} \approx \mathbb{Z}_n$.

8.7 Exercises

Answer the following questions:

Q1: Let $I_1 = [2,5], I_2 = [4,7]$. Prove that $I_1 = I_2$.

Q2: Evaluate each of

(i) $([3,1]+[5,8])+[8,3]$. (ii) $[4,3]\cdot([1,2]+[4,2])$. (iii) $([7,4]\cdot[5,3])\cdot[2,2]$. (iv) $[9,3]-[10,19]$.

Q3: (i) Is $([5,3] \div [0,5]) \in \mathbb{Z}$? (ii) Evaluate $[3,15] \div [8,4]$.

Q4: Let $(A,+,\cdot)$ be a ring, such that $x^2 = x, \forall x \in A$. Prove that $(A,+,\cdot)$ is the Boolean ring (commutative ring).

Q5: Let $(A,+,\cdot)$ be a commutative ring with the identity element. Prove that $(A,+,\cdot)$ is an integral domain if and only if $(ab = ac) \wedge (a \neq 0) \to b = c$.

Q6: Let A be a set of all real continuous functions defined on $[a,b]$. Define the addition and multiplication on A so that it becomes a ring. Define $\tau A \to \mathbb{R}$ such that $\tau(f(x)) = f(1/2)$. Prove that

(i) τ is homomorphism. (ii) find $ker\ \tau$.

Q7: Consider U an ideal in A such that $1 \in U$. Prove that $U = A$.

Q8: If each of U, V an ideal in A, such that $U + V = \{u + v | u \in U, v \in V\}$. Prove that $U + V$ is the ideal in A.

Q9: Let $(A,+,\cdot), U = (17)$. Prove that if there is an ideal V in $\mathbb{Z}$ such that $U \subset V \subset \mathbb{Z}$, then $V = \mathbb{Z} \vee V = U$.

Q10: Consider the ring $(A,+,\cdot)$ with the identity element 1, and the ring $(A',+',\cdot')$. If $\tau A \to A'$ is a surjective homomorphism, then $\tau(1)$ is the identity element for the ring $(A',+',\cdot')$.

Q11: Consider the ring $(A,+,\cdot)$ with the identity element 1, and let $\tau : A \to D$ be a homomorphism, such that $(D,\oplus,\odot)$ is the integral domain and $ker\ \tau \neq A$. Prove that $\tau(1)$ is the identity element in D.

8.8 The Order on $\mathbb{Z}$

Definition 8.18 The integer number a is called a positive if $m, n \in \mathbb{N} \ni (m, n) \in a, n < m$ (Evans, 1995; Weisstein, 2003b; Weisstein, 1999a; Weisstein, 2002a).

Example 8.16 $a = [3, 2]$ is a positive because $2 < 3$.

Theorem 8.15 *$a \in \mathbb{Z}$ is a positive if and only if $n < m, \forall (m, n) \in a$.*

Proof Suppose that a is a positive integer.
$\therefore \exists m, n \in \mathbb{N} \ni (m, n) \in a, n < m.$
$\because n < m,$
$\therefore \exists h \in \mathbb{N} \ni n + h = m.$
Assume that $(p, q) \in a,$
$\therefore (p, q) \sim (m, n).$
$\therefore p + n = m + q \rightarrow P + n = (n + h) + q.$
$\therefore p = h + q.$
Thereby, $p < q$.
Conversely, we can easily prove it based on the definition. ♦

Theorem 8.16 *If $a \in \mathbb{Z}$, then only one of the following cases satisfied (1) a is a positive. (2) $a = 0$. (3) $-a$ is a positive.*

Proof Let $a = [m, n]$. According to the Theorem 8.15, a will be a positive if and only if $n < m$.
$\because 0 = [0, 0],$
$\therefore [m, n] = [0, 0] \leftrightarrow a = 0 \wedge m = n.$
It should be noted that $-a = -[m, n] = [n, m]$.
$\therefore [n, m]$ is a positive if and only if $m < n$.
$\therefore -a$ is a positive if and only if $m < n$.
Thereby, according to the triple property on $\mathbb{N}$, we conclude that $(n < m) \vee (m = n) \vee (m < n)$.
$\therefore$ just on of $(1), (2), (3)$ is fulfilled. ♦

Definition 8.19 Let $a \in \mathbb{Z}$, a is called a negative integer if $-a \in \mathbb{Z}^+$ (Evans, 1995; Weisstein, 2003b; Weisstein, 1999a; Weisstein, 2002a).

Example 8.17 If $a = [8, 10]$ then $-a = [10, 8]$.

$\because 8 < 10$,

$\therefore -a \in \mathbb{Z}^+$.

Thereby, $a \in \mathbb{Z}^-$.

Note: $[8, 10] = [0, 2] = [6, 8] = [4, 6] = ...$

Theorem 8.17 *If each of a, b are positive integers then $a + b$ is a positive integer.*

Proof Let $a = [m, n], b = [p, q]$.

$\because a, b \in \mathbb{Z}^+$,

$\therefore n < m \wedge q < p$.

$\because a + b = [m, n] + [p, q] = [m + p, n + q]$.

$\because n + q < m + p$,

$\therefore [m + p, n + q] \in \mathbb{Z}^+$.

Thereby, $a + b$ is a positive integer. ♦

Definition 8.20 Let $a, b \in F$. then

(1) It is said that a is less than b, and written $a < b$ if $b - a$ is a positive integer.

(2) It is said that a is greater than b, and written $a > b$ if $a - b$ is a positive integer (Evans, 1995; Weisstein, 2003b; Weisstein, 1999a; Weisstein, 2002a).

Note: The expression $a \leq b$ indicates that $a < b \vee a = b$. And, $a \geq b$ indicates that $a > b \vee a = b$.

Example 8.18 let $a = [6, 2], b = [9, 4]$.

Then, $b - a = [9, 4] - [6, 2] = [9, 4] + [2, 6] = [9 + 2, 4 + 6] = [11, 10]$.

$\because 10 < 11$,

$\therefore [11, 10] \in \mathbb{Z}^+$.

$\therefore b - a \in \mathbb{Z}^+$.

$\therefore a < b$.

Theorem 8.18 *The system $(\mathbb{Z}, \leq)$ is a totally ordered set.*

Proof (1) $\because a \leq a, \forall a \in \mathbb{Z}$,

$\therefore \leq$ is a reflexive relation.

(2) Suppose that $(a \leq b) \wedge (b \leq a)$.

The expression $a \leq b \rightarrow b - a \in \mathbb{Z}^+ \vee a = b$.

Also, $b \leq a \rightarrow a - b \in \mathbb{Z}^+ \vee b = a$.

$\therefore b - a \in \mathbb{Z}^+ \wedge a - b \in \mathbb{Z}^+$.

But, $a - b = -(b - a) \rightarrow b - a, -(b - a) \in \mathbb{Z}^+$, and this is a contradiction.

$\therefore a - b = b - a = 0 \rightarrow a = b$.

$\therefore \leq$ is an anti-symmetric relation.

(3) The $\leq$ is a transitive relation.

Thereby, from (1), (2)& (3), the $\leq$ is a partially ordered relation.

Now, we have to prove that any two elements $a, b \in \mathbb{Z}$ are comparable.

$\because b - a \in \mathbb{Z}$,

$\therefore b - a \in \mathbb{Z}^+ \vee -(b - a) \in \mathbb{Z}^+ \vee a = b$.

$\therefore b > a \vee a > b \vee a = b \rightarrow a \geq b \vee b \geq a$.

Thus, $(\mathbb{Z}, \leq)$ is a totally ordered set. ⧫

Theorem 8.19 $\mathbb{Z}^+ = \{a | a \in \mathbb{Z} \wedge a > 0\} = \{-a | a \in \mathbb{Z} \wedge a < 0\}$.

Proof Suppose that $a \in \mathbb{Z}^+$.

$\therefore a$ is an integer number.

$\because a - 0 = a, \forall a \in \mathbb{Z}^+$,

$\therefore a - 0 \in \mathbb{Z}^+$.

$\therefore a > 0$, based on the definition of the positive integer number.

Thereby, $\mathbb{Z}^+ \subseteq \{a | a \in \mathbb{Z} \wedge a > 0\}$ ...(1).

In the same way, we can prove that $\{a | a \in \mathbb{Z} \wedge a > 0\} \subseteq \mathbb{Z}^+$... (2).

From (1), (2), we get that $\mathbb{Z}^+ = \{a | a \in \mathbb{Z} \wedge a > 0\}$.

Proof of $\mathbb{Z}^+ = \{-a | a \in \mathbb{Z} \wedge a < 0\}$ is left as an exercise for the reader. ⧫

Theorem 8.20 $\mathbb{Z}^+ = \{[n + 1, 0] | n \in \mathbb{N}\}$.

Proof Let $S = \mathbb{Z}^+ = \{[n+1, 0] | n \in \mathbb{N}\}$.

We have to prove that $S \subseteq \mathbb{Z}^+ \wedge \mathbb{Z}^+ \subseteq S \Leftrightarrow S = \mathbb{Z}^+$.

To prove $S \subseteq \mathbb{Z}^+$, suppose that $a \in S$.

$\therefore \exists n \in \mathbb{N} \ni a = [n+1, 0]$.

$\because 0 < n+1, \forall n \in \mathbb{N}$,

$\therefore [n+1, 0]$ is a positive integer.

$\therefore a \in \mathbb{Z}^+$.

$\therefore S \subseteq \mathbb{Z}^+$... (1).

To prove $\mathbb{Z}^+ \subseteq S$, suppose that $b \in \mathbb{Z}^+$.

$\therefore b$ is a positive integer.

If $b = [p, q]$, then according to the definition $q < p$.

(a) If $q = 0$, then $0 < p$.

$\therefore p = n+1, n \in \mathbb{N}$.

$\therefore b = [p, q] = [n+1, 0]$.

$b \in S$.

(b) If $q > 0$, then $p > q > 0$.

$\therefore q = n+1, n \in \mathbb{N}$.

$\therefore p = q + m + 1, m \in \mathbb{N}$.

$\therefore p = (n+1) + (m+1) = m + 1 + n + 1$

$\therefore b = [p, q] = [m+1+n+1, n+1] = [m+1, 0]$.

$\therefore b \in S$

From (a), (b) $\mathbb{Z}^+ \subseteq S$ ...(2).

From (1), (2) $\mathbb{Z}^+ = S$. ♦

Theorem 8.21 *If $a, b \in \mathbb{Z}^+$, then $a \cdot b \in \mathbb{Z}^+$.*

Proof $\because a, b \in \mathbb{Z}^+$,

$\therefore a = [n+1, 0], b = [m+1, 0], \forall n, m \in \mathbb{N}$.

$a \cdot b = [n+1, 0] \cdot [m+1, 0] = [nm + n + m + 1, 0] = [r+1, 0], r = nm + n + m \in \mathbb{N}$.

$\therefore a \cdot b \in \mathbb{Z}^+$. ♦

Corollary *If $0 \neq a, b \in \mathbb{Z}$ then $ab \neq 0$.*

Proof We have to take into account four cases, as follows;

(1) $a, b \in \mathbb{Z}^+$. (2) $a, -b \in \mathbb{Z}^+$. (3) $-a, b \in \mathbb{Z}^+$. (4) $-a, -b \in \mathbb{Z}^+$.

(1) According to Theorem 8.21, $a, b \in \mathbb{Z}^+$.

$\therefore a \cdot b \neq 0$.

(2) $a \cdot (-b) \in \mathbb{Z}^+$.

$\because a(-b) = -ab$.

$\therefore -ab \in \mathbb{Z}$.

$\therefore ab \neq 0$.

In the same way we can prove (3), (4).

Thus, in any case $ab \neq 0$. ♦

Theorem 8.22 *The mathematical system* $(\mathbb{Z}, +, \cdot)$ *is integral domain.*

Proof $\because (\mathbb{Z}, +, \cdot)$ is a commutative ring with an identity element $1 \neq 0$,

$\therefore$ it is enough to prove the system $(\mathbb{Z}, +, \cdot)$ has no zero divisors.

Suppose that $ab = 0, a, b \in \mathbb{Z}$.

Let $a, b \neq 0$.

Now, according to the previous corollary, $ab \neq 0 \to a = 0 \vee b = 0$.

This is contradiction.

$\therefore a = 0 \vee b = 0$. ♦

Theorem 8.23 *If* $a, b \in \mathbb{Z}$, *then* $a < b \leftrightarrow (a+c < b+c, \forall c \in \mathbb{Z}) \vee (ac < bc, \forall c \in \mathbb{Z}^+)$.

Proof Necessary condition.

Suppose that $a < c$.

$\therefore b - a \in \mathbb{Z}^+$.

$\because (b + c) - (a + c) = b - a \in \mathbb{Z}^+$,

$\therefore a + c < b + c, \forall c \in \mathbb{Z}$.

So as, $bc - ac = (b - a)c$.

$\because b - a \in \mathbb{Z}^+, c \in \mathbb{Z}^+$,

$\therefore (b - a)c \in \mathbb{Z}^+ \to bc - ac \in \mathbb{Z}^+$.

$\therefore ac < bc, \forall c \in \mathbb{Z}^+$ ...(1).

Sufficient condition.

Suppose that $(a + c < b + c, \forall c \in \mathbb{Z}) \vee (ac < bc, \forall c \in \mathbb{Z}^+)$.

We get that $a < b$ (Has is left for tha reader) ...(2).

From (1) & (2), we get the proof. ⧫

Definition 8.21 The ring $(A, +, \cdot)$ is said to be ordered ring if there is a totally ordered relation $\leq$ on A such that;

(1) $\forall a, b, c \in A$, if $a \leq b \rightarrow a + c \leq b + c$.

(2) $\forall a, b \in A$, if $a \leq b \rightarrow a \cdot c \leq b \cdot c, \forall\ 0 < c \in A$ (Lam, 1983a; Lenagan, 1994).

Note: Denotes to the ordered ring by the symbol $(A, +, \cdot, \leq)$.

Definition 8.22 The integral domain $(D, +, \cdot)$ is said to be ordered integral domain if there is totally ordered relation $\leq$ on D such that;

(1) $\forall a, b, c \in D$, if $a \leq b \rightarrow a + c \leq b + c$.

(2) $\forall a, b \in D$, if $a \leq b \rightarrow a \cdot c \leq b \cdot c, \forall\ 0 < c \in D$ (Mustafa et al., 1980).

Note: Denotes to the ordered integral domain by the symbol $(D, +, \cdot, \leq)$.

Theorem 8.24 *The mathematical system $(\mathbb{Z}, +, \cdot, \leq)$ is ordered integral domain.*

Proof $\because (\mathbb{Z}, +, \cdot)$ is integral domain based on Theorem 8.22.

$\because\ \leq$ is a tottal ordered relation on $\mathbb{Z}$ based on Theorem 8. 18.

$\because$ the conditions hold according to Theorem 8.23.

$\therefore (\mathbb{Z}, +, \cdot, \leq)$ is an ordered integral domain. ⧫

Definition 8.23 Let $(A, +, \cdot)$ be an integral domain. The set $A^+ \subset A$ is called set of the positive elements of A provided that

(1) $a + b \in A^+, \forall a, b \in A^+$.

(2) $a \cdot b \in A^+, \forall a, b \in A^+$.

(3) $\forall a \in A$, then $a \in A^+, a = 0_A, -a \in A^+$(Mustafa et al., 1980).

Theorem 8.25 *$\mathbb{Z}^+$ is the set of positive elements in $\mathbb{Z}$.*

Proof From Theorem 8.16, 8.17, 8.21, we get the Definition 8.23 and its three conditions.

Thereby, $\mathbb{Z}^+$ will be the set of positive elements in $\mathbb{Z}$. ♦

Theorem 8.26 *Consider the integral domain $(A, +, \cdot)$, and let A^+ be the set of positive elements in A, then*

(1) The subset T in $A \times A$ defined as $(a, b) \in T \leftrightarrow a = b \vee b - a \in A^+$ will be a total ordered relation on A.

(2) If the relation $\leq$ on A defined as $a \leq b \leftrightarrow (a, b) \in T$, then $(A, +, \cdot, \leq)$ will be integral domain.

(3) $A^+ = \{a | a > 0_A)\}$.

Proof (1) (i) $\because (a, a) \in T, \forall a \in A$,

$\therefore T$ is reflexive.

(ii) Let $(a, b) \in T \wedge (b, a) \in T$.

$\because (a, b) \in T \rightarrow a = b \vee b - a \in A^+$,

Also, $(b, a) \in T \rightarrow a = b \vee a - b \in A^+$.

Now, if $b - a \in A^+ \wedge a - b \in A^+ \rightarrow b - a \in A^+ \wedge -(b - a) \in A^+$.

Thereby, we get contradiction.

$\therefore a - b = 0 \rightarrow a = b$.

$\therefore T$ is antisymmetric.

(iii) Let $(a, b) \in T \wedge (b, c) \in T$.

$a = b \vee b - a \in A^+$.

Also, $c = b \vee c - b \in A^+$.

Let $b - a \in A^+ \wedge c - b \in A^+$.

$\because c - a = (c - b) + (b - a)$,

$\because (c - b) \in A^+(b - a) \in A^+$,

$\therefore c - a \in A^+ \rightarrow (a, c) \in T$.

$\therefore T$ is transitive.

From (i), (ii)& (iii), T is a partial ordered relation on A.

Now, we have to prove that every two elements in A are comparable.

Suppose $a, b \in A$,

$\therefore b - a \in A$.

Thereby, just one of the following satisfied;

$b - a \in A + \vee b - a = 0_A \vee a - b \in A^+$.

$\therefore (a, b) \in T \vee (b, a) \in T$.

Thus, T is a totally ordered relation on A.

(2) $\because T$ is a totally ordered relation on A,

$\therefore \leq$ is a totally relation on A.

Suppose that $a \leq b, \forall a, b \in A$.

$\therefore a = b \vee b - a \in A^+$.

If $a = b$,

$\therefore \exists c \in A \neq a + c = b + c$.

If $b - a \in A^+$,

$\therefore (b - a) = (b + c) - (a + c) \rightarrow (b + c) - (a + c) \in A^+$.

Thereby, $a + c \leq b + c$.

Suppose $a < b \wedge c > 0 \rightarrow bc - ac = (b - a)c$,

$\because c \in A^+ \wedge b - a \in A^+$,

$\therefore (b - a)c \in A^+ \rightarrow ac < bc$.

Thus, $(A, +, \cdot, \leq)$ is an ordered integral domain.

(3) It is left for the reader as an exercise. ♦

Note: If $(A, +, \cdot, \leq)$ is an ordered integral domain, then $A^+ = \{a | a \in A \wedge a > 0\}$ will be a set of positive elements in A, and the relation:

$T = \{(a, b) | (a = b) \wedge (b - a) \in A^+\}$ will be a totally ordered relation on $(A, +, \cdot, \leq)$.

Theorem 8.27 *Let $(A, +, \cdot, \leq)$ be an ordered integral domain, and $0 \neq a \in A$, then a^2 is a positive in A.*

Proof $\because a \neq 0$,

$\therefore a \in A^+ \vee -a \in A^+$.

If $a \in A^+ \rightarrow a \cdot a = a^2 \in A^+$.

If $-a \in A^+ \rightarrow (-a) \cdot (-a) = a^2 \in A^+$.

$\therefore a^2 \in A^+$.

$\because I_A \neq 0 \rightarrow I_A \cdot I_A$ will be a positive.

$\because I_A \cdot I_A = I_A \rightarrow I_A > 0$. ♦

Note: If $a, b \in \mathbb{Z}$, then $ab = 1 \leftrightarrow a = b = \mp 1$.

8.9 Embedding

Definition 8.24 Let $E_{\mathbb{N}}^{\mathbb{Z}} : \mathbb{N} \rightarrow \mathbb{Z}$ be a mapping, such that

$E_{\mathbb{N}}^{\mathbb{Z}}(n) = [n, 0], \forall n \in \mathbb{N}$. The mapping is called embedding $\mathbb{N}$ in $\mathbb{Z}$ (Mustafa et al., 1980; Palmer, 1994).

Note: For convenience, we use E instead of $E_{\mathbb{N}}^{\mathbb{Z}}$.

Theorem 8.28 *The mapping* $E_{\mathbb{N}}^{\mathbb{Z}} : \mathbb{N} \to \mathbb{Z}$ *is injective from* $\mathbb{N}$ *to* $\mathbb{Z}^+ \cup \{0\}$ *such that preserves addition, multiplication, and ordinal.*

Proof Let $m, n \in \mathbb{N}$.

(1) Preserving on addition.

$\because m, n \in \mathbb{N}$,

$\therefore E(m + n) = [m + n, 0] = [m, 0] + [n + 0] = E(m) + E(n)$.

$\therefore E$ preserves on addition.

(2) Preserving on multiplication.

$\because m, n \in \mathbb{N}$,

$\therefore E(mn) = [mn, 0] = [m, 0] \cdot [n, 0] = E(m) \cdot E(n)$.

$\therefore E$ preserves on multiplication.

(2) Preserving on ordinal.

$\because m, n \in \mathbb{N}$, and let $E(m) \leq E(n) \leftrightarrow [m, 0] \leq [n, 0], \forall m, n$.

$\because [m, 0] \leq [n, 0] \leftrightarrow [n, 0] - [m, 0] \in \mathbb{Z}^+ \vee m = n$.

$\leftrightarrow [n, 0] + [0, m] \in \mathbb{Z}^+ \vee m = n$,

$\leftrightarrow [n, m] \in \mathbb{Z}^+ \vee m = n$,

$\leftrightarrow m < n \vee m = n$,

$\leftrightarrow m \leq n$.

$\therefore E$ preserves on ordinal.

$\therefore$ from (1), (2)& (3), we get that $E : \mathbb{N} \to Z$ is isomorphism from $\mathbb{N}$ to $\mathbb{Z}^+ \cup \{0\}$ with respect to addition, multiplication, and ordinal operation. ⧫

Note: $E_{\mathbb{N}}^{\mathbb{Z}}(1) = [1, 0] = I_{\mathbb{Z}}$.

Notation: We use (1) n instead of $[n, 0]$. (2) 1 instead of $I_{\mathbb{Z}}$.

Definition 8.25 (1) Let $*, *'$ be a binary operations on the sets A, A' respectively. For the injective mapping $F : A \to A'$, the $(*, *')$ is said to be isomorphism if and only if $F(a * b) = F(a) *' F(b), \forall a, b \in A$.

(2) Let T, T' be a binary relations on the sets A, A' respectively. For the injective mapping $F : A \to A'$, the (T, T') is said to be isomorphism

if and only if $aTb \leftrightarrow F(a)T'F(b), \forall a, b \in A$ (Awodey, 2010; Vinberg, 2003; Mustafa et al., 1980).

The following definition is another expression of the previous definition, in which combines both parts of the definition into one expression.

Definition 8.26 Let each of A, A' be a set if there exists an isomorphic relation from A to A', then a pair of relations (α, α'), the A' is said to be an extension of A with respect to (α, α'), and A said to be isomorphically embedded in A' with respect to (α, α') (Mustafa et al., 1980).

Example 8.19 $\mathbb{Z}$ is extension of $\mathbb{N}$ with respect to the addition, multiplication, and the ordinal. Or, $(+_{\mathbb{N}}, +_{\mathbb{Z}}), (\cdot_{\mathbb{N}}, \cdot_{\mathbb{Z}}), (\leq_{\mathbb{N}}, \leq_{\mathbb{Z}})$.

8.10 Exercises

Answer the following questions:

Q1: Let $(A, +, \cdot)$ be a commutative ring with an identity element $1 \neq 0$ defined on the totally ordered relation $\leq$, where

(1) $a < b \to a+c < b+c, \forall a, b, c \in A$. (2) $a < b \to ac < bc, \forall a, b, c \in A \wedge c > 0$.

Prove that $(A, +, \cdot)$ is an ordered integral domain.

Q2: Consider the ordered integral domain $(A, +, \cdot, \leq)$. Prove that A is an infinite set.

Q3: Let $\mathbb{Z}_n$ ba the set of the integer numbers module n. The system $(\mathbb{Z}_n, +_n, \cdot_n)$ is integral domain if and only if n is a prime. Prove that if n is a prime then the system $(\mathbb{Z}_n, +_n, \cdot_n)$ can not be an ordered integral domain.

Q4: If $a \in \mathbb{Z}$, then $\nexists b \in \mathbb{Z} \ni a < b < a + 1$.

Q5: Any nonempty subset of $\mathbb{Z}^+$ has a least element.

Q6: Any nonempty subset of $\mathbb{Z}^- \ni -a \in \mathbb{Z}^+$ has a greatest element.

Q7: Let $\phi \neq A \subseteq \mathbb{Z}$, where A has a least element. Prove if $\phi \neq B \subseteq A$, then B has also a least element.

9

The Rational Numbers

9.1 Introduction

In this chapter, we extend the field of integers to another, more general, and comprehensive field within it to meet mathematical necessaries and practical reality. We call the new field the field of rational numbers, and denote it by $\mathbb{Q}$.

Let us consider the problem $ax = b, \forall 1 \neq a, b \in \mathbb{Z}$. When we are looking for the value of s in this problem, we find that $x = \left\{ \frac{b}{a} | a, b \in \mathbb{Z} \right\}$. The value of variable does not belongs to $\mathbb{Z}$. Thereby, it is inevitable for us to create a field of $\mathbb{Q}$ to overcome this defect and drawback in the field of $\mathbb{Z}$.

We are going to define the addition, multiplication, and partial order relation on $\mathbb{Q}$ denoted them $\mathbb{Q}_+, \mathbb{Q}., \mathbb{Q}_\leq$ respectively. To organizing the mathematical system $(\mathbb{Q}, \mathbb{Q}_+, \mathbb{Q}., \mathbb{Q}_\leq)$ to be extension of the system $(\mathbb{Z}, \mathbb{Z}_+, \mathbb{Z}., \mathbb{Z}_\leq)$ with respect to addition, multiplication, and partial ordered relation.

9.2 Construction of $\mathbb{Q}$

Let us define the equivalence relation on the ordered pairs of integer numbers in which we call to each equivalence class by rational numbers.

From now on, we express the order pairs (a, b) in the form of fractions denoted by $\frac{a}{b}, b \neq 0$. Mathematically, $A = \{(a, b) | a, b \in \mathbb{Z}, b \neq 0\}$ (Rosen and Krithivasan, 2012; Lass, 2009; Robinson, 1996; Weisstein, 2002c).

Theorem 9.1 (Introductory Theorem) *There is an equivalence relation R on the set A such that $(a, b)R(c, d)$ if and only if $ad = cb, \forall (a, b), (c, d) \in A$.*

Proof Since R is reflexive and symmetric, so we have to prove that it is a transitive.

Let $(a, b), (c, d), (e, f) \in A$, $(a, b)R(c, d) \wedge (c, d)R(e, f)$.
$\therefore (ad = cb) \wedge (cf = ed)$.
Now, we have $adf = cbf = bcf = bed$,
$\therefore afd = bed$.
$\because d \neq 0$,
$\therefore af = be$.
$\therefore (a, b)R(e, f)$.
$\therefore R$ is transitive.
Thereby, R is equivalence relation on A. ♦

Example 9.1 Let $(2, 3), (10, 15), (1, 3), (7, 8) \in A$.
$(2, 3)R(10, 15)$ because $2 \cdot 15 = 3 \cdot 10$.
$\therefore [(2, 3)] = [(10, 15)]$.
While $(1, 3) \not R (7, 8)$ because $1 \cdot 8 \neq 3 \cdot 7$.
$\therefore [(1, 3)] \neq [(7, 8)]$.

Notation: Then the expression $(a, b) \sim (c, d)$ to indicate that $(a, b), (c, d) \in R$. It reads $(a, b) \equiv (c, d)$.

Definition 9.1 Equivalence class that contains on (a, b) is called rational number, and it is denoted by $[a, b] = \{(c, d) | (c, d) \sim (a, b)\}$.

The set of all equivalence classes is called rational number, and denoted by $\mathbb{Q} = \left\{\frac{a}{b} | a, b \in \mathbb{Z} \wedge b \neq 0\right\}$ (Rosen and Krithivasan, 2012; Lass, 2009; Robinson, 1996; Weisstein, 2002c).

