DISTANCE LEARNING MATERIAL

VIDYASAGAR UNIVERSITY

DIRECTORATE OF DISTANCE EDUCATION

MIDNAPORE- 721 102

M. SC. IN APPLIED MATHEMATICS WITH OCEANOLOGY & COMPUTOR PROGRAMMING

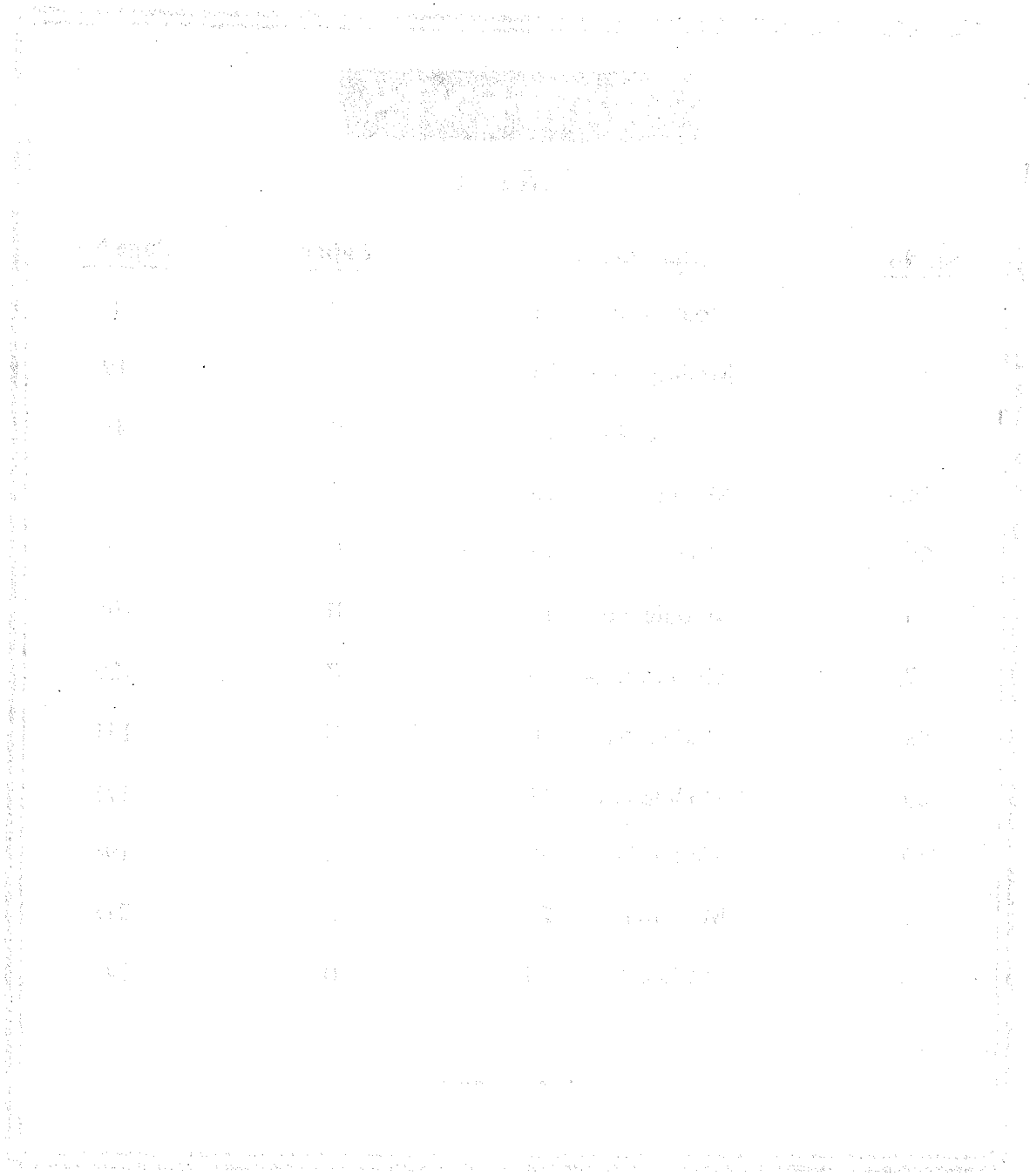
PART - I

Paper : II

Module No. : 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23 & 24

CONTENTS

PART - I



M.Sc. Course
in
Applied Mathematics with Oceanology
and
Computer Programming

PART-I

Paper-II Group-A

Module No. - 13
ALGEBRA
Graph Theory - I

CONTENT :

Objectives

1. To introduce the basic concepts of Graph Theory.
2. To discuss different aspects of connectivity of a graph.
3. To give an idea of the most important graph, tree which has a wide application area.
4. To relate connected and disconnected graphs through cutsets and cutvertices.
5. to discuss some physical problems which can be represented and solved by graph theory.

1.1 INTRODUCTION

What is a graph?

A **linear graph** (or simply a graph) G= (V,E) consists of a set of objects V= $\{v_1, v_2, \ldots\ldots\}$ called **vertices** and another set E = $\{e_1, e_2, \ldots\ldots\}$ whose elements are called **edges**, such that each edge e_k is defined with an unordered pair (v_i, v_j) of vertices. The vertices v_i, v_j associated with edge e_k are called end vertices of e_k. The most common representation of a graph is by means of a diagram, in which the vertices are represented as points and each edge as a line segment joining its end vertices.

An edge having the same vertex as both its end vertices is called a **self-loop** (or simply a loop) viz. e_1 in the fig 1. There may be more than one edge associated with a given pair of vertices for example, edge e_4,e_5 in figure 1. Such edge are referred to as **parallel edges**.

A graph that has neither self loop nor parallel edge is called a **simple** graph.

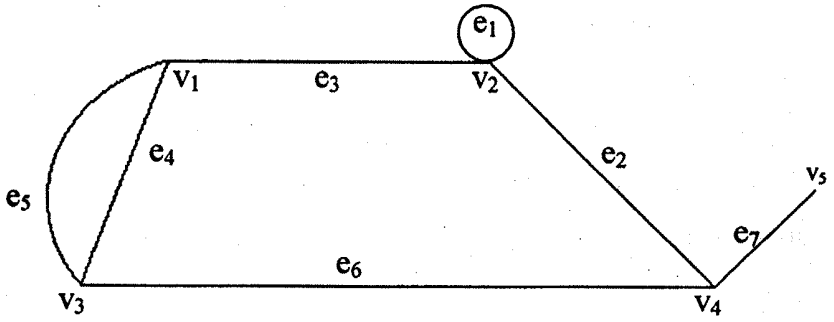


Fig.1: Graph with five vertices and seven edges

Incidence and Degree :

When a vertex v_i is an end vertex of some edge e_j, e_j is said to be incident with v_i, for example, edges e_2, e_6, & e_7 are said to be incident with vertex v_4. Two non parallel edges are said to be **adjacent** if they are incident on a common vertex. For example, e_2 & e_7 are adjacent.

Similarly, two vertices are said to be **adjacent** if they are the end vertices of the same edge. For example, v_4 & v_5 are adjacent but v_1 & v_4 are not.

The number of edges incident on a vertex v_i with self-loops counted twice is called the **degree d(v_i)** of vertex v_i.

For example, $d(v_1) = d(v_3) = d(v_4) = 3$, $d(v_2) = 4$ and $d(v_5) = 1$. The degree of a vertex is some times also refered to as its valency.

Let us now consider a graph G with e edges and n vertices $v_1, v_2, . v_n$. Since each edge contributes two degrees, the sum of the degrees of all vertices in G is twice the number of edges in G' that is

$$\sum_{i=1}^{n} d(v_i) = 2e \ldots (1.1)$$

For example for the graph in fig. 1,

$d(v_1) + d(v_2) + d(v_3) + d(v_4) + d(v_5)$

$= 3+4+3+3+1$

$=14$ = twice the number of edges.

Theorem 1.1 : The number of vertices of odd degree in a graph is always even.

Proof : If we consider the vertices with odd and even degrees separately, the quantity in the left side of (1.1) can be expressed as the sum of two sums each taken over vertices of even and odd degrees respectively, as follows:

$$\sum_{i=1}^{n} d(v_i) = \sum_{even} d(v_j) + \sum_{odd} d(v_j) \ldots\ldots (1.2)$$

Since the L. H. S of (1.2) is even and the first expression on the R. H. S is even (being a sum of even numbers), the second expression must also be even.

$$\sum_{odd} d(v_i) = \text{an even number} \ldots (1.3)$$

Because in (1.3), each $d(v_i)$ is odd, the total number of terms in the sum must be even to make the sum an even number.

Hence the theorem.•

Regular Graph : A graph in which all vertices are of equal degree is called a regular graph.

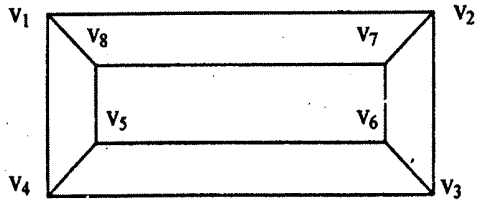


Fig. 2 : Regular Graph.

Isolated Vertex : Vertex having no incident edge is called an isolated vertex. In other words, isolated vertices are vertices of zero degree. Vertices v_4 and v_7 in fig. 3 are isolated vertices.

Pendant Vertex : A vertex of degree one in called a pendant vertex or an end vertex. Vertex v_3 is a pendant vertex in fig. 3.

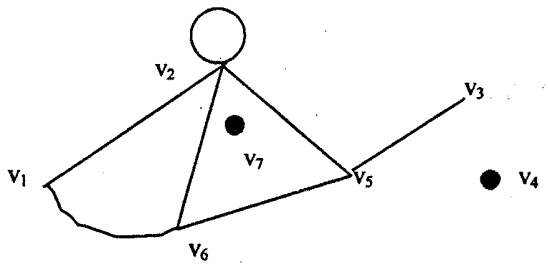


Fig. 3

Null graph : In the definition a a graph G= (V, E) it is possible for the edge set E to be empty. Such a graph without any edge is called null graph. Every vertex in a null graph is an isolated vertex.

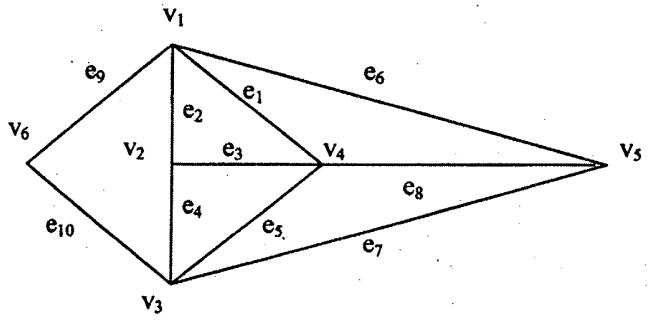
Problem 1.1 : Show that the maximum degree of any vertex in a simple graph with n vertices is (n-1).

Solution : Since the graph is a simple graph therefore no self loop and parallel edge is present in it. So in maximum case in a simple graph one vertex can be connected with the remaining vertices. So, in a simple graph with n vertices a vertex can be connected with maximum (n-1) vertices. Hence, the maximum degree of any vertex is a simple graph with n vertices is (n-1).•

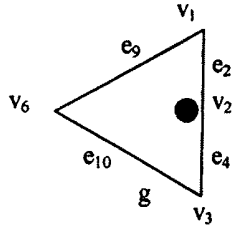
Problem 1.2 : Show that the maximum number of edges in a simple graph with n vertices is n (n-1) /2.

Solution : A simple graph has maximum number of edges only when there is an edge between every pair of vertices. Therefore out of n vertices, every two vertices can be joined in ${}^nc_2$ ways i.e., n(n-1)/2 ways. So the maximum number of edges present in a simple graph of n vertices is n(n-1)/2.•

Subgraph : A graph g is said to be a subgraph of a graph G if all the vertices and all the edges of g are in G, and each edge of g has the same end vertices in g as in G (fig. 4).



G



g

Fig. 4

Walk : A walk is defined as a finite alternating sequence of vertices and edges beginning and ending with vertices such that each edge is incident with the vertices preceding and following it. No edge appears more than once in a walk. A vertex, however, may appear more than once.

Closed Walk and Open Walk : If a walk begins and ends at the same vertex, then it is called a closed walk. A walk that is not closed is called an open walk.

Example : In the above fig.4, $v_1\ e_6\ v_5\ e_8\ v_4\ e_1\ v_1$ is a closed walk and $v_1\ e_2\ v_2\ e_3\ v_4\ e_8\ v_5$ is an open walk.

Path : An open walk in which no vertex appears more than once is called a path. A path does not intersect itself. The number of edges in a path is called the **length of a path**. In fig. 4, $v_1\ e_2\ v_2\ e_4\ v_3\ e_5\ v_4$ is a path of length 3.

Circuit : A closed walk in which no vertex (except the initial and the final vertex) appears more than once is called a circuit, ie. a circuit is a closed non-intersecting walk. e. g. in fig. 4, $v_5\ e_7\ v_3\ e_5\ v_4\ e_8\ v_5$ is a circuit of length 3.

1.2 Connectivity :

Connected Graph : A graph G is said to be **connected** if there is at least one path between every pair of vertices in G. Otherwise G is **disconnected.**

A disconnected graph consists of two or more connected subgraphs, each of which is called a **component.**

Consider a vertex v_1 in a disconnected graph G. By definition, not all vertices of G are joined by paths to v_1. Vertex v_1 and all the vertices of G that have paths to v_1 together with all the edges incident on them form a component

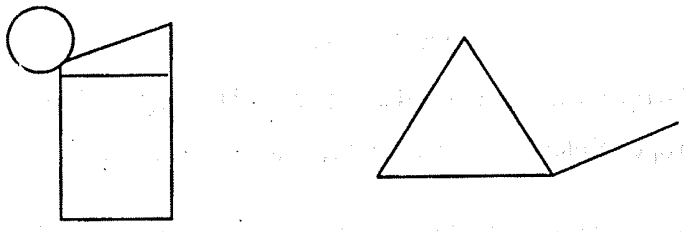


Fig. 5. A disconnected graph

Theorem 1.2 : A graph G is disconnected if and only if its vertex set V can be partitioned into two non-empty disjoint subsets V_1 and V_2 such that there exists no edge in G whose one end vertex is in subset V_1 and the other in subset V_2.

Proof : Suppose that such a partitioning exists. Consider two arbitrary vertices a and b of G, such that $a \in V_1$ and $b \in V_2$. No path can exist between vertices a and b; otherwise there would be at least one edge whose one end vertex would be in V_1 and the other in V_2. Hence if such a partition exists G is not connected.

Conversely, let G be a disconnected graph. Consider a vertex a in G. Let V_1 be the set of all vertices that are joined by paths to a. Since G is disconnected V_1 does not include all vertices of G. The remaining vertices will form a (non empty) set V_2. No vertex in V_1 is joined to any in V_2 by an edge. Hence the partition.•

Theorem 1.3 : If a graph (connected or disconnected) has exactly two vertices of odd degree, there must be a path joining these two vertices.

Proof : For a connected graph, theorem is obvious. For disconnected graph, let there be two components G_1 and G_2 respectively. Let v_1 and v_2 be the two vertices of odd degree contain G_1 and G_2 respectively. But since no graph can have an odd number of odd degree vertices. Therefore it is impossible that a component contains only one odd degree vertex. Hence, v_1 and v_2 must be in the same component and have a path between them.•

Euler Graph : If in a graph G, we can find a closed, walk running through every edge exactly once, then the graph is called an **Euler graph** and such a walk is called an **Euler line.**

Euler graph is always connected except for any isolated vertices the graph may have.

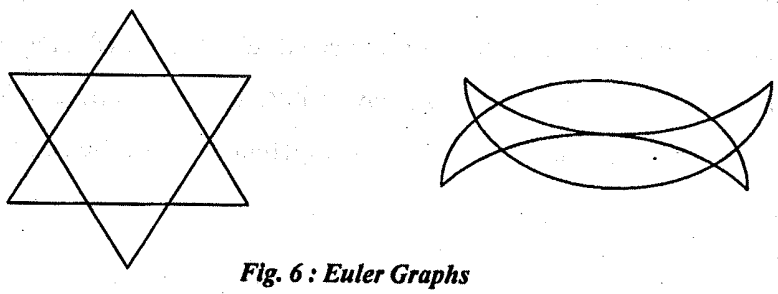


Fig. 6 : Euler Graphs

Unicursal Graph : An open walk that includes or traces all the edges of a graph without retracing any edge is called unicursal line or an open Euler line. A graph that has a unicursal line will be called a unicursal graph.

Theorem 1.4 : A given connected graph G is an Euler graph if and only if all vertices of G are of even degree.

Proof : Necessary Part :

Suppose that G is an Euler graph. It therefore contains an Euler line. While tracing this Euler line, we observe that every time the walk meets a vertex v, it goes through two "new" edges incident on v, with one we "entered" v and with the other "exited". This is true not only for all intermediate vertices of the walk but also for the terminal

vertex because we "exited" and "entered" the same vertex at the beginning and end of the walk, respectively. Thus if G is Euler graph, the degree of every vertex is even.

Sufficient Part :

To prove the sufficiency of the condition, assume that all vertices of G are of even degree. Now we construct a walk starting at an arbitrary vertex v and going through the edges of G such that no edge is traced more than once. We continue tracing as far as possible. Since every vertex is of even degree, we can exit from every vertex we enter. The tracing can not stop at any vertex but v and since v is also of even degree, shall eventually reach v when the tracing comes to an end. If this closed walk h we just traced, includes all the edges of G, G is an Euler graph. If not, we remove from G all the edges in h and obtain a subgraph h'. Since G is connected, h' must touch h at least at one vertex a. Starting from a, we can again construct a new walk in graph h' and this walk can be combined with h. This process can be repeated until we obtain a closed walk that traverses all the edges of G. Thus G is an Euler graph.•

Theorem 1.5 : A connected graph G is an Euler graph if and only if it can be decomposed into circuits.

Proof : Suppose graph G can be decomposed into edge disjoint circuits. Since the degree of every vertex in a circuit is two, the degree of every vertex in G is even. Hence G is an Euler graph.

Fig. 7

Conversely, let G be an Euler graph. Consider a vertex v_1. There are at least two edges incident on v_1. Let one of these edges be between v_1 & v_2, since vertex v_2 is also of even degree it must have at least another edge, say between v_2 and v_3. Proceeding in this fashion, we eventually arrive at a vertex that has previously been traversed, thus forming a circuit Γ. Let us remove Γ from G. All vertices in the remaining graph must also be of even degree. From the remaining graph remove another circuit in exactly the same way as we removed Γ from G. Continue this process until no edges are left. Hence the theorem.•

Application :

Königsberg Bridge Problem :

The problem is depicted in the above fig. 8. Two isolands C and D formed by the Pregel River in Königsberg (now renamed Kaliningrad) were connected to each other and to the banks A and B with seven bridges as shown in the figure. The problem was to start at any of the four land areas of the city A, B, C or D walk over each of the seven bridges exactly once and return to the starting point (with out swimming across the river, of course).

Euler represented this situation by means of a graph, as shown in the fig. 8. We find that not all its vertices are of even degree. Hence, it is not an Euler graph. Thus it is not possible to fine a closed walk containing all the bridges exactly once.

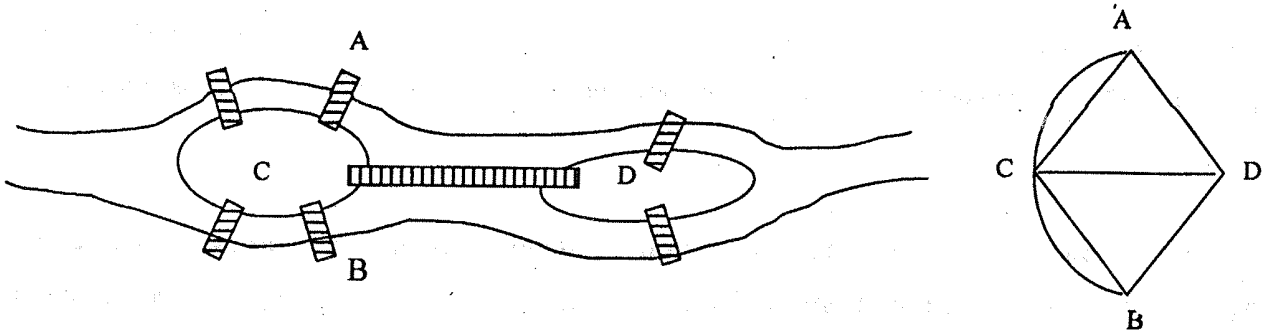


Fig. 8 : Königsberg Bridge Problem & its graph

Hamiltonian Circuit and Path :

A **Hamiltonian circuit** in a connected graph is defined as a closed walk that traverses every vertex of G exactly once, except the starting & ending vertex. If we remove any one edge from the Hamiltenian circuit we are left with a path called **Hamiltonian path** which traverses every vertex of G exactly once.

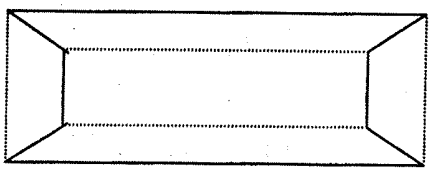


Fig. 9 : Hamiltonian Circuit

Complete graph / Universal Graph / Clique :

A simple graph, in which there exists an edge between every pair of vertices is called a complete graph or universal graph or clique.

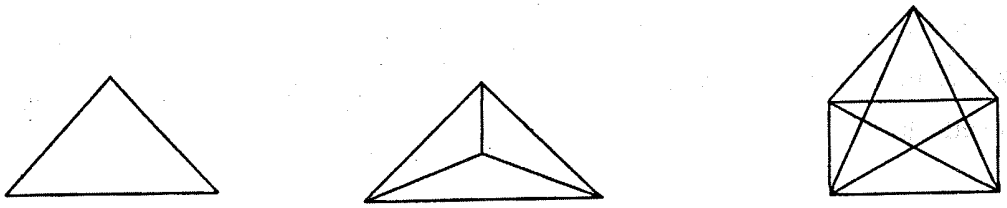


Fig. 10: Complete Graphs

Since every vertex is joined with every other vertex through one edge, the degree of every vertex is (n-1) in a complete graph G of n vertices. Also the total number of edges in G is n(n-1)/2.

It is always possible to construct a Hamiltonian circuit in a complete graph on n vertices.

Arbitrarily Traceable Graphs :

An Euler graph is said to be an arbitrarily traceable graph if every vertex v of it has the property that an Euler line is always obtained when one follows any walk form the vertex v according to the single rule that whenever one arrives at a vertex one shall select any edge which has not been previously traversed.

Fig. 11 : Arbitrarily Traceable Graph

1.3 Tree

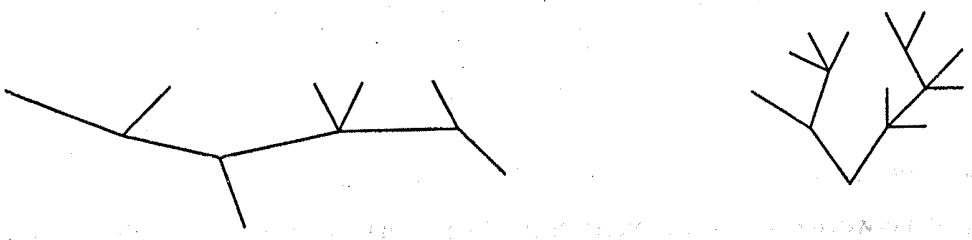


Fig. 12: Tree

Tree : A tree is a connected graph without any circuit. Tree has to be a simple graph because self loop and parallel edge both form circuits. To represent genealogy of family or a river with its tributaries and subtributaries, tree is used most effectively.

PROPERTIES :

Property 1 :There is one and only one path between every pair of vertices in a tree T.

Proof : Since T is a connected graph, there must exist at least one path between every pair of vertices in T. Now suppose that between two vertices a and b of T there are two distinct paths. The union of these two paths will contain a circuit and T can not be a tree.

Property 2 : If in a graph G there is one and only one path between every pair of vertices, then G is a tree.

Proof : Existence of a path between every pair of vertices assures that G is connected. A circuit in a graph (with two or more vertices) implies that there is at least one pair or vertices a, b such that there are two distinct paths between a and b. Since G has one and only one path between every pair of vertices, G can have no circuit, therefore, G is a tree.

Property 3 : A tree with n vertices has n-1 edges.

Proof : The theorem will be proved by induction on the number of vertices. It is easy to see that the theorem is true for n=1, 2, & 3. Assume that the theorem holds for all trees with fewer than n vertices.

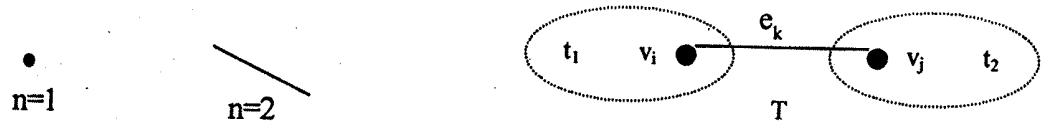


Fig. 13: Tree T with n vertices

Let us now consider a tree T with n vertices. In T let e_k be an edge with end vertices v_i and v_j. As there is one and only one path between every pair of vertices in a tree, then there is no other path between v_i & v_j except e_k. Therefore, deletion of e_k from T will disconnect the graph. Furthermore, T-e_k consists of exactly two components t_1 and t_2 and since there were no circuits in T to begin with, each of these components is a tree. Both these trees,

t_1 and t_2 have fewer that n vertices each, and therefore, by the induction hypothesis, each contains one less edge than the number of vertices in it. Thus T-e_k consists of n-2 edges (and n vertices). Hence T has (n-1) edges.

Property 4 : Any connected graph with n vertices and (n-1) edges is a tree.

Proof : Let T be a connected graph with n vertices and n-1 edges. To show that T is a tree, it is sufficient to prove that T is circuit free. Let if possible there exist a circuit with n_1 vertices where $n_1 < n$. Then there are n_1 edges in the circuit, we are left with $(n-n_1)$ vertices. Since T is connected we must have at least $(n-n_1)$ edges to connect $(n-n_1)$ vertices. Therefore total edges is $(n-n_1) + n_1 = n$ which is a contradiction. Therefore our assumption is incorrect. Hence the graph is circuit free and so it is a tree.

Property 5 : A circuit free graph with n vertices and (n-1) edges is a tree.

Proof : Let the graph be disconnected and the number of connected component be k where $k \geq 2$. Therefore each component is circuits free and connected which forms a tree.

Let components are $T_1, T_2, \ldots\ldots T_k$ contains $n_1, n_2, \ldots\ldots n_k$ no. of vertices and $e_1, e_2, \ldots\ldots e_k$ number of edges respectively.

The total number of edges

$$= e_1+e_2 +\ldots\ldots e_k$$
$$= (n_1-1)+(n_2-1) + \ldots\ldots (n_k-1)$$
$$= (n_1+n_2+ \ldots\ldots n_k) - k$$
$$= (n-k) < n-1$$

Therefore a contradiction arises. Hence the graph must be connected and so this is a tree.

Note : We may have noticed another important feature of a tree. Its vertices are connected together with the minimum number of edges. A connected graph is said to be minimally connected if removal of any one edge from it disconnects the graph. A minimally connected graph cannot have a circuit; otherwise we could remove one of the edges in the circuit and still leave the graph connected. Thus a minimally connected graph is a tree. Conversely if a connected graph G is not minimally connected, there must exist an edge e_i, in G such that G-e_i is connected. Therefore e_i is in some circuit which implies that G is not a tree.

Remark : The results of the preceding five theorems, can be summarized by saying that the following are five different but equivalent definitions of a tree i.e., a graph G with n vertices is called a tree if

1) G is connected and circuit less or
2) G is connected and has n-1 edges, or
3) G is circuitless and has n-1 edges, or
4) There is exactly one path between every pair of vertices in G, or
5) G is minimally connected graph.

Problem 1.3 : In any tree with two or more vertices there are at least two pendant vertices.

Solution : In a tree of n vertices we have (n-1) edges and hence 2(n-1) degrees to be divided among n vertices. Since no vertex can be of zero degree in a tree, so we must have at least two vertices of degree one in a tree.•

A non-pendant vertex in a tree is called an internal vertex.

Binary Tree : A binary tree is defined as a tree in which there is exactly one vertex of degree two, and each of the remaining vertices is of degree one or three. Since the vertex of degree two is distinct from all other vertices, this vertex is called a root. The binary tree is a rooted tree.

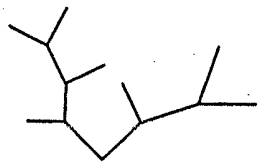


Fig. 14 : Binary Tree

Properties of binary tree :

Property 1 : The number of vertices n in a binary tree is always odd.

Proof : This is because there is exactly one vertex of even degree and the remaining (n-1) vertices are of odd degree. Since the number of vertices of odd degree in a graph is always even. So, (n-1) is even and hence n must be odd.

Property 2 : Let p be the number of pendent vertices in a binary tree T, then (n-p-1) is the number of vertices of degree three.

Therefore : [p+3(n-p-1)+2 x1] = 2(n-1)

Or, $3n - 2p - 1 = 2n - 2$

Or, $n - 2p = -1$

Or, p = n+1/2

Or, n-p = p-1

which implies that **the number of internal vertices in a binary tree is one less than the number of pendant vertices.**

Spanning Trees : A tree T is said to be a spanning tree of a connected graph G if T is a subgraph of G and T contains all vertices of G.

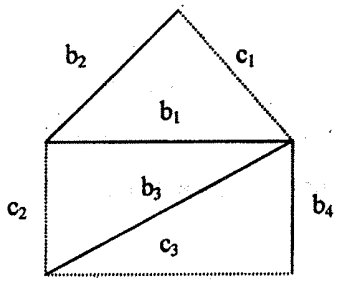


Fig. 15: Spanning Tree

We can find a spanning tree from each component of a disconnected graph. Thus a disconnected graph with k components has **spanning forest** consisting of k spanning tree.

Branch and Chord : The edges of the connected graph which are present in a spanning tree are called branches of a tree.

The edges of the connected graph which are not present in a spanning tree are called chords. See fig. 15 for example, $\{b_1, b_2, b_3, b_4\}$ are branches and $\{c_1, c_2, c_3\}$ are chords.

Theorem 1.6 : Every connected graph has at least one spanning tree.

Proof : To trace out a spanning tree, we start from any vertex whenever we come across a circuit, we delete any of the edges of the circuit. Thus we get at least one spanning tree.•

Fundamental Circuits : Addition of any chord to the spanning tree will create a circuit called fundamental circuit.

In fig. 15, $\{b_1, b_2, b_3, b_4\}$ is the spanning tree. Adding c_3 we get a fundamental circuit. $\{b_3, b_4, c_3\}$.

Distance and Centre : In a connected graph G the distance $d(v_i, v_j)$ between two of its vertices v_i & v_j is the length of the shortest path (i.e., the number of edges in the shortest path) between them.

Distance between vertices of a connected graph is a **metric.**

The **eccentricity E(v)** of the vertex v in a graph G is the distance from v to the vertex furthest from v in G.

i.e., $E(v) = \max_{v_i \in G} \{d(v,v_i)\}$

A vertex with minimum ecentricity in graph is called **centre** of G.

Theorem 1.7 : Every three has either one or two centres.

Radius & Diameter : The eccentricity of a centre (which is the distance from the centre of the tree to the furthest vertex) in a tree is defined as the radius of the tree.

The diameter of a tree T is defined as the length of the longest path in T.

Rank : Rank of a graph denoted by r and defined by **r = n-k** where n is the number of vertices & k is the number of components. Since each component contains at least one vertex, $n \geq k$.

Hence $r = n-k \geq 0$.

Again each component is connected and tree is a minimally connected graph. So, if e be the number of edges of a graph, then $e \geq n-k$

i.e., $e-n+k \geq 0$.

Hence, we define **nullity = μ = e-n+k**

Rank of G is the number of branches in any spanning tree or forest of G.

Nullity of G is the number of chords in G and rank + nullity = number of edges in G

1.4 Cut Sets and Cut Vertices :

Cut Sets: In a connected graph G, a cutset is a set of edges whose removal from G leaves G disconnected, provided removal of no proper subset of these edges disconnects G.

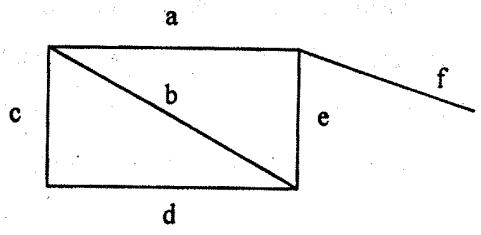


Fig. 16

In fig. 16, the set of edges {a, b, d}, {a, b, c}, {a, e}, {f} are cutsets.

Since removal of any edge from a tree breaks the tree into two parts. Every edge of a tree is a cutset. Number of cutset in a tree with n vertices in (n-1).

Connectivity and Separability :

Edge connectivity : The number of edges in the smallest cutset (i.e., cutset with fewest number of edges) is defined as the edge connectivity of G, i.e., the edge connectivity of a connected graph can be defined as the minimum number of edges whose removal or deletion makes the graph disconnected. The edge connectivity of a tree is one.

Vertex Connectivity : The vertex connectivity of a connected graph G is defined as the minimum number of vertices whose removal from G leaves the remaining graph disconnected.

Separable Graph : A connected graph is said to be separable if its vertex connectivity is one. All other connected graph are called non-seperable. e.g., a tree is a separable graph. A separable graph consists of two or more non separable subgraphs. Each of the largest non-separable subgraph is called a block. A non separable connected graph consists of just one block.

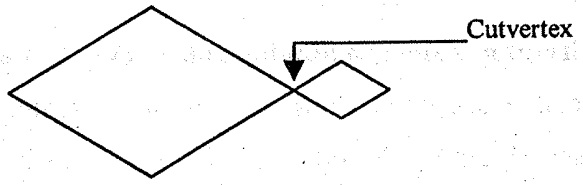


Fig. 17: Separable Graph

Cut Vertex: In a Separable graph a vertex whose removal disconnects the graph is called a cut vertex, cut-node or an articulation point.

Theorem 1.8 : The edge connectivity of a graph G cannot exceed the degree of the vertex of the smallest degree in G.

Proof : Let vertex v_i be the vertex with the smallest degree in G. Let $d(v_i)$ be the degree of v_i. Vertex vi can be separated from G by removing the $d(v_i)$ edges incident on vertex v_i. Hence the theorem.•

Theorem 1.9 : The vertex connectivity of any graph G can never exceed the edge connectivity of G.

Proof: Let r denote the edge connectivity of G. Therefore, there exists a cutest S in G with r edges. Let S partition the vertices of G into subsets V_1 and V_2. By removing at most r vertices from V_1 (or V_2) on which the edges in S are incident, we can effect the removal of at least S from G. Hence the theorem.•

Theorem 1.10 : Every cutset in a connected graph G must contain at least one branch of every spanning tree of G.

Proof : Let the spanning trees of G are $T_1, T_2, \ldots\ldots, T_p$ and S_1 be of cutset. Let there be no common edges between T_1 & S_1.Then removal of S_1 from G does not effect T_1 which means that removal of S_1 does not make G disconnected. This contradiction proves the theorem.•

Theorem 1.11 : In a connected graph G, any minimal set of edges containing at least one branch of every spanning tree of G is a cutset.

Proof : Let Q be the set containing at least one branch of every spanning tree of G. Since in (G-Q) we cannot get any spanning tree of G, (G-Q) must be disconnected. Further, addition of any one edge of Q in (G-Q) will create at least one spanning tree. Therefore Q is the minimal set of edges whose removal from G disconnects G. Hence Q is a cutset.•

Theorem 1.12 : Every circuit has an even numbers of edges in common with any cut set.

Proof : Let G be a connected graph. Consider a cutest S in graph G. Let the removal of S partition the vertices of G into two subsets V_1 and V_2. Consider a circuit Γ in G. If all the vertices in Γ are entirely within vertex set V_1 (or V_2), the number of edges common to S and Γ is zero an even number.

If on the other hand, some vertices of Γ are in V_1 and some in V_2, we traverse back and forth between the sets V_1 and V_2 as we traverse the circuit. Because of the closed nature of a circuit, the number of edges we traverse between V_1 and V_2 are even.•

Fundamental Cut-Sets: Let T be a spanning tree of a connected graph G. Take any branch b in T. Removal of b makes T disconnected. Consider the same partition of vertices in G and the cutset S in G that corresponds to this partition. Then cutset S will contain only one branch of T and some of the chords of T. Such a cutset S is known as fundamental cutset with respect to T. Every branch of spanning tree will give unique fundamental cut set.

Fundamental Cutsets with respect to T= $\{e_7, e_9, e_2, e_6, e_4\}$ of fig. 18 are as follows

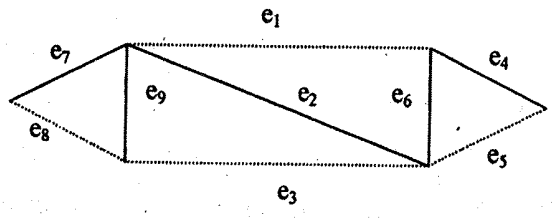


Fig. 18

from e_9 : $\{e_9, e_8, e_3\}$,

from e_2 : $\{e_1, e_2, e_3\}$,

from e_7 : $\{e_7, e_8\}$,

from e_4 : $\{e_4, e_5\}$,

from e_6 : $\{e_1, e_6, e_5\}$.

Theorem 1.13 : With respect to a given spanning tree a chord c_i that determines a fundamental circuit Γ occurs in every fundamental cut-set associated with the branches in Γ and in no other.

Proof: Let T be the given spanning tree of a graph G. Then let fundamental circuit Γ made by the chord c_i contains k branches $b_1, b_2, \ldots b_k$ i.e. $\Gamma = \{c_i, b_1, b_2, \ldots, b_k\}$

Let Sj be the fundamental cut set, determined by branch bj, j= 1, 2, 3, ..., k.

$\therefore$ Sj = $\{ b_j, c_1, c_2, \ldots c_q\}$, $c_1, c_2, \ldots c_q$ are chords.

The edge b_j is common in Γ & S_j

By the previous theorem Γ & S_j must have an even number of common edges but $c_1, c_2, \ldots c_q$ cannot be common to $b_1, b_2, \ldots b_k$. Therefore c_i must be one of $c_1, c_2, \ldots c_q$ i.e., c_i is included in every cutset corresponding to branches in Γ.

Let us consider another cutset which is defined by b_{k+1}, S= $\{b_{k+1}, c_1', c_2', \ldots c_p'\}$. If c_i is common in Γ & S' then b_{k+1} must be one of $b_1, b_2, \ldots b_k$ to make the number of common edges even which is a contradiction. Therefore c_i cannot be included in any cutset corresponding to branches of tree other than those in Γ.•

Complement : Complement of a simple graph with n vertices is defined to be its complement with respect to the complete graph Kn and is denoted by G' or $\overline{G}$

Clearly G U $\overline{G}$ = K_n

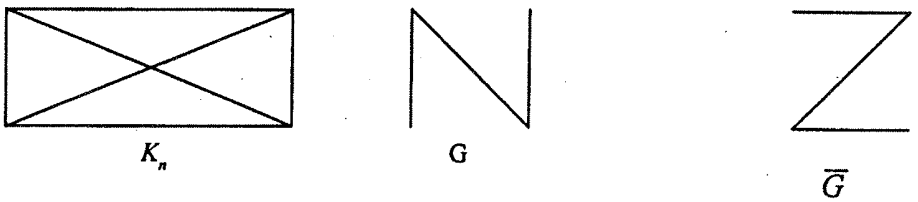


Fig: 19

Summary :

Graphs can be used to represent almost any problem involving discrete arrangements of objects, where concern is not with the internal properties of these objects, but with the relationships among them. Particularly, trees form the most important topic in graph theory. Different types of trees together with their properties and applications are discussed. In contrast to a spanning tree (which keeps the vertices together), a cutset separates the vertices. Consequently, there is bound to be a close relationship between the two, which is described, here by some theorems.

Exercise :

1. Show tree in which its diameter is not equal to twice the radius. Under what condition does this inequality hold? Elaborate.
2. Show that a path is its own spanning tree.
3. Write down all possible disconnected graph on four vertices? Find the number of components in each case.
4. Prove that any subgraph g of a connected graph G is contained in some spanning tree of G if and only if g contains no circuit.
5. Show that if G is a tree, and all the degrees of vertices in G are odd, then the number of edges is odd.
6. Show that the graph of a rhombic dodecahedron (with eight vertices of degree three and six vertices of degree four) has no Hamiltonian path (and therefore no Hamiltonian circuit).
7. Determine the number of vertices and edges in a tree consisting of 2n pendant vertices, 3n vertices of degree 2 and n vertices of degree 3.
8. How many cut vertices a binary tree on 2n+ 1 vertices may have? Justify you answer.

- - - - - 0 - - - - -

M.Sc. Course
in
Applied Mathematics with Oceanology
and
Computer Programming

PART-I

Paper-II Group-A

Module No. - 14
ALGEBRA
Graph Theory - II

CONTENT :

Objectives

1. To introduce the concept of planarity and other related topics which are of great significance.
2. To give an idea of different types of isomorphisms used in graph theory.
3. To develop the concept of proper colouring of the vertices of a graph and the concept of matching, both of which have great significance in practical life.
4. To discuss about the directed graphs-graphs in which edges have directions.
5. To demonstrate the use of matrices in studying graphs.
6. To use the high-speed electronic computers in solving graph-theoretic problems.

2.1 Planar graph and non planar graph:

Planar Graph : A graph G is said to be planar if there exists some geometric representation of G which can be drawn on a plane such that no two of its edges intersect. A graph G is said to be a planar graph if it can be represent on a plane such that no two edge of g intersect except at the vertices. A graph that cannot be drawn on a plane without a crossover between its edges is called **non planar**. Note that the "meeting' of edges at vertex is not considered as intersection.

Embedding : A drawing of a geometric representation of a graph on any surface such that no edges interest is call embedding.

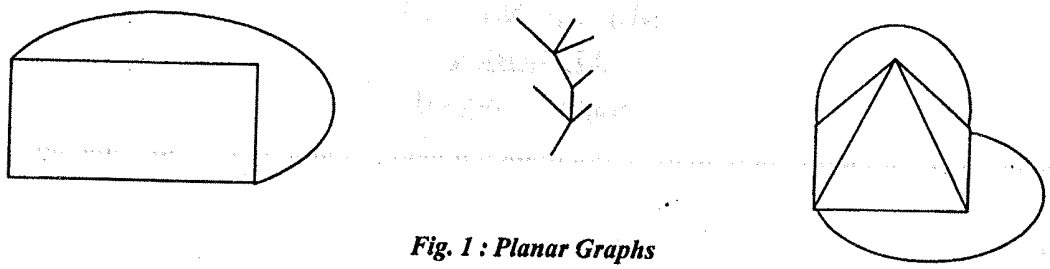


Fig. 1 : Planar Graphs

Thus to declare that graph G is non planar, we have to show that of all possible geometric representation of G none can be embedded in a plane.

A geometric graph G is planar if there exists a graph isomorphic to G that is embedded in a plane otherwise G is non planner. An embedding of a planar graph G on a plane is called a plane representation of G.

Kuratowski's Graphs: A natural question is now that how we tell if a graph G is planar or non planar? To answer this question let us discuss the graphs of fundamental importance. These are called Kuratowski's graph after the polish mathmatician Kasimir Kuratowski who discovered their unique property.

Type - I : K_5, the complete with five vertices.

Type - II : $K_{3,3}$, the utility graph involving three households H_1, H_2, H_3 and three services viz. Gas, water and electricity essential to all the houses.

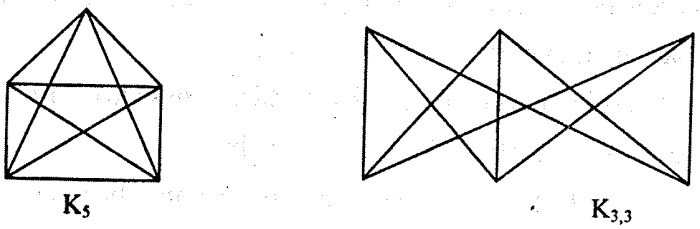


Fig. 2: Non planar Graphs

Properties :

i) Both K_5 and $K_{3,3}$ are regular and non planar graphs.

ii) Removal of one edge or a vertex makes each, a planar graph.

iii) Kuratowski's first graph K_5 is the non planar graph with the smallest number of vertices and Kuratowski's second graph $K_{3,3}$ is the non-planar graph with the smallest number of edges. Thus both are the simplest non planar graphs.

Region : A region is an area of a planar graph bounded by the edges such that the area cannot be subdivided. Region is also called window, mesh or face.

The plane lying outside a graph (region 5 of the fig. 3) is called the infinite, exterior region.

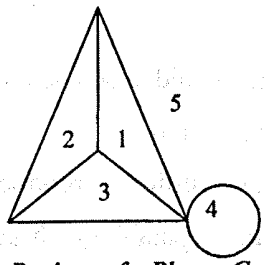


Fig. 3: Regions of a Planar Graph.

2.2 Isomorphic Graphs :

Two graphs G and G′ are said to be isomorphic to each other if there is a one to one correspondence between their vertices and between edges such that incidence relationship is preserved. In other words suppose that the edge e is incident on vertices v_1 & v_2 in G then the corresponding edge e′ of G′ must be incident on the vertices v_1' & v_2' that correspond to v_1 & v_2 respectively.

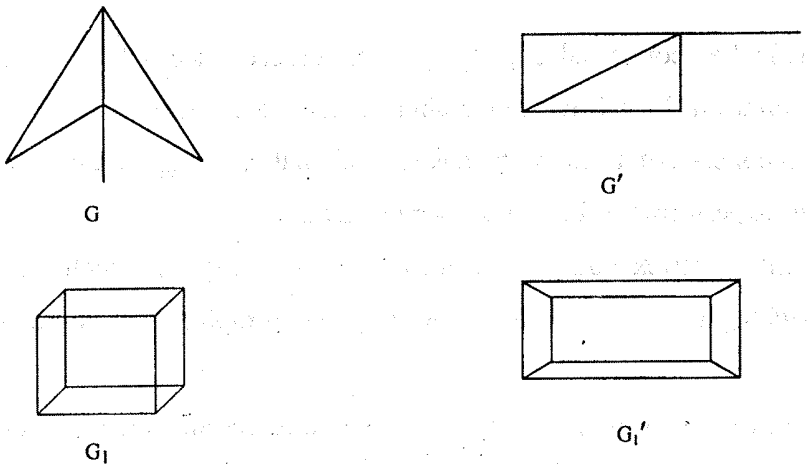


Fig. 4: Isomorphic Graphs

Homeomorphic Graphs : Two graphs are said to be homeomorphic if one graph can be obtained from the other by the creation of edges in series (i.e., by insertion of vertices of degree two) or by the merger of edge in series (i.e., deletion of vertices of degree two). A graph is planar if and only if every graph that is homeomorphic to G is planar.

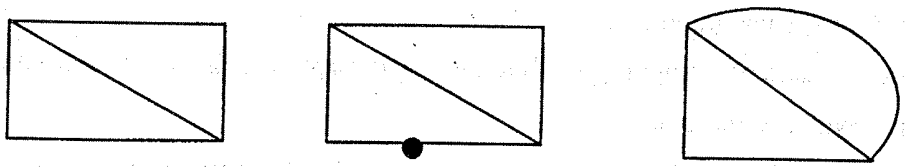


Fig. 5: Homeomorphic Graphs

1-Isomorphism : Two graphs G_1 & G_2 are said to be 1-isomorphic if they become isomorphic to each other under repeated application of the following operation.

Operation-1 : Split a cut vertex into two vertices to produce two disjoint subgraphs.

From this definition it follows that two non separable graph are 1 isomorphic if and only if they are isomorphic.

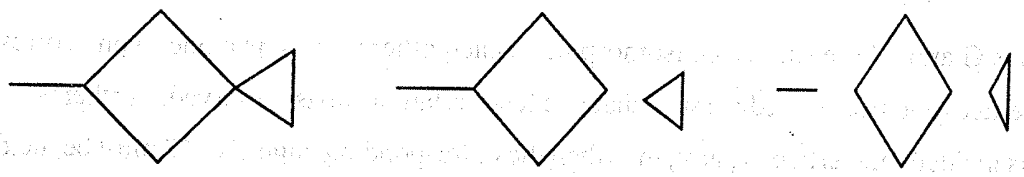


Fig. 6: 1-Isomorphic Graphs

2-Isomorphism : In the 2 connected graph (graph with vertex connectivity 2) G, let vertices x & y be a pair of vertices whose removal from G will leave the remaining graph disconnected.

In other words, G consists of a subgraph, g_1 & $g_{1,}$ such that g_1 and g_1 have exactly two vertices x & y in common. Suppose that we perform the following operation 2 on G.

Operation 2 : Split the vertex x into x_1 & x_2 and the vertex y into y_1 & y_2 such that G is split into g_1 and g_1. Let vertices x_1 & y_1 go with g_1 and x_2 & y_2 with g_1. Now we join the graph g_1 & g_1 by merging x_1 with y_2 & x_2 with y_1.

Two graphs are said to be 2-isomorphic if they become isomorphic after undergoing operation 1 or operation 2 or both the operations any number of times.

Isomorphic graphs are always 1-isomorphic and 1-isomorphic graphs are always 2-isomorphic, but the converse is not true.

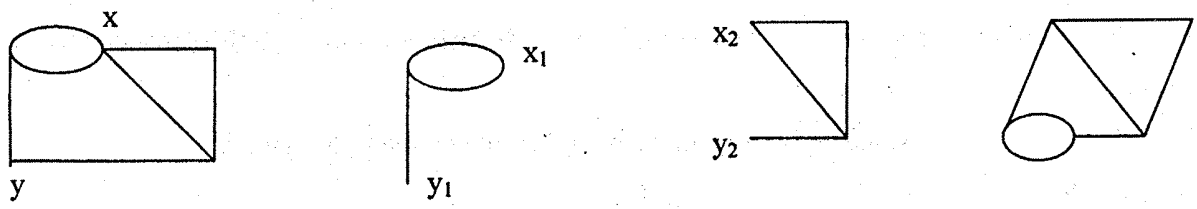


Fig. 7: 2-Isomorphic Graphs

Theorem 2.1 : A necessary and sufficient condition for a graph G to be planar is that G does not contain either of Kurotowski's two graphs or any graph homeomorphic to either of them.

Euler's Theorem 2.2 : A connected planar graph with n vertices and e edges has e-n+2 regions, i.e., the number of regions f= e-n+2 or, n-e+f = 2.

Proof: The theorem will be proved by induction on the number of edges e of G.

For e = 0 we get n=1, f = 1, n-e+f = 2

For e = 1 we get n=1, f = 2, n-e+f = 2

For e = 0 we get n=2, f = 1, n-e+f = 2

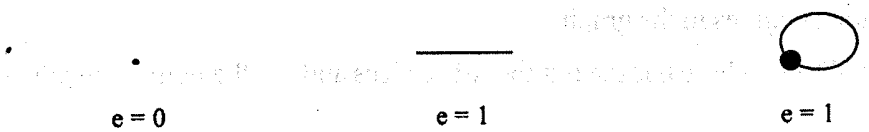


Fig. 8: Connected Graphs

Let the theorem be true for all graphs with at most (e-1) edges and G be a graph with e edges, n vertices and fregions.

If G is a tree, then e = n-1, f = 1, n-e+f = n-n+1+f = 2.

If G is not a tree, let e_1 be an edge contained in some circuit in G then $G - e_1$ is a planar connected graph with n vertices, (e-1) edges and (f-1) regions. So by induction hypothesis we have, n-(e-1)+(f-1) = 2

or, n-e+f = 2

Therefore the therem holds good for G.•

Simple connected planar graph :

In a simple planar connected graph non-existence of self loop or parallel edge, implies that the number of edges of the boundary of a region must be at least three.

Let T be the total number of edges of the boundaries of all the regions in a simple planar connected graph with f regions.

$T \geq 3f$ and also $T \leq 2e$, since every edge in the boundary of at most two regions.

$3f \leq T \leq 2e$

$\therefore 3f \leq 2e \Rightarrow e \geq 3f/2$

Also we know, $f = e-n+2$

$\therefore 3e - 3n + 6 \leq 2e$

i.e., $e \leq 3n - 6$

which is a necessary condition for simple planar connected graph, but not sufficient.

In the case of K_5, the complete graph of five vertices, $n=5$, $e=10$, $3n-6=9<e$. Thus the graph violets inequality and hence it is not planar.

Kuratowski's $K_{3,3}$ satisfies the inequality because $e=9$, $3n-6 = 3 \times 6-6$ yet the graph is non-planar.

Problem 2.1 : Show that a simple planar graph has at least a vertex of degree 5 or less.

Solution: If the graph is disconnected, we consider one connected component of it and proceed.

Let, if possible, the graph has the vertices, all of which are of degree 6 at least.

Let T be the total degrees in the graph.

$\therefore T = 2e$ and $T \geq 6n$, where n is the number of vertices and e is the number of edges.

or, $2e \geq 6n$

or, $e \geq 3n$.

But for a simple connected graph $e \leq 3n-6$. This contradiction disproves the assumption.•

Problem 2.2 : Show that in a connected simple planar graph with 6 vertices and 12 edges each of the regions is bounded by three edges.

Solution: Here $n=6$, $e=12$, then $n-e+f=2$ gives $f=8$

i.e., total no. of regions in the graph is 8.

Since the graph is connected simple planar, no selfloop, parallel edge is present in the graph. Therefore at least 3 edges are in the boundary of a region.

Let, there be at least one region bounded by four edges, other 7 regions by 3 edges.

Total no. of edges in the boundary, T=7 x 3 + 4 = 21 + 4 =25

Again $T \leq 2e \Rightarrow 2.12 = 24$

which is a contradiction. So each region is the graph bounded by 3 edges.•

Geometrical Dual : Consider the plane representation of a graph with f regions. Let us place F points F_1, F_2, ... F_f one in each of the regions. Next let us join these F points according to the following procedure:

If two regions i & j are adjacent draw a line joining points F_i and F_j that intersect the common edge between i and j th region exactly once. If there is more than one common edge draw one line for each of the common edges. For an edge e lying entirely in one region say F_k draw a selfloop at point F_k intersecting e exactly once. By this procedure we obtain a new graph G* consisting of f vertices F_1, F_2, ... F_f and of edges joining these vertices. Such a graph G* is called a dual of G.

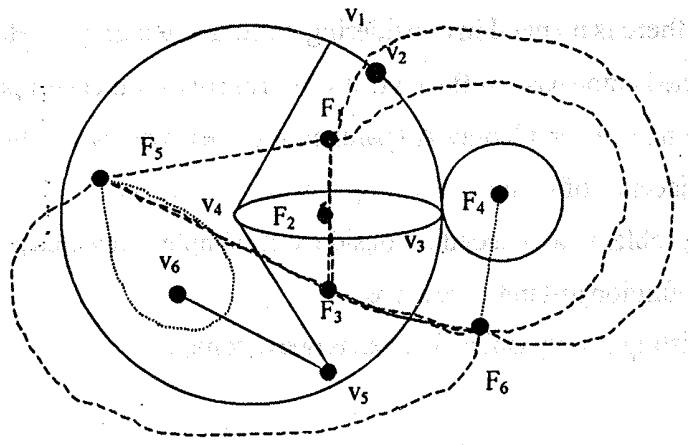


Fig. 9: Dual

Properties :

i) An edge forming a selfloop in G gives a pendant edge in G*.

ii) An pendant edge in G gives a self loop of G*.

iii) Edges in series in G produce parallel edges in G*.

iv) Parallel edges in G produce edges in series in G*.

v) The number of edges constituting the boundary of a region i in G is equal to the degree of the corresponding vertex F_i in G* and vice versa.

vi) The graph G* is also planar.

vii) G* and G are dual graph.

viii) If n, e, f, r, μ be the number of vertices, edges, regions, rank and nullity of G respectively and n*, e*, f*, r*, μ* be the corresponding quantities in G* then n* = f, e* =e, f* = n, r* =μ, μ*=r.

