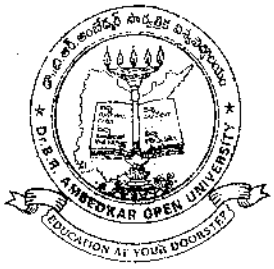
MATHEMATICS

Algebra & Analysis



Dr. B.R. AMBEDKAR OPEN UNIVERSITY
HYDERABAD
1996

Course Team

Editors

Prof. D. Rama Kotaiah
Prof. R. Sitarama Swamy

Associate Editors

Prof. K. Kuppuswamy Rao
Dr. N. Venkata Narayana

Writers

Sri. P.V. Krishnaiah
Dr. K. Kuppuswamy Rao
Sri. K. Munaswamy Reddy
Dr. I. H. Nagaraja Rao
Dr. K.N. Venkatasiva Murthy

Cover Design

Ramesh

Dr. B.R. Ambedkar Open University
Hyderabad.

First Published 1986
Reprint 1993

Further information on Open University Courses may be obtained from the Director (Academic)

Dr. B.R. Ambedkar Open University, Somajiguda, Hyderabad - 500 482.

Printed at Deepu Printers, Raghavaratna Towers, Hyderabad - 500 001.

PREFACE

This book deals with the topics in Algebra and Analysis included in the syllabus for the Third year of B.Sc. Course offered by the Andhra Pradesh Open University. These topics generally cover the advanced area of the subject to be studied in the Third year of the three year Degree Course in Science. The syllabus for the sake of conveience is divided into Blocks each of which comprises of numbers of units. Each Block generally covers a specific area of the subject. The units are prepard by specialists in accordance with a format so designed as to enable the student to read and understand them without much difficulty.

The book is divided into two parts. Part-I deals with algebra and part-2 with Analysis. In Algebra the topics of groups, rings and fields are dealt with. Algebra can be viewed as the study of structures. Groups and rings are structures that deal with one and two binary operations respectively. The study of groups and rings form the core of modern study of of mathematics. Apart from their own intrinsic interest they have applications in other branches of sciences and arts.

In recent years the study of analysis has become central in the study of Mathematics. Every effort is made to present the treatment rigour. This should help the student to develop analytical thinking and at the same time logical approach to problems. Analysis should not be any more as a tool but as a subject in its own right.

The University hopes that the course material will help the student to get acquainted with the concepts and principles of Algebra and Analysis.

contents

			Page
Block - 1	:	**Theory of Groups**	**1-70**
Unit1	:	Sets, Relations and Functions	1
Unit 2	:	Groups	13
Unit 3	:	Subgroups	23
Unit 4	:	Some interesting groups and subgroups	33
Unit 5	:	Normal Subgroups & Quotient groups	49
Unit 6	:	Homomorphism Theorems and Consequences	61
Block - 2	:	**Rings and Vector Spaces**	**71-114**
Unit 7	:	Rings and Subrings	73
Unit 8	:	Integral domains and fields	83
Unit 9	:	Ideals and quotient rings	93
Unit 10	:	Vector Spaces	101
Block - 3	:	**Real Number System**	**115-142**
Unit 11	:	Aigebraic properties of real numbers	116
Unit 12	:	Completeness properties of real number	127
Unit 13	:	Open sets and closed sets	135
Block - 4	:	**Sequences and Series**	**143-192**
Unit 14	:	Sequences	145
Unit 15	:	Infinite Series I	161
Unit 16	:	Infinite Series II	179
Block - 5	:	**Continuous Functions**	**193-220**
Unit 17	:	Limit of Function	195
Unit 18	:	Properties of continuous functions	205
Unit 19	:	Uniform continuity	215
Block - 6	:	**Differentiability and Integrebility**	**221-305**
Unit 20	:	Differentiability of Functions	223
Unit 21	:	Mean Value Theorem	237
Unit 22	:	Taylor's Theorem and Applications	251
Unit 23	:	Rieman Integrability	271
Unit 24	:	The Fundamental Theorem of Integration	297

BLOCK–1 : THEORY OF GROUPS

Unit–1 : Sets, Relations and Functions

Unit–2 : Groups

Unit–3 : Subgroups

Unit–4 : Some interesting Groups and Subgroups

Unit–5 : Normal Subgroups and Quotient groups

Unit–6 : Homomorphism Theorems and Consequences

The word algebra is derived from the word al-jabr from the book of the Persian mathematician Mohammed Al-Khowarizimi during the 9th century. Till the beginning of 19th Century algebra confined itself to searching solutions to equations. Today such kind of algebra is referred to as classical algebra by many. The term Modern Algebra (or Abstract Algebra) refers to investigations in classical algebra when the operations are extended to members of sets' and are not strictly confined to 'numbers' alone. The word Abstract algebra refers to the study of systems that are defined by axioms (postulates) with no meaning attributed to elements of the systems.

The notion of a group arises in divergent investigations. A group is a non empty set together with a binary operation and obeying certain axioms. The theory of groups has rich history and is an actively pursued research area in mathematics. Many of the problems still unsolved in this area require deep results in other branches of mathematics and open up new branches of study. Groups have applications in other branches of study. Physicists and chemists study groups to know answers to problems in crystollography and symmetries of solids.

UNIT–1 : SETS, RELATIONS AND FUNCTIONS

Contents

1.1 Aims and Objectives

1.2 Introduction

1.3 Algebra of sets

1.4 Relations

1.5 Functions

1.6 Summary

1.7 Model Examination Questions

1.8 Answers to Self Assessment Questions

1.9 Reference books

1.1 AIMS AND OBJECTIVES

After reading this unit you should be able to : (i) Recognise the set operations, (ii) Distinguish between various relations, (iii) Investigate whether a given function is one to one or onto or both or none, (iv) Perform various operations with functions.

1.2 INTRODUCTION

Towards the end of the nineteenth century the German Mathematician George Cantor developed a new branch of Mathematics called 'Set Theory'. It was later discovered that it is possible to deduce all known mathematics from a list of axioms about the sets. Formal study of set theory is a separate branch of Mathematics. Here we will use set theory as a convenient language to state algebraic results.

Mathematics deals with several different kinds of collections of objects. For example : Collection of points on a line or collection of all positive integers less than 100 or collection of all rational numbers between 0 and 1 etc. These are all typical examples of sets. We do not intend to formally define the term "set" but accept the term as undefined. But we know, without any ambiguity, whether or not a given object belongs to the "set" under consideration. We explain that a set is the collection of well defined objects. The collection of some positive integers does not constitute a set because the term "some positive integers" is not well defined since given a positive integer 10, it is not possible to tell wether 10 belongs to the collection of "some positive integers" or not.

It is customary to denote sets by capital letters and the objects (elements) of the set by small letters. If an element 'a' belongs to a set A, we write $a \in A$. If the element 'b' does not belong to the set A we write $b \notin A$. If A is a set, we can display all the elements of A or state clearly the property which makes an element belong to the set or not. For example, the set A of vowels of the English alphabet can be written as :

$A = \{a, e, i, o, u\}$ or $A = \{x / x \text{ is a vowel of English alphabet}\}$. Thus $b \notin A$ because b is not a vowel.

$B = \{1, 3, 5, \ldots\} = \{x / x$ is an odd positive integer$\}$. The set not consisting of any elements is called a "Null set" or an "empty set" and is denoted by ϕ. For example the set of real roots of the equation $x^2 + 1 = 0$ is an empty set.

SAQ 1 Which of the following is an empty set and why ?

(A) $\{0\}$, (B) $\{x / x$ is positive and $x + 1 = 0\}$, (c) $\{\phi\}$,

Subsets : If A and B are two sets such that every element of A is an element of B, then we say A is a subset of B and write as $A \subseteq B$. If A is a subset of B and B has atleast one element which is not in A, then A is called a proper subset of B and write $A \subset B$. Two sets A and B are said to be equal if $A \subseteq B$ and $B \subseteq A$.

Example : If $A = \{x / x$ is a non negative even integer$\} = \{0, 2, 4, 6, 8, \ldots\}$

and $B = \{x / x$ is a non negative integer$\}$

$= \{0, 1, 2, 3, 4, 5, \ldots\}$,

then A is a proper subset of B.

Example : $A = \{1, 2, 3, 4,\}$ and

$B = \{1, 2, 2, 2, 3, 3, 4, 4, 4, 1, 4\}$,

then $A \subseteq B$ because every element of A is in B. Further $B \subseteq A$ because every element of B is in A.

Therefore, A = B. Notice that the number of elements in a set is not a criterion to judge the equality of sets.

Example : ϕ is a subset of every set. To see this let us argue in the following way. ϕ will not be a subset of any non empty set if we could produce atleast one element of ϕ which is not in A. But ϕ is empty and hence has no element in it. Since we could not produce any element of ϕ which is not in A, we conclude, that ϕ is a proper subset of A.

Definition

> Let S be a set. The set of all subsets of S is called the power set of S. The power set of S written as $P(S) = \{A / A \subseteq S\}$. If S has a finite number of elements say n, then the number of elements in P (S) is 2^n.

SAQ 2 If $S = \{1, 2, 3\}$ write P (S)

SAQ 3 If $A = \{x / x^4 = 1\}$, $B = \{1, -1, i, -i\}$ which of the following are correct ?

(a) $A \subset B$ (b) $A = B$ (c) $A \subseteq B$ (d) A is not a subset of B.

1.3 ALGEBRA OF SETS

If $\{A, B, C, \ldots\}$ is a collection of sets, we can conbine these sets to form new sets. This is similar to the algebra we learnt in our earlier classes using numbers. Recall that the operations of "addition" (subtraction) multiplication (division) of Natural numbers resulted in negative integers, rational numbers etc and gave a rich variety of different new numbers from the existing numbers. We attempt a similar procedure here.

If A and B are two sets, we define the Union of A and B as another set whose elements belong to either A or B. We write this as

$$A \cup B = \{x / x \in A \text{ or } x \in B\}.$$

Similarly the intersection of the two sets A and B is defined as another set whose elements are common to A and B. We write this as

$$A \cap B = \{x / x \in A \text{ and } x \in B\}.$$

Two sets A and B are said to be disjoint if $A \cap B = \phi$.

Example : If $A = \{a, b, c, d, e, f, g, h, i\}$ and $B = \{d, e, g, h, i\}$

then $A \cup B = \{a, b, c, d, e, f, g, h, i\}$ and

$A \cap B = \{d, e, g, h, i\}$

Example : $A \cup \phi = A$; $A \cap \phi = \phi$; $A \cup A = A$ and $A \cap A = A$.

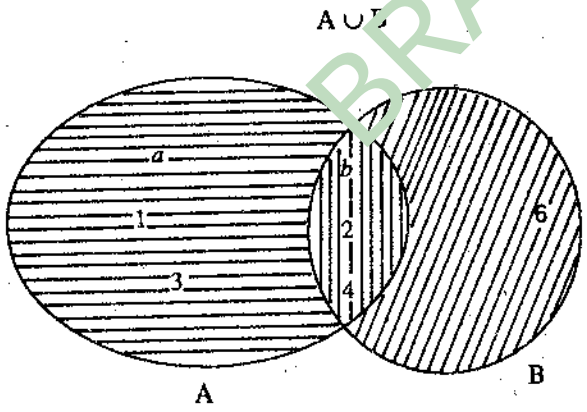
If A and B are two sets, then the difference of the sets A and B, written as A – B, is the set of elements of A which are not in B. This is written as $A - B = \{x / x \in A \text{ and } x \notin B\}$.

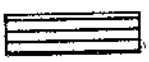
Example : If $A = \{a, b, 1, 2, 3, 4\}$ and $B = \{b, 2, 4, 6\}$

then $A - B = \{a, 1, 3\}$.

$B - A = \{6\}$.

To readily understand these concepts we represent these operations through Venn diagrams.



A – B =  $A \cap B$ =  B – A = 

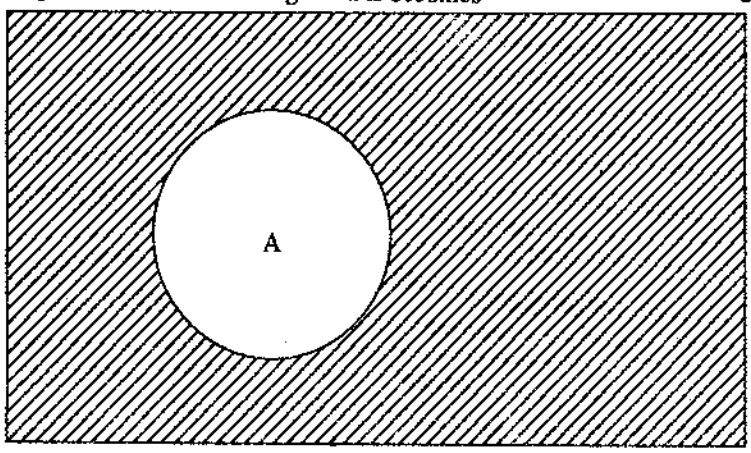
SAQ 4 If $A = \{a, b, c, 1, 2, 3\}$ and $B = \{b, 2\}$, write

(i) $A \cup B$; (ii) $A \cap B$; (iii) $A - (A \cap B)$; (iv) $A - B$.

We have seen that an empty set is the set consisting of no elements. Similarly a universal set is defined to be a set in which every other set is a subset of it. If we denote the set of integers by Z, the set of rational numbers by Q, then these two sets are the subsets of the universal set of Real numbers **R**. It is customary to denote the universal set by U. If A is any set which is a subset of the universal set, then U – A is called the complement of A and is denoted by A'. It is easy to see that

$$A' = \{x / x \in U \text{ and } x \notin A\}$$

Represented in a Venn diagram this becomes U



 $= A'$

Clearly $A \cup A' = U$.

SAQ 5 Let $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ and $A = \{1, 3, 5, 7, 9\}$. Write A'.

It is easy to see that the set operations "set union" and "set intersection" are associative as well as commutative. That is

$$A \cup (B \cup C) = (A \cup B) \cup C ; A \cup B = B \cup A.$$

and $$A \cap (B \cap C) = (A \cap B) \cap C ; A \cap B = B \cap A.$$

The proofs of these statements are left to the student as an exercise.

Theorem 1 :

> The set operation of "Union" is distributive over the set operation "intersection" and the set operation "intersection" is distributive over "Union".
>
> That is : (i) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and
>
> (ii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof : $A \cup (B \cap C) = \{x \mid x \in A \text{ or } x \in B \cap C\}$

$= \{x \mid x \in A \text{ or } x \in B \text{ and } x \in A \text{ or } x \in C\}$

$= \{x \mid x \in A \cup B \text{ and } x \in A \cup C\}$

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

$A \cap (B \cup C) = \{x \mid x \in A \text{ and } x \in B \cup C\}$

$= \{x \mid x \in A \text{ and } x \in B \text{ or } x \in A \text{ and } x \in C\}$

$= \{x \mid x \in A \cap B \text{ or } x \in A \cap C\}$

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

Theorem 2 (De Morgan's laws) :

> If A, B, C are any three sets,
>
> Then (i) $A - (B \cup C) = (A - B) \cap (A - C)$.
> (ii) $A - (B \cap C) = (A - B) \cup (A - C)$

Proof : $A - (B \cup C) = \{x \mid x \in A \text{ and } x \notin B \cup C\}$

$= \{x \mid x \in A \text{ and either } x \notin B \text{ or } x \notin C\}$

$= \{x \mid x \in A, x \notin B \text{ and } x \in A, x \notin C\}$

$= \{x \mid x \in A - B \text{ and } x \in A - C\}$

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

$A - (B \cap C) = \{x \mid x \in A \text{ and } x \notin B \cap C\}$

$= \{x \mid x \in A \text{ and } x \notin B \text{ and } x \notin C\}$

$= \{x \mid x \in A - B \text{ or } x \in A - C\}$

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

Corollary : As a particular case when A is the universal set, these laws become

(i) $U - (B \cup C) = (U - B) \cap (U - C)$

That is $(B \cup C)' = B' \cap C'$,

(ii) $U - (B \cap C) = (U - B) \cup (U - C)$

That is $(B \cap C)' = B' \cup C'$.

SAQ 6 Let $U = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$,

$A = \{0, 2, 4, 6, 8, 10\}$; $B = \{1, 3, 5, 7\}$

Verify de Morgan's laws.

Remark : Notice that the above laws of unions and intersections of sets is valid even if we consider more than two sets.

1.4 RELATIONS

Let A and B be two sets. The Cartesian Product of A and B is defined as the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$. The Cartesian Product of A and B is written as $A \times B$. The Cartesian Product of B and A is written as $B \times A$ and need not be same as $A \times B$.

Example : If $A = \{1, 2, 3\}$; $B = \{a, b\}$, then

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

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

Intuitively the Cartesian Product $R \times R$ corresponds to the coordinate plane in analytic geometry where each ordered pair (a, b) corresponds to a point in the plane, whose abscissa is a and whose ordinate is b.

SAQ 7 If $A = \{a, b, c, d\}$, write $A \times A$.

Let A and B be two non-empty sets. Any subset of $A \times B$ is called a *relation* from A to B. Since $A \times B$ and $B \times A$ need not be the same, a relation from A to B need not be a relation from B to A. If B = A, then $A \times A$ is called a binary relation.

If either A or B is the empty set then $A \times B = \phi$. If $(a, b) \in A \times B$, we say a is related to b and write $a \, R \, b$. Then a relation R can be written as

$$R = \{(a, b) : a \, R \, b\} \subset A \times B.$$

If $R \subset A \times B$, then $R^{-1} = \{(b, a) \mid a \, R \, b\}$ is called an inverse relation. Then if R denotes a relation from A to B, R^{-1} denotes a relation from B to A.

A relation $R \subset A \times A$, such that $a \, R \, a$, for every $a \in A$ is called a *reflexive relation.*

A relation $R \subset A \times A$ such that $a \, R \, b$ implies $b \, R \, a$ for every (a, b) in R is called a *symmetric relation.*

A relation $R \subset A \times B$ such that $a \, R \, b$ and $b \, R \, c$ implies $a \, R \, c$ is called a *transitive relation.*

A binary relation defined on A is called an equivalence relation if it satisfies the reflexive, symmetric and transitive properties.

Example : Let N be the set of positive integers and let a relation "is less than" be defined on N. Then this relation is not reflexive on N and is not symmetric on N but is only transitive. This is because (i) if a is a positive integer, then it is wrong to write $a < a$, (ii) if a and b are two positive integers such that $a < b$ then we can not say that $b < a$, (iii) where as if a, b, c are three positive integers such that $a < b$ and $b < c$, then we can say that $a < c$.

SAQ 8 In the set of non zero integers Z^*, let the relation R be defined as follows : If $a, b \in Z^*$ then $a \, R \, b$ means that a divides b. Investigate whether R is reflexive or symmetric or transitive.

Theorem 3 :

> Let A be a non-empty set and R an equivalence relation defined on A. Then R decomposes A into a union of mutually disjoint equivalence classes. Conversely, given a decomposition of A as a union of mutually disjoint non-empty subsets, an equivalence relation can be defined on A for which these subsets form distinct equivalence classes.

Proof : Let $a \in A$. Then the equivalence class of a, written as $[a]$ is the set of all $x \in A$ such that $a \, R \, x$ where R is an equivalence relation that is $[a] = \{x \mid x \in A \text{ and } a \, R \, x\}$. We first observe that $a \in [a]$, because $a \, R \, a$ (reflexive property). Further any two equivalence classes are either identical or disjoint. If possible let $x \in [a] \cap [b]$, where $[a]$ and $[b]$ are two equivalence classes. Then $x \, R \, a$ and $x \, R \, b$. Since R is an equivalence relation $x \, R \, a$ implies $a \, R \, x$ (symmetric property) and $a \, R \, x$ and $x \, R \, b$ implies $a \, R \, b$ (transitive property). Thus $[a] \subseteq [b]$ and by a similarl argument $[b] \subseteq [a]$. This implies that $[a] = [b]$. Thus if any two equivalence classes are not disjoint then they are identical. Further for every a in A, $a \in [a] \subseteq A$. Hence $A = \bigcup_{a \in A} \{a\} \subseteq \bigcup_{a \in A} [a] \subseteq A$. Thus $A = \bigcup_{a \in A} [a]$.

Conversely, suppose that $A = \bigcup \{A_\alpha \mid \alpha \in I\}$ is a partition of A. That is A_α's are pairwise disjoint non empty subsets whose union is A. Let $a \in A$. Then there exists a unique $\alpha \in I$, such that $a \in A_\alpha$. Let a relation R be defined on A such that for any a, b in A, $a \, R \, b$ if and only if there exists an $\alpha \in I$, such that $a, b \in A_\alpha$. Now clearly for any $a \in A$, $a \, R \, a$ and R satisfies the

reflexive property. Suppose a R b, then there exists an $\alpha \in I$ such that $a, b \in A_\alpha$. Then $b, a \in A_\alpha$ and b R a. Thus R satisfies the symmetric property. Suppose a R b and b R c. Then there exists $\alpha \in I$ such that $a, b \in A_\alpha$ and there exists $\beta \in I$ such that $b, c \in A_\beta$. This means that $b \in A_\alpha \cap A_\beta$. But A_α and A_β are disjoint subsets. Thus $b \in A_\alpha \cap A_\beta$ implies that $A_\alpha = A_\beta$. Hence $a, c \in A_\alpha$ and a R c. Thus R satisfies transitive property. Thus R is an equivalence relation.

Example : Let $a, b \in Z$, the set of integers. We say that a is congruent to b modulo n if n divides $a - b$. We write this as $a \equiv b \pmod{n}$. Thus $5 \equiv 7 \pmod 2$, $13 \equiv 4 \pmod 3$ etc. In the set of integers the relation "is congruent to modulo n" is an equivalence relation. Let $a, b, c \in Z$. Then clearly $a \equiv a \pmod n$, satisfies the reflexive property. If $a \equiv b \pmod n$ then n divides $(a - b)$ and hence n divides $(b - a)$ also. Thus $b \equiv a \pmod n$, satisfying symmetric property. If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then n divides $(a - b)$ and n divides $(b - c)$ and hence n divides the sum of $(a - b)$ and $(b - c)$, that is $a - c$. That is $a \equiv c \pmod n$, implies transitive property. Thus the relation "congruent modulo n" is an equivalence relation on Z, the set of integers. Two integers belong to the same equivalence class if they leave the same remainder when divided by n. Thus

$$Z = [0] \cup [1] \cup \ldots \cup [n-1].$$

SAQ 9 Find the Partitioning of Z under the relation "congruent modulo 3".

1.5 FUNCTIONS

Let A and B be two non empty sets. A function f from A to B is a rule which associates to every element x of A, a unique element $f(x)$ of B. We write this as $f : A \to B$. Some authors use the word "mapping" as a substitute to the word function. If $f : A \to B$ is a function from A to B, mapping an element $x \in A$ on to an element $f(x)$ of B, then $f(x)$ is called an image of x under f. The element $x \in A$ is called the pre-image of $f(x)$. The set A is called the domain of f and the set B is called the codomain of f. The set of all elements $f(x)$ such that $a \in A$ is called the range of f. The Range of a function f is a subset of the codomain of f. We also observe that a function defined from A to B is a special kind of relation from A to B. Let us recall that a relation f from A to B is a sub set of A x B. This relation f will be a function if the following conditions are satisfied.

(i) $a \in A$ implies that there is $b \in B$ such that $(a, b) \in f$ and (ii) If $(a, b) \in f$ and $(a, c) \in f$, then $b = c$.

Example 1 : Let $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$,

$R = \{(1, a), (2, c), (3, d)\}$ is an example of a function.

$f = \{(1, a), (2, a), (3, a)\}$ is also an example of a function

$g = \{(1, a), (1, b), (2, a), (3, c)\}$ is not a function because the image of $1 \in A$ is not unique.

$h = \{(1, b), (2, c)\}$ is not a function because $3 \in A$ has no image.

However all the above are examples of relations.

A function $f : A \to B$ is called a *one - one function* or *injection* if distinct elements in A have distinct images in B. Equivalently f is an injection if $x_1 \neq x_2 \in A \Rightarrow f(x_1) \neq f(x_2) \in B$. Or $f(x_1) = f(x_2)$ in $B \Rightarrow x_1 = x_2$ in A.

A function $f : A \to B$ is called an *onto function* or *surjection* if every element in B has a pre-image in A. Equivalently, f is a surjection if $b \in B$ implies that there is $a \in A$ such that $f(a) = b$. For a surjection the range and codomain are the same.

A function which is both an injection and surjection is called a bijection. It is also called a one - one and onto function. If $f: A \to B$ is a bijection then for every $b \in B$, there is exactly one $a \in A$ such that $f(a) = b$. Then we can define a function $f^{-1}: B \to A$ such that $f^{-1}(b) = a$. Such a function f^{-1} is called the inverse of f. Only bijective functions can have inverses.

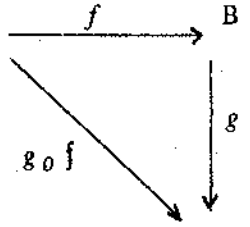
Example 2 : Let A and B be any two non empty sets and let $b \in B$. Define $f: A \to B$ by $f(x) = b$ for $x \in A$. Then f is a constant function. Clearly f is not one - one because $x_1 \neq x_2 \in A$ and $f(x_1) = f(x_2) = b \in B$.

Example 3 : Let $f: Z \to Z$ (the set of integers) be defined by $f(x) = 2x$. Let $x_1 \neq x_2 \in Z$; then $f(x_1) = 2x_1$; $f(x_2) = 2x_2$ and $f(x_1) \neq f(x_2)$. Since distinct elements are mapped onto distinct images, f is one - one. Clearly f is not onto. Because $1 \in Z$ (codomain of f) and there is no element x in Z (domain of f), such that $f(x) = 1$.

Example 4 : Let $f: A \to A$ be defined by $f(x) = x$. Such a function is called an identity function. Clearly f is a bijection. Let $x_1 \neq x_2 \in A$ (Dom), then $f(x_1) = x_1, f(x_2) = x_2$ and $f(x_1) \neq f(x_2) \in$ Range f. This shows f is one - one. Let $x \in$ Range f, then there is $x \in$ dom f such that $f(x) = x$. This shows f is onto. Here the inverse of $f = f^{-1} = f$.

SAQ 10 Let $f: R \to R$ (The set of reals) be defined by $f(x) = 2x + 3$. Find f^{-1}, if it exists.

Let $f: A \to B$ and $g: B \to C$ be two given functions. We can compose the two functions f and g to form a new function from A to C. We write this as $gof: A \to C$. Let $x \in A$, then $f(x) \in B$. The function g maps $f(x) \in B$ onto $g(f(x)) \in C$.



The composition of two functions is possible only when the range of the first function is same as the domain of the second function. The composition of two functions is not commutative in general. It may be observed that in the following example 5, though $g\,o\,f$ and $f\,o\,g$ is defined $f\,o\,g \neq g\,o\,f$.

We state without proof a theorem about the composition of one - one functions, onto functions and one - one and onto functions. The student shall try and prove this theorem

Theorem 4 :

> The composition of two one - one functions is again a one - one function. The composition of two onto functions is an onto function. The composition of two bijective functions is again a bijective function.

Example 5 : Let $f: R \to R$ and $g: R \to R$ be defined by $f(x) = x + 1$ and $g(x) = x^2$. Then $f\,o\,g$ and $g\,o\,f$ are both defined. $(f\,o\,g)\,x = f(g(x)) = f(x^2) = x^2 + 1$. $(g\,o\,f)\,x = g(f(x)) = g(x + 1) = (x + 1)^2$. Clearly $f\,o\,g \neq g\,o\,f$.

Example 6 : Let $f: R \to R$ be defined by $f(x) = x + 1$. Then f is one - one and onto (verify). Then f^{-1} exists. $f^{-1}: R \to R$ and $f^{-1}(x) = y$ where $f(y) = x$. But $f(y) = y + 1 = x$ and $y = x - 1$. Thus $f^{-1}(x) = x - 1$. $(f\,o\,f^{-1})(x) = f(f^{-1}(x)) = f(x - 1) = x - 1 + 1 = x$. Thus $f\,o\,f^{-1}$ = identity function. Similarly $f^{-1}\,o\,f$ is also the identity function.

Two functions f and g defined from the same domain A to the same range B are said to be equal if $f(x) = g(x)$ for all $x \in A$.

In the next unit we come across a special kind of function called a binary operation. Let A be a non empty set. A function defined from A x A to A is called a binary operation. That is $f: A \times A \to A$ is a binary operation. A binary operation associates two elements of a set to produce another element of the set.

Example : Let $f: Z \times Z \to Z$ be defined by $f(a, b) = a + b$. Since a and b are integers, $a + b$ is also an integer and f is a binary operation.

1.6. SUMMARY

This unit is intended to give the student an opportunity to recapitulate the necessary concepts that would be used in the next units. Sets and functions are very basic for the study of algebra. We have seen how sets could be combined to produce new sets. The relation "is equal to" we have been using in arithmetic is infact a special type of equivalence relation. An equivalence relation defined on a set partitions the set into mutually disjoint equivalence classes. A special kind of relation is a function. All relations are not functions. Two functions could be composed to obtain new functions, provided the range of the first function is the domain of the second function. A binary operation is a special kind of function.

1.7 MODEL EXAMINATION QUESTIONS

SECTION - A (Long Answers)

(i) Let $A = \{a, b, c, d\}$. Write all the subsets of A. Find two sub sets B and C such that B is not a subset of C and C is not a sub set of B.

(ii) Let $A = \{a, b, c\}$, $B = \{1, 2\}$ write all possible functions from A to B. Determine which of these are injective, surjective and bijective

SECTION - B (Short Answers)

(i) For any two integers a and b define

$a * b = a + b + 1$. Is * a binary operation on Z ?

(ii) Let $f: \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = x^2 + 1$. Is f one - one ? Is f onto ?

(iii) Let $f: Z \to Z$, $g: Z \to Z$ be defined by $f(x) = -x$ and $g(x) = x + 2$. Find $f \circ g$ and $g \circ f$. Is $f \circ g = g \circ f$?

1.8 ANSWERS TO SAQ'S

SAQ 1 $\{0\}$ is not empty because $0 \in \{0\}$. $\{\phi\}$ is not empty because $\phi \in \{\phi\}$. The set $\{x \mid x$ is positive and $x + 1 = 0\}$ is empty because there is no positive integer x which when added to 1 gives 0.

SAQ 2 $P(S) = \{\phi, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}\ \{1, 2, 3\}\}$.

SAQ 3 The elements of A are obtained by solving $x^4 - 1 = 0$. That is $(x^2 + 1)(x^2 - 1) = 0$.

Or $x = \pm 1$ and $x = \pm i$. Thus (b) and (c) are both correct.

SAQ 4 $A \cup B = A$; $A \cap B = B$; $A - (A \cap B) = A - B = \{a, c, 1, 3\}$

SAQ 5 $A' = \{2, 4, 6, 8, 10\}$

SAQ 6 $A' = \{0, 1, 3, 5, 7, 9\}$, $B' = \{0, 2, 4, 6, 8, 9, 10\}$

$A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8, 10\}$

$A \cap B = \phi$.

$(A \cup B)' = \{0, 9\} = A' \cap B'$.

$(A \cap B)' = U = A' \cup B'$.

SAQ 7 $A \times A = \{(a, a), (a, b), (a, c), (a, d), (b, a), (b, b), (b, c), (b, d), (c, a), (c, b), (c, c), (c, d), (d, a), (d, b), (d, c), (d, d)\}$

SAQ 8 Since a divides a, R is reflexive. If a divides b then b does not divide a. So R is not symmetric. If a divides b and b divides c, then a divides c and hence is transitive.

SAQ 9 $Z = [0] \cup [1] \cup [2]$.

$[0] = \{\ldots -6, -3, 0, 3, 6, 9, 12, \ldots\} = \{x \mid x = 3m, m \in Z\}$

$[1] = \{\ldots -5, -2, 1, 4, 7, 10, 13, \ldots\} = \{x \mid x = 3m + 1, m \in Z\}$

$[2] = \{\ldots -4, -1, 2, 5, 8, 11, 14, \ldots\} = \{x \mid x = 3m + 2, m \in Z\}$

SAQ 10 f is one - one, because let x_1, x_2 be any $f(x_1) = 2x_1 + 3$ and $f(x_2) = 2x_2 + 3$, $f(x_1) = f(x_2)$. Let $y \in$ Range

then $f(x) = 2x + 3 = y$, That is $x = \frac{y-3}{2}$ and $f\left(\frac{y-3}{2}\right) = y$. Thus f is onto. Therefore f^{-1} exists

$f^{-1}(y) = \left(\frac{y-3}{2}\right)$ or $f^{-1}(x) = \left(\frac{x-3}{2}\right)$.

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

1.9. REFERENCE BOOKS

(i) Surjeet Singh and Qazi Zameeruddin : Modern Algebra, Vikas Publishing House Pvt. Ltd.

(ii) I · N · Herstein : Topics in Algebra, Vikas Publishers

(iii) J. B. Fraleigh : A first Course in Abstract Algebra.

(iv) T.V. Ramana, Nagamuni Reddy, Hanumantha Chary : Aroopa Beeja Ganithamu, Telugu Akademi, Hyderabad.

(v) B · S. Vatsaa : Elements of Modern Algebra, Wiley Eastern.

UNIT–2 : GROUPS

Contents

2.1 Aims and Objectives

2.2 Introduction

2.3 Definitions and examples

2.4 Some simple properties

2.5 Workedout exercises

2.6 Summary

2.7 Model Examination Questions

2.8 Answers to Self Assessment Questions

2.1 AIMS AND OBJECTIVES

By the time you complete this unit you must be able to (i) Define a group and give examples, (ii) verify whether a given set forms a group under a given operation, (iii) state and prove certain properties of groups, (iv) solve problems based on definitions and properties of groups.

2.2 INTRODUCTION

It is difficult to establish a specific date for the beginning of the study of groups. But it is agreed that the work of the French Mathematician Evariste Galois (1811 - 1832) set the stage for the study of the subject. Another young Norwegian Mathematician Niels Abel (1802 - 1829) also contributed to the study of groups by establishing a connection to the solutions of a polynomial equation and the groups generated by the permutations of its roots. The abstract notion of a group was formulated and developed by Arthur Cayley (1853) and Cauchy (1840). Abstraction is a process by which similarities are recognised between seemingly dissimilar mathematical objects. This is achieved by establishing that the similarities are the result of a very few basic properties that are possessed by all mathematical objects under consideration. We call these basic properties as axioms or postulates.

2.3 DEFINITIONS AND EXAMPLES

Definition 1 :

A non empty set G together with an operations 'o' defined on elements of G is called a group if it satisfies the following postulates.

(i) Closure property : For $a, b, \in$ G, $a \, o \, b$ also is in G.

(ii) Associative law : For all $a, b, c, \in$ G, $a \, o \, (b \, o \, c) = (a \, o \, b) \, o \, c$

(iii) Existence of Identity : There exists an element $e \in$ G such that $a \, o \, e = e \, o \, a = a$ for every $a \in$ G.

(iv) Existence of Inverse : For every $a \in$ G, there exists $a^{-1} \in$ G such that $a \, o \, a^{-1} = a^{-1} o \, a = e$ (the identity)

(v) If in addition to these four postulates, the commutative law $a \, o \, b = b \, o \, a$ for all $a, b, \in$ G is also satisfied, then G is called an Abelian group or commutative group.

Note : If the operation 'o' is a binary operation then the closure property is automatically satisfied. Thus we can define a group to be a non empty set G together with a binary operation which satisfies the associative, identity and inverse properties. We write the group as (G, o). When we say that G is a group, it is understood that it is a group under an appropriate operation.

Definition 2 :

A non empty set G together with a binary operation 'o' is called a semi group if it satisfies the following postulate :

(i) Associativity : $a\ o\ (b\ o\ c) = (a\ o\ c)\ oc$ for all $a, b, c, \in$ G.

Definition 3 :

A semi group which has an identity element and each of whose elements have inverse is a group.

Definition 4 :

A group (semi group) is called a finite group (finite semi group) or an infinite group (infinite semi group) according as the number of elements it has is finite or infinite. If the group G is finite the order of G, written as o (G) is the number of elements in G.

Example 1 : Let Z denote the set of integers and let '+' denote the ordinary addition. Then (Z, +) is an infinite Abelian group. To see this, we verify the group postulates one by one. First of all the operation '+' is a binary operation, because if $a, b, \in$ Z then $a + b$ is also in Z. The associative property follows from the property of addition of integers. That is if $a, b, c \in$ Z, then $a + (b + c) = (a + b) + c$. The integer 0 (zero) serves as the identity because $a + 0 = 0 + a = a$ for every $a \in$ Z. For every $a \in$ Z, there is $-a \in$ Z such that $a + (-a) = (-a) + a = 0$, the identity element. Thus (Z, +) is a group. Further since addition is commutative, that is $a + b = b + a$ for $a, b, \in$ Z, (Z, +) is an Abelian group. Since Z has infinite elements, (Z, +) is an infinite Abelian group.

Example 2 : Let Q^* denote the set of non zero rational numbers and '.' denote the operation of multiplication. Then $(Q^*, \cdot)$ is an infinite Abelian group. The postulates could be verified easily. The operation '.' is a binary operation because the product of two rational numbers is again a rational number. Associativity follows from the property of multiplication of rationals. The rational number $1 \in Q^*$ is the identity element. For any non-zero rational number a/b, its reciprocal b/a is the inverse. Thus $(Q^*, \cdot)$ is a group. The commutativity property follows from the property of multiplication of rational numbers and Q^* has infinite elements. Thus $(Q^*, \cdot)$ is an infinite Abelian group.

SAQ 1 In the above example why did we exclude the rational number zero from the set?

Example 3 : Let M denote the set of 2 x 2 non singular matrices and let $\otimes$ denote the operation of matrix multiplication. Then $(M, \otimes)$ is a group. This group is not necessarily commutative since matrix multiplication is not commutative. The student may verify that the operation $\otimes$ is a binary operation. Associativity follows from the property of matrix multiplication. The 2 x 2 matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ serves as the identity element and for non singular matrix A, its inverse A^{-1} is the inverse element.

Example 4 : Let Z^+ denote the set of positive integers and let + denote the operation of multiplication. Then $(Z^+, +)$ is not a group because the identity (and hence the inverse) postulate is not satisfied. There is no positive integer e such that $a + e = e + a = a$ for $a \in Z^+$. But $(Z^+, +)$ is a semi group.

SAQ 2 Do the set of integers Z under the operation of multiplication form a group ?

SAQ 3 Do the set of odd integers under the operation of addition form a group ?

Example 5 : Let w be a cube roots of unity (a root of $x^3 - 1 = 0$). Then the set $\{1, w, w^2\}$ under the operation of multiplication form an Abelian group. Clearly 1 is the identity element. The inverse of w is w^2 and the inverse of w^2 is w, because $w \cdot w^2 = w^2 . w = w^3 = 1$. This is an example of a finite Abelian group.

Remark : Let n be a positive integer. Let the set of integers $S = \{0, 1, 2, \ldots, (n-1)\}$ is called the set of integers modulo n. These are also called residues modulo n. The operations of "modulo addition" and "modulo multiplication" is defined on S as follows. For $a, b \in S$; $a + b = c$ where $c \in S$ if $a + b < n$. If $a + b > n$, $a + b = d$ where d is the remainder left after dividing $(a + b)$ by n. Similarly for $a, b \in S$, $a \cdot b = c$ where $c \in S$ if $a \cdot b < n$. If $a \cdot b > n$, then $a \cdot b = d$ where d is the reminder left after dividing $(a \cdot b)$ by n. We denote by Z_n, the set of residues modulo n and Z_n^* the set of non zero residues modulo 'n'. That is $Z_n = \{0, 1, 2, \ldots (n-1)\}$ and $Z_n^* = \{1, 2, \ldots, (n-1)\}$.

Example 6 : Consider the set A of integer modulo 3. Then $A = \{0, 1, 2\}$. Here under modulo addition : $0 + 0 = 0$, $0 + 1 = 1$, $0 + 2 = 2$; $1 + 2 = 3 \notin A$, therefore $1 + 2 = 0$ which is the reminder left after dividing 3 with 3. Now $2 + 2 = 1$ because 1 is the reminder left after dividing $(2 + 2)$ with 3. Similarly $0.0 = 0$; $0.1 = 0$; $0.2 = 0$, $1.2 = 2$ and $2.2 = 1$. We express in tables as below.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Example 7 : The set of integers modulo 3, under the operation of modulo addition is a finite Abelian group. The operation table is given above.

From the table, it is clear that the operation is a binary operation. ϕ is the identity element and the inverse of 1 is 2 and the inverse of 2 is 1 under addition modulo 3. The commutativity is easily verified from the table.

Example 8 : The set of non zero integers modulo 5 under the operation of modulo multiplication form an Abelian group. The integers modulo 5 are 0, 1, 2, 3, 4. The non zero integers modulo 5 are 1, 2, 3, 4. Let us construct the modulo multiplication table.

•	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Here the multiplication is performed as follows. $1 \times 1 = 1$; $1 \times 2 = 2$ etc; $2 \times 1 = 2$ and $2 \times 2 = 4$. $2 \times 3 = 6$ but $6 \equiv 1 \pmod 5$.

Thus $2 \times 3 = 1$ under modulo 5 multiplication.

$2 \times 4 = 8$ and $8 \equiv 3 \pmod 5$

$3 \times 3 = 9$ and $9 \equiv 4 \pmod 5$

$3 \times 4 = 12$ and $12 \equiv 2 \pmod 5$ etc.

From the table, the operation of modulo multiplication is a binary operation. 1 is the identity element. The inverse of 1, 2, 3, and 4 are 1, 3, 2 and 4 respectively. Commutativity is easily verified from the table : 2 x 3 = 3 x 2 etc. If we include zero in the set then the inverse property is not satisfied.

Example 9 :An interesting Abelian group consisting of 4 elements named after the nineteenth century mathematician Felix Klein is given by the following relations.

$$S = \{e, a, b, ab\} ; a^2 = b^2 = (ab)^2 = e$$

Here e is the identity element and each element is its own inverse. That is $a = a^{-1}$; $b = b^{-1}$; $(ab)^{-1} = (ab)$. This group is called Klein 4 - group.

2.4 SOME SIMPLE PROPERTIES

Theorem 1 :

The identity element of a group is unique.

Proof : Let $(G, \cdot)$ be a group. If possible let e and e' be two identity elements of G. Recall that if e is an identity element of G, then $a \cdot e = e \cdot a = a$ for every a in G. Now e is the identity element of G and e' is an element of G. Then

$e \cdot e' = e' \cdot e = e'$, because e is the identity of G. But e' is also the identity element of G and e is an element of G.

Then $e \cdot e' = e' \cdot e = e$ giving $e = e'$.

Then G has only one identity e and it is unique.

Theorem 2 :

The inverse of every element in a group is unique.

Proof : Let $(G, \cdot)$ be a group and let $a \in G$. If possible let a^{-1} and a'^{-1} are two inverses of a. Let e be the identity element of G. Then

$$a \cdot a^{-1} = a^{-1} \cdot a = e, \text{ and}$$

$$a \cdot a'^{-1} = a'^{-1} \cdot a = e.$$

Now $$a^{-1} = a^{-1} \cdot e = a^{-1}\left(a \cdot a'^{-1}\right) = \left(a^{-1} \cdot a\right) \cdot a'^{-1}$$

$$= e \cdot a'^{-1} = a'^{-1}.$$

Thus $a^{-1} = a'^{-1}$ and the inverse of a is unique.

Theorem 3 :

Let $(G, \cdot)$ be a group and $a, b \in G$. Then

(i) $\left(a^{-1}\right)^{-1} = a$ and (ii) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

Proof : (i) Since $a \in G$, there exists a^{-1} such that

$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

It follows that a^{-1} is the inverse of a and a is the inverse of a^{-1}, that $\left(a^{-1}\right)^{-1}$. Thus $\left(a^{-1}\right)^{-1} = a$.

(ii) $(a \cdot b) \cdot \left(b^{-1} \cdot a^{-1}\right) = \left[a \cdot \left(b \cdot b^{-1}\right)\right] \cdot a^{-1}$, Associativity

$= [a \cdot e] \cdot a^{-1}$, inverse property

$= a \cdot a^{-1}$, identity property

$= e$

$\left(b^{-1} \cdot a^{-1}\right) \cdot (a \cdot b) = b^{-1} \cdot \left[a^{-1} \cdot (a \cdot b)\right]$

$= b^{-1} \cdot \left[\left(a^{-1} \cdot a\right) \cdot b\right]$

$= b^{-1} \cdot b$

$= e$

Thus $(a \cdot b) \cdot \left(b^{-1} \cdot a^{-1}\right) = \left(b^{-1} \cdot a^{-1}\right) \cdot (a \cdot b) = e.$

Thus $b^{-1} \cdot a^{-1}$ is the inverse of $(a \cdot b)$

and $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Theorem 4 :

Let $(G, \cdot)$ be a group and $a, b, c \in G$.

Then $a \cdot b = a \cdot c \Rightarrow b = c$ (left cancellation law)

and $b \cdot a = c \cdot a \Rightarrow b = c$ (right cancellation law)

(Cancellation laws hold good in a group)

Proof : Since $a \in G$, $a^{-1} \in G$. Then

$a \cdot b = a \cdot c \Rightarrow a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$

$\Rightarrow \left(a^{-1} \cdot a\right) \cdot b = \left(a^{-1} \cdot a\right) \cdot c$, associativity

$\Rightarrow e \cdot b = e \cdot c$, inverse property

$\Rightarrow b = c$; identity property.

The second part of the theorem is left to the student as an exercise.

Theorem 5 :

Let $(G, \cdot)$ be a group and $a, b, \in G$. Then there exists a unique $x \in G$ such that $ax = b$.

Proof : Since $a \in G$, a^{-1} exists and $a^{-1} \in G$. Put $x = a^{-1} \cdot b$. Since $a^{-1} \in G$ and $b \in G \Rightarrow a^{-1}b \in G$.

Then $ax = a \cdot \left(a^{-1} \cdot b\right) = \left(a \cdot a^{-1}\right) \cdot b$

$= e \cdot b = b.$

Thus there exists $x \in G$ such that $ax = b$. To show that x is unique, let $ax = ax' = b$. Then $a^{-1}(ax) = a^{-1}(ax')$. This implies

that $\left(a^{-1} \cdot a\right) \cdot x = (a^{-1} \cdot a) \cdot x' \Rightarrow x = x'$.

Thus there exists a unique x such that $ax = b$.

(The theorem states that in a group the equation $ax = b$ is solvable and admits a unique solution. The student should prove a similar theorem for the equation $ya = b$).

Theorem 6 :

A finite semi group is a group if and only if it satisfies the cancellation laws.

Proof : Let $G = \{a_1, a_2, \ldots, a_n\}$ be a finite semi group. That is under an appropriate binary operation, G satisfies the associative postulate. G will be a group if it satisfies the remaining two postulates - the identity and the inverse. We will prove that if G satisfies the cancellation laws, then G satisfies these two postulates. Let a_i be an arbitrary element of G. Consider the sets :

$$G = \{a_1, a_2, \ldots, a_n\} \text{ and}$$

$$a_i G = \{a_i a_1, a_i a_2, \ldots, a_i a_n\}, a_i \in G$$

We observe that all the elements of $a_i G$ are distinct and they are as many in number as the elements in G. To see this let $a_i a_k = a_i a_l$, then by left cancellation law $a_k = a_l$. Thus all the elements of $a_i G$ are distinct and they are same as the elements of G (from closure) in some order. So for $a_j \in G$, there exists $a_s \in G$ such that $a_j = a_i a_s$. In particular for $a_i \in G$, there exists $a_k \in G$ such that $a_i = a_i a_k$. Then $a_i a_j = (a_i a_k) a_j = a_i (a_k a_j)$ and by left cancellation law $a_j = a_k a_j$. Considering $G a_i = \{a_1 a_i, a_2 a_i, \ldots a_n a_i\}$ by a similar argument, we see that for $a_j \in G$ there exists $a_l \in G$ such that

$$a_j = a_j a_l.$$

If $j = l$, then from $a_j = a_k a_j$ we get $a_l = a_k a_l$

and if $j = k$ then from $a_j = a_j a_l$ we get $a_k = a_k a_l$.

Thus $a_l = a_k$ and a_k is the identity on G. Let us denote a_k by e.

Now $e \in G$ and there exist $a_n, a_m \in G$ such that

$$e = a_m a_i \text{ and } e = a_i a_n.$$

Then $a_n = e a_n = (a_m a_i) a_n = a_m (a_i a_n) = a_m e = a_m$.

Hence $a_m a_i = a_i a_m = e \Rightarrow a_m = a_i^{-1} \in G$.

Thus G is a group. The second part of the proof i. e., cancellation law hold good in a group, is given in theorem 4.

2.5 WORKEDOUT EXERCISES

Exercise 1 : Let Q^+ denote the set of positive rational numbers and define an operation 'o' on Q^+ by $a \circ b = \frac{ab}{2}$ for all $a, b \in Q^+$. Show that Q^+ is an Abelian group.

Ans : If $a, b \in Q^+$ then $a \circ b = \frac{ab}{2}$ also is in Q^+. Thus 'o' is a binary operation. To see that the associative property is satisfied, we evaluate $a \circ (b \circ c)$ and $(a \circ b) \circ c$ and verify that they are equal.

$$a \circ (b \circ c) = a \circ \frac{bc}{2} = \frac{abc}{4} \text{ and}$$

$$(a \circ b) \circ c = \frac{ab}{2} \circ c = \frac{abc}{4}.$$

Thus 'o' is associative. To verify that Q^+ has an identity element we observe that

$$a \circ 2 = 2 \circ a = \frac{2a}{2} = a \ \forall a \in Q^+.$$

Thus 2 is the identity element.

For $a \in Q^+$ we observe that, $(a \neq 0)$,

$$a \circ \frac{4}{a} = \frac{4}{a} \circ a = 2.$$

Thus $\frac{4}{a}$ is the inverse of a.

Thus $\left(Q^+, \circ\right)$ satisfies all the four postulates of a group. Further, $a \circ b = b \circ a$ $\forall\, a, b \in Q^+$.

Thus $\left(Q^+, \circ\right)$ is an Abelian group.

Exercise 2 : If G is a finite group with even number of elements, show that there exists atleast one element of G, which is its own inverse.

Ans : G is a group with $2n$ elements (Say).

Since G is a group it has an identity element, 'e'. Keeping this element separately the rest of the elements are $(2n - 1)$ in number. That is an odd number of elements are left out. Further G is a group implies that each element has an inverse. Identify and pair each element with its inverse. Out of the odd number of elements, if we pair two elements at a time, one element is left out. Since G is a group this element also must have an inverse. Since all the elements in G are exhausted, the only possibility is that it is its own inverse.

Exercise 3 : G is a group such that for each $x \in G$, $x^2 = e$, the identity. Show that G is Abelian.

Ans : We are required to show that $a \cdot b = b \cdot a$ for all $a, b \in G$. Since G is a group, the operation is a binary operation. This means that for $a, b \in G$, $a \cdot b$ also is in G. Now for any $x \in G$, $x^2 = x \cdot x = e$ the identity element of G. That is x is the inverse of x. That is $x^{-1} = x$.

For $a, b \in G$, $(a \cdot b)^2 = e$. But $(a \cdot b)^2 = (a \cdot b) \cdot (a \cdot b) = e$

Therefore $(a \cdot b) \cdot (a \cdot b) = a \cdot (b \cdot a) \cdot b = e$

$\therefore\ a \cdot [a \cdot (b \cdot a)\, b] \cdot b = a \cdot e \cdot b$

$a^2 \cdot (b \cdot a) \cdot b^2 = a \cdot b$

but $a^2 = b^2 = e$. Thus $e \cdot (b \cdot a) \cdot e = a \cdot b$

and $b \cdot a = a \cdot b$ implying G is Abelian

SAQ 2 Give an alternate proof for the above proposition.

Exercise 4 : If G is a group such that $(a \cdot b)^2 = a^2 \cdot b^2$ for all a, b in G, show that G is Abelian.

Ans : We are required to show that for all $a, b \in G$, $a \cdot b = b \cdot a$. Since G is group $a, b \in G$ implies a^{-1}, b^{-1} exist and are in G. Now $(a \cdot b)^2 = (a \cdot b) \cdot (a \cdot b) = a \cdot a \cdot b \cdot b$ (given) Therefore $a^{-1} \cdot [(a \cdot b) \cdot (a \cdot b)] \cdot b^{-1} = a^{-1} \cdot [a \cdot a \cdot b \cdot b] \cdot b^{-1}$

$$\Rightarrow \left(a^{-1} \cdot a\right) \cdot (b \cdot a) \cdot \left(b \cdot b^{-1}\right) = \left(a^{-1} \cdot a\right) \cdot (a \cdot b) \cdot \left(b \cdot b^{-1}\right)$$

$$\Rightarrow e \cdot (b \cdot a) \cdot e = e \cdot (a \cdot b) \cdot e$$

$$\Rightarrow b \cdot a = a \cdot b \Rightarrow G \text{ is Abelian}$$

Exercise 5 : If G is a group such that $(a \cdot b)^n = a^n \cdot b^n$ for three consecutive positive integers n and for $a, b \in G$, show that G is Abelian.

Ans : It is given that $(a \cdot b)^n = a^n \cdot b^n$; $(a \cdot b)^{n+1} = a^{n+1} \cdot b^{n+1}$ and $(a \cdot b)^{n+2} = a^{n+2} \cdot b^{n+2}$. We are required to show that $a \cdot b = b \cdot a$ for all $a, b \in G$. We show this in three steps.

Step (i) : $a^{n+1} \cdot b^{n+1} = (a \cdot b)^{n+1} = (a \cdot b)^n \cdot (a \cdot b)$.

$= \left(a^n \cdot b^n\right) \cdot (a \cdot b)$.

Thus $a^n \cdot a \cdot b^n \cdot b = a^n \cdot \left(b^n \cdot a\right) \cdot b$

By the cancellation laws we get

$a \cdot b^n = b^n \cdot a$

Step (ii) : $a^{n+2} \cdot b^{n+2} = (a \cdot b)^n \cdot (a \cdot b)^2$

$= (a \cdot b)^n \cdot (a \cdot b) \cdot (a \cdot b)$

$= \left(a^n \cdot b^n\right) \cdot (a \cdot b) \cdot (a \cdot b)$

$= a^n \cdot \left[b^n \cdot (a \cdot b)\, a\right] \cdot b$.

Thus $a^n \cdot a^2 \cdot b^{n+1} \cdot b = a^n \cdot \left[b^n \cdot (a \cdot b)\, a\right] \cdot b$.

By Cancellation laws,

$a^2 \cdot b^{n+1} = \left(b^n \cdot a\right) \cdot (b \cdot a)$

$= \left[\left(a \cdot b^n\right) \cdot b\right] a$ by step (i)

$= a \cdot b^{n+1} \cdot a$

Again by Cancellation laws we get

$a \cdot b^{n+1} = b^{n+1} \cdot a$

Step (iii) : $a \cdot b^{n+1} = b \cdot (b^n \cdot a) = b \cdot \left(a \cdot b^n\right)$ by step (i)

Thus $(a \cdot b) \cdot b^n = (b \cdot a) \cdot b^n$

By right Cancellation law we get that for $a, b \in G$,

$a \cdot b = b \cdot a$ implying G is Abelian

2.6 SUMMARY

A group is a non empty set together with a binary composition (operation) satisfying the postulates of associativity, identity and inverse. If in addition, the commutative property is satisfied, then the group is called an Abelian group or a commutative group. The identity element in a group is unique and the inverse of every element in a group is unique. Cancellation laws hold good in a group and the equations $ax = b$ and $yc = d$ have unique solutions. There are very many examples of groups from Number systems, Matrices, Geometry, Residue systems modulo n with appropriate binary composition defined on the set under consideration.

2.7 MODEL EXAMINATION QUESTIONS

SECTION - A (Long answer questions)

(i) Consider the set G consisting of the eight elements $\{1, -1, i, -i, j, -j, k, -k\}$ where $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$, $jk = -kj = i$ and $ki = -ik = j$. Construct the multiplication table and verify that G is a group under this operation.

(ii) Let S be the set of real numbers excluding – 1. That is S = R – {–1}. Define an operation 'o' on S by $a \, o \, b = a + b + ab$. Show that (S, o) is a group.

SECTION - B (Short answer questions)

(i) Show that the identity element and the inverse of an element are unique in a group.

(ii) If G is a group such that $x^2 = x \; \forall \; x \in G$, show that G is Abelian.

2.8 ANSWERS TO SELF ASSESSMENT QUESTIONS

SAQ 1 If zero is included in the set, then zero will have no inverse and the inverse postulate will not be satisfied.

SAQ 2 No. The inverse postulate is not satisfied.

SAQ 3 No. The operation is not a binary operation. That is the sum of two odd integers is not odd.

SAQ 4 $(a\,b) \cdot (a\,b) = e \Rightarrow (a \cdot b) = (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = b \cdot a.$

UNIT–3 : SUBGROUPS

Contents

3.1 Aims and Objectives

3.2 Introduction

3.3 Definition and Examples

3.4 Criterion for a subset to be a subgroup

3.5 Cosets

3.6 Lagrange's theorem and applications

3.7 Workedout exercises

3.8 Summary

3.9 Sample Examination Questions

3.10 Answers to Self Assessment Questions

3.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to (i) define a subgroup and give examples, (ii) state and prove Lagranges theorem, (iii) state and prove theorems on subgroups, (iv) determine the subgroups of some of the groups.

3.2 INTRODUCTION

Whenever we study a mathematical system it is natural to ask whether any subsystem inherits some or all the properties of the original. The notion of a sub group is one such. We have seen that a non-empty set G, together with a binary operation 'o' becomes a group if it satisfies some postulates. If H is a non empty subset of G, it is therefore natural to ask whether H together with the same binary operation defined on G becomes a group in its own right. If the answer is positive then H is called a subgroup of G. We then investigate the various types of relationships that might exist between H and G. Some group may not have any proper subgroups at all. Some others may have an abundant number of subgroups. It may be possible that a non-Abelian group may have Abelian subgroups. Each of these situations gives rise to very interesting consequences. Of special interest is the relation between a finite group and its subgroups.

3.3 DEFINITIONS AND EXAMPLES

Let $(G, \cdot)$ be a group and let H be a non empty subset of G. Then $(H, \cdot)$ is a subgroup of G, if $(H, \cdot)$ is a group (in the sense that it satisfies all the postulates of the group). Since G is a subset of itself, we can say that $(G, \cdot)$ is a subgroup of itself. Let 'e' be the identity element of $(G, \cdot)$ then $(\{e\}, \cdot)$, that is, the set consisting of identity element alone together with the same binary operation defined in G, satisfies all the axioms of the group. Thus $(\{e\}, \cdot)$ is a subgroup of $(G, \cdot)$ such subgroups are called improper subgroups or trivial subgroups. Any subgroup of G, other than G and the subgroup consisting of identity element alone is called a proper subgroup. We confine our attention to proper subgroups.

Definition. 1:

Let (G, ·) be a group and let H be a non empty proper subset of H. Then H is a subgroup of G if the binary operation '·' defined on G is also a binary operation on H and (H, ·) satisfies the postulates of associativity, identity and inverse.

Example. 1 : Let Z be set of integers. Then (Z, +) is a group. Let E denotes the set of all even integers. Then E is a subset of Z and (E, +) is a subgroup of (Z, +). Observe that zero being an even integer is an element of E and serves the identity element. For any even integer $2a \in E$, the even integer $(-2a)$ serves as the inverse element of $2a$. Since $2a + 2b = 2b + 2a$ for $2a, 2b \in E$, E is an Abelian subgroup of (Z, +)

Example. 2 : The group (Z, +), the group of integers under addition is a subgroup of (Q, +), the group of rational numbers under addition. The student may verify the postulates.

Example. 3 : Let $S = \{1, -1, i, -i\}$ where $i^2 = -1$. Then (S, ·) is a group. Then $(\{1, -1\}, \cdot)$ is a subgroup of (S, ·).

SAQ 1 Let O denotes the set of odd integers. Is (O, +) a subgroup of (Z, +)?

Example. 4 : Let w be a cube root of unity. Let $G = \{1, w, w^2\}$. Then (G, ·) is a group. G has no subgroup other than G and $(\{1\}, \cdot)$. That is G has no non-trivial subgroups.

Remark : Though we must always write (H, ·) as a subgroup of (G, ·) we write often that H is a subgroup of G when there is no ambiguity.

3.4 CRITERION FOR A SUBSET TO BE A SUBGROUP

Theorem. 1 :

A non empty subset H of G is a subgroup of G if and only if : (i) H is closed under the binary operations of G, (ii) The identity of G is in H and (iii) $a \in H \Rightarrow a^{-1} \in H$.

Proof : If H is a subgroup of G, by the definition of a subgroup, the conditions (i), (ii), (iii) are automatically satisfied.

Conversely, suppose H is a subset of G satisfies the conditions (i), (ii) and (iii). Then the group axioms of identity and inverse are satisfied by (ii) and (iii). The condition (i) states that the binary operations of G is a binary operation for H also. The members of H are members of G and hence associativity on H.

Thus H is a subgroup of G.

Theorem. 2 :

Let H be a non empty subset of G. Then H is a subgroup of G if and only if the following condition is satisfied.

(i) $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof. Let H be a subgroup of G. Let $a, b \in H$. Since H is a subgroup and $b \in H$, $b^{-1} \in H$ implies that $a \cdot b^{-1} \in H$, by closure property.

Conversely, Let H be a non empty subset of the group G such that for $a, b \in H$, $a\,b^{-1} \in H$. To prove that H is a subgroup we must verify the identity and inverse properties in H. Since $H \neq \phi$,

let $a \in H$. Now by the given condition (i), $a \in H$ and $a \in H \Rightarrow a \cdot a^{-1} = e \in H$. Thus H satisfies the identity postulate. Now $a \in H$ and $e \in H \Rightarrow$ that $a^{-1} \cdot e = a^{-1} \in H$. Thus for each $a \in H$, $a^{-1} \in H$ and H satisfies the inverse property. Suppose $a \in H$ and $b \in H$. This implies that $b^{-1} \in H$ and $a \cdot \left(b^{-1}\right)^{-1} = a \cdot b \in H$ satisfying the closure property, thus H is a subgroup of G.

Theorem. 3 :

> Lt G be a group and let H be a non empty finite subset of G. Then H is a subgroup of G if and only if H is closed.

Proof : Let H be a subgroup of G and let $a, b \in H$. Then $a \cdot b \in H$ so that H is closed.

Conversely, let H be a non empty finite subset of the group G such that $a, b \in H \Rightarrow ab \in H$. If $H = \{e\}$, the result is obvious since $e \cdot e \in H$. If $H \neq \{e\}$, let $a \in H$. Then $a.a = a^2, a^3 \ldots \in H$. But H is finite. Thus there exists a^r and $a^s \in H$ such that $a^r = a^s$. Without loss of generality let us assume that $r > s$. Then $a^{r-s} = e$, the identity element $\in H$. Now $a^{-1} = a^{r-s-1} \in H$. Thus $e \in H$ and for $a \in H$ $\Rightarrow a^{-1} \in H$ implies H is a subgroup of G.

SAQ 2 Give an example to show that theorem 3 is not true if the condition "finite" is dropped in the statement.

Theorem. 4 :

> Let G be a group and let H be a subgroup of G. Then for $a \in G$, and $b \in G$
>
> (i) $Ha = H$ if and only if $a \in H$.
>
> (ii) $Ha = Hb$ if and only if $ab^{-1} \in H$.

Proof : Before we prove the theorem, let us state the meaning of Ha. Let $H = \{h_1, h_2, \ldots\}$. We mean by Ha, $Ha = \{h_1 a, h_2 a \ldots\}$. If H is a subgroup then the identity 'e' of G (which is also the identity of H) is in H. Thus one of the h_i's is e.

(i) Suppose $Ha = H$. Writing $H = \{e, h_1, h_2, \ldots\}$

$$Ha = \{ea, h_1 a, h_2 a, \ldots\}$$

Thus $ea \in Ha = H \Rightarrow a \in H$.

Conversely suppose $a \in H$. Then H is a subgroup implies that H is closed. Thus $a \in H$ and $h \in H$ implies $ha \in H$. This is true for every $h \in H$. Thus $Ha \subseteq H$. But for $h \in H$, we can write $h = he = h\left(aa^{-1}\right) = h\left(a^{-1}a\right) = \left(ha^{-1}\right)a$. But $a \in H \Rightarrow a^{-1} \in H$ and $ha^{-1} \in H$ and $\left(ha^{-1}\right)a \in Ha$. Thus $H \subseteq Ha$. Hence $H = Ha$.

(ii) Suppose $Ha = Hb$. Since $e \in H$, $ea = a \in Hb$ This means that there is $h_i \in H$ such that $a = h_i b$ Then $ab^{-1} = h_i \in H$.

Conversely, suppose $ab^{-1} \in H$. Then there is $h_j \in H$ such that $ab^{-1} = h_j$. Then $a = h_j b$. Then $Ha = H\left(h_j b\right) = \left(Hh_j\right)b = Hb$. Since $h_j \in H \Rightarrow Hh_j = H$.

Theorem 5 :

> Let G be a group and let H and K be two subgroups of G. Then $H \cap K$ is a subgroup of G.

Proof. Since H and K are subgroups of G, the identity element 'e' belongs to both H and K. That is $e \in H \cap K$ and hence $H \cap K \neq \phi$. Let $a, b \in H$ and H is a subgroup implies that $ab^{-1} \in H$. Similarly $a, b \in K$ and K is a subgroup implies that $ab^{-1} \in K$. Thus $ab^{-1} \in H \cap K$. Since $a, b^{-1} \in H \cap K$ implies $ab^{-1} \in H \cap K$, $H \cap K$ is a subgroup of G.

SAQ 3 Let G = (Z, +); H = (2 Z, +) and K = (3 Z, +). Find $H \cap K$.

3.5 COSETS

Definition :

Let G be a group and let H be a subgroup of G. Let $a \in H$. The left coset of H in G generated by a is the set $aH = \{ah \mid h \in H\}$. The right coset Ha is defined to be the set $Ha = \{ha \mid h \in H\}$.

If G is an Abelian group, then the left and right cosets would be identical. Otherwise a left coset need not be identical with a right coset. We would study more about these facts when we study about normal subgroups. If H is finite, the number of elements in each of the right cosets (left cosets) of H contains exactly as many elements as those in H. To see this suppose H has n elements and these be listed as $H = \{h_1, h_2, \ldots h_n\}$. Let $a \in G$. Then $Ha = \{h_1a, h_2a, \ldots h_na\}$. To see that Ha has n elements, we must ensure that all the elements of Ha are distinct.

If possible let $h_i a = h_j a$. Then $a \in G \Rightarrow a^{-1} \in G$ and $(h_i a)a^{-1} = (h_j a)a^{-1} = h_j(aa^{-1})$ $= h_i(a a^{-1})$. That is $h_i = h_j$. Since H has n distinct elements, Ha also has the same number of distinct element.

Theorem. 6 :

Any two right (left) cosets are either disjoint or identical.

Proof : Let H be a subgroup of a group G and let $a, b \in G$. Then Ha and Hb are two right cosets. If possible let $Ha \cap Hb \neq \phi$. Then we shall show that $Ha = Hb$. Let $x \in Ha \cap Hb$. Then $x \in Ha$. That is, there exists $h_1 \in H$ such that $x = h_1 a$. Similarly, $x \in Hb$ implies $x = h_2 b$.

But $x = h_1 a = h_2 b \Rightarrow a = h_1^{-1} h_2 b$ and $Ha = H h_1^{-1} h_2 b$ (*). But H is a subgroup. Then $h_1^{-1}h_2 \in H$ and $H h_1^{-1} h_2 \subseteq H$. Further if $h \in H$, then $h = h\left(h_2^{-1}\left(h_1 h_1^{-1}\right) h_2\right)$

$= \left(h h_2^{-1} h_1\right)\left(h_1^{-1} h_2\right) \in H h_1^{-1}h_2$. This means that $H \subseteq H h_1^{-1} h_2$, implying $H = Hh_1^{-1}h_2$. Thus by (*) $Ha = Hb$.

Remark : Every element of G is contained in some right coset. For example $a \in G$ is contained in Ha. If G has k distinct right cosets with respect to H then it is possible to express G as a union of these k disjoint right cosets. This observation has far reaching consequences. The relation of belonging to the same right coset between the elements of a group can be seen to be an equivalence relation. This equivalence relation partitions the group into equivalence classes. Each right coset is an equivalence class.

3.6 LAGRANGE'S THEOREM AND APPLICATIONS

One of the most important and very difficult problems in the study of groups is to determine all subgroups of a group. If the given group is finite, the problem could be solved, though it is time consuming, to write all possible subsets and test each subset to determine whether it is a subgroup.

Lagrange's theorem gives a criterion to rule out several of the subsets from being tested for subgroups. This theorem is very fundamental in the study of finite groups.

The number of elements in a group is called the *order of the group.*

Theorem7 : (Lagrange) :

> Let G be a finite group and H a subgroup of G. Then the order of H divides the order of G. [The order of every subgroup of a finite group divides the order of the group].

Proof : Let G be a finite group and H be a subgroup of G. Let G have n elements so that its order is n. Let the m elements of H be written explicitly as

$$H = \{h_1, h_2, \ldots h_m\}$$

If $m = n$, that is if H has all the elements in G, then the theorem is trivially satisfied. Suppose that H is a proper subgroup of G so that G has atleast one element which is not in H. Let $a \in G$, and $a \notin H$. Consider the right coset Ha written explicitly as

$$Ha = \{h_1 a, h_2 a, \ldots h_m a\}$$

Then all the elements of Ha are distinct and are distinct from the elements of H. If all the elements of G are exhausted in H and Ha, then G has $2m$ elements and the theorem is satisfied. If H and Ha do not exhaust all the elements of G, let $b \in G$ and $b \notin H$ or Ha. Consider the right coset Hb written explicitly as

$$Hb = \{h_1 b, h_2 b, \ldots h_m b\}$$

The elements of Hb are m in number and are distinct among themselves and are distinct from the elements of H and Ha. If all the elements of G are exhausted in H, Ha and Hb, then G has 3m elements and the theorem is satisfied. If H, Ha and Hb do not exhaust all elements of G, we continue this process by choosing an element of G which is not in any of the cosets. Since G has finite number of elements, this process must stop in a finite number of steps. If the process stops in k number of steps, then G has k distinct right cosets, each coset consisting of m distinct elements. Thus the number of elements in G = $n = k \times$ (number of elements in H). Thus $n = km$ or m divides n proving that the order of H divides the order of G.

Remark : The converse of the above theorem is not true; the Lagranges theorem states that if a finite group G has a subgroup H, then the order of H divides the order of G. The theorem does not guarantee the existence of a subgroup of a given order even if the order of the subgroup divides the order of the group. We are going to study an example in the coming units where a group of order 12 does not have a subgroup of order 6 even though 6 divides 12.

Definition :

> Let G be a group and e the identity element of G. Let $a \in G$. We mean by the order of the element of a, the least positive integer m such that $a^m = e$. If there is no positive integer m such that $a^m = e$, then a is said to be of infinite order. The order of the identity element is 1. We denote the order of a by o (a).

Example. 1 : Let w be the cube root of unity. Let $S = \{1, w, w^2\}$. We have seen that $(S, \cdot)$ is a group. The identity element of $(S, \cdot)$ is 1. The order of w is the least positive integer m such that

$w^m = 1$. But w being a cube root of unity, $w^3 = 1$ and for $m < 3$, $w^m \neq 1$. Thus the order of w = o $(w) = 3$. Similarly, the order of w^2 is also 3 because $\left(w^2\right)^3 = 1$ and $\left(w^2\right)^m \neq 1$ for $m < 1$.

Example. 2 : We have seen that (Z, +) is a group. 0 is the identity element of (Z, +). Let $a \in Z$ be a non-zero integer. What is the order of a ? If there is a least positive integer m such that $a^m = 0$, then m will be its order. Here a^m means $a + a + \ldots$ m times. This is because the binary operation is '+'. But there is no positive integer m such that $a^m = 0$. Thus o (a) is infinite.

Theorem. 8 :

The order of every element in a finite group is finite.

Proof : Let G be a finite group with the identity e. Let $a \in G$. Since G is closed, $a, a^2, a^3, \ldots$ are all in G. But G is finite. This means all the exponents of a can not be distinct and they must repeat after some stage. Thus there exist two positive integers k and l such that $a^k = a^l$. Without loss of generality we can suppose that $k > l$. This means that $a^{k-l} = e$. Consider the set $S = \{n \mid n$ is a positive integer such that $a^m = e\}$. Then $(k - l)$ belongs to this set S. Since S is a set of positive integers there exists a least positive integer in S. Let this positive integer be denoted by m. Then order of a is m, which is finite. Since a is arbitrary element of G, we conclude that every element of G has finite order.

Corollary : If G is a finite group of order n and a is an element of G of order m. Then m divides n.

Proof : Let $H = \left\{a, a^2, \ldots a^m\right\}$. Now $a^m = e$ and $a^i \neq a^j$. Otherwise if $a^i = a^j$, $a^{i-j} = e$ and $i - j < m$, contradiction that m is the least positive integer such that $a^m = e$. Thus H has m distinct elements and H is a subgroup of G (Verify). By Lagranges theorem m divides n.

SAQ 4 If the order of a finite group is prime then prove that it has no proper subgroups.

Theorem. 9 :

Let G be a group. Then

(i) o (a) = o $\left(a^{-1}\right)$ for any $a \in G$.

(ii) o (a) = o $\left(x^{-1} a x\right)$ for any $a, x \in G$.

(iii) o (ab) = o $(b a)$ for any $a, b \in G$.

Proof : Let e be the identity of G. If o $(a) = m$, then $a^m = e$. Now $\left(a^{-1}\right)^m = \left(a^m\right)^{-1} = e^{-1} = e$. Thus the order of a^{-1} is also m. If a is of infinite order, then there does not exist any positive integer m such that $a^m = e$. Then there does not exist any positive integer such that $\left(a^{-1}\right)^m = e$ thus a^{-1} is also of infinite order. Thus o (a) = o $\left(a^{-1}\right)$.

(ii) Let o $(a) = m$ and o $\left(x^{-1} ax\right) = n$. Consider

$$\left(x^{-1} ax\right)^m = \left(x^{-1} ax\right)\left(x^{-1} ax\right)\left(x^{-1} ax\right) \ldots \left(x^{-1} ax\right), (m \text{ times}).$$

$$= x^{-1} a \left(x x^{-1}\right) a \left(x x^{-1}\right) \ldots ax$$

$$= \underbrace{x^{-1} a \cdot a \ \ldots \ a \cdot x}_{m \text{ times}} x = x^{-1} a^m x = e; \ \left(\because a^m = e\right).$$

implying $n \leq m$.

Now consider,

$$(x^{-1}ax)^n = e = (x^{-1}ax)(x^{-1}ax)(x^{-1}ax)\ldots(x^{-1}ax), (n \text{ times}).$$

$$= x^{-1}a(xx^{-1})a(xx^{-1})\ldots ax$$

$$= x^{-1}a^n x \Rightarrow a^n = e, \text{ implying } m \leq n.$$

Thus $n = m$ and $o(a) = o(x^{-1}ax)$

(iii) For any $a, b \in G$, $ba = e(ba) = a^{-1}(ab)a$

by (ii) $o(ba) = o(ab)$.

Definition :

> Let H be a subgroup of a finite group G. The index of H in G, written as |G : H| is the number of right (left) cosets of H in G. $|G : H| = \frac{o(G)}{o(H)}$.

3.7 WORKEDOUT EXERCISES

Exercise. (i) : Let H and K be two subgroups of a group G. Then prove that HK is a subgroup of G if and only if HK =KH.

Ans : Let HK be a subgroup of G. We are required to prove that HK = KH. Let $h \in H$ and $k \in K$. Since H and K are subgroups, $h^{-1} \in H$ and $k^{-1} \in K$. Consider $hk \in HK$. Then $(hk)^{-1} \in HK$ because HK is a subgroup and $(hk)^{-1} = h_1 \cdot k_1$, for some $h_1 \in H$ and $k_1 \in K$. This implies that

$hk = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} \in KH$. Thus $HK \subseteq KH$. Similarly $kh \in KH$ and $(kh)^{-1} = h^{-1}k^{-1} \in HK \Rightarrow KH \subseteq HK$. Thus KH = HK.

Conversely suppose H and K are subgroups of G such that HK = KH. To show that HK is a subgroup we must verify that HK is non empty and for $a, b \in HK$, $ab^{-1} \in HK$. Since $e \in H$ and $e \in K$, we have that $e \in HK$ and hence HK is not empty. Let $a, b \in HK$. Then $a = h_1 k_1$ and $b = h_2 k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Now $ab^{-1} = (h_1 k_1)(h_2 k_2)^{-1} = (h_1 k_1)(k_2^{-1} h_2^{-1}) = h_1 (k_1 k_2^{-1}) h_2^{-1}$. Now $(k_1 k_2^{-1}) h_2^{-1} \in KH$ and since KH = HK, $(k_1 k_2^{-1}) h_2^{-1} \in HK$.

Thus $(k_1 k_2^{-1}) h_2^{-1} = h_3 k_3$ for some $h_3 \in H$ and $k_3 \in K$. Thus $ab^{-1} = h_1 (h_3 k_3)$

$= (h_1 h_3) k_3 \in HK$. Thus HK is a subgroup of G.

SAQ 5 If H and K are two subgroups of an Abelian group G, then prove that HK is a subgroup of G.

Exercise 2 : If H and K are two finite subgroups of a group G, then prove that $O(HK) = \frac{O(H)\,O(K)}{O(H \cap K)}$. Here $HK = \{ x \in G \mid x = hk, h \in H, k \in K \}$.

Ans : Suppose that $H \cap K = \{e\}$. Then $O(H \cap K) = 1$. Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$ such that $h_1 k_1 = h_2 k_2$. This implies that $h_2^{-1}(h_1 k_1) k_1^{-1} = h_2^{-1}(h_2 k_2) k_1^{-1} \Rightarrow$

$(h_2^{-1} h_1)(k_1 k_1^{-1}) = (h_2^{-1} h_2)(k_2 k_1^{-1}) \Rightarrow$

$(h_2^{-1} h_1) e = e (k_2 k_1) \Rightarrow h_2^{-1} h_1 = k_2 k_1^{-1}$.

But $h_2^{-1} h_1 \in H$ and $k_2 k_1^{-1} \in K$ and $H \cap K = \{e\}$.

Thus $h_2^{-1} h_1 = e \Rightarrow h_2 = h_1$ and $k_2 k_1^{-1} = e \Rightarrow k_1 = k_2$.

Thus the set $HK = \{hk \mid h \in H, k \in K\}$ consists of only distinct elements so that the number of elements in HK is the product of the number of elements of H and the number of elements in K. Thus $O(HK) = O(H) \cdot O(K)$. Now let us suppose that $H \cap K \neq \{e\}$ so that $O(H \cap K) > 1$. Let $x \in H \cap K$. If $h \in H$ and $k \in K$, we can write

$hk = (hx)\left(x^{-1} k\right)$ where $hx \in H$ and $x^{-1} k \in K$. Thus hk is repeated in the product atleast $O(H \cap K)$ times.

If $h_1, h_2 \in H$ and $k_1, k_2 \in K$ be such that $h_1 k_1 = h_2 k_2$,

then $h_1^{-1}\left(h_1 k_1\right)k_2^{-1} = h_1^{-1}\left(h_2 k_2\right)k_2^{-1} \Rightarrow$

$\left(h_1^{-1} h_1\right)\left(k_1 k_2^{-1}\right) = \left(h_1^{-1} h_2\right)\left(k_2 k_2^{-1}\right) \Rightarrow$

$k_1 k_2^{-1} = h_1^{-1} h_2 = u$ (say).

Now u and $u^{-1} \in H \cap K$ and $h_2 = h_1 u$, and

$k_2 = k_1 u^{-1}$. Thus the product is repeated at the most $O(H \cap K)$ times in HK. Thus the term hk appears in the list of HK exactly $O(H \cap K)$ times. Thus

$$O(HK) = \frac{O(H) \cdot O(K)}{O(H \cap K)}$$

Exercise 3 : Let H be a subgroup of a group G and for $a, b \in G$ define $a \equiv b \pmod{H}$ if and only if $a b^{-1} \in H$. Show that $a \equiv b \pmod{H}$ for an $a, b \in G$ is an equivalence relation.

Ans : Let e be the identity of G so that $e \in H$. Since $e = a a^{-1} \in H$, we conclude $a \equiv a \pmod{H}$ and that the relation is reflexive. Let $a, b \in G$ be such that $a \equiv b \pmod{H}$. Then $a b^{-1} \in H$. But H is a subgroup. Thus $a b^{-1} \in H \Rightarrow \left(a b^{-1}\right)^{-1} = b a^{-1} \in H$. That is $b \equiv a \pmod{H}$ and the relation is symmetric. Let $a, b, c \in G$ be such that $a \equiv b \pmod{H}$ and $b \equiv c \pmod{H}$. That is $a b^{-1} \in H$ and $b c^{-1} \in H$. But H is a subgroup implies that $\left(a b^{-1}\right)\left(b c^{-1}\right) = a\left(b^{-1} b\right)c^{-1} = a c^{-1} \in H$. Thus $a \equiv c \pmod{H}$ and the relation is transitive. Thus the given relation is an equivalence relation on G.

Remark : This equivalence relation partitions G into mutually disjoint equivalence classes. For any $a \in G$, let us define the equivalence class of a by $[a] = \{x \in G \mid a \equiv x \pmod{H}\}$.

Then $[a] = Ha$, the right coset of H in G.

Exercise 4 : Let H be a subgroup of a group G. Then

(i) there exists a one-one onto, correspondence (bijection) between any two left cosets of H.

(ii) there exists a one - one, onto correspondence (bijection) between the set of left cosets and the set of right cosets.

Ans : (i) Let a H and b H be any two left cosets of H in G. Define $f : a\,H \to b\,H$ by $f(a\,h) = b\,h$, for $a\,h \in a\,H$, $h \in H$. We are required to verify that f is a bijection. Suppose that $a\,h_1, a\,h_2 \in a\,H$ such that $f(a\,h_1) = f(a\,h_2)$. This implies that $b\,h_1 = b\,h_2$ and that $h_1 = (b^{-1}\,b)\,h_2 \Rightarrow h_1 = h_2$. Thus f is one - one. Let $b\,h \in b\,H$. Then there is $a\,h \in a\,H$ such that $f(a\,h) = b\,h$. Thus f is onto.

(ii) Let $L = \{a\,H \mid a \in G\}$ and $R = \{H\,b \mid b \in H\}$. Define $f : L \to R$ by $f(a\,H) = H\,a^{-1}$. Now we must verify that f is well defined. That is we must verify that if $a_1\,H = a_2\,H$ for $a_1, a_2 \in G$ then $f(a_1\,H) = f(a_2\,H)$. This is obvious because $a_1\,H = a_2\,H$ implies $a_2^{-1}\,a_1 \in H$ and H is a subgroup implies that $a_1^{-1}(a_2^{-1})^{-1} = (a_2^{-1}a_1)^{-1} \in H$. That is $H\,a_1^{-1} = H\,a_2^{-1}$ (or) $f(a_1\,H) = f(a_2\,H)$.

To verify that f is one - one, let $f(a_1\,H) = f(a_2\,H)$ for $a_1, a_2 \in G$.

Then $H\,a_1^{-1} = H\,a_2^{-1} \Rightarrow a_1^{-1}\,a_2 = a_1^{-1}\,(a_2^{-1})^{-1} \in H$. But H is a subgroup. Thus $a_2^{-1}\,a_1 = (a_1^{-1}\,a_2)^{-1} \in H$. Thus $a_1\,H = a_2\,H$ and f is one - one. To verify that f is onto, we observe that for any $Hb \in R$, $b^{-1}.H \in L$ and $f(b^{-1}\,H) = H(b^{-1})^{-1} = Hb$. Thus f is onto.

3.8 SUMMARY

In this unit we have seen that every non-empty subset of a group need not be a subgroup. Only those subsets that are closed under binary operation and satisfy some other conditions form subgroups. If H is a subgroup of G, then for $a \in G$, and $a \notin H$, $a\,H$ and $H\,a$ are called left and right cosets of H in G. A coset need not be a subgroup. We have stated and proved a very important theorem that establishes an arithmatical relationship between the order of a finite group and its subgroup. Using this theorem we deduced that a group whose order is prime can not have any subgroup.

3.9 MODEL EXAMINATION QUESTIONS

Section - A (Long Answer)

i) State and prove a set of conditions under which a non-empty subset of a group may be a subgroup.

ii) State and prove Lagranges theorem for finite groups. Deduce that a group of prime order can not have proper subgroups.

iii) Show that there exists a one-one relationship between left cosets and right cosets of a subgroup of a group.

iv) If H and K are finite subgroups of a group G, prove that $O(HK) = \frac{O(H)\,O(K)}{O(H \cap K)}$.

Section - B (Short Answer)

i) Let G be a finite group. Show that a non-empty subset H of G is a subgroup if and only if it is closed.

ii) Show that any two left cosets are either identical or disjoint.

iii) Verify that the set of even integers under addition is a subgroup of the group of integers under addition. What can be said about the set of odd integers under addition. Justify your answer.

3.10 ANSWERS TO SAQ'S

SAQ 1 No. Because (0, +) is not closed. That is the sum of two odd integers is not odd.

SAQ 2 (Z, +) is a group and Z^+ is an infinite subset of Z such that $a + b \in Z^+$ for $a, b \in Z^+$. But $(Z^+, +)$ is not a subgroup because the identity element $0 \notin Z^+$.

SAQ 3 G = (Z, +) = {0, ±1, ±2, ...}; H = (2Z, +) = {0, ±2, ±4, ±6, ...}

K = (3 Z, +) = {0, ±3, ±6, ±9, ...}; H ∩ K = (6 Z, +) = {0, ±6, ±12, ...}

SAQ 4 Let O (G) = p, prime number. If G has a subgroup H, then the order of H must divide p. But p is a prime number and has no proper divisors. Thus G can not have a proper subgroup.

SAQ 5 Since HK = KH is satisfied, HK is a subgroup.

UNIT–4: SOME INTERESTING GROUPS AND SUB GROUPS

Contents

4.1 Aims and Objectives
4.2 Introduction
4.3 Cyclic groups
4.4 Permutation groups
4.5 Examples from Geometry
4.6 Summary
4.7 Model Examination Questions
4.8 Answers to Self Assessment Questions

4.1 AIMS AND OBJECTIVES

By the time you complete this unit you would be able to : (i) State and prove some important reltionships between cyclic groups and their subgroups, (ii) Perform composition of permutations and decompose cycles into transpositions, (iii) List all the elements of S_3, A_3, S_4 and A_4 and determine the orders of their elements, (iv) Determine the subgroups of S_3 and A_4 and prove that A_4 has no subgroup of order 6.

4.2 INTRODUCTION

In the previous units we have defined groups, subgroups and proved certain theorems. All this theory will not be of much value unless we give some important and interesting examples to which all this theory applies. Of all kinds of groups we come across, the cyclic groups are very elegant and simple to deal with. Cyclic groups are some special kinds of groups in which every element of the group can be generated by a single element of the group. Cyclic groups are necessarily abelian, though all abelian groups are not cyclic. Permutation groups, on the other hand, are non abelian and provide abundant examples to verify the theory learnt in earlier units. We will be using the examples from this unit in the next units of this Block.

4.3 CYCLIC GROUPS

Let $(G, \cdot)$ be a group and let $a \in G$. Then the set $H = \{a^n / n \in Z$, the set of integers$\}$ is a subset of G, generated by a. Then $(H, \cdot)$ will be a group and is called a cyclic subgroup of G. The element 'a' is called the generator of H. We write $H = \langle a \rangle$.

SAQ 1 Let G be a group and $a \in G$. Show that $H = \{a^n / n \in Z\}$ is a subgroup of G.

Definition 1 :

A group G is said be a **cyclic group** if there exists an element $a \in G$, such that every element of G can be written as 'an integer power of 'a'. The element 'a' is called a generator of G. If G is a cyclic group with 'a' as a generator, we write $G = \langle a \rangle$.

Remark : If the binary operation in G is addition, then every element of the cyclic group G should be obtained by repeated addition of the generator of a. Thus instead of writing $\underset{n \text{ times}}{a \cdot a \ldots . a} = a^n$ we write $\underset{n \text{ times}}{a + a \ldots . + a} = na$

Example 1 : Let w be a cube root of unity we have seen that $G = \left(\{1, w, w^2\}, \cdot\right)$ is a group. This is an example of a cyclic group because every element can be expressed as an integral power of w. Notice here that $w^3 = 1$.

Thus G is a finite cyclic group generated by w and its order is 3. Notice is w^2 is also a generator of G because $\left(w^2\right)^2 = w$ and $\left(w^2\right)^3 = 1$.

Example 2 : Let $i^2 = -1$, the set $\{1, -1, i, -i\}$ together with the binary operation of multiplication is a cyclic group generated by 'i'. Here $i^2 = -1, i^3 = i^2 \cdot i = -i, i^4 = \left(i^2\right)^2 = 1$. Thus every element of the set can be expressed as the integral power of a single element i. Notice that $-i$ is also a generator because $(-i)^2 = -1$; $(-i)^3 = i$, $(-i)^4 = 1$. There are no other generators.

Example 3 : Let $(Z, +)$ denote the group of integers. Since the group operation is addition, every integer $\in Z$ can be expressed as a power (repeated addition in this case) of a single element 1 (or -1). For example $2 \in Z = 1 + 1$, etc. Thus $(Z, +)$ is an infinite cyclic group generated by 1. i.e $Z = <1> = \{n \cdot 1 \,/\, n \in Z\}$ or $Z = <-1> = \{n \cdot (-1) \,/\, n \in Z\}$. Notice here that this cyclic group has too generators 1 and -1. Any other element is not a generator of $(Z, +)$. For example 2 is not a generator of $(Z, +)$ because $3 \in Z$ and $3 \neq 2 + 2 + \ldots$ or $3 \neq n \cdot 2$ for any $n \in Z$ (that is 3 can not be generated by 2).

Example 4 : $\left(Z_6, \oplus\right)$, the group of integers modulo 6 under modulo addition is an example of a cyclic group of order 6. Observe that $Z_6 = \{0, 1, 2, 3, 4, 5\}$. $3 \oplus 5 = 2$; $2 \oplus 5 = 1$, $2 \oplus 4 = 0$; $3 \oplus 4 = 1$, $1 \oplus 2 = 3$ etc. What are the generators of $\left(Z_6, \oplus\right)$? The gnerators are 1 and 5. Here 5 is the additive inverse of 1, (i.e -1 in $(Z, +)$).

SAQ 2 What are the generators of $\left(Z_5, \oplus\right)$? Verify that this cyclic group has 4 generators.

Theorem 1 :

Every cyclic group is abelian but not conversely.

Proof : Let $(G, \cdot)$ be a cyclic group generated by 'a' $\in G$. Then every element of G is of the form a^n, for some $n \in Z$. Let a^s and a^t be two elements of G. Then $a^s \cdot a^t = a^{s+t} = a^{t+s} = a^t \cdot a^s$. Here we have used the fact that addition of integers is commutative. Since $a^s \cdot a^t = a^t \cdot a^s$ for any two elements a^s and a^t of G, G is commutative.

To see that the converse of this theorem is not ture, we must produce an example of an abelian group which is not cyclic. We have already seen the Klein 4-group (example 8 of unit 1) is an abelian group consisting of 4 elements $\{1, a, b, ab\}$ in which $a^2 = b^2 = 1$ and $ab = ba$. Thus Klein 4-group is an abelian group. But it is not cyclic because none of the four elements generate the other elements. The abelian group $(Q, +)$ the group of rational numbers under addition is an abelian group. But it is not cyclic because it is not possible to generate every element of Q through a single element of Q.

Theorem 2 :

Every subgroup of a cyclic group is cyclic.

Proof : Let (G, ·) be a cyclic group and (H, ·) be a subgroup of (G, ·). Let 'a' be a generator of G so that G = $<a>$ and every element of G is of the form a^s for $s \in Z$. Since H is a subgroup of G, H $\subset$ G. Hence everfy element of H is of the form a^r where $r \in Z$. If H = $\{e\}$, the trivial subgroup consisting of the identity alone, then H = $< a^0 = e >$ and the theorem is trivially true. So let us assume that H $\neq \{e\}$. Let m be the least positive integer such that $a^m \in H$. Let be $b \in H$. Then $b = a^m \in H$. Let $b \in H$. Then $\exists$ a $n \in Z \ni a^n = b$. By Euclid's algorithm, there exist unique integers q and r such that

$$n = mq + r, 0 \leq r \leq m.$$

Then $b = a^n = a^{mq+r} = a^{mq} \cdot a^r$

That is : $a^r = a^{n-mq}$. H is a subgroup implies that $a^n \in H$ and $a^{-mq} \in H$ so that $a^r \in H$. But m is the least positive integer such that $a^m \in H$. Thus $r = 0$ and $n = mq$. This means that every element is H can be expressed as a power of a^m. Thus H is cyclic generated by a^m.

Theorem 3 :

If (G, ·) is a finite group whose order is a prime (number) then G is cyclic.

Proof : Since G is of prime order, o (G) ≥ 2. Let $e \in G$, be the identiry element of G. Let $a \in G$ and H = $< a >$, where a is distinct from e. Such an 'a' exists because o (G) ≥ 2. Now H is a subgroup of G. By Lagranges theorem o (H) must divide o (G). But o (G) = p, a prime (that is p has no divisors other than 1 and itself). Thus o (H) is 1 or p. But o (H) $\neq 1$ because $a \neq e$. Thus o (H) = p. That is H = G and G = $< a >$ and hence cyclic.

Theorem 4 :

If 'a' is a generator of a cyclic group (G, ·) then a^{-1} is also a generator of (G, ·)

Proof : If G = $\{e\}$, then $a = e = a^{-1}$ and the theorem is trivall, true. Let o (G) > 1. Then $a \neq e$ and G = $< a > = \{a^m / m \in Z\}$. Now $a \in G$ and G is group implies $a^{-1} \in G$. Now $a^m = \left(a^{-1}\right)^{-m}$ for any $m \in Z$, we see that G = $< a^{-1} > = \left\{ \left(a^{-1}\right)^{-m} / -m \in Z \right\}$. Thus a^{-1} is a generator of G.

Theorem 5 :

An infinite cyclic group has exactly two generators.

Proof : Let (G, ·) be a cyclic group generated by 'a'. Then by theorem 4 (of this unit), a^{-1} is aslo a generator (G, ·). Since G in infinite cyclic group, there does not exist any positive integer m such that $a^m = e$, the identity. That is $a^m = e$ implies that $m = 0$. Let $b \in G$, be a generator of (G, ·). Then $b = a^t$ for some $t \in Z$. G is a group and hence $a^{t+1} \in G$. Thus there exists an $r \in Z$ such that $a^{t+1} = \left(a^t\right)^r = a^{tr}$. Then $a^{t+1-tr} = e$ implying that $t(r-1) = 1$. Since t and $(r-1) \in Z$, it follows that either $r - 1 = t = 1$ or $r - 1 = t = -1$. Thus $b = a$ or $b = a^{-1}$. Thus G has exactly two generators.

Before we state and prove the next theorem let us recall that (i) An integer a which divides integers b and c called a common divisor. (ii) An integer d is called the greatest common divisor of two integers b and c if d is a common divisor of b and c and every common divisor of b and c divides d. We denote the g.c.d of b and c by (b, c). (iii) If $(b, c) = 1$, then b and c are called relatively prime. (iv) If $(b, c) = 1$, there exist integers m and n such that $mb + nc = 1$.

Theorem 6 :

Let (G, ·) be a finite cyclic group of order n (>1) and let 'a' be a generator of G. Then a^m is a generator of G if and only if $m < n$ and $(m, n) = 1$, (m being positive integer).

Proof : Let e be the identity element of G. Since $n > 1$, $a \neq e$. Let $G = \langle a \rangle = \{a^r / r = 0, 1, 2, \ldots, (n-1)\}$. Let m be a positive integer such that $m < n$ and m is relatively prime to n. Let $H = \langle a^m \rangle$ so that $H \subseteq G$. Since $(m, n) = 1$, there exist integers u and b such that $mu + nb = 1$. Hence $a^{mu+nb} = a^1 \Rightarrow (a^m)^u (a^n)^b = a$. But $a^n = e$ and $e^b = e$. Thus $(a^m)^u = a$ implying that $a \in H$. But H is a subgroup and $G = \langle a \rangle \subseteq H \Rightarrow H = G$ and that a^m is a generator of G.

Conversely suppose that a^m, for some positive integer $m < n$ be a generator of G. Since $a \in G$, there exists a positive integer u such $(a^m)^u = a$ or $a^{mu-1} = e$. Since $a^n = e$, and $mu - 1 > n$, we get that n is a divisor of $(mu - 1)$. This means there exists integer b such that $mu - 1 = nb$ or $mu - nb = 1$. But $m \cdot u + n(-b) = 1$ implies $(m, n) = 1$.