Example 9.2 $[0, 1] = \{(c, d) | (c, d) \sim (0, 1)\}$

$= \{(c,d)|c \cdot 1 = 0 \cdot d \sim (0,1)\}$
$= \{(c,d)|c = 0\}.$
$\therefore [0,1] = \{(0,1),(0,2),...\} = \{(0,-1),(0,-2),...\}$

Note: The number $\mathbb{Q}$ can be denoted $x, y, z, ...$

9.2.1 Addition and Multiplication on $\mathbb{Q}$

Before starting to define the operations of addition and multiplication on the set of $\mathbb{Q}$, we need the following introductory theorem;

Theorem 9.2 (Introductory Theorem)
If $(a,b) \sim (a',b') \wedge (c,d) \sim (c',d'), \forall (a,b),(a',b'),(c,d) \sim (c',d') \in A$, *then*
(1) $(ad+cb, bd) \sim (a'd'+c'b', b'd')$. *(2)* $(ac, bd) \sim (a'c', b'd')$.

Proof (1) $\because (a,b) \sim (a',b') \wedge (c,d) \sim (c',d')$,
$\therefore$ (1) $cd' = a'b$. (2) $cd' = c'd$.
Now, $(ad+cb)b'd'$
$= abb'd' + cbb'd'$
$= ab'dd' + cd'bb'$
$= a'bdd' + c'dbb'$
$= (a'd'+c'b')bd.$
$\therefore (ad+cb, bd) \sim (a'd'+c'b', b'd').$
(2) $(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd).$
$\because bd \neq 0 \wedge b'd' \neq 0,$
$\therefore (ac, bd) \sim (a'c', b'd').$ ♦

Theorem 9.3 *The addition* (F)*, and multiplication operation* (G) *on* $\mathbb{Q}$ *can be defined as follows;*
If $(a,b) \in x, (c,d) \in y$, *then*
(1) $F(x,y) = [ad+cb, bd]$. *(2)* $G(x,y) = [ac, bd]$.

Proof (1) It should be noted that
(i) $(ad+cb, bd) \in A$.
(ii) $F = \{((x,y),[ad+cb,bd])|(a,b) \in x \wedge (c,d) \in y; x,y \in \mathbb{Q}\} \subset (\mathbb{Q} \times \mathbb{Q}) \times \mathbb{Q}$. Or, $F : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ is a relation.

We have to prove that F is a functional relation.

Suppose that $\forall (x, y) \in \mathbb{Q} \times \mathbb{Q}\ \exists (a, b) \in x \wedge (c, d) \in y, z = [ad + cb, bd] | ((x, y), z) \in F$.

$\therefore domF = \mathbb{Q} \times \mathbb{Q}$.

Suppose that $(a', b') \in x, (c', d') \in y, z' = [a'd' + c'b', b'd'] \ni (a, b) \sim (a'b'), (c, d) \sim (c'd')$.

Now, based on Theorem 9.2, we conclude that

$(ad + cb, bd) \sim (a'd' + c'b', b'd')$.

$\therefore [ad + cb, bd] \sim [a'd' + c'b', b'd']$.

$\therefore F$ is a functional relation.

$\therefore F : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ is a mapping, and F is a binary operation on $\mathbb{Q}$.

(2) In the same way, we can prove that G is a binary operation on $\mathbb{Q}$. ♦

Definition 9.2 Let $x, y \in \mathbb{Q}$, where $(a, b) \in x, (c, d) \in y$. The binary operation F on $\mathbb{Q}$ such that $F(x, y) = [ad + cb, bd]$ is called addition on $\mathbb{Q}$, and expressed:

$F(x, y) = x +_{\mathbb{Q}} y, \forall x, y \in \mathbb{Q}$.

The binary operation G on $\mathbb{Q}$ such that $G(x, y) = [ac, bd]$ is called multiplication on $\mathbb{Q}$, and expressed:

$G(x, y) = x \cdot_{\mathbb{Q}} y, \forall x, y \in \mathbb{Q}$. (Rosen and Krithivasan, 2012; Lass, 2009; Robinson, 1996; Weisstein, 2002c).

Note: We will just write $x+y, xy$ instead of $x+_{\mathbb{Q}}y, x\cdot_{\mathbb{Q}}y$ respectively.

Example 9.3 Consider $x = [3, 5] \in \mathbb{Q}, y = [7, 8] \in \mathbb{Q}$, then

(1) $x + y = [3 \cdot 8 + 7 \cdot 5, 5 \cdot 8] = [59, 40] \in \mathbb{Q}$.

(2) $x \cdot y = [3 \cdot 7, 5 \cdot 8] = [21, 40] \in \mathbb{Q}$.

Theorem 9.4 *The mathematical system* $(\mathbb{Q}, +, \cdot)$ *is a commutative ring with unit element.*

Proof (1) The mathematical system $(\mathbb{Q}, +)$ is a commutative group.

(a) $x + (y + z) = (x + y) + z = (x + z) + y, \forall x, y, z \in \mathbb{Q}$ is left for the reader.

(b) $[0, 1]$ is the identity element with respect to the addition.

If $x = [a, b] \in \mathbb{Q}$, then

$x + [0,1] = [a,b] + [0,1] = [a \cdot 1 + 0 \cdot 0, b \cdot 1] = [a,b] = x$ ...(i).

In the same way, we can prove that $[0,1] + x = x$ ...(ii).

From (i)& (ii), $[0,1]$ is the identity element.

(c) For all $x \in \mathbb{Q}$, there is an inverse in $\mathbb{Q}$ with respect to the addition.

If $x = [a,b]$, then $x' = [-a,b]$ as an inverse for x where $x' \in \mathbb{Q}$.

Now, $x + x' = [a,b] + [-a,b] = [ab + (-a)b, b^2] = [0,b^2] = [0,1]$ ...(i).

In the same way $x' + x = [0,1]$ ...(ii).

From (i)& (ii), x' is the inverse of x.

(d) The commutative property $x + y = y + x, \forall x, y \in \mathbb{Q}$ is left for the reader.

Thereby, from (a), (b), (c)& (d), the system $(\mathbb{Q}, +)$ is a commutative group.

(2) The mathematical system $(\mathbb{Q}, \cdot)$ is a commutative semigroup with unit element.

(a) Let $x, y, z \in \mathbb{Q}$, where $x = [a,b], y = [c,d], z = [e,f]$.

$x \cdot (y \cdot z) = [a,b] \cdot ([c,d] \cdot [e,f])$

$= [a,b] \cdot ([c,d] \cdot [e,f])$

$= [a(ce), b(df)]$

$= [(ac)e, (bd)f]$

$= [ac, bd] \cdot [e,f]$

$= ([a,b] \cdot [c,d]) \cdot [e,f]$

$= (x \cdot y) \cdot z.$

(b) The $[1,1]! \in \mathbb{Q}$ such that

(i) $x \cdot [1,1] = [a,b] \cdot [1,1] = [a \cdot 1, b \cdot 1] = [a,b]$.

(ii) In the same way $[1,1] \cdot x = x$.

From (i)& (ii), $[1,1]$ is the unique element in $\mathbb{Q}$.

(c) The commutative property $x \cdot y = y \cdot x, \forall x, y \in \mathbb{Q}$ is left for the reader.

Thereby, from (a), (b)& (c), the system $(\mathbb{Q}, \cdot)$ is the commutative semigroup with unit element.

(3) Multiplication in distribution over addition

Let $x, y, z \in \mathbb{Q}$ where $x = [a,b], y = [c,d], z = [e,f]$.

$x \cdot (y + z) = [a,b] \cdot ([c,d] + [e,f])$

$= [a,b] \cdot ([cf + ed, df])$

$= [acf + aed, bdf]$

$= [acbdf + aebd, b^2df]$
$= [ac, bd] + [ae, bf]$
$= [a, b] \cdot [c, d] + [a, b] \cdot [e, f]$
$= x \cdot y + x \cdot z$ ...(i).

In the same way, $(y + z) \cdot z = y \cdot x + z \cdot x$ ...(ii).

From (i)& (ii) multiplication in distribution over addition.

Thus, from (1), (2)& (3), the system $(\mathbb{Q}, +, \cdot)$ is a commutative ring with unit element. ⧫

Note: The mathematical system $(\mathbb{Q}, +, \cdot)$ is a numerical system, and called system of the rational numbers.

Notation:

(1) $0_{\mathbb{Q}}\ vee0$ is denoted to $[0, 1]$.

(2) $-x$ is denoted to the inverse of x.

(3) $I_{\mathbb{Q}} \vee 1_{\mathbb{Q}}$ is denoted to $[1, 1]$.

Definition 9.3 Let $x, y \in \mathbb{Q}$, where $x = [a, b], y = [c, d]$. The subtraction $x - y$ is defined as

$x - y = x + (-y) = [a, b] + [-c, d] = [ad - cb, bd]$ (Rosen and Krithivasan, 2012; Lass, 2009; Robinson, 1996; Weisstein, 2002c).

Example 9.4 If $x = [3, 8], y = [5, 12]$, then

$x - y = [3, 8] + [-5, 12] = [3 \cdot 12 - 8 \cdot 5, 8 \cdot 12] = [-4, 96]$.

9.2.2 Fields

Definition 9.4 Let $\phi \neq A$, and $*, \#$ be binary operations on A. The mathematical system $(A, *, \#)$ is called a field if and only if

(1) $(A, *)$ is a commutative group.

(2) $(A', \#')$ is a commutative group where $A' = A \backslash \{0\}$, 0 is a unit element with respect to $*$, and $\#'$ is a restriction operation on A'.

(3) Distribution laws are fulfilled. Or, if $\forall x, y, z \in A$, then:

(a) $x \cdot (y + z) = x \cdot y + x \cdot z$.

(b) $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$ (Beachy and Blair, 2006; Fraleigh, 2003; McCoy, 1968; Sharpe, 1987).

Theorem 9.5 *The mathematical system* $(\mathbb{Q}, +, \cdot)$ *is a field.*

Proof $\because$ the system $(\mathbb{Q},+,\cdot)$ is a commutative field with an identity element.

$\therefore$ is enough to prove that $\forall x \in \mathbb{Q}\backslash\{0\}$ has an inverse in $\mathbb{Q}\backslash\{0\}$.

$\because x \in \mathbb{Q}\backslash\{0\}$,

$\therefore x=[a,b] \in \mathbb{Q}, x \neq 0[0,1]$.

$\therefore a \neq 0 \rightarrow x'=[b,a] \in \mathbb{Q} \wedge x' \neq 0$.

$\therefore x' \in \mathbb{Q}\backslash\{0\}$.

Furthermore, $x \cdot x'=[a,b]\cdot[b,a]=[ab,ba]=[1,1]=1$ ...(1).

In the same way, $x' \cdot x=1$ ...(2).

From (1) & (2), x' is the desired inverse element of x.

Thereby, the mathematical system $(\mathbb{Q}\backslash\{0\},\cdot)$ is a commutative group.

Thus, $(\mathbb{Q},+,\cdot)$ is a field. ♦

Note:

(1) The mathematical system $(\mathbb{Q},+,\cdot)$ is called the field of $\mathbb{Q}$.

(2) For the field $(A,*,\#)$, then $0_A, 1_A$, or $0,1$ as the additive identity, and multiplicative identity respectively.

(3) If $x \in A\backslash\{0\}$, then $\frac{1}{x}$ is to denote the multiplicative element $x \in A$.

Definition 9.5 Let $x \in \mathbb{Q}, y \in \mathbb{Q}\backslash\{0\}$. The quotient $\frac{x}{y}$ is defined as $\frac{x}{y}=x\cdot y^{-1}$ (Graham et al., 1994; Spanier, 1987; Epp, 2010).

Example 9.5 (1) If $x=[7,8], y=[1,1]$ then $\frac{1}{x}=[8,7]$.

$x\cdot\frac{1}{x}=[7,8]\cdot[8,7]=[7\cdot 8,8\cdot 7]=[1,1]$.

(2) If $x=[3,8], y=[-4,9]$ then $\frac{y}{x}=y\cdot x^{-1}=[-4,9]\cdot[8,3]=[-32,27]$.

It should be noted that

$(y\cdot x^{-1})\cdot x=[-32,27]\cdot[3,8]=[-72,216]=[-4,9]=y$.

9.2.3 Subfields

Definition 9.6 Consider the field $(A,*,\#)$, and $\phi \neq B \subseteq A$. The mathematical system $(B,*',\#')$ is a field such that $*',\#'$ are restriction of $*,\#$ respectively on B. The system $(B,*',\#')$ is subfield of $(A,*,\#)$ (Fraleigh, 2003; Herstein, 1964; Lang, 2004; McCoy, 1968).

Example 9.6 (1) The system $(\mathbb{Q}, +, \cdot)$ is a subgroup of the system $(\mathbb{R}, +, \cdot)$.

(2) The system $(\mathbb{Z}, +, \cdot)$ is not subgroup of the system $(\mathbb{Q}, +, \cdot)$ but it is a subdomain of it.

(3) The system $(\mathbb{R}, +, \cdot)$ is a subgroup of the system $(\mathbb{C}, +, \cdot)$.

Note: For convenient, we write $(A, +, \cdot)$ instead of $(A, *, \#)$. It is not necessarily $+, \cdot$ represent the addition and multiplication respectively.

Theorem 9.6 *If $x, y, z \in A$, and the mathematical system $(A, +, \cdot)$ is a field then*

(1) $x(-y) = (-x)y = -(xy)$.

(2) $x \cdot 0 = 0$.

(3) $x(y - z) = xy - xz$.

(4) $-(-x) = x$.

(5) $-(x + y) = -x - y$.

(6). If $x, y \neq 0$, then (a) $xy \neq 0$. (b) $(xy)^{-1} = x^{-1}y^{-1}$. Or, $\frac{1}{xy} = \frac{1}{x} \cdot \frac{1}{y}$.

(7) If $x \neq 0$, then $(x)^{-1^{-1}}$. Or, $\frac{1}{\frac{1}{x}} = x$.

Proof The proof is left for the reader as an exercise. ♦

Theorem 9.7 *Every field is an integral domain. Thereby, the field of rational numbers is an integral domain.*

Proof Suppose that $(A, +, \cdot)$ is a field, and $ab = 0, \forall a, b \in A$.

Now, let $a \neq 0$.

$\therefore a^{-1} \in A$,

$\therefore a^{-1}(ab) = a^{-1} \cdot = 0$.

$\therefore b = 0$ ...(1).

In the same way, if we suppose that $b \neq 0$. we get that

$a = 0$ ...(2).

From (1)& (2), we conclude that A have not zero divisors.

Thus, $(A, +, \cdot)$ is integral domain. ♦

Example 9.7 Let $k \in \mathbb{Z}^+$, and $\mathbb{Z}_k = \{r \in \mathbb{Z} | 0 \leq r < k - 1\}$.

Define the operation $\oplus$ on $\mathbb{Z}_k$ as follow;

$r \oplus s = t \in \mathbb{Z}_k$, where $(r + s) - t$ is multiples of $k \in \mathbb{Z}$ ($\oplus$ is addition module k).

Also, define $\odot$ on $\mathbb{Z}_k$ as follows;

$r \odot s = t \in \mathbb{Z}_k$, where $rs - t$ is multiples of $k \in \mathbb{Z}$ ($\odot$ is multiple module k).

The mathematical system $(\mathbb{Z}_k, \oplus, \odot)$ is a field if and only if k is a primal number.

Definition 9.7 For all a primal number k, $\mathbb{Z}_k$ is called field of integers *mod k* (Lidl and Niederreiter, 1997; Mustafa et al., 1980).

9.3 Exercises

Solve the following problems:

Q1: Prove that every finite integral domain is a field.

Q2: Give an example of a field consists of five elements.

Q3: Give an example of an integral domain that does not form a field.

Q4: Is there a field with ten elements?

Q5: Consider an integral domain D, and $a, b \in D$. Suppose that $a^n = b^n, a^m = b^m$ where $(m, n) = 1$ (m, n are relatively prime). Prove that $a = b$.

Q6: Let F be a field, and $F[x] = \{\sum_0^n a_i | n \in \mathbb{N}, a_i \in F\}$. Define the operations of addition and multiplication on $F[x]$ in order it be a ring of polynomials.

Q7: Consider the field $(\mathbb{Z}_{15}, +_{15}, \cdot_{15})$. Let $S = \{[0], [5], [10]\} \subset \mathbb{Z}_{15}$, and $T = \{[0], [3], [6], [9], [12]\} \subset \mathbb{Z}_{15}$. Prove that each of $(S_{15}, +_{15}, \cdot_{15}), (T_{15}, +_{15}, \cdot_{15})$ is a field.

9.4 Order on $\mathbb{Q}$

In this section we are going to present and deal with a set of element of $\mathbb{Q}$.

9.4.1 The Positive $\mathbb{Q}$

Notation: $\mathbb{Q}^+ = \{x \in \mathbb{Q} | ab > 0, (a,b) \in x\}$.

Theorem 9.8 *Let $x \in \mathbb{Q}, (a,b), (c,d) \in x$. If $ab > 0$, then $cd > 0$, and vise versa.*

Proof $\because (a,b) \sim (c,d)$,

$\therefore ad = cb$.

$\therefore (ab)(cd) = (cb)(cb)$.

$\therefore (ab)(cd) = (cb)(cb) \geq 0$.

$\because ab > 0$,

$\therefore cd > 0$. ♦

Corollary $\mathbb{Q}^+ = \{x \in \mathbb{Q} | ab > 0, \forall (a,b) \in x\}$

Proof The proof is left for the reader. ♦

Theorem 9.9 *The set $\mathbb{Q}^+$ is a positive elements of $\mathbb{Q}$.*

Proof Let $x, y \in \mathbb{Q}^+$.

(1) $\therefore x = [a,b], y = [c,d]$ where $(ab > 0) \wedge (cd > 0), a, b, c, d \in \mathbb{Z}$.

$\because$ $x + y = [a,b] + [c,d] = [ad + cb, bd]$ where $(ad + cb) \cdot bd = a \cdot b \cdot d \cdot d + c \cdot d \cdot b \cdot d$.

$\therefore x + y \in \mathbb{Q}^+$.

(2) $x \cdot y = [a,b] \cdot [c,d] = [ac, bd]$, where $(ac)(bd) = (ab)(cd) > 0$.

$\therefore x, y \in \mathbb{Q}^+$.

(3) By using the Trichotomy Property (Marsden et al., 1993; Bear, 1997; Patrick, 1960; Takeuti and Zaring, 2013; Suppes, 1960; Suppes, 1972) in $\mathbb{Z}$, only one of the following relationships can be satisfied;

(a) $ab > 0$. (b) $ab = 0$. (c) $-(ab) > 0$.

Now, if

(a) $ab > 0 \leftrightarrow x \in \mathbb{Q}^+$.

(b) $ab > 0 \leftrightarrow a = 0 \wedge b \neq 0, \mathbb{Z}$ is the integral domain.

Or, $ab = 0 \leftrightarrow x = [0,b] = 0$.

(c) $-(ab) > 0 = -(a) \cdot b = -ab > 0 \leftrightarrow [-a,b] = -x \in \mathbb{Q}^+$.

$\therefore x \in \mathbb{Q}^+ \vee x = 0 \vee -x \in \mathbb{Q}^+$.

$\therefore \mathbb{Q}^+$ is a positive elements of $\mathbb{Q}$. ♦

Now, lut us utilize $\mathbb{Q}^+$ to define a partial ordered relation on $\mathbb{Q}$.

Definition 9.8 Let $x, y \in \mathbb{Q}$. It said that x is less than y, and written $x < y \leftrightarrow y - x \in \mathbb{Q}^+$ (Itō, 1993; Mustafa et al., 1980; Bourbaki, 2003).

Notation: For all $x, y \in \mathbb{Q}$, then

(1) $x > y \to y < x$, and read x is greater than y.

(2) $x \leq y \to (x < y) \vee (x = y)$, and read x is less than or equal to y.

(3) $x \geq y \to (x < y) \vee (x = y)$, and read x is greater than or equal to y.

Theorem 9.10 *The mathematical system* $(\mathbb{Q}, \leq)$ *is a totally ordered set.*

Proof (1) $\because x \leq x, \forall x \in \mathbb{Q}$,

$\therefore \leq$ is a reflexive relation.

(2) Suppose that $x \leq y, y \leq x$.

$\because x \leq y \to (x = y) \vee (y - x \in \mathbb{Q}^+)$.

$\because y \leq x \to (y = x) \vee (x - y \in \mathbb{Q}^+)$.

$\because y - x \in \mathbb{Q}^+ \to -(y - x) \in \mathbb{Q}^+$.

This is a contradiction because $\mathbb{Q}^+$ consists of the positive elements only.

$\therefore x = y$.

In the same way, we can prove the other hypothesis (Have is to the reader).

$\therefore \leq$ is anti symmetric relation.

(3) Suppose that $x \leq y, y \leq z, \forall x, y, z \in \mathbb{Q}^+$.

$x \leq y \to (x = y) \vee (x < y)$.

$y \leq z \to (y = z) \vee (y < z)$.

$\because (x < y) \wedge (y < z)$,

$\therefore (y - x) \in \mathbb{Q}^+ \wedge (z - y) \in \mathbb{Q}^+$.

$\therefore (y - x) + (z - y) \in \mathbb{Q}^+ \to (z - x) \in \mathbb{Q}^+$.

$\therefore x < z$.

In the same way, we can prove the other hypothesis (Have is to the reader).

$\therefore x \leq z$.

$\therefore \leq$ is a transitive relation.

$\therefore \leq$ is an ordered relation on $\mathbb{Q}$.

(4) If $x, y \in \mathbb{Q}$, then

$((y - x) \in \mathbb{Q}^+ \vee (y - x = 0) \vee (-(y - x) \in \mathbb{Q}^+)$.

$\therefore (x < y) \vee (y = x) \vee (y < x)$.

$\therefore (x \leq y) \vee (y \leq x)$.

Thereby, every two elements in $\mathbb{Q}$ are comparable.

Thus, $\leq$ is a totally ordered relation on $\mathbb{Q}$. ♦

Note: The relation $\leq$ is not perfect ordered relation on the set $\mathbb{Q}$, because the set $S = \{x \in \mathbb{Q} | x \leq 1\}$ does not have first element.

Definition 9.9 Let $x \in \mathbb{Q}$. It is said that x is a negative rational number if $-x \in \mathbb{Q}^+$. Or, $x < 0 >$ (Mustafa et al., 1980; Rosen and Krithivasan, 2012; Lass, 2009; Robinson, 1996; Weisstein, 2002c).

Example 9.8 $[-7, 8] \in \mathbb{Q}^-$ because $-[-7, 8] = [7, 8] \in \mathbb{Q}^+$.

Generally, $[-a, b] \in \mathbb{Q}^- \rightarrow -[-a, b] = [a, b] \in \mathbb{Q}^+, \forall\ 0 < b, a \in \mathbb{Z}$.

Theorem 9.11 *The mathematical system* $(\mathbb{Q}, +, \cdot, \leq)$ *is ordered integral domain.*

Proof Since $\leq$ is a totally ordered relation, hence it is enough to prove that

(1) If $x < y$, then $x + z < y + z, \forall z \in \mathbb{Q}$.

(2) If $x < y, z \in \mathbb{Q}^+$, then $xz < yz$,

$\because yz - xz = (y - x)z$,

$\because (y - x) \in \mathbb{Q}^+, z \in \mathbb{Q}^+$,

$\therefore (y - x)Z \in \mathbb{Q}^+$.

$\therefore xz < yz$.

From (1)& (2), $(\mathbb{Q}, +, \cdot, \leq)$ is an ordered integral domain. ♦

Definition 9.10 The algebraic system $(A, +, \cdot, \leq)$ is an ordered integral domain such that the mathematical system $(A, +, \cdot)$ is a field.

The algebraic system $(A, +, \cdot, \leq)$ is called ordered field (Lam, 1983a; Lam, 1983b; Lang, 2002a; Lang, 1993a).

As a result of the definition, we can conclude the following corollary:

Corollary *The mathematical system* $(\mathbb{Q}, +, \cdot, \leq)$ *is an ordered field.*

Proof The proof can be obtained directly from the definition, and previous theorems. ♦

9.4.2 Embedding

Definition 9.11 The mapping from the set $\mathbb{Z}$ to the set $\mathbb{Q}$ denoted by $E_{\mathbb{Z}}^{\mathbb{Q}}$ defined as $E_{\mathbb{Z}}^{\mathbb{Q}} = [n, 1]$ is called embedding (Spivak, 1975; Sharpe, 1987; Gunderson, 2019; Smith, 2015; Junghenn, 2018).

Theorem 9.12 *The mapping* $E_{\mathbb{Z}}^{\mathbb{Q}} : \mathbb{Z} \to \mathbb{Q}$ *is an isomorphic embedding with respect to the addition, multiplication, and ordering.*

Proof (1) $E_{\mathbb{Z}}^{\mathbb{Q}}$ is an injective mapping.
Let $E_{\mathbb{Z}}^{\mathbb{Q}}(a) = E_{\mathbb{Z}}^{\mathbb{Q}}(b)$.
$\therefore [a, 1] = [b, 1]$,
$\therefore [a \cdot 1] = [b \cdot 1]$,
$\therefore a = b$.
(2) The mapping $E_{\mathbb{Z}}^{\mathbb{Q}}$ preserves addition.
Let $a, b \in \mathbb{Z}$.
$E_{\mathbb{Z}}^{\mathbb{Q}}(a + b) = [a + b, 1] = [a, 1] + [b, 1] = E_{\mathbb{Z}}^{\mathbb{Q}}(a) + E_{\mathbb{Z}}^{\mathbb{Q}}(b)$.
(3) The mapping $E_{\mathbb{Z}}^{\mathbb{Q}}$ preserves multiplication.
Let $a, b \in \mathbb{Z}$.
$E_{\mathbb{Z}}^{\mathbb{Q}}(ab) = [ab, 1] = [a, 1] \cdot [b, 1] = E_{\mathbb{Z}}^{\mathbb{Q}}(a) \cdot E_{\mathbb{Z}}^{\mathbb{Q}}(b)$.
(4) The mapping $E_{\mathbb{Z}}^{\mathbb{Q}}$ preserves order.
Let $a, b \in \mathbb{Z}, a \leq b$.
$\because a \leq b \leftrightarrow (b - a \in \mathbb{Z}^+) \vee (b = a)$
$\leftrightarrow ([b - a, 1] \in \mathbb{Z}^+) \vee ([b, 1] = [a, 1])$.
$\because [b - a, 1] = [b, 1] - [a, 1] = E_{\mathbb{Z}}^{\mathbb{Q}}(b) - E_{\mathbb{Z}}^{\mathbb{Q}}(a)$,
$\therefore a \leq b \leftrightarrow E_{\mathbb{Z}}^{\mathbb{Q}}(a) \leq E_{\mathbb{Z}}^{\mathbb{Q}}(b)$. ♦

Corollary *The ordered field* $(\mathbb{Q}, +, \cdot, \leq)$ *is an extension of the integral domain* $(\mathbb{Z}, +, \cdot, \leq)$.

Proof The proof is left for the reader. ♦

Notation: In the embedding isomorphism $E_{\mathbb{Z}}^{\mathbb{Q}}(b)(E_{\mathbb{N}}^{\mathbb{Z}}) = [n, 1]$. Or, we are using the same notation for both embedding.

(1) If $0 \neq k, h \in \mathbb{Z}$, then $[h, k] = \frac{[h,1]}{[k,1]} = \frac{E_{\mathbb{N}}^{\mathbb{Z}}}{E_{\mathbb{Z}}^{\mathbb{Q}}} = \frac{h}{k}$.

(2) We use the symbols $\mathbb{N}, \mathbb{Z}$ for the images of $\mathbb{N}, \mathbb{Z}$ in the set of $\mathbb{Q}$ respectively.

9.4.3 Absolute Value

Definition 9.12 Let the mathematical system $(A, +, \cdot, \leq)$ be an ordered field, and $F : A \rightarrow A$ be a mapping defined as follows, $F(x) = \max\{x, -x\}, \forall x \in A$. F is absolute value of x, and denoted as:

$$F(x) = |x| = \begin{cases} x; x \geq 0 \\ x; x < 0 \end{cases}$$

(Mendelson, 2009b; Stewart, 2009; Bartle and Sherbert, 2011; Schechter, 1996).

Note:

(1) The mapping F exists according of property of the triple ordered on A.

(2) The mapping F can be used to define a distance in the ordered field A as follows;

Let $x, y \in A$, then $d(x, y) = |x - y|$ (Trope and Liberman, 2010; Mendelson, 2009b; Stewart, 2009; Chamberlain, 2007; Thomas et al., 2010; Thomas et al., 2014; Hass et al., 2019; Anton et al., 2010).