Self Dual Graph : If a planar graph G is isomorphic to its own dual it is called a self dual graph.

Theorem 2.3 : A graph has dual if & only if it is planar.

2.3 Colouring and Matching :

Chromatic number : Minimum number of colours required to colour the vertices of a graph properly (i.e., no two adjacent vertices are of the same colour) is called the chromatic number of the graph. A graph G that requires k different colours for its proper colouring is called a k chromatic graph and the number k is called the chromatic number of G.

In colouring graph there is no need in considering disconnected graphs. How we colour vertices in one component of a disconnected graph has no effect on the colouring of the other components. Therefore it is usual to investigate colouring of connected graph only. All parallel edges between two vertices can be replaced by a single edge without effecting adjacency of vertices. Selfloop may be disregarded.

Thus for colouring problems we needed to consider only simple connected graphs. Some observations that follow directly from the definition just introduced are

1) A graph consisting of only isolated vertex is one chromatic.

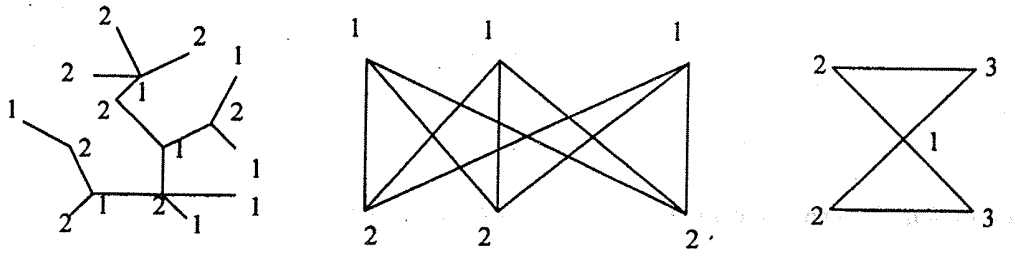


Fig. 10: Colouring of Graphs

2) A graph with one or more edges (not a selfloop) is at least 2 chromatic.
3) A complete graph of n vertices is n chromatic as all its vertices are adjacent. Hence a graph containing a complete graph of r vertices, is at least 3 chromatic.
4) A graph consisting of simply one circuit with $n \geq 3$ vertices is 2 chromatic if n is even and 3 chromatic if n is odd.

Theorem 2.4 : Every tree with two or more vertices is two chromatic.

Proof: Select any vertex v in the tree T. Paint v with colour 1. Paint all vertices adjacent to v with colour 2. Next paint all vertices adjacent to these (those that just have been colored with 2) using colour 1. Continue this process till every vertex in T has been painted. Now in T we find that al vertices at odd distance from v have colour 2 while v and verities of even distance form v have colour 1. Now along any path in T the vertices are of alternating colour. Since there is one and only one path between any two vertices in a tree, no two adjacent vertices have the same colour. Thus T has been coloured with two colours.•

Though a tree is 2 chromatic not every 2 chromatic graph is a tree (the utility graph, for instance, is not a tree. But is 2 chromatic).

Bipartite Graph : A graph G is called bipartite if its vertex set V can be decomposed into two disjoint subsets V_1 & V_2 such that every edge in G joints a vertex in V_1 with a vertex in V_2. Obviously a bipartite graph can have no self-loop. A set of parallel edges between a pair of vertices can all be replaced with one edge without affecting bipartiteness of graph.

Clearly every 2 chromatic graph is bipartite because the colouring partitions the vertex set into the subsets V_1 and V_2 such that no two vertex in V_1 (or V_2) are adjacent.

Similarly, every bipartite graph 2 chromatic with one trivial exception. A graph of two or more isolated vertices and with no edges is bipartite but is one chromatic.

Theorem 2.5 : If G (V_1, V_2) is a bipartite graph then every circuit of it (if exists) has even length.

Proof: Let $v_1 \to v_2 \to v_3 \ldots v_m \to v_1$ be a circuit in G (V_1, V_2) and without loss of generality, assume that $v_1 \in V_1$. Then since G (V_1, V_2) is bipartite, $v_2 \in V_2$ and by the same agreement $v_3 \in V_1$ and so on. It follows that $v_m \in V_2$ and hence the circuit has even length.•

Chromatic Polynomial : A given graph G of n vertices can be properly coloured in many different ways using a sufficiently by large number of colours. This property of a graph is expressed by means of a polynomial

called chromatic polynomial of G and is defined as a polynomial in λ, $P_n(\lambda)$ which gives the number of ways of properly colouring a graph G with n vertices using λ or fewer colours.

Let c_i be the number of different ways of properly colouring G using exactly i colours. There are ${}^{\lambda}c_i$ be the different ways of selecting exactly i colours out of λ colours. Since i can be any positive integer from 1 to n, the chromatic polynomial is given by

$$P_n(\lambda) = \sum_{i-1}^{\lambda} c_i \left(\frac{\lambda}{i}\right) = \sum_{i=k}^{\lambda} \left(\frac{\lambda}{i}\right) c_i$$

Where k is the chromatic number of the graph G. Each c_i has to be evaluated individually for the given graph.

Theorem : 2.6 : A graph of n vertices is a complete graph iff its chromatic polynomial is $P_n(\lambda) = \lambda(\lambda-1)(\lambda-2)\ldots(\lambda-n+1)$.

Proof : With λ colours, there are λ different ways of colouring any selected vertex of a graph. A second vertex can be coloured properly in exactly $(\lambda-1)$ ways, the third in $(\lambda-2)$ ways, the fourth in $(\lambda-3)$ ways ..... and the nth in $(\lambda-n+1)$ ways iff every vertex is adjacent to every other. That is, iff the graph is complete.•

Properties : Let G be a graph with n vertices e edges and k components $G_1, G_2, \ldots G_x$. Then

i) $P_n(\lambda)$ is of degree n.

ii) The co-efficient of λ^n in $P_n(\lambda)$ is 1.

iii) The co-efficient of λ^{n-1} in $P_n(\lambda)$ is (-e).

iv) The constant term of $P_n(\lambda)$ is zero.

v) $P_n(\lambda) = \prod_{i=1}^{k} Pn_i(\lambda)$ where n_i is the number of vertices in the component of G_i.

vi) The smallest exponent of λ in $P_n(\lambda)$ with the non-zero co-efficient is k where k is the number of components of G.

Theorem 2.7 : A n vertices graph is a tree iff its chromatic polynomial
$P_n(\lambda) = \lambda(\lambda-1)^{n-1}$.

Proof : Necessary Part.

(By mathematical induction on n)

$P_1(\lambda) = \lambda$

$P_2(\lambda) = \lambda(\lambda-1)$

Let it be true for a tree T with less than n vertices. Let v be a pendant vertex of T. Deleting v we get a tree T with (n-1) vertices. Therefore, its chromatic polynomial is

$P_{n-1}(\lambda) = \lambda(\lambda-1)^{n-2}$.

Now add v and since it has only one adjacent vertex, we have $(\lambda-1)$ colours in hand to colour v. We can not use the only one colour by which the said adjacent vertex has been coloured.

$P_n(\lambda) = \lambda(\lambda-1)^{n-2}(\lambda-1)$

$= \lambda(\lambda-1)^{n-1}$

Sufficient Part :

Since co-efficient of λ in $P_n(\lambda)$ is one, T is connected by property (vi) i.e., the smallest exponent of λ in $P_n(\lambda)$ with the non-zero co-efficient is the number of components present in the graph and the co-efficient of λ^{n-1} is -(n-1) so that T has (n-1) edges by the property (iii) that the co-efficient of λ^{n-1} in $P_n(\lambda)$ is negative of the number of edges present in the graph. Hence T is a tree.•

Theorem 2.8 : The vertices of every planar graph can be properly coloured with five colours.

Proof: Let n be the number of vertices of the given graph. For n = 1, 2, 3, 4, 5 the theorem holds obviously. Let us assume that the theorem is true for a graph with less than n vertices. Now we consider a graph G with n vertices.

G has at least one vertex v having less than or equal to five degrees. Select the vertex v and delete it from G. Then (G-v) can be coloured properly with five colours by our assumption. Now we insert v. If d(v) =1 or 2 or 3 or 4, then we can colour it easily. When d(v) =5 let all the colours have been used to colour the vertices adjacent to v.

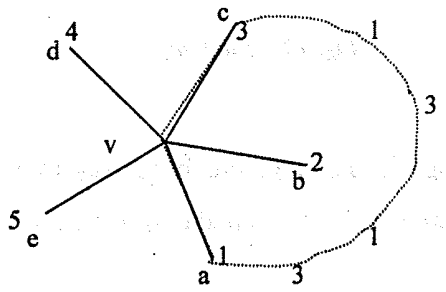


Fig. 11

Suppose that there is a path in G' = G-v between vertices 'a' and 'c' coloured alternately with colours 1 and 3. Then a similar path between b and d coloured alternately with colours 2 and 4 can not exist, since it will make G non-planar.

If there is no path between b and d coloured alternately with colours 2 and 4, starting from vertex b, we can interchange colours 2 and 4 of all vertices connected to b through vertices of alternating colour 2 and 4. This interchange will paint vertex b with colour 4 and yet keep G' properly coloured.

Since vertex d is still with colour 4 we have colour 2 left with which the vertex v can be coloured.

If there is no path between a and c of vertices painted alternately with colour 1 and 3, we could have released colour 1 or 3 to paint v. Hence the theorem.•

Four Colour Theorem : Every planar graph has a chromatic number of four or less.
[proved by Appel and Haken using large sale computers in 1976]

Matching : A matching in a graph is a subset of edges in which no two edges are adjacent.

Maximum Matching : Maximum matching is a matching to which no edge of the graph can be added.

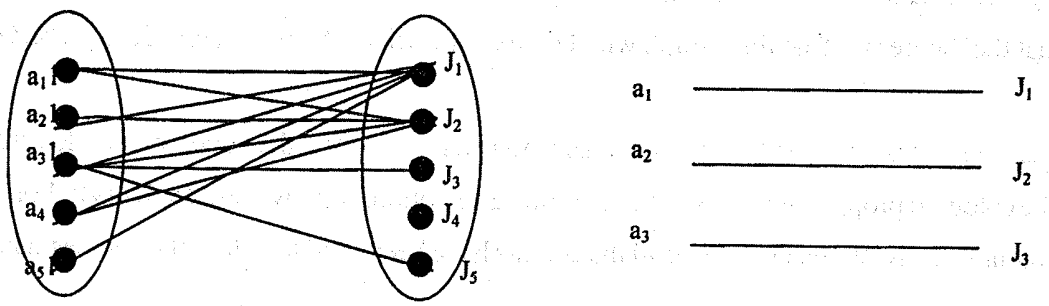


Fig. 12: Matching

Among these the maximum matching with the largest number of edges are called **largest maximum matching.** The number of edges in a largest maximum matching is called **matching number** of the graph.

Complete matching : In a bipartite graph having a vertex partition V_1 and V_2 a complete matching of vertices in set V_1 into those in V_2 is a matching in which there is one edge incident with every vertex in V_1 i.e., every vertex in V_1 is matched against some vertex in V_2.

Theorem 2.9 : A complete matching of V_1 and V_2 in a bipartite graph exists if and only if every subset of r vertices in V_1 collectively adjacent to r or more vertices in V_2 for all values of r.

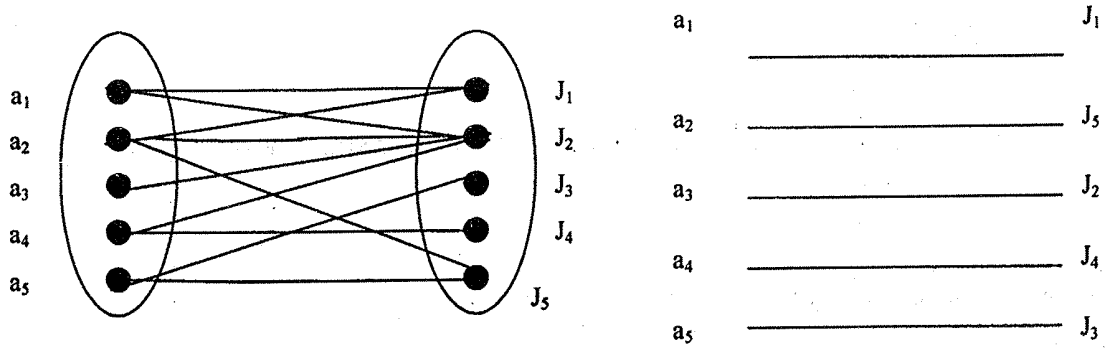


Fig. 13: Complete matching

2.4 Directed Graph :

Digraph : A directed graph (or a digraph) G consists of a set of vertices $V = \{v_1, v_2 \ldots\}$ a set of edges $E = \{e_1, e_2, \ldots.\}$ and a mapping that maps every edge onto some ordered pair of vertices (v_i, v_j). As in the case of undirected graph, a vertex is represented by a point and an edge by a line segment between v_i and v_j with an arrow directed from v_i to v_j.

The number of edges incident out of a vertex v_i called the **out degree** of v_i and is written as $d^+(v_i)$. The number of edges incident into v_i is called the **in degree** of v_i and is written as $d^-(v_i)$.

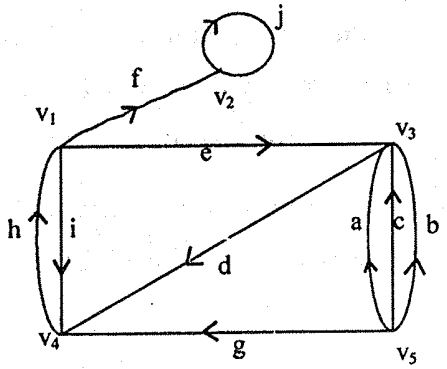


Fig. 14: Digraph

From the figure 14,

$d^+(v_1) = 3, d^-(v_1) = 1$

$d^+(v_2) = 1, d^-(v_2) = 2$

$d^+(v_5) = 4, d^-(v_5) = 0$

In any digraph G the sum of all in degree is equal to the sum of all out degrees, each sum being equal to the number of edges in G.

$$i.e., \sum_{i=1}^{n} d^{-}(v_i) = \sum_{i=1}^{n} d^{+}(v_i) = e$$

Isolated Vertex : An isolated vertex is a vertex in which the in degree and the out degree are both equal to zero,

i.e., $d^{+}(v_i) = 0 = d^{-}(v_i)$.

Pendant vertex : A vertex v in a digraph is called pendant vertex if

$d^{+}(v) + d^{-}(v) = 1$.

Parallel edge : Two directed edges are said to be parallel if they are mapped onto the same ordered pair of vertices. In the above Fig. 14, a, b, and c are parallel.

Simple Digraph : A digraph that has no selfloop or parallel edge is called a simple graph.

Asymmetric Digraph : Digraph that have at most one directed edge between pair of vertices, but are allowed to have self-loops, are called asymmetric or antisymmetric.

Symmetric Digraph : Digraphs in which for every edge (a, b) (i.e., from vertex a to b) there is also an edge (b, a).

Complete Digraphs : A **complete symmetric digraph** is a simple digraph in which there is exactly one edge directed from every vertex to every other vertex, and a **complete asymmetric digraph** is an asymmetric digraph in which there is exactly one edge between every pair of vertices.

A complete asymmetric digraph of n vertices contains **n(n-1)/2** edges, but a complete symmetric digraph of n vertices contains **n(n-1)** edges. A complete asymmetric digraph is also called a tournament or a complete tournament.

A digraph is said to be **balanced** or **pseudosymmetric** or an **isograph** if for every vertex vi the in degree equals the out-degree; that is $d^{+}(v_i) = d^{-}(v_i)$. A balanced digraph is said to be **regular** if every vertex has the same in-degree and out degree as every other vertex.

Directed Walk : A directed walk from a vertex v_i to v_j is an alternating sequence of vertices and edges beginning with v_i and ending with j, such that each edge is oriented from the vertex preceding it to the vertex

following it .No edge in a directed walk appears more than once, but vertices may appear may more than once. In fig 14, v_5 a v_3 d v_4 h v_1 is a directed walk.

Semi Walk : A semi walk in directed graph is a walk in corresponding undirected graph but is not a directed walk. e.g. v_1 i v_4 g v_5 c v_3 is a semiwalk in fig 14.

A walk in a digraph can mean either a directed or a semi walk.

Semi Path : A semi path in a digraph is a path in corresponding undirected graph but not in the digraph.

Strongly Connected : A digraph G is said to be a strongly connected if there is at least one directed path from every vertex to every other vertex.

Weakly Connected : A digraph G is said to be weakly connected if its corresponding undirected graph is connected but G is not strongly connected.

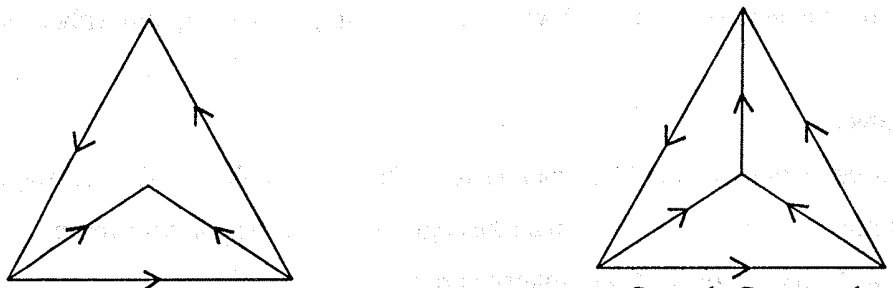


Fig. 15: Connectedness in Digraph

2.5 Matrix Representation of a graph :

Incidence Matrix :

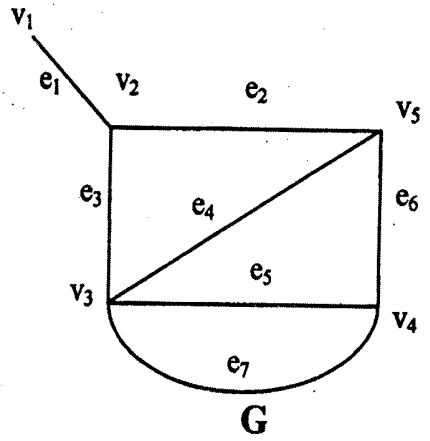
Let G be a graph with n vertices, e edges and no self-loop. Define an n x e matrix

$A = [a_{ij}]$ whose n rows corresponding to n vertices and the e columns correspond to the edges as follows: The matrix element

$a_{ij} = 1$, if j th edge e_j is incident on i th vertex v_i

$= o$, elsewhere.

Such a matrix A is called vertex-edge incidence matrix or simply incidence matrix and is denoted by A (G).



	e_1	e_2	e_3	e_4	e_5	e_6	e_7
v_1	1	0	0	0	0	0	0
v_2	1	1	1	0	0	0	0
v_3	0	0	1	1	1	0	1
v_4	0	0	0	0	1	1	1
v_5	0	1	0	1	0	1	0

Fig 16: Incidence Matrix of G

The incidence matrix contains only two elements 0 and 1. Such a matrix is called a binary matrix or a (0,1) matrix.

If we are given a incidence matrix A (G) we can construct its geometric graph without ambiguity.

Some Observations :

1) Since every edge is incident on exactly two vertices, each column of A has exactly two 1's.
2) The number of 1's in each row equals the degree of the corresponding vertex.
3) A row with all 0's represents an isolated vertex.
4) Parallel edges in a graph produce identical columns in its incidence matrix.
5) If a graph G is disconnected and consists of two components g_1 and g_2 the incidence matrix A(G) of graph G can be written in a block diagonal form as

$$A(G) = \left(\begin{array}{c|c} A(g_1) & 0 \\ \hline 0 & A(g_2) \end{array}\right)$$

where $A(g_1)$ and $A(g_2)$ are the incidence matrices of components g_1 and g_2.

6) Permutation of any two rows or columns in an incidence matrix simply corresponds to relabeling the vertices and edges of the same graph.

Two graphs G_1 and G_2 are isomorphic iff their incidence matrices $A(G_1)$ and $A(G_2)$ differs only by permutations of rows and columns.

Adjacency Matrix :

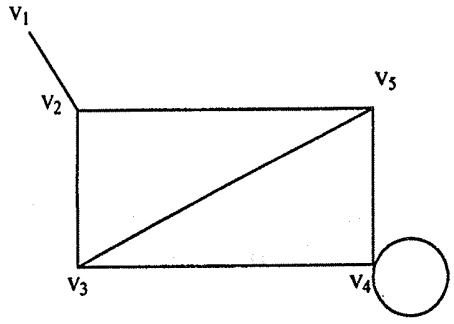
The adjacency matrix of a graph G with n vertex and no parallel edge is an **n x n** symmetric binary matrix $X = [x_{ij}]$ defined over the ring of integers such that

x_{ij} = 1, if there is an edge between ith & jth vertices.

= 0, if there is no edge between them.

Some Observations :

1) The entries along the principal diagonal of X are all 0's iff the graph has no self loop. A selfloop at the i th vertex corresponds to $x_{ii} = 1$.
2) If the graph has no self-loop the degree of vertex equals the number of 1's in the corresponding row or column of X.



G

	v_1	v_2	v_3	v_4	v_5
v_1	0	1	0	0	0
v_2	1	0	1	0	1
v_3	0	1	0	1	1
v_4	0	0	1	1	1
v_5	0	1	1	1	0

Fig. 17: Adjacency Matrix of G

3) Permutation of rows and of the corresponding columns imply reordering the vertices. It must be noted that the rows and columns must be arranged in the same order.
4) A graph G is disconnected and is in two components g_1 and g_2 iff its adjacency matrix X (G) can be partitioned as

$$X(G) = \begin{pmatrix} X(g_1) & 0 \\ 0 & X(g_2) \end{pmatrix}$$

where X (g_1) is the adjacency matrix of the component g_1 and X (g_2) is that of the component of g_2.

5) Given any square, symmetric binary matrix Q of order n, one can always construct a graph G of n vertices (& with no parallel edge) such that Q is the adjacency matrix of G.

Circuit Matrix :

Let the number of different circuits in a graph G be q and the number of edges in G be e. Then a circuit matrix $B = [b_{ij}]$ of G is a q x e, (0,1) matrix defined as follows:

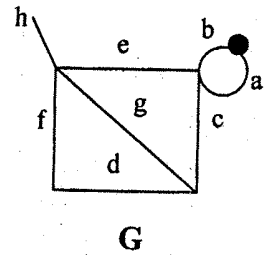
b_{ij} =1, if i th circuit includes j th edge and

= 0, otherwise.

This is generally denoted by B(G).

Observations :

1) A column with all zeros corresponds to a non circuit edge, e.g. edge h in Fig 18.
2) The number of 1's in a row is equal to the number of edges in the corresponding circuit.
3) It can represent a self loop and parallel edges.



G

	a	b	c	d	e	f	g	h
1	1	1	0	0	0	0	0	0
2	0	0	1	0	1	0	1	0
3	0	0	0	1	0	1	1	0
4	0	0	1	1	1	1	0	0

Fig. 18: G with Circuits {a, b}, {c, e, g}, {d, f, g}, {c, d, f, e} and its circuit matrix

4) If graph G is separable (or disconnected) and consists of two blocks (or components) g_1 and g_2 the circuit matrix B(G) can be written in a black diagonal form as

$$B(G) = \begin{pmatrix} B(g_1) & 0 \\ 0 & B(g_2) \end{pmatrix}$$

where B (g_1) and B (g_2) are the circuit matrices of g_1 and g_2 respectively.

5) Permutation of any two rows or columns imply reordering the circuits and edges.

6) Two graphs G_1 and G_2 will have same circuit matrix G_1 and G_2 are 2 isomorphic. In other words, the circuit matrix does not specify a graph completely. It specifies the graph within 2 isomorphism.

Cut Set Matrix : We can define a cutset matrix $\mathbf{C} = [c_{ij}]$ in which the rows correspond to the cutsets and the columns to the edges of the graph as follows:

c_{ij} = 1, if i th cutset contains j th edge
= 0, otherwise.

Observations :

1) Permutation of rows and columns in a cutset matrix correspond simply to a renaming of cutsets and edges respectively.
2) Column with all zeros corresponds to an edge forming a self loop.
3) Parallel edges produce identical columns in the cutset matrix.
Culsets of G in fig 18 are {h}, {a, b}, {c, e}, {c, d, g}, {f, d}, {e, g, f}, {f, g, c}, {e, d, g}.

	a	b	c	d	e	f	g	h
1	0	0	0	0	0	0	0	1
2	1	1	0	0	0	0	0	0
3	0	0	1	0	1	0	0	0
4	0	0	1	1	0	0	1	0
5	0	0	0	1	0	1	0	0
6	0	0	0	0	1	1	1	0
7	0	0	1	0	0	1	1	0
8	0	0	0	1	1	0	1	0

Cut set matrix of the graph G in fig 18

2.6. Graph Theoretic Algorithms :

Weighted graph shortest spanning tree :

If graph G is a weighted graph i.e., if there is a real number associated with each edge of G, then the weight of the spanning tree T of G is defined as the sum of the weights of all the branches in T. In general, different spanning

trees of G has different weights. Among all the spanning trees of G, one with the smallest weight is called a shortest spanning tree or shortest distance spanning tree or minimal spanning tree.

Algorithms for finding the shortest spanning tree in a weighted graph :

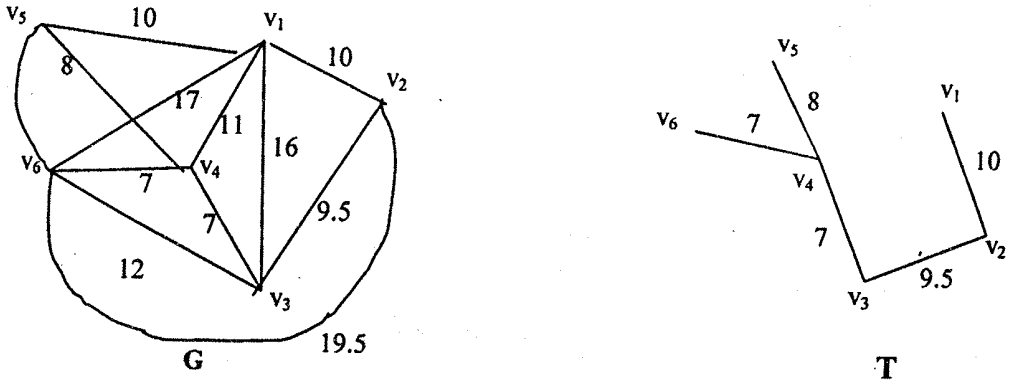


Fig. 19 Shortest spanning tree T of weighted graph G.

Kruskal algorithm :

List all edges of the graph G in order of non-decreasing weight. Next select the smallest edge of G. Then for each successive step, select (from all remaining edges of G) another smallest edge that makes no circuit with the previously selected edges. Continue until n-1 edges have been selected and these edges will construct the desired shortest spanning tree.

Prim's algorithm :

Draw n isolated vertices and label them $v_1, v_2, \ldots v_n$. Tabulate the given weights of the edge of G in n by n table. Set the weights of non existent edges as very large. Start from vertex v_1 and connect it to its nearest neighbour (i.e., to the vertex which has the smallest entry in row 1 of the table) say v_k. Now consider v_1 and v_k as one sub graph and connect these sub graph to its closest neighbour (i.e., to vertex other than v_1 and v_k that has the smallest entry among all entries in rows 1 and k). Let this new vertex be v_i. Next regard the tree with vertices v_1, v_k and v_i as one sub graph and continue the process until all n vertices have been connected by n-1 edges. For the graph G is fig 19, the 6 x 6 table is given below:

	v_1	v_2	v_3	v_4	v_5	v_6
v_1	-	10	16	11	10	17
v_2	10	-	9.5	∞	∞	19.5
v_3	16	9.5	-	7	∞	12
v_4	11	∞	7	-	8	7
v_5	10	∞	∞	8	-	9
v_6	17	19.5	12	7	9	-

Shortest path algorithm :

A large number of optimization problems are mathematically equivalent to finding shortest path in a graph.

Algorithm for finding out a shortest path, from a specified vertex (s) to another specified vertex (t) can be stated as follows:

A simple weighted digraph G with n vertices is described by an n x n matrix $\mathbf{D= [d_{ij}]}$

Where d_{ij} = weight of the directed edge from vertex i to vertex j ($d_{ij} \geq 0$)

d_{ij} = o

d_{ij} = α, if there is no edge from i to j.

In general $d_{ij} \neq d_{ji}$ and the triangle inequality need not be satisfied. That is $d_{ij} + d_{jk}$ may be less than d_{ik}. The distance of a directed path p is defined to be the sum of the lengths of the edges in p. The problem is to find the shortest possible path and its length from a starting vertex s to a terminal vertex T.

Dijkstra's Algorithim :

This algorithm levels the vertices of the given digraph. At each stage in the algorithm some vertices have permanent levels and other temporary levels. The algorithm begins by assigning permanent level 0 to the starting vertex s and temporary level ∞ to the remaining n-1 vertices. From then on, in each iteration another vertex gets a permanent level according to the following rules:

1) Each vertex j that is, not yet permanently leveled gets a new temporary level whose value is given by

min [old level of j, (old label of i + d_{ij})]

where i is the latest vertex permanently labeled in the previous iteration and d_{ij} is the direct distance between vertices i and j.

If i and j are not joined by an edge then $d_{ij} = \infty$.

2) The smallest value among all the temporary level is found and this becomes the permanent level of the corresponding vertex. In case of a tie, select any one of the candidates for permanent labeling.

Step (1) and (2) are repeated alternately until the destination vertex t gets a permanent label.

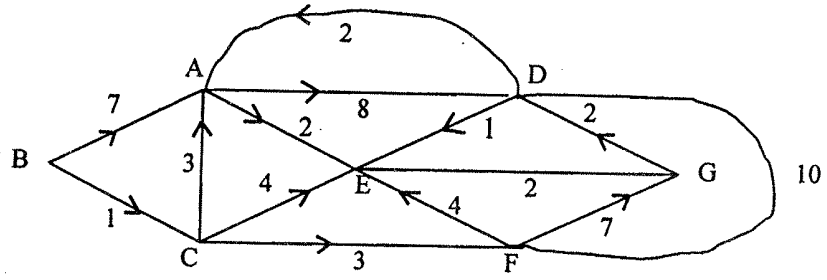


Fig. 20: weighted digraph G

The first vertex to be permanently label is at a distance of 0 from s. The 2nd vertex to get a permanent label is the vertex closest to s. From the remaining n-2 vertices, the next one to be permanently labeled is the 2nd closest vertex to s and so on.

The permanent label of each vertex is the shortest distance of that vertex from.

A	B	C	D	E	F	G
∝	[0]√	∝	∝	∝	∝	∝
7	[0]	[1]√	∝	∝	∝	∝
4	[0]	[1]	∝	5	4	∝
[4]	[0]	[1]	14	5	[4]√	11
[4]	[0]	[1]	12	[5]√	[4]	11
[4]	[0]	[1]	12	[5]	[4]	[7]√

□ Denotes permanent label.
√ Denotes the latest vertex permanently labelled.

Iteration for finding shortest path from B to G of the graph in fig. 20.

The algorithm described does not actually list the shortest path from starting vertex to the terminal vertex. It only gives the shortest distance. The shortest path can be easily constructed by working backward from the

terminal vertex such that we go to the predecessor whose label differs exactly by the length of the connecting edge. A tie indicates more than one shortest path. For the figure 20, the iterations show that the distance of the shortest path from B to g is 7 and the path is B→C →E →G.

Remark :

1) In this algorithm if we continue the labeling until every vertex gets a permanent label we will get an algorithm for thortest path from starting vertex s to all other vertices.
2) In this algorithm as more vertices acquired permanent labels, the number of addition and comparison needed to modify the temporary labels continues to decrease. Notice that for a given n, the continuation time is independent of number of edges in the digraph.
3) We have assumed distances d_{ij} are all non negative numbers. If some of the distance are negative, this algorithm will not work.

Summary :

One of the most fascinating areas of study is the interplay between considering a graph as a combinatorial object and as a geometric figure. The existence of a dual graph, in addition to being a condition equivalent to that of planarity, is important in its own right. Colouring is another very interesting problem of graph theory which has been discussed in this chapter. Matching is an independent set of edges, i.e., a set of edges no two of which are adjacent.

Many physical situations require directed graphs. Directed graphs are employed in abstract representations of computer programs, where the vertices stand for the program instructions and the edges specify the execution sequence. Most of the important and fundamental features of directed graphs are discussed in this chapter. The use of matrices in studying graphs has been demonstrated in this chapter. Finally, computational aspects of graph theory are presented here by the discussion of some graph-theoretic algorithms.

Exercise :

1. Show that the edges forming a fundamental circuit in a planar graph G correspond to a set of fundamental cutset in the dual G*.
2. Prove that the geometric dual of a self-loop-free non separable planar graph is also non separable.

3. Show that the edges forming a spanning tree in planar graph G correspond to the edges forming a set of chords in the dual G*.
4. Show that the complete graph of four vertices is self-dual. Give another example of a self-dual graph.
5. Show that if a bipartite graph has any circuits, they must all be of even length.
6. Show that a simple planar graph with less than 30 edges has a vertex of degree 4 or less.
7. Show that in a planar connected graph has less than 12 regions and degree of each vertices is at least 3 there is a region bounded by 4 or fewer edges.
8. Show that the chromatic polynomial of a graph consisting of a single circuit of length n (i.e., an n –gon) is $P_n(\lambda) = (\lambda-1)^n + (\lambda-1)(\lambda-1)^n$.
9. Prove the every edges in a digraph belongs either to a directed circuit of a directed cut-set.
10. A maximal planar graph is one to which no line can be added without losing planarity. Show that every region in a maximal planar graph is a triangle.

- - - -

M.Sc. Course
in
Applied Mathematics with Oceanology
and
Computer Programming

PART-I

Paper-II **Module No.- 15** **Group-A**

Groups

Module Structure

15.1 Introduction

The group theory arose mainly from attempts to "nd the roots of a polynomial in terms of its coecients. The learners are already familiar with group theory. In this module a recapitulation of group theory is given. The recapitulation is needed to continue the study of abstract algebra. Some properties of normal groups and the concept of quotient groups are studied here.

15.2 Objectives

After going through this unit you will be able to learn about -

- What is group?
- Types of groups
- Subsemigroups
- Subgroups
- Cosets and characteristic of a group
- Normal subgroup and its properties
- Quotient group and its properties

15.3 Keywords

Groups, subgroups, cyclic groups, normal subgroups, quotient groups.

15.4 Definition of Group

Before going to define group, we first define binary operation. It is a mapping from the set $S \times S$ into S, i.e., it is a function which associates to every pair of $S \times S$ a unique element of S. In other words, '$*$' is said to be a binary operation on S, iff $a * b \in S$ for all $a, b \in S$ and $a * b$ is unique.

Definition 15.1 (Groupoid) *A non-empty set G together with a binary operation $*$ is said to form a groupoid if $(G, *)$ satisfies the closure property, i.e., $a * b \in G$ for all $a, b \in G$.*

Definition 15.2 (Semi-group) *A non-empty set G together with a binary operation $*$ is said to form a semi-group if $(G, *)$ satisfies the following properties:*
1. *Closure: for all $a, b \in G \Rightarrow a * b \in G$.*
2. *Associative law: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.*

For example, $(\mathbf{N}, +)$ is a semi-group, where $\mathbf{N}$ is the set of natural numbers and $+$ is the ordinary addition.

Definition 15.3 (Monoid) *If the semi-group $(S, *)$ contains an identity element then it is called a monoid.*

For example, $(\mathbf{Z}, +)$ is a monoid with identity element 0 and $(\mathbf{Z}, .)$ is a monoid with 1 as identity element.

Definition 15.4 (Group) *A non-empty set G together with a binary operation $*$ is said to form a group if $(G, *)$ satisfies the following properties:*

1. *Closure: for all $a, b \in G \Rightarrow a * b \in G$,*
2. *Associative law: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$,*

3. *Existence of identity: There exists an element* $e \in G$ *such that* $a * e = a = e * a$ *for all* $a \in G$, *then* e *is called the identity element of* G.

4. *Existence of inverse: To every* $a \in G$, *there exists an element* $a' \in G$ *such that* $a * a' = a' * a = e$, *where* e *is the identity element of* G *and* a' *is called the inverse element of* a.

Some times the inverse of a *is denoted by* a^{-1}.

Definition 15.5 (Abelian group or commutative group) *A group* $(G, *)$ *is said to be an abelian or commutative group, if* $*$ *is commutative in* G, *i.e., if* $a * b = b * a$ *for all* $a, b \in G$.

A group which is not commutative is called ***noncommutative.***

Definition 15.6 (Order of a finite group) *The order of a finite group is the number of distinct elements in the finite set.*

If G *be a finite group with* n *distinct elements, then the order of the group* G, *to be denoted by* $O(G)$ *or* $|G|$ *is* n.

Definition 15.7 (Congruent modulo) *Let* a *and* b *be two integers and they are said to be congruent modulo* m *if* $a - b$ *is divisible by* m, m *is a positive integer. It is written as* $a \equiv b \pmod{m}$. *The integer* m *is called* ***modulus of the congruence.***

For example, $4 \equiv 2 \pmod 2$, $16 \equiv 0 \pmod 4$, $-6 \equiv 2 \pmod 4$, etc. It may be noted that, if $a \equiv b \pmod m$ then the remainders are same when a and b are divide by m.

In the congruent modulo m, the remainders are $0, 1, 2, \ldots, m-1$. Based on the remainders, the set of all integers can be divided into m mutually disjoint sets. These are known as **residue classes** and denoted by $[0], [1], [2], \ldots, [m-1]$. The set of all these elements, again forms a set, which is denoted by $\mathbb{Z}_m$, i.e., $\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$.

For example, $m = 5$ the residue classes are

$$\begin{aligned}
[0] &= \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\} \\
[1] &= \{\ldots, -9, -4, 1, 6, 11, 16, \ldots\} \\
[2] &= \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\} \\
[3] &= \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\} \\
[4] &= \{\ldots, -6, -1, 4, 9, 14, 19, \ldots\}
\end{aligned}$$

Also, $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

Addition and multiplication between two elements of $\mathbb{Z}_m$

Let $[a], [b]$ be any two elements of $\mathbb{Z}_m$. Then

$$\begin{aligned}
[a] + [b] &= [a + b] = [x] \\
[a] \cdot [b] &= [a \cdot b] = [y],
\end{aligned}$$

where, x (y) is the least positive remainder when $a + b$ (respectively $a \cdot b$) is divided by m.

Let n be a positive integer. Consider the set $\mathbb{Z}_n$ of all congruence classes of integers modulo n. Then $(\mathbb{Z}_n, +)$ is a commutative group. Also, it can be shown that the set $\mathbb{Z}_p = \{[1], [2], \ldots, [p-1]\}$ is an abelian group under the composition of multiplication of residue classes modulo p, where p is prime.

15.5 Order of an Element of a Group

Suppose G is a group and the composition has been denoted multiplication. By the order of an element $a \in G$ is meant the least positive integer n, if one exists, such that $a^n = e$ (the identity element of G).

If there exists no positive integer n such that $a^n = e$, then we say the order of a is infinite or zero. The order of an element a is denoted by $o(a)$.

In additive notation, $o(a)$ is n if $na = e$.

If general, for the group $(G, *)$ the order of a is equal to n if $\underbrace{a * a * \cdots * a}_{n\ a\text{'s}} = e$.

Consider the group $(\mathbf{Z}_6, +)$, where $+$ is the addition among classes defined as $[a] + [b] = [a + b]$. The order of the group $\mathbf{Z}_6$ is 6. The order of the elements [0], [1], [2], [3], [4], [5] are respectively 1, 6, 3, 2, 3, 6. For example, $3[2] = [2] + [2] + [2] = [6] = [0]$ and 3 is the smallest positive integer such that $3[2] = [0]$.

Definition 15.8 (Idempotent element) *Let $(S, \circ)$ be an algebraic structure (either groupoid, semigroup, monoid or group). An element $a \in S$ is said to be idempotent if $a \circ a = a$.*

Definition 15.9 (Subsemigroup) *Let $(G, *)$ be a semigroup and S be a subset of G. If S itself a semigroup with respect to the same composition $*$, then $(S, *)$ is called the subsemigroup of G.*

Example 15.1 Show that the set of all idempotent elements in a commutative semigroup S form a subsemigroup of S.

Solution. Let A be the set of all idempotent elements of the commutative semigroup $(S, *)$. Then $A \subset S$.

Let $a, b \in A$.

Therefore, $a * a = a, \quad b * b = b.$ (i)

Now,

$$\begin{aligned} (a * b) * (a * b) &= a * (b * a) * b && \text{[by associative]} \\ &= a * (a * b) * b && \text{[by commutative]} \\ &= (a * a) * (b * b) && \text{[by associative]} \\ &= a * b && \text{[using (i)]} \end{aligned}$$

Thus $a * b$ is an idempotent element.

Since $a, b \in A$, therefore $a * b \in A$, i.e. A is closed under $*$

Again, S satisfies associative property, therefore this property is also valid in A. Hence A is a subsemigroup of S.

Example 15.2 Show that if both cancellation laws hold in the semigroup $(S, *)$; then any idempotent element in S is a two sided identity element.

Solution. Let $a \in S$ and a being an idempotent element, $b \in S$ be any element of S.

Therefore, $a * a = a$.

Now,

$$\begin{aligned} a * b &= (a * a) * b && \text{[since } a = a * a\text{]} \\ &= a * (a * b) && \text{[by associative]} \end{aligned}$$

This implies $b = a * b$ by left cancellation law, i.e. $a * b = b$. Thus a is the left identity element in S.
Similarly, it can be shown that $b * a = b$, i.e. a is the right identity element in S.
Therefore, $a * b = b * a = b$. Hence a is the two sided identity element in S.

Example 15.3 Let S be a semigroup and $Z(S) = \{z \in S : zs = sz \text{ for all } s \in S\}$. Show that $Z(S)$ is a commutative subsemigroup of S.

Solution. Let $z_1, z_2 \in Z(S)$. Then $z_1 s = sz_1$ and $z_2 s = sz_2$ for all $s \in S$.
Now, $(z_1 z_2)s = z_1(z_2 s) = z_1(sz_2) = (z_1 s)z_2 = (sz_1)z_2 = s(z_1 z_2)$.
That is, $(z_1 z_2)s = s(z_1 z_2)$ for all $s \in S$. Thus $z_1 z_2 \in Z(S)$. Hence $Z(S)$ is closed.
Since $Z(S) \subset S$ and S satisfies associative property, therefore $Z(S)$ also satisfies this property.
Let $z_1, z_2 \in Z(S)$. Therefore, $z_1 s = sz_1$ for all $s \in S$. In particular, if we choose $s = z_2$ then from the relation $z_1 s = sz_1$, we have $z_1 z_2 = z_2 z_1$. Thus $Z(S)$ is commutative.
Hence $Z(S)$ is a commutative subsemigroup.

Quasi-group

A groupoid $(G, *)$ is said to be a quasi-group, if any two elements $a, b \in G$, each of the equations $a * x = b$ and $y * a = b$ has a unique solution in G.
For example, the groupoid $(\mathbb{Z}, +)$ is also a quasi-group. This is because for any two elements $a, b \in \mathbb{Z}$, the unique solution $x = b - a$ in $\mathbb{Z}$ for the equation $a + x = b$ and $y = b - a$ in $\mathbb{Z}$ for the equation $a + x = b$ and $y = b - a$ in $\mathbb{Z}$ for the equation $y + a = b$.
A subset of a group may or may not be a group. Many different types of groups and their subgroups are also important in the study of modern algebra.

15.6 Subgroups

Any non-empty subset H of a group G is called a **complex** of the group G. But, if H satisfies some specific conditions then H is called a subgroup of the group G, which is defined in the following.

Definition 15.10 (Subgroup) *A non-empty subset H of a group G is said to be a subgroup of G if the composition in G is also a composition in H and for this composition H itself is a group.*

For example, let $(\mathbb{R}, +)$ be a group. Then its two subgroups are $(\mathbb{Q}, +)$ and $(\mathbb{Z}, +)$.
This example shows that a group may have more than one subgroups.

Theorem 15.1 *(i) The identity element of a subgroup is the same as that of the group.*
(ii) The inverse of any element of a subgroup is the same as the inverse of the regarded as an element of the group.

Note 15.1 It may be noted that every group G has at least two subgroups, viz., $\{e\}$ and G itself. These two subgroups are called **trivial subgroups**. If H is a subgroup of the group G and $H \neq \{e\}$ and $H \neq G$, then H is called a **nontrivial subgroups**.

Thus every group has a subgroup.

Definition 15.11 *Let H and K be two non-empty subsets of a group G. The product of H and K is defined as $HK = \{hk : h \in H \text{ and } k \in K\}$*

Theorem 15.2 *If H is a subgroup of a group G, then $HH = H$.*

Now, we present a very useful result to test whether a subset of a group is a subgroup or not.

Theorem 15.3 (Condition for subgroup) *A necessary and sufficient condition for a non-empty subset H of a group G to be a subgroup is that, $a, b \in H, ab^{-1} \in H$ where b^{-1} is the inverse of $b \in G$.*

Theorem 15.4 *A necessary and sufficient condition for a non-empty finite subset H of a group G to be a subgroup is that $a, b \in H \Rightarrow ab \in H$.*

But, this condition is not valid for infinite group. For example, $(\mathbf{Z}, +)$ is a group but, its subset $\mathbf{Z}^+ = \{1, 2, 3, 4, \ldots\}$ is not a subgroup of G, though $a + b \in \mathbf{Z}^+$ for all $a, b \in \mathbf{Z}^+$.

Theorem 15.5 *If H and K are two subgroups of a group G then HK is a subgroup of G iff $HK = KH$.*

Proof. Let H and K be any two subgroups of a group G. Let $HK = KH$. In order to show that HK is a subgroup of G, it is sufficient to prove $(HK)(HK)^{-1} = HK$.
Now,

$$\begin{aligned}(HK)(HK)^{-1} &= (HK)(K^{-1}H^{-1}) = H(KK^{-1})H^{-1} = HKH^{-1} \\ &\quad (\because K \text{ is a subgroup therefore, } KK^{-1} = K) \\ &= K(HH^{-1}) \\ &= KH \ (\because KH = HK \text{ and } HH^{-1} = H).\end{aligned}$$

Therefore, $HK = KH \Rightarrow HK$ is a subgroup of G.
Conversely, suppose that HK is a subgroup. Then
$(HK)^{-1} = HK \Rightarrow K^{-1}H^{-1} = HK \Rightarrow KH = HK$
$(\because K$ is a subgroup so, $K^{-1} = K$ and $H^{-1} = H)$.
Hence the theorem. □

Theorem 15.6 *If H_1 and H_2 are two subgroups of a group G then $H_1 \cap H_2$ is also a subgroup of G.*

Definition 15.12 (Centre of a group) *In a group G, define $Z(G) = \{x \in G : gx = xg$, for all $g \in G\}$. Then $Z(G)$ is called the centre of the group G.*

From definition it follows that if G is a commutative group then $G = Z(G)$ and vice versa.

Theorem 15.7 *Let G be a group. Then $Z(G)$ is a subgroup of G.*

Proof. $Z(G)$ is non-empty, since $e \in Z(G)$. Let $a, b \in Z(G)$. Then $bg = gb$. This implies $gb^{-1} = b^{-1}g$ for all $g \in G$.
Now, $(ab^{-1})g = a(b^{-1}g) = a(gb^{-1}) = (ag)b^{-1} = (ga)b^{-1} = g(ab^{-1})$ for all $g \in G$. This shows that $ab^{-1} \in Z(G)$ and hence $Z(G)$ is a subgroup of G.

Definition 15.13 (Normalizer of an element) *Let G be a group and $a \in G$. The normalizer $N(a)$ of an element a of G is the set of all those elements of G which commutes with a. That is,*

$$N(a) = \{x \in G : ax = xa\}.$$

Lemma 15.1 *The normalizer $N(a)$ of $a \in G$ is a subgroup of G.*

Proof. By definition $N(a) = \{x \in G : ax = xa\}$. Let $x_1, x_2 \in N(a)$. Then $ax_1 = x_1a$ and $ax_2 = x_2a$.
To prove $x_2^{-1} \in N(a)$.
We have $ax_2 = x_2a \Rightarrow x_2^{-1}ax_2x_2^{-1} = x_2^{-1}x_2ax_2^{-1}$
$\Rightarrow x_2^{-1}a = ax_2^{-1}$
$\Rightarrow x_2^{-1} \in N(a)$.
Now, to prove $x_1x_2^{-1} \in N(a)$.
$a(x_1x_2^{-1}) = (ax_1)x_2^{-1} = (x_1a)x_2^{-1} = x_1(ax_2^{-1}) = x_1(x_2^{-1}a) = (x_1x_2^{-1})a$.
Therefore, $x_1x_2^{-1} \in N(a)$. Hence $N(a)$ is a subgroup of G. □

15.7 Cosets and Lagrange's Theorem

Definition 15.14 *Suppose G is a group and H is any subgroup of G. Let a be any element of G. The set $Ha = \{ha : h \in H\}$ is called a **right coset** of H in G generated by a.*
*Similarly, the set $aH = \{ah : h \in H\}$ is called a **left coset** of H in G generated by a.*

Theorem 15.8 *Any two left cosets of H in G are either identical or they have no common elements.*

Proof. Let aH, bH be two left cosets of H and x be an element common to aH and bH.
Therefore, $x \in aH \Rightarrow x = ah_1$ for some $h_1 \in H$ and $x \in bH \Rightarrow x = bh_2$ for some $h_2 \in H$.
Thus, $ah_1 = bh_2$ or $a = bh_2h_1^{-1}$ and $b = ah_1h_2^{-1}$.
Now, $aH = (bh_2h_1^{-1})H = b(h_3H)$, where $h_3 = h_2h_1^{-1}$
$= bH$ since $h_3H = H$.
Thus, if there is a common element then $aH = bH$, otherwise $aH \cap bH = \phi$. □

Theorem 15.9 *Any two left (right) cosets of H in G have the same number of elements.*

Theorem 15.10 *Two left cosets aH and bH of a subgroup H in G are identical iff $a^{-1}b \in H$.*

Proof. Let $aH = bH$. Then for some $h_1, h_2 \in H$, $ah_1 = bh_2$. Thus $ah_1h_2^{-1} = b$ or $h_1h_2^{-1} = a^{-1}b$.
Since H is a group, $h_1, h_2 \in H \Rightarrow h_1h_2^{-1} \in H$ and therefore, $a^{-1}b \in H$.
Conversely, let $a^{-1}b \in H$.
Let $a^{-1}b = h_1$. Then $a(a^{-1}b) \in aH \Rightarrow b \in aH$.
But, $b \in bH$. Therefore, the left cosets aH and bH have a common element b and therefore, they are identical. □

Example 15.4 Find all the distinct left cosets of $H = 5\mathbb{Z}$ in the group $(\mathbb{Z}, +)$.

Solution. All the left cosets of H in $(\mathbb{Z}, +)$ are $n + 5\mathbb{Z}$ for all $n \in \mathbb{Z}$.
Any integer n can be written in the form $n = 5q + r, r = 0, 1, 2, 3, 4$. Hence for any $n \in \mathbb{Z}$, $n + 5\mathbb{Z} = 5q + r + 5\mathbb{Z} = r + 5\mathbb{Z}$. Therefore, there are five distinct left cosets of $5\mathbb{Z}$ in $\mathbb{Z}$ and these are $0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}$.

Definition 15.15 *Let H be a subgroup of a group G. Then the number of distinct left (or right) cosets of H in G, denoted by $[G : H]$, is called the index of H in G.*

Theorem 15.11 (Lagrange's theorem) *The order of each subgroup of a finite group is a divisor of the order of the group.*

From Lagrange's theorem, we have

$$\frac{o(G)}{o(H)} = k$$

and k is the number of distinct left(right) cosets, which is nothing but the index of H in G. Therefore,

$$\frac{o(G)}{o(H)} = [G : H].$$

Thus the index of H in G is given by $o(G)/o(H)$.

15.8 Cyclic Group

In some cases, it is observed that all elements of a group can be generated by a single element of that group. This type of group is called cyclic group, which is defined below.

Definition 15.16 *A cyclic group is a group in which every element can be generated by a single element of the group. This single element is called the generator of the cyclic group.*

If a is a generator of the cyclic group, then the group is denoted by $G = \langle a \rangle$.

If the operation is an ordinary addition, then the elements of the cyclic group $\langle a \rangle$ are of the form $\{na, n \text{ is an integer}\}$ and if the operation is multiplication then the elements of the cyclic group $\langle a \rangle$ are of the form $\{a^n, n \text{ is an integer}\}$.

For example, $G = \{1, \omega, \omega^2\}$ is a group w.r.t. multiplication. It is also a cyclic group since ω and ω^2 are the generators.

Some more example of cyclic groups are

(i) $(\mathbb{Z}, +)$ is a cyclic group whose generator is 1,

(ii) $(G, +)$, where $G = \{3n : n \in \mathbb{Z}\}$ is a cyclic group whose generator is 3,

(iii) $(\mathbb{Z}_n, +)$ is a cyclic group as its generator is $[1]$.

The set of real numbers $\mathbb{R}$ forms a group under addition, but, it is not a cyclic group.

Theorem 15.12 *1. Every cyclic group is a commutative group.*
2. The inverse of a generator of a cyclic group is also its generator.
3. Every subgroup of a cyclic group is cyclic.

15.9 Normal Subgroup

In the theory of group, it is observed that if the left and right cosets of a subgroup coincide then this subgroup has great significance than the ordinary subgroups. It is also seen that a subgroup of a group induces two decompositions of the group in terms of its left and right cosets. These particular class of subgroups are now called normal subgroups.

Definition 15.17 (Normal subgroup) *A subgroup H of a group G is said to be a normal subgroup if every left coset of H is also a right coset of H in G, i.e., $Ha = aH$, for all $a \in G$.*

For any group G, $\{e\}$ and G are normal subgroups. Now, we can shown that every commutative group is normal.

Theorem 15.13 *Intersection of two normal subgroups of a group G is a normal subgroup of G. i.e. if H and K are two normal subgroups of G, then $H \cap K$ is also a normal subgroup of G.*

This theorem can be generalised as follows.

Corollary 15.1 *The intersection of any family of normal subgroups of a group is a normal subgroup.*

But, union of two normal subgroup is not necessarily a normal subgroup, as the union of two subgroup is not necessarily a subgroup.