Remark : If G is a finite cyclic group of order n, then the number of generators is equal to the number of positive integers less than n and prime to n. For example the number of generators of a cyclic group of order 5 is 4, because there are 4 positive integers less than 5 and prime to it. The number of positive integers less than and prime to n is denoted by $\phi(n)$ and ϕ is called the Euler totient function. ϕ has many interesting properties.

Theorem 7 :

If $(G, \cdot)$ is a finite cyclic group of order n and m is a divisor of n, then there exists exactly one subgroup H of G of order m. H is also cyclic.

Proof : Let a be a generator of G. Since m divides n, write $n = mq$, where $q \in Z$. Let $H = \{a^q / q \in Z\}$. Then H is a subgroup of G and $o(H) = m$. If possible let a^s and a^r be two elements of order m in G. That is :

$$o(a^r) = m \text{ and } o(a^s) = m.$$

Then $(a^s)^m = (a^r)^m = a^n$ implying $sm = rm$ and $s = r$. H is a unique subgroup of order m. H is cyclic follows from Theorem 2.

SAQ 3 Find all subgroups of the cyclic group $(Z_{10}, \oplus)$

4.4 PERMUTATION GROUPS

Let S be a nonempty set. A bijection of S onto S is called a permutation of S. A permutation of S gives a rearrangement of elements of S among themselves. In general S may be a finite set or an infinite set. For this course we will confine ourselves to situations where S is a finite set.

Let S be a finite set consisting of n elements and whose elements are denoted by the symbols 1, 2, ..., n. No arithmatical meaning is to be attached to these integers except that they are distinguish able from one another. It is convenient to represent a permutation $f : S \to S$ by writing the elements of S in first row and the corresponding images in the second row as :

$$f = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ f(1) & f(2) & f(3) & \ldots & f(n) \end{pmatrix}$$

Notice here that $f(1), f(2), f(3) \ldots f(n)$ are again 1, 2, 3, ... n is some order. Further the order of elements in the first row is not important as long as the correct image is written under each symbol.

If S has n elements, the number of bijection mappings are equal to the number of permutations of the n elements in S. But there are n ! (factorial n) number of permutations of n elements among themselves. Let S_n denote the set of all permutations of S. If f and g are two permutations in S_n , let us define an operation "Composition of mappings" on S_n . Which is same as the composition of mappings which we have seen in unit 1. Thus if f and g are two permutations given by :

$$f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix} \text{ and } g = \begin{pmatrix} 1 & 2 & \dots & n \\ g(1) & g(2) & \dots & g(n) \end{pmatrix}$$

define $g \, o \, f$ by :

$$g \, o \, f = \begin{pmatrix} 1 & 2 & \dots & n \\ g(1) & g(2) & \dots & g(n) \end{pmatrix} o \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & \dots & n \\ g(f(1)) & g(f(2)) & \dots & g(f(n)) \end{pmatrix}$$

Clearly $g \, o \, f$ is also a permutation of S, and the operation is a binary composition.

Example 5 : Let S = {1, 2, 3}. The three elements in S could be permuted among themselves in 3! = 6 ways. Let us write these six elements explicitely with their actions.

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \text{ where } f_1(1) = 1; f_1(2) = 2; f_1(3) = 3.$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \text{ where } f_2(1) = 1; f_2(2) = 3; f_2(3) = 2.$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \text{ where } f_3(1) = 2, f_3(2) = 1; f_3(3) = 3.$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \text{ where } f_4(1) = 2; f_4(2) = 3; f_4(3) = 1.$$

$$f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \text{ where } f_5(1) = 3; f_5(2) = 1; f_5(3) = 2.$$

$$f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \text{ where } f_6(1) = 3; f_6(2) = 2; f_6(3) = 1.$$

Consider

$$f_2 \, o \, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ f_2(f_3(1)) & f_2(f_3(2)) & f_2(f_3(3)) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ f_2(2) & f_2(1) & f_2(3) \end{pmatrix}, \text{ substituting } f_3(1), f_3(2) \text{ and } f_3(3).$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$ substituting $f_2(2), f_2(1)$ and $f_2(3)$.

$= f_5$, by definition of f_5.

Remark : After some time the student should be able to write the product directly, by observing :

$$f_2 \, o \, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ & \downarrow & \\ 1 & 3 & 2 \end{pmatrix} o \begin{pmatrix} \downarrow & & \\ 1 & 2 & 3 \\ \downarrow & & \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ & & \\ 3 & ? & ? \end{pmatrix}$$

In the right most bracket $1 \to 2$ and in the left bracket $2 \to 3$. Thus $1 \to 2 \to 3$ implies $1 \to 3$. Similarly $2 \to 1 \to 1 \Rightarrow 2 \to 1$ and $3 \to 3 \to 2 \Rightarrow 3 \to 2$. Thus the blanks could be filled in.

SAQ 4 Compute $f_3 \, o \, f_2$.

SAQ 5 Compute $f_2 \, o \, f_2$.

Example 6 : Let $S = \{1, 2, 3, 4\}$ and let f and g be defined by :

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}; \; g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

$$\text{Then } f \, o \, g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} o \begin{pmatrix} \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & & 4 \end{pmatrix}$$

Rule : $(f \; o \; g)(1) = f(g(1)) = f(1) = 3$; $(f \; o \; g)(2) = f(g(2)) = f(3) = 2$

$(f \; o \; g)(3) = f(g(3)) = f(2) = 1$; $(f \; o \; g)(4) = f(g(4)) = f(4) = 4$.

$$g \, o \, f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

Rule : $(g \; o \; f)(1) = g(f(1)) = g(3) = 2$; $(g \; o \; f)(2) = g(f(2)) = g(1) = 2$

$(g \; o \; f)(3) = g(f(3)) = g(2) = 3$; $(g \; o \; f)(4) = g(f(4)) = g(4) = 4$.

Theorem 8 :

> Let S be a non empty set with n symbols. The set of permutations S_n of S is a group of order $n!$ under the compostition of mappings (This group is called the symmetric group on n symbols and is denoted by S_n).

Proof : Recall that a permutation is a bijection and the composition of two bijective mappings is again a bijective mapping. Thus if f and $g \in S_n$ then $f \, o \, g$ also belongs to S_n. Thus the operation is a binary operation. Thus (S_n, o) satisfies the closure property. Since composition of mappings is associative, (S_n, o) satisfies the associativity property. Since S_n consists of all bijective mappings of S onto itself S_n consists of the identity mapping 'e' satisfying the property that $f \, o \, e = e \, o \, f = f$

for all $f \in S_n$. Recall that if $f : S \to S$ is a one-one onto mapping (or a bijection), then $f^{-1} : S \to S$ exists and $f \circ f^{-1} = f^{-1} \circ f = e$, the identity mapping $e : S \to S$. Thus every element in S_n has an inverse. Since (S_n, o) satisfies all the postulates of a group, (S_n, o) forms a group. The order of the group S_n is the number of elements in S_n. This is the number of permutations of n elements among themselves. Thus $o(S_n) = n!$. Since the composition of mappings is not commutative (in general), S_n is not commutative (if $n \geq 3$).

Remark: The identity element in S_n is an identity permutation given by $e = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$. The identity permutation maps each symbol onto itself. If $f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix} \in S_n$, then $f^{-1} = \begin{pmatrix} f(1) & f(2) & \dots & f(n) \\ 1 & 2 & \dots & n \end{pmatrix}$. Since $f(1), f(2), \dots f(n)$ are $1, 2, \dots, n$ in some order, f^{-1} could be rearranged with $1, 2, \dots n$ in the first row and the corresponding images in the second row. For example the inverse image of $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \in S_3; f_2^{-1} = \begin{pmatrix} 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_2$.

Similarly $f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}; f_4^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_5$ etc.

Example 7 : S_3 is non - abelian group. From example 5, $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$. We construct the multiplication table. (Verify each entry in the table by working out the composition independently)

$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}; f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}; f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

(i) f_1 is the identity element

(ii) $f_1^{-1} = f_1; f_2^{-1} = f_2; f_3^{-1} = f_3; f_4^{-1} = f_5; f_5^{-1} = f_4; f_6^{-1} = f_6;$

(iii) $o(f_4) = o(f_5) = 3$

$o(f_1) = o(f_2) = o(f_3) = o(f_6) = 2;$

o	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_6	f_5	f_1	f_2
f_5	f_5	f_6	f_2	f_1	f_4	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

(iv) S_3 is not abelian because $f_2 \circ f_4 = f_5; f_4 \circ f_2 = f_6$.

(v) S_3 has 4 subgroups. These are : $\{f_1, f_2, f_3\}, \{f_1, f_4\}, \{f_1, f_5\}, \{f_1, f_6\}$.

Definition 3 :

Let S be a finite set with n elements. Let $a_1, a_2, \ldots a_k$ be k distinct integers between 1 and n. A permutation $f \in S_n$ is called a cyclic permutation or a cycle of length k, if $f(a_1) = a_2$, $f(a_2) = a_3, \ldots f(a_k - 1) = a_k$ and $f(a_k) = a_1$ and $f(a_l) = a_l$ for $a_l \notin \{a_1, a_2, \ldots a_k\}$. If f is a cycle of length k, then this is written as $(a_1, a_2, \ldots a_k)$ indicating that each element is mapped onto its next and the last element on to the first. That is

$$(a_1, a_2, \ldots a_k) = \begin{pmatrix} a_1 & a_2 & \ldots & a_k \\ a_2 & a_3 & \ldots & a_1 \end{pmatrix}$$

Theorem 9 :

Let f be a permutation of a finite set S. Then any two cycles of f are disjoint. Further any two disjoint cycles commute with each other.

Proof : Let $x = (a_1, a_2, \ldots a_k)$; $y = (b_1, b_2, \ldots b_l)$ be two distinct cycles of f. Then x and y could be writtes as $x = (a_1, f(a_1), f^2(a_1), \ldots f^{k-1}(a_1))$ and

$y = (b_1, f(b_1), f^2(b_1), \ldots f^{k-1}(b_1))$. If we define a relation R on the set S by a R b if and only if there is an integer k such that $f^k(a) = b$ for $a, b \in$ S, then we see that R is an equivalence relation. Each equivalence class consists of elements in a cycle. Since any two equivalence classes are disjoint if they are not identical, we conclude that any two cycles are disjoint.

To show that two disjoint cycles commute, we have to verify that $(x \circ y)\, z_i = (y \circ x)\, z_i$ where z_i is any element of S. We need to consider three cases : (i) $z_i \in x$, (ii) $z_i \in y$ and (iii) $z_i \notin x$ or y. Case (i) : If $z_i \in x$, then by the definition of a cycle $x(z_i)$ is also in x.

In this case $z_i \notin y$ and $x(z_i) \notin y$. Thus $y(z_i) = z_i$ and $y(x(z_i)) = x(z_i)$. Hence

$$(x \circ y)\, z_i = x(y(z_i)) = x(z_i) \text{ and}$$

$$(y \circ x)\, z_i = y(x(z_i)) = x(z_i)$$

Case (ii) and Case (iii) can be similarly disposed of. Thus any two disjoint cycles commute.

SAQ 6 Show that the relation of belonging to the same cycle is an equivalence relation.

Example 8 : Express $f \in S_7$ given by $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 7 & 5 & 4 & 1 & 6 \end{pmatrix}$ as a product of two disjoint cycles. Here $f(1) = 2$; $f(2) = 3$, $f(3) = 7$, $f(7) = 6$ and $f(6) = 1$. Thus (1, 2, 3, 7, 6) is a cycle. $4 \in f$ and $4 \notin (1, 2, 3, 7, 6)$. Now $f(4) = 5$ and $f(5) = 4$ and (4, 5) is a cycle. Thus

$$f = (1, 2, 3, 7, 6)\,(4, 5).$$

Theorem 10 :

Any non identity permutation in S_n can be expressed uniquely as a product of disjoint cycles of length greater than 1, except for the orders in which the cycles are written.

Proof : Let f be a non identity permutation $\in S_n$. Let a_1 be an arbitrary element of S. Consider the elements :

$$a_1, f(a_1), f^2(a_1), \ldots$$

Since f is finite, all these elements can not be distinct. Let $f^r(a_1)$ be the first repetition, so that $f^r(a_1) = a_1$. Then the ordered r - triple

$$\sigma_1 = \left(a_1, f(a_1), \ldots, f^{r-1}(a_1)\right)$$

is a cycle of length r. If b is another element of S and $b_1 \notin \sigma$, consider

$$b_1, f(b_1), f^2(b_1), \ldots$$

All these elements can not be distinct and let $f^s(b_1)$ be the first repetition in this set. Then

$$\sigma_2 = \left(b_1, f(b_1), \ldots, f^{s-1}(b_1)\right)$$

is another cycle of length s. Since S is finite this process can be repeated till all the elements of S are exhausted. Further the cycles being disjoint, the order in which they are written is not important.

To see that this representation is unique, let $f = \sigma_1 \sigma_2 \ldots \sigma_k = \rho_1 \rho_2 \ldots \rho_m$ where ρ_i are cycles of length > 1. Let $a_i \in \sigma_i$. Then $a_i \in S$. Then a_i must belong to one of the cycles ρ_i say $a_i \in \rho_j$. Since any two cycles are either disjoint or identical we get $\sigma_i = \rho_j$. Thus each σ_i is some ρ_j and vice - versa, and the ρ_j are σ_i written in a different order.

Definition

A cycle of length 2 is called a **transposition.**

Theorem 11 :

Every permutation of S_n is a product of transpositions.

Proof : Theorem 10 asserts that every permutation is a product of disjoint cycles of length > 1. Let $(a_1, a_2, \ldots a_n)$ be any cycle. Then the product can be written as a product of transpositions. This expression need not be unique nor the transpositions disjoint.

For example : $(a_1, a_2, \ldots a_n) = (a_n, a_1)\ (a_{n-1}, a_1) \ldots (a_2, a_1)$. In case of a cycle of length 1 say a_i, we can write $(a_i) = (a_i, x)\ (x, a_i)$ where $x \neq a_i$ and $x \in S$. Thus any permutation is a product of transpositions.

Example 9 :

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix} = (1, 5)\ (2, 3, 4)$$

$$= (1, 5)\ (2, 4)\ (2, 3) = (1, 5)\ (4, 3)\ (4, 2)$$

$$= (2, 3)\ (1, 5)\ (2, 3)\ (4, 3)\ (4, 2)$$

Thus the expressions for a permutation as a product of transpositions is not unique. But the number of transpositions which, occur in a product is either always odd or always even.

SAQ 7 Express the cycle (1, 2, 3, 4) as a product of transpositions in the different ways.

Theorem 12 :

Let $f \in S_n$. In all the expressions of f as a product of transpositions, the number of transpositions is either always even or always odd.

Proof : We prove the theorem by induction. Let $f = \sigma_1 \sigma_2 \ldots \sigma_r$ be the expression of f as a product of disjoint cycles each of length > 1. Let $|\sigma_i|$ denote the length of cycle σ_i. Define $|f| = \sum_{i=1}^{r} \left(|\sigma_i| - 1\right)$. Cycles of lenth 1 do not contribute to $|f|$. Thus for any $f \in S_n$, $|f|$ is a unique positive integer. If σ_i is a transposition, then $|\sigma_i| = 2$ and $\left(|\sigma_i| - 1\right) = 1$. This implies that $|f|$ is an even integer or odd integer according as the number of transpositions in f is even or odd. Let $a, b \in S$. Then

$$(a, b)\left(a, x_1, \ldots x_m, b, y_1, \ldots y_n\right) = \left(b, y_1, \ldots y_n\right)\left(a, x_1, \ldots, x_m\right) \text{ and}$$

$$(a, b)\left(b, y_1, \ldots y_n\right)\left(a, x_1, \ldots x_m\right) = \left(a, x_1, \ldots x_m, b, y_1, \ldots y_n\right).$$

This implies that

$$|(a, b) f| = \begin{cases} |f| - 1, \text{ if } a, b \text{ occur in the same cycle of } f \\ |f| + 1, \text{ if } a, b \text{ occur in different cycles of } f \end{cases}$$

Thus $|(a, b) f| = |f| \pm 1$

Suppose that $f = \left(a_1, b_1\right)\left(a_2, b_2\right) \ldots \left(a_n, b_n\right)$

If $n = 1$, $f = \left(a_1, b_1\right)$ and $|f| = 2 - 1 = 1$.

Thus $|f|$ and the number of transpositions are both odd and the theorem is true for $n = 1$.

Assume the theorem to be true for every permutation expressed as a product of $(n - 1)$ transpositions. Then $\left(a_1, b_1\right) f = \left(a_1, b_1\right)\left(a_1, b_1\right)\left(a_2, b_2\right) \ldots \left(a_n, b_n\right)$.

$$= \left(a_2, b_2\right) \ldots \left(a_n, b_n\right)$$

because $\left(a_1, b_1\right)\left(a_1, b_1\right) = e$, the identity.

But by induction hypothesis $\left|\left(a_1, b_1\right) f\right|$ and $(n - 1)$ are both even or both odd. Since $\left|\left(a_1, b_1\right) f\right| = |f| \pm 1$, we conclude that $|f|$ and n are both odd, or both even.

Remarks : There are several ways this theorem could be proved. An interested student may refer to books given in references to get other proofs.

Definition :

A permutation $f \in S_n$ is said to be even or odd according as whether it can be expressed as a product of even number of transpositions or odd number of transpositions. As a thumb rule any cycle consisting of odd number of elements is an even permutation where as any cycle consisting of even number of letters is an odd permutation.

Theorem 13 :

In S_n, exactly half of the permutations are even and the rest half of the permutations odd.

Proof : Recall that $o\left(S_n\right) = n!$ Let $f_1, f_2, \ldots f_r$ be the even permutations and $o_1, o_2, \ldots o_s$ be the odd permutations of S_n. Then $r + s = n!$. Since no even permutation is odd and vice vessa, if we

multiply the r even permutations by a transposition T, then the r even permutations are transformed into r odd permutations. This implies that $r \leq s$. A similar argument shows that $s \leq r$. Thus $r = s$ and $r + s = n!$ imples that $r = s = \frac{1}{2}(n!)$.

Theorem 14 :

> The product of two even permutations is even, the product of two odd permutations is even, where as the product of an even permutation and an odd permutation is odd.

Proof : Recall that a permutation is even or odd according as it is the product of even number of transpositions or odd number of transpositions. The proof of the theorem follows from the fact that the sum of the even integers is even, the sum of two odd integers is even where as the sum of an even integer and an odd integer is odd.

Theorem 15 :

> The set of even permutations A_n of S_n $(n \geq 2)$ is a group of order $\frac{1}{2}(n!)$.
> (This group of even permutations is called an alternating group).

Proof : The Operation of composition of mappings is a binary operation, since the product of two even permutations is even. The identity permutation is an even permutation and hence $\in A_n$. If $f \in A_n$ is an even permutation, then f^{-1} obtained by writing these even number of transpositions in the reverse order is also an even permutation and hence $\in A_n$. The associativity of even permutations follows from the associativity of mappings. Thus A_n satisfies all the postulates of a group. Hence A_n is a subgroup of S_n. Since there are $\frac{1}{2}(n!)$ even permutations, $o(A_n) = \frac{1}{2}(n!)$.

SAQ 8 Do the set of odd permutations form a subgroup of S_n under the composition of mappings?

Example : Recall S_3. Writing in form of cycles we see that $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = e = (1)(2)(3)$ is an even permutation.

$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (1, 2, 3)$ is an even permutation

$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (1, 3, 2)$ is an even permutation

$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = (2, 3)$ is an odd permutation.

$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (1, 2)$ is an odd permutation

$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = (1, 3)$ is an odd permutation

Thus $A_3 = \{e, (1, 2, 3), (1, 3, 2)\}$ is of order 3.

Notice that A_3 is a cyclic, group generated by $(1, 2, 3)$, because $(1, 2, 3)\ (1, 2, 3) = (1, 3, 2)$,

$\{e, (2, 3)\}, \{e, (1, 2)\}, \{e, (1, 3)\}$ are three subgroups of order 2. Each of these groups is cyclic.

Enample 11 : Let $S = \{1, 2, 3, 4\}$. Then $o(S_4) = 4!$ and $o(A_4) = \frac{1}{2}(4!) = 12$. Let us list all the 12 even permutations of S_4 in the form of cycles. Recall an even permutation is either a cycle of length 3 or a product of two transpositions.

Thus $A_4 = \{e, (1, 2, 3), (1, 3, 2), (1, 2, 4), (1, 4, 2),$

$(1, 3, 4), (1, 4, 3), (2, 3, 4), (2, 4, 3),$

$(1, 2)(3, 4), (2, 3)(1, 4), (1, 3)(2, 4)\}$.

Notice here $(1, 2)(3, 4)$ is an even permutation. In case of difficulty the student is advised to write (at least initially) the cycles in the eloborate from.

For example

$$(1, 2, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \text{ etc., and } (1, 2)(3, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \text{ etc.}$$

A_4 being a group of order 12 has several sub groups. We write some of them below.

$H_1 = \{e, (1, 2, 3), (13, 2)\}$ of order 3;

$H_2 = \{e, (1, 2)(3, 4)\}$ of order 2 etc.

Remark : The Lagrange's theorem for finite groups states that the order of a finite group is divisible by the order of its subgroup. The converse of Lagranges theorem need not be true. Consider A_4, a group of order 12. A_4 has no sub group of order 6, though 6 divides 12.

Example 12 : A_4 has no subgroup of order 6. If possible let H be a subgroup of order 6 of A_4. Then H is not cyclic because no element of A_4 is of order 6 and H has no element of order 6. Since H is a subgroup H must have the identity element. Let H be written explicitely as $H = \{e, h_1, h_2, h_3, h_4, h_5\}$ where $h_1, h_2, h_3, h_4, h_5 \in A_4$. Now A_4 has 8 elements of order 3. These are $(1, 2, 3), (1, 3, 2), (1, 2, 4), (1, 4, 2), (1, 3, 4), (1, 4, 3), (2, 3, 4), (2, 4, 3)$. This can be verified easily as $(1, 2, 3) \, o \, (1, 3, 2) = (1) (2) (3) = e$ and $(1, 2, 3) \, o \, (1, 3, 2) = (1) (2) (3) = e$.

Thus $(1, 3, 2)$ is the inverse of $(1, 2, 3)$. Similarly others

Thus the eight elements of order 3 can be paired into four pairs, each pair consisting of an element and its inverse. Further A_4 has 3 elements of order 2. These are : $(1, 2)(3, 4)$; $(1, 3)(2, 4)$; $(1, 4)(2, 3)$. Notice here $(1, 2)(3, 4) \, o \, (1, 2)(3, 4) = (1)(2)(3)(4) = e$.

Since H is a subgroup, every element of H should have its inverse included in H. Thus the five elements h_1, h_2, h_3, h_4 and h_5 can not be all elements of order 3 and the elements of order 3 must appear in pairs : an element and its inverse. Also all the elements of H can not be elements of order 2 because there are only three such elements. Thus H must have

(i) three elements of order 2 and two elements of order 3, or

(ii) one element or order 2 and four elements of order 3

Case (i) : Without loss of generality let

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

Then $(1, 2)(3, 4)(1, 2, 3) = (2, 4, 3) \notin H$,

contradicting the clossure property. Thus H is not a subgroup.

Case (ii) Without loss of generality let

$$H = \{e, (1, 2, 3), (1, 3, 2), (1, 2, 4), (1, 4, 2), (1, 2)(3, 4)\}.$$

Then $(1, 2)(3, 4) \, o \, (1, 2, 3) = (2, 4, 3) \notin H$.

Thus H is not a subgroup.

Thus no six elements can be chosen from A_4 so that they form a subgroup.

Thus A_4 has no subgroup of order 6.

SAQ 9 Every element of A_n $(n > 3)$ is a product of 3 cycles.

4.5 EXAMPLES FROM GEOMETRY

Ancient study of mathematics laid more emphasis on the study of geometry and ignored algebra. It is the french mathematician and philosopher Descartes who fused algebra and geometry to create 'coordinate geometry' or 'analytical geometry'. It is Felix Klein in the later part of 19th century who unified the study of different geometries using the notion of a group. His "ERLANGEN PROGRAM" opened up new possibilities for the study of groups.

Let us recall that $\mathbf{R} \times \mathbf{R} = \{(x, b) \mid x, b \in \mathbf{R}\}$ is the usual coordinate plane we are familiar with. Let us write $\mathbf{R} \times \mathbf{R} = \mathbf{R}^2$. A motion of $\mathbf{R}^2$ is a permutation of $\mathbf{R}^2$ or a bijection of $\mathbf{R}^2$ onto itself.

A Linear motion of $\mathbf{R}^2$ is a transformation which maps the point (x, y) onto the point (x', y') when $x' = ax + by$, $y' = cx + dy$ and $ad - bc \neq 0$. We can see that the set of linear motions under the operation of composition form a group. This group is called the general linear group and is denoted by GL (2, R). Writing the transformation in the matrix form :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ s \end{pmatrix}, \text{ where } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ is a non singular matrix,}$$

we see that $A = I$ gives the identity element of the group and A^{-1} gives the inverse element of A mapping (x', y') onto (x, y).

A translation of $\mathbf{R}^2$ is a motion which maps the point (x, y) onto (x', y') where $x' = x + a$ and $y' = y + b$. This operation is similar to shifting of origin which we have seen in the first course in coordinate geometry. The composition of two translations is again a translation and the translation by $a = 0$; $b = 0$ gives the identity translation and translation $x = x' - a$ and $y = y' b$ gives the inverse translation. Thus the set of translations under the composition of translation form a group.

A symmetry of a sub set $S \subseteq \mathbf{R}^2$ is a permutation of $\mathbf{R}$ which preserves the distance between any two points of S. Rotation of $\mathbf{R}^2$ through an angle θ and translation of $\mathbf{R}^2$ are examples of symmetries.

Example 13 : The symmetries of a rectangle :

Let 1, 2, 3, 4 denote the vertices of a rectangle. Let O be the centre of the rectangle, OX and OY be the axes of symmetry. Consider the follwing symmetries of the rectangle 1, 2, 3, 4.

(i) identity permutation : $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e$

(ii) mapping the diagonally opposite vertices : $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \rho$

(iii) mapping the adjacent vertices : $\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} = \sigma$.

Now $\rho o \sigma = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} o \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} = \sigma o \rho$.

Writing ρ, σ and $\rho \circ \sigma$ in cycle notation we see that $\{e, (1, 3)(2, 4), (1, 4), (2, 3), (1, 2)(3, 4)\}$ is an abelian group of order 4. We see that this is same as Klein 4 group we have seen in Unit-2.

Example 14 : The symmetries of an equilateral traingle

Let 1, 2, 3 be the vertices of an equilateral triangle. Let O be the centre.

Let ρ denote the rotation of the triangle in the plane through an angle of $\frac{2\pi}{3}$ (=120°) about O. The rotation then is $P = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (1, 2, 3)$ in cycle form.

Now $\rho^2 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (1, 3, 2)$ in cycle form ρ^2.

$\rho = \rho^3 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = e$, identity.

Let σ denote a flip in space of the equilateral traingle about the altitude through O. The corresponding permutation is $\sigma = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ (1 2) in cycle form.

$$\sigma^2 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = e, \text{ identity.}$$

The set of permutations (symmetries)

$\{e, (1, 2, 3), (1, 3, 2), (1, 2), (2, 3), (1, 3)\}$ or

$\{e, \rho, \rho^2, \sigma, \rho^2\sigma, \rho\sigma\}$

form a group of order 6. This can be seen to be the same as S_3.

Example 15 : Symmetries of a square with vertices 1, 2, 3, 4.

Let O be the centre. Let ρ be the rotation by

90° about O. Then $\rho = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$;

$\rho^2 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$; $\rho^3 = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$; $\rho^4 = e$, the identity

$\rho = (1, 2, 3, 4)$; $\rho^2 = (1, 3)(2, 4)$; $\rho^3 = (1, 4, 3, 2)$ in cycle form.

Let σ denote the reflection (flip) of the square

by x–axis. Then $\sigma = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} = (1, 4)(2, 3)$ in cycle form.

The eight elements given by

$\{e, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$ or

$\{e, (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2), (1, 4)(2, 3), (1, 2)(3, 4), (2, 4), (1, 3)\}$.

This group is non abelian where $\rho\sigma = \sigma\rho^3 = \sigma\rho^{-1}$

Observe that this group has four even permutations given by

$\{e, (1, 3)(2, 4), (1, 4)(2, 3), (1, 2)(3, 4)\}$

and four odd permutations given by

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

The four even permutations form a subgroup.

Note : A group generated by the symmetries of a regular polygon is called a dihedral group. The square being an example of a regular polygon the above group is a dihedral group denoted by D_4.

4.6 SUMMARY

In this unit we have seen examples of some interesting groups. Cyclic groups are abelian groups. A cyclic group is generated by a single element called a generator, subgroups of cyclic groups are cyclic. On the other hand permutation groups on finite sets ($n > 2$) are non abelian. The set of even permutations form a subgroup. Permutation groups and then subgroups provide very interesting examples. A_4, the alternating group on 4 letters, (which is the group of even permutations of S_4) is a group of order 12 and this does not have a subgroup of order 6. We have also seen examples from geometry.

4.7 MODEL EXAMINATION QUESTIONS

SECTION - A (Long answer questions)

(1) Define a generator of a cyclic group. Prove that a finite cyclic group of order n (> 1) generated by 'a' has a^m as a generator if and only if $(m, n) = 1$. What can be said about generators of infinite cyclic groups.

(2) Show that a subgroup of a cyclic group is again cyclic. Consider both finite and infinite cyclic groups.

(3) Show that every permutation of a finite set can be written as a product of transpositions. Show further if a permutation is a product of 'r' transpositions, then either r is always even or always odd.

(4) Write all the elements of S_3 and construct the multiplication table. Identify the even permutations and verify that A_3 is a subgroup of S_3.

SECTION - B (Short Answers)

(1) Show that a cyclic group is abelian. Give an example to show that the converse is always not true.

(2) Let p be a prime number. Show that a group of order p is cyclic.

(3) Show that A_4 has no subgroup of order 6.

(4) Show that the product of two even permutations is even and the product of two odd permutations is even. What can be said about the product of an even permutation and an odd permutation?

(5) By writing the following permutations as products of disjoint cycles determine whether they are even or odd.

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$; (ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 4 & 7 & 8 & 6 \end{pmatrix}$.

4.8 ANSWERS TO SELF ASSESSMENT QUESTIONS

SAQ 1 H is not empty because $a = a' \in H$. Since $0 \in Z$, $a^0 = e \in H$. If $a^n \in H$, then $n \in Z$ and $a^{-n} \in H$, since $-n \in Z$. Further, $H \subset G$ and associativity is satisfied in H because it is satisfied in G. Then H is a subgroup of G.

SAQ 2 $Z_5 = \{0, 1, 2, 3, 4\}$. Under the operation of modulo addition $\oplus$, Z_5 is a cyclic group. is a generator because every element can be generated by 1 (ex : $3 = 1 \oplus 1 \oplus 1$ etc.). 2 is a generator of Z_5 because $1 = 2 \oplus 2 \oplus 2$; $3 = 2 \oplus 2 \oplus 2 \oplus 2$; $4 = 2 \oplus 2$; and $0 = 2 \oplus 2 \oplus 2 \oplus 2 \oplus 2$. Verify similarly 3 and 4 are also generators.

SAQ 3 $(Z_{10}, \oplus)$ is a cyclic group of order 10. 2 and 5 are the divisiors of 10. Thus $(Z_{10}, \oplus)$ has exactly two subgroups $(Z_2, \oplus)$ and $(Z_5, \oplus)$.

SAQ 4

$$f_3 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_4.$$

$f_3\left(f_2(1)\right) = f_3(1) = 2$, i, e, $1 \to 1 \to 2$ etc.

SAQ 5

$$f_2 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$

$f_2\left(f_2(1)\right) = f_2(1) = 1$, $f_2\left(f_2(2)\right) = f_2(3) = 2$

$f_2\left(f_2(3)\right) = f_2(2) = 3$.

SAQ 6 R is reflexive because $a = a$ since $f^0(a) = a$. Suppose a R b then there exists an integer k such that $f^k(a) = b$. Then $a = f^{-k}(b)$ so that b R a. If a R b and b R c then $a = f^k(b)$ and $b = f^l(c)$ so that $a = f^{k+l}(c)$ gives a R c. Then R is an equivalence relation.

SAQ 7 $(1, 2, 3, 4) = (1, 4)(1, 3)(1, 2) = (3, 2)(4, 3)(1, 4)$

$= (1, 4)(1, 3)(2, 3)(2, 3)(1, 2)$.

SAQ 8 No. Because the product of two odd permutations is not odd (it is even) and hence the operation is not a binary operation.

SAQ 9 Every element of A_n is an even permutation and hence is a product of even number of transpositions that can be grouped in pairs. Let $(a, b)(c, d)$ be a pair of distinct transpositions. If (a, b) and (c, d) are disjoint, then $(a, b)(c, d) = (c, d)(a, c)(a, c)(a, b) = (a, d, c)(a, b, c)$.

If (a, b) and (c, d) are not disjoint let $b = c$ so that $(a, b)(c, d) = (a, b)(b, d) = (a, b, d)$

Either way each pair of transpositions generates a 3-cycle.

UNIT–5 : NORMAL SUBGROUPS AND QUOTIENT GROUPS

Contents

5.1 Aims and Objectives

5.2 Introduction

5.3 Normal subgroups

5.4 Quotient groups

5.5 Conjugates and class equation

5.6 Workedout exercises

5.7 Summary

5.8 Model Examination Questions

5.9 Answers to Self Assessment Questions

5.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to (i) define a normal subgroup, state and prove conditions for a subgroup to be normal, (ii) compute quotient groups of some given groups, (iii) define the normaliser of an element and centre of a group and verify them to be subgroups, (iv) derive class equation and discuss consequences.

5.2 INTRODUCTION

One of the important problems that attracted the attention of mathematicians for several centuries is the solving of a polynomial equation by radicals. All of us know that a quadratic equation $ax^2 + bc + c = 0$ is solvable and its roots expressed in terms of the coefficients a, b, c. It was in the 16th century the Italian mathematicians Tartalia (1506-1557) and Cardon (1501-1576) gave a method of solving a cubic equation $ax^3 + bx^2 + cx + d = 0$, expressing its roots in terms of its coefficients. Another Italian by name Ferrari a student of Cardon gave a method of solving a biquadratic eqaution in 1545. After this nearly for three hundred years nothing could be said about solving fifth degree (quintic) equations nd equations of higher degree. It was the two brilliant child prodigies Abel (1828) and Galois (1830) who recognised the relation between the solving of an equation and the group of permutations of the roots of the equation. If the group of permutations of the roots of an equation has a structure of certain types of subgroups (for example subgroups for which a right coset is same as a left coset) then the group itself said to be solvable and the equation, for which this group is solvable, is solvable. The normal subgroup was such a group which played an important role in determining this solvability criterion. The contents of this unit play an important role in the study of group theory.

5.3 NORMAL SUBGROUPS

Definition.1:

A subgroup N of a group G is said to be a normal subgroup of G, if for every $g \in G$, $gNg^{-1} \subseteq N$. Equivalently, a subgroup N is normal in G if for every $n \in N$, $gng^{-1} \in N$, where $g \in G$.

Example. 1 : The subgroup $\{e\}$, the group consisting of the identity alone, and the group G itself are normal subgroups of G. These are called trivial normal subgroups. From now on, we mean by a normal subgroup which is a non trivial normal subgroup.

Example. 2 : If G is an abelian group, then any subgroup N of G is a normal subgroup of G. This is because for every $n \in N$ and $g \in G$, we have that $ng = gn$.

Thus $g\,n\,g^{-1} = n\left(g\,g^{-1}\right) = n \cdot e = n \in N$.

Example. 3 : Let $G = S_3 = \{e, (1, 2, 3), (1, 3, 2), (1, 2), (1, 3), (2, 3)\}$.

Let $H_1 = \{e, (1, 2, 3), (1, 3, 2)\}$. Then H_1 is a normal subgroup of G. To see this choose any $g \in G$, say (1, 2). Then $(1, 2)\,H_1\,(1, 2)^{-1} = (1, 2)\,H_1\,(1, 2)$, because $(1, 2)^{-1} = (1, 2)$.

$$(1, 2)\,H_1\,(1, 2) = \{(1, 2)\,e\,(1, 2);\ (1, 2)\,(1, 2, 3)\,(1, 2);\ (1, 2)\,(1, 3, 2)\,(1, 2)\}$$
$$= \{e, (1, 3, 2), (1, 2, 3)\} = H_1$$

$\subseteq H_1$. It can be similarly verfied that $(1, 3)\,H_1\,(1, 3) \subseteq H_1$ and

$(2, 3)\,H_1\,(2, 3) \subseteq H_1$. Thus H_1 is a normal subgroup of G.

Example. 4 : Let $G = S_3 = \{e, (1, 2, 3), (1, 3, 2), (1, 2), (1, 3), (2, 3)\}$. Let $H_2 = \{e, (1, 2)\}$ be a subgroup of G. H_2 is not a normal subgroup of S_3. To see this choose $(1, 2, 3) \in S_3$. Then

$$(1, 2, 3)\,H_2\,(1, 2, 3)^{-1} = \left\{(1, 2, 3)\,e\,(1, 2, 3)^{-1},\ (1, 2, 3)\,(1, 2)\,(1, 2, 3)^{-1}\right\}$$
$$= \{e, (1, 2, 3)\,(1, 2)\,(1, 3, 2)\}$$
$$= \{e, (1, 3)\} \not\subseteq H_2.$$

Thus H_2 is not a normal subgroup of S_3.

SAQ 1 Let $G = S_3$ and $H_3 = \{e, (1, 3)\}$, show that H_3 is not normal in S_3.

Theorem. 1 :

A subgroup N of G is a normal subgroup of G if and only if $g\,N\,g^{-1} = N, \forall\ g \in G$.

Proof : Let N be a normal subgroup of G. Then by the definition $g\,N\,g^{-1} \subseteq N$ for every $g \in G$. But $g \in G$ implies that $g^{-1} \in G$, and N is a normal subgroup implies that $g^{-1}N\left(g^{-1}\right)^{-1} = g^{-1}N\,g \subseteq N$. This means that

$g\left(g^{-1}\,N\,g\right)g^{-1} \subseteq g\,N\,g^{-1}$, or, $\left(g\,g^{-1}\right)N\left(g\,g^{-1}\right) = N \subseteq g\,N\,g^{-1}$. Thus $g\,N\,g^{-1} = N$.

Conversely if $g\,N\,g^{-1} = N$ for every $g \in G$, then $g\,N\,g^{-1} \subseteq N$ is trivally true for all $g \in N$. Thus N is normal in G.

Note : $g\,N\,g^{-1} = N$ for all $g \in G$, does not imply $g\,n\,g^{-1} = n$ for all $n \in N$.

Theorem. 2 :

A subgroup N of a group G is a normal subgroup of G if and only if every left (right) coset of N in G is a right (left) coset of N in G.

Proof : Let N be a normal subgroup of G. Then for $g \in G$, $g\,N\,g^{-1} = N$, by theorem 1 of this unit. But $g\,N\,g^{-1} = N \Rightarrow \left(g\,N\,g^{-1}\right)g = Ng$. That is $g\,N\left(g^{-1}\,g\right) = gN = Ng$. Here gN is a left coset of N and Ng is a right coset of N.

Conversely, suppose N is a subgroup of G such that every left coset of N in G is a right coset of N in G. Let $g \in G$ and consider gN which is a left coset of N in G. By hypothesis this left coset is some right coset of N in G. Since $g = g \cdot e \in gN$, $g \in g\,N$, the left coset. But again $g = e.g \in Ng$ so that $g \in Ng$, the right coset. Since any two right cosets are either identical or disjoint, $g \notin$ any other right coset except Ng. Hence $g\,N = Ng \Rightarrow g\,N\,g^{-1} = (Ng)\,g^{-1} = N\left(g\,g^{-1}\right) = Ne = N$. Thus N is a normal subgroup of G.

Remark. 1 : When we say that a left coset is same as the right coset we are talking of set equality but not in the sense of $gn = ng$, element wise.

Theorem. 3 :

> A subgroup N of G is a normal subgroup of a group G if and only if the Product of any two left cosets of N is again a left coset of N.

Proof : Let N be a normal subgroup of G. Let $a, b \in G$. Then by theorem 2 of this unit $Na = aN$ and $Nb = bN$. Consider the product of two left cosets aN and bN.

$$(aN)\,(bN) = a\,(Nb)\,N = a\,(bN)\,N = (ab)\,(NN)$$

Now $a, b \in G \Rightarrow a\,b \in G$ and $N.N = N$, by closure property in N. Thus $(aN)\,(bN) = (ab)\,N$, a left coset.

Conversely suppose that N is a subgroup of G such that $(aN)\,(bN)$ is again a left coset in G for $a, b \in G$. Let e be the identity element. Now $ab = ae.\ be \in aN.bN$, again

$$ab = ab\,e \in ab\,N \Rightarrow ab \in ab\,N.$$

Thus $aN.bN = (ab)\,N$ for $a, b \in G$.

Let $g \in G$. Then $gN\,.\,g^{-1}\,N = \left(g\,g^{-1}\right)N = N$.

Thus $\left(g\,N\,g^{-1}\right)N = N$.

This means that for every $a, n \in N$,

$$\left(g\,N\,g^{-1}\right)a \in N \Rightarrow \left(\left(g\,n\,g^{-1}\right)a\right)a^{-1} \in .\,N.$$

That is : $\left(g\,n\,g^{-1}\right)\left(a\,a^{-1}\right) = g\,n\,g^{-1} \in N$. Hence N is normal in G.

Theorem. 4 :

> If N_1 and N_2 are two normal subgroups of G, then $N_1 \cap N_2$ is also a normal subgroup of G.

Proof : Let e be the identity of G. Since $e \in N_1$ and $e \in N_2$, $e \in N_1 \cap N_2$. Thus $N_1 \cap N_2$ is not empty. Let $g \in G$, and $n \in N_1 \cap N_2$. Then $n \in N_1$ and $n \in N_2$. Since N_1 is normal in G, $g\,n\,g^{-1} \in N_1$. Similarly N_2 is normal in G implies that $g\,n\,g^{-1} \in N_2$. Thus $g\,n\,g^{-1} \in N_1 \cap N_2$. Since $g \in G$, $n \in N_1 \cap N_2 \Rightarrow g\,n\,g^{-1} \in N_1 \cap N_2$, we conclude that $N_1 \cap N_2$ is normal in G.

Remark. 2 : If N_1 and N_2 are two normal subgroups of a group G, then $N_1 \cup N_2$ need not be a normal subgroup. Let $G = (Z, +)$; $N_1 = (3Z, +)$ and $N_2 = (5Z, +)$. Now $N_1 \cup N_2$ is not a subgroup because $3 \in N_1, 5 \in N_2$ but $3 + 5 = 8 \notin N_1 \cup N_2$. If $N_1 \cup N_2$ is not a subgroup it is not a normal subgroup.

Theorem. 5 :

> If H is a subgroup of G and N is a normal subgroup of G, then $H \cap N$ is a normal subgroup of H.

Proof : Since H and N are subgroups of G, $H \cap N$ is a subgroup of G. Thus the identity element is in $H \cap N$ and hence $H \cap N \neq \phi$. Further $H \cap N \subseteq H$. Let $g \in H$ and $n \in H \cap N$. This implies that $g \in G$ and $n \in N$. Since N is normal in G, $g N g^{-1} = N$. But $g \in H$, $n \in H$ and H is a subgroup implies that $g N g^{-1} \in H$. Thus $g N g^{-1} \in H \cap N$ and $H \cap N$ is normal in H.

Remark. 3 : $H \cap N$ need not be normal in N or in G.

Example. 5 : Consider the quaternion group consisting of the 8 elements: $\{1, -1, i, -i, j, -j, k, -k\}$ where $i^2 = j^2 = k^2 = -1$, $ij = k, ji = -k, jk = i,\ kj = -i, ki = j, ik = -j$. G is a non abelian group. G has serveral subgroups. Let $H = \{1, -1\}$ and $N = (1, i, -1, -i)$ be two subgroups of G. Now N is a normal subgroup of G. To see this let $j \in G$.

$$Nj = \{j, ij, -j, -ij\} = \{j, k, -j, -k\} = \text{right coset}$$

$$jN = \{j, ji, -j, -ji\} = \{j, -k, -j, k\} = \text{left coset}$$

$Nj = jN$ and similarly it can be checked that $Nk = kN$. Thus N is normal in G. Now H is a subgroup of G and $H \cap N = \{1, -1\}$. $H \cap N$ is normal in N. Because $i\,(H \cap N) = \{i, -i\}$ and $(H \cap N)\, i = \{i, -i\}$. Thus $H \cap N$ is normal in N.

Remark. 4 : Every subgroup of the quaternion group is a normal subgroup.

Example. 6 : Consider the group of symmetries of a square (dihedral group). (example 15 of unit 4)

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

$$= \left\{e, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\right\} \text{ where}$$

$$\rho^4 = e, \sigma^2 = e \text{ and } \rho\sigma = \sigma\rho^3 = \sigma\rho^{-1}.$$

$$H = \left\{e, \rho^2, \sigma, \sigma\rho^2\right\} \text{ is a subgroup of G. To see this}$$

$$\text{consider } \rho H = \left\{\rho, \rho^3, \rho\sigma, \rho\sigma\rho^2\right\} = \text{left coset}$$

$$H\rho = \left\{\rho, \rho^3, \sigma\rho, \sigma\rho^3\right\} = \text{right coset}$$

$\rho H = H\rho$ because $\rho\sigma = \sigma\rho^3, \rho\,\sigma\,\rho^2 = \sigma\,\rho^3\,\rho^2 = \sigma\rho$

Similarly other verifications could be carried out. Thus H is normal in G. Now $N = \{e, \sigma\}$ is normal in H. Because let $\rho^2 \in H$. Then

$$\rho^2 N = \left\{\rho^2, \rho^2\sigma\right\} \text{ and } N\rho^2 = \left\{\rho^2, \sigma\rho^2\right\}, \text{ the left coset = right coset since } \rho^2\sigma = \sigma\rho^2. \text{ To see this observe}$$

$$\rho^2\sigma = \rho\cdot\rho\sigma = \rho\cdot\sigma\rho^3 = (\rho\sigma)\rho^3 = \left(\sigma\rho^3\right)\rho^3 = \sigma\rho^2.$$

Similarly other verifications can be carried out.

Thus N is normal in H.

But N is not normal in G. Consider $\rho \in G$.

$$N\rho = \{\rho, \sigma\rho\} \text{ and } \rho N = \{\rho, \rho\sigma\}$$

since $\sigma\rho \neq \rho\sigma$, the left coset is not the right coset.

Thus in this example, N is normal in H and H is normal in G but N is not normal in G.

Theorem. 6 :

If N and H are two normal subgroups of a group G, then NH is also a normal subgroup of G

Proof : NH = $\{nh : n \in N \text{ and } h \in H\}$. Let $e \in H$ be its identity. Since N, H are subgroups of G, $e = e.e \in NH \Rightarrow NH \neq \phi$. Let $x, y \in NH \Rightarrow n_1, n_2 \in N, h_1, h_2 \in H$ exists such that $x = n_1 h_1, y = n_2 h_2$. Now $x^{-1} y = (n_1 h_1)^{-1} (n_2 h_2) = (h_1^{-1} n_1^{-1})(n_2 h_2) = h_1^{-1} (n_1^{-1} n_2) h_2 = \{h_1^{-1} (n_1^{-1} n_2) h_1\}. \{h_1^{-1} h_2\} \in NH$ because $h_1^{-1} (n_1^{-1} n_2)\ h \in N$ ($\because$ N is normal in G), and $h_1^{-1} h_2 \in H$. Therefore $x, y \in NH \Rightarrow x^{-1} y \in NH \Rightarrow NH$, is a subgroup of G. Let $g \in G$ and $x \in NH \Rightarrow n \in N, h \in H$ such that $x = nh$. Now $gx g^{-1} = g(nh) g^{-1} = gn (g^{-1} g) hg^{-1} = (gn g^{-1})(ghg^{-1}) \in NH$. ($\because$ N and H are normal subgroups of G) $\Rightarrow$ NH is normal in G.

SAQ 2 If N is a normal subgroup in G and H is a subgroup in G then show that NH is a subgroup of G.

Theorem. 7 :

Let H be a subgroup of a group G and let $a \in G$. Then $aHa^{-1} = \{aha^{-1} / h \in H\}$ is a subgroup of G.

Proof : Let e be the identity element. Then $e = aea^{-1} \in a H a^{-1}$. Thus $a H a^{-1} \neq \phi$. Let $x, y \in aHa^{-1}$.

Then $x = ah_1 a^{-1}$ and $y = ah_2 a^{-1}$ for $h_1, h_2 \in H$.

Then $xy^{-1} = (ah_1 a^{-1})(ah_2 a)^{-1} = (ah_1 a^{-1})(ah_2^{-1} a^{-1})$

$= a h_1 (a^{-1} a) h_2^{-1} a^{-1} = a (h_1 h_2^{-1})\ a^{-1} \in a H a^{-1}$

because $h_1 h_2^{-1} \in H$. Thus $a H a^{-1}$ is a subgroup of G.

Remark. 5 : $a H a^{-1}$ is called a conjugate subgroup to H. In general $a H a^{-1}$ need not be same as H. If however, $a H a^{-1} = H$, then H is a normal subgroup or self conjugate subgroup or invariant subgroup. If G is a finite group and H is the only subgroup of G of order d (say) then the order of $a H a^{-1}$ being same as that of H, $a H a^{-1} = H$ and H is normal in G.

Example. 7 : If N is a subgroup of index 2 in G, then N is a normal subgroup. Recall the index of a subgroup is the number of distinct left cosets of a subgroup in the group. To show that N is normal in G, we have to show that $Ng = gN$, for $g \in G$. Since N is both left and right coset of G (because $Ne = eN = N$) we have that $G = N \cup Ng = N \cup gN$. This is because G has exactly two left (right cosets). Then $Ng = G - N = gN$, implying N is normal in G.

SAQ 3 Show that A_n is normal in S_n. ($n > 2$).

5.4 QUOTIENT GROUPS

Let H be a subgroup of a group G. Let G/H denote the set of all left cosets of H in G. A typical element of G/H is a set of the form aH, for $a \in G$. If H is a normal subgroup, then a right coset is a left coset and hence we need not distinguish between right cosets and left cosets. The question now is that whether we can define an appropriate binary operation on G/H so that G/H becomes a group. We have seen that if H is a normal subgroup, the product of two left cosets is again

a left coset. Then the operation is a binary operaton on G/H. Further the operation is associative. To see this consider $aH, bH, cH \in G/H$. Then $aH. (bH . cH) =$

$$aH . (b\,c\,H) = (a\,b\,c)\,H \text{ and}$$

$$(aH . b\,H).\,cH = (ab\,H)\,.\,cH = (abc)\,H.$$

Thus $aH . (b\,H\,.cH) = (aH.\,bH)\,.\,cH.$

To see that the identity postulate is satsified we observe that $H = e.\,H \in G/H$, where e is the identity.

$$H\,.\,aH = e\,H.\,aH = (e.a)\,H = aH \text{ and}$$

$$aH\,.\,H = aH\,.\,eH = (a.e)\,H = aH$$

Thus H is the identity element of G/H.

To see that the inverse postulate is satsified we observe that

$$aH\,.\,a^{-1}\,H = \left(a.a^{-1}\right)H = eH = H$$

and $a^{-1}\,H.\,aH = \left(a^{-1}.a\right)H = eH = H$. Thus $a^{-1}\,H$ is the inverse of aH.

Definition. 2 :

> Let H be a normal subgroup of a group G. Then the set of all cosets of H in G, denoted by G/H under the binary operation of coset multiplication given by $aH\,.\,bH = ab\,H$ for $aH, bH \in G/H$ is a group. This group is called quotient group of G modulo H or simply quotient group. Some text books call this a factor group also.

Remark. 6 : If G is finite, then o (G/H) = o (G)/o (H). Because o (G/H) is the number of distinct left cosets of H in G. This is equal to the index of H in G. Since G is finite, o (G) = o (H) · |G : H|. Thus $|G : H| = o\,(G/H) = \frac{o\,(G)}{o\,(H)}$. Hence |G : H| is the number. of cosets of H in G. Recall that we have defined this as the index of H in G.

Example 8 : Let G = (Z, +) and H = (3Z, +). Then G is abelian and H is a normal subgroup of G.

$$G/H = Z/3Z = \{3Z, 1 + 3Z, 2 + 3Z\}.$$

To state explicitely

$$Z = G = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

$$3Z = H = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

$$1 + 3Z = 1 + H = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$$

$$2 + 3Z = 2 + H = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$$

Let us construct the operation table.

(i) H is the identity of G/H.

(ii) Inverse of H is H

Inverse of 1 + H is 2 + H

Inverse of 2 + H is 1 + H

+	H	1 + H	2 + H
H	H	1 + H	2 + H
1 + H	1 + H	2 + H	H
2 + H	2 + H	H	1 + H

Example. 9 : Let $G = S_3$ and $H = A_3$. Since the index of A_3 in S_3 is 2, A_3 is normal in G, What is S_3/A_3?

Recall $S_3 = \{e, (1,2,3), (1,3,2), (1,2), (1,3), (2,3)\}$

$A_3 = \{e, (1,2,3), (1,3,2)\}$

$S_3/A_3 = \{x \cdot A_3 | x \in S_3\}$. Now $(1,2) \in S_3$.

$(1,2)\ A_3 = \{(1,2), (1,2)(1,2,3), (1,2)(1,3,2)\}$

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

Similarly $(1,3)\ A_3 = \{(1,2), (2,3), (1,3)\}$

$(2,3)\ A_3 = \{(1,2), (2,3), (1,3)\}$.

Thus $S_3/A_3 = \{A_3\ (1,2)\ A_3\}$ is a cyclic group of order 2.

•	A_3	$(1,2)\ A_3$
A_3	A_3	$(1,2)\ A_3$
$(1,2)\ A_3$	$(1,2)\ A_3$	A_3

Example. 10 : Let $G = \langle a \rangle$, be a cyclic group of order 12. That is $a^{12} = e$. Let $H = \langle a^4 \rangle$. Since G is abelian, H is normal. What is G/H?

$G = \{a, a^2, a^3, \ldots, a^{11}, a^{12} = e\}$

$H = \{a^4, a^8, a^{12} = e\}$

$o(G/H) = \frac{o(G)}{o(H)} = 4.$

$G/H = \{H, aH, a^2H, a^3H\}$

The operation table is

The inverse of aH is a^3H

The inverse of a^2H is a^2H

The inverse of a^3H is aH

+	H	aH	a^2H	a^3H
H	H	aH	a^2H	a^3H
aH	aH	a^3H	a^3H	H
a^2H	a^2H	a^3H	H	aH
a^3H	a^3H	H	aH	a^2H

5.5 CONJUGATES AND CLASS EQUATION

Definition :

Let G be a group and $a \in G$. An element $b \in G$ is said to be conjugate to 'a' if $b = x\,ax^{-1}$ for some $x \in G$.

Theorem. 8 :

The relation "is conjugate to" among the elements of a group is an equivalence relation

Proof : Let G be a group. Let R be the relation defined on the elements of G, by a R b if and only if b is conjugate to a. That is a R b if and only if there is $x \in G$ such that $b = x\,ax^{-1}$. To show that R is an equivalence relation we have to verify that it is reflexive, symmetric and transitive.

(i) R is reflexive, because a Ra. That is there is the identity element $e \in G$ such that $a = eae^{-1}$.

(ii) R is symmetric : To see that let a Rb. Then there is $x \in G$ such that $b = x\,ax^{-1}$. But $x \in G$ implies that $x^{-1} \in G$ and $x^{-1}\,bx = x^{-1}\left(x\,ax^{-1}\right)x = \left(x^{-1}\,x\right)a\left(x^{-1}\,x\right) = e\,ae = a$. Thus there is $x^{-1} \in G$ such that $a = x^{-1}\,b\left(x^{-1}\right)^{-1}$. Thus b R a.

(iii) R is transitive : To see this let a R b and b R c. This means that there exist $x, y \in G$ such that $b = x\,ax^{-1}$ and $c = y\,by^{-1}$. Now $c = y\,by^{-1} = y\left(x\,ax^{-1}\right)y^{-1} = (yx)\,a\left(x^{-1}\,y^{-1}\right) = (yx)\,a\,(yx)^{-1}$. But $x, y \in G$ implies that $xy \in G$. Thus there is $xy \in G$ such that $c = (xy)\,a\,(xy)^{-1}$. Thus a Rc. Thus "is conjugate to" is an equivalence relation on G.

Definition :

> Let G be a group and $a \in G$. The conjugate class of a, wirtten as C $[a]$ is the set of elements in G, which are conjugate to a. That is C $[a] = \left\{x\,ax^{-1} \middle| x \in G\right\}$.

Remarks. 7 : Recall that an equivalence relation on a set partitions the set into mutually disjoint equivalence classes. Thus the group G is also partitioned into mutually disjoint equivalence classes. Thus if G is finite, then the order of G is the sum of the number of elements in the conjugate classes. Let C_a denote o (C $[a]$), the number of elements in C $[a]$.

Example. 11 : Let G be an abelian group and $a \in G$. Then for $x \in G$, $x\,ax^{-1} = x\,x^{-1}a = ea = a$. That is a is the only element conjugate to a. Thus the conjugate class of a consists of a only. Thus C $[a] = \{a\}$. This means in an abelian group every element belongs to a distinct conjugate class.

Example. 12 : Let $G = S_3 = \{e, (1, 2, 3), (1, 3, 2), (2, 2), (1, 3), (2, 3)\}$. What are the conjugate class of (1, 2,3), (1, 2)?

C $[e] = \{e\}$,

C $[(1, 2, 3)] = \left\{x\,(1, 2, 3)\,x^{-1} \middle| x \in G\right\}$

$= \{e\,(1, 2, 3)\,e^{-1}, (1, 2, 3)\,(1, 2, 3)\,(1, 2, 3)^{-1}, (1, 3, 2)\,(1, 2, 3)\,(1, 3, 2)^{-1}, (1, 2)\,(1, 2, 3)\,(1, 2)^{-1}, (1, 3)\,(1, 2, 3)\,(1, 3)^{-1}, (2, 3)\,(1, 2, 3)\,(2, 3)^{-1}\}$

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

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

C $[(1, 2)] = \{e\,(1, 2)\,e^{-1}, (1, 2, 3)\,(1, 2)\,(1, 2, 3)^{-1}\,(1, 3, 2)\,(1, 2)\,(1, 3, 2)^{-1}, (1, 2)\,(1, 2)\,(1, 2)^{-1}, (1, 3)\,(1, 2)\,(1, 3)^{-1}, (2, 3)\,(1, 2)\,(2, 3)^{-1}\}$

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

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

Note : You are required to check the multiplication and verify that the result is correct.

Thus S_3 has 3 conjugate classes : $\{e\}$, $\{(1, 2, 3), (1, 3, 2)\}$, $\{(1, 2), (1, 3), (2, 3)\}$.

$o\left(S_3\right) = 6 = o(C\,[e]) + o(C\,[(1, 2, 3)]) + o(C\,[(1, 2)])$.

$= 1 + 2 + 3 = 6$

Definition. 5 :

Let G be a group. The center of G is the set of all elements in G, which commute with every element in G. It is customary to denote the centre of G by Z (G), (not to be confused with the set of integrs). Thus Z (G) = $\{a \in G | ax = xa, \forall x \in G\}$.

Example. 13 : If G is an abelian group, every element of G commutes with every other element and hence Z (G) = G.

Example. 14 : What is Z (S_3)?

Now by definition,

$$Z(S_3) = \{a \in S_3 | ax = xa \ \forall \ x \in G\}$$

Clearly $e \in Z(S_3)$ because $ex = xe \ \forall \ x \in S_3$.

$(1, 2, 3) \notin Z(S_3)$ because $(1, 2, 3)(1, 2) \neq (1, 2)(1, 2, 3)$

Similarly, $(1, 3, 2), (1, 2), (1, 3), (2, 3) \notin Z(S_3)$.

Thus $Z(S_3) = \{e\}$.

That is S_3 has a trivial center.

S A Q 4 Show that Z (G) is a subgroup of G.

S A Q 5 Is Z (G), a normal subgroup of G? Justify.

Definition. 6 :

Let G be a group and $a \in G$. The normalizer of a in G, written as N [a], is the set of all elements in G which commute with a. That is N [a] = $\{x \in G | xa = ax\}$.

Theorem. 9 :

Let G be group and $a \in G$. Then N [a] is a subgroup of G. Further if $a \in Z(G)$, then N [a] = G.

Proof : Let e be the identity of G. Since $ae = ea$, $e \in N[a]$ and hence N [a] $\neq \phi$. Let $x, y \in N[a]$. Then $ax = xa$ and $ay = ya$. This implies that $a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$. and $xy \in N[a]$. Similarly $ax = xa$ implies $x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} \Rightarrow x^{-1}a(xx^{-1}) = ax^{-1} \Rightarrow x^{-1}a = ax^{-1}$. Thus $x \in N[a] \Rightarrow x^{-1} \in N[a]$. Hence N [$a$] is a subgroup of G. If $a \in Z(G)$, then $ax = xa$ for every x in G. Thus N [a] = $\{x | x \in G\}$ = G. Conversely if $a \in G$ is so that N [a] = G, then $ax = xa \ \forall x \in G$ and hence $a \in Z(G)$.

Remark. 8 : If G is finite and $a \in Z(G)$, then o (N [a]) = o (G)

Remark. 9 : $Z(G) = \bigcap_{a \in G} N[a]$.

Theorem 10 :

Let G be a finite group and $a \in G$. Then C_a = the number of elements in the conjugate class of a, = $\frac{o(G)}{o(N[a])}$ = The index of N [a] in G. Further o (G) = $\sum_{a \in G} C_a$

Proof : Define a mapping $f : C[a] \to \{g.N[a] | g \in G\}$ by $f(x) = gN[a]$, for all $x \in C[a]$ and $x = gag^{-1}$ for some $g \in G$. We see that f is well defined : If $x \in C[a]$, such that $x = gag^{-1} = hah^{-1}$, then

$h^{-1}\left(g\,ag^{-1}\right)\ g = h^{-1}\left(h\,ah^{-1}\right)g$. This implies that $h^{-1}\,ga = ah^{-1}\,g \Rightarrow h^{-1}\,g \in N\,[a]$. That is $h \in g\,N\,[a]$ and $g\,N\,[a] = h\,N\,[a]$.

f is one-one : Let $x, y \in C\,[a]$ such that $f(x) = f(y)$. That is $x = g\,ag^{-1}$ and $y = h\,ah^{-1}$ for $g, h \in G$. Thus $g\,N\,[a] = h\,N\,[a] \Rightarrow g^{-1}\,h \in N\,[a] \Rightarrow ag^{-1}h = g^{-1}ha$. Then $g\left(a\,g^{-1}\,h\right)h^{-1} = g\left(g^{-1}\,ha\right)h^{-1}$ $\Rightarrow g\,ag^{-1} = h\,ah^{-1} \Rightarrow x = y$. Thus $f(x) = f(y) \Rightarrow x = y$ and f is one-one.

f is onto : Let $g \in G$. Consider $g\,N\,[a]$. Now $ag = g\,a \Rightarrow g\,ag^{-1} = a$; $gag^{-1} \in C\,[a]$ onto the set of left cosets of $N\,[a]$ is G, that in $\{g\,N\,[a] \mid g \in G\}$.

Thus $o\,(C\,[a]) = Ca$ = index of $N\,[a]$ in $G = \dfrac{o\,(G)}{o\,(N\,[a])}$.

Since G is finite $o\,(G) = \sum_a C_a$ where $a \in G$. We can also write

$$o\,(G) = \sum_a \frac{o\,(G)}{o\,(N\,[a])}$$

Remark. 10 : If G is a finite group and Z (G) is the centre then for $a \in Z\,(G)$, each $C\,[a] = \{a\}$ and hence $C_a = 1$. Then $o\,(G) = o\,(Z\,(G)) + \sum_a \dfrac{o\,(G)}{o\,(N\,[a])}$, where the summations runs over elements a, taken one from each of those conjugate classes containing more than one element.

Definition. 7 :

Let G be a finite group. Then the equation $o\,(G) = o\,(Z\,(G)) + \sum_a \dfrac{o\,(G)}{o\,(N\,[a])}$ where the summation runs over elements a, taken one from each of those dinstinct conjugate classes containing more than one element is called the class equation of the group G. Equivalently, the class equation of a finite group G states that

$$o\,(G) = C + n_1 + n_2 + \ldots n_r$$

where C is the number of elements in the centre of G and n_i are the number of elements in the ith non-trivial conjugate class consisting of more than one element.

Remark. 11 : Since Z (G) is a subgroup of G, $o\,(Z\,(G)) = C$ divides $o\,(G)$. Further n_i is the number of elements in $C\left[a_i\right]$ which is equal to the number of left cosets of the subgroup $N\left[a_i\right]$. Thus $n_i = \left|G : N\left[a_i\right]\right|$, the index of $N\left[a_i\right]$ in G. Thus n_i divides $o\,(G)$.

SAQ 6 Verify the class equation for S_3.

5.6 WORKEDOUT EXERCISES

Exercise. 1 : Let p be a prime number and G be a finite group of order p^n. Then $o\,(Z\,(G)) \geq 2$. That is a group of prime power order has a non trivial centre.

Ans : Let $a \in G$. Since $N\,[a]$ is a subgroup of G, the order of $N\,[a] = o\,(N\,[a])$ divides the order of $G = o\,(G)$, by Lagrange's theorem. Since $o\,(G) = p^n$, where p is a prime number, $o\,(N\,[a]) = p^m$ for

some non negative $m \leq n$. If $a \in Z(G)$, then $m = n$, other wise let o (Z (G)) = C, (say) Notice that $e \in Z(G)$ hence o (Z (G)) ≥ 1. That is $C \geq 1$. Then by class equation

$$p^n = C + \sum \left(p^n / p^m\right)$$

Now p divides p^n and p divides p^{n-m} and hence p must divide C also. Thus $C \neq 0$, $C \neq 1$ and $C \geq 2$ and is divisible by p. Thus Z (G) is not trivial.

Exercise. 2 : Let p be a prime number and G be a group of order p^2. Then prove that G is abelian.

Ans : By exercise 1 of this unit, Z (G) is non trivial. Further Z (G) being a subgroup of G, o (Z (G)) $= p$ or o (Z (G)) $= p^2$. If the order of Z (G) $= p^2$, then Z (G) = G and G is abelian.

If possible let o (Z (G)) $= p$. Since o (G) $= p^2$, there exists $a \in G$ such that $a \notin Z(G)$. Gonsider N [a]. N [a] is a subgroup of G and Z (G) $\subsetneq$ N [a]. Since $a \in$ N [a], o (N [a]) $> p$. Since o (N [a]) divides order of G, o (N [a]) $= p^2$. This implies that N (a) = G. But N (a) = G implies that $a \in$ Z (G) contradicting the assumption that $a \notin Z(G)$. Thus o (Z (G)) $\neq p$.

This implies that o (Z (G)) $= p^2$ and G = Z (G) and G is abelian.

5.7 SUMMARY

If H is a subgroup of a non abelian group G, then the right coset of H in G need not be same as the left coset of H in G. But there are certain subgroups for which the left coset and right coset are the same. Such subgroups are called normal subgroups. A subgroup H of G is normal in G, if and only if the product of the two left cosets is again a left coset. If H is normal in N and N is a normal subgroup of G, H need not be normal in G. we have seen an example in dihedral group to this effect. There is a natural way to convert the set of left cosets into a group by appropriately defining the multiplication between two left cosets. This group is called a quotient group. By defining conjugacy between two elements of a group we have seen that this relation is an equivalence relation and hence a group could be decomposed into mutually disjoint equivalence classes whose union is G. Normaliser of an element and the centre of a group are subgroups that play an important role in the analysis of the structure of a group. A group of prime power order has a non trivial centre. As a consequence of this we proved that a group of prime square order is abelian.

5.8 MODEL EXAMINATION QUESTIONS

Section - A (Long Answer)

i) Define a normal subgroup and show that a subgroup is normal if and only if the product of two left cosets is again a left coset.

ii) Explain in detail the construction of a quotient group and give an example.

iii) Obtain the class equation of a finite group and use this to show that a group of prime power order has a non trival centre.

Section - B (Short Answer)

i) Show that a subgroup of index 2 is a normal subgroup.

ii) Show that the intersection of two normal subgroups of a group is again a normal subgroup.

iii) If H is a subgroup of G and N is a normal subgroup of G, show that $H \cap N$ is normal in H.

iv) Give an example to show that a normal subgroup of a normal subgroup need not be normal in the original group.

5.9 ANSWERS TO SAQ'S

SAQ 1 $(2, 3) \in S_3$. $(2, 3)\, H_3\, (2, 3)^{-1} = (2, 3)\, H_3\, (2, 3) = \{(2, 3)\, e\, (2, 3), (2, 3)\, (1, 2)\, (2, 3)\}$

$= \{e, (1, 3)\} \not\subseteq H_3$.

SAQ 2 Recall from exercise (i) of unit 3 that if H and K are subgroups of G, HK is a subgroup if KH = KH. Since N is normal NH = HN.

SAQ 3 $|S_n : A_n| = 2$, that is the index of A_n in S_n is 2. Hence A_n is normal in S_n.

SAQ 4 $e \in Z(G)$, hence $Z(G) \neq \phi$. Let $a, b \in Z(G)$, then $ax = xa$ and $bx = xb\ \forall\ x \in G$. Consider $\left(ab^{-1}\right) x = a\left(b^{-1} x\right) = a\left(x\, b^{-1}\right) = (ax)\, b^{-1} = x\left(ab^{-1}\right)$. Thus Z (G) is a subgroup of G.

SAQ 5 For any $a \in Z(G)$ and $g \in G$, $ag = ga \Rightarrow a = gag^{-1} \in Z(G)$. Thus Z (G) is normal in G.

SAQ 6 $o\left(S_3\right) = 6$; $o\left(Z\left(S_3\right)\right) = 1$; o (C [1, 2, 3]) = 2 and o (C [1, 2,]) = 3. Thus 6 = 1 + 2 + 3; Here c = 1; $n_1 = 2$ and $n_2 = 3$.

UNIT–6: HOMOMORPHISM THEOREMS AND CONSEQUENCES

Contents

6.1 Aims and Objectives

6.2 Introduction

6.3 Definitions and examples

6.4 Homomorphism Theorems

6.5 Workedout exercises

6.6 Summary

6.7 Model Examination Questions

6.8 Answers to Self Assessment Questions

6.1 AIMS AND OBJECTIVES

After going through this unit, you should be able to : (i) define the terms homomorphism, kernel, isomorphism, (ii) state and prove fundamental theorem of homomarphism of groups, (iii) find the groups automorphic to the given groups (iv) list all the groups whose order is less than 6.

6.2 INTRODUCTION

One of the most difficult problems in the theory of groups is to list all finite groups having the same order. The difficulty is that we may list the same groups in different forms. The notion of isomorphism builds up an equivalence relation between groups so that we may consider any two groups belonging to given equivalence class as the same. Just as we can not conclude that two human beings are same because they wear an identical set of clothes or the same person putting on a different set of clothes does not become different, groups also are to be recognised as same or different on the basis of information that is not readily apparent. Consider the group $\{1, w, w^2\}$, where w is a cube root of unity under the operation of multiplication and the group $\{0, 1, 2\}$, if integers modulo three under the operation of modulo addition. If we define a mapping f between these groups by $f = (w^0 = 1) = 0; f(w^1) = 1; f(w^2) = 2$, then we see that f is one-one and onto (bijection). But what can we say about $f(1 \cdot w)$ or $f(1 \cdot w^2)$ or $f(w \cdot w^2)$ and their images $0 + 1$, $0 + 2$ and $1 + 2$. The theory we have learnt till now does not have answers to these questions. Thus we need a mapping which is not only bijective, but preserves group operations. Such a mapping has very interesting properties and opens up new openings for new investigations.

6.3 DEFINITIONS AND EXAMPLES

Definition 1 :

Let (G, o) and (G′, $*$) be two groups. A mapping $f : G \to G'$ is said to be group homorphism if for $x, y, \in G, f(x\ o\ y) = f(x) * f(y)$. Observe here that x and $y \in G$ implies that $x\ o\ y$ is defined in G, where as $f(x), f(y) \in G'$ implies that $f(x) * f(y)$ is defined in G′. Thus a group homomorphism is operation preserving mapping. If the homorphism $f : G \to G'$ is one-one mapping, f is called a monomorphism and if f is onto, f is called an epimorphism. If the homomorphism f is one-one and onto them f is called an isomophism.

Thus, an injective homomorphism is a monomorphism, a surjective homomorphism is an epimorphism and a bijective homonorphism is an isomorphism.

Note : Some authors call a one-one homomorphism an isopmorphism.

Definition 2 :

An isomorphism of a group onto itself is called an automorphism.

Definition 3 :

Let $f : G \to G'$ be a group homomorphism and let e and e' be the identity elements of G and G′ respectively. The kernel of the homomorphism is defined as the set of all elements in G, that are mapped onto the identity of G′. We write kernel of the homomorphism f as Ker f. That

$$\text{Ker } f = \{g \in G / f(g) = e', \text{ the identity of } G'\}$$

Example 1 : Let $G = (Z, +) = G'$. Define $f : G \to G'$ by $f(x) = 2x$. Then f is a homomorphism because let $x, y \in G = (Z, +)$. Then $f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y) \in G' = (Z, +)$. Further f is one-one, because $x \neq y \Rightarrow 2x \neq 2y$ and $f(x) \neq f(y)$. f is not onto because $1 \in G' = (Z, +)$ and there is $x \in G$ such that $f(x) = 1$. Thus f is a monomorphism and not an epimorphism. What is ker f? Ker $f = \{x \in Z / f(x) = 0\}$. But there is only $0 \in Z$ such that $2.0 = 0$. Thus ker $f = \{0\}$.

Example 2 : Let $G = \{1, -1, i, -i\}$ where $i^2 = -1$ and let $G' = \{1, -1\}$. Then G and G′ are groups under the operation of multiplication. Define $f : G \to G'$ by $f(x) = x^2$ for $x \in G$. Then f is a homomorphism.

For example $f((-1)(-i)) = f(i) = i^2 = -1$ and

$f(-1) \cdot f(-i) = (-1)^2 \cdot (-i)^2 = -1$ etc.

Thus f is homomorphism. What is ker f?

$$\text{Ker } f = \{x \in G / f(x) = 1\} = \{1, -1\}.$$

Example 3 : Let $G = (M_2, \times)$ where M_2 is the set of non singular 2 x 2 matrices with real numbers as entries, and $\times$ denotes matrix multiplication. Let $G' = (R', \cdot)$. Where R′ is the set of non zero reals and denotes ordinary multiplication. Define $f : G \to G'$ by $f(A) = |A|$, the determinant of A. This is a homomorphism because if A and B are two non singular 2 x 2 matrices than $f(AB) = |AB| = |A| \cdot |B| = f(A) \cdot f(B)$.

$$\text{Ker } f = \{A \in M_2 / f(A) = 1\} = \text{The set of all 2 x 2 matrices}$$

whose determinant is 1.

Example 4 : Let $G = S_3$ and $G' = (\{1, -1\}, \cdot)$. Define

$$f: G \to G' \text{ by } f(\rho) = \begin{cases} +1, \text{ if } \rho \text{ is even permutation} \\ -1, \text{ if } \rho \text{ is odd permutation} \end{cases}$$

Then f is a homomorphism. To see this we consider the cases :

Case (i) if σ and ρ are both even, then $\sigma\rho$ is even and

$f(\sigma\rho) = f$ (even permutation) $= 1$ and

$f(\sigma) f(\rho) = 1 \cdot 1 = 1$, Thus $f(\sigma\rho) = f(\sigma) f(\rho)$.

Case (ii) If σ and ρ are both odd, then $\sigma\rho$ is even and

$f(\sigma\rho) = f$ (even permutation) $= +1$ and

$f(\sigma) f(\rho) = (-1) \cdot (-1) = 1$. Thus $f(\sigma\rho) = f(\sigma) f(\rho)$.

Case (iii) If σ is even and ρ is odd, then $\sigma\rho$ is odd and

$f(\sigma\rho) = f$ (odd permutation) $= -1$

$f(\sigma) f(\rho) = (-1) \cdot (1) = -1$ and $f(\sigma\rho) = f(\sigma) f(\rho)$.

What is Ker f? Ker $f = \{\sigma \in S_3 \mid f(\sigma) = 1\}$. That is Ker $f = A_3$.

Example 5 : Let $G = (R^+, \cdot)$, the group if positive reals under multiplication and $G' = (R, +)$, the group of reals under addition. Define $f: G \to G'$ by $f(x) = \log x$. Then f is a homomorphism because $f(x \cdot y) = \log(x \cdot y) = \log x + \log y = f(x) + f(y)$. Ker $f = \{1\}$.

Example 6 : Let $G = (Z, +)$ and $G' = (\{1, -1\}, \cdot)$. Define

$$f: G \to G' \text{ by } f(x) = \begin{cases} 1 \text{ if } x \text{ is even} \\ -1 \text{ if } x \text{ is odd.} \end{cases}$$

Then f is a homomorphism because

$$f(x + y) = \begin{cases} f(x) \cdot f(y) = 1 \cdot 1 = 1 \text{ if both } x \text{ \& } y \text{ are even} \\ f(x) \cdot f(y) = -1 \cdot -1 = 1 \text{ if both } x \text{ \& } y \text{ are odd} \\ f(x) \cdot f(y) = 1 \cdot (-1) = -1, \text{if } x \text{ is even \& } y \text{ is odd} \end{cases}$$

Ker $f = \{2Z\}$, the set of even integers.

Example 7 : Let $G = (Z, +)$; and $G' = (Z_n, \oplus)$, Z_n is the set of integers modulo n and $\oplus$ is modulo addition. Define $f: G \to G'$ by $f(x) = r$ where r is the remainder of x when divided by n. That is if $x = q_i n + r_1$, $0 \le r_1 < q_i$ then $f(x) = r_1$ and if $y = q_2 n + r_2$, $0 \le r_2 < q_2$ then $f(y) = r_2$. To see that f is a homomorphism,

$$f(x) + f(y) = (r_1 + r_2) \bmod n = r_3$$

$$\text{That is } r_1 + r_2 = q_3 n + r_3.$$

$$\text{But } x + y = (q_1 + q_2) n + (r_1 + r_2) = (q_1 + q_2 + q_3) n + r_3.$$

$$\text{Thus } f(x + y) = f(x) + f(y)$$

$$\text{Ker } f = \{n Z\}, \text{ i.e. multiples of } n.$$

SAQ 1 Let $G = (Z, +)$, $G' = (\{2^n / n \in Z\}, \cdot)$. Define $f: G \to G'$ by $f(n) = 2^n$. Verify that f is a homomorphism. What is Ker f?

Theorem 1 :

Let $f : G \to G'$ be a homomorphism of groups. Let e and e' be the identities of G and G'. Then

(i) $f(e) = e'$; (ii) $f(x^{-1}) = (f(x)^{-1})$ and

(iii) Ker f is a normal subgroup of G.

Proof : $e \cdot e = e \Rightarrow f(e \circ e) = f(e)$. But f is homomorphism. Hence, $f(e \circ e) = f(e) \cdot f(e)$. Thus $f(e) \cdot f(e) = f(e)$ implies that $f(e) = e'$, identity of G'.

(ii) $e' = f(e) = f(x \circ x^{-1}) = f(x) \cdot f(x^{-1})$. That is $f(x) \cdot f(x^{-1}) = e'$. Then $f(x^{-1})$ is the inverse of $f(x)$ i.e. $(f(x))^{-1}$. Thus $f(x^{-1}) = (f(x))^{-1}$.

(iii) Ker $f \neq \phi$, because $e \in$ Ker f as $f(e) = e'$. Let $a, b \in$ Ker f; then $f(a) = e'$ and $f(b) = e'$. Now $f(a \cdot b) = f(a) \cdot f(b) = e' \Rightarrow a \cdot b \in$ Ker f. Thus $f(x^{-1}) \in$ Ker f. Thus Ker f is a subgroup of G. To show that Ker f is normal in G, let $x \in$ Ker f and $g \in G$. Then $f(x) = e'$.

$$\text{Consider } f(g\ x\ g^{-1}) = f(g) f(x) f(g^{-1}) = f(g) \cdot e' \cdot f(g^{-1})$$

$$= f(g) \cdot f(g^{-1}) = f(g \cdot g^{-1}) = f(e) = e'$$

Thus $g\ x\ g^{-1} \in$ Ker f. Hence Ker f is normal in G.

Theorem 2 :

Let $f : G \to G'$ be a group homomorphism. Let e and e' the identity elements of G and G' respectively. Then f is one-one if and only if Ker $f = \{e\}$.

Proof : Suppose f is one-one. Then we must show that Ker $f = \{e\}$. Clearly $e \in$ Ker f. Let $a \in$ Ker f. Then $f(a) = e' = f(e)$ and f is one-one implies $a = e$. Thus Ker $f = \{e\}$.

Conversely, suppose that Ker $f = \{e\}$. Let $a, b \in G$ and $f(a) = f(b)$. Then $f(a) \cdot (f(b))^{-1} = f(b) \cdot (f(b))^{-1} = e'$. This implies that $f(ab^{-1}) = e'$ or $a = b$. Since $f(a) = f(b) \Rightarrow a = b$; f is one-one.

SAQ 2 Let $f : G \to G'$ be a group homomorphism. Show that $f(G) = \{f(a) / a \in G\}$ is a subgroup of G'.

Theorem 3 : (Cayley's theorem) :

Every group is isomorphic to a subgroup of a permutation group.

Proof : Let G be a group and $g \in G$. Define a mapping $\rho_g : G \to G$ by $\rho_g(x) = xg^{-1}$ for x in G.

ρ_g is one - one : Let $\rho_g(x) = \rho_g(y)$. That is $xg^{-1} = yg^{-1}$ this implies that $x = y$. Since $\rho_g(x) = \rho_g(y) \Rightarrow x = y$, ρ_g one-one.

ρ_g is onto : Let $y \in G$, then $\rho_g(yg) = ygg^{-1} = y$. Thus ρ_g is a bijection and ρ_g is a permutation of elements of the set G and $\rho_g \in S_G$. Let us consider the mapping $\sigma : G \to S_G$ by $\sigma(g) = \rho_g$. σ is a homomorphism because $\sigma(gg') = \rho_{gg'}(x) = x(gg')^{-1} = \rho_g \rho_{g'}(x) = \sigma(g)\sigma(g')$. Now $g = 1_G$ if and only if $x \cdot g = x$ for all $x \in G$, that is if and only if $\rho_g = 1_{S_G}$. Thus Ker $\sigma = \{1_G\}$ and hence σ is a one-one mapping. Thus G is isomorphic to a subgroup of S_G.

Remark 1 : If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.

Theorem 4 :

The relation "is isomorphic to" is an equivalence relation in the set of groups.

Proof : Let G = {G / G is a group}. Define a relation R on G as follows. For G, H ∈ G define GRH if and only if G is isomorphic to H. To show that R is an equivalence relation we must verify that R is reflexive, symmetric and transitive. (i) R is reflexive : G is isomorphic to G, because the identity mapping $i : G \to G$, where $i(x) = x \; \forall x$ in G is a homomorphism. Further the identity mapping is one-one and onto. Thus R is reflexive.

(ii) R is symmetric : Let $f : G \to H$ be an isomorphism. $\Rightarrow f$ is bijectiveisomorphism, f^{-1} exists and f^{-1} is also a bijection from H to G. Let $a, b \in H$ be such that $f(x) = a, f(y) = b$, for $x, y \in G$. Then $x = f^{-1}(a)$ and $y = f^{-1}(b)$. $f(x \circ y) = f(x) \cdot f(y) = a \cdot b \Rightarrow x \circ y = f^{-1}(a \cdot b)$. But $f^{-1}(a \cdot b) = x \circ y = f^{-1}(a) \circ f^{-1}(b)$ implying that f^{-1} is a homomorphism. Thus f^{-1} is an isomorphism from H to G and f^{-1} is symmetric.

(iii) R is transitive : Let GRH and HRK. Let $f : G \to H$ and $g : H \to K$ be isomorphisms. Since f and g are bijections, $g \circ f$ is a bijection. To verify that $g \circ f$ is a homomorphism, consider

$$(g \circ f)(a \cdot b) = g(f(a \cdot b)) = g(f(a) \cdot f(b))$$
$$= g(f(a)) \cdot g(f(b)) = (g \circ f)a \cdot (g \circ f)b$$

Thus $g \circ f : G \to H$ is an isomorphism and R is transitive.

Thus R is an equivalence relation.

Remark 2 : R Partitions G into mutually disjoint equivalence classes. Each equivalence class consists of groups which are isomorphic to each other.

Notation : If G and G′ are isomorphic, we write $G \cong G'$.

6.4 HOMOMORPHISM THEOREMS

Theorem 5 :

Let H be a normal subgroup of G. Then the mapping $f : G \to G/H$, defined as $f(a) = a$ H, is a homomorphism of G onto G/H. (This homomorphism is called a natural homomorphism).

Proof : To verify that $f : G \to G/H$ defined by $f(a) = a$ H is a homomorphism, consider two elements $a, b \in H$.

Then by definition of f, we get

$$f(a \cdot b) = (a \cdot b)\,H = (a\,H) \cdot (b\,H), \text{ because H is normal in G.}$$
$$= f(a) \cdot f(b).$$

Thus f is a homomorphism.

$$\text{Ker} f = \{a \in G / f(a) = H, \text{ the identity of G/H}\}$$
$$= \{a \in G / f(a) = a\,H = H\}, \text{ But } a\,H = H \Rightarrow a \in H$$
$$= \{a \in G / a \in H\} = H.$$

Theorem 6 : Fundamental Homomorphism Theorem :

Let f be a homomorphism of a group G onto a group G′ with Kernel f = K. Then G/K is isomorphic to G′.

Proof : To prove that $G/K \cong G'$, we must first define a function $\psi : G/K \to G'$ and show that ψ is a homomorphism and that is one-one and onto. Before we proceed further we recall that Ker $f = K$ is a normal subgroup of G. As in Theorem 5 of this unit let us define the natural homomorphism $\sigma : G \to G/K$ by $\sigma(g) = Kg$. We shall use this σ and f to define ψ in such a way that G is associated with σ and f. Represented diagramatically, this means that $\psi \circ \sigma = f$. That is let $g \in G$, then $\sigma(g) = Kg$ and $\psi(Kg) = f(g)$. Keeping this in mind define $\psi : G/K \to G'$ by $\psi(Kg) = f(g)$.

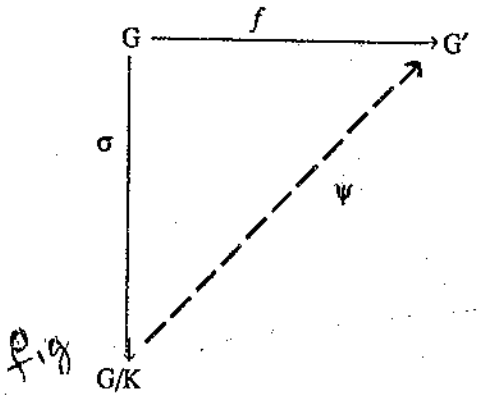


Fig. 4

(i) We must first verify that ψ is well defined. That is we must verify that if $Kg = Kg_1$, then

$$f(g) = f(g_1).$$

Let e and e' denote the identities of G and G' repectively. Then $Kg = Kg_1$ if and only if $gg_1^{-1} \in K$ or $f\left(gg_1^{-1}\right) = e'$.

$$\text{But } f\left(gg_1^{-1}\right) = f(g) \cdot f\left(g_1^{-1}\right) = f(g)\left(f(g_1)\right)^{-1}$$

$$f(g)\left(f(g_1)\right)^{-1} = e' \Rightarrow f(g) = f(g_1)$$

Thus ψ is well defined.

(ii) Further ψ is one-one because

$$\text{Ker } \psi = \{Kg / \psi(Kg) = e'\}$$
$$= \{Kg / f(g) = e'\}$$
$$= \{Kg / g \in K\} = K, \text{ identity of } G/K.$$

Since Ker ψ = identity of G/K, ψ is one-one (by Theorem 2 of this unit).

(iii) ψ is a homomorphism from G/K onto G'. To see this

Let $Kg_1, Kg_2 \in G/K$. Then

$$\psi\left(Kg_1 \cdot Kg_2\right) = \psi\left(Kg_1 g_2\right), \text{ because K is normal in G.}$$
$$= f\left(g_1 g_2\right), \text{ by definition of } \psi.$$
$$= f(g_1) f(g_2), \text{ because } f \text{ is a homomorphism}$$
$$= \psi\left(Kg_1\right) \cdot \psi\left(Kg_2\right)$$

Thus $\psi : G/K \to G'$ is a homomorphism.

(iv) ψ is onto : To see this let $g' \in G'$. Then we must exhibit a preimage for g' in G/K. Since $f : G \to G'$ is onto, for $g' \in G'$, there exists $g \in G$ such that $f(g) = g'$. But for $g \in G$, there exists $Kg \in G/K$. Thus $\psi(Kg) = f(g) = g'$ implying that Kg is the preimage of g' in G/K. Thus ψ is onto.

Since ψ is a bijective homomorphism from G/K onto G', we conclude $G/K \cong G'$.

Remark 3 : If in the statement of the theorem the condition onto is omitted, then $G/K \cong f(G)$.

Theorem 7 :

Any infinite cyclic group is isomorphic to (Z, +), the additive group of integers. Any finite cyclic group is isomorphic to Z_n, the group of integers modulo n under addition.

Proof : Let G be a cyclic group generated by a. Define a mapping $f : Z \to G$ by $f(n) = a^n$, $n \in Z$.

Then f is a homomorphism because

$$f(m + n) = a^{m+n} = a^m \cdot a^n = f(m) \cdot f(n).$$

Further f is onto becuase for each $a^n \in G$, there is $n \in Z$ such that $f(n) = a^n$. Also f is one-one. Let $m \neq n \in Z$, then G being infinite cyclic group, $a^m \neq a^n$.

Thus f is an isomorphism.

If G is finite cyclic group of order n generated by a, $G = \langle a \rangle$ and $a^n = e$. Further if $a^m = e$, then n divides m. Define $f : Z \to G$ by $f(n) = a^n$. The Ker $f = \langle n \rangle$ and $Z/\langle n \rangle \cong G$. Recall that $Z/\langle n \rangle = Z_n$.

Remark 4 : Any two cyclic groups of same order are isomorphic.

Theorem 8 :

If G is a group such that G / Z (G) is cyclic then G is abelian. Here Z (G) is the centre of G.

Proof : Z (G) the centre of G, is a normal subgroup of G. Consider G/Z (G).

Since G/Z (G) is cyclic, let $gZ(G)$ be its generator for $g \in G$.

That is $G / Z(G) = \langle g Z(G) \rangle$. Let $a, b \in G$.

Then $a Z(G) = (g Z(G))^m = g^m Z(G)$, for some $m \in Z$.

$b Z(G) = (g Z(G))^n = g^n Z(G)$, for some $n \in Z$.

Then $a = g^m x$ for $x \in Z(G)$

and $b = g^n y$ for $y \in Z(G)$

Now $ab = g^{m+n} xy$ and

$ba = g^{n+m} yx$.

But $x, y \in Z(G) \Rightarrow xy = yx$ and

$m + n = n + m$ for $m, n \in Z$.

Thus $ab = ba$ and G is abelian.

Example 8 : A non abelian group of order 6 is isomorphic to S_3.

Let G be non abelian group of order 6. Then G has no element of order 6, for G will be cyclic and hence abelian if it has an element of order 6. All elements of G can not be of order 2, for in that case each element of G is its own inverse and G will be abelian. Thus G must have an element of order 3. Let this element be denoted by x. Consider the set $\{I, x, x^2\}$. Let y be an element of G distinct from I, x and x^2. Now the six elements $\{I, x, x^2, y, xy, x^2 y\}$ are all distinct. Consider y^2. If $y^2 = x$ or $y = x^2$, $y^6 = x^3 = I$ and y is an element of order 2, 3 or 6. If $o(y) = 3^2$, then $x = I$ which is not true. If $o(y) = 3$, then $y^3 = I \Rightarrow xy = I$, $o(y) = 6$ makes G cyclic and hence abelian. Thus $o(y) = 2$. Similarly $y^2 \neq x^2$; $y^2 \neq y$, $y^2 \neq xy$ or $y^2 \neq x^2 y$. Thus $y^2 = I$. Thus

$G = \{I, x, x^2, y, xy, x^2, y\}$ is a group. Recall S_3.

$S_3 = \{e, (1, 2, 3), (1, 3, 2), (1, 2), (1, 3)(3, 2)\}$

Define $f: G \to S_3$ by $f(x) = (1, 2, 3)$ and

$f(y) = (1, 2)$. Then $f(x^2) = (1, 3, 2)$

$f(xy) = (1, 3), f\left(x^2 y\right) = (2, 3)$

Thus f is one - one and onto. Futher, f is a homomorphism because

$f(x y) = (1, 3)$ and $f(x) f(y) = (1, 2, 3)\ (1, 2) = (1, 3)$

Thus $f(xy) = f(x) f(y)$ etc.

Thus f is an isomorphism and $G \cong S_3$.

Remark 4 : It is not always easy to set up an isomorphism as in the case of above example. More often than not it is easy to prove that two groups are not isomorphic. Consider for example the groups : $G = (R', \cdot)$, the group of non zero reals under multiplication and $G' = (R, +)$, the group of reals under addition. The G is not isomorphic to G' because R' has an element of order 2 (which is – 1) and R has no element of order 2. Since an isomorphism must map an element of order 2 onto another element of order 2 only.

6.5 WORKEDOUT EXERCISES

Example 1 : Enumerate all groups whose orders are less than or equal to 6.

Ans : (i) If o (G) = 1, then $G = \{e\}$ is the trivial group.

(ii) If o (G) = 2, 2 is an even prime, A group of prime order is cyclic and hence abelian. Since any two cyclic groups of same order are isomorphic there is a group $G = (\{1, -1\}, \cdot)$, which is isomorphic to any other group of order 2.

(iii) If o (G) = 3, 3 is a prime number and hence G is cyclic and hence abelian.

$G = \left(\left\{1, w, w^2\right\}, \cdot\right)$ is isomorphic to any other group of order 3.

(iv) If o (G) = $4 = 2^2$. We have seen that a group of order p^2, p, a prime, is abelian. Thus G is abelian. But there are two possibilities. Let $a \in G$. Then o $(a) = 2$ or o $(a) = 4$, because o (a) divides o (G). If o $(a) = 2$, then the identity element 'e' and a do not exhaust all the elements of G. Let $b \in G$, and $b \neq a$. Then o $(b) = 4$ and the number of elements in G will be more than 4. Then G is a group implies $a \cdot b \in G$. Further o $(ab) = 2$. Thus $G = \{e, a, b, ab\}$, the Klein 4 - group. This is abelian generated by two elements a and b. G is not cyclic because, no single element generate the entire group. If o $(a) = 4$, then G is cyclic and hence abelian. Since any two cyclic groups of the same order are isomorphic, $G = (\{1, -1, i, -i\}, \cdot)$ is isomorphic to any group of order 4.

(v) If o (G) = 5, a prime, then G is cyclic and hence abelian. G is isomorphic to any other group of order 5.

(vi) If o (G) = 6, then there are two possibilities. Either G has an element of order 6 or G has no element of order 6. If G has an element of order 6, then it must have elements of order 2 and order 3. In the case $G = S_3$, G is non abelian (Example 8).

Exercise 2 : Let G be a group. Let H be a subgroup of G and K, a normal subgroup of G. Then $H/H \cap K \cong HK/K$ (Second isomorphism theorem).

Ans : Since H is a subgroup of G, and K is a normal subgroup of G, $H \cap K$ is normal in H and HK a subgroup of G. Define $f: H \to HK/K$ by $f(h) = h K$. Then f is a homomorphism. Because for

$$h_1, h_2 \in H, f\left(h_1 h_2\right) = \left(h_1 h_2\right) K = \left(h_1 K\right)\left(h_2 K\right)$$

$$= f(h_1) f(h_2)$$

Further f is onto, because any element of HK/K is of the form hk K and is equal to h K which is the image of h under f. Hence by the fundamental theorem of homomorphism H /Ker $f \cong$ HK/K. But what is Ker f? Recall that if $a \in$ Ker f, then $f(a) =$ K, the identity of HK/K. Thus $a \in$ Ker f if and only if a K = K i.e. $a \in$ H $\cap$ K.