(3) If $x \in A$, then

(a) $|x| = |-x| \geq 0$.

(b) $x < |x|, -x < |x|$.

(c) $|x| = 0 \leftrightarrow x = 0$.

Theorem 9.13 *Let the algebric system* $(A, +, \cdot, \leq)$ *be an ordered field, and* $x, y \in A$, *then* $|x + y| \leq |x| + |y|$.

Proof $\because x + y \leq |x| + |y|$, $-(x + y) \leq |x| + |y|$.

$$\because |x + y| = \begin{cases} x + y; (x + y) \geq 0 \\ -(x + y); (x + y) < 0 \end{cases}$$

$\therefore |x + y| \leq |x| + |y|$. ♦

9.5 Exercises

Solve the following problems:

Q1: Consider the injective mapping $F : A \to B$ from the field A into the field B such that F preserves addition and transports the positive elements. Prove that F preserves order.

Q2: If $x, y \in \mathbb{Q}$ then $x = \frac{h}{n}, y = \frac{k}{n}$ where $n \in \mathbb{Z}^+, h, k \in \mathbb{Z}$.

Q3: Prove that the ordered field of $\mathbb{Q}$ can isomorphically embedded in any other ordered field. Or, the field of $\mathbb{Q}$ is a smallest order field.

Q4: Let $x, y \in \mathbb{Q}$ where the mathematical system $(A, +, \cdot, \leq)$ is an ordered field. Prove that

(a) $|xy| = |x| \cdot |y|$.

(b) $|x| \cdot |y| \leq ||x| - |y|| \leq |x - y|$.

Q5: Let $x, y \in \mathbb{Q}$ if $x < y$, then $\frac{1}{x} > \frac{1}{y}$.

Q6: Prove that every rational number can be expressed as a terminating or repeating decimal, and vice versa.

Q7: Let $z < 0$. Prove that $xz < yz \leftrightarrow x > y, \forall x, y \in \mathbb{Q}$.

9.6 Properties of $\mathbb{Q}$

This section addresses the properties of the set $\mathbb{Q}$ where some of these properties are general properties of any ordered field and others are the specific properties of the set $\mathbb{Q}$.

Theorem 9.14 $\mathbb{Q}$ *is a countable set.*

Proof We will insert the positive rational numbers in an infinite number of sequences without repetition according to the sizes of their denominators, as follows;

$$\begin{array}{ccccc}
\frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \cdots \\
\frac{1}{2} & \frac{3}{2} & \frac{5}{2} & \frac{7}{2} & \cdots \\
\frac{1}{3} & \frac{2}{3} & \frac{4}{3} & \frac{5}{3} & \cdots \\
\frac{1}{4} & \frac{3}{4} & \frac{5}{4} & \frac{7}{4} & \cdots \\
. & . & . & . & \cdots \\
. & . & . & . & \cdots \\
. & . & . & . & \cdots
\end{array}$$

When listing all the positive rational numbers as follows; We start from the first number, which is $\frac{1}{1}$, and go down to the number $\frac{1}{2}$, and go up at the angle of 45° to the number$\frac{2}{1}$. Then, we go back to the third row and start at the number $\frac{1}{3}$, and go up at an angle of 45° until we reach the number $\frac{3}{1}$, and so on...

Thus, we can list $\mathbb{Q}^+$ as follows;

$\{1, \frac{1}{2}, 2, \frac{1}{3}, \frac{3}{2}, 3, \frac{1}{4}, \frac{2}{3}, \frac{5}{5}, 4, \frac{1}{5}, ...\}$

Thereby, the bijective mapping between (It does not preserve addition and multiplication) the set of $\mathbb{Q}$ and $\mathbb{N}$ can be;

$$\begin{aligned}
&0 \leftrightarrow 0 \\
&1 \leftrightarrow 1 \\
&-1 \leftrightarrow 2 \\
&\frac{1}{2} \leftrightarrow 3 \\
&-\frac{1}{2} \leftrightarrow 4 \\
&...
\end{aligned}$$

Thus, the set of $\mathbb{Q}$ is a countable. ♦

9.6.1 Dense Order

Theorem 9.15 (Introductory Theorem) *If $x \in \mathbb{Z}$, then there is not integer number between $n, n+1$.*

Proof Suppose that there is $m \in \mathbb{Z}$ between $n, n+1 \rightarrow n+1 < m < m$.

$\therefore \exists p \in \mathbb{Z}^+ \ni n = n + p$.

$\therefore n + 1 = m + p + 1$.

$\therefore m + p + 1 < m$,

$\therefore p + 1 < 0$, and this is contradiction.

$\therefore$ there is not an integer between $n, n + 1$. ♦

As a result of this introductory theorem, we realize that the order on $\mathbb{Z}$ is not dense as we introduce in the following definition.

Definition 9.13 Let $\leq$ be a partially ordered relation on the set A. $\leq$ said to be dense if and only if $((a, b \in A) \wedge (a < b)) \rightarrow (\exists c \in A \ni a < c < b)$(Roitman, 1990; Dasgupta, 2014; Schmidt, 2011).

Theorem 9.16 *If the algebric system $(A, +, \cdot, \leq)$ is an ordered field, then the relation $\leq$ is a dense.*

Proof $\because a < b$,

$\therefore 2a = a + a < a + b < b + b = 2b$.

$\because 2 = I_A + I_A > 0_A \rightarrow \frac{1}{2} > 0$.

$\therefore a < \frac{a+b}{2} < b$.

Now, put $c = \frac{a+b}{2} \rightarrow a < c < b, c \in A$.

$\therefore \quad \leq$ is a dense. ♦

Corollary *The ordering on the set $\mathbb{Q}$ in a dense, and there is not a rational number r between any two rational numbers p, q such that $p < r < q$ where $p < q$.*

Proof The proof is left to the reader. ♦

Corollary *Between any two elements in an ordered field there is an infinite family of the field elements. Thus, as a special case, between any two rational numbers there are infinite rational numbers.*

Although $\mathbb{Q}$ have the characteristic of density, but there are gaps in its ordering, as shown in the following theorem.

Theorem 9.17 *There is not $x \in \mathbb{Q}$ such that $x^2 = 2$.*

Proof Suppose that $\exists x \in \mathbb{Q} \ni x^2 = 2, x = \frac{a}{b}, 0 \neq b, a \in \mathbb{Z}$.

$\therefore a^2 = 2b^2$.

$\therefore a^2$ is an even number which leads to a an even number, and this is contradiction.

$\therefore a = 2k, k \in \mathbb{Z}^+$.

$\therefore a^+ = 4k^2$.

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

$\therefore b^2 = 2k^2$.

$\therefore b^2$ is an even number.

$\therefore b$ is an even number.

$\therefore b = 2l, l \in \mathbb{Z}$.

Now, we have $\frac{a}{b} = \frac{2k}{2l} = \frac{k}{l}$.

Thereby, we got $k \in \mathbb{Z} \ni x = \frac{k}{l}, k < a$, and this is contradiction.

$\nexists x \in \mathbb{Q} \ni x^2 = 2$.

Thus, $\mathbb{Q}$ does not contain the square root of 2. ♦

Definition 9.14 Let the algebraic system $(A, +, \cdot, \leq)$ be an ordered field. The ordered pair (X, Y) is said to be a cut in A, if each of $\phi \neq X, Y \subset A$ such that

(1) $X \cap Y \neq \phi$. (2) $X \cup Y = A$. (3) $(x \in X \wedge y \in Y) \rightarrow x < y$ (Rudin et al., 1976; Rudin, 1953; Dedekind, 1963; Dedekind, 1901; Mustafa et al., 1980).

Note: At the ordered pair of the cut (X, Y).

(1) X is called lower class.

(2) Y is called upper class.

(3) The cut is a gap if the lower class does not contain the maximum element of A, and the upper class does not contain the minimum element of A.

Example 9.9 Let $X = \{x | (x < 0) \cup (x^2 \leq 2)\} \subseteq \mathbb{Q}$,

$Y = \{x | (x > 0) \cup (x^2 > 2)\} \subseteq \mathbb{Q}$.

The ordered pair (X, Y) is a cut. More explicitly, it is a gap in $\mathbb{Q}$, since $\mathbb{Q}$ does not contains the square root of 2.

Example 9.10 Let $X = \{x | x \leq 2\} \subseteq \mathbb{Q}$,

$Y = \{x | x > 2\} \subseteq \mathbb{Q}$.

The ordered pair (X, Y) is a cut. It is not a gap in $\mathbb{Q}$ since the lower class X contains the maximum element 2.

9.6.2 Archimedean Order

There is an important and distinctive property of the ordered field $\mathbb{Q}$ which is for every positive element there is arbitrarily large integral multiples. We can abstract this property in the following definition.

Definition 9.15 The ordered field $(A, +, \cdot, \leq)$ is called Archimedean order if and only if $\forall a, b \in A, a \leq b, \exists n \in \mathbb{N} - \{0\} \ni na \geq b$ (Marvin, 2012; Kurosh, 2014; Alajbegovic and Mockor, 2012; Belegradek, 2002).

Theorem 9.18 *The ordered field* $(\mathbb{Q}, +, \cdot, \leq)$ *is Archimedean field.*

Proof Let $0 < x < y, \forall x, y \in \mathbb{Q}$.
$\therefore \exists p, q, r \in \mathbb{Z}$, such that $x = \frac{p}{r}, q = \frac{q}{r}$.
$\therefore 0 < \frac{p}{r} < \frac{q}{r}$.
Let $n = rq$.
Now we have $nx = rq \cdot \frac{p}{r} = pq \geq q \geq \frac{q}{r} = y$.
$\therefore nx \geq y$. ⧫

Note: In general if $(A, +, \cdot, \leq)$ is an ordered field which is not necessary be Archimedean field, as shown in the following example.

Example 9.11 Let $K = \left\{\sum_{-\infty}^{\infty} r_j x^j, r_j \in \mathbb{Q}, j \in \mathbb{Z}\right\}$ where if $j < 0$, then just a finite of coefficients $r_j \neq 0$.
Now, define $\oplus$ on K as follows:
$\sum_{-\infty}^{\infty} r_j x^j \oplus \sum_{-\infty}^{\infty} a_j x^j = \sum_{-\infty}^{\infty} (r_j + a_j) x^j$.
We define $\odot$ on K as follows;
$\sum_{-\infty}^{\infty} r_j x^j \odot \sum_{-\infty}^{\infty} a_j x^j = \sum_{p+q=j\infty} (r_p a_q) x^j$.
Finally, define the ordering on K as follows;
$\sum_{-\infty}^{\infty} r_j x^j < \sum_{-\infty}^{\infty} a_j x^j$.
Now, if $\exists k \in \mathbb{Z}^+$, such that $r_j = a_j, \forall j < k, r_k = a_k$, then the ordered field $(A, +, \cdot, \leq)$ is not Archimedean field.

9.7 Exercises

Solve the following problems:

Q1: If $0 \neq x, y \in \mathbb{Q}$ then prove that $\exists n \in \mathbb{N} - \{0\}$, such that $nx > y$.

Q2: Prove that $\nexists x \in \mathbb{Q} \ni x^2 = 6$.

Q3: Prove that $\nexists x \in \mathbb{Q} \ni x^3 = 4$.

Q4: Let $(A, +, \cdot, \leq)$ be an ordered field. What is a necessary and sufficient condition in order to $(A, +, \cdot, \leq)$ be Archimedean field?

Q5: Let $(A, +, \cdot, \leq)$ be a field, and $\leq$ be a partial ordered relation on A, and let it be a dense relation. Is it necessary $(A, +, \cdot, \leq)$ to be ordered field?

Q6: Consider the subset $D \subseteq \mathbb{Q}$ in which D bounded above. Is there least upper bound for the D?

Q7: Let $\mathbb{Q}[x]$ be a set of all polynomials $\sum_{i=0}^{n} a_i x^i$ where $n \in \mathbb{N}, a_i \in \mathbb{Q}$, and x is a variable.

(a) Define addition and multiplication operation on $\mathbb{Q}[x]$ in which $\mathbb{Q}[x]$ be an integral domain.

(b)Let $f(x) \in \mathbb{Q}[x], 0 \neq g(x) \in \mathbb{Q}[x]$. Prove that there are polynomials $t(x), r(x) \in \mathbb{Q}[x]$ in which $f(x) = t(x)g(x) + r(x)$ where $r(x) = 0$. Or, degree of $r(x)$ is less than degree of $g(x)$.

10

The Real Numbers

10.1 Introduction

This chapter deals with structuring the real numbers ($\mathbb{R}$) in the same methodology in which we have structured the $\mathbb{Q}$, in which ere we defined the $\mathbb{Q}$ as equivalence classes to the ordered pairs of the $\mathbb{Z}$. The chapter begins with defining the equivalence relations on the set of all basic sequences. So the $\mathbb{R}$ is the equivalence class of a basic rational sequence.

We will define the following operations; addition, multiplication, and ordering on the set of $\mathbb{R}$ so that the set becomes an ordered field and is an expansion to the ordered field of the $\mathbb{Q}$. Thereby, the ordering of the elements on the set $\mathbb{R}$ is free of gaps, and this means that each sequence of real numbers has a limit in $\mathbb{R}$.

This chapter attempts to prove the gaps in $\mathbb{Q}$ are quite narrow and can be approximated by $\mathbb{Q}$ sequences. More precisely, the process of expanding from the $\mathbb{Q}$ into the $\mathbb{Q}$ came to fill each gap of $\mathbb{Q}$ with equivalence classes of sequences that almost fill the gaps, so that we can find the solution to the equation $x^2 - 2 = 0$ in the set $\mathbb{R}$.

10.2 Construction of $\mathbb{R}$

Definition 10.1 The mapping $F : \mathbb{N} \to A$ is called a sequence in A. If $F(n) = a_n, \forall n \in \mathbb{N}$, then we will expressed it by (a_n) to denote the mapping of F (Gaughan, 2009a; Saff and Snider, 1993).

Example 10.1 Let $A = \mathbb{Z}$, and define the mapping $F : \mathbb{N} \to \mathbb{Z}$ where $F(n) = 3n^2$. Then:

$F(1) = 3(1^2) = 3,$
$F(2) = 3(2^2) = 12,$
$F(3) = 3(3^2) = 27,$
$F(4) = 3(4^2) = 48,$
.,
.,
.,
$F(n) = 3n^2,$
.,
.,
.,
Thus, $\{F_a\} = \{3, 12, 27, 48, ..., 3n^2, ...\}$.

Example 10.2 Let $A = \mathbb{R}$, and define the mapping $F : \mathbb{N} \to \mathbb{R}$ where $F(n) = \sqrt{n^3}$. Then:

$F(1) = \sqrt{1^3} = 1,$
$F(2) = \sqrt{2^3} = \sqrt{8},$
$F(3) = \sqrt{3^3} = \sqrt{27},$
$F(4) = \sqrt{4^3} = \sqrt{64},$
.,
.,
.,
$F(n) = \sqrt{n^3},$
.,
.,
.,
Thus, $\{F_a\} = \left\{1, \sqrt{8}, \sqrt{27}, \sqrt{64}, ..., \sqrt{n^3}, ...\right\}$.

Theorem 10.1 *If the ordered pair (X, Y) is a gap in the set $\mathbb{Q}$ then there is a sequences $(x_n), (y_n)$ in $\mathbb{Q}$ where for all $n \in \mathbb{N}, x_n \in X, y_n \in Y$ such that $y_n - x_n = \frac{1}{n}$.*

Moreover, in $\mathbb{Q}$, the following inequalities are satisfied;

$|x_m - x_n| < \frac{1}{n}, |y_m - y_n| < \frac{1}{n}, \forall n \in \mathbb{N} - \{0\}$.

Proof $\because (X, Y)$ is a cut

$\therefore (X \neq 0, Y \neq 0) \wedge (x \in X \wedge y \in Y) \rightarrow y - x > 0$.

Now, $\forall n \in \mathbb{N} - \{0\}, 0 < \frac{1}{n} \in \mathbb{Q}$,

$\exists k_n \in \mathbb{N} - \{0\} \ni k_n \cdot \frac{1}{n} \geq y - x$ (Based on Archimedean property in $\mathbb{Q}$).

$\because x + \frac{k_n}{n} \geq y$,

$\therefore x + \frac{k_n}{n} \in Y$.

Thereby, $\forall n \in \mathbb{N} - \{0\}$, the set $M_n = \left\{m \in \mathbb{N} | x + \frac{m}{n} \in Y\right\} \neq \phi$.

$\because M_n \subseteq \mathbb{N}$,

$\therefore M_n$ contains of the first element m_n.

For instant $n \in \mathbb{N} - \{0\}$,

$x_n = x + \frac{m_n - 1}{n} \in X, y_n = x + \frac{m_n}{n} \in Y, y_n - x_n = \frac{1}{n}$.

$\because (X, Y) \in \mathbb{Q}$ is a cut,

$\therefore x_n < y_n, \forall m, n \in \mathbb{N} - \{0\}$.

$\therefore x_n < y_m = x_m + \frac{1}{n}, x_m < y_n = x_n + \frac{1}{n}, \forall m, n \in \mathbb{N} - \{0\}$.

$\therefore$ $(\forall n \in \mathbb{N} - \{0\}) \wedge ((m \leq n) \in \mathbb{N})$, the absolute value of the following term being:

$|x_m - x_n| = max\left\{x_m - x_n, x_m - x_n\right\} < max\left\{\frac{1}{n}, \frac{1}{m}\right\} = \frac{1}{n}$.

In the same way, we can prove that the $|y_m - y_n| < \frac{1}{n}$. ♦

Definition 10.2 Consider an ordered field $(A, +, \cdot, \leq)$. The sequence (a_n) is said to be bounded if there exists $a \in A$ such that $|a_n| < a$ in $A, \forall n \in \mathbb{N}$ (Gaughan, 2009a; Saff and Snider, 1993; Thomas et al., 2010; Hass et al., 2019).

Example 10.3 Let $(\mathbb{Q}, +, \cdot, \leq)$ be an ordered field. The sequence (a_n) where $a_n = \frac{1}{n}, \forall n \in \mathbb{N} - \{0\}$ is bounded because $|a_n| = |\frac{1}{n}| < 2 \in \mathbb{Q}$. The sequence $(b_n), b_n = n^3, n \in \mathbb{N}$ is unbounded sequence because $\nexists b \in \mathbb{Q} \ni b_n < b, \forall n \in \mathbb{Q}$.

10.2.1 Fundamental Sequences

Definition 10.3 Let $(A, +, \cdot, \leq)$ be an ordered field. The sequence (a_n) in A is a fundamental (Cauchy) sequence if and only if $0 < \forall\epsilon \in A, \exists n_\epsilon \in \mathbb{N} \ni |a_n - a_m| < \epsilon, \forall m, n \geq n_\epsilon$(Lang, 2002a; Lang, 1993a; Lang, 1993b).

Example 10.4 (1) All convergent sequences to the gap in Theorem 10.1 are Cauchy sequences.

(2) Divergent sequences to the gap in the theorem are not Cauchy sequences. For example $(a_n), a_n = n^3$ is not fundamental sequence.

Theorem 10.2 *If $(A, +, \cdot, \leq)$ be an ordered field then all fundamental sequences (a_n) in A are bounded.*

Proof Let $0 < \epsilon \in A$.

$\therefore \exists n_\epsilon \in \mathbb{N} \ni |a_n - a_m| < \epsilon, \ \forall m, n \geq n_\epsilon$.

Now, let $D = \{|a_1|, |a_2|, ..., |a_{n_\epsilon}|\} \subseteq A$.

It should be noted that D contains of maximum element which is denoted it by b.

$\therefore |a_n| \leq b < b + \epsilon, \ \forall n \leq n_\epsilon$.

Also, $|a_n| = |a_n - a_{n_\epsilon} + a_{n_\epsilon}| \leq |a_n + a_{n_\epsilon}| + |a_{n_\epsilon}|$.

$\therefore \forall n > n_\epsilon \Rightarrow |a_n| \leq \epsilon + |a_n| \leq \epsilon + b$.

$\therefore \forall n \in \mathbb{N} \Rightarrow |a_n| \leq \epsilon + b$.

$\therefore (a_n)$ is bounded. ⧫

Example 10.5 The sequence $(a_n)|a_n = \begin{cases} 1, n \text{ is even} \\ -1, n \text{ is odd} \end{cases}$.

a_n is a sequence in $\mathbb{Q}$, but it is not Cauchy sequence.

Theorem 10.3 *Let $(A, +, \cdot, \leq)$ be an ordered field, and if each of $(a_n), (b_n)$ be sequences in A, then*

(a) $(a_n + b_n)$ is a sequence in A.

(b) $(a_n b_n)$ is a sequence in A.

Proof (a) It is left as an exercise to the reader.

(b) $\because (a_n), (b_n)$ are fundamental sequences,

$\therefore (a_n), (b_n)$ are bonded based on Theorem 10.2.

$\therefore \exists a, b \in A \ni |a_n| < a, |b_n| < b$

Now, let $\forall n \in \mathbb{N}$, and let $0 < \epsilon \in A$.

$\therefore 0 < \frac{\epsilon}{2a} \in A, 0 < \frac{\epsilon}{2b} \in A$.

Thereby, $\exists n'_\epsilon, n''_\epsilon \ni |a_n - a_m| < \frac{\epsilon}{2b}, \forall m, n \geq n'_\epsilon, |b_n - b_m| < \frac{\epsilon}{2a}, \forall m, n \geq n''_\epsilon$.

Now, let us put $n_\epsilon = max\,\{n'_\epsilon, n''_\epsilon\}$.

$\therefore |a_nb_n - a_mb_m| = |a_nb_n - a_nb_m + a_nb_m - a_mb_m| = |a_nb_n - a_nb_m| + |a_nb_m - a_mb_m| = |a_n||b_n - b_m| + |b_m||a_n - a_m| < a \cdot \frac{\epsilon}{2a} + b \cdot \frac{\epsilon}{2b} = \epsilon, \forall m, n \geq n_\epsilon$.

Thus, (a_nb_n) is a Cauchy sequence in A. ♦

Definition 10.4 Let $(A, +, \cdot, \leq)$ be an ordered field. The sequence (a_n) is called converges to $a \in A$ if and only if $\forall 0 < \epsilon \in A, \exists n_\epsilon \ni |a_n - a| < \epsilon$. a is a limit for (a_n) in A (D'angelo and West, 1997; Jeffreys et al., 1999; Weisstein et al., 2004).

Note: If the sequence is not convergent, then it is divergent.

Example 10.6 The sequence $(\frac{1}{n^2}) \in \mathbb{Q} \to 0$.

Because $0 < \epsilon \in \mathbb{Q}, \exists n_\epsilon = [\frac{2}{\sqrt{\epsilon}}] \in \mathbb{N}$.

$\therefore \forall n > [\frac{2}{\sqrt{\epsilon}}]$ where $[x]$ is a greatest integer number.

$\because (n^2) \in \mathbb{Q}$ is not converges to $a \in \mathbb{Q}$(Say).

$\because \forall n_\epsilon \in \mathbb{N}, \nexists 0 < \epsilon \in \mathbb{Q} \ni |n^2 - a| \geq \epsilon, \forall n \geq n_\epsilon$.

$\therefore (n^2) \in \mathbb{Q} \nrightarrow a \in \mathbb{Q}$.

$\therefore (n^2)$ is divergent.

$\therefore (\frac{1}{n^2}) \to 0$.

Theorem 10.4 *The sequence (a_n) in the ordered field A has at most one limit in A.*

Proof Suppose that each of a', a" is a limit in A for the (A_n).

Let $0 < \epsilon \in A$.

$\therefore \forall 0 < \frac{\epsilon}{2}, \exists n'_\epsilon, n"_\epsilon \ni (|a_n - a'| < \frac{\epsilon}{2}, \forall n \geq n'_\epsilon) \wedge (|a_n - a"| < \frac{\epsilon}{2}, \forall n \geq n"_\epsilon)$.

Now, let us put $n_\epsilon = max\,\{n'_\epsilon, n"_\epsilon\}$.

$\therefore |a' - a"| = |a' - a_n + a_n - a"| \leq |a' - a_n| + |a_n - a"|$.

$\therefore |a' - a"| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon, \forall n \geq n_\epsilon$.

$\therefore 0 \leq |a' - a"| < \epsilon, \forall \epsilon > 0$.

$\therefore a' - a" = 0 \Rightarrow a' = a"$. ♦

Notation: For convenience, we use the symbol $L(a_n)$ for a convergent sequence (a_n) in the ordered field A.

Theorem 10.5 *Let A be an ordered field. If (a_n) is a convergent sequence in A, then it is a Cauchy sequence.*

Proof Let $a = L(a_n), 0 < \epsilon \in A$.

$\therefore \exists n_\epsilon \in \mathbb{N} \ni |a_n - a_m| < \frac{apsilon}{2}, \forall n \geq n_\epsilon$.

$\therefore |a_n - a_m| + |a_n - a + a - a_m|$

$\leq |a_n - a| + |a - a_m| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon, \forall m, n \geq n_\epsilon$.

$\therefore (a_n)$ is Cauchy sequence. ♦

Corollary *If (a_n) is a convergent sequence in the ordered field then it is a bounded.*

Proof $\because (a_n)$ is a convergent sequence,

$\therefore (a_n)$ is a fundamental sequence (Theorem 10.5).

$\because (a_n)$ is a fundamental sequence,

$\therefore (a_n)$ is a bounded (Theorem 10.2). ♦

Theorem 10.6 *If (a_n) be a sequence in the ordered field $A \ni |a_n| \leq b, \forall n \in \mathbb{N} \wedge L(a_n) = a$, then $|a| \leq b, \forall b \in A$.*

Proof We will prove the theorem by contradiction.

Let $|a| > b$.

$\therefore |a| = b + \epsilon, \epsilon > 0$.

$\because L(a_n) = a$,

$\therefore \exists n_\epsilon \in \mathbb{N} \ni |a_n - a| < \frac{\epsilon}{2}, \forall n > n_\epsilon$.

$\because (|a| - |a_n| \leq |a_n - a|) \wedge (b + \epsilon - b \leq |a| - |a_n|)$,

$\therefore \epsilon = b + \epsilon - b \leq |a_n - a|$.

$\therefore \epsilon \leq |a_n - a| < \frac{\epsilon}{2}$. And this is contradiction.

$\therefore |a| \leq b.$ ♦

Theorem 10.7 *If A be an ordered field, and $L(a_n) = a, L(b_n) = b$, then*

(a) $L(a_n + b_n) = a + b$.

(b) $L(a_n b_n) = ab$.

Proof Suppose that $0 < \epsilon \in A$,

$\therefore \exists n'_\epsilon, n"_\epsilon \in \mathbb{N}$

$\ni |a_n - a| < \frac{\epsilon}{2} \forall n \geq n'_\epsilon,$

$|b_n - b| < \frac{\epsilon}{2} \forall n \geq n"_\epsilon.$

Let us put $n_\epsilon = max\,\{n'_\epsilon, n"_\epsilon\}$.

$\therefore |(a_n + b_n) - (a + b)| \leq |a_n - a| + |b_n - b| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon, \forall n \geq n_\epsilon.$

$\therefore L(a_n + b_n) = a + b.$

$\because$ $(a_n), (b_n)$ are convergent sequences, thereby they are bonded sequences.

$\therefore \exists a', b' \in A \ni |a_n| < a' \wedge |b_n| < b', \forall n \in \mathbb{N}.$

Let us put $c = max\,\{a', b'\}$,

$\therefore \frac{\epsilon}{2c} > 0.$

Now, based on the hypothesis

$\exists \dot{n}_\epsilon, \ddot{n}_\epsilon \in \mathbb{N} \ni |a_n - a| < \frac{\epsilon}{2c}, n \geq \dot{n}_\epsilon \wedge |b_n - b| < \frac{\epsilon}{2c}, n \geq \ddot{n}_\epsilon.$

Let us put $\check{n}_\epsilon = max\,\{\dot{n}_\epsilon, \ddot{n}_\epsilon\}$.