Theorem 15.14 *Let H be a normal subgroup of a group G and K be any subgroup of G, then $H \cap K$ is a normal subgroup of K.*

Proof. Since H and K are subgroups of G, therefore $H \cap K$ is also a subgroup of G. Also $H \cap K \subseteq K$.
Therefore, $H \cap K$ is a subgroup of K. Now, we have to prove that $H \cap K$ is a normal subgroup of K.
Let x be any element of K and a be any element of $H \cap K$. Then $a \in H$ and $a \in K$.
Since H is a normal subgroup of G, $xax^{-1} \in H$. Also, K is a subgroup of G.
Therefore, $x \in K, a \in K \Rightarrow xax^{-1} \in K$. Thus $xax^{-1} \in H \cap K$.
For $x \in K$ and $a \in H \cap K$, we have seen that $xax^{-1} \in H \cap K$. Consequently, $H \cap K$ is a normal subgroup of K. □

Corollary 15.2 *(i) If H is a normal subgroup of G and K be a subgroup of G then HK, KH are both subgroups of G and $HK = KH$.*
(ii) If H and K are both normal subgroups of G then HK, KH are also normal subgroups of G, moreover $HK = KH$.

Definition 15.18 (Simple group) *A group G is called a simple group if $G \neq \{e\}$ and G has no nontrivial (i.e., other than G and $\{e\}$) normal subgroups.*

For example, every group of prime order is simple.

15.10 Quotient Group or Factor Group

The collection of all cosets of a group form a group under certain binary operation. This group is called quotient group or factor group, which is discussed below.

Proof. (i) *Closure property*
Let $a, b \in G$ then $aH, bH \in G/H$.
Now,

$$\begin{aligned}(aH)(bH) &= a(Hb)H \\ &= a(bH)H \text{ [Since } H \text{ is a normal subgroup of } G] \\ &= ab(HH) \\ &= abH.\end{aligned}$$

By closure property $ab \in G$. Therefore, abH is a coset of H in G and hence $abH \in G/H$. Thus G/H is closed with respect to coset multiplication.

(ii) *Associative property*
Let $a, b, c \in G$. Then $aH, bH, cH \in G/H$.

$$\begin{aligned}(aH)\{(bH)(cH)\} &= aH(bcH) \\ &= abcH \\ &= (abH)(cH) \\ &= \{(aH)(bH)\}(cH).\end{aligned}$$

Thus the product of cosets in G/H satisfies the associative property.

(iii) *Existence of identity*
Let $e \in G$ be the identity element of G. Then $H = eH \in G/H$.
Also, if aH is any element of G/H then $H(aH) = (eH)(aH) = eaH = aH$.
Therefore, the coset H (i.e. eH) is the identity element of G/H.

(iv) *Existence of inverse*
Let $aH \in G/H$. Then $a^{-1}H \in G/H$. We have $(aH)(a^{-1}H) = aa^{-1}H = eH = H$ and $(a^{-1}H)(aH) = a^{-1}aH = eH = H$.
Therefore, the coset $a^{-1}H$ is the inverse of (aH), i.e. $a^{-1}H = (aH)^{-1}$.
Thus each element of G/H possesses inverse. Hence G/H is a group with respect to the product of cosets. □

Definition 15.19 *Let G be a group and H be a normal subgroup of G. Then the group G/H of all cosets of H in G under the binary operation $aH * bH = abH$ is called the quotient group or factor group of G by H.*

Example 15.5 Let us consider the group S_3 and one of its subgroup $H = \{\rho_0, \rho_3, \rho_4\}$, where $\rho_0 = (1), \rho_3 = (1\ 2\ 3), \rho_4 = (1\ 3\ 2)$. It is shown that H is a normal subgroup of S_3 and $[G : H] = \frac{o(G)}{o(H)} = 2$. Hence there are two distinct cosets of H in G and these are $\rho_0 H$ and $\rho_2 H$ where $\rho_2 = (1\ 2)$. Thus, the quotient group is $G/H = \{\rho_0 H, \rho_2 H\}$.
The composition table for the group operation of the quotient group is shown below.

	$\rho_0 H$	$\rho_2 H$
$\rho_0 H$	$\rho_0 H$	$\rho_2 H$
$\rho_2 H$	$\rho_2 H$	$\rho_0 H$

Example 15.6 Let H be a subgroup of a group G such that $[G : H] = 2$. Then prove that H is a normal subgroup of G.

Solution. Since $[G : H] = 2$, i.e., the index is 2, the group has only two distinct left and right cosets. One of them is H. Let $a \in G$. Then a may or may not belongs to H. If $a \in H$ then $aH = H = Ha$. If $a \notin H$, then $aH \neq H$. Hence $G = H \cup aH$ and $H \cap aH = \phi$. Then $aH = G - H$.

Again, since $a \notin H$ and H has only two right cosets, then $G = H \cup Ha$ where $H \cap Ha = \phi$. Thus $Ha = G - H$.

Therefore, $aH = Ha$ for all $a \in G$. Hence H is a normal subgroup of G.

Example 15.7 If $\mathbb{Z}$ is the group of integers under addition and H be the subgroup of $\mathbb{Z}$ consisting of the multiplies of 5. Show that H is a normal subgroup of $\mathbb{Z}$. Find also the quotient group $\mathbb{Z}/H$.

Solution. It is known that $\mathbb{Z}$, the set of all integers, forms a commutative group under addition. Also, $H = 5\mathbb{Z} = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$ is a subgroup of $\mathbb{Z}$ under addition. Obviously, H is a commutative subgroup. Therefore, $aH = Ha$ for all $a \in \mathbb{Z}$ and hence H is a normal subgroup.

Second part. Let $a = m \in \mathbb{Z}$. Then by division algorithm, there exists $q, r \in \mathbb{Z}$ such that $m = 5q + r, 0 \leq r < 5$. Thus, $a + 5\mathbb{Z} = (5q + r) + 5\mathbb{Z} = r + 5q + 5\mathbb{Z} = r + 5\mathbb{Z}$. Hence $\mathbb{Z}/5\mathbb{Z} = \{r + 5\mathbb{Z} : r = 0, 1, 2, 3, 4\} = \{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$. The composition table for the quotient group $\mathbb{Z}/5\mathbb{Z}$ is shown below.

	$0+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$0+5\mathbb{Z}$	$0+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$1+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$0+5\mathbb{Z}$
$2+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$0+5\mathbb{Z}$	$1+5\mathbb{Z}$
$3+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$0+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$
$4+5\mathbb{Z}$	$4+5\mathbb{Z}$	$0+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$

Example 15.8 Find the quotient group $\mathbb{Z}_{10}/H$, where $H = \{[0], [5]\}$ is a normal subgroup of $\mathbb{Z}_{10}$.

Solution. Here $o(\mathbb{Z}_{10}) = 10$ and $o(H) = 2$. Thus $o(\mathbb{Z}_{10}/H) = o(\mathbb{Z}_{10})/o(H) = 5$.

Hence $\mathbb{Z}_{10}/H$ has five elements. Now,

$$[0] + H = H = [5] + H$$
$$[1] + H = \{[1], [6]\} = [6] + H$$
$$[2] + H = \{[2], [7]\} = [7] + H$$
$$[3] + H = \{[3], [8]\} = [8] + H$$
$$[4] + H = \{[4], [9]\} = [9] + H$$

Hence the quotient group $\mathbb{Z}_{10}/H$ is $\{[0] + H, [1] + H, [2] + H, [3] + H, [4] + H\}$.

Example 15.9 Let H be a subgroup of a group G. If $x^2 \in H$ for all $x \in G$, then prove that H is a normal subgroup of G and G/H is commutative.

Solution. By the given condition, if $g \in G$ then $g^2 \in H$. Let $h \in H$. Then $h^{-1} \in H$.

Since $g \in G \Rightarrow g^{-1} \in G$ and $g^{-1}h \in G$ [H is a subgroup of G]

Since $g^{-1}h \in G \Rightarrow (g^{-1}h)^2 \in H$.

Thus we have $(g^{-1}h)^2 \in H, g^2 \in H$. Since H is a subgroup of G, then by closer property
$(g^{-1}h)^2h^{-1}g^2 \in H$
$\Rightarrow (g^{-1}h)(g^{-1}h)h^{-1}(gg) \in H$
$\Rightarrow (g^{-1}h)g^{-1}(hh^{-1})(gg) \in H$
$\Rightarrow (g^{-1}h)g^{-1}(gg) \in H$
$\Rightarrow g^{-1}hg \in H$.
Hence H is a normal subgroup of G.

To prove G/H is commutative
Let $aH, bH \in G/H$. We have to prove $xHyH = yHxH$ i.e., $xyH = yxH$
or, $(yx)^{-1}(xy) \in H$.
Now, $(yx)^{-1}(xy) = (x^{-1}y^{-1})(xy) = (x^{-1}y^{-1})^2(yxy^{-1})^2y^2$.
Since $a^2 \in H$ for all $a \in G$, therefore, $(x^{-1}y^{-1})^2(yxy^{-1})^2y^2 \in H$ and hence $(yx)^{-1}(xy) \in H$. Thus G/H is commutative.

Lemma 15.2 *A subgroup N of a group G is a normal subgroup of G iff the product of two right (left) cosets of N in G is again a right (left) cosets of N in G.*

Proof. Let N be a normal subgroup of the group G. Let $a, b \in G$. Since N is a normal subgroup, $Na = aN$ for all $a \in G$.
Now,

$$\begin{aligned} (Na)(Nb) &= N(aN)b \\ &= N(Na)b \text{ [since } aN = Na] \\ &= (NN)ab \\ &= Nab \end{aligned}$$

Therefore, $(Na)(Nb) = Nab$ for all $a, b \in G$.
This implies that the product of two right cosets of N is again a right coset of N in G.
Conversely, let $(Na)(Nb) = Nab$.
Let $n_1, n_2 \in N$.
Therefore, $(n_1a)(n_2b) \in Nab$
$\Rightarrow n_1an_2bb^{-1} \in Nabb^{-1}$ [since $b \in G \Rightarrow b^{-1} \in G$]
$\Rightarrow n_1an_2 \in Na$
$\Rightarrow n_1an_2a^{-1} \in Naa^{-1}$
$\Rightarrow n_1^{-1}n_1an_2a^{-1} \in n_1^{-1}N$
$\Rightarrow an_2a^{-1} \in n_1^{-1}N$
$\Rightarrow an_2a^{-1} \in N$ [since $n_1^{-1}N = N$].
Hence N is a normal subgroup of G.

□

15.11 Module Summary

In this module, some common terms like group, semigroup, subgroup, etc. are defined. Some simple properties of them are stated. Different types of subgroups, viz., cyclic subgroup, normal subgroups are defined and presented some important properties of normal subgroups. The concept of quotient/ factor groups are introduced here. Different examples and theorems on these groups are presented in this modulo. A nice exercise is provided in the next section.

15.12 Self Assessment Questions

1. Find all distinct left cosets of $H = 5\mathbb{Z}$ in the group $(\mathbb{Z}, +)$.
2. In the multiplicative group $\mathbb{C}^* = \mathbb{C} - \{0\}$, find all cosets of the subgroup $H = \{z \in \mathbb{C}^* : |z| = 1\}$.
3. Let $G = (\mathbb{Z}_4, +)$. Determine all the left cosets of $H = \{[0]\}$ in G.
4. Let $G = (\mathbb{Z}_4, +)$. Determine all the left cosets of $H = \{[0], [1], [2], [3]\}$ in G.
5. Determine all the left cosets of $H = \{[0], [4]\}$ in $(\mathbb{Z}_8, +)$.
6. Let $\mathbb{Z}$ be the group of integers under the operation of addition, and let $G = \mathbb{Z} \times \mathbb{Z}$. Consider the subgroup $H = \{(m, n) : m = n\}$ of G. Find the left cosets of H in G.
7. Show that the set of all right cosets of the subgraph $7\mathbb{Z}$ in the group $(\mathbb{Z}, +)$ is given by $\{7\mathbb{Z} + r : r = 0, 1, 2, \ldots, 6\}$.
8. Show that the set S of all cosets of $\mathbb{Z}$ in the additive group $(\mathbb{R}, +)$ of all real numbers is given by $S = \{x + \mathbb{Z} : 0 \leq x < 1\}$.
9. Let $G = \mathbb{R} \times \mathbb{R}$ be the group under binary operations $\circ$ defined by $(a, b) \circ (c, d) = (a + c, b + d)$. Let $H = \{(a, 5a) : a \in \mathbb{R}\}$. Show that H is a subgroup of G. Describe the left cosets of H in G.
10. Prove that two left cosets aH and bH of a subgroup H in G are identical iff $a^{-1}b \in H$.
11. Prove that any two left cosets of H in G are either identical or they have no common element.
12. Show that any two left (right) cosets have same cardinality.
13. Let H be a subgroup of G and aH is a left coset other than H. Prove that aH is not a subgroup of G.
14. Let H be a subgroup of G. If $a \in H$ then prove that $aH = Ha = H$.
15. Let G be a group and H, K are finite subgroups of G such that $o(H)$ and $o(K)$ are relatively prime. Show that $H \cap K = \{e\}$.
16. If H be a normal subgroup of a finite group G, then prove that $o(G/H) = \frac{o(G)}{o(H)}$.
17. Let H be a subgroup of a group G and let $a \in G$. Define $a^{-1}Ha = \{a^{-1}ha : h \in H\}$. Prove that H is a normal subgroup of G iff $a^{-1}Ha = H$ for all $a \in G$.
18. Construct the composition table for the quotient group $\mathbb{Z}/3\mathbb{Z}$.
19. If $\mathbb{Z}$ is the group of integers under addition and H be the subgroup of $\mathbb{Z}$ consisting of the multiples of 5. Show that H is a normal subgroup of $\mathbb{Z}$. Find also the quotient group $\mathbb{Z}/H$.
20. Let H be a normal subgroup of a group G. Prove that
    (a) if G is abelian then G/H is also abelian
    (b) if G is cyclic then also G/H.

15.13 Suggested Further Readings

1. M. Artin, *Algebra*, PHI, 1991.

2. J.B. Fraleigh, *A First Course in Abstract Algebra* , Narosa, New Delhi, 1982.

3. J.A. Gallian, *Contemporary Abstract Algebra*, Narosa, New Delhi, 1999.

4. J.P. Tremblay and R. Manohar, *Discrete Mathematical Structures with Applications to Computer Science*, McGraw-Hill Book Company, 1975.

5. B. Kolman, R.C. Busby and S.C. Ross, *Discrete Mathematical Structures*, 4ed, Pearson Education, 2000.

6. M.K. Sen, S. Ghosh and P. Mukhopadhyay, *Topics in Abstract Algebra*, 2ed, University Press, 2ed, 2006.

7. D.S. Malik, J.M. Mordeson and M.K.Sen, *Fundamental of Abstract Algebra*, The McGraw-Hill Companies, Inc., 1997.

M.Sc. Course
in
Applied Mathematics with Oceanology
and
Computer Programming

PART-I

Paper-II **Module No.- 16** Group-

HOMOMORPHISM OF GROUPS AND SYLOW GROUP

Module Structure

16.1 Introd ıction

In this module, a special type of function is de"ned between two groups (i.e., the domain and the codomain both are groups) with a particular restriction and leads to the concept of homomorphism. This function establishes a structural compatibility between two groups. Then the concept of isomorphism is gradually developed. In the next part of this modulo, the Sylow theorem and the class equation are introduced.

16.2 Objectives

After going through this unit you will be able to learn about -

- What is group homomorphism?

- Kernel and image of homomorphism
- What is group isomorphism?
- Automorphism
- Conjugacy and conjugacy class
- Sylow theorem
- Class equation
- Cauchy's theorems on groups
- P-Sylow group
- Solvable groups
- Direct product of groups

16.3 Keywords

Group homomorphism, kernel, image, isomorphism, automorphism, conjugacy, conjugacy class, Sylow theorem, class equation, P-Sylow group, solvable groups, direct product of groups.

16.4 Homomorphism of Groups

Definition 16.1 (Homomorphism) *Let $(G, *)$ and $(G, \circ)$ be two groups and $f : G \to G'$ be a mapping from G to G'.*

If $f(a * b) = f(a) \circ f(b)$, where $a, b \in G$, then the mapping f is said to be a **homomorphism** *of the group G into the group G'.*

Example 16.1 Let $(G, *)$ and $(G', \circ)$ be two groups and $f : G \to G'$ by $f(a) = e'$ for all $a \in G$, where e' is the identity element of G'.

Let $a, b \in G \Rightarrow a * b \in G$. Then $f(a * b) = e' = e' \circ e' = f(a) \circ f(b)$ for all $a, b \in G$. Hence f is a homomorphism.

This homomorphism is called the **trivial homomorphism.**

Example 16.2 Let us consider the group $(GL(2, \mathbb{R}), .)$ of all 2×2 non-singular matrices under matrix multiplication and the group $(\mathbb{R}^*, .)$, where $\mathbb{R}^*$ is the set of all non-zero real numbers. Define $f : GL(2, \mathbb{R}) \to \mathbb{R}^*$ by $f(A) = det\ A$ for all $A \in GL(2, \mathbb{R})$, where $det\ A$ is the determinant value of the matrix A.

Let $A, B \in GL(2, \mathbb{R})$. Then $f(A.B) = det\ (AB) = det\ A.det\ B = f(A).f(B)$.

This shows that f is a homomorphism.

Example 16.3 Consider the groups $(\mathbb{R}, +)$ and $(\mathbb{R}^+, .)$. Define $f : \mathbb{R} \to \mathbb{R}^+$, where $f(a) = e^a$ and $\mathbb{R}^+$ is the set of all positive real numbers.

Then $f(a + b) = e^{a+b} = e^a e^b = f(a)f(b)$ for all $a, b \in \mathbb{R}$. Hence f is a homomorphism.

Example 16.4 Consider the group $(\mathbf{Z}, +)$ and define $f : \mathbf{Z} \to \mathbf{Z}$, where $f(a) = a + 3$, for all $a \in \mathbf{Z}$.
Then $f(a+b) = (a+b)+3 = (a+3)+b = f(a)+b \neq f(a)+f(b)$, $a, b \in \mathbf{Z}$. This shows that f is not a homomorphism.

Example 16.5 Let $G = (\mathbf{Z}, +)$ and $G' = (\mathbf{Z}, +)$ be two groups and $f : G \to G'$ be a mapping defined by $f(x) = |x|$ for all $x \in G$. This mapping is not homomorphism as $f(-3+2) = f(-1) = |-1| = 1 \neq 5 = |-3| + |2| = f(-3) + f(2)$.

Theorem 16.1 *Let $f : G \to G'$ be a homomorphism and e, e' be the identity elements of G and G' respectively. Then*
(i) $f(e) = e'$.
(ii) $f(a^{-1}) = \{f(a)\}^{-1}$ for all $a \in G$.
(iii) $f(a^n) = \{f(a)\}^n$ for all $a \in G$ and for all $n \in \mathbf{Z}$.

Proof. (i) Since f is homomorphism $f(e) = f(ee) = f(e)f(e)$. Also, $f(e) \in G'$, by identity property of G', $f(e) = f(e)e'$.
Therefore, $f(e)e' = f(e)f(e)$ and by cancellation law $f(e) = e'$.
(ii) Let $a \in G$. Since f is homomorphism $f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e'$ (by (i)). Similarly, $f(a^{-1})f(a) = f(a^{-1}a) = f(e) = e'$. Thus $f(a^{-1})$ is the inverse of $f(a)$ in G'.
Therefore, $f(a^{-1}) = \{f(a)\}^{-1}$.

(iii) *Case I.* Let $n = 0$.
Then from (i) $f(a^0) = f(e) = e' = \{f(a)\}^0$.

Case II. Let $n = 1$.
Then $f(a^1) = f(a) = \{f(a)\}^1$.

Case III. Let $n = k$, k is some positive integer.
Suppose that $f(a^k) = \{f(a)\}^k$. Then
$f(a^{k+1}) = f(a^k a) = f(a^k)f(a)$ (since f is homomorphism)
$= \{f(a)\}^k f(a)$ (by assumption)
$= \{f(a)\}^{k+1}$.
Hence by mathematical induction, $f(a^n) = \{f(a)\}^n$ for all $n \geq 1$.

Case IV. Let $n = -m$, where m is positive integer.
Then $f(a^n) = f(a^{-m}) = f((a^{-1})^m) = \{f(a^{-1})\}^m$ (since $m > 0$)
$= (\{f(a)\}^{-1})^m$ (by (ii))
$= \{f(a)\}^{-m} = \{f(a)\}^n$.
Hence $f(a^n) = \{f(a)\}^n$ for all $a \in G$ and $n \in \mathbf{Z}$.

Definition 16.2 (Image and Kernel of a Homomorphism) *Let $(G, *)$ and $(G', \circ)$ be two groups and $f : G \to G'$ be a homomorphism. Then the image of f is denoted by Im f and is defined by*

$$Im\ f = \{f(a) \in G' : a \in G\}$$

and the kernel of f is denoted by ker f and is defined by

$$ker\ f = \{a \in G : f(a) = e', e' \text{ is the identity element of } G'\}.$$

Example 16.6 A function f is defined as follows:
$f : \{\mathbb{C} - \{0\}, \times\} \to \{\mathbb{C} - \{0\}, \times\}$, where $f(z) = z^4$, $\mathbb{C}$ is the set of complex numbers and $\times$ is the usual multiplication. Is f a homomorphism? If so find ker f.

Solution. Let $z_1, z_2 \in \mathbb{C} - \{0\}$. Now, $f(z_1 z_2) = (z_1 z_2)^4 = z_1^4 z_2^4 = f(z_1) f(z_2)$.
Hence f is homomorphism.
To find kernel.
Obviously, $1 \in \{\mathbb{C} - \{0\}$ is the identity element. If $z \in \ker f$ then $f(z) = 1$, i.e., $z^4 = 1$. This gives $z = -1, 1, -i, i$. Hence ker $f = \{-1, 1, -i, i\}$.

Theorem 16.2 *Let $f : G \to G'$ be a homomorphism. Then Im f is a subgroup of G'.*

Proof. Since $f(e) = e'$, where e, e' are the identity elements of G and G' respectively. Therefore, Im f is non-empty.

Let $a, b \in G$. Then there exists some $p, q \in$ Im f such that $f(a) = p$ and $f(b) = q$. Since G is a group, $ab^{-1} \in G$ and hence $f(ab^{-1}) \in$ Im f. Again, f is homomorphism, $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)\{f(b)\}^{-1} = pq^{-1}$. Thus $pq^{-1} \in$ Im f. Therefore, Im f is a subgroup of G. □

Theorem 16.3 *Let $f : G \to G'$ be a homomorphism. Then ker f is a normal subgroup of G.*

Proof. Let e, e' be the identities of G and G' respectively. Then $f(e) = e'$. Hence ker f is non-empty.
Let $a, b \in$ ker f. Then $f(a) = e'$ and $f(b) = e'$.
Now, $f(a * b^{-1}) = f(a) \circ f(b^{-1})$ (since f is homomorphism)
$= f(a) \circ \{f(b)\}^{-1} = e' \circ (e')^{-1} = e'$.
Therefore, $a * b^{-1} \in$ ker f. Thus ker f is a subgroup of G.
To prove ker f is normal, let $g \in G$ and $h \in$ ker f. Since $h \in$ ker f, $f(h) = e'$.
Now, $f(g * h * g^{-1}) = f(g) \circ f(h) \circ f(g^{-1}) = f(g) \circ e' \circ f(g^{-1}) = f(g) \circ \{f(g)\}^{-1} = e'$.
Therefore, $g * h * g^{-1} \in$ ker f and hence ker f is a normal subgroup of G.

16.5 Isomorphism of Groups

By definition homomorphism is a mapping. Since mapping are of different types, so homomorphism can also be classified into different ways.

A homomorphism is said to be **monomorphism** if it is one-to-one and is said to be **epimorphism** if it is onto.

If a homomorphism mapping f be one-to-one and onto, then f is said to be an **isomorphism** of the group G onto the group G'. A group G' is said to be **isomorphic** to a group G, if there exists an isomorphism from G onto G'. If G is isomorphic to G' then we write $G \simeq G'$.

In particular, if $G' \subset G$ then the homomorphism involved is called **endomorphism**.

Example 16.7 Let $\mathbb{Z}$ be the additive group of all integers and G be a multiplicative infinite cyclic group with generator a. Let the mapping $f : \mathbb{Z} \to G$ be defined by $f(n) = a^n$. Prove that f is a homomorphism. Is it an isomorphism? Justify your answer.

Solution. Let $n_1, n_2 \in \mathbf{Z}$. Now, $f(n_1 + n_2) = a^{n_1+n_2} = a^{n_1}.a^{n_2} = f(n_1)f(n_2)$.
This shown that f is homomorphism.
Let n_1 and n_2 be two distinct elements of $\mathbf{Z}$. Therefore, $f(n_1) = a^{n_1}$ and $f(n_2) = a^{n_2}$.
If possible, let $f(n_1) = f(n_2) \Rightarrow a^{n_1} = a^{n_2} \Rightarrow n_1 = n_2$, which contradicts that $n_1 \neq n_2$.
Therefore, $f(n_1) \neq f(n_2)$, i.e., f is one-to-one mapping.
Let $y = f(n) = a^n$ or, $n = \dfrac{\log y}{\log a} = \dfrac{\log a^k}{\log a} = k \in \mathbf{Z}$.
Again, $f(n) = f(k) = a^k = y \in G$.
Therefore, f is onto mapping. Hence f is isomorphism.

Theorem 16.4 *A homomorphism $f : G \to G'$ of groups is a monomorphism if and only if ker $f = \{e\}$.*

Proof. Let f be monomorphism. Then f is one-to-one. Let e and e' be the identity elements of G and G' respectively. If $a \in \ker f$ then $f(a) = e' = f(e)$. Since f is one-to-one, $a = e$. Hence ker $f = \{e\}$.
Conversely, we assume that ker $f = \{e\}$. Let $a, b \in G$ such that $f(a) = f(b)$. Obviously, $f(a), \{f(b)\}^{-1} \in G'$. Therefore, $f(a)\{f(b)\}^{-1} = e' \Rightarrow f(a)\{f(b^{-1})\} = e' \Rightarrow f(ab^{-1}) = e'$.
This shows that $ab^{-1} \in \ker f = \{e\}$. Therefore, $ab^{-1} = e$ i.e., $a = b$. Thus f is one-to-one and hence f is monomorphism. □

Example 16.8 Let $S = \{1, -1, i, -i\}$ be a group w.r.t. multiplication. Define a mapping $f : (\mathbf{Z}, +) \to (S, .)$, where

$$f(n) = \begin{cases} 1, & \text{if } n = 4k \\ -1, & \text{if } n = 4k+1 \\ i, & \text{if } n = 4k+2 \\ -i, & \text{if } n = 4k+3, \end{cases}$$

where k is an integer and $n \in \mathbf{Z}$.

Solution. Let $m, n \in \mathbf{Z}$. Then $m = 4k + a, n = 4k + b; a, b = 0, 1, 2, 3$. We construct the following tables to prove homomorphism of f.

$f(m+n)$	$4k$	$4k+1$	$4k+2$	$4k+3$
$4k$	1	i	-1	$-i$
$4k+1$	i	-1	$-i$	1
$4k+2$	-1	$-i$	1	i
$4k+3$	$-i$	1	i	$-i$

$f(m)f(n)$	$4k$	$4k+1$	$4k+2$	$4k+3$
$4k$	1	i	-1	$-i$
$4k+1$	i	-1	$-i$	1
$4k+2$	-1	$-i$	1	i
$4k+3$	$-i$	1	i	$-i$

These two tables are identical, so one can conclude that $f(m+n) = f(m)f(n)$ for all $m, n \in \mathbf{Z}$. Thus f is homomorphism. Since f is onto so it is epimorphism but not monomorphism, as f is not one-one.

Definition 16.3 *A group G' is called a homomorphic image of a group G if there exists an epimorphism f from the group G onto the group G'.*

Example 16.9 Show that the group $(\mathbf{Z}_6, +)$ is a homomorphic image of the group $(\mathbf{Z}, +)$.

Solution. Define a mapping $f : \mathbf{Z} \to \mathbf{Z}_n$ by $f(n) = [n]$ for all $n \in \mathbf{Z}$. Now, $f(m+n) = [m+n] = [m] + [n] = f(m) + f(n)$ for all $m, n \in \mathbf{Z}$. Hence f is homomorphism.
Let $[p] \in \mathbf{Z}_6$. Then $p \in \mathbf{Z}$ and hence $f(p) = [p]$. Thus f is onto. Hence $\mathbf{Z}_6$ is a homomorphic image of $\mathbf{Z}$.

Theorem 16.5 *Let H be a normal subgroup of a group G. Define a mapping ϕ from G to G/H by $\phi(x) = Hx$ for all $x \in G$. Then ϕ is homomorphism of G onto G/H and kernel of ϕ is H.*

Proof. Consider the mapping $\phi : G \to G/H$ such that $\phi(x) = Hx$ for all $x \in G$.
Let Hx be any element of G/H. Then $x \in G$, we have $\phi(x) = Hx$.
Therefore, the mapping ϕ is onto G/H.
Let $a, b \in G$ then $\phi(ab) = Hab = (Ha)(Hb) = \phi(a)\phi(b)$ [since H is normal]
Therefore, ϕ is homomorphism of G onto G/H.
Thus every quotient group of a group is a homomorphic image of the group.
To find kernel
Let K be the kernel of this homomorphism ϕ. The identity element of the quotient group G/H is the coset H. Thus $K = \{x \in G : \phi(x) = H\}$.
Let $x \in K$ then $\phi(x) = H$. But, by definition of ϕ, $\phi(x) = Hx$. Therefore, $Hx = H \Rightarrow x \in H$.
Thus $K \subseteq H$. (i)
Again, let h be any element of H. Then $Hh = H \Rightarrow \phi(h) = H$ by definition. Therefore, $h \in K$.
Thus $h \in H \Rightarrow h \in K$. Therefore, $H \subseteq K$. (ii)
From (i) and (ii), $K = H$. □

Theorem 16.6 (Fundamental theorem of homomorphism). *Every homomorphic image of a group G is isomorphic to some quotient group of G*

Proof. Let G' be the homomorphic image of G and f be the homomorphism from G onto G', i.e., $f : G \to G'$. If K be the kernel of this homomorphism then K is a normal subgroup of G.
Let us consider the quotient group G/K and define a mapping $\phi : G/K \to G'$ by $\phi(Kx) = f(x)$ for all $x \in G$.
(i) *To prove ϕ is well defined.*
That is, to prove if $x, y \in G$ and $Kx = Ky$ then $\phi(Kx) = \phi(Ky)$.
Let $Kx = Ky \Rightarrow xy^{-1} \in K$. By definition of kernel $f(xy^{-1}) = e'$, where e' is the identity of G'.
$f(x)f(y^{-1}) = e'$ [since f is a homomorphism]
$f(x)\{f(y)\}^{-1} = e' \Rightarrow f(x) = f(y) \Rightarrow \phi(Kx) = \phi(Ky)$.
Hence ϕ is well defined.
(ii) *To prove ϕ is homomorphism.*
Let $Kx, Ky \in G/K$. Then $\phi\{(Kx)(Ky)\} = \phi(Kxy) = f(xy) = f(x)f(y) = \phi(Kx)\phi(Ky)$.
Hence ϕ is homomorphism.
(iii) *To prove ϕ is one-to-one.*
Let $Kx \neq Ky$ but, $\phi(Kx) = \phi(Ky)$.
Now, $\phi(Kx) = \phi(Ky) \Rightarrow f(x) = f(y) \Rightarrow f(x)[f(y)]^{-1} = e'$
$\Rightarrow f(x)f(y^{-1}) = e' \Rightarrow f(xy^{-1}) = e'$.
Therefore, $xy^{-1} \in K \Rightarrow Kx = Ky$, which contradicts that $Kx \neq Ky$. Thus for different Kx and Ky, there are different images. Hence ϕ is one-to-one.
(iv) *To prove ϕ is onto.*
Let $y \in G'$. Then for some $x \in G$, $y = f(x)$, as f is onto.
Now, $\phi(Kx) = f(x) = y$. Therefore, ϕ is onto.
Hence ϕ is an isomorphism of G/K onto G'. □

Theorem 16.7 *The product (composition of function) of two isomorphisms is also an isomorphism.*

Proof. Let $f : G_1 \to G_2$ and $g : G_2 \to G_3$ be two isomorphisms. Then f and g are one-to-one and onto. The composite mapping $(gf) : G_1 \to G_3$ is also one-to-one and onto.

Also, $(gf)(xy) = g[f(xy)] = g[f(x)f(y)] = g(f(x))g(f(y))$ [since both f and g are isomorphisms]

This shows that (gf) is homomorphism and hence (gf) is an isomorphism. □

Theorem 16.8 *A finite cyclic group of order n is isomorphic to the additive group of residue classes modulo n.*

Proof. Let $G = \langle a \rangle$ be a finite cyclic group of order n, i.e., $G = \{e = a^0, a, a^2, a^3, \ldots, a^{n-1}\}$ and $G' = \{[0], [1], [2], \ldots, [n-1]\}$. G' is an additive group.

Define a mapping $f : G \to G'$, where $f(a^r) = [r], 0 \leq r \leq n-1$.

To prove f is one-one.

Let a^r and a^s, $0 \leq r \leq n-1$ and $0 \leq s \leq n-1$ be two distinct elements of G. If possible, let $f(a^r) = f(a^s)$. Then $[r] = [s]$, i.e., $r - s = kn$, $k \in \mathbb{Z}$.

$\Rightarrow r - s = 0$ choosing $k = 0$

$\Rightarrow r = s \Rightarrow a^r = a^s$.

That is, different elements of G have different images. Thus f is one-one.

Since $O(G) = O(G')$ and f is one-one, therefore, f is onto.

Also, $f(a^r a^s) = f(a^{r+s}) = [r+s] = [r] + [s] = f(a^r) + f(a^s)$, i.e., f is homomorphism. Hence G is isomorphic to G'.

Example 16.10 Show that $(\mathbb{Q}, +)$ is not isomorphic to $(\mathbb{Q}^+, .)$.

Solution. Let $f : \mathbb{Q} \to \mathbb{Q}^+$ be an isomorphism and $3 \in \mathbb{Q}^+$.

Hence there exists $x \in \mathbb{Q}$ such that $3 = f(x) = f(x/2 + x/2) = f(x/2)f(x/2) = [f(x/2)]^2$.

But, there is no rational number y such that $3 = y^2$. Hence there does not exist any isomorphism between $(\mathbb{Q}, +)$ and $(\mathbb{Q}^+, .)$.

16.6 Automorphism

If $f : G \to G$ is an isomorphism then f is called **automorphism.**

Example 16.11 Let G be any group and g be a fixed element in G. Define $\phi : G \to G$ by $\phi(x) = gxg^{-1}$ for all $x \in G$. Prove that ϕ is an automorphism of G.

Solution. Given $\phi : G \to G$ such that $\phi(x) = gxg^{-1}$ for all $x \in G$.

To prove ϕ is homomorphism

Let $x_1, x_2 \in G$, then $\phi(x_1) = gx_1g^{-1}$ and $\phi(x_2) = gx_2g^{-1}$

Now,

$$\begin{aligned} \phi(x_1x_2) &= g(x_1x_2)g^{-1} \\ &= (gx_1)(x_2g^{-1}) \\ &= (gx_1)(g^{-1}g)(x_2g^{-1}) \text{ [since } gg^{-1} = e \in G] \\ &= (gx_1g^{-1})(gx_2g^{-1}) \\ &= \phi(x_1)\phi(x_2). \end{aligned}$$

Thus ϕ is a homomorphism.

To prove ϕ is one-to-one

Let x_1, x_2 be two distinct elements of G (domain). If possible let, $\phi(x_1) = \phi(x_2)$.

$\Rightarrow gx_1g^{-1} = gx_2g^{-1}$

$\Rightarrow gx_1g^{-1}g = gx_2g^{-1}g$

$\Rightarrow gx_1 = gx_2$

$\Rightarrow g^{-1}gx_1 = g^{-1}gx_2$

$\Rightarrow x_1 = x_2$,

which contradicts that $x_1 \neq x_2$.

Thus ϕ is one-to-one mapping.

To prove ϕ is onto

Let $y \in G$ (codomain) then there exists an element $x \in G$ (domain) such that $\phi(x) = y$.

$\Rightarrow gxg^{-1} = y$

$\Rightarrow gxg^{-1}g = yg$

$\Rightarrow gx = yg$

$\Rightarrow g^{-1}gx = g^{-1}yg$

$\Rightarrow x = g^{-1}yg \in G$ (domain).

Therefore, ϕ is an onto mapping.

Thus ϕ is one-to-one and onto homomorphism from G to G. Hence ϕ is automorphism itself.

Definition 16.4 (Inner automorphism) *If G is a group. The mapping $T_g : G \to G$ defined by $T_g(x) = g^{-1}xg$ for all $x \in G$ is an automorphism of G known as* ***inner automorphism.***

An automorphism which is not inner is called an ***outer automorphism.***

Let us consider a mapping $f : a \to a^{-1}$ for all $a \in G$, where G is a group. The mapping is one-one and onto, because inverse of an element of a group is unique and each element has an inverse.

Suppose G is abelian. Now $f(ab) = (ab)^{-1} = (ba)^{-1} = a^{-1}b^{-1} = f(a)f(b)$.

Hence f is an automorphism of G.

If G is not abelian then $f(ab) = (ab)^{-1} = b^{-1}a^{-1} = f(b)f(a) \neq f(a)f(b)$. That is, f is not homomorphism and hence in this case f is not an automorphism.

Different automorphisms can be defined from a group to another group. Let $A(G)$ be the set of all automorphism of a group G, i.e. $A(G) = \{f : f$ is an automorphism of $G\}$.

It can be shown that $A(G)$ is a group, which is proved in the following theorem.

Theorem 16.9 *The set of all automorphisms of a group G into itself forms a group with respect to function composition.*

Proof. (i) *Closure property*

Let $f, g \in A(G)$. Then f, g are one-to-one mapping of G onto itself. Therefore, fg is also one-to-one mapping of G onto itself.

Let $a, b \in G$ then $ab \in G$. Now

$$\begin{aligned} (fg)(ab) &= f[g(ab)] = f[g(a)g(b)] \text{ [since } g \in A(G)] \\ &= f[g(a)]f[g(b)] \\ &= (fg)(a)(fg)(b) \end{aligned}$$

Therefore, $fg \in A(G)$.
Hence $A(G)$ is closed with respect to composition of function.

(ii) *Associative property*
We know that the composition of any mapping is associative. Thus $A(G)$ is associative.

(iii) *Existence of identity*
Let i be the identity mapping of G. Then obviously i is one-to-one mapping of G onto itself.
Let $a, b \in G$ then $ab \in G$. Therefore, $i(ab) = ab = (i(a))(i(b))$.
Thus $i \in A(G)$ and hence identity element exists.

(iv) *Existence of inverse*
Let $f \in A(G)$, then f^{-1} exists.
Since f is one-to-one mapping of G onto itself so f^{-1} is also one-to-one.
Let $a, b \in G$ then there exists $x, y \in G$ (domain) such that $f(x) = a$ and $f(y) = b$.
Therefore, $x = f^{-1}(a)$ and $y = f^{-1}(b)$.
Now, $ab = f(x)f(y) = f(xy)$ [since $f \in A(G)$]
$\Rightarrow xy = f^{-1}(ab)$
$\Rightarrow f^{-1}(a)f^{-1}(b) = f^{-1}(ab)$
$\Rightarrow f^{-1} \in A(G)$.
Therefore, each element of $A(G)$ possesses inverse. Hence $A(G)$ is a group with respect to composition of function. □

Theorem 16.10 *$T_{a^{-1}}$ is the inverse of inner automorphism $T_a : x \to a^{-1}xa$, where $T_{a^{-1}} : x \to axa^{-1}$.*

Proof. T_a is defined as $T_a(x) = a^{-1}xa$ for all $x \in G$, a is a fixed element in G.
Then $T_{a^{-1}}(x) = (a^{-1})^{-1}xa^{-1} = axa^{-1}$. Let $y = T_a(x) = a^{-1}xa$, then $x = aya^{-1}$. Now, $T_{a^{-1}}(y) = T_{a^{-1}}(T_a(x)) = T_{a^{-1}}(a^{-1}xa) = a(a^{-1}xa)a^{-1} = (aa^{-1})x(aa^{-1}) = x$.
Therefore, $T_aT_{a^{-1}}(x) = x$.
Similarly, it can be shown that $T_{a^{-1}}T_a(x) = x$.
Thus $T_aT_{a^{-1}}(x) = T_{a^{-1}}T_a(x) = x$ for all $x \in G$.
Hence $T_{a^{-1}}$ is the inverse of T_a, i.e. the inverse of an inner automorphism T_a is an inner automorphism. $T_{a^{-1}}$ is defined by $T_{a^{-1}} = axa^{-1}$ for all $x \in G$.

Theorem 16.11 *The inner automorphisms of any group G form a subgroup denoted by $I_n(G)$ of the group of all automorphism of G.*

Proof. Let $I_n(G)$ be the set of all inner automorphisms. Let $T_a(x) \in I_n(G)$, where $T_a(x) = a^{-1}xa$. The identity inner automorphism $T_e(x) = x \in I_n(G)$. Thus $I_n(G)$ is non-empty.
Let $T_a, T_b \in I_n(G)$. Therefore, $T_a(x) = a^{-1}xa$ and $T_b(x) = b^{-1}xb$.
Now,

$$\begin{aligned} T_aT_{b^{-1}}(x) &= T_a[T_{b^{-1}}(x)] \\ &= T_a(bxb^{-1}) \\ &= a^{-1}(bxb^{-1})a \\ &= (a^{-1}b)x(b^{-1}a) \\ &= (b^{-1}a)^{-1}x(b^{-1}a) \\ &= T_{b^{-1}a}(x). \end{aligned}$$

Thus $T_a T_{b^{-1}} \in I_n(G)$. Hence $I_n(G)$ is a subgroup of all automorphism of G. □

Example 16.12 Let G be a group and ϕ be an automorphism of G. If $a \in G$ is of order $o(a) > 0$ then $o(\phi(a)) = o(a)$.

Solution. Let $o(a) = n > 0$. Therefore, $a^n = e$ and $a^m \neq e$ for $m < n$. (i)

We have to prove that $\{\phi(a)\}^n = e$ and $\{\phi(a)\}^m \neq e$ for $m < n$.

Now, $[\phi(a)]^n = \{\phi(a)\phi(a)\cdots n \text{ times}\}$

$= \phi(a.a.\cdots n \text{ times}) = \phi(a^n) = \phi(e) = e$.

If possible, let m be the order of $\phi(a)$ where $m < n$.

Therefore, $\{\phi(a)\}^m = e$. This implies $\phi(a^m) = e = \phi(e)$. [since ϕ is automorphism]

$\Rightarrow a^m = e$, which contradicts $a^m \neq e$.

Thus $\{\phi(a)\}^n = e$ and $\{\phi(a)\}^m \neq e$ for $m < n$. Hence $o(\phi(a)) = o(a)$.

16.7 Sylow Theorems

If a, b be two elements of a group G, then b is said to be **conjugate to** a if there exists an element $x \in G$ such that $b = x^{-1}ax$. If b is conjugate to a, then symbolically we shall write $b \overset{c}{=} a$ and this relation in G is called the **relation of conjugacy**. Thus $b \overset{c}{=} a$ iff $b = x^{-1}ax$ and conversely $a \overset{c}{=} b$ iff $a = x^{-1}bx$ or $b = xax^{-1}$.

Lemma 16.1 *The conjugacy relation is an equivalence relation.*

Proof. (i) *Reflexive*

If $a \in G$ then we have $a = e^{-1}ae \Rightarrow a \overset{c}{=} a$ for all $a \in G$.

Thus the relation is reflexive.

(ii) *Symmetry*

Let $a \overset{c}{=} b$ holds. Then we have $a = x^{-1}bx$ for some $x \in G$.

$\Rightarrow xax^{-1} = b \Rightarrow b = (x^{-1})^{-1}ax^{-1}$ [since $x^{-1} \in G$].

Hence $b \overset{c}{=} a$ and the relation is symmetric.

(iii) *Transitive*

Let $a \overset{c}{=} b$ and $b \overset{c}{=} c$. Then $a = x^{-1}bx$ and $b = y^{-1}cy$ for some $x, y \in G$. We have

$a = x^{-1}bx = x^{-1}(y^{-1}cy)x = (x^{-1}y^{-1})c(yx) = (yx)^{-1}c(yx)$ where $yx \in G$.

Therefore $a \overset{c}{=} c$ and thus the relation is transitive. Hence the conjugacy relation in a group G is an equivalence relation. □

The equivalence class for an element $a \in G$ with respect to this relation is called **conjugacy class** of a, which is denoted by $cl(a)$. Thus

$$cl(a) = \{x \in G : x \overset{c}{=} a\} = \{x \in G : x = bab^{-1} \text{ for some } b \in G\} = \{xax^{-1} : x \in G\}.$$

If G is finite, then the number of conjugacy classes are finite. If $a_1, a_2, \ldots, a_k$ are representatives from each of the distinct conjugacy classes, then

$$G = cl(a_1) \cup cl(a_2) \cup \cdots \cup cl(a_k).$$

Definition 16.5 (Centralizer) *Let G be a group and $a \in G$. Then the centralizer of a is the subset $C(a) = \{x \in G : xa = ax\}$.*

Clearly, $e, a \in C(a)$ and it can be shown that $C(a)$ is a subgroup of G such that $Z(G) \subseteq C(a)$.

Theorem 16.12 *In a finite group G, for each $a \in G$, the number of different conjugates of a in G equals the number of distinct left cosets of the subgroup $C(a)$ in G, i.e. $|cl(a)| = [G : C(a)]$, where $|cl(a)|$ denotes the number of elements in $cl(a)$.*

Alternatively, in a finite group G the number of elements in $cl(a)$ of all elements conjugate to a in G is the index of normalizer of a in G, i.e.

$$|cl(a)| = [G : N(a)] = \frac{o(G)}{o(N(a))}.$$

Corollary 16.1 *For a finite group G*

$$o(G) = \sum_{a \in G} |cl(a)| = \sum_{a \in G} \frac{o(G)}{o(N(a))},$$

where the sum runs over one element a in each conjugate class.

Proof. We know that the relation of conjugacy is an equivalence relation on G. Therefore, it partitions G into disjoint conjugate classes. The union of all distinct conjugate classes will be equal to G and two distinct conjugate classes will have no common element. Since G is a finite group therefore, the number of distinct conjugate classes of G will be finite say equal to k. Suppose $cl(a)$ denotes the conjugate class of a in G and $|cl(a)|$ denotes the number of elements in this class. If $cl(a_1), cl(a_2), \cdots, cl(a_k)$ are the k distinct conjugate classes of G then $G = cl(a_1) \cup cl(a_2) \cup \cdots \cup cl(a_k)$.

This implies that the number of elements of in G = the number of elements in $cl(a_1)$ + the number of elements in $cl(a_2) + \cdots +$ the number of elements in $cl(a_k)$.

That is, $o(G) = \sum |cl(a)|$, the summation is being run over each element a in each conjugate class. Hence

$$o(G) = \sum_{a \in G} \frac{o(G)}{o(N(a))}.$$

□

Lemma 16.2 *Let $Z(G)$ be the centre of a group G and let $a \in G$, then $a \in Z(G)$ iff $N(a) = G$.*

Proof. Let $a \in Z(G)$ then by definition of $Z(G)$, we have $ax = xa$ for all $x \in G$. Also, $N(a) = \{x \in G : ax = xa\}$.

Obviously, $N(a) \subseteq G$.

Now, $a \in Z(G) \Rightarrow ax = xa$ for all $x \in G$.

$\Rightarrow x \in N(a)$ by definition of $N(a)$.

$\therefore G \subseteq N(a)$.

$\therefore N(a) = G$.

Conversely, let $N(a) = G$. Therefore, $ax = xa$ for all $x \in G$.

□

Let G be a group and $Z(G)$ be the centre of G. If $a \in Z(G)$ then $cl(a) = \{a\}$ and

Proof. Let $a \in Z(G)$. Thus a commutes each g in G.
That is, $ga = ag$ for all $g \in G$
$\Rightarrow gag^{-1} = agg^{-1}$
$\Rightarrow gag^{-1} = a$ for all $g \in G$.
Hence $cl(a) = \{a\}$.
Conversely, let $cl(a) = \{a\}$. Thus
$g^{-1}ag = a$ for all $g \in G$.
$\Rightarrow ag = ga$ for all $g \in G$
$\Rightarrow ga = ag$ for all $g \in G$
$\Rightarrow a \in Z(G)$. □

From this lemma it follows that the elements of $Z(G)$ are self-conjugate elements. If $a \in Z(G)$, the conjugacy class of a is said to be trivial conjugacy class because it contains a only.

Theorem 16.13 *Let G be a finite group and $Z(G)$ is its centre. Let $cl(a_1), cl(a_2), \ldots, cl(a_m)$ be the distinct multi-numbered conjugacy classes of G. Then*

$$o(G) = o[Z(G)] + \sum_{i=1}^{m} |cl(a_i)|,$$

where $|cl(a_i)|$ denotes the number of distinct elements in the conjugacy class $cl(a_i)$. This equation is knows as class equation.

Proof. If $a \in Z(G)$, then $|cl(a)| = 1$. G is partitioned into distinct conjugacy classes. The elements of $Z(G)$ form single membered conjugacy classes and the elements of $G - Z(G)$ belong to multi-numbered conjugacy classes.

$o(G) = o[Z(G)] + |G - Z(G)| = o[Z(G)] + |cl(a_1)| + |cl(a_2)| + \cdots + |cl(a_m)|$
where $cl(a_1), cl(a_2), \cdots, cl(a_m)$ are distinct conjugacy classes of $G - Z(G)$.

Hence $o(G) = o[Z(G)] + \sum_{i=1}^{m} |cl(a_i)|$. □

Corollary 16.2 *Let G be a finite group and $Z(G)$ be the centre of G. Then the class equations of G can be written as*

$$o(G) = o[Z(G)] + \sum_{a \notin Z(G)} \frac{o(G)}{o[N(a)]} = o[Z(G)] + \sum_{a \notin Z(G)} [G : Z(G)].$$

Theorem 16.14 *If $o(G) = p^n$ where p is a prime number then the centre $Z(G) \neq \{e\}$.*

Proof. Since $N(a)$ is a subgroup of G, then by Lagrange's theorem we have $o[N(a)]/p^n$. Since p is prime, $o[N(a)]$ must be of the form p^{na}, where na is the integer such that $0 < na \leq n$. We have

$$o(G) = \sum \frac{o(G)}{o(N(a))} = \sum_{a} \frac{p^n}{p^{na}},$$

where summation runs over one element a in each conjugacy class.

We assume that there are precisely m elements in $Z(G)$, i.e. $o[Z(G)] = m$.

Now, $a \in N(a) \Rightarrow N(a) = G$
$\Rightarrow o[N(a)] = o(G)$
$\Rightarrow p^{na} = p^n$
$\Rightarrow na = n$.

Hence if $a \notin Z(G)$ then $na < n$. Then

$$p^n = o(G) = o[Z(G)] + \sum_{a \notin Z(G)} \frac{o(G)}{o[N(a)]}$$

$$= m + \sum_{na<n} \frac{p^n}{p^{na}}$$

$$\text{or } m = p^n - \sum_{na<n} \frac{p^n}{p^{na}}.$$

Since p is a divisor of r.h.s. this implies p divides m. Now if $e \in Z(G)$, then $Z(G)$ is non-empty, i.e. $m \geq 1$. Thus the positive integer $m(\neq 0)$ is multiple of the prime number p. Therefore, $m > 1$. Hence $Z(G)$ must contains an element beside e. □

Corollary 16.3 *If $o(G) = p^2$ where p is a prime number then G is abelian.*

Proof. Since p is prime, by Theorem 16.14, $o[Z(G)] > 1$.

But, $Z(G)$ is a subgroup of G. Therefore, by Lagrange's theorem we have $o[Z(G)]/p^2$. Since p is prime and $o[Z(G)] > 1$, $o[Z(G)] = p$ or p^2.

If $o[Z(G)] = p^2$, then $Z(G) = G$ and our proof is complete.

If $o[Z(G)] = p$ then G must contain an element a such that $a \in G$ but $a \notin Z(G)$.

Now, $x \in Z(G) \Rightarrow xa = ax$ for all $x \in G$.
$\Rightarrow x \in N(a)$
$\Rightarrow Z(G) \subseteq N(a)$
$\Rightarrow o[N(a)] > o[Z(G)]$ $[a \in N(a)$ and $a \notin Z(G)]$
$\Rightarrow o[N(a)] > p$.

But, $N(a)$ is a subgroup of G and $o[N(a)]/o(G)$.
Therefore, $o[N(a)] = p^2$ or $N(a) = G$
$\Rightarrow a \in Z(G)$ which contradicts.

Hence $o[Z(G)] \neq p$ but $o[Z(G)] = p^2$, i.e. $G = Z(G)$ which shows that G is an abelian.

□

Theorem 16.15 (Cauchy theorem for abelian group) *Suppose G is a finite abelian group and $p/o(G)$, i.e. p is a divisor of $o(G)$ where p is a prime number. Then there is an element $a(\neq e) \in G$ such that $a^p = e$.*

Proof. We prove this theorem by induction on the order of G.

Clearly, the theorem is true for group of order one. Let the theorem be true for abelian groups of order less than that of G.

If G has no proper subgroups, then G must be of prime order (because every group of composite order possesses proper subgroups). Since p is prime and $p/o(G)$, therefore $o(G)$ must be equal to p.

Also, every group of prime order is cyclic. Therefore, each element $a \neq e$ of G is a generator of G. Thus G has $p-1$ elements $a \neq e$ such that $a^p = a^{o(G)} = e$.

If G has a proper subgroup H, i.e, $H \neq \{e\}$ and $H \neq G$, then if $p/o(H)$, by induction hypothesis the theorem is true for H since H is an abelian group and $o(H) < o(G)$. Therefore, there exists an element $b \in H$, $b \neq e$ such that $b^p = e$. But, $b \in H \Rightarrow b \in G$ because $H \subset G$. Thus there exists an element $b \in G, b \neq e$ such that $b^p = e$.

Suppose p does not divide $o(H)$. Since G is abelian therefore H is a normal subgroup of G and so G/H is a quotient group.

Since G is abelian, therefore G/H is also abelian. Also we have $o(G/H) = \frac{o(G)}{o(H)} < o(G)$ since $o(H) > 1$.

Since $p/o(G)$ and p does not divide $o(H)$, therefore p is a divisor of $\frac{o(G)}{o(H)}$. Hence by induction hypothesis the theorem is true for the group G/H.

Therefore, there exists an element $c \in G$ and $Hc \neq G/H$ such that $(Hc)^p = H$ (since H is the identity of G/H)

Therefore, $o(Hc) = p$.

Now, $(Hc)^p = H \Rightarrow Hc^p = H \Rightarrow c^p \in H$. Therefore, $(c^p)^{o(H)} = e \Rightarrow (c^{o(H)})^p = e$.

This implies either $c^{o(H)} = e$ or $c^{o(H)}$ has order p.