Thus Ker f = H $\cap$ K and H /H$\cap$K $\cong$ HK/K

Exercise 3 : First isomorphism theorem :

Let G be a group and H and K are normal subgroups in G with K$\subset$ H. Then G/H $\cong$ (G/K)/(H/K)

Ans : Define f : G/K $\to$ G/H by f (Kg) = Hg.

(i) f is well defined because Kg = K$g_1 \Rightarrow gg_1^{-1} \in$ K and since K$\subset$ H,

$gg_1^{-1} \in$ H $\Rightarrow$ Hg = Hg_1.

(ii) f is onto because H$g \in$ G/H $\Rightarrow$ then K$g \in$ G/K such that f (Kg) = Hg.

(iii) f is a homomorphism, because

$$f\left(\mathrm{K}g_1 \cdot \mathrm{K}g_2\right) = f\left(\mathrm{K}g_1 g_2\right) = \mathrm{H}g_1 g_2$$
$$= \mathrm{H}g_1 \cdot \mathrm{H}g_2 = f(\mathrm{K}g_1) \cdot f(\mathrm{K}g_2)$$

(iv) $$\text{Ker}f = \{\mathrm{K}g \in \mathrm{G/K} \mid \mathrm{H}g = \mathrm{H}\}$$
$$= \{\mathrm{K}g \mid g \in \mathrm{H}\} = \mathrm{H/K}.$$

Hence by the fundamental theorem of homomorphism (G/K)/(H/K) $\cong$ G/H.

Exercise 4 : Let G be a group. The mapping f : G $\to$ G given by $f(g) = g^{-1}$ is an automorphism if and only if G is abelian.

Ans : Recall that an automorphism is an isomorphism of a group onto itself.

(i) f is calearly one-one, because $g_1 \neq g_2 \Rightarrow g_1^{-1} \neq g_2^{-1} \Rightarrow f(g_1) \neq f(g_2)$.

(ii) f is onto because $g \in$ G $\Rightarrow$ there is $g^{-1} \in$ G such that $f(g^{-1}) = (g^{-1})^{-1} = g$.

(iii) Is f a homomorphism ? Let $g, h \in$ G

$$f(gh) = (gh)^{-1} = h^{-1} g^{-1} = f(h) \cdot f(g)$$

If f were to be a homomorphism we require

$$f(gh) = f(g) f(h).$$

Thus f will be a homomorphism if and only

if $f(g) f(h) = f(h) f(g)$ or equivalently

$g^{-1} h^{-1} = h^{-1} g^{-1}$ or

$(hg)^{-1} = (gh)^{-1}$ or $hg = gh$.

Thus f is an automorphism if and only if G is abelian.

6.6 SUMMARY

A homorphism between groups is a mapping that is different from ordinary mappings we have learnt earlier. A homomorphism is a mapping that relates the structure of a group to another group. If a homomorphism is also a bijective mapping then it is called an isomorphism. The Kernal of a

homomorphism is the set of elements that get mapped onto the identity element. Homomorphism are closely related to quotient groups. The fundamental theorem of homomorphism states that the image of a group under a homomorphism is the quotient group modulo the kernal. This theorem has several consequences. We have studied some of them. The first one is that any two cyclic groups of same order are isomorphic. The second one is that if the quotient group modulo the center is cyclic, then the group is abelian. The concept of a group homomorphism and its application have far reaching consequences in the study of goups.

6.7 MODEL EXAMINATION QUESTIONS

SECTION - A (Long answer questions)

1. State and prove the fundamental theorem of homomorphism for goups.
2. Define a group homomorphism, the kernal of a homomorphism and give an example. Show that a homomorphism maps the identity onto identity, the inverse onto the inverse. Show further their ker f is normal subgroup.
3. Show that any two cyclic groups of the same order are isomorphic.

SECTION - B (Short answer questions)

1. State and prove Cayley's theorem for groups.
2. Let G be a group and H, a normal subgroup of G. Show that there is a natural homomorphism of G onto G/H.
3. G is a group and Z (G) the center of G. Show that if G/Z (G) is cyclic then G is abelian.
4. Let G and G′ be groups. Show that $f : G \to G'$ defined by $f(g) = g^{-1}$ is an automorphism if and only if G is abelian.

6.8 ANSWERS TO SELF ASSESSMENT QUESTIONS

SAQ 1 $f(x + y) = 2^{x+y} = = 2^x \cdot 2^y = f(x) \cdot f(y)$. Hence f is a homomorphism.

Ker $f = \{x \in G / f(x) = 1\} = \{0\}$.

SAQ 2 Since $e \in G$; $f(e) = e' \in f(G)$. Thus $f(a) \cdot (f(a))^{-1} = f(a) \neq \phi$. Let $a, b \in G$, then $f(a), f(b) \in f(G)$. Now $f(a) \cdot (f(b))^{-1} = f(a) f(b)^{-1} = f(ab)^{-1} \in f(G)$ since $ab^{-1} \in G$. Thus $f(G)$ is a subgroup of G′.

BLOCK–2 : RINGS AND VECTOR SPACES

Unit–7 : Rings and subrings

Unit–8 : Integral domains and fields

Unit–9 : Ideals and quotient rings

Unit–10 : Vector spaces

In Block 1 we have introduced algebraic systems that admit a single binary operation. In this Block we introduce algebraic systems with two binary operations. The mathematical objects of this Block are of relatively recent origin when compared to groups. The study of rings and ideals has gained importance by the contributions of Kummer (1835) to the theory of numbers. Integral domains and fields are special kinds of rings. Vector spaces are motivated by the consideration of Vectors in Physics. But today in many branches of mathematics the concept of a Vector space has become fundamental necessity

UNIT–7 : RINGS AND SUBRINGS

Contents

7.1 Aims and Objectives
7.2 Introduction
7.3 Rings
7.4 Subrings
7.5 Workedout exercises
7.6 Summary
7.7 Model Examination Questions
7.8 Answers to Self Assessment Questions

7.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to : (i) Define and give examples of rings and subrings, (ii) Verify certgain simple properties of rings, (iii) Solve problems on rings based on definitions and properties of rings.

7.2 INTRODUCTION

In Block 1 we have seen algebraic systems with one binary operation. We have studied in detail the set of integers under addition. We have seen that $(Z, +)$ is an abelian group. We also noticed that Z admits a second binary operation '.', (multiplication). And the operation '.' is distributive over addition. That is $a.(b + c) = a.b + a.c$ for $a, b, c \in Z$. This inspires us to define an algebraic structure with two binary operations and naturally $(Z, +, .)$ is an example of such a system. Such systems are called rings. It was David Hilbert (1862–19[illegible]) who first used the term Zahlring (Number ring) in describing sets of the form $\{a + b\xi \mid a, b \in Z\}$ where $\xi^2 + A\xi + B = 0$ with $A, B \in Z$. The ring of matrices and ring of polynomials play important role in investigation of problems in other branches of mathematics. Ring theory is a very active subject of research in mathematics.

7.3 RINGS

Definition :

A ring is a non empty set R together with two binary operations '+' and '.' and satsifying the following axioms :

(i) (R, +) is an abelian group,

(ii) (R, .) is a semi group,

(iii) $\left.\begin{array}{l} a.(b + c) = a.b + a.c \\ (b + c).a = b.a + c.a \end{array}\right\}$ for all $a, b, c \in R$.

Equivalently a ring is a triple (R, +, .) where

I. With respect to addition R is an abelian group. That is

(i) For all $a, b \in R$, $a + b \in R$, (closure property)

(ii) For all $a, b, c \in R$, $a + (b + c) = (a + b) + c$, (associative property)

(iii) For all $a \in R$, there exists $0 \in R$ such that

$$a + 0 = 0 + a = a, \text{ (identity property)}$$

(iv) For every $a \in R$, there exists $-a \in R$ such that

$$a + (-a) = (-a) + a = 0, \text{ (inverse property)}$$

(v) For every $a, b \in R$, $a + b = b + a$, (commutative property)

II. With respect to multiplication R is a semi group.

(vi) For all $a, b \in R$, $a \,.\, b \in R$, (closure property)

(vii) For all $a, b, c \in R$, $a.\ (b \,.\, c) = (a \,.\, b) \cdot c$, (associative property)

III. The operation of multiplication is distributive over the operation of addition

(viii) $a \,.\, (b + c) = a \,.\, b + a \,.\, c$, left distributive property

$$(b + c) \,.\, c = b \,.\, a + c \,.\, a, \text{ right distributive property}$$

IV. If in addition to these properties the commutative property with respect to multiplication ($a \,.\, b = b \,.\, a$ for $a, b \in R$) is satisfied, then we call the ring; a *commutative ring*

V. If the ring (R, +, .) has an identity element with respect to multiplication ($a \,.\, e = e \,.\, a = a$ for $a \in R$) then R is called a ring with unity.

Remark. 1 : It is customary to denote the additive identity of a ring by 0 (zero) and the multiplicative identity, if it exists, by 1 (one).

Example. 1 : Let Z denote the set of integers and + and . denote ordinary addition and multiplication. Then (Z, +, .) is a commutative ring with unity. We have already seen in unit 2 that (Z, +) is an abelian group. Since $a \,.\, b \in Z$, for $a, b \in Z$ the operation '.' is closed on Z. Further, for $a, b, c \in Z$, $(a \,.\, b) \,.\, c = a \,.\, (b \,.\, c)$ hence the associative property is satisfied. For any $a, b, c \in Z$, $a \,.\, (b + c) = a \,.\, b + a \,.\, c$ follows from ordinary arithmetic. Thus (Z, +, .) is a ring. Further, $a \,.\, b = b \,.\, a$ for $a, b \in Z$, implies that the ring (Z, +, .) is commutative. Since $1 \in Z$ and $a \,.\, 1 = 1 \,.\, a = a$ for $a \in Z$, 1 is the unity. Thus (Z, +, .) is a commutative ring with unity.

SAQ 1 Let 2Z denote the set of even integers. Verify that (2Z, +, .) is a commutative ring without unity.

Example. 2 : Let $M_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \text{ are reals} \right\}$ be the set of 2×2 matrices with real numbers as entries. Then under the operations of matrix addition and matrix multiplication $(M_2, +, .)$ is a ring. The addition and multiplication of 2×2 matrices yields again 2×2 matrices. Thus the operations are closed. If A, B, C are 2×2 matrices, then $(A + B) + C = A + (B + C)$ and $A \,.\, (B \,.\, C) = (A \,.\, B) \,.\, C$ showing that the operations are associative. The zero matrix is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the additive identity and the unit matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the multiplicative identity because

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ and}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

For $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2$, $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ is the additive inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, because

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Further, matrix addition is commutative

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix}$$

To verify left distributivity, we proceed as follows.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left\{ \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} + \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \right\} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' + a'' & b' + b'' \\ c' + c'' & d' + d'' \end{pmatrix}$$

$$= \begin{pmatrix} aa' + aa'' + bc' + bc'' & ab' + ab'' + bd' + bd'' \\ ca' + ca'' + dc' + dc'' & cb' + cb'' + dd' + dd'' \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cd' + dd' \end{pmatrix} + \begin{pmatrix} aa'' + bc'' & ab'' + bd'' \\ ca'' + dc'' & cb'' + dd'' \end{pmatrix}$$

$$= \begin{pmatrix} aa' + bc' + aa'' + bc'' & ab' + ab'' + bd' + bd'' \\ ca' + dc' + ca'' + dc'' & cb' + cb'' + dd' + dd'' \end{pmatrix}$$

Thus for A, B, C $\in M_2$,

$$A \cdot (B + C) = A \cdot B + A \cdot C$$

Similarly it can be verified that $(B + C) \cdot A = B \cdot A + C \cdot A$. Thus $(M_2, +, .)$ is a ring with unity. But it is not commutative as matrix multiplication is not commutative in general.

Example. 3 : Let $R = \{a + b\sqrt{2} / a, b \in Z\}$. Then $(R, +, .)$ is a commutative ring with unity. First of all + and . are binary operations because

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} = p + q\sqrt{2} \text{ for } p, q \in Z$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2cd + \sqrt{2}(ad + bc))$$

$$= p' + q'\sqrt{2} \text{ for } p', q' \in Z$$

The associativity can be easily verified.

The element $0 = 0 + 0\sqrt{2} \in R$ is the additive identity element and the element $1 = 1 + 0\sqrt{2} \in R$ is the multiplicative identity. For each $(a + b\sqrt{2}) \in R$, there is $(-a - b\sqrt{2}) \in R$ such that $(a + b\sqrt{2}) + (-a - b\sqrt{2}) = 0$.

Further $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (c + d\sqrt{2}) + (a + b\sqrt{2})$. Distributivity can be easily verified.

Thus (R, +, .) is a commutative ring with unity.

Example. 4 : Let $R = Z_2 = \{0, 1\}$, then $(R, \oplus, \odot)$ where $\oplus$ and $\odot$ are addition modulo 2 and multiplication modulo 2 is a cummutative ring with unity. To see this let us construct the addition and multiplication tables.

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

Here $1 \oplus 1 = 2 = 0 \pmod 2$

It can be verified that $(Z_2, \oplus)$ is an abelian group with 0 as the additive identity and 1 is the additive inverse of 1. 1 is the multiplicative identity.

Example. 5 : Let Z be the set of intergers and consider (Z, ⊕, ʘ) where ⊕ and ʘ are operations defined on Z as follows.

For $a, b \in Z$ define : $\begin{cases} a \oplus b = a + b - 1 \text{ and} \\ a \odot b = a + b - ab \end{cases}$

Then (Z, ⊕, ʘ) is a commutative ring with identity. To verify this we must veirfy that (i) the operations ⊕ and ʘ are binary associative operatons on Z (ii) The operaton ⊕ satsifies the identity, inverse and commutative properties and (iii) ʘ is distributive over ⊕.

(i) If a and b are integers $a + b - 1$ and, $a + b - ab$ are also integers. Let $a, b, c \in Z$.

$$a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + (b + c - 1) - 1 = a + b + c - 2$$

$$(a \oplus b) \oplus c = (a + b - 1) \oplus c = (a + b - 1) + c - 1 = a + b + c - 2$$

Thus $(a \oplus b) \oplus c = a \oplus (b \oplus c)$

$$a \odot (b \odot c) = a \odot (b + c - bc) = a + (b + c - bc) - a(b + c - bc)$$

$$= a + b + c - ab - ac - bc - abc.$$

$$(a \odot b) \odot c = (a + b - ab) \odot c = (a + b - ab) + c - (a + b - ab)c$$

$$= a + b + c - ab - ac - bc - abc.$$

Thus $a \odot (b \odot c) = (a \odot b) \odot c.$

Thus the operations ⊕ and ʘ are binary associative operations. The elements $1 \in Z$ and $0 \in Z$ are the identity elements with respect to ⊕ and ʘ respectively. Because

$$a \oplus 1 = a + 1 - 1 = a, 1 \oplus a = 1 + a - 1 = a \text{ and}$$

$$a \odot 0 = a + 0 - a.0 = a, 0 \odot a = 0 + a - 0.a = a.$$

The element $-a$ is the inverse of $a \in Z$ because

$$a \oplus (-a) = a - a + 1 = 1; (-a) \oplus a = -a + a + 1 = 1$$

$$\text{and } a \oplus b = b \oplus a = a + b - 1; a \odot b = b \odot a = a + b - ab.$$

Then (Z, ⊕) is an abelian group and (Z, ʘ) is a commutative semigroup with unity. Now to check distributive laws,

$$a \odot (b \oplus c) = a \odot (b + c - 1) = a + (b + c - 1) - a(b + c - 1)$$

$$= 2a + b + c - ab - ac + a - 1 = 2a + b + c - ab - ac - 1$$

$$a \odot b \oplus a \odot e = (a + b - ab) \oplus (a + c - ac) = a + b - ab + a + c - ac - 1$$

$$= 2a + b + c - ab - ac - 1. \text{ Thus}$$

$$a \odot (b \oplus c) = a \odot b \oplus a \odot c.$$

Since ʘ is commutative : $(b \oplus c) \odot a = b \odot a \oplus c \odot a.$

Thus (Z, ⊕, ʘ) is a commutative ring with unity.

Example. 6 : Let **R** denote the set of real numbers. Consider the set R of continuous real valued functions with "addition" and multiplication as follows :

$$R = \{f \mid f : \mathbf{R} \to \mathbf{R}, f \text{ is continuous}\}$$

For $f, g \in R$, $(f + g)x = f(x) + g(x) \; \forall \; x \in \mathbf{R}$ and

$$(fog)x = f(x)\, g(x) \; \forall \; x \in \mathbf{R}.$$

Then the operations + and o are binary associative because $f(x)$, $g(x)$ etc., are real numbers. The zero function defined by $f(x) = 0\ \forall x \in \mathbf{R}$ is the additive identity and the inverse of f is defined by $-f$, that is $(-f)(x) = -f(x)\ \forall x \in \mathbf{R}$ is the additive inverse. $f + g = g + f$ follows from the properties of real numbers. Thus $(R, +, o)$ is a cummutative ring. The identity function $f(x) = x$, $\forall x \in \mathbf{R}$ is the identity of R. Thus R is a commutative ring with unity.

SAQ 2 Let G be an abelian group with respect to "+" and with identity '0'. Define multiplication on G by $a \,.\, b = 0\ \forall\ a, b \in$ G. Show that (G, +, .) is a ring.

Example. 7 : Let S be any set and let P (S) denote the Power set of S (i.e., P (S) is the collection of all the subsets of S). Define "+" and "·" on P (S) by

$A + B = (A \cup B) - (A \cap B)$; $A.B = A \cap B\ \forall\ A, B \in P(S)$.

Then P (S) is a commutative ring under the operations of "+" and "·".

The empty set ϕ is the additive identity and the set A itself is the inverse of A. The operations "+" and "." are binary operatons follows from the fact that unions and intersections of subsets from the power set give again subsets from the power set. The only operation to be verified are the properties of distributivity. That is

$$\begin{aligned} A \,.\, (B + C) &= A \cap (B + C) = A \cap \{(B \cup C) - (B \cap C)\} \\ &= A \cap (B \cup C) - A \cap (B \cap C) \\ &= (A \cap B) \cup (A \cap C) - A \cap B \cap C \\ \text{Now } A \,.\, B + A \,.\, C &= A \cap B + A \cap C \\ &= (A \cap B) \cup (A \cap C) - (A \cap B) \cap (A \cap C) \\ &= (A \cap B) \cup (A \cap C) - A \cap B \cap C. \end{aligned}$$

Similarly the other distributive law could be verified.

SAQ 3 Verify that the set of integers modulo 5 form a commutative ring with unity under modulo addition and multiplication.

Theorem. 1 :

> Let R be a ring with 0 as the additive identity. Let $a, b \in$ R. Then
>
> (i) $a \,.\, 0 = 0 \,.\, a = 0$
>
> (ii) $(a) \,.\, (-b) = (-a) \,.\, (b) = -(a \,.\, b)$
>
> (iii) $(-a) \,.\, (-b) = a \,.\, b$
>
> (iv) If R has unity 1, then $(-1)(-1) = 1$

[Before we give the proof, it must be emphasised to the student that the above statements are not as obvious as they appear to be. This is because we can only use those axioms that are used in the definition of the ring]

Proof : (i) Since 0 is the additive identity we have that $0 + 0 = 0$.

Thus $a \,.\, 0 = a \,.\, (0 + 0) = a \,.\, 0 + a \,.\, 0$ But $a \,.\, 0 = a \,.\, 0 + a \,.\, 0 \Rightarrow a \,.\, 0 = 0$

Here we have used the fact that if $x + y = x$ then

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

SAQ 4 Prove that, $0 \,.\, a = 0$ for $a \in$ R, R a ring.

(ii) Let $x = -(a \cdot b)$. Then $x + (a \cdot b) = -(a \cdot b) + a \cdot b$ and hence $x + (a \cdot b) = 0 = (a \cdot b) + x$

$$\begin{aligned}
\text{Now } (-a) \cdot b &= (-a) \cdot b + 0, \text{ identity property} \\
&= (-a) \cdot b + (a \cdot b) + x \\
&= \{(-a) \cdot b + (a \cdot b)\} + x, \text{ associativity} \\
&= (-a + a) \cdot b + x, \text{ distributivity property} \\
&= 0 \cdot b + x \text{ additive inverse property} \\
&= 0 + x \text{ by (i)} \\
&= x \text{ by additive identity} \\
\text{Thus } (-a) \cdot b &= -(a \cdot b)
\end{aligned}$$

SAQ 5 $a \cdot (-b) = -(-a \cdot b)$ for $a, b \in R$, a ring.

(iii) $(-a) \cdot (-b) = -a \cdot (-b) = -(-a \cdot b) = a \cdot b$ because $\left(a^{-1}\right)^{-1} = a$ in a group and (R, +) is a group.

(iv) If the multiplicative identity (unity) $1 \in R$, then (R, +) being a group, the additive inverse $(-1) \in R$. Then $(-1)(-1) = 1$ by (iii).

Remark. 1: If R is a ring with unity 1, then there is an element $-1 \in R$ which is self invertable. Equivalently R has an element of order 2.

Definition :

> Let R be a ring with identity and let $a \in R$. If a has a multiplicative inverse in R, then a is called a *unit* of R.

SAQ 6 What are the units of the ring $(\mathbb{Z}, \cdot)$?

7.4 SUBRINGS

Whenever we introduce an algebraic structure it is natural to ask whether any substructure inherits the properties of the original structure. Recall the definition of a subgroup, where a non empty subset inherits all the properties of the group. The notion of a sub ring is one such.

Defintion. 2 :

> Let (R, +, .) be a ring and let S be a non empty subset of R. we say that S is a subring of (R, +, .) if S is a ring with respect to the operations defined on R. That is, a nonempty subset S of a ring (R, +, .) is a subring if (S, +, .) is a ring in its own right. This means that (S, +) must be an abelian group and (S, .) must be a semigroup and for $a, b, c \in S$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

Theorem. 2 :

> Let S be a nonempty subset of a ring (R, +, .) Then S is a subring of R if and only if
>
> (i) $a, b \in S \Rightarrow a \cdot b \in S$
>
> (ii) $a, b \in S \Rightarrow a - b \in S$

Proof : Suppose $S \subseteq R$ and $S \neq \phi$ is a subring of R. Then (S, +, .) is a ring. Then by the hypothesis that (S, .) is a semigroup implies that (S, .) is closed. That is $a, b \in S \Rightarrow a \cdot b \in S$. Further (S, +) is an abelian group or (S, +) is an abelian subgroup of (R, +). Recall from unit 3, that S is a

subgroup of a group R if and only if $a \cdot b^{-1} \in S$ for $a, b \in S$. Under the operation of addition $b^{-1} = -b$ and $ab^{-1} = a - b$. Then $a - b \in S$. Conversely suppose $S \subseteq R$, $S \neq \phi$ is such that for $a, b \in S$, $a \cdot b \in S$ and $a - b \in S$. Now $a, b \in S \Rightarrow a - b \in S \Rightarrow$ that (S, +) is a (abelian) subgroup of (R, +). And $a.b \in S$ for $a, b \in S \Rightarrow$ that (S, .) is closed. The associativity in (S, .) is a consequence of (R, .) and the distributivity of '.' over '+' is a consequence of the same property in R, Thus (S, +, .) is a subring.

Theorem. 3 :

> If (S, +, .) and (T, +, .) are subrings of (R, +, .) then (S ∩ T, +, .) is also a subring of (R, +, .).

Proof : Let $a, b \in S \cap T$, then $a, b \in S$ and $a, b \in T$. But S is a subring $\Rightarrow$ that $a \cdot b \in S$ and $a - b \in S$, for $a, b \in S$ and T is a subring $\Rightarrow$ that $a \cdot b \in T$ and $a - b \in T$, for $a, b \in T$. Thus $S \cap T \subset R$, $S \cap T \neq \phi$ and $a \cdot b \in S \cap T$ and $a - b \in S \cap T$. Thus (S ∩ T, +, .) is a subring of (R, +, .).

Remark. 3 : If S and T are subrings of R, then S ∪ T need not be a subring of R. Consider $R = Z_6 = \{0, 1, 2, 3, 4, 5\}$, the set of integers modulo 6, under the operations of modulo addition and modulo multiplication. Now $R' = \{0, 3\}$ and $S' = \{0, 2, 4\}$ are subrings of $R = Z_6$. Now $R' \cup S' = \{0, 2, 3, 4\}$ is not a subring of R because $2 \in R' \cup S'$, $3 \in R' \cup S'$ but $2 + 3 = 5 \notin R' \cup S'$. Another example is R = (Z, +, .); S = (2Z, +, .); T = (3 Z, +, .). Then S ∩ T = (6Z, +, .) is a ring but S ∪ T is not.

Example. 8 : Let (R, +, .) be a ring. Then R is a subring of itself. Similarly R = {0} is a sub ring. These are called trivial subrings of R.

Example. 9 : (Z, +, .) is the ring of integers. Then (2Z, +, .) is a subring of (Z, +, ·). Noice here that the subring has no unity though the ring has the unit element.

Example. 10 : Let $R = M_2(Q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in Q \right\}$ be the ring of 2×2 matrices over the rationals. Let $S = T_2(Q) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a, b, d \in Q \right\}$. Then $T_2(Q)$ is a subring of $M_2(Q)$. Notice here that $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} p & q \\ 0 & r \end{pmatrix} \in T_2(Q)$ and $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} - \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} p' & q' \\ 0 & r' \end{pmatrix} \in T_2(Q)$.

7.5 WORKEDOUT EXERCISES

Exercise. 1 : Let R be a ring such that for every $x \in R$, $x^2 = x$. Show that R is commutative.

Ans : We are required to show that for $x, y \in R$, $x.y = y.x$ (i) consider $(x + x)^2 = (x + x)$, by hypothesis. But

$$(x + x)^2 = (x + x) \cdot (x + x) = x \cdot x + x \cdot x + x \cdot x + x \cdot x$$

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

But $(x + x)^2 = (x + x) \Rightarrow x + x + x + x = x + x$ or $x + x = 0 \Rightarrow x = -x$.

Let $x, y \in R$. Then $x + y \in R$ and $(x + y)^2 = x + y$. That is

$(x + y) \cdot (x + y) = x + y \Rightarrow x^2 + x \cdot y + y \cdot x + y^2 = x + y$

But $x^2 = x$ and $y^2 = y \Rightarrow x + x \cdot y + y \cdot x + y = x + y$.

$\Rightarrow x \cdot y + y \cdot x = 0 \Rightarrow x \cdot y = -y \cdot x = y \cdot x$ $(\because x = -x)$

Thus R is commutative.

Exercise. 2 : Let R be a ring with unity such that $(x \,.\, y)^2 = x^2 \,.\, y^2$ for all $x, y \in R$. Show that R is commutative.

Proof : Let x and y be any two arbitrary elements in R.

We are required to show that $x \,.\, y = y \,.\, x$. Consider $(x + xy)^2$. Since $x + xy = x\,(1 + y)$ by left distributivity $(x + xy)^2 = [x\,(1 + y)]^2$. That is

$$x^2 + x\,(xy) + (xy)\,x + x^2\,y^2 = x^2\,(1 + y)^2 \qquad \left(\because (xy)^2 = x^2\,y^2\right)$$

$x^2 + x^2\,y + xy\,x + x^2\,y^2 = x^2\left(1 + 2y + y^2\right)$. Then

$$x^2 + x^2\,y + xyx + x^2\,y^2 = x^2 + 2x^2\,y + x^2\,y^2$$

$$\Rightarrow xy\,x = x^2\,y.$$

Since this result is true for all $x, y \in R$ and since R is a ring with unity, this is true for $(x + 1)$ and y also

Thus $(x + 1)\,y\,(x + 1) = (x + 1)^2\,y$. This implies

$$xy\,x + xy + yx + y = x^2\,y + 2xy + y$$

$$\Rightarrow xy + yx = 2xy \quad \left(\because xyx = x^2\,y\right)$$

$$\Rightarrow yx = xy.$$

(Notice here at each stage we have used only those operatons permitted by the axiom in the definition of the ring. The difficultly has been that existence of x^{-1} could not be assumed).

Exercise. 3 : Let R be an algebraic system satisfying all axioms of a ring with unity except the axiom of additive commutativity. Show that this axiom must hold in R, so that R becomes a ring with unity.

Ans : Let a and b be any two arbitrary elements of R and let 1 be the unity in R. That is $a \,.\, 1 = 1 \,.\, a = a, \forall\, a \in R$.

Consider $(a + b) \cdot (1 + 1) = (a + b) \,.\, 1 + (a + b) \,.\, 1$

$$= a + b + a + b$$

But $(a + b) \,.\, (1 + 1) = a \,.\, (1 + 1) + b \,.\, (1 + 1)$ also

$$= a + a + b + b. \text{ Thus}$$

$$a + b + a + b = a + a + b + b$$

$$\Rightarrow b + a = a + b \text{ and R is a ring.}$$

Exercise. 4 : Show that a ring R is commutative if and only if $(a + b)^2 = a^2 + 2ab + b^2$ for $a, b \in R$.

Ans : Suppose R is a commutative ring. Then $a \,.\, b = b \,.\, a$.

Now $(a + b)^2 = (a + b) \,.\, (a + b) = a^2 + b \,.\, a + a \,.\, b + b^2$

But $b \,.\, a = a \,.\, b \Rightarrow b \,.\, a + a \,.\, b = 2a \,.\, b$

Thus $(a + b)^2 = a^2 + 2\,ab + b^2$.

Conversely, suppose $(a + b)^2 = a^2 + 2\,ab + b^2$ for all $a, b \in R$, Then we are required to show that $a \,.\, b = b \,.\, a$ for all $a, b \in R$. Now

$$(a + b)^2 = (a + b) \,.\, (a + b) = a^2 + a \,.\, b + b \,.\, a + b^2$$

$$= a^2 + 2ab + b^2. \text{ Thus}$$

$$a \,.\, b + b \,.\, a = 2\,(a \,.\, b) \Rightarrow b \,.\, a = a \,.\, b$$

and R is commutative.

7.6 SUMMARY

In this unit we have defined an algebraic structure consisting of a non empty set admitting two binary operations. For easy identification we have named the operations as addition and multiplication. This algebraic system then becomes a ring if it is abelian group with respect to addition and a semi group with respect to multiplication. We also require the operation of multiplication to be distributive over addition. Such algebraic systems are very abundant. We have defined the notion of a subring and given examples. We have applied the theory to solve same exercises.

7.7 MODEL EXAMINATION QUESTIONS

SECTION - A (Long Answers)

(i) Define a ring and give an example. Show that a ring R with unity is commutative if

$(x \cdot y)^2 = x^2 \cdot y^2$ for all $x, y \in R$.

(ii) Define the subring of a ring and give an example. Show that the intersection of two subrings is again a subring. What can be said about the union of two subrings? Justify your answer.

SECTION - B (Short Answers)

(i) Show that a ring R is commutative if and only if $(a + b)^2 = a^2 + 2ab + b^2$ for all $a, b \in R$.

(ii) A ring R is called boolean ring if $x^2 = x$ for all $x \in R$. Show that a boolean ring is commutative.

(iii) Let R be a ring. Show that for $a, b \in R$

$a \cdot 0 = 0 \cdot a = 0$ and $(-a)(b) = -(ab)$.

(iv) Show that the set of all 2×2 matrices with real entries is a ring with unity.

(v) Let $i^2 = -1$. Show that the set $R = \{a + bi \mid a, b \in Z\}$ is a ring under the operations of addition and multiplication of complex numbers.

7.8 ANSWERS TO SAQ'S

SAQ 1 $(2Z, +)$ is an abelian group. 0 is the additive identity. Since $2a \cdot 2b = 2(2ab) \in Z$, '.' is closed. That it is associative follows from elementary arithmatic. Distributive laws hold good.

Thus $(2Z, +, .)$ is a ring. $1 \notin 2Z$. Thus there is no $e \in 2Z$ such that $a \cdot e = e \cdot a = a$ for $a \in 2Z$.

SAQ 2 $(G, +)$ is already abelian, The operation '.' is a binary operation because $a \cdot b = 0 \in G$ $\forall a, b \in G$. $a \cdot (b \cdot c) = a \cdot 0 = 0 = (a \cdot b) \cdot c$, shows that $(G, .)$ is a semi group. (Here $a \cdot 0 = 0$ by definition of '.') Now $a \cdot (b + c) = 0$ because $b + c = d \in G$ and $a \cdot d = 0$ by definition, so is $a \cdot b + a \cdot c$. Similarly the other distributive law.

SAQ 3 We construct addition and multiplication modulo 6 for the set of integers modulo 6 = $\{0, 1, 2, 3, 4, 5\}$.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Closure is obvious from the tables. Associativity could be verified as :

$$(1 + 4) + 5 = 5 + 5 = 4 = 1 + (4 + 5) \text{ etc.}$$

$$(2. 3) . 4 = 0 . 4 = 0 = 2 . (3 . 4) \text{ etc}$$

0 is the additive identity 1 is the unity. The additive inverse of 1, 2, 3, 4, 5 are 5, 4, 3, 2, 1 respectively. Commutativity with respect to addtion is verified from the table. Distributivity can also be verified as

$$2 . (3 + 4) = 2 . 1 = 2; 2 . 3 + 2 . 4 = 0 + 2 = 2 \text{ etc.}$$

SAQ 4 $0 . a = (0 + 0) . a = 0 . a + 0 . a$ by right distributive property.

$0 . a = 0 . a + 0 . a \Rightarrow 0 . a = 0.$

SAQ 5 $a . (-b) = a . (-b) + 0.$

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

$= [a . (-b) + a . b] - (a . b)$

$= [a . (-b + b)] - (a . b)$

$= [a . 0] - a . b = 0 - a . b = - a . b.$

SAQ 6 1 and – 1 are the only units of (Z, +, .). If possible let $a \in R$ and a is a unit. Then there is $b \in Z$ such that $a . b = 1$, but the only integers whose product is 1 are 1 and – 1.

UNIT–8: INTEGRAL DOMAINS AND FIELDS

Contents

8.1 Aims and Objectives

8.2 Introduction

8.3 Integral Domains and Fields

8.4 Polynomial Rings

8.5 Workedout exercises

8.6 Summary

8.7 Model Examination Questions

8.8 Answers to Self Assessment Questions

8.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to : (i) Define an integral domain and a field and give examples (ii) Prove theorem connecting integral domains and fields (iii) Define a polynomial ring and prove that $R[x]$ is a ring (iv) Verify that real quaternions form a skew field.

8.2 INTRODUCTION

In the study of rings in Unit 7, we have carefully avoided certain questions regarding the multiplication properties. Consider for example the ring $(Z_6, \oplus, \odot)$, where Z_6 is the set of integers modulo 6, and $\oplus, \odot$ are modulo addition and modulo multiplication. When we constructed the multiplication tables we had a situation where the product of two non zero integers gave zero under the binary composition of multiplication. For example, $2 \odot 3 = 0 = 3 \odot 2$; $4 \odot 3 = 0 = 3 \odot 4$, thus 2, 3 and 4 are themselves non zero. We cannot simply carry our cancellations like $a \cdot b = a \cdot c \Rightarrow b = c$. Notice that $3 \odot 2 = 3 \odot 4$. If we allow left concellation of 3 we get the absurd conclusion $2 = 4$. Consider also the example of ring of 2×2 matrices $(M_2, +, \cdot)$ under matrix addition and multiplication. $A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ are non zero matrices in M_2, but their product AB is the zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ These examples and others make us look for algebraic structures where the cancellation laws with respect to multiplication hold and that we can talk of multiplicative inverses of elements as well. Integral domains and fields appear in this context.

8.3 INTEGRAL DOMAINS AND FIELDS

Definition 1 :

Let R be a ring and $a \neq 0$ be an element of R. We say that a is a left zero divisor if there exists $b \in R$, $b \neq 0$ such that $a \cdot b = 0$. Similarly, we can define a right zero divisor. An element $a \in R$ is called a zero divisor if it is both a right zero divisor and a left zero divisor. If R is a commutative ring then every left zero divisor is a right zero divisor as well.

Example 1 : $M_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in Z \right\}$ is the ring of 2 x 2 matrices under matrix addition and matrix multiplication. Let $A = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$ and $B = \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix}$ Then A and B are non zero matrices and $AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ Thus A is a left zero divisor, and B is the right zero divisor. Notice here that $BA = \begin{pmatrix} 0 & bd \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Example 2 : $R = (Z_{12}, +, \cdot)$ is the set of integers modulo 12. Under modulo addition and modulo multiplication. Z_{12} is a commutative ring. The zero divisors of Z_{12} are 2, 3, 4, 6, 8, 9 and 10 because none of these members in Z_{12} is zero and yet $2.6 = 0$; $3.4 = 0$; $3.8 = 0$; $4.6 = 0$; $4.9 = 0$; $6.8 = 0$; $6.10 = 0$; $8.9 = 0$ etc.

Definition 2 :

An *integral domain* is a commutative ring with unity and having no zero divisors. Equivalently a commutative ring with unity is called an integral domain if for $a, b \in R$ and if $a \cdot b = 0$, then either $a = 0$ or $b = 0$.

Remark 1 : Some text books do not insist on the existence of unity element in the integral domain. But most examples we can think of have unity element.

Example 3 : $(Z, +, \cdot)$ is an integral domain. We have already seen this to be a commutative ring with unity. Observe that if a and b are integers such that $a \cdot b = 0$, then either $a = 0$ or $b = 0$ (or $a \cdot b = 0$ and $a \neq 0 \Rightarrow b = 0$).

Example 4 : $(Z_5, +, \cdot)$, the set of integers modulo 5 under the operations of modulo addition and modulo multiplication is an integral domain. We have already seen that $(Z_5, +, \cdot)$ is a commutative ring with unity. Recall that $Z_5 = \{0, 1, 2, 3, 4\}$. If $a, b \in Z_5$ and if $a \cdot b = 0$ and $a \neq 0$, then $b = 0$. Thus $(Z_5, +, \cdot)$ does not admit zero divisors. $2.3 = 1 \neq 0$; $2.4 = 3 \neq 0$; $3.4 = 2 \neq 0$. Of course 1.2, 1.3, 1.4 are non zero elements of Z_5.

Remark 2 : Compare this example with $(Z_6, +, \cdot)$ which is not an integral domain because $2 \neq 0$; $3 \neq 0$ and $2.3 = 0$. This makes us state the following theorem.

Theorem 1 :

In the commutative ring $(Z_n, +, \cdot)$, the zero divisors are those elements which are not relatively prime to n.

Proof : Recall that $Z_n = \{0, 1, 2, \ldots, (n-1)\}$. Let $m \in Z_n$ be such that $m \neq 0$ and $(m, n) = d \neq 1$. Here (m, n) denotes the g.c. d of m and n. That is 'd' divides m and d divides n. Then $(m) \cdot \left(\frac{n}{d}\right) = \left(\frac{m}{d}\right) \cdot (n) = 0$ in Z_n because $\left(\frac{m}{d}\right) \cdot n$ is a multiple of n. But neither m nor $\frac{n}{d}$ is zero in Z_n. Thus m is a zero divisor of Z_n.

If $m \in Z_n$ be such that $m \neq 0$ and $(m, n) = 1$, then $m \cdot r \neq 0$ for $r \in Z_n$ and $r \neq 0$. To see this let $m \cdot r = 0$. Then n divides $m \cdot r$. But $(m, n) = 1$ implies n divides r and $r \in Z_n \Rightarrow r = 0$. Thus $m \cdot r = 0$ and $m \neq 0 \Rightarrow r = 0$ and hence m is not zero divisor.

Remark 3 : Let p be a prime number. Then $(Z_p, +, \cdot)$ is an integral domain because Z_p does not admit zero divisors. Observe that p is relatively prime to all non zero integers in Z_p.

Theorem 2 :

> Let $(R, +, \cdot)$ be a commutative ring. R does not admit zero divisors if and only if cancellation laws (with respect to multiplication) hold in R.

Proof : Let $(R, +, \cdot)$ be a commutative ring and let R not admit any zero divisors. We are required to show that cancellation laws hold good in R. Since R is commutative it is enough if we verify one cancellation law. Let $x, y, z \in R$ be such that $x \cdot y = x \cdot z$ and $x \neq 0$.

$$\text{Now } x \cdot y = x \cdot z \Rightarrow x \cdot y - x \cdot z = 0$$

$$\Rightarrow x \cdot (y - z) = 0.$$

But $x \in R$ and $(y - z) \in R$ and R does not admit zero divisors. This means that $y - z = 0$ or $y = z$. Since $x \cdot y = x \cdot z$ implies $y = z$, the left cancellation law holds good in R and R being commutative, the right cancellation law holds good in R as well.

Conversely suppose $(R, +, \cdot)$ is a commutative ring in which $x \cdot y = x \cdot z \Rightarrow y = z$, for all x, y, z in R. We are required to show that R does not admit zero divisors. Let $x \neq 0$ be such that $xy = 0$. Since $x \cdot 0 = 0$ in a ring, we can write $x \cdot y = x \cdot 0 = 0$. But by cancellation laws $y = 0$. Thus x is not a zero divisor.

SAQ 1 Solve $3x = 2$ in Z_7.

Definition 3 :

> Let D be an integral domain. If there exists a positive integer n such that $na = 0$ for all $a \in D$, then the least such positive integer is called the characteristic of the integral domain. If no such positive integer exists, then D is said to be of cahracteristic zero. For example, the characteristic of the integral domain $(Z, +, \cdot)$ is zero, where as the characteristic of $(Z_5, +, \cdot)$ is 5.

Remark 4 : Though we have defined the characteristic for an integral domain, it can be defined for a ring also in the similar way.

Theorem 3 :

> The characteristic of an integral domain is either zero or a prime number.

Proof : Let D be an integral domain whose characteristic is not zero. Then the characteristic of D is a positive integer $m > 1$. If possible let $m = a \cdot b$ for some positive integers a and b where $1 < a < m$

and $1 < b < m$. Then $m \cdot 1 = 0$ because m is the characteristic of D and $1 \in D$. This implies that $m = a \cdot b = (a \cdot 1)(b \cdot 1) = 0$. But D being an integral domain $(a \cdot 1)(b \cdot 1) = 0$, implies $a \cdot 1 = 0$ or $b \cdot 1 = 0$. This means that the characteristic of D is either a or b. But m is the characteristic of D implies that m is the least positive integer such that $m \cdot 1 = 0$. Thus the assumption $m = a \cdot b$ is wrong. That means that m is a prime number.

Definition 4 :

An integral domain is said to be a *field* if the non-zero elements under multiplication form a group. Equivalently a non empty set F with atleast two elements is said to be a field under the binary compositions of "+" and "·" if

(i) (F, +) is an abelian group,

(ii) (F′, ·) is an abelian group where $F' = F - \{0\}$

(iii) $a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a, b, c \in F$.

Example 5 : (R, +, ·), the set of real numbers under the binary operations of addition and multiplication is a field. This is because (R, +) is an abelian group, (R′, ·) is an abelian group '·' is distributitive over addition.

Example 6 : (Q, +, ·), the set of rational numbers under addition and multiplication is a field.

Example 6 : The set of integers modulo 3, under the operations of modulo addition and modulo multiplication is a field. Consider $(Z_3, +, \cdot)$ and construct the addition and multiplication tables. $Z_3 = \{0, 1, 2\}$ and $Z_3' = \{1, 2\}$.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	1	2
1	1	2
2	2	1

$(Z_3, +)$ is an abelian group. $(Z_3', \cdot)$ is an abelian group and '·' is distributive over addition.

SAQ 2 Find the inverses of 3 and 7 in Z_{11}.

Theorem 4 :

Every field is an integral domian but not conversely.

Proof : Let F be a field. Then (F, +) and (F′, ·) are abelian groups. Lets $a, b \in F$ and let $a \neq 0$. Then a^{-1} exists. Suppose that $a \cdot b = 0$.

Then $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$. That is

$(a^{-1} \cdot a) \cdot b = 0$ or $e \cdot b = 0 \Rightarrow b = 0$.

Then $a \cdot b = 0$ and $a \neq 0 \Rightarrow b = 0$. Thus F does not admit zero divisors. Since F is a commutative ring with unity and without zero divisors, F is an integral domain.

The converse is not true. Consider (Z, +, ·). This is an integral domain but (Z, +, ·) is not a field because (Z′, ·) is not a group. Given $a \in Z$, there is no 'b' $\in Z$ such that $a \cdot b = 1$. Thus (Z, +, ·) is not a field.

Remark 5 : Though an integral domain is not a field, in general, an additional condition on the integral domain makes it a field as the following theorem indicates.

Theorem 5 :

Every finite integral domain is a field.

Proof : Let D be a finite integral domain whose distinct elements are listed as :

$$D = \{0, 1, a_1, \ldots a_n\}$$

Let $a \neq 0$, be an arbitrary element of D. Then $a \cdot D' = \{a \cdot 1, a \cdot a_1, \ldots a \cdot a_n\}$ are distinct among themselves and distinct from the non zero elements of D. To see this suppose $a \cdot a_i = a \cdot a_j$. Then $a \cdot (a_i - a_j) = 0$. Since D is an integral domain and $a \neq 0$ implies that $a_i - a_j = 0$ or $a_i = a_j$. Further, none of the elements in a D′ is zero, because in an integral domain the product of two non zero elements is again non zero. Thus the non zero elements of D are same as the elements of a D′ in some order. Since $1 \in$ D, there exists an $a_i \in$ such that $a\, a_i = 1$ and by commutativity in D, $a_i a = 1$ as well. Thus a_i is the multiplicative inverse of a. Since 'a' is arbitrary every element in D′= D – {0} has a multiplicative inverse and (D′, ·) is a group. Since (D, +, ·) is an integral domain in which non zero elements of D form a group, (D, +, ·) is a field.

SAQ 3 Show that Z_p, p a prime is a field.

Definition 5 :

Let (R, +, ·) be a ring with unity. If R′ = R – {0} forms a group under the operation of '·' then R is called a skew field. Equivalently a skew field is an algebraic structure in which all the conditions of the field, except the commutativity with respect to multiplication hold. A commutative skew field is a field. Different authors use the term division ring to denote a skew field.

Example 7 : The set of non-singular matrices of order 2 x 2 is an example of a skew field or a divison ring. All the properties of the field except the commutativity of multiplication hold and hence this set forms a skew field.

Example 8 : We have already seen that the eight elements $\{\pm 1, \pm i, \pm j, \pm k\}$ where $i^2 = j^2 = k^2 = -1$ and $ij = -ji = 1$; $jk = -kj = 1$ and $ki = -ik = 1$ form a non abelian group under the operation of multiplication. Let us now consider the set of real quaternions of the form

$Q = \{a + bi + cj + dk \mid a, b, c, d$ are reals and i, j, k as defined above$\}$.

Addition is defined on Q by point wise. That is

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')\, i + (c + c')\, j + (d + d')\, k \in Q.$$

The element $(0 + 0i + 0j + 0k)$ is the additive identity and $(-a - bi - cj - dk)$ is the additive inverse of $(a + bi + cj + dk)$. The commutativity property

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a' + b'i + c'j + d'k) + (a + bi + cj + dk)$$
$$= (a + a') + (b + b')\, i + (c + c')\, j + (d + d')\, k$$

follows from the commutativity of real numbers.

Then (Q, +) is an abelian group.

$$(a + bi + cj + dk) \cdot (a' + b'i + c'j + d'k) = (ab' - bb' - cc' - dd')$$
$$+ (ab' + ba' + cd' - dc')\, i + (ac' - bd' + ca' + db')\, j$$
$$+ (ad' + bc' - cb' + da')\, k \in Q$$

$(1 + 0i + 0j + 0k)$ is the multiplicative identity (unity), and the multiplicative inverse of $(a + bi + cj + dk)$

$$= \frac{1}{\left(a^2 + b^2 + c^2 + d^2\right)} (a - bi - cj - dk).$$

Thus $(Q', \cdot)$ is a group (not necessarily commutative because $ij \neq ji$ etc).

The distributive property could be similarly verified . Thus $(Q, +, \cdot)$ is a skew field.

8.4 POLYNOMIAL RINGS

Right from the days of secondary school, we are familiar with polynomials, their addition and multiplication. But we have not attempted to give a formal definition of a polynomial and avoided polynomials with irrational coefficients or polynomials whose coefficients belong to Rings and finite integral domains. Rings of polynomials play a very important role in the advanced study of Rings and provide examples in the abstract study of divisibility properties.

Definition 6 :

> A polynomial with coefficients in Q is an infinite sequence $(a_0, a_1, a_2 \ldots)$ in which all but a finite $a_i \in Q$ are zero.

Remark 6 : This kind of definition answers several questions regarding the "indeterminate" x and also the questions regarding "+" among the terms of the polynomial and "." between a_i and x^i. Such a kind of definition will allow us to have the coefficients from an arbitrary ring instead of having the coefficeints always from Z, or Q or R. We treat the terms, $x, x^2, x^3, \ldots$ as nothing more than position markers.

Thus the polynomial $(a_0, a_1, a_2 \ldots a_n) \equiv a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$.

Remark 7 : Let R be a ring. Then a polynomial in x (where x is a symbol or x is an indeterminate) with coefficient in R is a formal sum

$$a_0 + a_1 x + a_2 x^2 + \ldots = \sum_i a_i x^i$$

where $a_i \in R$ for all i and $a_i = 0$ for sufficiently large i.

Remark 8 : If f and g be two polynomials given by

$$f = (a_0, a_1, \ldots a_n) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n.$$

$$g = (b_0, b_1, \ldots a_n) = \sum_{i=0}^{n} b_i x^i = b_0 + b_1 x + \ldots + b_n x^n.$$

Then
$$f + g = (a_0 + b_0, a_1 + b_1, \ldots a_n + b_n) = \sum_{i=0}^{n} (a_i + b_i) x^i$$
$$= (a_0 + b_0) + (a_1 + b_1)x + \ldots\ldots + (a_n + b_n)x^n$$
$$\text{and } f \cdot g = (a_0, a_1, \ldots a_n) \cdot (b_0, b_1, \ldots b_n)$$

$$= \left(a_0 + a_1 x + \ldots + a_n x^n\right) \cdot \left(b_0 + b_1 x + \ldots + b_n x^n\right)$$

$$= d_0 + d_1 x + \ldots + d_{2n} x^{2n}, \text{ where}$$

$$d_i = \sum_{r=0}^{i} a_r b_{i-r}$$

Theorem 6 :

> Let R be a ring and let R [x] denote the set of polynomials in x with coefficients in R. Then R [x] is a ring under the operations of polynomial addition and polynomial multiplication. If R has unity so has R [x] and if R is commutative, then so is R [x].

Proof : The operations of polynomial addition and polynomial multiplication are binary operations in R [x], because the sum of two polynomials is again a polynomial and the product of two polynomials is again a polynomial. The operations are associative also.

Let $f = \left(a_0, a_1, \ldots\right)$; $g = \left(b_0, b_1, \ldots\right)$ and $h = \left(c_0, c_1, \ldots\right)$ be elements in R [x]. Then

$$f + (g + h) = (f + g) + h = \left(a_0 + b_0 + c_0, a_1 + b_1 + c_1, \ldots\ldots\right)$$

$$\text{and } f \cdot (g \cdot h) = (f \cdot g) \cdot h = \left(a_0 b_0 c_0, \sum_{i+j+k=n} a_i b_j c_k, \ldots\ldots\right)$$

The zero polynomial $0 = (0, 0, \ldots\ldots)$ is the additive identity.

If $f = \left(a_0, a_1, \ldots a_n\right) \in$ R [x], then $-f = \left(-a_0, -a_1, \ldots -a_n\right) \in$ R [x]

and $f + (f) = (-f) + f = 0$ polynomial. Thus $-f$ is the inverse of f. Further $f + g = g + f$.

Thus (R [x], +) is an abelian group and (R [x], ·) is a semi group. The distributive laws can similarly be verified. That is

$$f \cdot (g + h) = \left(a_0, a_1, \ldots\right) \cdot \left[\left(b_0, b_1, \ldots\right) + \left(c_0, c_1, \ldots\right)\right]$$

$$= \left(a_0, a_1, \ldots\right) \cdot \left(b_0 + c_0, b_1 + c_1, \ldots\ldots\right)$$

$$= \left(a_0 \left(b_0 + c_0\right), \sum_{i+j=n} a_i \left(b_j + c_j\right), \ldots\ldots\right)$$

$$= \left(a_0 b_0 + a_0 c_0, \ldots + \sum_{i+j=n} a_i b_j + \sum_{i+j=n} a_i c_j, \ldots\ldots\right)$$

$$= \left(a_0 b_0, \ldots, \sum_{i+j=n} a_i b_j, \ldots\right) + \left(a_0 c_0, \ldots, \sum_{i+j=n} a_i c_j, \ldots\right)$$

$$= fg + fh.$$

Similarly, $(g + h) \cdot f = g \cdot h + h \cdot f$

Thus (R [x], +, ·) is a ring. If R has unity 1, then for any $f \in$ R [x], and $f = \left(a_0, a_1, \ldots\right)$ then $1 \cdot f = (1, 0, \ldots\ldots) \cdot \left(a_0, a_1, \ldots\right) = \left(a_0, a_1, \ldots\right) = f \cdot 1$. If R is commutative $a_i b_j = b_j a_i$ $\forall a_i, b_j \in$ R so that

$$f \cdot g = (a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots)$$

$$= \left(a_0 b_0, \ldots \sum_{i+j=n} a_i b_j, \ldots\right) = \left(b_0 a_0, \ldots \sum_{j+i=n} b_j a_i, \ldots\right)$$

$$= g \cdot f$$

so that R [x] is commutative.

Definition 7 :

Let $f \in$ R [x] and let $f = (a_0, a_1, \ldots)$. If for some $i > 0$, $a_i \neq 0$, then the largest such value of i is called the degree of f. If no such $i > 0$ exists, then $f(x)$ is of degree zero. Equivalently if $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, and if $a_n \neq 0$ then n is called the degree of f and write it as deg (f). An element of R is called a constant polynomial. The degree of a constant polynomial is zero. A special mention has to be made about the zero polynomial $0 + 0 \cdot x + 0 \cdot x^2 + \ldots\ldots$

As a matter of convenience we assign a symbol '$-\infty$' to the degree of the zero polymial where the arithmatic of $-\infty$ is :

$-\infty + n = -\infty$; $(-\infty) + (-\infty) = -\infty$, $-\infty < n$ for every $n \in$ Z. Such a definition has become necessary because the zero polynomial shall have a degree less than any non zero polynomial.

Theorem 8 :

Let R be an integral domain. Then for $f, g \in$ R [x], deg (fg) = deg (f) + deg (g)

Proof : If f or g happens to be the zero polynomial then fg is also a zero polynomial so that by definition of the degree of a zero polynomial deg (fg) = $-\infty$ = deg (f) + deg (g) = $(-\infty) + (-\infty) = -\infty$.

If f and g are non zero polynomials, then let deg (f) = m and deg (g) = n so that

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m, a_m \neq 0$$

$$g(x) = b_0 + b_1 x + \ldots + b_n x^n, b_n \neq 0$$

$$\text{and } fg = c_0 + c_1 x + \ldots + c_{m+n} x^{m+n} \text{ where}$$

$$c_{m+n} = a_m b_n \neq 0 \left(\because a_m b_n \in \text{R, an integral domain}\right).$$

$$\text{Hence, deg } (f \cdot g) = m + n = \text{deg } (f) + \text{deg } (g).$$

8.5 WORKEDOUT EXERCISES

Exercise 1 : Let p be a prime number and $a \in$ Z be such that $(a, p) = 1$. Then p divides $\left(a^{p-1} - 1\right)$.

Ans : Since p is a prime number Z_p is a field. By definition of the field, the non zero elements of Z_p form an abelian group of order $(p - 1)$. Since $a \in Z_p - \{0\}$, $a^{p-1} = 1$, the multiplicative identity in Z_p. Since the operations are modulo addition and modulo multiplication in Z_p, this means that $a^{p-1} \equiv 1 \pmod{p}$. That is $\left(a^{p-1} - 1\right)$ is a multiple of p or p divides $\left(a^{p-1} - 1\right)$.

Remark : This result is known as Fermat's theorem and is a very important result in Number theory. There are other ways of proving this theorem without using the properties of finite fields.

Exercise 2 : Let $F = \{a, b, c, d\}$ in which "+" and "·" are defined by the tables below. Show that $(F, +, \cdot)$ is a field.

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

Ans : From the addition and multiplication we see that the operations '+' and '·' are binary operations so that the closure property is verified from the tables. Observe that 'a' is the additive identity and 'b' is the multiplicative identity. The additive inverses of b, c and d are b, c and d respectively. The operation + is commutative because $b + c = c + b = d$; $c + d = d + c = b$ and $b + d = d + b = c$ etc. The non 'zero' (additive identity) elements of F are b, c and d and $b \cdot b = 1$; $c \cdot d = d \cdot c = b$ so that the multiplicative inverses of b, c and d are b, d and c respectively. Further, $c \cdot d = d \cdot c = b$ etc. Thus $(F, +)$ is an abelian group and $(F', \cdot)$ is also an abelian group. The distributive laws hold good in F, since

$$a \cdot (b + c) = a \cdot d = a \text{ and}$$

$$a \cdot b + a \cdot c = a + a = a \text{ etc.}$$

Thus $(F, +, \cdot)$ is a field.

Exercise 3 : If $(R, +, \cdot)$ be an integral domain, show that R [x] is also an integral domain. Show further R [x] is not a field for any integral domain R.

Ans : Let the non zero polynomials f and $g \in R[x]$ and let deg $f = m$ and deg $g = n$ then,

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m \quad a_m \neq 0$$

$$g(x) = b_0 + b_1 x + \ldots + b_n x^n \quad b_n \neq 0$$

Now $f(x)\, g(x) = a_0 b_0 + \left(a_0 b_1 + b_0 a_1\right) x + \ldots\ldots + a_m b_n x^{m+n}$

Since R is an integral domain, and $a_m \neq 0, b_n \neq 0 \in R$ implies $a_m \cdot b_n \neq 0$.

Thus $f(x) \cdot g(x) \neq 0$

Thus R [x] is an integral domain. We also observe that the degree of $f \cdot g$ is $m + n$. That is deg $(f \cdot g)$ = deg f + deg g. Similarly

$$\deg (f + g) = \max (m, n).$$

If R [x] were to be a field, for $f \in R[x]$, whose degree > 0 there must be $g \in R[x]$ such that $f \cdot g = 1$, the unity polynomial of R [x]. This is not possible because the degree of unity polynomial is 0 (zero) and the degree of $f \cdot g$ = deg f + deg $g > 0$.

Thus R [x] is not a field.

8.6 SUMMARY

In this unit we investigated the multiplicative questions in commutative rings. The zero divisors are defined and a commutative ring with unity which does not admit zero divisors is defined to be an integral domain. If in an integral domain, the non zero elements form a group then it is called a field. Every field is an integral domain but only finite integral domains are fields. We have also given an example of a skew field. Polynomial rings which play a very important role in the study of rings have been specifically studied.

8.7 MODEL EXAMINATION QUESTIONS

SECTION - A (Long Answers)

(i) Define an integral domain and a field. Give examples. Show that a finite integral domain is a field. Hence show that Z_p is a field (p, a prime)

(ii) Show that the set of polymials R [x] with coefficient in a ring R is a ring under the operation of polynomial addition and polynomial multiplication. Show further that if R is an integral domain so is R [x].

SECTION - B (Short Answers)

(i) Show that every field is an integral domain but not conversely.

(ii) Define the characteristic of an integral domain and show that the characteristic of an integral domain is either zero or a prime number.

(iii) Show that $(Z_3, +, \cdot)$ is a field.

(iv) Show that a commutative ring admits cancellation laws if and only if it does not have zero divisors.

8.8 ANSWERS TO SELF ASSESSMENT QUESTIONS

SAQ 1 $Z_7 : 3.3 = 2 = 3.3$ Thus $x = 3$.

SAQ 2 In Z_{11} ; $3 \times 4 = 1$ hence 4 is inverse of 3

$7 \times 8 = 1$ hence 8 is inverse of 7.

SAQ 3 Z_p has already seen to be an integral domain whose characteristic is p. This is because $1 + 1 \ldots p$ times $= 0$ and $1 + 1 \ldots m$ times $\neq 0$ of $m < p$. Since a finite integral domain is a field Z_p is a field.

UNIT–9 : IDEALS AND QUOTIENT RINGS

Contents

9.1 Aims and Objectives

9.2 Introduction

9.3 Ideals

9.4 Quotient rings and homomorphism theorems

9.5 Workedout exercises

9.6 Summary

9.7 Sample Examination Questions

9.8 Answers to Self Assessment Questions

9.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to (i) define and give examples of ideals, (ii) prove theorems and results on the properties of ideals, (iii) state and prove homomorphism theorems for rings, (iv) Workout exercises on the properties of ideals and quotient rings.

9.2 INTRODUCTION

Pierre de Fermat (1601 - 1665) was an amateur French mathematician contributed extensively to different branches of mathematics. One of his theorems which claims that it is impossible to find non zero integers x, y and z such that $x^n + y^n = z^n$, ($n \geq 3$), has attained the status of legendary conjecture which has neither been proved or disproved even after three hundred and fifty years. In the course of investigations of this Fermat's conjecture, the German methematician Ernst Kummer (1810-1893) used the concept of an ideal in the ring of integers. An ideal is special case of a subring. An ideal is to a ring as a normal subgroup is to a group. Thus in the ring homomorphism the kernel of the homomorphism is an ideal. To day the study of ideals is central to research in ring theory. Special ideals like prime ideals maximal ideals and principal ideals play a very important role in the study of factorization in rings and integral domains.

9.3 IDEALS

Definition. 1 :

A subring I of a ring R is called a right ideal if $a \in I$ and $r \in R$ implies that $ar \in I$. Similarly a subring I of a ring R is called a left ideal if $a \in I$ and $r \in R$ implies that $ra \in I$. A subring is called an ideal (or a two sided ideal) if it is both a left ideal and a right ideal. If the ring R is commutative then every left ideal will be a right ideal and in this case we do not distinguish between a right ideal and a left ideal.

Remark. 1 : Observe that every ideal of a ring is a subring. But there may be subrings which are not ideals. For example Z, the ring of integers, is a subring of Q, the ring of rational numbers. But Z is not an ideal in Q because $1 \in Z$ and $\frac{1}{2} \in Q$ but $1 . \frac{1}{2} = \frac{1}{2} \notin Z$.

Example. 1 : In any ring R, the subring R and the subring {0} are ideals. These are called trivial ideals or improper ideals.

Example. 2 : In the ring of integers Z the subring of even integers 2Z is an ideal. Let $a \in Z$ and $2r \in 2Z$ then $a \,.\, (2r)$ and $(2r \,.\, a) \in 2Z$.

Example. 3 : Let $M_2 = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in Z\right\}$, be the set of 2×2 matrices over Z. Let $L_2 = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| a, b \in Z\right\}$. Then L_2 is a left ideal of M_2. To see this let $\begin{pmatrix} x & y \\ z & q \end{pmatrix} \in M_2$ and $\begin{pmatrix} \alpha & 0 \\ \beta & 0 \end{pmatrix} \in L_2$. Then $\begin{pmatrix} x & y \\ z & q \end{pmatrix}\begin{pmatrix} \alpha & 0 \\ \beta & 0 \end{pmatrix} = \begin{pmatrix} u & 0 \\ v & 0 \end{pmatrix} \in L_2$ where $u = x\alpha + y\beta$ and $v = z\alpha + q\beta$. Observe here that L_2 is not a right ideal. This is because

$$\begin{pmatrix} \alpha & 0 \\ \beta & 0 \end{pmatrix}\begin{pmatrix} x & y \\ z & q \end{pmatrix} = \begin{pmatrix} \alpha x & \alpha y \\ \beta x & \beta y \end{pmatrix} \notin L_2.$$

SAQ 1 Verify that L_2 is a subring.

SAQ 2 Verify that $R_2 = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in Z\right\}$ is a right ideal of M_2.

Example. 4 : $(Z_{12}, +, .)$ is a commutative ring under modulo addition and modulo multiplication Some ideals of Z_{12} are

$$\begin{aligned} Z_{12} &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} \\ I_1 &= \{0, 2, 4, 6, 8, 10\} \\ I_2 &= \{0, 3, 6, 9\} \\ I_3 &= \{0, 4, 8\} \\ I_4 &= \{0, 6\} \end{aligned}$$

Example. 5 : Let R be a ring and $a \in R$. The subset $I = \{r \in R \mid ar = 0\}$ is a right ideal of R. To see this let $x, y \in I$ then $ax = 0$ and $ay = 0 \Rightarrow a \,.\, (x - y) = 0$.Thus $x - y \in I$. Similarly $x \,.\, y \in I$. Thus I is a subring. Further for any $r \in R$, $a\,(xr) = (ax)\, r = 0 \Rightarrow xr \in I$. Thus I is a right ideal.

Theorem. 1 :

If I and J are ideals in a ring R, $I \cap J$ is also an ideal in R.

Proof : Since I and J are subrings of R, $I \cap J$ is a subring of R. Let $a \in I \cap J$. Then $a \in I$ and $a \in J$. But I and J being ideals $x\,a \in I$ and $x\,a \in J$ for $x \in R$. Thus $x\,a \in I \cap J$ and $I \cap J$ is an ideal in R.

Remark. 2 : The union of two ideals need not be an ideal. Let R = Z, the ring of integers. Then I = 2Z and J = 3Z are ideals in Z. Then $I \cup J$ is not an ideal because it is not even a sub ring. For example $2 \in I \cup J$, $3 \in I \cup J$ but $3 - 2 \notin I \cup J$.

Theorem. 2 :

A commutative ring R with unity is a field if and only if it has no proper ideals.

Proof : Let R be a field. Let $I \neq \{0\}$ be an ideal of R. Let $a \in I$. Then $a \in R$ and R being a field a^{-1} exists and is in R. By the definition of the ideal $a \,.\, a^{-1} = 1 \in I$. But $1 \in I$ implies that for any x, $x \,.\, 1 \in I$. Thus $R \subseteq I$. But I is an ideal of R and $I \subseteq R$ thus I = R. That is R has no proper ideals.

Conversely, suppose R has no proper ideals. That is if I is an ideal and $I \neq \{0\}$, then I = R. Let $a \in R$, $a \neq 0$. Consider the set $I = \{ax \mid x \in R\}$. Then I is an ideal of R and $I \neq \{0\}$. Then I = R. That is $1 \in R$, implies that there is $b \in R$ such that $a \cdot b = 1$, and b is the multiplicative inverse of a. Since every non zero element of R has an inverse, R is a field.

Definition. 2 :

> Let R be a commutative ring. An ideal $I \subset R$ is called a prime ideal if $ab \in I$ implies either $a \in I$ or $b \in I$ for all $a, b \in R$.

Example. 6 : In the ring Z, the ideal 3Z is a prime ideal because if $ab \in 3Z$, then $ab = 3n$ for some $n \in Z$. That is 3 divides a or 3 divides b. That is either $a \in 3Z$ or $b \in 3Z$.

Definition. 3 :

> Let R be a commutative ring with unity and let $a \in R$. The ideal $I = \{ra \mid r \in R\}$ of all multiples of a is the *principal ideal* generated by a. A commutative ring is called a principle ideal ring if every ideal in it is a principal ideal.

Example. 7 : In the ring Z, the ideal 3Z is a principal ideal generated by 3. In fact Z is a principal ideal ring.

Definition. 4 :

> An ideal M of a ring R is called a *maximal ideal* if $M \neq R$ and if for any ideal I such that $M \subseteq I \subseteq R$, either I = M or I = R.

Example. 8 : In the ring of even integers 2Z, the ideal generated by 4, that is the ideal 4Z is a maximal ideal. Observe that this ideal is not prime because $2.2 = 4 \in 4Z$, but $2 \notin 4Z$.

9.4 QUOTIENT RINGS AND HOMOMORPHISMS

Theorem. 3 :

> Let R be a ring and N be an ideal of R. Then R/N is a ring under the operations of addition and multiplication defined for $r + N, s + N \in R/N$ by $(r + N) + (s + N) = (r + s) + N$ and $(r + N) \cdot (s + N) = rs + N$ where $r, s \in R$.

Proof : (i) The addition and multiplication are well defined. Since R is an abelian group under addition and N is a subgroup, R/N is already defined to be the quotient group and the addition is well defined (Unit 4). To see that the multiplication is well defined we proceed as follows. Suppose that $r + N = r' + N$ and $s + N = s' + N$ for $r, r', s, s' \in R$. This means that $r - r' = r_1 \in N$ and $s - s' = s_1 \in N$ for some $r_1, s_1 \in N$. This implies that $r = r' + r_1$ and $s = s' + s_1$ so that $rs = r's' + r's_1 + r_1 s' + r_1 s_1$. Since N is an ideal and $r_1, s_1 \in N$, we have that $r's' + r's_1 + r_1 s' \in N$. This implies that $rs - r's' \in N$. This means that $rs + N = r's' + N$ and

$$(r + N)(s + N) = (r' + N)(s' + N).$$

This shows that the product is independent of the choice of coset representatives. Thus the operations of multiplication is well defined

(ii) The operation of multiplication is associative.

$$(r + N)\{(s + N) \cdot (t + N)\} = (r + N)(st + N) = r(st) + N$$
$$= (rs)t + N = (rs + N)(t + N)$$
$$= \{(r + N)(s + N)\}(t + N)$$

This is because $r, s, t \in R$ and R is associative.

(iii) Distributive laws are satsified.

$$(r + N) . [(s + N) + (t + N)] = (r + N) . (s + t + N)$$

$$= (r . (s + t) + N) = ((rs + rt) + N)$$

$$= (rs + N) . (rt + N)$$

$$= (r + N) . (s + N) + (r + N) . (t + N)$$

Similarly the other distributive law can be verified.

Thus (R/N, +) is an abelian group.

(R/N, .) is a semi group and (R/N, +, .) is distributive over '+'.

Then (R/N, +, .) is a ring.

Definition 5 :

> Let R be a ring and N be an ideal of R. Then under the operation of coset addition and coset multiplication R/N is a ring. This ring is called the *quotient ring* of R with respect to N.

Example. 9 : Let Z be the ring of integers and 3Z an ideal of Z. Then Z/3Z = {3Z, 3Z + 1, 3Z + 2} is a quotient ring of Z with respect to 3Z. The addition and multiplication tables are as follows :

+	3Z	3Z+1	3Z+2
3Z	3Z	3Z+1	3Z+2
3Z+1	3Z+1	3Z+2	3Z
3Z+2	3Z+2	3Z	3Z+1

•	3Z	3Z+1	3Z+2
3Z	3Z	3Z	3Z
3Z+1	3Z	3Z+1	3Z+2
3Z+2	3Z	3Z+2	3Z+1

Definition 6 :

> A mapping $f : R \to R'$ from a ring R to a ring R' is called a *ring homomorphism* if for all $a, b \in R$
>
> (i) $f(a + b) = f(a) + f(b)$
>
> (ii) $f(a . b) = f(a) . f(b)$.

A one-one homomorphism is called a monomorphism and onto homomorphism is called an epimorphism. A one-one onto homomorphism is called an isomorphism. The Kernal of a ring homomorphism is defined to be the set of elements in R that are mapped onto zero. That is Ker f : $\{r \in R \mid f(r) = 0\}$.

Example. 10 : Let R be a commutative ring and let R [x] denote the ring of polynomials with coefficients in R. For $a \in R$ and $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots$, let

$$f(a) = a_0 + a_1 a + a_2 a^2 + \ldots\ldots \text{ Define}$$

$f_a : R[x] \to R$ by $f_a(f(x)) = f(a)$, for $f \in R[x]$.

Then f_a is a ring homomorphism.

$$f_a(f + g) = f(a) + g(a) = f_a(f) + f_a(g)$$

$$f_a(f . g) = f_a \left\{ \left(a_0 + a_1 x + \ldots\right) \left(b_0 + b_1 x + \ldots\right) \right\}$$

$$= f_a\left(c_0 + c_1 x + \ldots\ldots\right) \text{ where } c_i = \sum_{r=0}^{i} a_r b_{i-r}$$

$$= c_0 + c_1 a + \ldots$$

$$= \left(a_0 + a_1 a + \ldots\right)\left(b_0 + b_1 a + \ldots\right)$$

$$= f_a(f) \cdot f_a(g).$$

Theorem. 4 :

> Let f be a ring homomorphism from a ring R to a ring R′. Let 0 and 0′ be the identities of R and R′ respectively. Then
>
> (i) $f(0) = 0'$; (ii) $f(-a) = -f(a)$,
>
> (iii) $f(a - b) = f(a) - f(b)$.

Proof : Though f is a ring homomorphism, restricted to '+' f is a group homomorphsim and we have already proved that $f(0) = 0'$ and $f\left(a^{-1}\right) = (f(a))^{-1}$. Here $a^{-1} = -a$.

$$f(a - b) = f(a + (-b)) = f(a) + f(-b) = f(a) - f(b) \text{ by (ii).}$$

Remark : If R has a unity then R′ need not have a unity and even if R′ has a unity, the image of 1 $\in$ R under f need not by $1' \in R'$.

Theorem. 5 :

> Let $f : R \to R'$ be a ring homomorphism. Then the ker f is an ideal of R.

Proof : Let $f : R \to R'$ be a ring homomorphism. Then $f(0) = 0'$ implies that ker $f \neq \phi$. Let $x, y \in$ Ker f. Then $f(x) = 0$ and $f(y) = 0$ implies that $f(x - y) = f(x) - f(y) = 0$. Thus $x - y \in$ Ker f and $f(x \cdot r) = f(x) \cdot f(r) = 0$ and $f(r \cdot x) = f(r) \cdot f(x) = 0$, for $x \in$ Ker f and $r \in$ R implies that xr and $rx \in$ Ker f. Thus Ker f is an ideal of R.

Theorem. 6 : Fundamental theorem of ring homomorphism :

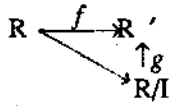
> Let I be an ideal of a ring R. Then R/I is a homomorphic image of R. Conversely, if f is a homomorphism of a ring R onto a ring R′ then R′ is isomorphic to R/Ker f.

Proof : Define a mapping $f : R \to R/I$ by $f(x) = x + I$. Then f is well defined and is independent of the choice of the representative. To see that f is a homomorphism,

$$f(x + y) = (x + y) + I = (x + I) + (y + I) = f(x) + f(y) \text{ and}$$

$$f(xy) = xy + I = (x + I)(y + I) = f(x) f(y).$$

Conversely, Let $f : R \to R'$ be a ring homomorphism. Let I = Ker f. Then I is an ideal of R. Define $g : R/I \to R'$ by $g(x + I) = f(x)$. Then g is well defined.



(i) g is one-one. For, let $x + I = y + I$. This implies that $x - y \in I =$ Ker f, so that $f(x - y) = 0$ and $f(x) = f(y)$. That is $g(x + I) = g(y + I)$.

(ii) g is onto. For, let $y \in R'$. Since f is onto, there is an element $x \in R$ such that $f(x) = y$. Now $x + I \in R/I$ and $g(x + I) = f(x) = y$.

(iii) g is a **homomorphism :**

$$g\{(x+I)+(y+I)\} = g\{(x+y+I)\} = f(x+y)$$
$$= f(x)+f(y) = g(x+I)+g(y+I)$$
$$g\{(x+I).(y+I)\} = g(xy+I) = f(xy) = f(x)f(y)$$
$$= g(x+I)\,g(y+I)$$

Then g is a homomorphism and hence is isomorphim.

9.5 WORKEDOUT EXERCISES

Exercise. 1 : For any two ideals I and J of a ring R, the set $I + J = \{a + b \mid a \in I, b \in J\}$ is an ideal of R containing both I and J.

Ans : Since I and J are ideals, they are subrings. Then $0 \in I$ and $0 \in J$ so that $0 \in I + J$ and $I + J \neq \phi$. Let x and $y \in I + J$. Then $x = a_1 + b_1$ and $y = a_2 + b_2$ where $a_1, a_2 \in I, b_1, b_2 \in J$. Then

$$x - y = (a_1 + b_1) - (a_2 + b_2)$$
$$= (a_1 - a_2) + (b_1 - b_2); \text{ (by using properties of ring).}$$

Thus $x - y \in I + J$. Further if $r \in R$, $xr = a_1 r + b_1 r$ is an element of I + J. Similarly, $rx = ra_1 + rb_1$ is an element of I + J, because I and J are ideals. Thus I + J is an ideal.

For each $a \in I$, $a = a + 0$ where $0 \in J$ and thus $a \in I + J$. Thus $I \subseteq I + J$. Similarly $J \subseteq I + J$.

Exercise. 2 : Show that an ideal M of a commutative ring R with unity is a maximal ideal if and only if R/M is a field.

Ans : Since R is a commutative ring with unity, R/M is also a commutative ring with unity. We are required to prove that if M is maximal, then every non zero element of R/M has a multiplicative inverse in R/M. Let $a + M \neq 0 + M \in R/M$. Then $a \notin M$. Consider the set $aR = \{ar \mid r \in R\}$. Then a R is an ideal of R. Further $a = a \cdot 1 \in R$.

Since $a \in M + a$ R and $a \notin M$, we have that $M \subset M + a$R. But M is maximal. Then $M + a$ R = R. Since $1 \in R$, there exists $m \in M$ and $r \in R$ such that $m + ar = 1$. This implies that $1 + M = ar + m + M = ar + M$. This implies that $(a + M) . (r + M) = (1 + M)$ or $(r + M)$ is inverse of $(a + M)$ in R/M. Thus R/M is a field.

Conversely suppose R/M is a field. To prove that M is a maximal ideal of R we have to show that if there is an ideal N of R such that $M \subseteq N \subseteq R$, then N = R. If possible let N be an ideal of R and let $M \subset N$. Then there exists $a \in N$, $a \notin M$, such that $a + M \neq M$. But R/M is a field. That is, there is $(b + M) \in R/M$ such that $(a + M)(b + M) = 1 + M$. This implies that

$$ab + M = 1 + M \text{ or } 1 - ab \in M \subset N \text{ and } a . b \in N$$

This means that $1 \in N$ and consequently N = R. Thus M is maximal.

Exercise. 3 : An ideal P of a commutative ring R is a prime ideal if and only if R/P is an integral domain.

Ans : Suppose that R/P is an integral domain. By the definition of integral domain, R/P does not admit zero divisors, that is $a + P, b + P \in R/P$ and $(a + P)(b + P) = P \Rightarrow a \in P$ or $b \in P$. Observe here that P is the additive identity (zero)of R/P and $(a + P)(b + P) = ab + P$ and $ab + P = P$ implies that $ab \in P$. Since $ab \in P \Rightarrow a \in P$ or $b \in P \Rightarrow P$ is a prime ideal by definition.

Conversely, suppose that P is a prime ideal. This means $ab \in P \Rightarrow a \in P$ or $b \in P$. But $ab \in P$ means $ab + P = P$ or $(a + P)(b + P) = P$, P being a prime ideal either $a + P = P$ or $b + P = P$. Then R/P has no zero divisors.

Exercise. 4 : Every maximal ideal of a commutative ring is a prime ideal.

Ans : Let M be a maximal ideal of a ring R. Then R/M is a field. But every field is an integral domain. Therefore R/M is also an integral domain. This implies that M is a prime ideal. Thus every maximal ideal is prime.

Exercise. 5 : Let R be a ring and let $a \in R$. Let M_2 be the ring of 2×2 matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$. Define a mapping $f : M_2 \to R$ by $f(A) = a$ for all $A \in M_2$. Show that f is an isomorphism.

Ans : To verify that f is a homomorphism. We need to check that

$$f(A + B) = f(A) + f(B) \text{ and}$$
$$f(A \cdot B) = f(A) \cdot f(B) \text{ for all } A, B \in M_2.$$

Let $A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$ for $a, b \in R$.

Then $A + B = \begin{pmatrix} a+b & 0 \\ 0 & 0 \end{pmatrix}$ and $AB = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$. Now

$$f(A + B) = a + b = f(A) + f(B)$$
$$f(A \cdot B) = a \cdot b = f(A) \cdot f(B)$$

Thus f is a homomorphism.

To see that f is one-one mapping let $A \neq B$ [illegible] be given by $A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$

Then $f(A) = a; f(B) = b$ and $f(A) \neq f(B)$.

To see that f is onto, let $a \in R$, then $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in M_2$ such that $f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a$. Then f is onto and hence is a bijective homomorphism and hence an isomorphism.

9.6 SUMMARY

In this unit we have defined an ideal of a ring. A field does not admit any non trivial ideals. We have defined a ring homomorphism and proved that the Kernel of a ring homorphism is an ideal. We have defined the quotient rings and proved the fundamental theorem of ring homomorphism which is analogous to fundamental theorem of homomorphism of groups. We have defined some special ideals which play an important role in tackling questions about uinique factorisation. Maximal ideals, prime ideals, principal ideals are defined and some consequences studied. For example every Maximal ideal of a commutative ring is a prime ideal.

9.7 MODEL EXAMINATION QUESTIONS

Section A (Long Answer)

i) Define a maximal ideal. Let R be a ring and M an ideal of R. Show that M is maximal if and only if R/M is a field.

ii) State and prove fundamental homomorphism theorem for rings.

iii) Let R be a commutative ring with unity. Show that R is a field if and only if R has no non trival ideals.

Section B (Short Answer)

i) Define an ideal and show that the intersection of two ideals of a ring is again an ideal. What can be said about the union of two ideals?

ii) Define a ring homomorphism and Kernel of a ring homomorphism. Show that the Kernel of a ring homomorphism is an ideal.

iii) Explain in detail the construction of a quotient ring.

9.8 ANSWERS TO SAQ'S

SAQ 1 We have to verify that $A \cdot B \in L_2$ and $A - B \in L_2$ for $A, B \in L_2$

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} ac & 0 \\ bc & 0 \end{pmatrix} \in L_2 \;\&\; \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} - \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} a-c & 0 \\ b-d & 0 \end{pmatrix} \in L_2$$

Thus L_2 is a subring.

SAQ 2 $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ z & q \end{pmatrix} = \begin{pmatrix} ax+bz & ay+bz \\ 0 & 0 \end{pmatrix} \in K_2$ and R_2 is a right ideal.

UNIT–10: VECTOR SPACES

Contents

10.1 Aims and Objectives

10.2 Introduction

10.3 Vector spaces and Subspaces

10.4 Basis and dimension

10.5 Workedout exercises

10.6 Summary

10.7 Model Examination Questions

10.8 Answers to Self Assessment Questions

10.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to : (i) Define a vector space and give examples of vector spaces and vector subspaces, (ii) Given a set of vectors verify whether they are linear dependent or independent, (iii) Define dimension and basis of a vector space (iv) Prove theorems that relate the dimension of a vector space and its subspaces.

10.2 INTRODUCTION

In Block 1 we have introduced algebraic systems that admit one binary operation. In the previous units of this block we introduced algebraic systems which admit two binary operations. In this unit we introduce an algebraic system called vector space which is a combination of two distinct algebraic systems, an abelian group and a Field. The concept of a vector space is motivated by the consideration of vectors in physics. It was William Rowan Hamilton (1805 - 1865) who introduced an ordered pair to represent a complex number, without using the symbol 'i' . He extended this notion to ordered 4 - tuples by inventing the quaternions $\{\pm 1, \pm i, \pm j, \pm k\}$ which do not statisfy the commutative property. Himilton's invention paved way for Gibbs and Heaviside to introduce a vector to represent quatities which have both magnitude and direction. From the point of view of a phisicist a vector (for example force) has a magnitude and a direction in which it is applied. The vector from the point of view of a mathematician is an ordered pair or ordered triple of real numbers. A quantity which is not a vector is called a scalar. If v is a vector and α is a scalar, then αv is a vector whose magnitude is α times the magnitude of v, and the times direction of αv is same (parallel to) as that of v. From the point of view of a mathematician an algebriac system consisting of ordered pairs or ordered triples of reals, following point wise addition forms an abelian group. There is a field whose elements are called scalars. If (a, b) is vector and α is a scalar then there is an operation of scalar multiplication between α and (a, b) making $(\alpha a, \alpha b)$ a vector. These two operations of vector addition and scalar multiplication combines the two algebriac systems into a vector space over the field.

10.3 VECTOR SPACES AND SUB SPACES

Definition 1 :

Let F be a field. A vector space over F is a non empty set V together with a binary operation '+' defined on V such that (V, +) is an abelian group and an operation of scalar multiplication of each element of V by each element of F such that for $a, b \in F$ and $u, v, \in V$, the following conditions are satisfied.

(i) $av \in V$

(ii) $a(bv) = (ab)v$

(iii) $a \cdot (u + v) = a \cdot u + a \cdot v$

(iv) $(a + b) \cdot u = au + bu$

(v) $1 \cdot v = v$; where 1 is the multiplicative identity of F.

Equivalently, a non empty set V is called a vector space over a field F if we can define a binary operation called vector additon '+' fromV x V $\rightarrow$ V and a binary operation called a scalar multiplication '.' from F x V $\rightarrow$ V such that the following conditions are statisfied.

(i) (V, +) is an abelian group.

(ii) For all $a \in F$, $u, v \in V$, $a \cdot (u + v) = a \cdot u + a \cdot v$

(iii) For all $a, b \in F$ and $u \in V$, $(a + b) \cdot u = a \cdot u + b \cdot u$

(iv) For all $a, b \in F$ and $u \in V$; $a \cdot (b \cdot u) = (a \cdot b) \cdot u$

(v) For all $u \in V$ and $1 \in F$, $1 \cdot u = u$.

Remark 1 : Whenever we talk of a vector space we always mean a vector space over a field. However, when there is no ambiguity we need not over emphasize the underlying filed.

Example 1 : Let F be any field. Let V be the set of n - tuples

$$V = \left\{ \left(x_1, x_2, \ldots, x_n \right) \middle| \, x_i \in F \right\}. \text{ Define '+' on V by}$$

$$\left(x_1, x_2, \ldots x_n \right) + \left(y_1, y_2, \ldots y_n \right) = \left(x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n \right).$$

For $a \in F$ and $u = \left(x_1, x_2, \ldots x_n \right) \in V$, define the scalar multiplication. '.' by

$$a \cdot u = a\left(x_1, x_2, \ldots x_n \right) = \left(a x_1, a x_2, \ldots a x_n \right). \text{ Then V is a vector space.}$$

To see that (V, +) an abelian group we observe that (i) $0 = (0, 0, \ldots 0)$, n - tuple of zeros is the additive identity : $\left(x_1, x_2, \ldots x_n \right) + (0, 0, \ldots 0) = \left(x_1, x_2, \ldots x_n \right)$.

(ii) For each $u \in V$, $-u \in V$ is the additive inverse of u.

$$u = \left(x_1, x_2, \ldots x_n \right); \; -u = \left(-x_1, -x_2, \ldots -x_n \right)$$

and $u + (-u) = (-u) + u = (0, 0, \ldots 0) = \mathbf{0}$

(iii) $(x_1, x_2, \ldots x_n) + (y_1, y_2, \ldots y_n) = (y_1, y_2, \ldots y_n) + (x_1, x_2, \ldots x_n)$

follows from commutativity of addition of real numbers.

Thus (V, +) is an abelian group. Let $u = (x_1, x_2, \ldots x_n)$; $v = (y_1, y_2, \ldots y_n) \in V$.

(iv) For $a, b \in F$ and $u \in V$, $(a + b)\, u = au + bu$ because

$$(a+b)(x_1, x_2, \ldots x_n) = ((a+b)x_1, (a+b)x_2, \ldots, (a+b)x_n)$$

$$= (a x_1 + b x_1, a x_2 + b x_2, \ldots, a x_n + b x_n)$$

$$= (a x_1, a x_2, \ldots a x_n) + (b x_1, b x_2, \ldots b x_n)$$

$$= a(x_1, x_2, \ldots x_n) + b(x_1, x_2, \ldots x_n)$$

$$= au + bu$$

(v) For $a \in F$ and $u, v \in V$; $a(u + v) = au + av$.

$$a\{(x_1, x_2, \ldots x_n) + (y_1, y_2, \ldots y_n)\} = a(x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

$$= (a(x_1 + y_1), a(x_2 + y_2), \ldots a(x_n + y_n))$$

$$= (a x_1 + a y_1, a x_2 + a y_2, \ldots a x_n + a y_n)$$

$$= a(x_1, x_2, \ldots x_n) + a(y_1, y_2, \ldots y_n)$$

$$= au + av.$$

(vi) For $a, b \in F$ and $u \in V$

$$(a \cdot b) \cdot u = a \cdot (b \cdot u) \text{ because}$$

$$ab(x_1, x_2, \ldots x_n) = a(b x_1, \ldots b x_n) = a(bu)$$

$1 \cdot u = u$ is clear from the scalar multiplication. Then V is a vector space over F.

Example 2 : Let F be a field. Let V be the set of all $m \times n$ matrices over F. Let '+' be matrix addition and '·' denote the scalar multiplication. Then V is a vector space over F. All the properties can be verified using the properties of matrix addition.

Example 3 : Let V denote the set of vectors in a plane and R denote the field of real numbers. Recall that the sum of two vectors $\bar{a}$ and $\bar{b}$ is the resultant $\bar{a} + \bar{b}$ and if α is a scalar then $\alpha \bar{a}$ is a vector. Then the set of vectors in a plane is a vector space under the operations of vector addition and scalar multiplication.

Example 4 : Let F be a field and let F [x] denote the ring of polynomials with coefficients in F. Recall that if f and $g \in F[x]$ be given by

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \equiv (a_0, a_1, \ldots a_n)$$

$$g(x) = b_0 + b_1 x + \ldots + b_m x^m \equiv (b_0, b_1, \ldots b_m)$$

$$\text{then } f(x) + g(x) = \left(a_0 + b_0\right) + \left(a_1 + b_1\right)x + \ldots + \left(a_m + b_m\right)x^m + \ldots + a_n x^n$$

$$= \left(a_0 + b_0, a_1 + b_1, \ldots, a_m + b_m, \ldots a_n\right)$$

$$\text{and for } \alpha \in F;\ \alpha f(x) = \alpha a_0 + \alpha a_1 x + \alpha a_2 x^2 + \ldots + \alpha a_n x^n.$$

Then F [x] is a vector space of polynomial functions.

SAQ 1 Show that the set of complex numbers form a vector space over the field of reals.

Theorem 1 :

> Let V be a vector space over the field F. Then for $x, y \in V$ and $\alpha \in F$,
>
> (i) $0x = 0$; (ii) $\alpha \cdot 0 = 0$. (iii) $-(\alpha x) = (-\alpha)x = \alpha(-x)$ (iv) $\alpha(x - y) = \alpha x - \alpha y$
>
> (v) $\alpha x = 0$ and $\alpha \neq 0 \Rightarrow x = 0$ (vi) $\alpha x = \alpha y$ and $\alpha \neq 0 \Rightarrow x = y$.

proof :

(i) Consider $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$

Since (V, +) is an abelian group in which cancellation laws hold good. Thus

$0 \cdot x = 0 \cdot x + 0 \cdot x \Rightarrow 0 \cdot x = 0$.

(ii) $\alpha \cdot 0 = \alpha(0 + 0) = \alpha \cdot 0 + \alpha \cdot 0 \Rightarrow \alpha \cdot 0 = 0$

(iii) $0 = 0 \cdot x = (\alpha + (-\alpha))x = \alpha x + (-\alpha)x$. Thus

$\alpha x + (-\alpha x) = 0$ implies that $(-\alpha x)$ is the additive inverse of $(-\alpha x)$ i.e. $(-\alpha x) = -\alpha x$

Similarly $\alpha(-x) + \alpha(x) = \alpha(-x + x) = \alpha \cdot 0 = 0$ and αx is the additive inverse of $\alpha(-x)$

i.e. $\alpha(-x) = -\alpha x$.

(iv) $\alpha(x - y) = \alpha[x + (-y)] = \alpha x + \alpha(-y) = \alpha x - \alpha y$

(v) Since $\alpha \neq 0$ and $\alpha \in F$, a field, α^{-1} exists. Then $\alpha^{-1}(\alpha_n) = \alpha^{-1} \cdot 0$. That is $\left(\alpha^{-1} \cdot \alpha\right)x = 0$ or $x = 0$.

(vi) Since $\alpha \neq 0$ and $\alpha \in F$, α^{-1} exists. Thus

$$\alpha x = \alpha y \Rightarrow \alpha^{-1}(\alpha x) = \alpha^{-1}(\alpha y) = (\alpha^{-1}\alpha)x = (\alpha^{-1}\alpha)y$$

$$\Rightarrow x = y$$

Remark 2 : F being a field F has the additive identity which we donate by 0 (zero). (V, +) being an abelian group V also has the additive identity which is the zero vector (null vector) which we should distinguish from the scalar zero. Similarly for $a, b \in F$, the scalars, $a \cdot b \in F$. But for $a \in F$, a scalar and $u \in V$, a vector $au \in V$.

Definition 2 :

> Let V be a vector space over the field F. Let W be a non empty subset of V. Then W is a subspace of V over F if W is a vector space over F in its own right. Equivalently a nonempty subset of V, a vector space over F, is a vector subspace over F, if (i) (W, +) is a subgroup of (V, +) and (ii) W is closed under the operation of scalar multiplication.

Example 5 : Let V be a vector space over a field F. Since $V \subseteq V$, V is a vector subspace of V over F. Similarly $\{0\}$, the vector space consisting of the zero vector alone is a vector subspace of V. These are called trivial subspaces.

Example 6 : Let $V = \left\{ (a_1, a_2, a_3) \mid a_1, a_2, a_3 \in F, \text{ a field} \right\}$. Then V is a vector space under the operation "+" and '·' defined on $(a_1, a_2, a_3), (b_1, b_2, b_3) \in V$ by

$$(a_1, a_2, a_3) + (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3) \text{ and}$$

$$\alpha \cdot (a_1, a_2, a_3) = (\alpha a_1, \alpha a_2, \alpha a_3) \text{ for } \alpha \in F.$$

Let $W = \left\{ (a_1, a_2, a_3) \mid (a_1, a_2, a_3) \in V \text{ and } a_1 + a_2 + a_3 = 0 \right\}$.

Then W is a vector subspace over F. To see this let (a_1, a_2, a_3) and $(b_1, b_2, b_3) \in W$. Then $(a_1, a_2, a_3) + (b_1, b_2, b_3) \in W$. Because

$$(a_1, a_2, a_3) + (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3)$$

Now $(a_1 + b_1) + (a_2 + b_2) + (a_3 + b_3) = (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3)$

$$= 0 + 0 = 0$$

Hence W is closed under addition.

Let $\alpha \in F$. Then $\alpha (a_1, a_2, a_3) = (\alpha a_1, \alpha a_2, \alpha a_3)$

But $\alpha a_1 + \alpha a_2 + \alpha a_3 = \alpha (a_1 + a_2 + a_3) = \alpha \cdot 0 = 0$.

Thus $\alpha (a_1, a_2, a_3) \in W$.

Since W is closed under the operations of vector addition and scalar multiplication. That (W, +) is a subgroup of (V, +). Also, it is clear from the fact that for $W_1 = (a_1, a_2, a_3)$ and $W_2 = (b_1, b_2, b_3)$, $W_1 \cdot W_2^{-1} = W_1 - W_2$ (because the operation is addition in V) again $\in W$. Thus W is a sub space of V.

SAQ 2 Let C denote the vector space of complex numbers of the form $a + ib$ over the field of real numbers R. Let $W \subset C$ be given by $W = \{ib \mid b \in R\}$, the sub set of pure imaginary numbers. Verify that W is a subspace of C.

Theorem 2 :

> Let V be a vector space over a field F. Let W be a non empty subset of V. Then W is a vector subspace of V if and only if $(\alpha u + \beta v) \in W$ for $u, v \in W$ and $\alpha, \beta \in F$.

Proof : Let W be a vector subspace of V. Let $u, v \in W$ and $\alpha, \beta \in F$. Then W is a vector space over F in its own right and hence satisfies all the conditions of the vector space. That is (W, +) is an abelian group and W is closed under the operation of scalar multiplication. Then $\alpha u \in W$ and $\beta v \in W$ and $\alpha u + \beta v \in W$.

Conversely, suppose that W is a nonempty subset of V such that for $u, v \in W$ and $\alpha, \beta \in F$, $\alpha u + \beta v \in W$. Then taking $\alpha = 1, \beta = 1$, we get that $u + v \in W$ and $\alpha = 1, \beta = 0$ gives $\alpha u \in W$. That is W is closed under vector addition and scalar multiplication. Thus W is a sub space of V.

Theorem 3 :

The intersection of two vector subspaces of a vector space is again a vector subspace.