Thereby, based on Theorem 10.6, we have

$|a_n b_n - ab| = |a_n b_n - a_n b + a_n b - ab|$

$\leq |a_n b_n - a_n b| + |a_n b - ab|$

$= |a_n||b_n - b| + |b||a_n - a|.$

$\therefore |a_n b_n - ab| < a' \cdot \frac{\epsilon}{2c} + b' \cdot \frac{\epsilon}{2c}$

$\leq c \cdot \frac{\epsilon}{2c} + c \cdot \frac{\epsilon}{2c} = \epsilon, \forall n \geq \check{n}_\epsilon.$

$\therefore L(a_n b_n) = ab.$ ♦

Note: Let A be an ordered field then

(1) $L(a_n) = a \rightarrow L(|a_n|) = |a|, \forall a \in A.$

(2) $L(|a_n|) = 0 \rightarrow L(a_n) = 0.$

Theorem 10.8 *There is a divergent fundamental sequence in $\mathbb{Q}$.*

Proof Let $X = \{x \in \mathbb{Q} | x < 0 \vee x^2 < 2\}$,
$Y = \{x \in \mathbb{Q} | x > 0 \vee x^2 > 2\}$.

Based on Theorem 10.1, the ordered pair (X, Y) is a gap because $\sqrt{2} \notin \mathbb{Q}$.

There exists a sequences $(x_n), (y_n) \ni x_n \in X, y_n \in Y$, and $y \in Y$ such that

$y_n - x_n = \frac{1}{n}$,
$y_n = x_n + \frac{1}{n} < y + 1, \forall n \in \mathbb{N} - \{0\}$.
It should be noted that $|x_m - x_n| < \frac{1}{n}, \forall m \geq n$.
$\because L(\frac{1}{n}) = 0$,
$\therefore (x_n)$ is a Cauchy in $\mathbb{Q}$.
$\because (x_n)$ does not converge in $\mathbb{Q}$.
If $L(x_n) = a \in \mathbb{Q}$, then $L(x_n^2) = a^2$
$\therefore \forall n \in \mathbb{N} - \{0\}$, we have
$0 < 2 - x_n^2 < y_n^2 - x_n^2 = (y_n - x_n)(y_n + x_n)$.
$\because y_n - x_n = \frac{1}{n}$,
$\therefore y_n + x_n < y_n + y_n = 2y_n$.
$\therefore 0 < 2 - x_n^2 < \frac{2y_n}{n} < 2\frac{y+1}{n}$.
Also, $L(\frac{1}{n}) = 0$ in $\mathbb{Q}$.
$\therefore L(x_n^2) = 2$.
Now, based on the uniqueness of the limit, we have
$a^2 = L(x_n^2) = 2 \to a^2 = 2, \forall a \in \mathbb{Q}$, and this is impossible.
$\therefore (x_n)$ is a disonvergent fundamental sequence in $\mathbb{Q}$. ♦

10.2.2 Positive Sequences

Definition 10.5 The sequence (a_n) in the ordered field A is called positive sequence if and only if $\exists\ 0 < \epsilon \in A, k \in \mathbb{N} \ni a_n \geq \epsilon, \forall n \geq k$ (Landau, 1987; Gaughan, 2009a; Saff and Snider, 1993).

Example 10.7 (1) The sequence $\frac{1}{n} \in \mathbb{Q}$ is not positive because $\forall 0 < \epsilon \in A, \exists k \in \mathbb{N} \ni \frac{1}{n} < \epsilon$.

(2) The sequence $n^2 \in \mathbb{Q}$ is a positive because $\forall \epsilon = 1, k = 1 \ni n^2 > 1, \forall n \geq 1$.

Theorem 10.9 *For all fundamental sequence (a_n) in the ordered field A, one of the following statements is true*

(1) $L(a_n) = 0$.
(2) (a_n) *is positive.*
(3) $-(a_n)$ *is positive.*

Proof Suppose that $L(a_n) \neq 0$.
$\therefore 0 < \epsilon \in A, \exists k \geq n \in \mathbb{N} \ni |a_k| \geq \epsilon ...(1)$.
$\because \frac{0<\epsilon}{2} \in A$, (a_n) is a fundamental sequence
$\therefore \exists n_\epsilon \in \mathbb{N} \ni |a_n - a_m| < \frac{\epsilon}{2}, \forall m, n \geq n_\epsilon$.
Now, by utilizing (1), and putting $m = n_\epsilon$, we get
$max\,\{a_k, -a_k\} = |a_k| \geq \epsilon, k \geq n_\epsilon$.
Also, if $a_k \geq \epsilon$, we conclude that
$a_n = a_k - (a_k - a_n) \geq \epsilon - |a_k - a_n| > \frac{\epsilon}{2}$.
$\therefore (a_n)$ is a positive.
While, if $-a_k \geq n_\epsilon$, we have
$-a_n = -a_k - (a_k - a_n) \geq \epsilon - |a_k - a_n| > \frac{\epsilon}{2}$.
$\therefore -(a_n)$ is a positive.
Thereby, we have proved that one of (1), (2), and (3) is true.

Now, we have to prove that no more than one of the statements might be true.

Suppose that $L(a_n) = 0$.
$\therefore 0 < \forall\epsilon \in A, \exists n_\epsilon \in \mathbb{N} \ni max\,\{a_n, -a_n\} = |a_n| < \epsilon, \forall n \geq n_\epsilon$.

$$\nexists 0 < \epsilon \in A, \forall k \in \mathbb{N} \ni \begin{cases} a_n \geq \epsilon, \forall n \geq k \\ \qquad\vee \\ -a_n \geq \epsilon, \forall n \geq k \end{cases}$$

$\therefore$ if the statement (1) is true, then each of the statement (2) and (3) are false.

Now, suppose that one of the statements (2) and (3) is true.

$$\therefore \exists 0 < \epsilon' \in A \wedge 0 < \epsilon" \in A, k', k" \in \mathbb{N} \ni \begin{cases} a_n \geq \epsilon, \forall n \geq k' \\ \qquad\wedge \\ -a_n \geq \epsilon, \forall n \geq k" \end{cases}$$

Let us put $n = max\,\{k', k"\}$.
$\therefore 0 < \epsilon' \leq -a_n \leq -\epsilon' < 0$. This is impossible.
Thus, just one on the statements (1), (2) and (3) is true. ♦

Notation: The symbol $F_{\mathbb{Q}}$ is denoted to the rational fundamental sequences.

Theorem 10.10 *There is the equivalence relation T in $F_{\mathbb{Q}}$, such that $(x_n)T(y_n) \leftrightarrow L(x_{-}y_n) = 0$.*

Proof (1) T is reflexive.
$\because L(x_n - x_n) = L(0) = 0, \forall (x_n) \in F_{\mathbb{Q}}$.
$\therefore (x_n)T(x_n)$.
$\therefore T$ is reflexive.
(2) T is symmetric.
If $L(x_n - y_n) = 0$, then $L(-(x_n - y_n)) = L(y_n - x_n) = 0$.
$\therefore (x_n)T(y_n) \to (y_n)T(x_n), \forall (x_n), (y_n) \in F_{\mathbb{Q}}$.
$\therefore T$ is symmetric.
(3) T is transitive.
If $L(x_n - y_n) = 0 \wedge L(y_n - z_n) = 0 \to L(x_n - z_n)$
$= L(x_n - y_n + y_n - z_n)$
$= L(x_n - y_n) + L(y_n - z_n)$
$) + 0 = 0$.
$\therefore T$ is transitive.
From (1), (2), and (3), T is the equivalence relation in $F_{\mathbb{Q}}$. ♦

Notation:
(1)If $(x_n), (y_n) \in T$, then $(x_n) \sim (y_n)$.
(2) We denote to the equivalence class contains of (x_n) by the symbol $[(x_n)]$.

Definition 10.6 Let $(x_n) \in F_{\mathbb{Q}}$, and T be equivalence relation on $F_{\mathbb{Q}}$. The real number is the equivalence class $[(x_n)]$ with respect to the equivalence relation T(Mustafa et al., 1980; Gaughan, 2009a; Saff and Snider, 1993).

Example 10.8 (1) Let $x_n = \frac{1}{n}$, then $(x_n) \sim (0)$.
$\therefore [(x_n)] = [(0)]$.
Thereby, the equivalence class $[(0)]$ is the zero real number.
(2) Let $y_n = 1 + \frac{1}{n}$, then $(y_n) \sim (1)$.
$\therefore [(y_n)] = [(1)]$.
Thereby, the equivalence class $[(1)]$ is the real number one.
(3) Let $a_1 = 1$,

$a_{n+1} = a_n + \frac{b_n}{10^n}, \forall n \in \mathbb{N}, b_n \in \mathbb{Z}^+ \cup \{0\}$, where $(a_n + \frac{b_n}{10^n})^2 < 2 < (a_n \frac{b_{n+1}}{10^n})^2$.

$\therefore [(a_n)] = [(\sqrt{2})]$.

10.2.3 Addition and Multiplication of $\mathbb{R}$

In this section, we will define the addition operation $+_{\mathbb{R}}$, and multiplication operation $\cdot_{\mathbb{R}}$ on $\mathbb{R}$. So that the system $(\mathbb{R}, +_{\mathbb{R}}, \cdot_{\mathbb{R}})$ becomes a field.

Theorem 10.11 (Introductory Theorem)

If $(x_n), (y_n), (x'_n), (y'_n) \in F_{\mathbb{Q}}$, where: $(x_n) \sim (x'_n)$, $(y_n) \sim (y'_n)$, then:
(1) $(x_n + y_n) \sim (x'_n + y'_n)$.
(2) $(x_n y_n) \sim (x'_n y'_n)$.

Proof (1) It is left as an exercise for the reader.

(2) $\because (x_n), (y'_n) \in F_{\mathbb{Q}}, a, b \in \mathbb{Q}$,
$\therefore |x_n| < a, |y'_n| < b, \forall n \in \mathbb{N}$ (Every Cauchy sequence is bounded).

According Theorem 10.3, we conclude that the sequences $(x_n y_n), (x'_n y"_n)$ are fundamental sequences in $\mathbb{Q}$.

$\because (x_n) \sim (x'_n), (y_n) \sim (y'_n)$,
$\therefore \forall 0 < \epsilon \in \mathbb{Q}, \exists n'_\epsilon \in \mathbb{N}, n"_\epsilon \in \mathbb{N} \ni$:
$|x_n - x'_n| < \frac{\epsilon}{2b}, \forall n \geq n'$,
$|y_n - y'_n| < \frac{\epsilon}{2a}, \forall n \geq n"$.
$\therefore |x_n y_n - x'_n y'_n| \leq |x_n||y_n - y'_n| + |y'_n||x_n - x'_n|$
$< a \cdot \frac{\epsilon}{2a} + b \cdot \frac{\epsilon}{2b} = \epsilon, \forall n \geq n_\epsilon = max\,\{n'_\epsilon, n"_\epsilon\}$.
$\therefore L(x_n y_n - x'_n y'_n) = 0$.
$\therefore (x_n y_n) \sim (x'_n y'_n)$. ♦

Theorem 10.12 *There are two binary operations F, G in $\mathbb{R}$ such that if $(x_n) \in r_1, (y_n) \in r_2$, then $\forall r_1, r_2 \in \mathbb{R}$*
(1) $F(r_1, r_2) = (x_n + y_n)$.
(2) $G(r_1, r_2) = (x_n y_n)$.

Proof Let us define the sets below as:

$F = \{((r_1, r_2), (x_n + y_n)) : (x_n) \in r_1, (y_n) \in r_2; r_1, r_2 \in \mathbb{R}\}$.

$G = \{((r_1, r_2), (x_n y_n)) : (x_n) \in r_1, (y_n) \in r_2; r_1, r_2 \in \mathbb{R}\}$.

Each of F, G are subset of $(\mathbb{R} \times \mathbb{R}) \times \mathbb{R}$.

If $(r_1, r_2) \in \mathbb{R} \times \mathbb{R}$, then

$r_1 = (x_n), r_2 = (y_n) \ni (x_n), (y_n) \in F_{\mathbb{Q}}$.

$\because (x_n + y_n) \in F_{\mathbb{Q}}$,

$\therefore$ the ordered pair $(x_n+y_n) \in F_{\mathbb{Q}}$, $((r_1, r_2), w) \in F \ni w = (x_n+y_n)$.

$\therefore domF = \mathbb{R} \times \mathbb{R}$.

Now, suppose that $((r_1, r_2), w') \in F$.

$\therefore w' = [(x'_n + y'_n)], x'_n \in r_1, y'_n \in r_2$.

But according to Theorem 10.11,

$[(x'_n) \sim (x_n) \wedge (y'_n) \sim (y_n)] \rightarrow (x'_n + y'_n) \sim (x_n + y_n)$.

$\therefore w = w'$.

$\therefore F$ is a functional relation.

$\therefore F : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ is a mapping.

$\therefore F$ is a binary operation on $\mathbb{R}$.

Through the same method, we can prove that G is a binary operation on $\mathbb{R}$. ⧫

Note: The addition operation (F), and multiplication operation (G) on $\mathbb{R}$ can be written

$r_1 +_{\mathbb{R}} r_2$ instate of $F(r_1, r_d)$. $r_1 \cdot_{\mathbb{R}} r_2$ instate of $G(r_1, r_d)$. Can be expressed as $r_1 + r_2, r_1 r_d$ for convenience.

Example 10.9 If $r_1 = [(0)], r_2 = [(\frac{3n+1}{n})] = [(3)], n \in \mathbb{N}$, then

$r_1 + r_2 = [(0 + 3)] = [(3)]$.

$r_1 r_2 = [(0 \cdot 3)] = [(0)]$.

Theorem 10.13 (Introductory Theorem) *If* $(x_n) \in F_{\mathbb{Q}} \ni [(x_n)] \neq [(0)]$, *then* $\exists (y_n) \in F_{\mathbb{Q}} \ni [(x_n)][(y_n)] = [(1)]$.

Proof $\because L(x_n) \neq 0$,

$\therefore \exists 0 < \bar{\epsilon} \in \mathbb{Q} \ni \forall n \in \mathbb{N}, \exists k \geq n \ni |x_k| \geq \bar{\epsilon}$.

$\because (x_n)$ is a fundamental sequence,

$\therefore \exists \bar{n} \in \mathbb{N} \ni |x_m - x_n| \leq \frac{\bar{\epsilon}}{2}, \forall m, n \geq \bar{n}$.

Currently, $\forall \bar{n} \in \mathbb{N}, \exists \bar{k} > \bar{n} \ni |x_{\bar{k}}| \geq \bar{\epsilon}$.

$\therefore |x_n| = |x_{\bar{k}} - (x_{\bar{k}} - x_n)| > |x_{\bar{k}}| - |x_{\bar{k}} - x_n| > \bar{\epsilon} - \frac{\bar{\epsilon}}{2} = \frac{\bar{\epsilon}}{2}, \forall n \geq \bar{n}.$
$\therefore x_n \neq 0, \forall n \geq \bar{n}.$
Now, let us suppose that $y_n = \begin{cases} 1; \forall n < \bar{n} \\ \frac{1}{x_n}; \forall n \geq \bar{n} \end{cases}$
Thereby, y_n is a fractional sequence.
Let $0 < \epsilon \in \mathbb{Q}, \exists n_\epsilon \in \mathbb{N} \ni |x_m - x_n| < \frac{\epsilon^{-2}\epsilon}{4}, \forall m, n \geq n_\epsilon.$
$\therefore |y_m - y_n| = |\frac{1}{x_m} - \frac{1}{x_n}| = |\frac{x_n - x_m}{x_m x_n}| = \frac{|x_m - x_n|}{|x_m||x_n|}$
$< \frac{\epsilon^{-2}\epsilon}{4} \cdot \frac{2}{\bar{\epsilon}} \cdot \frac{2}{\bar{\epsilon}} = \epsilon, \forall m, n \geq max\,\{\bar{n}, n\}.$
$\therefore y_n$ is a fundamental sequence in $\mathbb{Q}$.
Also, and since $x_n y_n = 1, \forall n \geq \bar{n}$, hence $L(x_n y_n) = 1$.
$\therefore (x_n y_n) \sim (1).$
$\therefore [(x_n)][(y_n)] = [(x_n y_n)] = [(1)].$ ♦

Theorem 10.14 *The mathematical system* $(\mathbb{R}, +, \cdot)$ *is a field.*

Proof (1) $(\mathbb{R}, +)$ is a commutative group.
The system $(\mathbb{R}, +)$ has associative property.
$r_1 + (r_2 + r_3) = (r_1 + r_2) + r_3, \forall r_1, r_2, r_3 \in \mathbb{R}.$
Also, $[(0)]$ is the additive identity in which
$[(0)] + [(x_n)] = [(0 + x_n)] = [(x_n)], \forall x_n \in \mathbb{R}.$
Now, let $r = [(x_n)] \in \mathbb{R}$.
$\because [(x_n)] \in \mathbb{R}, \exists [(-x_n)] \in \mathbb{R} \ni [(x_n)] + [-(x_n)] = [(x_n) - (x_n)] = [(0)].$
$\therefore -[(x_n)] = [(-x_n)]$ is the additive inverse of $[(x_n)]$.
Moreover, $r_1 + r_2 = r_2 + r_1, \forall r_1, r_2 \in \mathbb{R}.$
(2) The mathematical system $(\mathbb{R} - [(0)], \cdot)$ is a commutative group.
The system $(\mathbb{R} - [(0)], \cdot)$ has associative property.
$r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3, \forall r_1, r_2, r_3 \in \mathbb{R}.$
Also, $[(1)]$ is a multiplicative identity in which
$[(1)] \cdot [(x_n)] = [(1) \cdot (x_n)] = [(x_n)], \forall [(x_n)] \in \mathbb{R}.$
Now, let $r = [(x_n)] \in \mathbb{R} - [(0)]$.
$\therefore [(x_n)] \neq [(0)].$
Thereby, according to Theorem 10.13
$\exists y_n \in F_{\mathbb{Q}} \ni [(x_n)] \cdot [(y_n)] = [(1)].$
$\therefore [(x_n)]^{-1} = [(y_n)].$
$\therefore [(y_n)]$ is the multiplicative inverse of $[(x_n)]$.

Moreover, the system has a commutative property with respect to multiplication.

$r_1 \cdot r_2 = r_2 \cdot r_1, \forall r_1, r_2 \in \mathbb{R}$.

(3) Distributive law.

$r_1 \cdot (r_2 + r_3) = (r_1 \cdot r_2) + (r_1 \cdot r_3) \forall r_1, r_2, r_3 \in \mathbb{R}$.

Also $(r_1 + r_2) \cdot r_3 = (r_1 \cdot r_3) + (r_2 \cdot r_3) \forall r_1, r_2, r_3 \in \mathbb{R}$.

Thus, from (1), (2) & (3) the mathematical system $(\mathbb{R}, +, \cdot)$ is a field. ⧫

Notation: (1) We express $0_{\mathbb{R}}$ in stead of $[(0)]$, and for convenient, we write 0.

(2) We express $1_{\mathbb{R}}$ in stead of $[(1)]$, and for convenient, we write 1.

10.3 Exercises

Solve the following questions:

Q1: Give an example of a bounded but not fundamental sequence.

Q2: Give an example of A that has no singularity limit.

Q3: If A be Archimedean field then $L(\frac{1}{n}) = 0$, and $L(\frac{1}{p^n}) = 0, \forall 0, p \neq 1 \in \mathbb{N}$.

Q4: Give an example of a fundamental but Divergent sequence.

Q5: If a_n is a fundamental sequence in the field A such that $L(a_n) = 0$, then $(|a_n|)$ is a positive fundamental sequence.

Q6: If $(a_n), (b_n)$ are positive fundamental sequences in the ordered field A, then $(a_n + b_n), (a_n b_n)$ are positive sequences in A.

Q7: Let A, B be ordered fields, and $F : A \to B$ be a bijective mapping such that preserves on addition, multiplication, and ordering. Prove that

(1) (a_n) is a fundamental sequence in A if and only if $(F(a_n))$ is a fundamental sequence in B.

(2) $L(a_n) = a$ if and only if $L(F(a_n)) = F(a)$.

(3) (a_n) is a positive sequence in A if and only if $(F(a_n))$ is a positive sequence in B.

Q8: Let (x_n) be a convergent sequence in the ordered field A. Prove that (x_n) is a positive sequence in A if and only if $L(x_n) > 0$ in A.

10.4 Order on $\mathbb{R}$

Definition 10.7 The set of all equivalence classes belonging to the positive sequences in $F_{\mathbb{Q}}$ is called positive real numbers, and denoted $\mathbb{R}$. Mathematically, $\mathbb{R}^+ = \{r|(x_n) \text{ is a positive}, (x_n) \in r\}$(Temirovna, 2021; Dijksterhuis, 1961; Kist and Leestma, 1970).

Theorem 10.15 *Let* $(x_n), (x'_n) \in F_{\mathbb{Q}}$. *If* $(x_n) \sim (x'_n)$, (x_n) *is a positive sequence, then* (x'_n) *is a positive sequence.*

Proof $\because (x_n)$ is a positive sequence
$\therefore \exists 0 < \epsilon \in \mathbb{Q}, n_\epsilon \in \mathbb{N} \ni x_n \geq \epsilon, \forall n \geq n_\epsilon.$
$\because (x_n) \sim (x'_n),$
$\therefore L(x_n - x'_n) = 0.$
$\therefore \exists n'_\epsilon \in \mathbb{N} \ni |x_n - x'_n| < \frac{\epsilon}{2}, \forall n \geq x'_n.$
$\therefore -\frac{\epsilon}{2} < x'_n - x_n < \frac{\epsilon}{2}, \forall n \geq n'.$
Now, let $\bar{n}_\epsilon = max\,\{n_\epsilon, n'_\epsilon\},$
$\therefore n'_n = (n'_n - x_n) + x_n > -\frac{\epsilon}{2} + \frac{\epsilon}{2} > 0, \forall n \geq \bar{n}.$
$\therefore (x'_n)$ is a positive sequence in $\mathbb{Q}$. ♦

Corollary $\mathbb{R}^+ = \{r|(x_n) \in r, \forall \textit{ positive } (x_n)\}.$

Proof Suppose that $r \in \mathbb{R}^+$.
$\therefore \exists$ a positive sequence $(x_n) \in r$.
If $(x'_n) \in r$, then based on Theorem 10.15 $(x'_n) \sim (x_n)$.
$\therefore (x'_n)$ is a positive.
Thereby, $\mathbb{R}^+ = \{r|(x_n) \in r, \forall \textit{ positive } (x_n)\}.$ ♦

Theorem 10.16 $\mathbb{R}^+$ *is a set of positive elements of* $\mathbb{R}$.

Proof Suppose that $r_1, r_2 \in \mathbb{R}^+ \ni r_1 = [(x_n)], r_2 = [(y_n)]$ where $(x_n), (y_n)$ are positive sequences in $\mathbb{R}$.
$\therefore \exists 0 < \epsilon_1 \in \mathbb{Q}, n_{\epsilon_1} \in \mathbb{N} \ni x_n \geq \epsilon_1, \forall n \geq n_{\epsilon_1}.$
Also, $\therefore \exists 0 < \epsilon_2 \in \mathbb{Q}, n_{\epsilon_2} \in \mathbb{N} \ni y_n \geq \epsilon_2, \forall n \geq n_{\epsilon_2}.$
Now, let $n = \{n_{\epsilon_1}, n_{\epsilon_2}\},$
$\therefore (x_n \geq \epsilon_1) \wedge (y_n \geq \epsilon_2), \forall n \geq n_\epsilon.$

$\therefore x_n + y_n \geq \epsilon_1 + \epsilon_2 = \epsilon, \forall n \geq n_\epsilon.$

$\therefore (x_n + y_n)$ is a positive sequence in $\mathbb{Q}$.

In the same way, we can prove that $x_n y_n$ is a positive sequence in $\mathbb{Q}$.

$\therefore (r_1 + r_2 = [(x_n + y_n)] \in \mathbb{R}) \wedge (r_1 r_2 = [(x_n y_n)] \in \mathbb{R}).$

Now, to prove the third property, let $r = [(x_n)]$.

$\therefore (x_n)$ is a positive sequence in $\mathbb{Q} \leftrightarrow r \in \mathbb{R}^+$.

Thereby $0 = r \in \mathbb{R} \leftrightarrow L(x_n) = 0 \in \mathbb{Q}$.

$\therefore -r = [(-x_n)] \in \mathbb{R}^+ \leftrightarrow (-x_n) \in \mathbb{Q}$ is a positive sequence.

But, according on Theorem 10.15 one of the following statements is true

$((-x_n)$ is a positive$) \vee ((x_n)$ is a positive$) \vee (L(x_n) = 0.$

Thereby, one of the following statements is true

$(-r \in \mathbb{R}6^+) \vee (r \in \mathbb{R}) \vee (r = 0).$

Thereby, the third property is satisfied.

Thus, $\mathbb{R}^+$ is a set of positive elements of $\mathbb{R}$. ♦

Definition 10.8 Let $r_1, r_2 \in \mathbb{R}$, then $r_1 < r_2$ if and only if $r_2 - r_1 \in \mathbb{R}^+$(Temirovna, 2021; Dijksterhuis, 1961; Kist and Leestma, 1970).

Note:

(1) $r_1 > r_2 \leftrightarrow r_2 < r_1$.

(2) $r_1 \leq r_2 \leftrightarrow (r_1 < r_2) \vee (r_1 = r_2)$.

(3) $r_1 \geq r_2 \leftrightarrow (r_1 > r_2) \vee (r_1 = r_2)$.

Theorem 10.17 *The mathematical system* $(\mathbb{R}, \leq)$ *is totally ordered set.*

Proof (1) Reflexive.

$\because r_1 \leq r_1, \forall r_1 \in \mathbb{R},$

$\therefore \ \leq$ is a reflexive relation.

(2) Anti-symmetric.

Suppose that $(r_1 \leq r_2) \wedge (r_2 \leq r_)$,

$\therefore (r_1 - r_2 \in \mathbb{R}^+) \wedge (r_2 - r_1 \in \mathbb{R}^+)).$

But, $r_1 - r_2 = -(r_2 - r_1)$.

$\therefore (r_2 - r_1 \in \mathbb{R}^+) \wedge -(r_2 - r_1 \in \mathbb{R}^+).$ And this contradicts the triple property.

$\therefore r_2 - r_1 = 0.$
$\therefore r_1 = r_2.$
Thereby, $\leq$ is anti-symmetric.
(3) Transitive.
Suppose that $r_1 \leq r_2, r_2\ leq r_3$.
$\therefore (r_2 - r_1 \in \mathbb{R}^+) \vee (r_1 = r_2),\ (r_3 - r_2 \in \mathbb{R}^+) \vee (r_3 = r_2).$
If, $(r_2 - r_1 \in \mathbb{R}^+) \wedge (r_3 - r_2 \in \mathbb{R}^+)$,
then $(r_3 - r_2) + (r_2 - r_1) \in \mathbb{R}^+$.
$\therefore r_3 - r_1 \in \mathbb{R}^+.$
$\therefore r_1 < r_3 \to r_1 \leq r_3.$
In the same way, we can prove the other cases.
$\therefore \leq$ is transitive.
Thereby, $\leq$ is a partial ordered relation.
(4) Ordering.
Let $r_1, r_2 \in \mathbb{R}$.
$\therefore r_1 - r_2 \in \mathbb{R}.$
Now, according on triple property, we have
$(r_1 - r_2 \in \mathbb{R}^+) \vee (r_1 = r_2) \vee (-(r_1 - r_2) \in \mathbb{R}^+).$
$\therefore (r_1 < r_2) \vee (r_2 < r_1) \vee (r_1 = r_2) \to (r_1 \leq r_2) \vee (r_2 \leq r_1).$
Thereby, every pair element in $\mathbb{R}$ is comparable.
Thus, $\leq$ is a totally ordered relation. ⧫

Theorem 10.18 *The mathematical system* $(\mathbb{R}, +, \cdot, \leq)$ *is an ordered domain.*

Proof Since $\leq$ is the totally ordered relation on $\mathbb{R}$, hence its enough to prove

(1) Add a number to both sides of the inequality.
Suppose that $a < b \in \mathbb{R}, \forall a, b \in \mathbb{R}$.
$\therefore b - a \in \mathbb{R}^+.$
Now, $\forall c \in \mathbb{R}$, we have $(b + c) - (a + c) = (b - a) \in \mathbb{R}^+$.
$\therefore a + c < b + c, \forall a, b, c \in \mathbb{R}.$
(2) Multiply both sides of the inequality by a positive number.
Suppose that $a < b \in \mathbb{R}, \forall a, b \in \mathbb{R}$.
Now, let $c \in \mathbb{R}$, and $b - a \in \mathbb{R}^+$.
$\therefore (b - a)c \in \mathbb{R}^+.$

$\therefore bc - ac \in \mathbb{R}^+$.