But $c^{o(H)} \neq e$ else $(Hc)^p = H$ yielding $p/o(H)$, a contradiction. Thus $c^{o(H)}$ has order p and $c^{o(H)}$ is the desired element of G. □

Theorem 16.16 (Cauchy theorem) *Let G be a group of finite order and $p/o(G)$ where p is a prime number. Then G contains an element of order p.*

Proof. Suppose the theorem is true for groups of order less than that of G. We shall prove that the theorem is also true for G. If $o(G) = 1$, then there is no such p and the theorem is obviously true.

If there exists a proper subgroup H of G such that $p/o(G)$, then by our induction hypothesis the theorem is true for H since $o(H) < o(G)$. Therefore, there exists an element $a \in H$ such that $o(a) = p$. But, $a \in H \Rightarrow a \in G$ because $H \subset G$. Hence the result.

Now, let p does not divide $o(H)$. Let Z be the centre of G. The class equation of G can be written as

$$o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o[N(a)]} \qquad \text{(i)}$$

Now, $N(a)$ is a subgroup of G. If $a \notin Z$ then $N(a)$ is a proper subgroup of G and hence p does not divide $o[N(a)]$.

But, $p/o(G)$. Therefore, $p \Big/ \frac{o(G)}{o[N(a)]}$ for all $a \notin Z$. This implies

$p \Big/ \sum_{a \notin Z} \frac{o(G)}{o[N(a)]}$ and hence $p \Big/ \left[o(G) - \sum_{a \notin Z} \frac{o(G)}{o[N(a)]}\right]$

From (i) we conclude that $p/o(Z)$.

Thus Z is a subgroup of G and the order of Z is divisible by p. But, according to our assumption p is not a divisor of the order of any proper subgroup of G. Consequently $Z = G$. But, then G is abelian. Therefore, by Cauchy's theorem for abelian groups there exists an element in G of order p. This completes the proof. □

Example 16.13 Prove that every abelian group of order 6 is cyclic.

Solution. Let G be an abelian group of order 6. Since the prime integers 3 and 2 are both divisors of $o(G)$, therefore by Cauchy's theorem for abelian groups there exists elements a and b in G such that $o(a) = 3$, $o(b) = 2$. We shall prove that $o(ab) = 6$ and consequently G will be the cyclic group generated by ab.

We have $b^{-1} \neq a$ since $o(b^{-1}) = o(b) = 2$ while $o(a) = 3$. Thus $ab \neq e$.

Now, $(ab)^2 = a^2b^2 = a^2e = a^2 \neq e$ since $o(b) = 2$. Also, $(ab)^3 = a^3b^3 = eb^3 = b^3 = b^2b = b \neq e$ since $o(a) = 3$.

Therefore, we must have $o(ab) > 3$. But, $o(ab)$ must be a divisor of $o(G)$, i.e. 6 since $o(ab)$ can neither be 4 nor it can be 5. Hence we must have $o(ab) = 6$ and consequently G is cyclic.

Definition 16.6 (P-Sylow subgroup) *Let G be a finite group and $o(G) = p^m n$, where p is a prime number and p is not a divisor of n. Then a subgroup H of G is said to be a p-Sylow subgroup of G iff $o(H) = p^m$.*

Theorem 16.17 (Sylow's Theorem) *Let G be the group of infinite order and p be the prime number. If p^m divides $o(G)$ (m being a positive integer) but p^{m+1} does not divide $o(G)$, G has a subgroup of order p^m.*

Proof. The theorem will be proved by induction on $o(G)$. If $o(G) = 2$, the only relevant prime is 2 and the group certainly has the subgroup of order two namely itself.

So we assume that the result is correct for all groups of order less than the order of G. From this we will show that the result is valid for G.

Suppose p^m divides $o(G)$ and p^{m+1} does not divide $o(G)$, where p is prime and $m \geq 1$. If $p^m / o(H)$ for any subgroup H of G, where $H \neq G$, then by induction hypothesis H has a subgroup T of order p^m. However since T is a subgroup of H and H is a subgroup of G, T is a subgroup of G.

Therefore, we assume that p^m does not divide $o(H)$, for any subgroup H of G, where $H \neq G$. Let us consider the subgroup $N(a)$ of G. Moreover if $a \notin Z(G) \Rightarrow N(a) \neq G$.

By our assumption p^m does not divide $o[N(a)]$, but p^m divides $o(G)$, then we must have p divides $o(G)/o[N(a)]$ for all $a \in G$ and $a \notin Z(G)$. Then p divides $\sum_{a \in Z(G)} o(G)/o[N(a)]$ for all $a \in G$ and $a \notin Z(G)$.

Therefore, the class equation

$$o(G) = o[Z(G)] + \sum_{a \notin Z(G)} \frac{o(G)}{o[N(a)]}$$

gives p divides $o[Z(G)]$.

By Cauchy's theorem $Z(G)$ has an element $b (\neq e)$ of order p. Let B be the cyclic subgroup of G generated by b. Therefore, B is of order p.

Moreover, since $b \in Z(G)$, B must be normal in G.

Hence we can form the quotient group $\overline{G} = G/B$.

Now,

$$o(\overline{G}) = \frac{o(G)}{o(B)} = \frac{o(G)}{p}.$$

Hence $o(\overline{G})$ is certainly less than the order of G. We have p^{m-1} divides $o(\overline{G})$, but p^m does not divide $o(\overline{G})$.

By induction hypothesis $\overline{G}$ has a subgroup $\overline{P}$ of order p^{m-1}.
Let $P = \{x \in G : xB \in \overline{P}\}$. Therefore, P is a subgroup of G. Thus

$$p^{m-1} = o(\overline{P}) = \frac{o(P)}{o(B)} = \frac{o(P)}{p}$$

or $o(P) = p^m$, which implies that $o(P) = p^m$. Therefore, P is required P-Sylow subgroup of G. This completes the induction and hence the proved. □

Example 16.14 If H is a p-Sylow subgroup of G and $x \in G$ then $x^{-1}Hx$ is also a p-Sylow subgroup of G.

Solution. Let G be a finite group and $o(G) = p^m n$ where p is a prime number and p is not a divisor of n. If H is a p-Sylow subgroup of G then $o(H) = p^m$.

Now $x^{-1}Hx$ will be a p-Sylow subgroup of G if $x^{-1}Hx$ is a subgroup of G and $o(x^{-1}Hx) = p^m$.

First we shall show that $x^{-1}Hx$ is a subgroup of G. Let $x^{-1}h_1x$, $x^{-1}h_2x$ be any two elements of $x^{-1}Hx$. Then $h_1, h_2 \in H$.

Also, $(x^{-1}h_1x)(x^{-1}h_2x)^{-1} = x^{-1}h_1xx^{-1}h_2^{-1}(x^{-1})^{-1} = x^{-1}h_1eh_2^{-1}x = x^{-1}h_1h_2^{-1}x \in x^{-1}Hx$ since $h_1h_2^{-1} \in H$.

Therefore, $x^{-1}Hx$ is a subgroup of G.

Now, let f be a mapping from H to $x^{-1}Hx$ defined as $f(h) = x^{-1}hx$ for all $h \in H$.

f is one-one

Let $h_1, h_2 \in H$ then

$f(h_1) = f(h_2) \Rightarrow x^{-1}h_1x = x^{-1}h_2x \Rightarrow h_1 = h_2$.

Hence f is one-one.

f is onto

Let $x^{-1}hx$ be any element of $x^{-1}Hx$. Then $h \in H$ and $f(h) = x^{-1}hx$. Hence f is onto.

Therefore, $o(x^{-1}Hx) = o(H) = p^m$.

Hence $x^{-1}Hx$ is a p-Sylow group of G.

Example 16.15 If a group G has only one p-Sylow subgroup H, then H is normal in G.

Solution. Suppose a group G has only one p-Sylow subgroup H and x be any element of G.

By previous example, $x^{-1}Hx$ is also a p-Sylow subgroup of G. But, H is the only p-Sylow subgroup of G. Therefore, $x^{-1}Hx = H$ for all $x \in G$.

Hence H is a normal subgroup of G.

Solvable groups

Let G be a group and $G = N_0 \supseteq N_1 \supseteq N_2 \supseteq \cdots \supseteq N_n = \{e\}$ be a finite chain of subgroups of G. The chain is called a **subnormal series** if each N_i is normal in N_{i-1}.

A group G is said to be **solvable** if if has a subnormal series $G = N_0 \supseteq N_1 \supseteq N_2 \supseteq \cdots \supseteq N_k = \{e\}$ such that each quotient group N_{i-1}/N_i is abelian.

Such a subnormal series is called a **solvable series** of G.

Example 16.16 Show that every abelian group is solvable.

Solution. Let G be an abelian group. Take $N_0 = G$ and $N_1 = \{e\}$. Then $G = N_0 \supseteq N_1 = \{e\}$ is a solvable series for G. Obviously, $N_1 = \{e\}$ is a normal subgroup of $N_0 = G$ because if a is any element of G, then $a^{-1}ea = a^{-1}a = e \in \{e\}$.

Further, since G is abelian, the quotient group $N_0/N_1 = G/\{e\}$ is also abelian. Hence G is solvable group.

16.8 Direct Product of Groups

Let G_1 and G_2 be two groups. Now, the cartesian product of the sets G_1 and G_2 is the set $G_1 \times G_2$ of all ordered pair (a_1, b_1), where $a_1 \in G_1$ and $b_1 \in G_2$. Define a binary operation $*$ on $G_1 \times G_2$ as follows:

$$(a_1, b_1) * (a_2, b_2) = (a_1a_2, b_1b_2) \text{ for all } (a_1, b_1), (a_2, b_2) \in G_1 \times G_2. \tag{16.1}$$

Here a_1a_2 denotes the product of a_1 and a_2 in the group G_1 and b_1b_2 denotes the product of b_1 and b_2 in the group G_2.

In the following theorem we shall prove that $G_1 \times G_2$ is a group.

Theorem 16.18 *Let G_1 and G_2 be two groups. Then the set*

$$G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1 \text{ and } g_2 \in G_2\}$$

is a group under the binary operations defined in (16.1). Moreover,
(i) $H_1 = \{(a_1, e_2) \in G_1 \times G_2 : e_2$ is the identity element of $G_2\}$ is a normal subgroup of $G_1 \times G_2$ and $G_1 \simeq H_1$.
(ii) $H_2 = \{(e_1, b_2) \in G_1 \times G_2 : e_1$ is the identity of $G_1\}$ is a normal subgroup of $G_1 \times G_2$ such that $G_2 \simeq H_2$.

Proof. It is obvious that the operation defined in (16.1) is well-defined binary operation on $G_1 \times G_2$. The associativity of this operation follows from the group operations of G_1 and G_2. The element (e_1, e_2) is the identity element of $G_1 \times G_2$, where e_1 and e_2 are the identity elements of the groups G_1 and G_2 respectively. Finally (a_1^{-1}, b_1^{-1}) is the inverse of (a_1, b_1) for all $(a_1, b_1) \in G_1 \times G_2$. Hence $(G_1 \times G_2, *)$ is a group.

(i) Since $(e_1, e_2) \in H_1, H_1 \neq \phi$. Let $(a_1, e_2), (a_2, e_2) \in H_1$. Then $(a_1, e_2)^{-1}(a_2, e_2) = (a_1^{-1}a_2, e_2^{-1}e_2) = (a_1^{-1}a_2, e_2) \in H_1$, since $a_1^{-1}a_2 \in G_1$. Now, for any $(a_1, b_1) \in G_1 \times G_2$ and $(g_1, e_2) \in H_1$, we find that $(a_1, b_1) * (g_1, e_2) * (a_1, b_1)^{-1} = (a_1g_1a_1^{-1}, b_1e_2b_1^{-1}) = (a_1g_1a_1^{-1}, e_2) \in H_1$. Hence H_1 is a normal subgroup. Now the function $f_1 : G_1 \to H_1$, defined by $f_1(a_1) = (a_1, e_2)$ is a bijective function and for any $a_1, a_2 \in G_1$, $f_1(a_1a_2) = (a_1a_2, e_2) = (a_1, e_2) * (a_2, e_2) = f_1(a_1)f_1(a_2)$. Hence $G_1 \simeq H_1$.

(ii) Proof is similar to (i). □

The group $(G_1 \times G_2, *)$ is called the **external direct product** or simply **direct product** of the groups G_1 and G_2. It is easy to observed that we can extend the definition for any finite number of groups $G_1, G_2, \ldots, G_n$.

16.9 Module Summary

A function between two groups with a specific property is defined as homomorphism of groups. Since homomorphism is a function, therefore it must have domain and codomain. The domain and codomain are respectively called kernel and image. A bijective homomorphism is called isomorphism. Several properties of homomorphism and isomorphism are presented here. If the domain and codomain are same then the homomorphism is termed as automorphism. A lot of properties on automorphism are provided. The class equation and Sylow theorem are studied here. The cauchy's theorem for abelian groups and for arbitrary groups are stated and proved. A concept of solvable group with an example is given. The direct product between groups is defined in this module.

16.10 Self Assessment Questions

1. Let $G = (\mathbb{R}, +)$ and $G' = (\mathbb{R}^+, .)$. Show that $f : G \to G'$, where $f(a) = 2^a$ for all $a \in G$ is a homomorphism. Find its kernel.

2. If $\mathbb{R}$ is the additive group of real numbers and $\mathbb{R}_+$ is the multiplicative group of positive numbers, then prove that the mapping $f : \mathbb{R} \to \mathbb{R}_+$ defined by $f(x) = e^x$ $(x \in \mathbb{R})$ is an isomorphism.

3. Let $(\mathbb{Z}, +)$ be the additive group of all integers and $(\mathbb{Q} - \{0\})$ be the multiplicative group of non-zero rational numbers. Define $f : \mathbb{Z} \to (\mathbb{Q} - \{0\})$ by $f(x) = 3^x, x \in \mathbb{Z}$.
   Show that f is homomorphism but not isomorphism.

4. Show that the mapping $f : M \to \mathbb{R}^*$ defined by $f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$ is a homomorphism of the multiplicative group M into the multiplicative group $\mathbb{R}^*$ of all non-zero real numbers. Is f an isomorphism ? Justify your answer.

5. If $M = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} : a, b \in \mathbb{Z} \right\}$, show that $f : M \to \mathbb{Z}$ defined by $f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) = a - b$ is a homomorphism.

6. Let $G = (\mathbb{R}, +)$ and $G' = \{z \in \mathbb{C} : |z| = 1\}$ and $f : G \to G'$ defined by $f(x) = e^{2\pi i x}$ for all $x \in G$. Show that f is a homomorphism and ker $f = \mathbb{Z}$.

7. Let $G = (\mathbb{Z}, +)$ and $G' = (\mathbb{Z}, +)$ and $f : G \to G'$ defined by $f(x) = |x|$. Show that f is a homomorphism and ker $f = \{0\}$.

8. Show that the mapping $f : (\mathbb{Z}, .) \to (\mathbb{R}, .)$ defined by $f(x) = x^2$ for all $x \in \mathbb{Z}$ is a monomorphism but not isomorphism.

9. (a) Let $A = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in R \right\}$. Show that the mapping $f : (A, .) \to (\mathbb{R}, +)$ defined by $f\left(\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}\right) = a$ for all $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \in A$ is an isomorphism.

   (b) Let $G = (\mathbb{R}^*, .)$ and $G' = GL(2, \mathbb{R})$. Defined a function $f : G \to G'$ by $a \in \mathbb{R}^*$. Show that f is homomorphism and ker $f = \{1\}$.

(c) If G is a group of real, non-singular, n-square matrices under multiplication show that the determinant function is a homomorphism of G into G', where G' is the group of non-zero real numbers under multiplication.

10. If $\mathbb{R}$ is the additive group of real numbers and $\mathbb{R}^+$ is the multiplicative group of positive real numbers, prove that the mapping $f : \mathbb{R} \to \mathbb{R}^+$ defined by $f(x) = e^x$ for all $x \in \mathbb{R}$ is an isomorphism of $\mathbb{R}$ onto $\mathbb{R}^+$.

11. Let G_1 and G_2 be two groups. Show that the function $f : G_1 \times G_2 \to G_1$ defined by $f(a, b) = a$ for $a \in G_1$ and $b \in G_2$, is a homomorphism. Is it isomorphism?

12. Let $(\mathbb{Z}, +)$ be a group. Prove that the function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $f(a, b) = a + b$ is a homomorphism. Is it isomorphism?

13. Show that the function $f : G \to G$ defined by $f(a) = a^{-1}$ for all $a \in G$ is a homomorphism if G is a commutative group.

14. $f : (\mathbb{C} - \{0\}, .) \to (\mathbb{C} - \{0\}, .)$ defined by $f(z) = z^4$.
(i) Show that f is a homomorphism, (ii) find the kernel of f.

15. Let $\mathbb{C}^* = \mathbb{C} - \{0\}$, where $\mathbb{C}$ is a set of complex numbers. Show that the function $f : (\mathbb{C}^*, .) \to (\mathbb{C}^*, .)$ is a homomorphism and ker $f = \{1, \omega, \omega^2\}$.

16. Let $G = (S, .)$ where $S = \{1, i, -1, -i\}$ and let $f : G \to G$ be defined by $f(a) = a^3$ for all $a \in G$. Show that f is an isomorphism and automorphism.

17. Let $f \quad (\mathbb{C}, +) \to (\mathbb{C}, +)$ be defined by $f(z) = \bar{z}$, the conjugate of z. Then prove that f is automorphism.

18. Let G be a group and a be a fixed element of G. Define a mapping $\phi : G \to G$ by $\phi(x) = a^{-1}xa$. Prove that ϕ is an automorphism.

19. Let H be the set of all complex numbers whose modulus is 1. Then $(H, .)$ is a group. Define a mapping $f : (H, .) \to (H, .)$ by $f(z) = z^3, z \in H$. Prove that f is an epimorphism but not a monomorphism. Find kernel of f.

20. Let $G = (\mathbb{R}^*, .)$ and $f : G \to G$, defined by $\phi(x) = \frac{1}{x}$ for all $x \in \mathbb{R}^*$. Show that f is homomorphism and ker $f = \{1\}$.

21. Let $S = \{z \in \mathbb{C} : z^4 = 1\}$ and $G = (S, .)$, $G' = (\mathbb{Z}_4, +)$. Define a mapping $f : G \to G'$ such that G and G' are isomorphic.

22. (a) Let $S = \{1, -1\}$ and $G = (S, .)$. Define a mapping $f : S_3 \to G$, S_3 is the symmetric group, by

$$f(\rho) = \begin{cases} 1, & \text{if } \rho \text{ is an even permutation} \\ -1, & \text{if } \rho \text{ is an odd permutation} \end{cases}$$

for all $\rho \in S_3$. Show that f is an f an epimorphism but not monomorphism. Also, find its kernel.

(b) Let $G = (\mathbb{R}^*, .)$ and $G' = \{1, -1\}$. Define a function $f : G \to G'$ by

$$f(a) = \begin{cases} 1, & \text{if } a > 0 \\ -1, & \text{if } a < 0. \end{cases}$$

Show that f is homomorphism and find its kernel.

23. Show that the following mappings are homomorphism. Determine the kernel in each case.

(a) $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ where $f(n) = -n$ for all $n \in \mathbb{Z}$

(b) $f : (\mathbb{R}, +) \to (\mathbb{C}^*, .)$ where $f(x) = \cos x + i \sin x$ for all $x \in \mathbb{R}$

(c) $f : (\mathbb{R}, .) \to (\mathbb{R}, +)$ where $f(x) = \log_e x$ for all $x \in \mathbb{R}^+$

(d) $f : (\mathbb{Z}, +) \to (3\mathbb{Z}, +)$ where $f(x) = -3x$ for all $x \in \mathbb{Z}$

24. Show that the following mappings $f : G \to G$ are not homomorphism.

(a) $G = (\mathbb{R}, +)$ and $f(x) = x + 3$, $x \in \mathbb{R}$

(b) $G = (\mathbb{R}^*, .)$ and $f(x) = 2x$, $x \in \mathbb{R}^*$.

25. Let (G, o) be a group and a be a fixed element of G. Prove that the mapping $f_a : G \to G$ by $f_a(x) = a \circ x$, $x \in G$ is a bijective mapping but not a homomorphism.

26. (a) Show that $(S, \times_{12})$ where $S = \{1, 5, 7, 11\}$ is isomorphic to Klein-four group.

(b) Show that the set of matrices $\left\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\right\}$ is isomorphic to $\{e, a, a^2, a^3\}$ where $a^4 = e$ by properly defined mapping and group composition.

(c) Show that every cyclic group of order n is isomorphic to the group $(\mathbb{Z}_n, +_n)$ where $\mathbb{Z}_n$ is the set of equivalence classes for the congruence modulo n over the set of integers.

27. Show that all groups of order two are isomorphic.

28. Show that $(\mathbb{R}^*, .)$ is not isomorphic to $(\mathbb{R}, +)$

16.11 Suggested Further Readings

1. M. Artin, *Algebra*, PHI, 1991.

2. J.B. Fraleigh, *A First Course in Abstract Algebra* , Narosa, New Delhi, 1982.

3. J.A. Gallian, *Contemporary Abstract Algebra*, Narosa, New Delhi, 1999.

4. J.P. Tremblay and R. Manohar, *Discrete Mathematical Structures with Applications to Computer Science*, McGraw-Hill Book Company, 1975.

5. B. Kolman, R.C. Busby and S.C. Ross, *Discrete Mathematical Structures*, 4ed, Pearson Education, 2000.

6. M.K. Sen, S. Ghosh and P. Mukhopadhyay, *Topics in Abstract Algebra*, 2ed, University Press, 2ed, 2006.

7. D.S. Malik, J.M. Mordeson and M.K.Sen, *Fundamental of Abstract Algebra*, The McGraw-Hill Companies, Inc., 1997.

M.Sc. Course
in
Applied Mathematics with Oceanology
and
Computer Programming

PART-I

Paper-II

Module No.- 17

Group-A

Ring, Integral Domain and Field

Module Structure

17.1 Introduction

The three important algebraic structures, viz., ring, integral domain and "eld are also learnt by the students in under graduate course. But, for further study the de"nitions of such algebraic structures and their variations are given here. In this module the ideal and ring homomorphism are introduced here.

17.2 Objectives

After going through this unit you will be able to learn about -

- What is ring homomorphism?
- What is ideal?
- Quotient ring or factor ring
- Euclidean domain/ Euclidean ring
- Greatest common divisor
- Unique factorization theorem
- Polynomial rings

17.3 Keywords

Homomorphism of ring, isomorphism, kernel and image, ideal, principle ideal, maximal ideal, quotient ring, prime ideal, Euclidean domain/ ring, associates, prime element, relatively prime, unique factorization theorem, polynomial rings.

17.4 Ring

A non-empty set R along with two binary compositions $+$ and $.$ usually called addition and multiplication is said to be a ring if the following axioms are satisfied.

A. Under addition composition

(i) *Closure:* $a+b \in R$, for all $a, b \in R$

(ii) *Associative:* $(a+b)+c = a+(b+c)$, for all $a, b, c \in R$

(iii) *Identity:* $a+0 = 0+a = a$, for all $a \in R$, 0 is the additive identity or zero element

(iv) *Inverse:* $a+(-a) = (-a)+a = 0$, for all $a \in R$, $-a$ is the additive inverse of a

(v) *Commutative:* $a+b = b+a$, for all $a, b \in R$.

B. Under multiplicative composition

(vi) *Closure:* $a.b \in R$, for all $a, b \in R$

(vii) *Associative:* $(a.b).c = a.(b.c)$, for all $a, b, c \in R$

C. Under addition and multiplicative compositions

(viii) *Distributive:* $a.(b+c) = a.b + a.c$ and $(b+c).a = b.a + c.a$, for all $a, b, c \in R$.

Alternatively, a ring can be defined as follows:

An algebraic $(R, +, .)$ is said to be a ring if

(i) $(R, +)$ is an abelian group,

(ii) $(R, .)$ is a semi-group,

(iii) both left and right distributive laws hold in R.

Note 17.1 It may be remembered that $0 \in R$ is the symbol to represent additive identity, it is not necessarily the number zero.

Illustrations

1. $\mathbf{R}, \mathbf{Q}, \mathbf{Z}$ all are rings.
2. Set of even integers.
3. Set of complex numbers $\mathbf{C}$.
4. Set of all $n \times n$ matrices.

It may be noted that the identity, inverse and commutative axioms under multiplication are not included in the definition of ring. If a ring satisfies one or more of these axioms then different types of rings can be defined. Such rings are defined below.

Definition 17.1 (Commutative ring) *If a ring satisfies commutative axiom under multiplication is called a commutative ring.*

If the multiplication is not commutative, then the ring is said to be ***non-commutative.***

For examples, $(\mathbf{Z}, +, .)$ is a commutative ring but, $(M, +, .)$, where M is the set of all $n \times n$ matrices, is non-commutative ring.

Definition 17.2 (Ring with unity) *If a ring contains a multiplicative identity then it is called a ring with unity. The multiplicative identity is generally denoted by the symbol 1.*

If R is a ring with unity then $a \in R$ is called invertible, if there exists $b \in R$ such that $a.b = b.a = 1$. The element b is said to be the multiplicative inverse of a and a is called the *unity* in R.

For example, $(\mathbf{Z}, +, .)$ is a ring with unity but, the set of even integers is a ring without unity.

Definition 17.3 (Zero ring or trivial ring) *It can be shown that the singleton $\{0\}$ is a ring and this ring is known as* ***zero-ring*** *or* ***trivial ring.***

Thus a ring containing two or more elements is a ***non-trivial ring.***

Definition 17.4 (Divisor of zero) *Let a, b be any two elements of a ring and $a.b = 0$ though $a \neq 0, b \neq 0$ then a and b are called* ***divisor of zero.***

For example, let $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}$. Then $AB = 0$ although $A \neq 0$ and $B \neq 0$. Therefore, A and B are divisor of zero.

Definition 17.5 (Ring with or without zero divisors) *Let $(R, +, .)$ be a ring and $a, b \in R$. If $a.b = 0$ but $a \neq 0, b \neq 0$ then R is said to be ring with* ***zero divisors.***

If $a.b = 0$ implies $a = 0$ or $b = 0$ for all $a, b \in R$, then R is called a ***ring without zero divisors.***

For example, $(\mathbf{Z}, +, .)$ is a ring without zero divisors, but, $(M, +, .)$, where M is a set of all $n \times n$ matrices, is a ring with zero divisors.

Definition 17.6 (Division ring or skew field) *A ring $(R, +, .)$ with unity containing at least two elements is called a* ***skew-field*** *or* ***division ring*** *if every non-zero element of R has a multiplicative inverse.*

For example, $(\mathbf{Q}, +, .)$ is a division ring, but, $(\mathbf{Z}, +, .)$ is not a division ring.

Simple properties

1. The unit element of a ring with unity is unique.
2. If R is a non-trivial ring with unity 1, then $1 \neq 0$.
3. If a is a unit in a ring, then its multiplicative inverse is unique.
4. In a non-trivial ring with unity, the zero has no multiplicative inverse.

Definition 17.7 (Idempotent) *An element a in a ring R is called idempotent if $a^2 = a$.*

In a non-trivial ring the obvious idempotent elements are 0 and 1.

Definition 17.8 (Boolean ring) *A ring R is called a Boolean ring if every element of R is idempotent, i.e., $a^2 = a$ for all $a \in R$.*

Definition 17.9 (Nilpotent) *An element a in a ring R is said to be nilpotent if $a^n = 0$ for some positive integer n. The smallest positive integer which satisfy the condition $a^n = 0$ is called the degree of nilpotency of the element a.*

Example 17.1 Find the nilpotent elements of the ring $\mathbb{Z}_8$.

Solution. The elements of $\mathbb{Z}_8$ are $[0], [1], [2], [3], [4], [5], [6], [7]$.

Here $[2]^3 = [0]$ and $[4]^2 = [0]$. Thus, $[2]$ and $[4]$ are the nilpotent elements of degree 3 and 2 respectively.

Example 17.2 Show that sum of two nilpotent elements of a ring is nilpotent.

Solution. Let a, b be two nilpotent elements of the ring R and their degree of nilpotency be m and n. Then $a^m = 0$ and $b^n = 0$.

Now,

$$\begin{aligned}(a+b)^{m+n} &= a^{m+n} + {}^{m+n}C_1 a^{m+n-1}b + {}^{m+n}C_2 a^{m+n-2}b^2 + {}^{m+n}C_3 a^{m+n-3}b^3 \\ &\quad + \cdots + {}^{m+n}C_{m+n} b^{m+n} \\ &= a^m\{a^n + {}^{m+n}C_1 a^{n-1}b + {}^{m+n}C_2 a^{n-2}b^2 + {}^{m+n}C_3 a^{n-3}b^3 \\ &\quad + \cdots + {}^{m+n}C_n b^n\} \\ &\quad + \{{}^{m+n}C_{n+1} a^{m-1}b + \cdots + b^m\}b^n \\ &= 0 + 0 = 0.\end{aligned}$$

Hence $a + b$ is nilpotent element with degree of nilpotency is $m + n$, sum of the individual degree of nilpotency.

Example 17.3 The set $\{[0], [1], [2], \ldots, [m-1]\}$ of residue classes modulo m is a commutative ring.

Definition 17.10 (Characteristic of a ring) *Let $(R, +, .)$ be a ring. For any $a \in R$, there exists a positive integer n such that $na = 0$, then the smallest value of n is called the characteristic of R.*

If there exists no such integer, then R is of characteristic zero or infinite.

For example, the characteristic of the ring $(\mathbb{Z}, +, .)$ is zero. In this ring the order of each element of $(\mathbb{Z}, +)$ is zero except the identity element.

Example 17.4 Find the characteristic of the ring $(\mathbb{Z}_6, +, .)$.

Solution. The set $\mathbb{Z}_6$ is $\{[0], [1], [2], [3], [4], [5]\}$.
Here $[0]$ is the zero element of $\mathbb{Z}_6$.
Now, $1[0] = [0], 6[1] = [0], 3[2] = [0], 2[3] = [0], 3[4] = [0], 6[5] = [0]$.
Hence the characteristic of $\mathbb{Z}_6$ is 6.
In fact, the characteristic of the ring $(\mathbb{Z}_n, +, .)$ is n.

Example 17.5 Find all idempotent elements of the ring $\mathbb{Z}_6$.

Solution. The elements of $\mathbb{Z}_6$ are $[0], [1], [2], [3], [4], [5]$.
Now, $[0][0] = [0]$, i.e., $[0]^2 = [0]$, $[0]$ is idempotent.
$[1][1] = [1]$, i.e., $[1]^2 = [1]$, $[1]$ is idempotent.
$[2][2] = [4] \neq [2]$, $[3][3] = [3]$, i.e., $[3]^2 = [3]$, $[3]$ is idempotent.
$[4][4] = [4]$, i.e., $[4]^2 = [4]$, $[4]$ is idempotent.
$[5][5] = [1] \neq [5]$.
Hence the idempotent elements of $\mathbb{Z}_6$ are $[0], [1], [3]$ and $[4]$.
Like subgroup of a group one can define the subring of a ring R.

Definition 17.11 (Subring) *Let $(R, +, .)$ be a ring and let S be a non-empty subset of R. If $(S, +, .)$ is a ring then S is called subring of R.*

Illustrations

1. $(\mathbb{Z}, +, .)$ is a subring of $(\mathbb{Q}, +, .)$.
2. $(\mathbb{Q}, +, .)$ is a subring of $(\mathbb{R}, +, .)$, which is also subring of $(\mathbb{C}, +, .)$.
3. Every non-zero ring has two trivial subrings, the ring itself and the zero-ring.

Theorem 17.1 *Let R be a ring and S be a non-empty subset of R. A necessary and sufficient condition that S is a subring of R is*

$$\text{(i) } a - b \in S \text{ and (ii) } ab \in S \text{ for all } a, b \in S. \tag{17.1}$$

Definition 17.12 (Centre of a ring) *Let R be a ring. Define*

$$C(R) = \{a \in R : xa = ax \text{ for all } x \in R\}. \tag{17.2}$$

$C(R)$ is called the centre of R.

17.5 Integral Domain

Definition 17.13 (Integral domain) *A non-trivial ring R with unity is said to be an integral domain if it is commutative and contains no divisor of zero.*

From this definition it follows that an integral domain D must have at least two elements 0 and 1.
Alternatively, a set D is called an integral domain if the following axioms hold.

A. Under additive composition
(i) *Closure:* $a + b \in D$, for all $a, b \in D$

(ii) *Associative:* $a + (b + c) = (a + b) + c$, for all $a, b, c \in D$
(iii) *Identity:* $a + 0 = 0 + a = a$, for all $a \in D$
(iv) *Inverse:* $a + (-a) = 0 = (-a) + a$, for all $a \in D$
(v) *Commutative:* $a + b = b + a$, for all $a, b \in D$.

B. Under multiplicative composition
(vi) *Closure:* $a.b \in D$, for all $a, b \in D$
(vii) *Associative:* $a.(b.c) = (a.b).c$, for all $a, b, c \in D$
(viii) *Identity:* $a.1 = 1.a = a$, for all $a \in D$
(ix) *Commutative:* $a.b = b.a$, for all $a, b \in D$
(x) *Without zero-divisor:* $a.b = 0 \Rightarrow a = 0$ or $b = 0$.

C. Distributive laws
(xi) $a.(b + c) = a.b + a.c$ and $(a + b).c = a.c + b.c$ for all $a, b, c \in D$.

The rings $(\mathbb{Z}, +, .)$, $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$ and $(\mathbb{C}, +, .)$, all are integral domains. The ring of even integers is not an integral domain as it has no identity element. $(\mathbb{Z}_5, +, .)$ is an integral domain while $(\mathbb{Z}_6, +, .)$ is not an integral domain as $[3], [4] \in \mathbb{Z}_6$ and $[3][4] = [0]$, with zero-divisor.

In the following theorem a sufficient condition is given for which $\mathbb{Z}_p$ becomes an integral domain.

Theorem 17.2 *The characteristic of an integral domain is either zero or prime.*

Proof. Let R be an integral domain and its characteristic be n. If $n = 0$ then there is nothing to do. Suppose $n \neq 0$. Then $na = 0$ for all $a \in R$. Also, $n1 = 0$ since $1 \in R$.

Now, suppose n is not prime. Then $n = pq$ for some integers p, q where $1 < p < n$ and $1 < q < n$.

Therefore, $n1 = 0 \Rightarrow pq1 = 0 \Rightarrow (p1)(q1) = 0$. This implies either $p1 = 0$ or $q1 = 0$ [since R is without zero-divisor]

None of these are true, because if $p1 = 0$ and $a \in R$ then $pa = p(1a) = (p1)a = 0 \Rightarrow p(< n)$ is the characteristic of R which contradicts that n is the characteristic of R. Thus n is prime. □

17.6 Field

A commutative ring with unity satisfies all five axioms for an abelian group except multiplicative inverse. If it satisfies this axiom for every non-zero element then this ring becomes another important algebraic structure called field.

Definition 17.14 (Field) *A commutative ring with unity, containing at least two elements, is called a field if every non-zero element has inverse.*

That is, a set F containing at least two elements, is a field if the following axioms hold for all $a, b, c \in F$.

A. Under additive composition
(i) *Closure:* $a + b \in F$
(ii) *Associative:* $a + (b + c) = (a + b) + c$
(iii) *Identity:* $a + 0 = 0 + a = a$, $0 \in F$
(iv) *Inverse:* $a + (-a) = 0 = (-a) + a$, $-a \in F$
(v) *Commutative:* $a + b = b + a$.

B. Under multiplicative composition
(vi) *Closure:* $a.b \in F$
(vii) *Associative:* $a.(b.c) = (a.b).c$
(viii) *Identity:* $a.1 = 1.a = a$, for all $1 \in F$
(ix) *Inverse:* $a.a^{-1} = a^{-1}.a = 1, a^{-1} \in F$ where $a \neq 0$
(x) *Commutative:* $a.b = b.a$

C. Distributive laws
(xi) $a.(b + c) = a.b + a.c$ and $(a + b).c = a.c + b.c$ for all $a, b, c \in F$.

The rings $(\mathbf{R}, +, .)$, $(\mathbf{Q}, +, .)$, $(\mathbf{C}, +, .)$ are fields. The ring $(\mathbf{Z}, +, .)$ is not a field as it has no inverse.

It can be shown that the multiplicative inverse of a non-zero element in a field is unique.

From the definitions of field and integral domain we see that there is only one difference between them. The integral domain is without zero-divisor and in field every non-zero element has inverse.

Theorem 17.3 *The characteristic of a field is either 0 or a prime number.*

Let S be a non-empty subset of the field $(F, +, .)$. If $(S, +, .)$ is a field the it is said to be **subfield** of F. The set of rational numbers $\mathbf{Q}$ is a subfield of the field of real numbers $\mathbf{R}$.

Theorem 17.4 *A subset S of a field $(F, +, .)$ having at least two elements is a subfield iff*
(i) $a - b \in S$ for all $a, b \in S$, and
(ii) $ab^{-1} \in S$ for all $a \in S, b(\neq 0) \in S$.

17.7 Ideal

A subring satisfies some special algebraic structure called ideal, which is defined below.

Definition 17.15 (Left ideal) *A non-empty subset S of a ring $(R, +, .)$ is said to be a left ideal of R if $(S, +)$ is a subring of R and $r.a \in S$ for all $r \in R$ and for all $a \in S$.*

Definition 17.16 (Right ideal) *A non-empty subset S of a ring $(R, +, .)$ is said to be a right ideal of R if $(S, +)$ is a subring of R and $a.r \in S$ for all $r \in R$ and for all $a \in S$.*

If S is a left ideal as well as right ideal of R then S is called a **two-sided ideal** or simply an **ideal** of R. That is, if S is an ideal of R, $(S, +)$ is a subgroup of R and $r.a \in S, a.r \in S$ for all $r \in R$ and for all $a \in S$.

From definition it follows that for a commutative ring left ideal is an right ideal.

Every ring has two ideals. One the singleton $\{0\}$ known as **zero-ideal** and other is the ring itself called **unit ideal**. These two ideals are called **improper ideals**. A ring without no proper ideal is said to be a **simple ring**.

For example, $S = \{kx : x \in \mathbf{Z}$, for any fixed $k\}$ is an ideal of the ring $(\mathbf{Z}, +, .)$.

Theorem 17.5 *Every ideal S of a ring R is a subring of R.*

Proof. Since $(S,+)$ is a subgroup, therefore, $a-b \in S$ for all $a,b \in S$. Also, $r.a \in S, a.r \in S$ for all $r \in R$ and $a \in S$. Since $S \subseteq R$, $r.a \in S, a.r \in S$ for all $r \in S$ and $a \in S$. Hence S is a subring of R. □

But, the converse of this theorem is not true. For example, $(\mathbf{Z},+,.)$ is a subring of $(\mathbf{Q},+,.)$ but it is not an ideal.

Theorem 17.6 *Intersection of two ideals of a ring is an ideal of the ring.*

Proof. Let S and T be two ideals of the ring $(R,+,.)$. Therefore, $(S,+)$ and $(T,+)$ are subgroups of R. Hence $S \cap T$ is also a subgroup of R w.r.t. addition.

Let $a \in S \cap T$. That is, $a \in S$ and $a \in T$. Since S is an ideal, $a.r \in S$ and $r.a \in S$ for all $r \in R$ and for all $a \in S$.

Again, T is an ideal. Thus, $r.a \in T$ and $a.r \in S$ for all $r \in R$ and $a \in T$.

Therefore, $a.r \in S \cap T$ and $r.a \in S \cap T$ for all $r \in R$ and $a \in S$. Hence $S \cap T$ is an ideal.

□

This result is valid for arbitrary number of ideals (left ideals and also for right ideals).

But, the union of ideals may not be an ideal. For example, $2\mathbf{Z}$ and $5\mathbf{Z}$ are ideals of $\mathbf{Z}$ but $2\mathbf{Z} \cup 5\mathbf{Z}$ is not an ideal of $\mathbf{Z}$.

Theorem 17.7 *A field has no proper ideals.*

Proof. Let F be a filed and S be a non-zero ideal of it.

Let $a \in S, a \neq 0$. Then $a^{-1} \in F \Rightarrow a.a^{-1} \in S$ since S is an ideal.

$\Rightarrow 1 \in S$. (1 being the identity element).

Thus for all $a \in F, 1 \in S \Rightarrow 1.a \in S \Rightarrow a \in S$. That is, $a \in F \Rightarrow a \in S$ and hence $F \subseteq S$.

Again, by definition $S \subseteq F$. Thus $S = F$. Hence F has only two ideals $\{0\}$ and F itself. □

Example 17.6 Show that $S = \{kx : x \in \mathbf{Z}, k \text{ is a fixed integer}\}$ is an ideal of $\mathbf{Z}$.

Solution. The set S is $\{\ldots, -3k, -2k, -k, 0, k, 2k, 3k, \ldots\}$.

To prove $(S,+)$ *is a group*

Let $km, kn \in S$; $m, n \in \mathbf{Z}$.

Then $km + kn = k(m+n) \in S$ as $m+n \in S$. Therefore, S is closed.

Obviously, $(km+kn)+kp = km+(kn+kp)$ for all $km, kn, kp \in S$.

Associative law holds.

Now, $0 \in S$ and $0 + km = km = km + 0$ for all $km \in S$. o is the identity element.

Since $km + (-km) = 0 = (-km) + km$, $-km \in S$ is the inverse of $km \in S$. That is, inverse exists for all elements of S.

Hence S is a group.

Let $r \in \mathbf{Z}$ and $km \in S$. Then $r.km = k(rm) \in S$ since $r \in \mathbf{Z}, m \in \mathbf{Z}$ so $rm \in \mathbf{Z}$.

Similarly, $(km).r = k(mr) \in S$.

That is, for all $r \in \mathbf{Z}, km \in S, r.(km) \in S$ and $(km).r \in S$.

Hence S is an ideal of $\mathbf{Z}$.

The following result is the generalization of this result.

Example 17.7 Let R be a ring. Then $nR = \{nx : x \in R\}, n \in \mathbf{N}$, is an ideal of R.

Since $\mathbf{Z}$ is a ring, therefore, $2\mathbf{Z}, 3\mathbf{Z}, 4\mathbf{Z}, \ldots$ etc. are ideal of $\mathbf{Z}$.

Example 17.8 Show that the set of matrices $S = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}$ is a left ideal but not a right ideal of 2×2 real matrices.

Solution. Let $M_2(\mathbb{R})$ be the set of all 2×2 real matrices.

To prove $(S, +)$ *is a group.*

Let $A = \begin{pmatrix} a_1 & 0 \\ b_1 & 0 \end{pmatrix}, B = \begin{pmatrix} a_2 & 0 \\ b_2 & 0 \end{pmatrix} \in S$. Then $A + B = \begin{pmatrix} a_1 + a_2 & 0 \\ b_1 + b_2 & 0 \end{pmatrix} \in S$, i.e., S is closed.

Matrix addition is associative.

$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S$ is the additive identity of S.

$\begin{pmatrix} -a_1 & 0 \\ -b_1 & 0 \end{pmatrix} \in S$ being the inverse of $A \in S$.

Thus $(S, +)$ is a group.

Let $X = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \in M_2(\mathbb{R})$. Then

$$AX = \begin{pmatrix} a_1 & 0 \\ b_1 & 0 \end{pmatrix} \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} = \begin{pmatrix} a_1x_1 & a_1y_1 \\ b_1x_1 & b_1y_1 \end{pmatrix} \notin S \text{ for all } A \in S \text{ and } X \in M_2(\mathbb{R}),$$

but, $$XA = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ b_1 & 0 \end{pmatrix} = \begin{pmatrix} a_1x_1 + b_1y_1 & 0 \\ a_1x_2 + b_1y_2 & 0 \end{pmatrix} \in S$$

for all $A \in S$ and $X \in M_2(\mathbb{R})$.

Thus S is a left ideal but not right ideal.

Theorem 17.8 *If R is a commutative ring the set $Ra = \{xa : x \in R\}$ of all multiplies of any fixed $a \in R$ is an ideal of R.*

Proof. We first prove that Ra is a subgroup of R under addition. Let $x, y \in R$.

Therefore, by definition $xa, ya \in Ra$. Now

$xa - ya = (x - y)a \in Ra$ [since $x - y \in R$]

Therefore, Ra is a subgroup of R under addition.

Next we shall prove that for every $xa \in Ra$ and $z \in R$, both $(xa)z$ and $z(xa)$ are in Ra.

For $xa \in Ra$ and $z \in R$. Now,

$z(xa) = (zx)a \in Ra$ [since $zx \in R$]

and $(xa)z = x(az)$ [by associative]

$= x(za)$ [by commutative in R]

$= (xz)a \in Ra$ [associative and $xz \in R$]

Hence Ra is an ideal of R.

This ideal is known as principal ideal. The formal definition of principal ideal is given below. □

Definition 17.17 *The ideal $Ra = \{xa : x \in R\}$ which consists of all the multiplies of same fixed a in R is called principal ideal.*

Theorem 17.9 *A commutative ring with unity has no proper ideals iff it is a filed.*

Proof. Let R be a commutative ring with unity. Let us assume that R is a filed. Then for any element $a \in R$, $a^{-1} \in R$.

Let H be an ideal of R. Let us assume that $a \in H$. Since $a \in H$ and $a^{-1} \in R$. Therefore, $aa^{-1} = 1 \in H$ [since H is an ideal]

Now, considering any element $x \in R$, we have

$x.1 \in H$ [since $1 \in H$]

$\Rightarrow x \in H$ for all $x \in R$

$\Rightarrow H = R$.

Hence R has no proper ideal.

Conversely, let R has no proper ideal. If R is not a field then there exists at least one element a which has no multiplicative inverse in R. Let us consider the principal ideal $Ra = \{xa : x \in R\}$. Now since a has no inverse, the product of a with any element of R does not give 1. Therefore, in this case $1 \in R$ but $1 \notin Ra$.

Therefore Ra is the proper ideal. Contradiction proves that R is a field. □

17.8 Quotient Ring

Let H be an ideal of a ring R. Let R/H denotes the family of cosets of H in R, i.e. $R/H = \{H + a : a \in R\}$. Let $H + a, H + b$ be two arbitrary elements of R/H. Define the operations of addition and multiplication of R/H as follows:

$$\begin{aligned}(H + a) + (H + b) &= H + (a + b)\\ (H + a).(H + b) &= H + ab.\end{aligned}$$

In the following we prove that R/H is a ring.

Theorem 17.10 *Given an ideal H of a ring R the additive coset $H + a$ of H form the quotient ring R/H under the definition*

$$(H + a) + (H + b) = H + (a + b) \tag{17.3}$$

$$(H + a).(H + b) = H + ab \tag{17.4}$$

for all $a, b \in R$.

Proof. Since $H + (a + b)$ and $H + ab$ are also residue classes of H in R, therefore R/H is closed with respect to addition and multiplication of residue classes. First of all we shall show that both addition and multiplication in R/H are well defined. For this we are to show that if $H + a = H + a'$ and $H + b = H + b'$ then $(H + a) + (H + b) = (H + a') + (H + b')$ and $(H + a)(H + b) = (H + a')(H + b')$.

We have $H + a = H + a' \Rightarrow a' \in H + a$ and $H + b = H + b' \Rightarrow b' \in H + b$.

Therefore, there exists $x, y \in H$ such that $a' = x + a, b' = y + b$.

Now, $a' + b' = (x + a) + (y + b) = (a + b) + (x + y)$

Therefore, $(a' + b') - (a + b) = x + y \in H$

Thus $H + (a' + b') = H + (a + b)$

$\Rightarrow (H + a') + (H + b') = (H + a) + (H + b)$.

Thus addition in R/H is well defined. Similarly, we can prove that multiplication is also well defined.

Associativity of addition in R/H
We have $(H+a)+[(H+b)+(H+c)]$
$=(H+a)+[H+(b+c)]=H+[a+(b+c)]$
$=H+[(a+b)+c]=[H+(a+b)]+(H+c)$
$=[(H+a)+(H+b)]+(H+c)$.

Commutativity of addition in R/H
$(H+a)+(H+b)=H+(a+b)=H+(b+a)=(H+b)+(H+a)$.
Existence of additive identity
Since $(H+a)+(H+0)=H+(a+0)=H+a$ and also $(H+0)+(H+a)=H+(0+a)=H+a$.
Hence $H+0=H$ is the additive identity of R/H.

Existence of additive inverse
Let $H+a\in R/H$. Then $H+(-a)\in R/H$.
Now, $[H+(-a)]+(H+a)=H+[(-a)+a]=H+0=H$,
Therefore, $H+(-a)$ or $H-a$ is the additive inverse of $H+a$.

Associativity of multiplication
$(H+a)[(H+b)(H+c)]=(H+a)[H+bc]=H+[a(bc)]=H+[(ab)c]$
$=(H+ab)(H+c)=[(H+a)(H+b)](H+c)$.

Distributivity property
$(H+a)[(H+b)+(H+c)]=(H+a)[H+(b+c)]=H+[a(b+c)]$
$=(H+ab)+(H+ac)=(H+a)(H+b)+(H+a)(H+c)$.
Similarly, it can be shown that
$[(H+b)+(H+c)](H+a)=(H+b)(H+a)+(H+c)(H+a)$.
Hence R/H is a ring with respect to the two compositions. □

Definition 17.18 *Let R be a ring and H be an ideal of R. Then the ring $R/H=\{H+a : a\in R\}$ is called the* ***quotient ring*** *or* ***factor ring*** *or a* ***difference ring*** *or a* ***residue class ring****, where addition $(+)$ and multiplication $(.)$ are defined as*
$(H+a)+(H+b)=H+(a+b)$ *and* $(H+a)(H+a)=H+ab$ *for all* $a,b\in R$.

Example 17.9 Let us consider the ring $\mathbb{Z}$. Then $3\mathbb{Z}=\{3k : k\in\mathbb{Z}\}$ is an ideal of $\mathbb{Z}$. Then $\mathbb{Z}/3\mathbb{Z}=\{k+3\mathbb{Z} : k\in\mathbb{Z}\}$ and it is a ring, where $+$ and $.$ are defined below.
$(m+3\mathbb{Z})+(n+3\mathbb{Z})=(m+n)+3\mathbb{Z}$ and $(m+3\mathbb{Z})(n+3\mathbb{Z})=mn+3\mathbb{Z}$.

This is the quotient ring of $\mathbb{Z}$ by the ideal $3\mathbb{Z}$. Since $\mathbb{Z}$ is a commutative ring with unity, $\mathbb{Z}/3\mathbb{Z}$ is also a commutative ring with unity.

17.9 Homomorphism of Rings

Like group homomorphism, a homomorphism can also be defined between two rings.

Definition 17.19 *Let R and R' be two rings. A mapping $f : R\to R'$ is called a* ***homomorphism*** *of R into R', if*

$$f(a+b)=f(a)+f(b) \text{ and } f(ab)=f(a)f(b)$$

for all $a,b\in R$.

An injective (surjective) homomorphism is called **monomorphism (respectively epimorphism)**. A bijective homomorphism is called an **isomorphism** and we write $R \simeq R'$. If $R = R'$ then the homomorphism is called an **endomorphism** and a bijective endomorphism is called an **automorphism**.

Example 17.10 Define a mapping $f : \mathbb{Z} \to \mathbb{Z}_n$ by $f(a) = [a]$, where $[a]$ denote the equivalence class of a modulo n, $n \in \mathbb{N}$. Of course, $(\mathbb{Z}, +, .), (\mathbb{Z}_n, +, .)$ both are rings.
Then $f(a+b) = [a+b] = [a] + [b] = f(a) + f(b)$ and $f(ab) = [ab] = [a][b] = f(a)f(b)$ for all $a, b \in R$.
Hence f is a homomorphism of the ring $\mathbb{Z}$ onto the ring $\mathbb{Z}_n$.

Example 17.11 Consider the ring $(\mathbb{Z}, +, .)$. Define $f : \mathbb{Z} \to \mathbb{Z}$ by $f(n) = 2n$. Let $m, n \in \mathbb{Z}$. Then $f(m+n) = 2(m+n) = 2m + 2n = f(m) + f(n)$.
But, $f(mn) = 2mn \neq f(m)f(n)$.
This shows that f is a *group homomorphism but not a ring homomorphism.*

Example 17.12 Let $M = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in R \right\}$ where R is a ring.
Define $f : M \to R$ by $f \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = a$ for all $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \in M$.
Let $A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \in M, B = \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} \in M$. $AB = \begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix}$.
Then $f(A+B) = a + b = f(A) + f(B)$ and $f(AB) = ab = f(A)f(B)$.
Hence f is homomorphism.
Also, $f(A) = f(B)$ only if $a = b$. Thus f is one-one.
Now, for any $a \in R$, $f^{-1}(a) = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \in M$. Therefore, f is onto.
Hence f is an isomorphism.

Theorem 17.11 *Let R and R' be two rings and $f : R \to R'$ be a homomorphism of R into R'. Then*
(i) $f(0) = 0'$ where $0 \in R$ and $0' \in R'$ be the zero elements
(ii) $f(-a) = -f(a)$
(iii) $f(a-b) = f(a) - f(b)$
for all $a, b \in R$.

Proof. (i) Let $a \in R$, then $f(a) \in R'$. Now,
$f(0) = f(0+0)$
$\Rightarrow f(0) + 0' = f(0) + f(0)$ [since f is homomorphism]
$\Rightarrow 0' = f(0)$.
(ii) Let a be any element of R, then $-a \in R$. Also, $f(0) = 0'$
Therefore, $f(a-a) = f(0)$
$\Rightarrow f(a) + f(-a) = f(0)$ [since f is homomorphism]
$\Rightarrow f(a) + f(-a) = 0'$.
Therefore, $f(-a)$ is the additive inverse of $f(a)$ in the ring. Hence $f(-a) = -f(a)$.
(iii) Since f is homomorphism,
$f(a-b) = f(a+(-b)) = f(a) + f(-b) = f(a) - f(b)$ [by (ii)].

Example 17.13 Let R be a ring and let $(S, +, .)$ be an algebraic system with addition $(+)$ and multiplication $(.)$. Let $f : R \to S$ be an epimorphism for $+$ and $.$. Then show that S is a ring.

Solution. Let $a, b, c \in S$ and $x, y, z \in R$. Assume that $a = f(x), b = f(y), c = f(z)$.

Since R is a ring, $x, y \in R \Rightarrow x + y \in R$.

Now, $a + b = f(x) + f(y) = f(x + y) \in S$ [since f is homomorphism].

Therefore, closure property holds.

(ii)

$$\begin{aligned}(a+b)+c &= [f(x)+f(y)]+f(z)\\ &= f(x+y)+f(z) \quad \text{[since } f \text{ is homomorphism]}\\ &= f(x+y+z)\\ &= f(x)+f(y+z)\\ &= f(x)+[f(y)+f(z)]\\ &= a+(b+c),\end{aligned}$$

Hence associative property holds.

(iii) Let 0 be the additive identity element of R. Then

$f(x) = f(x + 0) = f(x) + f(0)$.

This implies, $f(0)$ is the additive identity element of S.

(iv) Let $x \in R \Rightarrow -x \in R$.

Now, $f(0) = f(x - x) = f(x) + f(-x)$. Thus $f(-x)$ is the additive inverse of $f(x)$.

(v)

$$\begin{aligned}a+b = f(x)+f(y) &= f(x+y) \quad \text{[since } f \text{ is homomorphism]}\\ &= f(y+x) \quad \text{[since in } R,\ x+y = y+x]\\ &= f(y)+f(x) = b+a.\end{aligned}$$

Therefore, a, b are commutative under addition.