Proof : Let V be a vector space over a field F and let W_1 and W_2 be subspaces of V over F. Then $(W_1, +)$ and $(W_2, +)$ are abelian subgroups of (V, +). That is the **0**, (The zero vector), the additive identiry of V, is in W_1 and also in W_2. Hence $W_1 \cap W_2 \neq \phi$. Let $u, v \in W_1 \cap W_2$ and $\alpha, \beta \in F$. Then $\alpha u + \beta v \in W_1$, because W_1 is a subspace and $\alpha u + \beta v \in W_2$, because W_2 is a subspace. Thus $u, v \in W_1 \cap W_2$ and $\alpha, \beta \in F \Rightarrow \alpha u + \beta v \in W_1 \cap W_2$. Hence $W_1 \cap W_2$ is a sub space of V.

Remark 2 : The union of two subspaces of a vector space need not be a subspace.

Example 7 : Let $V = M_2$, the set of 2 x 2 matrices over a field F. Let $W_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| \begin{matrix} a \neq 0 \text{ and} \\ a \in F \end{matrix} \right\}$ and $W_2 = \left\{ \begin{pmatrix} 0 & b \\ b & 0 \end{pmatrix} \middle| \begin{matrix} b \neq 0 \text{ and} \\ b \in F \end{matrix} \right\}$. Then $W_1 \cap W_2 = \{0\}$ the subspace consisting of the zero vector alone. But $W_1 \cup W_2 =$ is not a subspace because $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in W_1, \begin{pmatrix} 0 & b \\ b & 0 \end{pmatrix} \in W_2$ but $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & b \\ b & 0 \end{pmatrix} \notin W_1 \cup W_2$.

Theorem 4 :

Let V be a vector space over a field F and W_1 and W_2 be subspaces of V. Then $W_1 + W_2 = \{ u + v \mid u \in W_1, v \in W_2 \}$ is also a subspace of V.

Proof : Since **0** (the zero vector) $\in W_1$ and W_2, we have that $\mathbf{0} \in W_1 + W_2$. Thus $W_1 + W_2 \neq \phi$.

Let $x, y \in (W_1 + W_2)$ and $\alpha, \beta \in F$.

Then $\left.\begin{matrix} x = w_1 + w_2 \\ y = w_1' + w_2' \end{matrix}\right\}$ where $w_1, w_1' \in W_1$ and $w_2, w_2' \in W_2$.

Now $\alpha x + \beta y = \alpha (w_1 + w_2) + \beta (w_1' + w_2')$

$= (\alpha w_1 + \beta w_1') + (\alpha w_2 + \beta w_2')$

$\in W_1 + W_2$, because W_1 and W_2 are subspaces.

Theorem 5 :

Let V be a vector space over a field F and let W_1 and W_2 be subspaces of V. Then $W_1 + W_2$ is the smallest subspace containing both W_1 and W_2.

Proof : Recall from theorem 4 of this unit that $W_1 + W_2 = \{ w_1 + w_2 \mid w_1 \in W_1 \text{ and } w_2 \in W_2 \}$ is a subspace of V. For any $w_1 \in W_1, w_2 \in W_2$ and **0** (zero vector) $\in W_2, w_1 + 0 = w_1 \in W_1 + W_2$. Thus $W_1 \subseteq W_1 + W_2$.

$0 + w_2 = w_2 \in W_1 + W_2$. Thus $W_2 \subseteq W_1 + W_2$.

Hence $W_1 \cup W_2 \subseteq W_1 + W_2$. Let W be any subspace of V containing $W_1 \cup W_2$. Then for any $w_1 \in W_1$ and $w_2 \in W_2$, $w_1 \in W_1 \cup W_2$ and $w_2 \in W_1 \cup W_2$. This implies that $w_1 + w_2 \in W$, for $w_1, w_2 \in W$. But this implies that $W \subset W_1 \cup W_2$. Thus $W_1 + W_2$ is same as the space generated by $W_1 \cup W_2$.

Theorem 6 :

Let V be a vector space over a field F and W_1 and W_2 be subspaces of V. Then $W_1 \cap W_2 = \{0\}$, if and only if every vector of $W_1 \cup W_2$ is uniquely represented as $u + v$ for $u \in W_1$ and $v \in W_2$.

Proof : Suppose that $W_1 \cap W_2 = \{0\}$. Let $w \in W_1 \cup W_2$ be represented as $w = u_1 + v_1$ and $w = u_2 + v_2$ for $u_1, u_2 \in W_1$ and $v_1, v_2 \in W_2$. Since W_1 and W_2 are subspaces, $u_1 - u_2 \in W_1$ and $v_1 - v_2 \in W_2$. But $w = u_1 + v_1 = u_2 + v_2$ implies that $u_1 - u_2 = v_2 - v_1 = 0$ or $u_1 = u_2$ & $v_1 = v_2$. Conversely suppose $w \in W_1 \cup W_2$ is uniquely represented in the form $u + v$, $u \in W_1$ & $v \in W_2$. If possible let $w \in W_1 \cap W_2$. Then

$w = w + 0$, with $w \in W_1$ and $0 \in W_2$ and

$w = 0 + w$ with $0 \in W_1$ and $w \in W_2$. But

the uniqueness of representation of w gives $w = 0$ or $W_1 \cap W_2 = \{0\}$.

Definition 3 :

Let V be a vector space and W_1 and W_2 be subspaces of V such that $W_1 \cap W_2 = \phi$ and $W_1 + W_2 = V$. Then the sum $W_1 + W_2$ is called a direct sum and is represented by $W_1 \oplus W_2$. The two subspaces are called complementary.

10.4 BASIS AND DIMENSION

Definiton 4 :

Let V be a vector space over a field F. For a finite set of vectors $u_1, u_2, \ldots u_n$ in V and scalars $\alpha_1, \alpha_2, \ldots \alpha_n$ in F, the vector $\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_n u_n$ is called a *linear combination* of $u_1, u_2, \ldots u_n$.

Definition 5 :

Let V be a vector space over a field F. A finite set of vectors $v_1, v_2, \ldots v_n$ in V is said to be *linearly independent* if for all $\alpha_i \in F$, $(i = 1, 2, \ldots n)$, $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = 0$ implies $\alpha_1 = \alpha_2 = \ldots \alpha_n = 0$. The set of vectors $v_1, v_2, \ldots v_n$ is linearly dependent if for some $\alpha_1, \alpha_2, \ldots \alpha_n \in F$, with atleast one of them non zero, $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = 0$.

Remark 3 : The singleton set $\{x\}$, $x \neq 0$ is linearly independent since for any $\alpha \in F$, $\alpha x = 0$, $x \neq 0 \Rightarrow \alpha = 0$. The empty set is taken as a linearly independent set. The set consisting of zero vector alone is linearly dependent because for any $\alpha \in F$, $\alpha \neq 0$, $\alpha \cdot 0 = 0$.

SAQ 3 Show that $\{0, v_1, \ldots, v_n\}$ is linearly dependent.

Example 8 : Let V be a vector space over the field of rationals check whether the set of vectors $\{(1, 1, 1), (1, 0, 1), (0, 1, 0)\}$ is linearly dependent or independent. Let $v_1 = (1, 1, 1)$, $v_2 = (1, 0, 1)$, $v_3 = (0, 1, 0)$. Let $\alpha_1, \alpha_2, \alpha_3$ be scalars $\in$ Q, the field of rationals such that $\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = 0$, the zero vector.

i.e. $\alpha_1 (1, 1, 1) + \alpha_2 (1, 0, 1) + \alpha_3 (0, 1, 0) = (0, 0, 0)$

i.e. $(\alpha_1 + \alpha_2, \alpha_1 + \alpha_3, \alpha_1 + \alpha_2) = (0, 0, 0)$

i.e., $\alpha_1 + \alpha_2 = 0, \alpha_1 + \alpha_3 = 0 \Rightarrow \alpha_2 = \alpha_3 ; \alpha_2 = -\alpha_1$

Let $\alpha_1 = 1$, so that $\alpha_2 = 1, \alpha_3 = -1$.

Since the α_i's are not zero the set is linearly dependent.

Example 9 : The set of vectors $\{(1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1)\}$ are linearly independent. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be scalars such that

$\alpha_1 (1, 0, 0, 0) + \alpha_2 (0, 1, 0, 0) + \alpha_3 (0, 0, 1, 0) + \alpha_4 (0, 0, 0, 1) = (0, 0, 0, 0)$

i.e. $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (0, 0, 0, 0) \Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = 0.$

Since $\sum_{i=1}^{4} \alpha_i v_i = 0 \Rightarrow \alpha_i = 0$, the vectors are linearly independent.

SAQ 4 If v_1, v_2 and v_3 are linearly independent vectors, then show that $v_1 + v_2$, $v_1 + v_3$, $v_2 + v_3$ are also linearly independent.

Definition 6 :

Let X be a subset of a vector space V. A sub space W of V is said to be spanned by X, if every element of W can be expressed as a linear conbination of elements of X. Equivalently, W is spanned by X, if W is generated by X. That is $X \subseteq W$ and for any subspace W' of V, $X \subseteq W' \Rightarrow W \subseteq W'$.

Definition 7 :

Let V be a vector space over a field F. A subset B of V is called a basis of V if

(i) B is linearly independent set

(ii) B spans V.

Definition 8 :

A vector space V is said to be finitely generated if it has a finite subset which spans V.

Definition 9 :

The number of elements in a vector space is called the dimension of the vector space. If the basis has n elements then n is the dimension. If the basis does not have a finite dimension, then it is called inifinite dimensional vector space.

Theorem 7 :

Let V be a vector space and let $\{u_1, u_2, \ldots u_n\}$ be a set of n vectors in V. If $\beta \in$ V is a linear combination of these n vectors, then the set $\{\beta, u_1, u_2, \ldots u_n\}$ is linearly dependent. Conversely, if $\{\beta, u_1, \ldots u_n\}$ is linearly dependent then β can be expressed as a linear conbination of $\{u_1, \ldots u_n\}$.

Proof : Since β is a linear combination of $u_1, u_2, \ldots u_n$, we can write $\beta = \alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_n u_n$, $\alpha_i \in F$

i.e. $\beta + (-\alpha_1)u_1 + (-\alpha_2) u_2 + \ldots + (-\alpha_n)u_n = 0$ and atleast one of the coefficients (coefficient of β is 1) is not zero. This means that $\{\beta, u_1, \ldots u_n\}$ is linearly dependent.

Conversely, suppose $\{\beta, u_1, \ldots u_n\}$ is linearly dependent. Then there exist scalars $\alpha_0, \alpha_1, \ldots \alpha_n$, not all of them zero such that

$\alpha_0 \beta + \alpha_1 u_1 + \ldots + \alpha_n u_n = 0, \alpha_i \in F.$

Then $\alpha_0 \beta = \left(-\alpha_1 u_1 - \alpha_2 u_2 - \ldots - \alpha_n u_n\right)$

Two cases need be considered $\alpha_0 \neq 0$ and $\alpha_0 = 0$. If $\alpha_0 \neq 0$; α_0^{-1} exists and hence

$$\beta = \left(\alpha_0^{-1} \alpha_1\right)u_1 + \left(-\alpha_0^{-1} \alpha_2\right)u_2 + \ldots + \left(-\alpha_0^{-1} \alpha_n\right)u_n.$$

and β is a linear combination of $u_1, u_2, \ldots u_n$.

If $\alpha_0 = 0$, then each of $\alpha_1, \alpha_2, \ldots \alpha_n$ is zero contradicting the fact that $u_1, u_2, \ldots u_n$ are linearly dependent.

Theorem 8 :

> Let V be a vector space spanned by a set consisting of m vectors. If S is a set of n linearly independent vectors in V, then $n \leq m$. Hence any two bases of a finitely generated vector space have the same number of vectors.

Proof : Let the m vectors $\{v_1, v_2, \ldots v_m\}$ span V. Let S = $\{u_1, u_2, \ldots u_n\}$ be a set of independent vectors in V. Since $u_1 \in V$ and $\{v_1, v_2, \ldots v_m\}$ spans V, u_1 can be written as a linear combination of $v_1, v_2, \ldots v_m$. That is

$$u_1 = \alpha_1 v_1 + \alpha_2 v_2 + \ldots \alpha_m v_m.$$

This equation can be solved for some v_i say v_k, so that v_k is a linear combination of u_1 and v_i's other than v_k. Then the set $\{u_1, v_1, \ldots v_{k-1}, v_{k+1}, \ldots v_m\}$ span V. Now $u_2 \in V$ and hence u_2 can be expressed as a linear combination of vectors from $\{u_1, v_1, \ldots v_{k-1}, v_{k+1}, \ldots v_m\}$. Again this equation can be solved for v_i say v_j. Then v_j is a linear combination of :

$u_1, u_2, v_1 \ldots v_{k-1}, v_{k+1}, v_{j-1}, v_{j+1}, \ldots v_m$. This process could be continued till all the n vectors $u_1, u_2, \ldots u_n$ are exhausted. Since at each stage one vector v_i is replaced by one vector u_j, the number of v_i s must be atleast as many as u_i' s. Thus $n \leq m$.

If possible let B be a finite basis of V containing n vectors and B′ be another finite basis of V containing m vectors. Since B spans V and B′ is a linearly independent set, $m \leq n$. Again B′ spans V and B is a linearly independent set $n \leq m$. Thus $m = n$.

Theorem 9 :

> Let V be a vector space of dimension n over a field F. Let S be a sub set of V consisting of n linearly independent vectors. Then S is a basis of V.

Proof : Let S = $\{v_1, v_2, \ldots v_n\}$. Let $x \in V$ and $x \notin S$ then the set $\{u_1, u_2, \ldots u_n, x\}$ is linearly dependent. Hence there exist scalars $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta$ not all zero such that

$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n + \beta x = 0.$

If $\beta = 0$; $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = 0$, giving $\alpha_1 = \alpha_2 = \ldots \alpha_n = 0$. This is not possible because not all $\alpha_1, \alpha_2, \ldots \alpha_n, b$ are zero. Thus $\beta \neq 0$. Hence

$$x = \left(-\beta^{-1} \alpha_1\right)v_1 + \left(-\beta^{-1} \alpha_2\right)v_2 + \ldots + \left(-\beta^{-1} \alpha_n\right)v_n.$$

That is S is a linearly independent set of vectors that spans V. Thus S is a basis of V.

Theorem 10 :

> Any linearly independent subset of a finite dimensional vector space can be extended to a basis.

Proof : Let dim V = n, so that the basis of V has n vectors. Let S be a set of linearly independent vectors :

$S = \{u_1, u_2, \ldots u_m\}$ where $m \leq n$. Let W be the set of linear combinations of vectors from S. If W = V, then S is the basis of V. If W ≠ V, then there exists $u_{m+1} \in$ V and $u_{m+1} \notin$ W. Let α_1, $\alpha_2, \ldots \alpha_{m+1}$ be a set of scalars such that

$$\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_{m+1} u_{m+1} = 0.$$

If $\alpha_{m+1} \neq 0$, then $u_{m+1} = \left(-\alpha_{m+1}^{-1} \alpha_1\right)u_1 + \ldots + \left(-\alpha_{m+1}^{-1} \alpha_m\right)x_m$. This implies that $u_{m+1} \in$ W which is a contradiction. Thus $\alpha_{m+1} = 0$.

This means that $\alpha_1 u_1 + \ldots + \alpha_{m+1} u_{m+1} = 0$

$\Rightarrow \alpha_1 = \alpha_2 = \ldots = \alpha_{m+1} = 0$. Thus the set $\{u_1, u_2, \ldots u_{m+1}\}$ is linearly independent.

Now let W′ be the subspace generated by $\{u_1, u_2, \ldots u_{m+1}\}$. If W′ = V, then $\{u_1, \ldots u_{m+1}\}$ will be a basis of V containing S or S has been extended to a basis. If W′ ≠ V then there exists u_{m+2} ∈ V – W. By repeating the same process as above we can show that

$\{u_1, u_2, \ldots u_{m+1}, u_{m+2}\}$ is a linearly independent set continuing this process $(n - m)$ times we get

$$\{u_1, u_2, \ldots, u_n\}$$

is a linearly independent set consisting of n elements. Then $\{u_1, \ldots u_n\}$ is a basis of V.

Theorem 11 :

> Let V be a finite dimensional vector space and W, a sub space of V. Then W is finite dimensional and dim W ≤ dim V.

Proof : Let dim V = n. Then there is a linearly independent set of vectors $\{u_1, u_2, \ldots u_n\}$ which spans V and this set is a basis of V. Since W is a subspace of V, W must also have a basis. That is there must exist a linearly independent set of vectors.

$$\{y_1, y_2, \ldots, y_m\}$$

which span W. That is dim W = m.

Now the set of m linearly independent vectors $\{y_1, y_2, \ldots y_m\}$ can be extended to be the set of linearly independent vectors $\{y_1, \ldots y_m, y_{m+1}, \ldots y_n\}$ such that this set spans V. This shows that the basis of W is a subset of the basis of V.

Thus $m \leq n$.

10.5 WORKEDOUT EXERCISES

Exercise. 1 : Let V be a vector space over a field F and let S be a non empty subset of V. Let L (S) denote the set of all linear combinations of elements of S. Show that L (S) is a sub space of V.

Ans : If $S = \phi$, then L (S) = {0} and hence is a sub space of V. If $S \neq \phi$, let $u \in S$. Now $u = 1.u$ is a linear combination and hence $u \in L(S)$ and $L(S) \neq \phi$. Then for $x, y \in L(S)$ and α and $\beta \in F$, there exist $x_1, x_2, \ldots x_n, y_1, y_2, \ldots y_m \in S$ and $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m \in F$ such that

$$x = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n ;$$

$$y = b_1 y_1 + b_2 y_2 + \ldots + b_m y_m .$$

Then $$ax + by = a\left(a_1 x_1 + \ldots + a_n x_n\right) + b\left(b_1 y_1 + \ldots + b_m y_m\right)$$

$$= a\,a_1 x_1 + \ldots + a\,a_n x_n + b\,b_1 y_1 + \ldots + b\,b_m y_m$$

Since $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m \in S$ and $a\,a_1, \ldots a\,a_n, b\,b_1, b\,b_2, \ldots b\,b_m \in F$, $ax + by \in L(S)$. Thus L (S) is a subspace of V.

Exercise. 2 : Let V be a vector space and S be a finite set of linearly independent vectors. Show that every subset of S is also linearly independent.

Ans : Let $S = \{u_1, u_2, \ldots, u_n\}$ and let $T = \{u_1, \ldots, u_m\}$ where $m < n$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a set of scalars such that $\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_m u_m = 0$. This implies $\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_m u_m + 0.u_{m+1} + \ldots 0\,u_n = 0$.

Thus for scalars $\alpha_1, \alpha_2, \ldots, \alpha_m, 0$ we have that

$\alpha_1 u_1 + \ldots + \alpha_m u_m + 0.u_{m+1} + \ldots 0\,u_n = 0$ and S is a linearly independent set. This implies

$\alpha_1 = \alpha_2 \ldots = \alpha_m = 0$.

So T is a linearly independent set.

Exercise 3 : Let V be a vector space of finite dimension. Let W_1 and W_2 be subspaces of V. Then

$$\dim\left(W_1 + W_2\right) = \dim W_1 + \dim W_2 - \dim\left(W_1 \cap W_2\right).$$

Ans : Let $\{w_1, w_2, \ldots, w_k\}$ be a basis of $W_1 \cap W_2$. Since $W_1 \cap W_2 \subset W_1$ and $W_1 \cap W_2 \subset W_2$, the basis of $W_1 \cap W_2$ can be extended to a basis of W_1 and to a basis of W_2. Thus let

$\{w_1, w_2, \ldots w_k, u_1, \ldots, u_r\}$ be a basis of W_1 and $\{w_1, w_2, \ldots, w_k, v_1, v_2, \ldots v_s\}$ be a basis of W_2. Let W be a sub space generated by $\{u_1, u_2, \ldots, u_r\}$. Then $W \cap W_2 = \{0\}$, because if $w \in W \cap W_2 \subseteq W_1 \cap W_2$, then

$$w = \alpha_1 w_1 + \ldots + \alpha_k w_k, \text{ for scalars } \alpha_1, \alpha_2, \ldots \alpha_k .$$

But $w \in W$ and hence

$$w = \beta_1 w_1 + \ldots + \beta_r u_r \text{ for scalars } \beta_1, \beta_2, \ldots \beta_r$$

Thus $$0 = w - w = \alpha_1 w_1 + \ldots + \alpha_k w_k + \left(-\beta_1\right) u_1 + \ldots + \left(-\beta_r\right) u_r$$

Since $\{w_1, w_2, \ldots w_k, u_1, \ldots, u_r\}$ is a basis of W_1 these are linearly independent we conclude

$\alpha_1 = \alpha_2 \ldots = \alpha_k = b_1 = \ldots = b_r = 0.$

That is $w = 0$ and $W \cap W_2 = \{0\}$

Consider $\alpha_1 w_1 + \ldots + \alpha_k w_k + \beta_1 u_1 + \ldots + \beta_r u_r + \gamma_1 v_1 + \ldots + \gamma_s v_s = 0.$

Let $w = \beta_1 u_1 + \ldots + \beta_r u_r = -\left(\alpha_1 w_1 + \ldots + \alpha_k w_k + \gamma_1 v_1 + \ldots + \gamma_s v_s\right)$

Then $w \in W \cap W_2$ and hence $w = 0$.

That is $\beta_1 u_1 + \ldots + \beta_r u_r = 0$ and

$\alpha_1 w_1 + \ldots + \alpha_k w_k + \gamma_1 v_1 + \ldots + \gamma_s v_s = 0$

By linear independece of $\{u_1, \ldots u_r\}$ and $\{w_1, \ldots w_k, v_1, v_2, \ldots v_s\}$

$\alpha_1 = \ldots = \alpha_k = \beta_1 = \ldots = \beta_r = \gamma_1 \ldots \gamma_s = 0.$

Thus $\{w_1, w_2, \ldots w_k, u_1, u_2, \ldots u_r, v_1, v_2, \ldots v_s\}$ is a linearly independent set and this set spans $W_1 + W_2$.

Hence it is a basis of $W_1 + W_2$. This means that

$\dim\left(W_1 + W_2\right) = k + r + s = (k + r) + (k + s) - k = \dim W_1 + \dim W_2 - \dim\left(W_1 \cap W_2\right)$.

Exercise. 4 : Show that $\{(1, i, 0), (2i, 1, 1), (0, 1 + i, 1 - i)\}$ is a linearly independent set of vectors in a vector space of dimension 3 over the field of complex numbers.

Ans : Let $x_1 + i y_1, x_2 + i y_2, x_3 + i y_3$ be scalars belonging to the underlying field of complex numbers such that

$$\left(x_1 + i y_1\right)(1, i, 0) + \left(x_2 + i y_2\right)(2i, 1, 1) + \left(x_3 + i y_3\right)(0, 1 + i, 1 - i) = (0, 0, 0)$$

this implies that

$$\left(x_1 + i y_1\right) 1 + \left(x_2 + i y_2\right) 2i + \left(x_3 + i y_3\right) . 0 = 0$$

$$\left(x_1 + i y_1\right) .i + \left(x_2 + i y_2\right) .1 + \left(x_3 + i y_3\right)(1 + i) = 0$$

$$\left(x_1 + i y_1\right) .0 + \left(x_2 + i y_2\right) .1 + \left(x_3 + i y_3\right)(1 - i) = 0$$

That is $x_1 + i y_1 + 2x_2 i - 2y_2 = 0 \Rightarrow$ $\begin{cases} x_1 - 2y_2 = 0 \text{ and} \\ y_1 + 2x_2 = 0 \text{ (by equating real and imaginary parts} \end{cases}$

separately to zero),

$i x_1 - y_1 + x_2 + i y_2 + x_3 + i y_3 + i x_3 - y_3 = 0 \Rightarrow - y_1 + x_2 + x_3 - y_3 = 0$ and $x_1 + y_2 + x_3 + y_3 = 0$ (by equating real and imaginary parts separately to zero)

$- x_2 + i y_2 + x_3 + i y_3 - i x_3 + y_3 = 0 \Rightarrow$

$x_2 + x_3 + y_3 = 0$ and $y_2 + y_3 - x_3 = 0$

This gives $x_1 = x_2 = x_3 = y_1 = y_2 = y_3 = 0$

Thus the given set is linearly independent.

10.6 SUMMARY

In this unit we have seen an algebraic structure which has wide applications in physics and other branches of mathematics. In fact the discovery of vector space has been necessitated from questions arising out of physical world that do not admit commutative properties. A vector space is an amalgamation of two different algebraic structures – an abelian group and a field. A set of vectors that generate a vector space (in the sense every vector in the space can be written as a linear combination of vectors from this set) is called a basis of the vector space. A vector space can have different bases, but the number of elements in each basis is the same. This number is called the dimension of the vector space.

10.7 MODEL EXAMINATION QUESTIONS

Section - A (Long Answer)

i) Show that the set $\{(1, i, 0), (2i, 1, 1), (0, 1 + i, 1 - i)\}$ is a basis of a vector space over the field of complex numbers. Express the vectors $\{(1, 0, 0), (0, 1, 0)$ and $(0, 0, 1)\}$ in terms of the basis vectors.

ii) Show that any two bases of a finite dimensional vector space have the same number of elements.

iii) Let V be a vector space of finite dimensions and W_1 and W_2 be sub spaces of V. Show that

$$\dim\left(W_1 + W_2\right) = \dim W_1 + \dim W_2 - \dim\left(W_1 \cap W_2\right).$$

Section - B (Short Answer)

i) Define a vector space and give an example. Show that a non empty sub set W of a vector space V over a field F is a subspace if and only if $\alpha x + \beta y \in w$ for $x, y \in W$ and $\alpha, \beta \in F$.

ii) Define the basis of a vector space. Show that $\{(1, 2, 1), (2, 1, 0), (1, -1, 2)\}$ is a basis of a three dimensional vector space.

iii) Show that the sum of two vector subspaces of a vector space is a vector subspace.

10.8 ANSWERS TO SAQ'S

SAQ 1 If we denote the complex numbers by C, then (C, +) is an abelian group.

$a + R, X, Y \in C \Rightarrow a \,.\, (X + Y) = a \,.\, X + a \,.\, Y, a, b \in R, X \in C \Rightarrow ab\,(X) = a\,(b\,X)$ and $1 \in R \Rightarrow 1 \,.\, X = X \,. \Rightarrow C$ is a vector space over R.

SAQ 2 Follow the same lines as in SAQ 1.

BLOCK–3 : REAL NUMBER SYSTEM

Unit–11 : Algebraic properties of real numbers

Unit–12 : Completeness properties of Real numbers

Unit–13 : Open sets and closed sets in R

By 19th century it had become evident that rational numbers alone are not sufficient in answering many questions in Mathematics. A rational number is a ratio of two relatively prime integers. By associating rational numbers with the points on a line it was noticed that there are certain gaps which can not be filled with rational numbers alone. It was known to ancient Greeks that the diagonal of a unit square is not a rational number. Though several attempts have been made to "complete" the set of rational numbers by several mathematicians only two procedures have stood the test of time. One of them was due to Dedikind (1831-1916) using the method of "cuts" and the other was due to Cantor (1845-1918) using the method of "Cauchy sequences". For a beginner both the methods appear to be too technical and abstract. This is the reason why many authors introduce the existence of a real number axiomatically rather than go through a lengthy process of evolving integers (Z) from natural numbers (N), rationals (Q) from integers and finally the reals (**R**).

UNIT–11 : ALGEBRAIC PROPERTIES OF REAL NUMBERS

Contents

11.1 Aims and Objectives

11.2 Introduction

11.3 Real numbers as an ordered field

11.4 Natural numbers and Principle of Induction

11.5 Countable and uncountable sets

11.6 Summary

11.7 Model Examination Questions

11.8 Answers to Self Assessment Questions

11.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to : (i) Define an ordered field and prove certain properties of real numbers using the axioms, (ii) Define countable and uncountable sets and prove that the set of rationals is countable where as the set of reals is not countable.

11.2 INTRODUCTION

Towards the end of 18th century and the beginning of 19th century mathematicians were very busy in developing applications of differential and integral calculus to mechanics, astronomy and technology. However there was no uniformity of approach to the basic understanding of the concepts involved. The rigorous definition of a function or the properties of continuous functions or the relation between continuous and differentiable functions have not been fully investigated. The emphasis was more on intuition than on abstraction. It was realised that real numbers played an important role in the investegation of these basic concepts in calculus. But what is a real number? Though intuitively the concept seems to be agreeable, their acceptability was not universal. That there exist certain numbers like $\sqrt{2}$, the length of a diagional of a unit square, which can not be represented as a ratio of two integers is known from the times of Greeks. But their formalisation posed several constraints. Even today the introduction of a real number for the first time to a student seems to be laborious and often lacks the simplicity and straight forwardness. That is why the student must show more patience and perserverance in reading this unit and the next.

11.3 REAL NUMBERS AS AN ORDERED FIELD

In the set of **R** of real numbers there are two binary operations '+' and '.' called addition and multiplication satsifying the following properties.

A1 : $a + b = b + a$ for all $a, b \in \mathbf{R}$

A2 : $(a + b) + c = a + (b + c)$ for all a, b, c in **R**

A3 : There exists an element '0' in **R** such that

$$a + 0 = 0 + a = a \text{ for all } a \text{ in } \mathbf{R}$$

A4 : For each a in $\mathbf{R}$, there exists $-a$ in $\mathbf{R}$ such that

$a + (-a) = (-a) + a = 0$.

M1 : $a \cdot b = b \cdot a$ for all a, b in $\mathbf{R}$

M2 : $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, c in $\mathbf{R}$

M3 : There exists $1 \in \mathbf{R}$ such that $a \cdot 1 = 1 \cdot a = a$ for all a in $\mathbf{R}$

M4 : For each $a \neq 0$ in $\mathbf{R}$, there exists a^{-1} in $\mathbf{R}$ such that $a \cdot a^{-1} = 1$

D1 : $a \cdot (b + c) = a \cdot b + a \cdot c$ for all a, b, c in $\mathbf{R}$.

All these properties are familiar to us when we defined a field in unit 8. Let us recall that these conditions give rise to some consequences which we have already seen in earlier units. These are listed below. The student shall verify each of the results using the axioms stated above. Let $a, b, c \in \mathbf{R}$.

SAQ 1 (i) $a + b = a + c \Rightarrow b = c$.

SAQ 2 (ii) $a + a = a \Rightarrow a = 0$.

SAQ 3 (iii) $a + b = 0 \Rightarrow b = -a$.

SAQ 4 (iv) $-(a - b) = (b - a)$.

(v) $a \cdot b = 1 \Rightarrow a = b^{-1}, (b \neq 0)$

(vi) $a \neq 0 \Rightarrow a^{-1} \neq 0$ and $\left(a^{-1}\right)^{-1} = a$.

(vii) $ab = a \Rightarrow b = 1$

(viii) $(-1) \cdot a = -a$

(xi) $(-a) \cdot b = a \cdot (-b) = -ab$

(x) $(-a) \cdot (-b) = ab$

(xi) The equation $a + x = b$ has a unique solution in x for every $a, b \in \mathbf{R}$

(xii) The eqution $ax = b$, $a \neq 0$ has a unique solution in x for every $a, b \in \mathbf{R}$.

(xiii) $a \cdot b \neq 0$ if and only if $a \neq 0$ and $b \neq 0$.

In addition to the field axioms the real numbers have an order relation. The axioms of order is related to the abstract property of positiveness. We do not intend to define positiveness but accept it as an undefined term.

Definition. 1 :

> There is a non empty subset P of $\mathbf{R}$ called the set of strictly positive real numbers satsifying
>
> (i) If $a, b \in$ P then $a + b \in$ P.
>
> (ii) If $a, b \in$ P then $a \cdot b \in$ P
>
> (iii) If $a \in \mathbf{R}$, then exactly one of the following relations holds :
>
> $a \in$ P, $a = 0$, $-a \in$ P.

The property (iii) is called the law of Trichotomy. It implies that the set $N = \{-a \mid a \in P\}$ is called strictly negative real numbers and $N \cap P = \phi$. Further $\mathbf{R} = N \cup \{0\} \cup P$.

Notation : If $a \in$ P we write $a > 0$. If $a \in P \cup \{0\}$ we write $a \geq 0$. If $-a \in$ P, we write $a < 0$ and if $-a \in P \cup \{0\}$, we write $a \leq 0$. If $a, b \in \mathbf{R}$ and if $a - b \in$ P, we write $a > b$. If $-(a - b) \in$ P, then we write $a < b$. If $a - b \in P \cup \{0\}$, we write $a \geq b$ and if $-(a - b) \in P \cup \{0\}$ we write $a \leq b$.

Theorem. 1 :

Let $a, b, c \in \mathbf{R}$ then

(i) If $a > b$ and $b > c \Rightarrow a > c$.

(ii) exactly one of these holds : $a > b, a = b, a < b$

(iii) If $a \geq b$ and $b \geq a$, then $a = b$.

Proof : (i) By definition 1, $a - b \in P$ and $b - c \in P$ implies $(a - b) + (b - c) \in P$. i.e., $a - c \in P$. That is $a > c$.

(ii) By Trichotomy property of order exactly one of the following holds : $a - b \in P$; $a - b = 0$; $b - a = -(a - b) \in P$. That is $a > b$; $a = b$ or $a < b$.

(iii) If $a \neq b$ then $a - b \in P$ or $-(a - b) \in P$. Hence either $a > b$ or $b > a$.

SAQ 5 If $a \neq 0$ and $a \in R$, then $a^2 > 0$.

SAQ 6 If $x > 0$, $y > 0$, then $x < y$ if and only if $x^2 < y^2$.

Definition :

Let $a \in \mathbf{R}$, the absolute value of a, denoted by $|a|$ is defined by :

$$|a| = a \text{ if } a \geq 0$$
$$= -a \text{ if } a < 0$$

Theorem. 2 :

(i) $|a| = 0$ if and only if $a = 0$.

(ii) $|-a| = a$ for all $a \in \mathbf{R}$.

(iii) $|ab| = |a||b|$ for all $a, b \in \mathbf{R}$.

(iv) If $c \geq 0$ then $|a| \leq c$ if and only if $-c \leq a \leq c$.

(v) $-|a| \leq a \leq |a|$ for all $a \in \mathbf{R}$.

Proof : (i) If $a = 0$, then $|0| = 0$. If $a \neq 0$ then $-a \neq 0$ so that $|a| \neq 0$.

(ii) If $a = 0$; $|a| = |0| = 0 = |-a| = |-0|$. If $a > 0$ then $|a| = a = |-a|$. If $a < 0$, $|a| = -a = |-a|$.

(iii) If $a > 0$ and $b > 0$, then $ab > 0$ so that $|ab| = ab = |a||b|$. If $a < 0$ and $b > 0$, then $ab < 0$ and $|ab| = -(ab) = (-a)b = |a||b|$.

(iv) If $|a| \leq c$, then $a \leq c$ and $-a \leq c$. Thus $-c \leq a$ and $-c \leq a \leq c$. Conversely if $-c \leq a \leq c$ then $a \leq c$ and $-a \leq c$ so that $|a| \leq c$.

(v) follows from (iv) where $c = |a| \geq 0$.

Theorem. 3 : (Triangle inequality) :

If $a, b \in \mathbf{R}$ then $||a| - |b|| \leq |a \pm b| \leq |a| + |b|$

Proof : Since $-|a| \leq a \leq |a|$ and $-|b| \leq \pm b \leq |b|$ we have that

$$-(|a| + |b|) = -|a| - |b| \leq a \pm b \leq |a| + |b|$$

Thus $|a \pm b| \leq |a| + |b|$.

Now $|a| = |(a - b) + b| \leq |a - b| + |b|$. This means

$|a| - |b| \leq |a - b|$. Similarly $|b| - |a| \leq |b - a| = |a - b|$.

Thus $||a| - |b|| \leq |a - b|$. Similarly the other inequality can be proved.

11.4 NATURAL NUMBERS AND THE PRINCIPLE OF INDUCTION

Definition :

Let **R** be the set of real numbers. A subset A of **R** is called an inductive set if $1 \in A$ and whenever $n \in A$, $n + 1$ also is in A.

Theorem. 4 :

If S is a nonempty collection of inductive sets, then $B = \cap \{A \mid A \in S\}$ is an inductive set.

Proor : Since $1 \in A$ and $A \in S$, it follows that $1 \in B$. If $x \in B$ then $x \in A$ for every $A \in S$. This implies that $x + 1 \in A$ for every $A \in S$. That is $(x + 1) \in B$. Thus B is an inductive set.

Remark. 1 : The set $N = \cap \{A \mid A \in I$, the collection of inductive sets$\}$ is called the set of natural numbers. We take that N is the smallest inductive set.

Theorem. 5 : (The principle of induction) :

Let N be the set of natural numbers. For each $n \in N$, let $P(n)$ be a statement about the natural number n. If (i) $P(1)$ is true and (ii) $P(n)$ is true $\Rightarrow P(n + 1)$ is true, then $P(n)$ is true for every $n \in N$.

Proof : Let n be a natural number > 1, so that $(n - 1)$ is a natural number. If possible let $S = \{n \mid P(n)$ is not true$\}$. We would prove that $S = \phi$. If $S \neq \phi$, then since the set of natural numbers has a minimum element m (say). Since $P(1)$ is true $1 \notin S$. Hence $m \neq 1$. This means that $(m - 1)$ is a natural number. But m is a minimum of $S \Rightarrow (m - 1) \notin S$. This means that $P(m - 1)$ is true. But $P(m - 1)$ is true $\Rightarrow P(m)$ is true. This means $m \notin S$ contradicting the assumption that $m \in S$. Thus the assumption $S \neq \phi$ is wrong. This means $S = \phi$.

Theorem. 6 :

Let N be the set of natural numbers. Then

(i) $p \in N \Rightarrow p \geq 1$

(ii) $n \in N$ and $n \neq 1 \Rightarrow n - 1 \in N$

(iii) $p, q \in N$ and $q < p \Rightarrow p - q \in N$.

(iv) $n \in N$ and $n < x < (n + 1) \Rightarrow x \notin N$.

Proof : (i) It is enough if we show that the set $A = \{n \mid n \in N, n \geq 1\}$ is an inductive set. Since $1 \in N$ and $1 \geq 1$, $1 \in A$. If $n \in A \Rightarrow n \in N$ and $n \geq 1$. This implies that $(n + 1) \in N$, $n + 1 > n \geq 1$. ($\because$ N is an inductive set). This means that $n + 1 \in N$, $n + 1 \geq 1$. That is $(n + 1) \in A$.

(ii) Suppose $(n - 1) \notin N$ for some $n \in N$, $n \neq 1$. Let $A = N - \{n\}$. Since $n \neq 1$; $1 \in A$.

Further $p \in A \Rightarrow p \in N$, $p \neq n$. This implies that $p + 1 \in N$, $p + 1 \neq n$.

For if $p + 1 = n$, then $n - 1 = p \in N$ contradicting $n - 1 \notin N$. Thus $(p + 1) \in A$. But if an inductive set $A \subset N$ then $A = N$. Thus $A = N - \{n\} = N$, implying that $n \notin N$. This contradicts the hypothesis that $n \in N$. Therefore $(n - 1) \in N$ when $n \in N$ and $n \neq 1$.

(iii) Let $A = \{n \in N / m \in N, m > n \Rightarrow m - n \in N\}$.

Then by (ii) $1 \in A$. If $n \in A$, then

$m \in N, m > n + 1 \Rightarrow m \in N, m \neq 1$

$\Rightarrow (m - 1) \in N$.

$n \in A, m \in N, m > n+1 \Rightarrow m-1 \in N, m-1 > n.$

$\Rightarrow (m-1)-n \in N.$

$\Rightarrow m-(n+1) \in N$

$\Rightarrow (n+1) \in A.$

Thus A = N.

(iv) If possible let $x \in N$. Then $x - n \in N$. This implies that $x - n \geq 1$, or $x \geq (n+1)$. This contradicts the hypothesis that $x < n+1$.

Definition. 4 :

Let A be a non-empty subset of real numbers. A real number a is said to be a least element of A if $a \leq x$ for every $x \in A$.

Theorem. 7 : Well ordering principle :

Every non empty subset of N has a least element.

Proof : Let $A \subset N$ and $A \neq \phi$. Let us suppose that A has no least element. Define a set $B = \{n \in N \mid m \in N, m \leq n \Rightarrow m \notin A\}$. Now $1 \in B$, for if $1 \notin B$, then $1 \in A$ and 1 would be least element of A contradicting the supposition that A has no least element. Let $n \in B$. Then $m \in N, m \leq n \Rightarrow m \notin A$. We claim that $n+1 \in B$. For, if $n+1 \notin B$, then there exists a number m such that $m \in N, m \geq (n+1)$ and $m \in A$. It now follows that $m = n+1$ and $(n+1) \in A$, because if $m < n+1$, then $m \leq n$ and $m \notin A$, a contradiction.

Since by our suppositions that A has no least number, there exists a number $p \in A$ such that $p < n+1$. If $n < p < n+1$, then $p \notin N$. Hence $p \leq n$. But $p \in N, p \leq n \Rightarrow p \notin A$. This contradicts the fact that $p \in A$. Therefore $n \in B \Rightarrow n+1 \in B$ and B = N. Then from the definitions of B, $m \notin A$ implying that $A = \phi$. Thus the assumption that A has no least number is wrong. Thus A has a least element.

Definition. 5 :

The set $R = \{x \mid x \in \mathbb{R}, x = 0 \text{ or } x \in N \text{ or } -x \in N\}$ is called the set of integers Z.

If $x \in N$, x is a positive integer and if $-x \in N$, x is called a negative integer. The number 0 is considered to be a non negative integer (not positive integer). The set of non negative integers is $N \cup \{0\}$.

Definition. 6 :

The set $Q = \left\{ mn^{-1} = \frac{m}{n} \mid m \in Z, n \in N \right\}$ is called the set of rational numbers. Equivalently $Q = \{x \mid x \in \mathbb{R}$ and there exists $n \in N$ such that $nx \in Z\}$.

Theorem. 8 : (Archimedian property)

If $x, y \in Q$ and $x > 0$, then there is $n \in N$ such that $nx > y$.

Proof : If $x > y$, then $n = 1$. If $x = y$ then $n = 2$. Let $0 < x < y$. By taking $x = \frac{p}{q}$ and $y = \frac{r}{s}$ where $p, q, r, s \in N$, and $n = rq + 1$, we get $nps \geq n > rq$ and $\frac{nps}{qs} > \frac{rq}{qs}$ or, $\frac{np}{q} > \frac{r}{s}$ implying $nx > y$.

11.5 COUNTABLE AND UNCOUNTABLE SETS

Definition 7 :

Let A and B be two non empty sets. If there exists a bijection from A to B, then A and B are called *similar sets*. Similarity of sets is an equivalence relation on the set of sets. A set A is said to be *finite* if it is similar to $\{1, 2, \ldots n\}$ for some fixed $n \in N$. A is said to be a *countable* set if (i) A is empty set or (ii) A is a finite set or (iii) A is similar to N, the set of natural numbers. Equivalently an infinite set is said to be countable if there is a bijection of the set onto N. A countable set is called a denumerable set or an enumerable set by some authors.

Example 1 : N is a countable set because $f : N \to N$ by $f(n) = n$ is a bijective (identity) mapping.

Example 2 : Let 2N denote the set of positive even integers. Then the sets N and 2N are (similar) equivalent because the mapping $f : N \to 2N$ defined by $f(n) = 2n$ is one - one and onto. Thus the set of even integers is countable. Observe here that the set of even integers is a proper subset of the set of integers. But there are "as many" even integers as there are integers. Some authors characterise a set to be an inifite set if and only if it can be placed in one - one correspondence with a proper subset of itself.

Example 3 : Define $f : N \to Z$ by, $f(n) = 2n - 1$. Then the set of odd positive integers is similar to N.

SAQ 7 Let $A = \{x \in R \mid -1 < x < 1\}$. Define $f : R \to A$ by $f(x) = \frac{x}{1 + |x|}$. Show that R is similar (equivalent) to A.

Theorem 9 :

Any subset of N is countable.

Proof : Let $A \subset N$. If A is empty or finite then A is countable. So let A be an infinite subset of N. Since A is not empty and $A \subset N$, A has a least element x_1 (say). Consider $A - \{x_1\}$ and let x_2 be the least element of $A - \{x_1\}$. Consider $A - \{x_1, x_2\}$ and let x_3 be the least element of $A - \{x_1, x_2\}$. Continue this process so that x_{n+1} is the least element of $A - \{x_1, x_2, \ldots x_n\}$. Define $f : N \to A$ by $f(1) = x\s\do3(1)$, and $f(n + 1) = x\s\do3(n+1)$ where $x\s\do3(n+1)$ is the least element of $A - \{x_1, x_2, \ldots x_n\}$. Thus we have a set of numbers $\{x_1, x_2, \ldots, x_n, \ldots\}$ where $x_1 < x_2 \ldots < x_n < x_{n+1} < \ldots$; f is clearly one - one because $a \neq b \Rightarrow f(a) \neq f(b)$. To see that f is onto, we suppose the opposite. That means that there is no $n \in N$ such that $x_n = x$. This means $x \in A - \{x_1, \ldots x_n\}$ for every n. Since x_{n+1} is the least element of $A - \{x_1, x_2, \ldots x_n\}$, it means $x > x_{n+1} \geq n + 1 > n$. Thus $x > n$, for every $n \in N$. In particular $x > x$. This impossibility proves that $x \in \{x_1, \ldots x_p\}$ for some $p \in N$. Therefore $x = x_k$ for some $k \in N$ and $f(k) = x_k$ for this unique k.

Remark 3 : A non empty set A is countable if and only if there exists a B such that $B \subset N$ and A is equivalent to B.

Theorem 10 :

A countable union of countable sets is countable.

Proof : Consider the sets

$$S_1 = \{a_{11}, a_{21}, a_{31}, \ldots\}$$
$$S_2 = \{a_{12}, a_{22}, a_{32}, \ldots\}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

The sets $S_1, S_2, \ldots$ are countable in number. To show that $S_1 \cup S_2 \ldots$ is a countable set, we have to set up a one - one correspondence between elements of $S_1 \cup S_2 \ldots$ and the set N of natural numbers. Let the elements of $S_1 \cup S_2 \ldots$ be arranged in the following form connected by directed arrows.

$$\begin{array}{llll} a_{11} \rightarrow a_{21} & a_{31} \rightarrow a_{41} & \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{12} \quad a_{22} & a_{32} \quad a_{42} & \ldots\ldots\ldots\ldots\ldots\ldots \\ \downarrow & & \\ a_{13} \quad a_{23} & a_{33} \quad a_{43} & \ldots\ldots\ldots\ldots\ldots\ldots \\ & & \\ a_{14} \quad a_{24} & a_{34} \quad a_{44} & \ldots\ldots\ldots\ldots\ldots\ldots \\ \downarrow & & \\ a_{15} & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

Listing the elements of $S_1 \cup S_2 \ldots$ in a particular way by following the direction of arrows, we get the set $\{a_{11}, a_{21}, a_{12}, a_{13}, a_{22}, a_{31}, a_{41}, a_{32}, a_{23}, a_{14}, \ldots\}$ where the first element has subscripts whose sum is 2, the next two elements have subscripts whose sum is 3, the next three have sum of subscripts 4 etc. This establishes a 1 – 1 correspondence of $S_1 \cup S_2 \cup \ldots$ with N. Thus $S_1 \cup S_2 \cup \ldots$ is countable.

Theorem 11 :

The set of all rational numbers is countable.

Proof : It is sufficient if we establish a one - one correspondence between the set of rationals and N. For this let us arrange all the rational numbers according to the following rule.

(i) All the natural numbers are placed in the first row in ascending order.

(ii) Zero and all negative integers are placed in the second row in desending order.

(iii) All positive reduced fractions with denominator 2 are placed in third row increasing order.

(iv) All negative reduced fractions with denominator 2 are placed in fourth row in decreasing order etc .....

Every rational number occurs only once in this table.

1	2	3	4	5	6	...
0	–1	–2	–3	–4	–5	...
$\frac{1}{2}$	$\frac{3}{2}$	$\frac{5}{2}$	$\frac{7}{2}$	$\frac{9}{2}$	$\frac{11}{2}$	...
$-\frac{1}{2}$	$-\frac{3}{2}$	$-\frac{5}{2}$	$-\frac{7}{2}$	$-\frac{9}{2}$	$-\frac{11}{2}$	...
$\frac{1}{3}$	$\frac{2}{3}$	$\frac{4}{3}$	$\frac{5}{3}$	$\frac{7}{3}$	$\frac{8}{3}$	...
$-\frac{1}{3}$	$-\frac{2}{3}$	$-\frac{4}{3}$	$-\frac{5}{3}$	$-\frac{7}{3}$	$-\frac{8}{3}$	...

Then all the rational numbers can be arranged in correspondence with natural numbers in the following way

Natural Number	1	2	3	4	5	6	7	8	9	...
Rational number	1	2	0	3	–1	1/2	4	–2	3/2	...

This establishes a one - one correspondence between rational numbers and N. Thus the set of ratinal numbers is countable.

Remark 3 : It is also possible to view Q as a countable union of countable sets by arranging elements of Q as

$$A_0 = \{0\}$$

$$A_1 = \left\{\frac{1}{1}, \frac{-1}{1}, \frac{2}{1}, \frac{-2}{1}, \frac{3}{1}, \frac{-3}{1}, \ldots\right\}$$

$$A_2 = \left\{\frac{1}{2}, \frac{-1}{2}, \frac{2}{2}, \frac{-2}{2}, \frac{3}{2}, \frac{-3}{2}, \ldots\right\}$$

$$A_3 = \left\{\frac{1}{3}, \frac{-1}{3}, \frac{2}{3}, \frac{-2}{3}, \frac{3}{3}, \frac{-3}{3}, \ldots\right\}$$

$$\vdots$$

$$A_n = \left\{\frac{1}{n}, \frac{-1}{n}, \frac{2}{n}, \frac{-2}{n}, \frac{3}{n}, \frac{-3}{n}, \ldots\right\}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$Q = A_0 \cup A_1 \cup \ldots A_n \cup \ldots$$

Since each A_i is countable their union is also countable.

Theorem 12 :

The set of real numbers is not countable

Proof : In fact we show that the set of real numbers x such that $0 \le x \le 1$ is itself not countable. We assume that every real number x with $0 \le x < 1$ has a decimal representation in the form

$$x = 0 \cdot a_1 a_2 a_3 \ldots\ldots\ldots$$

where each a_i is one of the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. We assume that numbers whose decimal expansion terminates, such as 0.1728, are written as 0.1728000 ... and also 0.17279999 ...

If all the real numbers x, $0 \le x \le 1$, were to be countable then we can place them in one - one correspondence with natural numbers as follows :

$$1 \leftrightarrow 0.a_1 a_2 a_3 a_4 \ldots$$

$$2 \leftrightarrow 0.b_1 b_2 b_3 b_4 \ldots$$

$$3 \leftrightarrow 0.c_1 c_2 c_3 c_4 \ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Now let us form a real number y, $0 \le y \le 1$ and show that it is not listed in the above listing. For this let y_1 be a digit different from 0, a_1 and 9; let y_2 be a digit different from 0, b_2 and 9; let y_3 be a digit different from 0, c_3 and 9 etc. Consider the number y with the decimal expansion

$$y = 0 \cdot y_1 y_2 y_3 y_4 \ldots$$

Now clearly $0 \le y < 1$. The number y is not one of the numbers with two decimal representations because $y_n \neq 0$, $y_n \neq 9$. At the same time $y \neq x_n$ for any n, since the n^{th} digits in the decimal representation for y and x_n are different. Thus the real number y is not in the list mentioned above. Therefore we conclude that any countable collection of real numbers x, $0 \le x \le 1$, will not have atleast one real number from this set. Thus the real numbers x, $0 \le x \le 1$ is not countable. R

being a super set having the set $\{x \in \mathbf{R} \mid 0 \leq x \leq 1\}$ as a subset which is not countable is itself not countable.

Remark 4 : We have seen that both **R**, the set of real numbers and Q, the set of rational numbers are ordered fields. We have also seen that the set of rationals is a countable set where as the set of reals is not countable. This means that there do exist real numbers which are not rational. In this sense, the reals satisfy a property called "completeness property" which rationals do not possess. We end this unit by exhibiting a number which is not rational.

Example : $\sqrt{2}$ is not a rational number (or, there is no rational number x such that $x^2 = 2$).

Let if possible $\sqrt{2} = \frac{p}{q}$, where $q \neq 0$ and p, q are integers prime to each other. That is 1 is the g.c.d of p and q. Now $\sqrt{2} = \frac{p}{q} \Rightarrow 2 = \frac{p^2}{q^2}$ or $p^2 = 2q^2$. Now q is an integer and hence q^2 is an integer and $2q^2$ is an even integer. But $2q^2$ is an even integer implies that p^2 is also an even integer. But p^2 is an even integer implies that p is an even integer. Let $p = 2m$, where m is an integer. Then $p^2 = 4m^2$ and $p^2 = 2q^2 \Rightarrow 4m^2 = 2q^2$ or $2m^2 = q^2$. Now q^2 is an even integer implies q is an even integer. Hence both p and q are even integers contradicting the fact that they are relatively prime. Thus our assumption $\sqrt{2} = \frac{p}{q}$ with $(p, q) = 1$ is wrong. That means $\sqrt{2}$ is not a rational number.

SAQ 8 If a^2 is even then a is even.

11.6. SUMMARY

Every student of mathematics is aware that real numbers exist and that they behave in a similar way as the rationals. But introducing a student formally to the concept of real number is always laborious and technical. Even among eminent mathematicians there is no uniformly accepted way of presentation. In this unit we have defined a real number as belonging to an ordered field. But rational numbers also from an ordered field. So how can we distinguish real numbers from rational numbers is the question. We proved that the set of rationals is countable where as the set of reals is not. This means that there exist real numbers which are not rational. We exhibited one such real number $\sqrt{2}$, which is not a rational number.

11.7 MODEL EXAMINATION QUESTIONS

SECTION - A (Long Answers)

(i) Define a countable set. Show that the set of rationals is countable where as the set of reals is not.

(ii) Show that every non empty subset of N has a least element.

SECTION - B (Short Answers)

(i) Define an inductive set and give an example. Show that $n \in \mathbf{N}, n < x < n + 1 \Rightarrow x \notin \mathbf{N}$.

(ii) Show that any subset of N is countable.

(iii) Prove that $n \in \mathbf{N}$ and $n \neq 1 \Rightarrow n - 1 \in \mathbf{N}$ and $p, q \in \mathbf{N}$ and $p < q \Rightarrow q - p \in \mathbf{N}$.

11.8 ANSWERS TO SELF ASSESSMENT QUESTIONS

SAQ 1 $a + b = a + c \Rightarrow (-a) + (a + b) = (-a) + (a + c) \Rightarrow (-a + a) + b = (-a + a) + c \Rightarrow 0 + b = 0 + c \Rightarrow b = c$.

SAQ 2 $a + a = a \Rightarrow a + a = a + 0$ by (SAQ 1), $a = 0$.

SAQ 3 $a + b = 0 = a + (-a) \Rightarrow b = -a$ by (SAQ 1).

SAQ 4 $a + (-a) = 0 = b + (-b) \therefore [a + (-a)] + [b + (-b)] = 0$

$\Rightarrow (a - b) + (b - a) = 0 \Rightarrow -(a - b) = (b - a)$.

SAQ 5 Either $a \in P$ or $-a \in P$. If $a \in P$ then $a^2 = a \cdot a \in P$.

If $-a \in P$, then $a^2 = (-a) \cdot (-a) \in P$. Either way $a^2 \in P$.

SAQ 6 $x < y$ and $x > 0 \Rightarrow x^2 < xy$; Similarly $xy < y^2$. Thus $x^2 < xy < y^2 \Rightarrow x^2 < y^2$. Conversely if $x^2 < y^2 \Rightarrow x^2 - y^2 < 0$.

$(x + y)(x - y) < 0$. But $x > 0$; $y > 0 \Rightarrow x + y > 0$. Thus $x - y < 0$ or $x < y$.

SAQ 7 f is one - one : Let $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$.

SAQ 8 We prove by contrapositive equivalence that if a is odd then a^2 is odd. Let $a = (2n + 1)$, n an integer then $a^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1 = 2m + 1$, $m = 2n^2 + 2n$. Thus a^2 odd.

UNIT–12: COMPLETENESS PROPERTIES OF REAL NUMBERS

Contents

12.1 Aims and Objectives

12.2 Introduction

12.3 Bounded and unbounded sets

12.4 Completeness axiom and Dedekind's property

12.5 Workedout exercises

12.6 Summary

12.7 Model Examination Questions

12.8 Answers to Self Assessment Questions

12.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to : (i) Determine the l. u. b and g.l.b of a bounded set (ii) Derive the properties of l.u.b and g.l.b (iii) State completeness axiom and dedikind's property and establish their equivalence. (iv) To represent real numbers as points on a line.

12.2 INTRODUCTION

In unit 11 we have established a number $\sqrt{2}$, which is not a rational number. This means that rational numbers alone are not sufficient to measure quantities which can be represented as distances on a line. The German mathematician Dedekind (1831 - 1916) defined a real number to be a "cut" in the rational number system. This Dedekind's cut is not the only way of establishing the existence of a real number. Cantor (1845 - 1918) used the method of nested intervels. Weierstrass (1815 - 1897) and Cauchy (1789 - 1857) used the method of sequences to establish the existence of a real number and study its properties. In this unit we establish the equality between the completeness axiom : A non empty set of reals bounded above has a least upper bound and the Dedekind cut. Some authors call this as continuum property also.

12.3 BOUNDED AND UNBOUNDED SETS

A non empty subset of real numbers is called an *aggregate* of real numbers or simply an *aggregate.*

Definition 1 :

Let A be an aggregate. If there exists a real number M such that $x \leq M$ for every $x \in A$, then M is called an *upper bound* of A and A is said to be *bounded above*. An upper bound of an aggregate is not unique because if M is an upper bound of an aggregate A and $M_1 > M$ is also an upper bound of A.

Definition 2 :

Let A be an aggregate. If there exists a real number m such that $x \geq m$ for every x in A, then m in called a *lower bound* of A and A is said to be bounded below. The lower bound of an aggregate is not unique for if m is a lower bound and $m_1 < m$, then m_1 is also a lower bound.

Defintion 3 :

An aggregate A is said to be bounded if it is both bounded above and bounded below. An aggregate which is not bounded is called unbounded.

Defintion 4 :

If M is an upper bounded of an aggregate A and if any real number less than M is not an upper bound of A, then M is called the *least upper bound* (l.u.b) of A. A least upper bound is also called a *supremum* of S.

Definition 5 :

If m is a lower bound of an aggregate of A and any real number greater than m is not a lower bound of A, then m is called the *greatest lower bound* (g.l.b) of A. A greatest lower bound is also called an *infimum* of A.

Definition 6 :

If M is the l.u.b and m is the g.l.b of an aggregate A, then M - m is called the oscillation of the aggregate A.

Remark 1 : If an aggregate A has a largest element M, then M is called the maximum of A. If A has a smallest element m, then m is called the minimum of A. It is obvious that if an aggregate A has a maximum M, then A is bounded above and M is the l.u.b and in this case l.u.b A = Sup A = max A. Similarly, for minimum.

Remark 2 : A common mistake commited very often is to suppose that l.u.b of an aggregate A is always the maximum of A. But we have examples of sets which are bounded above, have a l.u.b but have no maximum. Consider $A = \{x \in \mathbf{R} \mid 0 \leq x < 1\}$. Then 1 is not the maximum of A because $1 \notin A$. But 1 is the l.u.b. Ofcourse 0 is the g.l.b and also the minimum of A.

Example 1 : A = {1, 3, 5, 7, 9, 11}; A is bounded, upper bounds of A are 11, 12, $\frac{111}{10}$ etc; The lower bounds are 0, $\frac{1}{2}$, –3, etc, the l.u.b = 11 = max A; g.l.b = 1 = min A.

Example 2 : $A = \left\{\frac{1}{n} \mid n \in \mathbf{N}\right\} = \left\{1, \frac{1}{2}, \frac{1}{3}, \ldots\right\}$. A is bounded, upper bounds of A are 1, $\frac{3}{2}$, 1.1, 2 etc; l.u.b = 1 max A = 1; lower bounds 0, $-\frac{1}{2}$, –1, – 0.1 etc. g.l.b = 0 min. A does not exist.

Example 3 : If $A = \left\{\frac{2x+3}{3x+4} \mid x \in \mathbf{R}, x > 0\right\}$, max A, min A do not exist. A is bounded; l.u.b = $\frac{3}{4}$, g.l.b = $\frac{2}{3}$.

SAQ 1 Find l.u.b and g.l.b of $A = \left\{\frac{(-1)^n}{n} \mid n \in \mathbf{N}\right\}$

SAQ 2 Find l.u.b and g.l.b of $A = \left\{ 1 + \frac{(-1)^n}{n} \mid n \in N \right\}$

SAQ 3 Find l.u.b and g.l.b of $A = \left\{ \frac{-(n+1)}{n} \mid n \in N \right\}$

Theorem 1 :

Let A be an aggregate.

(i) If M is an upper bound and m is the lower bound of A, then $m \leq M$.

(ii) The l.u.b and g.l.b if they exist are unique

Proof : (i) M is an upper bound of A $\Rightarrow x \leq M \; \forall x \in A$.

m is a lower bound of A $\Rightarrow x \geq m \; \forall x \in A$. Therefore $m \leq x \leq M \; \forall x \in A$.

(ii) Let M_1 and M_2 be two l.u.b s of A. If $M_1 < M_2$, then M_2 is not the l.u.b of A. Therefore $M_1 \geq M_2$. Similarly $M_2 \geq M_1$. Thus $M_1 = M_2$. A similar proof holds for g.l.b

Theorem 2 :

If M is the l.u.b of an aggregate A and $y < M$ is a real number, then there exists $x \in A$ such that $y < x \leq M$. Similarly if m is the g.l.b of A and $y > m$ is any real number, then there exists $x \in A$ such that $y > x \geq m$.

Proof : Suppose M = l.u.b of A, $y < M$ and there is no $x \in A$ such that $y < x \leq M$. This means that y is an upper bound and $y < M$ contradicts the fact that M is l.u.b. Thus there is $x \in A$ such that $y < x \leq M$.

Remark 3 : Completeness axiom

An aggregate of real numbers which is bounded above has a least upper bound. Thus the real number system can be precisely described as a complete ordered field.

Theorem 3 : (Archimedean Principle)

If b and c are real numbers and if $c > 0$, then there exists a natural number n such that $nc > b$.

Proof : Suppose there exist real numbers b and c with $c > 0$ and $nc \leq b$ for every $n \in N$. Then b is the upper bound of the aggregate $A = \{x \mid x = nc, n \in N\}$. By the Axiom of completeness, there exist a real number a = l.u.b A. Since $a - c < a$, $a - c$ is not an upper bound of A. Hence there exists $nc \in A$ such that $nc > a - c$. But this means that $(n + 1)c > a$. Since $(n + 1)c$ also belongs to A, this contradicts the assumption that a is an upper bound of A.

Remark 4 : Taking $c = 1$ in the above theorem we get that for every real number b, there exists a positive integer n such that $n > b$. Similarly for every real number b, there exists an integer m such that $m < b$. Further, for every real number b, there exists a natural number n such that $\frac{1}{n} < b$.

Remark 5 : Dedekind's Completness property : Let A and B be two non empty aggregates (subsets of R). Then an ordered pair (A, B) is said to form a "cut" (or Dedekind's cut) if $A \cap B = \phi$; $A \cup B = R$ and $a < b$ for all $a \in A$ and all $b \in B$. The Dedikind's property states that either A has the maximum number or B has the minimum number.

Theorem 4 :

Equivalence of completeness axiom and Dedekind's property. The following are equivalent :

(i) If all the real numbers are divided into two classes L and R such that each class is not empty, every real number has a class and every member of L < every member of R, then either L has the greatest number or R has the least number.

(ii) Every non empty subset of R which is bounded above has a least upper bound.

Proof : (ii) $\Rightarrow$ (i). Suppose (ii) holds. Let L and R be two non empty subsets of **R** such that $L \cup R = \mathbf{R}$ and $x \in L, y \in R \Rightarrow x < y$. We are required to show that either L has the largest (maximum) number or R has the smallest (minimum) number. Since every member of L is less than every member of R, L is bounded above. If L has the largest number there is nothing elese to prove. If L has no largest number, then the set of its upper bounds is R and R has the smallest number. Thus either L has the largest number or R has the smallest number.

(i) $\Rightarrow$ (ii). Conversely, suppose that Dedikind's property holds. Let S be a non empty set of reals bounded above. Define $L = \{x \mid x \text{ is not an upper bound of } S\}$ and

$R = \{x \mid x \text{ is an upper bound of } S\}$. Clearly $L \neq \phi, R \neq \phi, L \cup R = \mathbf{R}$ and $x \in L, y \in R \Rightarrow x < y$. Then by Dedekind's property either L has the largest number or R has the least number.

Let if possible L have the largest number say, α. Then $\alpha \in L \Rightarrow \alpha \notin R \Rightarrow \alpha$ is not an upper bound of S. This means that there is an $a \in S$ such that $\alpha < a$. Consider the real number $\frac{\alpha + a}{2}$. Then $\alpha < \frac{\alpha + a}{2} < a$. Since $\frac{\alpha + a}{2} > \alpha \Rightarrow \frac{\alpha + a}{2} \in R$. But $\frac{\alpha + a}{2} < a$. Therefore $\frac{\alpha + a}{2} \in L$. Thus $\frac{\alpha + a}{2}$ is not an uper bound of S. This is a contradiction. Thus L has no largest number. Therefore R has the least number and hence S has a l.u.b.

Theorem 5 :

If a and b are any two real numbers with $a < b$, then there exists a rational number r such that $a < r < b$. (Equivalently, a real number can be approximated by a rational number in the sense that for any real number b, there exists a rational number r such that $b - \epsilon < r < b$ for any $\epsilon > 0$).

Proof : Recall from Archimedes principle that for any two real numbers b and c, $c > 0$, there is $n \in N$ such that $nc > b$. In particular $n > \frac{1}{b}$ or $\frac{1}{n} < b$. Since a, b are natural numbers and $a < b$, $b - a$ is a natural number. Then there exists $n \in N$ such that $\frac{1}{n} < (b - a)$. This means that $a < b - \frac{1}{n}$. Since there exists an integer k such that $nb - 1 < k < nb$, we have that $b - \frac{1}{n} \leq \frac{k}{n} < b$. Thus $a < b - \frac{1}{n} \leq \frac{k}{n} < b$. Taking $r = \frac{k}{n}$ we have $a < r < b$.

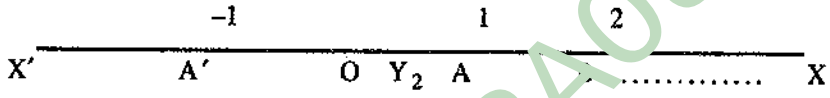
SAQ 4 For any real x, there is an integer n such that $x - 1 < n < x$.

Theorem 6 :

For any two real numbers a and b with $a > 1$, there is $n \in N$, such that $a^n > b$.

Proof : Suppose $a^n \leq b$ for all $n \in N$. Then the set $S = \{x \mid x = a^n, n \in N\}$ is bounded above. Hence by completeness axiom. there exists a l.u.b of S. Let c = l.u.b S. But $c < ac$ or $\frac{c}{a} < c$ since $a > 1$. Since $\frac{c}{a} < c$, the l.u.b of S, there exists $a^n \in S$ such that $a^n > \frac{c}{a}$ or $a^{n+1} > c$ and $a^{n+1} \in S$, this contradicts that c is an upper bound. Hence the assumption that $a^n \leq b$ is wrong. Thus $a^n > b$.

Remark 6 : The geometrisation of arithmatic helps us to gain an intuitive insight into the properties of real numbers. It is customary to identify real numbers as points on a line. Let X′ X be a real line (x - axis). Mark an arbitary point O on X′ X. Let A be a point to the right of O such that OA = 1 unit. Then O corresponds to zero and A corresponds to 1. Let us designate the right side of O as a positive segment and the left side of O as negative segment. Thus if A′ is on to the left of O such that OA′ = OA = 1 unit then we assign –1 to A′. To designate the rational number $\frac{m}{n} > 0$ we take a point P to the right of O such that OP is m times the n^{th} part of OA. This way there exists a correspondence between rational numbers and the points on X′ X.



Even though rational numbers appear to cover all the points on this line X′ X, there exist points on the line that do not correspond to rationals. For example $\sqrt{2}$ is one such. Such points on the line X′ X that do not correspond to rational numbers are called irrational points and the numbers correspond to them are called irrational numbers. It can be proved that there always exist an irrational number between any two rationals. This number between the set of reals and the points on a line is stated by Dedekind - Cantor Axiom : "To every real number there corresponds a unique point on a directed line and to every point on a directed line there corresponds a real number. **R** is called the arithmatic continuum if we talk of real numbers and is called geometric continuum if we talk about the points on a line.

12.5 WORKED OUT EXERCISES

Exercise 1 : If a is rational and b is irrational, show that $a + b$ is irrational.

Ans : Let a be a rational number and b an irrational number. If possible let $(a + b)$ be rational. Then $a = p/q$ and $a + b = \frac{r}{s}$, where p, q, r, s are integers and $q \neq 0, s \neq 0$. Now $b = (a + b) - a \Rightarrow b = \frac{r}{s} - \frac{p}{q} = \frac{rq - ps}{sq}$ implying that b is rational, a contradiction. Thus $a + b$ is not rational.

Exercise 2 : If S is a non empty subset of reals with a lower bound show that S has a g.l.b.

Ans : Let b be a lower bound of S. Define a set T, $T = \{x \mid -x \in S\}$. Then $-b$ is an upper bound of T. This is because if $x \in T$, then $-x \in S$ and hence $b \le -x$ which implies that $-b \ge x$. Let c be the least upper bound of T. Then $-c$ is the greatest lower bound of S. Because $-c$ is a lower bound for S and $x \in S \Rightarrow -x \in T$. Consequently $-x \le c$ and $x \ge -c$. Now suppose a is any lower bound for S. Then $-a$ is an upper bound of T. Since c is the l.u.b of T, $c \le -a$ and consequently $-c \ge a$.

Exercise 3 : For any two real numbers a, b prove that $|a \cdot b| = |a| \cdot |b|$ and $|a + b| \le |a| + |b|$

Ans : $|a \cdot b| = \sqrt{(a \cdot b)^2} = \sqrt{a^2 \cdot b^2} = \sqrt{a^2} \cdot \sqrt{b^2} = |a| \cdot |b|$

$(|a + b|)^2 = (a + b)^2 = a^2 + 2ab + b^2 = |a|^2 + 2ab + |b|^2$

But for any real x, $-|x| \le x \le |x|$, Therefore

$$\begin{aligned} |a|^2 + 2ab + |b|^2 &\le |a|^2 + 2|a \cdot b| + |b|^2 \\ &\le |a|^2 + 2|a| \cdot |b| + |b|^2 \\ &= (|a| + |b|)^2 \end{aligned}$$

Since $|a + b|^2 \le (|a| + |b|)^2$ we have

$$|a + b| \le |a| + |b|.$$

Exercise 4 : If x is any real number, prove that $x^2 > 0$.

(i) If $0 < a < 1$ and $b > 1$, prove that $0 < a^2 < a < 1 < b^2 > b > 1$.

(ii) If $\frac{a}{b} < \frac{A}{B}$, prove that $\frac{a}{b} < \frac{a + A}{b + B} < \frac{A}{B}$ $(b, B > 0)$.

Ans : We need to consider theree possibilities $x = 0$; $x > 0$ and $x < 0$. If $x = 0$, then $x^2 = 0$. If $x > 0$, then $x \cdot x > x \cdot 0$. Thus $x^2 > 0$ If $x < 0$, write $0 < x$. Then $0 \cdot x < x \cdot x$ or $0 < x^2$ or $x^2 > 0$. Thus in any case $x^2 \ge 0$.

Since $0 < a < 1$ and $a > 0$, we have from above that $0 < 0 \cdot a < a \cdot a < 1 \cdot a$ or $0 < a^2 < a < 1$.

Similarly since $b > 0$, and hence $b^2 = b \cdot b > 1 \cdot b$ or $b^2 > b$.

Since $b\,B > 0$, $a\,B = \frac{a}{b} \cdot b\,B < \frac{A}{B} \cdot b\,B = AB$. Then $a(b + B) = ab + a\,B < ab + AB = (a + A)\,b$.

Since $(b + B)^{-1} > 0$ and $b^{-1} > 0$; $ab^{-1} < (a + A)(b + B)^{-1}$ or $\frac{a}{b} < \frac{a + A}{b + B}$. Similarly the other inequality.

Example 5 : If a is a positive real number and $n \in N$ then there exists a unique $x > 0$ such that $x^n = a$. This is denoted by $a^{1/n}$ or $\sqrt[n]{a}$, n^{th} root of a.

Ans : The result is true for $n = 1$. Let $n > 1$. Consider $A = \{y \in R \mid y > 0;\ y^n > a\}$. Since $a + 1 > 1$, $(a + 1)^n > a + 1 > a$. Thus $a + 1 \in A$ and hence A is an aggregate. Since 0 (zero) is a lower bound of A, the g.l.b of A exists. Let x = g.l.b of A. Then $x \ge 0$. We shall prove that $x^n = a$. If possible let $x^n < a$. Let $\delta = \min\left\{1, \frac{a - x^n}{n(1 + x)^{n-1}}\right\}$. Then $\delta > 0$ and $(x + \delta)^n - x^n < n(x + \delta)^{n-1} \cdot \delta \le n(x + 1)^{n-1} \cdot \delta \le a - x^n$. Thus $(x + \delta)^n < a$.

x = g.l.b $A \Rightarrow$ there is $y \in A$ such that $x \le y < x + \delta$ and $y \in A \Rightarrow y^n > a$. Thus $a < y^n < (x + \delta)^n < a$. This is a contradiction. Thus the assumption $x^n < a$ is wrong. If possible

let $x^n > a$. Now $x^n > a > 0$; $x \geq 0 \Rightarrow x > 0$. Let $\delta = \frac{x^n - a}{n\, x^{n-1}}$. Then $\delta > 0$. Thus $n > 1$, $x > 0 \Rightarrow$ $(n-1)\, x^n > 0$; $a > 0 \Rightarrow -a < 0$. Thus $(n-1)\, x^n > -a$ and $n\, x^n > x^n - a$ giving $x > \frac{x^n - a}{n\, x^{n-1}}$. $\therefore x > \delta > 0$. But then $\left(x^n - (x-\delta)^n\right) < n\, x^{n-1}\, \delta = x^n - a$. Therefore $(x-\delta)^n > a$. $\therefore x - \delta \in$ A contradicting x = g.l.b A. $\therefore x^n > a$ is wrong. Thus $x^n = a$.

To see x is unique let $x \neq y$, $y > 0$, $y^n = a$. Then $0 = x^n - y^n = (x-y) \sum_{r=0}^{n-1} x^r\, y^{n-1-r} \neq 0$; since $x \neq y$. This is a contradiction. Thus x is unique.

Exercise 6 : Suppose n is an even natural number. Prove that the equation $x^n = y$ has no real solutions if $y < 0$, one solution if $y = 0$ and two solutions if $y > 0$. If n is odd natural number, show that $x^n = y$ has exactly one solution.

Ans : If n is an even natural number, then $n = 2k$ so that $x^n = x^{2k} = (x^k)^2 \geq 0$, for all values of x. Hence if $y < 0$, $x^n = y$ has no solutions. The equation $x^n = 0$ has exactly one solution $x = 0$, because $x \neq 0 \Rightarrow x^n \neq 0$. If $y > 0$, then $x = y^{1/n}$ and $x > 0$ and is unique. If n is even $x^n = y$ if and only if $(-x)^n = y$. Hence the equation has two solutions, one positive and one negative.

Suppose n is odd. If $y = 0$, there is exactly one solution for $x^n = 0$. If $y > 0$, there is exactly one positive solution and this is the only solution because $x < 0 \Rightarrow x^n < 0$ when n is odd. If $y < 0$, let $z^n = -y$. Then this equation has one and only one solution and hence the same solution is true for $(-x)^n = -y$. That is $x^n = y$.

12.6 SUMMARY

In the previous unit we exhibited a number $\sqrt{2}$ and showed that it is not a rational number. Ofcourse $\sqrt{2}$ is not the only irrational number and our ability to extract n^{th} roots allows us to construct many others. In this unit we presented a property of the real number system which is called the completeness property. But there are several versions of this property. We have chosen to give here one version which assumes that an aggregate bounded above has a least upper bound. We have introduced the Dedekind's version of cuts and showed that these two versions are equivalent. Finally we conclude that a real number system is a complete ordered field.

12.7 MODEL EXAMINATION QUESTIONS

SECTION - A (Long Answers)

(i) State the completeness axiom and the Dedikend's version of the axiom. Establish the equivalence of these two.

(ii) Explain in detail how real numbers could be exhibited as points on a line and vice versa.

SECTION - B (Short Answers)

(i) Define l.u.b and g.l.b of an aggregate and give examples. Show that if M is the l.u.b of an aggregate A and $y < M$ is a real number then there exists $x \in$ A such that $y < x \leq M$.

(ii) If a is a positive real number and $n \in$ N, then show that there exists a unique $x > 0$ such that $x^n = a$.

(iii) State and prove Archemede's theorem.

12.8 ANSWERS TO SELF ASSESSMENT QUESTIONS

SAQ 1 g.l.b = -1 = min A; l.u.b = $\frac{1}{2}$ = max A

SAQ 2 g.l.b = 0 = min A; l.u.b = $\frac{3}{2}$ = max A

SAQ 3 g.l.b = -2 = min A; l.u.b = -1; max A $\notin$ A.

SAQ 4 As a consequence of Archimedes principle, $\exists$ (there exist) integers m and n such that $m < x < n$. Let k = max $\{m, m+1, \ldots n\}$ such that $k < n$. Then $k + 1 \geq x$. Consequently $k \geq x - 1$.

UNIT–13 : OPEN SETS AND CLOSED SETS IN R

Contents

13.1 Aims and Objectives

13.2 Introduction

13.3 Open and closed sets

13.4 Limit point of a set

13.5 Worked out exercises

13.6 Summary

13.7 Sample Examination Questions

13.8 Answers to Self Assessment Questions

13.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to (i) define open and closed sets in **R** and determine a given aggregate is open or closed, (ii) define a limit point and determine the limit point of an aggregate if it exists, (iii) state and prove Bolzano Weierstrass Theorem, (iv) Prove that every non-empty open subset of **R** is a union of countable disjoint collection of open intervals.

13.2 INTRODUCTION

Most of the deepest results in the study of real number system depend on the notion and properties of open and closed sets of real numbers. In this course we are confined to the study of the real line and as such the open and closed sets correspond to open and closed intervals. This in turn leads to the concept of a neighbourhood of a point. If A is an aggregate and P is a real number (*a* point) in A, then it is natural to ask how the numbers (points) in A are arranged in relation to P. If there are infinitely many numbers (points) of A which are arbitrarily close to P, then P is called a limit point of A. Of course P itself may or may not belong to A. The Bolzano (1781-1848) and Weirstrass (1815-1897) theorem states that every bounded infinite aggregate has atleast one limit point. We prove that an aggregate (set) is closed if and only if it contains all its limit points. The study of limit points is fundamental to the study of Real Analysis.

13.3 OPEN AND CLOSED SETS IN R

Let a and b be two real numbers (points on the real line). Then the real number $|a-b|$ is called the distance between (the points) a and b. If $a, b \in \mathbf{R}$, then we observe that

(i) $|a-b| = 0$ if and only if $a = b$

(ii) $|a-b| = |b-a|$,

(iii) $|a-c| \leq |a-b| + |b-c|$ (traingle inequality). A subset A of **R** is called an interval if $x, y \in A, z \in \mathbf{R}, x < z < y \Rightarrow z \in A$.

Notation : We use parentheses (brackets) of two different kinds to distinguish different types of intervals (subsets of **R**).

$(a, b) = \{x \in \mathbf{R} \mid a < x < b\}$ = open interval (a, b)

$[a, b] = \{x \in \mathbf{R} \mid a \leq x \leq b\}$ = Closed interval $[a, b]$

$[a, b) = \{x \in \mathbf{R} \mid a \leq x < b\}$ = Semi closed or Semi open

$(a, b] = \{x \in \mathbf{R} \mid a < x \leq b\}$ = Semi closed or Semi open.

All these intervals are bounded intervals. If either a or b or both are '∞' a symbol which means that $\infty > x \; \forall \; x \in \mathbb{R}$, we call the intervels as unbounded intervals.

Definition. 1 :

If $a \in \mathbb{R}$ and $\in > 0$ is a real number, then the set $\{x \mid x \in \mathbb{R}, |x - a| < \in\}$ is called the $\in$ - *neighbourhood* of 'a'. It is easy to see that $\in$ - neighbourhood of a real number (point) 'a' is the open interval $(a - \in, a + \in)$. Some authors use the notation $N_{\in}(a)$, or $N(\in, a)$ to denote the $\in$ - neighbourhood of the real number 'a'. For example $\left(2 - \frac{1}{4}, 2 + \frac{1}{4}\right)$ is the $\frac{1}{4}$– neighbourhood of 2.

Definition. 2 :

Let $A \subseteq \mathbb{R}$ and $a \in A$. If there exists a real number $\in > 0$, such that the $\in$ - neighbourhood of a is contained in A, then the point a is called an *interior point* of A. If $A \subseteq \mathbf{R}$ and if every $a \in A$ is an interior point of A then A is called an open set in **R**.

Example. 1 : **R** and ϕ are open sets in $\mathbb{R}$. This is because $x \in \mathbf{R} \Rightarrow (x - \in, x + \in) \subseteq \mathbb{R}$ for any $\in > 0$. ϕ is empty because it contains no points and hence satisfies the definition of an open set trivially.

Example. 2 : Let $\in > 0$. Then $[a, \in) \subseteq \mathbb{R}$ is not an open set because any $\in$ – neighbourhood of a, namely $(a - \in, a + \in)$ contains points which do not belong to $[a, \in)$. Similarly $(a, b]$, $[a, b]$ are not open sets.

Example. 3. Any finite set $A \subseteq \mathbb{R}$ is not an open set in **R**. To see this let $A = \{x_1, \ldots, x_n\}$ for some $n \in N$ and $x_1 < x_2 < \ldots < x_n$. An $\in$ – neighbourhood of x_1, namely $(x_1 - \in, x_1 + \in)$ is an infinite set and hence not contained in A. Thus x_1 is not an interior point of A. Similarly other points of A.

Example. 4 : The set Q of rational numbers is not open in $\mathbb{R}$. To see this let $x \in Q$ then for any $\in > 0$, there exists an irrational number y such that $x - \in < y < x + \in$. Hence $(x - \in, x + \in) \not\subset Q$. This means that no point of Q is an interior point.

Theorem. 1 :

Every open set in $\mathbb{R}$ is a union of open intervals in **R**.

Proof : If A is an open set in $\mathbb{R}$, then any point $a \in A$ is an interior point. For any $\in > 0$, the $\in$ – neighbourhood of a is contained in A. Since this is true for every $a \in A$, we have

$$A = \cup \left\{ N_{\in}(a) \mid a \in A \right\}.$$

Definition. 3 :

If A is a subset of $\mathbf{R}$ such that the complement of A in $\mathbf{R}$, that is $\mathbf{R} - A = \{x \mid x \in \mathbf{R}, x \notin A\}$ is open in $\mathbf{R}$, then A is called a *closed* set in R.

Example 5 : $\mathbf{R}$ and ϕ are closed sets in $\mathbf{R}$ because they are the complements of the open sets ϕ and R. Q, the set of rationals not closed in $\mathbf{R}$ because its complement the set of irrationals is not open in $\mathbf{R}$. This is because there is a rational between any two irrationals. Observe that the set Z of integers *is closed in R.*

Remark 1 : The words open set and closed set are not opposites like open door and closed door. For example $\mathbf{R}$ and ϕ are both open and closed. In fact, these are the only sets with this property. The set of rationals is neither closed nor open.

Theorem 2 :

(i) The intersection of two open sets is an open set

(ii) The union of any collection of open sets is an open set.

Proof : (i) Let A and B be two open sets in $\mathbf{R}$. let $x \in A \cap B$. $x \in A$ and A is an open set $\Rightarrow$ there is $\in_1 > 0$ such that $N(\in_1, x) \subset A$. Similarly, $x \in B$ and B is an open set $\Rightarrow$ there is $\in_2 > 0$ such that $N(\in_2, x) \subset B$. If $\in = \min(\in_1, \in_2)$, then $N(\in, x) \subset A \cap B$. This means that any $x \in A \cap B$ is an interior point of $A \cap B$. Thus $A \cap B$ is an open set.

(ii) Let A be a collection of open sets. Then consider $X = \cup \{A \mid A \in \mathcal{A}\}$. If $x \in X$, then there exists an open set $A \in \mathcal{A}$ with $x \in A$. Therefore, there exists $\in > 0$, such that $N(\in, x) \subset A$. But this implies that $N(\in, x) \subset X$ and hence X is open.

Remark 2 : The intersection of any **Finite** number of open sets is open. But if the constraint of "Finite" is relaxed the statement is not true. That is, for an arbitrary number of open sets, their intersection need not be an open set. Consider $A_n = \left(-\frac{1}{n}, \frac{1}{n}\right)$, $n \in N$. Then each A_n is an open set. But $\bigcap_{n \in N} A_n = \{0\}$, the set consisting of the singleton element zero. This means $\bigcap_{n \in N} A_n$ is not open though each of A_n is open.

Theorem 3 :

If a set A is both open and closed, then $A = \phi$ or $A = \mathbf{R}$. (This means that ϕ and $\mathbf{R}$ are the only subsets which are both open and closed in $\mathbf{R}$).

Proof : Suppose $A \neq \phi$, $A \neq \mathbf{R}$ and A is open. It is enough to show that $\mathbf{R} - A$ is not open. Since $A \neq \phi$, $A \neq \mathbf{R}$ and A is open, there exist a and b in $\mathbf{R}$ such that $a \in A$ and $b \notin A$. Let $a < b$ and consider the set $B = A \cap [a, b)$. Let α = l.u.b B. We shall first show that $\alpha \notin A$. If possible let $\alpha \in A$. Then $\alpha \neq b$ and hence $\alpha < b$. Further $\alpha \in A$, A is open implies that there exists $\in > 0$, such that $(\alpha - \in, \alpha + \in) \subset A$. Since $\alpha < b$, we can choose $0 < \in_1 < \in$ such that $\alpha + \in_1 < b$. Then $\alpha + \in_1$ belongs to B, a contradiction to the fact that α is the l.u.b of B. Therefore our assumption that $\alpha \in A$ is wrong. Thus $\alpha \notin A$ or $\alpha \in \mathbf{R} - A$.

Since α = l.u.b of B, for any $\alpha > 0$, there exists $x \in B \subset A$, such that $\alpha - \in < x \leq \alpha$. Since $\alpha \notin A$, we have that $\alpha - \in < x < \alpha$. But $\in > 0$. This means $(\alpha - \in, \alpha) \cap A \neq \phi$. That is $N(\in, \alpha) \not\subset \mathbf{R} - A$ for any $\in > 0$. Therefore α is not an interior point of $\mathbf{R} - A$ and hence $\mathbf{R} - A$ is not open.

If $a > b$, we take $B = [b, a) \cap A$.

Theorem 4 :

Any non empty open subset of R is a union of countable collection of disjoint open sets.

Proof : Let A be a nonempty open set. If $x \in A$, there exists a neighbourhood of x contained in A. Let C be the collection of all open intervals containing x and contained in A. Let I_x be the union of all open intervals in C.

(i) I_x is an open interval. First of all I_x is an open set by theorem 2 of this unit. To show that I_x is an open interval we have to show that if $p, q \in I_x$, $p < q$ and $p < r < q$ then $r \in I_x$. To prove this, we observe that if $p, q \in I_x$ then there exist $I_1, I_2 \in C$ such that $p \in I_1$ and $q \in I_2$. Let $p < q$. Notice that $x \in I_1, I_2$. Let $r \in \mathbb{R}$, and $p < r < q$. Then $r \leq x$ or $r > x$. If $r \leq x$, then $p < r \leq x$. This implies that $r \in I_1 \subset I_x$. If $r > x$, then $x < r < q$ and $r \in I_2 \subset I_x$. Thus $p < r < q \Rightarrow r \in I_x$ and I_x is an open interval.

(ii) $y \in I_x \Rightarrow I_x = I_y$. To prove this let $y \in I_x$. This implies that there exists $I_1 \in C$ such that $y \in I_1$. Hence $I_1 \subset I_y$ and $x \in I_y$. Thus $y \in I_x \Rightarrow I_x \subseteq I_y$. But $y \in I_x \Rightarrow x \in I_y \Rightarrow I_y \subseteq I_x$. Thus $I_x = I_y$.

(iii) $x, y \in A, x \neq y \Rightarrow I_x \cap I_y = \phi$ or $I_x = I_y$. To prove this let $I_x \cap I_y \neq \phi$. Let $z \in I_x \cap I_y$. Then $z \in I_x$ and $z \in I_y$. That is $I_z = I_x$; $I_z = I_y \Rightarrow I_x = I_y$.

(iv) Let $D = \{ I_x \mid x \in A \}$. Then D is countable. Take any rational number $r_x \in I_x$.

Now $I_x, I_y \in D \Rightarrow I_x \cap I_y = \phi$ or $I_x = I_y$. If $I_x = I_y$, take $r_x = r_y$. If $I_x \cap I_y = \phi$ take $r_x \neq r_y$. Then the set of all such $r_x = \{ r_x \mid x \in A \}$ is similar (equivalent) to D and is contained in Q, the set of rationals which is countable. Then D is countable.

Theorem 5 :

(i) The union of two closed sets is a closed set.

(ii) The intersection of any collection of closed sets is a closed set.

Proof : (i) Suppose B_1 and B_2 are closed sets. Then their complements to $B_1' = \mathbb{R} - B_1$ and $B_2' = \mathbb{R} - B_2$ are open. By theorem 2, $(B_1' \cap B_2')$ is an open set. This means $(B_1' \cap B_2')' = B_1 \cup B_2$ is a closed set.

(ii) Let B be a collection of closed sets. Then by theorem 2, $\cup \{ B' \mid B \in B \} = \mathbb{R} - \cap \{ B \mid B \in B \}$ is open. Hence $\cap \{ B \mid B \in B \}$ is a closed set.

SAQ 1 Let A be a closed aggregate (subset of real numbers). If M = l.u.b of A, then $M \in A$. If m = g.l.b of A, $m \in A$.

13.4 LIMIT POINT OF AN AGGREGATE

Definition 4 :

A point $a \in \mathbb{R}$ is called a *limit point* of an aggregate A, if every neighbourhood of a contains a point of A other than a itself.

Equivalently, a real numer 'a' is a limit point of a set $A \subset \mathbb{R}$, if every neighbourhood of 'a' contains an infinite number of members of A. This means that for every neighbourhood N of a, $N \cap A$ is an infinite set. Some authors use the terms 'accumulation point', 'condensation point' or a 'cluster point' for limit point.

Remark 3 : A limit point of an aggregate may or may not be a member of the set. A finite set can not have a limit point. An infinite set may have a unique point or many limit points or no limit point.

Definition 5 :

The set of all limit points of an aggregate A is called the derived set of A and is denoted A′; $A' = \{x \in \mathbb{R} \mid x \text{ is a limit point of } A\}$.

Example 6 : The empty set, a finite set and Z, the set of integers do not have limit points.

Example 7 : The set $\left\{\frac{1}{n} \mid n \in N\right\}$ has only one limit point 0. This limit point is not a member of the set. No point of the set is a limit point of the set.

Example 8 : Every point of $\mathbb{R}$ is a limit point because every neighbourhood of each of its points has an infinite number of members of the set. Thus $\mathbb{R}' = \mathbb{R}$.

Example 9 : Every real number of Q, the set of rationals, is a limit point of Q. That is $Q' = \mathbb{R}$. To see this we observe that between any two rational numbers, there exist an infinite number of rationals. But there are also infinite number of rational numbers between any two irrational numbers. Thus every irrational number is a limit point of Q. Thus every real number is a limit point of Q.

SAQ 2 What are the derived sets of $[a, b]$, (a, b) ?

Theorem. 6:

An aggregate A is closed if and only if the derived set A′ is a subset of A.

Proof : Suppose A is a closed aggregate. If $A' = \phi$ then the theorem is trivially true. If $A' \neq \phi$, let $\alpha \in A'$. Then $\alpha \in A$. To prove this, let if possible, $\alpha \notin A$. Then $\alpha \in \mathbb{R} - A$, which is an open set. This implies that there exists $\epsilon > 0$, such that $N(\epsilon, \alpha) \subset \mathbb{R} - A$. This implies that $N(\epsilon, \alpha) \cap A = \phi$ and this means that α is not a limit point of A. Hence our assumption that $\alpha \notin A$ is wrong. Thus $\alpha \in A' \Rightarrow \alpha \in A$ or $A' \subset A$.

Conversely, suppose $A' \subset A$. To show that $\mathbb{R} - A$ is open we suppose that $\alpha \in \mathbb{R} - A$. This implies that $\alpha \notin A$. But $A' \subset A \Rightarrow \alpha \notin A'$. Therefore there exists $\epsilon > 0$ such that $N(\epsilon, \alpha) \cap A - \{\alpha\} = \phi$. But $\alpha \notin A$. Therefore $N(\epsilon, \alpha) \cap A = \phi \Rightarrow N(\epsilon, \alpha) \subset \mathbb{R} - A$. Thus $\mathbb{R} - A$ is open or A is closed.

Definition 6 :

Let A be an aggregate. The *closure of* A is defined to be the union of A and A′. The closure of A is denoted of $\overline{A}$. Thus $\overline{A} = A \cup A'$. If A is closed then $A' \subset A$ and in this case $\overline{A} = A$. Equivalently, an aggregate A is defined to be closed if $\overline{A} = A$.

Theorem 7 : (Bolzano and Weierstrass) :

Every bounded infinite aggregate has a limit point.

Proof : Suppose A is a bounded infinite aggregate. Let 'a' be the lower bound and 'b' the upper bound. Consider the set $S = \{x \in \mathbb{R} \mid (-\infty, x) \cap A \text{ is at the most finite}\}$. Since a is a lower bound of A, $(-\infty, a) \cap A$ is empty. This implies that $a \in S$ and S is an aggregate. $x > b$ implies that $(-\infty, x) \cap A = A$, an infinite set and $x \notin S$. Thus $x \in S \Rightarrow x \leq b$ and b is an upper bound of S. Therefore the l.u.b of S exists. Let c = l.u.b of S. Then for $\epsilon > 0$, there exists $x \in S$, such that $-c - \epsilon < x \leq c$. Then $(-\infty, c - \epsilon) \cap A \subset (-\infty, x) \cap A$.

But $(-\infty, x) \cap A$ is at the most finite because $x \in S$. Therefore $(-\infty, c - \epsilon) \cap A$ is at the most finite. Further c = l.u.b of $S \Rightarrow c + \epsilon \notin S$. Therefore $(-\infty, c + \epsilon) \cap A$ is infinite. Now

$(c-\epsilon, c+\epsilon) \cap A = (-\infty, c+\epsilon) \cap A - (-\infty, c-\epsilon) \cap A$ is an infinite set for every $\epsilon > 0$. Hence c is a limit point of A.

Remark 4 : If $T = \{x \in \mathbf{R} \mid (x, \infty) \cap A$ is at the most finite$\}$, then it can be proved that T is bounded below and the g.l.b of T is a limit point of A.

Remark 5 : The conditions stated in the Bolzano and Weierstrass theorem are only sufficient conditions. A set may be unbounded set but still can have a limit point. For example **R** and Q are unbounded and have infinitely many limit points.

Theorem 8 :

A bounded infinite aggregate has lower and upper limit points.

Proof : Let A be a bounded infinite aggregate. Define

$S = \{x \in \mathbf{R} \mid (-\infty, x) \cap A$ is at the most finite$\}$. Let c = l.u.b of S. Then c is a limit point of A and $c \in A'$, the derived set of A. If $x < c$, it is possible to choose $y \in S$ such that $x < y \leq c$. Now $y \in S \Rightarrow (-\infty, y) \cap A$ is at the most a finite set. Since $x < y$, we can choose $\epsilon > 0$ such that $(x-\epsilon, x+\epsilon) \subset (-\infty, y)$. Then $N(\epsilon, x) \cap A = (x-\epsilon, x+\epsilon) \cap A \subset (-\infty, y) \cap A$ which at the most a finite set. Therefore $N(\epsilon, x) \cap A$ is a finite set. Thus x which is less than c is not a limit point of A. That is $x \notin A'$ and hence c is the least element of A'. Similarly it can be proved that d = g.l.b of $\{x \in \mathbf{R} \mid (x, \infty) \cap A$ is at the most finite$\}$ then d is the greatest element of A'.

Definition 7 :

The set of all interior points of a set A is called the interior of A and is denoted by A^i.

SAQ 3 What is the interior of Q and closure of Q ?