$\therefore ac < bc, \forall a, b \in \mathbb{R}, \forall c \in \mathbb{R}^+$.

Thus, the mathematical system $(\mathbb{R}, +, \cdot, \leq)$ is the ordered domain. ♦

Corollary *The mathematical system* $(\mathbb{R}, +, \cdot, \leq)$ *is an ordered field.*

Proof The proof is left as an exercise to the reader. ♦

10.4.1 Embedding

In this section, we will explain that it is possible to embed the ordered field $(\mathbb{Q}, +, \cdot, \leq)$ into the ordered field $(\mathbb{R}, +, \cdot, \leq)$, which is ordered field $(\mathbb{R}, +, \cdot, \leq)$ is the expansion to the ordered field $(\mathbb{Q}, +, \cdot, \leq)$.

Notation: We denote to the mapping $E_{\mathbb{Q}}^{\mathbb{R}} : \mathbb{Q} \to \mathbb{R}$ in which $E_{\mathbb{Q}}^{\mathbb{R}} = [(x)]$ by E.

Theorem 10.19 *The mapping* $E : \mathbb{Q} \to \mathbb{R}$ *is an isomorphic preserves on addition, multiplication, and ordering.*

Proof (1) Injective.

$E : \mathbb{Q} \to \mathbb{R}$ is injective mapping.

Suppose that $E(x) = E(y)$ in the $\mathbb{R}$.

$\therefore [(x)] = [(y)]$.

$\therefore (x) \sim (y)$.

$\therefore L(x - y) = 0$.

$\therefore x = y$ in $\mathbb{Q}$.

$\therefore (E(x) = E(y)) \in \mathbb{R} \to (x = y) \in \mathbb{Q}$.

Thus, E is the injective mapping.

(2) Preserving on addition and multiplication.

Suppose that $x, y \in \mathbb{Q}$.

$\therefore E(x + y) = [(x + y)] = [(x)] + [(y)] = E(x) + E(y)$.

Also, $E(xy) = [(xy)] = [(x)][(y)] = E(x)E(y)$.

Thereby, E preserves on addition and multiplication.

(3) Preserving on ordering.

Suppose that $(x < y) \in \mathbb{Q}$.

$x < y \leftrightarrow (y - x) > 0,$
$\leftrightarrow (y - x)$ is a positive sequence in $F_{\mathbb{Q}}$
$\leftrightarrow [(y)] - [(x)] > 0.$
$\leftrightarrow [(x)] < [(y)].$
$\leftrightarrow E(x) < E(y).$
From (1), (2)& (3) E is preserves on ordering. ♦

Note:

(1) We are going to write x instead of $[(x)]$. Or, we don't differentiate between $\mathbb{Q}$ and is isomorphic image in $\mathbb{R}$.

(2) The mathematical system $(\mathbb{Q}, +, \cdot)$ is a subfield of $(\mathbb{R}, +, \cdot)$.

10.4.2 Completeness on $\mathbb{R}$

We have demonstrated in Theorem 10.5 that in any ordered field A, every convergent sequence is a fundamental sequence, whereas the opposite is not true according in Theorem 10.8. Or every convergent sequence is a fundamental sequence, but the opposite is not true.

Definition 10.9 The ordered field A is a complement if and only if every fundamental sequence in A is a convergent (Körner, 2004; Aliprantis and Burkinshaw, 1998; Browder, 2012; Bartle and Sherbert, 2011; Bartle and Sherbert, 2000; Bressoud, 2007).

Theorem 10.20 (Introductory Theorem) *For every* $0 < \epsilon \in \mathbb{R}$, *there exists* $e \in \mathbb{Q}$, *such that* $0 < e < \epsilon$.

Proof Let $\epsilon = [(x_n)]$.
$\because \epsilon > 0,$
$\therefore (x_n)$ is a positive sequence in F.
$\therefore \exists 0 < k \in \mathbb{Q}, m \in \mathbb{N} \ni x_n \geq k, \forall n \geq m.$
$\therefore x_n > \frac{k}{2} > 0, \forall n \geq m.$
$\therefore x_n - \frac{k}{2} > 0, \forall n \geq m.$
Or, the sequence $(x_n - \frac{k}{2})$ is positive in $F_{\mathbb{Q}}$.
$\therefore [(x_n - \frac{k}{2})] > 0.$
$\therefore [(x_n)] - [(\frac{k}{2})] > 0.$
$\therefore [(\frac{k}{2})] < [(x_n)] = \epsilon.$

Now, if we consider the rational number $e = [(\frac{k}{2})]$, then we have found $0 < e < \epsilon \in \mathbb{Q}$. ♦

In the next theorem, we prove that every fundamental sequence in $\mathbb{Q}$ is a convergent in $\mathbb{R}$.

Theorem 10.21 *If $(x_n) \in r$, then $L(x_n) = r$ in $\mathbb{R}$.*

Proof Let $0 < \epsilon \in \mathbb{R}$.

According to the previous introductory theorem (Theorem 10.20), $\exists e \in \mathbb{Q} \ni 0 < e < \epsilon$, and since (x_n) is a fundamental sequence in $\mathbb{Q}$,

$\therefore \exists n_e \in \mathbb{N} \ni |x_m - x_n| < \frac{e}{2}, \forall m, n \geq n_e$.

$\therefore e - |x_n - x_m| > \frac{e}{2}, \forall m, n \geq n_e$.

Now, $(y_m) = (e - |x_n - x_m|), \forall n \geq n_e$ is a positive fundamental sequence in $\mathbb{R}$.

$\therefore (y_m) = (e - |x_n - x_m|) > 0, \forall n \geq n_e$ in $\mathbb{R}$.

Now, based on the use of the following fact;

$\forall (x_n) \in F_{\mathbb{Q}}$, we have $(|[(x_n)]|) = [(|x_n|)]$.

$\therefore |x_n - r| = |x_n - [(x_m)]| = [(|x_n - x_m|)]$.

$\therefore |x_n - r| = (|x_n - x_m|) < [(e)] = e < \epsilon, \forall n \geq n_e$.

Thus, $L(x_n) = r \in \mathbb{R}$. ♦

Corollary *If $r \in \mathbb{R}, 0 < \epsilon \in \mathbb{R}$, then $\exists x \in \mathbb{Q} \ni |r - x| < \epsilon$.*

Proof Let $(x_n) \in r$.

$\therefore L(x_n) = r$.

$\therefore \forall\ 0 < \epsilon \in \mathbb{R}, \exists n_\epsilon \in \mathbb{N} \ni |r - x_n| < \epsilon$.

Now, $\forall n \geq n_\epsilon$, let $x = x_n \in \mathbb{Q}$.

$\therefore |r - x| < \epsilon$. ♦

Theorem 10.22 $\mathbb{R}$ *is a complete.*

Proof Let (r_n) be a fundamental sequence in $\mathbb{R}$.

Based on Theorem 10.21, $\forall n \in \mathbb{N} - \{0\}, \exists q_n \in \mathbb{Q} \ni |r_n - q_n| < \frac{1}{n}$.

$\because L(\frac{1}{n}) = 0 \in \mathbb{R}$,

$\therefore \forall 0 < \epsilon \in \mathbb{R}, \exists n_1 \in \mathbb{N} \ni |r_m - q_n| < \frac{1}{n} < \frac{\epsilon}{3}, \forall n \geq n_1$.

$\because (r_n)$ is a fundamental sequence,

$\therefore \exists n_2 \in \mathbb{N} \ni |r_m - r_n| < \frac{\epsilon}{3}, \forall m, n \geq n_2$.

Thereby, $|q_m - q_n| = |q_m - r_m + r_m - r_n + r_n - q_n|$

$\leq |q_m - r_m| + |r_m - r_n| + |r_n - q_n|$

$< \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon, \forall m, n \geq n_3 = max\,\{n_1, n_2\}$.

$\therefore (q_n)$ is a fundamental sequence in $\mathbb{Q}$.

According on Theorem 10.21, we conclude that $L(q_n) = [(q_n)] = r \in \mathbb{R}$.

$\therefore \exists n_4 \in \mathbb{N} \ni |q_n - r| < \frac{2\epsilon}{3}, \forall n \geq n_4$.

$\therefore |r_n - r| = |r_n - q_n + q_n - r|$

$\leq |r_n - q_n| + |q_n - r|$

$< \frac{\epsilon}{3} + \frac{2\epsilon}{3} = \epsilon, \forall n \geq max\,\{n_1, n_4\}$.

$\therefore L(r_n) = r$.

$\therefore$ every fundamental sequence in $\mathbb{R}$ is a convergent.

$\therefore \mathbb{R}$ is a complete. ♦

10.4.3 Density of $\mathbb{Q}$ in $\mathbb{R}$

Definition 10.10 If B is a subset of the ordered set A, then B is a dense in A if and only if $\forall a, b \in A, (a < b) \in A, \exists c \in B \ni a < c < b$ (Bourbaki, 2013; Steen et al., 1978; Kleiber and Pervin, 1969).

Theorem 10.23 *The set $\mathbb{Q}$ is a dense in $\mathbb{R}$.*

Proof Let $(r_1 < r_2) \in \mathbb{R}$.

$\because (\mathbb{R}, +, \cdot, \leq)$ is the ordered field

$\therefore \leq$ on $\mathbb{R}$ is a dense.

$\therefore \exists r_3 \in \mathbb{R} \ni r_1 < r_3 < r_2$.

Let $\epsilon = min\,\{r_3 - r_1, r_2 - r_3\}$.

$\therefore$ based on corollary of Theorem 10.21 $\exists q \in \mathbb{Q} \ni |r_3 - q| < \epsilon$.

$\therefore r_1 \leq r_3 - \epsilon < q < r_3 + \epsilon \leq r_2$.

$\therefore$ we have got $q \in \mathbb{Q} \ni r_1 < q < r_2$.

$\therefore \mathbb{Q}$ is a dense in $\mathbb{R}$. ♦

10.4.4 Archimedean Property in $\mathbb{R}$

Theorem 10.24 *The ordered field $(\mathbb{R}, +, \cdot, \leq)$ is Archimedean field.*

Proof Let $(0 < r_1 < r_2) \in \mathbb{R}$.

Let $x, y \in \mathbb{Q} \ni 0 < x < r_1 < r_2 < y < r_1 + r_2$.

$\because \mathbb{Q}$ is Archimedean, there is an isomorphic embedding between $\mathbb{Q}$ and $\mathbb{R}$, and preserves on addition and multiplication.

$\therefore \exists n \in \mathbb{N} - \{0\} \ni (nx \geq y) \in \mathbb{R}$.

$\therefore nr_1 > nx \geq y > r_2$.

$\therefore nr_1 > r_2$.

$\therefore \mathbb{R}$ is is Archimedean field. ♦

Theorem 10.25 *If $(A, +, \cdot, \leq)$ be an ordered field, then the following statements are equivalence:*

(1) A is the Archimedean field, and all fundamental sequences in A have a limit.

(2) All nonempty subset of A, provided will be bounded above, has a least upper bound in A.

(3) There are no gaps in A.

(4) All nonempty subset of A, provided will be bounded below, has a greatest lower bound in A.

Proof We will prove the equivalence of the statements as shown in Figure 10.1 from implication.

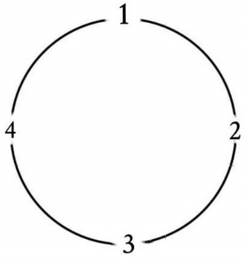


Figure 10.1: Equivalence of Statements (Implication)

$1 \to 2$: Let $\phi \neq X \subseteq A$, b be a bounded above of X, and $\bar{x} \in X$.

$\because A$ is the Archimedean field,

$\therefore n, \bar{m} \in \mathbb{N} \ni \bar{x} + \frac{\bar{m}}{n} \geq b$.

Thereby, $\bar{x} + \frac{\bar{m}}{n}$ is a bounded above of X.

$\therefore \phi \neq B_n = \left\{ m | \bar{x} + \frac{\bar{m}}{n} \text{ is a bounded above of } X \right\} \subseteq \mathbb{N}, \forall n \in \mathbb{N}$.

$\because \mathbb{N}$ is well ordered set.

$\therefore B_n$ contains of first natural number m_n.

$\therefore \forall n \in \mathbb{N}$, it should be

(i) $y_n = \bar{x} + \frac{m_n}{n}$ is bounded above of x.

(ii) $x_n = y_n - \frac{1}{n} = \bar{x} + \frac{m_n - 1}{n} \leq x$.

$\therefore (x_m < y_n) \wedge (x_m - x_n < y_n - (y_n - \frac{1}{n}) = \frac{1}{n}, x \in X$.

$$\text{Now, } |x_m - x_n| = max\left\{x_m - x_n, x_n - x_m\right\}$$
$$\leq max\left\{\frac{1}{n}, \frac{1}{m}\right\}, \forall m, n \in \mathbb{N} - \{0\}$$

$\because L(\frac{1}{n}) = 0$ in the Archimedean field A.

$\therefore (x_n)$ is a fundamental sequence in A. And based on sequential hypothesis (x_n) has a limit $a \in A$.

Now, we have to prove that $a = supX$.

(i) a is maximum of X.

If a does not have upper bound of X, then $\exists x \in X \ni a < x$.

$\because L(x_n) = 0 \wedge L(\frac{1}{n}) = 0$,

$\therefore \exists n \in \mathbb{N} \ni x_n - a \leq |x_n - a| < \frac{x-a}{2} \wedge \frac{1}{n} < \frac{x-a}{2}$.

$\therefore y_n = x_n + \frac{1}{n} < (a + \frac{x-a}{2}) + \frac{x-a}{2} = x$.

This is impossible because y_n is a maximum of X.

$\therefore a$ is a maximum to X.

(ii) Let c be a maximum to X.

$\therefore a \leq c$, because if $a > c$, then $a - c > 0$.

$\therefore \exists n \in \mathbb{N} \ni a - x_n \leq |a - x_n| < a - c$.

$\therefore c < x_n$.

Also, $\nexists x \in X \ni x_n \leq X$.

$\therefore c < x_n \leq x$. And this is impossible because c is maximum to X.

$\therefore a = supX$.

$2 \rightarrow 3$:

Let (X, Y) be a cut in A.

$\therefore (\phi \neq X \subseteq A) \wedge (\forall y \in Y)$ is a maximum to X.

Thereby, according to the axiom, $a \in A \ni a = supX$.

$\because (X, Y)$ is a cut in A,

$\therefore (a = maxX) \vee (a = minY)$.

Thereby, $a \in X \vee a \in Y$.

If $a \in X$, then $supX = a = maxX$.

If $a \in Y$, then because every element in Y is a maximum to X, then $supX = a = minY$.

$3 \to 4:$

Let $\phi \neq B \subseteq A$, where B is bounded below.

Let $\begin{cases} X = \{x : x \leq b, \forall b \in B\} \\ \qquad Y = A - X \end{cases}$

$\therefore (X, Y)$ is a cut in A, because

(1) $X = \phi$ is the set of all bounded below to B, and B is bounded below.

(2) $Y \neq \phi$ because $b + 1 \in Y, \forall b \in B \neq \phi$.

(3) $(X \cup Y = A) \wedge (X \cap Y = \phi)$.

(4) If $x \in X, y \in Y$, then $x < y$.

If $x \geq y$, then $y \leq x \leq b, \forall b \in B$.

$\therefore y \in X$, and this is contradiction.

$\therefore (X, Y)$ is a cut to A.

If $b \in X, \forall b \in B$, then $b = maxX = infB$.

If $(b \in Y, \forall b \in B) \wedge (y_o)$ minimum in Y, then y_o is a bounded below to B.

$\therefore y_o \in X$.

This is impossible since $X \cap Y = \phi$.

$\therefore Y$ has no minimum.

$\because (X, Y)$ is not a gap,

$\therefore X$ has a maximum, say x_o.

Thereby, $x_o = infB$.

$4 \to 1$: It is left for the reader. ♦

Theorem 10.26 *Every Archimedean ordered field can be isomorphic embedding in the ordered field* $\mathbb{R}$.

Proof Let A be Archimedean ordered field, and $\mathbb{Q}_A$ be the set of all rational elements in A. Or, $A = \left\{\frac{hI_A}{kI_A} | h, k \in \mathbb{Z}, k \neq 0\right\}$.

If $x = \frac{h}{k}$, then $\bar{x} = \frac{hI_A}{kI_A} \in \mathbb{Q}$.

Now, let us define the mapping

$F : A \to \mathbb{R} \ni F(L(\bar{x}_n)) = L(x_n), (x_n) \in F$.

(1) F is injective.

F is injective because if $a \in A$, then $a = L(\bar{x}_n), (\bar{x}_n) \in A$.

$\because (\bar{x}_n)$ is a fundamental sequence in A,

$\therefore (\bar{x}_n)$ is a fundamental sequence in $\mathbb{Q} \wedge \mathbb{R}$.

Since $\mathbb{R}$ is a complete, hence $L(x_n) \in \mathbb{R}$.
$(a, L(x_n)) \in F$.
Assume that $(x_n), (y_n) \in F_{\mathbb{Q}}$.
$\because L(x_n) = L(y_n)$
$\leftrightarrow L(x_n - y_n) = 0$
$\leftrightarrow L(\bar{x}_n - \bar{y}_n) = 0$
$\leftrightarrow L(\bar{x}_n) = L(\bar{y}_n) = 0$
$\therefore F : A \to \mathbb{R}$ is the injective.
(2) F is preserves on the addition and multiplication.
$\because F(a + b) = F(a) + F(b), F(ab) = F(a)F(b)$.
$\therefore F$ is preserves on the addition and multiplication.
(3) F is preserves on the ordering.
If $a = L(\bar{x}_n)$, then $a \in A$ is a positive element.
$\therefore \bar{x}_n \in \mathbb{R}$ is a positive sequence.
$\therefore L(x_n)$ is a positive real number.
$\therefore F : A \to \mathbb{R}$ is preserves on the ordering.
Thus, from (1), (2)& (3), $F : A \to \mathbb{R}$ is isomorphic embedding. ♦

Theorem 10.27 *In the previous theorem, $F : A \to \mathbb{R}$ is isomorphism.*

Proof If A is a complete, then according to Theorem 10.26, the mapping F is a surjective.

If $x = L(x_n) \in \mathbb{R}$, then $(\bar{x}_n)$ is a fundamental sequence in A.
$\because A$ is complete,
$\therefore L(\bar{x}_n) = a \in A$.
$\because x = F(a)$,
$\therefore F : A \to \mathbb{R}$ is isomorphism. ♦

Theorem 10.28 $\mathbb{R}$ *is uncountable set.*

Proof If x is a real number in the interval $(0, 1]$, then a representing of x will be in a unique way, and on the infinite decimal $a_1a_2a_3$....

In other words, x is a limit of the unique sequence u_n in the form

$$\begin{array}{l} u_1 = \frac{a_1}{10} \\ . \\ . \\ . \\ u_n = u_{n-1} + \frac{a_n}{10^n}, n > 1 \end{array}$$

where $a \leq a_n \leq q, u_n < x, \forall n$.

Now, we have to prove the interval $(0, 1]$ is uncountable.

If the sequence is countable on the $(0, 1]$, then its elements will be as follows

$$\begin{array}{llllll} x_1 : & a_{11} & a_{12} & a_{13} & ... \\ x_2 : & a_{21} & a_{22} & a_{23} & ... \\ x_3 : & a_{31} & a_{32} & a_{33} & ... \\ ... : & ... & ... & ... & ... \\ ... : & ... & ... & ... & ... \\ ... : & ... & ... & ... & ... \end{array}$$

Now, $y = -b_1 \;\; b_2 \;\; b_3 ..., b_n \neq a_{nn}; \forall n$.

It should be noticed that y is infinite decimal fraction. In addition, $y \notin (0, 1]$.

This is contradiction.

$\therefore (0, 1]$ is uncountable.

Since $(0, 1] \subset \mathbb{R}$, hence R is uncountable. ♦

10.5 Exercises

Answer the following questions:

Q1: If $(x_n) \in F_{\mathbb{Q}}$, then $|[(x_n)]| = [(|x_n|)]$.

Q2: Prove that the $(x_n) \in \mathbb{Q}$ is fundamental in $\mathbb{Q}$ if and only if it is fundamental in $\mathbb{R}$.

Q3: Let (x_n) be a quotient sequence, and $x \in \mathbb{Q}$. Prove that $(L(x_n) = x) \in \mathbb{Q} \leftrightarrow (L(x_n) = x) \in \mathbb{R}$.

Q4: Prove that the ordered field A is Archimedean if and only if the subset $\mathbb{Q}_A$ of all quotient elements of A is dense in A.

Q5: Consider the ordered fields A, B, where B is a dense in A. If (x_n) be a sequence in B, then prove that

(i) (a_n) is a fundamental sequence in A if and only if is a fundamental in B.

(ii) $(L(a_n) = a) \in A \leftrightarrow (L(a_n) = a) \in B$.

(iii) (a_n) is a positive sequence in A if and only if is a positive in B.

Q6: Prove that an ordered field A is Archimedean if and only if each element in A is a limit to a sequence of rational elements in A.

Q7: Give an example of a complete ordered field and not Archimedean.

Q8: Prove that, every ordered field contains a copy of the natural numbers, all of which are positive.

Q9: Prove that, $\forall a, b \in \mathbb{R}, a > 0, \exists n \in \mathbb{N} \ni na > b$

Q10: Prove that, any two complete ordered fields are isomorphic.

Q11: Prove that any two complete ordered fields are isomorphic.

Q12: If (x_n) and (y_n) are Cauchy, then:

(i) $(x_n + y_n)$, and

(ii) $(x_n y_n)$ are Cauchy sequences.

Q13: If $(x_m) \cong (y_m)$. Prove that;

(i) If one of them is Cauchy or convergent, then so is the other.

(ii) $\lim x_m = \lim y_m$ (if it exists).

Q14: Is Cauchy sequence convergent?

Q15: Prove that every Cauchy sequnece is bounded.

Q16: Show that the sequence:

(i) $(\frac{1}{n})$ is a Cauchy sequence.

(ii) $((-1)^n)$ is not a Cauchy sequence.

(iii) $(\frac{1}{n^2})$ is a Cauchy sequnce.

(iv) $(cos(\frac{1}{n}))$ is a Cauchy sequnce.

Q17: Considder the following Lemma:

If (a_n) is a Cauchy sequence of real numbers then (a_n) is also bounded.

Show that the convergent of this lemma is false.

Q18: Prove the Convergent and Divergent of the following sequences:

(i) $(\frac{n}{n+1})$.

(ii) (n).

(iii) $(2n+3)$.

(iv) $(\frac{n+2}{2n-1})$.

11
The Complex Numbers

11.1 Introduction

Attempts that were efforts to solve the equation in the kind of $x^2 + 1 = 0$ of the real numbers led to the system of new kinds of numbers, called the system of complex numbers. A complex number is a number that can be expressed in the form $a + bi$ where a and b are real numbers, and i is a symbol called the imaginary unit and satisfying the equation $i^2 = -1$. Because no real number satisfies this equation, i was called an imaginary number by René Descartes. The set of complex numbers is denoted by $\mathbb{C}$. Despite the historical nomenclature "imaginary", complex numbers are regarded in the mathematical sciences just as "real" as real numbers and are fundamental in many aspects of the scientific description of the natural world (Bourbaki, 1994; Andreescu et al., 2006).

11.2 Field of the Complex Numbers

Definition 11.1 The set $\mathbb{C} = \mathbb{R} \times \mathbb{R} \{(x, y)|x, y \in \mathbb{R}\}$ is called the set of the complex numbers (Bourbaki, 1994; Andreescu et al., 2006).

Note:

(1) We will use the symbols $z, w, u, v, ...$ to denote the complex numbers.

(2) The equivalence relations on the set $\mathbb{C}$ are equal to the ordered pairs. Thereby, each equivalence class consists of one element, and each ordered pair (x, y) is called a complex number.

Theorem 11.1 *If* $u = (x_1, y_1), v = (x_2, y_2)$ *and* $F(u, v) = (x_1+x_2, y_1+y_2), G(u, v) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$ *then* $F = \{((u, v), F(u, v))|u, v \in \mathbb{C}\}, G = \{((u, v), G(u, v))|u, v \in \mathbb{C}\}$ *are binary operations on* $\mathbb{C}$.

Proof $\because \forall(u, v) \in \mathbb{C} \times \mathbb{C}$,

$\therefore F(u, v)$ will be a unique image because every two ordered pairs of the $\mathbb{R}$ are equal if and only if the first element of the first ordered pair is equal to the first element of the second ordered pair and, the second element of the first ordered pair is equal to the second element of the second ordered pair.

$\therefore F : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ is a mapping.

$\therefore F$ is a binary operation on $\mathbb{C}$.

In the same way G is a binary operation on $\mathbb{C}$. ♦

Definition 11.2 F is called addition operation on $\mathbb{C} \times \mathbb{C}$, and denoted by $u +_{\mathbb{C}} v$ instead of $F(u, v)$. In addition, G is called multiplication operation on $\mathbb{C} \times \mathbb{C}$, and denoted by $u \cdot_{\mathbb{C}} v$ instead of $G(u, v)$. For convenient, it is written $u + v, u \cdot v$ respectively (Sikka, 2017; Weisstein, 2003a; Kasana, 2005; Hardy et al., 1979; Argand, 1814b; Argand, 1814a; Hankel, 1867; Ahlfors, 1979).

Example 11.1 If $u = (-5, -7), v = (3, \frac{15}{7})$, then

(1) $u + v = (-5 + 3, -7 + \frac{15}{7}) = (-2, -\frac{34}{7})$.

(2) $u \cdot v = (-5 \cdot 3 - (-7) \cdot \frac{15}{7}, -5 \cdot \frac{15}{7} + 3 \cdot (-7)) = (0, -\frac{222}{7})$.

Theorem 11.2 *The mathematical system* $(\mathbb{C}, +_{\mathbb{C}}, \cdot_{\mathbb{C}})$ *is a field.*

Proof (1) The mathematical system $(\mathbb{C}, +_{\mathbb{C}}, \cdot_{\mathbb{C}})$ is a commutative field with(The proof is left to the reader).

(a) An additive identity element $(0, 0) = 0_{\mathbb{C}}$.

(b) Multiplicative identity element $(1,0) = 1_{\mathbb{C}}$.
Now, it should be noted that
if $u = (x, y) \neq 0_{\mathbb{C}} = (0,0)$, then $(x \neq 0) \vee (y \neq 0)$.
$\therefore x^2 + y^2 \in \mathbb{R}^+$.
Suppose that $v = (x_1, y_1)$.
$\therefore u \cdot v = (x, y)(x_1, y_1) = (xx_1 - yy_1, xy_1 + x_1 y) = (1, 0)$.
$\therefore xx_1 - yy_1 = 1$ ... (1)
$xy_1 + x_1 y = 0$ ...(2).
By solving (1)& (2) simultaneously, we get
$x_1 = \frac{x}{x^2+y^2}, y_1 = \frac{-y}{x^2+y^2}$.
$\therefore v = (\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}) \in \mathbb{C}$.
$\therefore u \cdot v = (1, 0) = 1_{\mathbb{C}}$.
Thereby, $\forall\ 0 \neq c \in \mathbb{C}$ has a multiplicative inverse.
Thus, the mathematical system $(\mathbb{C}, +_{\mathbb{C}}, \cdot_{\mathbb{C}})$ is a ring. ♦

Definition 11.3 The field $(\mathbb{C}, +_{\mathbb{C}}, \cdot_{\mathbb{C}})$ is called complex field (Apostol, 1974; Apostol and Ablow, 1958; Apostol, 1981).

Notation: We denote to the element $(0, 1)$ by i, so $-1 = (0, -1)$.

Theorem 11.3 *The complex numbers $\mp i$ are solutions to the equation $x^2 = -1$.*

Proof $\because (\mp i)^2 = i^2 = (0, 1)(0, 1) = (-1, 0) = -1$.
$\therefore -1$ is a solution to the equation $x^2 = -1$. ♦

Definition 11.4 If $u = (x_1, y_1), v = (x_2, y_2)$, then $u < v$ if and only if $(x_1 < x_2) \vee ((x_1 = x_2) \wedge (y_1 < y_2))$(Apostol, 1981).