Hence $(S, +)$ is a commutative group.

(vi) Let $x, y \in R \Rightarrow x.y \in R$. Since f is homomorphism,

$a.b = f(x).f(y) = f(x.y) \in S$.

Hence S is closed under multiplication.

(vii) $(a.b).c = [f(x).f(y)].f(z) = f(x.y).f(z) = f(x.y.z)$

$= f(x).f(y.z) = f(x)[f(y).f(z)] = a.(b.c)$.

Hence S satisfies associative property under multiplication.

(viii)

$$\begin{aligned}a.(b+c) &= f(x).[f(y)+f(z)]\\ &= f(x).f(y+z)\\ &= f[x.(y+z)]\\ &= f(xy+xz)\\ &= f(xy)+f(xz)\\ &= f(x).f(y)+f(x).f(z)\\ &= a.b+a.c.\end{aligned}$$

That is, left distributive property holds. Similarly, we can prove right distributive law.

Hence $(S, +, .)$ is the ring under addition $(+)$ and multiplication $(.)$.

Definition 17.20 (Kernel) *Let R and R' be two rings and $f : R \to R'$ be a homomorphism of R into R'. Then the kernel of f is denoted by* ker f *and is defined as*

$$\ker f = \{x \in R : f(x) = 0', 0' \text{ is the zero element of } R'\}.$$

Example 17.14 If f is a homomorphism of R into R' with kernel ker f, then
(i) ker f is the subgroup of R under addition,
(ii) if $a \in ker\ f$ and $r \in R$, then both ar and ra are in ker f.

Solution. (i) The ring R and R' are both commutative group under addition (+). Thus ker f is a normal subgroup of R. Hence obviously, ker f is a subgroup of R under addition.

(ii) For $a \in ker\ f$, $r \in R \Rightarrow ar \in R$ and $f(a) = 0'$, $0'$ is the additive identity element of R'.

Since f is homomorphism,

$f(ar) = f(a)f(r) = 0'f(r) = 0' \Rightarrow ar \in ker\ f$.

Similarly, $f(ra) = 0' \Rightarrow ra \in ker\ f$.

Hence $ra, ar \in ker\ f$.

Theorem 17.12 *Let R and R' be two rings and $f : R \to R'$ be a homomorphism. Then ker f is an ideal of R.*

Proof. By definition ker $f = \{x \in R : f(x) = 0', 0' \in R'\}$.

Since $f(0) = 0'$, 0 is the zero element of R. Thus $0 \in$ ker f. Henoe ker f is non-empty. Let $a, b \in$ ker f.

Then $f(a) = 0'$ and $f(b) = 0'$. Since $a \in R, -b \in R$.

Now, $f(a - b) = f(a + (-b)) = f(a) + f(-b)$ [$\because f$ is homomorphism]

$= f(a) - f(b) = 0' - 0' = 0'$.

Therefore, $a - b \in$ ker f.

Again, let r be any element of R. Then for any $a \in R$,

$f(ar) = f(a)f(r) = 0'f(r) = 0'$ and similarly, $f(ra) = f(r)f(a) = f(r)0' = 0'$.

Therefore, $ar \in$ ker f and $ra \in$ ker f.

Hence ker f is an ideal of R. □

Theorem 17.13 *Let R be a ring and S be an ideal of R and $f : R \to R/S$ defined by $f(a) = S + a$ for all $a \in R$.*

Then f is a homomorphism of R onto R/S.

Proof. Here $R/S = \{S + a : a \in R\}$ and $f(a) = S + a$.

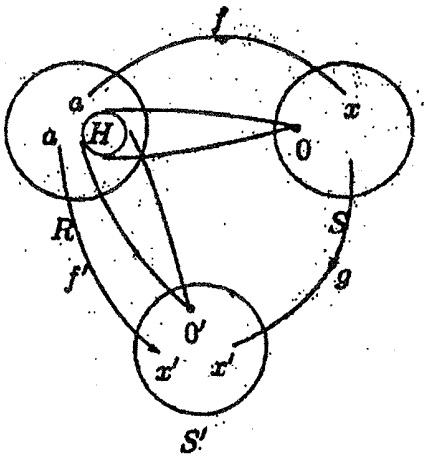
Let $a, b \in R$. Then $f(a + b) = S + (a + b) = (S + a) + (S + b) = f(a) + f(b)$ and $f(ab) = S + ab = (S + a)(S + b) = f(a)f(b)$ for all $a, b \in R$.

Therefore, f is a homomorphism of R onto R/S.

For all $x \in R, S + x \in R/S$ and $f(x) = S + x$. Thus the mapping f is onto R/S. □

Theorem 17.14 *Let $f : R \to S$ and $f' : R \to S'$ be two epimorphisms of ring with the same domain R and kernel H. Then show that the mapping from S to S' is isomorphism.*

Proof. Since f and f' are epimorphism from R to S and S' respectively. Then for $x \in S$ and $x' \in S'$ we must find $a \in R$ such that $f(a) = x$ and $f'(a) = x'$.



We consider a coset $(a+H)$ in R/H. Clearly,
$f(a+H) = f(a) + f(H)$ [since f is epimorphism]
$= f(a) + 0$ [since $h \in H$ is kernel and $f(H) = 0$, the zero element of S]
$= f(a) = x \in S$.

Thus $f(a+H) = x$.

Similarly, $f'(a+H) = x'$. Let us defined the mapping $g : S \to S'$ such that $g(x) = x'$ iff $f^{-1}(x)$ and $f^{-1}(x')$ correspond to the same additive coset of H.

Since f is the homomorphism therefore for $y = f(b)$ and $y' = f'(b)$ we have
$f[(a+H)+(b+H)] = f(a+H) + f(b+H) = x + y$.

Similarly, $f'[(a+H)+(b+H)] = f'(a+H) + f'(b+H) = x' + y'$

Therefore $g(x+y) = x' + y' = g(x) + g(y)$.

Also, $f[(a+H)(b+H)] = f(a+H)f(b+H) = xy$ [since f is homomorphism]
$\Rightarrow f(ab+H) = xy$.

Similarly, $f'[(a+H)(b+H)] = x'y'$.

Therefore, $f^{-1}(xy) = ab + H = f'^{-1}(x'y')$ and $g(xy) = x'y' = g(x)g(y)$.

Hence g is homomorphism from ring S to S'. Also g is onto since f and f' are onto.

Assume $g(x) = g(y)$
$\Rightarrow g(x) - g(y) = 0' \in S'$
$\Rightarrow g(x-y) = 0' \in S'$ [since g is a morphism]
$\Rightarrow f^{-1}(x-y) = f'^{-1}(0) = H$.

Therefore, $f(H) = x - y$ since $f(H) = 0$ for kernel.

This implies $x = y$. Hence g is one-one.

Therefore g is an isomorphism from ring S to S'.

Definition 17.21 (Homomorphic image) *A group G' is called a homomorphic image of a group G if there exists an epimorphism f from the group G onto the group G'.*

Example 17.15 Let f be a homomorphism mapping of a ring R into a ring S. Let S' be the homomorphic image of R in S. Then S' is a subring of S.

Solution. Since S' is the image of R in S under the mapping f. Therefore, $f(R) = S' \subseteq S$.

Let $a', b' \in S'$. Since $S' = f(R)$, then there exists elements $a, b \in R$ such that $f(a) = a'$, $f(b) = b'$.

Now, $a' - b' = f(a) - f(b) = f(a-b) \in S'$ [since f is homomorphism and $a - b \in R$]
Further, $a'b' = f(a)f(b) = f(ab) \in S'$ [since $ab \in R$]
Thus $a', b' \in S' \Rightarrow a' - b' \in S'$ and $a'b' \in S'$.
Hence S' is a subring of S.

Theorem 17.15 *Every homomorphic image of a ring R is isomorphic to some quotient ring of R.*

Example 17.16 Consider the ring $\mathbf{Z}$ and $\mathbf{Z}_5$. Let $f : \mathbf{Z} \to \mathbf{Z}_5$ be defined by $f(r) = [r], r \in \mathbf{Z}$. Show that f is a homomorphism and find $\ker f$.

Solution. Let $m, n \in \mathbf{Z}$. Then $f(m+n) = [m+n] = [m] + [n] = f(m) + f(n)$ and $f(mn) = [mn] = [m][n] = f(m)f(n)$.
Hence f is a homomorphism.
Now,

$$\begin{aligned} \ker f &= \{n \in \mathbf{Z} : f(n) = [0]\} \\ &= \{n \in \mathbf{Z} : [n] = [0]\} \\ &= \{n \in \mathbf{Z} : n \equiv 0 \pmod 5\} \\ &= \{n \in \mathbf{Z} : n = 5k \text{ where } k \in \mathbf{Z}\} \\ &= 5\mathbf{Z}. \end{aligned}$$

Example 17.17 Prove that every homomorphic image of a commutative ring is commutative.

Solution. Let R and R' be two rings and there is a homomorphic mapping $f : R \to R'$. R' is the homomorphic image of R.
Let $a', b' \in R'$. Then there exists some $a, b \in R$ such that $f(a) = a', f(b) = b'$.
Now,

$$\begin{aligned} a'b' &= f(a)f(b) = f(ab) = f(ba) \qquad [\text{since } R \text{ is commutative}] \\ &= f(b)f(a) = b'a'. \end{aligned}$$

Hence R' is commutative.

Example 17.18 If the ring R consists of all multiples of 2 and R' consists of all multiples of 3, show that R is not isomorphic to R'.

Solution. Here $R = \{2k : k \in \mathbf{Z}\} = 2\mathbf{Z}$ and $R' = \{3k : k \in \mathbf{Z}\} = 3\mathbf{Z}$.
Suppose there be a ring isomorphism $f : R \to R'$ i.e., $f : 2\mathbf{Z} \to 3\mathbf{Z}$. Thus f is a group isomorphism of $(2\mathbf{Z}, +)$ onto $(3\mathbf{Z}, +)$. Both $(2\mathbf{Z}, +)$ and $(3\mathbf{Z}, +)$ are cyclic groups. $2, -2$ are the generators of $2\mathbf{Z}$ and $3, -3$ are the generators of $3\mathbf{Z}$. Hence $f(2)$ must be a generator of $3\mathbf{Z}$. Suppose $f(2) = 3$. Then $f(4) = f(2+2) = f(2) + f(2) = 3 + 3 = 6$. Again, $f(4) = f(2.2) = f(2).f(2) = 3.3 = 9$.
Thus, $f(4) = 6 \neq 9 = f(4)$.
Again, if we take $f(2) = -3$ then $f(4) = f(2) + f(2) = -3 - 3 = -6$ and $f(4) = f(2)f(2) = (-3)(-3) = 9$. This case is also not possible.
Hence there does not exist any ring isomorphism $f : 2\mathbf{Z} \to 3\mathbf{Z}$.

Definition 17.22 (Prime ideal) *An ideal $H (\neq R)$ in a commutative ring R is a prime ideal if $ab \in H$ implies either $a \in H$ or $b \in H$ for all $a, b \in R$.*

Theorem 17.16 *If R is a commutative ring with unity and H is an ideal of R then R/H is an integral domain iff H is prime.*

Proof. Let R be a commutative ring with unity and H is an ideal of R. Then $R/H = \{H + a : a \in R\}$. Let $H + a, H + b$ be any two elements of R/H. Then $a, b \in R$ we have $(H + a), (H + b)$ be any two elements of R/H.

Then $a, b \in R$ we have

$(H + a)(H + b) = H + ab = H + ba = (H + b)(H + a)$.

Therefore, R/H is a commutative ring.

Now, let H be a prime ideal of R. Then we are to prove that R/H is an integral domain. For this we have to show that R/H is without zero divisors.

The zero element of the ring R/H is the residue class H itself. Let $H + a, H + b \in R/H$ then

$(H + a)(H + b) = H$

$\Rightarrow H + ab = H$ [the zero element of R/H]

$\Rightarrow ab \in H$.

This implies, either $a \in H$ or $b \in H$ for definition of prime ideal

Implies either $H + a$ or $H + b$ is zero element of R/H.

Since R/H is a commutative ring without zero divisors, therefore R/H is an integral domain.

Conversely, let R/H be an integral domain. Then we are to prove that H is prime ideal of R.

Let $a, b \in R$ such that $ab \in H$. Now

$ab \in H \Rightarrow H + ab \in H \Rightarrow (H + a)(H + b) = H$

$\Rightarrow$ either $(H + a)$ or $(H + b)$ is zero

$\Rightarrow$ either $(H + a) = H$ or $(H + b) = H$ is zero

$\Rightarrow$ either $a \notin H$ or $b \in H$

$\Rightarrow H$ is a primal ideal.

This completes the proof of the theorem. □

If R is a ring with unity then R/H is also a ring with unity. The residue class $H + 1$ is the unity element of R/H. Therefore, if we define an integral domain as a commutative ring with unity and without zero divisors, even then the above theorem will be true. But, in that case R must be a commutative ring with unity.

Definition 17.23 (Maximal ideal) *The maximal ideal of a ring R is an ideal $H(\neq R)$ such that there is no proper ideal H' of R properly containing H, i.e. $H \subsetneq H' \Rightarrow$ either $H = H'$ or $R = H'$.*

Example 17.19 In the ring of integer $\mathbf{Z}$, the ideal $\mathbf{Z}6$ is not maximal since it is properly contained in the ideal $\mathbf{Z}3$, which in turn is properly contained in $\mathbf{Z}$, on the other hand $\mathbf{Z}5$ is a maximal ideal since the only ideal properly containing $\mathbf{Z}5$ is $\mathbf{Z}$ itself.

In other word an ideal H of a ring R is said to be maximal ideal if there exists no ideal properly contained in R which itself properly contains H, i.e. if it is impossible to find an ideal which lies between H and the full ring R.

Theorem 17.17 *If R be the commutative ring with unity and H is an ideal then R/H is the field iff H is maximal.*

Proof. First we assume that H is a maximal ideal in R and consider any nonzero element $H+a \in R/H$ where $a \notin H$.

Consider a set $S = \{h + ax : h \in H, x \in R\}$. To prove S is an ideal. Let $h_1 + ax_1 \in S$ and $h_2 + ax_2 \in S$ for $x_1, x_2 \in R$ and $h_1, h_2 \in H$.

Now, $(h_1 + ax_1) - (h_2 + ax_2) = (h_1 - h_2) + a(x_1 - x_2)$.

[since $h_1, h_2 \in H \Rightarrow h_1 - h_2 \in H$ and $x_1 - x_2 \in R$]

Therefore, S is a subgroup.

Now, $(h_1 + ax_1)x_2 = h_1x_2 + ax_1x_2 \in S$

[since $x_1x_2 \in R$ and $h_1x_2 \in H$ as H is an ideal]

Similarly, $x_2(h_1 + ax_1) \in S$. Hence S is an ideal.

Since $a \notin H$ so H is the prime subset of S.

i.e. $H \subset S \Rightarrow S = R$ [since H is maximal ideal]

Therefore, it follows that $1 = h + ax$ for some $h \in H$ and $x \in R$ (1 is the identity element in R)

$\Rightarrow H + 1 = H + h + ax$

$\Rightarrow H + 1 = H + ax$ [since $h \in H \Rightarrow H + h = H$]

$\Rightarrow H + 1 = (H + a)(H + x)$ [by definition of R/H]

This shows that the existence of an inverse element for any nonzero element $H+a$ of the commutative ring R/H. So R/H is the field.

Conversely, we assume that R/H is a field. Let M be an ideal which properly contain H (i.e. $H \subset M$). So that there is an element $a \in R$ such that $a \in M$ but $a \notin H$.

Now as R/H is field. The equation $(H + a)(H + x) = H + b$ is solvable for any $b \in R$.

Hence $H + ax = H + b \Rightarrow ax - b \in H \Rightarrow ax - b \in M$ (since $H \subset M$)

But since M is an ideal and $a \in M$, $ax \in M$ for all $x \in R$.

Therefore, $ax - (ax - b) \in M$ [since $ax \in M$ and $ax - b \in M$]

$\Rightarrow b \in M$ for all $b \in R$

$\Rightarrow R \subseteq M$ but $M \subseteq R$

$\Rightarrow R = M$.

Hence H is the maximal ideal of R. □

Corollary 17.1 *In a commutative ring R with unity every maximal ideal of R is a prime ideal.*

Proof. R is a commutative ring with unity. Let S be a maximal ideal of R. Then R is a field.

Now, every field is an integral domain. Therefore, the commutative ring with unity and S is an ideal of R, then R/S is an integral domain iff S is prime.

So S is a prime ideal of R. This completes the proof. □

But, it may be noted that the converse of the above result is not true, i.e. every prime ideal is not necessarily a maximal ideal.

Theorem 17.18 (Fundamental theorem on homomorphism of rings) *Let $f : R \to S$ be the homomorphism of a ring R into the ring S and let H be the kernel of homomorphism f, then $f(R)$ is homomorphic with the quotient ring of R modulo H, i.e. $f(R) \approx R/H$.*

Proof. Let us consider a mapping $\phi : R/H \to S$ defined by $\phi(H+x) = f(x)$ for all $x \in R$. First we shall show that the mapping ϕ is well defined, i.e. if $a, b \in R$ and $H + a = H + b$ then $\phi(H + a) = \phi(H + b)$.

Now, $(H + a) = (H + b)$

$\Rightarrow a - b \in H$

$\Rightarrow f(a-b) = 0'$ [zero element of S]
$\Rightarrow f(a) - f(b) = 0'$
$\Rightarrow f(a) = f(b)$
$\Rightarrow \phi(H+a) = \phi(H+b)$
Therefore, ϕ is well defined.

ϕ is one-one:
We have $\phi(H+a) = \phi(H+b)$
$\Rightarrow f(a) = f(b)$
$\Rightarrow f(a) - f(b) = 0'$
$\Rightarrow f(a) + f(-b) = 0'$
$\Rightarrow f(a-b) = 0'$
$\Rightarrow a - b \in H$
$\Rightarrow H + a = H + b$
Thus ϕ is one-one.

ϕ is onto S:
Let $y \in S$ then $y = f(a)$ for $a \in R$ because f is onto S. Now, $H + a \in R/H$ and we have $\phi(H+a) = f(a) = y$.

Therefore, ϕ is onto S.

Finally,

$$\phi[(H+a)+(H+b)] = \phi[H+(a+b)]$$
$$= f(a+b) = f(a) + f(b) = \phi(a+H) + \phi(b+H).$$

Also, $\phi[(H+a)(H+b)] = \phi(H+ab) = f(ab) = f(a)f(b) = \phi(H+a)\phi(H+b)$.

Thus ϕ is an isomorphism of R/H onto S.

Hence $R/H \approx R/H$. □

17.10 Euclidian Domains/Euclidian Rings

An integral domain R is said to be an Euclidian domain if to every nonzero element $a \in R$, we can assign a non-negative integer $d(a)$ such that
(i) for all $a, b \in R$, both nonzero, $d(ab) \geq d(a)$;
(ii) for any $a, b \in R$ and $b \neq 0$ there exists $q, r \in R$ such that $a = qb + r$ where either $r = 0$ or $d(r) < d(b)$.

$d(a)$ is called the valuation.

The set of integers $\mathbf{Z}$ is a Euclidian domain with valuation $d(a) = |a|$.

Definition 17.24 (Principal ideal ring) *An integral domain R with unity is a principal ideal ring (or domain) if every ideal of R is principal, i.e. of the form Ra for some $a \in R$.*

Divisibility in an integral domain

If $a \neq 0$ and b are in a commutative ring R then a is said to be divide b if there exists $c \in R$ such that $b = ac$. Symbolically, a/b means a divides b and $a \nmid b$ means a does not divisible by b.

Theorem 17.19 *If R is a commutative ring then*
(i) a/b and $b/c \Rightarrow a/c$, the relation of divisibility in R is a transitive relation;

(ii) a/b *and* $a/c \Rightarrow a/(b+c)$;
(iii) $a/b \Rightarrow a/bx$ *for all* $x \in R$.

Proof. (i) $a/b \Rightarrow b = ap$ for some $p \in R$ and $b/c \Rightarrow c = bq = (ap)q = a(pq)$ for some $q \in R$.
This implies, a/c [since $pq \in R$]
(ii) $a/b \Rightarrow b = ap$ for some $p \in R$ and $a/c \Rightarrow c = aq$ for some $q \in R$.
Now, $b + c = ap + aq = a(p+q) \Rightarrow a/(b+c)$ since $p + q \in R$.
(iii) $a/b \Rightarrow b = ap$ for some $p \in R$.
Now, $b = ap \Rightarrow bx = (ap)x$ for all $x \in R$
$\Rightarrow bx = a(px) \Rightarrow a/bx$ since $px \in R$. □

Lemma 17.1 *In any Euclidian domain* D *for nonzero* $x, y \in D$, $d(xy) = d(x)$ *if* y *is invertible, whereas* $d(xy) > d(x)$ *if* y *is not.*

Proof. For any nonzero $x, y \in D$ we have $d(xy) \geq d(x)$, (i)
Now, if y is invertible, then $d(x) = d(xyy^{-1}) \geq d(xy)$. (ii)
From (i) and (ii), $d(x) = d(xy)$.
Moreover, if $xy/x \Rightarrow xyz = x$ for $z \in D$
$\Rightarrow yz = 1$ [by left cancellation law]
$\Rightarrow y$ is invertible, i.e. z is multiplicative inverse.
If xy/x then $x = (xy)q + r$ either $r = 0$ or $d(r) < d(xy)$.
Therefore, $r = x - (xy)q = x(1 - yq)$.
Now, $d(r) = d[x(1-yq)] \geq d(x)$.
Since $r \neq 0$, therefore $d(x) \leq d(r) < d(xy) \Rightarrow d(xy) > d(x)$. □

Theorem 17.20 *In any Euclidian domain every ideal is principal.*

Proof. Let R be an Euclidian ring and S be an arbitrary, i.e. the ideal of R generated by 0. Therefore, S is a principal ideal. So let us suppose that S is not a null ideal. Then there exists an element in S not equal to zero. Let b be any nonzero element in S such that $d(b)$ is maximal, i.e. there exists no element c in S such that $d(c) < d(b)$. We shall show that $S = Rb$, i.e. S is nothing but the ideal generated by b.

Let a be any element of S. Then by definition of Euclidean ring there exists elements q and r in R such that $a = qb + r$ where either $r = 0$ or $d(r) < d(b)$. Now, $q \in R$, $b \in S \Rightarrow qb \in S$ because S is an ideal.

Further $a \in S, qb \in S \Rightarrow q - qb = r \in S$. Thus $r \in S$ and we have either $r = 0$ or $d(r) < d(b)$.

If $r \neq 0$ then $d(r) < d(b)$ which contradicts our assumption that no element in S has value smaller than $d(b)$. Therefore, we must have $r = 0$ then $a = qb$. Thus every element $a \in S$ is of the generating element b. Thus $a \in S \Rightarrow a \in Rb$.

Therefore, $S \subseteq Rb$.

Again, if xb is any element of Rb. Then $x \in R$. Now, $x \in R, b \in S \Rightarrow xb \in S$. Therefore, $Rb \subseteq S$.

Hence $S = Rb$.

Thus every ideal S in R is a principal ideal, therefore R is a principal ideal ring. □

Definition 17.25 (Greatest common divisor (gcd)) *Let* R *be a ring and* $a, b \in R$. *Then* $d \in R$ *is said to be greatest common divisor of* a *and* b *if*
(i) d/a *and* d/b;
and (ii) whenever c/a *and* c/b *then* c/d, *this is denoted by* $d = gcd(a, b)$.

Theorem 17.21 *Let D be an Euclidian domain. Then any two elements a and b in D have a greatest common divisor d, moreover $d = \lambda a + \mu b$ for some $\lambda, \mu \in D$.*

Proof. We consider the set $H = \{ra + sb : r, s \in D\}$. We claim that H is an ideal of D.

Let $x, y \in H$ then $x = r_1a + s_1b$ and $y = r_2a + s_2b$ and so $x - y = (r_1 - r_2)a + (s_1 - s_2)b \in H$, since $r_1 - r_2, s_1 - s_2 \in D$.

$ux = u(r_1a + s_1b) = (ur_1)a + (us_1)b \in H$ for $u \in D$ and $ur_1, us_1 \in D$.

Therefore H is an ideal of D.

Every ideal in Euclidian domain is principal it follows that $H = Rd$ for some $d \in D$. Then $d/(ra+sb)$ for all $r, s \in D$.

When $r = 0, s = 1$ we have d/b and when $r = 1, s = 0$ then d/a. Therefore, d is common divisor of a and b.

Now, let c be any other divisor of a and b. Therefore, c/a and $c/b \Rightarrow c/ra$ and $c/sb \Rightarrow c/(ra+sb), r, s \in D$.

Thus $c \in H$. Now, $c = q(ra+sb) = (qr)a+(qs)b \in H$. Hence d is the gcd of a and b. By construction we can conclude that there exists μ and $\lambda \in D$ such that $d = \lambda a + \mu b$.

□

Definition 17.26 (Unit) *An element $a \in R$ of a ring is called unit if there exists $b \in R$ such that $ab = 1$.*

Definition 17.27 (Associates) *Let R be a commutative ring with unit element. Two elements (nonzero) a and b in R are said to be associates if $b = ua$ for some unit $u \in R$.*

The only units of the integral domain of integers are 1 and -1. Therefore, if a is any nonzero integer then it has exactly two associates namely $1.a$ and $(-1)a$, i.e. a and $-a$. Thus the two associates of 2 are 2 and -2.

In any commutative ring with unity the associates of 0 is only 0.

Definition 17.28 (Prime element) *In an Euclidian domain D a non unit p is said to be a prime element of D if whenever $p = ab$ where $a, b \in D$ then one of a, b is unit in R.*

Theorem 17.22 *For an Euclidian domain D, $d(1)$ is minimal among all $d(a)$ for nonzero $a \in D$, and $a \in D$ is a unit iff $d(a) = d(1)$.*

Proof. Let a be a unit in D.

By definition of Euclidian ring $d(1.a) \geq d(1) \Rightarrow d(a) \geq d(1)$. (i)

Since a is unit in D, therefore a^{-1} exists and $1 = aa^{-1}$.

$\Rightarrow d(1) = d(aa^{-1})$.

But, $d(aa^{-1}) \geq d(a)$. Therefore, $d(1) \geq d(a)$. (ii)

From (i) and (ii) we conclude that $d(a) = d(1)$.

Conversely, let $d(a) = d(1)$, then to prove that a is a unit in D. If a is not a unit in D then we have by previous theorem $d(a) > d(1)$.

Thus we get a contradiction. Hence a must be a unit. □

Theorem 17.23 *Let R be a Euclidian ring. Then every nonzero element in R is either a unit in R or can be written as a product of a finite numbers of prime elements S of R.*

Proof. Let a be a nonzero element of R. We are to prove that either a is a unit in R or it can be written as a product of finite number of prime elements of R. We shall prove that the result by induction on $d(a)$, i.e. by induction on the d-value of a.

Let us first start the induction. We have $a = 1.a$ therefore $d(a) \geq d(1)$. Thus 1 is an element in R which has the minimal d-value. If $d(a) = d(1)$ then a is a unit in R. Thus the result of the theorem is true if $d(a) = d(1)$ and so we have started the induction.

Now, as our induction hypothesis $d(x) \leq d(a)$. Then we shall show that the theorem is true for a also. If a is a prime element of R, the theorem is obviously true so suppose that a is not prime. Then we can write $a = bc$ where neither b nor c is a unit in R. Since both b and c are not units in R, therefore $d(bc) > d(b)$ and $d(bc) > d(c)$ but $d(a) = d(bc)$.

Therefore, we have $d(b) < d(a)$ and $d(c) < d(a)$. So by our induction hypothesis each of b and c are written as a product of a finite numbers of prime element of R.

Let $b = p_1p_2 \cdots p_n$, $c = q_1q_2 \cdots q_m$, where the p's and q's are prime elements of R. Then $a = bc = p_1p_2 \cdots p_nq_1q_2 \cdots q_m$. Thus we have written a as a product of a finite number of prime elements of R. This completes the induction and so the theorem has been proved. □

Definition 17.29 (Relatively prime) *In any Euclidian domain D and $a, b \in D$ are said to be relatively prime if their greatest common divisor is unit in D.*

Example 17.20 Any associates of gcd in D is gcd.

Solution. Let d be a gcd of a and b, then it implies
(i) d/a and d/b, and (ii) whenever c such that c/a and c/b then c/d.

Let associates of d be d', then $d' = ud$ for some unit u in D. To prove d' is gcd, i.e. d' satisfies (i) and (ii).

To prove (i):
Since $d = gcd(a, b)$, i.e. gcd of a and b, i.e. d/a and d/b.
$\Rightarrow a = cd$ for some $c \in D$
$\Rightarrow ua = ucd$
$\Rightarrow a = (u^{-1}c)(ud)$ [since D is commutative]
$\Rightarrow a = c'ud$
$\Rightarrow ud/a$.
To prove (ii):
c/a and $c/b \Rightarrow c/d$ [By second condition of gcd]
$\Rightarrow d = rc$ [for some $r \in D$]
$\Rightarrow ud = u(rc) = (ur)c = r'c$
$\Rightarrow c/ud \Rightarrow c/d'$.

Hence any associates of gcd is gcd in a commutative ring D.

Lemma 17.2 *Let D be an Euclidian domain, suppose that for $a, b, c \in D$, a/bc but $gcd(a, b) = 1$ then a/c.*

Proof. We know that gcd d of a, b is related by $\lambda a + \mu b = d = gcd(a, b)$.

Thus by our assumption $\lambda a + \mu b = 1$. (i)

Multiplying both members of (i) by c we get

$c = \lambda ac + \mu bc$ (ii)

But, a/bc so there exists an element $q \in D$ such that $bc = qa$. Substituting this value of bc in (ii) we get

$c = \lambda ac + \mu qa = (\lambda c + \mu q)a$,

which shows that a is a divisor of c, that is, a/c. □

Lemma 17.3 *If p is a prime element in the Euclidian ring R and p/ab where $a, b \in R$ then p divides at least one of the a and b.*

Proof. If p/a then we are noting to prove. Suppose $p \nmid a$.

Since p is prime and $p \nmid a$, therefore p and a are relatively prime, i.e. the gcd of p and a is 1. Hence p/b. □

Theorem 17.24 (Unique factorisation theorem) *Let R be a Euclidian ring and a be a nonzero unit element in R. Suppose that $a = p_1p_2 \cdots p_m = q_1q_2 \cdots q_n$, where the p's and q's are prime elements of R. Then $m = n$ and each p's is an associate of some q and each q's is an associate of some p's.*

Proof. Given $p_1p_2 \cdots p_m = q_1q_2 \cdots q_n$. Now p_i is a divisor of $p_1p_2 \cdots p_m$. Therefore, p_1 is also a divisor of $q_1q_2 \cdots q_n$. Thus p_1 must divide at least one of $q_1q_2 \cdots q_n$. Since R is a commutative ring therefore without loss of generality we may suppose that p_1 divides q_1.

But p_1 and q_1 be associates and we have $q_1 = up_1$, where u is a unit. Cancelling $p_1 \neq 0$ from both sides we get

$$p_2p_3 \cdots p_m = uq_2 \cdots q_n. \qquad \text{(i)}$$

Now, we can repeat the above argument on the relation (i) with p_2. If $n > m$ then after m steps the left hand side becomes 1 and the right hand side reduces to a product of some units in R. But the q's are prime elements of R and so they are not units in R. So the product of some unity in R and contain numbers of q's cannot be equal to 1. Therefore, n cannot greater than m. Thus $n \leq m$.

Similarly, interchanging the roles of p's and q's we get $m \leq n$.

Hence $m = n$.

Also, in the above process we have show that every p is an associate of some q and conversely every q is an associate of some p. Hence the theorem. □

17.11 Polynomial Rings

Let $F[x]$ be the set of all polynomials over the filed F. The polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is a member of the set $F[x]$ if its coefficients $a_0, a_1, \ldots, a_n$ are the members of the field F. If the coefficients $a_0, a_1, \ldots, a_n$ are real numbers then the set of polynomials are called real polynomials and we denote this set of polynomials by $R[x]$. The degree of a polynomial $f(x)$ is denoted by $deg(f)$ and it is a positive integer.

Example 17.21 Let $\mathbb{R}$ be the set of all real numbers. Let $R[x]$ be the set of all polynomials with real coefficients in the indeterminate x. Prove that $(R[x], +, .)$ is a commutative ring with unity under usual addition and multiplication of polynomials. [This ring is known as the polynomial ring over R]

Solution. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ be two polynomials of $R[x]$.

Then $f(x)+g(x)=(a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots+(a_p+b_p)x^p$ (i)
where $p=\max\{m,n\}$ and taking $a_k=0$ for any $k>n$ and $b_k=0$ for $k>m$
and $f(x).g(x)=c_0+c_1x+c_2x^2+\cdots+c_{m+n}x^{m+n}$ (ii)
where

$$c_k=\sum_{\substack{i,j=0\\ i+j=k}}^{k} a_ib_j$$

for each $k=0,1,2,\ldots,m+n$.

It is obvious, that $f(x)+g(x)\in R[x]$ and $f(x).g(x)\in R[x]$ as both are real polynomials.

Again, it is easy to observed that
$(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x))$ and $(f(x).g(x)).h(x)=f(x).(g(x).h(x))$ hold for all $f(x),g(x),h(x)\in R[x]$.

That is, associative property holds under addition and multiplication compositions.

$0=0+0.x+0.x^2+\cdots+o.x^n\in R[x]$ is the additive identity element.

$-f(x)\in R[x]$ is the additive inverse of $f(x)\in R[x]$ as $-f(x)+f(x)=0=f(x)+(-f(x))$ for all $f(x)\in R[x]$.

Obviously, $f(x)+g(x)=g(x)+f(x)$ for all $f(x),g(x)\in R[x]$.

Also, it is easy to verify that
$f(x).[g(x)+h(x)]=f(x).g(x)+f(x).h(x)$ and $[f(x)+g(x)].h(x)=f(x).h(x)+g(x).h(x)$ for all $f(x),g(x),h(x)\in R[x]$.

Hence $R[x]$ is a ring.

From (ii) it is easy to obtained that
$f(x).g(x)=g(x).f(x)$ for all $f(x),g(x)\in R[x]$.

Thus $R[x]$ is a commutative ring.

Again, $1=1+0.x+0.x^2+\cdots+0.x^n\in R[x]$ be the identity element, as $1.f(x)=f(x).1=f(x)$. That is, 1 is the identity element.

Hence $R[x]$ is a commutative ring with unity.

Lemma 17.4 *If $f(x)$ and $g(x)$ are two nonzero polynomials of $F[x]$ over the field F then $deg(fg)=deg(f)+deg(g)$.*

Proof. Suppose $f(x)=a_0+a_1x+a_2x^2+\cdots+a_mx^m$ and $g(x)=b_0+b_1x+b_2x^2+\cdots+b_nx^n$ where $a_m\neq 0$ and $b_n\neq 0$.

Then $deg(f)=m$ and $deg(g)=n$. By definition $f(x)g(x)=c_0+c_1x+c_2x^2+\cdots+c_kx^k$ where $c_i=a_ib_0+a_{i-1}b_1+\cdots+a_0b_i$.

Also $c_{m+n}=a_mb_n\neq 0$. Moreover, $c_i=0$ for $i>m+n$.

Since c_i is the sum of terms of the form $c_i=\sum_j a_jb_{i-j}$.

Since $i=j+(i-j)>m+n$ so either $j>m$ or $i-j>n$ but one of a_j or b_{i-j} is zero.

Therefore, $a_jb_{i-j}=0$, i.e. $c_i=0$ for $i>m+n$. Thus the highest nonzero coefficient of $f(x)g(x)$ is c_{m+n}.

Hence $deg(fg)=deg(f)+deg(g)$. □

Corollary 17.2 *If $f(x)$ and $g(x)$ are nonzero elements of $F[x]$ then $deg(f)\leq deg(fg)$.*

Proof. Since $deg(fg)=deg(f)+deg(g)$ and $deg(g)\geq 0$, therefore $deg(fg)\geq deg(f)$. □

17.11.1 Reducible and irreducible polynomials

The polynomial $f(x)$ of $F[x]$ is said to be reducible (over F) if $f(x) = a(x)b(x)$ for some non-constants polynomials $a(x), b(x) \in F[x]$. Otherwise $f(x)$ is said to be irreducible.

Irreducibility depends on the field F. For example, x^2+1 is irreducible over the real field R whereas it is reducible over the complex field $\mathbb{C}$, because $x^2+1 = (x+i)(x-i)$.

The polynomial x^2-2 is irreducible over the field of rational numbers while it is reducible over the field of real numbers, since $x^2-2 = (x+\sqrt{2})(x-\sqrt{2})$.

Theorem 17.25 (Division algorithm) *Let $f(x)$ and $g(x) \neq 0$ be any two polynomials of $F[x]$ over the field F. Then there exists unique two polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = q(x)g(x) + r(x)$ where either $r(x) = 0$ or $deg(r) < deg(g)$.*

Proof. Let us consider $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$, where $a_m \neq 0$ and $b_n \neq 0$. Here $deg(f) = m$ and $deg(g) = n$. If we consider $m < n$ or $f(x) = 0$ then the theorem is obviously true, because $f(x)$ can be written as $f(x) = 0.g(x) + r(x)$. In this case $q(x) = 0, r(x) = f(x)$. So we have either $r(x) = 0$ or $deg(r) < deg(g)$.

Let us assume that $m \geq n$. In this case we shall proof this theorem by induction on m. If $m = 0$ then $n = 0$. Therefore $f(x)$ and $g(x)$ are both nonzero constant polynomials.

We have $f(x) = a_0, a_0 \neq 0$ and $g(x) = b_0, b_0 \neq 0$. We have $f(x) = a_0 = a_0(b_0^{-1}b_0) = (a_0b_0^{-1})b_0 + 0 = (a_0b_0^{-1})g(x) + 0$.

Therefore, $f(x) = q(x)g(x) + r(x)$, where $q(x) = a_0b_0^{-1}$ and $r(x) = 0$. Thus the theorem is true when $m = 0$.

Let us assume that this theorem is true when $f(x)$ is a polynomial of degree less than m. We are to prove this theorem when $f(x)$ is a polynomial of degree m.

Let $f_1(x) = f(x) - (a_mb_n^{-1})x^{m-n}g(x)$ obviously $deg(f_1) < m$. (i)

Therefore, there exists polynomials $s(x)$ and $r(x)$ such that $f_1(x) = s(x)g(x) + r(x)$ where either $r(x) = 0$ or $deg(r) < deg(g)$. Substituting $f_1(x)$ in (i) we get

$s(x)g(x) + r(x) = f(x) - (a_mb_n^{-1})x^{m-n}g(x)$

or, $f(x) = [s(x) + (a_mb_n^{-1})x^{m-n}]g(x) + r(x)$

$= q(x)g(x) + r(x)$,

where $q(x) = (s(x) + a_mb_n^{-1})x^{m-n}$ and either $r(x) = 0$ or $deg(r) < deg(g)$. This proves the existence of polynomial $q(x)$ and $r(x)$. Now, we are to show that $q(x)$ and $r(x)$ are unique.

Let us assume that $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$.

Then $q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$ or $[q_1(x) - q_2(x)]g(x) = r_2(x) - r_1(x)$. (ii)

If $q_1(x) - q_2(x) \neq 0$ then $[q_1(x) - q_2(x)]g(x) \neq 0$, since $g(x) \neq 0$. Also the degree of $q_1(x) - q_2(x)$ is at least n and $r_2(x) - r_1(x)$ is either zero or its degree is less than n.

Hence the equation (ii) holds only when $q_1(x) - q_2(x) = 0$ and $r_1(x) - r_2(x) = 0$, i.e. $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$. Thus polynomials $q(x)$ and $r(x)$ are unique. □

17.12 Module Summary

The ring, integral domain and field and their variants are defined in this modulo as recapitulation. The ideal and different types of ideal are defined and presented a lot of properties on them. The quotient ring and its properties are also given here. Like group homomorphism, ring homomorphism is also defined and studied thoroughly. The fundamental theorem on homomorphism of rings is stated

and proved. The concept of Euclidian domain is given. The prime and relatively prime elements are introduced. The unique factorization theorem is also stated and proved in this module.

17.13 Self Assessment Questions

1. Prove that the set $R[x]$ of all polynomials over an arbitrary ring R is a ring w.r.t. addition and multiplication of polynomials.
2. If a is an idempotent element of a ring R, then prove that for any $b \in R$, the product $(1-a)ba$ is nilpotent.
3. Find all idempotent elements of the ring $\mathbf{Z}_{12}$.
4. If R is an integral domain, then show that the polynomial ring $R[x]$ over R is an integral domain.
5. Show that $S = \{5n : n \in \mathbf{Z}\}$ is an ideal of $\mathbf{Z}$.
6. R is the set of matrices of all 2×2 over $\mathbf{Z}$. Prove that $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbf{Z} \right\}$ is neither a right nor a left ideal in R.
7. Show that $(\mathbf{Z}, +, .)$ is a subring of $(\mathbf{Q}, +, .)$ but not an ideal.
8. Consider the polynomial ring $R[x]$ over a commutative ring R with identity. Let P_0 be the set of all polynomials whose constant terms are zero, i.e.,

   $$P_0 = \{a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in R, n \in \mathbf{N}\}.$$

   Show that P_0 is an ideal of $R[x]$.
9. Show that the set $S = \{a+b\sqrt{3} : a-b \text{ is an even integer}\}$ is an ideal in the ring $\{a+b\sqrt{3} : a, b \in \mathbf{Z}\}$.
10. Show that the set $I = \{(a, 0) : a \in \mathbf{Z}\}$ is an ideal in the ring $R = \mathbf{Z} \times \mathbf{Z}$.
11. Show that $9\mathbf{Z}$ is an ideal of the ring $\mathbf{Z}$.
12. Prove that the set $I = \left\{ \begin{bmatrix} 0 & b \\ 0 & d \end{bmatrix} : b, d \in \mathbf{Z} \right\}$ is not an ideal of $M_2(\mathbf{Z})$.
13. Let $I = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbf{Z}) : a, b, c, d \text{ are even integers} \right\}$. Show that I is an ideal of $M_2(\mathbf{Z})$.
14. Show that $\mathbf{Z}/5\mathbf{Z}$ is a quotient ring.
15. Define $f : \mathbf{C} \to \mathbf{C}$ by $f(z) = \overline{z}$, where $\mathbf{C}$ is the set of complex numbers. Show that f is an isomorphism on $\mathbf{C}$.
16. Let $f : \mathbf{Z} \to \mathbf{Z}_6$ be defined by $f(n) = [n]$ for all $n \in \mathbf{Z}$. Show that f is a homomorphism and find $\ker f$.
17. Consider two rings $Z_1 = \{a + b\sqrt{2} : a, b \in \mathbf{Z}\}$ and $Z_2 = \{a + b\sqrt{3} : a, b \in \mathbf{Z}\}$. Define $f : Z_1 \to Z_2$ by $f(a+b\sqrt{2}) = a+b\sqrt{3}$. Show that f is a group homomorphism but not a ring homomorphism.

18. Show that the mapping $f : \mathbf{Z} \to M_2(\mathbf{Z})$ defined by $f(r) = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix}$ is a homomorphism of rings. Is the mapping an isomorphism? Find its kernel.

19. Show that the mapping $f : Z_1 \to M_2(R)$ defined by $f(a+b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$, where $Z_1 = \{a+b\sqrt{2} : a, b \in \mathbf{Z}\}$, is a homomorphism of rings. Find $\ker f$.

20. Show that the mapping $f : \mathbf{C} \to M_2(\mathbb{R})$ defined by $f(a+ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ is a homomorphism of rings. Find $\ker f$. Is f a monomorphism?

21. Show that the mapping $f : Z[x] \to \mathbf{Z}$ defined by $f(a_0+a_1x+\cdots+a_nx^n) = a_0$ is a homomorphism from the ring $Z[x]$ (the set of polynomial with integer coefficients) onto the ring $\mathbf{Z}$. Is f an isomorphism?

22. Let $\mathbf{Z}^e$ be the set of all even integers. Let us define multiplication in Z^e to be denoted by $*$ and defined as

$$a * b = \frac{a.b}{2} \text{ for all } a, b \in \mathbf{Z}.$$

Prove that $\mathbf{Z}$ is isomorphic to $\mathbf{Z}^e$.

17.14 Suggested Further Readings

1. M. Artin, *Algebra*, PHI, 1991.
2. J.B. Fraleigh, *A First Course in Abstract Algebra* , Narosa, New Delhi, 1982.
3. J.A. Gallian, *Contemporary Abstract Algebra*, Narosa, New Delhi, 1999.
4. J.P. Tremblay and R. Manohar, *Discrete Mathematical Structures with Applications to Computer Science*, McGraw-Hill Book Company, 1975.
5. B. Kolman, R.C. Busby and S.C. Ross, *Discrete Mathematical Structures*, 4ed, Pearson Education, 2000.
6. M.K. Sen, S. Ghosh and P. Mukhopadhyay, *Topics in Abstract Algebra*, 2ed, University Press, 2ed, 2006.
7. D.S. Malik, J.M. Mordeson and M.K.Sen, *Fundamental of Abstract Algebra*, The McGraw-Hill Companies, Inc., 1997.

M.Sc. Course
in
Applied Mathematics with Oceanology
and
Computer Programming

PART-I

Paper-II **Module No.- 18** Group-A

Posets and Lattices

Module Structure

18.1 Introduction

The learners are acquainted with the set theory and equivalence relation. Here the de"nition of partial order set is given and studied it thoroughly. Another algebraic structure called lattice is de"ned. The lattice is also of dierent types. All of these are de"ned and studied their properties.

18.2 Objectives

After going through this unit you will be able to learn about

- What is partial order set?
- Hasse diagram of poset
- Bounds and least element, greatest element of poset
- What is lattice?
- Types of lattice

18.3 Keywords

Poset, Hasse diagram, lattice, sublattices, bounded lattice, isomorphic lattice, distributive lattice, complemented lattice.

18.4 Partial Order Set

A relation R defined on a set S is called a **partial order** or **partial ordering relation** if and only if R satisfies the following conditions:
(i) R is reflexive, i.e., aRb for all $a \in S$.
(ii) R is antisymmetric, i.e., if aRb and bRa iff $a = b$ for all $a, b \in S$.
(iii) R is transitive, i.e., aRb, bRc implies aRc for all $a, b, c \in S$.

The set S on which a partial order relation R is defined is called a **partial ordered set** or simply a poset and it is denoted by (S, R) or $(S, \preccurlyeq)$, where $\preccurlyeq$ denote some relation R associated to the poset.

Illustration

1. Let N be the set of natural numbers and '$\leq$' be the ordinary 'less than or equal to' relation defined on N. Now, $x \leq x$ for all $x \in \mathbf{N}$, if $x \leq y$ and $y \leq x$ then $x = y$ and if $x \leq y, y \leq z$ then $x \leq z$ for all $x, y, z \in \mathbf{N}$. Hence $(\mathbf{N}, \leq)$ is a poset.

2. Let N be the set of natural numbers and '/' be the divisibility relation, i.e., x/y means x divides y. Here also, x/x for all $x \in \mathbf{N}$, if x/y and y/x then $x = y$. Again, if $x/y, y/z$ then x/z for every $x, y, z \in \mathbf{N}$. Hence $(\mathbf{N}, /)$ is a poset.

3. If Z is a set of integers and '/' be the divisibility relation, then $(\mathbf{Z}, /)$ is not a poset. As $3/(-3)$ and $(-3)/3$ but $-3 \neq 3$. But, $(\mathbf{Z}, \leq)$ is a poset.

Example 18.1 Show that the relation $\subseteq$ (subset) defined on the power set $P(S)$ of the set S is a partial order relation.

(ii) Antisymmetric. If $S_1 \subseteq S_2$ and $S_2 \subseteq S_1$ then only possibility is $S_1 = S_2$. Hence $\subseteq$ is antisymmetric.

(iii) Transitive. If $S_1 \subseteq S_2$ and $S_2 \subseteq S_3$ then obviously $S_1 \subseteq S_3$. Hence $\subseteq$ is transitive.

Therefore, $(P(S), \subseteq)$ is a poset.

Example 18.2 Let $A = \{1, 4, 9, 16, 36\}$. Show that the divisibility relation / is partial order on A.

Solution. (i) Reflexive. For all $a \in A$, a/a, i.e., / is reflexive.

(ii) Antisymmetric. Let $a, b \in A$. If a/b and b/a then a must be equal to b, i.e., / is antisymmetric.

(iii) Transitive. Let $a, b, c \in A$ and a/b and b/c, implies a/c. That is, / is transitive.

Therefore, $(A, /)$ is a poset.

Definition 18.1 (Comparable elements) *Let $(A, \preccurlyeq)$ be a poset. Then the elements $a, b \in A$ are said to be* ***comparable*** *if $a \preccurlyeq b$ or $b \preccurlyeq a$.*

If two elements a and b are not comparable then they are called ***non-comparable elements.***

Definition 18.2 (Linear order set or totally ordered set) *If every pair of elements of a poset A is comparable then A is said to be* ***linearly order set*** *or* ***totally ordered set.*** *The partial order relation is called a* ***linear order relation*** *or* ***totally order relation.***

The relation '$\leq$' over the set $\mathbb{Z}^+$ is a partial as well as linear ordered relation. But, the relation 'divides' is not linear order relation over $\mathbb{Z}^+$ as $3, 5 \in \mathbb{Z}^+$ are not comparable.

Also, the poset $(P(S), \subseteq)$ is not totally ordered set as $\{a\}$ and $\{b\}$ are not comparable.

Definition 18.3 (Predecessor and successor) *Let $(S, \preccurlyeq)$ be a poset. If $a \preccurlyeq b$ where $a, b \in S$ then 'a precedes b' and 'b succeeds a'. If $a \preccurlyeq b$ but $a \neq b$ then we say 'a strictly precedes b' and 'b strictly succeeds a', and it is denoted by $a \prec b$.*

An element a is called an 'immediate predecessor of b' or 'b is an immediate successor of a' if $a \prec b$ and there is no any element $c \in S$ such that $a \prec c \prec b$. That is, if $a \prec b$ and there is no element of S which lies between a and b w.r.t. the relation $\preccurlyeq$. Sometimes it is written as $a \prec\!\prec b$.

For example, in the poset $(A, /)$, where $A = \{2, 4, 9, 16, 36\}$, $2/2$ and $2/16$ but, 2 is not immediate predecessor of 16. Since $9/36$ and there is no element c between 9 and 36 such that $9/c$. So, 9 is immediate predecessor of 36.

18.5 Hasse Diagram of a Poset

The diagrammatic representation of a partial order relation associated to as set is called **Hasse diagram.** Using the following steps one can draw the Hasse diagram of a poset $(A, \preccurlyeq)$.

Step 1. Draw a point for each element of the set A.

Step 2. Find the immediate successor(s) of each element of A. If $b \in A$ is an immediate successor of the element $a \in A$ then place b 'higher than' a and draw a line connecting a and b. (In this case, we say that the element b *covers* a).

The diagram obtained by these steps is called **Hasse diagram.**

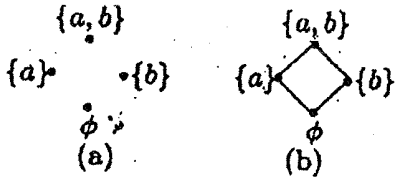


Figure 18.1: Hasse diagram of the poset $(P(S), \subseteq)$, where $S = \{a, b\}$.

Example 18.3 Let $A = \{a, b\}$ and its power set $P(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$.
Draw the points for all elements of $P(A)$ (see Fig. 18.1(a)).
The immediate successor of ϕ are $\{a\}$, $\{b\}$ and that of $\{a\}$, $\{b\}$ is $\{a, b\}$. Then draw a line segment for each pair $(\phi, \{a\})$, $(\phi, \{b\})$, $(\{a\}, \{a, b\})$ and $(\{b\}, \{a, b\})$. The Hasse diagram is shown in Fig. 18.1(b).

Example 18.4 Let $A = \{a, b, c\}$ be a set and $(P(A), \subseteq)$ be the poset on A. Draw the Hasse diagram of the poset $(P(A), \subseteq)$.

Solution. Here $P(A) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.
Step 1. Draw the points corresponding to all elements of the set $P(A)$ (see Fig. 18.2(a)).

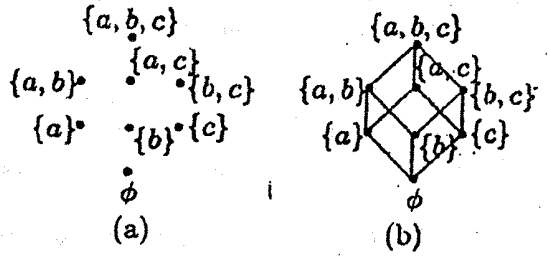


Figure 18.2: Hasse diagram of the poset $(P(A), \subseteq)$, where $A = \{a, b, c\}$.

Step 2. The immediate successor list is given in the following table.

Elements of A	Immediate successor
ϕ	$\{a\}, \{b\}, \{c\}$
$\{a\}$	$\{a, b\}, \{a, c\}$
$\{b\}$	$\{a, b\}, \{b, c\}$
$\{c\}$	$\{a, c\}, \{b, c\}$
$\{a, b\}, \{a, c\}, \{b, c\}$	$\{a, b, c\}$

Draw a line segment between an element of A and its immediate successor. Hence the Hasse diagram of $(P(A), \subseteq)$ is shown in Fig. 18.2(b).

18.6 Elements of Posets

Definition 18.4 (Maximal and minimal elements) *Let $(A, \preccurlyeq)$ be a poset. An element $a \in A$ is called a maximal element of A if there is no element $b \in A$ such that $a \preccurlyeq b$.*

Similarly, an element a is called a minimal element of A if there is no element $b \in A$ such that $b \preccurlyeq a$.

Note 18.1 In a poset there may be more than one maximal and minimal elements.

Example 18.5 Let $D = \{2, 3, 4, 6, 8, 24, 48\}$ be a poset under divisibility. Its Hasse diagram is shown in Fig. 18.3.

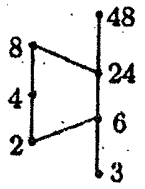


Figure 18.3: Hasse diagram of $(D, /)$

Its minimal elements are 2 and 3 and maximal element is 48.

Example 18.6 Let $A = \{2, 3, 6, 12, 24, 36\}$ and the relation $/$ be such that x/y, if x divides y. Draw the Hasse diagram of $(A, /)$.

Also, find the maximal and minimal elements.

Solution. Step 1. Draw a point for each element of A (see Fig. 18.4(a)).

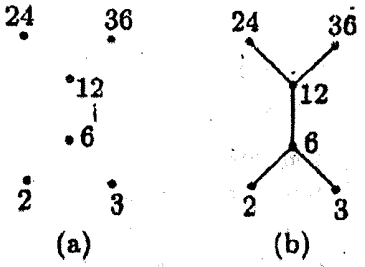


Figure 18.4: Hasse diagram of $(A, /)$

Step 2. The immediate successor list is given below.

Elements of A	Immediate successor
2	6
3	6
6	12
12	24, 36 (because 12/24/36 is not true)

Join each member of A to its immediate successor by a line se4gment, shown in Fig. 18.4(b).