13.5 WORKED OUT EXERCISES

Exercise. 1 : Show that the interior of a set A is an open set and is the largest open subset of A.

Ans : Let A be a given set. Let A^i denote the interior of A. That is A^i is the set of all interior points of A. If $A^i = \phi$, then A^i is open because ϕ is an open set. If $A^i \neq \phi$, let $x \in A^i$. Since x is an interior point of A, there exists an open interval I_x such that $x \in I_x \subset A$. But I_x being an open interval is a neighbourhood of each of its points. This implies that every point of I_x is an interior point of I_x. But $I_x \subset A$. Hence every point of I_x is an interior point of A. Thus $x \in I_x \subset A^i \Rightarrow A^i$ is an open set.

To show that A^i is the largest open set, it is required to prove that A^i contains every open set of A. Let A_1 be any open set of A. Let $x \in A_1$. Since an open set is a neighbourhood of each of its points, A_1 is a neighbourhood of x. But $A_1 \subset A$ and hence A is also a neighbourhood of x. This implies that x is an interiorpoint of A or $x \in A^i$. Thus $x \in A_1 \Rightarrow x \in A^i$ and hence $A_1 \subset A^i$. Since every open subset of A is contained in A^i, A^i is the largest open subset of A.

Exercise 2 : Let S and T be aggregates and S′ and T′ denote the derived sets of S and T. Then

(i) $S \subset T \Rightarrow S' \subset T'$,

(ii) $(S \cup T)' = S' \cup T'$ and

(iii) $(S \cap T)' \subset S' \cap T'$

Ans : (i) If $S' = \phi$ $S' \subset T'$. If then $S' \neq \phi$, let $x \in S'$. Then $N(\epsilon, x)$ contains an infinite number of members of S. But $S \subset T \Rightarrow$ that $N(\epsilon, x)$ contains an infinite number of members of T. This implies that x is a limit point of T or $x \in T'$. Thus $x \in S' \Rightarrow x \in T'$ and hence $S' \subset T'$.

(ii) $S \subset S \cup T \Rightarrow S' \subset (S \cup T)'$ and $T \subset S \cup T \Rightarrow T' \subset (S \cup T)'$. Thus $S' \cup T' \subset (S \cup T)'$.

To show that $(S \cup T)' \subset S' \cup T'$ we first consider the case $(S \cup T)' = \phi$. Then $(S \cup T)' \subset S' \cup T'$ trivially. If $(S \cup T)' \neq \phi$, let $x \in (S \cup T)'$. Now since x is a limit point of $S \cup T$, every neighbourhood of x contains an infinite number of points of $S \cup T$. This implies that every neighbourhood of x contains infinitely many points of S or of T or of both. This means that x is a limit point of S or a limit of T. That is $x \in S'$ or $x \in T'$ implying $x \in S' \cup T'$. Thus $x \in (S \cup T)' \Rightarrow x \in S' \cup T'$. Since $S' \cup T' \subset (S \cup T)'$ and $(S \cup T)' \subset S' \cup T'$, we conclude that $(S \cup T)' = S' \cup T'$.

(iii) Since

$S \cap T \subset S \Rightarrow (S \cap T)' \subset S'$ and

$S \cap T \subset T \Rightarrow (S \cap T)' \subset T'$ we conclude that $(S \cap T)' \subset S' \cap T'$.

To see that the other inclusion is not correct, let $S = (1, 2)$ and $T = (2, 3)$. Then $S \cap T = \phi$ and $(S \cap T)' = \phi' = \phi$. But $S' = [1, 2]$ and $T' = [2, 3]$ so that $S' \cap T' = \{2\}$ and $(S \cap T)' \not\subset S' \cap T'$.

Exercise 3 : The derived set of a set is a closed set.

Ans : Let A' be the derived set of the set A. We have seen that a set A is closed if and only if $A' \subset A$. Thus to porve that A' is closed we have to show that the derived set of the derived set, that is $(A')'$ is contained in A'. If $(A')' = \phi$, then $(A')' \subset A'$, trivially, and A' is closed. Suppose that $(A')' \neq \phi$. Let $x \in (A')'$. Then x is a limit point of A'. Then every neighbourhood N of x contains at least one point $y \neq x$ of A'. But $y \in A' \Rightarrow y$ is a limit point of A. This means every neighbourhood of y contains infinitely many points of A. But N is one such neighbourhood. Thus every neighbourhood N of x contains infinitely many points of A. This implies that x is a limit point of A. Thus $x \in (A')' \Rightarrow x \in A'$ and hence $(A')' \subset A'$. Thus $(A')'$ is a closed set.

13.6 SUMMARY

The study of analysis rests basically on the understanding the properties of open sets, closed sets and limit points. An open interval is an example of an open set and a closed interval is an example of a closed set. In fact every open set of $\mathbb{R}$ can be characterised as a union of open intervals in $\mathbb{R}$. A closed set is defined as the complement of an open set. It is also possible to study closed sets in their right not just as complements of open sets. For this purpose we have to use limit points. An arbitrary union of open sets in an open set and a finite intersection of open sets is open. Similarly the intersection of an arbitrary collection of closed sets is closed where as a finite union of closed sets is closed. We define a limit point of a set as that point whose every neighbourhood contains an infinite numbers of members of the set. The terms cluster point, accumulation point are also used for a limit point. We proved an important theorem due to Bernard Bolzano (1781 - 1848) and KarlWeiestrass (1815 - 1897) that every bounded infinite set has atleast one limit point.

13.7 MODEL EXAMINATION QUESTIONS

Section A (Long Answer)

i) Define an open set and a closed set. Show that a set is both open and closed if and only if it is either $\mathbb{R}$ or ϕ.

ii) Prove that every non empty open subset of $\mathbb{R}$ is a union of countable collection of disjoint open intervals.

iii) Define a limit point of a set. Show that a bounded infinite aggregate has atleast one limit point.

Section B (Short Answer)

i) Show that the intersection of two open sets in $\mathbb{R}$ is an open set and the union of any collection of open sets is an open set.

ii) Define the derived set of a set. Show that a set A is closed if and only if $A' \subset A$.

iii) Prove that the derived set is a closed set in $\mathbb{R}$.

iv) Let A′ denote the derived set of A. Show that $A \subset B \Rightarrow A' \subset B'$ and $(A \cup B)' = A' \cup B'$ what can be said about $(A \cap B)'$.

13.8 ANSWERS TO SELF ASSESSMENT QUESTIONS

SAQ 1 Suppose M = l.u.b of A. If $M \notin A$, then $M \in A' = \mathbb{R} - A$. Then given $\in > 0$, there exists $x \in A$ such that $M - \in < x \leq M$. Since $M \notin A$, $x < M$ and $x \in A \cap N(\in, M)$, $x \neq M$. That is $N(\in, M) \not\subset \mathbb{R} - A$ and $\mathbb{R} - A$ is not an open set and A is not a closed set. This is a contradiction. Hence $M \notin A$ is wrong. Similarly (ii) can be proved.

SAQ 2 Every point of $[a, b]$ is a limit point and no point not in $[a, b]$ is a limit point. Thus $[a, b]' = [a, b]$. Similarly every point of (a, b) is a limit point and the end points a and b are also limit points. Thus $(a, b)' = [a, b]$.

SAQ 3 Interior of $Q = Q^i = \phi$, the empty set and the closure of $Q = Q \cup Q' = \mathbb{R}$.

BLOCK–4 : SEQUENCES AND SERIES

Unit–14 : Sequences

Unit–15 : Infinite Series - I

Unit–16 : Infinite Series - II

In Block 3, we have introduced the algebraic and geometric properties of real numbers. In this Block we look into properties of real numbers which are more analytic in nature. A sequence is a special kind of function whose domain is N, the set of natural numbers. The study of sequences naturally leads to the study of infinite series which could be viewed as a sequence of partial sums. The questions about convergence of sequences and series form a fundamental area of study in Analysis.

UNIT–14 : SEQUENCES

Contents

14.1 Aims and Objectives

14.2 Introduction

14.3 Sequences and sub sequences

14.4 Limit and convergence

14.5 Monotonic sequences

14.6 Cauchy sequences

14.7 Workedout exercises

14.8 Summary

14.9 Model Examination Questions

14.8 Answers to Self Assessment Questions

14.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to (i) Define the limit of a sequence and a sub sequence (ii) Establish the relation between a convergent sequence and a bounded sequence (iii) Define a monotic sequence and prove that a monotonic sequence is convergent if and only if it is bounded (iv) State and prove Cauchy's general principle of convergence for sequences.

14.2 INTRODUCTION

In our day to day life we come across many examples of sequences. Leonardo Fibonacii (1170 - 1240) gave a model for counting the rabbits in a colony by assuming that a pair of adult rabbits produce a pair of young rabbits every month and the new born rabbits become adults in two months and produce another pair of rabbits. Then the number of pairs of rabbits after first, second, third, ... n^{th} months are given by

1, 1, 2, 3, 4, 5, 8, 13, 21, ...

This is an example of a sequence where the n^{th} term ($n > 2$) is obtained by adding the previous two terms. Consider a rubber (elastic) ball dropped from a height of 'a' mts (say) above a rough horizantal surface. Consider the height reached by the ball on each bounce. These heights can be related to a sequence which ultimately "converges" to zero. If we would like to know the distance travelled by the ball then the resulting infinite series has to converge to be a finite real number. The study of questions related to the existence of a limit of a sequence and the convergence of a sequence are important in the study of coming units.

14.3 SEQUENCES AND SUB SEQUENCES

Definition 1 :

A sequence is a set of numbers presented in an order starting with a first, a second, a third etc. Equivalently, if S is an aggregate (or a set) a sequence in S is a function defined from N to S. It is cunstomary to represent a sequence as

$$x_1, x_2, x_3 \ldots, x_n, \ldots \text{ or}$$

$$f(1), f(2), f(3), \ldots f(n), \ldots$$

We follow the notation $x_1, x_2, x_3 \ldots, x_n, \ldots$ and write the sequence as $\langle x_n \rangle$.

Defintion 2 :

If $\langle x_n \rangle$ is a sequence and if $r_1 < r_2 < r_3 \ldots < r_n, \ldots$ is strictly increasing natural numbers then the sequence $\langle x_{r_n} \rangle = x_{r_1}, x_{r_2}, \ldots$ is called a subsequence of $\langle x_n \rangle$.

A subsequence could be viewed as a composition of two functions. A sequence may have several subsequences.

Remark 1 : The easiest way to define (give) a sequence is to give a formula for the n^{th} term of a sequence and specify for what values of n_1 this formula holds good. Writing a few terms alone is not enough to define a sequence.

Example 1 : Let $x_n = n$, Then the sequence $\langle x_n \rangle$ is $\langle x_n \rangle = 1, 2, 3, 4, 5, \ldots n, \ldots$

Consider a subsequence of the sequence $\langle x_{2n} \rangle$ given by $\langle x_{2n} \rangle = 2, 4, 6, 8, \ldots, 2n, \ldots$

Example 2 : Consider the sequence : 1, –1, 1, –1, –1, ... This sequence can be written as $x_n = (-1)^{n-1}$.

SAQ 1 Write two subsequences of the above sequence.

Example 3 :

$$x_n = \begin{cases} \frac{1}{n} \text{ if } n \text{ is even} \\ -\frac{1}{n} \text{ if } n \text{ is odd} \end{cases} \quad \text{or } x_n = \frac{(-1)^n}{n}$$

$$\langle x_n \rangle = -1, \frac{1}{2}, -\frac{1}{3}, \frac{1}{4}, -\frac{1}{5}, \ldots$$

Example 4 : Fibonacci sequence 1, 1, 2, 3, 5, 8, 13, ...,$x_1 = 1, x_2 = 1, x_n = x_{n-2} + x_{n-1}$ for $n > 2$.

Definition 3 :

If the range of a sequence $\langle a_n \rangle$ is bounded below then the sequence $\langle a_n \rangle$ is said to be bounded below. If the range of a sequence $\langle a_n \rangle$ is bounded above, then the sequence $\langle a_n \rangle$ is said to be bounded above. A sequence is said to be bounded if it is both bounded above and bounded below. Equivalently a sequence $\langle x_n \rangle$ is bounded if there exist finite numbers m and M such that $m < x_n < M$ for every $n \in N$. If the sequence $\langle x_n \rangle$ is bounded above, the least of the upper bounds is called l.u.b or the least upper bound similarly the g.l.b.

Example 5 : Consider the sequence $\langle x_n \rangle$ given by $x_n = \frac{1}{n}$. Here $x_1 = 1$ and $x_n < 1$ for each $n > 1$. Thus the sequence is bounded above and 1 is the l.u.b. If $\delta > 0$, then for $n > \frac{1}{\delta}$, we have $0 < a_n < \delta$. Consequently no positive number is a lower bound for this sequence and 0 is the g.l.b.

Example 6 : For the sequence $\langle x_n \rangle$, where $x_n = \frac{(-1)^n}{n}$, $x_1 = -1$ and $x_2 = \frac{1}{2}$. All the other members of the sequence lie between these two numbers. Hence l.u.b $= \frac{1}{2}$ and g.l.b $= -1$.

Example 7 : For the sequence $\langle x_n \rangle$ given by

$$x_n = \begin{cases} +1, \text{ if } n \text{ is divisible by } 5 \\ 0, \text{ other wise} \end{cases}$$

each term of the sequence is either 1 or zero. Hence l.u.b is 1 and g.l.b is 0.

Example 8 : For the sequence $\langle x_n \rangle$ where $x_n = \sqrt{n} + (-1)^n$, $x_1 = 0$ and all the other terms are positive. Hence g.l.b. is 0. The sequence is not bounded above, since for any given $\delta > 0$, we can choose $n > (\delta + 1)^2$ to obtain $a_n = \sqrt{n} + (-1)^n \geq \sqrt{n} - 1 > \delta$.

SAQ 2 Find l.u.b and g.l.b if they exist for the sequence $\langle x_n \rangle$ where

$$x_n = \begin{cases} 0 \text{ if } n < 100 \\ 1 \text{ if } 100 \leq n < 1000 \\ 2 \text{ if } 1000 \leq n \end{cases}$$

14.4 LIMIT AND CONVERGENCE

Definition 4 :

A real number l is said to be a limit point of a sequence $\langle x_n \rangle$ if every neighbourhood of l contains an infinite number of members of the sequence. Equivalently l is a limit point of a sequence if for any $\in > 0$, however small, $x_n \in (l - \in, l + \in)$ for infinitely many values of n. We write this as $\lim_{n \to \infty} x_n = l$. A limit point is also called a clustor point or a condensation point. A sequence which is not convergent is said to be divergent.

Some authors differentiate between the case of a sequence which is not bounded and hence diverge to $+\infty$ or $-\infty$ and the case where the sequence has more than one limit point. If a sequence has more than one limit point the sequence is called oscillatory.

Remark 2 : From the defintion of a limit point of a sequence, the limit point is the limit of the range of the sequence and as such is a limit of the set which is the range. But there do exist a subtle difference in the limit of a sequence and the limit of the range set. Consider the sequence $\langle x_n \rangle$ where $x_n = 1$. Then as a sequence $\{1, 1, 1, \ldots\ldots\}$, 1 is the limit point of the seqence $\langle x_n \rangle$. But as a set, the range set is $\{1\}$ and being a finite set (consisting of a singleton element) has no limit point.

Reamrk 3 : Since by the members of a sequence we mean the elements in the range set, all the theorems on the limit points of sets apply to sequences also.

Example 9 : 0 is the limit point of the sequence $\langle x_n \rangle$ where $x_n = \frac{1}{n}$, since each neighbourhood of 0, contains infinitely many terms of the sequence $\frac{1}{n}$.

Example 10 : 1 and –1 are limit points of the sequence $\langle x_n \rangle$ where $x_n = (-1)^n$ because 1 and –1 are repeated infinitely many times and as such every neighbourhood of 1 (and also –1) trivially contain infinitely many 1*s* (and also –1*s*).

Example 11 : The sequence $\langle x_n \rangle$ where $x_n = n$ has no limit points since no real number has infinitely many members of the sequence in any of its neighbourhood.

Theorem 1 : (Bolzano Weierstrass theorem for sequences) :

Every bounded sequence has a limit point.

Proof : Let $\langle x_n \rangle$ be a bounded sequence and let $S = \{ x_n \mid n \in N \}$. Since $\langle x_n \rangle$ is bounded, S is bounded. There are two possibilites (i) Either S is finite set or (ii) S is infinite set.

(i) If S is a finite set then atleast one element of S, say l, is repeated infinite number of times in $\langle x_n \rangle$. This means for any $\epsilon > 0$, however small, the interval $(l - \epsilon, l + \epsilon)$ containing infinite number of values of $\langle x_n \rangle$. Thus l is a limit point of $\langle x_n \rangle$.

(ii) If S is infinite then by Bolzano and Weierstrass theorem for bounded aggregates S has atleast one limit point 'l'. Since l is a limit point of S, every neighbourhood $(l - \epsilon, l + \epsilon)$ of 'l' contains an infinite number of members of S. That is $x_n \in (l - \epsilon, l + \epsilon)$ for infinite values of n. This means that 'l' is a limit point of the sequence.

Remark 4 : A sequence may have no limit point or exactly one (unique) limit point or more than one limit point. The main interest in the study of sequences is the situation when a sequence has a unique limit point. Such sequences are called convergent sequences.

Definition 5 :

A sequence $\langle x_n \rangle$ is said to converge to a limit 'l' if for every $\epsilon > 0$, there exists a positive integer m, depending on ϵ, such that $|x_n - l| < \epsilon$ for all $n \geq m$. This means that except for a finite number of members of the sequence all the other members of the sequence shall be clustered around l.

Theorem 2 :

Every convergent sequence is bounded but not conversely.

Proof : Let $\langle x_n \rangle$ be a sequence, converging to a limit 'l'. Taking $\delta = 1$, we see that there is an integer m such that

$|x_l - l| < 1$ for all $n \geq m$. This means that $l - 1 < x_n < l + 1$ for all $n \geq m$. Let λ and μ are the greatest and the least elements respectively of the finite set $\{ x_1, x_2, \ldots x_{m-1}, l - 1, l + 1 \}$. Then $\mu \leq x_n \leq \lambda$ for all n. Thus the sequence $\langle x_n \rangle$ is bounded.

Consider the sequence $\langle x_n \rangle$ defined by $x_n = (-1)^n$. Then $-1 \leq x_n \leq 1$ for all $n \in N$. Thus $\langle x_n \rangle$ is bounded. But $\langle x_n \rangle$ has more than one limit point and as such $\langle x_n \rangle$ is not convergent, though $\langle x_n \rangle$ is bounded.

Theorem 3 :

If the sequence $\langle x_n \rangle$ converges to l and also to m, then $l = m$.

Proof : Let $\delta > 0$ be given. Since $\langle x_n \rangle$ converges to l, there exists m_1 such that $|x_n - l| < \frac{\delta}{2}$ for all $n \geq m_1$. Since $\langle x_n \rangle$ converges to m, there exists m_2 such that $|x_n - m| < \frac{\delta}{2}$ for all $n \geq m_2$. Then for all $n \geq \max \{m_1, m_2\}$, $|a_n - l| < \frac{\delta}{2}$ and $|a_n - m| < \frac{\delta}{2}$. Then $|l - m| \leq |l - a_n| + |a_n - m| < \frac{\delta}{2} + \frac{\delta}{2} = \delta$. Thus $|l - m|$ is a non negative number which is less than each $\delta > 0$. Hence $|l - m| = 0$ or $l = m$.

Theorem 4 :

A real number l is a limit point of the sequence $\langle a_n \rangle$ if and only if there exists a subsequence $\langle a_{r_n} \rangle$ of $\langle a_n \rangle$ that converges to l.

Proof : Suppose that $\langle a_{r_n} \rangle$ is a subsequence of $\langle a_n \rangle$ and $a_{r_n} \to l$ as $n \to \infty$. Let $\delta > 0$. Then there exist N such that $a_{r_n} \in (l - \delta, l + \delta)$ for all $n \geq N$. Since $r_N < r_{N+1} < r_{N+2} < \ldots$, it follows that the neighbourhood $(l - \delta, l + \delta)$ of l contains infinitely many terms of $\langle a_n \rangle$. Since this is ture for each neighbourhood of l, it follows that l is a limit point of $\langle a_n \rangle$. Conversely, suppose that l is a limit point of $\langle a_n \rangle$. Choose a positive integer r_1 such that $a_{r_1} \in (l - 1, l + 1)$. This is possible since $(l - 1, l + 1)$ contains infinitely many terms. Now choose $r_2 > r_1$ such that $a_{r_2} \in \left(l - \frac{1}{2}, l + \frac{1}{2}\right)$. This is also possible since $\left(l - \frac{1}{2}, l + \frac{1}{2}\right)$ contains infinitely many terms. Continue this process so that $r_1, r_2, \ldots, r_n$ are chosen such that $r_1 < r_2 < \ldots r_n$, and $a_{r_j} \in \left(l - \frac{1}{j}, l + \frac{1}{j}\right)$. Thus we can choose integers $r_1, r_2, \ldots$ so that $r_1 < r_2 < \ldots$ and $|a_{r_n} - l| < \frac{1}{n}$. Thus the subsequence $\langle a_{r_n} \rangle$ converges to l.

Theorem 5 :

Let $\langle a_n \rangle$ and $\langle b_n \rangle$ be sequences such that $\lim_{n \to \infty} a_n = l$ and $\lim_{n \to \infty} b_n = m$. Then

(i) $\lim_{n \to \infty} (a_n + b_n) = l + m$

(ii) $\lim_{n \to \infty} a_n \cdot b_n = l \cdot m$

(iii) If $l \neq 0$, then $\lim_{n \to \infty} \frac{b_n}{a_n} = \frac{m}{l}$

Proof : (i) Let $\delta > 0$ be given. Since $a_n \to l$ as $n \to \infty$ there exists N_1 such that $|a_n - l| < \frac{\delta}{2}$ $\forall n \geq N_1$. Similarly $b_n \to m$ as $n \to \infty$ implies that there exists N_2 such that $|b_n - m| < \frac{\delta}{2}$ $\forall n \geq N_2$. Then for all $n \geq \text{Max}\,(N_1, N_2)$

$$\left|\left(a_n + b_n\right) - (l + m)\right| = \left|\left(a_n - l\right) + \left(b_n - m\right)\right|$$

$$\leq \left|a_n - l\right| + \left|b_n - m\right| < \frac{\delta}{2} + \frac{\delta}{2} = \delta$$

Thus $\left(a_n + b_n\right) \to (l + m)$ as $n \to \infty$.

(ii) Write $a_n b_n = \left(a_n - l\right) b_n + l\left(b_n - m\right) + lm$. Now $a_n \to l$ as $n \to \infty$ implies that $\left(a_n - l\right) \to 0$ as $n \to \infty$. Again since $\langle b_n \rangle$ is bounded. $|b_n| < \lambda$ for all n. Thus $\left(a_n - l\right)b_n \to 0$ as $n \to \infty$. Similarly $\left(b_n - m\right) \to 0$ as $n \to \infty$ and 'l' being a constant, $l\left(b_n - m\right) \to 0$ as $n \to \infty$. Thus

$$\left|a_n b_n - lm\right| = \left|\left(a_n - l\right)b_n + l\left(b_n - m\right)\right|$$

$$\leq \left|\left(a_n - l\right)b_n\right| + \left|l\left(b_n - m\right)\right| \to 0 \text{ as } n \to \infty$$

Thus $a_n b_n \to lm$ as $n \to \infty$.

(iii) This is a special case of (ii) where $c_n = \frac{1}{a_n}$. Now $a_n \to l$ as $n \to \infty$ and $l \neq 0$ implies $\frac{1}{a_n} \to \frac{1}{x}$ an $n \to \infty$. To see this we observe that the sequence $\left\langle \frac{1}{a_n} \right\rangle$ is well defined, because $\left|a_n - l\right| < \frac{|l|}{2}$ for $n \geq$ K (say) and $|a_n| > |l| - \left|\frac{l}{2}\right| = \left|\frac{l}{2}\right| > 0$ for $n \geq$ K.

Now $\left|\frac{1}{a_n} - \frac{1}{l}\right| = \frac{\left|l - a_n\right|}{|a_n|\,|l|} < \frac{2\left|a_n - l\right|}{l^2} < \delta$ by choosing $\left|a_n - l\right| < \frac{1}{2}\delta l^2$ for all $n \geq$ N.

This means that if $a_n \to l$ as $n \to \infty$ then $\frac{1}{a_n} \to \frac{1}{l}$ as $n \to \infty$. Now $\frac{b_n}{a_n} = b_n \cdot \left(\frac{1}{a_n}\right)$ and hence $\frac{b_n}{a_n} \to \frac{m}{l}$ as $m \to \infty$.

Theorem 6 : (Sandwich Theorem)

> If $a_n \leq b_n \leq c_n$ for $n \geq$ K and if $\langle a_n \rangle$ and $\langle c_n \rangle$ coverge to a limit l, then $\langle b_n \rangle$ also converges to l.

Proof : Let $\delta > 0$. Since $a_n \to l$ as $n \to \infty$, there exists N_1 such that $\left|a_n - l\right| < \delta$ for all $n \geq N_1$. Similarly $c_n \to l$ as $n \to \infty$, $\left|c_n - l\right| < \delta$ for all $n \geq N_2$.

Let N = max $\left\{K, N_1, N_2\right\}$. Then for all $n \geq$ N,

$$a_n - l \leq b_n - l \leq c_n - l \text{ and}$$

$$l - c_n \leq l - b_n \leq l - a_n.$$

$$\text{Therefore } \left|b_n - l\right| = \text{Max}\left\{\left(b_n - l\right), \left(l - b_n\right)\right\}$$

$$\leq \text{Max}\left\{\left(c_n - l\right), \left(l - a_n\right)\right\}$$

$$\leq \text{Max}\left\{|c_n - l|,\ |a_n - l|\right\}$$

Thus $|b_n - l| < \delta$ for all $n \geq N$ and hence $b_n \to l$ as $n \to \infty$.

Example 12 : Let $\langle b_n \rangle$ be a sequence where

$$b_n = \frac{1}{(n+1)^2} + \frac{1}{(n+2)^2} + \ldots + \frac{1}{(2n)^2}$$

Then $\langle b_n \rangle$ converges to zero. To see this we define two sequences $\langle a_n \rangle$ and $\langle c_n \rangle$ where

$$a_n = \frac{n}{(2n)^2} = \frac{1}{4n} \text{ and } c_n = \frac{n}{n^2} = \frac{1}{n}.$$

Now $a_n \leq b_n \leq c_n$ and $\lim_{n\to\infty} a_n = 0 = \lim_{n\to\infty} c_n$. Hence by sandwich theorem $\lim_{n\to\infty} b_n = 0$.

SAQ 3 If λ is a positive number, $\frac{1}{n^\lambda} \to 0$ as $n \to \infty$.

Example 13 : If $\lambda > 0$, then $\lambda^{1/n} \to 1$ as $n \to \infty$. We need to consider 3 cases : $\lambda > 1$; $\lambda = 1$ and $\lambda < 1$. Suppose $\lambda > 1$. Put $a_n = \lambda^{1/n} - 1$. Then $a_n > 0$ for $n \geq 1$. But

$a_n = \lambda^{1/n} - 1 \Rightarrow \lambda = (1 + a_n)^n \geq 1 + n.\, a_n$, by binominal theorem. Thus $0 < a_n < \frac{\lambda - 1}{n}$.

By sandwich theorem $a_n \to 0$ as $n \to \infty$, since $\frac{\lambda - 1}{n} \to 0$ as $n \to \infty$. If $\lambda = 1$, then $\lambda^{1/n} = 1$ for all n. If $0 < \lambda < 1$, then $\frac{1}{\lambda} > 1$ and $\frac{1}{\lambda^{1/n}} = \left(\frac{1}{\lambda}\right)^{1/n} \to 1$ as $n \to \infty$ by case (i).

Example 14 : $n^{1/n} \to 1$ as $n \to \infty$. Put $a_n = n^{1/n} - 1$ for each $n \geq 1$. Then clearly $a_n > 0$ for all $n \geq 2$ and $n = (1 + a_n)^n \geq \frac{n(n-1)}{2} a_n^2$ for all $n \geq 2$. Therefore, $0 < a_n \leq \sqrt{\frac{2}{n-1}} \leq \frac{2}{\sqrt{n}}$ for all $n \geq 2$, since $(n - 1) \geq \frac{n}{2}$ for all $n \geq 2$. Thus by Sandwich theorem and example 13, $a_n \to 0$ as $n \to \infty$.

Example 15 : If $\lambda > 1$ and α is a real number then $\frac{n^\alpha}{\lambda^n} \to 0$ as $n \to \infty$. Since $\lambda > 1$, let $\lambda = 1 + p$ and choose a positive integer $K > \alpha$. Then for all $n > 2K$ we have

$$\lambda^n = (1+p)^n > \frac{n(n-1)\ldots(n-K+1)}{K!} p^K, \text{ by binominal theorem.}$$

$$> \frac{p^K}{K!}\left(\frac{n}{2}\right)^K, \text{ since each of } n, n-1, \ldots (n-K+1) \text{ is} > \frac{n}{2}$$

$$= \frac{p^K}{2^K \cdot K!} \cdot n^K$$

$$\text{Thus } 0 < \frac{n^\alpha}{\lambda^n} = \frac{n^K}{\lambda^n} \cdot n^{n-K} < \frac{2^K \cdot K!}{p^K} \cdot n^{\alpha - K}$$

$$= \frac{2^K \cdot K!}{p^K} \cdot \frac{1}{n^{K-\alpha}}$$

Then by Sandwich theorem $\frac{n^\alpha}{\lambda^n} \to 0$ as $n \to \infty$.

SAQ 4 If $|x| < 1$, Show that $x^n \to 0$ as $n \to \infty$.

SAQ 5 If $a_n = \sqrt{n+1} - \sqrt{n}$, show that $a_n \to 0$ as $n \to \infty$.

14.5 MONOTONIC SEQUENCES

Definition 6 :

A sequence $\langle x_n \rangle$ is said to be monotonically increasing if $x_{n+1} \geq x_n$ for all n. A sequence $\langle x_n \rangle$ is said to be monotonically decreasing if $x_{n+1} \leq x_n$ for all n. A sequence is said to be a monotonic sequence if it is either monotonically increasing or monotonically decreasing.

Difinition 7 :

A sequence $\langle x_n \rangle$ is said to be strictly increasing (or strictly decreasing) if $x_{n+1} > x_n$ (or $x_{n+1} < x_n$) for all n.

Remark 5 : We have proved Theorem 2 of this unit that every convergent sequence is bounded but there are bounded sequences which are not convergent. We prove now that if additional condition of monotonicity is added to boundedness the resulting sequence is convergent.

Theorem 6 :

A monotonic sequence is convergent if and only if it is bounded.

Proof : We prove the theorem for monotonically increasing sequence. For a monotonically decreasing sequence, a similar proof holds good. Let $\langle a_n \rangle$ be a monotonically increasing sequence. If $\langle a_n \rangle$ is convergent then it is bounded by theorem 2 of this unit.

Conversely suppose $\langle a_n \rangle$ is bounded. Let λ be its l.u.b. Let $\delta > 0$. Since λ is the l.u.b of $\langle a_n \rangle$, we conclude that $\lambda - \delta$ is not an upper bound of the sequence. Hence there exists an N such that $a_N > \lambda - \delta$. Since $\langle a_n \rangle$ is monotonically increasing, $a_n \geq a_N$ for all $n \geq N$. Therefore $\lambda - \delta < a_N \leq a_n \leq \lambda < \lambda + \delta$, for all $n \geq N$. Hence $a_n \to \lambda$ as $n \to \infty$.

A similar argument shows that a bounded and monotonically decreasing sequence converges to its g.l.b.

Remark 6 : Every monotonically increasing sequence which is not bounded above, diverges to $+\infty$.

Example 16 : The sequence $\langle a_n \rangle$ given by $a_n = \left(1 + \frac{1}{n}\right)^n$ is a convergent sequence. To see this, we expand $\left(1 + \frac{1}{n}\right)^n$ by using binominal theorem for $n \geq 2$.

$$\left(1 + \frac{1}{n}\right)^n = \sum_{K=0}^{\infty} \frac{n(n-1)\ldots(n-K+1)}{K!} \cdot \frac{1}{n^K}$$

$$= 1 + 1 + \sum_{K=2}^{n} \frac{1}{K!}\left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right)\ldots\left(1 - \frac{K-1}{n}\right)$$

$$< 1 + 1 + \sum_{K=2}^{n} \frac{1}{K!}\left(1 - \frac{1}{n+1}\right)\left(1 - \frac{2}{n+1}\right)\cdots\left(1 - \frac{K-1}{n+1}\right)$$

$$\left(\text{because } 1 - \frac{r}{n} < 1 - \frac{r}{n+1}\right)$$

$$\leq 1 + 1 + \sum_{K=2}^{n+1} \frac{1}{K!}\left(1 - \frac{1}{n+1}\right)\cdots\left(1 - \frac{K-1}{n+1}\right)$$

$$= \left(1 + \frac{1}{n+1}\right)^{n+1}$$

Thus $\langle a_n \rangle$ is an increasing sequence (clearly $a_1 < a_2$)

But

$$2 < \left(1 + \frac{1}{n}\right)^n = 1 + 1 + \sum_{K=2}^{n} \frac{1}{K!}\left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right)\cdots\left(1 - \frac{K-1}{n}\right)$$

$$< 1 + 1 + \sum_{K=2}^{n} \frac{1}{K!}$$

$$< 1 + 1 + \frac{1}{2} + \frac{1}{2^2} + \ldots + \frac{1}{2^{K-1}}$$

$$< 3$$

for all $n \geq 2$ and $a_1 = 2 < 3$.

Thus $\langle a_n \rangle$ is a bounded and monotonically increasing sequence and hence is convergent.

$\lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n$ is denoted by 'e' (the exponential).

14.6 CAUCHY'S SEQUENCES

Theorem 7 : (Cauchy's first theorem) :

If $a_n \to l$ as $n \to \infty$ and $b_n = \frac{a_1 + a_2 + \ldots a_n}{n}$, then $b_n \to l$ as $n \to \infty$.

Proof : $b_n - l = \frac{(a_1 - l) + (a_2 - l) + \ldots + (a_n - l)}{n}$. We are required to show that $b_n - l \to 0$ as $n \to \infty$. Without loss of generality we can assume $l = 0$. Let $\delta > 0$. Since $\langle a_n \rangle$ is convergent, $\langle a_n \rangle$ is bounded. There exists $\lambda > 0$ such that $|a_n| < \lambda$, for all n. Also since $a_n \to 0$ as $n \to \infty$, there exists M such that $|a_n| < \frac{\delta}{2}$ for all $n \geq M$.

Put $N = \frac{2\lambda M}{\delta}$. Then for all $n \geq N$, we have

$$|b_n| = \frac{|a_1 + a_2 + \ldots a_n|}{n} \leq \frac{|a_1| + |a_2| + \ldots |a_M|}{n} + \frac{|a_{M+1}| + \ldots + |a_n|}{n}$$

$$< \frac{M\lambda}{n} + \frac{(n - M)\delta}{2n} < \frac{\delta}{2} + \frac{\delta}{2} = \delta.$$

Hence $b_n \to 0$ as $n \to \infty$.

Theorem 8 :

If each a_n is positive and $a_n \to l$ as $n \to \infty$ then $b_n = \left(a_1 a_2 \ldots a_n\right)^{1/n} \to l$ as $n \to \infty$.

Proof : (i) Suppose $l = 0$. Then from the fact that G.M ≤ A. M, we have

$$0 < \left(a_1 a_2 \ldots a_n\right)^{1/n} \leq \frac{a_1 + a_2 + \ldots + a_n}{n}$$

Applying the same argument to $\langle 1/a_n \rangle$ we get

$$0 < \frac{1}{\left(a_1 \ldots a_n\right)^{1/n}} \leq \frac{\frac{1}{a_1} + \ldots + \frac{1}{a_n}}{n}$$

This means $\frac{n}{\frac{1}{a_1} + \ldots + \frac{1}{a_n}} \leq \left(a_1 \ldots a_n\right)^{1/n} \leq \frac{a_1 + \ldots + a_n}{n}$

Using Cauchy's first theorem and Sandwich theorem we conclude that $\left(a_1 \ldots a_n\right)^{1/n} \to l$ as $n \to \infty$.

Remark 7 : If $a_n \to \infty$ as $n \to \infty$ then $\left(a_1 \ldots a_n\right)^{1/n} \to \infty$ as $n \to \infty$.

SAQ 6 If each $a_n > 0$ and $\frac{a_{n+1}}{a_n} \to l$ as $n \to \infty$ S.T. $\left(a_n^{1/n}\right) \to l$ as $n \to \infty$.

Definition 8 :

A sequence $\langle a_n \rangle$ is called a Cauchy sequence if and only if to each $\delta > 0$ corresponds an N such that $|a_m - a_n| < \delta$, for all m and $n \geq N$.

Theorem 9 :

If a subsequence of a Cauchy sequence $\langle a_n \rangle$ is convergent then $\langle a_n \rangle$ also is convergent.

Proof : Suppose that $\langle a_{r_n} \rangle$ is a subsequence of $\langle a_n \rangle$ that $\langle a_n \rangle$, is Cauchy and that $\langle a_{r_n} \rangle$ converges to l as $n \to \infty$. Let $\delta > 0$. Since $\langle a_{r_n} \rangle \to l$ as $n \to \infty$, there exists M such that $|a_{r_n} - l| < \frac{\delta}{2}$ for all $n \geq M$. Since $\langle a_n \rangle$ is Cauchy, there exists T such that $|a_m - a_n| < \frac{\delta}{2}$, for each $m, n \geq T$. Put N = Max {M, T}. If $n \geq N$, then since $n \geq M$ we have $|a_{r_n} - l| < \frac{\delta}{2}$ and since $r_n \geq n \geq T$ we have $|a_n - a_{r_n}| < \frac{\delta}{2}$ so that $|a_n - l| < \delta$. Hence $a_n \to l$ as $n \to \infty$.

Theorem 10 : (Cauchy's general principle) :

A real sequence is convergent if and only if it is a Cauchy sequence.

Proof : Suppose $a_n \to l$ as $n \to \infty$. Let $\delta > 0$, then there exists N such that $|a_n - l| < \frac{\delta}{2}$, for all $n \geq N$. Hence for all m and $n \geq N$, we have

$$|a_m - a_n| \leq |a_m - l| + |l - a_n| < \frac{\delta}{2} + \frac{\delta}{2} = \delta.$$

Thus every convergent sequence is a cauchy sequence. Conversely, suppose $\langle a_n \rangle$ is a real cauchy sequence. Without loss of generality let $\delta = 1$. Then there exists a K such that $|a_m - a_n| < 1$ for all $m, n \geq K$. In particular $|a_n - a_K| < 1$ for all $n \geq K$ or $a_K - 1 < a_n < a_K + 1$ for all $n \geq K$. Let λ and μ be the least and the greatest members of the set.

$$\{a_1, \ldots a_{K-1}, a_K - 1, a_K + 1\}$$

Then $\lambda \leq a_n \leq \mu$ for every n. Hence $\langle a_n \rangle$ is bounded. This means that $\langle a_n \rangle$ has a limit point, say l. Then $\langle a_n \rangle$ has a subsequence $\langle a_{r_n} \rangle$ such that $a_{r_n} \to l$ as $n \to \infty$. Then by theorem 9, $\langle a_n \rangle$ is convergent.

14.7 WORKED OUT EXERCISES

Exercise 1 : Let $a_n = \frac{1}{\sqrt{n^2+1}} + \frac{1}{\sqrt{n^2+2}} + \ldots + \frac{1}{\sqrt{n^2+n}}$, $n \geq 1$. Show that $a_n \to 1$ as $n \to \infty$.

Ans : Since $\frac{1}{\sqrt{n^2+1}} \geq \frac{1}{\sqrt{n^2+k}} \geq \frac{1}{\sqrt{n^2+n}}$ for $1 \leq k \leq n$,

we have $\frac{n}{\sqrt{n^2+1}} \geq a_n \geq \frac{n}{\sqrt{n^2+n}}$

Therefore $\frac{1}{\sqrt{1+\frac{1}{n}}} \leq a_n \leq \frac{1}{\sqrt{1+\frac{1}{n^2}}}$

This is because $1 < \sqrt{1+\frac{1}{n}} < 1 + \frac{1}{2n}$

Now $\sqrt{1+\frac{1}{n}} \to 1$ as $n \to \infty$ and $\sqrt{1+\frac{1}{n^2}} \to 1$ and $n \to \infty$.

By Sandwich theorem $a_n \to 1$ as $a_n \to \infty$.

Exercise 2 : Let $\alpha > 0$ and β be a real number $> \sqrt{\alpha}$. Let the sequence $\langle \alpha_n \rangle$ be defined by $\alpha_1 = \beta$ and $\alpha_{n+1} = \frac{1}{2}\left(a_n + \frac{\alpha}{a_n}\right)$ for all $n > 1$. Prove that $\langle a_n \rangle$ is decreasing sequence converging to $\sqrt{\alpha}$.

Ans : From the recurrence relation we obtain $2\, a_n\, a_{n+1} = a_n^2 + \alpha = 2\, a_n^2 + \alpha - a_n^2$.

Therefore $a_n^2 - \alpha = 2\, a_n \left(a_n - a_{n+1}\right)$,

That is $a_n - a_{n+1} = \frac{a_n^2 - \alpha}{2a_n} = \frac{\left(a_n - \sqrt{\alpha}\right)\left(a_n + \sqrt{\alpha}\right)}{2a_n}$

Since $a_1 > \sqrt{\alpha}$, it follows from induction $a_n > \sqrt{\alpha}$. But this imples $\frac{a_n + \sqrt{\alpha}}{2a_n} < 1$.

This inturn implies that

$a_n - a_{n+1} < a_n - \sqrt{\alpha} \Rightarrow a_{n+1} > \sqrt{\alpha}$.

Thus $a_{n+1} < a_n$ for all n and $\langle a_n \rangle$ is a decreasing sequence which is bounded below. Further

$$a_{n+1} - \sqrt{\alpha} = \left(a_n - \sqrt{\alpha}\right)\left(a_n - a_{n+1}\right)$$

$$= \left(a_n - \sqrt{\alpha}\right)\left(1 - \frac{a_n + \sqrt{\alpha}}{2a_n}\right)$$

$$< \left(a_n - \sqrt{\alpha}\right)\left(1 - \frac{a_n}{2a_n}\right) < \frac{a_n - \sqrt{\alpha}}{2}$$

By repeated application we get

$$0 < a_n - \sqrt{\alpha} < \frac{a_n - \sqrt{\alpha}}{2^{n-1}}$$

This shows that $a_n \to \sqrt{\alpha}$ as $n \to \infty$.

Remark 7 : This example provides us with a procedure to find an approximate square root of a positive number α. By taking n sufficiently large and computing a_n we get as close an aproximation to $\sqrt{\alpha}$ as needed.

Exercise 3 : If $a_n \to l$ as $n \to \infty$ and $\langle b_n \rangle$ is a subsequence of $\langle a_n \rangle$, then $b_n \to l$ as $n \to \infty$.

Ans : By the definition of a subsequence, there exists a strictly increasing sequence of positive integers $\langle r_n \rangle$ such that $b_n = a_{r_n}$ for each n. Since $r_1 \geq 1$, if follows that $r_n \geq n$ for all n. (This is because by assuming $r_n > n$ we get that $r_{n+1} > r_n \Rightarrow r_{n+1} \geq r_n + 1 \geq n + 1$ by induction). Let $\delta > 0$. Since $a_n \to l$ as $n \to \infty$, there exists N such that $|a_n - l| < \delta$ for all $n \geq N$. Now for $n \geq N$ we have $r_n \geq n \geq N$, and

$$|b_n - l| = |a_n - l| < \delta.$$

Thus $b_n \to l$ as $n \to \infty$.

Remark 8 : This result can be conveniently used to prove that a certain sequence does not converge. If we could exhibit more than one subsequence of a given sequence that converge respectively to more than one limit then the given sequence is not convergent.

SAQ 7 Show that the sequence $\langle a_n \rangle$ given by $a_n = (-1)^n$ is not convergent.

Exercise 4 : Let α and β be distinct real numbers. If $\langle a_n \rangle$ is defined by $a_1 = \alpha$; $a_2 = \beta$ and

$a_{n+2} = \frac{1}{2}\left(a_{n+1} + a_n\right)$ for each $n \geq 1$, then prove that $\langle a_{2n-1} \rangle$ and $\langle a_{2n} \rangle$ are monotonic and they converge to the same limt $\frac{1}{3}(\alpha + 2\beta)$.

Ans : Without loss of generality assume that $\alpha < \beta$. Clearly $a_2 > a_1$. Since $a_3 = \frac{1}{2}(a_2 + a_1)$, we have $a_1 < a_3 < a_2$. Since $a_4 = \frac{1}{2}(a_3 + a_2)$ it follows that $a_3 < a_4 < a_2$ and $a_1 < a_3 < a_4 < a_2$.

Inductively assume that $a_{2n-1} < a_{2n+1} < a_{2n+2} < a_{2n}$. Then $a_{2n+1} < a_{2n+3} < a_{2n+2}$ (because $a_{2n+3} = \frac{1}{2}(a_{2n+2} + a_{2n+1})$) and $a_{2n+3} < a_{2n+4} < a_{2n+2}$ $\left(\because a_{2n+4} = \frac{1}{2}(a_{2n+3} + a_{2n+2})\right)$.

Thus $a_{2n+1} < a_{2n+3} < a_{2n+4} < a_{2n+2}$

Thus (i) $\langle a_{2n-1} \rangle$ is an increasing sequence.

(ii) $\langle a_{2n} \rangle$ is a decreasing sequence

(iii) Each term of $\langle a_{2n-1} \rangle$ is less than each term of $\langle a_{2n} \rangle$.

In particular a_1 is a lower bound and a_2 is an upper bound of both the sequences. Thus $\langle a_{2n} \rangle$ and $\langle a_{2n-1} \rangle$ are monotonic and bounded and hence they are convergent.

Write $\lim_{n\to\infty} a_{2n} = \lambda$ and $\lim_{n\to\infty} a_{2n-1} = \mu$

Also $a_{2n+2} - a_{2n+1} = \frac{1}{2}(a_{2n+1} + a_{2n}) - a_{2n+1}$

$= \frac{1}{2}(a_{2n} - a_{2n+1})$

$= \frac{1}{2}\left\{a_{2n} - \frac{1}{2}(a_{2n} + a_{2n-1})\right\}$

$= \frac{1}{4}(a_{2n} - a_{2n-1})$ for each $n \geq 1$.

Thus taking limits on both sides we see that

$$\lambda - \mu = \frac{1}{4}(\lambda - \mu).$$

This is possible only when $\lambda = \mu$ and $\lim_{n\to\infty} a_n = \lambda$

Now $a_{2n+1} - a_{2n-1} = a_{2n} - a_{2n+1}$, $(\text{since } 2a_{2n+1} = a_{2n} + a_{2n-1})$

$= 2(a_{2n} - a_{2n+2})$

$\left(\text{Since } a_{2n+2} = \frac{1}{2}(a_{2n} + a_{2n+1})\right)$

For each $n \geq 1$ and summing over $n = 1, 2 \ldots k$ we get

$$a_{2k+1} - \alpha = 2(\beta - a_{2k+2})$$

Taking limits on both sides as $k \to \infty$ we get

$$\lambda - \alpha = 2(\beta - \lambda) \text{ or } \lambda = \frac{1}{3}(\alpha + 2\beta).$$

The case $\alpha > \beta$ can be similarly dealt with.

Exercise 5 : If $a_n > 0$, then $a_n \to \infty$ as $n \to \infty$ if and only if $\frac{1}{a_n} \to 0$ as $n \to \infty$.

Ans : Suppose $a_n \to \infty$ as $n \to \infty$. Let $\delta > 0$. Then there exists N such that $a_n > \frac{1}{\delta}$ for all $n \geq N$. This means that $0 < \frac{1}{a_n} < \delta$ for all $n \geq N$. Therefore $\frac{1}{a_n} \to 0$ as $n \to \infty$. Conversely suppose that $\frac{1}{a_n} \to 0$ as $n \to \infty$ and each $a_n > 0$. Let $\delta > 0$. Then there exists N such that $\left|\frac{1}{a_n}\right| < \frac{1}{\delta}$ for all $n \geq N$. That is $0 < \frac{1}{a_n} < \frac{1}{\delta}$ for all $n \geq N$. Therefore $a_n > \delta$ for $n \geq N$. That is $a_n \to \infty$ as $n \to \infty$.

14.8 SUMMARY

A sequence of real numbers is a function whose domain of definition is the set of natural numbers and the range is a subset of real numbers. A real number l is said to be a limit of the sequence $\langle a_n \rangle$ if every neighbourhood of l contains an infinite number of members of the sequence.

A sequence may not have a limit point, or exactly one limit point or more than one limit point. If a sequence has exactly one limit point we say that the sequence converges to that limit. Convergent sequences play an important role in the study of Analysis. Naturally every convergent sequence is bounded though there exist bounded sequences which are not convergent. But bounded monotonic sequences are necessarily convergent. A sequence is called a Cauchy sequence if, except for a finite number of terms, the difference between any two terms of the sequence can be made arbitrarily small. A convergent sequence is a Cauchy sequence and every Cauchy sequence is convergent.

14.9 MODEL EXAMINATION QUESTIONS

SECTION - A (Long Answers)

(i) Define the limit of a sequence and explain its relation to convergence of a sequence. Show that a convergent sequence is bounded. Show that a monotonic sequence which is bounded is convergent.

(ii) Define a Cauchy sequence. Show that a sequence is convergent if and only if it is a Cauchy sequence.

(iii) State and prove Sandwich theorem for convergent sequences. Use this theorem to prove that the sequence $\langle a_n \rangle$ where $a_n = \sqrt{n+1} - \sqrt{n}$ converges to 0.

(iv) Define subsequence of a sequence. Show that if a sequence $\langle a_n \rangle$ is convergent, then each subsequence of $\langle a_n \rangle$ converges to the same limit.

SECTION - B (Short Answers)

(i) If $\langle a_n \rangle$ and $\langle b_n \rangle$ are sequences such that $a_n \to l$ and $b_n \to l$ as $n \to \infty$, then $a_n b_n \to lm$ as $n \to \infty$.

(ii) Let $\langle a_n \rangle$ be a sequence where $a_n = \sum_{k=1}^{n} \frac{1}{\sqrt{n^2 + k}}$. Prove that $\langle a_n \rangle$ converges to 1.

(iii) Show that a monotonic sequence is convergent if and only if it is bounded.

(iv) If $a_n \to l$ as $n \to \infty$, and $b_n = \dfrac{a_1 + a_2 + \ldots + a_n}{n}$ then show that $b_n \to l$ as $n \to \infty$.

(v) If a subsequence of a Cauchy sequence $\langle a_n \rangle$ is convergent show that the sequence $\langle a_n \rangle$ is also convergent.

(vi) If $\langle a_n \rangle$ is a sequence given by $a_n = \left(1 + \dfrac{1}{n}\right)^n$, show that $\langle a_n \rangle$ is convergent.

14.8 ANSWERS TO SAQ'S

SAQ 1 1, 1, 1, ... is one subsequence, –1, –1, ... is another subsequence.

SAQ 2 The range of the sequence consist of 0, 1, and 2 only. Thus g.l.b = 0 = l.u.b. = 2.

SAQ 3 Let $\delta > 0$. For $n > \dfrac{1}{\delta^{1/\lambda}}$ we have $\dfrac{1}{n^\lambda} < \dfrac{1}{\left(\delta^{1/\lambda}\right)^\lambda} = \delta$. Thus choosing $N = \dfrac{1}{\left(\delta^{1/\lambda}\right)} + 1$, we obtain that $\left|\dfrac{1}{n^\lambda}\right| < \delta$ for all $n \geq N$. Thus $\dfrac{1}{n^\lambda} \to 0$ as $n \to \infty$.

SAQ 4 If $x = 0$, $x^n = 0$ for all n. If $x \neq 0$ put $\lambda = \left|\dfrac{1}{x}\right|$ so that $\lambda > 1$. Taking $\alpha = 0$ by example 15, $\dfrac{1}{\lambda^n} \to 0$ as $n \to \infty$.

SAQ 5 For $n \geq 1$; $0 < a_n = \sqrt{n+1} - \sqrt{n} = \dfrac{1}{\sqrt{n+1} + \sqrt{n}} < \dfrac{1}{2\sqrt{n}}$. By Sandwich theorem $a_n \to 0$ as $n \to \infty$.

SAQ 6 We write $a_0 = 1$, $b_n = \dfrac{a_n}{a_{n-1}}$ for each $n \geq 1$. By hypothesis $b_n \to l$ as $n \to \infty$. Since $b_1 = a_1, b_2 = a_1 a_2, \ldots a_n = b_1 \ldots b_n$ and consequently $a_n^{1/n} = \left(b_1 b_2 \ldots b_n\right)^{1/n}$. Conclusion follows from Theorem 8.

SAQ 7 $\langle a_n \rangle$ has two subsequences $\langle a_{2n} \rangle$ and $\langle a_{2n-1} \rangle$

$\langle a_{2n} \rangle = \{a_2, a_4, \ldots\} = \{1, 1, \ldots\}$

$\langle a_{2n-1} \rangle = \{a_1, a_3, \ldots\} = \{-1, -1, \ldots\}$

$a_{2n} \to 1$ as $n \to \infty$ and $a_{2n-1} \to -1$ as $n \to \infty$ as such $\langle a_n \rangle$ is not convergent.

UNIT–15 : INFINITE SERIES (I)

Contents

15.1 Aims and Objectives

15.2 Introduction

15.3 Convergence of an infinite series

15.4 Tests of Convergence of non-negative terms

15.5 Worked out exercises

15.6 Summary

15.7 Model Examination Questions

15.8 Answers to Self Assessment Questions

15.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to (i) distinguish the notions of convergence, absolute convergence and condtional convergence of an infinite series, (ii) state different tests of convergence and decide their suitability for a particular application, (iii) given an infinite series test it for its convergence, (iv) discuss the convergence of series with positive and negative terms.

15.2 INTRODUCTION

Roughly speaking a series is the sum of the terms of a sequence. Thus if $\langle a_n \rangle$ is a sequence then $a_1 + a_2 + \ldots$ or $\sum_{n=1}^{\infty} a_n$ is called an infinite series. We have one example of an infinite series in the Geometric Progression $a + ar + ar^2 + \ldots + ar^{n-1} + \ldots$ where $r < 1$. The summation of an infinite series is always a troublesome process. Consider the following example :

$$S = 1 - 1 + 1 - 1 + 1 - 1 + \ldots$$

Now $S = (1 - 1) + (1 - 1) + (1 - 1) + \ldots = 0$. But

$$S = 1 - (1 - 1 + 1 - 1 + 1 - 1 + \ldots) = 1 - S. \text{ Thus } 2S = 1 \text{ or } S = \frac{1}{2}$$

$$S = 1 - \{(1 - 1) + (1 - 1) + \ldots\} = 1.$$

Thus the sum is three different values, depending on the way we arrange the terms of the series. In fact we have a funny situation where an infinite number of addition of 1's and – 1's will give a sum of $\frac{1}{2}$. This is because the given series does not converge to a unique limit. Whenever we deal with infinite series we come across three distinct situations. An infinite series of the form $\sum_{n=1}^{\infty} u_n$, where u_n's are constants; An infinite series of the form $\sum_{n=1}^{\infty} x_n$ where $x \in \mathbf{R}$, the third one is

a power series $\sum_{n=1}^{\infty} u_n x^n$ where $x \in C$ (complex numbers). Given an infinite series there are several "tests" by which whether given series converges or not. Some of these tests give the "rapidity" by which the series converge.

15.3 CONVERGENCE OF AN INFINITE SERIES

The student is exposed to methods of summation of finite number of terms that follow a definite rule. For example the summation of Arithmatic and Geometric progressions have been studied in lower classes. As a special case when the modulus of common ratio of a Geometric progression is less than one, the sum of infinite number of terms was computed. But the problems of summability of an infinite series has not been attempted in lower classes. The study of infinite series and their convergence formed a core of study in classical mathematics.

Definition. 1 :

Let u_n be defined for all $n \in N$. Define $S_n = u_1 + u_2 + \ldots + u_n = \sum_{k=1}^{n} u_k$. As $n \to \infty$ if $S_n \to l$, a finite limit, then we say that the infinite series $\sum_{n=1}^{\infty} u_n = u_1 + u_2 + \ldots + u_n + \ldots$ converges and equals 'l' as its sum. Otherwise the series is said to diverge.

Equivalently, given a sequence $\langle u_n \rangle$ of real numbers the sequence $\langle s_n \rangle$ defined by $s_n = \sum_{k=1}^{n} u_k = u_1 + \ldots + u_n$ is called a sequence of partial sums of the infinite series $\sum_{n=1}^{\infty} u_n$. If $s_n \to s$ as $n \to \infty$, the series is said to converge to the sum s.

Example. 1 : Consider the infinite geometric series $\sum_{n=1}^{\infty} u_n = 1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \ldots + \frac{1}{2^n} + \ldots$

Recall that $S_n = \frac{a\left(1 - r^n\right)}{(1 - r)}$ is the formula for the sum of a G.P. whose first term is a and common ratio $r < 1$. Thus in this case

$$S_n = \frac{1 \cdot \left(1 - \frac{1}{2^n}\right)}{1 - \frac{1}{2}} = 2\left(1 - \frac{1}{2^n}\right) = 2 - \frac{1}{2^{n-1}}$$

As n increases $\frac{1}{2^{n-1}}$ decreases and hence S_n approaches 2. Let $\in > 0$ be given. Then by choosing n appropriately we can make $|S_n - 2| < \in$. Thus $\lim_{n \to \infty} S_n = 2$. Thus the given series converges to 2.

Example. 2 : Consider the series $\sum_{n=1}^{\infty} \frac{1}{n\,(n+1)}$. Let $u_n = \frac{1}{n\,(n+1)} = \frac{1}{n} - \frac{1}{n+1}$.

Thus $u_1 = 1 - \frac{1}{2}$; $u_2 = \frac{1}{2} - \frac{1}{3}$ etc. Thus

$$S_n = \sum_{k=1}^{n} u_k = \left(1 - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \ldots + \left(\frac{1}{n} - \frac{1}{n+1}\right)$$

$$= 1 - \frac{1}{n+1}.$$

$\lim_{n\to\infty} S_n = 1$. Thus the given series converges to 1.

Example. 3 : The infinite series $\sum_{k=1}^{\infty} u_k$ given by $u_k = k$ is not convergent but diverges to ∞.

Example. 4 : The series $\sum_{n=1}^{\infty} \frac{1}{n}$ is not convergent, though the sequence $\left\langle \frac{1}{n} \right\rangle$ converges to zero. To see that the series $\sum \frac{1}{n}$ diverges we exhibit a subsequence of the sequence $\left\langle \frac{1}{n} \right\rangle$ which is not bounded. Let

$$S_{k_1} = \frac{1}{1} + \frac{1}{2};$$

$$S_{k_2} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = S_{k_1} + \frac{1}{3} + \frac{1}{4} > S_{k_1} + \frac{1}{4} + \frac{1}{4}$$

$$\therefore S_{k_2} > 1 + \frac{1}{2} + \frac{1}{2} = 1 + \frac{2}{2}.$$

Similarly $S_{k_3} > 1 + \frac{3}{2}, \ldots, S_{k_r} > 1 + \frac{r}{2}$.

This means that the sub sequence $\langle S_{k_n} \rangle$ is not bounded and hence is not convergent.

Theorem. 1 :

> Let $\sum_{n=1}^{\infty} a_n$ and $\sum_{n=1}^{\infty} b_n$ be two infinite series converging to l and m respectively. Then for numbers p and q the series $\sum_{n=1}^{\infty} (p\,a_n + q\,b_n)$ converges to $pl + qm$.

Proof : Let $\langle A_n \rangle$, $\langle B_n \rangle$ and $\langle C_n \rangle$ denote the partial sum sequences of $\sum_{n=1}^{\infty} a_n$ and $\sum_{n=1}^{\infty} b_n$ and $\sum_{n=1}^{\infty} (p\,a_n + q\,b_n)$ respectively. Then

$$C_n = \sum_{k=1}^{n} \left(p\, a_k + q\, b_k\right) = p \sum_{k=1}^{n} a_k + q \sum_{k=1}^{n} b_k$$

$$= p\, A_n + q\, B_n.$$

Since $A_n \to l$ and $B_n \to m$ as $n \to \infty$, we get $C_n \to pl + qm$ as $n \to \infty$.

Theorem. 2 :

> If the series $\sum_{n=1}^{\infty} a_n$ is convergent then $a_n \to 0$ as $n \to \infty$.

Proof : Let $\langle s_n \rangle$ denote the partial sum sequence of the given series and write $t_n = s_{n-1}$ for all $n > 1$. If s is the sum of the series, then $s_n \to s$ as $n \to \infty$. Then clearly $t_n \to s$ as $n \to \infty$ since $t_n = s_{n-1}$.

Now $\quad a_n = \left(s_n - s_{n-1}\right) = s_n - t_n$ for all n.

Thus $\lim_{n\to\infty} a_n = \lim_{n\to\infty} \left(s_n - t_n\right) = \lim_{n\to\infty} s_n - \lim_{n\to\infty} t_n$

$$= l - l = 0.$$

Remark. 1 : This theorem is very useful to conclude that a given series is not convergent if its nth term does not tend to zero as $n \to \infty$. The converse of the theorem is not true, because there exist examples of series whose nth term tends to zero but yet the series is not convergent.

Example. 5 : The series $\sum_{n=1}^{\infty} \frac{n}{n+1}$ is not convergent because $a_n = \frac{n}{n+1}$ and

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} \frac{n}{n+1} = \lim_{n\to\infty} \frac{1}{1 + \frac{1}{n}} = 1 \neq 0.$$

Since $a_n \not\to 0$ as $n \to \infty$, $\sum a_n$ is not convergent.

Example. 6 : The series $\sum_{n=1}^{\infty} \frac{1}{n}$ is such that its nth term $a_n = \frac{1}{n} \to 0$ as $n \to \infty$. But the series is not convergent as seen in example. 4.

Theorem. 3 : (Cauchy's General Principle of Convergence) :

> A series $\sum_{n=1}^{\infty} a_n$ is convergent if and only if to each $\delta > 0$, there exists N such that for each $m > n \geq N$, $|a_{n+1} + a_{n+2} + \ldots + a_m| < \delta$.

Proof : Let s_m and s_n denote the partial sums of m terms and n terms respectively of $\sum_{n=1}^{\infty} a_n$. Then $a_{n+1} + a_{n+2} + \ldots + a_m = s_m - s_n$. Now $\sum_{n=1}^{\infty} a_n$ is convergent if and only if $\langle s_n \rangle$ converges. Thus by the Cauchy's general principle of convergence for sequence the theorem is true.

Theorem. 4 : (Pringsheim) :

If the sequence $\langle a_n \rangle$ is a decreasing sequence of positive terms and the series $\sum_{n=1}^{\infty} a_n$ is convergent, then $n\,a_n \to 0$ as $n \to \infty$.

Proof : Let $\delta > 0$. By Cauchy's principle, there exists N such that : $a_{m+1} + \ldots + a_n = \sum_{k=m+1}^{n} a_k < \frac{\delta}{2}$ for all $n > m \geq N$.

If $n > 2N + 1$, then $\frac{n-1}{2} > N$ and $\sum a_k < \frac{\delta}{2}$ where summation is over k and $\frac{n-1}{2} < k \leq n$. But $a_k \geq a_n$ and the number of terms is less than $\frac{n}{2}$. Thus $\sum a_k \geq \frac{n}{2} a_n$. Thus $n\,a_n < \delta$ for all $n > 2N + 1$ or $n\,a_n \to 0$ as $n \to \infty$.

Example. 7 : Let $a_n = \begin{cases} \frac{1}{n}, \text{ if } n = 2^k \text{ for some interger } k \geq 0 \\ 0, \text{ otherwise} \end{cases}$ If $k \geq 0$ observe that $S_{2^k} = \sum_{n=1}^{2^k} a_n$

$= \sum_{j=0}^{k} \frac{1}{2^j} = 2\left(1 - \frac{1}{2^{k+1}}\right)$ and that $S_n = S_{2^k}$ if $2^k \leq n < 2^{k+1}$.

This shows that $\lim_{n\to\infty} S_n = \lim_{k\to\infty} S_{2^k} = 2$. Thus $\sum_{n=1}^{\infty} a_n$ converges although $n\,a_n$ does not tend to 0 as $n \to \infty$. $\left(n\,a_n = 1 \text{ if } n = 2^k\right)$.

Definition. 2 :

An infinite series $\sum_{n=1}^{\infty} a_n$ is said to be absolutely convergent or converges absolutely if the series $\sum_{n=1}^{\infty} |a_n|$ (obtained by taking modulus value of each term of the original series) is convergent. A series which is convergent but is not absolutely convergent is called conditionally convergent series.

Theorem. 5 :

Every absolutely convergent series is convergent.

Proof : Suppose that $\sum_{n=1}^{\infty} a_n$ is absolutely convergent. That is $\sum_{n=1}^{\infty} |a_n|$ is convergent. Let $\delta > 0$. By Cauchy's general principle of convergence there is an N such that $|a_{m+1}| + |a_{m+2}| + \ldots + |a_n| < \delta$, for all $n > m \geq N$.

But $|a_{m+1} + a_{m+2} + \ldots + a_n| \leq |a_{m+1}| + |a_{m+2}| + \ldots + |a_n| < \delta$

Thus $\sum_{n=1}^{\infty} a_n$ converges, by Cauchy's principle.

Example. 8 : The series $\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \ldots$ is convergent though it is not absolutely convergent. To see this consider $\sum_{k=n+1}^{m} \frac{(-1)^{k-1}}{k}$. This can be written as :

$$\sum_{k=n+1}^{m} \frac{(-1)^{k-1}}{k} = \frac{1}{n+1} - \frac{1}{n+2} + \frac{1}{n+3} - \frac{1}{n+4} + \ldots \frac{(-1)^{m-n-1}}{m}$$

$$= \frac{1}{(n+1)(n+2)} + \frac{1}{(n+3)(n+4)} + \ldots$$

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

$$= \frac{1}{n+1} - \frac{1}{n+2} + \frac{1}{n+2} - \frac{1}{n+3} + \ldots$$

$$= \frac{1}{n+1} - \frac{1}{n+p+1} \text{ or } \frac{1}{n+1} - \frac{1}{n+p+1} + \frac{1}{m}$$

(according as $m - n = 2p$ or $m - n = 2p + 1$). Either way this is

$$< \frac{1}{n+1} + \frac{1}{n+1} = \frac{2}{n+1} < \frac{2}{n} \text{ for all } m > n > \frac{2}{\delta}.$$

Hence the series is convergent. But $\sum |a_n| = \sum \frac{1}{n}$ is not convergent as seen in example 4.

15.4 TESTS OF CONVERGENCE OF NON-NEGATIVE TERMS

Given an infinite series there is no universal way to say immediately whether the series is convergent or not. Though there are many tests available to test the convergence of a series an important technique which is most useful is to compare the series with a carefully selected series whose behaviour is known. If $\sum u_n$ is the given series and if $\sum v_n$ is a carefully selected series which is convergent then $\sum u_n$ is convergnet if $u_n \leq v_n$ for each n. Similarly $\sum v_n$ is divergent then $\sum u_n$ is divergent if $u_n \geq v_n$ for each n.

Theorem. 6 : (p – test)

> An infinite series of positive terms $\sum_{n=1}^{\infty} \frac{1}{n^p}$ is convergent if $p > 1$ and is divergent if $p \leq 1$.

Proof : Let S_n denote the partial sum of the first n terms of the series

(i) Let $p > 1$. Then the terms of the given series can be grouped as

$$\frac{1}{1^p} = \frac{1}{1^p}$$

$$\frac{1}{2^p} + \frac{1}{3^p} < \frac{1}{2^p} + \frac{1}{2^p} = \frac{2}{2^p} = \frac{1}{2^{p-1}}$$

$$\frac{1}{4^p}+\frac{1}{5^p}+\frac{1}{6^p}+\frac{1}{7^p} < \frac{1}{4^p}+\frac{1}{4^p}+\frac{1}{4^p}+\frac{1}{4^p} = \frac{4}{4^p} = \frac{1}{4^{p-1}} = \frac{1}{2^{2(p-1)}}$$

$$\frac{1}{8^p}+\frac{1}{9^p}+\ldots+\frac{1}{15^p} < \frac{1}{8^p}+\frac{1}{8^p}+\ldots = \frac{8}{8^p} = \frac{1}{8^{p-1}} = \frac{1}{2^{3(p-1)}}$$

....

....

Thus at each step we take, $1, 2^1, 2^2, 2^3, \ldots, 2^n$, terms. Adding all these terms the left hand side is the sum of 2^n terms. Thus

$$S_{2^n} < 1 + \frac{1}{2^{p-1}} + \frac{1}{2^{2(p-1)}} + \frac{1}{2^{3(p-1)}} + \ldots$$

The right hand side is a Geometric progression whose common ratio is $\frac{1}{2^{p-1}} < 1$ because $p > 1$. Thus the sum of the given series is less than the sum of a convergent series. Thus the given series is convergent if $p > 1$.

(ii) Let $p \leq 1$. Then $\frac{1}{n^p} \geq \frac{1}{n}$. The terms of the given series can be grouped as

$$1+\frac{1}{2^p} \geq 1+\frac{1}{2} > \frac{1}{2}$$

$$\frac{1}{3^p}+\frac{1}{4^p} > \frac{1}{3}+\frac{1}{4} > \frac{1}{4}+\frac{1}{4} = \frac{1}{2}$$

$$\frac{1}{5^p}+\frac{1}{6^p}+\frac{1}{7^p}+\frac{1}{8^p} \geq \frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8} \geq \frac{4}{8} = \frac{1}{2}$$

....

....

After m steps the left hand side is the sum of 2^m terms of the given series and $S_{2^m} > \frac{1}{2}+\frac{1}{2}+\ldots$ m terms. Thus the given series is greater than an unbounded series whose sum diverges to ∞. Thus the given series is divergent.

Remark. 2 : This series $\sum \frac{1}{n^p}$ is a very useful series which will be one of our "carefully selected series whose behavour is known" with which the given series will be compared.

SAQ 1 : Discuss the convergence of $\frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\ldots+\frac{1}{\sqrt{n}}+\ldots$

SAQ 2 : Discuss the convergence of $\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\ldots+\frac{1}{n^2}+\ldots$

Theorem. 7:

> Let $\sum a_n$ and $\sum b_n$ be two series of positive terms. Let K be a positive number independent of n and let m is a positive integer. Then (i) if $a_n \leq K\, b_n$ for all $n \geq m$ and if $\sum b_n$ is convergent then $\sum a_n$ is convergent (ii) If $a_n \geq K\, b_n$ for all $n \geq m$ and $\sum b_n$ is divergent then $\sum a_n$ is divergent.

Proof : Write $s_n = a_1 + a_2 + \ldots + a_n$ and

$$t_n = b_1 + b_2 + \ldots + b_n$$

By hypothesis $0 \le s_n \le t_n$ for every n. If $\sum b_n$ is convergent then $\langle t_n \rangle$ is bounded. If T is an upper bound of the sequence $\langle t_n \rangle$, then $0 \le s_n \le T$ for each n so that $\langle s_n \rangle$ bounded. Thus $\sum a_n$ is convergent. Similarly it $s_n \ge t_n$ for all n and $\sum b_n$ is divergent, then $\langle t_n \rangle$ is not bounded; and consequently s_n is not bounded given that $\sum_{n=1}^{\infty} a_n$ is divergent.

Theorem 8 : (Comparison Test) :

Let $\sum_{n=1} a_n$ and $\sum_{n=1} b_n$ be two infinite series of positive terms such that $\lim_{n\to\infty} \frac{a_n}{b_n} = l$. Then if l is finite non zero number then $\sum a_n$ and $\sum b_n$ both converge or diverge together. Equivalently $\sum_{n=1}^{\infty} a_n$ and $\sum_{n=1}^{\infty} b_n$ act alike. If $l = 0$, then $\sum_{n=1} b_n$ converges, then $\sum_{n=1} a_n$ also converges.

Proof : $\lim_{n\to\infty} \frac{a_n}{b_n} = l$ implies that for a given $\in > 0$, there exists $m \in \mathbb{N}$ such that $l - \in < \frac{a_n}{b_n} < l + \in$ for all $n \ge m$ or $(l - \in)\, b_n < a_n < (l + \in)\, b_n$ for all $n \ge m$. Then by theorem 7, $\sum_{n=1}^{\infty} a_n$ and $\sum_{n=1}^{\infty} b_n$ both converge or diverge together.

If $\lim_{n\to\infty} \frac{a_n}{b_n} = 0$, then for any given $\in > 0$ there exists $m \in \mathbb{N}$ such that $\frac{a_n}{b_n} < \in$ for all $n \ge m$.

That is $a_n < \in b_n$ for all $n \ge m$. Thus if $\sum_{n=1}^{\infty} b_n$ converges then $\sum_{n=1}^{\infty} a_n$ converges.

Remark. 3 : Given an infinite series $\sum a_n$ we choose an appropriate infinite sereis $\sum b_n$ which is of the form of the p – series $\sum \frac{1}{n^p}$ and use Theorem 8 to discuss the behavior of $\sum a_n$ depending on the nature of the limit l. The technique lies in choosing an appropriate $\sum \frac{1}{n^p}$ to compare $\sum a_n$ with. One way would be to examine $\sum a_n$ carefully and choose $\sum b_n$ in such a way that

$$b_n = \frac{\text{highest positive power of } n \text{ in the numerator of } a_n}{\text{highest positive power of } n \text{ in the denominator of } a_n}$$

Example. 9 : Test the convergence of $\sum_{n=1}^{\infty} \frac{\sqrt{n}}{n^2 + 1}$.

Here $a_n = \frac{\sqrt{n}}{n^2 + 1}$. We choose $b_n = \frac{\sqrt{n}}{n^2} = \frac{1}{n^{3/2}}$.

Then $\frac{a_n}{b_n} = \frac{\sqrt{n}}{n^2 + 1} \times \frac{n^{3/2}}{1} = \frac{n^2}{n^2 + 1}$.

$$\lim_{n\to\infty} \frac{a_n}{b_n} = \lim_{n\to\infty} \frac{n^2}{n^2 + 1} = \lim_{n\to\infty} \frac{1}{1 + \frac{1}{n^2}} = 1, \text{ (finite and non zero)}$$

Then by Theorem 8, $\sum a_n$ and $\sum b_n$ act alike. But $\sum b_n = \sum \frac{1}{n^{3/2}}$ where $p = \frac{3}{2} > 1$. Thus $\sum b_n$ is convergent by p – test. Thus $\sum a_n$ is convergent.

SAQ 3 : Discuss the convergence of $\sum_{n=1}^{\infty} \frac{\sqrt{n+1} - \sqrt{n-1}}{n}$.

Theorem. 9 : (Ratio Test)

> Let $\sum a_n$ and $\sum b_n$ be two infinite series of positive terms and let $\frac{a_{n+1}}{a_n} \leq \frac{b_{n+1}}{b_n}$ for all $n \geq N$, for a given N, then if $\sum b_n$ converges then $\sum a_n$ also converges.

Proof : Let $n > N$. Then $0 < \frac{a_{k+1}}{a_k} \leq \frac{b_{k+1}}{b_k}$ implies that for $k = N, N+1, \ldots$ and $(n-1)$ we get a series of in equalities which by multiplying give us $0 < \frac{a_n}{a_N} \leq \frac{b_n}{b_N}$ or $0 < a_n \leq \left(\frac{a_N}{b_N}\right) b_n$ for all $n > N$. The conclusion follows from comparison test.

Theorem. 10 : (Cauchy's root test)

> Let $\sum a_n$ be an infinite series of positive terms. If there is an integer N and a positive $\lambda < 1$ such that $a_n^{1/n} \leq \lambda$ for all $n \geq N$ then $\sum a_n$ converges. If there is an N such that $a_n^{1/n} \geq 1$ for all $n \geq N$, then $\sum a_n$ diverges.

Proof : The hypothesis implies that $0 \leq a_n < \lambda^n$ for all $n \geq N$. Since $\sum_{1}^{\infty} \lambda^n$ being a geometric progression with common ratio less than 1, is convergent. Now $a_n < \lambda^n$ for each n implies that $\sum a_n$ is less than a convergent series and hence is convergent.

Theorem. 11 : (D'Alembert's Ratio Test) :

> Let $\sum a_n$ be an infinite series with positive terms. If there exists an integer N and a positive number $\lambda<1$ such that $\frac{a_{n+1}}{a_n} \leq \lambda$ for all $n \geq N$, then $\sum a_n$ is convergent.
>
> If there exists N such that that $\frac{a_{n+1}}{a_n} \geq 1$ for all $n \geq N$, then $\sum a_n$ is divergent.

Proof : If $0 < \lambda < 1$, then $\sum_{1}^{\infty} \lambda^n$ converges. Applying the ratio test on $\sum_{n=1}^{\infty} a_n$ and $\sum_{n=1}^{\infty} \lambda^n$ we get the required reslt. Since $a_n \geq a_N > 0$ for all $n \geq N$ the sequence $\langle a_n \rangle$ can not converge to zero.

Remark. 3 : The Ratio test due to D'Alembert (1717-1783) can also be stated as follows. Let $\sum_{n=1}^{\infty} a_n$ be a series with positive terms such that $\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = l$. Then $\sum a_n$ converges if $l < 1$ and diverges if $l > 1$. If $l = 1$, then test fails.

Theorem. 12 : (Cauchy's condensation test) :

Suppose that $a_n \geq a_{n+1} \geq 0$ for all n. Then the series $\sum_{n=1}^{\infty} a_n$ and the series $\sum_{k=1}^{\infty} 2^k a_{2^k}$ converge or diverge together.

Proof : Let s_n denote the partial sum $a_1 + a_2 + \ldots + a_n$ and t_k denote the partial sum $a_1 + 2a_2 + 4a_4 + \ldots + 2^k a_{2^k}$. If the second series converges and its sum is t then,

$$s_n = (a_1 + a_2 + \ldots + a_n) \leq a_1 + (a_2 + a_3) + (a_4 + \ldots a_7) + \ldots + (a_{2^k} + \ldots + a_{2^{k+1}-1})$$

where k is so chosen that $n < 2^{k+1}$

$$\leq a_1 + 2a_2 + \ldots + 2^k a_{2^k} = t_k \leq t.$$

Thus $\langle s_n \rangle$ is an increasing sequence which is bounded. Thus the convergence of the second series implies that of the first. On the other hand if the first series converges and has sum s then

$$\begin{aligned} t_k &= a_1 + 2a_2 + \ldots + 2^k a_{2^k} \\ &\leq 2a_1 + 2a_2 + 4a_4 + \ldots + 2^{k+1} a_{2^k} \\ &\leq 2\left\{(a_1 + a_2) + (a_3 + a_4) + \ldots + (a_{2^{k-1}+1} + \ldots + a_{2^k})\right\} \\ &= 2\, s_{2^k} \leq 2s \end{aligned}$$

so that the increasing sequence $\langle t_k \rangle$ is bounded. Thus the convergence of the first implies that of the second.

Remark. 4 : Though several tests have been given here to test an infinite series for its convergence, these tests are neither exhaustive nor answer every type of infinite series that we come across. The theory of infinite series has a rich history and posed challenging problems to mathematicians in the earlier century. Generally speaking, the ratio test and comparison tests are most widely applied tests. Other tests apply in cases when these tests fail. There is absolutely no way to prejudge as to which test applies when. The student shall develop an intuitive skill of picking up the right test for the right series.

15.5. WORKEDOUT EXERCISES

Exercise. (i) : If $\sum_{n=1}^{\infty} a_n$ is a convergent series of non negative terms show that $\sum_{n=1}^{\infty} \frac{\sqrt{a_n}}{n}$ is also convergent.

Ans : Now $0 < \frac{\sqrt{a_n}}{n} = \sqrt{\frac{a_n}{n^2}} \leq a_n + \frac{1}{n^2}$ because $\frac{a_n}{n^2} \leq \left(a_n + \frac{1}{n^2}\right)^2$. But $\sum_{n=1}^{\infty} a_n$ is given to be convergent and $\sum_{n=1}^{\infty} \frac{1}{n^2}$ is convergent by p – test. Thus $\sum_{n=1}^{\infty} \left(a_n + \frac{1}{n^2}\right)$ is convergent. Since $\sum_{n=1}^{\infty} \frac{\sqrt{a_n}}{n}$ is less than a convergent series and hence is convergent.

Exercise. (ii) : If $\sum_{n=1}^{\infty} a_n$ is a series of positive terms then $\sum_{n=1}^{\infty} a_n$ and $\sum_{n=1}^{\infty} \frac{a_n}{1 + a_n}$ converge or diverge together.

Ans : If $\sum_{n=1}^{\infty} \frac{a_n}{1 + a_n}$ is convergent, then by writing $b_n = \frac{a_n}{1 + a_n}$ we observe that $0 < b_n < 1$ and $a_n = \frac{b_n}{1 - b_n}$ for all n. Since $\sum_{n=1}^{\infty} b_n$ is convergent, $b_n \to 0$ as $n \to \infty$. This means there exists N such that $0 < b_n < \frac{1}{2}$ for all $n \geq N$. Thus $1 - b_n > \frac{1}{2}$ for $n \geq N$ and $0 < a_n < 2\, b_n$ for all $n \geq N$ and $\sum_{n=1}^{\infty} a_n$ converges.

If $\sum_{n=1}^{\infty} a_n$ is convergent, then $0 < \frac{a_n}{1 + a_n} < a_n$ for all n and by comparison test $\sum_{n=1}^{\infty} \frac{a_n}{1 + a_n}$ is convergent.

Exercise. (iii) : Discuss the convergence of (a) $\sum_{n=1}^{\infty} \frac{1}{(\log n)^n}$; (b) $\sum_{n=1}^{\infty} \left(\sqrt[n]{n} - \frac{1}{100}\right)^n$;

(c) $\sum_{n=1}^{\infty} \frac{n^q}{p^n}$ where p, q are real numbers and $p > 0$; (d) $\sum_{n=1}^{\infty} \frac{n!}{n^n}$

Ans : (a) Let $a_n = \frac{1}{(\log n)^n}$. Then $a_n^{1/n} = \frac{1}{\log n} < \frac{1}{2}$ for all $n > e^2$. Then by Cauchy's root test the given series in convergent.

(b) Let $a_n = \left(\sqrt[n]{n} - \frac{1}{100}\right)^n$. Then $a_n > 0$ for all $n \geq 1$. $a_n^{1/n} = \left(\sqrt[n]{n} - \frac{1}{100}\right) \to 1 - \frac{1}{100}$ as $n \to \infty$. This means that there exists N such that $a_n^{1/n} = \sqrt[n]{n} - \frac{1}{100} < 1 - \frac{1}{200}$ for every $n \geq N$. Now by Cauchy's root test $\sum_{n=1}^{\infty} a_n$ is convergent.

(c) We need to consider two cases $p > 1$ and $p < 1$. First of all $\left(n^q\right)^{1/n} = \left(n^{1/n}\right)^q \to 1$ as $n \to \infty$. So $\lim_{n\to\infty} \left(\frac{n^q}{p^n}\right)^{1/n} = \frac{1}{p}$. If $p > 1$ then $\frac{1}{p} < 1$ and hence there exists N such that $\left(\frac{n^q}{p^n}\right)^{1/n} < \frac{1}{2}\left(1 + \frac{1}{p}\right) < 1$ for all $n \geq N$. Then by Cauchy's root test $\sum a_n$ is convergent. If $p < 1$, then $\frac{1}{p} > 1$ and hence there exists M such that $\left(\frac{n^q}{p^n}\right)^{1/n} > 1$ for all $n \geq M$. The series is thus divergent.

(d) Let $a_n = \frac{n!}{n^n}$. Then $\frac{a_{n+1}}{a_n} = \frac{(n+1)!}{n^{n+1}} \times \frac{n^n}{n!} = \left(\frac{n}{n+1}\right)^n$. But $\lim_{n\to\infty} \left(\frac{n+1}{n}\right)^n = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n = e$. Thus $\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = \frac{1}{e} < 1$. By D'Alembert's test $\sum a_n$ is convergent.

Exercise. (iv) : Test the convergence of the series :

(a) $\frac{1}{(\log 2)^p} + \frac{1}{(\log 3)^p} + \ldots + \frac{1}{(\log n)^p} + \ldots$ where $p > 0$.

(b) $\frac{1}{1.2.3} + \frac{3}{2.3.4} + \frac{5}{3.4.5} + \ldots$

(c) $\frac{1}{\sqrt{1 \times 2}} + \frac{1}{\sqrt{2 \times 3}} + \frac{1}{\sqrt{3 \times 4}} + \ldots$

Ans : (a) If $p > 0$, then $\lim_{n\to\infty} \frac{(\log n)^p}{n} = 0$. Thus $(\log n)^p < n$ for every $n > 1$. Therefore $\frac{1}{(\log n)^p} > \frac{1}{n}$ $\forall\ n > 1$. But $\sum \frac{1}{n}$ is a divergent series and the given series is greater than a divergent series and hence is divergent.

(b) $a_n = \frac{2n - 1}{n \,.\, (n + 1)\,(n + 2)}$ (Recall 1, 3, 5, is an A.P with first term 1 and common difference 2 hence $T_n = a + (n - 1)\,d = 1 + (n - 1).2$ $= 2n - 1$. Similarly the denominator)

Choose $b_n = \frac{n}{n^3} = \frac{1}{n^2}$.

Now $\sum b_n = \sum \frac{1}{n^2}$ is convergent by p-test because $p > 1$.

$\lim_{n\to\infty} \frac{a_n}{b_n} = \lim_{n\to\infty} \frac{2n - 1}{n \,.\, (n + 1)\,(n + 2)} \times \frac{n^2}{1} = \lim_{n\to\infty} \frac{2 - \frac{1}{n^3}}{1 \cdot \left(1 + \frac{1}{n}\right)\left(1 + \frac{2}{n}\right)} = 2$. Then by comparison test $\sum a_n$ and $\sum b_n$ act alike but $\sum b_n$ is convergent. Hence $\sum a_n$ is convergent

(c) $a_n = \frac{1}{\sqrt{n\,(n + 1)}}$ (Because the nth term of 1, 2, ... is n and ..., ... is $n + 1$)

Choose $b_n = \frac{1}{\sqrt{n^2}} = \frac{1}{n}$. By p - test $\sum b_n$ is divergent. Now $\lim_{n\to\infty} \frac{a_n}{b_n} = \lim_{n\to\infty} \frac{n}{\sqrt{n\,(n + 1)}} =$

$\lim_{n\to\infty} \frac{1}{\sqrt{1 \,.\, \left(1 + \frac{1}{n}\right)}} = 1.$

By comparision test $\sum a_n$ and $\sum b_n$ act alike. But $\sum b_n$ is divergent. Hence $\sum a_n$ is divergent.

Excersie. (v) : Test the convergence of

(a) $\sum_{n=1}^{\infty} \left(\sqrt{n^4 + 1} - \sqrt{n^4 - 1}\right)$; (b) $\sum_{n=1}^{\infty} \left(\sqrt[3]{n^3 + 1} - n\right)$; (c) $\sum \frac{n + 1}{n^p}$.

Ans : (a) Let $a_n = \sqrt{n^4 + 1} - \sqrt{n^4 - 1} = \frac{\left(\sqrt{n^4 + 1} - \sqrt{n^4 - 1}\right)\left(\sqrt{n^4 + 1} + \sqrt{n^4 - 1}\right)}{\left(\sqrt{n^4 + 1} + \sqrt{n^4 - 1}\right)}$

Thus $a_n = \frac{\left(n^4 + 1\right) - \left(n^4 - 1\right)}{\sqrt{n^4 + 1} + \sqrt{n^4 - 1}} = \frac{2}{\sqrt{n^4 + 1} + \sqrt{n^4 - 1}}$

Choose $b_n = \frac{1}{\sqrt{n^4}} = \frac{1}{n^2}$. Then by p – test $\sum b_n$ is convergent.

$$\lim_{n\to\infty} \frac{a_n}{b_n} = \lim_{n\to\infty} \frac{2}{\sqrt{n^4+1}+\sqrt{n^4-1}} \times \frac{n^2}{1} = \lim_{n\to\infty} \frac{2}{\sqrt{1+\frac{1}{n^4}}+\sqrt{1-\frac{1}{n^4}}} = 2.$$

Then by comparison test $\sum a_n$ and $\sum b_n$ act alike. But $\sum b_n$ is convergent. Hence $\sum a_n$ is convergent.

(b) Let $a_n = \sqrt[3]{n^3+1} - n$.

Rationalising we get using

$$\left(a^3 - b^3\right) = (a-b)\left(a^2 + ab + b^2\right)$$

$$a_n = \frac{\left[\left(n^3+1\right)^{1/3} - n\right]\left[\left(n^3+1\right)^{2/3} + n\left(n^3+1\right)^{1/3} + n^2\right]}{\left[\left(n^3+1\right)^{2/3} + n\left(n^3+1\right)^{1/3} + n^2\right]}$$

$$= \frac{\left(n^3+1-n^3\right)}{\left[\left(n^3+1\right)^{2/3} + n\left(n^3+1\right)^{1/3} + n^2\right]}$$

$$= \frac{1}{\left[\left(n^3+1\right)^{2/3} + n\left(n^3+1\right)^{1/3} + n^2\right]}$$

Choose $b_n = \frac{1}{n^2}$. Then $\sum b_n$ is convergent by p - test.

$$\lim_{n\to\infty} \frac{a_n}{b_n} = \lim_{n\to\infty} \frac{n^2}{\left[\left(n^3+1\right)^{2/3} + n\left(n^3+1\right)^{1/3} + n^2\right]}$$

$$= \lim_{n\to\infty} \frac{1}{\left[\left(1+\frac{1}{n^3}\right)^{2/3} + \left(1+\frac{1}{n}\right)^{1/2} + 1\right]}$$

$$= \frac{1}{3}.$$

Thus by comparison test $\sum a_n$ and $\sum b_n$ act alike but $\sum b_n$ is convergent and hence $\sum b_n$ is convergent.

(c) Let $a_n = \frac{n+1}{n^p}$, choose $b_n = \frac{n}{n^p} = \frac{1}{n^{p-1}}$. By the p – test $\sum b_n$ is convergent if $p - 1 > 1$ and divergent if $p - 1 \le 1$, or $\sum b_n$ is convergent if $p > 2$ and divergent if $p \le 2$.

$$\lim_{n\to\infty} \frac{a_n}{b_n} = \lim_{n\to\infty} \frac{n+1}{n^p} \times \frac{n^{p-1}}{1} = \lim_{n\to\infty} \frac{1+\frac{1}{n}}{1} = 1.$$

Thus by comparison test $\sum a_n$ and $\sum b_n$ act alike. But $\sum b_n$ is convergent if $p > 2$ and divergent if $p \le 2$. Therefore $\sum a_n$ is also convergent if $p > 2$ and divergent if $p \le 2$.

Excersie. (vi) : Test the convergence of :

(a) $\sum_{n=1}^{\infty} \frac{x^n}{n}$ (b) $\sum_{n=1}^{\infty} \sqrt{\frac{n+1}{n^2+1}} x^n$ (c) $x + \frac{3}{5}x^2 + \frac{8}{10}x^3 + \ldots + \frac{n^2-1}{n^2+1}x^n + \ldots$

Ans : (a) Let $a_n = \frac{x^n}{n}$; $a_{n+1} = \frac{x^{n+1}}{n+1}$

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = \lim_{n\to\infty} \frac{x^{n+1}}{n+1} \times \frac{n}{x^n} = \lim_{n\to\infty} \frac{1}{1+\frac{1}{n}} \cdot x = x$$

If $x < 1$, $\sum_{n=1}^{\infty} a_n$ is convergent. If $x > 1$, $\sum_{n=1}^{\infty} a_n$ is divergent if $x = 1$, this test fails. If $x = 1$; then $a_n = \frac{1}{n}$ and $\sum a_n$ is divergent by p – test. Thus the given series $\sum_{n=1}^{\infty} a_n$ is convergent if $x < 1$ and it is divergent if $x \geq 1$.

(b) Let $a_n = \sqrt{\frac{n+1}{n^2+1}} \cdot x^n$; then $a_{n+1} = \sqrt{\frac{n+2}{(n+1)^2+1}} \cdot x^{n+1}$.

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = \lim_{n\to\infty} \sqrt{\frac{n+2}{(n+1)^2+1}} \times x^{n+1} \times \frac{n^2+1}{n+1} \cdot \frac{1}{x^n}$$

$$= \lim_{n\to\infty} \sqrt{\frac{1+\frac{2}{n}}{\left(1+\frac{1}{n}\right)^2+\frac{1}{n^2}}} \times \sqrt{\frac{1+\frac{1}{n^2}}{1+\frac{1}{n}}} \cdot x = x$$

If $x < 1$, $\sum a_n$ is convergent and if $x > 1$ the series is divergent. If $x = 1$, this test fails. If $x = 1$, $a_n = \sqrt{\frac{n+1}{n^2+1}}$ and choose $b_n = \frac{1}{\sqrt{n}}$

$$\lim_{n\to\infty} \frac{a_n}{b_n} = \lim_{n\to\infty} \sqrt{\frac{n+1}{n^2+1}} \times \frac{\sqrt{n}}{1} = \lim_{n\to\infty} \sqrt{\frac{1+\frac{1}{n}}{1+\frac{1}{n^2}}} = 1$$

Thus $\sum a_n$ and $\sum b_n$ act alike but $b_n = \frac{1}{n^{1/2}}$ and by p- test $\sum b_n$ is divergent. Thus $\sum a_n$ is divergent. Thus $\sum a_n$ is convergent if $x < 1$, and $\sum a_n$ is divergent if $x \geq 1$.

(c) Let $a_n = \frac{n^2-1}{n^2+1} x^n$. Then $a_{n+1} = \frac{(n+1)^2-1}{(n+1)^2+1} \cdot x^{n+1}$.

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = \lim_{n\to\infty} \frac{(n+1)^2-1}{(n+1)^2+1} \cdot x^{n+1} \frac{n^2+1}{n^2-1} \frac{1}{x^n}$$

$$= \lim_{n\to\infty} \frac{\left(1+\frac{1}{n}\right)^2-1}{\left(1+\frac{1}{n}\right)^2+1} \times \frac{\left(1+\frac{1}{n^2}\right)}{\left(1-\frac{1}{n^2}\right)} \cdot x = x$$

If $x < 1$, $\sum a_n$ is convergent and if $x > 1$, $\sum a_n$ is divergent. If $x = 1$, then $a_n = \frac{n^2 - 1}{n^2 + 1}$ and $\lim_{n\to\infty} a_n = \lim_{n\to\infty} \frac{1 - \frac{1}{n^2}}{1 + \frac{1}{n^2}} = 1 \neq 0$. Since $\lim_{n\to\infty} a_n \neq 0$, $\sum a_n$ is not convergent. Thus $\sum a_n$ is convergent if $x < 1$ and divergent if $x \geq 1$.

SAQ 4 : Test the convergence of $\sum_{n=1}^{\infty} \left(\sqrt{(2n+1)} - \sqrt{2n-1}\right)$.

SAQ 5 : Test the convergence of $\sum_{n=1}^{\infty} \frac{n^n}{(n+1)(n+2)\ldots 2n}$.

SAQ 6 : Test the convergence of $\sum_{n=1}^{\infty} \frac{100^n}{n!}$.

15.6 SUMMARY

The summation of an infinite series has kept the mathematicians in the 18th and 19th century fully engaged about several questions that arise out of convergence. There are several tests to test the convergence of a given infinite series. The most popular among them are the ratio test, comparison test, Cauchy's root test and Cauchy's condensation test. There are several other tests which are beyond the scope of this course. In spite of all these tests there is no guarantee that the convergence of every infinite series could be readily answered. The most useful result is that if the nth term of an infinite series does not tend to zero as n tends to infinity, then the given series is not convergent. The p - test tells us the series $\sum_{n=1}^{\infty} \frac{1}{n^p}$ is convergent if $p > 1$ and divergent if $p \leq 1$. One way to test the convergence of a given series is to compare it with the behaviour of a known series.

15.7 MODEL EXAMINATION QUESTIONS

Section A (Long Answer)

i) Test the convergence of : (a) $\frac{1}{2\sqrt{1}} + \frac{x^2}{3\sqrt{2}} + \frac{x^4}{4\sqrt{3}} + \ldots$ (b) $\sum_{n=1}^{\infty} \left(\sqrt{n^4 + 1} - \sqrt{n^4 - 1}\right)$.

ii) State and prove Cauchy's condensation test and apply the same to discuss the behaviour of $\sum_{n=2}^{\infty} \frac{1}{n (\log n)^p}, p > 0$.

iii) Discuss the convergence of the series : (a) $\frac{2}{1^p} + \frac{3}{2^p} + \frac{4}{3^p} + \ldots$ (b) $\sum_{n=1}^{\infty} \frac{1}{n^p (n+1)^p}$.