Example 11.2 (1) $(7, 5) < (8, 3)$.
(2) $(a, b) < (a, b + \delta); \forall a, b \in \mathbb{R}, \delta \in \mathbb{R}^+$.

Theorem 11.4 *The relation $\leq$ is a totally ordered relation on $\mathbb{C}$.*

Proof (1) Reflexive.

$\because u_1 \leq u_2, \forall u_1, u_2 \in \mathbb{C}$,

$\therefore \leq$ is a reflexive relation.

(2) Antisymmetric.

Let $u_1 \leq u_2, u_2 \leq u_1 \ni u_1 = (x_1, y_1), u_2 = (x_2, y_2)$.

$\because u_1 < u_2$,

$\therefore (x_1 < x_2) \vee ((x_1 = x_2) \wedge (y_1 < y_2))$.

And, $\because u_2 < u_1$,

$\therefore (x_2 < x_12) \vee ((x_2 = x_1) \wedge (y_2 < y_1))$.

First case;

Suppose that $(x_1 < x_2) \wedge (x_2 < x_1)$,

$\therefore x_1 = x_2$ because $\mathbb{R}$ is ordered field.

This implies that $(y_1 < y_2) \wedge (y_2 < y_1)$,

$\therefore y_1 = y_2$ because $\mathbb{R}$ is ordered field.

$\therefore (x_1 = x_2) \wedge (y_1 = y_2)$.

$\therefore u_1 = u_2$.

Thus, $\leq$ is the antisymmetric relation.

The proof of the other cases are left to the reader.

(3) Transitive.

Let $u_1 \leq u_2, u_2 \leq u_3 \ni u_1 = (x_1, y_1), u_2 = (x_2, y_2), u_3 = (x_3, y_3) \forall u_1, u_2, u_3 \in \mathbb{C}$.

$\because u_1 \leq u_2$,

$\therefore (x_1 < x_2) \vee ((x_1 = x_2) \wedge (y_1 < y_2))$.

And, $\because u_2 \leq u_3$,

$\therefore (x_2 < x_3) \vee ((x_2 = x_3) \wedge (y_2 < y_3))$.

First case;

$(x_1 < x_2) \wedge (x_2 < x_3)$,

$\therefore x_1 < x_3$.

Thus, $u_1 < u_3$.

Second case;

$(x_1 < x_2) \wedge ((x_2 = x_3) \wedge (y_2 < y_3))$.

$\therefore x_1 < x_2$.

Thus, $u_1 < u_3$.

Third case;

$((x_1 = x_2) \wedge (y_1 < y_2)) \wedge (x_2 < x_3)$.

$\therefore x_1 < x_2$.

Thus, $u_1 < u_2$.
Fourth case;
$((x_1 = x_2) \wedge (y_1 < y_2)) \wedge ((x_2 = x_3) \wedge (y_2 < y_3))$.
$(x_1 = x_3) \wedge (y_1 < y_2) \wedge (y_2 < y_3)$.
$(x_1 = x_3) \wedge (y_1 < y_3)$.
$\therefore u_1 < u_2$.
Thus, $\leq$ is a transitive relation.
(4) Comparison.
Let $u_1 = (x_1, y_1), u_2 = (x_2, y_2)$.
First case:
$x_1 \neq x_2$.
$\because (y_1 \leq y_2) \vee (y_2 \leq y_1)$,
$\therefore (u_1 \leq u_2) \vee (u_2 \leq u_1)$.
Second case;
$x_1 \neq x_2$.
$\therefore (x_1 < x_2) \vee (x_2 \leq x_1)$.
$\therefore (u_1 < u_2) \vee (u_2 < u_1)$.
$\therefore (u_1 \leq u_2) \vee (u_2 \leq u_1)$.
Thereby, every two elements are comparable.
Thus, $\leq$ is totally ordered relation on $\mathbb{C}$. ♦

Theorem 11.5 *The complex field* $(\mathbb{C}, +, \cdot, \leq)$ *is not ordered field.*

Proof In fact, $0 = (0, 0) < (0, 1) = i$.
Suppose that $(\mathbb{C}, +, \cdot, \leq)$ is ordered field.
$\because (\mathbb{C}, +, \cdot, \leq)$ is ordered field,
$\therefore 0 \cdot i < i \cdot i$,
$\therefore 0 < -1$.
$\therefore (0, 0) < (-1, 0)$.
And, this is contradiction in the $\mathbb{R}$.
Thus, $(\mathbb{C}, +, \cdot, \leq)$ is not ordered field. ♦

11.3 Embedding

The symbol E is used to denote the mapping $R_{\mathbb{R}}^{\mathbb{C}} : \mathbb{R} \to \mathbb{C}$, where $R_{\mathbb{R}}^{\mathbb{C}} = (r, 0), r \in \mathbb{R}$ (Spivak, 1975; Sharpe, 1987; Gunderson, 2019; Smith, 2015;

Junghenn, 2018; Adachi, 1993a; Adachi, 1993b).

Theorem 11.6 *The mapping $E : \mathbb{R} \to \mathbb{C}$ is isomorphic from the field $(\mathbb{R}, +_{\mathbb{R}}, \cdot_{\mathbb{R}})$ to the field $(\mathbb{C}, +_{\mathbb{C}}, \cdot_{\mathbb{C}})$.*

Proof (1) Injective mapping

E is injective because if we suppose that $E(r_1) = E(r_2)$.

Now, $E(r_1) = E(r_2) \leftrightarrow (r_1, 0) = (r_2, 0) \leftrightarrow r_1 = r_2, \forall r_1, r_2 \in \mathbb{R}$.

(2) E is preserves addition, and multiplication;

$E(r_1 +_{\mathbb{R}} r_2) = (r_1 + r_2, 0) = (r_1, 0) +_{\mathbb{C}} (r_2, 0) = E(r_1) +_{\mathbb{C}} E(r_2)$.

And, $E(r_1 \cdot_{\mathbb{R}} r_2) = (r_1 \cdot r_2, 0) = (r_1, 0) \cdot_{\mathbb{C}} (r_2, 0) = E(r_1) \cdot_{\mathbb{C}} \mathbb{C}E(r_2), \forall r_1, r_2 \in \mathbb{R}$.

Thus, E is isomorphic mapping from the field $(\mathbb{R}, +_{\mathbb{R}}, \cdot_{\mathbb{R}})$ to the field $(\mathbb{C}, +_{\mathbb{C}}, \cdot_{\mathbb{C}})$. ♦

Notation: We will write r instead of $E(r) = (r, 0), \forall r \in \mathbb{R}$ for convenience.

Theorem 11.7 *If $z \in \mathbb{C}$, then it can only be expressed in a unique way $z = x + iy \ni i = (0, 1), \forall x, y \in \mathbb{R}$.*

Proof $\because z \in \mathbb{C}$,

$\therefore z = (x, y), \forall x, y \in \mathbb{R}$.

$\therefore z = (x, y) = (x, 0) + (0, y) = (x, 0) + (y, 0)(0, 1) = x + iy$.

Now, suppose that $z = x' + y'i \ni x', y' \in \mathbb{R}$.

$\because x' + y'i = (x', 0) + (y', 0)(0, 1) = (x', 0) + (0, y') = (x' + y') = z = (x, y)$,

$\therefore x = x', y = y'$.

Thus, z can only be expressed in a unique way. ♦

11.4 Vector Space

All ordered pairs of real numbers or complex numbers can be expressed by points or vectors in the Cartesian plane. The addition of the complex numbers in such a representation corresponds to the addition of the vectors and the multiplication of the complex numbers by real numbers corresponds to the multiplication of the vectors.

Definition 11.5 Let $(K, +_K, \cdot_K)$ be a field, $(V, +_V)$ be a commutative group, and $\circ$ be a binary operation from $K \times V$ to V. V is called vector space or linear space on K if:

(1) $\alpha \circ (a +_V b) = (\alpha \circ a) +_V (\alpha \circ b)$.

(2) $(\alpha +_K \beta) \circ a = (\alpha \circ a) +_V (\beta \circ a)$.

(3) $(\alpha \circ \beta) \circ a = \alpha \circ (\beta \circ a)$.

(4) $I_K \circ a = a$, $\forall\ \alpha, \beta \in K; a, b \in V$ (Weisstein, 1999b; Halmos, 1958; Halmos, 2017a; Treves, 1967; Bourbaki, 1987; Luenberger, 1997).

Definition 11.6 The operation $\circ$ is called scalar multiplication, and the addition in V is called vector addition (Gutknecht, 2005; Strang, 2006; Axler, 1997; Axler, 2015; Dummit and Foote, 2004a; Dummit and Foote, 2004b; Dummit and Foote, 2004c; Lang, 2002c).

Example 11.3 If K be an arbitrary field, and $K_{\mathbb{N}}$ be the set of all sequences (a_n) in K. Define the addition and scalar multiplication as follows;

$(a_n) + (b_n) = (a_n + b_n)$.

$\lambda \circ (a_n) = (\lambda a_n)$.

Then, $K_{\mathbb{N}}$ is a vector space on the field K because

(1) $K_{\mathbb{N}}$ is a commutative group because

(a) Associative property.

$(a_n) + ((b_n) + (c_n)) = ((a_n) + (b_n) + (c_n)), \forall (a_n), (b_n), (c_n) \in K_{\mathbb{N}}$.

(b) The sequence (0) is a zero element because

$(a_n) + (0) = (0) + (a_n) = (a_n), \forall (a_n) \in K_{\mathbb{N}}$.

(c) Additive inverse.

$(-a_n)$ is additive inverse of (a_n) because

$(a_n) + (-a_n) = (a_n - a_n) = (0), \forall (a_n), (-a_n) \in K_{\mathbb{N}}$.

(d) Commutative property.

$(a_n) + (b_n) = (b_n) + (a_n), \forall (a_n), (b_n) \in K_{\mathbb{N}}$.

(2) $\circ : K \times K_{\mathbb{N}} \to K \times K_{\mathbb{N}}$ is the binary operation because

(a) $\lambda \circ ((a_n) + (b_n)) = (\lambda(a_n + b_n)) = (\lambda a_n + \lambda b_n) = (\lambda a_n) + (\lambda b_n) = \lambda \circ (a_n) + \lambda \circ (b_n)$.

(b) $(\lambda + \gamma) \circ (a_n) = ((\lambda + \gamma) a_n) = (\lambda a_n + \gamma a_n) = \lambda \circ (a_n) + \gamma \circ (a_n)$.

(c) $(\lambda\gamma) \circ (a_n) = ((\lambda\gamma) a_n) = \lambda \circ (\gamma a_n) = \lambda \circ (\gamma \circ (a_n))$.

(3) $I_K \circ (a_n) = (I_K a_n) = (a_n)$.

From (1), (2) & (3), we get that $K_{\mathbb{N}}$ is a vector space.

Definition 11.7 Let V be a vector space on the field K. The $n-$ ordered $(a_1, a_2, ..., a_n)$ of the vectors $a_i, i = 1, 2, ..., n$ is called basis for V if and only if every vector $v \in V$ has a unique representation $v = \sum_{i=1}^{n} \lambda_i a_i, \lambda_i \in K, i = 1, 2, ..., n$(Halmos, 1958; Halmos, 2017a; Halmos and F. D. V. Spaces, 1987).

Definition 11.8 If V is vector space on the field K, and $n \in \mathbb{N}$, then V has dimension n of basis with n of elements (Halmos, 1958; Halmos, 2017a; Halmos and F. D. V. Spaces, 1987; Halmos, 2016).

Note: Let $a_1, a_2 \in V$ be two basis for V have the same elements. Space finite dimensional vector can be identified in a unique way.

Theorem 11.8 $\mathbb{C}$ *is a two dimensional vector space on* $\mathbb{R}$.

Proof Firstly, $\mathbb{C}$ is a vector space on $\mathbb{R}$ (The proof is left to the reader).

Secondly, by utilizing Theorem 11.7, we note that
$(1_{\mathbb{C}} = (1, 0) \wedge (i_{\mathbb{C}} = (0, 1))$.
Or, $\{(1, 0), (0, 1)\}$ are are form a base to $\mathbb{C}$.
$\therefore z = (x, y) = x(1, 0) + y(0, 1)$.
$\therefore$ this base is consists only two elements.
$\therefore$ $\mathbb{C}$ is a two dimensional vector space on $\mathbb{R}$. ♦

11.5 Exercises

Solve the following questions:

Q1: Consider a field K, $n \in \mathbb{Z}^+$, and K_n is a set of $n-$ tuples. The operations $+, \circ$ are defined as follows respectively;

$(a_i) + (b_i) = (a_1 + b_1, ..., a_n + b_n)$, $\lambda \circ (a_i) = (\lambda a_1, ..., \lambda a_n)$.

Prove that K_n is is a two dimensional vector space on K.

Q2: Prove that each field is a one dimensional vector space on itself.

Q3: Prove that $\mathbb{C}$ is a smallest field contains of $\mathbb{R}$ in which every equation in the second degree has a solution.

11.6 Properties of The Complex Numbers

In the previous section, it was shown that complex number is a point in the plane in which the operations addition and multiplication on the two complex numbers were defined. The complex number was also considered as a vector in the plane to which the rules of vector addition and vector multiplication apply. Therefore, the complex number can be represented by either of the two ways;

(i) ordered pair corresponding to a point in the plane $\mathbb{R}^+$; $z = \left\{(a+ib) : a, b \in \mathbb{R} \wedge \sqrt{i} = -1\right\}$, or,

(ii) in the form of a vector $\vec{oz}$, where the two components of the vector represent the real part $a = Re(z)$ and the imaginary part $b = Im(z)$ as in the Figure 11.1.

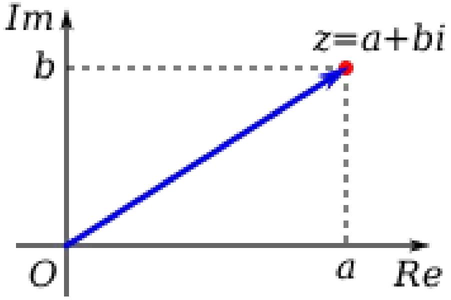


Figure 11.1: The Complex Number

11.6.1 Adding of Complex Numbers

When adding two complex numbers graphically, we add the two real parts and the two imaginary parts to get the new point in the plane $\mathbb{R}^2$. It should be noted that as shown in the Figure 11.2, the addition is the point that represents the end of the diagonal of the parallelogram.

11.6.2 Multiplying Complex Numbers

To find the multiplication of complex numbers graphically, for convenience it is preferable to use the polar form of the complex

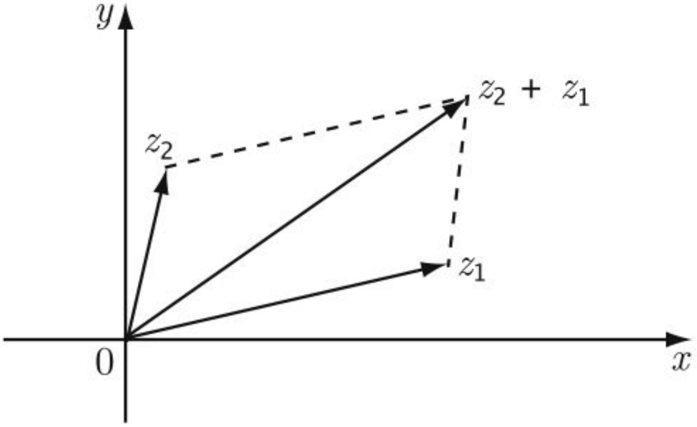


Figure 11.2: Parallelogram Rule for Addition

number. Thus, we define the polar form of the complex number in the following definition.

Definition 11.9 Absolute value of $z = (a, b)$ is $|z| = \sqrt{a^2 + b^2}$ (Ponnusamy and Silverman, 2006; Brown and Churchill, 2009; Ablowitz et al., 2003).

Let us assume that z makes an angle ϕ with the positive x-axis where $0 \leq \theta < 2\pi$, as described in Figures 11.3, 11.4, and 11.5.

Thus, $tan\theta = \frac{b}{a}$. $z = a + ib = rcos\theta + irsin\theta = r(cos\theta + isin\theta)$.

This method of representing the complex number is called polar form. The angle θ is called argument of the complex number, and denoted by $\theta = Arg(z)$, as shown in Figure 11. 5.

The polar form of z facilitates the process of multiplying the complex numbers graphically, as shown in Figure 11.6, where

$z_1 z_2 = r_1(cos\theta_1 + isin\theta_1) \cdot r_2(cos\theta_2 + isin\theta_2) = r_1 r_2(cos(\theta_1 + \theta_2) + isin(\theta_1 + \theta_2))$.

11.7 Euler's Formula

Euler's formula, named after Leonhard Euler, is a mathematical formula in complex analysis that establishes the fundamental

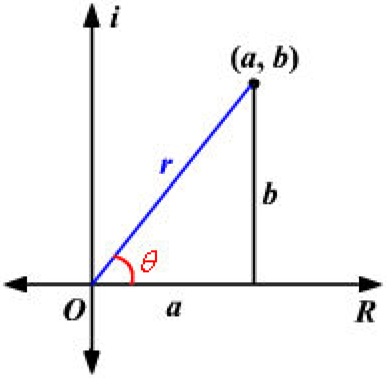


Figure 11.3: Polar Form of z (1)

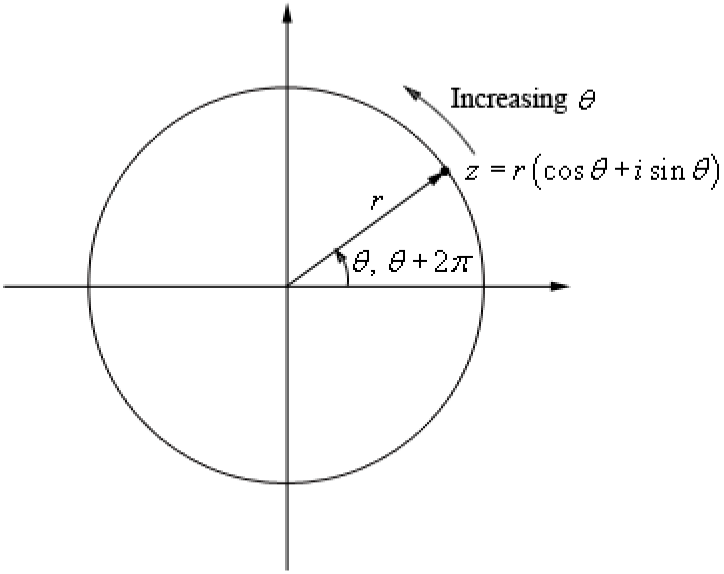


Figure 11.4: Polar Form of z (2)

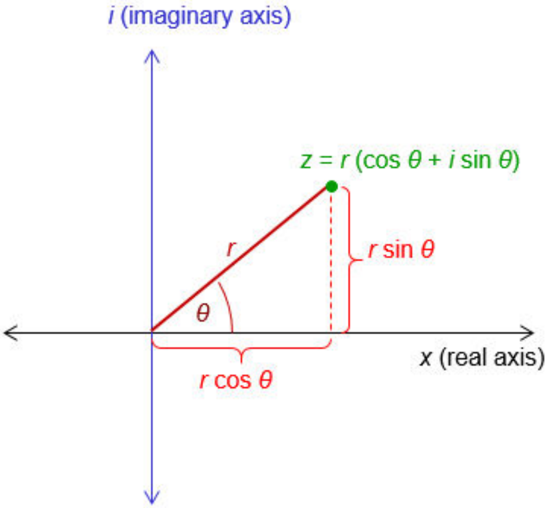


Figure 11.5: Polar Form of z

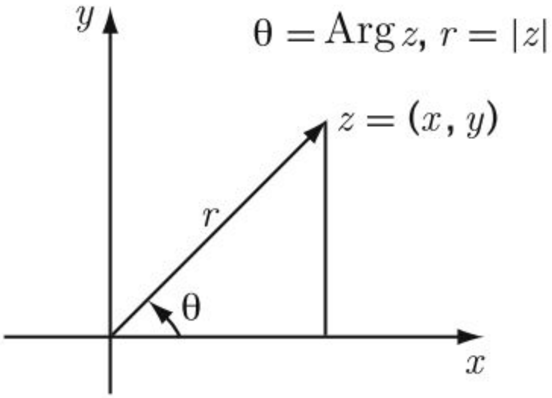


Figure 11.6: Arg z

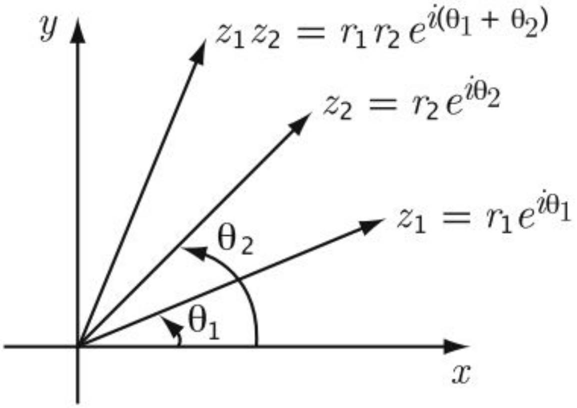

y
$z_1 z_2 = r_1 r_2 e^{i(\theta_1 + \theta_2)}$
$z_2 = r_2 e^{i\theta_2}$
$z_1 = r_1 e^{i\theta_1}$
θ_2
θ_1
x

Figure 11.7: Polar Representation of $z_1 z_2$

relationship between the trigonometric functions and the complex exponential function.

Definition 11.10 Euler's formula states that for any real number θ, there are

(1) $e^{i\theta} = cos\theta + isin\theta$.

(2) $e^{-i\theta} = cos\theta - isin\theta$.

where e is the base of the natural logarithm, i is the imaginary unit, cos, sin are the trigonometric functions cosine and sine respectively (Moskowitz, 2002).

Definition 11.11 If $\theta = \pi$, then Euler's formula evaluates to $e^{i\pi} + 1 = 0$, which is known as Euler's identity (Moskowitz, 2002; Wilson, 2018; Feynman, 1977).

When we consider the Euler's Formula, the result of $z_1 z_2$ becomes $r_1 r_2 e^{i(\theta_1 + \theta_2)}$ as shown in Figure 11.7.

Theorem 11.9 *If z_1, z_2 are complex numbers, then $|z_1 z_2| = |z_1|\,|z_2|$.*

Proof $Arg(z_+ z_2) = Arg(z_1) + Arg(z_2)$.

Let $z_1 = r_1(cos\theta_1 + isin\theta_1), z_2 = r_2(cos\theta_2 + isin\theta_2)$.

$\because z_1 \cdot z_2 = r_1 r_2(cos(\theta_1 + \theta_2) + isin(\theta_1 + \theta_2))$
$\therefore |z_1 z_2| = r_1 r_2 \sqrt{cos^2(\theta_1 + \theta_2) + sin^2(\theta_1 + \theta_2)}$
$= r_1 r_2.$
$\because r_1 = |z_1|, r_2 = |z_2|, \theta_1 = Arg(z_1), \theta_2 = Arg(z_2),$
$\therefore |z_1 z_2| = |z_1| |z_2|.$
$\therefore Arg(z_1 z_2) = \theta_1 + \theta_2 = Arg(z_1) + Arg(z_2)$. ♦

Theorem 11.10 (De Moiver's Theorem)
If $z = r(cos\theta + isin\theta)$, *then* $z^n = r^n(cos(n\theta) + isin(n\theta))$

Proof By using Theorem 10.9, we get
$z^2 = r^2(cos(\theta + \theta) + isin(\theta + \theta)) = r^2(cos(2\theta) + isin(2\theta))$ ...(1)
Now, multiply (1) by z to get
$z^2 \cdot z = z^3 = r^3(cos(2\theta + \theta) + isin(2\theta + \theta))$
$= r^3(cos(3\theta) + isin(3\theta)).$

Continuously this process n times, and by utilizing the mathematical induction, we can prove the theorem is true for all $n \in \mathbb{N}$.

Thus, the theorem is completely proved. ♦

Corollary *If* $w = \mathbb{C} - \{0\}$, *where* $w = r(cos\theta + isin\theta)$, *then*
$\sqrt{w} = \sqrt{r}(cos(\frac{\theta}{n} + \frac{2\pi k}{n}) + isin(\frac{\theta}{n} + \frac{2\pi k}{n})); k = 0, 1, 2, ..., n - 1.$

Proof The proof is left to the reader as exercise. ♦

Definition 11.12 The complex conjugate of a complex number $z = a + ib$ is a complex number $a - ib$, and denoted by $\bar{z}$ (Ledermann, 2013; Andreescu et al., 2006).

Example 11.4 Solve $z^3 = 1$.

Solution. Based on the corollary of De Moiver's Theorem, the complex number $z^3 = 1(cos0 + isin0)$ has three solutions, as the following
$z = cos(\frac{2k\pi}{3}) + isin(\frac{2k\pi}{3}), k = 0, 1, 2.$
$\therefore z = \left\{1, \frac{-1}{2} + i\frac{\sqrt{3}}{2}, \frac{-1}{2} - i\frac{\sqrt{3}}{2}\right\}.$

The following theorem deals with the properties of the conjugates of complex numbers.

Theorem 11.11 *If* $z, w \in \mathbb{C}$, *then*

(1) $\overline{z+w} = \bar{z} + \bar{w}$.

(2) $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$.

(3) $\overline{(\frac{z}{w})} = \frac{\bar{z}}{\bar{w}}; w \neq 0$.

(4) If $z \neq 0$, *then* $z^{-1} = \frac{\bar{z}}{|z|^2}$.

(5) $z = \bar{z}$ *if and only if* $z = a + i0$.

Proof (1) Suppose that $z = a + ib, w = c + id, \forall a, b, c, d \in \mathbb{R}$.

$\because z + w = (a + c) + i(b + d)$,

$\therefore \overline{z + w} = \overline{(a + c) + i(b + d)} = (a+c)-i(b+d) = (a-ib)+(c-id) = \bar{z} + \bar{w}$.

(2) $\because z \cdot w = (ac - bd) + i(ad + bc)$,

$\therefore \overline{zw} = \overline{(ac - bd) + i(ad + bc)} = (ac - bd) - i(ad + bc)$...(i).

On the other hand, $\bar{z} \cdot \bar{w} = (a-ib)(c-id) = (ac-bd)-i(ad+bc)$...(ii).

From (i)& (ii), we get $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$

(3) By utilizing (2), we have

$\bar{w}\overline{(\frac{z}{w})} = \overline{(\frac{wz}{w})} = \bar{z}$.

$\therefore \overline{(\frac{z}{w})} = \frac{\bar{z}}{\bar{w}}$.

(4) $\because z \cdot \bar{z} = (a + ib)(a - ib) = a^2 + b^2 = |z|^2$,

$\therefore z^{-1} = \frac{\bar{z}}{|z|^2}$.

(5) Suppose that $z = \bar{z}$.

$\therefore a + ib = a - ib$,

$\therefore ib = -ib$,

$\therefore (2i) \cdot b = 0$,

$\therefore b = 0$. ⧫

We are going to finish this part with the following theorem. For further research and scientific endeavor, the reader can benefit from other sources such as; (Yaglom, 2014; law, 1990a; Schwerdtfeger, 2020; Hahn, 1994; Olariu, 2002; Meyer, 1979; Spiegel et al., 2009).

Theorem 11.12 *If* $z, w \in \mathbb{C}$, *then*

(1) $\left|\frac{z}{w}\right| = \frac{|z|}{|z|}, w \neq 0$.

(2) $-|z| \leq R(z) \leq |z| \leq R(z)$, $-|z| \leq I(z) \leq |z| \leq R(z)$.

(3) $|\bar{z}| = |z|$.

(4) $|z + w| \leq |z| + |w|$.

(5) $|z - w| \geq ||z| - |w||$.

Proof (1) Based on Theorem 11.11, we find that

$|w|\left|\frac{z}{w}\right| = \left|w\cdot(\frac{z}{w})\right| = |z|$.

$\therefore \left|\frac{z}{w}\right| = \frac{|z|}{|w|}$.

(2) Let $z = a + ib$.

$\because b^2 \geq 0$,

$\therefore -\sqrt{a^2+b^2} \leq a \leq \sqrt{a^2+b^2}$.

$\therefore -|z| \leq R(z) \leq |z|$.

And, for the same reason, we can get that

$-|z| \leq I(z) \leq |z|$.

(3) $|\bar{z}| = \left|\overline{a+ib}\right| = |a-ib| = \sqrt{a^2+(-b)^2} = \sqrt{a^2+b^2} = |z|$.