The maximal elements are 24, 36 and minimal elements are 2, 3.

Theorem 18.1 *Prove that every finite non-empty poset $(A, \preccurlyeq)$ has at least one maximal and one minimal element in A.*

Proof. Let $A = \{a_1, a_2, \ldots, a_n\}$ be a finite poset under $\preccurlyeq$, containing n elements. If a_1 is not maximal element, then by definition there is another element $a_2 \in A$ such that $a_1 \prec a_2$. Again, if a_2 is not

a maximal element, then there is another element $a_3 \in A$ such that $a_2 \prec a_3$. Since, A is finite, this process will terminate after a finite number of times. Hence, we obtain a finite sequence of elements of A in the following order: $a_1 \prec a_2 \prec a_3 \prec \cdots \prec a_n$.

Therefore, there is no x such that $a_n \prec x$ for any $x \in A$. Hence a_n is a maximal element of $(A, \preccurlyeq)$.

Similarly, one can prove that $(A, \preccurlyeq)$ has at least one minimal element. □

Definition 18.5 (Greatest and least element) *An element $g \in A$ is called a **greatest (maximum)** element of A if for all $a \in A$, $a \preccurlyeq g$.*

*Similarly, $l \in A$ is called a **least (minimum)** element of A if for all $a \in A$, $l \preccurlyeq a$.*

Note 18.2 The greatest element of a poset is denoted by 1 and is called the unit element and the least element of a poset is denoted by 0 and is called the zero element.

In the poset $(P(S), \subseteq)$, ϕ is the least element and S is the greatest element.

Also, in the poset $(D, \preccurlyeq)$ of Example 18.5 has greatest element 48 but, it has no least element.

Theorem 18.2 *A poset has at most one greatest element and at most one least element.*

Proof. Let $(A, \preccurlyeq)$ be a poset. If possible let, $g_1, g_2 \in A$ be two greatest elements of A.

Since g_1 is a greatest element of A, $g_2 \preccurlyeq g_1$, $g_2 \in A$. Also, g_2 is a greatest element of A, $g_1 \preccurlyeq g_2$, $g_1 \in A$.

Hence $g_1 = g_2$. Thus A has only one greatest element.

The proof is similar for the case of least element. □

It may be noted that a greatest element is 'bigger' in the sense of $\preccurlyeq$, than every other element in the set while a maximal element is the element which is not less than any other element.

In the poset $(\{\{a\}, \{b\}, \{c\}, \{a, c\}\}, \subseteq)$, there is neither a greatest nor a least elements, while each of $\{a\}$, $\{b\}$ and $\{c\}$ is minimal and both $\{b\}$ and $\{a, c\}$ are maximal.

Example 18.7 Determine the maximum (greatest), minimum (least), maximal and minimal elements in the posets whose Hasse diagrams are shown in Fig. 18.5.

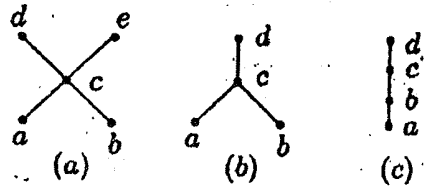


Figure 18.5:

Solution. The maximum, minimum, maximal and minimal elements are shown in the following table.

Figure 18.5	maximum	minimum	maximal	minimal
(a)	none	none	d, e	a, b
(b)	d	none	d	a, b
(c)	d	a	d	a

Definition 18.6 (Upper and lower bounds) *Let A be a subset of a poset $(S, \preccurlyeq)$. An element $a \in S$ is called an* ***upper bound*** *of A if $x \preccurlyeq a$ for every $x \in A$.*

Similarly, an element $b \in S$ is called a ***lower bound*** *of A if $b \preccurlyeq x$ for every $x \in A$.*

Example 18.8 Consider the poset $(S, \preccurlyeq)$, where $S = \{2, 3, 4, 5, 6, 7\}$ and $A = \{4, 5\}$.

The upper bounds of A are 5, 6, 7 because every element of A is $\preccurlyeq$ 5, 6, 7 and lower bounds of A are 2, 3, 4, because 2, 3, 4 are $\preccurlyeq$ every element of A.

Example 18.9 Consider the poset $S = \{1, 2, 3, 4, 5, 6, 7\}$ be ordered as shown in Fig. 18.6. Let $A = \{3, 4, 5\}$.

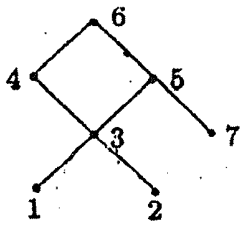


Figure 18.6:

The upper bound of A is 6 as every element is $\preccurlyeq$ 6.

The lower bound of A are 1, 2 and 3 because all of these are $\preccurlyeq$ every element of A. 7 is not a lower bound of A as $7 \not\preccurlyeq 3$ and $7 \not\preccurlyeq 4$.

Note 18.3 (a) From the above example it is observed that a poset may have more than one upper bound or lower bound.

(b) A lower or upper bound may or may not belong to a subset of poset itself.

Definition 18.7 (Supremum and infinmum) *Let A be a subset of a poset $(S, \preccurlyeq)$. An element $g \in S$ is called a* ***least upper bound (lub)*** *of A or* ***supremum (sup)*** *of A if g is an upper bound of A and $g \preccurlyeq g'$ for every upper bound g' of A.*

An element $l \in S$ is called a ***greatest lower bound (glb)*** *or* ***infinum (inf)*** *of A if l is a lower bound of A and $l' \preccurlyeq l$ for every lower bound l' of A.*

Note 18.4 The greatest element is always the supremum but the converse is not true. That is, $a = \sup(A)$ is the greatest element iff $a \in A$.

Similarly, least element is always the infimum but converse is not true.

Example 18.10 Let $S = \{a, b, c\}$ be a set and the poset $(P(S), \subseteq)$. Also, let $A = \{\{a\}, \{c\}\}$ be a subset of $P(S)$.

Here $\sup(A) = \{a, c\}, \inf(A) = \phi$, $\sup(S) = S, \inf(S) = \phi$.

Example 18.11 Consider the poset $(S, \preccurlyeq)$ whose Hasse diagram is shown in Fig. 18.7. Let $A = \{a, b, c\}$.

The glb of A is c and lub is f.

Example 18.12 Let $(A, /)$, where $A = \{2, 3, 4, 6\}$ be a poset and $B = \{4, 6\}$. The $\sup(B)$ and $\inf(B)$ do not exist, also $\sup(A)$ and $\inf(A)$ do not exist.

Here 2 is not $\inf(A)$ as '2 does not divide 3' and 6 is not $\sup(A)$ as '4 does not divide 6'.

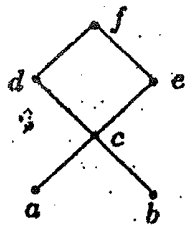


Figure 18.7:

Note 18.5 From these examples, it is observed that sup/inf of a poset may not exist. It is unique if exist.

Let D_n be the set of all positive divisors of a positive integer n. For example, $D_{10} = \{1, 2, 5, 10\}$, $D_{40} = \{1, 2, 4, 5, 8, 10. 20, 40\}$.

Example 18.13 Let D_{50} be the set of all positive divisors of 50. Show that D_{50} is a poset w.r.t. the relation $\preccurlyeq$ where $a \preccurlyeq b$ means a divides b. Draw the Hasse diagram of $(D_{50}, \preccurlyeq)$. Find maximal and minimal elements of D_{50}. Find lub and glb of $A = \{5, 10, 25\}$.

Solution. The set $D_{50} = \{1, 2, 5, 10, 25, 50\}$. For every element $a \in D_{50}$, a/a so $\preccurlyeq$ is reflexive.
If a/b and b/a then only possibility is $a = b$ for all $a, b \in D_{50}$, i.e., $\preccurlyeq$ is antisymmetric.
If a/b and b/c then obviously a/c for all $a, b, c \in D_{50}$. Therefore, $\preccurlyeq$ is transitive.
Hence $(D_{50}, \preccurlyeq)$ is a poset.
The immediate successor list of D_{50} is given below.

Elements of D_{50}	Immediate successor
1	2, 5
2	10
5	10, 25
10	50
25	50

Hasse diagram of $(D_{50}, \preccurlyeq)$ is shown in Fig. 18.8.

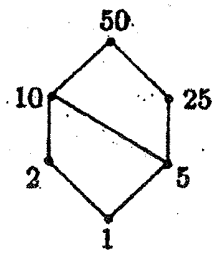


Figure 18.8: Hasse diagram of $(D_{50}, \preccurlyeq)$.

The minimal and maximal elements are 1 and 50.
From Hasse diagram, it is seen that $1 \preccurlyeq 5, 10, 25$; $5 \preccurlyeq 10, 25$. Also, $5 \preccurlyeq 10, 25$ and $10 \preccurlyeq 50, 25 \preccurlyeq 50$.
Therefore, lower bounds of A are 1, 5 and the upper bound of A is only 50 (25 is not an upper bound of A as '10 does not divide 25').
Hence lub of A is 5 and glb of A is 50.

Example 18.14 Show that $(\mathbf{N} \times \mathbf{N}, \preccurlyeq)$ where $(a, b) \preccurlyeq (c, d)$ iff $a \leq c$ and $b \geq d$, $\mathbf{N}$ is the set of natural numbers, is a poset.

Solution. Let $(a, b) \in \mathbf{N} \times \mathbf{N}$. Obviously, $(a, b) \preccurlyeq (a, b)$ since $a \leq a$ and $b \geq b$ hold as equality. So $\preccurlyeq$ is reflexive.

Let $(a, b) \preccurlyeq (c, d)$ and $(c, d) \preccurlyeq (a, b)$. Then $a \leq c, b \geq d$ and $c \leq a, d \geq b$. These relations valid only when $a = c$ and $b = d$, i.e., when $(a, b) = (c, d)$. Hence $\preccurlyeq$ is antisymmetric.

Let $(a, b) \preccurlyeq (c, d)$ and $(c, d) \preccurlyeq (e, f)$. Therefore, $a \leq c, b \geq d$ and $c \leq e, d \geq f$. Then imply, $a \leq e$ and $b \geq f$.

Therefore, $(a, b) \preccurlyeq (c, d)$, $(c, d) \preccurlyeq (e, f)$ $Ra(a, b) \preccurlyeq (e, f)$, i.e., $\preccurlyeq$ is transitive. Hence $(\mathbf{N} \times \mathbf{N}, \preccurlyeq)$ is a poset.

Example 18.15 Let $A = \{a, b, c, d\}$. Find the relation R whose Hasse diagram is shown in Fig. 18.9.

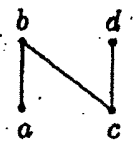


Figure 18.9:

Solution. Since the Hasse diagram is a pictorial representation of the poset (A, R), R is reflexive, antisymmetric and transitive.

Since R is reflexive, $(a, a), (b, b), (c, c), (d, d)$ all are members of R.

From Hasse diagram, it is seen that $(c, d) \in R, (d, a) \in R, (a, b) \in R$. Since $(c, d) \in R$ and $(d, a) \in R$ implies $(c, a) \in R$ (transitive).

Also, $(d, a) \in R$ and $(a, b) \in R$ implies $(d, b) \in R$.

Hence $R = \{(a, a), (b, b), (c, c), (d, d), (c, d), (d, a), (a, b), (c, a), (d, b)\}$.

Example 18.16 Let $A = \mathbf{Z} \times \mathbf{Z}$, $\mathbf{Z}$ is the set of integers. Let $a = (a_1, a_2)$ and $b = (b_1, b_2)$ be two elements of A. Define $a \preccurlyeq b$ iff $a_1 \leq b_1$ and $a_1 + a_2 \leq b_1 + b_2$. Prove that $\preccurlyeq$ is a partial order on A. In this partial order a total order? Justify your answer.

Solution. Obviously, $a \preccurlyeq a$ $a_1 \leq a_1$ and $a_1 + a_2 \leq a_1 + a_2$. Therefore, $\preccurlyeq$ is reflexive. Let $a \preccurlyeq b$ and $b \preccurlyeq a$. Thus $a_1 \leq b_1, a_1 + a_2 \leq b_1 + b_2$ and $b_1 \leq a_1$ and $b_1 + b_2 \leq a_1 + a_2$. These relations imply that $a_1 = b_1$ and $a_2 = b_2$. Thus $a = b$. Hence $\preccurlyeq$ is antisymmetric.

Let $a \preccurlyeq b$ and $b \preccurlyeq c$. Then $a_1 \leq b_1, a_1 + a_2 \leq b_1 + b_2, b_1 \leq c_1$ and $b_1 + b_2 \leq c_1 + c_2$.

Therefore, $a_1 \leq b_1 \leq c_1$ and $a_1 + a_2 \leq b_1 + b_2 \leq c_1 + c_2$.

This $a \preccurlyeq b$ and $b \preccurlyeq c$ implies $a \preccurlyeq c$, i.e., $\preccurlyeq$ is transitive.

Hence $(A, \preccurlyeq)$ is a poset.

But, this is not a total order, because if $a = (1, 3) \in A$ and $b = (5, -3)$ then $1 \leq 5$ but, $1 + 3 \not\leq 5 - 3$, i.e., $a \preccurlyeq b$ does not hold for any elements $a, b \in A$.

18.7 Lattices

Let $(L, \preccurlyeq)$ be a poset and $a, b \in L$. Then lub of the subset $\{a, b\}$ is denoted by $a \vee b$ and is called the **join** of a and b, i.e., $a \vee b = \sup\{a, b\}$.

The glb of the subset $\{a, b\}$ is denoted by $a \wedge b$ and is called the **meet** of a and b, i.e., $a \wedge b = \inf\{a, b\}$.

Definition 18.8 (Lattice) *A non-empty set L with two binary operations $\wedge$ and $\vee$ is called a lattice if the following axioms hold.*

1. Closure property. For all $a, b \in L$

(a) $a \wedge b \in L$ *(b)* $a \vee b \in L$

2. Commutative property. For all $a, b \in L$

(a) $a \wedge b = b \wedge a$ *(b)* $a \vee b = b \vee a$

3. Associative law. For all $a, b, c \in L$

(a) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ *(b)* $(a \vee b) \vee c = a \vee (b \vee c)$

4. Absorption law. For all $a, b \in L$

(a) $a \wedge (a \vee b) = a$ *(b)* $b \vee (a \wedge b) = a$.

A lattice L with two binary operations $\wedge$ and $\vee$ is denoted by $(L, \wedge, \vee)$.

Lattice as a poset.

A lattice is a poset $(L, \preccurlyeq)$ in which every 2-element subset $\{a, b\}$ has a lub and glb. That is, the poset $(L, \preccurlyeq)$ is a lattice if for every $a, b \in L$, lub(a, b) and glb(a, b) exist in L.

Example 18.17 Let $\mathbf{N}$ be the set of natural numbers and $\leq$ is the 'less than or equal to' relation. Then $(\mathbf{N}, \leq)$ is a lattice in which the operation $\wedge$ and $\vee$ are defined as

$$a \wedge b = \inf\{a, b\} = \min\{a, b\} \text{ and } a \vee b = \sup\{a, b\} = \max\{a, b\}.$$

Since $\min\{a, b\}$ and $\max\{a, b\}$ exist for all $a, b \in \mathbf{N}$ and they belong to $\mathbf{N}$, so $(\mathbf{N}, \leq)$ is a lattice.

Example 18.18 Let D_n be the set of all positive divisors of the positive integer n. Then $(D_n, /)$ is a lattice, where join $(\vee)$ and meet $(\wedge)$ operations are defined as

$a \vee b = \sup\{a, b\} =$ lcm of a and b, and

$a \wedge b = \inf\{a, b\} =$ gcd of a and b.

For example, let $D_{10} = \{1, 2, 5, 10\}$. The poset $(D_{10}, /)$ is a lattice, since every pair of elements has inf and sup.

Example 18.19 Let $A = \{2, 3, 4, 6\}$. Then $(A, /)$ is a poset but not a lattice as $\sup\{4, 6\}$ does not exist in A.

Example 18.20 Let $P(S)$ be the power set of S. Define $A \wedge B = A \cap B$ and $A \vee B = A \cup B$, for all $A, B \in P(S)$. Then show that $(P(S), \subseteq)$ is a lattice.

Solution. Let $A, B, C \in P(S)$.

(i) If $A, B \in P(S)$ then obviously, $A \cup B \in P(S)$ and $A \cap B \in P(S)$. That is, $P(S)$ is closed under $\cup$ and $\cap$.

(ii) For any $A, B \in P(S)$, $A \cap B = B \cap A$ and $A \cup B = B \cup A$. Therefore, commutative property holds.

(iii) Set union and intersection follows associative laws. Thus associative law holds.

(iv) To prove $A \cap (A \cup B) = A$, let $x \in A \cap (A \cup B)$.
Then $x \in A$ and $x \in (A \cup B)$
$\Leftrightarrow x \in A$ and ($x \in A$ or $x \in B$)
$\Leftrightarrow x \in A$.
Thus $A \cap (A \cup B) = A$.
Similarly, it can be shown that $A \cup (A \cap B) = A$.
Therefore, absorption law holds.
Hence $(P(S), \cap, \cup)$ is a lattice.

The lower and upper bounds of lattice

If $a \prec a \vee b$ and $b \preccurlyeq a \wedge b$ then $a \vee b$ is the upper bound of the elements $a, b \in L$. Also, if $a \preccurlyeq c$ and $b \preccurlyeq c$ then $a \vee b \preccurlyeq c$. Also, $a \vee b = \text{lub}\{a, b\} = \sup\{a, b\}$ for all $a, b \in L$.

Again, if $a \wedge b \preccurlyeq a$ and $a \wedge b \preccurlyeq b$ then $a \wedge b$ is the lower bound of the elements $a, b \in L$. Also, if $c \preccurlyeq a$ and $c \preccurlyeq b$ then $c \preccurlyeq a \wedge b$ then $a \wedge b = \text{glb}\{a, b\} = \inf\{a, b\}$ for all $a, b \in L$.

Some times the lattice $(L, \preccurlyeq)$ with join ($\vee$) and meet ($\wedge$) operators is denoted by $(L, \wedge, \vee)$.

18.8 Duality

The dual of any statement in a lattice $(L, \wedge, \vee)$ is defined to be the statement that is obtained by replacing $\wedge$ by $\vee$ and $\vee$ by $\wedge$.

For example, the dual of $a \vee (b \vee c) = (a \vee b) \vee c$ is $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

Principle of duality

Any property of a lattice yields another property by replacing
(i) the relation $\preccurlyeq$ with $\succcurlyeq$,
(ii) the join operation ($\vee$) with meet operation ($\wedge$) and vice versa.

The lattices $(L, \preccurlyeq)$ and $(L, \succcurlyeq)$ are the dual of each other. That is, if $\preccurlyeq$ is a partial order on L then also $\succcurlyeq$ is a partial order on L, because, $\text{lub}\{a, b\}$ in $(L, \preccurlyeq)$ is equal to the $\text{glb}\{a, b\}$ in $(L, \succcurlyeq)$ for all $a, b \in L$.

Theorem 18.3 (Idempotent law) *Let $(L, \wedge, \vee)$ be a lattice and $a \in L$. Then*
(a) $a \wedge a = a$ (b) $a \vee a = a$.

Proof. (a) $a \wedge a = a \wedge (a \vee (a \wedge b))$ [by absorption property]
$= a \wedge (a \vee c)$ [assuming $c = a \wedge b$]
$= a$ [by absorption property]
(b) $a \vee a = a \vee (a \wedge (a \vee b))$ [by absorption property]
$= a \vee (a \wedge c)$ [where $c = a \vee b$]
$= a$ [by absorption property] □

Theorem 18.4 *In a lattice $(L, \wedge, \vee)$, $a \wedge b = a$ iff $a \vee b = b$.*

Proof. Let $a \wedge b = a$.

Now, by absorption law,
$b = b \vee (b \wedge a) = b \vee (a \wedge b)$ [by commutative]
$= b \vee a$ [by assumption $a \wedge b = a$]
$= a \vee b$ [by commutative property]
Conversely, let $a \vee b = b$.
Again, by absorption property $a = a \wedge (a \vee b) = a \vee b$. □

Theorem 18.5 *Let $(L, \preccurlyeq)$ be a lattice then for every element $a, b \in L$,*
(a) $a \vee b = b$ iff $a \preccurlyeq b$
(b) $a \wedge b = a$ iff $a \preccurlyeq b$.

Proof. (a) Let $a \preccurlyeq b$. We known that $b \preccurlyeq b$. Then by definition of least upper bound, $a \vee b \preccurlyeq b$. Again, since $a \vee b$ is an upper bound of a and b, therefore, $b \preccurlyeq a \vee b$. Hence $a \vee b = b$.
Conversely, assume $a \vee b = b$. Since $a \preccurlyeq a \vee b = b$, therefore, $a \preccurlyeq b$.
(b) Proof is similar to (a). □

Example 18.21 Prove that in a lattice $(L, \preccurlyeq)$ for any $a, b \in L$,
if $a \preccurlyeq b \preccurlyeq c$ Rna $a \vee b = b \wedge c$ and $(a \wedge b) \vee (b \wedge c) = b = (a \vee b) \wedge (a \vee c)$.

Solution. From Theorem 18.5, we have
$a \wedge b = a$ and $a \vee b = b$ iff $a \preccurlyeq b$.
Here $a \preccurlyeq b \preccurlyeq c$, therefore, $a \vee b = b$ and $b \wedge c = b$.
Hence $a \vee b = b = b \wedge c$.
Second part. $(a \wedge b) \vee (b \wedge c) = a \vee b = b$, [$\because a \wedge b = a$ and $b \wedge c = b$]
Again, $(a \vee b) \wedge (a \vee c) = b \wedge c = b$ [$\because a \vee b = b$ and $a \vee c = c$]

Theorem 18.6 *Let $(L, \preccurlyeq)$ be a lattice and $a, b, c \in L$. Then if $a \preccurlyeq b$ and $a \preccurlyeq c$ then*
(a) $a \preccurlyeq b \vee c$ and (b) $a \preccurlyeq b \wedge c$.

Proof. (a) By the definition of join operation $b \wedge c = \sup\{b, c\}$.
Therefore, $b \preccurlyeq b \vee c$, i.e., $a \preccurlyeq b$ and $b \preccurlyeq b \vee c$. Hence by transitive property $a \preccurlyeq b \vee c$.
(b) Again, since $a \preccurlyeq b$ and $a \preccurlyeq c$, therefore, a is a lower bound of b and c. Thus, $a \preccurlyeq b \wedge c$. □

Corollary 18.1 *Let $(L, \preccurlyeq)$ be a lattice and $(L, \succcurlyeq)$ be its dual. If $a \succcurlyeq b$ and $a \succcurlyeq c$ then*
(a) $a \succcurlyeq b \wedge c$ and (b) $a \succcurlyeq b \vee c$ for all $a, b, c \in L$.

Theorem 18.7 *Let $(L, \preccurlyeq)$ be a lattice. Then*
(a) if $b \preccurlyeq c$ then (i) $a \wedge b \preccurlyeq a \wedge c$ and (ii) $a \vee b \preccurlyeq a \vee c$
(b) if $a \preccurlyeq b$ and $c \preccurlyeq d$ then (i) $a \vee c \preccurlyeq b \vee d$ and (ii) $a \wedge c \preccurlyeq b \wedge d$
for all $a, b, c, d \in L$.

Proof. (a) (i) From Theorem 18.5(b), we know that $a \wedge b = a$ iff $a \preccurlyeq b$. Therefore, to prove $a \wedge b \preccurlyeq a \wedge c$, we have to prove $(a \wedge b) \wedge (a \wedge c) = a \wedge b$.
Now, $(a \wedge b) \wedge (a \wedge c) = (a \wedge a) \wedge (b \wedge c)$ [by associative property]
$= a \wedge (b \wedge c)$ [$\because a \wedge a = a$, idempotent law]
$= a \wedge b$ [$\because b \wedge a = b$]
Hence $a \wedge b \preccurlyeq a \wedge c$.

(ii) Similarly, $(a \vee b) \vee (a \vee c) = (a \vee a) \vee (b \vee c)$ [by associative property]
$= a \vee (b \vee c) = a \vee c$ [$\because b \vee c = b$]

Therefore, $a \vee b \preccurlyeq a \vee c$ [by Theorem 18.5(a)]

(b) (i) Let $a \preccurlyeq b$ and $c \preccurlyeq d$. Then by definition of join operation $b \preccurlyeq b \vee d$ and $d \preccurlyeq b \vee d$.

Now, by transitivity,

$a \preccurlyeq b$ and $b \preccurlyeq b \vee d$ we have $a \preccurlyeq b \vee d$

and $c \preccurlyeq d$ and $d \preccurlyeq b \vee d$, $c \preccurlyeq b \vee d$.

These relations show that $b \vee d$ is an upper bound of a and c. Also, $a \vee c$ is the lub of a and c. Hence $a \vee c \preccurlyeq b \vee d$.

(ii) Proof is similar to (i). □

Theorem 18.8 (Distributive inequalities) *For any lattice* $(L, \preccurlyeq)$
(a) $a \wedge (b \vee c) \succcurlyeq (a \wedge b) \vee (a \wedge c)$
(b) $a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge (a \wedge c)$
for any $a, b, c \in L$.

Proof. (a) For any $a, b, c \in L$

$a \wedge b \preccurlyeq a$ and $a \wedge b \preccurlyeq b \preccurlyeq b \vee c$.

These two relations indicate that $a \wedge b$ is a lower bound of a and $b \vee c$. Thus $a \wedge b \preccurlyeq a \wedge (b \vee c)$ (i)
as $a \wedge (b \vee c)$ is the glb of a and $b \vee c$.

Again, $a \wedge c \preccurlyeq a$ and $a \wedge c \preccurlyeq c \preccurlyeq b \vee c$.

Thus, $a \wedge c \preccurlyeq a \wedge (b \vee c)$. (ii)

From (i) and (ii), it follow that $a \wedge (b \vee c)$ is an upper bound of $a \wedge b$ and $a \wedge c$. Since $(a \wedge b) \vee (a \wedge c)$ is the lub, therefore $(a \wedge b) \vee (a \wedge c) \preccurlyeq a \wedge (b \vee c)$.

(b) This result is the dual of the result of (a). □

Note 18.6 The distributive laws are not hold in lattices.

Theorem 18.9 (Modular inequality) *In a lattice* $(L, \preccurlyeq)$

$$a \preccurlyeq c \Leftrightarrow a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge c$$

for any $a, b, c \in L$.

Proof. We know that $a \vee c = c$ iff $a \preccurlyeq c$.

From Theorem 18.8(b), we have

$$a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c.$$

Thus $a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge c$ iff $a \preccurlyeq c$. □

Theorem 18.10 *Every linearly ordered set is a lattice.*

Proof. Let $(L, \preccurlyeq)$ be a lattice. Since L is linearly ordered set then either $a \preccurlyeq b$ or $b \preccurlyeq a$ for any $a, b \in L$.

Let $a \preccurlyeq b$. Then $a \preccurlyeq b$ and $b \preccurlyeq b$. Therefore, b is an upper bound of $\{a, b\}$. Let x be another upper bound of $\{a, b\}$. Then $a \preccurlyeq x$ and $b \preccurlyeq x$. This shows that $b \preccurlyeq x$.

Thus b is lub of $\{a, b\}$, i.e., $a \vee b = \sup\{a, b\} = b$.

Similarly, it can be shown that $a \wedge b = \inf\{a, b\} = a$.

That is, every 2-element subset $\{a, b\}$ has supremum and infimum. Hence L is a lattice. □

Theorem 18.11 *The dual of a lattice is a lattice.*

Proof. Let $(L, \preccurlyeq)$ be a lattice and its dual be $(L, \succcurlyeq)$.

Now, we prove that $(L, \succcurlyeq)$ is a poset.

If $a, b \in L$, then $\sup\{a, b\}$ exists in $\preccurlyeq$ as $(L, \preccurlyeq)$ is a lattice. Let $a \vee b = \sup\{a, b\}$ in $(L, \preccurlyeq)$. Then $a \preccurlyeq (a \vee b)$ and $b \preccurlyeq (a \vee b)$. These relations imply that $a \vee b \succcurlyeq a$ and $a \vee b \succcurlyeq b$. That is, $a \vee b$ is a lower bound of $\{a, b\}$ in $(L, \succcurlyeq)$.

To prove $a \vee b$ is the glb of $\{a, b\}$ in $(L, \succcurlyeq)$, let c be a lower bound of $\{a, b\}$ in $(L, \succcurlyeq)$. Then $c \succcurlyeq a$ and $c \succcurlyeq b$.

Now, $a \preccurlyeq c$ and $b \preccurlyeq c$

$\Rightarrow c$ is an upper bound of $\{a, b\}$ in $(L, \preccurlyeq)$

$\Rightarrow (a \vee b) \preccurlyeq c$ since $a \vee b = \sup\{a, b\}$ in $(L, \preccurlyeq)$

$\Rightarrow c \succcurlyeq (a \vee b)$

$\Rightarrow a \vee b$ is the glb of $\{a, b\}$ in $(L, \succcurlyeq)$.

Similarly, it can be shown that $a \wedge b$ is the lub in $(L, \succcurlyeq)$.

Hence $(L, \succcurlyeq)$ is a lattice. □

Example 18.22 Determine whether the posets shown in Fig. 18.10 are lattices or not.

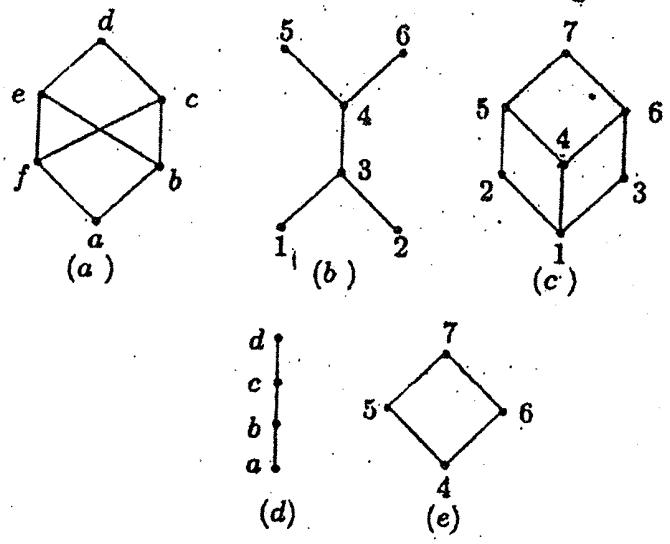


Figure 18.10:

Solution. The posets shown in Fig. 18.10 (c), (d) and (e) are lattices.

The posets shown in Fig. 18.10(a) is not a lattice since the pair (c, e) has three lower bounds f, b and a but, $\inf\{c, e\}$ does not exist. Also, $\sup\{f, b\}$ does not exist.

Again, the poset shown in Fig. 18.10(b) is not a lattice, since 5 and 6 have no upper bound and hence $\sup\{5, 6\}$ does not exist. Also, $\inf\{1, 2\}$ does not exist.

18.9 Types of Lattices

18.9.1 Sublattices

Let L_1 be a non-empty subset of a lattice L. Then L_1 is called a **sublattice** of L if L_1 itself is a lattice w.r.t. the operations of L, i.e., if $a \vee b \in L_1$ and $a \wedge b \in L_1$ for all $a, b \in L_1$.

Example 18.23 It is known that **N** is a lattice under the operations of divisibility. Let D_n be the set of all positive divisor of a positive integer n. Since $D_n \subseteq \mathbf{N}$ and every pair of elements $a, b \in D_n$ has a glb and a lub, therefore, $(D_n, /)$ is a lattice and it is a sublattice of $(\mathbf{N}, /)$.

Example 18.24 Consider the lattice $L = \{1, 2, 3, 4, 5\}$ whose Hasse diagram is shown in Fig. 18.11. Determine all sublattices containing three or more elements.

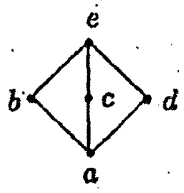


Figure 18.11: Diamond lattice.

Solution. All the sublattices containing three or more elements are $\{a, b, e\}, \{a, c, e\}, \{a, d, e\}, \{a, b, c, e\}, \{a, c, d, e\}, \{a, b, d, e\}$ and $\{a, b, c, d, e\}$ as every pair of elements of these sets have glb and lub.

Example 18.25 Consider the lattice $L = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$ whose Hasse diagram is shown in Fig. 18.12. Let $S_1 = \{a_5, a_6, a_7\}$ and $S_2 = \{\{a_1, a_2, a_3, a_5, a_6, a_7\}$.

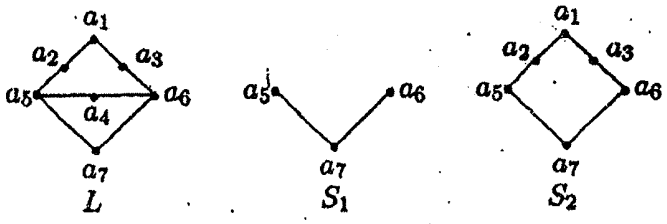


Figure 18.12:

S_1 is not a sublattice since $\sup\{a_5, b_6\}$ does not exist.
Also, S_2 is not a sublattice as $\sup\{a_5, a_6\}$ does not exist.

Theorem 18.12 *Intersection of two sublattices is a sublattice.*

Proof. Let S and T be two sublattices of a lattice $(L, \wedge, \vee)$. Let $a, b \in S \cap T$. Then $a, b \in S$ and $a, b \in T$. Since S is a sublattice, therefore, $a \wedge b \in S$ and $a \vee b \in S$. Similarly, $a \wedge b \in T$ and $a \vee b \in T$. Thus, $a \wedge b \in S \cap T$ and $a \vee b \in S \cap T$.

Hence $S \cap T$ is a sublattice of L. □

But, the union of two sublattices is not necessarily a sublattice. For example, $D_{24} = \{1, 2, 3, 4, 6, 8, 12, 24$ is a lattice where $a \wedge b =$ gcd of a, b and $a \vee b =$ lcm of a, b. The subset $S = \{1, 3\}$ and $T = \{1, 4\}$ are sublattices, but, $S \cup T = \{1, 3, 4\}$ is not a sublattice, since $3, 4 \in S \cup T$ but $3 \vee 4 = 12 \notin S \cup T$.

18.9.2 Bounded lattices

A lattice L is said to be **bounded** if it has both a least element (lower bound) 0 and a greatest element (upper bound) 1.

Example 18.26 (a) The lattice $(P(S), \subseteq)$ is bounded since it has lower bound ϕ and upper bound S.

(b) The lattice $(\mathbb{N}, \leq)$ is not bounded since it has a least element 1 but the upper bound does not exist.

(c) Let $L = \{a_1, a_2, a_3, \ldots, a_n\}$, where $a_1 \preccurlyeq a_2 \preccurlyeq a_3 \preccurlyeq \cdots \preccurlyeq a_n$, i.e, $\preccurlyeq$ is a partial order, i.e., L is a chain. The chain is a bounded lattice.

Theorem 18.13 *Every finite lattice $L = \{a_1, a_2, \ldots, a_n\}$ is bounded.*

Proof. For this lattice the greatest element is

$$a_1 \vee a_2 \vee a_3 \vee \cdots \vee a_n$$

and the least element is

$$a_1 \wedge a_2 \wedge a_3 \wedge \cdots \wedge a_n.$$

Since the greatest and the least elements exist for every finite lattice, hence is bounded.

Example 18.27 If $(L, \preccurlyeq)$ is a lattice with least element 0 and greatest element 1. Then for any $a \in L$ show that

(a) (i) $a \vee 1 = 1$, (ii) $a \wedge 0 = 0$

(b) (i) $a \wedge 1 = a$, (ii) $a \vee 0 = a$.

Solution. (a) (i) Let $a \in L$. Since 1 is the greatest element of L, $a \vee 1 \preccurlyeq 1$. Also, $a \vee 1$ is the supremum of a and 1. Thus $1 \preccurlyeq a \vee 1$. Hence $a \vee 1 = 1$.

(ii) Dual of (i).

(b) (i) Since $a \wedge 1$ is the glb of $\{a, 1\}$, $a \wedge 1 \preccurlyeq a$.

Again, $a \preccurlyeq a$ and $a \preccurlyeq 1$, so $a \preccurlyeq a \vee 1$. Thus $a \wedge 1 = a$.

(ii) Dual of (i).

18.9.3 Isomorphic lattices

Two lattices L_1 and L_2 are said to be **isomorphic** if there is a bijection from L_1 to L_2, i.e., $f : L_1 \to L_2$ such that $f(a \wedge b) = f(a) \wedge f(b)$ and $f(a \vee b) = f(a) \vee f(b)$ for every elements $a, b \in L_1$.

Since f is one-to-one and onto, the number of elements of L_1 and L_2 must be equal.

Example 18.28 Show that the lattice $D_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$ under divisibility relation and the lattice $(P(S), \subseteq)$ where $S = \{a, b, c\}$ are isomorphic.

Solution. We define a mapping $f : D_{24} \to P(S)$ as follows.

$$f(1) = \phi, \quad f(2) = \{a\}, \quad f(3) = \{b\}, \quad f(4) = \{c\},$$
$$f(6) = \{a, b\}, \quad f(8) = \{b, c\}, \quad f(12) = \{a, c\}, \quad f(24) = \{a, b, c\}$$

Obviously, f is one-to-one and onto.

Also, for all $a, b \in D_{24}$

$$f(a \wedge b) = f(a) \wedge f(b) \text{ and } f(a \vee b) = f(a) \vee f(b).$$

Thus, f is an isomorphism and hence the lattice $(D_{24}, /)$ is isomorphic to the lattice $(P(S), \subseteq)$.

Example 18.29 Let $(D_{12}, /)$ and $(\mathbf{N}, \leq)$ be two lattices, where $D_{12} = \{1, 2, 3, 4, 6, 12\}$, $\mathbf{N}$ is the set of natural numbers, / is the divisibility relation and $\leq$ is the usual 'less than or equal to' relation on $\mathbf{N}$.

These two lattices are not isomorphic as they have different numbers of elements.

Theorem 18.14 *If L_1 and L_2 are two isomorphic lattices and $f : L_1 \to L_2$ then $a \preccurlyeq bRaf(a) \preccurlyeq f(b)$ for all $a, b \in L_1$.*

Proof. Let $a, b \in L_1$ and $a \preccurlyeq b$. Then $a = a \wedge b$.

Therefore, $f(a) = f(a \wedge b) = f(a) \wedge f(b) Raf(a) \preccurlyeq f(b)$.

18.9.4 Distributive lattice

A lattice L is said to be **distributive** if for any elements $a, b, c \in L$, the following distributive laws hold.

(a) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$,

(b) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

If the lattice L does not satisfies the above properties, it is called a **non-distributive** lattice.

Example 18.30 (a) Every chain is a distributive lattice.

(b) The lattice $(P(S), \subseteq)$ is a distributive lattice under the operations of intersection and union, since for any sets $A, B, C \in P(S)$,
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ hold.

Example 18.31 Show that the lattice shown in Fig. 18.13 is not distributive.

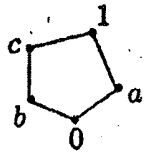


Figure 18.13: Non-distributive lattice

Solution. From the Hasse diagram $c \wedge (a \vee b) = c \wedge 1 = a$
but, $(c \wedge a) \vee (c \wedge b) = 0 \vee b = b$.

That is, $c \wedge (a \vee b) \neq (c \wedge a) \vee (c \wedge b)$.

Hence the lattice is not distributive.

Example 18.32 In a distributive lattice $(L, \wedge, \vee)$, $a \wedge b = a \wedge c$ and $a \vee b = a \vee c$ $Rab = c$.

Solution. Since every lattice satisfies commutative property, we have $b \wedge a = c \wedge a$ and $b \vee a = c \vee a$.

Now,	$b = b \wedge (a \vee b)$	[by absorption law]
	$= b \wedge (a \vee c)$	[since $a \vee b = a \vee c$]
	$= (b \wedge a) \vee (b \wedge c)$	[by distributive]
	$= (c \wedge a) \vee (b \wedge c)$	[$\because b \wedge a = c \wedge a$]
	$= (c \wedge a) \vee (c \wedge b)$	[by commutative]
	$= c \wedge (a \vee b)$	[by distributive]
	$= c \wedge (a \vee c)$	
	$= c$	[by absorption law]

Hence $b = c$.

18.9.5 Complemented lattices

Let L be a lattice whose greatest and least elements are respectively 1 and 0. An element $a' \in L$ is called a **complement** of a if

$$\text{(i) } a \vee a' = 1 \text{ and (ii) } a \wedge a' = 0.$$

From definition it follows that a is also the complement of a'. An element may have more than one complement.

It may be noted that $0' = 1$ and $1' = 0$.

Definition 18.9 (Complemented lattice) *A lattice L is called a complemented lattice if L is bounded and every element in L has a complement.*

Example 18.33 Every chain with more than two elements is not a complemented lattice.

Example 18.34 Let $S = \{a, b, c\}$. Then $(P(S), \subseteq)$ is a lattice, where
$P(S) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

The complement of each element is listed below.

Element of $P(S)$	Complement
ϕ	$\{a, b, c\}$
$\{a\}$	$\{b, c\}$
$\{b\}$	$\{a, c\}$
$\{c\}$	$\{a, b\}$
$\{a, b\}$	$\{c\}$
$\{b, c\}$	$\{a\}$
$\{c, a\}$	$\{b\}$
$\{a, b, c\}$	ϕ

This table shows that each element of $P(S)$ has a complement in $P(S)$. Hence $(P(S), \subseteq)$ is a completed lattice.

Here the complement of each element is unique.

Example 18.35 Let $D_{20} = \{1, 2, 4, 5, 10, 20\}$. Then the lattice $(D_{20}, /)$, where $/$ stands for divisibility, is complemented. Here 1 is the least element and 20 is the greatest element as $1/x$ and $x/20$ for all $x \in D_{20}$.

The Hasse diagram of this lattice is shown Fig. 18.14.

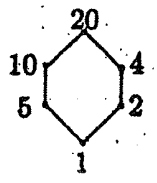


Figure 18.14: Complemented lattice

Thus the complement of 1, 2, 4, 5, 10, 20 are respectively 20, 10, 5, 4, 2,

Example 18.36 Consider the lattice $L = \{1, 2, 3, 4, 6, 12\}$ ordered by divisibility $(/)$. Find the lower and upper bounds of L. Is L a complemented lattice?

Solution. Since $1/x$ and $x/12$ for all $x \in L$, 1 is the lower bound and 12 is the upper bound of L. The complement of 1, 2, 3, 4, 6, 12 are respectively 12, 6, 4, 3, 2, 1 and all of them belong to L. Hence L is a complemented lattice.

Example 18.37 Show that the lattice shown in Fig. 18.15 is not complemented.

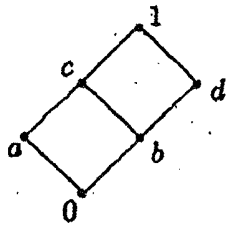


Figure 18.15: Non-complemented lattice

Solution. The complement of a is d, since $a \vee d = 1$ and $a \wedge d = 0$. The complement of c does not exist. Hence the lattice of Fig. 18.15 is not complemented.

Example 18.38 Show that the lattice shown in Fig. 18.16 is complemented.

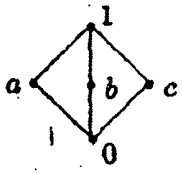


Figure 18.16: Complemented lattice

Solution. Let $L = \{0, a, b, c, 1\}$ be the lattice shown in Fig. 18.16. It is bounded, since 0 and 1 are the least and greatest elements.

From Hasses diagram we see that

$a \wedge b = 0, a \vee b = 1; a \wedge c = 0, a \vee c = 1; b \wedge c = 0, b \vee c = 1.$

Thus complement of a are b and c; that of b are a and c; and of c are a and b. That is, every element has complement and hence this lattice is a complemented lattice.

It may be noted that the complement of the elements are not unique.

Theorem 18.15 *0 and 1 are complement to each other.*

Proof. To prove 1 is the only complement of 0.

If possible, let c ($\neq 1$) be the complement of 0 and c belongs to the lattice L.

Then by definition of complement $0 \wedge c = 0$ and $0 \vee c = 1$.

But, by the property of bounded lattice, $0 \vee c = c$, which is a contradiction for $c \neq 1$.

Hence 1 is the only complement of 0.

Similarly, it can be prove that 0 is the only complement of 1. □

Theorem 18.16 *The complement (if exists) of elements of a bounded distributive lattice L is unique.*

Proof. If possible, let a_1 and a_2 be two complements of an element $a \in L$. Then by definition of complement, $a \vee a_1 = 1, a \wedge a_1 = 0$ and $a \vee a_2 = 1, a \wedge a_2 = 0$.

Now, $a_1 = a_1 \vee 0 = a_1 \vee (a \wedge a_2)$ $[\because a \wedge a_2 = 0]$
$= (a_1 \vee a) \wedge (a_1 \vee a_2)$ [by distributive property]
$= 1 \wedge (a_1 \vee a_2)$ $[\because a_1 \vee a = 1]$
$= a_1 \vee a_2$.

Again, $a_2 = a_2 \vee 0 = a_2 \vee (a \wedge a_1)$ $[\because a \wedge a_1 = 0]$
$= (a_2 \vee a) \wedge (a_2 \vee a_1)$ [by distributive property]
$= 1 \wedge (a_2 \vee a_1)$ $[\because a_2 \vee a = 1]$
$= a_2 \vee a_1 = a_1 \vee a_2$.

Therefore, $a_1 = a_2$. Hence the complement is unique. □

Theorem 18.17 (De Morgan's law) *Let L be a complemented distributive lattice. Then*
(a) $(a \vee b)' = a' \wedge b'$
(b) $(a \wedge b)' = a' \vee b'$, *for all* $a, b \in L$.

Proof. (a) To prove (a), we have to show that
$(a' \wedge b') \vee (a \vee b) = 1$ and $(a' \wedge b') \wedge (a \vee b) = 0$.

Now, $(a' \wedge b') \vee (a \vee b) = \{a' \vee (a \vee b)\} \wedge \{b' \vee (a \vee b)\}$ [by distributive property]
$= \{(a' \vee a) \vee b\} \wedge \{(b' \vee b) \vee a\}$ [by associative property]
$= (1 \vee b) \wedge (1 \vee a)$ [by definition of complement]
$= 1 \wedge 1 = 1$.

Also, $(a' \wedge b') \wedge (a \vee b) = \{(a' \wedge b') \wedge a\} \wedge \{(a' \wedge b') \wedge b\}$ [by distributive property]
$= \{(a' \wedge a) \wedge b\} \wedge \{a' \wedge (b' \wedge b)\}$ [by associative property]
$= (0 \wedge b) \wedge (a' \wedge 0)$ [by definition of complement]
$= 0 \wedge 0 = 0$.

Hence by definition of complement $a' \wedge b'$ is the complement of $a \vee b$, i.e., $(a \vee b)' = a' \wedge b'$.
(b) Dual of (a).

Theorem 18.18 *The dual of a distributive lattice is a distributive lattice.*

Proof. Let $(L, \wedge, \vee)$ be a distributive lattice. We have to prove that $(L, \bar{\wedge}, \bar{\vee})$ is also a distributive lattice, where $\bar{\wedge} = \vee$ and $\bar{\vee} = \wedge$.

Let $a, b, c \in L$. Since $(L, \wedge, \vee)$ is a distributive lattice, therefore,
$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
and $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Replacing $\vee$ by $\bar{\wedge}$ and $\wedge$ by $\bar{\vee}$, we obtain
$a \,\bar{\wedge}\, (b \bar{\vee} c) = (a \,\bar{\wedge}\, b) \bar{\vee} (a \,\bar{\wedge}\, c)$
and $a \bar{\vee} (b \,\bar{\wedge}\, c) = (a \bar{\vee} b) \,\bar{\wedge}\, (a \bar{\wedge} c)$.

Thus $(L, \bar{\wedge}, \bar{\vee})$ satisfies distributive laws. Hence the complemented lattice $(L, \bar{\wedge}, \bar{\vee})$ is distributive. □

Theorem 18.19 *Every sublattice of a distributive lattice is distributive.*

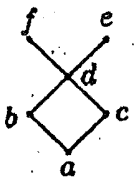
Proof. Let L_1 be a sublattice of a distributive lattice L. Let $a, b, c \in L_1$, then $a, b, c \in L$.
Since L is distributive, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \in L$.
Again, since L_1 is a sublattice, so it is closed w.r.t. $\wedge$ and $\vee$. Therefore, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \in L_1$.
Hence L_1 is distributive. □

18.10 Module Summary

The partial order set (poset) is defined and illustrated by several examples. Some properties of it are also presented. In the next part of this modulo, the lattice is defined and given some examples. Different types of lattices, viz., sublattices, bounded lattice, isomorphic lattice, distributive lattice and complemented lattice are also defined and studied their properties. A long exercise is provided at the end of this modulo.

18.11 Self Assessment Questions

1. Define poset. Show that $(\mathbf{Z}, /)$ is not a poset, where $\mathbf{Z}$ is the set of all integers and a/b means b is divisible by a.
2. Let $A = \{2, 3, 5, 30, 60, 120, 180, 360\}$. Show that $(A, /)$, / means divide, is a poset. Find the immediate successors of all elements of A and draw the Hasse diagram.
3. Show that $(P(S), \subseteq)$, where S is any finite set, is a poset.
4. Show that the set $A = \{4, 9, 16, 36\}$ is a poset under divisibility relation.
5. Let $A = \{n \in \mathbf{N} : 1 \leq n \leq 50\}$. Define a relation R on A by aRb iff 5 divides $a - b$ for all $a, b \in A$. Examine whether (A, R) is a poset.
6. Show that $(D_{100}, \preccurlyeq)$, where $a \preccurlyeq b$ means a divides b, is a poset. Draw the Hasse diagram of it. Find the maximal and minimal elements of $(D_{100}, \preccurlyeq)$. Also, find glb and lub of $A = \{5, 10, 20, 25\} \subset D_{100}$.
7. Draw the Hasse diagram of D_{40} and find its maximal and minimal elements.
8. Let $S = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$. Find the infimum and supremum of the sets $\{6, 18\}$ and $\{4, 6, 9\}$ in the poset $(S, /)$. Also, find maximal and minimal elements of S.
9. Draw the Hasse diagrams of
   (a) $(\{1, 2, 3, 4, 5\}, \leq)$
   (b) $(\{\{a\}, \{a, b\}, \{a, b, c\}, \{a, b, c, d\}, \{a, c\}, \{c, d\}\}, \subseteq)$
   (c) $(P(\{a, b, c\}), \subseteq)$
   (d) $(\{a, ab, abc, b, bcd, bc, abcd\}, \preccurlyeq)$ where $\preccurlyeq$ is the dictionary order.
10. Find the lub and glb of $A = \{b, c, d\}$ if they exist, of the poset whose Hasse diagram is shown below.



11. Find the maximum and minimum elements of the following posets
    (a) $(P(\{a, b, c\}), \subseteq)$
    (b) $(\{\{a\}, \{b\}, \{c\}, \{a, c\}\}, \subseteq)$
    (c) $(\{1, 2, 3, 4, 5, 6\}, \geq)$.

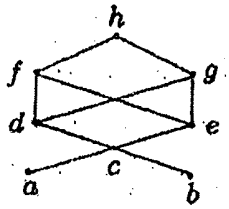
12. Let $A = \{1, 2, 4, 6, 8\}$ and for $a, b \in A$, define $a \preccurlyeq b$ iff b/a is an integer.
    (a) Prove that $\preccurlyeq$ defines a partial order on A.
    (b) Draw the Hasse diagram for $\preccurlyeq$.
    (c) List all minimum, minimal, maximum and maximal elements.
    (d) Is $(A, \preccurlyeq)$ totally ordered? Explain.

13. Prove that in a totally ordered set, any maximal element is a maximum.

14. Prove that any finite non-empty poset must contain maximal and minimal elements.

15. (a) Prove that a poset has at most one maximum element.
    (b) Prove that a poset has at most one minimum element.

16. Consider the partial ordered set $S = \{a, b, c, d, e, f, g, h\}$ under the relation whose Hasse diagram shown below.



    Consider the subsets $S_1 = \{a, b\}, , S_2 = \{c, d, e\}$ of A. Find
    (a) all the lower and upper bounds of S_1 and S_2
    (b) $\sup(S_1), \inf(S_1), \sup(S_2), \inf(S_2)$.

17. Prove that the poset $A = \{2, 3, 6, 12, 24, 36, 72\}$ under the relation 'divides' is a lattice.

18. Prove that the set $\{\phi, \{a\}, \{a, c\}, \{c\}, \{a, b, c\}\}$ is a lattice w.r.t. the operations $\cap$ and $\cup$. Is it complemented ?

19. Prove that the set D_n of all divisors of n is a lattice w.r.t. the operations $\wedge, \vee$ where $\wedge$ and $\vee$ stand for hcf and lcm respectively.

20. Let $L = \{a_1, a_2, a_3, \ldots, a_n\}$, where $a_1 \preccurlyeq a_2 \preccurlyeq \cdots \preccurlyeq a_n$, $\preccurlyeq$ is a partial order, i.e., L is a chain. Prove that L is a distributive lattice.

21. Let $(L, \preccurlyeq)$ be a lattice. Let $a, b \in L$ and $[a, b] = \{x : x \in L \text{ and } a \preccurlyeq x \preccurlyeq b\}$. Prove that $[a, b]$ is a sublattice of L.

22. Let $\mathbb{Z}^+$ be the set of all positive integers. $\wedge$ and $\vee$ are defined as $a \wedge b =$ hcf of a and b, $a \vee b =$ lcm of a and b. Prove that $(\mathbb{Z}^+, \wedge, \vee)$ is a lattice.

23. Show that in a bounded distributive lattice, the elements which have complements form a sublattice.

24. Prove that the non-empty intersection of two sublattices is a sublattice of the given lattice.

25. If L is a lattice and $a, b \in L$, then show that the subset $\{a, b\}$ of L is sublattice iff a and b are comparable.

26. If a bounded lattice has two or more elements then show that $0 \neq 1$.

27. Let L be a lattice. If $a \preccurlyeq b \preccurlyeq c$, $a, b, c \in L$ then prove that
(a) $a \vee b = b \wedge c$ (b) $(a \wedge b) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) = b$.

28. If $a \preccurlyeq b$ and $c \preccurlyeq d$ in a lattice L, then prove that $a \wedge c \preccurlyeq b \wedge d$.

29. Let L be a bounded lattice. If $a, b \in L$ and a' be the complement of a, then show that
(a) $a \wedge (a' \wedge b) = a \vee b$ and (b) $a \wedge (a' \vee b) = a \wedge b$.

30. If L is a distributed lattice and $a \wedge b = a \wedge c$ and $a \vee b = a \vee c$ for any $a \in L$ then $b = c$.

31. Prove that in a distributive lattice L,
$(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$ for any $a, b, c \in L$.

32. In a lattice $(L, \preccurlyeq)$, show that $a \vee (b \wedge c) = (a \vee b) \wedge c$ whenever $a \preccurlyeq c$.

33. Prove that every sublattice of a distributive lattice is a distributive lattice.

34. Consider the lattice shown in Fig. 18.17.
(a) Show that L is not distributive and not complemented,
(b) Find the complements of c, d and e.