Section B (Short Answer)

i) Show that if $\sum_{n=1}^{\infty} a_n$ is convergent then $\lim_{n\to\infty} a_n = 0$. Is the converse true? Justify your answer.

ii) Discuss the convergence of $\sum_{n=1}^{\infty} \frac{1}{n^p}$.

iii) Discuss the convergence of the series $\sum_{n=1}^{\infty} \left(\frac{\sqrt{n+1} - \sqrt{n-1}}{n}\right)$.

iv) Test the convergence of $\sum_{n=1}^{\infty} \frac{(n+1)\,x^n}{n^3}$.

v) Show that $\sum_{n=1}^{\infty} \frac{2^n}{n^2+1}$ is divergent.

15.8 ANSWERS TO SAQ'S

SAQ 1 Divergent because this is a p - series $p = \frac{1}{2} < 1$.

SAQ 2 Convergent because $p = 2 > 1$.

SAQ 3 $a_n = \dfrac{\sqrt{n+1} - \sqrt{n-1}}{n} = \dfrac{(n+1)-(n-1)}{n\left(\sqrt{n+1} + \sqrt{n-1}\right)} = \dfrac{2}{n\left(\sqrt{n+1} + \sqrt{n-1}\right)}$

Chosse $b_n = \frac{1}{n^{3/2}}$. Then $\dfrac{a_n}{b_n} = \dfrac{2n \cdot \sqrt{n}}{n\left(\sqrt{n+1} + \sqrt{n-1}\right)} = \dfrac{2\sqrt{n}}{\sqrt{n+1} + \sqrt{n-1}}$

$\lim_{n\to\infty} \dfrac{a_n}{b_n} = \lim_{n\to\infty} \dfrac{2}{\sqrt{1+\frac{1}{n}} + \sqrt{1-\frac{1}{n}}} = 2$, finite. Thus $\sum a_n$ and $\sum b_n$ act alike. But $b_n = \frac{1}{n^{3/2}}$ (by p – test) $\sum b_n$ is convergent. So is $\sum a_n$. (If we take $b_n = \dfrac{\sqrt{n}}{n}$ we get $\lim_{n\to\infty} \dfrac{a_n}{b_n} = 0$ and the test could be applied only when $\sum b_n$ is convergent which in this case is not).

SAQ 4 $a_n = \dfrac{\left(\sqrt{2n+1} - \sqrt{2n-1}\right)\left(\sqrt{2n+1} + \sqrt{2n-1}\right)}{\left(\sqrt{2n+1} + \sqrt{2n-1}\right)} = \dfrac{2}{\sqrt{2n+1} + \sqrt{2n-1}}$

Let $b_n = \frac{1}{\sqrt{n}}$. Then $\sum b_n$ is divergent by p – test.

Now $\lim_{n\to\infty} \frac{a_n}{b_n} = \lim_{n\to\infty} \frac{2\sqrt{n}}{\sqrt{2n+1}+\sqrt{2n-1}} = \frac{1}{\sqrt{2}}$. Thus $\sum a_n$ and $\sum b_n$ act alike.

Hence $\sum a_n$ is divergent.

SAQ 5 $a_n = \frac{n^n}{(n+1)(n+2)\ldots(n+n)}$; $\lim_{n\to\infty} a_n = \lim_{n\to\infty} \frac{1}{\left(1+\frac{1}{n}\right)\ldots(1+1)}$. Since

$\lim_{n\to\infty} a_n \neq 0$, $\sum a_n$ is not convergent.

SAQ 6 $a_n = \frac{100^n}{n!}$; $a_{n+1} = \frac{100^{n+1}}{(n+1)!}$

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = \lim_{n\to\infty} \frac{100^{n+1}}{(n+1)!} \times \frac{n!}{100^n} = \lim_{n\to\infty} \frac{100}{n+1}$$

$$= \lim_{n\to\infty} \frac{100}{1+\frac{1}{n}} = 100 > 1.$$

By D'Alembert's ratio test $\sum a_n$ is divergent.

UNIT–16: INFINITE SERIES (II)

Contents

16.1 Aims and Objectives

16.2 Introduction

16.3 Alternating series

16.4 Product of series

16.5 Power seirs

16.6 Workedout exercises

16.7 Summary

16.8 Model Examination Questions

16.8 Answers to Self Assessment Questions

16.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to : (i) State convergence tests for series with both positive and negative terms and apply them to discuss the behavour of an infinite series with positive and negative terms. (ii) Analyse the problem of rearrangement of terms of an infinite series (iii) Define the Cauchy product of the infinite series (iv) State and prove Abel's and Merten's tests for the convergence of product of series.

16.2 INTRODUCTION

In unit 15 we considered the convergence of an infinite series and stated tests to test the convergence of an infinite series with positive terms. In those cases the notions of absolute convergence coincides with that of convergence since all the terms are positive. If the series consist of both positive and negative terms, many of those tests do not apply as they were. This is because an infinite series with positive and negative terms may behave differently if the terms are rearranged. There are not many tests to deal with series with positive and negative terms. We state in this unit the tests due to leibnitz (1646 - 1716) and Dirichlet (1805 - 1859). We also tackle the problem of multiplying two infinite series and under what conditions the product might be convergent.

16.3 ALTERNATING SERIS

Definition 1 :

A sequence $\langle x_n \rangle$ of non zero real numbers is alternating if the terms $(-1)^n x_n$ are all positive or all negative real numbers. If a sequence $\langle x_n \rangle$ is alternating then we say that $\sum x_n$ generates an alternating series.

Example 1 : $\sum_{n=1}^{\infty} \frac{(-1)^n}{n} = -1 + \frac{1}{2} - \frac{1}{3} + \ldots$ is an example of alternating series.

Remark 1 : If $\sum_{n=1}^{\infty} a_n$ is a convergent series and $\sum_{n=1}^{\infty} |a_n|$ is divergent we say $\sum_{n=1}^{\infty} a_n$ is conditionally convergent.

Theorem 1 : (Dirchlet's Test) :

> Suppose that each a_n of a given series can be expressed as a product $b_n c_n$ where $\langle b_n \rangle$ is a decreasing sequence of positive terms with limit zero and the partial sum sequence of the series $\sum_{n=1}^{\infty} c_n$ is bounded. Then $\sum_{n=1}^{\infty} a_n$ is convergent.

Proof : Write $s_1 = c_1$ and $s_n = c_1 + c_2 + \ldots c_n$ so that $c_n = s_n - s_{n-1}$ for each $n > 1$. If $m > n > 1$, then

$$\begin{aligned} a_{n+1} + a_{n+2} + \ldots + a_m &= b_{n+1} c_{n+1} + \ldots + b_m c_m \\ &= \sum_{k=n+1}^{m} b_k \left(s_k - s_{k-1} \right) \\ &= \sum_{k=n+1}^{m} b_k s_k - \sum_{j=n+1}^{m} b_j s_{j-1} \\ &= \sum_{k=n+1}^{m} b_k s_k - \sum_{k=n}^{m-1} b_{k+1} s_k \\ &= \sum_{k=n+1}^{m-1} s_k \left(b_k - b_{k+1} \right) + b_m s_m - b_{n+1} s_n \end{aligned}$$

By hypothesis $\langle s_n \rangle$ is bounded. Let λ be a positive number such that $|s_n| < \lambda$ for all n. Now

$$\begin{aligned} |a_{n+1} + \ldots + a_m| &\leq \sum_{k=n+1}^{m-1} |s_k| \left(b_k - b_{k+1} \right) + b_m |s_m| + b_{n+1} |s_n| \\ &\leq \lambda \sum_{k=n+1}^{m-1} \left(b_k - b_{k+1} \right) + \lambda \left(b_m + b_{n+1} \right) \\ &= 2 \lambda b_{n+1} \left(\text{Since } b_k > b_{k+1}, \left(b_k - b_{k+1} \right) = |b_k - b_{k+1}| \right) \end{aligned}$$

Let $\delta > 0$. Since $b_n \to 0$ as $n \to \infty$, there exists N such that $b_n < \frac{\delta}{2\lambda}$ for all $n \geq N$. Thus for $m > n > N$, we have $|a_{n+1} + \ldots + a_n| \leq 2 \lambda b_{n+1} < \delta$. This shows that $\sum_{n=1}^{\infty} a_n$ converges by Cauchy's principle for series.

Theorem 2 : (Leibnitz Test) :

If in an alternating series $\sum_{n=1}^{\infty} a_n$, the sequence $\langle |a_n| \rangle$ is a decreasing sequence converging to zero, then the series $\sum_{n=1}^{\infty} a_n$ is convergent.

Proof : Write $b_n = |a_n|$ and $c_n = (-1)^n$ or $(-1)^{n+1}$ according as a_1 is positive or negative. Then since the series is alternating, $a_n = |a_n| c_n = b_n c_n$ for all n. Now $\langle b_n \rangle$ is a decreasing sequence with limit zero and the partial sum sequence of $\sum_{n=1}^{\infty} c_n$ is bounded. Hence by Dirichlet's theorem $\sum_{n=1}^{\infty} a_n$ is convergent.

Remark 2 : Leibnitz theorem can be proved independently without using Dirichelt's theorem. To see this let $a_n = (-1)^{n+1} b_n$ where each b_n is positive. Now $\langle b_n \rangle$ is a decreasing sequence with limit zero.

Now $s_{2n+2} = s_{2n} + a_{2n+1} + a_{2n+2} = s_{2n} + b_{2n+1} - b_{2n+2}$

$\geq s_{2n}$ since $b_{2n+1} \geq b_{2n+2}$.

Thus the subsequence $\langle s_{2n} \rangle$ of the partial sum sequence $\langle s_n \rangle$ of the given series is an increasing sequence. More over

$$\begin{aligned} s_{2n} &= s_{2n-1} + a_{2n} = s_{2n-1} - b_{2n} \leq s_{2n-1} \\ &= b_1 - (b_2 - b_3) - (b_4 - b_5) - \ldots - (b_{2n-2} - b_{2n-1}) \\ &\leq b_1 \text{ since } (b_2 - b_3), \ldots \text{ are all } \geq 0. \end{aligned}$$

Hence the subsequence $\langle s_{2n} \rangle$ is convergent because it is an increasing sequence bounded above. Let $s_{2n} \to s$ as $n \to \infty$. Since $s_{2n-1} = s_{2n} - a_{2n}$ and $a_{2n} \to 0$ as $n \to \infty$, it follows that $s_{2n-1} \to s$ as $n \to \infty$. Hence $s_n \to s$ as $n \to \infty$.

Example (i) : $\sum_{n=1}^{\infty} \frac{(-1)^n}{\sqrt{n}}$. This is an alternating series and the sequence $\left\langle \frac{1}{\sqrt{n}} \right\rangle$ decreases to zero. Hence the given series is convergent.

Example (ii) : $\sum_{n=1}^{\infty} (-1)^n b_n$ where $b_n = \dfrac{1 + \frac{1}{2} + \ldots + \frac{1}{n}}{n}$

Then $b_n - b_{n+1} = \dfrac{1 + \frac{1}{2} + \ldots + \frac{1}{n}}{n} - \dfrac{1 + \frac{1}{2} + \ldots + \frac{1}{n+1}}{n+1}$

$$= \frac{(n+1)\left(1 + \frac{1}{2} + \ldots + \frac{1}{n}\right) - n\left(1 + \frac{1}{2} + \ldots + \frac{1}{n+1}\right)}{n(n+1)}$$

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

$$= \frac{\left(1 - \frac{1}{n+1}\right) + \left(\frac{1}{2} - \frac{1}{n+1}\right) + \ldots + \left(\frac{1}{n} - \frac{1}{n+1}\right)}{n(n+1)} > 0$$

Thus $\langle b_n \rangle$ is a decreasing sequence. Since $\frac{1}{n} \to 0$ as $n \to \infty$, it follows that $b_n \to 0$ as $n \to \infty$, by Cauchy's first theorem.

Example (iii) : The series $\sum_{n=0}^{\infty} \frac{\cos n\theta}{\log (n+2)}$ is not an alternating series unless $\cos \theta = -1$. If $\cos \theta = 1$, then θ is an integral multiple of 2π and $\cos n\theta = 1$ for all n . In this case the series diverges. Let $\cos \theta \neq 1$. Let $b_n = \frac{1}{\log (n+2)}$ and $c_n = \cos n\theta$. Clearly $\langle b_n \rangle$ is a decreasing sequence tending to 0 as $n \to \infty$. Let $s_n = c_0 + c_1 + \ldots + c_n = 1 + \cos\theta + \ldots + \cos n\theta$ and $t_n = \sin\theta + \sin 2\theta + \ldots + \sin n\theta$. Let $i = \sqrt{-1}$.

Then $s_n + i\,t_n = 1 + (\cos\theta + i \sin\theta) + (\cos\theta + i \sin\theta)^2 + \ldots + (\cos\theta + i \sin\theta)^n$.

$$= \frac{1 - (\cos\theta + i \sin\theta)^{n+1}}{\left(1 - (\cos\theta + i \sin\theta)\right)} = \frac{1 - \cos(n+1)\theta - i \sin(n+1)\theta}{1 - \cos\theta - i \sin\theta}$$

$$= \frac{[1 - \cos(n+1)\theta - i \sin(n+1)\theta][1 - \cos\theta + i \sin\theta]}{(1 - \cos\theta)^2 + \sin^2\theta}$$

Equating real parts we get

$$s_n = \frac{[1 - \cos(n+1)\theta](1 - \cos\theta) + \sin(n+1)\theta \cdot \sin\theta}{2(1 - \cos\theta)}$$

and $|s_n| \leq \frac{5}{2(1 - \cos\theta)}$ since, $|\cos(n+1)\theta|, |\sin(n+1)\theta|,$

$|\cos\theta|$ and $|\sin\theta|$ are all ≤ 1.

Since $\cos\theta \neq 1$, $\langle s_n \rangle$ is bounded. By Dirichelet test the given series is convergent.

SAQ 1 Discuss the convergence of $\sum (-1)^{n-1} \frac{n}{5^n}$.

Definition 2 :

An infinite series $\sum b_n$ is said to be a rearrangement of the infinite series $\sum a_n$ if there exists a bijection f from N onto N such that $b_m = a_{f(m)}$, for all $m \in$ N. It is easy to see that the terms of the orginal series including repetitions are present in the rearrangement, may be, in a different order. Observe that if $\sum b_n$ is a rearrangement of $\sum a_n$, then $\sum a_n$ is a rearrangement of $\sum b_n$, and if $\sum b_n$ is a rearrangement of $\sum c_n$ then $\sum c_n$ is a rearrangement of $\sum a_n$.

Theorem 3 :

If $\sum_{n=1}^{\infty} a_n$ is a convergent series of non-negative terms and $\sum_{n=1}^{\infty} b_n$ is a rearrangement of $\sum_{n=1}^{\infty} a_n$, then $\sum_{n=1}^{\infty} b_n$ is convergent and has the same sum of $\sum_{n=1}^{\infty} a_n$.

Proof : Let $\sum_{n=1}^{\infty} a_n = S$ and $b_n = a_{f(n)}$ where f is a bijection from N onto N. Write $t_n = b_1 + b_2 + \ldots + b_n = a_{f(1)} + a_{f(2)} + \ldots + a_{f(n)}$

If $m = \max \{f(1), f(2), \ldots, f(n)\}$, then $f(1), f(2) \ldots f(n)$ are distinct positive integers each $\leq m$, then $t_n = a_{f(1)} + a_{f(2)} + \ldots + a_{f(n)} \leq a_1 + a_2 + \ldots + a_m \leq S$. This shows that the partial sum sequence of $\sum_{n=1}^{\infty} b_n$ is bounded above and S is an upper bound for this sequence. Hence $\sum_{n=1}^{\infty} b_n$ is convergent and its sum $T \leq S$. Since $\sum_{n=1}^{\infty} a_n$ is a rearrangement of $\sum_{n=1}^{\infty} b_n$, the roles of $\sum a_n$ and $\sum b_n$ could be interchanged to get the conclusion that $S \leq T$. Thus $\sum_{n=1}^{\infty} a_n$ and $\sum_{n=1}^{\infty} b_n$ both converge to the same limit.

Theorem 4 :

If $\sum_{n=1}^{\infty} a_n$ is an absolutely convergent series of real numbers and $\sum_{n=1}^{\infty} b_n$ is a rearrangement of $\sum_{n=1}^{\infty} a_n$, then $\sum_{n=1}^{\infty} a_n$ and $\sum_{n=1}^{\infty} b_n$ both converge to the same limit.

Proof : Let f be a bijection of N onto N such that $b_n = a_{f(n)}$, for all n. Write

$$p_n = \frac{1}{2}\left(|a_n| + a_n\right) \text{ and } q_n = \frac{1}{2}\left(|a_n| - a_n\right).$$

Then $|a_n| = p_n + q_n$, and $a_n = p_n - q_n$ for all n. Since $\sum_{n=1}^{\infty} a_n$ and $\sum_{n=1}^{\infty} |a_n|$ are both convergent series it follows that $\sum_{n=1}^{\infty} p_n$ and $\sum_{n=1}^{\infty} q_n$ are both convergent series of non negative terms.

Then $\sum_{n=1}^{\infty} p_{f(n)}$ converges to the same limit as $\sum_{n=1}^{\infty} p_n$, and $\sum_{n=1}^{\infty} q_{f(n)}$ converges to the same limit as $\sum_{n=1}^{\infty} q_n$. Hence $\sum_{n=1}^{\infty} \left(p_{f(n)} - q_{f(n)}\right) = \sum_{n=1}^{\infty} a_{f(n)}$ converges to the same limit as $\sum_{n=1}^{\infty} \left(p_n - q_n\right) = \sum_{n=1}^{\infty} a_n$. Thus $\sum b_n$ and $\sum a_n$ converge to the same limit.

Example 4 : Consider the alternating series $\sum a_n = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \ldots$ and let $\sum b_n$ be the rearrangement obtained by taking two positive terms, then one negative term at a time in order without changing the order of the positive terms and negative terms. Thus $\sum b_n = 1 + \frac{1}{3} - \frac{1}{2} + \frac{1}{5} + \frac{1}{7} - \frac{1}{4} + \frac{1}{9} + \frac{1}{11} - \frac{1}{6} + \ldots$ Let S_n and T_n denote the n^{th} partial sums of the $\sum a_n$ and $\sum b_n$ respectively. Then

$$\begin{aligned} T_{3n} &= 1 + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \ldots + \frac{1}{4n-1} - \frac{1}{2} - \frac{1}{4} - \ldots - \frac{1}{2n} \\ &= S_{4n} + \frac{1}{2n+2} + \frac{1}{2n+4} + \ldots + \frac{1}{4n} \\ &= S_{4n} + \frac{1}{2}\left(\frac{1}{n+1} + \frac{1}{n+2} + \ldots + \frac{1}{2n}\right) \\ &> S_{4n} + \frac{1}{4}\left(\because \frac{1}{n+1} + \ldots \frac{1}{2n} > \frac{1}{2n} + \ldots \frac{1}{2n} = \frac{1}{2}\right) \end{aligned}$$

Now by Leibnitz theorem $\sum a_n$ is a convergent series whose sum is S (say).

Then $T = \lim_{n\to\infty} T_{3n}$. Then $T = \lim_{n\to\infty} T_{3n} \geq \lim_{n\to\infty} \left(S_{4n} + \frac{1}{4}\right) = S + \frac{1}{4}$ whether $\sum b_n$ converges or not, its sum is different from that of $\sum a_n$. This means that the conclusion of Theorem 4 need not hold good if $\sum a_n$ is conditionally convergent. (Recall that $\sum a_n$ is not absolutely convergent).

16.4 PRODUCT OF SERIES

Definition 3 :

Let $\sum_{n=0}^{\infty} a_n$ and $\sum_{n=0}^{\infty} b_n$ be two given series. The series $\sum_{n=0}^{\infty} c_n$ where $c_n = a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0$ is called the Cauchy product of the two given series.

Example 5 : Let $a_n = b_n = \frac{(-1)^n}{n+1}$ for all $n \geq 0$. Then the Cauchy product $\sum_{n=0}^{\infty} a_n$ with itself is given by $\sum_{n=0}^{\infty} c_n$ where $c_n = a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0 = \sum_{k=0}^{n} a_k b_{n-k}$

$$= (-1)^n \sum_{k=0}^{n} \frac{1}{\sqrt{k+1}\sqrt{n-k+1}}$$

$$\text{Now } |c_n| = \sum_{k=0}^{n} \frac{1}{\sqrt{k+1}\sqrt{n-k+1}} \geq \sum_{k=0}^{\infty} \frac{1}{\left(\frac{n}{2}+1\right)} = \frac{2(n+1)}{n+2} \geq 1.$$

Since $c_n \not\to 0$ as $n \to \infty$, $\sum c_n$ is not convergent though $\sum a_n$ is convergent. Thus the Cauchy product of two convergent series need not be convergent.

Theorem 5 :

If $A_n \to A$ and $B_n \to B$ and $n \to \infty$ and if the sequence $\langle L_n \rangle$ is defined by $L_n = \dfrac{A_0 B_n + A_1 B_{n-1} + \ldots + A_n B_0}{n}$ then $L_n \to AB$ as $n \to \infty$.

Proof : Write $\alpha_n = A - A_n$ and observe that $\alpha_n \to 0$ as $n \to \infty$.

$$\text{Write } J_n = A \cdot \left(\frac{B_0 + B_1 + \ldots + B_n}{n}\right) \text{ and}$$

$$K_n = \frac{\alpha_0 B_n + \alpha_1 B_{n-1} + \ldots + \alpha_n B_0}{n}$$

$$\text{Then } L_n = J_n - K_n \text{ for all } n .$$

By Cauchy's first theorem $\dfrac{B_0 + B_1 + \ldots + B_n}{n} \to B$ so that $J_n \to AB$ as $n \to \infty$.

Since $\langle B_n \rangle$ is convergent, $\langle B_n \rangle$ is bounded and hence there exists a positive number λ such that $|B_n| < \lambda$ for all n. Now

$$0 \le |K_n| \le \frac{|\alpha_0|\,|B_n| + |\alpha_1|\,|B_{n-1}| + \ldots + |\alpha_n|\,|B_0|}{n}$$

$$\le \frac{\lambda\left(|\alpha_0| + |\alpha_1| + \ldots + |\alpha_n|\right)}{n}$$

Since $|\alpha_n| \to 0$ as $n \to \infty$, by Cauchy's first theorem $\dfrac{|\alpha_0| + |\alpha_1| + \ldots + |\alpha_n|}{n} \to 0$ as $n \to \infty$.

Thus by Sandwich theorem $K_n \to 0$ as $n \to \infty$ and hence $L_n \to AB$, as $n \to \infty$.

Theorem 6 : (Abel) :

Let $\sum_{n=0}^{\infty} a_n$ and $\sum_{n=0}^{\infty} b_n$ converge to A and B respectively and the Cauchy product of $\sum a_n$ and $\sum b_n$ given by $\sum_{n=0}^{\infty} c_n$ converges to C, then C = AB.

Proof :

$$\text{Let } A_n = a_0 + a_1 + \ldots + a_n,$$

$$B_n = b_0 + b_1 + \ldots + b_n \text{ and}$$

$$C_n = c_0 + c_1 + \ldots + c_n$$

$$\text{Then } C_n = a_0 b_0 + \left(a_0 b_1 + a_1 b_0\right) + \left(a_0 b_2 + a_1 b_1 + a_2 b_0\right) + \ldots + \left(a_0 b_n + \ldots + a_n b_0\right)$$

$$= a_0 B_n + a_1 B_{n-1} + \ldots + a_n B_0 \text{ and}$$

$$C_0 + C_1 + \ldots + C_n = a_0 B_0 + \left(a_0 B_1 + a_1 B_0\right) + \ldots + \left(a_0 B_n + \ldots + a_n B_0\right)$$

$$= A_n B_0 + A_{n-1} B_1 + \ldots + A_0 B_n$$

$$= A_0 B_n + A_1 B_{n-1} + \ldots + A_n B_0$$

Let $L_n = \dfrac{C_0 + C_1 + \ldots + C_n}{n}$. Then $L_n \to C$ as $n \to \infty$ by Cauchy's first theorem. But by Theorem 5, $L_n \to AB$. Thus $C = AB$.

Remark 3 : Cauchy first proved that the Cauchy product of two absolutely convergent series is itself absolutely convergent. Subsequently Mertens proved that if one series converges absolutely and the other converges then their Cauchy product is convergent.

Theorem 7 : (Mertens) :

Suppose $\sum_{n=0}^{\infty} a_n = A$, $\sum_{n=0}^{\infty} b_n = B$ and that $\sum_{n=0}^{\infty} a_n$ converges absolutely. Then the Cauchy product of $\sum_{n=0}^{\infty} a_n$ and $\sum_{n=0}^{\infty} b_n$ converges and its sum is AB.

Proof : Write $C_n = a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0$ for all $n \geq 0$. We are requried to show that $\sum_{n=0}^{\infty} c_n = AB$.

Put $A_n = a_0 + a_1 + \ldots + a_n$; $B_n = b_0 + b_1 + \ldots + b_n$, $C_n = c_0 + c_1 + \ldots + c_n$.

$\beta_n = B_n - B$; $\gamma_n = a_0 \beta_n + \ldots + a_n \beta_0$ and $\alpha = \sum_{n=0}^{\infty} |a_n|$.

Now
$$\begin{aligned} C_n &= a_0 b_0 + (a_0 b_1 + a_1 b_0) + \ldots + (a_0 b_n + \ldots + a_n b_0) \\ &= a_0 B_n + a_1 B_{n-1} + \ldots + a_n B_0 \\ &= a_0 (B + \beta_n) + a_1 (B + \beta_{n-1}) + \ldots + a_n (B + \beta_0) \\ &= A_n B + a_0 \beta_n + a_1 \beta_{n-1} + \ldots + a_n \beta_0 \\ &= A_n B + \gamma_n \end{aligned}$$

Since $A_n B \to AB$ as $n \to \infty$, it is enough to show that $\gamma_n \to 0$ as $n \to \infty$.

Let $\delta > 0$. Since $\beta_n \to 0$ as $n \to \infty$, there exists N such that $|\beta_n| < \dfrac{\delta}{2\alpha + 1}$ for all $n > N$.

Let λ be an upper bound of $\langle |\beta_n| \rangle$.

Since $\sum_{n=0}^{\infty} |a_n|$ is convergent, there exists M such that

$|a_{n+1}| + |a_{n+2}| + \ldots + |a_{n+k}| < \dfrac{\delta}{2\lambda + 1}$ for all $n \geq M$.

Now $n > M + N$, we have $n - N > M$ and

$$\begin{aligned} |\gamma_n| &\leq |\beta_0 a_n + \beta_1 a_{n-1} + \ldots + \beta_n a_{n-N}| \\ &\quad + |\beta_{n+1} a_{n-N-1} + \ldots + \beta_n a_0| \\ &\leq \lambda \left(|a_n| + |a_{n-1}| + \ldots + |a_{n-N}| \right) \end{aligned}$$

$$+\frac{\delta}{2\alpha+1}\left(|a_0|+\ldots+|a_{n-N-1}|\right)$$

$$<\lambda\frac{\delta}{2\lambda+1}+\alpha\frac{\delta}{2\alpha+1}<\frac{\delta}{2}+\frac{\delta}{2}=\delta.$$

This shows that $\gamma_n \to 0$ as $n \to \infty$ and consequently that $C_n \to A\,B$ as $n \to \infty$.

Theorem 8 : (Cauchy) :

> If $\sum_{n=0}^{\infty} a_n$ and $\sum_{n=0}^{\infty} b_n$ are absolutely convergent and $\sum_{n=0}^{\infty} c_n$ is their Cauchy product, then $\sum_{n=0}^{\infty} c_n$ is also absolutely convergent.

Proof : Put $d_n = |a_0 b_n| + |a_1 b_{n-1}| + \ldots + |a_n b_0|$. Since $\sum_{n=0}^{\infty} d_n$ is the Cauchy product of $\sum_{n=0}^{\infty} |a_n|$ and $\sum_{n=0}^{\infty} |b_n|$ which are absolutely convergent, it follows that $\sum_{n=0}^{\infty} d_n$ converges by Merter's theorem.

But $|C_n| = |a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0| \le d_n$ and $\sum_{n=0}^{\infty} d_n$ is convergent. Then by comparision test $\sum_{n=0}^{\infty} c_n$ is convergent.

SAQ 2 Show that convergence of $\sum a_n$ implies the convergence of $\sum \sqrt[n]{n}\, a_n$.

Example 6 : If $|x| < 1$, then $\left(\frac{1}{1-x}\right)\log\left(\frac{1}{1-x}\right) = \sum_{n=1}^{\infty}\left(1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}\right)x^n$. To see this let $A = \frac{1}{1-x} = 1 + x + x^2 + \ldots + x^n + \ldots = \sum_{n=1}^{\infty} x^{n-1} = \sum_{n=1}^{\infty} a_n$

$$B = \log\left(\frac{1}{1-x}\right) = x + \frac{x^2}{2} + \ldots + \frac{x^n}{n} + \ldots = \sum_{n=1}^{\infty}\frac{x^n}{n} = \sum_{n=1}^{\infty} b_n$$

Since $|x| < 1$, $\sum a_n$ and $\sum b_n$ both converge absolutely. Let $\sum c_n$ denote the Cauchy product of $\sum a_n$ and $\sum b_n$. Then

$$\begin{aligned} c_n &= a_1 b_n + a_2 b_{n-1} + \ldots + a_n b_1 \\ &= 1\cdot\frac{x^n}{n} + x\cdot\frac{x^{n-1}}{n-1} + \ldots + x^{n-1}\cdot\frac{x}{1} \\ &= \left(1+\frac{1}{2}+\ldots+\frac{1}{n}\right)x^n \end{aligned}$$

Since $\sum a_n$ and $\sum b_n$ both converge absolutely for $|x| < 1$. $\sum c_n$ also converges for $|x| < 1$ and has the sum AB.

Thus $\left(\frac{1}{1-x}\right)\log\left(\frac{1}{1-x}\right) = \sum_{n=1}^{\infty}\left(1 + \frac{1}{2} + \ldots + \frac{1}{n}\right)x^n$, for $|x| < 1$.

16.5 POWER SERIES

The series $\sum_{n=0}^{\infty} a_n \left(x - x_0\right)^n$ is called a power series in $\left(x - x_0\right)$. The numbers a_n, $n \in N$ are called the coefficients of the power series. By a simple change of variable $x - x_0 = X$, the above power series become $\sum_{n=0}^{\infty} a_n X^n$. We can use the tests of convergence like the ratio test or root test to study the convergence of a power series.

Theorem 8 :

> If a power series $\sum a_n x^n$ converges for $x = x_1 \neq 0$, then the series converges absolutely for every x such that $|x| < |x_1|$.

Proof : $\sum a_n x^n$ converges for $x = x_1$ implies that $a_n x_1^n \to 0$ as $n \to \infty$. This means that there exists N such that $|a_n x_1^n| < 1$ for $n \geq N$. This implies that

$$|a_n x^n| = |a_n x_1^n| \left|\frac{x^n}{x_1^n}\right| < \left|\frac{x}{x_1}\right|^n = t^n \text{ where}$$

$t = \left|\frac{x}{x_1}\right| < 1$. Since $\sum t^n$ converges, then by comparision test $\sum_{n=N}^{\infty} |a_n x^n|$ converges.

Hence $\sum_{0}^{\infty} |a_n x^n|$ converges for $|x| < |x_1|$.

Theorem 9 :

> If the power series $\sum a_n x^n$ converges for a value $x_1 \neq 0$ and diverges for a value x_2, then there exists a positive real number r such that the series is absolutely convergent for $|x| < r$ and diverges for $|x| > r$.

Proof : Let $S = \left\{x \in R \mid \sum a_n x^n \text{ converges}\right\}$. Since $x_1 \in S$, and hence $S \neq \phi$. Further if $x \in S$, then $x < |x_2|$. Thus S is an aggregate bounded above and r = l.u.b S exists. We observe $r \geq |x_1| > 0$.

If $|x| > r$ then $x \notin S$. For if $x \in S$, then $|x| \in S$ and $|x| > r$ = l.u.b of S, which is not correct. Thus the series diverges for $|x| > r$. If $|x| < r$, then there exists a number $y \in S$ such that $|x| < y < r$. By theorem 8, $\sum a_n x^n$ converges absolutely if $|x| < r$.

Definition 4 :

A real number r is called the radius of convergence of a power series if the power series converges absolutely for all x such that $|x| < r$ and diverges for all x such that $|x| > r$. The interval $(-r, r)$ is called the interval of convergence.

Theorem 10 :

Suppose $\sum a_n x^n$ is a power series and $\lim_{n\to\infty} \left|\frac{a_{n+1}}{a_n}\right| = q$. Then the radius of convergence of the power series is $r = \frac{1}{q}$ if $0 < q < \infty$. If $q = 0$ then $r = \infty$ and if $q = \infty$ then $r = 0$.

Proof : If $q = 0$, then for any $x \in \mathbf{R}, x \neq 0$,

$$\lim_{n\to\infty} \left|\frac{a_{n+1}\, x^{n+1}}{a_n\, x^n}\right| = \lim_{n\to\infty} \left|\frac{a_{n+1}}{a_n}\right| |x| = 0.$$

Therefore the power series converges. Hence $r = \infty$. If $q = \infty$, for any $x \neq 0$, in $\mathbf{R}$ the series diverges. Hence $r = 0$.

If $0 < q < \infty$, then $\lim_{n\to\infty} \left|\frac{a_{n+1}\, x^{n+1}}{a_n\, x^n}\right| = q\,|x|$

By ratio test the power series converges absolutely if $q|x| < 1$ and diverges if $q|x| > 1$. This means that the radius of convergence is $\frac{1}{q}$.

Theorem 11 :

Suppose $\sum a_n x^n$ is a power series and $\lim_{n\to\infty} |a_n|^{1/n} = q$. Then the radius of convergence of the power series is $\frac{1}{q}$ if $0 < q < \infty$. If $q = 0$, then $r = \infty$ and if $q = \infty$, then $r = 0$.

Proof : If $q = 0$, then for any $x \in \mathbf{R}, x \neq 0$, $\lim_{n\to\infty} |a_n x^n|^{1/n} = \lim_{n\to\infty} |a_n|^{1/n} \cdot |x| = q|x| = 0$.

Therefore by Cauchy's root test the power series converges for all $x \in \mathbf{R}$. Hence $r = \infty$. If $q = \infty$, then the series diverges for any $x \in \mathbf{R}, x \neq 0$. Hence $r = 0$. If $0 < q < \infty$, then $\lim |a_n x^n|^{1/n} = q|x|$. By Cauchy's test, the power series converges if $q|x| < 1$ and diverges for $q|x| > 1$.

Thus the radius of convergence is $\frac{1}{q}$.

SAQ 3 What is the radius of convergence of the power series $\sum_{n=0}^{\infty} \frac{x^n}{n!}$.

Example 7 : The power series $\sum_{0}^{\infty} n!\, x^n$ diverges for any non zero $x \in \mathbf{R}$ and as such the radius of convergence $r = 0$. This is because $\lim_{n\to\infty} \left|\frac{a_{n+1}}{a_n}\right| = \lim (n + 1) = \infty$.

Example 8 : For the infinite series $\sum_{1}^{\infty} \frac{(-1)^n x^n}{n}$, $\lim_{n\to\infty} \left|\frac{a_{n+1}}{a_n}\right| = 1$. The radius of convergence is 1.

When $x = 1$; the series $\sum_{1}^{\infty} \frac{(-1)^n}{n}$ which is convergent. When $x = -1$, the series $\sum_{1}^{\infty} \frac{1}{n}$ which is divergent the interval of convergence is $(-1, 1] = \{x / -1 < x \leq 1\}$.

16.6 WORKEDOUT EXERCISES

Exercise (i) : Discuss the convergence of (a) $\sum \frac{(-1)^n}{\sqrt{n}}$ (b) $\sum_{n=2}^{\infty} \frac{(-1)^n}{\log n}$ (c) $\sum \frac{(-1)^n}{n+2}$.

(a) Let $a_n = \frac{1}{\sqrt{n}}$, then $a_{n+1} = \frac{1}{\sqrt{n+1}}$. But $\sqrt{n+1} > \sqrt{n}$ implies $\frac{1}{\sqrt{n+1}} < \frac{1}{\sqrt{n}}$ and $a_{n+1} < a_n$ for every n. $\langle a_n \rangle$ is monotonically decreasing and converges to 0. Hence by Leibnitz test the given series is convergent.

(b) Let $a_n = \frac{1}{\log n}$ so that $a_{n+1} = \frac{1}{\log (n+1)}$. Now $\frac{1}{\log (n+1)} < \frac{1}{\log n}$ because $(n+1) > n$ $\Rightarrow \log (n+1) > \log n$. Thus $a_{n+1} < a_n$, for every n and $\langle a_n \rangle$ is monotonically decreasing and $\langle a_n \rangle$ converges to 0, because $\lim_{n\to\infty} \frac{1}{\log n} = 0$. Hence by Leibnitz test the given series is convergent.

(c) Let $a_n = \frac{n}{n+2}$; $a_{n+1} = \frac{n+1}{n+3}$.

$$a_n - a_{n+1} = \frac{n}{n+2} - \frac{n+1}{n+3} = \frac{n(n+3) - (n+1)(n+2)}{(n+2)(n+3)}$$

$$= \frac{-2}{(n+2)(n+3)} < 0.$$

Thus $a_n < a_{n+1}$, and $\langle a_n \rangle$ is monotonic increasing and $\lim_{n\to\infty} a_n = \lim_{n\to\infty} \frac{n}{n+2} = \lim_{n\to\infty} \frac{1}{1 + \frac{2}{n}} = 1 \neq 0$.

Thus the given series is not convergent.

Exercise (ii) : Determine the radius of convergence of the power series : (a) $\sum_{n=1}^{\infty} (-1)^n \sqrt{n} \left(\frac{x-5}{3}\right)^n$

(b) $\sum_{n=0}^{\infty} \frac{(n!)^2}{(2n)!} x^n$ (c) $\sum_{n=0}^{\infty} 2^n x^n$

Ans : (a) The given series $\sum_{n=1}^{\infty} \frac{(-1)^n \sqrt{n}}{3^n} (x-5)^n$ is of the form $\sum a_n \left(x - x_0\right)^n$ where $a_n = \frac{(-1)^n \sqrt{n}}{3^n}$ and $x_0 = 5$.

$$\lim_{n\to\infty} |a_n|^{1/n} = \lim_{n\to\infty} \left(\sqrt{n} \cdot \frac{1}{3^n}\right)^{1/n} = \lim_{n\to\infty} \left(n^{1/n}\right)^{1/2} \cdot \frac{1}{3} = \frac{1}{3}$$

Hence the radius of convergence is $r = \frac{1}{q} = 3$ and the interval of convergence is $(5 - 3, 5 + 3) = (2, 8)$. This is because $|X| = |x - 5| < 3$.

(b) Let $a_n = \frac{(n\,!)^2}{(2n)\,!}$ so that $a_{n+1} = \frac{[(n+1)\,!]^2}{(2n+2)!}$

$$\frac{a_{n+1}}{a_n} = \frac{[(n+1)\,!]^2}{(2n+2)!} \times \frac{(2n)\,!}{(n\,!)^2} = \frac{(n+1)^2}{(2n+2)(2n+1)}$$

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

$$\therefore \lim_{n\to\infty} \left|\frac{a_{n+1}}{a_n}\right| = \lim_{n\to\infty} \frac{n+1}{2(2n+1)} = \lim_{n\to\infty} \frac{1 + \frac{1}{n}}{2\left(2 + \frac{1}{n}\right)} = \frac{1}{4}$$

Thus radius of convergence is 4 and the interval of convergence is $(-4, 4)$. Let $a_n = 2^n$ so that $\lim_{n\to\infty} |a_n|^{1/n} = 2$. The radius of convergence is $\frac{1}{2}$. When $x = \frac{1}{2}$, the given series is $\sum_0^\infty 1$ which diverges to ∞. When $x = -\frac{1}{2}$ the series oscilates. The interval of convergence is $\left(-\frac{1}{2}, \frac{1}{2}\right)$.

16.7 SUMMARY

The convergence of an infinite series consisting of positive and negative terms has to be treated on a different footing. Two tests of convergence to deal with such series have been stated and proved. The most useful test the Leibnitz test states that the alternating series $\sum a_n$ is convergent if $\sum |a_n|$ is a decreasing sequence. If $\sum a_n$ is an absolutely convergent series then the rearrangement of terms has no effect on its behaviour or sum. The Cauchy product of two infinite series is defined. The Cauchy theorem states that the Cauchy product of two absolutely convergent series is again absolutely convergent. The radius of convergence of a power series is defined. Given a power series theorems for determining radius of convergence are stated and proved.

16.8 MODEL EXAMINATION QUESTIONS

SECTION - A (Long Answers)

(i) State and prove Leibnitz test for the convergence of an alternating series. Apply this to test the convergence of the series : $1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots$

(ii) State Dirichlet's test of convergence of an alternating series and derive Leibnitz test as a special case. Apply the results to discuss the convergence of $\sum_{n=1}^{\infty} \frac{(-1)^n}{\sqrt{n}}$.

(iii) Define the Cauchy product of two infinite series. State and prove Abel's theorem on the Cauchy product of two series.

SECTION - B (Short Answers)

(i) If $\sum_{n=1}^{\infty} a_n$ is an absolutely convergent series prove that $\sum_{n=1}^{\infty} a_{2n}$ and $\sum_{n=1}^{\infty} a_{2n-1}$ Converge and that

$$\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty} a_{2n} + \sum_{n=1}^{\infty} a_{2n-1}.$$

(ii) Discuss the effect of rearrangement of terms on an absolutely convergent series and conditionally convergent series. Justify your answer.

(iii) Discuss the convergence of $\sum_{n=2}^{\infty} \frac{(-1)^n}{\log n}$.

(iv) Show that the Cauchy product of two absolutely convergent series is absolutely convergent.

(v) Find the radius of convergence of $\sum_{n=0}^{\infty} \frac{(n\,!)^2}{(2n)\,!} x^n$.

(vi) If $|x| < 1$, prove that $\left(\frac{1}{1-x}\right) \log\left(\frac{1}{1-x}\right) = \sum_{n=1}^{\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \ldots \frac{1}{n}\right) x^n$.

16.9 ANSWERS TO SELF ASSESSMENT QUESTIONS

SAQ 1 $a_n = \frac{n}{5^n}$; $a_{n+1} = \frac{n+1}{5^{n+1}}$; $a_n - a_{n+1} > 0$ and $\lim a_n = 0$. By Leibnitz test the given series is convergent.

SAQ 2 Let $a_n = \sqrt[n]{n}$. Then $\langle a_n \rangle$ decreases monotonically to 1. Then by Abel's theorem $\sum \sqrt[n]{n}$ is convergent.

SAQ 3 $\frac{a_{n+1}}{a_n} = \frac{x^{n+1}}{(n+1)\,!} \times \frac{n\,!}{x^n} = \frac{x}{n+1}$; $\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = 0$. The radius of convergene is ∞. That is the interval of convergence is $\mathbb{R}$.

BLOCK–5 : CONTINUOUS FUNCTIONS

Unit–17 : Limit of a function

Unit–18 : Properties of continuous functions

Unit–19 : Uniform continuity

Continuous functions form a very important class of functions in the study of the functions in mathematical analysis. Continuous functions satisfy very important requirements. Roughly speaking a continuous function maps "neighbouring points into neighbouring points". The image of an interval under a continuous function is an interval. A continuous function defined on a closed interval is bounded and attains its bounds. Continuity is a local property whereas uniform continuity is a global property.

UNIT–17 : LIMIT OF A FUNCTION

Contents

17.1 Aims and Objectives

17.2 Introduction

17.3 Definition and examples

17.4 Properties of limits

17.5 Workedout exercises

17.6 Summary

17.7 Model Examination Questions

17.8 Answers to Self Assessment Questions

17.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to : (i) Define the limit of a function at a point, (ii) Compute the right hand and left hand limits and examine whether they are equal or not, (iii) State and prove certain important theorems on limits, (iv) Evaluate limits of certain functions at given points.

17.2 INTRODUCTION

The branch of mathematics referred to as mathematical analysis deals with limits of functions and different types of limit operations. The student has already been exposed to the concept of a limit as applied to sequences and series. But sequence is only a special kind of a function. In this unit we would extend the concept to any function in general. Historically, the concept of a limit has troubled the mathematicians for several centuries. With the advent of calculus, there was an explosion of knowledge and enough time was not devoted to explore the implication of concepts like continuity and differntiability of a function. It is only in the last century these concepts were rigorously examined.

17.3 DEFINITIONS AND EXAMPLES

Definition. 1 :

Let S and R be aggregates (that is S and R are subsets of **R**). Let 'a' be a limit of S. Let $f : S \to R$ be a function. Then we say that the 'limit of f as x approaches a' exists if there exists number L having the following property :

Given $\epsilon > 0$, there exists a number δ such that for all $x \in S$ satsifying $0 < |x - a| < \delta$, we have $|f(x) - L| < \epsilon$. We write $\lim_{x \to a} f(x) = L$ or $f(x) \to L$ as $x \to a$.

Remark. 1 : The point 'a' which the existence of the limit of a function is to be examined is a limit point of the domain set. This is a prerequisite. Then only we can find a point in any deleted neighbourhood $0 < |x - a| < \delta$ of the point 'a'.

Remark. 2 : The Limit may or may not exist at a limit point of the given set S.

Remark. 3: The definition of limit at a point does not involve the definition of f at the point. The definition of limit thus ensures the independence of the limit of f at $x \to a$ from the value that f may have at the point a.

Theorem. 1 :

If the limit of a function f exists at a point 'a', then it is unique.

Proof : If possible let L and M be two limits of f as $x \to a$. Let $\epsilon > 0$ be given and $f : S \to R$. Then there exist δ_1 and δ_2 such that

$x \in S, 0 < |x - a| < \delta_1 \Rightarrow |f(x) - L| < \epsilon$.

$x \in S, 0 < |x - a| < \delta_2 \Rightarrow |f(x) - M| < \epsilon$.

Let $\delta = \min(\delta_1, \delta_2)$. Then

$x \in S, 0 < |x - a| < \delta = 1 \Rightarrow |f(x) - L| < \epsilon$, and $|f(x) - M| < \epsilon$.

Now $|L - M| = |L - f(x) + f(x) - M| \leq |L - f(x)| + |f(x) - M| < \epsilon + \epsilon = 2\epsilon$.

Thus for any $\epsilon > 0$, $|L - M| < 2\epsilon \Rightarrow L = M$.

Definition. 2 :

Let $f : S \to R$, where S and R are aggregates. Let a be a limit point of S such that for each $\delta > 0$ there exists $x \in S$ with $a < x < a + \delta$. We say that the 'limit of f as x approaches 'a' from right' exists if there is a number L with the following property :

For $\epsilon > 0$, there exists a number δ such that $|f(x) - L| < \epsilon$ for all $x \in S$ with $a < x < a + \delta$.

We write $\lim_{x \to a^+} f(x) = L$ or $f(x) \to L$ as $x \to a^+$. Similarly, we say that the 'limit of f as x approahces 'a' from the left' exists if there is a number M with the following property :

For $\epsilon > 0$, there exists a number $\delta > 0$ such that $|f(x) - M| < \epsilon$ for all $x \in S$ with $a - \delta < x < a$.

We write $\lim_{x \to a^-} f(x) = M$ or $f(x) \to M$ as $x \to a^-$.

Remark. 4 : The number $|f(x) - L|$ can be thought of as the error in approximating of $f(x)$ to L. The definition $f(x) \to L$ as $x \to a^+$, then, can be thought of as an affordable error we can make in approximating $f(x)$ to L as minimal as possible by taking x sufficiently close to a from the right. A similar interpretation can be given to left hand limits.

Remark. 5 : $\lim_{x \to a} f(x)$ exists if and only if both the right hand and left hand limits exist and are equal.

Example. 1 : If f is a constant function defined by $f(x) = c$ for all $x \in \mathbf{R}$, then at any point $a \in \mathbf{R}$, $\lim_{x \to a} f(x) = c$.

Example. 2 : If $f : \mathbf{R} \to \mathbf{R}$ is a function defined by

$$f(x) = \frac{|x - 4|}{x - 4}; \text{ if } x \neq 4$$

$$= 0, \text{ if } x = 4$$

then $\lim_{x\to 4} f(x)$ does not exist. To see this let $x = 4 + \epsilon, \epsilon > 0$. Then $\lim_{x\to 4} f(x) = \lim_{\epsilon\to 0} \frac{\epsilon}{\epsilon} = 1$. If $x = 4 - \epsilon, \epsilon > 0$, then $\lim_{x\to 4} f(x) = \lim_{\epsilon\to 0} \frac{\epsilon}{-\epsilon} = -1$. Thus the limit of the function depends on the direction of approach of x to 4. That is, the left hand limit ≠ the right hand limit at $x = 4$. Then $\lim_{x\to 4} f(x)$ does not exist.

SAQ 1 Show that $\lim_{x\to 0} \frac{|x|}{x}$ does not exist.

Example. 3 : Let $f : \mathbf{R} \to \mathbf{R}$ be given by $f(x) = 3x^2 - 2x$. Then $\lim_{x\to 2} f(x) = 8$. To see this consider $|f(x) - 8| = |3x^2 - 2x - 8| = |3x + 4|\,|x - 2|$. Let $\epsilon > 0$ be given. Choose N such that $0 < \frac{13}{N} < 1$ and $0 < \frac{\epsilon}{N} < 1$ choose $\delta = \frac{\epsilon}{N}$. Then $\delta < \frac{\epsilon}{13}$. If $0 < |x - 2| < \delta$, then $2 - \delta < x < 2 + \delta$. Then $10 - 3\delta < 3x + 4 < 10 + 3\delta$. If $\delta < 1$, then $7 < 3x + 4 < 13$ and $< |3x + 4|\,|x - 2| < 13\,\delta < \epsilon$.

Example. 4 : Let $f : \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = \begin{cases} 1 \text{ if } 0 < x < 1 \\ x \text{ if } 1 \le x < \infty \end{cases}$. Then $\lim_{x\to 1} f(x) = 1$ because $\lim_{x\to 1^+} f(x) = \lim_{x\to 1^-} f(x) = 1$.

Example. 5 : Let $f : \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = \begin{cases} 2 \text{ if } 0 < x < 1 \\ x \text{ if } 1 < x < \infty \end{cases}$. Then $\lim_{x\to 1} f(x)$ does not exist because $\lim_{x\to 1^+} f(x) = 1$ and $\lim_{x\to 1^-} f(x) = 2$ and are not equal.

Example. 6 : Let $S = (0, 1]$. That is $S = \{x \in \mathbf{R} \mid 0 < x \le 1\}$. Let $f : S \to S$ be defined by $f(x) = x$. Then f is not defined at $x = 0$. But $\lim_{x\to 0^+} f(x) = 0$.

Example. 7 : $\lim_{x\to 0} x \sin\frac{1}{x} = 0$. To see this we write $\left|x \sin\frac{1}{x}\right| = |x|\,|\sin x| < |x|$, because $|\sin\theta| \le 1$. Let $\epsilon > 0$ be given. Choose $\delta = \epsilon$. Then $\left|x \sin\frac{1}{x}\right| < x$ when $0 < |x| < \delta$. Thus $\lim_{x\to 0} x \sin\frac{1}{x} = 0$.

Example. 8 : Let $f : \mathbf{R} \to \mathbf{R}$ be defined by

$$f(x) = \begin{cases} 3x - 1, \text{ if } x < 0 \\ 0, \text{ if } x = 0 \\ 2x + 4, \text{ if } x = 0 \end{cases}$$

$$\lim_{x\to 1} f(x) = \lim_{x\to 1} (2x + 4) = 6.$$

$$\lim_{x\to -2} f(x) = \lim_{x\to -2} (3x - 1) = -7.$$

$$\lim_{x\to 0^+} f(x) = \lim_{x\to 0^+} (2x + 1) = 4$$

$$\lim_{x\to 0^-} f(x) = \lim_{x\to 0^-} (3x - 1) = -1$$

$\lim_{x\to 0} f(x)$ does not exist.

Definition. 3 :

> The function f (defined on Reals) is said to tend to $+\infty$ as x approaches a, if for each real number $B > 0$, there exists a number $\delta > 0$ such that $|x - a| < \delta \Rightarrow f(x) > B$.

Similarly the function f is said to tend to $-\infty$ as $x \to a$ if for each $B > 0$, there exists $\delta > 0$ such that $|x - a| < \delta \Rightarrow f(x) < -B$.

The function f is said to tend to $+\infty$ as $x \to \infty$ if for $B > 0$, there exists $\delta > 0$ such that

$$x > \delta \Rightarrow f(x) > B.$$

Example. 9 : $\lim_{x\to\infty} \frac{1}{x} = \lim_{x\to-\infty} \frac{1}{x} = 0.$

Example.10 : If $f(x) = \frac{1}{1-x}$, $0 \le x < 1$, then

$$\lim_{x\to1^+} f(x) = \lim_{x\to1^-} f(x) = \infty.$$

17.4 PROPERTIES OF LIMITS

Theorem. 2:

> If $f : S \to R$ is a function, $a \in S'$, then the following statements are equivalent.
>
> (i) $\lim_{x\to a} f(x)$ exists
>
> (ii) For $\epsilon > 0$, there exists a number $\delta > 0$ such that
>
> $x, y \in S, 0 < |x - a| < \delta, 0 < |y - a| < \delta$
>
> $\Rightarrow |f(x) - f(y)| < \epsilon$
>
> (iii) For every sequence $\{x_n\}$ in $S - \{a\}$ converging to a,
>
> the sequence $\{f(x_n)\}$ converges.

Proof : **(i) $\Rightarrow$ (ii) :** Let $\lim_{x\to a} f(x) = L$. Then given $\epsilon > 0$, there exists $\delta > 0$ such that

$$x \in S, 0 < |x - a| < \delta \Rightarrow |f(x) - L| < \epsilon/2.$$

$$\therefore x, y \in S, 0 < |x - a| < \delta, 0 < |y - a| < \delta \Rightarrow$$

$$|f(x) - f(y)| = |f(x) - L + L - f(y)|$$

$$\le |f(x) - L| + |L - f(y)| < \epsilon.$$

(ii) $\Rightarrow$ (iii) : Given $\epsilon > 0$, suppose there exists $\delta > 0$ such that the conclusion in (ii) is true. Consider a sequence $\{x_n\}$ in $S - \{a\}$ which converges to a. Then for $\delta > 0$, $\exists\, n \in N$ such that $n \ge M \Rightarrow 0 < |x_n - a| < \delta$.

Now take $m, n \ge M$. Then

$$m, n \ge M \Rightarrow |x_m - a| < \delta \text{ and } 0 < |x_n - a| < \delta.$$

$$\Rightarrow |f(x_m) - f(x_n)| < \epsilon \text{ by (ii)}$$

$$\Rightarrow \{f(x_n)\} \text{ is a cauchy sequence in } \mathbf{R} \text{ and hence converges.}$$

(iii) $\Rightarrow$ (i) : Suppose (iii) is true. If $\{x_n\}$ is a sequence in $S - \{a\}$ which converges to 'a', let $\lim_{n\to\infty} f(x_n) = L$. Note that this limit is independent of the choice of $\{x_n\}$ in $S - \{a\}$. [see note

below]. We shall show that $\lim_{x\to a} f(x) = L$. If this limit is not L, then for some $\epsilon > 0$ and for any $\delta > 0$, there exists $x \in S$ with

$$0 < |x - a| < \delta \text{ and } |f(x) - L| \geq \epsilon \qquad (1)$$

Taking $\delta = \frac{1}{n} (n \in N)$, let the points x given by (1) be denoted by x_n. Then $\{x_n\}$ is a sequence in $S - \{a\}$ converging to a and hence by hypothesis $\{f(x_n)\}$ converges to L. But this contradicts (1).

$$\therefore \lim_{x\to a} f(x) = L.$$

Note : Let $\lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n = a$ with $x_n, y_n \in S - \{a\}; n \in N$.

If we define $\{z_n\}$ such that $z_{2n} = y_n, z_{2n-1} = x_n$

$(n \in N)$, then $\{z_n\}$ is a sequence in $S - \{a\}$ converging to 'a'.

Let $\lim_{n\to\infty} f(z_n) = L$. Since $\{f(x_n)\}$ and $\{f(y_n)\}$ are subsequences of $\{f(z_n)\}$, we have $\lim_{n\to\infty} f(x_n) = \lim_{n\to\infty} f(y_n) = \lim_{n\to\infty} f(z_n) = L$.

Theorem. 3 :

Let $S \subset \mathbf{R}$, f, g be two functions from S into R, $a \in S'$, $\lim_{x\to a} f(x) = L$,

$\lim_{x\to a} g(x) = M$.

$(L, M \in \mathbf{R})$. Then

(i) $\lim_{x\to a} (f + g)(x)$ exists and is equal to L + M.

(ii) $\lim_{x\to a} (fg)(x)$ exists and is equal to LM.

(iii) If $M \neq 0$ and S_0 be the subset of S consisting of all x such that $g(x) \neq 0$.

Then $a \in S_0'$ and $\lim_{x\to a} \left(\frac{f}{g}\right)(x)$ exists and is equal to L/M.

Proof : (i) Let $\epsilon > 0$ be given. For $\epsilon/2 > 0$, $\exists\ \delta_1$ and δ_2 such that

$x \in S, 0 < |x - a| < \delta_1 \Rightarrow |f(x) - L| < \epsilon/2$

and $x \in S, 0 < |x - a| < \delta_2 \Rightarrow |g(x) - M| < \epsilon/2$

If $\delta = \min(\delta_1, \delta_2)$, then

$x \in S, 0 < |x - a| < \delta \Rightarrow |f(x) - L| < \epsilon/2$ and $|g(x) - M| < \epsilon/2$.

$$\Rightarrow |f(x) - g(x) - (L + M)| \leq |f(x) - L| + |g(x) - M| < \epsilon$$

$\therefore \lim_{x\to a} (f + g)(x) = L + M$.

(ii) Given $\epsilon > 0$, there exist numbers δ_1 and δ_2 such that

$$x \in S, 0 < |x - a| < \delta_1 \Rightarrow |f(x) - L| < \frac{1}{2} \cdot \frac{\epsilon}{|M| + \epsilon} \qquad \ldots (1)$$

$$x \in S, 0 < |x - a| < \delta_2 \Rightarrow |g(x) - M| < \frac{1}{2} \cdot \frac{\epsilon}{|L| + \epsilon} \qquad \ldots (2)$$

Also, for $\epsilon > 0, \exists\ \delta_3 > 0$ such that

$$x \in S, 0 < |x - a| < \delta_3 \Rightarrow |f(x) - L| < \epsilon$$

$$\Rightarrow ||f(x)| - |L|| < \epsilon$$

$$\left(\because ||f(x)| - |L|| < |f(x) - L|\right)$$

$$\Rightarrow |f(x)| < |L| + \epsilon \qquad \ldots (3)$$

If $\delta = \min\left(\delta_1, \delta_2, \delta_3\right)$, then for $0 < |x - a| < \delta$, all the three relations on the RHS of (1), (2) and (3) hold

$$\begin{aligned}
\therefore |f(x)\, g(x) - LM| &= |f(x)\, g(x) - f(x)\, M + f(x)\, M - LM| \\
&\leq |f(x)\, g(x) - f(x)\, M| + |f(x)\, .\, M - LM| \\
&\leq |f(x)|\, |g(x) - M| + |f(x) - L|\, |M| \\
&< [|L| + \epsilon] \cdot \frac{1}{2} \cdot \frac{\epsilon}{|L| + \epsilon} + \frac{1}{2} \cdot \frac{\epsilon}{|M| + \epsilon}\, |M| \\
&< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.
\end{aligned}$$

(iii) We shall first show that $a \in S_0'$. We claim that every neighbourhood of a has a point $x \neq a$, $x \in S$ such that $g(x) \neq 0$. If this is not so, let $\delta_1 > 0$ be such that $g(x) = 0\ \forall\ x \in N\left(\delta_1, a\right) - \{a\}$ and $x \in S$. Since $\lim_{x \to a} g(x) = M\ (\neq 0)$, given $\epsilon < |M|$ there exists a number $\delta_2 > 0$ such, that $x \in S$, $0 < |x - a| < \delta_2 \Rightarrow |g(x) - M| < \epsilon$. If $\delta = \min\left(\delta_1, \delta_2\right)$ then

$x \in S, 0 < |x - a| < \delta \Rightarrow |g(x) - M| = |M| < \epsilon < |M|$.

This contradiction shows that given $\delta_1 > 0$ then

$g(x) \neq 0$ for some $x \in N\left(\delta_1, a\right) - \{a\}$ and $x \in S$. Hence $a \in S_0'$.

We shall now show that $\lim_{x \to a} \left(\frac{1}{g}\right)(x) = \frac{1}{M}$

Given $\epsilon > 0$, let $\epsilon_1 = \min\left(\frac{\epsilon\, |M|^2}{2}, \frac{|M|}{2}, \epsilon\right)$. Then there exists a number δ such that

$$x \in S_0, 0 < |x - a| < \delta \Rightarrow |g(x) - M| < \epsilon_1$$

$$\Rightarrow |g(x)| > |M| - \epsilon_1$$

$$\geq |M| - \frac{|M|}{2} = \frac{|M|}{2}$$

$$\Rightarrow \left|\frac{1}{g(x)} - \frac{1}{M}\right| = \frac{|M - g(x)|}{|M|\, |g(x)|}$$

$$< \frac{1}{|M|} \cdot \frac{\epsilon\, |M|^2/2}{|M|/2} = \epsilon.$$

$$\therefore \lim_{x \to a} \left(\frac{1}{g}\right)(x) = \frac{1}{M}$$

Now, applying the product rule (ii) we have

$$\lim_{x \to a} \left(\frac{f}{g}\right)(x) = \lim_{x \to a} \left(f \cdot \frac{1}{g}\right)(x) = L \cdot \frac{1}{M} = \frac{L}{M}$$

Remark. 4 : Under the conditions of the theorem, if c is any number then $\lim_{x\to a} c f(x) = c\,L$.

Remark. 5 : $\lim_{x\to a} (f-g)(x) = \lim_{x\to a} [f(x) - g(x)] = L - M$.

Remark. 6 : Let g be a bounded function defined on S, $a \in S'$ and $f : S \to R$ be a function such that $\lim_{x\to a} f(x) = 0$. Then $\lim_{x\to a} f(x)\, g(x) = 0$.

Theorem. 4 :

> Let S be an aggregate, $a \in S'$ and f, g be functions from S to R. Let $\lim_{x\to a} f(x) = L$ and $\lim_{x\to a} g(x) = M$ and $g(x) \le f(x)$ for all $x \in N(\delta, a) - \{a\}, x \in S$ for some δ. Then $M \le L$.

Proof : Let $\phi(x) = f(x) - g(x)$. Then $\phi(x) \ge 0$ for

$x \in N(\delta, a) - \{a\}, x \in S.$ ... (1)

$\lim_{x\to a} \phi(x) = \lim_{x\to a} (f-g)(x) = L - M$ (=K say).

It will suffice to prove that $K \ge 0$.

If $K < 0$, then there exists $\delta > 0$ such that

$$x \in S, 0 < |x - a| < \delta \Rightarrow |\phi(x) - K| < \frac{|K|}{2}.$$

$$\Rightarrow \phi(x) < K + \frac{|K|}{2} = \frac{K}{2} < 0 \qquad (\because K < 0)$$

But this contradicts (1).

Theorem. 5 :

> Let f, g, h be functions from S to R, $a \in S'$ and $\lim_{x\to a} f(x) = \lim_{x\to a} g(x) = L$. Also let $g(x) \le h(x) \le f(x)$ for all $x \in N(\delta_1, a) - \{a\}$ and $x \in S$ and for some $\delta_1 > 0$. Then $\lim_{x\to a} h(x) = L$.

Proof : Given $\epsilon > 0$, $\exists\, \delta_2 > 0$ such that

$$x \in S, 0 < |x - a| < \delta_2 \Rightarrow |f(x) - L| < \epsilon/3 \text{ and } |g(x) - L| < \epsilon/3.$$

$$\Rightarrow |f(x) - g(x)| < 2\epsilon/3.$$

If $\delta = \min(\delta_1, \delta_2)$ then for $x \in S$, $0 < |x - a| < \delta$ we have

$$\begin{aligned} |h(x) - L| &\le |h(x) - f(x)| + |f(x) - L| \\ &\le |g(x) - f(x) + |f(x) - L| \\ &< 2\epsilon/3 + \epsilon/3 = \epsilon. \end{aligned}$$

Remark. 7 : If the condition in the statement of the theorem is changed to $g(x) \ge h(x) \ge f(x)$, the same result still holds.

SAQ 2 Let $f(x) = \frac{1}{x}$, $(0 < x < \infty)$; $g(x) = x + \frac{1}{x}$, $(0 < x < \infty)$. What is $\lim_{x\to\infty} f(x)\, g(x)$?

SAQ 3 Evaluate $\lim_{x\to 1} \frac{x^2 - 4}{x^2 - 2}$.

SAQ 4 Evaluate $\lim_{\theta\to 0} \frac{\sin\theta}{\theta}$.

17.5 WORKEDOUT EXCERCISES

Exercise. 1 : Evaluate $\lim_{x\to 0} \frac{e^{1/x}}{e^{1/x}+1}$ if it exists.

Ans : As $x \to 0^+$; $\frac{1}{x} \to \infty$ and $e^{-1/x} \to 0$ and as $x \to 0^-$, $\frac{1}{x} \to -\infty$ and $e^{1/x} \to 0$.

Thus $\lim_{x\to 0^+} \frac{e^{1/x}}{e^{1/x}+1} = \lim_{x\to 0^+} \frac{1}{1+e^{-1/x}} = 1.$

$\lim_{x\to 0^-} \frac{e^{1/x}}{e^{1/x}+1} = \frac{0}{1} = 0.$

Since the left hand limit ≠ right hand limit, $\lim_{x\to 0} \frac{e^{1/x}}{e^{1/x}+1}$ does not exist.

Exercise. 2 : Let f: **R** → **R** be defined by

$$f(x) = \begin{cases} 3-x, & \text{if } x > 1 \\ 1 & \text{if } x = 1 \\ 2x & \text{if } x < 1 \end{cases}$$

sketch the graph of $f(x)$ and show that $\lim_{x\to 1} f(x) = 2$. Is $\lim_{x\to 1} f(x) = f(1)$?

Ans : Let $\epsilon > 0$ be given. As $x \to 1^-$, we must find δ with $1-\delta < x < 1$ such that $|f(x) - 2| < \epsilon$. Since x is approaching 1 from the left, $x < 1$ and $f(x) = 2x$. Thus $|2x - 2| < \epsilon$ or $1 - \frac{\epsilon}{2} < x < 1 + \frac{\epsilon}{2}$. Thus we are required to find $\delta > 0$ such that $1 - \frac{\epsilon}{2} < x < 1 + \frac{\epsilon}{2}$ provided that $1 - \delta < x < 1$. Thus given $\epsilon > 0$, we can choose $\delta = \frac{\epsilon}{2}$ to satisfy the given requirement.

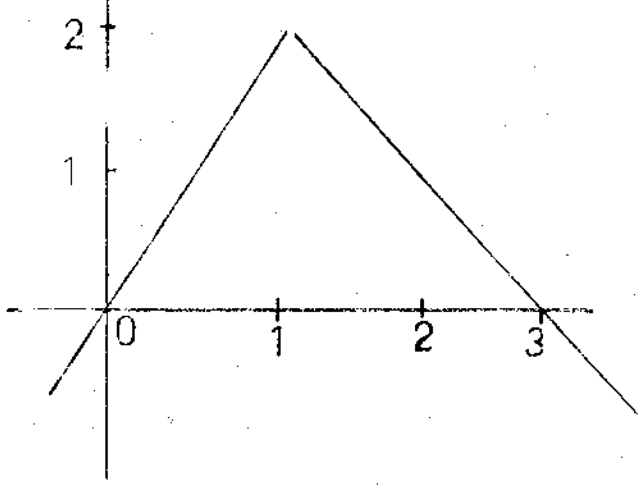


Fig.

Similarly $f(x) \to 2$ as x approaches 1 from the right. That is $f(x) \to 2$ as $x \to 1^+$. Let $\epsilon > 0$ be given. Then we must find $\delta > 0$ such that $|f(x) - 2| < \epsilon$ for $1 < x < 1 + \delta$. Since $x > 1$, $f(x) = 3 - x$. Thus $|f(x) - 2| = |3 - x - 2| = |1 - x| < \epsilon$ or $1 - \epsilon < x < 1 + \epsilon$. Choosing $\epsilon = \delta$ we see that the given requirement is satsified.

Since $\lim_{x\to 1^+} f(x) = \lim_{x\to 1^-} f(x) = 2$, we conclude that $\lim_{x\to 1} f(x) = 2$. But $f(1) = 1$. Thus

$\lim_{x\to 1} f(x) \neq f(1)$.

Exercise. 3 : Suppose that $\lim_{x\to a} f(x) = l$. If $l > 0$, show that there exists some $\delta' > 0$, such that

$f(x) > 0$ for $|x - a| < \delta', x \neq a$.

Ans : $\lim_{x\to a} f(x) = l$. Let $\epsilon > 0$ be given. Then there exists $\delta > 0$ such that $|f(x) - l| < \epsilon$, for $|x - a| < \delta$. Since this holds good for any ϵ, this must be true for $\epsilon = l$ as well. Let $\delta = \delta'$ in this situation. Thus for $\delta' > 0$ $|f(x) - l| < l$ for $|x - a| < \delta'$ or $l - l < f(x) < l + l$ or $0 < f(x) < 2l$ for $|x - a| < \delta'$. Thus $f(x) > 0$ for $|x - a| < \delta'$ and $x \neq a$.

Exercise. 4 : Let $f : \mathbf{R} \to \mathbf{R}$ be defined by

$$f(x) = \begin{cases} 1, \text{ if } x \text{ is rational} \\ 0, \text{ if } x \text{ is irrational} \end{cases}$$

show that $\lim_{x\to 0} f(x)$ does not exist.

Ans : Consider two sequences $\langle x_n \rangle$ and $\langle y_n \rangle$ defined by $x_n = \frac{1}{n}$ and $y_n = \frac{\sqrt{2}}{n}$. Then $f(x_n) = 1$ and $\lim_{n\to\infty} f(x_n) = 1$. $f(y_n) = 0$ and $\lim_{n\to\infty} f(y_n) = 0$. Then by theorem 2 of this unit, $\lim_{x\to 0} f(x)$ does not exist.

17.6 SUMMARY

The limit of a function f as the variable approaches a given real number 'a' is that unique real numbers l, such that the difference between $f(x)$ and l approaches zero as the difference between x and a approaches zero. This approach of x to a must be independent of the path that x takes to reach a. If left hand limit (or the value of f obtained by letting x approach 'a' from the left) is different from the right hand limit (or the value of f obtained by letting x approach 'a' from the right), then limit of f does not exist. The limit of a function at a point, if it exists is unique. The limits of sum, product and quotient (if properly defined) of functions equals the sum, product and quotient of their limits respectively, provided that they are properly defined. If $\langle x_n \rangle$ is a sequence of real numbers such that $x_n \to a$ as $n \to \infty$, then $f(x) \to l$ as $x \to a$ if and only if $f(x_n) \to l$ as $n \to \infty$.

17.7 MODEL EXAMINATION QUESTIONS

SECTION - A (Long Answers)

(i) Let S and R be aggregates and $f : S \to R$ with $a \in S'$, the derived set of S. Show that the following statements are equivalent

(a) $\lim_{x\to a} f(x)$ exists

(b) for $\epsilon > 0$, there exists $\delta > 0$ such that $x, y \in S, 0 < |x - a| < \delta$,

$0 < |y - a| < \delta \Rightarrow |f(x) - f(y)| < \epsilon$.

(c) For every sequence $\langle x_n \rangle$ in $S - \{a\}$, converging to a, the sequence $\langle f(x_n) \rangle$ converges.

(ii) If $S \subseteq R$ and $a \in S'$, the derived set of S and $\lim_{x\to a} f(x) = l$, $\lim_{x\to a} g(x) = m$, then prove that

$\lim_{x\to a} (f+g)(x) = l + m$; $\lim_{x\to a} (fg)x = lm$; $\lim_{x\to a} \left(\frac{f}{g}\right)(x) = \frac{l}{m}$ if $m \neq 0$.

SECTION - B (Short Answers)

(i) If f and g are functions defined from aggregates S to R such that $\lim_{x\to a} f(x) = l$, $\lim_{x\to a} g(x) = m$ and $g(x) \leq f(x)$ for all x in the deleted neighbourhood of a, then prove that $m \leq l$.

(ii) Define the limit of a function at a point, the right hand and left hand limits at that point. Apply these definitions to discuss the existence of $\lim_{x\to 4} \frac{|x-4|}{x-4}$.

(iii) Show that $\lim_{x\to a} f(x)$, if it exists, is unique. Show that $\lim_{x\to 0} \frac{e^{1/x} - 1}{e^{1/x} + 1}$ does not exist.

17.8 ANSWERS TO SAQ'S

SAQ 1 $\lim_{x\to 0^+} \frac{|x|}{x} = 1$ and $\lim_{x\to 0^-} \frac{|x|}{x} = -1$. Thus $\lim_{x\to 0^+} \frac{|x|}{x} \neq \lim_{x\to 0^-} \frac{|x|}{x}$. Thus $\lim_{x\to 0} \frac{|x|}{x}$ doesn't exist.

SAQ 2 $\lim_{x\to\infty} f(x) = 0$ and $\lim_{x\to\infty} g(x) = \infty$.

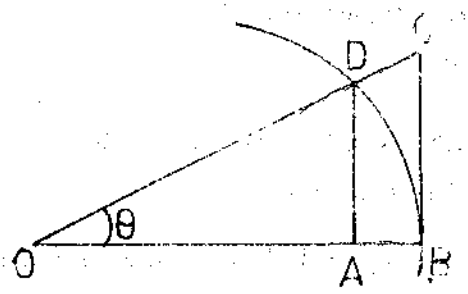
$\lim_{x\to\infty} (f(x) \cdot g(x)) = (0) \left(\infty + \frac{1}{x^2}\right) = 1$.

SAQ 3 $\lim_{x\to 1} \frac{x^2+4}{x^2-2} = \frac{1+4}{1-2} = -5$.

SAQ 4 Consider a sector OBD of unit radius (OB = OD = 1 unit) and let $\angle DOB = \theta$, θ, very small. DA $\perp$ OB and CB $\perp$ OB. Then area of Δ OAD < Area of sector OBD < Area of Δ OBC. That is $\frac{1}{2}\sin\theta\cos\theta < \frac{1}{2}\theta < \frac{1}{2}\tan\theta$.

$\cos\theta < \frac{\theta}{\sin\theta} < \frac{1}{\cos\theta}$. As $\theta \to 0$; $\cos\theta \to 1$.

Thus $1 \leq \lim_{\theta\to 0} \frac{\theta}{\sin\theta} \leq 1$ and hence $\lim_{\theta\to 0} \frac{\theta}{\sin\theta} = 1$, or $\lim_{\theta\to 0} \frac{\sin\theta}{\theta} = 1$.



UNIT–18 : PROPERTIES OF CONTINUOUS FUNCTIONS

Contents

18.1 Aims and Objectives

18.2 Introduction

18.3 Definition and Examples

18.4 Properties of continuous functions

18.5 Worked out exercises

18.6 Summary

18.7 Sample Examination Questions

18.8 Answers to Self Assessment Questions

18.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to (i) Define the continuity of a function at a point and in an inverval and give examples, (ii) Distinguish between various types of discontinuities, (iii) Prove that a continuous function defined on a closed interval is bounded and attains its bounds, (iv) Prove that a continous function f defined on $[a, b]$ assumes every value between $f(a)$ and $f(b)$.

18.2 INTRODUCTION

Continuous functions constitute one of the most important classes of functions in the study of Mathematical Analysis. Intuitively there is an obvious connection between the graph of a function and the continuity of a function in a given interval. Interpreted geometrically, this means that the graph of a continuous function is unbroken or the graph could be traced continuously without lifting the pencil from the paper. These notions, however, are very vague, not precisely mathematical and tend to give wrong conclusions. We have seen in unit 17, that $\lim_{x \to a} f(x)$ exists but may be different from $f(a)$. Such examples are examples of functions which are not continuous at $x = a$. Continuous functions have very nice properties. These functions have a very important role to play in the coming units.

18.3 DEFINITIONS AND EXAMPLES

Definition. 1 :

Let A and B be aggregates and $f : A \to B$. The function f is said to be continuous at $a \in A$ if $\lim_{x \to a} f(x) = f(a)$. This means that (i) f is defined at 'a' or $f(a)$ exists, (ii) $\lim_{x \to a} f(x)$ exists and (iii) $\lim_{x \to a} f(x) = f(a)$. Equivalently f is continuous at 'a' if for any given $\epsilon > 0$, there exists $\delta > 0$ such that $|x - a| < \delta \Rightarrow |f(x) - f(a)| < \epsilon$.

Definition. 2 :

A function $f: A \to B$, is said to be continuous on an interval $I \subset A$, if f is continuous at every point of I.

Remark. 1 : If f is not continuous at a point 'a', then it is said to be discontinuous at 'a'.

Remark. 2 : If $\lim_{x \to a} f(x) = l$ exists and $f(a) \neq l$, then we say that f has a removable discontinuity at 'a'. We can define a new function g by $g(x) = f(x)$ for all $x \neq a$ in the domain of definition of f and define $g(a) = l$. Then g is continuous at 'a'. If the right hand and left hand limits of f at a exist but are not equal, then we say that f has a jump discontinuity at a. A removable discontinuity or a jump discontinuity is called a simple discontinuty. A discontinuity which is not a simple discontinuity is called an infinite discontinuity. Some authors use the terms "discontinuity of first kind of the left had and right hand limits exist and are not equal and the term "discontinuity of second kind if these limits do not exist".

SAQ 1 Verify that $f(x) = \frac{\sin x}{x}$, $x \neq 0$ and $f(0) = 1$ is continuous at $x = 0$.

Example. 1 : The function $f: \mathbf{R} \to \mathbf{R}$ given by $f(x) = c$ (constant) is continuous.

Given $\epsilon > 0$, choosing any $\delta > 0$ we have

$x \in \mathbf{R}, |x - a| < \delta \Rightarrow |f(x) - f(a)| = |c - c| = 0 < \epsilon$.

Example. 2 : The function $f: \mathbf{R} \to \mathbf{R}$ given by $f(x) = x$ is continuous.

Given $\epsilon > 0$, choosing $\delta = \epsilon$ we have

$x \in \mathbf{R}, |x - a| < \delta \Rightarrow |f(x) - f(a)| = |x - a| < \delta = \epsilon$.

Example. 3 : The function $f: \mathbf{R} \to \mathbf{R}$ given by $f(x) = x^2$ is continous.

Given $\epsilon > 0$, choosing $\delta = |x| + \sqrt{x^2 + \epsilon}$, we have

$x, y \in \mathbf{R}, |x - y| < \delta \Rightarrow |x + y| = |y - x + 2x|$

$\leq |y - x| + 2|x| < \delta + 2|x|$

$\therefore |x + y| < |x| + \sqrt{x^2 + \epsilon}$

$\therefore |f(x) - f(y)| = |x^2 - y^2|$

$= |x - y|\,|x + y| < \delta\left[|x| + \sqrt{x^2 + \epsilon}\right] = \epsilon$

$\therefore$ Given $\epsilon > 0$, we have found a number δ such that

$x, y \in \mathbf{R}, |x - y| < \delta \Rightarrow |f(x) - f(y)| < \epsilon$.

Example. 4 : The function $f: \mathbf{R} \to \mathbf{R}$ given by

$f(x) = x$ when x is irrational

$= -x$ when x is rational

continuous only at $x = 0$.

Given $\epsilon > 0$, let $\delta = \epsilon/2$. (or any number $< \epsilon$).

Then $x \in \mathbf{R}, |x - 0| < \delta \Rightarrow |f(x) - f(0)| = |x| < \epsilon$.

$\therefore \lim_{x \to 0} f(x) = f(0) = 0$.

The function is continuous at $x = 0$.

Let $x \neq 0$ be any rational number. Then $f(x) = -x$. There exists an irrational number x_n such that $|x_n - x| < \frac{1}{n}$ $(n \in N)$. Then $\{x_n\}$ is a sequence of irrational numbers such that $\lim_{n\to\infty} x_n = x$. Now $\lim_{n\to\infty} f(x_n) = \lim_{n\to\infty} x_n = x \neq -x = f(x)$. The function is not continuous at any non zero rational number. In a similar way we can prove that f is not continuous at any irrational number.

Example. 5 : A function f is defined on [0, 1] by

$$f(x) = \begin{cases} -x^2 & \text{if } x \leq 0 \\ 5x - 4 & \text{if } 0 < x \leq 1 \\ 4x^2 - 3x & \text{if } 1 < x < 2 \\ 3x + 4 & \text{if } x \geq 2 \end{cases}$$

Examine the continuity of f at $x = 0, 1, 2$.

We shall directly verify the continuity by verifying the equality or otherwise, of the limits from right and left.

$$\lim_{x\to 0-} f(x) = \lim_{x\to 0-} (-x^2) = 0$$

$$\lim_{x\to 0+} f(x) = \lim_{x\to 0+} (5x - 4) = -4$$

The two limits are not equal. The given function is not continuous at $x = 0$.

$$\lim_{x\to 1-} f(x) = \lim_{x\to 1-} 5x - 4 = 1$$

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

The two limits are equal and hence the given function is not continuous at $x = 1$.

It is left as an exercise to the student to verify the continuity at $x = 2$.

Example. 6 : $f: \mathbf{R} \to \mathbf{R}, f(x) = \frac{x - |x|}{x}$ $(x \neq 0), f(0) = 0$, is continuous for all $x \in \mathbf{R}$ except $x = 0$

$$\text{for } x < 0, f(x) = \frac{x + x}{x} = 2 \qquad [\because |x| = -x \text{ if } x < 0]$$

$$\text{for } x > 0, f(x) = \frac{x - x}{x} = 0.$$

$\therefore f$ is continuous for all $x < 0$ and for all $x > 0$ (example. 1)

$$\text{Also } \lim_{x\to 0-} f(x) = 2, \lim_{x\to 0+} f(x) = 0.$$

$\therefore f$ is not continuous at $x = 0$.

Example. 7 : $f: \mathbf{R} \to \mathbf{R}, f(x) = \frac{x - |x|}{x}$ if $x \neq 0$,

$= 2$ if $x = 0$,

is continuous at all points of $\mathbf{R}$ except at $x = 0$. (verify).

Example. 8 : $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = [x]$ [the integral part of x] is not continuous at $x = 3$.

$$\lim_{x \to 3-} f(x) = \lim_{x \to 3-} \{x - [x]\} = 3 - 2 = 1.$$

$$\lim_{x \to 3+} f(x) = \lim_{x \to 3+} \{x - [x]\} = 3 - 3 = 0.$$

In fact f is not continuous at any integral value of x.

18.4 PROPERTIES OF CONTINUOUS FUNCTIONS

Theorem. 1 :

> Let f, g be functions defined on S and continuous at $a \in S$. Then $f + g$ and fg are continuous at 'a'. If $g(a) \neq 0$, then $\frac{f}{g}$ is continuous at a $\left(\frac{f}{g}\right.$, viewed as a function on the set S_0 consisting of all $x \in S$ such that $g(x) \neq 0$).

Proof : Workedout in exercises. But the student is advised to attempt the proof.

Theorem. 2 :

> Let S, T be two aggregates. Let $f : S \to T$ and $g : T \to R$ be functions. Let $a \in S$ and $b = f(a)$. Assume that f is continuous at 'a' and g is continuous at 'b'. Then the composition $g \circ f$ is continuous at 'a'.
>
> This result can be expressed as $\lim_{x \to a} g(f(x)) = g\left(\lim_{x \to a} f(x)\right)$.

Proof : Given $\in > 0$, $\exists\ \delta_1 > 0$ such that

$$y \in T, |y - b| < \delta_1 \Rightarrow |g(y) - g(b)| < \in \qquad \ldots (1)$$

Given $\delta_1 > 0$, $\exists\ \delta_2$ such that

$$x \in S, |x - a| < \delta_2 \Rightarrow |f(x) - b| < \delta_1$$

$$\Rightarrow |g(f(x)) - g(b)| < \in \text{ by (1)}$$

$$\Rightarrow |g(f(x)) - g(f(a))| < \in.$$

Theorem. 3 :

> A function $f : S \to R$ is continuous at a point $a \in S$ if and only if $f(x_n) \to f(a)$ for every sequence $\{x_n\}$ converging to a in S.

Proof : Let f be continuous at $a \in S$ and let $\{x_n\}$ be a sequence converging to $a \in S$. Given $\in > 0$, $\exists$ $\delta > 0$ such that

$$x \in S, |x - a| < \delta \Rightarrow |f(x) - f(a)| < \in \qquad \ldots (1)$$

Also we can find $n \geq N$ such that

$$n \geq N \Rightarrow |x_n - a| < \delta$$

$$\Rightarrow |f(x_n) - f(a)| < \in \qquad \text{by (1)}$$

$\therefore \lim_{n\to\infty} f\left(x_n\right) = f(a)$.

Conversely, let $\lim_{n\to\infty} f\left(x_n\right) = f(a)$ for every sequence $\left\{x_n\right\}$ in S converging to $a \in S$. Then we claim that f is continuous at a. If not, for some $\epsilon > 0$, for any $\delta > 0$, there exists $x \in S$ with

$$|x - a| < \delta, |f(x) - f(a)| \geq \epsilon \qquad \ldots (2)$$

Taking $\delta = \frac{1}{n}$ $(n \in N)$, let the point x given by (2) be denoted by x_n. Then $\left\{x_n\right\}$ is a sequence converging to a and hence $\lim_{n\to\infty} f\left(x_n\right) = f(a)$. But this contradicts (2).

$\therefore f$ is continuous at $a \in S$.

Theorem. 4 :

Let f be a continuous function on a bounded closed interval $[a, b]$. Then f is bounded.

Proof : If f is not bounded above, given $n \in N$, $\exists x_n \in [a, b]$ such that $f\left(x_n\right) > n$. Then $\left\{x_n\right\}$ is a sequence in $[a, b]$ and by Bolzano Weierstrass theorem $\left\{x_n / n \in N\right\}$ has a limit point c in $[a, b]$. Then $\lim_{n\to\infty} x_{r_n} = c$ for a subsequence $\left\{x_{r_n}\right\}$ of $\left\{x_n\right\}$. Since f is continuous on $[a, b]$, given $\epsilon = 1$, there exists $\delta > 0$ such that

$$x \in [a, b], |x - c| < \delta \Rightarrow |f(x) - f(c)| < 1 \qquad \ldots (1)$$

Since $\lim_{n\to\infty} x_{r_n} = c$, given $\delta > 0$, $\exists N_1 \in N$

such that $n \geq N_1 \Rightarrow \left|x_{r_n} - c\right| < \delta$

$\Rightarrow \left|f\left(x_{r_n}\right) - f(c)\right| < 1$ by (1).

$\Rightarrow \left|f\left(x_{r_n}\right)\right| < 1 + |f(c)|$

Now $n \leq r_n < \left|f\left(x_{r_n}\right)\right| < 1 + |f(c)|$

i.e., $n < 1 + |f(c)|$

This is a contradiction for sufficiently large n.

$\therefore f$ is bounded above.

In a similar way, we can prove that f is bounded below.

Theorem. 5 :

A continuous function f on a closed bounded interval $[a, b]$ attains its bounds.

Proof : By Theorem 4, f is bounded, by say M and m where

$$M = lub\{f(x) / x \in [a, b]\} = sup f([a, b])$$

$$m = glb\{f(x) / x \in [a, b]\} = inf f([a, b])$$

Then we show that there exists $c, d \in [a, b]$ such that

$$f(c) = M, \text{ and } f(d) = m.$$

If possible let $f(x) < M \; \forall \; x \in [a, b]$. Since a constant function is continuous, $M - f \neq 0$, on $[a, b]$ and is continuous (theorem. 1). Hence $\frac{1}{M - f}$ is continuous on $[a, b]$ and hence bounded (theorem 4). Let $k > 0$ be such that

$$\frac{1}{M - f(x)} \leq k \; \forall \; x \in [a, b].$$

Then $M - f(x) \geq \frac{1}{k} > 0$.

$$\therefore f(x) \leq M - \frac{1}{k}.$$

This contradicts the fact that M is the *lub* of f on $[a, b]$.

$\exists\, c \in [a, b] \ni f(c) = M$.

Similarly, we can prove that

$\therefore \exists\, d \in [a, b] \ni f(d) = m$.

Theorem. 6 :

> Let f be a continuous function on a closed interval $[a, b]$. Let $\alpha = f(a)$ and $\beta = f(b)$. Let $\alpha < \beta$ and γ be a real number such that $\alpha < \gamma < \beta$. Then there exists a number c $(a < c < b)$ such that $f(c) = \gamma$.

Proof : Let $S = \{x \in [a, b] \mid f(x) \leq \gamma\}$.

Then $a \in S$ and S is bounded above by b. Let $c = lub\ S$.

Since f is continuous at 'a', given $\gamma - \alpha > 0$, there exists $\delta > 0$ such that $a + \delta < b$ and

$$x \in (a, a + \delta) \Rightarrow |f(x) - f(a)| < \gamma - \alpha$$

$$\Rightarrow f(x) < f(a) + \gamma - \alpha = \gamma.$$

$$\therefore x \in (a, a + \delta) \Rightarrow x \in S$$

$$\Rightarrow a + \frac{\delta}{2} \leq lub\ S = c.$$

$$\Rightarrow a < c.$$

Since c is a limit point of $S \subset [a, b]$, we have $c \in [a, b] = [a, b]$.

We shall prove that

$c \in (a, b)$ and $f(c) = \gamma$.

For any $\delta > 0$, $c - \delta < c = \sup S \Rightarrow \exists\, x \in S : c - \delta < x \leq c$.

$$x \in S \Rightarrow f(x) \leq \gamma$$

and $\lim_{x \to c} f(x) \leq \gamma \Rightarrow f(c) \leq \gamma < f(b)$

Hence $c \in S$ and $c < b$.

If $x \in [a, b]$, $x > c$, then we claim that $f(x) > \gamma$. For if $f(x) \leq \gamma$, then $x \in S$ and hence $x \leq c$, a contradiction to $x > c$.

Now, let $T = \{x \in [a, b] \mid x > c\} = (c, b]$

Then T is non-empty ($\because b \in T$). Also c is a limit point of T.

$$\therefore f(c) = \lim_{x \to c} f(x) \geq \gamma.$$

$$\therefore f(c) = \gamma.$$

Note : If $\alpha > \beta$ and if γ is a number such that

$\alpha > \gamma > \beta$, let $F = -f$.

Then $F(a) = -f(a) = -\alpha$, $F(b) = -\beta$.

and $-\alpha < -\gamma < -\beta$.

Applying the theorem 6 to F, we find that there exists c in $a < c < b$ such that

$$F(c) = -\gamma. \text{ i.e., } -f(c) = -\gamma, \text{ or } f(c) = \gamma.$$

Remark. 3 : If a function f is continuous on a closed interval $[a, b]$ and $f(a), f(b)$ are of opposite signs, then there exists a point $c \in (a, b)$ such that $f(c) = 0$.

Theorem. 7 :

If f is continuous on a closed interval $[a, b]$, then the image of f namely $f([a, b])$ is a closed interval.

Proof : Since f is continuous on $[a, b]$, f attains its bounds. There exist $c, d \in [a, b]$ such that

$$f(c) = M = lub\ \{f(x) \mid x \in [a, b]\}$$

$$f(d) = m = glb\ \{f(x) \mid x \in [a, b]\}.$$

Then by the theorem 6, f assumes every value between m and M. Hence $f([a, b]) = [m, M]$.

Note : The image of f is not necessarily the interval lying between $f(a)$ and $f(b)$.

Theorem. 8 :

If a function f is continuous at an interior point c of $[a, b]$ and $f(c) \neq 0$, then $\exists\ \delta > 0$ such that $f(x)$ has the same sign as $f(c)$ in $(c - \delta, c + \delta)$.

Proof : Since the function f is continuous at an interior point c of $[a, b]$, for any $\in > 0$, $\exists\ \delta > 0$ such that

$$|f(x) - f(c)| < \in \forall\ x \in (c - \delta, c + \delta).$$

When $f(c) > 0$, taking $\in < f(c)$, there exists a number δ such that

$$f(x) > 0\ \forall\ x \in (c - \delta, c + \delta).$$

When $f(x) < 0$, taking $\in < -f(c)$, there exists a number δ such that

$$f(x) < 0\ \forall\ x \in (c - \delta, c + \delta).$$

Remark. 4 : If f is continuous at the end point b of $[a, b]$ and $f(b) \neq 0$, then there exists an interval $(b - \delta, b)$ such that $f(x)$ has the same sign as $f(b)$ for all x in $(b - \delta, b)$.

S A Q 2 If f is continuous at 'a', then $|f|$ is also continuous at a.

18.5 WORKEDOUT EXERCISES

Exercise. 1 : Show that every polynomial of odd degree has atleast one real root.

Ans : Let $f(x) = a_{2n+1}x^{2n+1} + a_{2n}x^{2n} + \ldots + a_0$, $a_{2n+1} \neq 0$ be a polynomial of degree $(2n + 1)$. Write

$$f(x) = x^{2n+1}\left[a_{2n+1} + \frac{a_{2n}}{x} + \ldots + \frac{a_0}{x^{2n+1}}\right].$$

If $a_{2n+1} > 0$ then $f(x) \to +\infty$ as $x \to +\infty$ and $f(x) \to -\infty$ as $x \to -\infty$. Thus there exist a and b such that $f(a) < 0 < f(b)$.

But f is a continuous function and hence by Remark 3 of this unit there exist $a < c < b$ such that $f(c) = 0$. A similar argument holds for $a_{2n+1} < 0$.

Exercise. 2 : Show that the product of continuous functions is again continuous.

Ans : Let f and g be continuous functions at $x = a$. Let $\in > 0$ be given. Without loss of generality assume $\in < 1$ and let $\in' = \frac{\in}{k}$ where k is a constant and $k \geq 1$.

Since f and g are continuous at $x = 0$, there exist $\delta_1 > 0$ and $\delta_2 > 0$ such that

$$|x - a| < \delta_1 \Rightarrow |f(x) - f(a)| < \in'$$

$$|x - a| < \delta_2 \Rightarrow |g(x) - g(a)| < \in'.$$

Now $|x - a| < \delta_2 \Rightarrow |g(x)| \leq |g(x) - g(a)| + |g(a)| < \in' + |g(a)|$

Let $\delta = \min\{\delta_1, \delta_2\}$. Thus if $|x - a| < \delta$,

$$\begin{aligned} |f(x)\,g(x) - f(a)\,g(a)| &= |f(x)\,g(x) - f(a)\,g(x) + f(a)\,g(x) - f(a)\,g(a)| \\ &\leq |f(x) - f(a)|\,|g(x)| + |f(a)|\,|g(x) - g(a)| \\ &\leq \in' |g(x)| + \in' |f(a)| \\ &\leq \in' (\in' + |g(a)|) + \in' |f(a)|. \\ &\leq \in' (1 + |g(a)| + |f(a)|) \end{aligned}$$

Choose $k = 1 + |g(a)| + |f(a)|$ so that

$|x - a| < \delta \Rightarrow |f(x)\,g(x) - f(a)\,g(a)| < \in$.

Thus fg is continuous at $x = a$.

SAQ 3 Define $f(0)$ so that $f(x) = \dfrac{\sin 2x}{x}$, $x \neq 0$ becomes continuous at $x = 0$.

18.6 SUMMARY

Intuitively speaking, a continuous function maps neighbourhood points onto neighbourhood points. That is as $x \to a$, $f(x) \to f(a)$. For a function to be continuous at a point, the function must be defined at that point, the limit must exist at that point and these two must be equal. A continuous function defined on a closed interval has many nice properties. It is bounded and attains its bounds. It assume every value on the interval. As a special case if a continuous function defined on an interval changes its sign then there must be atleast one point where the function is zero.

18.7 MODEL EXAMINATION QUESTIONS

Section A (Long Answer)

i) Define the continuity of a function at a point and on an interval. Show that a continuous function defined on a closed interval is bounded and attains its bounds.

ii) Define the continuity of a function at a point and show that a function f is continuous if and only if $f(x_n) \to f(a)$ for every sequence $\langle x_n \rangle$ converging to a.

iii) Define a continuous function and give an example. Show that a continuous function defined on a closed interval $[a, b]$ assumes every value between $f(a)$ and $f(b)$. Hence show that a polynomial of odd degree has at least one real root.