(4) Based on Theorem 11.11, we can get

$|z+w|^2 = (z+w)\overline{(z+w)} = (z+w)(\bar{z}+\bar{w}) = z\bar{z}+z\bar{w}+w\bar{z}+w\bar{w} = |z|^2+|w|^2+z\bar{w}+w\bar{z} = |z|^2+|w|^2+z\bar{w}+\overline{z\bar{w}}$.

$\because \overline{z\bar{w}} = \bar{z}w$,

$\therefore |z+w|^2 = |z|^2+|w|^2+2R(z\bar{w}) \leq |z|^2+|w|^2+2z\bar{w} = |z|^2+|w|^2+2|z||w| = (|z|+|w|)^2$.

$\therefore |z+w| \leq |z|+|w|$.

(5) By utilizing (4), we have

$|z| = |w+(z-w)| \leq |w|+|z-w|$.

$\therefore |z-w| \geq |z|-|w|$.

Also, $|w| = |z+(w-z)| \leq |z|+|w-z|$...(i).

$\therefore |w-z| \geq |w|-|z| = -(|z|-|w|)$...(ii).

From (i)& (ii), we get

$|z-w| \geq ||z|-|w||$. ♦

Example 11.5 Prove that $\overline{(4+6i)^2/3+2i} = \overline{(4-6i)^2/3-2i}$.

Solution. By utilizing these relations;

$\overline{z^2} = (\bar{z})^2$ and $\overline{(\frac{z}{w})} = \frac{\bar{z}}{\bar{w}}$, we get that

$\overline{(4+6i)^2/3+2i} = (\overline{4+6i})^2/\overline{3+2i} = (4-6i)^2/(3-2i)$.

Example 11.6 If $|z| = 1$, prove that $|\left|\frac{az+b}{\bar{b}z+\bar{a}}\right|, \forall a,b \in \mathbb{C}$.

Solution.

$\because |z| = 1$,

$\therefore z = (\bar{z})^{-1}$.

$\therefore \frac{az+b}{\bar{b}z+\bar{a}} = \frac{az+b}{\bar{b}+\bar{a}\bar{z}}\cdot\frac{1}{z}$.

$$\therefore \left|\frac{az+b}{\bar{b}z+\bar{a}}\right| = \left|\frac{az+b}{\bar{b}+\bar{a}\bar{z}} \cdot \frac{1}{z}\right| = \left|\frac{az+b}{\bar{b}+\bar{a}\bar{z}}\right| \cdot \left|\frac{1}{z}\right| = 1 \ (\overline{az+b} = \bar{a}\bar{z}+\bar{b}).$$

11.8 Exercise

Answer the following questions:

Q1: Prove that:

(1) $\frac{1}{i} = -i$.

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

(3) $\frac{1}{z_1 z_2} = \frac{1}{z_1} \cdot \frac{1}{z_2}$.

(4) $\frac{1}{z_1} + \frac{1}{z_2} = \frac{z_1+z_2}{z_1 z_2}$.

(5) $I(iz) = R(z), R(iz) = -I(z)$.

(6) z is a real number if and only if $R(z) = z$.

Q2: What is the simplest result of the following?

(1) $(1+i)^8$.

(2) $(-i)^{-3}$.

(3) $(1+i)5(1-i)^2$.

(4) $\frac{1+i}{-i}$.

Q3: If $\frac{x-iy}{x+iy} = a+ib$, then prove that $a^2+b^2 = 1$.

Q4: Let $a \in \mathbb{R}, z \in \mathbb{C}$. Prove that $f(az) = ar(z)$. (Hint: In general prove that $f : \mathbb{X} \to \mathbb{R}$ is a linear mapping. Or, $f(az+bw) = af(z)+bf(w), \forall a, b \in \mathbb{R}, z, w \in \mathbb{C}$).

Q5: Iz $f(zw) = f(z) \cdot f(w)$?

Q6: Let $z = xiy \in \mathbb{C}$, and $f_z : \mathbb{C} \to \mathbb{C}$ defined as $f_z(w) = zw, \forall w \in \mathbb{C}$. Prove that $f_{z_1 z_2} = fz_1 \cdot fz_2, \forall z_1, z_2 \in \mathbb{C}$.

Q7: Solve the following equations;

(1)$x^2 = 3-4i$.

(2) $x^4 = i$.

(3) $z^8 = 1$.

Q8: Find each of $R(z), I(z)$ for the following;

(1) $\frac{1}{z^2}$.

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

(3) $\frac{z+1}{2z-1}$.

(4) z^5.

Q9: Prove that the greatest absolute value of z^2+1 on the set $A = \{z : |z| \leq 1\}$ is 2.

Q10: If $w = \sqrt[n]{1}, w \neq 1$ (w is a n^{th} root of unity), then prove that $1 + \sum_{i=1}^{i=n-1} w^i = 0$.

Q11: Let $z = x + iy, w = a + ib$. Prove that

(1)$|x| + |y| \leq \sqrt{2}\,|z|$.

(2) $Arg(\bar{z}) = -Arg(z)$.

(3) $Arg(\frac{z}{w}) = Arg(z) - Arg(w) mod(2\pi)$.

Q12: Find the greatest value of $|z^n + a|$ such that $|z| \leq 1$.

Q13: Prove that $|a - b|^2 + |a + b|^2 = 2(|a|^2 + |b|^2)$.

Bibliography

Ablowitz, M. J., Fokas, A. S. and Fokas, A. S. (2003). *Complex variables: introduction and applications*. Cambridge University Press.

Abramsky, S., Gabbay, D. and Maibaurn, T. (1992). Handbook of logic in computer science. . .

Adachi, M. (1993a). Embeddings and immersions. transl. math. monographs, vol. 124. *Amer. Math. Soc., Providence, RI. MR1225100 (95a: 57039)*. .

Adachi, M. (1993b). Umekomi to hamekomi (embeddings and immersions), translated by k. *Hudson, AMS*. .

Adams, C. C. and Franzosa, R. D. (2008). *Introduction to topology: pure and applied*. number Sirsi) i9780131848696. Pearson Prentice Hall Upper Saddle River.

Ahlfors, L. (1979). Complex analysis mcgraw-hill. *Inc., New York*. .

Alajbegovic, J. and Mockor, J. (2012). *Approximation theorems in commutative algebra: classical and categorical methods*. Vol. 59. Springer Science & Business Media.

Albert, A. A. (1956). *Fundamental concepts of higher algebra*. Vol. 507. University of Chicago Press Chicago.

Aleksandrov, P. S. (1967). *Einführung in die Mengenlehre und die Theorie der reellen Funktionen*. Vol. 23. Deutscher Verlag der Wissenschaften.

Aliprantis, C. D. and Burkinshaw, O. (1998). *Principles of real analysis*. Gulf Professional Publishing.

Andreescu, T., Andrica, D. et al. (2006). *Complex Numbers from A to... Z*. Vol. 165. Springer.

Anton, H. A., De Sesa, B., Black, C., Gregas, M., Grobe, C. A. and Grobe, E. M. (2005). *Elementary linear algebra: student solutions manual*. Wiley.

Anton, H., Bivens, I., Davis, S. and t. Polaski (2010). *Calculus: early transcendentals*. Wiley Hoboken, NJ.

Anton, H. and Rorres, C. (1994). Elementary linear algebra, john wiley & sons. *Inc., Newyork*. .

Antonella, C. (2011). *The Nuts and bolts of proofs: An Introduction to mathematical proofs*. Academic Press.

Apostol, T. (1981). *Mathematical analysis*. Addison-Wesley.

Apostol, T. M. (1974). 'Mathematical analysis addison'.

Apostol, T. M. and Ablow, C. M. (1958). Mathematical analysis. *Physics Today*. 11(7): 32.

Argand, J. R. (1814a). 1815. réflexions sur la nouvelle théorie des imaginaires, suivies d'une application à la démonstration d'un théorème d'analyse. *Annales de Mathématiques Pures et Appliquées (de Gergonne)*. 5: 197–209.

Argand, J. R. (1814b). Réflexions sur la nouvelle théorie d'analyse. In *Annales de Mathématiques*. Vol. 5. 197–209.

Armstrong, M. N. (1997). 'Basic topology, rev. ed'.

Artemov, S. N. (1994). Logic of proofs. *Annals of Pure and Applied Logic.* 67(1-3): 29–59.

Artin, M. (1991). *Algebra.* Prentice Hall, Inc.

Aschbacher, M. (2004). The status of the classification of the finite simple groups. *Notices of the American Mathematical Society.* 51(7): 736–740.

Atiyah, M. F. and Macdonald, I. G. (1969). Introduction to commutative algebra. reading, mass. *Menlo Park, Calif.-London-Don Mills, Ont.: Addison-Wesley Publishing Company.* .

Avelsgaard, C. (1990). *Foundations for Advanced Mathematics.* Scott, Foresman/Little, Brown Higher Education.

Awodey, S. (2010). *Category theory.* Oxford University Press.

Axler, S. (2015). *Linear algebra done right.* Springer.

Axler, S. J. (1997). *Linear algebra done right.* Vol. 2. Springer.

Baader, F. and Nipkow, T. (1999). *Term rewriting and all that.* Cambridge university press.

Balakrishnan, R. and Ramabhadran, N. (1986). *A textbook of modern algebra.* Vikas publishing house PVT Ltd.

Balcerzyk, S. and Józefiak, T. (1989). *Commutative Noetherian and Krull Rings.* Ellis Horwood.

Ballester-Bolinches, A., Esteban-Romero, R. and Asaad, M. (2010). *Products of finite groups.* Vol. 53. Walter de Gruyter.

Bancerek, G. (1989). Sequences of ordinal numbers. *Journal of Formalized Mathematics.* 1.

Bancerek, G. (1990). The fundamental properties of natural numbers. *Formalized Mathematics.* 1(1): 41–46.

Bartle, R. G. and Sherbert, D. R. (2011). *Introduction to real analysis.* Hoboken, NJ: Wiley.

Bartle, R. G. et al. (1976). *The elements of real analysis.* Wiley.

Bartle, R. and Sherbert, D. R. (2000). *Introduction to real analysis.* Vol. 2. Wiley New York.

Bather, J. A. (1994). Mathematical induction. . .

Beachy, J. A. and Blair, B. W. (2006). Abstract algebra , waveland pr. *Inc.* .

Bear, H. S. (1997). *An introduction to mathematical analysis.* Academic Press.

Belegradek, O. (2002). Poly-regular ordered abelian groups. *Contemporary Mathematics.* 302: 101–112.

Bell, J. L. (1993). Hilbert's ϵ-operator in intuitionistic type theories. *Mathematical Logic Quarterly.* 39(1): 323–337.

Bernstein, F. (1905). Untersuchungen aus der mengenlehre. *Mathematische Annalen.* 61(1): 117–155.

Birkhoff, G. (1935). On the structure of abstract algebras. In *Mathematical proceedings of the Cambridge philosophical society.* Vol. 31. Cambridge University Press. 433–454.

Birkhoff, G. (1940). *Lattice theory.* Vol. 25. American Mathematical Soc.

Birkhoff, G. (1967). Lattice theory, colloquium, publications, vol. 25. *New York: American Mathematical Society.* .

Birkhoff, G. and Mac, L. S. (1962). *A survey of modern algebra.* Technical Report.

Birkhoff, G. and Mac, L. S. (2017). *A survey of modern algebra.* CRC Press.

Bittinger, M. L. (1970). Logic and proof. . .

Bittinger, M. L. (1985). Logic, proof, and sets. *Journal of Symbolic Logic*. 50(3).

Blyth, T. S. (1975). *Set theory and abstract algebra*. Longman mathematical texts.

Borgers, A. (1960). Stoll robert r. sets, logic, and axiomatic theories. wh freeman and company, san francisco and london 1961, x+ 206 pp. . .

Bourbaki, N. (1987). Topological vector spaces, elements of mathematics. . .

Bourbaki, N. (1989a). *Algebra: Elements of Mathematics*. Springer-Verlag.

Bourbaki, N. (1989b). *Commutative Algebra: Chapters 1-7*. Springer-Verlag New York.

Bourbaki, N. (1994). Foundations of mathematics; logic; set theory. In *Elements of the History of Mathematics*. Springer. 1–44.

Bourbaki, N. (2003). *Algebra II: Chapters 4-7*. Springer Science & Business Media.

Bourbaki, N. (2004). Theory of sets. In *Theory of Sets*. Springer. 65–129.

Bourbaki, N. (2013). *General Topology: Chapters 1–4*. Vol. 18. Springer Science & Business Media.

Bressoud, D. M. (2007). *A radical approach to real analysis*. Vol. 2. MAA.

Bridges, D. S., S. Douglas, S. et al. (1998). *Foundations of real and abstract analysis*. number 146. Springer Science & Business Media.

Broad, C. D. (1916). Cantor, g.-contributions to the founding of the theory of transfinite numbers. trans. peb jourdain. . .

Browder, A. (2012). *Mathematical analysis: an introduction.* Springer Science & Business Media.

Brown, J. W. and Churchill, R. V. (2009). *Complex variables and applications eighth edition.* McGraw-Hill Book Company.

Brualdi, R. A. (1992). Introductory combinatorics. *New York.* 3.

Bruno, L. C. and Baker, L. W. (1999). *Math & Mathematicians: AH.* Vol. 1. UXL.

Burali-Forti, C. (1897). Una questione sui numeri transfiniti. *Rendiconti del Circolo Matematico di Palermo (1884-1940).* 11(1): 154–164.

Burnside, W. (1911). *Theory of groups of finite order.* University.

Burris, S. and Sankappanavar, H. P. (2006). *A Course in Universal Algebra-With 36 Illustrations.*

Bylinski, C. (1989a). Binary operations. *Journal of Formalized Mathematics.* 1(198): 9.

Bylinski, C. (1989b). Functions from a set to a set. *Journal of Formalized Mathematics.* 1(198): 9.

Cameron, P. J. (2008). *Introduction to algebra.* Oxford University Press on Demand.

Campbell, H. E. (1970). *The structure of arithmetic.* Appleton-Century-Crofts: New York.

Cantor, G. (1878). Ein beitrag zur mannigfaltigkeitslehre. *Journal fur die reine und angewandte Mathematik.* 84: 242–258.

Cantor, G. (1883a). ‘Über unendliche lineare punktmannigfaltigkeiten, 5. grundlagen einer allgemeinen mannigfaltigkeitslehre. ein mathematisch-philosophischer versuch in der lehre des unendlichen’.

Cantor, G. (1883b). Ueber unendliche, lineare punktmannichfaltigkeiten. *Mathematische Annalen.* 21(4): 545–591.

Cantor, G. (1899). Letter to dedekind. . .

Cantrell, C. D. (2000). *Modern mathematical methods for physicists and engineers.* Cambridge University Press.

Carolyn, K. (1981). Concepts associated with the equality symbol. *Educational studies in Mathematics.* 12(3): 317–326.

Carothers, N. L. (2000). *Real analysis.* Cambridge University Press.

Cauman, L. G. (1998). *First order logic: an introduction.* Berlin-New York: Walter de Gruyter.

Celia, H. and Dietmar, K. (2002). Students' understandings of logical implication. *Educational Studies in Mathematics.* 51(3): 193–223.

Chamberlain, R. G. (2007). Great circle distance between 2 points. *web page: www. movable-type. co. uk/scripts/gis-faq-5.1. html.* .

Childs, L. N. (2009). *A concrete introduction to higher algebra.* Springer.

Chowdhury, A. (1970). *Design of an Efficient Multiplier using DBNS.* GIAP Journals.

Christoph, B., Armin, F., Malte, G., Helmut, H., Ivana, K., Manfred, P., Jörg, S., Dimitra, T., Bao Quoc, V. and Magdalena, W. (2003). Tutorial dialogs on mathematical proofs. In *Proceedings of IJCAI-03 Workshop on Knowledge Representation and Automated Reasoning for E-Learning Systems.* 12–22.

Ciesielski, K. et al. (1997). *Set theory for the working mathematician.* Vol. 39. Cambridge University Press.

Cohen, L. W. and Ehrlich, G. (1969). The structure of the real number system. *Journal of Symbolic Logic.* 34(4).

Cohen, P. J. (1964). The independence of the continuum hypothesis, ii. *Proceedings of the National Academy of Sciences of the United States of America*. 51(1): 105.

Cohen, P. J. (2008). *Set theory and the continuum hypothesis*. Courier Corporation.

Cohn, P. M. (2012). *Basic algebra: groups, rings and fields*. Springer Science & Business Media.

Cohn, P. M. and Cohn, P. M. (1981). *Universal algebra*. Vol. 159. Reidel Dordrecht.

Conway, J. H. and Guy, R. (2012). *The book of numbers*. Springer Science & Business Media.

Conway, J. H. and Guy, R. K. (1996). Infinite and Infinitesimal Numbers. In *The Book of Numbers*. Springer. 265–300.

Copi, I. M. (1958). The burali-forti paradox. *Philosophy of Science*. 25(4): 281–286.

Courant, R., Herbert, H. and Stewart, I. (1996). *What is Mathematics?: an elementary approach to ideas and methods*. Oxford University Press, USA.

Crow, J. F. (1993). Felix bernstein and the first human marker locus. *Genetics*. 133(1): 4.

Dalen, D. V. (1998). *Logic and structure*. Springer.

D'angelo, J. P. and West, D. B. (1997). Mathematical thinking. *Problem Solving and Proofs*. .

Daniel, A. and Michael, T. (2002). Research on mathematical proof. In *Advanced mathematical thinking*. Springer. 215–230.

Daniel, G. (2018). Logic and proofs. In *Exploring Mathematics*. Springer. 157–179.

Dasgupta, A. (2014). *Set theory with an introduction to real point sets.* Springer.

Dauben, J. W. (1977). Georg cantor and pope leo xiii: Mathematics, theology, and the infinite. *Journal of the History of Ideas.* 85–108.

Dauben, J. W. (1990). *Georg Cantor: His mathematics and philosophy of the infinite.* Princeton University Press.

Davey, B. A. and Priestley, H. A. (2002). *Introduction to lattices and order.* Cambridge university press.

Dean, R. A. (1967). *Elements of abstract algebra.* John Wiley and Sons.

Dedekind, R. (1901). *Essays on the theory of numbers: I. Continuity and irrational numbers, II. The nature and meaning of numbers.* Open court publishing Company.

Dedekind, R. (1963). 'Essays on the theory of numbers, english translation of dedekind 1888, by berman ww'.

Deiser, O. (2010). On the development of the notion of a cardinal number. *History and Philosophy of Logic.* 31(2): 123–143.

Deskins, W. E. (1995). *Abstract algebra.* Courier Corporation.

Devlin, K. (2003). *Sets, functions, and logic: an introduction to abstract mathematics.* CRC Press.

Devlin, K. J. (2012). *Fundamentals of contemporary set theory.* Springer Science & Business Media.

Di, B. G. and Tamassia, R. (1988). Algorithms for plane representations of acyclic digraphs. *Theoretical Computer Science.* 61(2-3): 175–198.

Dijksterhuis, E. J. (1961). *The mechanization of the world picture.* Vol. 184. JSTOR.

Drake, F. R. (1980). Fundamental of contemprory set theory. *Bulletin of the London Mathematical Society.* 12(6): 480–480.

Dummit, D. S. and Foote, R. M. (2004a). *Abstract algebra*. Vol. 3. Wiley Hoboken.

Dummit, D. S. and Foote, R. M. (2004b). Abstract algebra. john wile & sons. *Inc., Hoboken, NJ.* .

Dummit, D. S. and Foote, R. M. (2004c). Abstract algebra, john wiley&sons. *Inc., Hoboken, NJ.* .

Durbin, J. R. (1992a). Modern algebra, an introduction, john willey & sons. *Inc., NewYork.* .

Durbin, J. R. (1992b). 'Modern algebra an introduction third edition. new york: John willey & sons'.

Dwinger, P. (1971). *Introduction to Boolean algebras*. Physica-Verlag.

Ebbinghaus, H. D., Flum, J. and Thomas, W. (2013). *Mathematical logic*. Springer Science & Business Media.

Eccles, P. J. (1997). *An Introduction to Mathematical Reasoning: numbers, sets and functions*. Cambridge University Press.

Eggen, M., Smith, D. and St, A. R. (2006). A transition to advanced mathematics thomson brooks. *Cole, California.* .

Elliott, M. (2009). *Introduction to mathematical logic*. Chapman and Hall/CRC.

Enderton, H. B. (1977). *Elements of set theory*. Academic press.

Epp, S. S. (2010). *Discrete mathematics with applications*. Cengage learning.

Eric, G. (2009). *Discrete mathematics with proof*. John Wiley & Sons.

Evans, N. (1995). A-quantifiers and scope in mayali. In *Quantification in natural languages*. Springer. 207–270.

Eves, H. and Newsom, C. V. (1958). An introduction to the foundations and funda mental concepts of mathematics. new york: Rinehart & company. *Inc©, i960.* 523.

Eves, H. W. (1963). *A Survey of Geometry.* Allyn and Bacon.

Eves, H. W. (1992). *Fundamentals of modern elementary geometry.* Royal Society of Chemistry.

Feferman, S. (1964). Some applications of the notions of forcing and generic sets. *Fundamenta mathematicae.* 56: 325–345.

Ferreirós, J. (2005). Richard dedekind (1888) and giuseppe peano (1889), booklets on the foundations of arithmetic. In *Landmark Writings in Western Mathematics 1640-1940.* Elsevier. 613–626.

Feynman, R. P. (1977). 'The feynman lectures on physics, vol. 1, chapters 22 and 50'.

Flaška, V., Ježek, J., Kepka, T. and Kortelainen, J. (2007). Transitive closures of binary relations. i.. *Acta Universitatis Carolinae. Mathematica et Physica.* 48(1): 55–69.

Fleming, W. (2012). *Functions of several variables.* Springer Science & Business Media.

Flood, R., Rice, A., Wilson, R. et al. (2011). *Mathematics in Victorian Britain.* Oxford University Press.

Forster, T. (2003). *Logic, induction and sets.* Vol. 56. Cambridge University Press.

Fountain, J. B. (1997). Fundamentals of semigroup theory (london mathematical society monographs, new series 12) by john m. howie: 351 pp.,£ 45.00, lms members' price£ 33.75, isbn 0 19 851194 9 (clarendon press, 1995).. *Bulletin of the London Mathematical Society.* 29(3): 369–381.

Fraenkel, A. A. (1969). Set theory and logic. *Journal of Symbolic Logic.* 34(1).

Fraleigh, J. B. (2003). *A first course in abstract algebra.* Pearson Education India.

Freese, R. (2004). Automated lattice drawing. In *International Conference on Formal Concept Analysis*. Springer. 112–127.

Frobisher, L. (1999). *Learning to teach number: a handbook for students and teachers in the primary school*. Nelson Thornes.

Gallian, J. A. (2006). *Student's Solutions Manual to Accompany: Contemporary Abstract Algebra*. Houghton Mifflin Company.

Gårding, L. and Skau, C. (1994). Niels henrik abel and solvable equations. *Archive for History of Exact Sciences*. 81–103.

Gaughan, E. (2009a). 1.1 sequences and convergence. *Introduction to Analysis. AMS.* .

Gaughan, E. (2009b). *Introduction to analysis*. Vol. 1. American Mathematical Soc.

Gauss, C. F. (1966). *Disquisitiones arithmeticae*. Vol. 157. Yale University Press.

Gauss, C. F. (2006). *Untersuchungen über höhere Arithmetik*. Vol. 191. American Mathematical Soc.

Gilbert, L. (2014). *Elements of modern algebra*. Nelson Education.

Gillispie, C. C., Holmes, F. L. and Koertge, N. (2008). *Complete dictionary of scientific biography*. Charles Scribner's Sons.

Gilmore, P. C. and Hoffman, A. J. (2003). A characterization of comparability graphs and of interval graphs. In *Selected Papers Of Alan J Hoffman: With Commentary*. World Scientific. 65–74.

Givant, S. and Halmos, P. (2008). *Introduction to Boolean algebras*. Springer Science & Business Media.

Gödel, K. (1938). The consistency of the axiom of choice and of the generalized continuum-hypothesis. *Proceedings of the National Academy of Sciences of the United States of America*. 24(12): 556.

Gödel, K. (1947). What is cantor's continuum problem?. *The American Mathematical Monthly*. 54(9): 515–525.

Goldschmidt, R. E. (1964). *Applications of division by convergence*. Massachusetts Institute of Technology: Ph. D. Thesis.

Goodman, F. M. (1998). *Algebra: abstract and concrete*. Prentice Hall.

Graham, R., Knuth, D. and Patashnik, O. (1994). 'Concrete mathematics, second ediction'.

Grassmann, H. (1861). *Lehrbuch der Arithmetik für höhere Lehranstalten*. Th. Chr. Fr. Enslin.

Grattan-Guinness, I. (2009). *Routes of learning: Highways, pathways, and byways in the history of mathematics*. Johns Hopkins University Press.

Grätzer, G. (1979). 'Universal algebra, springer'.

Grätzer, G. (2011). *Lattice theory: foundation*. Springer Science & Business Media.

Grillet, P. A. (2007). *Abstract algebra*. Vol. 242. Springer Science & Business Media.

Grossman, S. I. (1994). *Elementary linear algebra*. Brooks/Cole Publishing Company.

Guinness, I. G. (1971). Towards a biography of georg cantor. *Annals of science*. 27(4): 345–391.

Guinness, I. G. (2000). 'The search for mathematical roots 1870–1940'.

Gunderson, D. S. (2019). *Handbook of mathematical induction: theory and applications*. Chapman and Hall/CRC.

Gutknecht, M. H. (2005). Lineare algebra. *Lecture Notes ETH Zurich*. .

Gwynne, M. (2009). Csm25-the cantor-schröder-bernstein theorem. . .

Hafstrom, J. E. (2013). *Basic concepts in modern mathematics.* Courier Corporation.

Hahn, L. (1994). *Complex numbers and geometry.* Vol. 1. Cambridge University Press.

Hall, G. G. (1967). *Applied group theory (Mathematical Physics).* Elsevier.

Hall, M. (1962). The theory of groups [russian translation]. *Izdat. Inostr. Lit., Moscow.* .

Hall, M. (2018). *The theory of groups.* Courier Dover Publications.

Halmos, P. R. (1958). *Finite dimensional vector spaces.* Princeton: Second edition, D. Van Noetrand Com. Inc.

Halmos, P. R. (2016). *Finite Dimensional Vector Spaces.(AM-7), Volume 7.* Princeton University Press.

Halmos, P. R. (2017a). *Finite-dimensional vector spaces.* Courier Dover Publications.

Halmos, P. R. (2017b). *Naive set theory.* Courier Dover Publications.

Halmos, P. R. and F. D. V. Spaces, F.-D. V. (1987). Undergraduate texts in mathematics. *Finite-Dimensional Vector Spaces.* .

Hamilton, A. G. (1982). *Numbers, sets and axioms: the apparatus of mathematics.* Cambridge University Press.

Hamilton, A. G. (1988). *Logic for mathematicians.* Cambridge University Press.

Hankel, H. (1867). *Vorlesungen über die complexen Zahlen und ihre Functionen: in zwei Theilen.* Voss.

Hardy, D. W., Richman, F. and Walker, C. L. (2011). *Applied algebra: codes, ciphers and discrete algorithms.* CRC Press.

Hardy, G. H., Wright, E. M. et al. (1979). *An introduction to the theory of numbers*. Oxford university press.

Harper, J. M., Rubin, J. E. et al. (1976). Variations of zorn's lemma, principles of cofinality, and hausdorff's maximal principle. i. set forms.. *Notre Dame Journal of Formal Logic*. 17(4): 565–588.

Harzheim, E. (2006). *Ordered sets*. Vol. 7. Springer Science & Business Media.

Hass, J. R., Heil, C. E. and Weir, M. D. (2019). *Thomas' Calculus: Early Transcendentals*. Pearson.

Hasselström, K. (2003). *Fast division of large integers: A comparison of algorithms*.

Hausdorff, F. (1914a). 'Grundzű̋ge der mengenlehre'.

Hausdorff, F. (1914b). *Grundzuge der mengenlehre (leipzig: Veit)*. Technical Report. ISBN 978-0-8284-0061-9.

Hazewinkel, M., Gubareni, N. and Kirichenko, V. V. (2004). *Algebras, rings and modules*. Vol. 1. Springer Science & Business Media.