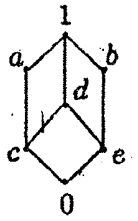


Figure 18.17:

35. Consider the lattice $L = \{0, 1, 2, 3, 6, 9, 18\}$ under divisibility relation. What is the greatest element of L? Is L complemented?

36. Consider the lattice $L = (P(S), \subseteq)$ where $S = \{1, 2, 3\}$. Determine whether or not each of the following is a sublattice of L.
$A = \{\phi, \{1, 2\}, \{2, 3\}, \{1, 2, 3\}\}$, $B = \{\phi, \{1\}, \{1, 2\}, \{1, 2, 3\}\}$
$C = \{\phi, \{3\}, \{1, 3\}, \{1, 2, 3\}\}$, $D = \{\{1\}, \{3\}, \{1, 3\}, \{1, 2, 3\}\}$,
$E = \{\phi, \{3\}, \{1, 2\}, \{1, 2, 3\}\}$.

37. Show that a lattice with three or fewer elements is a chain.

18.12 Suggested Further Readings

1. M. Artin, *Algebra*, PHI, 1991.

2. J.B. Fraleigh, *A First Course in Abstract Algebra* , Narosa, New Delhi, 1982.

3. J.A. Gallian, *Contemporary Abstract Algebra*, Narosa, New Delhi, 1999.

4. J.P. Tremblay and R. Manohar, *Discrete Mathematical Structures with Applications to Computer Science*, McGraw-Hill Book Company, 1975.

5. B. Kolman, R.C. Busby and S.C. Ross, *Discrete Mathematical Structures*, 4ed, Pearson Education, 2000.

6. M.K. Sen, S. Ghosh and P. Mukhopadhyay, *Topics in Abstract Algebra*, 2ed, University Press, 2ed, 2006.

7. D.S. Malik, J.M. Mordeson and M.K.Sen, *Fundamental of Abstract Algebra*, The McGraw-Hill Companies, Inc., 1997.

M.Sc. Course
in
Applied Mathematics with Oceanology
and
Computer Programming

PART-I

Paper-II Group-B

Module No. - 19

Functional Analysis

(Matric Space)

Contents :

19. Metric Space

19.1 Introduction :

Mathematicians observed that problems from different fields often enjoy related features and properties. This fact was used for an effective unifying approach towards such problems. This unification avoids unessential details and only concentrates on the essential facts. In this respect the abstract method is the simplest and most

economical method for treating mathematical systems. It is found that the abstract method is quite versatile in its application to concrete situations. It helps to free the problem from isolation and creates relations and transitions between fields which have at first no contact with one another.

In the abstract approach, one usually starts from a set of elements satisfying certain axioms. The nature of the elements is left unspecified. This is done on purpose. The theory then consists of logical consequences which result from the axioms and are derived as theorems once and for all. This means that in this axiomatic fashion one obtains a mathematical structure whose theory is developed in an abstract way. Those general theorems can then later be applied to various special sets satisfying those axioms.

In algebra this approach is used in connection with fields, rings and groups. In functional analysis we use it in connection with abstract spaces. Different such abstract spaces will be a set of (unspecified) elements satisfying different sets of axioms. Examples of such abstract spaces are metric space, normed linear space, inner product space, Banach space, Hilbert space etc. In this chapter we consider metric space. This space is fundamental in functional analysis because it playes a role similar to that of the real line R in calculus. In fact, it generalizes R and has been created in order to provide a basis for a unified treatment of important problems from various branches of analysis.

A metric space is a set X with a metric on it. The metric associates with any pair of elements of X. This metric is called a "distance". The distance function is defined axiomatically. The axioms are suggested by simple and most fundamental properties of the familiar distance function between points on the real line R and on the complex plane C. The concept of metric space was formulated by M. Frechet in 1906.

19.2 Objective

Analysis is mainly concerned with processes pertaining to limits. The definitions of covergence, continuity, differentiability and integrability are given in terms of limits. The concept of limit viz. $x \to \alpha$ means x approaches to α i.e. distance between x and α approaches to zero. This means whole analysis stands on the notion of distance. This notion of distance is extended to the elements of abstract set in the metric space. A metric space is nothing more than a non-empty set equipped with a concept of distance. We replace the set of real numbers R by an abstract set X containing elements of unspecified nature and introduce on X an "distance function". This distance function is chosen to satisfy a few of the most fundamental properties of the distance function in R and in C. In fact, the choice and formulation of these axioms always needs experience, familiarily with practical problems and a clear

idea of the goal to be reached. The axioms of distance function is an outcome of the long experience of many years. There are four axioms in it.

The purpose of this module is to develop in a systematic manner the main elementary facts about metric spaces.

19.3 Definition

Let X be any non empty set of elements $x, y, z, \ldots$ and $X \times X$ be the Cartesian product of X with itself. A metric on X is a mapping $d : X \times X \to \mathrm{R}$ which satisfies the following axioms for all $x, y, z \in X$

i) $d(x,y) \geq 0$ (non-negativity)

ii) $d(x,y) = 0$ if and only if $x = y$ (identity)

iii) $d(x,y) = d(y,x)$ (symmetry)

iv) $d(x,y) \leq d(x,z) + d(z,y)$ (triangle inequality)

The pair (X, d) is called a metric space, the real number $d(x,y)$ is called the distance between the elements x and y. The elements $x, y, z, \ldots$ are sometimes called points.

For a given non-empty set X we can define an infinite number of functions satisfying the above axioms. Thus for a given X it is possible to define an infinite number of metric spaces corresponding to these infinite number of distance functions. For examples, given a metric space (X, d) we may replace d by $\frac{d}{2}, \frac{d}{3}, \ldots$ and obtain metric spaces $\left(X, \frac{1}{k}d\right)$ for $k = 2, 3, 4, \ldots$

19.4 Examples

Example 19.4.1. Let R be the set of real numbers and d be a mapping $d : X \times X \to R$ defined as $d(x,y) = |x - y|$. Then (R, d) is a metric space known as usual metric space.

Example 19.4.2. Discrete metric space or Trivial metric space. Let X be a non empty set and define a mapping $X \times X \to R$ as follows

$$d(x,y) = \begin{cases} 0 \text{ when } x = y \\ 1 \text{ when } x \neq y \end{cases}$$

for all $x, y \in X$.

Then (X, d) is a metric space known as discrete metric space.

Solution : We have $d(x, y) \geq 0$ and $d(x, y)$ iff $x=y$.

If $x = y$ then $d(x, y) = 0 = d(y, x)$.

If $x \neq y$ then $d(x, y) = 1 = d(y, x)$.

$\therefore$ For all $x, y \in X$ we have $d(x, y) = d(y, x)$

To prove triangle inequality let $x, y, z \in X$.

If $x = y$, then $d(x, y) = 0$. Also $d(x, z) \geq 0$ and $d(z, y) \geq 0$.

Hence $d(x, y) \leq d(x, z) + d(z, y)$.

If $x \neq y$, then either $x \neq y \neq z \neq x$ or $x \neq y = z$ or $y \neq x = z$.

When $x \neq y \neq z \neq x$ then $d(x, y) = 1 < 1+1 = d(x, z) + d(z, y)$.

When $x \neq y = z$ then $d(x, y) = 1 = 1 + 0 = d(x, z) + d(z, y)$.

When $y \neq x = z$ then $d(x, y) = 1 = 0 + 1 = d(x, z) + d(z, y)$.

Thus $d(x, y) \leq d(x, z) + d(z, y) \quad \forall \quad x, y, z \in X$.

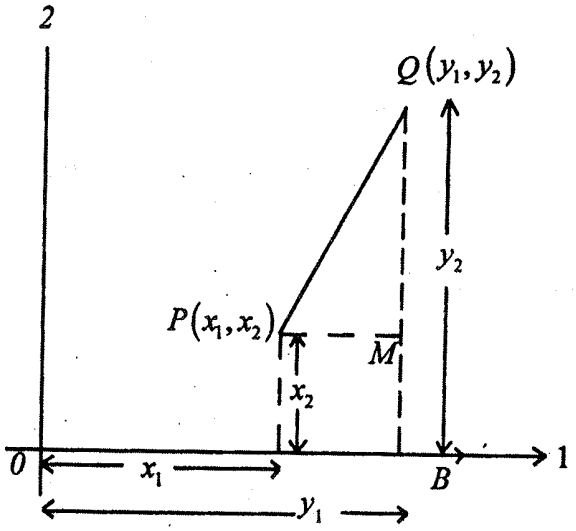
Hence (X, d) is a metric space.

Example 19.4.3. Usual metric space in R^2.

Let d be a mapping $d : R^2 \times R^2 \to R$ defined by

$d(x, y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}$ where $x = (x_1, x_2) \in R^2$ and $y = (y_1, y_2) \in R^2$, then (R^2, d) is a metric space, known as usual metric space

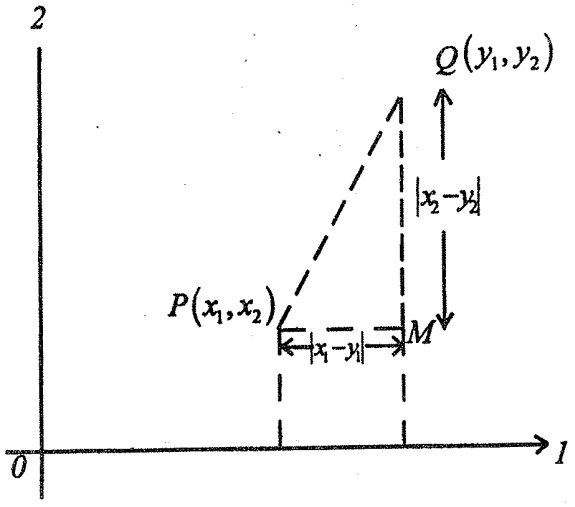
Here $d(x, y) = PQ$.



Example 19.4.4.

Let d be a mapping $d : R^2 \times R^2 \to R$ defined by $d(x,y) = |x_1 - y_1| + |x_2 - y_2|$ where $x = (x_1, x_2) \in R^2$ and $y = (y_1, y_2) \in R^2$ then (R^2, d) is a metric space

Here
$d(x, y) = PM + MQ$



Example 19.4.5

Let d be a mapping $d : R^2 \times R^2 \to R$ defined by $d(x,y) = \max\{|x_1 - y_1|, |x_2 - y_2|\}$ where $x = (x_1, x_2) \in R^2$ and $y = (y_1, y_2) \in R^2$, then (R^2, d) is a metric space.

Solution : Obviously, $d(x,y) \geq 0$

$d(x,y) = 0 \Leftrightarrow x = y$

and $d(x, y) = d(y, x)$.

To prove triangle inequality

Let $\alpha = d(x,z) = \max\{|x_1 - z_1|, |x_2 - z_2|\}$

$\beta = d(z,y) = \max\{|z_1 - y_1|, |z_2 - y_2|\}$.

Now $d(x,y) = \max\{|x_1 - y_1|, |x_2 - y_2|\}$

$\leq \max\{|x_1 - z_1| + |z_1 - y_1|, |x_2 - z_2| + |z_2 - y_2|\}$

$\leq \max\{\alpha + \beta, \alpha + \beta\}$

$= \alpha + \beta$

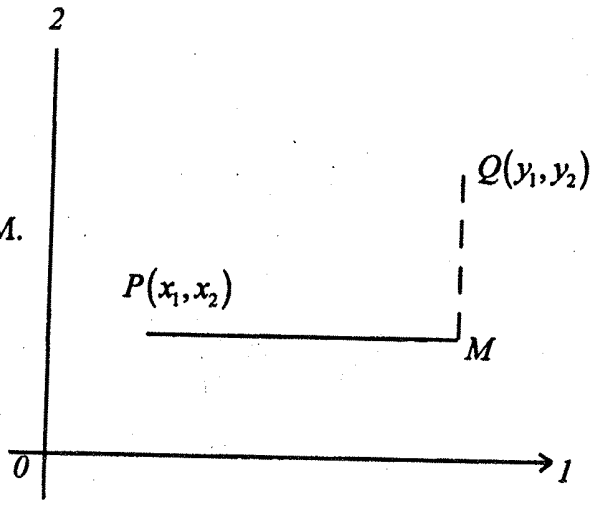
$= d(x, y) + d(z, y)$

i.e. $d(x,y) \leq d(x,z)+d(z,y)$

Thus (R^2, d) is a metric space.

Here

$d(x, y) = PM$ as PM>QM.



19.4.6 Some Important Inequalities

i) Cauchy-Schwarz inequality : If $u_1, u_2, ..., u_n$ and $v_1, v_2, ..., v_n$ are two sets of real numbers, then

$$\left(\sum_{i=1}^{n} u_i v_i\right)^2 \leq \left(\sum_{i=1}^{n} u_i^2\right)\left(\sum_{i=1}^{n} v_i^2\right)$$

ii) If a, b are real numbers, then

$$\frac{|a+b|}{1+|a+b|} \leq \frac{|a|}{1+|a|} + \frac{|b|}{1+|b|}$$

iii) **Minkowski's inequality : Let $u_1, u_2, ..., u_n \geq 0$ and $v_1, v_2, ..., v_n \geq 0$ be two sets of non-negative reals** and $p \geq 1$ then

$$\left(\sum_{i=1}^{n} (u_i + v_i)^p\right)^{\frac{1}{p}} \leq \left(\sum_{i=1}^{n} u_i^p\right)^{\frac{1}{p}} + \left(\sum_{i=1}^{n} v_i^p\right)^{\frac{1}{p}}$$

iv) Holder's inequality : Let $u_1, u_2, ..., u_n \geq 0$, $v_1, v_2, ..., v_n \geq 0$ be two sets of non-negative reals and $p > 1, \frac{1}{p} + \frac{1}{q} = 1$, then

$$\sum_{i=1}^{n} u_i v_i \le \left(\sum_{i=1}^{n} u_i^p\right)^{\frac{1}{p}} \left(\sum_{i=1}^{n} v_i^p\right)^{\frac{1}{p}}$$

Let $u_1, u_2, ..., u_n, ...$ and $v_1, v_2, ..., v_n, ...$ be two sets of real or complex numbers such that

$$\sum_{i=1}^{\infty} |u_i|^p < +\infty \text{ and } \sum_{i=1}^{\infty} |v_i|^p < +\infty \text{ where } p>1$$

Collection of such sets is denoted by the symbol l_p.

v) Minkowski's inequality :

If $x = (u_1, u_2, ..., u_n, ...) \in l_p$ and $y = (v_1, v_2, ..., v_n, ...) \in l_p$ where $p>1$ then

$$\left(\sum_{i=1}^{\infty} |u_i + v_i|^p\right)^{\frac{1}{p}} \le \left(\sum_{i=1}^{\infty} |u_i|^p\right)^{\frac{1}{p}} + \left(\sum_{i=1}^{\infty} |v_i|^p\right)^{\frac{1}{p}}$$

vi) Holder's inequality : If $x = \{u_i\} \in \ell_p$ and $y = \{v_i\} \in \ell_2$ where $\frac{1}{p} + \frac{1}{q} = 1, p > 1$, then

$$\left(\sum_{i=1}^{\infty} |u_i v_i|\right) \le \left(\sum_{i=1}^{\infty} |u_i|^p\right)^{\frac{1}{p}} \left(\sum_{i=1}^{\infty} |v_i|^p\right)^{\frac{1}{p}}.$$

19.4.7 Further Examples of Metric Spaces

Using above inequalities the triangle inequality axiom can be easily established for the following metric spaces.

Example 19.4.7.1 Three-dimensional Euclidean Space R^3. This metric space consists of the set R^3 of all ordered triples of real numbers $x = (x_1, x_2, x_3), y = (y_1, y_2, y_3)$ etc. and the Euclidean metric is defined by

$$d(x,y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + (x_3 - y_3)^2}$$

Example 19.4.7.2. n-dimensional Euclidean Space R^n.

This metric space consists of the set R^n of all ordered n-tuples of real numbers

$x = (x_1, x_2, ..., x_n), y = (y_1, y_2, ..., y_n)$ etc. and the Euclidean metric is defined by

$$d(x,y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + ... + (x_n - y_n)^2}$$

Example 19.4.7.3. n-dimensional unitary space C^n or complex Euclidean n-space. n-dimensional unitary space C^n.

This is the space of all ordered n-tuples of complex numbers $x = (x_1, x_2, ..., x_n), y = (y_1, y_2, ..., y_n)$ etc. with metric defined by

$$d(x,y)=\sqrt{|x_1-y_1|^2+|x_2-y_2|^2+...+|x_n-y_n|^2}$$

For n=1 we get the metric space of complex plane C with the usual metric defined by $d(x,y)=|x-y|$. Here x, y are complex numbers.

Example 19.4.7.4

The set R^n of all ordered n-tuples of real numbers $x=(x_1,x_2,...,x_n), y=(y_1,y_2,...,y_n)$ etc. forms a metric space with metric defined by

$$d(x,y)=\left(\sum_{j=1}^{n}|x_j-y_j|^p\right)^{\frac{1}{p}} \text{ where } p\geq 1$$

For $p=2$ we get the n-dimensional Euclidean space R^n

For $p=1$ we get a metric space for R^n with the metric as

$$d(x,y)=\sum_{j=1}^{n}|x_j-y_j|$$

Example 19.4.7.5.

The set C^n of all ordered n-tuples of complex numbes $x=(x_1,x_2,...,x_n), y=(y_1,y_2,...,y_n)$ etc. forms a metric space with metric defined by

$$d(x,y)=\left(\sum_{j=1}^{n}|x_j-y_j|^p\right)^{\frac{1}{p}} \text{ where } p\geq 1.$$

Here all x_j and y_j are complex numbers and p is real number.

Example 19.4.7.6 Sequence Space s.

This space consists of the set of all (bounded or unbounded) sequences of real a complex numbers and the metric d is defined by

$$d(x,y)=\sum_{j=1}^{\infty}\frac{1}{2^j}\left(\frac{|x_j-y_j|}{1+|x_j-y_j|}\right)$$

where $x=\{x_j\}$ and $y=\{y_j\}$.

Example 19.4.7.7 Real or Complex l^p space.

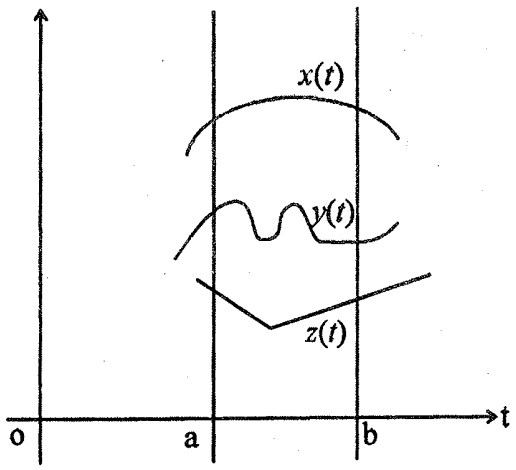
Let $p \geq 1$ be a fixed real number and l^p be the set of all real or complex sequences $x = \{x_j\}$, such that $|x_1|^p + |x_2|^p + ... + |x_n|^p + ...$ converges. Then

$d(x,y) = \left(\sum_{j=1}^{\infty} |x_j - y_j|^p \right)^{\frac{1}{p}}$ is a metric and (l^p, d) is a real or complex l^p space according as the sequences forming the set l^p is real or complex respectively.

Example 19.4.7.8 Function Space $C[a, b]$.

Let $C[a, b]$ be the set of all continuous functions $x = x(t), y = y(t)$, etc. defined on the closed interval $[a, b]$

Then $d(x,y) = \max_{a \leq t \leq b} |x(t) - y(t)|$ is a metric and $(C[a,b], d)$ forms a metric space known as function space.



Example 19.4.7.9 Convergent Sequence Space c.

Let c be the set of all convergent sequences $x = \{x_j\}, y = \{y_j\}$. etc. Then

$d(x,y) = \sup_j |x_j - y_j|$ is a metric and (c, d) is known as convergent sequence space.

Example 19.4.7.10. Null Sequence Space c_o.

Let c_o be the set of all null sequences $x = \{x_j\}, y = \{y_j\}$. etc.

Then $d(x,y) = \sup_j |x_j - y_j|$ is a metric and the metric space (c_o, d) is known as the null sequence space c_o.

19.5 Open set, closed set and their properties

19.5.1 Definition : Open Sphere or Open Ball

Let (X, d) be a metric space and 'a' be any point of it.

Then for any real number $r>0$, the set

$$B_r(a)=\{x\in X : d(x,a)<r\}$$

is called an open sphere or an open ball with centre 'a' and radius r.

The notations $B(a, r)$, $S_r(a)$, $S(a, r)$ are also used to denote $B_r(a)$.

19.5.2. Definition : Closed Sphere a Closed Ball

Let (X, d) be a metric space and 'a'f be any point of X. Then for any real number $r>0$, the set

$$\overline{B}_r(a)=\{x\in X : d(x,a)\le r\}$$

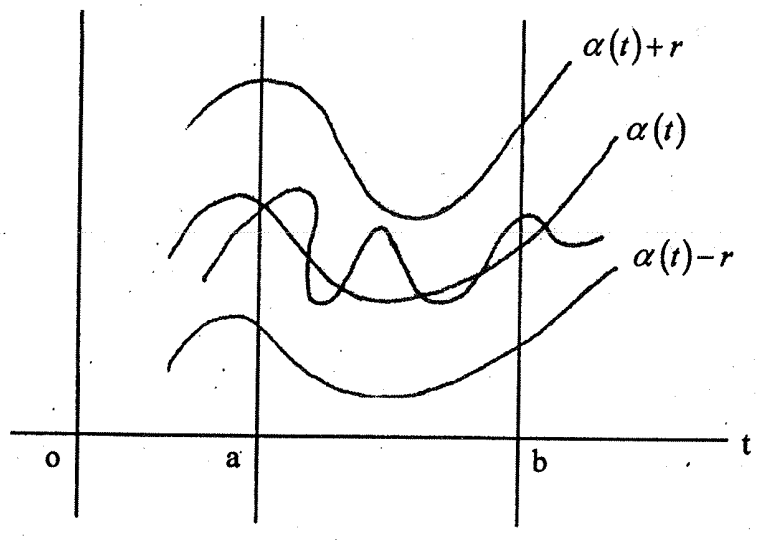
is called a closed sphere or a closed ball with centre 'a' and radius r.

Examples : For the usual metric space (R, d), the open interval $]a-r, a+r[$ and the closed interval $[a-r, a+r]$ are respectively open ball and closed ball with centre 'a' and radius r.

For the function space $C[a, b]$, the open ball with centre $\alpha(t)$ and radius $r>0$ is given by the set of all continuous function $x(t)$ defined on the closed interval $[a, b]$ satisfying the condition

$$\alpha(t)-r<x(t)<\alpha(t)+r$$

i.e. $$B_r(\alpha)=\{x(t)\in C[a,b] : \max_{a\le t\le b}|x(t)-\alpha(t)|<r\}.$$



Open Set $B_r(\alpha)$ in $C[a,b]$

For trivial metric space (X, d)

$B_r(a) = \{a\}$ for all r in $(0, 1]$

and $B_r(a) = X$ for all $r>1$

19.5.3 Definition. Neighbourhood of a point

Let (X, d) be a metric space. A set $N \subset X$ is called a *nbd* of a point $a \in X$ if there exists some $r>0$ such that $B_r(a) \subset N$.

19.5.4 Definition. Open Set.

Let (X, d) be a metric space. A set $G \subset X$ is said to be an open set if for each $x \in G$, there exists $r>0$ such that $B_r(x) \subset G$.

19.5.5. Theorem. Each Open sphere is an open set but the converse is not true.

Proof. Let (X, d) be any metric space and $B_r(a)$ be any open sphere in X. Let $x \in B_r(a)$. Then $d(x,a)<r$. Hence $r-d(x, a)>0$. Let $r_1 = r - d(x,a)$. We now show that $B_{r_1}(x) \subset B_r(a)$. To show this let $y \in B_{r_1}(x)$. Then $d(y,x) < r_1$.

Therefore, $d(y,a) \leq d(y,x) + d(x,a)$

$< r_1 + d(x,a)$

$= r$

$\therefore y \in B_r(a)$. Thus $B_{r_1}(x) \subset B_r(a)$ showing that each point of $B_r(a)$ is the centre of an open sphere contained in it. Hence $B_r(a)$ is an open set.

The converse is not true. For example in the usual metric space (R, d) the set $]2, 4[\cup]8, 12[$ is an open set but not an open sphere.

19.5.6. Theorem: A subset G of a metric space (X, d) is open if and only if it is a union of open spheres.

Proof. Let G be an open set of (X, d) and x be any point of G. Since G is an open set there exists an open ball $B_{r_x}(x) \subset G$. Hence $G = \bigcup_{x \in G} B_{r_x}(x)$.

Conversely, let G be the union of a collection F of open spheres. If F is empty, then G is also empty and hence it is open. If F is non empty then G is also non-empty. Let x be any point of G. Since G is the union of open spheres there exists an open sphere, say $B_r(a)$ such that $x \in B_r(a)$. We note that $B_r(a) \subset G$, as G is the union of open spheres. Since each open sphere is an open set and $x \in B_r(a)$ there exists an open sphere $B_{r_1}(x)$ such that $B_{r_1}(x) \subset B_r(a)$. Hence $B_{r_1}(x) \subset G$ showing that G is an open set.

19.5.7. Theorem. Let (X, d) be a metric space. Then

i) ϕ and X are open sets.

ii) the union of any number of open sets in X is open

iii) the intersection of a finite number of open sets in X is open.

Proof.

(i) To prove that ϕ is open, we have to show that each point in ϕ is the centre of an open sphere contained in ϕ. Since there is no point in ϕ, this requirement is automatically satisfied. Hence ϕ is an open set. Let $x \in X$. Now from the definition of open sphere, every open sphere $B_r(x)$ is contained in X. Hence X is an open set.

(ii) Let $\{G_\lambda : \lambda \in I\}$ be any arbitrary collection of open sets in a metric space (X, d) and $G = \bigcup_{\lambda \in I} G_\lambda$ Let x be an arbitrary point of G. Then for at least one index λ_1 we have $x \in G_{\lambda_1}$. Since G_{λ_1} is open, there exists $r>0$ such that $B_r(x) \subset G_{\lambda_1}$ and hence $B_r(x) \subset G$. Thus G is an open set.

(iii) Let $\{G_i : i = 1, 2, ..., n\}$ be a finite collection of open sets in X and $G = \bigcap_{i=1}^{n} G_i$. If G is empty then it is open. Let G be non-empty and x be any arbitrary point of G. Then $x \in G_i$ for each $i = 1, 2, ..., n$. But each G_i is open. Hence for each i there exists $r_i > 0$ such that $B_{r_i}(x) \subset G_i$. Let $r = \min\{r_1, r_2, ..., r_n\}$. Then for each i, $B_r(x) \subset G_i$. Hence $B_r(x) \subset \bigcap_{i=1}^{n} G_i$ i.e. $B_r(x) \subset G$. This G is open.

19.5.8. Definition. Closed Set.

A subset F of a metric space (X, d) is said to be closed if tis complement in X is open i.e. if $X-F$ is open.

19.5.9. Theorem. Let (X, d) be a metric space. Then

i) ϕ and X are closed sets

ii) the intersection of any number of closed sets in X is closed.

iii) the union of a finite number of closed sets in X is closed.

Proof. Left as an exercise for the reader.

19.5.10. Topological Space.

Let X be any nonempty set. A topology on X is a collection $\Im$ of subsets of X which satisfies the following

axioms :

i) $\phi, X \in \Im$

ii) any union of members of $\Im$ is a member of $\Im$.

iii) the intersection of finite number of members of $\Im$ is a member of $\Im$.

The set X together with a topology $\Im$ is called a topological space and is written as $(X, \Im)$.

The members of the topology $\Im$ are called open sets of the topological space $(X, \Im)$.

The complement of the members of the topology $\Im$ with respect to X are called closed sets of the topologcal space $(X, \Im)$.

19.5.11. Examples.

Discrete Topology : If X is any non empty set and $\Im$ consists of all subsets of X, then $\Im$ is a topology of X and this is called the discrete topology.

Indiscrete Topology : If X is any non empty set and $\Im = \{\phi, X\}$, then $\Im$ is a topology for X and this is called the indiscrete topology.

From Theorem 19.5.7 it follows that every metric space is a topological space with the corresponding topology as the collection of all open sets of the metric space.

Let $X = \{a, b, c\}$, then $\Im = \{\phi, X, \{a\}, \{b\}, \{a,b\}\}$ is a topology.

Let $X = \{a, b, c\}$ then $\Im = \{\phi, X, \{a\}, \{b\}, \{c\}\{a,b\}, \{b,c\}, \{c,a\}\}$ is a topology.

Let $X = \{a, b, c\}$ then $\Im = \{\phi, X, \{a\}, \{b\}, \{b,c\}\}$ is not a topolgy since $\{a\}, \{b\} \in \Im$ but $\{a,b\} \notin \Im$.

Let $X = R$ and let $\Im$ consists of the null set ϕ and all open intervals only. Then $\Im$ is not a topology on R since $]2,3[,]5,8[\in \Im$ but their union $]2,3[\cup]5,8[\notin \Im$.

19.6 Seperable Metric Space

19.6.1 Definition. Interior of a Set.

Let (X, d) be a metric space. The interior of a set $A \subset X$ is the union of all open sets contained in A.

19.6.2. Definition : Nowhere dense and Dense subset.

A set $A \subset X$ is said to be nowhere dense if the closure set $\bar{A}$ of A has empty interior.

A set $A \subset X$ is said to be dense in X if $\bar{A} = X$.

e.g. The set of all natural numbers is nowhere dense in R and set of all rational numbers is dense in R.

19.6.2. Definition. Separable metric space.

A metric space X is said to be separable if X has a countable dense subset i.e. if there is a countable subset A of X such that $\bar{A} = X$.

e.g. The metric space (R, d) where d is the usual distance is separable since the set Q of rational numbers is countable and $\bar{Q} = R$.

19.6.3. Theorem. The space ℓ^p is separable.

Proof. We know that $\ell^p = \left\{ x = \{x_n\} : \sum_{n=1}^{\infty} |x_n|^p < \infty \right\}$

and $d(x, y) = \left(\sum_{n=1}^{\infty} |x_n - y_n|^p \right)^{\frac{1}{p}}$

Let $D_1 = \{ x \in \ell^p : x = \{x_n\}$ with all x_n rational$\}$

and $D_2 = \{ x \in \ell^p :$ the set of n for which $x_n \neq 0$ is finite$\}$

Then both D_1 and D_2 are countable.

Let $D = D_1 \cup D_2$. Therefore D is countable subset of ℓ^p. We show now that $\bar{D} = \ell^p$ i.e. for any given $\varepsilon > 0$ and for any $x \in \ell^p$ there exists $y \in D$ such that $d(x, y) < \varepsilon$.

Let $\varepsilon > 0$ be given and $x = \{x_n\}$ be any element of ℓ^p. Since $\sum_{n=1}^{\infty} |x_n|^p$ is convergent there exists positive integer n_0 such that

$$\sum_{n=n_0+1}^{\infty} |x_n|^p < \frac{\varepsilon^p}{2} \qquad \text{..... (1)}$$

We choose $y = \{y_n\}$ of D such that all y_n are rational with $y_n = 0$ for all $n > n_0$ and $|x_k - y_k|^p < \frac{\varepsilon^p}{2n_0}$ for all $k = 1, 2, ..., n_0$. ..... (2)

Now $d(x, y) = \left(\sum_{n=1}^{\infty} |x_n - y_n|^p \right)^{\frac{1}{p}}$

$$= \left(\sum_{n=1}^{n_0} |x_n - y_n|^p + \sum_{n=n_0+1}^{\infty} |x_n - 0|^p \right)^{\frac{1}{p}}$$

$$< \left(n_0 \cdot \frac{\varepsilon^p}{2n_0} + \frac{\varepsilon^p}{2} \right), \text{ [by (1) and (2)]}$$

$$< \left(\frac{\varepsilon^p}{2} + \frac{\varepsilon^p}{2} \right)^{\frac{1}{2}}$$

$$= \varepsilon$$

i.e. $d(x, y) < \varepsilon$

Hence ℓ^p is separable metric space.

19.6.4. Theorem : The metric space $\ell_\infty = \{x = \{x_k\} : \sup|x_k| < \infty\}$ with the metric $d(x, y) = \sup_k |x_k - y_k|$ is not separable.

Proof. Let $\{x^i\}$ be any countable set in ℓ_∞ where

$x^i = \{x_n^i\} \in \ell_\infty$.

Let us consider the element $x = \{x_n\}$ of ℓ^p defined as follows.

For each $k = 1, 2, 3, \ldots$

$x_k = x_k^k + 1$ if $|x_k^k| \leq 1$

$= 0$ if $|x_k^k| > 1$

$\therefore$ For each $k = 1, 2, 3, \ldots$ we have $|x_k - x_k^k| \geq 1$ ..... (1)

Now $d(x, x^k)$

$= \sup|x_n - x_n^k|$

$= \sup\{|x_1 - x_1^k|, |x_2 - x_2^k|, \ldots, |x_{k-1} - x_{k-1}^k|, |x_k - x_k^k|, |x_{k+1} - x_{k+1}^k|, \ldots, |x_n - x_n^k|, \ldots\}$

≥ 1 [by (1)]

Thus for each $k = 1, 2, 3, \ldots$ we have $d(x, x^k) \geq 1$.

This means x is not a limit point of $\{x^i\}$

Hence closure of $\{x^i\}$ is not ℓ_∞.

This is true for any countable set $\{x^i\}$ of ℓ_∞. Hence ℓ_∞ is not separable.

19.6.5. Definition. Hausdorff space.

A metric space (X, d) is said to be Hausdorff if for any pair of distinct points x and y in X, there exist two disjoint open sets, one containing x and other containing y.

19.6.6. Theorem. Every metric space is a Hausdorff space.

Proof. Let (X, d) be a metric space and x, y be any two distinct points of X i.e. $x \neq y$ and $x, y \in X$.

Since $x \neq y, d(x,y) > 0$.

Let $d(x,y) = r$. Then $r > 0$. Let us consider the open balls $B_{\frac{r}{4}}(x)$ and $B_{\frac{r}{4}}(y)$.

We show now that $B_{\frac{r}{4}}(x)$ and $B_{\frac{r}{4}}(y)$ are disjoint.

If possible, let they be not disjoint. Then there exists $z \in X$ such that $z \in B_{\frac{r}{4}}(x)$ and $z \in B_{\frac{r}{4}}(y)$.

Hence $d(x,z) < \frac{r}{4}$ and $d(y,z) < \frac{r}{4}$.

Now $d(x,y) \leq d(x,z) + d(y,z) < \frac{r}{4} + \frac{r}{4} = \frac{r}{2}$

or, $d(x,y) < \frac{r}{2}$.

But $d(x,y) = r$. $\therefore r < \frac{r}{2}$. This is a contradiction

Thus $B_{\frac{r}{4}}(x)$ and $B_{\frac{r}{4}}(y)$ are disjoint.

Hence the theorem.

19.7. Illustrative Examples

19.7.1 Show that R^n is a metric space with metric $d(x,y) = \max_i |x_i - y_i|$ where $x = (x_1, x_2, ..., x_n)$ and $y = (y_1, y_2, ..., y_n)$.

Solution. Here $d(x,y) = \max_i |x_i - y_i|$

i) As $|x_i - y_i| \geq 0$ we have $d(x,y) \geq 0$.

ii) $d(x,y)=0 \Leftrightarrow \max_i |x_i - y_i| = 0$

$\Leftrightarrow |x_i - y_i| = 0$ for all $i = 1, 2, ..., n$

$\Leftrightarrow x_i = y_i$ for all $i = 1, 2, ..., n$

$\Leftrightarrow x = y$

iii) $d(x,y) = \max_i |x_i - y_i|$

$= \max_i |y_i - x_i|$

$= d(y,x)$

iv) $d(x,y) = \max_i |x_i - y_i|$

$\leq \max_i \{|x_i - z_i| + |z_i - y_i|\}$

$\leq \max_i |x_i - z_i| + \max_i |z_i - y_i|$

$= d(x, z) + d(z, y)$

$\therefore d(x,y) \leq d(x,z) + d(z,y)$

So R^n is a metric space with $d(x,y) = \max_i |x_i - y_i|$.

19.7.2. Prove that $C[a,b]$, the set of all continuous real valued functions defined on a closed bounded interval $[a, b]$ is a metric space with the metric

$$d(x,y) = \int_a^b |x(t) - y(t)|\, dt.$$

Solution :

i) We have $|x(t) - y(t)| \geq 0$ for all $t \in [a,b]$

$\therefore \int_a^b |x(t) - y(t)|\, dt \geq 0$ i.e. $d(x,y) \geq 0$.

ii) $d(x,y) = 0 \Leftrightarrow \int_a^b |x(t) - y(t)|\, dt = 0$

$\Leftrightarrow |x(t) - y(t)| = 0$ [as $x(t), y(t)$ are continuous in $[a, b]$]

$\Leftrightarrow x(t) - y(t) = 0$ for all $t \in [a,b]$

$\Leftrightarrow x = y$

iii) $d(x,y)=\int_a^b |x(t)-y(t)|\,dt$

$=\int_a^b |y(t)-x(t)|\,dt$

$=d(y,x)$

iv) $d(x,y)=\int_a^b |x(t)-y(t)|\,dt$

$=\int_a^b |x(t)-z(t)+z(t)-y(t)|\,dt$

$\leq \int_a^b |x(t)-z(t)|\,dt+\int_a^b |z(t)-y(t)|\,dt$

$=d(x,z)+d(z,y)$

$\therefore d(x,y)\leq d(x,z)+d(z,y)$

So, $C[a, b]$ is a metric space with d as metric.

19.7.3. Let (X, d) be a metric space. Show that

$d'(x,y)=\dfrac{d(x,y)}{1+d(x,y)}$ for all $x, y \in X$ is also a metric of X.

Solution. Since (X, d) is a metric space we have fro any $x, y, z \in X$

i) $d(x,y)\geq 0$

ii) $d(x,y)=0 \Leftrightarrow x=y$

iii) $d(x,y)=d(y,x)$

and iv) $d(x,y)\leq d(x,z)+d(z,y)$

Now $d'(x,y)=\dfrac{d(x,y)}{1+d(x,y)}$ ..... (1)

For any $x, y, z \in X$ we have

i) Since $d(x,y)\geq 0$ from (1) it follows that $d'(x,y)\geq 0$

ii) $d'(x,y)=0 \Leftrightarrow \dfrac{d(x,y)}{1+d(x,y)}=0$

$\Leftrightarrow d(x,y)=0$

$\Leftrightarrow x=y$

iii) $d'(x,y)=\frac{d(x,y)}{1+d(x,y)}=\frac{d(y,x)}{1+d(y,x)}=d'(y,x)$

iv) We have

$$d'(x,z)+d'(z,y)$$

$$=\frac{d(x,z)}{1+d(x,z)}+\frac{d(z,y)}{1+d(z,y)}$$

$$\geq\frac{d(x,z)}{1+d(x,z)+d(z,y)}+\frac{d(z,y)}{1+d(z,y)+d(x,z)}\quad\left[\because d(z,y)\geq 0 \text{ and } d(x,z)\geq 0\right].$$

$$=\frac{d(x,z)+d(z,y)}{1+d(x,z)+d(z,y)}$$

$$=1-\frac{1}{1+d(x,z)+d(z,y)} \qquad \text{..... (2)}$$

Now, $d(x,z)+d(z,y)\geq d(x,y)$

or, $1+d(x,z)+d(z,y)\geq 1+d(x,y)$

or, $\frac{1}{1+d(x,z)+d(z,y)}\leq\frac{1}{1+d(x,y)}$

or, $1-\frac{1}{1+d(x,z)+d(z,y)}\geq 1-\frac{1}{1+d(x,y)}$

Thus from (2), we get

$$d'(x,z)+d'(z,y)$$

$$\geq 1-\frac{1}{1+d(x,y)}$$

$$=\frac{d(x,y)}{1+d(x,y)}$$

$$=d'(x,y)$$

i.e. $d'(x,y)\leq d'(x,z)+d'(z,y)$

Hence the result.

We note that (X, d') is always bounded since $d'(x,y) = \dfrac{d(x,y)}{1+d(x,y)} \leq 1$.

19.7.4. Let X be a non-empty set and $\rho : X \times X \to R$ be defined satisfying

i) $\rho(x,y) = 0$ if and only if $x = y$

and ii) $\rho(x,y) \leq \rho(x,z) + \rho(y,z)$ for any $x, y, z \in X$

Show that (X, ρ) is a metric space.

Proof. Putting $x = y$ in (ii) we get

$$0 \leq \rho(x,z) + \rho(x,z)$$

or, $0 \leq 2\rho(x,z)$

or, $\rho(x,z) \geq 0$.

Since x, z are arbitrary, it follows that $\rho(x,y) \geq 0$ for all $x, y \in X$.

Putting $z = x$ in (*ii*) we have

$$\rho(x,y) \leq \rho(x,x) + \rho(y,x)$$

or, $\rho(x,y) \leq 0 + \rho(y,x)$

or, $\rho(x,y) \leq \rho(y,x)$ ..... (1)

This is true for any $x, y \in X$. So interchanging x and y in (1) we get

$$\rho(y,x) \leq \rho(x,y)$$ ..... (2)

From (1) and (2) $\rho(x,y) = \rho(y,x)$.

Hence (X, ρ) is a metric space.

19.8. Summary

In real analysis we have studied limit, continuity, derivative, integration etc. All these are dependent on the concept of distance $|x-y|$ between two points x and y on the real axis. It is seen that distance $|x-y|$ between two points $x, y \in R$ is nothing but a function from $R \times R$ to R satisfying some axioms.

Replacing R by any set X and the distance $|x-y|$ by the distance function $d : X \times X \to R$ we have defined a metric space (X, d). Various metric spaces and properteis of such metric spaces have been studied in this module.

19.9 Self Assessment Questions

1. Let C be the set of all complex numbers. Show that the mapping $d: C \times C \to R$ defined by $d(z_1, z_2) = |z_1 - z_2|$ is a metric for C.

2. Let $d: R \times R \to R$ be defined by

$$d(x,y) = \min[1, y-x] \text{ if } x \le y$$
$$= 0 \qquad \text{if } x > y.$$

Show that d is not a metric.

3. Let R^2 be the set of all ordered pairs of real numbers and let $d: R^2 \times R^2 \to R$ by defined by

$$d((x_1,x_2),(y_1,y_2)) = \left\{(x_1-y_1)^2 + (x_2-y_2)^2\right\}^{1/2} \text{ is a metric}$$

4. Let R^n be the set of all ordered n-touples of real numbers and let $d: R^n \times R^n \to R$ be defined by

$$d(x,y) = \left\{\sum_{i=1}^{n}(x_i - y_i)^2\right\}^{1/2} \text{ where } x = (x_1, x_2, ..., x_n) \text{ and } y = (y_1, y_2, ..., y_n).$$

Show that d is a metric.

5. Let S be the set of all sequences of reals and let $d: S \times S \to R$ be defined by

$$d(x,y) = \sum_{n=1}^{\infty} \frac{|x_n - y_n|}{2^n(1+|x_n - y_n|)}$$

where $x = \{x_n\}$ and $y = \{y_n\}$. Show that d is a metric.

6. Let R^n be the set of all ordered n-tuples of real numbers and let $d: R^n \times R^n \to R$ be defined by

$$d(x,y) = \left\{\sum_{i=1}^{n}|x_i - y_i|\right\} \text{ where } x = (x_1, x_2, ..., x_n) \text{ and } y = (y_1, y_2, ..., y_n).$$

Show that d is a metric.

7. Prove that $C[a,b]$, the set of all continuous real valued functions defined on the closed interval $[a,b]$ is a metric space with metric as

$$d(x,y) = \max_{a \le t \le b}|x(t) - y(t)|$$

8. Let ℓ_∞ denote the set of all bounded sequences. If $x=\{x_n\}$ and $y=\{y_n\}$ are any two points of ℓ_∞ and $d(x,y)=\sup_n|x_n-y_n|$ then show that ℓ_∞ is a metric space under d.

9. Described open spheres of unit radius about (0, 0) for each of the following metrices for R^2

   i) $d_1(x,y)=\left\{(x_1-x_2)^2+(y_1-y_2)^2\right\}^{1/2}$

   ii) $d_1(x,y)=|x_1-x_2|+|y_1-y_2|$

   iii) $d_3(x,y)=\max\{|x_1-x_2|,|y_1-y_2|\}$

   where $x=(x_1,x_2)$ and $y=(y_1,y_2)$ are any two points of R^2.

19.10. Suggested books for further reading

1. Functional Analysis with Applications : B. Choudhary and Sudarsan Nanda; Wiley Eastern Limited.
2. Elements of Functional Analysis : B.K. Lahiri; World Press
3. Introductory Functional Analysis with Applications : Erwin Kreyszig; John Wiely & Sons
4. Mathematical Analysis : S.C. Malik, Savita Arora; Wiely Eastern Limited
5. Functional Analysis : J.N. Sharma, A.R. Vasishtha; Krishna Prakashan Mandir
6. Elements of Real Analysis : Shanti Narayan, M.D. Raisinghania; S. Chand.

---- 0 ----

M.Sc. Course
in
Applied Mathematics with Oceanology
and
Computer Programming

PART-I

Paper-II Group-B

Module No. - 20

Functional Analysis

(Complete and Compact Metric Spaces)

Contents :

20. Complete and Compact Metric Spaces

19.1 Introduction :

Completeness, compactness and separability of a metric space are additional properties of a metric space. A metric space may or may not have any one of these properties. But if a metric space has such properties then the metric space becomes much nicer and simpler. The set of all real numbers R has all of these properties. If a metric space has such properties then the metric space becomes closer to the properties of real numbers. Completeness

of the real line R is the main reason why in calculus we use R rather than the rational line Q. Compact property of a metric space has some relation with uniform continuity. It has connection with the closed and bounded properties of the space. Separable space has a close relation with the dense property of the space. These three properties are also interrelated. In fact every compact metric space is separable and every sequentially compact metric space is complete.

19.2 Objective

The main objective is to study the important properties of special metric spaces viz. complete metric space and compact metric space. These two metric spaces are not independent to one another. Their interrelations are studied here.

20.3 Complete Metric Space

20.3.1 Definition. Cauchy Sequence

Let (X, d) be a metric space and let $\{x_n\}$ be a sequence in it. The sequence $\{x_n\}$ is said to be a Cauchy sequence if for every $\varepsilon > 0$ there exists a positive integer n_0 such that

$$d(x_m, x_n) < \varepsilon \text{ for all } m, n \geq n_0$$

20.3.2 Definition. Convergent Sequence

Let (X, d) be a metric space and let $\{x_n\}$ be a sequence in it. The sequence $\{x_n\}$ is said to be convergent to an element x in X if for every $\varepsilon > 0$ there exists a positive integer n_0 such that

$d(x_n, x) < \varepsilon$ for all $n \geq n_0$. We write it as $\lim_{n \to \infty} x_n = x$.

20.3.3. Theorem. Every convergent sequence in a metric space is a Cauchy sequences, but the converse is not true in general.

Proof. Let (X, d) be a metric space and $\{x_n\}$ be any convergent sequence in X converging to the element x in X.

Let $\varepsilon > 0$ be any pre assigned positive number, however small. Then there exists n_0 such that

$d(x_n, x) < \varepsilon/2$ for all $n \geq n_0$.

For $m, n \geq n_0$ we have

$$d(x_m, x_n) \leq d(x_m, x) + d(x_n, x) < \varepsilon/2 + \varepsilon/2 = \varepsilon$$

Hence $\{x_n\}$ is a Cauchy sequence.

To show that the converse of this theorem is not true let $X = (1, 2)$ and the metric d be $d(x, y) = |x - y|$.

Then $\left\{1 + \frac{1}{n}\right\}$ is a Cauchy sequence. But this sequence does not converge in X as $\lim_{n \to \infty}\left(1 + \frac{1}{n}\right) = 1$ but $1 \notin X$.

20.34. Definition. Complete Metric Space.

A metric space (X, d) is said to be complete if every Cauchy sequence in it converges to an element of it.

20.3.5. Examples of Incomplete Metric Spaces .

The set of all rational numbers Q is an incomplete metric space with the usual metric $d(x, y) = |x - y|$. This is because the sequence {1.4, 1.41, 1.414,...} is a Cauchy sequence but it is not convergent in Q as $\sqrt{2} \notin Q$.

If $X = (2, 5)$ then with the usual metric it is not complete as $\left\{2 + \frac{1}{n}\right\}$ is a Cauchy sequence in X but it is not convergent in X, since here $2 \notin X$.

20.3.6. Examples of Complete Metric Spaces

i) The real line R with the usual metric $d(x, y) = |x - y|$ is a complete metric space.

ii) The set C of all complex numbers is a complete metric space with the usual metric $d(x, y) = |x - y|$.

iii) If $X = [2, 5]$ then with the usual metric it is a complete metric space.

iv) The set R^n of all n-tuples of real numbers is a complete metric space with metric

$$d(x, y) = \sqrt{\sum_{j=1}^{n}(x_j - y_j)^2} \text{ where } x = (x_1, x_2, ..., x_n) \text{ and } y = (y_1, y_2, ..., y_n).$$

v) The set C^n of all n-tuples of complex numbers is a complete metric space with metric

$$d(x,y)=\sqrt{\sum_{j=1}^{n}|x_j-y_j|^2} \text{ where } x=(x_1,x_2,...,x_n) \text{ and } y=(y_1,y_2,...,y_n).$$

20.3.7. Show that any set X with the discrete metric forms a complete metric space.

Solution. Let $\{x_n\}$ be any Cauchy sequence in the discrete metric space (X, d).

Then $d(x_m,x_n)=0$ if $x_m=x_n$

$=1$ if $x_m\neq x_n$

Since $\{x_n\}$ is a Cauchy sequence for any $\varepsilon>0$ there exists n_0

s.t. $d(x_m,x_n)<\varepsilon$ for all $m,n\geq n_0$.

Let us take $\varepsilon=\frac{1}{2}$ then there exists p s.t.

$$d(x_m,x_n)<\varepsilon\ \forall m,n\geq p$$

As $\varepsilon=\frac{1}{2}<1$ we have $x_m=x_n\ \forall\ m,n\geq p$

i.e. $x_n=x_m\ \forall\ n\geq p$

i.e. $x_n\to x_m$ as $n\to\infty$

i.e. $\{x_n\}$ converges to $x_m\in X$.

Hence discrete metric space is complete.

20.3.8. Show that for $p\geq 1$ the set $\ell^p=\left\{x=\{x_j\}:\sum|x_j|^p<\infty\right\}$ forms a complete metric space with metric

$$d(x,y)=\left(\sum_{j=1}^{\infty}|x_j-y_j|^p\right)^{1/p}$$

Solution. Let $\{x^i\}$ be any Cauchy sequence in ℓ^p where $x^i=\{x_k^i\}\in\ell^p$ for each i.

Now for each fixed k we have

$$|x_k^i-x_k^j|=\left(0+0+0+|x_k^i-x_k^j|^p+0+...+o\right)^{\frac{1}{p}}$$

$$\leq \left(\sum_{\ell=1}^{\infty} \left|x_\ell^i - x_\ell^j\right|^p\right)^{\frac{1}{p}}$$

$$= d\left(x^i, x^j\right) \qquad \text{..... (1)}$$

Since $\{x^i\}$ is Cauchy sequence we have $d\left(x^i, x^j\right) \to 0$ as $i, j \to \infty$

Thus for each fixed k from (1) we get $\left|x_k^i - x_k^j\right| \to 0$ as $i, j \to \infty$..

This means $\{x_k^i\}$ is a Cauchy sequence of real numbers for each fixed k. Now we know that the set of real numbers is complete. Hence for each k there exists real number x_k such that $x_k^i \to x_k$ as $i \to \infty$.

Let $x = \{x_k\}$. We now show that $x \in \ell^p$ and that $x^i \to x$ as $i \to \infty$.

Now for any t we have

$$\left(\sum_{k=1}^{t} \left|x_k^i\right|^p\right)^{\frac{1}{p}} \leq \left(\sum_{k=1}^{\infty} \left|x_k^i\right|^p\right)^{\frac{1}{p}}$$

$$\leq K$$

Letting $i \to \infty$, we get

$$\left(\sum_{k=1}^{t} \left|x_k\right|^p\right)^{\frac{1}{p}} \leq K \text{ [from definition of } \ell^p\text{]}$$

Letting $t \to \infty$, we get $\left(\sum_{k=1}^{\infty} \left|x_k\right|^p\right)^{\frac{1}{p}} \leq K$.

This shows that $x \in \ell^p$.

Now we show that $x^i \to x$ as $i \to \infty$ i.e. $d\left(x^i, x\right) \to 0$ as $i \to \infty$.

Since $\{x^i\}$ is a Cauchy sequence, for given $\varepsilon > 0$ there exists an integer n_0 such that

$$d\left(x^i, x^j\right) < \varepsilon/2 \text{ for all } i, j \geq n_0 \qquad \text{..... (2)}$$

Therefore, for any t and for $i, j \geq n_0$ we get

$$\left(\sum_{k=1}^{t} \left|x_k^i - x_k^j\right|^p\right)^{\frac{1}{p}} \leq \left(\sum_{k=1}^{\infty} \left|x_k^i - x_k^j\right|^p\right)^{\frac{1}{p}} = d\left(x^i, x^j\right) < \frac{\varepsilon}{2}, \text{ [by (2)].}$$

Letting $j \to \infty$ we get

$$\left(\sum_{k=1}^{i}\left|x_k^i - x_k\right|^p\right)^{\frac{1}{p}} \le \frac{\varepsilon}{2} \text{ for } i \ge n_0$$

Since t is arbitrary we get as $t \to \infty$

$$\left(\sum_{k=1}^{\infty}\left|x_k^i - x_k\right|^p\right)^{\frac{1}{p}} \le \frac{\varepsilon}{2} < \varepsilon \text{ for all } i \ge n_0$$

i.e. $d(x^i, x) < \varepsilon$ for all $i \ge n_0$

i.e. $x^i \to x$ as $i \to \infty$

Hence the Cauchy sequence $\{x^i\}$ is convergent in ℓ^p i.e. ℓ^p is complete.

20.3.9. Show that $C[a, b]$ is complete metric space.

Solution. Let $\{f_n\}$ be any Cauchy sequence in $C[a, b]$

Then $d(f_m, f_n) \to 0$ as $m, n \to \infty$.

Now for each $x \in [a,b]$ we have

$$|f_m(x) - f_n(x)| \le \max_{a \le x \le b}|f_m(x) - f_n(x)| = d(f_m, f_n) \quad \ldots\ldots\ldots\ldots (1)$$

As $d(f_m, f_n) \to 0$ as $m,n \to \infty$ it follows that $|f_m(x) - f_n(x)| \to 0$ as $m, n \to \infty$ for each $x \in [a,b]$ i.e. for each $x \in [a,b]$ the sequence $\{f_n(x)\}$ is a Cauchy sequence of real numbers. Since the set of real numbers is complete $\{f_n(x)\}$ is convergent i.e. for each $x \in [a,b]$ there exists $f(x)$ such that $\lim_{n\to\infty} f_n(x) = f(x)$. .....(2)

We now show that $f(x) \in C[a,b]$ and $d(f_n, f)$ as $n \to \infty$.