Section B (Short Answer)

i) If f is a continuous function on $[a, b]$, show that $f([a, b])$ is a closed interval.

ii) If f is continuous at a point c of $[a, b]$ and $f(c) \neq 0$, show that there exists $\delta > 0$ such that $f(x)$ has the same sign as $f(c)$ in $(c - \delta, c + \delta)$.

iii) Show that the composition of two continuous functions is a continuous function.

18.8 ANSWERS TO SAQ'S

SAQ 1 $\lim_{x \to 0} \frac{\sin x}{x} = 1 = f(0)$. Thus f is continuous at $x = 0$.

SAQ 2 Let $\epsilon > 0$ be given. Then f is continuous at 'a' implies that there is $\delta > 0$ such that $|x - a| < \delta \Rightarrow |f(x) - f(a)| < \epsilon$.

But $||f(x)| - |f(a)|| \leq |f(x) - f(a)|$. Thus given $\epsilon > 0$, there is $\delta > 0$ such that

$|x - a| < \delta \Rightarrow ||f(x)| - |f(a)|| < \epsilon$. Thus $|f|$ is continuous at $x = a$.

SAQ 3 $\lim_{x \to 0} \frac{\sin 2x}{x} = \left(\lim_{2x \to 0} \frac{\sin 2x}{2x} \right) \times 2 = 2$. Thus if we define $f(0) = 2$, then $\lim_{x \to 0} f(x) = f(0)$ and the function becomes continuous at $x = 2$.

UNIT–19: UNIFORM CONTINUITY

Contents

19.1 Aims and Objectives

19.2 Introduction

19.3 Definitions and examples

19.4 Properties of uniformly continuous functions

19.5 Workedout exercises

19.6 Summary

19.7 Model Examination Questions

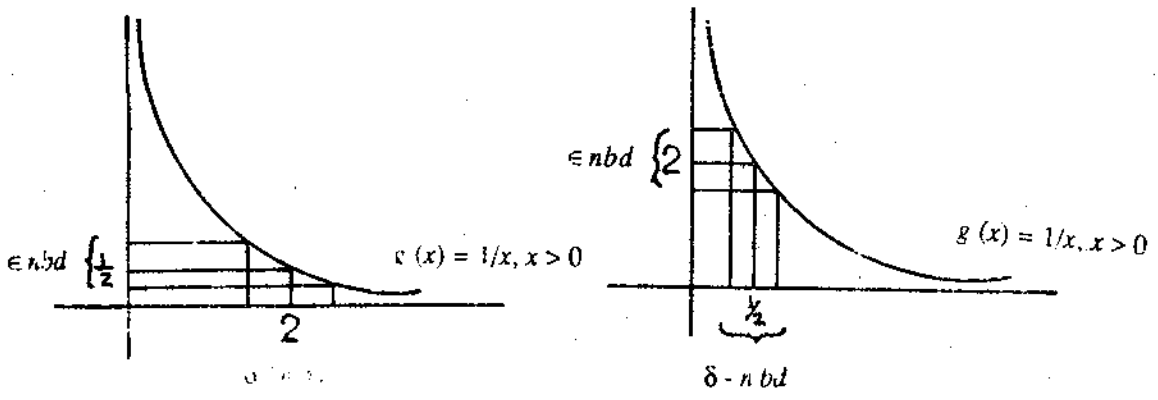
19.8 Answers to Self Assessment Questions

19.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to (i) Define uniform continuity of a function and distinguish the concept from that of continuity (ii) Give examples of functions which are continuous but not uniformly continuious (iii) Prove that every uniformly continuous function is continuous but not conversely (iv) A continuous function on a closed interval is uniformly continuous.

19.2 INTRODUCTION

Recall that a function f defined on an interval I is said to be continuous at a point $a \in I$ if for any $\epsilon > 0$, there exists $\delta > 0$ such that $|x - a| < \delta \Rightarrow |f(x) - f(a)| < \epsilon$. If b is any other point of I, then for the same $\epsilon > 0$, there would exist $\delta_1 > 0$, (not necessarily the same δ), such that $|x - b| < \delta_1 \Rightarrow |f(x) - f(a)| < \epsilon$. Thus in the definition of the continuity the choice of δ depends on ϵ and on the point c. The fact that δ depends on 'a' reflects the fact that f may change its values rapidly near certain points and slowly near other points. But there do exist functions where δ could be chosen independent of the point and depend only on ϵ. Such functions need special consideration. For example consider the function $f: \mathbf{R} \to \mathbf{R}$ where $f(x) = 2x$. Then for any point 'a', $|f(x) - f(a)| = 2|x - a|$ so that for any given $\epsilon > 0$ we can choose $\delta = \frac{\epsilon}{2}$ and this δ is independent of the point. On the other hand for the function $g: \mathbf{R}^+ \to \mathbf{R}^+$ given by $g(x) = \frac{1}{x}$ we see that the choice of δ depend not only on given ϵ but also on the point. As the point 'a' approaches '0', the permissable values of δ approach 0.



To see this consider $|g(x) - g(a)| = \left|\frac{a-x}{ax}\right|$. Let $\epsilon > 0$ be given. If $0 < \delta < a$ and $|x - a| \leq \delta$, then $|g(x) - g(a)| \leq \frac{\delta}{a(a-\delta)}$ and equality sign holds for $x = a - \delta$. Thus to make $|g(x) - g(a)| \leq \epsilon$, the largest δ we can select is $\delta = \frac{\epsilon a^2}{1 + \epsilon a}$. Thus the choice of δ depends on both ϵ and a. There is no 'δ' which will work for all points 'a' and for a given ϵ. This property that a single δ will suffice for all points in an interval is called the uniform continuity of a function. Since the property of continuity is restricted to a point in the interval, it is referred to as a local property and the property of uniform continuity is referred to as a global property.

19.3 DEFINITIONS AND EXAMPLES

Definition 1 :

Let $A \subseteq \mathbb{R}$ and $f : A \to \mathbb{R}$. The function f is said to be uniformly continuous on A, if for any given $\epsilon > 0$, there is a $\delta > 0$, (depending on ϵ alone) such that if $x \in A$, $a \in A$ and $|x - a| < \delta$, then $|f(x) - f(a)| < \epsilon$.

Equivalently, f is said to be uniformly continuous on A if for a given $\epsilon > 0$ there exists $\delta > 0$ such that $x, y \in S$, $|x - y| < \delta \Rightarrow |f(x) - f(y)| < \epsilon$.

Example 1 : Let $A = \{x \mid 0 < x \leq 1\}$ be an aggregate and let $f : A \to \mathbb{R}$ be defined by $f(x) = \frac{1}{x}$. Then f is clearly continuous on A (note that $x \neq 0$). But f is not uniformly continuous on A. To see this let $\epsilon > 0$ be given. If f were to be uniformly continuous then there must a 'δ' independent of x and a in A such that $\left|\frac{1}{x} - \frac{1}{a}\right| < \epsilon$ when $|x - a| < \delta$ (say) $\left|\frac{a-x}{ax}\right| < \epsilon$, when $a - \delta < x < a + \delta$.

In particular when $a = \delta$, then $(a - \delta, a + \delta) = (0, 2\delta)$. Then $\frac{\delta - x}{\delta x} \to \infty$ as $x \to 0$ so that $\left|\frac{a-x}{ax}\right|$ can not be made less than ϵ when $a = \delta$. Thus f is not uniformly continuous on A, though it is continuous on A.

SAQ 1 A constant function $f : \mathbf{R} \to \mathbf{R}$ is uniformly continuous on $\mathbf{R}$.

Example 2 : $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = x^2$ is a continuous function on $\mathbf{R}$ but not uniformly continuous.

Given $\epsilon > 0$, there is no single δ that serves for all $x \in \mathbb{R}$ in the condition of continuity. To see this, let us assume that there exists such a numbers $\delta > 0$. Then for x and

$$y = x + \frac{\delta}{2}, \quad |x - y| = \frac{\delta}{2} < \delta.$$

$$\therefore |f(x) - f(y)| = \left|x^2 - y^2\right| = |x - y|\,|x + y|$$

$$= \frac{\delta}{2}\left|2x + \frac{\delta}{2}\right|$$

$$= x\delta + \frac{\delta^2}{4} < \epsilon \text{ if } x > 0.$$

Since $\frac{\delta^2}{4} > 0$, we have $x\delta < \epsilon \ \forall\, x \in \mathbb{R}, x > 0$.

This is impossible. Therefore δ depends on ϵ and x. The given function is not uniformly continuous on $\mathbb{R}$, though it is a continuous function on $\mathbb{R}$.

Example 3 : If $1 < b \in \mathbf{R}$, the function $f : [1, b] \to \mathbf{R}$ given by $f(x) = x^2$ is uniformly continuous on $[1, b]$. Given $\epsilon > 0$, let $\delta = -|b| + \sqrt{b^2 + \epsilon}$. Then as in example 4, we can show that

$$x, y, \in [1, b], |x - y| < \delta \Rightarrow |f(x) - f(y)| < \epsilon .$$

Example 4 : $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = 2x$ is uniformly continuous on $\mathbf{R}$. Given $\epsilon > 0$, choose $\delta = \epsilon/2$. Then for all

$$x, y, \in \mathbf{R}, |x - y| < \epsilon/2 \Rightarrow |f(x) - f(y)| = 2|x - y| < \epsilon .$$

Example 5 : $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = |x - a|$, $(a \in \mathbf{R})$ is uniformly continuous on $\mathbf{R}$.

Given $\epsilon > 0$, choose $\delta = \epsilon$. Then

$$|x - y| < \delta \Rightarrow |f(x) - f(y)| = ||x - a| - |y - a|| \leq |x - y| < \epsilon$$

19.4 PROPERTIES OF CONTINUOUS FUNCTIONS

Theorem 1 :

> A function which is uniformly continuous on an interval is continuous on that interval but not conversely.

Proof : Let a function f be continuous on an interval I. Then for any given $\epsilon > 0$, there exists $\delta > 0$, (depending on ϵ alone) such that

$|f(x) - f(y)| < \epsilon$, for any $x, y \in$ I such that $|x - y| < \delta$. In particular let $a \in$ I and $y = a$ (say). Then for any $\epsilon > 0$, there is $\delta > 0$ such that

$|f(x) - f(y)| < \epsilon$ when $|x - a| < \delta$.

This means that f is continuous at 'a'. Since a is an arbitrary point of I, f is continuous on I.

The converse is not necessarily true. There do exist functions which are continuous on an interval but are not uniformly continuous. For example the function $f(x) = x^2$ is continuous but is not uniformly continuous (example 2).

Theorem 2 :

> A function which is continuous on a closed interval is uniformly continuous on that interval.

Proof : Let f be a function which is continuous on a closed interval I. If possible let f be not uniformly continuous on I. Then there exists an $\epsilon > 0$ such that for $\delta > 0$, we can find $x, y \in$ I for which

$|f(x) - f(y)| \not< \epsilon$ when $|x - y| < \delta$.

In particular for each positive integer n, we can find real numbers x_n, y_n in I such that

$$\left|f(x_n) - f(y_n)\right| \not< \epsilon \text{ when } |x_n - y_n| < \frac{1}{n}.$$

But $\langle x_n \rangle$ and $\langle y_n \rangle$ are sequences in the closed interval I. Hence they are bounded and have atleast one limit point each. Let l and m be the limit points of $\langle x_n \rangle$ and $\langle y_n \rangle$ respectively. Futher $l \in$ I and $m \in$ I. Since l and m are limit points of $\langle x_n \rangle$ and $\langle y_n \rangle$, there exist convergent subsequences $\langle x_{n_k} \rangle$ and $\langle y_{n_k} \rangle$ respectively such that $x_{n_k} \to l$ and $y_{n_k} \to m$. Thus we have

$$\left|f\left(x_{n_k}\right) - f\left(y_{n_k}\right)\right| \not< \in \text{ when } \left|x_{n_k} - y_{n_k}\right| < \frac{1}{n_k}.$$

Thus we have a situation where $\lim_{n\to\infty} x_{n_k} = \lim_{n\to\infty} y_{n_k}$ where as $f\left(x_{n_k}\right)$ and $f\left(y_{n_k}\right)$ converge to different limits. This contradicts the fact that f is continuous. Thus the assumption that f is not uniformly continuous is wrong.

Definition 2 :

Let $A \subseteq R$ and $f : A \to R$. Then f is said to be Lipschitz function (or satisfy Lipschitz condition) if there exists a constant $k > 0$ such that

$$|f(x) - f(a)| \le k\,|x - a|, \text{ for all } x, a \in A.$$

(Rudolph Lipschitz (1832 - 1903).

Theorem 3 :

If $f : A \to R$ is Lipschitz function then f is uniformly continuous on A.

Proof : The function f satisfies Lipschitz condition implies that there exists a constant $k > 0$ such that $|f(x) - f(a)| \le k\,|x - a|$ for all $x, a \in A$. Let $\in > 0$ be given. Choose $\delta = \frac{\in}{k}$. Then δ depends on $\in$ alone and not on a. Now

$$|x - a| < \delta \Rightarrow |f(x) - f(a)| < k.\left(\frac{\in}{k}\right) = \in.$$

Thus f is uniformly continuous on A.

Remark 1 : Every uniformly continuous function is a Lipschitz function. Consider for example $f(x) = \sqrt{x}$ defined on $[0, 1]$. Since f is continuous on a closed interval I, f is uniformly continuous on I. But there does not exist a number $k > 0$ such that $|f(x)| < k\,|x|$ for all $x \in I$.

Difinition 2 :

Let $A \subseteq R$. A function $f : A \to R$ is said to be increasing on A if $x_1, x_2 \in A$ and $x_1 \le x_2 \Rightarrow f\left(x_1\right) \le f\left(x_2\right)$. The function said to be strictly incresing if $x_1, x_2 \in A$ and $x_1 < x_2 \Rightarrow f\left(x_1\right) < f\left(x_2\right)$. Similarly $g : A \to R$ is said to be decreasing if $x_1, x_2 \in A$ and $x_1 \le x_2 \Rightarrow g\left(x_1\right) \ge g\left(x_2\right)$. The function is said to be strictly decreasing if $x_1, x_2 \in A$, $x_1 < x_2 \Rightarrow g\left(x_1\right) > g\left(x_2\right)$. A function which is either increasing or decreasing on A is called a monotone function on A. If a function is strictly increasing or strictly decreasing, it is called strictly monotone.

SAQ 2 Are monotonic functions always continuous ?

19.5 WORKEDOUT EXERCISES

Exercise 1 : Show that the function $f(x) = x^2$ is uniformly continuous on $[-1, 1]$.

Ans : Let x and y be any two points of $[-1, 1]$, then $|f(x) - f(y)| = \left|x^2 - y^2\right| = |x - y|\cdot|x + y| < \in$ when $|x - y| < \frac{\in}{2} = \delta$. Here the choice of δ depends on $\in$ alone and not on the choice of x and y.

Thus for any $\epsilon > 0$, there exists $\delta > 0$ and $\delta = \frac{\epsilon}{2}$ such that for any $x, y \in [-1, +1]$, $|f(x) - f(y)| < \epsilon$ when $|x - y| < \frac{\epsilon}{2} = \delta$. Thus f is uniformly continuous on $[-1, 1]$.

19.6 SUMMARY

In the definition of continuity of a function 'f' at a point 'a' we have stated that for any given $\epsilon > 0$ we should be able to find $\delta > 0$ such that $|f(x) - f(a)| < \epsilon$ when $|x - a| < \delta$. Here the choice of δ depends not only on the given ϵ but on the point 'a' also. For a given ϵ, we may have to choose different δ s depending on the point 'a' under consideration. If one single δ could be choosen to 'work' for all the points then the choice of δ depends on ϵ alone. Thus δ is independent of the point at which we are considering continuity. This notion of continuity is called uniform continuity. Every uniformly continuous function is continuous. But every continuous function need not be uniformly continuous. The notion of continuity is local in nature but the notion of uniform continuity is global in nature. A continuous function defined on a closed and bounded interval is uniformly continuous.

19.7 MODEL EXAMINATION QUESTIONS

SECTION - A (Long Answers)

(i) Show that a uniformly continuous function is continuous. Show further a continuous function on a closed and bounded interval is uniformly continuous.

SECTION - B (Short Answers)

(i) Define the uniform continuity of a function. Show that a uniformly continuous function is continuous. Give an example to show that the converse is not true.

(ii) Discuss the continuity and uniform continuity of $f(x) = x^2$ on $(-1, 1)$ and $[-1, 1]$.

19.8 ANSWERS TO SELF ASSESSMENT QUESTIONS

SAQ 1 Let $\epsilon > 0$ be given then $|f(x) - f(a)| < \epsilon$ for any $|x - a| < \delta$. Since δ is independent of the choice of 'a', f is uniformly continuous.

SAQ 2 No. Define $f(x) = \begin{cases} 0 \text{ if } 0 \le x \le 1 \\ 1, \text{ if } 1 < x \le 2 \end{cases}$

Then f is increasing on $[0, 2]$, but is not continuous at $x = 1$.

BLOCK–6 : DIFFERENTIABILITY AND INTEGRABILITY

Unit–20 : Differentiability of functions

Unit–21 : Mean Value theorems

Unit–22 : Taylor's Theorem and Applications

Unit–23 : Rieman Integrability

The notions of computing the rate of change of a variable or the area of a geometrical figure can be traced to the beginning of the revolutionary thinking in mathematics. The difficulty about answering questions about differentiability of a function at a point arises because it involves the approach of a function to the point by different paths. Differentiability is more a stringent constraint on a function than continuity. Integration could be viewed as an inverse process of differentiation. But Integrability of a function could be studied independently of differentiability of a function.

UNIT–20 : DIFFERENTIABILITY OF A FUNCTION

Contents

20.1 Aims and Objectives

20.2 Introduction

20.3 Definition and examples

20.4 Algebra of derivatives

20.5 Applications of differentiability

20.6 Workedout exercises

20.7 Summary

20.8 Model Examination Questions

20.9 Answers to Self Assessment Questions

20.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to (i) define differentiability of a function at a point and in an interval (ii) Show that every differentiable function is continuous but not conversely (iii) Test the differentiability of a function at a point (iv) discuss applications of differentiabiliy.

20.2 INTRODUCTION

Seventeenth century was a turning point in the development of mathematical ideas. Rene descartes (1596 - 1650) and Perire de Fermat (1601 - 1655) have discovered analytic geomentry which used the language of algebra to solve intricate and laborious geometric problems. In the same century Isaac Newton(1642 - 1727) and Gottfried Leibnitz (1646 - 1716) discovered calculus independently. Newton was faced with the problems of (i) drawing a tangent to a given curve at a given point and (ii) determining the maximum and minimum values of a function. Leibnitz had been working on determining the area of a given geomertic figure and the inverse problem leading to a problem of differentiation. The notation and terminology of Newton was based on theory of fluxions which was difficult to comprehend where as the ideas of Leibritz were relatively simple. But due to patriotic reasons, the followers of Newton in Britian and the followers of Leibnitz in the continent faught academic battles for over a century with each group caliming that one had plagarised the ideas of the other. Mathematical Historians give the controversy as a reason for the poor contribution of mathematicians from England in the eighteenth century.

20.3 DEFINITIONS AND EXAMPLES

Defintion 1 :

Let $f : [a, b] \to R$ be a function. Let $c \in (a, b)$. Then f is said to be derivable (differentiable) at $x = c$ if

$$\lim_{x \to c} \frac{f(x) - f(c)}{x - c}, (x \neq c)$$

exists finitely. This limit if it exists is called the derivative of f at $x = c$. The derivative of f at $x = c$ is denoted by $f'(c)$. It can be seen that

$$\lim_{x \to c} \frac{f(x) - f(c)}{x - c} = \lim_{h \to 0} \frac{f(c + h) - f(c)}{h}$$

Defintion 2 :

Let $f : [a, b] \to R$ be a function. Let $c \in (a, b)$. If $\lim_{x \to c+0} \frac{f(x) - f(c)}{x - c}, (x \neq c)$ exists finitely, then f is said to be derivable from the right at $x = c$. This limit is called the right hand derivative of f at $x = c$ and is denoted $f'(c + 0)$.

Defintion 3 :

Let $f : [a, b] \to R$ be a function. Let $c \in (a, b)$. If $\lim_{x \to c-0} \frac{f(x) - f(c)}{x - c}, (x \neq c)$, exists finitely, then f is said to be derivable from the left at $x = c$. Thus limit is called the left hand derivative of f at $x = c$ and is denoted by $f'(c - 0)$.

Remark 1 : It is evident that a function f is derivable at $x = c$ iff $f'(c + 0) = f'(c - 0)$. Further observe that

$$f'(c + 0) = \lim_{h \to 0} \frac{f(c + h) - f(c)}{h}, h > 0 \text{ and}$$

$$f'(c - 0) = \lim_{h \to 0} \frac{f(c - h) - f(0)}{h}, h > 0.$$

Definition 4 :

If a function f is defined on $[a, b]$, then f is said to be derivable on $[a, b]$ if (i) f is derivable at every point of (a, b) and (ii) f is derivable from the right at 'a' and from the left at 'b'.

SAQ 1 If $f(x) = x^2$ for $x \in \mathbf{R}$, find $f'(a)$ where $a \in \mathbf{R}$

Theorem 1 :

If f is derivable at a point then it is continuous at that point.

Proof : Let $f : [a, b] \to R$ be derivable at an interior point c of $[a, b]$

Then $\lim_{x \to c} \frac{f(x) - f(c)}{x - c}$ $(x \neq c)$ exists finitely. Let this limit be denoted by $f'(c)$.

$$\text{Now } \lim_{x\to c}[f(x)-f(c)] = \lim_{x\to c}\left\{\frac{f(x)-f(c)}{x-c}\right\}(x-c)$$

$$= \lim_{x\to c}\frac{f(x)-f(c)}{x-c}\cdot\lim_{x\to c}(x-c)$$

$$= f'(c)\cdot 0$$

$$= 0$$

$$\therefore \lim_{x\to c} f(x) = f(c)$$

$\therefore f$ is continuous at $x = c$.

Remark 2 : If f is derivable at a point from the left or from the right, accordingly f is continuous from the left or from the right at that point.

Remark 3 : The converse of the above theorem is not ture. That is if a function is continuous at a point, it need not be derivable at that point.

For example, consider the function f defined by

$$f(x) = |x| \;\forall\; x \in \mathbb{R}$$

$$\lim_{x\to 0+0} f(x) = \lim_{h\to 0} f(0+h)$$

$$= \lim_{h\to 0} |0+h| \;(h>0)$$

$$= \lim_{h\to 0} h$$

$$= 0$$

$$\lim_{x\to 0-0} f(x) = \lim_{h\to 0} f(0-h) = \lim_{h\to 0} |0-h| \;(h>0)$$

$$= \lim_{h\to 0} h = 0$$

Also $f(0) = |0| = 0$

$$\therefore \lim_{x\to 0} f(x) = f(0)$$

Hence f is continuous at $x = 0$

$$\text{But } \lim_{x\to 0+0}\frac{f(x)-f(0)}{x-0} = \lim_{h\to 0}\frac{|0+h|-|0|}{0+h-0}\;(h>0)$$

$$= \lim_{h\to 0}\left(\frac{h}{h}\right) = 1$$

$$\therefore \lim_{x\to 0-0}\frac{f(x)-f(0)}{x-0} = \lim_{h\to 0}\frac{|0-h|-|0|}{0-h-0}\;(h>0)$$

$$= \lim_{h\to 0}\left(\frac{h}{-h}\right) = -1$$

$$\therefore f'(0+0) \neq f'(0-0)$$

$\therefore f$ is not derivable at $x = 0$.

Thus continuity of f at a point does not imply the derivability at that point.

(In 1872 Weierstrass Karl astounded the mathematical world by exhibiting a function which is continuous every where but differentiable nowhere. This function is f where

$$f(x) = \sum_{n=0}^{\infty} \frac{1}{2^n} \cos(3^n x)$$

Example 1 : Show that the function $f(x) = x^2 \sin \frac{1}{x}$ for $x \neq 0$ and $f(0) = 0$ has derivative at $x = 0$.

Solution : We have

$$\lim_{x \to 0} \frac{f(x) - f(0)}{x - 0} = \lim_{x \to 0} \left(\frac{x^2 \sin \frac{1}{x}}{x} \right)$$

$$= \lim_{x \to 0} (x) \cdot \lim_{x \to 0} \left(\sin \frac{1}{x} \right)$$

$$= 0. \text{ (a finite quantity lying between } -1 \text{ and } +1)$$

$$= 0.$$

$\therefore f'(x)$ exists and is finite at $x = 0$

Hence f has a derivative at $x = 0$

Example 2 : Find out right hand and left hand derivatives at the origin for the function.

$$f(x) = \begin{cases} x \tan^{-1} \frac{1}{x} & \text{for } x \neq 0 \\ 0 & x = 0 \end{cases}$$

Solution : $\lim_{h \to 0} \frac{f(0 + h) - f(0)}{h}$

$$= \lim_{h \to 0} \left[\frac{h \tan^{-1} \left(\frac{1}{h} \right)}{h} \right] (h > 0)$$

$$= \lim_{h \to 0} \tan^{-1} \left(\frac{1}{h} \right)$$

$$= \frac{\pi}{2}$$

$\therefore f'(0 + 0)$ exists and is equal to $\frac{\pi}{2}$

Again $\lim_{h \to 0} \frac{f(0 - h) - f(0)}{-h}$

$$= \lim_{h \to 0} \left(\frac{-h \tan^{-1} \left[\frac{1}{-h} \right]}{-h} \right) (h > 0)$$

$$= \lim_{h \to 0} \tan^{-1}\left[\frac{-1}{h}\right]$$

$$= \frac{-\pi}{2}$$

$\therefore f'(0-0)$ exists and is equal to $\frac{-\pi}{2}$.

Since $f'(0+0) \neq f'(0-0)$, the function f has no derivative at $x = 0$.

Example 3 : Show that the function

$$f(x) = x \sin \frac{1}{x}, x \neq 0$$

$$= 0 \text{ for } x = 0$$

is continuous but not derivable at $x = 0$.

Solution : $\lim_{x \to 0+0} f(x) = \lim_{h \to 0} f(0+h)$ $(h > 0)$

$$= \lim_{h \to 0} (0+h) \sin\left[\frac{1}{0+h}\right]$$

$$= \lim_{h \to 0} (h) \cdot \lim_{h \to 0} \left[\frac{1}{h}\right]$$

= 0 (a finite quantity which lies between -1 and $+1$)

$\therefore \lim_{x \to 0+0} f(x) = 0$

Again $\lim_{x \to 0-0} f(x) = \lim_{h \to 0} f(0-h)$ $(h > 0)$

$$= \lim_{h \to 0} (-h) \sin\left[\frac{1}{-h}\right]$$

$$= \lim_{h \to 0} (h) \cdot \lim_{h \to 0} \left[\sin \frac{1}{h}\right]$$

= 0 as before

$\therefore \lim_{x \to 0-0} f(x) = 0$

Hence $\lim_{x \to 0+0} f(x) = \lim_{x \to 0-0} f(x) = f(0)$ by data

$\therefore \lim_{x \to 0} f(x) = f(0)$

$\therefore f$ is continuous at $x = 0$.

Next we shall examine the derivability of $f(x)$ at $x = 0$

$$\lim_{x \to 0+0} \frac{f(x) - f(0)}{x - 0} = \lim_{h \to 0} \frac{f(0+h) - f(0)}{0 + h - 0} \quad (h > 0)$$

$$= \lim_{h \to 0} \frac{h \sin\left(\frac{1}{h}\right)}{h}$$

$$= \lim_{h \to 0} \left[\sin \frac{1}{h}\right]$$

Since $\sin\frac{1}{h}$ oscillates between -1 and $+1$, $\lim_{h\to 0} \sin\left(\frac{1}{h}\right)$ does not exist. Therefore $f'(0+0)$ does not exist. Hence $f'(0)$ does not exist.

SAQ 2 Examine the continuity and differentiability of f defined by

$$f(x) = \begin{cases} 1 + x \text{ if } x < 2 \\ 5 - x \text{ if } x \geq 2 \end{cases} \quad \text{at } x = 2.$$

20.4 ALGEBRA OF DERIVATIVES

In this section we state some theorems regarding the sum, difference, product and quotient of two derivable functions which follow, directly from the definition of the derivative of a function at any point and the theorems on limits of sum, difference, product and quotient of two functions.

Theorem 2 :

If f and g are two functions which are defined on $[a, b]$ and are derivable at any point $c \in [a, b]$ then

(i) their sum $f + g$ defined by $(f + g)(x) = f(x) + g(x)$ is also derivable at $x = c$ and

$$(f+g)'(c) = f'(c) + g'(c)$$

(ii) their differnce $f - g$ defined by

$$(f-g)(x) = f(x) - g(x)$$

is also derivable at $x = c$ and $(f-g)'(c) = f'(c) - g'(c)$.

(iii) their product $f g$ defined by

$$(fg)(x) = f(x)\, g(x)$$

is derivable at $x = c$ and $(fg)'(c) = g(c) f'(c) + f(c) g'(c)$.

(iv) $$\left[\frac{1}{f}\right](x) = \frac{1}{f(x)}$$

is derivable at $x = c$ if $f(x) \neq 0$ and

$$\left[\frac{1}{f}\right]'(c) = -\frac{f'(c)}{[f(c)]^2}$$

(v) the quotient $\left(\frac{f}{g}\right)$ defined by $\left(\frac{f}{g}\right)(x) = \frac{f(x)}{g(x)}$

$(g(x) \neq 0)$ is derivable at $x = c$ and

$$\left[\frac{f}{g}\right]'(c) = \frac{g(c) f'(c) - f(c) g'(c)}{[g(c)]^2}$$

Theorem 3 :

Let $X \subseteq R$, $Y \subseteq R$. The function $f : X \to Y$ is derivable at $a \in X \cap X'$; $f(a) \in Y'$ and the function $g : Y \to R$ is derivable at $f(a)$. Then $g \circ f : X \to R$ is derivalbe at 'a'.

Moreover $(g \circ f)'(a) = g'(f(a)) f'(a)$

Proof : Let $f(a) = b$. If we define a function $h : Y \to R$ by

$$h(y) = \begin{cases} \frac{g(y) - g(b)}{y - b} & \text{for } y \neq b \\ g'(b) & \text{for } y = b \end{cases}$$

then because g is derivable at b

$$\lim_{y \to b} h(y) = g'(b)$$

Further $g(y) - g(b) = (y - b)\, h(y)$

$\therefore$ for every x in the deleted neighbourhood of 'a' we have

$$\frac{(g \circ f)(x) - (g \circ f)(a)}{x - a} = \frac{g(f(x)) - g(b)}{x - a}$$

$$= \left(\frac{f(x) - b}{x - a}\right) h(f(x))$$

$$= \frac{f(x) - f(a)}{x - a} \cdot h(f(x))$$

But f is derivable at 'a'.

$\therefore f$ is continuous at 'a'.

Further h is continuous at $b = f(a)$

$\therefore h \circ f$ is continuous at 'a'

That is $\lim_{x \to a} h(f(x)) = h(f(a)) = h(b)$

$$= g'(f(a))$$

$$\therefore \lim_{x \to a} \frac{(g \circ f)(x) - (g \circ f)(a)}{x - a} = f'(a) \cdot g'(f(a))$$

That is $(g \circ f)'(a) = g'(f(a))\, f'(a)$.

Theorem 4 :

> Let X and Y be two aggregates of real numbers. If $f : X \to Y$ is a bijection, f is derivable at a, $f'(a) \neq 0$ and $f(a) \in Y'$, f^{-1} is continuous at $f(a)$ then f^{-1} is derivable at $f(a)$ and
>
> $$\left(f^{-1}\right)'(f(a)) = \frac{1}{f'(a)}$$

Proof : Let $g = f^{-1}$, then $g : Y \to X$ is a bijection. Let $f(x) = y$ and $f(a) = \alpha$, then $g(y) = x$ and $g(\alpha) = a$. Since g is continuous at $\alpha \in Y'$, $y \in Y$, $y \to \alpha \Rightarrow g(y) \to g(\alpha)$ i.e., $y \to \alpha \Rightarrow x \to a$ and $x \neq a$ if $y \neq \alpha$ (since g is a bijection)

Now $$\lim_{y \to \alpha} \frac{g(y) - g(\alpha)}{y - \alpha} = \lim_{x \to a} \frac{x - a}{f(x) - f(a)}$$

$$= \lim_{x \to a} \frac{1}{\frac{f(x) - f(a)}{x - a}} = \frac{1}{f'(a)}.$$

i.e., $$g'(x) = \frac{1}{f'(a)}$$

Remark : Let X be an interval of real numbers and f a strictly monotone and continuous function on X, then Y = Range f, is also an interval and f has a unique inverse function f^{-1} from Y onto X. Further f^{-1} is continuous on Y. If $a \in X$, then $f(a) \in Y$ which is an interval and therefore $f(a) \in Y'$. If now f is differentiable at $a \in X$ and $f'(a) \neq 0$, then f^{-1} is differentiable at $f(a)$ in Y and $(f^{-1})'(f(a)) = \frac{1}{f'(a)}$.

20.5 APPLICATIONS OF DIFFERENTIABILITY

Theorem 5 :

If $f : [a, b] \to R$ is differentiable at $c \in (a, b)$ and if $f'(c) < 0$ then there exists an interval $[c - h, c + h] \subset [a, b]$ such that $f(x) > f(c)$ for all x in $[c - h, c)$ and $f(x) < f(c)$ for all x in $(c, c + h]$

Proof : Since f is derivable at c, therefore for any $\epsilon > 0$, there exists $\delta > 0$ such that

$$\left|\frac{f(x) - f(c)}{x - c} - f'(c)\right| < \epsilon$$

for all $x \in [a, b]$ with the condition that

$$0 < |x - c| < \delta$$

$$\Rightarrow f'(c) - \epsilon < \frac{f(x) - f(c)}{x - c} < f'(c) + \epsilon$$

$\forall\, x \in [a, b]$ with the condition $0 < |x - c| < \delta$

If we choose $\epsilon < |f'(c)|$ then $f'(c) - \epsilon$, $f'(c)$, $f'(c) + \epsilon$ are negative.

Corresponding to this ϵ if we choose $\delta > 0$

then $\frac{f(x) - f(c)}{x - c} < 0 \;\forall\, x \in [a, b]$

with $0 < |x - a| < \delta$.

If $c - \frac{\delta}{2} \leq x < c, x \in [a, b]$ then $x - c < 0$

$$\therefore f(x) > f(c)$$

If $c < x \leq c + \frac{\delta}{2}, x \in [a, b]$ then $x - c > 0$

$$\therefore f(x) < f(c)$$

Let $h = \min\left\{\frac{\delta}{2}, c - a, b - c\right\}$

then $f(x) > f(c)$ for $x \in [c - h, c), x \in [a, b]$

and $f(x) < f(c)$ for $x \in (c, c + h], x \in [a, b]$

Thus if $f'(c) < 0$, there exists an interval

$[c - h, c + h] \subset [a, b]$ such that

$f(x) > f(c)$ for all $x \in [c - h, c)$

and $f(x) < f(c)$ for all $x \in (c, c + h]$

Note : (i) If $f : [a, b] \to R$ is differentiable at 'a' such that $f'(a) < 0$ then there exists $h > 0$ such that

$f(x) < f(a)$ for all $x \in (a, a + h] \subset [a, b]$

(ii) If $f : [a, b] \to R$ is differentiable at b such that $f'(b) < 0$ then there exists $h > 0$ such that

$f(x) > f(b)$ for all $x \in [b - h, b) \subset [a, b]$

Theorem 6 :

If $f : [a, b] \to R$ is differentiable at $c \in (a, b)$ and if $f'(c) > 0$ then there exists an interval $[c - h, c + h] \subset [a, b]$ such that

$f(x) < f(c)$ for all $x \in [c - h, c) \subset [a, b]$

and $f(x) > f(c)$ for all $x \in (c, c + h] \subset [a, b]$

Proof : Since f is differentiable at $c \in (a, b)$, therefore for any $\epsilon > 0$ there exists $\delta > 0$ such that

$$\left| \frac{f(x) - f(c)}{x - c} - f'(c) \right| < \epsilon$$

for all $x \in [a, b]$ with the condition $0 < |x - c| < \delta$

$$\Rightarrow f'(c) - \epsilon < \frac{f(x) - f(c)}{x - c} < f'(c) + \epsilon$$

for all $x \in [a, b]$ with the condition $0 < |x - c| < \delta$.

If we choose $\epsilon < f'(c)$

then $f'(c) - \epsilon, f'(c), f'(c) + \epsilon$ are positive

Corresponding to this ϵ, if we choose $\delta >$,

$$\frac{f(x) - f(c)}{x - c} > 0 \text{ for all } x \in [a, b]$$

with the condition $0 < |x - c| < \delta$

If $c - \frac{\delta}{2} \leq x < c, x \in [a, b]$ then $x - c < 0$

$$\therefore f(x) < f(c)$$

If $c < x \leq c + \frac{\delta}{2}, x \in [a, b]$ then $x - c > 0$

$$\therefore f(x) > f(c)$$

Let $h = \left\{ \frac{\delta}{2}, c - a, b - c \right\}$

Then $f(x) < f(c)$ for all $x \in [c - h, c) \subset [a, b]$

and $f(x) > f(c)$ for all $x \in (c, c + h] \subset [a, b]$.

Note : (i) if $f : [a, b] \to R$ is differentiable at 'a' and if $f'(a) > 0$

then $f(x) > f(a)$ for all $x \in (a, a + h] \subset [a, b]$

(ii) If $f : [a, b] \to R$ is differentiable at 'b' and if $f'(b) > 0$

then $f(x) < f(b)$ for all $x \in [b - h, b] \subset [a, b]$

Definition 5 :

Let $f : [a, b] \to R$ be a function. Let $c \in (a, b)$. The function f is said to be increasing at c if there exists an interval

$[c - h, c + h] \subset [a, b]$

such that

$f(x) < f(c) \forall x \in [c - h, c) \subset [a, b]$

and $f(x) > f(c) \forall x \in (c, c + h] \subset [a, b]$

Note : (i) The function $f : [a, b] \to R$ is said to be increasing at the end point 'a' if there exists an interval

$(a, a + h] \subset [a, b]$ such that

$f(x) > f(a) \forall x \in (a, a + h] \subset [a, b]$

(ii) The function $f : [a, b] \to R$ is said to be increasing at the end point 'b' if there exists an interval

$[b - h, b) \subset [a, b]$ such that

$f(x) < f(b) \forall x \in [b - h, b) \subset [a, b]$

Definition 6 :

Let $f : [a, b] \to R$ be a function and let $c \in (a, b)$. The function f is said to be decreasing at c if there exists an interval

$[c - h, c + h] \subset [a, b]$ such that

$f(x) > f(c) \quad \forall x \in [c - h, c) \subset [a, b]$

and $f(x) < f(c) \quad \forall x \in (c, c + h] \subset [a, b]$

Note : (i) The function $f : [a, b] \to R$ is said to be decreasing at the end point 'a' if there exists an interval

$(a, a + h] \subset [a, b]$ such that

$f(x) < f(a) \quad \forall x \in (a, a + h] \subset [a, b]$

(ii) The function $f : [a, b] \to R$ is said to be decreasing at the end point b if there exists an interval

$[b - h, b) \subset [a, b]$ such that

$f(x) > f(b) \quad \forall x \in [b - h, b) \subset [a, b]$

(iii) If $f'(c) > 0$ then f is increasing at c.

(iv) If $f'(c) < 0$ then f is decreasing at c.

The converses of (iii) and (iv) are not true. That is if f is increasing at c then $f'(c)$ need not be greater than zero. For example the function $f(x) = x^3$ is increasing at $x = 0$. But $f'(0) = 0$.

Similarly if f is decreasing at c, $f'(c)$ need not be less than zero. For example the function $f(x) = -x^3$ is decreasing at $x = 0$. But $f'(0) = 0$.

(v) A function f is said to be decreasing in $[a, b]$ if f is decreasing at every point in $[a, b]$.

(vi) A function f is said to be increasing in $[a, b]$ if f is increasing at every point in $[a, b]$.

(vii) A function f is said to have a stationary value at $x = a$ if $f'(a) = 0$.

Example 4 : Find the interval over which the function $f(x) = \sqrt{9 - x^2}$ is increasing or decreasing

Solution :

$$f(x) = \sqrt{9 - x^2}$$

$$\therefore f'(x) = \frac{-x}{\sqrt{9 - x^2}}$$

Now $f'(x) > 0 \; \forall \; x \in (-3, 0)$

$f'(x) < 0 \; \forall \; x \in (0, 3)$

Hence the function is increasing over $(-3, 0)$ and is decreasing over $(0, 3)$.

Example 5 : For what values of x the function $f(x) = ax^2 + bx + c \;\; (a \neq 0)$ has stationary values ?

Solution :

$$f(x) = ax^2 + bx + c \;\; \therefore f'(x) = 2ax + b$$

$$f'(x) = 0 \Rightarrow 2ax + b = 0$$

$$\Rightarrow x = \frac{-b}{2a}$$

$\therefore f$ has a stationary value at $x = \frac{-b}{2a}$ and the stationary value of f is

$$f\left(\frac{-b}{2a}\right) = \frac{4ac - b^2}{4a}$$

Example 6 : For what values of x the function $f(x) = \frac{\log x}{x}$ has stationary values ?

Solution :

Assume that $\frac{d}{dx}(\log x) = \frac{1}{x}$ for $x > 0$

$$f'(x) = \frac{1 - \log x}{x^2}$$

$$\therefore f'(x) = 0 \Rightarrow \log x = 1$$

$$\Rightarrow x = e$$

$\therefore f$ has a stionary value at $x = e$ and the stationary value of f is

$$\frac{\log e}{e} = \frac{1}{e}$$

Example 7 : Show that $\frac{x}{1 + x} < \log(1 + x) < x, x > 0$

Solution :

$$\text{Let } f(x) = \log(1 + x) - \frac{x}{1 + x}$$

$$= \log(1 + x) + \frac{1}{x + 1} - 1$$

$$\therefore f'(x) = \frac{1}{1 + x} - \frac{1}{(1 + x)^2} = \frac{x}{(1 + x)^2} > 0 \;\; (\because x > 0)$$

$\therefore f$ is an increasing function for all $x > 0$ ... (1)

$$\text{But } f(0) = 0 \qquad \ldots (2)$$

(1) and (2) $\Rightarrow f(x) > 0, x > 0$

$$\Rightarrow \log(1+x) - \frac{x}{1+x} > 0, x > 0$$

$$\Rightarrow \frac{x}{1+x} < \log(1+x) \qquad \ldots (3)$$

Let $\phi(x) = x - \log(1+x)$

$$\therefore \phi'(x) = 1 - \frac{1}{1+x} = \frac{x}{1+x} > 0 \quad (\because x > 0)$$

$\Rightarrow \phi(x)$ is an increasing function of x ... (4)

$$\text{Also } \phi(0) = 0 \qquad \ldots (5)$$

(4), (5) $\Rightarrow \phi(x) > 0$

$$\Rightarrow x - \log(1+x) > 0$$

$$\Rightarrow \log(1+x) < x \qquad \ldots (6)$$

(3) and (6) $\Rightarrow \frac{x}{1+x} < \log(1+x) < x \quad (x > 0)$

20.6 WORKEDOUT EXERCISES

Exercise (i) : What conditions are to be imposed on n if the function f defined by $f(x) = x^n \cos\left(\frac{1}{x}\right), x \neq 0$ and $f(0) = 0$ if f is to be continuous at $x = 0$ and differentiable at $x = 0$?

Ans : $f\left(0^+\right) = \lim_{h\to 0} h^n \cos\left(\frac{1}{h}\right)$ and $f\left(0^-\right) = \lim_{h\to 0} \left(-h^n\right) \cos\left(-\frac{1}{h}\right)$.

$$\text{But } \lim_{h\to 0} \left(-h^n\right) \cos\left(-\frac{1}{h}\right) = \lim_{h\to 0} \left(-h^n\right) \cos\left(\frac{1}{h}\right)$$

Thus if the function has to be continuous at $x = 0$

$$\lim_{h\to 0} h^n \cos\left(\frac{1}{h}\right) = \lim_{h\to 0} \left(-h^n\right) \cos\left(\frac{1}{h}\right) = 0.$$

This is possible only when n is positive. Thus f is continuous only if $n > 0$.

$$f'\left(0^+\right) = \lim_{h\to 0} \frac{h^n \cos\left(\frac{1}{h}\right)}{-h} = \lim_{h\to 0} h^{n-1} \cos\left(\frac{1}{h}\right)$$

$$f'\left(0^-\right) = \lim_{h\to 0} \frac{\left(-h^n\right) \cos\left(-\frac{1}{h}\right)}{-h} = \lim_{h\to 0} (-1)^n \cdot h^{n-1} \cos\left(\frac{1}{h}\right)$$

If $f'(0)$ has to exist, $f'\left(0^+\right)$ and $f'\left(0^-\right)$ must be equal, this is possible only when $(n-1)$ is positive or when $n > 1$.

20.7 SUMMARY

A function f is said to be derivable at a point if $\lim_{x \to a} \frac{f(x) - f(a)}{x - a}$ exists finitely.

Geometrically this means that a tangent can be drawn to the curve $y = f(x)$ at $x = a$. The slope of this tangent is $f'(a)$. When compared to continuity of a function, differentiability is a stronger constraint. Every differentiable function is continuous but not conversely. For example $f(x) = |x|$ is continuous at $x = 0$. A function f is increasing at $x = c$ if $f'(c) > 0$ and is decreasing at $x = c$ if $f'(c) < 0$.

20.8 MODEL EXAMINATION QUESTIONS

SECTION - A (Long Answers)

(i) Define the concepts of differentiability and continuity of a function. Show that a function which is differentiable at a point is continuous at that point. Give an example of a function which is continuous at a point but is not differentiable at that point.

(ii) If $f : [a, b] \to R$ is differentiable at $c \in (a, b)$ and if $f'(c) < 0$, show that there exists an interval $[c - h, c + h] \subset [a, b]$ such that $f(x) > f(c)$ for all x in $[c - h, c)$ and $f(x) < f(c)$ for all x in $(c, c + h]$. State the corresponding theorem if $f'(c) > 0$.

SECTION - B (Short Answers)

(i) Discuss the continuity and differentiability of $f(x) = x\left[1 + \frac{1}{3}\sin\left(\log x^2\right)\right]$, $x \neq 0$ and $f(0) = 0$ at $x = 0$.

(ii) Discuss the continuity and differentiability of $f(x) = x^2 \cos\frac{1}{x}$, $x \neq 0$ and $f(0) = 0$ at $x = 0$.

(iii) Show that $\frac{x}{1 + x} < \log(1 + x) < x$, for $x > 0$.

20.9 ANSWERS TO SAQ'S

SAQ 1 $f'(a) = \lim_{x \to 0} \frac{f(x) - f(a)}{x - a} = \lim_{x \to a} \frac{x^2 - a^2}{x - a} = \lim_{x \to a} (x + a) = 2a.$

SAQ 2 $f(2) = 3$; $f\left(2^-\right) = \lim_{h \to 0} (1 + 2 - h) = 3$ and $f\left(2^+\right) = \lim_{h \to 0} \left(5 - \overline{2 + h}\right) = 3$. Thus $f\left(2^-\right) = f\left(2^+\right) = f(2)$. Thus f is continuous at $x = 2$. But f is not differentiable at $x = 2$, because the left hand derivative is not equal to right hand derivative. To see this consider

$$f'\left(2^-\right) = \lim_{h \to 0} \frac{1 + (2 - h) - 3}{-h} = \lim_{h \to 0} \frac{h}{h} = 1$$

$$f'\left(2^+\right) = \lim_{h \to 0} \frac{5 - (2 + h) - 3}{h} = \lim_{h \to 0} \frac{-h}{h} = -1$$

UNIT–21 : MEAN VALUE THEOREMS

Contents

21.1 Aims and Objectives
21.2 Introduction
21.3 Rolle's theorem
21.4 Lagranges mean value theorem
21.5 Cauchy's mean value theorem
21.6 Applications
21.7 Summary
21.8 Sample Examination Questions
21.9 Answers to Self Assessment Questions

21.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to (i) state and prove the Rolle's theorem, (ii) State and prove Lagranges and Cauchy's Mean value theorem, (iii) Discuss the applicability of these theorems to given functions in given interval (iv) Discuss applications of these theorems.

21.2 INTRODUCTION

Mean value theorems relate the values of a function to values of its derivative. This in turn permits us to draw conclusions about the nature of a function from the information about its derivative. Seen from the geometrical point of view the mean value theorems state that there is some point on the curve $y = f(x)$ at which the tangent is parallel to the line segment drawn through the points $(a, f(a))$ and $(b, f(b))$.

21.3 ROLLE'S THEOREM

Theorem. 1 :

If a function $f : [a, b] \to R$ such that

(i) f is continuous on the closed interval $[a, b]$

(ii) f is derivable in the open interval (a, b) and

(iii) $f(a) = f(b)$

Then $\exists$ a real number $c \in (a, b)$ such that $f'(c) = 0$.

Proof : f is continuous in $[a, b]$

$\Rightarrow f$ is bounded in $[a, b]$ and attains its bounds in $[a, b]$

$\Rightarrow \exists\, c, d$ in $[a, b]$ such that

$f(c) = M$ and $f(d) = m$

where m and M are infimum and supremum of f in $[a, b]$.

Two cases may arise

(i) $M = m$

(ii) $M \neq m$

Case (i) When $M \neq m$, f is constant

$\Rightarrow f'(x) = 0 \; \forall \; x \in [a, b]$

$\Rightarrow$ in particular $f'(c) = 0$

Case (ii) when $M \neq m$

since $f(a) = f(b)$ and $M \neq m$

either M or m is different from $f(a)$ and $f(b)$

$\Rightarrow$ either $M \neq f(a)$ and $M \neq f(b)$

or $m \neq f(a)$ and $m - f(b)$

Let us consider the case when $M \neq f(a)$ and $M \neq f(b)$

Since $M = f(c)$

$f(c) \neq f(a)$

$\Rightarrow c \neq a.$

Similarly it can be shown that $c \neq b$

$\therefore c \in (a, b)$

f is derivable in (a, b) $\Rightarrow f$ is derivable at c

We shall show that $f'(c) = 0$

If possible let $f'(c) > 0$

Then $\exists \; \delta > 0$ such that

$f(x) > f(c) \; \forall \; x \in (c, c + \delta] \subset [a, b]$

$\Rightarrow f(x) > M \; \forall \; x \in [c, c + \delta) \subset [a, b]$

$(\because f(c) = M)$

This contradicts the fact that M is the least upper bound of f in $[a, b]$.

$\therefore$ Our assumption that $f'(c) > 0$ must be wrong

$\Rightarrow f'(c) \not> 0$ ... (1)

Again if possible let $f'(c) < 0$

Then there exists $h > 0$ such that

$f(x) > f(c) \; \forall \; x \in [c - h, c) \subset [a, b]$

$\Rightarrow f(x) > M \; \forall \; x \in [c - h, c) \subset [a, b]$ $(\because f(c) = M)$

This contradicts the fact that M is the least upper bound of f in $[a, b]$.

$\therefore$ our assumption that $f'(c) < 0$ must be wrong.

$$\Rightarrow f'(c) \not< 0 \qquad \ldots (2)$$

(1) and (2) $\Rightarrow f'(c) = 0$

Similarly we can prove that

If $m - f(a)$ and $m \neq f(b)$

then $f'(d) = 0, d \in (a, b)$

Note. 1 : There may exist more than one real number $c \in (a, b)$ such that $f'(c) = 0$, but Rolle's theorem ensures the existence of at least one real number c QŒ (a, b) with $f'(c) = 0$.

Note. 2 : Geometrically Rolle's theorem asserts that there is a least one point c, between $x = a$ and $x = b$ at which the tangent to the curve representing the graph of $y = f(x)$ is parallel to the x - axis.

Note. 3 : conditions of Rolle's Theorem are sufficient conditions. That is satisfying the conditions suffices to force the conclusion Functions can be constructed which violate all the three conditions in the theorem but yet the result might still hold. In short the conditions are not necessary for the result to be obtained.

SAQ 1 Discuss the application of Rolle's theorem to $f(x) = |x|$ in the interval $[-1, 1]$.

Example. 1 : Discuss the applicability of Rolle's theorem for the function

$$f(x) = (x - a)^m (x - b)^n \text{ in } [a, b]$$

m, n being positive integers.

Sol : Since f is a polynomial in x, f is continuous in $[a, b]$

$$\text{Also } f(a) = 0 = f(b).$$

$$f'(x) = (x - a)^{m-1} (x - b)^{n-1} . [m (x - b) + n (x - a)]$$

$$= (x - a)^{m-1} (x - b)^{n-1} . [(m + n) x - (an + bm)]$$

$\therefore f$ is derivable in (a, b)

So Rolle's theorem is applicable.

The point c in (a, b) is given by

$$f'(c) = 0$$

$$\Rightarrow c = \frac{mb + na}{m + n}$$

Example. 2 : Examine the applicability of Rolle's theorem for the function

$$f(x) = 2 + (x - 1)^{2/3} \text{ defined in the interval } [0, 2].$$

Sol. : The function $f(x) = 2 + (x - 1)^{2/3}$, being an algebraic function, is continuous in $[0, 2]$... (1)

$$\text{Now } f'(x) = \frac{2}{3} (x - 1)^{-1/3} = \frac{2}{3 (x - 1)^{1/3}}$$

which does not exist at $x = 1$

$\Rightarrow f$ is not derivable at $x = 1$

$\Rightarrow f$ is not derivable in $(0, 2)$ ... (2)

$$\text{Also } f(0) = 3 = f(2) \qquad \ldots (3)$$

(1), (2) and (3) $\Rightarrow f$ does not satisfy all the Rolle's conditions and consequently the Rolle's theorem is not applicable for the given function.

21.4LAGRANGES MEAN VALUE THEOREM

Theorem. 2 :

> If $f : [a, b] \to R$ is such that
>
> (i) f is continuous in $[a, b]$ and
>
> (ii) f is derivable in (a, b)
>
> then $\exists$ a real number $c \in (a, b)$
>
> such that $f(b) - f(a) = (b - a) f'(c)$

Proof : Define a function $\phi : [a, b] \to R$

$$\text{by } \phi(x) = f(x) + kx \; \forall \; x \in [a, b]$$

where k is a constant given by

$$\phi(a) = \phi(b) \qquad \ldots (1)$$

$$\Rightarrow k = \frac{f(b) - f(a)}{a - b} \qquad \ldots (2)$$

f is continuous in $[a, b]$ by hypothesis. kx, being a polynomial in x, is continuous in $[a, b]$.

$\therefore \phi$, being the sum of two continuous functions in $[a, b]$ is continuous in $[a, b]$. ... (3)

Also ϕ, being the sum of two derivable functions is derivable in (a, b) ... (4)

Conditions (1), (3) and (4) $\Rightarrow$ all the Rolle's condition are satsified by ϕ.

$\therefore$ By Rolle's $\exists\, c \in (a, b)$

such that $\phi'(c) = 0$

$\Rightarrow f'(c) + k = 0$

or $k = -f'(c)$ ... (5)

(2) and (5) $\Rightarrow -f'(c) = \dfrac{f(b) - f(a)}{a - b}$

$\Rightarrow f(b) - f(a) = (b - a) f'(c)$.

Note : Lagrange's mean value theorem may be stated as follows :

If $f : [a, a + h] \to R$ is such that

(i) f is continuous i $[a, a + h]$

(ii) f is derivable in $(a, a + h)$

then $\exists$ a number $\theta \in (0, 1)$

such that $f(a + h) - f(a) = h f'(a + \theta h)$

Putting $b = a + h$ in Lagrange's mean value theorem, we get this form of the theorem.

Deduction. 1 : If $f : [a, b] \to R$ is such that

(i) f is continuous in $[a, b]$

(ii) f is derivable in (a, b) and

(iii) $f'(x) = 0 \; \forall \; x \in (a, b)$

then f is constant in (a, b)

Proof : Let x_1, x_2 be any two points in (a, b).

$$\text{Let } x_1 < x_2$$

Then $\left[x_1, x_2\right] \subset [a, b]$

By hypothesis f is continuous in $\left[x_1, x_2\right]$ and derivable in $\left(x_1, x_2\right)$.

By Lagrange's mean value theorem

$\exists$ a point $c \in \left(x_1, x_2\right)$ such that

$$f\left(x_2\right) - f\left(x_1\right) = \left(x_2 - x_1\right) f'(c)$$

$$\text{By data } f'(c) = 0$$

$$\therefore f\left(x_2\right) = f\left(x_1\right)$$

i.e., f is constant in (a, b)

By continuity, f is a constant in $[a, b]$.

Deduction. 2 : If $f : [a, b] \to R$ and $g : [a, b] \to R$ are two functions such that

(i) f, g are continuous in $[a, b]$

(ii) f, g are derivable in (a, b) and

(iii) $f'(x) = 0 \; \forall \; x \in (a, b)$

then f and g differ by a constant.

Proof : Let $\phi(x) = f(x) - g(x) \; \forall \; x \in [a, b]$

Then ϕ, being the difference of two continuous functions f and g, is continuous in $[a, b]$. Similarly ϕ, being the difference of two derivable functions f and g in (a, b), is derivable in (a, b).

Also $\phi'(x) = f'(x) - g'(x) = 0$

$\therefore \phi$ is constant in $[a, b]$.(By deduction 1)

$\therefore$ $f(x) - g(x) = \text{constant} \; \forall \; x \in (a, b)$

$\therefore f$ and g differ by a constant in $[a, b]$.

Monotone Functions : Let $f : S \to R$ be a function where S is an aggregate. f is said to be monotonically increasing (decreasing) on S if $x, y \in S$ and

$$x < y \Rightarrow f(x) \leq f(y) \; (f(x) \geq f(y))$$

f is said to be strictly monotonically inceasing (strictly monotonically decreasing) on S if $x, y \in S$ and

$$x < y \Rightarrow f(x) < f(y) \; (f(x) > f(y))$$

Monotonically increasing or monotonically decreasing functions are referred to by the common phrase "monotone" functions.

Deducation. 3 : A function $f : [a, b] \to R$ having a positive derivative for every value of x in $[a, b]$ is a monotonically increasing function in $[a, b]$; $f : [a, b] \to R$ having a negative derivative for every value of x in $[a, b]$ is a monotonically decreasing function in $[a, b]$.

Proof : **First part**

Let $f'(x) > 0 \forall x \in [a, b]$

Let x_1, x_2 be any two points of $[a, b]$ such that $x_2 > x_1$

Since f is derivable in $[a, b]$, f is continuous in $[a, b]$ and hence continuous in $\left[x_1, x_2\right]$

Also f is derivable in (a, b) and hence in $\left(x_1, x_2\right)$

$\therefore$ by Lagrange's mean value theorem

$$f\left(x_2\right) - f\left(x_1\right) = \left(x_2 - x_1\right) f'(c)$$

where $x_1 < c < x_2$

Now $x_2 - x_1 > 0$ and $f'(c) > 0$

$$\therefore f\left(x_2\right) - f\left(x_1\right) > 0$$

$$\therefore f\left(x_2\right) > f\left(x_1\right)$$

Hence f is strictly monotonically increasing in $[a, b]$

Second part

If $f'(c) > 0 \forall x \in [a, b]$

then proceeding as in part I

we get $f\left(x_2\right) - f\left(x_1\right) = \left(x_2 - x_1\right) f'(c)$

where $x_1 < c < x_2$

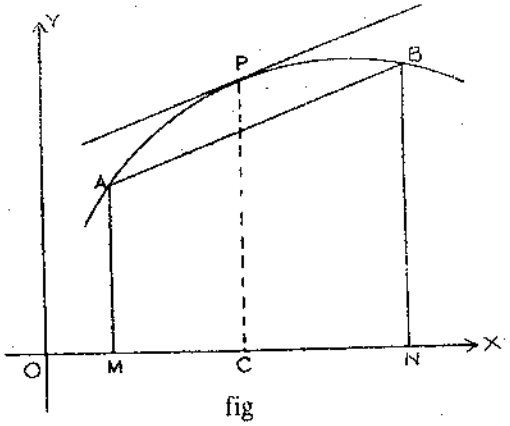
Now $x_2 - x_1 > 0$ and $f'(c) > 0$

$$\therefore f\left(x_2\right) - f\left(x_1\right) > 0$$

$$\therefore f\left(x_2\right) < f\left(x_1\right)$$

Hence f is a strictly monotonically decreasing function in $[a, b]$

Remark. 1 : **Geometrical Interpretation of Lagrange's Mean Value Theorem**



fig

Let APB be the graph of the function $y = f(x)$ satisfying the conditions of Lagrange's mean value theorem between $x = a$ and $x = b$.

Then $\frac{f(b)-f(a)}{b-a}$ = slope of the chord AB

$f'(c)$ = slope of the tangent at $x = c \in (a, b)$

$\therefore \frac{f(b)-f(a)}{b-a} = f'(c) \Rightarrow$

the chord AB is parallel to the tangent at $x = c$.

Thus geometrically, Lagrange's mean value theorem asserts that if APB be the graph of the curve represented by the function $y = f(x)$ satisfying the conditions of the mean value theorem, then there is some point P on the curve between $x = a$ and $x = b$ the tangent at which is parallel to the chord AB.

Example. 3 : Find c of Lagrange's Mean Value theorem for the function f given by

$$f(x) = x(x-1)(x-2) \; \forall \; x \in \left[0, \frac{1}{2}\right]$$

Sol. : f, being a polynomial, is continuous in $\left[0, \frac{1}{2}\right]$ and derivable in $\left(0, \frac{1}{2}\right)$

$$\therefore \frac{f\left(\frac{1}{2}\right) - f(0)}{\frac{1}{2} - 0} = f'(c)$$

$$\frac{\frac{3}{8} - 0}{\frac{1}{2} - 0} = f'(c)$$

$$\therefore f'(c) = \frac{3}{4}$$

Now $f(x) = x^3 - 3x^2 + 2x$

$f'(x) = 3x^2 - 6x + 2$

$f'(c) = 3c^2 - 6c + 2$

$\therefore 3c^2 - 6c + 2 = \frac{3}{4}$

Solving $c = \frac{6 + \sqrt{21}}{6}$ or $\frac{6 - \sqrt{21}}{6}$

Of these two values only $\frac{6-\sqrt{21}}{6}$ lies in the inverval $\left(0, \frac{1}{2}\right)$

Hence the required value of c is $\frac{6-\sqrt{21}}{6}$.

Example. 4 : Show that $\tan x > x > \sin x \; \forall \; x \in \left(0, \frac{\pi}{2}\right)$

Sol. : Let $f(x) = \tan x - x$

Then $f'(x) = \sec^2 x - 1 > 0$ for $x \in \left(0, \frac{\pi}{2}\right)$

$\therefore f$ is an increasing function in $\left(0, \frac{\pi}{2}\right)$ ... (1)

But $f(0) = 0$ ... (2)

$\therefore f$ is an increasing function in $\left(0, \frac{\pi}{2}\right)$ ... (1)

But $f(0) = 0$ ... (2)

$\therefore$ (1) and (2) $\Rightarrow f(x) > 0 \; \forall \; x \in \left(0, \frac{\pi}{2}\right)$

$\therefore \tan x - x > 0$ for $x \in \left(0, \frac{\pi}{2}\right)$ ... (I)

Again let $\phi(x) = x - \sin x \; \forall \; x \in \left(0, \frac{\pi}{2}\right)$

$\phi'(x) = 1 - \cos x > 0 \; \forall \; x \in \left(0, \frac{\pi}{2}\right)$

$\therefore \phi$ is an increasing function in $\left(0, \frac{\pi}{2}\right)$ ... (3)

Also $\phi(0) = 0$ ... (4)

$\therefore$ (3) and (4) $\Rightarrow \phi(x) > 0 \; \forall \; x \in \left(0, \frac{\pi}{2}\right)$

$\Rightarrow x - \sin x > 0$

$\Rightarrow x > \sin x \; \forall \; x \in \left(0, \frac{\pi}{2}\right)$ ... (II)

I and II $\Rightarrow \tan x > x > \sin x$.

Example. 5 : Show that $\frac{\tan x}{x} > \frac{x}{\sin x} \; \forall \; x \in \left(0, \frac{\pi}{2}\right)$

Sol : $\frac{\tan x}{x} - \frac{x}{\sin x} = \frac{\tan x \sin x - x^2}{x \sin x}$

Let $f(x) = \tan x \sin x - x^2$

Then $f' = \sec^2 \sin x + \tan x \cos x - 2x$

$= \sin x \left(\sec^2 x + 1\right) - 2x$

Let $g(x) = f'(x)$

Then $g'(x) = \cos x \left(\sec^2 x + 1\right) + \sin x \, . \, 2\sec^2 x \tan x - 2$

$= \sec x + \cos x + 2 \sin^2 x \sec^3 x - 2$

$= \left(\sqrt{\sec x} - \sqrt{\cos x}\right)^2 + 2 \sin^2 x \sec^3 x$

> 0 for $x \in \left(0, \frac{\pi}{2}\right)$

$\therefore g(x)$ is an increasing function in $\left(0, \frac{\pi}{2}\right)$

Also $g(0) = 0$

$\therefore g(x) > g(0) = 0$

$\therefore g(x) > 0 \; \forall \; x \in \left(0, \frac{\pi}{2}\right)$

$\therefore f'(x) > 0 \; \forall \; x \in \left(0, \frac{\pi}{2}\right)$

$\therefore f$ is an increasing function in $\left(0, \frac{\pi}{2}\right)$

$$\therefore f(x) > f(0) = 0$$

$$\therefore f(x) > 0$$

$\therefore \tan x \sin x - x^2 > 0$

Also $x \sin x > 0$ in $\left(0, \frac{\pi}{2}\right)$

$$\therefore \frac{\tan x \sin x - x^2}{x \sin x} > 0$$

$$\Rightarrow \frac{\tan x}{x} > \frac{x}{\sin x}$$

21.5 CAUCHY'S MEAN VALUE THEOREM

Theorem. 3 :

If $f : [a, b] \to R$, $g : [a, b] \to R$ are such that

(i) f and g are continuous on $[a, b]$

(ii) f and g are derivable on (a, b) and

(iii) $g'(x) \neq 0$ for any $x \in (a, b)$

Then $\exists$ a point $c \in (a, b)$ such that

$$\frac{f(b) - f(a)}{g(b) - g(a)} = \frac{f'(c)}{g'(c)}$$

Proof : In order to prove the theorem let us define a function $[a, b]$ involving the two given functions f and g and apply Rolle's theorem to the new function

Define $\phi : [a, b] \to R$ by

$$\phi(x) = f(x) + kg(x) \; \forall \; x \in [a, b]$$

where k is a constant given by

$$\phi(a) = \phi(b) \qquad \ldots (1)$$

$$\text{i.e., } k = -\frac{[f(b) - f(a)]}{g(b) - g(a)} \qquad \ldots (2)$$

provided $g(b) - g(a) \neq 0$

We shall prove that $g(b) - g(a) \neq 0$

If possible let $g(b) - g(a) = 0$

$$\Rightarrow g(b) = g(a)$$

Then g satsifies all the three conditions of Rolle's theorem on $[a, b]$

$\therefore$ there exists a point $c \in (a, b)$ such that $g'(c) = 0$ which contradicts the fact that

$$g'(x) \neq 0 \text{ for any } x \in (a, b)$$

Hence $g(b) - g(a) \neq 0$.

Now ϕ, being a linear combination of two continuous functions f and g in $[a, b]$ is continuous in $[a, b]$. ... (3)

Also ϕ, being a linear combination of two derivable functions f and g in (a, b) is derivable in (a, b) ... (4)

$\therefore$ (1), (3) and (4) $\Rightarrow$ that ϕ satisfies all the three conditions of Rolle's theorem.

$\therefore$ By Rolle's theorem there exists a point $c \in (a, b)$ such that

$$\phi'(c) = 0$$

$$\phi'(x) = f'(x) + kg'(x)$$

$$\therefore \phi' = 0 \Rightarrow k = \frac{-f'(c)}{g'(c)} \quad \ldots (5)$$

($\because g'(x) \neq 0$ for any $x \in (a, b)$)

(2) and (5) $\Rightarrow$

$$\frac{f(b) - f(a)}{g(b) - g(a)} = \frac{f'(c)}{g'(c)}$$

Note : Putting $b = a + h$ we get another form of Cauchy's Mean value theorem as follows :

$$\frac{f(a + h) - f(a)}{g(a + h) - g(a)} = \frac{f'(a + \theta h)}{g'(a + \theta h)} \text{ where } 0 < \theta < 1$$

Theorem. 4 :

If $f : [a, b] \to R$, g $[a, b] \to R$

$h : [a, b] \to R$ are such that

(i) f, g and h are continuous in $[a, b]$,

(ii) f, g and h are derivable in $[a, b]$

then $\exists$ a real number $c \in (a, b)$ such that

$$\begin{vmatrix} f'(c) & g'(c) & h'(c) \\ f(a) & g(a) & h(a) \\ f(b) & g(b) & h(b) \end{vmatrix} = 0$$

Proof : In order to prove the theorem let us define a new function on $[a, b]$ involving f, g and h and then apply Rolle's theorem to the new function.

Let $\phi : [a, b] \to R$ be defined by

$$\phi(x) = \begin{vmatrix} f(x) & g(x) & h(x) \\ f(a) & g(a) & h(a) \\ f(b) & g(b) & h(b) \end{vmatrix} \quad \forall x \in [a, b]$$

Now ϕ being a linear combination of continuous functions f, g and h is continuous on $[a, b]$. ... (1)

ϕ, being a linear combination of derivable functions f, g, h is derivable in (a, b) ... (2)

Also $\phi(a) = 0 = \phi(b)$

($\because$ two rows become identical in the determinant)

$$\therefore \phi(a) = \phi(b) \qquad \ldots (3)$$

$\therefore$ (1), (2) and (3) $\Rightarrow$ that ϕ satisfies all the conditions of Rolle's theorem

$\therefore$ by Rolle's theorem there exists a point c in (a, b) such that

$$\phi'(c) = 0$$

Now
$$\phi'(x) = \begin{vmatrix} f'(x) & g'(x) & h'(x) \\ f(a) & g(a) & h(a) \\ f(b) & g(b) & h(b) \end{vmatrix}$$

$$\therefore \phi'(c) = 0 \Rightarrow \begin{vmatrix} f'(c) & g'(c) & h'(c) \\ f(a) & g(a) & h(a) \\ f(b) & g(b) & h(b) \end{vmatrix} = 0$$

Deducation. 1 : Taking $g(x) = x$ and $h(x) = 1 \ \forall \ x \in [a, b]$ in the above theorem we obtain Lagrange's mean value theorem.

Deduction. 2 : Taking $h(x) = 1$ in the above theorem we obtain Cauchy's mean value theorem.

SAQ 2 Discuss the application of Cauchy's mean value theorem to the functions x^2 and x^3 in the interval [1, 2].

21.6 APPLICATIONS

Exercise. 1 : Use Lagranges Mean Value theorem to evaluate $\sqrt{105}$.

Ans : Consider $f(x) = \sqrt{x}$ in the interval $[a, b]$ where $a = 100$, $b = 105$. Then f satisfies all the conditions of Lagranges mean value theorem. Then

$$\frac{f(b) - f(a)}{b - a} = \frac{\sqrt{105} - \sqrt{100}}{5} = \frac{1}{2\sqrt{c}} \text{ for some } c \in (100, 105).$$

Thus $\sqrt{105} - \sqrt{100} = \frac{5}{2\sqrt{c}}$ for $100 < c < 105$.

Since $10 < \sqrt{c} < \sqrt{105} < \sqrt{121} = 11$, we get

$$\frac{5}{2(11)} < \sqrt{105} - 10 < \frac{5}{2(10)}$$

$$10.22 < \sqrt{105} < 10.25.$$

This inequality could be further sharpened by taking a smaller interval. For example $\sqrt{105} < 10.25$ and hence $\sqrt{c} < 10.25$ so that

$$0.243 < \frac{5}{2(10.25)} < 0.250.$$

or $10.243 < \sqrt{105} < 10.250$ etc.

Exercise. 2 : Show that $\frac{x - y}{1 + x^2} < \tan^{-1} x - \tan^{-1} y < \frac{x - y}{1 + y^2}$ if $0 < x < y$.

Ans : Let $f(\theta) = \tan^{-1}\theta$, so that $f'(\theta) = \frac{1}{1+\theta^2}$; f satisfies the conditions of mean value theorem in the interval.

$$\text{Hence } \frac{\tan^{-1}x - \tan^{-1}y}{x-y} = \frac{1}{1+c^2} \text{ for } x < c < y$$

$$\text{But } c > x \Rightarrow \frac{1}{1+c^2} < \frac{1}{1+x^2}$$

$$\text{and } c < y \Rightarrow \frac{1}{1+c^2} > \frac{1}{1+y^2}.$$

$$\therefore \frac{1}{1+x^2} > \frac{\tan^{-1}x - \tan^{-1}y}{x-y} < \frac{1}{1+y^2}.$$

$$\text{or } \frac{x-y}{1+x^2} < \tan^{-1}x - \tan^{-1}y < \frac{x-y}{1+y^2}.$$

21.7 SUMMARY

Rolle's theorem states that if a continuous function defined on a closed interval is such that it is differentiable and has equal values at the end points of the interval then there must exist atleast one point where the derivative vanishes. In case we relax the condition of equality of the function at the end points of the interval then there must exist atleast one point where the tangent is parallel to the chord. These mean value theoems have far reaching consequences especially when we wish to linearise (approximate) a nonlinear function or estimate its value at a point.

21.8 MODEL EXAMINATION QUESTIONS

Section A (Long Answer)

i) State and prove Rolle's theorem and discuss its application to the function $f(x) = 8x - x^2$ in the interval $[0, 8]$.

ii) State and prove Lagranges Mean Value theorem and discuss its application to $f(x) = \sqrt{x^2 - 4}$ in the interval $[2, 4]$.

iii) State and prove Cauchy's Mean value theorem and discuss its application to $f(x) = \sqrt{x}$ and $g(x) = \frac{1}{\sqrt{x}}$ in $[a, b]$ where $0 < a < b$.

Section B (Short Answer)

i) If f, g and h are continuous in $[a, b]$ and derivable in $[a, b]$, show that there exists $c \in (a, b)$ such that

$$\begin{vmatrix} f'(c) & g'(c) & h'(c) \\ f(a) & g(a) & h(a) \\ f(b) & g(b) & h(b) \end{vmatrix} = 0.$$

ii) By applying appropriate mean value theorem to $f(x) = \tan x \sin x - x^2$ show that

$$\frac{\tan x}{x} > \frac{x}{\sin x} \text{ for } x \in \left(0, \frac{\pi}{2}\right).$$

21.9 ANSWERS TO SAQ'S

SAQ 1 $f(-1) = f(1)$ and $f(x)$ is continuous in $[-1, 1]$. But $f(x)$ is not differentiable at $x = 0 \in (-1, 1)$. Hence Rolle's theorem is not applicable to f in $[-1, 1]$.

SAQ 2 Let $f(x) = x^2$ and $g(x) = x^3$. Then f and g are continuous in $[1, 2]$ and f and g are differentiable in $[1, 2]$ and $f(x) \neq 0$ in $[1, 2]$.

$$\therefore \frac{g(2) - g(1)}{f(2) - f(1)} = \frac{8 - 1}{4 - 1} = \frac{7}{3} ; \frac{g'(x)}{f'(x)} = \frac{3x^2}{2x} = \frac{3}{2} x.$$

$$\therefore \frac{g'(c)}{f'(c)} = \frac{3}{2} \cdot c.$$

$$c = \frac{7}{3} \times \frac{2}{3} = \frac{14}{9} \in (1, 2).$$

Thus there exists $\frac{14}{9} \in (1, 2)$ such that

$$\frac{g'(c)}{f'(c)} = \frac{g(2) - g(1)}{f(2) - f(1)}$$ and the theorem is satsified.

UNIT–22 : TAYLOR'S THEOREM AND APPLICATIONS

Contents

22.1 Aims and Objectives
22.2 Introduction
22.3 Taylor's theorem
22.4 Expansion of a function
22.5 Indeterminate forms
22.6 Worked out exercises
22.7 Summary
22.8 Sample Examination Questions

22.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to (i) State and prove the Taylor's theorem, (ii) State Maclaurin's theorem and apply the same to expand a given function, (iii) State L'Hospital's rule and apply the same to evaluate limits to indeterminate forms, (iv) Apply Taylor's theorem to solve polynomial and other equations

22.2 INTRODUCTION

One of the problems one encounters in analysis is the approximation of a given function by an appropriate polynomial. A fundamental result towards this goal was given by Brook Taylor (1685-1731). Taylor's theorem is also a mean value theorem where higher order derivatives are used to provide a relation between the values of a function and its derivatives. The notion of a higher order derivative is a natural extension of the differentiation process. If the derivative f' of a function f exists in an interval, then f'' or f^2 is the derivative of f' in that interval (if it exists). This process could be continued to define nth order derivatives. Then if a function satisifies certain conditions regarding its nth order derivatives, then the function could be approximated by a Taylor's polynomial. The remainder term R_n in the Taylor's theorem could be used to estimate the error of approximation. Colin Maclaurin (1698-1746) and Marquis Guillame Francios L' Hospital (1661-1704) have given the applications of mean value theorems to expansions of functions and evaluating limits.

22.3 TAYLOR'S THEOREM

Theorem. 1 :

If a function $f : [a, b] \to R$ is such that

(i) f^{n-1} is continuous on $[a, b]$

(ii) f^{n-1} is derivable on (a, b) i.e., f^n exists in (a, b) and p is a positive integer then there exists a point $c \in (a, b)$ such that

$$f(b) = f(a) + \frac{(b-a)}{1!} f'(a) + \frac{(b-a)^2}{2!} f''(a) + \ldots + \frac{(b-a)^n}{(n-1)!} f^{n-1}(a) + R_n$$

where $R_n = \dfrac{(b-a)^p (b-c)^{n-p} f^{(n)}(c)}{p\,(n-1)!}$

Proof : Define a function $\phi : [a, b] \to R$ by

$$\phi(x) = f(b) - f(x) - \frac{(b-x)}{1!} f'(x) - \frac{(b-x)^2}{2!} f''(x)$$

$$- \frac{(b-x)^{n-1}}{(n-1)!} f^{(n-1)}(x) - A\left(\frac{b-x}{b-a}\right)^p$$

where A is chosen such that $\phi(a) = 0$.

f^{n-1} is continuous on $[a, b]$ and derivable on $(a, b) \Rightarrow f, f', f'', \ldots f^{n-1}$ are all continuous on $[a, b]$ and derivable on (a, b).

Also $\left(\frac{b-x}{b-a}\right)^p$ is continuous on $[a, b]$ and derivable on (a, b) for each positive integer p.

$$\text{Now } \phi(b) = 0$$

$$\therefore \phi(a) = \phi(b)$$

Thus the function ϕ is such that

(i) ϕ is continuous on $[a, b]$

(ii) ϕ is derivable in (a, b) and

(iii) $\phi(a) = \phi(b)$

$\therefore$ "äüy Rolle's theorem there exists a point $c \in (a, b)$ such that

$$\phi'(c) = 0$$

$$\phi(a) = 0 =$$

$$f(b) - f(a) - \frac{(b-a)}{1!} (a - \frac{(b-a)^2}{2!} f''(a) - \ldots$$

$$- \frac{(b-a)^{n-1}}{(n-1)!} f^{(n-1)}(a) - A = 0 \qquad \ldots (IV)$$

$$\text{Now } \phi'(x) = -f'(x) - [-f'(x) + (b-x) f''(x)]$$

$$- \left[- (b-x) f''(x) + \frac{(b-x)^2}{2!} f'''(x) \right] - \ldots$$

$$- \left[- \frac{(b-x)^{n-2}}{(n-2)!} f^{(n-1)}(x) + \frac{(b-x)^{n-1}}{(n-1)!} f^{(n)}(x) \right]$$

$$+ \frac{Ap}{(b-a)^p} (b-x)^{p-1}$$

(The second term in each bracket cancells with the first term of the succeeding bracket)

On simplification

$$\phi'(x) = - \frac{(b-x)^{n-1}}{(n-1)!} f^{(n)}(x) + \frac{pA(b-x)^{p-1}}{(b-a)^p}$$

$$\therefore \phi'(c) = 0 \Rightarrow A = \frac{(b-a)^p (b-c)^{n-p} \cdot f^{(n)}(c)}{p\,(n-1)!}$$

On substituting this value of A in (iv) we get

$$f(b) = f(a) + \frac{(b-a)}{1!} f'(a) + \frac{(b-a)^2}{2!} f''(a) + \ldots$$

$$+ \frac{(b-a)^{n-1}}{(n-1)!} f^{(n-1)}(a)$$

$$+ \frac{(b-a)^p (b-c)^{n-p}}{p\,(n-1)!} f^{(n)}(c)$$

Note : Schlomilche-Roche form of the remainder R_n is given by

$$R_n = \frac{(b-a)^p (b-c)^{n-p}}{p\,(n-1)!} f^{(n)}(c)$$

Putting $p = n$ we get Cauchy's form of the remainder R_n given by

$$R_n = \frac{(b-a)^n f^{(n)}(c)}{n!}$$

Putting $p = 1$ we get Cauchy's form of the remainder R_n given by

$$R_n = \frac{(b-a)(b-c)^{n-1} f^{(n)}(c)}{(n-1)!}$$

***Remark. 1 :* Alternative Form of Taylor's Theorem**

If a function f defined on $[a, a+h]$ is such that

(i) f^{n-1} is continuous on $[a, a+h]$

(ii) f^{n-1} is derivable on $(a, a+h)$

and p is a positive integer.

then $\exists$ a real number $\theta \in (0, 1)$ such that

$$f(a+h) = f(a) + \frac{h}{1!} f'(a) + \frac{h^2}{2!} f''(a) + \ldots$$

$$+ \frac{h^{n-1}}{(n-1)!} f^{(n-1)}(a)$$

$$+ \frac{h^n}{p\,(n-1)!} (1-\theta)^{n-p} f^{(n)}(a+\theta h)$$

This form can be obtained by putting $b = a + h$ and $c = a + \theta h$ where $\theta \in (0, 1)$ in the above theorem.

In this form of Taylor's theorem, Lagrange's form of the remainder is

$$\frac{h^n}{n!} f^{(n)}(a+\theta h)$$

and Cauchy's form of the remainder is

$$\frac{h^n}{n!} (1-\theta)^{n-1} f^{(n)}(a+\theta h)$$

Theorem. 2 : Maclaurin's theorem with Schlomiche-Roche form of the remainder

If a function f defined on $[0, x]$ is such that

(i) f^{n-1} is continuous on $[0, x]$ and

(ii) f^{n-1} is derivable on $(0, x)$
and p is a positive integer

then there exists some $\theta \in (0,1)$ such that

$$f(x) = f(0) + \frac{x}{1!} f'(0) + \frac{x^2}{2!} f''(0) + \ldots + \frac{x^{n-1}}{(n-1)!} f^{(n-1)}(0) + \frac{x^n (1-\theta)^{n-p}}{p\,(n-1)!} f^{(n)}(\theta x)$$

Proof : If we put $a = 0$, $h = x$, $c = \theta x$ for some $\theta \in (0, 1)$ in Taylor's theorem we get Maclaurin's theorem.

On putting $p = n$ in Schlomilche-Roche form of the remainder we get Lagrange's form of the remainder viz,

$$R_n = \frac{x^n}{n!} f^{(n)}(\theta x)$$

On putting $p = 1$ in Schlomilche - Roche form of the remainder we get Cauchy's form of the remainder viz,

$$R_n = \frac{x^n (1-\theta)^{n-1}}{(n-1)!} f^{(n)}(\theta x)$$

22.4 POWER SERIES EXPANSION

Let us suppose that a function f defined on $[a, a + h]$ possess continuous derivatives of every order in $[a, a + h]$ then for all $n \in N$ we have

$$f(a+h) = f(a) + \frac{h}{1!} f'(a) + \frac{h^2}{2!} f''(a) + \ldots + \frac{h^{n-1}}{(n-1)!} f^{(n-1)}(a) + R_n \quad \ldots (1)$$

where R_n is Taylor's remainder after n terms.

$$\text{Let } S_n = f(a) + \frac{h}{1!} f'(a) + \frac{h^2}{2!} f''(a) + \ldots + \frac{h^{n-1}}{(n-1)!} f^{(n-1)}(a) \quad \ldots (2)$$

$$\text{Then } f(a+h) = S_n + R_n$$

Now if $R_n \to 0$ as $n \to \infty$, then

$$\lim_{n\to\infty} (S_n) = f(a+h), \text{ a finite quantity.}$$

i.e., the sequence $\{S_n\}$ converges to $f(a+h)$

i.e., the series

$$f(a)+\frac{h}{1!}f'(a)+\frac{h^2}{2!}f''(a)+\ldots+\frac{h^{n-1}}{(n-1)!}f^{(n-1)}(a)+\ldots \text{ converges to } f(a+h)$$

Thus we conclude that

(i) if f possesses continuous derivatives of every order in $[a, a+h]$ and

(ii) the remainder R_n after n terms tends to zero as $n \to \infty$

$$\text{Then } f(a+h) = f(a)+\frac{h}{1!}f'(a)+\frac{h^2}{2!}f''(a)+\ldots+\frac{h^n}{n!}f^{(n)}(a)\ldots$$

The series on R.H.S. is known as the Taylor's series.

Expansion of Some Basic Functions in Series

If $a = 0$ in Taylor's series, the resulting series is called Malclaurin series.

We shall find the Maclaurin expansion of e^x, $\sin x$, $\cos x$, $\log(1+x)$ and $(1+x)^p$

Example 1 : Expansion of e^x

Case (i) If $x \neq 0$, let $X = \begin{cases} [0, x] \text{ for } x > 0 \\ [x, 0] \text{ for } x < 0 \end{cases}$

Let $f: X \to R$ be defined by

$$f(x) = e^x \; \forall \; x \in X$$

$$\text{Then } f^{(n)}(x) = e^x \; \forall \; x \in X \text{ and } n \in N$$

$$\therefore f^{(n)}(0) = 1 \; \forall \; n \in N$$

Lagrange's form of the remainder R_n after n terms is $\frac{h^n}{n!}f^{(n)}(a+\theta h)$

$$= \frac{x^n f^{(n)}(\theta x)}{n!}$$

$$= \frac{x^n}{n!}e^{\theta x} \text{ where } 0 < \theta < 1$$

We shall show that $R_n \to 0$ as $n \to \infty$

$$\text{Let } u_n = \frac{x^n}{n!}$$

$$\text{Then } \frac{u_{n+1}}{u_n} = \frac{x^{n+1}}{(n+1)!}\cdot\frac{n!}{x^n} = \frac{x}{n+1}$$

$$\therefore \left|\frac{u_{n+1}}{u_n}\right| = \frac{|x|}{n\left(1+\frac{1}{n}\right)}$$

$$\therefore \lim_{n\to\infty}\left|\frac{u_{n+1}}{u_n}\right| = 0 < 1$$

$$\therefore \lim_{n\to\infty} \left(u_n\right) = 0$$

$$\therefore \lim_{n\to\infty} R_n = \lim_{n\to\infty} \left(u_n\right) e^{\theta x} = 0.\ e^{\theta x} = 0$$

Case (ii) At $x = 0, S_n = 0$

$$\therefore \lim_{n\to\infty} \left(S_n\right) = 0$$

Hence f has a Maclaurin's expansion for each $x \in [-h, h], h > 0$. Equivalently we have

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots + \frac{x^n}{n!} + \ldots \ \forall\, x \in R$$

Note : Result used in the proof of the theorem.

If a sequence $\left\{u_n\right\}$ is such that

$$\lim_{n\to\infty} \left|\frac{u_{n+1}}{u_n}\right| = l < 1 \text{ then } \lim_{n\to\infty} \left(u_n\right) = 0.$$

Example. 2 : Expansion of sin x

Case (i) Let $x \neq 0$

$$\text{Let } X = \begin{cases} [0, x] & \text{if } x > 0 \\ [x, 0] & \text{if } x < 0 \end{cases}$$

Then for the function $f : X \to R$

defined by $f(x) = \sin x$,

we have $f^{(n)}(x) = \sin\left(x + \frac{n\pi}{2}\right)$.

Also $f^{(n)}$ is continuous in X.

$$\therefore f(x) = \sin x = f(0) + \frac{x}{1!} f'(0) + \frac{x^2}{2!} f''(0) + \ldots$$

$$+ \frac{x^{n-1}}{(n-1)!} f^{(n-1)}(0) + R_n$$

If Lagrange's form of R_n is taken,

$$\text{then } R_n = \frac{x^n}{n!} f^{(n)}(\theta x)$$

$$= \frac{x^n}{n!} \sin\left[\theta x + \frac{n\pi}{2}\right] \text{ where } 0 < \theta < 1.$$

$$\therefore |R_n| \leq \frac{|x^n|}{n!}$$

$$\text{But } \lim_{n\to\infty} \frac{|x^n|}{n!} = 0$$

$\therefore R_n \to 0$ as $n \to \infty$

Therefore, for $x \neq 0$,

$$\sin x = f(0) + \frac{x}{1!}f'(0) + \frac{x^2}{2!}f''(0) + \ldots$$

$$+ \frac{x^n}{n!}f^n(0) + \ldots$$

$$= \frac{x}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} - \ldots$$

$(\because f(0) = 0; f'(0) = 1; f''(0) = 0;$

$f'''(0) = -1$ and so on)

Case (ii) Let $x = 0$

$$S_n = 0 \text{ for } x = 0$$

$$\therefore \lim_{n\to\infty}(S_n) = 0. \text{ Further } \sin x = 0 \text{ for } x = 0$$

$$\therefore \sin x = \frac{x}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} - \ldots$$

Hence for all $x \in R$

$$\sin x = \frac{x}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} - \ldots$$

Example. 3 : Expansion of $\cos x$

Case (i) Let $x \neq 0$

$$\text{Let } X = \begin{cases} [0, x] \text{ for } x > 0 \\ [x, 0] \text{ for } x < 0 \end{cases}$$

Then $f: X \to R$ defined by

$$f(x) = \cos x \; \forall \; x \in X$$

$$\text{We have } f^{(n)}(t) = \cos\left(t + \frac{n\pi}{2}\right)$$

Further $f^{(n)}$ is continuous on X.

$$\therefore f(x) = \cos x = f(0) + \frac{x}{1!}f'(0) + \frac{x^2}{2!}f''(0) + \ldots$$

$$+ \frac{x^{n-1}}{(n-1)!}f^{(n-1)}(0) + R_n$$

Lagrange's form of the remainder R_n is given by

$$R_n = \frac{x^n}{n!}f^{(n)}(\theta x)$$

$$= \frac{x^n}{n!}\sin\left(\theta x + \frac{n\pi}{2}\right) \text{ where } 0 < \theta < 1$$

$$\therefore |R_n| \leq \frac{|x^n|}{n!}$$

$$\text{But } \lim_{n\to\infty}\frac{|x^n|}{n!} = 0$$

$$\therefore \text{for } x = 0$$

$$\cos x = f(0) + \frac{x}{1!}f'(0) + \frac{x^2}{2!}f''(0) + \ldots$$

$$= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \ldots$$

$(\because f(0) = 1; f'(0) = 0; f''(0) = -1, f'''(0) = 0; f^{(4)}(0) = 1$ and son on)

Case (ii) Let $x = 0$

Then $S_n = 1$ at $x = 0$

$$\therefore \lim_{n\to\infty} (S_n) = 1$$

Further $\cos x = 1$ at $x = 0$

$\therefore$ if $x = 0$

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \ldots$$

Hence for all $x \in R$

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \ldots$$

Example. 4 : Expansion of $\log_e (1 + x)$

Let $X = (-1, 1]$

Let $X_1 = \begin{cases} [0, x], x > 0, x \in X \\ [x, 0], x < 0, x \in X \end{cases}$

Let $f : X \to R$ be defined by

$$f(x) = \log_e (1 + x) \; \forall \; x \in X$$

Case (i) Let $x \in X - \{0\}$

Then the function

$g : X_1 \to R$ defined by

$g(x) = \log_e (1 + x)$ has derivatives of all orders and

$$g^{(n)}(x) = \frac{(-1)^{n-1}(n-1)!}{(1+x)^n}$$

Further $g^{(n)}$ is continuous in X_1

$$\therefore g(x) = \log_e (1 + x)$$

$$= g(0) + \frac{x}{1!}g'(0) + \frac{x^2}{2!}g''(0) + \ldots$$

$$+ \frac{x^{n-1}}{(n-1)!}g^{(n-1)}(0) + R_n$$

(i) If $X_1 = [0, x], 0 < x \leq 1$

then Lagrange's form of the remainder is given by

$$R_n = \frac{x^n g^n(\theta x)}{n!}, \; 0 < \theta < 1$$

$$= \frac{x^n (-1)^{n-1} (n-1)!}{n! (1+\theta x)^n}$$

$$= \frac{(-1)^{n-1}}{n} \left(\frac{x}{1+\theta x}\right)^n$$

$\therefore$ for $0 < x \leq 1$, $0 < \frac{x}{1+\theta x} < 1$.

$$\therefore |R_n| < \frac{1}{n}$$

$$\therefore \lim_{n \to \infty} R_n = 0$$

$\therefore$ for $0 < x \leq 1$

$$\log_e (1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots$$

($\because g(0) = 0, g'(0) = 1; g''(0) = -1; g'''(0) = 1$ and so on)

(ii) If $X_1 = [x, 0], -1 < x < 0$ then

Cauchy's form of the remainder R_n is given by

$$R_n = \frac{x^n (1-\theta)^{n-1} g^n (\theta x)}{(n-1)!} (0 < \theta < 1)$$

$$= \frac{x^n (1-\theta)^{n-1} (-1)^{n-1} (n-1)!}{(n-1)! (1+\theta x)^n}$$

$$= (-1)^{n-1} \frac{x^n}{1-\theta} \left(\frac{1-\theta}{1+\theta x}\right)^n$$

$$= (-1)^{n-1} \frac{x^n}{1+\theta x} \left(\frac{1-\theta}{1+\theta x}\right)^{n-1}$$

$-1 < x < 0 \Rightarrow 1 + \theta x > 1 - \theta > 0$

$$\therefore 0 < \frac{1-\theta}{1+\theta x} < 1$$

$$\therefore |R_n| < \frac{|x^n|}{1+\theta x}$$

$$\Rightarrow |R_n| < \frac{|x^n|}{1+x} \qquad (\because 1 + \theta x > 1 + x)$$

$$\therefore \lim_{n \to \infty} (R_n) = 0.$$

$\therefore$ for $-1 < x < 0$

$$\log_e (1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots$$

Case (ii) If $x = 0$ then $S_n = 0$

$$\therefore \lim_{n \to \infty} (S_n) = 0$$

Further at $x = 0$, $\log_e (1+x) = 0$.

$\therefore$ If $x = 0$, we have

$$\log_e (1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots$$

Hence $\log_e (1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots \forall x \in (-1, 1]$

Example. 5 : Expansion of $(1 + x)^a$

Case (i) If $X = \begin{cases} [0, x], 0 < x < 1 \\ [x, 0], -1 < x < 0 \end{cases}$

Since $|x| < 1, x \neq 0, 0 < \theta < 1$

therefore $0 < 1 - \theta < 1 + \theta x$

$\therefore 0 < \left(\frac{1 + \theta}{1 + \theta x}\right) < 1$ ... (ii)

$0 < \theta < 1, |x| < 1, x \neq 0$

$\Rightarrow |\theta x| < 1$

$\Rightarrow -1 < \theta x < 1$

$\Rightarrow 0 < 1 + \theta x < 2$

$\Rightarrow 0 < (1 + \theta x)^{a-1} < 2^{a-1}$ for $a > 1$ ... (iii)

$0 < \theta < 1, |x| < 1, x \neq 0$

$\Rightarrow 1 + \theta x > 1 - |x| > 0$

$\Rightarrow 0 < (1 + \theta x)^{a-1} < (1 - |x|)^{a-1}$ for $a < 1$ ... (iv)

$(1 + \theta x)^{a-1} = 1$ for $a = 1$ ... (v)

If $\max \left\{2^{a-1}, (1 - |x|)^{a-1}, 1\right\} = k$

then $0 < (1 + \theta x)^{a-1} < k$ ... (vi)

(from (iii), (iv) and (v))

From results (ii) and (iii), $|R_n| < k\ A_n$

From results (i) $\lim_{n \to \infty} (A_n) = 0$

$\therefore \lim_{n \to \infty} (R_n) = 0$

$\therefore$ for $|x| < 1, x \neq 0$

$$(1 + x)^a = 1 + \sum_{n=1}^{\infty} \frac{a\ (a - 1)\ (a - 2) \ldots \left(a - \overline{n - 1}\right)}{n!} x^n$$

Case (ii) Let $x = 0$

then $S_n = 0$

$$\therefore \lim_{n\to\infty} (S_n) = 0$$

Further $(1+x)^a = 1$ at $x = 0$

Hence $$(1+x)^a = 1 + \sum_{n=1}^{\infty} \frac{a\,(a-1)\,(a-2)\ldots(a-n+1)}{n!}\,x^n$$

for $a \in R$ ans $-1 < x < 1$.