Henry, P. (1993). A logical framework for modelling legal argument. In *Proceedings of the 4th international conference on Artificial intelligence and law*. ACM. 1–9.

Herstein, I. N. (1964). Topics in algebra. *Algebra. Waltham: Blaisdell Publishing Company.* .

Herstein, I. N. (1975). 'Topics in algebra, lexington, mass'.

Herstein, I. N. (1996). 'Abstract algebra (3rd ed.)'.

Herstein, I. N. (2006). *Topics in algebra*. John Wiley & Sons.

Hinkis, A. (2013). *Proofs of the Cantor-Bernstein Theorem*. Springer.

Hinman, P. G. (2005). *Fundamentals of mathematical logic*. AK Peters/CRC Press.

Holz, M., Steffens, K. and Weitz, E. (2010). *Introduction to cardinal arithmetic*. Birkhäuser.

Howie, J. M. (1995). Fundamentals of semigroup theory, vol. 12 of. *London Mathematical Society Monographs.* .

Hrbacek, K. and Jech, T. (1999). *Introduction to Set Theory, Revised and Expanded*. Crc Press.

Hu, S. T. (1965). *Elements of modern algebra*. Holden-Day.

Humphreys, J. F., Humphreys, J. F. and Liu, Q. (1996). *A course in group theory*. Vol. 6. Oxford University Press on Demand.

Hungerford, T. W. (1974). Algebra. 1974. *Grad. Texts in Math.* .

Hunter, R. H., Arnold, D. M. and Walker, E. (1977). *Abelian Group Theory: Proceedings of the 2nd New Mexico State University Conference, Held at Las Cruces, New Mexico, December 9-12, 1976*. Springer-Verlag.

Ian, S. (1995). *Concepts of modern mathematics*. Courier Corporation.

Ian, S. and David, T. (2015). *The foundations of mathematics*. OUP Oxford.

Itō, K. (1993). *Encyclopedic dictionary of mathematics*. Vol. 1. MIT press.

Jacobson, N. (1951). *Lectures in abstract algebra. Vol. I. Basic concepts*. Princeton, NJ: D. Van Nostrand Co. Inc.

Jacobson, N. (1984). *Structure of rings*. American Mathematical Society.

Jacobson, N. (2009a). 'Basic algebra i. basic algebra'.

Jacobson, N. (2009b). 'Basic algebra i. basic algebra'.

Jacobson, N. (2012). *Basic algebra I*. Courier Corporation.

Jech, T. J. (1977). About the axiom of choice. In *Studies in Logic and the Foundations of Mathematics*. Vol. 90. Elsevier. 345–370.

Jech, T. J. (2008). *The axiom of choice*. Courier Corporation.

Jeffreys, H., Jeffreys, B. and Swirles, B. (1999). *Methods of mathematical physics*. Cambridge university press.

Jónsson, B. (1984). Maximal algebras of binary relations. *Contemporary Mathematics*. 33: 299–307.

Joshi, K. D. (1989). *Foundations of discrete mathematics*. New Age International.

Junghenn, H. D. (2018). *Principles of Analysis: Measure, Integration, Functional Analysis, and Applications*. CRC Press.

Kamke, E. (1950). *Theory of sets*. Courier Corporation.

Kapur, D., Narendran, P. and Zhang, H. (1986). Proof by induction using test sets. In *International Conference on Automated Deduction*. Springer. 99–117.

Kasana, H. S. (2005). *Complex variables: theory and applications*. PHI Learning Pvt. Ltd.

Kelley, J. L. (1955). *General topology, volume 27 of Graduate texts in Mathematics*. New work: Springer-Verlag.

Kelley, J. L. (2017). *General topology*. Courier Dover Publications.

Kirby, L. and Paris, J. (1982). Accessible independence results for peano arithmetic. *Bulletin of the London Mathematical Society*. 14(4): 285–293.

Kist, J. and Leestma, S. (1970). Additive semigroups of positive real numbers. *Mathematische Annalen*. 188(3): 214–218.

Kjos-Hanssen, B., Merkle, W. and Stephan, F. (2011). Kolmogorov complexity and the recursion theorem. *Transactions of the American Mathematical Society*. 363(10): 5465–5480.

Kleene, S. C. (1938). On notation for ordinal numbers. *The Journal of Symbolic Logic*. 3(4): 150–155.

Kleene, S. C. (2002). *Mathematical logic*. Courier Corporation.

Kleiber, M. and Pervin, W. J. (1969). A generalized banach-mazur theorem. *Bulletin of The Australian Mathematical Society*. 1(2): 169–173.

Klein, F. (1974). Le programme d'erlangen. . .

Knapp, A. W. (2007). *Basic algebra*. Springer Science & Business Media.

König, J. (1905). Zum kontinuum-problem. *Mathematische Annalen*. 60(2): 177–180.

Körner, T. W. (2004). *A companion to analysis: a second first and first second course in analysis*. Vol. 62. American Mathematical Soc.

Kroon, F. W. (1986). William s. hatcher. the logical foundations of mathematics. foundations and philosophy of science and technology series. pergamon press, oxford etc. 1982, x+ 320 pp.-william s. hatcher. foundations of mathematics. wb saunders company, philadelphia, london, and toronto, 1968, xiii+ 327 pp.. *The Journal of Symbolic Logic*. 51(2): 467–470.

Kuratowski, K. and Mostowski, A. (1976). 'Set theory, volume 86 of studies in logic and the foundations of mathematics'.

Kurosh, A. G. (2014). *Lectures in general algebra*. Elsevier.

Lajoie, C. and Mura, R. (2000). What's in a name? a learning difficulty in connection with cyclic groups. *For the learning of Mathematics*. 20(3): 29–33.

Lam, T. Y. (1983a). *Orderings, valuations and quadratic forms*. Vol. 52. American Mathematical Soc.

Lam, T. Y. (1983b). Orderings, valuations and quadratic forms, cbms regional conf. ser. math., 52. published for the conf. board of the math. *Sciences, Washington.* .

Landau, H. J. (1987). *Moments in mathematics.* Vol. 37. American Mathematical Soc.

Lane, S. M. and Moerdijk, I. (1992). Sheaves in geometry and logic: A first introduction to topos theory. *New York etc.: Springer-Verlag.* 627: 1992.

Lang, S. (1993a). Algebra, 3rd. *Edition Addison–Wesley.* .

Lang, S. (1993b). *Algebra (Third ed.).* Reading, Mass.: Addison-Wesley Pub. Co.

Lang, S. (1993c). Real and functional analysis. *Grad. Texts in Math.* 142: 396.

Lang, S. (2002a). *Algebra (Third ed.).* Springer-Verlag.

Lang, S. (2002b). *Graduate texts in mathematics: Algebra.* Springer.

Lang, S. (2002c). *Graduate Texts in Mathematics: Algebra.* Springer.

Lang, S. (2004). Algebra, volume 211 of. *Graduate Texts in Mathematics.* 29–30.

Lanski, C. (2005). *Concepts in abstract algebra.* Vol. 14. American Mathematical Soc.

Lass, H. (2009). *Elements of pure and applied mathematics.* Courier Corporation.

law, B. C. (1990a). The complex numbers. *Formalized Mathematics.* 1(3): 507–513.

Law, B. C. (1990b). Functions and their basic properties. *Formalized Mathematics.* 1(1): 55–65.

Lay, D. C. (2005). ‘Linear algebra and its applications, 3rd updated edition’.

Ledermann, W. (1973). Introduction to group theory. . .

Ledermann, W. (2013). *Complex Numbers*. Springer Science & Business Media.

Lenagan, T. H. (1994). Ty lam a first course in noncommutative rings (graduate texts in mathematics 131, springer-verlag, heidelberg1991), xvi+ 397 pp., 3 540 97523 3,£ 35.50.. *Proceedings of the Edinburgh Mathematical Society*. 37(3): 545–545.

Levy, A. (2002). *Basic set theory*. Vol. 13. Courier Corporation.

Liapin, E. S. (1968). *Semigroups*. Vol. 3. American Mathematical Soc.

Lidl, R. and Niederreiter, H. (1997). *Finite fields*. number 20. Cambridge university press.

Lipschutz, S. and Lipson, M. L. (1992). *2000 solved problems in discrete mathematics*. McGraw-Hill.

Lucas, J. F. (1990). *Introduction to abstract mathematics*. Rowman & Littlefield.

Luenberger, D. G. (1997). *Optimization by vector space methods*. John Wiley & Sons.

MacLane, S. and Birkhoff, G. (1999). *Algebra. 1967*. Macmillan, New York.

Maclane, S. and Moerdijk, I. (2012). *Sheaves in geometry and logic: A first introduction to topos theory*. Springer Science & Business Media.

Maddox, R. (2002). *Mathematical thinking and writing: a transition to higher mathematics*. Academic Press.

Mapa, S. K. (2003). *Higher Algebra: Abstract And Linear (revised Ninth Edition)*. Sarat Book Distributors.

Markowsky, G. (1976). Chain-complete posets and directed sets with applications. *Algebra universalis.* 6(1): 53–68.

Marsden, J. E., Hoffman, M. J. et al. (1993). *Elementary classical analysis.* Macmillan.

Martino, I. and Martino, L. (2014). On the variety of linear recurrences and numerical semigroups. In *Semigroup Forum.* Vol. 88. Springer. 569–574.

Marvin, S. (2012). *Dictionary of scientific principles.* John Wiley & Sons.

McCann, M. and Pippenger, N. (2005). Srt division algorithms as dynamical systems. *SIAM Journal on Computing.* 34(6): 1279–1301.

McCoy, N. H. (1968). *Introduction to modern algebra.* Boston: Allyn and Bacon.

Mendelson, E. (1964). Introduction to mathematical logic, d. van nonstrand co. *Inc., Princeton, New Jersey.* .

Mendelson, E. (1973). *Number systems and the foundations of analysis.* Technical Report.

Mendelson, E. (2009a). *Introduction to mathematical logic.* Chapman and Hall/CRC.

Mendelson, E. (2009b). *Introduction to mathematical logic* . CRC press.

Menzel, C. (1984). Cantor and the burali-forti paradox. *The Monist.* 67(1): 92–107.

Meyer, R. M. (1979). Complex variables. In *Essential Mathematics for Applied Fields.* Springer. 319–393.

Miller, G. (2012). *Theory and applications of finite groups.* Applewood Books.

Miller, W. (1973). *Symmetry groups and their applications.* Academic Press.

Milnor, E., Milnor, J., John, M. and Mather, J. N. (1971). *Introduction to algebraic K-theory.* number 72. Princeton University Press.

Monk, J. D. (1973a). *Introduction to set theory.* New work: McGraw Hill Book Company.

Monk, J. D. (1973b). Introduction to set theory. *Journal of Symbolic Logic.* 38(1): 51–151.

Moore, G. H. (2012). *Zermelo's axiom of choice: Its origins, development, and influence.* Courier Corporation.

Moore, G. H. and Garciadiego, A. (1981). Burali-forti's paradox: A reappraisal of its origins. *Historia Mathematica.* 8(3): 319–350.

Morash, R. P. (1987). 'Bridge to abstract mathematics; the handom house'.

Moskowitz, M. A. (2002). *A course in complex analysis in one variable.* World Scientific.

Moskowitz, M. A. and Paliogiannis, F. (2011). *Functions of several real variables.* World Scientific.

Munkres, J. R. (2000). *Topology.* Prentice Hall.

Mustafa, H. J., Naoum, R. S. and Mansour, N. G. (1980). *Foundations of mathematics* . Basrah- Iraq, Vol. I & II (In arabic): University of Basrah.

Nagornyi, N. M. (1971). A. zulauf. the logical and set-theoretical foundations of mathematics. part i. edinburgh, oliver and boyd, 1969, vii+ 259 pp.(book review). *Zhurnal Vychislitel'noi Matematiki i Matematicheskoi Fiziki.* 11(3): 793–793.

Nešetřil, J. (1972). On symmetric and antisymmetric relations. *Monatshefte für Mathematik.* 76(4): 323–327.

Nicholson, W. K. (2012). *Introduction to abstract algebra.* John Wiley & Sons.

Nicolas, B. (1968). 'Elements of mathematics: Theory of sets'.

Nicos, C. (1975). 'Graph theory: An algorithmic approach'.

Nordahl, T. E. and Scheiblich, H. E. (1978). Regular semigroups. In *Semigroup Forum.* Vol. 16. Springer-Verlag. 369–377.

Obermann, S. F. and Flynn, M. J. (1995). *An analysis of division algorithms and implementations.* Technical Report. Technical Report CSL-TR-95-675, Stanford University.

O'Connor, J. J. and Robertson, E. F. (2001). The mactutor history of mathematics archive. *World Wide Web page¡ http://www-history. mcs. st-and. ac. uk/¿(accessed April 22, 2004).* .

Olariu, S. (2002). *Complex numbers in n dimensions.* Elsevier.

Padlewska, B. (1990). Families of sets. *Formalized Mathematics.* 1(1): 147–152.

Palagallo, J. (1991). A transition to advanced mathematics. by douglas smith, maurice eggen, and richard st. andre/foundations for advanced mathematics. by carol avelsgaard/introduction to advanced mathematics. by william barnier and norman feldman. *The American Mathematical Monthly.* 98(2): 179–181.

Paley, H. and Weichsel, P. M. (1966). *A first course in abstract algebra.* Holt, Rinehart and Winston.

Palmer, R. S. (1994). *Chain models and finite element analysis.* Technical Report. Cornell University.

Patrick, S. (1960). 'Axiomatic set theory'.

Patrick, S. (1999). *Introduction to logic* . Courier Corporation.

Peano, G. (1889). The principles of arithmetic. *van Heijenoort.* 1967: 85–97.

Peano, G. (1967). The principles of arithmetic, presented by a new method. *Heijenoort*. 83–97.

Peirce, C. S. (1881). On the logic of number. *American Journal of Mathematics*. 4(1): 85–95.

Pervin, W. J. (1964). *Foundation of general topology.* New York: Academic Press.

Pervin, W. J. (2014). *Foundations of general topology.* Academic Press.

Pinter, C. C. (1976). Set theory. . .

Pinter, C. C. (2014). *A book of set theory.* Courier Corporation.

Plotkin, B. I. and Plotkin, B. J. (1972). *Groups of automorphisms of algebraic systems.* Vol. 8. Wolters Noordhoff Publishing.

Poincaré, H. (1898a). *Des fondements de la géométrie.* Chiron.

Poincaré, H. (1898b). *On the Foundations of Geometry.* Open Court Publishing Company.

Ponnusamy, S. and Silverman, H. (2006). *Complex variables with applications.* Springer.

Poonen, B. (2019). Why all rings should have a 1. *Mathematics Magazine*. 92(1): 58–62.

Puntambekar, A. A. (2007). *Theory Of Automata And Formal Languages.* Technical Publications.

Quine, W. v. (1969). *Set theory and its logic.* Vol. 9. Harvard University Press.

Quine, W. V. O. (2013). *Word and object.* MIT press.

Ramsey, F. P. (1926). The foundations of mathematics. *Proceedings of the London Mathematical Society*. 2(1): 338–384.

Remmel, J. B. (1981). On the effectiveness of the schröder-bernstein theorem. *Proceedings of the American Mathematical Society.* 83(2): 379–386.

Renteln, P. and Dundes, A. (2005). Foolproof: A sampling of mathematical folk humor. *Notices of the AMS.* 52(1): 24–34.

Richmond, B. and Richmond, T. (2004). *A discrete transition to advanced mathematics.* American Mathematical Society.

Robinson, D. J. (2012). *A Course in the Theory of Groups.* Vol. 80. Springer Science & Business Media.

Robinson, J. (1996). *The collected works of Julia Robinson.* Vol. 6. American Mathematical Soc.

Rogers, J. H. (1987). Theory of recursive functions and effective computability. . .

Roitman, J. (1990). *Introduction to modern set theory.* Vol. 8. John Wiley & Sons.

Rosen, K. H. and Krithivasan, K. (2012). *Discrete mathematics and its applications: with combinatorics and graph theory.* Tata McGraw-Hill Education.

Rosser, B. (1942). The burali-forti paradox. *The Journal of Symbolic Logic.* 7(1): 1–17.

Rosser, J. B. (2008). *Logic for mathematicians.* Courier Dover Publications.

Roth, R. L. (2001). A history of lagrange's theorem on groups. *Mathematics Magazine.* 74(2): 99–108.

Rotman, J. J. (1973). The theory of groups: An introduction. . .

Rotman, J. J. (2000). *A first course in abstract algebra.* Pearson College Division.

Rotman, J. J. (2010). *Advanced modern algebra.* Vol. 114. American Mathematical Soc.

Rotman, J. J. (2012). *An introduction to the theory of groups.* Vol. 148. Springer Science & Business Media.

Rotman, J. J. (2013). *First Course in Abstract Algebra: with Applications.* Prentice Hall PTR.

Rubin, H. and Rubin, J. E. (1985). *Equivalents of the Axiom of Choice, II.* Vol. 116. Elsevier.

Rubin, J. E. (1967). *Set theory for the mathematician.* Holden-Day.

Rucker, R. (2013). *Infinity and the mind: The science and philosophy of the infinite.* Vol. 26. Princeton University Press.

Rudin, W. (1953). Principles of mathematical analysis.(1964.) mcgraw-hill. *New York.* .

Rudin, W. (1991). Functional analysis 2nd ed. *International Series in Pure and Applied Mathematics. McGraw-Hill, Inc., New York.* 10.

Rudin, W. et al. (1976). *Principles of mathematical analysis.* Vol. 3. McGraw-hill New York.

Russell, B. (1980). Correspondence with frege. *Philosophical and mathematical correspondence.* 130–170.

Saff, E. B. and Snider, A. D. (1993). *Fundamentals of complex analysis for mathematics, science, and engineering.* Prentice Hall.

Sándor, D. (2008). Mathematics basics. In *the modern algebra of information retrieval.* Springer. 27–44.

Saunders, M. and Garrett, B. (1967). *Algebra.* AMS Chelsea.

Saunders, M. L. and Birkhoff, B. (1999). *Algebra: Third Edition.* American Mathematical Society. Providence, Rhode, Island.

Saunders, M. L. and Birkhoff, G. (1967). *Algebra (First ed.)*. New York: Macmillan.

Schechter, E. (1996). *Handbook of Analysis and its Foundations*. Academic Press.

Scheinerman, E. R. (2000). 'Mathematics: A discrete introduction, brooks'.

Scheinerman, E. R. (2012). *Mathematics: a discrete introduction*. Nelson Education.

Schmidt, G. (2010). 'Relational mathematics (encyclopedia of mathematics and its applications)'.

Schmidt, G. (2011). *Relational mathematics*. number 132. Cambridge University Press.

Schmidt, S. (1993). 93. g. schmidt, t. ströhlein: Relations and graphs. *Discrete Mathematics for Computer Scientists. EATCS Monographs on Theoretical Computer Science. Berlin: Springer.* .

Schröder, B. S. (2003). *Ordered sets*. Springer.

Schwerdtfeger, H. (2020). *Geometry of complex numbers*. University of Toronto Press.

Scott, D. (1967). 'Axiomatizing set theory "symposium in pure mathematics" los angeles'.

Scott, W. R. (1987). 'Group theory'.

Scott, W. R. (2012). *Group theory*. Courier Corporation.

Shan-Hwei, N., RJ, V. P. and Leendert, V. T. (1993). Constructing refinement operators by decomposing logical implication. In *Congress of the Italian Association for Artificial Intelligence*. Springer. 178–189.

Sharma, A. (2006). *Theory of automata and formal languages*. Firewall Media.

Sharpe, D. (1987). *Rings and factorization.* CUP Archive.

Shelah, S. (2000). The generalized continuum hypothesis revisited. *Israel Journal of Mathematics.* 116(1): 285–321.

Shen, S., Vereshchagin, N. K. and Shen, A. (2002). *Basic set theory.* number 17. American Mathematical Soc.

Shilnikov, L. P. (1967). On a poincaré–birkhoff problem. *Matematicheskii Sbornik.* 116(3): 378–397.

Sierpiński, W. (1958). *Cardinal and ordinal numbers.* Vol. 1958. Warszawa.

Sikka, H. (2017). Complex numbers: Its operations and properties. . .

Simmons, G. F. and Hammitt, J. K. (1963). *Introduction to topology and modern analysis.* McGraw-Hill New York.

Simovici, D. A. and Djeraba, C. (2008). Partially ordered sets. In *Mathematical Tools for Data Mining.* Springer. 129–172.

Smith, D. E. and Karpinski, L. C. (1911). Book review: The hindu-arabic numerals, by david eugene smith and louis charles karpinski. *Popular Astronomy.* 19: 662.

Smith, J. D. H. (2015). *Introduction to abstract algebra.* Vol. 31. CRC Press.

Smith, P. (1975). Bourbaki nicolas. theory of sets. elements of mathematics. english translation of xxxvii 636, xl 289. hermann, publishers in arts and science, paris, and addison-wesley publishing company, reading, mass., menlo park, calif., london, don mills, ontario, 1968, viii+ 414 pp. . .

Smullyan, R. (1996). Set theory and the continuum problem. . .

Spanier, J. (1987). ‘Oldham, kb: An atlas of functions’.

Spiegel, M. R., Lipschutz, S., Schiller, J. J. and d. Spellman (2009). *Schaum’s outline of Complex Variables.* McGraw Hill Professional.

Spivak, M. (1975). *A comprehensive introduction to differential geometry*. Vol. 5. Publish or Perish, Incorporated.

Steen, L. A., Seebach, J. A. and Steen, L. A. (1978). *Counterexamples in topology*. Vol. 18. Springer.

Stewart, I. N. (2015). *Galois theory*. CRC Press.

Stewart, J. (2009). *Calculus: Concepts and contexts*. Cengage Learning.

Stoll, R. R. (1960). Sets, logic, and axiomatic theories. *Journal of Symbolic Logic*. 25(3): 278–279.

Stoll, R. R. (1979). *Set theory and logic*. Courier Corporation.

Strang, G. (2006). Linear algebra and its applications. 4th. *Brooks Cole*. .

Suppes, P. (1960). *Axiomatic set theory*. New York: Courier Corporation.

Suppes, P. (1972). *Axiomatic set theory*. Courier Corporation.

Suppes, P. (1999). *Introduction to logic*. Courier Corporation.

Szmielew, W. (1959). Elementary properties of abelian groups. . .

Takeuti, G. and Zaring, W. M. (2013). *Axiomatic set theory*. Vol. 8. Springer Science & Business Media.

Tanton, J. (2005). *Encyclopedia of mathematics*. Facts On File, inc.

Tarski, A. (1941). 1994. *Introduction to Logic and to the Methodology of Deductive Sciences*. .

Tarski, A. and Givant, S. R. (1987). *A formalization of set theory without variables*. Vol. 41. American Mathematical Society.

Taton, R. (1972). Servois. *Dictionary of Scientific Biography*. 325–326.

Temirovna, O. L. (2021). Equation, identities, equivalent equation, equation with one unknown of the first order, fractional rational equations and their solution. In *Archive of Conferences.* 103–106.

Thomas, G. B., Weir, M. D., Hass, J. and Giordano, F. R. (2010). *Thomas' calculus.* Pearson Boston.

Thomas, J. G. B., Weir, M. D., Hass, J., Heil, C. and Edition, T. (2014). Early transcendentals. . .

Tignol, J. P. (2015). *Galois' theory of algebraic equations.* World Scientific Publishing Company.

Treves, F. (1967). Topological vector spaces, distributions and kernels, acad. *Press, New York.* .

Troelstra, A. S. and Dalen, D. V. (1988). *Constructivism in mathematics I, II* . Amsterdam: North Holland publ. Co.

Trope, Y. and Liberman, N. (2010). Construal-level theory of psychological distance.. *Psychological review.* 117(2): 440.

Trotter, W. T. (1992). *Combinatorics and partially ordered sets: Dimension theory.* Vol. 59. Johns Hopkins University Press Baltimore.

Trybulec, A. (1989). Tarski grothendieck set theory. *Journal of Formalized Mathematics.* 1.

Uri, L. (1983). Structuring mathematical proofs. *The American Mathematical Monthly.* 90(3): 174–185.

Van der Waerden, B. L., Artin, E. and Noether, E. (1950). *Moderne algebra.* Vol. 31950. Springer.

Van, H. J. (1967). *From Frege to Gödel: a source book in mathematical logic, 1879-1931.* Vol. 9. Harvard University Press.

Vander Waerden, B. L. (1949). *Modern Algebra [Translated from the second revised German edition], Vol. II.* New York: Frederick Ungar Publishing Co.

Varberg, D. E. and Purcell, E. J. (1992). *Calculus with Analytic Geometry.* Prentice Hall.

Velleman, D. J. (2006). *How to prove it: A structured approach.* Cambridge University Press.

Vinberg, Ė. B. (2003). *A course in algebra.* number 56. American Mathematical Soc.

Vinogradov, I. M. (2016). *Elements of number theory.* Courier Dover Publications.

Wallace, D. A. (2012). *Groups, rings and fields.* Springer Science & Business Media.

Walton, D. N. (1990). What is reasoning? what is an argument?. *The Journal of Philosophy.* 87(8): 399–419.

Warner, S. (1965). *Modern algebra.* Dover Publications, Inc.

Warner, S. (1990). *Modern algebra.* Courier Corporation.

Weisstein, E. W. (1999a). Crc concise encyclopedia of mathematics (crc). . .

Weisstein, E. W. (1999b). Vector space. *Math World–A Wolfram Web Resource.* .

Weisstein, E. W. (2000). Countably infinite. . .

Weisstein, E. W. (2002a). *CRC concise encyclopedia of mathematics.* CRC press.

Weisstein, E. W. (2002b). Division algebra. *https://mathworld. wolfram. com/.* .

Weisstein, E. W. (2002c). Egyptian fraction. *https://mathworld. wolfram. com/.* .

Weisstein, E. W. (2002d). Finite set. . .

Weisstein, E. W. (2002e). Multiplicative identity. . .

Weisstein, E. W. (2002f). Ring. . .

Weisstein, E. W. (2003a). Complex number. *https://mathworld. wolfram. com/.* .

Weisstein, E. W. (2003b). Zero. *https://mathworld. wolfram. com/.* .

Weisstein, E. W. (2019). Cardinal number. *V: MathWorld–A Wolfram Web Resource. Retrieved.* 15(2).

Weisstein, E. W. et al. (2004). 'Mathworld–a wolfram web resource'.

Wilder, R. L. (1952). *Introduction to the foundations of mathematics.* New York : John Wiley & Sons, Inc. ; London : Chapman & Hall, Limited.

Wilder, R. L. et al. (2012). *Introduction to the Foundations of Mathematics.* Courier Corporation.

Willard, S. (2004). *General topology.* Courier Corporation.

Wilson, R. (2018). *Euler's Pioneering Equation: The most beautiful theorem in mathematics.* Oxford University Press.

Wolf, R. S. (1998). *Proof, Logic, and Conjecture: The Mathematician's Toolbox.* St. Martin's Press.

Wussing, H. (2007). *The genesis of the abstract group concept: a contribution to the history of the origin of abstract group theory.* Courier Corporation.

Yaglom, I. M. (2014). *Complex numbers in geometry.* Academic Press.

Zariski, O. and Samuel, P. (1958). Commutative algebra, v1. *New York.* .

Zariski, O. and Samuel, P. (2013). *Commutative algebra: Volume II.* Vol. 29. Springer Science & Business Media.

Zermelo, E. (1904). Beweis, daß jede menge wohlgeordnet werden kann. *Mathematische Annalen.* 59(4): 514–516.

Zermelo, E. (1908). Untersuchungen über die grundlagen der mengenlehre. i. *Mathematische Annalen.* 65(2): 261–281.

Zermelo, E. (1930a). Uber grenzzahlen und mengenbereiche: Neue untersuchungen äuber die grundlagen der mengenlehre. *Fundamenta mathematicae.* .

Zermelo, E. (1930b). Uber grenzzahlen und mengenbereiche: neue untersuchungen über die grundlagender mengenlehre. *Fundamenta Mathematicae.* 14: 339–344.

Zulauf, A. (1969a). *The logical and set-theoretical foundations of mathematics.* Edinburgh, Oliver and Boyd.

Zulauf, A. (1969b). *The Logical and Set-Theoretical Foundations of Mathematics: Part One of a Modern Introduction to Pure Mathematics.* Oliver and Boyd.

Index