22.5 INDETERMINATE FORMS

If $\lim_{x\to a} f(x) = \lim_{x\to a} g(x) = 0$ then

$\lim_{x\to a} \frac{f(x)}{g(x)}$ is said to assume the indeterminate form $\frac{0}{0}$.

If $\lim_{x\to a} |f(x)| = \infty$ and $\lim_{x\to a} |g(x)| = \infty$

then $\lim_{x\to a} \left|\frac{f(x)}{g(x)}\right|$ is said to assume the indeterminate form $\frac{\infty}{\infty}$.

There are several kinds of indeterminate forms like $0 \cdot \infty$, $(\infty - \infty)$, 1^∞, ∞^0, 0^0. The indeterminate form $\frac{0}{0}$ and $\frac{\infty}{\infty}$ are regarded as fundamental forms and all other forms are deal with by converting them into either of these two forms. French Mathematician L' Hospital (1661-1704) gave a method to evaluate the limits of the functions which assume the indeterminate forms.

Theorem. 3 :

> If f, g are derivable at 'a',
>
> $f(a) = g(a) = 0$ and $g'(a) \neq 0$
>
> then $\lim_{x\to a} \frac{f(x)}{g(x)} = \frac{f'(a)}{g'(a)}$

Proof : $g'(a) \neq 0$

$\therefore$ there exists $h > 0$ such that

$$0 < |x-a| < h \Rightarrow \frac{g(x)-g(a)}{x-a} \neq 0$$

$$\Rightarrow g(x) \neq 0 \qquad (\because g(a) = 0)$$

$$\therefore 0 < |x-a| < h \Rightarrow \frac{f(x)}{g(x)} = \frac{f(x)-f(a)}{g(x)-g(a)}$$

$$= \frac{\frac{f(x)-f(a)}{x-a}}{\frac{g(x)-g(a)}{x-a}}$$

$$\lim_{x\to a}\frac{f(x)}{g(x)} = \frac{\lim\limits_{x\to a}\dfrac{f(x)-f(a)}{x-a}}{\lim\limits_{x\to a}\dfrac{g(x)-g(a)}{x-a}}$$

$$= \frac{f'(a)}{g'(a)}$$

Theorem. 4 : (L'Hospital's rule)

If f, g are derivable in a deleted neighbourhood of 'a',

$$\lim_{x\to a} f(a) = \lim_{x\to a} g(a) = 0 \text{ and } \lim_{x\to a}\frac{f'(x)}{g'(x)} = l$$

then $\lim\limits_{x\to a}\dfrac{f(x)}{g(x)} = l$

Proof : If we define $f(a) = g(a) = 0$ then f and g are continuous at 'a'.

Since $\lim\limits_{x\to a}\dfrac{f'(x)}{g'(x)} = l$, for any given $\epsilon > 0$

there exists a $\delta > 0$ such that

$0 < |x - a| < \delta \Rightarrow \left|\dfrac{f'(x)}{g'(x)} - l\right| < \epsilon$

(i) Let $a < x < a + \delta$ then it is clear that f, g are continuous in $[a, x]$ and derivable in (a, x)

Also $g'(t) \neq 0$ for any $t \in (a, x)$

(∵ by data it follows that $\dfrac{f'}{g'}$ is defined in $(a, (a + \delta))$

∴ By Cauchy's mean value theorem there exists a point $y \in (a, x)$ such that

$$\frac{f'(y)}{g'(y)} = \frac{f(x) - f(a)}{g(x) - g(a)} = \frac{f(x)}{g(x)}$$

Now $a < y < x < a + \delta$ $\quad\therefore \left|\dfrac{f'(y)}{g'(y)} - l\right| < \epsilon$

$$\therefore a < x < a + \delta \Rightarrow \left|\frac{f(x)}{g(x)} - l\right| < \epsilon$$

$$\therefore \lim_{x\to a+0}\frac{f(x)}{g(x)} = l \qquad \ldots (1)$$

(ii) $a - \delta < x < a$

Then as before f, g are continuous in $[x, a]$ and derivable in (x, a) and

$$g'(t) \neq 0 \text{ for any } t \in (x, a)$$

$\therefore$ By Cauchy's mean value theorem there exists a point $y \in (x, a)$ such that

$$\frac{f'(y)}{g'(y)} = \frac{f(x) - f(a)}{g(x) - g(a)} = \frac{f(x)}{g(x)}$$

Now $a - \delta < x < a$

$$\therefore \left|\frac{f'(y)}{g'(y)} - l\right| < \epsilon$$

$$\therefore a - \delta < x < a \Rightarrow \left|\frac{f(x)}{g(x)} - l\right| < \epsilon$$

$$\therefore \lim_{x \to a-0} \frac{f(x)}{g(x)} = l \qquad \ldots (2)$$

$$(1) \text{ and } (2) \Rightarrow \lim_{x \to a} \frac{f(x)}{g(x)} = l.$$

Theorem. 5 : (Generalisation of L' Hospital's Rule)

If f, g are functions such that

(i) $f^{(n)}, g^{(n)}$ exists in a deleted neighbourhood of 'a'

(ii) $\lim_{x \to a} f^{(r)}(x) = 0 = \lim_{x \to a} g^{(r)}(x)$ for $r = 0, 1, 2, \ldots (n-1)$

and (iii) $\lim_{x \to a} \frac{f^{(n)}(x)}{g^{(n)}(x)} = l$

then $\lim_{x \to a} \frac{f(x)}{g(x)} = l$

Proof : If $n = 1$ the theorem is equivalent to L' Hospital's rule which we have proved already. Next assuming the theorem to be true for $n = k$ we shall prove that the theorem is true for $n = k + 1$.

Let us assume that $f^{(k+1)}, g^{(k+1)}$ exist in the deleted neighbourhood of 'a' and

$$\lim_{x \to a} f^{(r)}(x) = \lim_{x \to a} g^{(r)}(x) = 0 \text{ for } r = 0, 1, 2, \ldots k$$

$$\text{and } \lim_{x \to a} \frac{f^{(k+1)}(x)}{g^{(k+1)}(x)} = l$$

From L' Hospital's rule we will get that

$\lim_{x \to a} \frac{f^{(k)}(x)}{g^{(k)}(x)}$ exists and equal to l.

Now by the induction hypothesis it follows that

$$\lim_{x \to a} \frac{f(x)}{g(x)} = l.$$

$\therefore$ By mathematical induction the theorem it true for all positive integral values of n.

Theorem. 6 :

If f, g are functions such that

(i) $f^{(n)}, g^{(n)}$ exists in a deleted neighbourhood of 'a'

$f(x) \to \pm\infty$ as $x \to a+$; $g(x) \to \pm\infty$ as $x \to a+$ and

$$\lim_{x \to a+} \frac{f'(x)}{g'(x)} = l,$$

then $$\lim_{x \to a+} \frac{f(x)}{g(x)} = l$$

Proof : Since $\lim_{x \to a+} \frac{f'(x)}{g'(x)} = l$, for any given

$\epsilon > 0$ there exists $\delta > 0$ such that

$$a < y < a + \delta \Rightarrow \left| \frac{f'(y)}{g'(y)} - l \right| < \epsilon/3$$

Let $a + \frac{\delta}{2} = x_0$

If $a < x < x_0$ then f, g are continuous in $[x, x_0]$ and derivable in (x, x_0)

and $g'(t) \neq 0$ for any $t \in (x, x_0)$

$\therefore$ By Cauchy's mean value theorem

$$\frac{f(x_0) - f(x)}{g(x_0) - g(x)} = \frac{f'(y)}{g'(y)} \text{ for } y \in (x, x_0)$$

$$\frac{f'(y)}{g'(y)} = \frac{f(x) - f(x_0)}{g(x) - g(x_0)} = \frac{f(x)}{g(x)} \cdot \left(\frac{1 - \frac{f(x_0)}{f(x)}}{1 - \frac{g(x_0)}{g(x)}} \right)$$

$$\therefore \frac{f(x)}{g(x)} = \frac{f'(y)}{g'(y)} \left(\frac{1 - \frac{g(x_0)}{g(x)}}{1 - \frac{f(x_0)}{f(x)}} \right)$$

$$\therefore \frac{f(x)}{g(x)} - l = \left(\frac{f'(y)}{g'(y)} - l \right) \left(\frac{1 - \frac{g(x_0)}{g(x)}}{1 - \frac{f(x_0)}{f(x)}} \right)$$

$$+ l \left(\frac{1 - \frac{g(x_0)}{g(x)}}{1 - \frac{f(x_0)}{f(x)}} - 1 \right) \qquad \ldots (1)$$

Now from hypothesis we get

$$\lim_{x \to a+} \frac{g\left(x_0\right)}{g\,(x)} = 0,$$

$$\lim_{x \to a+} \frac{f\left(x_0\right)}{f\,(x)} = 0.$$

$$\therefore \lim_{x \to a+} \left(\frac{1 - \dfrac{g\left(x_0\right)}{g\,(x)}}{1 - \dfrac{f\left(x_0\right)}{f\,(x)}} \right) = 1$$

$\therefore$ there exists a $\delta > 0$ such that

$$a < x < a + \delta \Rightarrow \left| \frac{1 - \dfrac{g\left(x_0\right)}{g\,(x)}}{1 - \dfrac{f\left(x_0\right)}{f\,(x)}} - 1 \right| < \frac{\epsilon}{3\epsilon + 3\,|l|}$$

Now from (1) we get

$$a < x < a + \delta \Rightarrow \left| \frac{f\,(x)}{g\,(x)} - l \right| < \frac{\epsilon}{3} \left(1 + \frac{\epsilon}{3\epsilon + 3\,|l|} \right) + |l| \cdot \frac{\epsilon}{3\epsilon + 3\,|l|}$$

$$< \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon$$

$$\therefore \frac{f\,(x)}{g\,(x)} \to l \text{ as } x \to a+.$$

Note : Similarly theorems corresponding to left limits and the limits at $+\infty, -\infty$ can be stated and proved.

Example. 1 : If a, b, c, d are positive numbers, $c \neq d$ then show that

$$\lim_{x \to 0} \left(\frac{a^{-x} - b^{-x}}{c^{-x} - d^{-x}} \right) = \frac{\log b - \log a}{\log d - \log c}.$$

Sol. : Both numerator and denominator of L.H.S are derivable and their values are zero at $x = 0$. Therefore it assumes indeterminate from $\frac{0}{0}$.

Now $\quad \dfrac{d}{dx}\left(a^{-x} - b^{-x}\right) = -a^{-x} \log a + b^{-x} \log b$

and its value at $\quad x = 0$ is $(\log b - \log a)$.

$$\frac{d}{dx}\left(c^{-x} - d^{-x}\right) = -c^{-x} \log c + d^{-x} \log d$$

and its value at $\quad x = 0$ is $\log d - \log c$.

Since $c \neq d$, the derivative of the denominator is not zero at $x = 0$

$\therefore$ By theorem 3

$$\lim_{x \to 0} \left(\frac{a^{-x} - b^{-x}}{c^{-x} - d^{-x}} \right) = \frac{\log b - \log a}{\log d - \log c}.$$

Example. 2 : Show that

$$\lim_{x \to +\infty} x \left(\sqrt{x^2 + a^2} - x \right) = \frac{1}{2} a^2$$

Sol. : If we write $x = \frac{1}{y}$

then the above form is equivalent to

$$\lim_{y \to 0+} \frac{\sqrt{1 + a^2 y^2} - 1}{y^2}.$$

Limits of numerator and denominator are zero at $x = 0$

$\therefore$ This assumes the indeterminate form $\frac{0}{0}$.

$$\frac{d}{dy} \left(\sqrt{1 + a^2 y^2} - 1 \right) = \frac{a^2 y}{\sqrt{1 + a^2 y^2}}$$

$$\frac{d}{dy} \left(y^2 \right) = 2y$$

$$\therefore \frac{\frac{d}{dy} \sqrt{1 + a^2 y^2} - 1}{\frac{d}{dy} \left(y^2 \right)} = \frac{a^2 y}{2y \sqrt{1 + a^2 y^2}}$$

$$= \frac{a^2}{2 \sqrt{1 + a^2 y^2}} \quad (y \neq 0)$$

$\therefore$ By L'Hospital's Rule

$$\lim_{y \to 0+} \frac{\sqrt{1 + a^2 y^2} - 1}{y^2} = \lim_{y \to 0+} \frac{a^2}{2 \sqrt{1 + a^2 y^2}} = \frac{a^2}{2}.$$

Example. 3 : Show that

$$\lim_{x \to \pi/2} \left(\frac{1 + \cos x}{1 - \cos x} \right)^{\frac{1}{\cos x}} = e^2$$

Sol. : Denote the given function by f and $\log f$ by g

Then $$g(x) = \frac{\log (1 + \cos x) - \log (1 - \cos x)}{\cos x}$$

If the numerator and denominator of $g(x)$ are denoted by $p(x)$ and $q(x)$ respectively then

$$p \left(\frac{\pi}{2} \right) = q \left(\frac{\pi}{2} \right) = 0$$

$\therefore$ This assumes the indeterminate form $\frac{0}{0}$.

$$\text{Now } p'(x) = \frac{-\sin x}{1 + \cos x} - \frac{\sin x}{1 - \cos x} = \frac{-2 \sin x}{1 - \cos^2 x}$$

$$= -2 \operatorname{cosec} x$$

$$q'(x) = -\sin x$$

$$\therefore \lim_{x\to\pi/2} \frac{p'(x)}{q'(x)} = \lim_{x\to\pi/2} \frac{2}{\sin^2 x} = 2.$$

$$\therefore \lim_{x\to\pi/2} g(x) = 2$$

$$\therefore \lim_{x\to\pi/2} f(x) = e^2$$

22.6 WORKED OUT EXERCISES

Exercise. (i) : Evaluate $\lim_{x\to 0}\left(\frac{1}{x^2} - \frac{1}{\sin^2 x}\right)$.

Ans : The given indeterminate is of the form $(\infty - \infty)$ which could be brought to the form $\frac{0}{0}$ by considering

$$\lim_{x\to 0} \frac{\sin^2 x - x^2}{x^2 \sin^2 x}$$

Applying L' Hospitals' rules this is equal to

$$= \lim_{x\to 0} \frac{2 \sin x \cos x - 2x}{2x \sin^2 x + 2x^2 \sin x \cos x} \text{ which is in } \frac{0}{0} \text{ form}$$

$$= \lim_{x\to 0} \frac{2\left(\cos^2 x - \sin^2 x - 1\right)}{4x \sin x \cos x + 2 \sin^2 x + 2x^2\left(\cos^2 x - \sin^2 x\right) + 4x \sin x \cos x}$$

$$= \lim_{x\to 0} \frac{\cos 2x - 1}{\sin^2 x + 2x \sin 2x + x^2 \cos 2x} \left(\frac{0}{0} \text{form}\right)$$

$$= \lim_{x\to 0} \frac{-2 \sin 2x}{3 \sin 2x + 6x \cos 2x - 2x^2 \sin 2x} \left(\frac{0}{0} \text{form}\right)$$

$$= \lim_{x\to 0} \frac{-\cos 2x}{3 \cos 2x - 4x \sin 4x - x^2 \cos 2x}$$

$$= -\frac{1}{3}.$$

Exercise. 2 : Evaluate $\lim_{x\to 0}\left(\frac{\tan x}{x}\right)^{1/x^2}$.

Ans : This is of the form 1^∞

$$\text{Let } k = \lim_{x\to 0}\left(\frac{\tan x}{x}\right)^{1/x^2}$$

$$\log k = \lim_{x\to 0} \frac{1}{x^2} \log\left(\frac{\tan x}{x}\right)$$

Since $\lim_{x\to 0} \frac{\tan x}{x} = \lim_{x\to 0} \frac{\sin x}{x} \cdot \frac{1}{\cos x} = 1,$

the given indeterminate is reduced to $\frac{0}{0}$ form. By repeated application of L' Hospital's rule the R.H.S. is reduced to

$$= \lim_{x\to 0} \frac{x \sec^2 x - \tan x}{\frac{x \tan x}{2x}}$$

$$= \lim_{x\to 0} \frac{x \sec^2 x - \tan x}{2x^2 \tan x} \quad , \left(\frac{0}{0} \text{form}\right)$$

$$= \lim_{x\to 0} \frac{2x \sec^2 x \tan x + \sec^2 x - \sec^2 x}{4x \tan x + 2x^2 \sec^2 x}$$

$$= \lim_{x\to 0} \frac{\sec^2 x \tan x}{2 \tan x + x \sec^2 x}$$

$$= \lim_{x\to 0} \frac{\tan x}{\sin 2x + x} = \lim_{x\to 0} \frac{\sec^2 x}{2 \cos 2x + 1} = \frac{1}{3}.$$

Since $\log k = \frac{1}{3}, k = e^{1/3}$.

Exercise. 3 : Assuming that $x > -1$, and using Taylor's theorem find the value of $\sqrt[3]{1.3}$ up to 2 decimal places and estimate the error.

Ans : Let $f(x) = (1 + x)^{1/3}$; Then $f'(x) = \frac{1}{3}(1 + x)^{-2/3}$ and $f''(x) = \left(\frac{1}{3}\right)\left(-\frac{2}{3}\right)(1 + x)^{-5/3}$. Thus

Thus $f'(0) = \frac{1}{3}$ and

$f''(0) = -\frac{2}{9}$.

Thus $f(x) = 1 + \frac{1}{3}x - \frac{1}{9}x^2 + R(x)$ where $R(x)$ is remainder after 3 terms.

$R(x) = \frac{f'''(c)}{3!}x^3 = \frac{5}{81}(1 + c)^{-8/3}x^3$ for some 'c' between 0 and x.

Let $x = 0.3$.

$$\text{Then } f(1.3) = 1 + \frac{1}{3}(0.3) - \frac{1}{9}(0.09) + R$$

$$= 1.09 + R$$

$$\text{The error is } R = \frac{5}{81}(1 + c)^{-8/3} \cdot (0.3)^3.$$

$$\leq \frac{5}{81}(0.027) = \frac{5 \times 27}{81000} = \frac{1}{600}.$$

$$\text{Thus } \left|\sqrt[3]{1.3} - 1.09\right| < \frac{1}{600}$$

22.7 SUMMARY

Taylor's theorem could be viewed as a generalisation of Mean Value theorem where the value of a function could be approximated by Values of its derivatives. This could also be used to approximate a function through a polynomial or a power series. We have expanded some standard functions using Maclaurin's theorem. Certain types of evaluation of limits to indeterminate forms have been computed by L' Hospital rule.

22.8 MODEL EXAMINATION QUESTIONS

Section A (Long Answer)

i) State and prove Taylor's theorem and derive Malcaurins expansion of a function.

ii) State Taylor's theorem and write a detailed note on remainder after n terms. State and prove the conditions under which a function could be expanded in Taylor's series.

Section B (Short Answer)

i) Expand $\log(1 + x)$ by Maclaurins series and the range in which this expansion is valid.

ii) Expand $(1 + x)^n$ and state the conditions under which this expansion is valid.

iii) Evaluate $\lim_{x \to \pi/2} (\sin x)^{\tan x}$.

iv) Evaluate $\lim_{x \to 0} \frac{(a + x)^x - a^x}{x^2}$.

v) Evaluate $\lim_{x \to 0} \left(\frac{1}{x^2} - \frac{1}{\sin^2 x} \right)$

UNIT–23 : RIEMANN INTEGRABILITY

Contents

23.1 Aims and Objectives

23.2 Introduction

23.3 The Riemann integral

23.4 Algebra of integrable functions

23.5 Summary

23.6 Model Examination Questions

23.7 Answers to Self Assessment Questions

23.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to (i) define Riemann integrability of a function (ii) state and prove Darboux's theorems (iii) prove that continuous functions and monotonic functions are Riemann integrable (iv) The sum, product and quotient (if properly defined) of Riemann integrable functions is Riemann integrable.

23.2 INTRODUCTION

Newton (1642 - 1727) used his theory of fluxions to initiate the process of finding tangents to find areas of curves. Independently Leibnitz (1646 - 1716) used a different process by methods "calculus differentialis" and "calculus integralis" to arrive at similar conclusions of Newton. Thus both Newton and Leibnitz could be credited with the discovery of integral calculus either as limit of a summation process or as an inverse process of differentiation. Bernare Riemann (1826 - 1866) used altogether a different approach by considering certain functions defined on an interval. These functions have been identified as Riemann integrable functions. Stieltjes (1856 - 1894) generalised the concept of Rieman integral by defining the integral of a bounded real valued function with respect to another bounded real valued function. These Riemann - Stieltjes integrals have wide applications in statistics and have paved way for a still more generalised Lebesgue (1875 - 1941) theory of integration.

23.3 THE RIEMANN INTEGRAL

Defintion 1 :

Let I = $[a, b]$ be any closed bounded interval in **R**. Then a partition of I is a finite ordered set of points in I given by

$$P = (x_0, x_1, \ldots, x_n) \text{ such that}$$

$$a = x_0 < x_1 < x_2 < \ldots < x_n = b.$$

The points of P divide $[a, b]$ into non-over lapping sub intervals $[x_0, x_1]$, $[x_1, x_2]$, ... $[x_{n-1}, x_n]$. If $P = (x_0, x_1, \ldots, x_n)$ and $Q = (y_0, y_1, \ldots, y_n)$ are two partitions of I, then Q is

called a refinement of P if each partition point $x_k \in P$ belongs to Q. That is $P \subseteq Q$. A refinement Q of a partition P can be obtained by adjoining a finite number of points to P.

Definition 2 :

Let $P = \{ a = x_0, x_1, x_2, \ldots x_n = b \}$ be a partition of $[a, b]$. Then the maximum of the lengths of the subintervals $[a, x_1], [x_1, x_2], \ldots [x_{n-1}, b]$ is called the norm of the partition. The norm of the partition is denoted by $\|P\|$ or by Δ (P). If P^* is a refinement of P, then $\|P^*\| \leq \|P\|$.

Definition 3 :

Let $f : [a, b] \to \mathbf{R}$ be a bounded function. Let $P = \{ a = x_0, x_1, x_2, \ldots x_n = b \}$ be a partition of $[a, b]$.

For $k = 1, 2, \ldots n$, let m_k denotate the infimum (g.l.b) of f in the k^{th} sub interval and M_k denote the supremum (l.u.b) of f in the k^{th} subinterval.

That is $m_k = \inf \{ f(x) : x \in [x_{k-1}, x_k] \}$

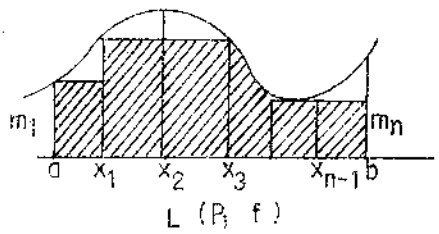
$M_k = \sup \{ f(x) : x \in [x_{k-1}, x_k] \}$.

Then the lower Riemann sum L (P; f) and the upper Riemann sum U (P; f) are defined by

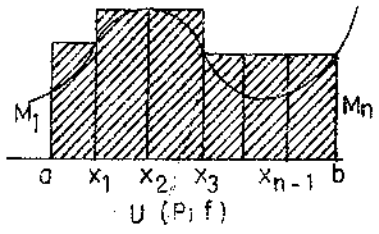
$$L(P; f) = \sum_{k=1}^{n} m_k (x_k - x_{k-1}) = \sum_{k=1}^{n} m_k \delta_k$$

$$U(P; f) = \sum_{k=1}^{n} M_k (x_k - x_{k-1}) = \sum_{k=1}^{n} M_k \delta_k$$

If f is a positive function, then the lower Riemann sum L (P; f) can be interpreted as the area of the union of rectangles with base $[x_{k-1}, x_k]$ and heights m_k. Similarly the upper Riemann sum U (P; f) can be interpreted as the area of the union of rectangles with base $[x_{k-1}, x_k]$ and heights M_k. Viewed geometrically :



L (P; f)



U (P; f)

SAQ 1 Show that L (P; f) $\leq$ U (P, f)

Theorem 1 :

Let f be a real valued bounded function defined on $[a, b]$. Let P^* be a refinement of the partition P of $[a, b]$. Then

(i) $L(P, f) \leq L(P^*, f)$

(ii) $U(P^*, f) \leq U(P, f)$

(iii) $L(P, f) \leq L(P^*, f) \leq U(P^*, f) \leq U(P, f)$.

Proof : Let $P = \{a = x_0, x_1, x_2, \ldots x_n = b\}$ be any partition of $[a, b]$. Let $y \in [a, b]$ be such that $x_{i-1} < y < x_i$. Then $P^* = P \cup \{y\}$ is a refinement of P. Let m_i and M_i be the infimum (g.l.b) and supremum (l.u.b) of f in $[x_{i-1}, x_i]$, $i = 1, 2, \ldots n$. Let m_i' and m_i'' be the infima of f in $[x_{i-1}, y]$ and $[y, x_i]$ respectively. Let M_i', M_i'' be the suprema of f in $[x_{i-1}, y]$ and $[y, x_i]$ respectively. Then $m_i \leq m_i'$; $m_i \leq m_i''$ and $M_i \geq M_i'$, $M_i \geq M_i''$. Now

$$U(P; f) - U(P^*, f) = \sum_{k=1}^{i-1} M_k \delta_k + M_i \delta_i + \sum_{k=i+1}^{n} M_i \delta_i$$

$$- \left\{ \sum_{k=1}^{i-1} M_k \delta_k + M_i' (y - x_{i-1}) + M_i'' (x_{i-1} - y) + \sum_{k=i+1}^{n} M_i \delta_i \right\}$$

$$= M_i \delta_i - M_i' (y - x_{i-1}) - M_i'' (x_i - y)$$

$$= M_i (x_i - x_{i-1}) - M_i' (y - x_{i-1}) - M_i'' (x_i - y)$$

$$= M_i (x_i - y + y - x_{i-1}) - M_i' (y - x_{i-1}) - M_i'' (x_i - y)$$

$$= (M_i - M_i') (y - x_{i-1}) + (M_i - M_i'') (x_i - y)$$

But $0 \leq M_i - M_i' \leq |M_i| + |M_i'| \leq 2k$, (if $|f| < k$ on $[a, b]$

and $x_i - x_{i-1} = (y - x_{i-1}) + (x_i - y) \leq \|P\|$

Thus $0 \leq U(P; f) - U(P^*, f) \leq 2k \|P\|$

Similarly, we can show that

$$0 \leq L(P^*, f) - L(P; f) \leq 2k \|P\|.$$

If P^* has p number of points more than the number of points in P, then we can take these points to be $y_1, y_2, \ldots y_p$ and let $P = P_0$; $P_1 = P_0 \cup \{y_1\}$; $P_2 = P_1 \cup \{y_2\}$ ...

$P^* = P_p = P_{p-1} \cup \{y_p\}$. Then

$P \subset P_1 \subset P_2 \ldots P_{p-1} \subset P^*$

Then $0 \leq U(P_{i-1}; f) - U(P_i; f) \leq 2k \|P_{i-1}\| \leq 2k \|P\|$

and $0 \leq L(P_i; f) - L(P_{i-1}; f) \leq 2k \|P_{i-1}\| \leq 2k \|P\|$

By taking $i = 1, 2, \ldots p$ we get

$$0 \le U(P_0; f) - U(P_1, f) \le 2k \|P\|$$

$$0 \le U(P_1, f) - U(P_2, f) \le 2k \|P\|$$

.....

.....

$$0 \le U(P_{p-1}; f) - U(P_p; f) \le 2k \|P\|$$

Adding $0 \le U(P_0; f) - U(P_p; f) \le 2kp \|P\|$

Similar argument gives : $0 \le L(P_p; f) - L(P_0; f) \le 2kp \|P\|$

Hence $L(P, f) \le L(P^*, f) \le U(P^*, f) \le U(P; f)$

Remark 1 : If $P_1, P_2 \in \mathbf{P}[a, b]$, then $L(P_1; f) \le U(P_2; f)$ where P is the set of all partitions of $[a, b]$. To see this let $P^* = P_1 \cup P_2$. Then P^* is common refinement of P_1 and P_2.

$$\text{Then } L(P_1; f) \le L(P^*; f)$$

$$\le U(P^*; f)$$

$$< U(P_2; f)$$

Remark 2 : We observe that a refinement of a partition increases lower sums and decreases upper sums.

Definition 4 :

Let the collection of all partitions of the interval $I = [a, b]$ be denoted by $\mathbf{P}(I)$. Let $f : I \to \mathbf{R}$ be a bounded function. Then the lower integral or the lower Riemann integral on $[a, b]$ is defined by

$$\underline{\int_a^b} f(x)\,dx = \text{Sup}\{L(P; f) \mid P \in \mathbf{P}(I)\}$$

The upper integral or the upper Riemann integral is defined by

$$\overline{\int_a^b} f(x)\,dx = \inf\{U(P; f) \mid P \in \mathbf{P}(I)\}$$

Remark 3 : Since f is a bounded function there exist real numbers m and M such that $m = \inf\{f(x) \mid x \in I\}$ and $M = \sup\{f(x) \mid x \in I\}$. For any $P \in \mathbf{P}(I)$, we have that $m(b - a) \le L(P; f) \le U(P, f) \le M(b - a)$. Consequently the lower and upper integrals exist and

$$m(b-a) \le \underline{\int_a^b} f(x)\,dx \le M(b-a)\,;\; m(b-a) \le \overline{\int_a^b} f(x)\,dx \le M(b-a).$$

Definition 5 :

Let I = $[a, b]$ and $f : I \to R$ be a bounded function Then f is said to be Riemann integrable on I if the lower Riemann integral is equal to the upper Riemann integral. That if f is Riemann integrable if $\underline{\int_a^b} f(x)\,dx = \overline{\int_a^b} f(x)\,dx$.

Theorem 2 :

$$\underline{\int_a^b} f(x)\,dx \leq \overline{\int_a^b} f(x)\,dx$$

Proof : Let $P_1, P_2 \in \mathbf{P}[a, b]$. Then by Remark 1, $L(P_1, f) \leq U(P_2, f)$ is an upper bound for the set of lower sums $\{L(P_1, f)\}$. But the supremum (or l.u.b) of lower Riemann sums is $\underline{\int_a^b} f(x)\,dx$. Since supremum $\leq$ any upper bound we have

$$\underline{\int_a^b} f(x)\,dx \leq U(P_2, f).$$

Thus means that $\underline{\int_a^b} f(x)\,dx$ is a lower bound of the set of all upper Riemann sums. But the greatest lower bound of $\{U(P_2, f)\}$ is $\overline{\int_a^b} f(x)\,dx$. Since lower bound is $\leq$ the greatest lower bound we have

$$\underline{\int_a^b} f(x)\,dx \leq \overline{\int_a^b} f(x)\,dx.$$

Theorem 3 : (Darboux Theorem) :

If f is a bounded function on $[a, b]$, then for any $\epsilon > 0$, there exists $\delta > 0$ such that

$$U(P, f) < \overline{\int_a^b} f(x)\,dx + \epsilon,$$

$$L(P, f) > \underline{\int_a^b} f(x)\,dx - \epsilon,$$

for any $P \in \mathbf{P}[a, b]$ with $\|P\| < \delta$.

Proof : By defintion of upper and lower integrals

$$\underline{\int_a^b} f(x)\,dx = \text{Sup}\,\{L(Q, f) \mid Q \in \mathbf{P}[a, b]\}$$

$$\text{and } \overline{\int_a^b} f(x)\,dx = \inf\{U(Q, f) \mid Q \in \mathbf{P}[a, b]\}$$

Since the upper integral is the infimum of $\{U(Q, f)\}$, there exists a partition P_1 of $[a, b]$ such that

$$U(P_1, f) < \overline{\int_a^b} f(x)\,dx + \frac{\epsilon}{2}.$$

If the number of points of subdivision in P_1 is m, then we can choose δ_1 such that

$0 < \delta_1 < \frac{\epsilon}{4km}$ where $|f(x)| < k$ for $x \in [a, b]$. Let P be any partition of $[a, b]$ withe $\|P\| < \delta_1$.

If $P_2 = P_1 \cup P$, then $P_1 \subset P_2$ and $P \subset P_2$. Therefore $U(P_2, f) \le U(P_1, f) < \int_a^b f(x)\,dx + \frac{\epsilon}{2}$. If the number of points in P_2 which are not in P is l then $0 \le l \le m - 2 < m$. Then

$$U(P, f) - U(P_2, f) \le 2kl\,\|P\| \le 2kl\,\delta_1.$$

$$\text{Therefore } U(P, f) \le U(P_2, f) + 2kl\,\delta_1 < \int_a^b f(x)\,dx + \frac{\epsilon}{2} + 2m\,\delta_1.$$

$$< \overline{\int_a^b} f(x)\,dx + \frac{\epsilon}{2} + \frac{\epsilon}{2}, \quad \left(\because \delta_1 < \frac{\epsilon}{4km}\right)$$

$$\text{Thus } U(P, f) < \overline{\int_a^b} f(x)\,dx + \epsilon.$$

Similarly it can be proved that for $\epsilon > 0$, there exists $\delta > 0$ such that

$$L(P, f) > \underline{\int_a^b} f(x)\,dx - \epsilon$$

for all partitions P of $[a, b]$ with $\|P\| < \delta_2$.

$$\text{Let } \delta = \min\{\delta_1, \delta_2\}.$$

Then for $\epsilon > 0$, there exists $\delta > 0$ such that

$$U(P, f) < \overline{\int_a^b} f(x)\,dx + \epsilon$$

$$L(P, f) > \underline{\int_a^b} f(x)\,dx - \epsilon$$

for all partitions $\|P\| < \delta$.

Remark 1 : As $\|P\| \to 0$, $\lim_{\|P\| \to 0} U(P; f) = \overline{\int_a^b} f(x)\,dx$ and $\lim_{\|P\| \to 0} L(P; f) = \underline{\int_a^b} f(x)\,dx$

Theorem 4 :

A bounded function $f : [a, b] \to \mathbb{R}$ is Riemann integrable if and only if for any $\epsilon > 0$, there exists a partition P of $[a, b]$ such that

$$U(P; f) - L(P; f) < \epsilon$$

Proof : Let f be Riemann integrable on $[a, b]$. Then

$$\underline{\int_a^b} f(x)\,dx = \overline{\int_a^b} f(x)\,dx = \int_a^b f(x)\,dx \qquad \ldots (i)$$

Let $\epsilon > 0$ be any given number. Then by Darboux Theorem there exists $\delta > 0$ such that

$$U(P; f) < \overline{\int_a^b} f(x)dx + \frac{\epsilon}{2}$$

$$\text{and } L(P; f) > \underline{\int_a^b} f(x)dx + \frac{\epsilon}{2}$$

for all partitions P of $[a, b]$ with $\|P\| < \delta$. Using (i) this implies

$$U(P; f) < \int_a^b f(x)\,dx + \frac{\epsilon}{2} \text{ and}$$

$$\int_a^b f(x)\,dx < L(P; f) + \frac{\epsilon}{2}$$

Thus $U(P; f) - L(P; f) < \epsilon$

Conversely, suppose that for any $\epsilon > 0$, there exists a partition P of $[a, b]$ such that $U(P; f) - L(P; f) < \epsilon$.

But $\overline{\int_a^b} f(x)dx = \inf \{U(P; f) | P \in \mathbf{P}[a, b]\}$ implies

$$\overline{\int_a^b} f(x)\,dx \leq U(P; f)$$

and $\underline{\int_a^b} f(x)dx = \sup \{L(P; f) | P \in \mathbf{P}[a, b]\}$ implies

$$\underline{\int_a^b} f(x)dx \geq L(P; f), \text{ or, } -\underline{\int_a^b} f(x)dx \leq -L(P, f)$$

Thus $\overline{\int_a^b} f(x)dx - \underline{\int_a^b} f(x)dx \leq U(P; f) - L(P; f) < \epsilon$.

Thus $\overline{\int_a^b} f(x)dx - \underline{\int_a^b} f(x)dx < \epsilon$ implies

$$\overline{\int_a^b} f(x)dx = \underline{\int_a^b} f(x)dx$$

Thus f is Riemann integrable on $[a, b]$.

Notation : The statement that "f is Riemann integrable on $[a, b]$" be denoted by $f \in R[a, b]$.

Theorem 5 :

If f is continuous on $[a, b]$, then $f \in R[a, b]$.

Proof : Recall that f is continuous on $[a, b] \Rightarrow f$ is uniformly continuous on $[a, b]$. This means that for any given $\epsilon > 0$, there exists $\delta > 0$ such that for all points x_1, x_2 of $[a, b]$ such that $|x_1 - x_2| < \delta$, $|f(x_1) - f(x_2)| < \frac{\epsilon}{b-a}$.

Consider any partition $P = \{a = x_0, x_1, \ldots x_n = b\}$ of $[a, b]$ with $\|P\| < \delta$. Since f is continuous on $[x_{i-1}, x_i]$, f is bounded and attains its bounds. Let m_i be the infimum and M_i the supremum of f at points α_i, β_i in $[x_{i-1}, x_i]$. That is $f(\alpha_i) = m_i$ and $f(\beta_i) = M_i$. Since $\alpha_i, \beta_i \in [x_{i-1}, x_i]$ we have $|\alpha_i - \beta_i| < \delta$. Therefore $|f(\alpha_i) - f(\beta_i)| < \frac{\epsilon}{b-a}$.

That is $M_i - m_i < \frac{\epsilon}{b-a}$, $i = 1, 2, \ldots n$.

Therefore $\sum_{i=1}^{n} M_i \delta_i - \sum_{i=1}^{n} m_i \delta_i < \frac{\epsilon}{b-a} \sum_{i=1}^{n} \delta_i$

Therefore $U(P, f) - L(P, f) < \epsilon$, because $\sum_{i=1}^{n} \delta_i = b - a$

$\therefore f \in R[a, b]$.

Theorem 6 :

If $f : [a, b] \to \mathbf{R}$ is monotonic on $[a, b]$, then $f \in R[a, b]$.

Proof : Without loss of generality assume that f is monotonic non decreasing on $[a, b]$. For $\epsilon > 0$, consider any partition $P = \{a = x_0, x_1, \ldots x_n = b\}$ of $[a, b]$ with

$$\|P\| < \frac{\epsilon}{f(b) - f(a) + 1}$$

Let m_i, M_i be infimum and supremum of f on $[x_{i-1}, x_i]$. Then $m_i = f(x_{i-1})$; $M_i = f(x_i)$ (because f is non decreasing on $[a, b]$). Hence

$$U(P; f) - L(P; f) = \sum_{i=1}^{n} (M_i - m_i) \delta_i$$

$$= \sum_{i=1}^{n} [f(x_i) - f(x_{i-1})] \delta_i$$

$$< \sum_{i=1}^{n} [f(x_i) - f(x_{i-1})] \cdot \left[\frac{\epsilon}{f(b) - f(a) + 1}\right]$$

$$= \frac{[f(b) - f(a)] \cdot \lambda}{[f(b) - f(a) + 1]}$$

$$< \epsilon.$$

Thus $f \in R[a, b]$.

SAQ 2 Show that a constant function is Riemann integrable.

Example 1 :

Let $a > 0$ and f defined on $[0, a]$ by $f(x) = x^2$. Show that $f \in R[0, a]$ and $\int_0^a f(x)\, dx = \frac{a^3}{3}$.

Solution : Let $P = \left\{0, \frac{a}{n}, \frac{2a}{n}, \ldots \frac{na}{n}\right\}$ be a partition. Then for any interval $\left[\frac{(i-1)a}{n}, \frac{ia}{n}\right]$, $i = 1, 2, \ldots n$ we have $M_i = \frac{i^2 a^2}{n^2}$; $m_i = \frac{(i-1)^2 a^2}{n^2}$ and $\delta_i = \frac{ia}{n} - \frac{(i-1)a}{n} = \frac{a}{n}$.

$$\text{Therefore, } U(P,f) = \sum_{i=1}^{n} M_i \delta_i = \sum_{i=1}^{n} \frac{i^2 a^2}{n^2} \cdot \frac{a}{n} = \frac{a^3}{n^3} \sum_{i=1}^{n} i^2$$

$$= \frac{a^3}{n^3} \cdot \frac{n(n+1)(2n+1)}{6} = \frac{a^3}{6}\left(1+\frac{1}{n}\right)\left(1+\frac{2}{n}\right)$$

$$\therefore \int_{\underline{0}}^{a} f(x)\,dx = \inf\{U(P,f)\}$$

$$= \lim_{\|P\| \to 0} U(P;f) = \frac{a^3}{6}(1)(2) = \frac{a^3}{3}.$$

$$\text{Similarly, } L(P,f) = \sum_{i=1}^{n} M_i \delta_i = \sum_{i=1}^{n} \frac{(i-1)^2}{n^2} a^2 \cdot \frac{a}{n}$$

$$= \frac{a^3}{n^3} \sum_{i=1}^{n} (i-1)^2 = \frac{a^3}{n^3} \frac{(n-1)(n)(2n-1)}{6}$$

$$= \frac{a^3}{6}\left(1-\frac{1}{n}\right)\left(2-\frac{1}{n}\right)$$

$$\int_{\underline{0}}^{a} f(x)\,dx = \sup\{L(P;f)\} = \lim_{\|P\| \to 0} L(P;f) = \frac{a^3}{3}$$

$$\text{Then} \quad \int_{0}^{\overline{a}} f(x)\,dx = \int_{0}^{a} f(x)\,dx = \frac{a^3}{3} \text{ and } f \in R[0,a]$$

$$\text{and} \int_{0}^{a} f(x)\,dx = \frac{a^3}{3}.$$

Example 2 : Let f be defined on [0, 1] by

$$f(x) = \begin{cases} 1, \text{ if } x \text{ is rational} \\ -1, \text{ if } x \text{ is irrational} \end{cases}$$

Show that $f \notin R[0, 1]$.

Solution : f is bounded on [0, 1]. Let $P = \{0 = x_0, x_1, \ldots x_n = 1\}$ be a partition on [0, 1]. Then $M_i = 1$ and $m_i = -1$ on $[a, b]$

$$U(P;f) = \sum_{i=1}^{n} M_i \delta_i = \sum_{i=1}^{n} \delta_i = 1 \text{ and}$$

$$L(P;f) = \sum_{i=1}^{n} m_i \delta_i = \sum_{i=1}^{n} (-1)\delta_i = -1$$

$$\text{Thus} \int_{0}^{1} f(x)dx = \inf\{U(P,f)\} = +1$$

$$\text{and } \underline{\int_0^1} f(x)dx = \sup \{L(P, f)\} = -1$$

$$\text{Since } \overline{\int_0^1} f(x)dx \neq \underline{\int_0^1} f(x)dx \quad f \notin R[0, 1].$$

23.4 ALGEBRA OF RIEMANN INTEGRABLE FUNCTIONS

Theorem 7 :

If $f, g \in R[a, b]$ then $(f + g) \in R[a, b]$ and

$$\int_a^b (f + g)(x)\,dx = \int_a^b f(x)\,dx + \int_a^b g(x)\,dx$$

Proof : First we shall prove that

$$U(P, f + g) \leq U(P, f) + U(P, g)$$

$$L(P, f + g) \geq L(P, f) + L(P, g)$$

$$\text{Let } P = \{a = x_0, x_1, x_2, \ldots, b\}$$

be any partition of $[a, b]$.

Let the suprema of $f + g, f, g$ in $[x_{i-1}, x_i]$ be M_i, M_i', M_i'' respectively and the infima of $f + g, f, g$ in $[x_{i-1}, x_i]$ be m_i, m_i', m_i'' respectively.

Now $f(x) \leq M_i'$ and $g(x) \leq M_i''$ in $[x_{i-1}, x_i]$.

$\therefore (f + g)(x) \leq M_i' + M_i''$ in $[x_{i-1}, x_i]$.

$\therefore M_i' + M_i''$ is an upper bound of $f + g$ in $[x_{i-1}, x_i]$

But the least upper bound $\leq$ an upper bound.

$\therefore M_i \leq M_i' + M_i''$ in $[x_{i-1}, x_i]$

$$\text{Now } U(P, f + g) = \sum_{i=1}^{n} M_i (x_i - x_{i-1})$$

$$\leq \sum_{i=1}^{n} (M_i' + M_i'')(x_i - x_{i-1})$$

$$= \sum_{i=1}^{n} M_i'(x_i - x_{i-1}) + \sum_{i=1}^{n} M_i''(x_i - x_{i-1})$$

$$= U(P, f) + U(P, g)$$

$$\therefore U(P, f + g) \leq U(P, f) + U(P, g)$$

Similarly, $L(P, f+g) \geq L(P, f) + L(P, g)$

Since $f \in R[a, b]$ therefore for any $\epsilon > 0$ there exists a partition P_1 of $[a, b]$ such that

$$U(P_1, f) - L(P_1, f) < \frac{\epsilon}{2} \quad \ldots (1)$$

Since $g \in R[a, b]$, therefore for $\epsilon > 0$ there exists a partition P_2 of $[a, b]$ such that

$$U(P_2, g) - L(P_2, g) < \frac{\epsilon}{2} \quad \ldots (2)$$

Let $P_3 = P_1 \cup P_2$.

Then $U(P_3, f+g) - L(P_2, f+g)$

$$\leq L(P_3, f) + U(P_3, g) - \{L(P_3, f) + L(P_3, g)\}$$

$$= U(P_3, f) - L(P_3, g) + U(P_3, g) - L(P_3, g)$$

$$< \frac{\epsilon}{2} + \frac{\epsilon}{2}$$

$$\therefore U(P_3, f+g) < \epsilon$$

$\therefore (f+g) \in R[a, b]$

$$\text{Again } \int_a^{\overline{b}} (f+g)(x)\,dx \leq U(P, f+g)$$

$$\leq U(P, f) + U(P, g) \quad \ldots (1)$$

This is true for every partition P of $[a, b]$.

Since $\int_a^{\overline{b}} f(x)\,dx$ is the infimum of $\{U(P, f)\}$, there exists a partition P_1 of $[a, b]$ such that

$$U(P_1, f) < \int_a^{\overline{b}} f(x)\,dx + \frac{\epsilon}{2} \quad (\epsilon > 0).$$

Similarly there exists a partition P_2 of $[a, b]$ such that

$$U(P_2, g) < \int_a^{\overline{b}} f(x)\,dx + \frac{\epsilon}{2} \text{ for } (\epsilon > 0)$$

Let $P = P_1 \cup P_2$

Then $U(P, f) \leq U(P_1, f)$; $U(P, g) \leq U(P_2, g)$

$$\therefore \int_a^{\overline{b}} (f+g)(x)\,dx \leq U(P, f) + U(P, g)$$

$$\leq U(P_1, f) + U(P_2, g)$$

$$< \overline{\int_a^b} f(x)\,dx + \overline{\int_a^b} g(x)\,dx + \in \qquad \ldots \text{I}$$

Similarly, we can prove that

$$\underline{\int_a^b} (f+g)(x)\,dx > \underline{\int_a^b} f(x)\,dx + \underline{\int_a^b} g(x)\,dx - \in \qquad \ldots \text{II}$$

Since $f \in R[a, b]$, $g \in R[a, b]$ and $f + g \in R[a, b]$

therefore we have

$$\overline{\int_a^b} f(x)\,dx = \underline{\int_a^b} f(x)\,dx = \int_a^b f(x)\,dx$$

$$\overline{\int_a^b} g(x)\,dx = \underline{\int_a^b} g(x)\,dx = \int_a^b g(x)\,dx$$

$$\overline{\int_a^b} (f+g)(x)\,dx = \underline{\int_a^b} (f+g)(x)\,dx = \int_a^b (f+g)(x)\,dx$$

Hence I and II $\Rightarrow$

$$\int_a^b f(x)\,dx + \int_a^b g(x)\,dx - \in < \int_a^b (f+g)(x)\,dx < \int_a^b f(x)\,dx + \int_a^b g(x)\,dx + \in$$

$$\Rightarrow \left| \int_a^b (f+g)(x)\,dx - \left\{ \int_a^b f(x)\,dx + \int_a^b g(x)\,dx \right\} \right| < \in$$

$$\Rightarrow \int_a^b (f+g)(x)\,dx = \int_a^b f(x)\,dx + \int_a^b g(x)\,dx$$

Theorem 8 :

$$f \in R[a, b] \Rightarrow -f \in R[a, b]$$
$$\text{and } \int_a^b (-f)(x)\,dx = -\int_a^b f(x)\,dx$$

Proof : Let $P = \{a = x_0, x_1, x_2, \ldots x_n = b\}$ be any partition of $[a, b]$.

$$\text{Inf}(-f) = -\text{Sup}(f) = -M_i \text{ in } [x_{i-1}, x_i]$$

$$\text{Sup}(-f) = -\text{Inf}(f) = -m_i \text{ in } [x_{i-1}, x_i]$$

$$\therefore U(P, -f) = \sum_{i=1}^{n} (-m_i)\,\delta_i$$

$$= -\sum_{i=1}^{n} m_i\,\delta_i = -L(P, f)$$

$$L(P, -f) = \sum_{i=1}^{n} (-M_i)\,\delta_i = -\sum_{i=1}^{n} M_i\,\delta_i = -U(P, f)$$

$$\overline{\int_a^b} (-f)\,dx = \text{Inf}\{U(P, -f)\}$$

$$= \text{Inf}\{-L(P, f)\}$$

$$= -\text{Sup}\{L(P, f)\}$$

$$= -\underline{\int_a^b} f(x)\,dx = -\int_a^b f(x)\,dx \qquad \ldots (1)$$

$(\because f \in R[a, b])$

$$\underline{\int_a^b} (-f)(x)\,dx = \text{Sup}\{L(P, -f)\}$$

$$= \text{Sup}\{-U(P, f)\}$$

$$= -\text{Inf}\{U(P, f)\}$$

$$= -\overline{\int_a^b} f(x)\,dx = -\int_a^b f(x)\,dx \qquad \ldots (2)$$

$(\because f \in R[a, b])$

$\therefore$ (1) and (2) $\Rightarrow$

$$\underline{\int_a^b} (-f)(x)\,dx = \overline{\int_a^b} (-f)\,dx = -\int_a^b f(x)\,dx$$

$\Rightarrow -f \in R[a, b]$ and

$$\int_a^b (-f)(x)\,dx = -\int_a^b f(x)\,dx$$

Theorem 9 :

If $f \in R[a, b]$ then $\alpha f \in R[a, b]$

$$\int_a^b \alpha f\,dx = \alpha \int_a^b f\,dx \text{ where } \alpha \in R$$

Proof : Case (i) Let $\alpha \geq 0$

$$\text{Let } P = \left\{ a = x_0, x_1, x_2, \ldots x_n = b \right\}$$

be any partition of $[a, b]$

$$\text{Inf}(\alpha f) = \alpha . \text{Inf}(f)$$

$$\text{Sup}(\alpha f) = \alpha . \text{Sup}(f)$$

$$\therefore U(P, \alpha f) = \alpha . U(P, f)$$

$$\therefore L(P, \alpha f) = \alpha . L(P, f)$$

$$\int_a^{\bar{b}} \alpha f(x)\, dx = \text{Inf}\{U(P, \alpha f)\}$$

$$= \alpha \text{ Inf}\{U(P, \alpha f)\}$$

$$= \alpha \int_a^{\bar{b}} f(x)\, dx$$

$$= \alpha \int_a^{b} f(x)\, dx \qquad (\because f \in R[a, b])$$

$$\int_{\underline{a}}^{b} \alpha f(x)\, dx = \text{Sup}\{L(P, \alpha f)\}$$

$$= \alpha \text{ Sup}\{L(P, \alpha f)\}$$

$$= \alpha \int_{\underline{a}}^{b} f(x)\, dx$$

$$= \alpha \int_a^{b} f(x)\, dx \qquad (\because f \in R[a, b])$$

Case (ii) Let $\alpha > 0$

Let $\beta = -\alpha$ where $\beta > 0$

$$\text{Then } \alpha f = (-\alpha)(-f) = \beta(-f)$$

$$\text{But } f \in R[a, b] \Rightarrow -f \in R[a, b]$$

$\therefore$ By Case (i)

$\beta(-f) \in R[a, b]$

$$\text{Further } \int_a^b \alpha f = \int_a^b \beta\,(-f)\,dx \text{ by case (i)}$$

$$= \beta \int_a^b (-f)\,dx$$

$$= \beta \left(- \int_a^b f\,dx \right)$$

$$= -\beta \int_a^b f\,dx$$

$$= \alpha \int_a^b f\,dx$$

Theorem 10 :

If $f, g \in R[a, b]$ and $\alpha, \beta \in R$ then $\alpha f + \beta g \in R[a, b]$

and $\int_a^b (\alpha f + \beta g)\,dx = \alpha \int_a^b f\,dx + \beta \int_a^b g\,dx$

Proof : By theorem 9, $\alpha f \in R[a, b]$ and $\beta g \in R[a, B]$

$$\text{and } \int_a^b \alpha f\,dx = \alpha \int_a^b f\,dx; \int_a^b \beta g\,dx = \beta \int_a^b g\,dx$$

By theorem 1, $\alpha f + \beta g \in R[a, b]$

$$\text{and } \int_a^b (\alpha f + \beta g)\,dx = \int_a^b \alpha f\,dx + \int_a^b \beta g\,dx$$

$$= \alpha \int_a^b f\,dx + \beta \int_a^b g\,dx$$

Theorem 11 :

$$f \in R[a, b] \Rightarrow |f| \in R[a, b]$$

Proof : Let $P = \{a = x_0, x_1, x_2, \ldots x_n = b\}$ be any partition of $[a, b]$.

Let m_i, M_i be the infimum and supremum of f in $[x_{i-1}, x_i]$.

Let m_i', M_i' be the infimum and supremum of $|f|$ in $[x_{i-1}, x_i]$

Then $M_i' - m_i' \leq M_i - m_i$

$$\therefore U(P, |f|) - L(P, |f|) = \sum_{i=1}^{n} (M_i' - m_i') \delta_i$$

$$\leq \sum_{i=1}^{n} (M_i - m_i) \delta_i$$

$$= U(P, f) - L(P, f)$$

$$< \epsilon \qquad (\because f \in R[a, b])$$

$\therefore |f| \in R[a, b]$

Theorem 12 :

$$\boxed{f \in R[a, b] \Rightarrow f^2 \in R[a, b]}$$

Proof : $f^2 = |f|^2$

$f \in R[a, b] \Rightarrow |f| \in R[a, b]$

$\therefore$ Without loss of generality we can assume that $f \geq 0$

$$\text{Let } P = \{a = x_0, x_1, x_2, \ldots x_n = b\}$$

be any partition of $[a, b]$.

Let M be the supremum of f in $[a, b]$

Let $\epsilon > 0$; $f \in R[a, b] \Rightarrow U(P, f) - L(P, f) < \frac{\epsilon}{2M + 1}$

$$\text{Then } \inf(f^2) = [\inf(f)]^2 = m_i^2 \text{ on } [x_{i-1}, x_i]$$

$$\text{Sup } (f^2) = [\text{Sup } (f)]^2 = M_i^2 \text{ on } [x_{i-1}, x_i]$$

$$\therefore U(P, f^2) - L(P, f^2) = \sum_{i=1}^{n} (M_i^2 - m_i^2) \delta_i$$

$$= \sum_{i=1}^{n} (M_i + m_i)(M_i - m_i) \delta_i$$

$$\leq 2M \sum_{i=1}^{n} (M_i - m_i) \delta_i$$

$$= 2M (U(P, f) - L(P, f))$$

$$< 2M \cdot \frac{\epsilon}{2M + 1} < \epsilon$$

Thus for $\epsilon > 0$ we can find a partition P of $[a, b]$ such that

$$U\left(P, f^2\right) - L\left(P, f^2\right) < \epsilon$$

$$\therefore f^2 \in R\,[a, b]$$

Theorem 13 :

$$\boxed{f, g \in R\,[a, b] \Rightarrow fg \in R\,[a, b]}$$

Proof : We have

$$(f+g)^2 - (f-g)^2 = 4fg$$

$$\therefore fg = \frac{1}{4}\left[(f+g)^2 - (f-g)^2\right]$$

Now $f, g \in R\,[a, b] \Rightarrow (f+g)$ and $(f-g) \in R\,[a, b]$

$\Rightarrow (f+g)^2$ and $(f-g)^2 \in R\,[a, b]$

$\Rightarrow (f+g)^2 - (f-g)^2 \in R\,[a, b]$

$\Rightarrow \frac{1}{4}\left[(f+g)^2 - (f-g)^2\right] \in R\,[a, b]$

$\Rightarrow fg \in R\,[a, b]$

Theorem 14 :

Let $f, g \in R\,[a, b]$. Let the infimum and supremum of f in $[a, b]$ be m, M respectively. Then

(i) $f(x) \geq 0\ \forall\ x \in [a, b] \Rightarrow \int_a^b f(x)\,dx \geq 0$

(ii) $g(x) \geq f(x)\ \forall\ x \in [a, b]$

$$\Rightarrow \int_a^b g(x)\,dx \geq \int_a^b f(x)\,dx.$$

(iii) $\left|\int_a^b f(x)\,dx\right| \leq \int_a^b |f(x)|\,dx$, if $a < b$.

(iv) $m(b-a) \leq \int_a^b f(x)\,dx \leq M(b-a)$

(v) $|f(x)| \leq k\ \forall\ x \in [a, b] \Rightarrow \left|\int_a^b f(x)\,dx\right| \leq k(b-a)$

Proof : (i) $f(x) \geq 0\ \forall\ x \in [a, b]$

$\Rightarrow m \geq 0$

$$\Rightarrow L(P, f) \geq 0$$

$$\Rightarrow \int_{\underline{a}}^{b} f(x)\,dx \geq 0 \qquad \ldots (1)$$

$$f \in R[a, b] \Rightarrow \int_{\underline{a}}^{b} f(x)\,dx = \int_{a}^{b} f(x)\,dx \qquad \ldots (2)$$

$$(1), (2) \Rightarrow \int_{a}^{b} f(x)\,dx \geq 0$$

(ii) $f, g \in R[a, b] \Rightarrow -f, g \in R[a, b]$

$$\Rightarrow (g - f) \in R[a, b]$$

$$\int_{a}^{b} (g - f)\,dx = \int_{a}^{b} g\,dx - \int_{a}^{b} f\,dx$$

But $g(x) \geq f(x)\ \forall x \in [a, b] \Rightarrow (g - f) \geq 0$

$$\Rightarrow \int_{a}^{b} (g - f)\,dx \geq 0 \text{ from (i)}$$

$$\Rightarrow \int_{a}^{b} g\,dx \geq \int_{a}^{b} f\,dx$$

(iii) $f \in R[a, b] \Rightarrow |f| \in R[a, b]$

Now $-|f| \leq f \leq |f|$

$$\Rightarrow -\int_{a}^{b} |f|\,dx \leq \int_{a}^{b} f\,dx \leq \int_{a}^{b} |f|\,dx$$

$$\Rightarrow \left| \int_{a}^{b} f\,dx \right| \leq \int_{a}^{b} |f|\,dx$$

If $b < a$, then $\left| \int_{a}^{b} f\,dx \right| \leq \left| \int_{a}^{b} |f|\,dx \right|$

(iv) Let $h : [a, b] \to R$ be a function defined by

$$h(x) = m\ \forall x \in [a, b]$$

and $g : [a, b] \to R$ be a function defined by

$$g(x) = M \ \forall x \in [a, b]$$

Then $h, g \in R[a, b]$

Now $f \in R[a, b]$, $h \le f$; $g \ge f$

$$\Rightarrow \int_a^b h\,dx \le \int_a^b f\,dx \le \int_a^b g\,dx$$

$$\Rightarrow \int_a^b m\,dx \le \int_a^b f\,dx \le \int_a^b M\,dx$$

$$\Rightarrow m(b-a) \le \int_a^b f\,dx \le M(b-a)$$

(v) $|f(x)| \le k \ \forall x \in [a, b]$

$$\Rightarrow -k \le f(x) \le k \ \forall x \in [a, b]$$

$$\Rightarrow -k \le m \le M \le k$$

$$\Rightarrow -k(b-a) \le m(b-a) \le M(b-a) \le k(b-a)$$

But $m(b-a) \le \int_a^b f\,dx \le M(b-a)$ form (iv)

$$\therefore -k(b-a) \le \int_a^b f\,dx \le k(b-a)$$

$$\Rightarrow \left| \int_a^b f(x)\,dx \right| \le k(b-a)$$

Theorem 15 :

If $f \in R[a, b]$ and $c \in (a, b)$
then $f_1 = f\big|_{[a, c]} \in R[a, c]$; $f_2 = f\big|_{[c, b]} \in R[c, b]$

and conversely. Also

$$\int_a^b f(x)\,dx = \int_a^c f_1(x)\,dx + \int_c^b f_2(x)\,dx$$

Proof : Since $a < c < b$, $[a, c] \subset [a, b]$ and $[c, b] \subset [a, b]$

$$f_1(x) = f(x) \ \forall x \in [a, c]$$

is defined as restriction of f to $[a, c]$ and is written as $f_1 = f\big|_{[a, c]}$. Similarly for f_2.

The domain of definition of f_1 is $[a, c]$ and that of f_2 is $[c, d]$

If m and M are the exact lower and upper bounds of f on $[a, b]$

then $m \leq f(x) \leq M \; \forall \; x \in [a, b]$.

Hence $m \leq f_1(x) \leq M \; \forall \; x \in [a, c]$

and $m \leq f_2(x) \leq M \; \forall \; x \in [c, b]$

The two functions f_1 and f_2 are thus bounded on their respective domains which are bounded and closed intervals.

We can therefore find out their integrability. Since $f \in R[a, b]$ there exists a partition $P_0 \in P[a, b]$ such that

that $U(P_0, f) - L(P_0, f) < \epsilon$

If $P = P_0 \cup \{c\}$ then

$0 \leq U(P, f) - L(P, f) \leq U(P_0, f) - L(P_0, f) < \epsilon$

Taking $P \cap [a, c] = P_1$ and $P \cap [c, b] = P_2$

we find that

$$U(P_1, f_1) + U(P_2, f_2) = U(P, f)$$

and $L(P_1, f_1) + L(P_2, f_2) = L(P, f)$

$$\therefore 0 \leq U(P_1, f_1) - L(P_1, f_1) + U(P_2, f_2) - L(P_2, f_2) < \epsilon$$

This means that

$f_1 \in R[a, c]$ and $f_2 \in R[c, b]$

Conversely if $f_1 \in R[a, c]$ and $f_2 \in R[c, b]$

then for $\epsilon > 0$ there exist partitions

$P_1 \in P[a, c]$ and $P_2 \in P[c, b]$

such that

$$0 \leq U(P_1, f_1) - L(P_1, f_1) < \frac{\epsilon}{2}$$

and $0 \leq U(P_2, f_2) - L(P_2, f_2) < \frac{\epsilon}{2}$

If $P = P_1 \cup P_2$ then P is a partition of $[a, b]$ and

$$U(P, f) = U(P_1, f_1) + U(P_2, f_2)$$

$$\text{and } L(P, f) = L(P_1, f_1) + L(P_2, f_2)$$

Hence for this partition P

$0 \leq U(P, f) - L(P, f) < \epsilon$

and therefore $f \in R[a, b]$

Finally if $P_0 \in \mathbf{P}[a, b]$ and $c \in (a, b)$

then $P = P_0 \cup \{c\} \in \mathbf{P}[a, b]$

Hence $\{P\} \cup \mathbf{P}[a, b]$ and therefore

$$\text{Inf } U(P, f) \geq \text{inf } U(P_0, f)$$

Further if $P = P_0 \cup \{c\}$ then

$$U(P, f) \leq U(P_0, f)$$

$$\text{and Inf } U(P, f) \leq U(P, f) \leq U(P_0, f)$$

$$\text{Hence Inf } U(P, f) \leq \text{Inf } U(P_0, f)$$

$$\text{Thus Inf } U(P_0, f) = \text{Inf } U(P, f)$$

where $P_0 \in \mathbf{P}[a, b]$ and $P = P_0 \cup \{c\}$

P is a partition of $[a, b]$ and $c \in P$ iff

$P_1 = P \cap [a, c]$, $P_2 = P \cap [c, b]$

are partitions of $[a, c]$ and $[c, b]$

$$\text{Now } \int_a^b f(x)\,dx = \text{Inf}_{c \in P} U(P, f)$$

$$= \text{Inf}\left[U(P_1, f_1) + U(P_2, f_2)\right]$$

$$\geq \text{Inf } U(P_1, f_1) + \text{Inf } U(P_2, f_2)$$

$P_1 \in \mathbf{P}[a, c]$ $P_2 \in \mathbf{P}[c, b]$

$$= \int_a^c f_1(x)\,dx + \int_c^b f_2(x)\,dx$$

Note : It has been the practice to write f in place of both f_1 and f_2 and also write

$$\int_a^b f(x)\,dx = \int_a^c f(x)\,dx + \int_c^b f(x)\,dx$$

Theorem 16 :

If $f \in R[a, b]$, $g \in R[a, b)$ and if there exists $t > 0$ such that

$|g| \geq t$ on $[a, b]$

then $\frac{f}{g} \in R[a, b]$.

Proof : $|g(x)| \geq t > 0 \quad \forall x \in [a, b]$

$\Rightarrow \quad \left|\frac{1}{g(x)}\right| \leq \frac{1}{i} \; \forall x \in [a, b]$

$\Rightarrow \frac{1}{g}$ is bounded on $[a, b]$.

$g \in R[a, b] \Rightarrow g$ is bounded on $[a, b]$

Let $P = \{a = x_0, x_1, x_2, \ldots x_n = b\}$ be any partition of $[a, b]$.

Then $g, \frac{1}{g}$ are bounded on every subinterval $[x_{i-1}, x_i]$ for $i = 1, 2, \ldots n$

Let M_i', M_i be the suprema of g and $\frac{1}{g}$ on $[x_{i-1}, x_i]$ respectively.

Let m_i', m_i be the infima of g and $\frac{1}{g}$ on $[x_{i-1}, x_i]$ respectively.

$x_1, x_2 \in [x_{i-1}, x_i] \Rightarrow m_i' \leq g(x_1); g(x_2) \leq M_i'$

Then $m_i \leq \frac{1}{g}(x_1); \left(\frac{1}{g}\right)(x_2) \leq M_i$

$\Rightarrow |g(x_1) - g(x_2)| \leq M_i' - m_i'$

$\left|\left(\frac{1}{g}\right)(x_1) - \left(\frac{1}{g}\right)(x_2)\right| \leq M_i - m_i \quad \ldots (1)$

$x_1, x_2 \in [x_{i-1}, x_i] \Rightarrow$

$$\left|\left(\frac{1}{g}\right)(x_1) - \left(\frac{1}{g}\right)(x_2)\right| = \left|\frac{g(x_2) - g(x_1)}{g(x_1)\, g(x_2)}\right|$$

$$\leq \frac{1}{i^2} |g(x_1) - g(x_2)|$$

$$\leq \frac{1}{i^2} (M_i' - m_i') \quad \ldots (2)$$

Let $M_i - m_i = l; \frac{1}{i^2}(M_i' - m_i') = l_1$

If $l > l_1$ then $\in_1 = l - l_1 > 0$

M_i = Sup of $\frac{1}{g}$ on $[x_{i-1}, x_i]$

m_i = Inf of $\frac{1}{g}$ on $[x_{i-1}, x_i]$

$\Rightarrow$ there exists α_1, α_2 in $[x_{i-1}, x_i]$

such that

$$\left(\frac{1}{g}\right)(\alpha_1) > M_i - \frac{\in_1}{2}$$

and $\left(\frac{1}{g}\right)(\alpha_2) < m_i + \frac{\epsilon_1}{2}$

$\Rightarrow \left(\frac{1}{g}\right)(\alpha_1) - \left(\frac{1}{g}\right)(\alpha_2) > M_i - m_i - \epsilon = l - \epsilon_1 = l_1$

$\Rightarrow l_1 < \left(\frac{1}{g}\right)(\alpha_1) - \left(\frac{1}{g}\right)(\alpha_2)$

$\leq \left|\left(\frac{1}{g}\right)(\alpha_1) - \left(\frac{1}{g}\right)(\alpha_2)\right|$

$\leq \frac{1}{l^2}\left(M_i' - m_i'\right) = l_1$

$\Rightarrow l_1 < l$ which is absurd.

$\therefore$ Our assumption that $l > l_1$ must be wrong.

$\therefore l \leq l_1 \Rightarrow M_i - m_i \leq \frac{1}{l^2}\left(M_i' - m_i'\right)$

$$\sum_{i=1}^{n}\left(M_i - m_i\right)\left(x_i, x_{i-1}\right) \leq \sum_{i=1}^{n} \frac{1}{l^2}\left(M_i' - m_i'\right)\left(x_i - x_{i-1}\right)$$

$\Rightarrow$ for any $P \in \mathbf{P}[a, b]$

$U\left(P, \frac{1}{g}\right) - L\left(P, \frac{1}{g}\right) \leq \frac{1}{l^2}\left(U(P, g) - L(P, g)\right)$

$g \in R[a, b] \Rightarrow$ for $\epsilon > 0$ there exists a partition P_1 of $[a, b]$ such that

$U\left(P_1, g\right) - L\left(P_1, g\right) < \epsilon \cdot l^2$

$\therefore$ from (3) it follows that for any $\epsilon > 0$ there exists $P_1 \in \mathbf{P}[a, b]$

$U\left(P_1, \frac{1}{g}\right) - L\left(P_1, \frac{1}{g}\right) < \epsilon$

$\Rightarrow \frac{1}{g} \in R[a, b]$

Now $f, \frac{1}{g} \in R[a, b]$

$\Rightarrow f \cdot \left(\frac{1}{g}\right) \in R[a, b]$

$\Rightarrow \left(\frac{f}{g}\right) \in R[a, b]$

23.5 SUMMARY

The Riemann integrability of a function over an interval has been introduced through the concepts of upper sums and lower sums. Continuous functions defined on closed intervals and monotonic functions defined on closed intervals are shown to be Riemann integrable functions. The sum, product, quotient (when defined properly) of Riemann integrable functions are again Riemann integrable. Certain important properties of Riemann integrable functions have been stated and proved.

23.6 MODEL EXAMINATION QUESTIONS

SECTION - A (Long Answers)

(i) Define the concept of Riemann integrability of a function and give an example of a function which is Riemann integrable and a function which is not Riemann integrable. State and prove a theorem which gives a necessary and sufficient condition for a function to be Riemann integrable.

(ii) Show that the sum and product of Riemann integrable functions is Riemann integrable.

(iii) State and prove Darboux theorem on Riemann integrability of a function.

SECTION - B (Short Answers)

(i) Show that continuous functions are Riemann integrable.

(ii) If $f \in R[a, b]$, show that $|f| \in R[a, b]$ and $f^2 \in R[a, b]$.

(iii) Show that if $f, g \in R[a, b]$ and $g(x) \geq f(x)$ for $x \in [a, b]$ then $\int_a^b g(x)\,dx \geq \int_a^b f(x)\,dx$.

Hence or otherwise prove that $\left|\int_a^b f(x)\,dx\right| \leq \int_a^b |f(x)|\,dx$ $(a < b)$.

(iv) If $f, g \in \mathbf{R}[a, b]$ and there is $t > 0$ such that $|g| > t$ on $[a, b]$, then show that $\frac{f}{g} \in R[a, b]$.

23.7 ANSWERS TO SELF ASSESSMENT QUESTIONS

SAQ 1 Let $P = (x_0, x_1, x_2, \ldots x_n)$. Since $m_k \leq M_k$ for $k = 1, 2, \ldots n$ and since $x_k - x_{k-1} > 0$, for $k = 1, 2, \ldots n$; it follows that

$$L(P; f) = \sum_{i=1}^{n} m_k \left(x_k - x_{k-1}\right) \leq M_k \left(x_k - x_{k-1}\right) = U(P; f)$$

SAQ 2 Let $f(x) = k$ for $a \leq x \leq b$. Then $m_i = M_i = k$ on $[a, b]$.

Let $P = \{a = x_0, x_1, x_2, \ldots x_n = b\}$ be a partition of $[a, b]$.

Then $U(P, f) = \sum_{i=1}^{n} M_i \delta_i = \sum_{i=1}^{n} k\,\delta_i = k \sum_{i=1}^{n} \delta_i = k(b - a)$

$$L(P, f) = \sum_{i=1}^{n} m_i \delta_i = \sum_{i=1}^{n} k\,\delta_i = k \sum_{i=1}^{n} \delta_i = k(b - a).$$

$$\therefore \underline{\int_a^b} f(x)\,dx = \overline{\int_a^b} f(x)\,dx = k(b - a) = \int_a^b f(x)\,dx.$$

UNIT–24 : THE FUNDAMENTAL THEOEM OF INTEGRATION

Contents

24.1 Aims and Objectives

24.2 Introduction

24.3 Fundamental Theorem of Integral Calculus

24.4 Mean Value Theorems

24.5 Integral as a limit of sum

24.6 Worked out exercises

24.7 Summary

24.8 Sample Examination Questions

24.1 AIMS AND OBJECTIVES

By the time you complete this unit you should be able to (i) State and prove fundamental theorem of integral calculus, (ii) State and prove Mean Value theorem for integrals, (iii) State and prove Cauchy's Fundamental theorem of calculus, (iv) Evaluate an integral as the limit of a sum.

24.2 INTRODUCTION

The fundamental theorem of calculus states that in broad terms differentiation and integration are inverse operations. It is natural to ask questions about the conditions that a function f may have to satsify so that it may be the derivative of some other function F defined on an interval. It turns out that if f is continuous on $[a, b]$, then there exists a function F on $[a, b]$ such that $F'(x) = f(x)$ for all $x \in [a, b]$. Such a function F is called a primitive (antiderivative) of f on $[a, b]$. A primitive of a given function is unique only upto an arbitrry constant. Thus the fundamental theorem of calculus opens the study of functions of the form $x \to \int_a^x f$, where f is an integrable function on an interval $[a, b]$, $x \in [a, b]$. However there are limitation to the application of fundamental theorem. A function may be integrable on $[a, b]$ but may not possess anti derivative on $[a, b]$. A function F may be differentiable with derivative $F'(x) = f(x)$ for all x, without f being integrable. A second version of Fundamental theorem states that

$$\lim_{n\to\infty} \sum_{1}^{n} hf(a + rh) = \int_a^b f \text{ where } h = \frac{b-a}{n}.$$

24.3 FUNDAMENTAL THEOREM OF INTEGRATION

Theorem. 1 :

If $f \in R[a, b]$ then the function F defined on $[a, b]$ by $F(x) = \int_a^x f(t)\,dt$ for $x \in [a, b]$ is continuous on $[a, b]$. Further if f is continuous at $c \in [a, b]$ then F is derivable at c and $F'(c) = f(c)$.

Proof : First part

$$f \in R[a, b] \Rightarrow f \text{ is bounded on } [a, b]$$
$$\Rightarrow |f| \text{ is bounded on } [a, b]$$

Let the supremeum of $|f|$ on $[a, b]$ ne M

For $\epsilon > 0$, there exists $\delta > 0$ such that

$0 < \delta < \epsilon/M$.

If $x \in [a, b]$, $x + h \in [a, b]$ and $|h| < \delta$

$$\text{then } |F(x+h) - F(x)| = \left| \int_a^{x+h} f(t)\,dt - \int_a^x f(t)\,dt \right|$$

$$= \left| \int_x^{x+h} f(t)\,dt \right|$$

$$\leq \left| \int_x^{x+h} f(t)\,dt \right|$$

$$\leq M|h|$$

$$< M\delta$$

$$< \epsilon$$

Hence F is continuous on $[a, b]$.

Second part

Let f be continuous at $c \in [a, b]$.

For $\epsilon > 0\ \exists\ \delta > 0$ such that

$t \in [a, b]$ and $|t - c| < \delta \Rightarrow |f(t) - f(c)| < \epsilon$.

Take h such that $|h| < \delta$.

$$F(c + h) - F(c) = \int_c^{c+h} f(t)\,dt \text{ and } \int_c^{c+h} f(c)\,dt = hf(c)$$

Therefore $$\frac{F(c+h) - F(c)}{h} - f(c) = \frac{1}{h} \int_c^{c+h} [f(t) - f(c)]\,dt$$

Hence $\left|\frac{F(c+h)-F(c)}{h} - f(c)\right| = \frac{1}{|h|}\left|\int_c^{c+h} [f(t) - f(c)]\, dt\right|$

$$\leq \frac{1}{|h|}\left|\int_c^{c+h} |f(t) - f(c)|\, dt\right|$$

$$< \frac{1}{|h|} \cdot \in |h| = \in .$$

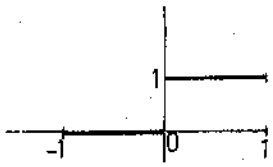
Hence F is derivable at c and $F'(c) = f(c)$.

Remark. 1 : If f is continuous on $[a, b]$ and if $F(x) = \int_a^x f(t)\, dt$ for $x \in [a, b]$ then F is derivable on $[a, b]$ and $F'(x) = f(x)$ on $[a, b]$.

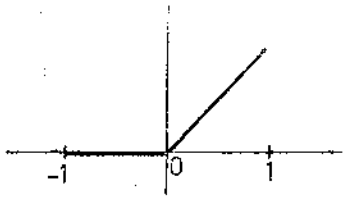
Example. 1 : Let $I = [-1, 1]$ and define $f : I \to \mathbf{R}$ by

$$f(x) = \begin{cases} 0, \text{ if } -1 \leq x < 0 \\ 1, \text{ if } 1 \leq x \leq 1 \end{cases}$$

Then for $x \in I$ we have $F(x) = \int_{-1}^{x} f = 0$, for $-1 \leq x \leq 0$ and $F(x) = x$ for $0 < x \leq 1$.



Graph of f



Graph of F

To see this we observe that for $0 < x \leq 1$, the partition $P(-1, 0, x)$ of $[-1, x]$ has $L(P, f) = x = U(P; f)$ so that $F(x) = x$. If $-1 \leq x \leq 0$, then $F(x) = 0$. We see that F is continuous on I but is not differentiable at $x = 0$ where f is not continuous.

Definition. 1 :

If $f \in R[a, b]$ and if there exists a function ϕ on $[a, b]$ such that $\phi'(x) = f(x)$ for all $x \in [a, b]$, then ϕ is called the primitive (anti derivative) of f.

Theorem. 2 : (Fundamental theorem of integral calculus)

If $f \in R[a, b]$ ad ϕ is the primitive of f, then $\int_a^b f(x)\, dx = \phi(b) - \phi(a)$.

Proof : $\phi'(x) = f(x)$ for every $x \in [a, b]$

and $\phi' = f \in R[a, b]$

But $f \in R[a, b]$ implies that for any given $\in > 0$, there exists $\delta > 0$ and a partition P with $\|P\| < \delta$ such that

$$\left| \sum_{i=1}^{n} f(y_i)\, \delta_i - \int_a^b f(x) \right| < \in$$

where $P = \{a = x_0, x_1, \ldots, x_n = b\}$ and $x_{i-1} \le y_i \le x_i$ $i = 1, 2, \ldots, n$. Since ϕ is differentiable on $[a, b]$, ϕ is continuous on $[a, b]$. Thus ϕ satisfies all the conditions of MeanValue Theorem and hence $\phi(x_i) - \phi(x_{i-1}) = (x_i - x_{i-1})\, \phi'(y_i)$ for some $y_i \in (x_{i-1}, x_i)$.

$$\text{Therefore} \sum_{i=1}^{n} \left[\phi(x_i) - \phi(x_{i-1}) \right] = \sum_{i=1}^{n} \phi'(y_i)\, \delta_i = \sum_{i=1}^{n} f(y_i)\, \delta_i$$

$$\text{But} \sum_{i=1}^{n} \left[\phi(x_i) - \phi(x_{i-1}) \right] = \phi(b) - \phi(a)$$

$$\therefore \left| \phi(b) - \phi(a) - \int_a^b f(x)\, dx \right| < \in$$

$$\text{or} \int_a^b f(x)\, dx = \phi(b) - \phi(a)$$

Remark. 1 : If f and g have continuous derivatives on $I = [a, b]$ then

$$\int_a^b f'(x)\, g(x)\, dx = [f(b)\, g(b) - f(a)\, g(a)] - \int_a^b f(x)\, g'(x)\, dx.$$

This "formula" called Integration by parts is a consequence of Fundamental theorem of integration. To see this let $h = f(x)\, g(x)$. Then h and $h' = f'(x)\, g(x) + f(x)\, g'(x)$ are continuous so that

$$\int_a^b (f'(x)\, g(x) + f(x)\, g'(x))\, dx = \int_a^b h'(x)\, dx = h(b) - h(a)$$

$$= f(b)\, g(b) - f(a)\, g(a)$$

$$\text{and} \int_a^b f'(x)\, g(x)\, dx = [f(b)\, g(b) - f(a)\, g(a)] - \int_a^b f(x)\, g'(x)\, dx.$$

Theorem. 3 :

Let I = $[a, b]$ and let $\phi : I \to \mathbf{R}$, have a continuous derivative on I, If f is continuous on J = ϕ (I), then $\int_a^b f(\phi(t))\,\phi'(t)\,dt = \int_{\phi(a)}^{\phi(b)} f(x)\,dx$.

Proof : Let $c = \phi(a)$ and $d = \phi(b)$. Since f is continuous on J = ϕ (I), define F : J $\to$ **R** by

$$F(u) = \int_c^d f(x)\,dx, \text{ for } u \in I$$

Let H : I $\to$ R be defined by H (t) = F $(\phi(t))$ for $t \in$ T.

Then H′ (t) = F′ $(\phi(t))\,\phi'(t)$ for $t \in$ T

Applying fundamental theorem and using the fact that

H (α) = F $(\phi(a))$ = F $(c) = 0$, we get

$$\int_a^b f(\phi(t))\,\phi'(t)\,dt = H(b) - H(a) = H(b)$$

But H (b) = F $(\phi(b))$ = F $(d) \int_c^d f(\ldots)\ldots$

Hence $\int_a^b f(\phi(t))\,\phi'(t)\,dt = \int_c^d f(x)dx$

24.4 MEAN VALUE THEOREMS

Theorem 4 : Mean Value Theorem

Let f be continuous on $[a, b]$ and let g be integrable on $[a, b]$ such that $g(x) \geq 0$ for all $x \in [a, b]$. Then there exists a point $c \in [a, b]$ such that

$$\int_a^b f(x)\,g(x)\,dx = f(c)\int_a^b g(x)\,dx.$$

Proof : Since f and g are integrable, the product fg is also integrable. Let m = inf $(f[a, b])$ and M = sup $(f[a, b])$. Then $m\,g(x) \leq f(x)\,g(x) \leq M\,g(x)$ for all $x \in [a, b]$. Hence

$$m\int_a^b g(x)\,dx \leq \int_a^b f(x)\,g(x)\,dx \leq M\int_a^b g(x)\,dx.$$

If $\int_a^b g(x)\,dx = 0$, we choose c arbitrarily in $[a, b]$.

$$\text{Otherwise } m \leq \frac{\int_a^b f(x)\, g(x)\, dx}{\int_a^b g(x)\, dx} \leq M.$$

Since f is continuous, there exists a point $c \in [a, b]$

$$\text{such that } f(c) = \frac{\int_a^b f(x)\, g(x)\, dx}{\int_a^b g(x)\, dx}.$$

Remark. 2 : If f is continuous on $[a, b]$, there exists $c \in [a, b]$ such that $\int_a^b f(x)\, dx = f(c)\,(b-a)$

(Take $g(x) = 1$ in Mean value theorem).

24.5 INTEGRAL AS A LIMIT OF SUM

Theorem. 5 :

If $f \in R[a, b]$ then, $\int_a^b f = \lim_{n\to\infty} \sum_1^n hf(a + rh)$ where $h = \frac{b-a}{n}$.

Proof : Let $P = \{a = x_0, x_1, \ldots, x_n = b\}$ be a partition of $[a, b]$ into n equal parts. Then $x_r = a + \frac{r(b-a)}{n}$ and put $h = \frac{b-a}{n}$ so that $x_r = a + rh$ and using the definition of Riemann integrability of f, we get

$$\int_a^b f = \lim_{\|P\|\to 0} \sum_{r=1}^n f(x_r)(x_r - x_{r-1})$$

$$= \lim_{n\to\infty} \sum_{r=1}^n f(a + rh) \cdot h$$

$$= \lim_{n\to\infty} \sum_{r=1}^n h \cdot f(a + rh).$$

Remark. 3 : In particular when $a = 0$ and $b = 1$, $h = \frac{1}{n}$ and $\int_0^1 f(x)\, dx = \lim_{n\to\infty} \sum_{r=1}^n \frac{1}{n} f\left(\frac{r}{n}\right)$. In working out problems we replace $\frac{r}{n}$ by x, $\frac{1}{n}$ by dx and $\lim_{n\to\infty} \Sigma$ by $\int$ sign

24.6 WORKEDOUT EXERCISES

Exercise. (i) : Using the integral as limit of sum show that $\lim_{n\to\infty}\left(\frac{n^n}{n!}\right)^{1/n} = e$.

Ans : Let $A = \lim_{n\to\infty}\left(\frac{n}{1}\cdot\frac{n}{2}\cdot\ \ldots\ \cdot\frac{n}{n}\right)^{1/n}$

$$\text{Then Log A} = \lim_{n\to\infty}\frac{1}{n}\left[\log n + \log\frac{n}{2} + \ \ldots\ + \log\frac{n}{n}\right]$$

$$= \lim_{n\to\infty}\frac{1}{n}\sum_{r=1}^{n}\log\frac{n}{r} = \int_0^1 \log\frac{1}{x}\,dx = -\int_0^1 \log x\,dx$$

$$= -[x\log x]_0^1 + -[x]_0^1 = 1$$

$$\text{Since log A} = 1;\ A = e^1 = e.$$

Exercise. (ii) : Show that $\lim_{n\to\infty}\left[\frac{1}{n} + \frac{n^2}{(n+1)^3} + \frac{n^2}{(n+2)^3} + \ \ldots\ + \frac{1}{8n}\right] = \frac{3}{8}$

Ans : $\frac{n^2}{(n+r)^3} = \frac{1}{n\left[1+\frac{r}{n}\right]^3}$ Hence the given series can be written as

$$\sum_{r=0}^{n}\frac{1}{n}\cdot\frac{1}{\left(1+\frac{r}{n}\right)^3} = \sum_{r=0}^{n-1}\frac{1}{n}\cdot\frac{1}{\left(1+\frac{r}{n}\right)^3} + \frac{1}{8n}$$

$$\therefore \lim_{n\to\infty}\frac{1}{n}\sum_{r=0}^{n} f\left(\frac{r}{n}\right) = \int_0^1 f(x)\,dx \quad \text{where } f(x) = \frac{1}{(1+x)^3}.$$

Now $(1+x)^3 \in R\,[0, 1]$ and $(1+x)^3 \geq 1$ for $x \in [0, 1]$.

$$\therefore \frac{1}{(1+x)^3} \in R\,[0, 1].$$

$$\therefore \lim_{n\to\infty}\frac{1}{n}\sum_{r=0}^{n} f\left(\frac{r}{n}\right) = \int_0^1 \frac{dx}{(1+x)^3} = \left[\frac{(1+x)^{-2}}{-2}\right]_0^1 = \frac{3}{8}.$$

Eercise. (iii) : Evaluate $\lim_{n\to\infty}\left(\frac{1}{n} + \frac{1}{n+1} + \ \ldots\ + \frac{1}{3n}\right)$.

Sol : The given sum $\sum_{r=0}^{2n} \frac{1}{n+r} = \frac{1}{n} \sum_{r=0}^{2n} \frac{1}{\left(1 + \frac{r}{n}\right)}$

$$\therefore \lim_{n\to\infty} \sum_{r=0}^{2n} \frac{1}{(n+r)} = \lim_{n\to\infty} \frac{1}{n} \sum_{r=0}^{2n} \left(\frac{1}{\left(1 + \frac{r}{n}\right)}\right)$$

$$= \lim_{n\to\infty} \frac{1}{n} \sum_{r=0}^{2n} f\left(\frac{r}{n}\right), \text{ where } f\left(\frac{r}{n}\right) = \frac{1}{1 + \frac{r}{n}}$$

$$\therefore \text{Let } f(x) = \frac{1}{1+x}. \text{ Then } f \in R\,[0, 2]$$

$$\text{and } \lim_{n\to\infty} \frac{1}{n} \sum_{r=0}^{2n} \left(\frac{1}{1 + \frac{r}{n}}\right) = \int_0^2 f(x)\,dx = \int_0^2 \frac{1}{1+x}\,dx$$

$$= [\log |1 + x|]_0^2 = \log 3.$$

Exercise. (iv) : Prove that

$$\lim_{n\to\infty} \left[\left(1 + \frac{1}{n}\right)\left(1 + \frac{2}{n}\right) \cdots \left(1 + \frac{4n}{n}\right)\right]^{1/n} = \frac{5}{e^4}.$$

Ans : $\text{Let A} = \lim_{n\to\infty} \left[\left(1 + \frac{1}{n}\right)\left(1 + \frac{2}{n}\right) \cdots \left(1 + \frac{4n}{n}\right)\right]^{1/n}$

$$\text{Then log A} = \lim_{n\to\infty} \frac{1}{n}\left[\log\left(1 + \frac{1}{n}\right) + \log\left(1 + \frac{2}{n}\right) + \ldots + \log\left(1 + \frac{4n}{n}\right)\right]^{1/n}$$

$$= \lim_{n\to\infty} \frac{1}{n} \sum_{r=1}^{4n} \log\left(1 + \frac{r}{n}\right) = \int_0^4 \log(1+x)$$

$$= [x \log(1+x)]_0^4 - [x - \log(1+x)]_0^4$$

$$= 4 \log 5 - 4 + \log 5 = 5 \log 5 - 4$$

$$\therefore \text{A} = e^{5\log 5 - 4} = 5^5 \cdot e^{-4}$$

24.7 SUMMARY

The fundamental theorem of integral calculus establishes a formal relationship between the integral of a function and the derivative of the function. For simple functions the integration and differentiation are seen to be inverse operations. But if we consider all functions then it is not obvious

that these two operations are not always inverse to each other. The process of integration improves the status of a function from integrable to continuous. If f is continuous on $[a, b]$, then the indefinite integral $\phi_a(x) = \int_a^x f$, for $x \in [a, b]$ is an antiderivative of f. Thus a continuous function always possesses atleast one antiderivative. The Mean Value theorem states that if $f \in R[a, b]$ then there exists a number $c \in [a, b]$ such that $\int_a^b f = f(c)(b - a)$ we have also interpreted an integral as the limit of sum.

24.8 MODEL EXAMINATION QUESTIONS

Section A (Long Answer)

i) State and prove the fundamental theorem of integration.

ii) Show that

(a) $\lim_{n\to\infty} \left(\frac{1}{n} + \frac{1}{n+1} + \ldots + \frac{1}{2n-1}\right) = \log 2.$

(b) $\lim_{n\to\infty} \left(\frac{n}{n^2+1^2} + \frac{n}{n^2+2^2} + \ldots \frac{1}{2n}\right) = \frac{\pi}{4}.$

Section B (Short Answer)

i) Prove that $\left|\int_a^d f(x)\,dx\right| \leq \int_a^d |f(x)|\,dx$

ii) If $f \in R[a, b]$ then $F(x) = \int_a^x f(t)\,dt$, for $x \in [a, b]$ is continuous on $[a, b]$. Under what conditions will $F' = f(c)$ for $c \in [a, b]$.

MATHEMATICS - COURSE III

ASSIGNMENT - I

SECTION - A

1. With the usual notation pove that $\left(I_m, +_m\right)$ is a group.
2. State and prove Cayley's theorem on groups. If G is a finite cyclic group, show that |Aut G| = 2.
3. Define a ring. Explain the concept of an ideal in a ring. Show that a field has no proper ideals.

SECTION - B

1. State and prove Lagrange's theorem on finite groups. What can you say about the converse of the theorem?
2. Prove that the set A_n of ever permutations of S_n from a normal subgroup of S_n for $n \geq 2$.
3. Define a vector space and give an example. If V is a vector space over the field F and W is a subset of V, then prove that W is a subspace of V if and only if $\alpha x + \beta y \in W$, for $x, y \in W$, $\alpha, \beta \in F$.

MATHEMATICS - COURSE III

ASSIGNMENT - II

SECTION - A

1. Prove that the real number system is a complete ordered field.
2. State and prove the Cauchy's general principle of convergence of real sequences. What are the limit points of the sequence $\{(-1)^n\}$? Why ?
3. Discuss the convergence of $\sum_{n=1}^{\infty} \frac{1}{n^p}$.

SECTION - B

1. State and prove Bolzano - Weirstrass theorem for real numbers.
2. Obtain the rearrangement of the series $1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \ldots$ which diverges to ∞.
3. Define Cauchy product of two infinite series. Give an example of a pair of conditionally convergent series whose product is also convergent.

MATHEMATICS - COURSE III

ASSIGNMENT - III

SECTION - A

1. Define a uniform continuous function. Show that a continuous function defined on a compact aggregate is uniformly continuous. Give an example of a continuous function which is not uniformly continuous.

2. (i) State and prove Lagrange's mean value theorem.

   (ii) Prove that monotonic functions defined on a closed interval are Riemann integrable.

3. Define radius of convergence of a power series. Prove that the series $\sum_{n=1}^{\infty} x\, a_n\, x^{n-1}$ has the same radius of convergence as $\sum_{n=1}^{\infty} a_n\, x^n$.

SECTION - B

1. Find the Maclaurin expansion of $\log (1 + x)$.

2. State the conditions on the functions for the change of variable in an integral and evaluate $\int_{-1}^{1} dx$ by substituting $x = t^{3/2}$.

3. Prove that there exist real functions f and g such that $f' = g$, $g' = f$ and $f(0) = 0$ and $g(0) = 1$.

FACULTY OF SCIENCE

B.SC. III YEAR (3 YEAR DEGREE COURSE) EXAMINATION

MATHEMATICS - COURSE III

(ALGEBRA AND ANALYSIS)

Time : 3 hrs

Max Marks : 100

Min Marks : 35

SECTION - A

Answer any four Questions

1. Define a binary operation and a group. Show that the set of all non-singular matrices of order 2×2 forms a non-abelian group under the matrix multiplication.

2. State and prove the fundamental theorem of homomorphism of groups.

3. Define an integral domain and characteristic of an integral domain. Prove that the characteristic of an integral domain is either zero or a prime number.

4. Define a limit point of an aggregate. State and prove Bolzano-Weierstrass theorem on real numbers. What are the limit points of the set $\left\{\frac{1}{n} / n \in N\right\}$?

5. Establish cauchy's condensation test for convergence of series. For what values of p is the series $\sum_{n=1}^{\infty} \left(\sqrt{n-1} - \sqrt{n}\right)^p$ convergent? Justify your answer.

6. Show that a function which is differentiable at a point is continuous at that point. Show that the converse is not true.

7. Define Riemann integral and show that monotonic functions defined on a closed interval are Riemann integrable.

8. Define a power series and radius of convergence and interval of convergence of power series.

   Find the radius of convergence and interval of convergence of the series $\sum_{n=1}^{\infty} \frac{(-1)^n x^n}{n}$.

SECTION - B

Answer any five Questions

9. Define the order of an element and order of a group. State and prove the Lagrange's theorem on finite groups. What can you say about the converse of the theorem ?

10. Define a permutation goup. Prove that the set A_n of even permutations of S_n form a normal subgoup of S_n for $n \geq 2$.

11. Define a ring. Explain the concept of an ideal in a ring. Show that a field has no proper ideals.

12. Define an inductive set. Show that the set of rationals is countable, where as the set of reals is not.

13. Define a Cauchy's sequence. Show that every convergent sequence is bounded but not conversely.

14. Obtain the rearrangement of the series $1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \ldots$ which diverges to ∞ and explain.

15. State and prove the L - Hospital's rule concerning indeterminate forms. Using this evaluate $\lim_{x \to 0} \left(\frac{a^{-x} - n^{-x}}{c^{-x} - d^{-x}} \right)$, where a, b, c, d are positive and $c \neq d$.

16. State and prove Lagranges mean value theorem.

17. If $f \in R[a, b]$ and $a < b$, show that $\left| \int_a^b f(x)\, dx \right| \leq \int_a^b |f(x)|\, dx$.

18. Use Maclaurin's theorem to expand $f(x) = \sin x$.