Since $\{f_n\}$ is Cauchy, for given $\varepsilon > 0$ there exists n_0 such that

$$d(f_m, f_n) < \varepsilon/3 \text{ for all } m, n \ge n_0. \quad \ldots\ldots\ldots\ldots (3)$$

$\therefore$ For any $x \in [a,b]$ we have from (1) that

$$|f_m(x) - f_n(x)| < \varepsilon/3 \text{ for all } m, n \ge n_0 \quad \ldots\ldots\ldots\ldots (4)$$

Now $f_{n_0}(x)$ is continuous at $x_0 \in [a,b]$. Therefore, there exists $\delta > 0$ such that $|f_{n_0}(x) - f_{n_0}(x_0)| < \varepsilon/3$ whenever $x \in]x_0 - \delta, x_0 + \delta[\subset [a,b]$ $\ldots\ldots\ldots\ldots (5)$

For $x \in]x_0 - \delta, x_0 + \delta[\subset [a,b]$ we have

$$|f(x_0) - f(x)| = \lim_{n\to\infty} |f_n(x_0) - f_n(x)|, \text{ [by (2)]}$$

$$\leq \lim_{n\to\infty} \{|f_n(x_0) - f_{n_0}(x_0) + f_{n_0}(x_0) - f_{n_0}(x) + f_{n_0}(x) - f_n(x)|$$

$$\leq \lim_{n\to\infty} \{|f_n(x_0) - f_{n_0}(x_0)| + |f_{n_0}(x_0) - f_{n_0}(x)| + |f_{n_0}(x) - f_n(x)|\}$$

$$\leq \lim_{n\to\infty} \{\varepsilon/3 + \varepsilon/3 + \varepsilon/3\} \text{ [by (4), (5) and (4) respectively as } n \text{ is very large]}$$

$$= \varepsilon$$

Thus $|f(x) - f(x_0| < \varepsilon$ whenever $x \in]x_0 - \delta, x_0 + \delta[\subset [a,b]$.

This shows that $f(x)$ is continuous at $x_0 \in [a,b]$.

This is true for any $x_0 \in [a,b]$. Hence $f \in C[a,b]$.

Now we show that $f_n \to f$ as $n \to \infty$.

For $n \geq n_0$ and $x \in [a,b]$, we have

$$|f_n(x) - f(x)|$$

$$= |f_n(x) - \lim_{m\to\infty} f_m(x)| \quad \text{[by (2)]}$$

$$= \lim_{m\to\infty} |f_n(x) - f_m(x)|$$

$$\leq \lim_{m\to\infty} \{\max_{a\leq x\leq b} |f_n(x) - f_m(x)|\}$$

$$= \lim_{m\to\infty} d(f_n, f_m)$$

$$< \varepsilon/3 \quad \text{[by (3)]}$$

This is true for any $x \in [a,b]$

$$\therefore \max_{a\leq x\leq b} |f_n(x) - f(x)| \leq \varepsilon/3 < \varepsilon \text{ for all } n \geq n_0$$

or, $d(f_n, f) < \varepsilon$ for all $n \geq n_0$

Thus $f_n \to f$ as $n \to \infty$.

Hence the Cauchy sequence $\{f_n\}$ is convergent in $C[a, b]$ i.e. $C[a, b]$ is complete.

20.3.10. Cautor's Intersection Theorem.

If $\{F_n\}$ is a sequence of non-empty closed subsets of a metric space (X, d) such that $F_{n+1} \subset F_n$ for all positive integer n and $\delta(F_n) \to 0$ as $n \to \infty$, then X is complete if and only if $\bigcap_{n=1}^{\infty} F_n$ consists of exactly one point, where $\delta(F_n)$ is the diameter of F_n.

Proof. We first suppose that X is complete and $\{F_n\}$ is a sequence of non-empty closed subsets of X such that $F_1 \supset F_2 \supset F_3 \supset \ldots$ and $\delta(F_n) \to 0$ as $n \to \infty$.

We choose $x_n \in F_n$ for every $n = 1, 2, \ldots$. Thus we get a sequence $\{x_n\}$. We verify that $\{x_n\}$ is a Cauchy sequence.

Now $x_n \in F_n$ and for every positive integer p

$$x_{n+p} \in F_{n+p} \subset F_n.$$

So, $d(x_n, x_{n+p}) \leq \delta(F_n) \to 0$ as $n \to \infty$.

This shows that $\{x_n\}$ is a Cauchy sequence. Because the space X is complete, the sequence $\{x_n\}$ converges to a point $x \in X$. i.e. $\lim_{n\to\infty} x_n = x \in X$. ..... (1)

Let k be an arbitrary positive integer and consider the set F_k. Then $x_k, x_{k+1}, x_{k+2}, \ldots \in F_k$. Since F_k is closed F_k also contains the limit of this sequence. Now from (1) the limit of the sequence $\{x_{k+n}\}$ is x. Hence $x \in F_k$. Because k is arbitrary positive integer, $x \in F_k$ for each $k = 1, 2, \ldots$.

Therefore, $x \in \bigcap_{k=1}^{\infty} F_k$. This shows that the intersection is non-empty. We now prove the unicity of x. If possible let there be $x' (\neq x)$ such that $x' \in \bigcap_{k=1}^{\infty} F_k$

Then for each k, $x \in F_k$ and $x' \in F_k$.

So $d(x, x') \leq \delta(F_k) \to 0$ as $k \to \infty$.

This implies that $x = x'$ which is a contradiction since $x' \neq x$.

Conversely, we suppose that the conditions of the theorem are satisfied. We have to show that X is complete. Let $\{x_n\}$ be any Cauchy sequence in X. For given $\varepsilon > 0$, there exists a positive integer n_0 such that

$d(x_m, x_n) < \varepsilon$ for all $m, n \geq n_0$.

Let $H_n = \{x_n, x_{n+1}, ...\}$. Then $\delta(H_n) \leq \varepsilon$ for all $n \geq n_0$.

Also we have $\delta(\bar{H}_n) = \delta(H_n)$ where $\bar{H}_n$ is closure of H_n.

So, $\delta(\bar{H}_n) \leq \varepsilon$ for all $n \geq n_0$ i.e. $\delta(\bar{H}_n) \to 0$ as $n \to \infty$.

Also, clearly $H_{n+1} \subset H_n$ for each n and therefore $\bar{H}_{n+1} \subset \bar{H}_n$ for each n.

So $\{\bar{H}_n\}$ constitutes a closed, nested sequence of non-empty set in X whose diameters tend to zero. By hypothesis, there exists a unique $x \in X$ such that

$$x \in \bigcap_{n=1}^{\infty} \bar{H}_n.$$

Now, for each $n = 1, 2, ...$

$x_n \in H_n \subset \bar{H}_n$ and $x \in \bar{H}_n$.

So, $d(x, x_n) \leq \delta(\bar{H}_n) \to 0$ as $n \to \infty$.

Thus $\{x_n\}$ is convergent sequence in X. Hence X is complete.

20.3.11. Definition Nowhere Dense.

A set E of a metric space (X, d) is said to be nowhere dense in X if there exists for every sphere $S(x, r)$ another sphere $S(x_1, r_1)$ such that $S(x_1, r_1) \subset S(x, r)$ and $S(x_1, r_1)$ is free from any point of the set E.

In R, any set of a finite number of elements is nowhere dense in R. Also set of all integers is nowhere dense in R.

20.3.12. Definition. First Category, Second Category.

A set E of a metric space (X, d) is said to be of the first category if E is the union of a countable family of nowhere dense sets.

If E is not of the first category, then it is said to be of the second category.

The set of all rational numbers is of the first category in R.

The set of irrational numbers is of the second category in R.

The set of all real numbers is of the second category.

20.3.13. Baire's Category Theorem.

Every complete metric space is of second category.

Proof. Let (X, d) be a complete metric space. If possible, let X be of the first category. Then X can be represented as $X = \bigcup_{k=1}^{\infty} E_k$ where each E_k is nowhere dense in X.

Since E_1 is nowhere dense, there exists a sphere $S(x_1, r_1)$ that does not contain any point of E_1. Since E_2 is nowhere dense, there exists a sphere $S(x_2, r_2) \subset S(x_1, r_1/2)$ that does not contain any point of E_2. We choose r_1 and r_2 such that $r_2 < r_1/2$.

Similarly, because E_3 is nowhere dense, there exists a sphere $S(x_3, r_3) \subset S(x_2, r_2/2)$ that does not contain any point of E_3. Also we take $r_3 \leq r_2/2 \leq r_1/2^2$.

Proceeding in this way, we construct a sequence of spheres $S(x_n, r_n)$ such that

i) $S(x_n, r_n) \subset S(x_{n-1}, r_{n-1}/2)$

ii) $S(x_n, r_n) \cap E_n = \phi$

iii) $r_n \leq r_{n-1}/2$ for all $n = 2, 3, \ldots$

i.e. $r_n \leq r_{n-1}/2 \leq r_{n-2}/2^2 \leq \ldots \leq r_1/2^{n-1}$.

As the sphere $S(x_n, r_n/2)$ contains all the subsequent spheres, we have for any positive integer p,

$$d(x_{n+p}, x_n) < r_n/2 \qquad \ldots\ldots\ldots\ldots (1)$$

Now $r_n \leq r_1/2^{n-1}$. Therefore, $r_n \to 0$ as $n \to \infty$.

Hence from (1) we have $d(x_{n+p}, x_n) \to 0$ as $n \to \infty$ i.e. $\{x_n\}$ is a Cauchy sequence. Since X is complete, the sequence $\{x_n\}$ is convergent i.e. there exists $x \in X$ such $x_n \to x$ that as $n \to \infty$.

Letting $p \to \infty$ we get from (1)

$$d(x, x_n) < r_n/2 < r_n.$$

Therefore, $x \in S(x_n, r_n)$ for all $n = 1, 2, ...$

Now $S(x_n, r_n) \cap E_n = \phi$. Therefore x cannot belong to E_n for any $n = 1, 2, ...$

But $x \in X = \bigcup_{k=1}^{\infty} E_k$. So x must appear in at least one of the sets E_n. This is a contradiction. Hence the theorem is proved.

20.4. Completion of Metric Spaces

We know that the set Q of all rational numbers is not complete but the set R of all real numbes is complete and the closure of Q is R i.e. $\bar{Q} = R$. Thus the incomplete set Q can be enlarged to the complete set R and this completion R of Q is such that Q is dense in R. From this fact a natural question arises whether an arbitrary incomplete metric space can be completed in a similar fashion. The answer is in the affirmative.

20.4.1. Definition. Dense Set.

A subset M of a metric space (X, d) is said to be dense in X if closure of M is X i.e. if $\bar{M} = X$.

Hence if M is dense in X, then every open ball in X, no matter however small, will contain points of M. In other words there is no point $x \in X$ which has a neighbourhood that does not contain points of M.

The set Q of all rational numbers is dense in R.

20.4.2. Definition. Isometric Mapping and Isometric Spaces.

Let (X, d) and (X', d') be metric spaces. A mapping T of X into X' is said to be isometric mapping if T preserves distances i.e. if for all $x, y \in X$

$$d'(Tx, Ty) = d(x, y)$$

where Tx and Ty are the images of x and y respectively.

The space X is said to be isometric with the space X' if there exists a bijective isometry of X onto X'. The spaces X and X' are then called isometric spaces. Thus isometric spaces are indistinguishable from the viewpoint of metric, they may differ at most by the nature of their points.

20.4.3. Completion Theorem.

For an incomplete metric space (X, d) there exists a complete metric space (X', d') which has a subspace M that is isometric with X and is dense in X'. This space X' is unique except for isometries, i.e. if X'' is any complete metric space having a dense subspace M' isometric with X, then X' and X'' are isometric.

Proof. The theorem is proved in the following four steps

i) To construct (X', d')

ii) To form an isometry T of X onto M where $\bar{M} = X'$

iii) To prove completeness of X'

iv) To prove uniqueness of X', except for isometrices.

i) **Construction of (X', d')**

Let $\{x_n\}$ and $\{x_n'\}$ be Cauchy sequences in X. We call $\{x_n\}$ and $\{x_n'\}$ equivalent if $\lim_{n\to\infty} d(x_n, x_n') = 0$ and we write it as $\{x_n\} \sim \{x_n'\}$.

We divide the set of all Cauchy sequences into classes. All equivalent sequences are put into the same class. Let X' be the set of all such classes denoted by $\bar{x}, \bar{y}, \ldots$ etc.

We write $\{x_n\} \in \bar{x}$ to mean that $\{x_n\}$ is a member of the class $\bar{x}$.

Let $\{x_n\} \in \bar{x}$ and $\{y_n\} \in \bar{y}$. We show now that $\lim_{n\to\infty} d(x_n, y_n)$ exists.

We have $d(x_n, y_n) \le d(x_n, x_m) + d(x_m, y_m) + d(y_m, y_n)$

or, $d(x_n, y_n) - d(x_m, y_m) \le d(x_n, x_m) + d(y_m, y_n)$

Interchanging m and n we get,

$$d(x_m, x_n) - d(x_n, y_n) \le d(x_m, x_n) + d(y_n, y_m)$$

Thus $|d(x_n, y_n) - d(x_m, y_m)| \le d(x_m, x_n) + d(y_m, y_n)$ ..... (1)

Since $\{x_n\}$ and $\{y_n\}$ are Cauchy the *RHS* of (1) tends to zero as $m, n \to \infty$. So $|d(x_n, y_n) - d(x_m, y_m)| \to 0$ as $m, n \to \infty$.

i.e. $\{d(x_n, y_n)\}$ is a Cauchy sequence of real numbers.

As R is complete it follows that $\{d(x_n, y_n)\}$ is convergent in R i.e. $\lim_{n\to\infty} d(x_n, y_n)$ exists.

We now set $d'(\bar{x}, \bar{y}) = \lim_{n\to\infty} d(x_n, y_n)$ ..... (2)

Now we show that the limit in (2) is independent of the particular choice of representatives.

Let $\{x_n\} \sim \{x_n'\}$ and $\{y_n\} \sim \{y_n'\}$. In (1) replacing x_m by x_n' and y_m by y_n'

We have $|d(x_n, y_n) - d(x_n', y_n')| \le d(x_n, x_n') + d(y_n, y_n')$.

Now as $n \to \infty$ we have $d(x_n, x_n') \to 0$ and $d(y_n, y_n') \to 0$.

Therefore $|d(x_n, y_n) - d(x_n', y_n')| \to 0$ as $n \to \infty$

i.e. $\lim_{n\to\infty} d(x_n, y_n) = \lim_{n\to\infty} d(x_n', y_n')$

Using (2) we get $\lim_{n\to\infty} d(x_n', y_n') = d'(\bar{x}, \bar{y}) = \lim_{n\to\infty} d(x_n, y_n)$

i.e. $d'(\bar{x}, \bar{y})$ is independent of the particular choice of the members of the classes $\bar{x}$ and $\bar{y}$.

We now prove that $d'(\bar{x}, \bar{y})$ in (2) is a metric on X'.

Obviously $d'(\bar{x}, \bar{y}) \ge 0$.

Now $d'(\bar{x}, \bar{y}) = 0 \Leftrightarrow \lim_{n\to\infty} d(x_n, y_n) \Leftrightarrow \{x_n\} \sim \{y_n\} \Leftrightarrow \bar{x} = \bar{y}$

Also $d'(\bar{x}, \bar{y}) = \lim_{n\to\infty} d(x_n, y_n) = \lim_{n\to\infty} d(y_n, x_n) = d'(\bar{y}, \bar{x})$

We have $d(x_n, y_n) \le d(y_n, z_n) + d(z_n, y_n)$

Therefore $\lim_{n\to\infty} d(x_n, y_n) \le \lim_{n\to\infty} d(x_n, z_n) + \lim_{n\to\infty} d(z_n, y_n)$

or, $d'(\bar{x}, \bar{y}) \le d'(\bar{x}, \bar{z}) + d'(\bar{z}, \bar{y})$

Hence d' defined by (2) is a metric of X'.

(ii) Construction of an isometry.

For each $x \in X$ we consider the Cauchy constant sequence $\{x, x, x, ...\}$ and denote it by $\hat{x}$. Let M be the collection of all such classes i.e. $M = \{\hat{x} : x \in X\}$. Then $M \subset X'$ and there is a one-to-one correspondence between $x \in X$ and $\hat{x} \in M$. Since $\hat{x} = \{x, x, ...\}$ & $\hat{y} = \{y, y, ...\}$ we have from (2) $d'(\hat{x}, \hat{y}) = d(x, y)$

So the above correspondence $T : X \to M$ defined by $Tx = \hat{x}$ is an isometric mapping and X and M become isometric spaces. We now show that M is everywhere dense in X'. i.e. $\bar{M} = X'$.

Let us consider any $\bar{x} = \{x_n\}$ of X'.

Then $d(x_m, x_n) \to 0$ as $m, n \to \infty$. So for given $\varepsilon > 0$ there exists N such that

$d(x_n, x_N) < \varepsilon/2$ for all $n > N$

Now $\{x_N, x_N, ...\} = \hat{x}_N$ and $\hat{x}_N \in M$.

We have $d'(\hat{x}_N, \bar{x}) = \lim_{n\to\infty} d(x_N, x_n) \leq \varepsilon/2 < \varepsilon$.

This shows that every ε-neighbourhood of the arbitrary $\bar{x} \in X'$ contains an element of M. Hence M is dense in X'.

iii) Completeness of X'.

Let $\{\bar{x}_n\}$ be any Cauchy sequence in X'. Since M is dense in X', for every $\bar{x}_n$ there is a $\hat{z}_n \in M$ such that

$$d'(\bar{x}_n, \hat{z}_n) < \frac{1}{n} \qquad \text{..... (3)}$$

Hence by the triangle inequality

$$d'(\hat{z}_m, \hat{z}_n) \leq d'(\hat{z}_m, \bar{x}_m) + d'(\bar{x}_m, \bar{x}_n) + d'(\bar{x}_n, \hat{z}_n)$$

$$< \frac{1}{m} + d'(\bar{x}_m, \bar{x}_n) + \frac{1}{n}$$

Let $\varepsilon > 0$ be given

Since $\{\bar{x}_n\}$ is Cauchy for sufficiently large m, n we have $d'(\hat{z}_m, \hat{z}_n) < \varepsilon$. Hence $\{\hat{z}_n\}$ is Cauchy sequence.

Since $T : X \to M$ is isometric and $\hat{z}_n \in M$, the sequence $\{z_n\}$, where $z_n = T^{-1}\hat{z}_n$, is Cauchy sequence in X.

Let $\bar{x} \in X'$ be the class to which $\{z_n\}$ belongs. We show that $\bar{x}$ is the limit of $\{\bar{x}_n\}$.

By (3), we have

$$d'(\bar{x}_n, \bar{x}) \leq d'(\bar{x}_n, \hat{z}_n) + d'(\hat{z}_n, \bar{x})$$

$$< \frac{1}{n} + d'(\hat{z}_n, \bar{x}) \qquad \text{..... (4)}$$

Since $\{z_n\} \in \bar{x}$ and $\hat{z}_n \in M$, so that $\{z_n, z_n, ...\} = \hat{z}_n$ the inequality (4) becomes

$$d'(\bar{x}_n, x) < \frac{1}{n} + \lim_{m\to\infty} d(z_n, z_m) \qquad \text{..... (5)}$$

Since $\{z_n\}$ is a Cauchy sequence, the right hand side of (5) can be made smaller than any given $\varepsilon > 0$ for sufficiently large n. Hence the arbitrary Cauchy sequence $\{\bar{x}_n\}$ in X' has the limit $\bar{x} \in X'$. So X' is complete.

iv) Uniqueness of X' except for isometrics.

Let (X'', d'') be another complete metric space with a subspace M'' dense in X'' and isometric with X. We prove that X'' is isometric to X'.

For any $\bar{x}', \bar{y}' \in X''$ we have sequences $\{\bar{x}_n'\}, \{\bar{y}_n'\}$ in M'' such that $\bar{x}_n' \to \bar{x}'$ and $\bar{y}_n' \to \bar{y}'$ as $n \to \infty$.

We can show easily that

$$\left|d''(\bar{x}', \bar{y}') - d''(\bar{x}_n', \bar{y}_n')\right| \le d''(\bar{x}', \bar{x}_n') + d''(\bar{y}', \bar{y}_n').$$

The $RHS \to 0$ as $n \to \infty$. Therefore $d''(\bar{x}_n', \bar{y}_n') \to d''(\bar{x}', \bar{y}')$ as $n \to \infty$

or, $\lim_{n\to\infty} d''(\bar{x}_n', \bar{y}_n') = d''(\bar{x}', \bar{y}')$.

Since M'' is isometric with X and X is isometric with M, it follows that M'' is isometric with $M \subset X'$ and $\bar{M} = X'$, the distances on X'' and X' must be same. Hence X'' and X' are isometric. This proves the theorem.

20.5. Continuity and Compactness

20.5.1. Definition. Continuous function

Let (X_1, d_1) and (X_2, d_2) be metric spaces. A function $f : X_1 \to X_2$ is said to be continuous at the point $a \in X_1$ if for each $\varepsilon > 0$ there exists $\delta = \delta(\varepsilon, a) > 0$ such that $d_2(f(x), f(a)) < \varepsilon$ whenever $d_1(x, a) < \delta$

i.e. $f(x) \in B_\varepsilon(f(a))$ whenever $x \in B_\delta(a)$

i.e. $f(B_\delta(a)) \subset B_\varepsilon(f(a))$

The function f is said to be continuous on X_1 if it is continuous at each point of X_1.

The function f is said to be uniformly continuous if for every $\varepsilon > 0$ there exists $\delta = \delta(\varepsilon > 0)$ (dependent on ε only) such that

$d_2(f(x_1), f(x_2)) < \varepsilon$ whenever $d_1(x_1, x_2) < \delta$.

The following theorem is the characterisation of continuous function in terms of open sets.

20.5.2. Theorem. Let (X_1, d_1) and (X_2, d_2) be metric spaces. Then $f : X_1 \to X_2$ is continuous if and only if $f^{-1}(G)$ is open in X_1 whenever G is open in X_2.

Proof. Let f be continuous on X_1 and G be any open set in X_2.

We are to show that $f^{-1}(G)$ is open in X_1.

Let $x \in f^{-1}(G)$. Then $f(x) \in G$. Since G is open and $f(x) \in G$ there exists some $r>0$ such that $B_r(f(x)) \subset G$.

Now by the continuity of f, there exists an open sphere $B_\delta(x)$ such that $f(B_\delta(x)) \subset B_r(f(x))$.

Since $B_r(f(x)) \subset G$, it follows that

$$f(B_\delta(x)) \subset B_r(f(x)) \subset G$$

Therefore $B_\delta(x) \subset f^{-1}(G)$. Hence $f^{-1}(G)$ is open.

Conversely, let $f^{-1}(G)$ be open in X_1 whenever G be open in X_2.

Let us consider the open set $G = B_\epsilon(f(x))$ in X_2.

Then $f^{-1}(G)$ is open in X_1.

Now $G = B_\epsilon(f(x))$ implies that $f(x) \in G$ and so $x \in f^{-1}(G)$.

Since $f^{-1}(G)$ is open in X_1 and $x \in f^{-1}(G)$, there exists

$B_\delta(x) \subset f^{-1}(G)$ i.e. $f(B_\delta(x)) \subset G = B_\epsilon(f(x))$.

Hence f is continuous at x. This is true for any $x \in X_1$.

So f is continuous on X_1.

20.5.3. Definition. Sequentially Compact, Frechet Compact and Compact Metric Spaces

A metric space (X, d) is said to be sequentially compact if every sequence in X has a convergent subsequence converging to a point of X.

A metric space (X, d) is said to be Frechet compact if every infinite subset of X has a limit point in X.

A family A of subsets of X is said to cover X if the union of all members of A is X.

A cover of X is said to be an open cover if every member of the cover is an open set.

A subfamily of a cover which is also a cover is called a subcover.

A metric space (X, d) is said to be compact if each open cover of X has a finite subcover.

We now state the following theorem.

20.5.4. Theorem. Let (X, d) be a metric space. Then the following three compactness are equivalent

i) X is sequentially compact.

ii) X is Frechet compact.

iii) X is compact.

20.5.5. Theorem. Let (X, d_1) and (Y, d_2) be metric spaces and $f : X \to Y$ be a continuous mapping. Then $f(A)$ is compact in Y if A is compact in X.

Proof. Let $\{G_\lambda : \lambda \in I\}$ be an open cover of $f(A)$, where I is an index set. Then $\{f^{-1}(G_\lambda) : \lambda \in I\}$ is an open cover of A. Since A is compact there exist a finite subcover of this cover.

Let this finite subcover be $f^{-1}(G_1), f^{-1}(G_2), ..., f^{-1}(G_n)$.

i.e. $A = \bigcup_{i=1}^{n} f^{-1}(G_i)$.

Now $\bigcup_{i=1}^{n} f^{-1}(G_i) = f^{-1}\left(\bigcup_{i=1}^{n} G_i\right)$. Thus $A = f^{-1}\left(\bigcup_{i=1}^{n} G_i\right)$

From this we have $f(A) \subset \bigcup_{i=1}^{n} G_i$

i.e. $G_1, G_2, ..., G_n$ is a finite subcover of $f(A)$.

Hence $f(A)$ is compact in Y.

This completes the proof.

The following theorem says that continuous functions defined on a compact metric space are uniformly continuous.

20.5.6. Theorem. Let (X_1, d_1) and (X_2, d_2) be metric spaces. If $f : X_1 \to X_2$ be continuous and X_1 be compact then f is uniformly continuous.

Proof. Let $x \in X_1$ and f is continuous at x. Then for given $\varepsilon > 0$ there exists $\delta_x > 0$ such that

$d_2(f(x), f(y)) < \varepsilon/2$ whenever $d_1(x, y) < \delta_x$ ..... (1)

Let G_x be the set defined by

$$G_x = \left\{ y \in X_1 : d_1(x, y) < \frac{1}{2}\delta_x \right\}$$

Then $\{G_x : x \in X_1\}$ is an open cover of X_1. Since X_1 is compact, there exist finite number of points $x_1, x_2, ..., x_n$ in X_1 such that $X_1 \subset \bigcup_{k=1}^{n} G_{x_k}$. ..... (2)

Let $\delta = \frac{1}{2}\min\{\delta x_1, \delta x_2, ..., \delta_{x_n}\}$ ..... (3)

Then $\delta > 0$ and does not depend on x.

Now let $x, y \in X_1$ such that $d_1(x, y) < \delta$.

Since $x \in X_1$ from (2) it follows that $x \in G_{x_p}$ for at least one p = 1, 2, ..., n. This shows that $d_1(x, x_p) < \frac{1}{2}\delta_{x_p} < \delta_{x_p}$. Hence from (1) we get $d_2(f(x), f(x_p)) < \varepsilon/p$ ..... (4)

Now, $d_1(x_p, y) \le d_1(x_p, x) + d_1(x, y)$

$$< \frac{1}{2}\delta_{x_p} + \delta$$

$$\le \frac{1}{2}\delta_{x_p} + \frac{1}{2}\delta_{x_p}$$

$$= \delta_{x_p}$$

or, $d_1(x_p, y) < \delta_{x_p}$.

Therefore, by (1) we have $d_2(f(x_p), f(y)) < \varepsilon/2$. ..... (5)

Thus $d_2(f(x), f(y))$

$$\le d_2(f(x), f(x_p)) + d_2(f(x_p), f(y))$$

$< \varepsilon/2 + \varepsilon/2$, [by (4) and (5)]

i.e. $d_2(f(x), f(y)) < \varepsilon$ whenever $d_1(x, y) < \delta$

Hence f is uniformly continuous. This completes the proof.

The famous Heine-Borel theorem states that every closed and bounded subset of R^n is compact. In the following theorem it is shown that the converse of Heine-Borel Theorem is true in any metric space.

20.5.7. Theorem. Every compact subset of a metric space is closed and bounded

Proof. Let (X, d) be a metric space and A be any compact subset of X. To prove that A is closed we shall show that A^c is open.

Let z be any element of A^c. Then for each $x \in A$ we note that $x \neq z$. As every metric space is Hausdorff there exist disjoint open sets W_x and V_x such that $x \in W_x$ and $z \in V_x$.

Now $\{W_x \cap A : x \in A\}$ is an open cover of A. Since A is compact, there exists a finite set $\{x_1, x_2, ..., x_n\} \subset A$ such that $A \subset \bigcup_{i=1}^{n} W_{x_i}$.

Let $V_z = \bigcup_{i=1}^{n} V_{x_i}$. Then V_z is an open set containing z.

Now for all $i = 1, 2, ..., n$ we have $W_{x_i} \cap V_{x_i} = \phi$

Therefore $W_{x_i} \cap V_z = \phi$ for all $i = 1, 2, ..., n \left[\because V_z \subset V_{x_i}\right]$

Hence $\left(\bigcup_{i=1}^{n} W_{x_i}\right) \cap V_z = \phi$. So $A \cap V_z = \phi$. This implies that $V_z \subset A^c$.

Hence for any $z \in A^c$ there exists open set $V_z \subset A^c$. Thus A^c is an open set i.e. A is closed set.

To prove that A is bounded let us consider an element ξ of A.

Then $A \subset \bigcup_{n=1}^{\infty} B_n(\xi)$. Since A is compact, there exists an integer n_0 such that $A \subset B_{n_0}(\xi)$.

This proves that A is bounded. Hence the theorem.

The next theorem establishes the fact that every compact metric space is complete.

20.5.8. Theorem. A compact metric space is complete.

Proof. Let X be a compact metric space and let $\{x_n\}$ be any Cauchy sequence in X.

Then given $\varepsilon > 0$, there exists a positve integer n_0 such that $d(x_n, x_{n_0}) < \varepsilon$ for all $n \geq n_0$..... (1)

Because X is compact, there exists a subsequence $\{x_{n_k}\}$ converging to an element ξ (say) of X.

Thus $\lim_{k\to\infty} x_{n_k} = \xi$.

So there exists positive integer $n_{k_0} (> n_0)$ such that

$$d(x_{n_{k_0}}, \xi) < \varepsilon \qquad \text{..... (2)}$$

Since $n_{k_0} > n_0$ we have $d(x_{n_{k_0}}, x_{n_0}) < \varepsilon$ ..... (3)

From (1), (2) and (3) we have for $n > n_0$

$$d(x_n, \xi) \leq d(x_n, x_{n_0}) + d(x_{n_0}, x_{n_{k_0}}) + d(x_{n_{k_0}}, \xi)$$

$$< \varepsilon/3 + \varepsilon/3 + \varepsilon/3 = \varepsilon$$

Thus the Cauchy sequence $\{x_n\}$ is convergent. Hence X is complete.

20.6. Illustrative Examples

20.6.1. Example. Let $X =]0, 1[$ and $d(x, y) = |x - y|$ for all x, y in X. Show that (X, d) is an incomplete metric space.

Solution. Let $\{x_n\}$ be sequence in X defined by $x_n = \frac{1}{n}$ for all natural number n.

Now $d(x_m, x_n) = |x_m - x_n| = \left|\frac{1}{m} - \frac{1}{n}\right|$.

$\therefore d(x_m, x_n) \to 0$ as $m, n \to \infty$.

Thus $\{x_n\}$ is a Cauchy sequence in X.

We now show that $\{x_n\}$ cannot converge to any point $x \in X$.

Let x be an arbitrary point of X. Then by the Archimedean property of real number, there exists natural number n such that

$$n \le x < n+1$$

i.e. $\frac{1}{n+1} < x \le \frac{1}{n}$.

If $x = \frac{1}{n}$ then $\left]\frac{1}{n-1}, \frac{1}{n+1}\right[$ is an open set of X containing x which contains only one member of $\{x_n\}$.

If $x \neq \frac{1}{n}$ then $\left]\frac{1}{n+1}, \frac{1}{n}\right[$ is an open set of X containing x which does not contain any member of $\{x_n\}$.

Hence $\{x_n\}$ cannot converge to x. Since x is any point of X, it follows that $\{x_n\}$ cannot converge to any point of X. So (X, d) is incomplete metric space.

20.6.2. Example. Let X be the set of all rational numbers and let $d(x, y) = |x - y|$ for all x, y in X.

Then (X, d) is an incomplete metric space.

Solution. Let $\{x_n\}$ be sequence in X defined by

$$x_n = \left(1 + \frac{1}{n}\right)^n \text{ for all } n = 1, 2, 3, \ldots.$$

Then $\{x_n\}$ is a Cauchy sequence in X.

We know that in the space of real numbers $\lim_{n\to\infty} x_n = \lim_{n\to\infty}\left(1 + \frac{1}{n}\right) = e$. But e is an irrational number and so is not an element of X.

So the Cauchy sequence $\left\{\left(1 + \frac{1}{n}\right)^n\right\}$ of X does not converge to any element of X. Hence (X, d) is incomplete.

20.6.3. Example. Let X be the set of all polynomials $P(t)$ defnied on [0, 1] with real coefficients and with distance function as $d(P(t), Q(t)) = \sup_{0 \le t \le 1} |P(t) - q(t)|$.

Then (X, d) is an incomplete metric space.

Solution. Let us consider the sequence of polynomials $\{P_n(t)\}$

where $P_n(t)+1+t+\frac{t^2}{\lfloor 2}+....+\frac{t^n}{\lfloor n}$.

If $n>m$ then

$$d\left(P_n(t),P_m(t)\right)=\sup_{0\le t\le 1}\left|P_n(t)-P_m(t)\right|$$

$$=\sup_{0\le t\le 1}\left|\frac{t^{m+1}}{\lfloor m+1}+\frac{t^{m+2}}{\lfloor m+2}+....+\frac{t^n}{\lfloor n}\right|$$

$$\le\frac{1}{\lfloor m+1}+\frac{1}{\lfloor m+2}+....+\frac{1}{\lfloor n}.$$

For given $\varepsilon>0$, the right hand side expression can be made less than ε by choosing m sufficiently large. So $\{P_n(t)\}$ is a Cauchy sequence in X. But this sequence does not converge to any element of X. In fact in $C[0, 1]$ this Cauchy sequence $\{P_n(t)\}$ converges to the function $P(t)=e^t$ of $C[0, 1]$. As $e^t\notin X$ it follows that (X, d) is not complete.

20.6.4. The metric space (R, d) where $d(x,y)=|x-y|$ for any real x and y, is not compact.

Solution. Let us consider the sequence $\{x_n\}$ where $x_n=2n$ for all natural number n i.e. the sequence is {2, 4, 6, 8,...}

This sequence of R has no convergent subsequence.

Hence (R, d) is not compact.

20.6.5. The subset A of ℓ_2 consisting of all elements

$x=\{x_n\}$ such that $\left(\sum_{i=1}^{\infty}|x_i|^2\right)^{1/2}\le 1$ is not compact.

Solution. We choose the following sequence of points of A

$$x_1=\{1,0,0,0,...\},x_2=\{0,1,0,0,...\},x_3=\{0,0,1,0,...\},...$$

Then $d(x_i,x_j)=\sqrt{2}$ for any $i\neq j$.

So neither the sequence $\{x_n\}$ nor any of its subsequence can converge. Hence A is not compact.

20.7. Summary

Among all metric spaces complete metric spaces and compact metric spaces play very important role in functional analysis. These two metric spaces are defined and their properties are studied in this module. The theorems relating to these spaces are proved and examples are solved to have a clear knowledge about these two important spaces.

20.8. Self Assessment Question

1. Show that the set C of complex numbers with usual metric is a complete metric space.
2. Show that the set Z of integers with the usual metric is a complete metric space.
3. Prove that the metric space (ℓ_2, d) where ℓ_2 is the set of all real sequences $\{x_n\}$ with $\sum x_n^2$ convergent and metric d defined by

$$d(x_m, x_n) = \left[\sum_{i=1}^{n} \left(x_{m_i} - x_{n_i}\right)^2\right]^{1/2}$$ is a complete metric space.

4. Show that $]2, 5[$ with usual metric is an incomplete metric space.
5. Show that any closed subset of a complete metric space is complete.
6. Show that every Cauchy sequence in a metric space is bounded.
7. Sow that if a Cauchy sequence in a metric space has a convergent subsequence, then the whole sequence is convergent.
8. Prove that any function from a discrete metric space into a metric space is continuous.
9. Show that every compact metric space is separable.
10. Show that every sequentially compact metric space is compact.
11. Let $X = \left\{1, \frac{1}{2}, \frac{1}{3}, \ldots\right\}$ and d be the usual metric. Show that the set $\left\{1, \frac{1}{3}, \frac{1}{5}, \ldots\right\}$ is closed and bounded set in (X, d) but not compact.
12. Let X be the set of all continuous real valued functions defined on $[0, 1]$ and let

$$d(x, y) = \int_0^1 |x(t) - y(t)|\, dt \quad \text{for all } x, y \in X.$$

Show that (X, d) is not complete.

13. Show that the space C of all convergent sequences of real numbers with metric d defined by $d(\{x_n\},\{y_n\}) = \sup_n |x_n - y_n|$ is complete.

20.9. Suggested books for further reading

1. Functional Analysis with Applications : B. Choudhury and Sudarsan Nanda; Wiley Eastern Limited
2. Elements of Functional Analysis : B.K. Lahiri; World Press
3. Introductory Functional Analysis with Applications: Erwin Kreyszig; John Wiely & Sons
4. Mathematical Analysis : S.C. Malik, Savita Arora; Wiely Eastern Limited
5. Functional Analysis: J.N. Sharma, A.R. Vasishtha; Krishna Prakashan Mandir
6. Elements of Real Analysis : Shanti Narayan, M.D. Raisinghania; S. Chand

---- 0 ----

M.Sc. Course
in
Applied Mathematics with Oceanology
and
Computer Programming

PART-I

Paper-II Group-B

Module No. - 21

Functional Analysis

(Banach Fixed Point Theory)

Contents :

21.1. Introduction

Fixed points have long been used in analysis to solve various kinds of equations. The work of Cauchy on differential equations is fundamental one to the concept of existence theorem in mathematics. The Banach fixed point theorem is important as a source of existence and uniqueness theorems in different branches of analysis. This theorem provides an impressive illustration of the unifying power of functional analytic methods. It shows the usefulness of fixed point theorem in analysis. In fact, to establish the existence of solutions of different functional

equations, Banch fixed point theorem is marvellous one. The given functional equation is put in the form $Tx=x$ and thus the fixed point of the operator T becomes the required solution of $Tx=x$. To get this fixed point the method of successive approximation is used. It is seen that with any arbitrary point x_0 as the starting point the iterative sequence $\{T_{x_0}^n\}$ converges to the fixed point. So the method of successive approximations is used here not only for the prove of the existence of the fixed point but also for finding an approximate value of this fixed point. We thus can estimate the error which shows how many approximations we should take to get the required accuracy.

21.2. Objectives

Banach fixed point theorem needs a complete metric space X and a contraction mapping $T: X \to X$. The solution of the functional equation $Tx=x$ is found by finding the fixed point of this contraction operator T. With any arbitrary point x_0 of X as starting point the limit of the iterative sequence $\{T_{x_0}^n\}$ becomes the fixed point. Also this fixed point is found to be unique. Hence we can obtain the unique solution of the functional equation $Tx=x$. In contraction mapping the distance between images of any two distinct points is less than the distance the original points. As Banach fixed point theorem uses the contraction mapping it is also called contraction theorem. This theorem states sufficient conditions for the existence and uniqueness of a fixed point and this fixed point is obtained by iterative process. In this module we consider three important fields of applications of this famous theorem, namely, linear algebraic equations, ordinary differential equations and integral equations of both kinds Volterra and Fredholm. Examples are given to illustrate the theorem and the applications of the theorem.

21.3 Definition of fixed point and examples

21.3.1. Definition. Fixed Point

Let X be a set and T be a mapping from X to X. A fixed point of T is a point $\xi \in X$ such that $T\xi = \xi$ i.e a fixed point of T is a solution of the functional equation $Tx = x, x \in X$.

21.3.2. Examples of fixed points

i) The mapping $T: R \to R$ defined by $Tx=x^2$ has two fixed points $x=0$ and $x=1$ since $T0=0^2=0$ and $T1 = 1^2 = 1$.

ii) The mapping $T: R \to R$ defnined by $Tx = x^3$ has three fixed points $x = 0, x = 1$ and $x = -1$ as $T(0) = 0^3 = 0$ and $T(1) = 1^3 = 1$ and $T(-1) = (-1)^3 = 1$.

iii) The mapping $T: R \to R$ defined by $Tx = -x^3$ has only one fixed point $x = 0$ as $T0 = 0$.

iv) The mapping $T: C \to C$ defined by $Tx = -x^3$, where C is the set of all complex numbers, has three fixed points $x = 0, i$ and $-i$ as $T0 = 0, T(i) = i$ and $T(-i) = -i$.

v) The mapping $T: R \to R$ defined by $Tx = x + \sin x$ has infinitely many fixed points $x = n\pi, n = 0, \pm 1, \pm 2, \ldots$

vi) The mapping $T: R \to R$ defined by has $Tx = x^2 + 2x + 1$ has no fixed point, whereas the same function has two fixed point $T: C \to C$ (C is set of all complex numbers).

vii) A translation has no fixed point.

viii) A rotation of the plane has a single fixed point. The centre of rotation is the only fixed point here.

ix) Let $T: C[0,1] \to C[0,1]$ defined by

$T(f) = \alpha \int_0^x t f(t) dt, \alpha$ is a constant and $f \in C[0,1]$.

Then T has a unique fixed point.

x) Let $T: R^2 \to R^2$ defined by

$$T\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 4x_1 + 2x_2 - 5 \\ 4x_1 - 4x_2 + 1 \end{bmatrix}$$

has a unique fixed point $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$.

xi) The mapping $T: R \to R$ defined by $Tx = \frac{x}{2} + \frac{1}{x}$ has two fixed points $x = \sqrt{2}$ and $x = -\sqrt{2}$.

xii) The projection $T[(x_1, x_2)] = x_1$ of R^2 onto x_1-axis has infinitely many fixed points all lying on x_1-axis.

21.4. Banach Fixed Point Theorem

21.4.1. Definition. Contraction mapping.

Let (X, d) be a metric space. The mapping $T: X \to X$ is said to satisfy Lipschitz condition with constant α if $d(Tx, Ty) \leq \alpha d(x, y)$ holds for all $x, y \in X$.

If the above condition is satisfied when the Lipschitz constant α be such that $0 < \alpha < 1$ then the mapping T is called a contraction mapping.

21.4.2. Theorem. Any contraction mapping is uniformly continuous

Proof. Let (X, d) be a metric space and $T: X \to X$ be a contraction mapping. Then there is a constant $\alpha \in (0,1)$ such that $d(Tx, Ty) \leq \alpha\, d(x, y)$ for all $x, y \in X$.

Let ε be any given positive number and δ be such that $0 < \delta < \varepsilon/\alpha$.

Then for $d(x, y) < \delta$ we have

$$d(Tx, Ty) \leq \alpha\, d(x, y) < \alpha\delta < \varepsilon$$

So, $d(Tx, Ty) < \varepsilon$ whenever $d(x, y) < \delta$

Hence T is uniformly continuous.

Note. Since uniformly continuous mapping is always continuous, it follows from above theorem that every contraction mapping is continuous.

We now state and prove the famous Banach fixed point theorem. This theorem gives sufficient condition for the existence and uniqueness of a fixed point for a class of mapping, known as contraction mapping.

21.4.3. Banach Fixed Point Theorem (Contraction Theorem).

Every contraction mapping on a complete metric space has a unique fixed point.

Proof. Let (X, d) be a complete metric space and $T: X \to X$ be a contraction mapping. Then there is a constant α where $0 < \alpha < 1$ such that

$$d(Tx, Ty) \leq \alpha\, d(x, y) \quad \text{..... (1)}$$

for all $x, y \in X$.

Let x_0 be an arbitrary point in X. We define the "iterative sequence" $\{x_n\}$ by

$$x_1 = Tx_0$$

$$x_2 = Tx_1$$

$$x_3 = Tx_2$$
$$\vdots\ \vdots$$
$$x_n = Tx_{n-1}$$
$$\vdots\ \vdots$$

Then we have

$$x_1 = Tx_0$$
$$x_2 = T(Tx_0) = T^2x_0$$
$$x_3 = T(T^2x_0) = T^3x_0$$
$$\vdots\ \vdots$$
$$x_n = T(T^{n-1}x_0) = T^nx_0 \qquad \text{..... (2)}$$
$$\vdots\ \vdots$$

We now show that the sequence $\{x_n\}$ is Cauchy.

$$d(x_1, x_2) = d(Tx_0, Tx_1) \le \alpha\, d(x_0, x_1)$$
$$d(x_2, x_3) = d(Tx_1, Tx_2) \le \alpha\, d(x_1, x_2) \le \alpha^2 d(x_0, x_1)$$
$$d(x_3, x_4) = d(Tx_2, Tx_3) \le \alpha\, d(x_2, x_3) \le \alpha^3 d(x_0, x_1)$$
$$\vdots\ \vdots$$

Thus in general for any positive integer k we have

$$d(x_k, x_{k+1}) \le \alpha^k d(x_0, x_1) \qquad \text{..... (3)}$$

By the triangle inequality we have for $n > m$

$$\begin{aligned} d(x_m, x_n) &\le d(x_m, x_{m+1}) + d(x_{m+1}, x_{m+2}) + ... + d(x_{n-1}, x_n) \\ &\le \alpha^m d(x_0, x_1) + \alpha^{m+1} d(x_0, x_1) + ... + \alpha^{n-1} d(x_0, x_1) \text{ [by (3)]} \\ &\le \alpha^m d(x_0, x_1)\{1 + \alpha + ... + \alpha^{n-m-1}\} \\ &< \alpha^m d(x_0, x_1)\{1 + \alpha + ... + \alpha^{n-m-1} + \alpha^{n-m} + ...\} \end{aligned}$$

Thus $d(x_m, x_n) \le \dfrac{\alpha^m d(x_0, x_1)}{1-\alpha}$ ..... (4)

Since $0 < \alpha < 1$ we have $\alpha^m \to 0$ as $m \to \infty$. Also as $n > m$ we have $n \to \infty$ as $m \to \infty$. Thus from (4) it follows that $d(x_m, x_n) \to 0$ as $m, n \to \infty$. This means the iterative sequence $\{x_n\}$ is Cauchy.

Since X is complete, the sequence $\{x_n\}$ is convergent. So there exists $\xi \in X$ such that $x_n \to \xi$ as $n \to \infty$.

We now show that this limit ξ is a fixed point of T.

We have $d(\xi, T\xi) \le d(\xi, x_{n+1}) + d(x_{n+1}, T\xi)$

$$= d(\xi, x_{n+1}) + d(Tx_n, T\xi)$$

$$\le d(\xi, x_{n+1}) + \alpha d(x_n, \xi)$$

Since $x_n \to \xi$ as $n \to \infty$ we have as $n \to \infty$

$d(\xi, T\xi) \le 0$. But $d(\xi, T\xi) \not< 0$. Hence $d(\xi, T\xi) = 0$

or, $T_\xi = \xi$. i.e. ξ is a fixed point of T.

If possible, let $\eta (\neq \xi)$ be another fixed point of T i.e. $T\eta = \eta$.

Now $d(\xi, \eta) = d(T\xi, T\eta) \le \alpha d(\xi, \eta)$ ..... (5)

As $\eta \neq \xi$ we have $d(\xi, \eta) > 0$. Thus from (5) we have $1 \le \alpha$. This is a contradiction since $0 < \alpha < 1$.

Hence ξ is the only fixed point of T and the theorem is proved.

21.4.4 Estimation for the error of the *n*th approximation.

In the Banach fixed point theorem the iterative sequence $\{x_n\}$ with arbitrary $x_0 \in X$ converges to the unique fixed point $\xi \in X$. The prior estimate is

$$d(x_n, \xi) \le \frac{\alpha^n}{1-\alpha} d(x_0, x_1).$$

ans the posterior estimate is

$$d(x_n, \xi) \le \frac{\alpha}{1-\alpha} d(x_{n-1}, x_n).$$

Proof. We have for $n > m$

$$d(x_m, x_n) \le \frac{\alpha^m d(x_0, x_1)}{1-\alpha}$$

Thus for $m > n$ we have

$$d(x_n, x_m) \leq \frac{\alpha^n d(x_0, x_1)}{1-\alpha} \quad \text{..... (1)}$$

Since $x_m \to \xi$ as $m \to \infty$ we get from (1) letting $m \to \infty$

$$d(x_n, \xi) \leq \frac{\alpha^n d(x_0, x_1)}{1-\alpha} \quad \text{.....(2)}$$

This is the prior error bound and it can be used at the beginning of a calculation for estimating the number of steps necessary to obtain a given accuracy.

Taking $n = 1$ in (2) we get

$$d(x_1, \xi) \leq \frac{\alpha\, d(x_0, x_1)}{1-\alpha}$$

This is true for any $x_0 \in X$. Replacing x_0 by x_{n-1} we get

$$d(x_n, \xi) \leq \frac{\alpha\, d(x_{n-1}, x_n)}{1-\alpha}$$

This is the posterior estimate and it can be used at intermediate stages or at the end of calculation.

Note. Banach fixed point theorem gives a sufficient condition for the existence of unique fixed point. So an operater may have unique fixed point even if the condition of this theorem do not hold. The sufficient conditions are (*i*) the metric space X is complete and (*ii*) the mapping T is contraction. The following example shows that a contraction mapping T may have unique fixed point even if X is not complete.

21.4.5 Example.

Let $X = [0,1[$. Then X is not complete. Let $T : X \to X$ be defined as $Tx = \frac{x}{2}$. Here for any $x, y \in X$ we have $|Tx - Ty| = \left|\frac{x}{2} - \frac{y}{2}\right| = \frac{1}{2}|x - y|$. Thus T is a contraction mapping and T has the unique fixed point $x = 0$. But here X is not complete.

The following example shows that a mapping $T : X \to X$ may have unique fixed point when X is complete but T is not contraction.

21.4.6. Example.

Let $T : R \to R$ defined by

$$Tx = \frac{5x+3}{2},$$

Here R is complete. But T is not contraction as

$$|Tx - Ty| = \left|\frac{5x+3}{2} - \frac{5y+3}{2}\right| = \frac{5}{2}|x-y| \text{ for any } x, y \in R.$$

So the space is complete and the mapping is not contraction. But here $x = -1$ is the only fixed point of the mapping.

Finally, the next example shows that a mapping $T : X \to X$ may have unique fixed point even when X is not complete and T is not contraction.

21.4.7. Example.

Let Q be the set of all rational numbers and $T : Q \to Q$ be defined by

$$Tx = \frac{3x-4}{2}$$

Here for any $x, y \in Q$ we have

$$|Tx - Ty| = \left|\frac{3x-4}{2} - \frac{3y-4}{2}\right| = \frac{3}{2}|x-y|.$$

So T is not contraction. Also Q is not complete. But here $x = 4$ is the only fixed point of T.

21.5. Application of Banach Fixed Point Theorem.

21.5.1. Theorem. Solution of a System of Algebraic Linear Equations.

The system of linear equations

$$x_1 = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n + b_1$$
$$x_2 = a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n + b_2$$
$$\cdots \quad \cdots \quad \cdots$$
$$\cdots \quad \cdots \quad \cdots$$
$$x_n = a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n + b_n$$

in n unknows $x_1, x_2, ..., x_n$ has a unique solution if $\sum_{k=1}^{n} |a_{jk}| < 1$ for all $j = 1, 2, ..., n$.

Proof. The given system of linear equation can be written in matrix notation as

$$x = Ax + b \qquad \text{..... (1)}$$

where $x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$, $b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$ and $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$.

Let X be the set of all ordered n - tuples of real numbers:

$x = [x_1, x_2, ..., x_n]^T$, $y = [y_1, y_2, ..., y_n]^T$ etc.

On X we define a metric d by

$$d(x, y) = \max_i |x_i - y_i|$$

We know that this metric space (X, d) is complete.

On X we define $T : X \to X$ by

$$Tx = Ax + b \qquad \text{..... (2)}$$

The system of linear equation (1) thus becomes

$$x = Tx$$

Hence the solution of the given system of linear equations is nothing but the fixed point of the operator $T : X \to X$ defined by (2).

From (2) we see

$$Tx = T\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \sum_{k=1}^{n} a_{1k}x_k + b_1 \\ \sum_{k=1}^{n} a_{2k}x_k + b_2 \\ \cdots \\ \sum_{k=1}^{n} a_{nk}x_k + b_n \end{bmatrix}$$

$$\therefore d(Tx,Ty) = \max_j \left| \left(\sum_{k=1}^{n} a_{jk}x_k + b_j \right) - \left(\sum_{k=1}^{n} a_{jk}y_k + b_j \right) \right|$$

$$= \max_j \left| \sum_{k=1}^{n} a_{jk}(x_k - y_k) \right|$$

$$\leq \max_j \sum_{k=1}^{n} \left| a_{jk}(x_k - y_k) \right|$$

$$= \max_j \sum_{k=1}^{n} |a_{jk}||x_k - y_k|$$

$$= \max_j \sum_{k=1}^{n} |a_{jk}| \left(\max_i |x_i - y_i| \right)$$

$$= \left(\max_j \sum_{k=1}^{n} |a_{jk}| \right) d(x,y)$$

$$= \alpha\, d(x,y) \quad \text{where } \alpha = \max_j \sum_{k=1}^{n} |a_{jk}|$$

Thus for any $x, y \in X$

$d(Tx,Ty) \leq \alpha d(x,y)$ where $0 < \alpha < 1$.

So $T : X \to X$ is a contraction mapping and X is complete metric space. Hence by Banach fixed point theorem T has a unique fixed point $\xi = [\xi_1, \xi_2, ..., \xi_n]^T$ of X and this fixed point is the unique solution of the given system of algebraic simultaneous equation.

From Banach fixed point theorem we know that this fixed point is the limit of the iterative sequence $\{x^{(n)}\}$ where $x^{(n)} = Ax^{(n-1)} + b, n = 1, 2, 3, ...$ with any arbitrary point $x^{(0)}$ as starting point.

The prior error bound and posterior error bound are respectively

$$d\left(x^{(n)}, \xi\right) \leq \frac{\alpha^n}{1-\alpha} d\left(x^{(0)}, x^{(1)}\right)$$

and $$d\left(x^{(n)}, \xi\right) \leq \frac{\alpha}{1-\alpha} d\left(x^{(n-1)}, x^{(n)}\right)$$

We now show that the theorem of the existence and uniqueness of the solution of a differential equation can be obtained using Banach fixed point theorem.

21.5.2. Picard's Theorem.

Let $f(x,y)$ and $\frac{\partial f}{\partial y}$ be continuous in a closed rectangle $D=\{(x,y): a_1 \le x \le a_2, b_1 \le y \le b_2\}$ and (x_0,y_0) be and interior point of D. Then the differential equation

$$\frac{dy}{dx}=f(x,y)$$

has a unique solution $y=g(x)$ which passes through (x_0,y_0)

Proof. Here $f(x,y)$ and $\frac{\partial f}{\partial y}$ are continuous in the closed set D and so they are bounded. Hence there exist constants K and M such that

$$|f(x,y)| \le K \qquad \text{..... (1)}$$

$$\left|\frac{\partial f(x,y)}{\partial y}\right| \le M \qquad \text{..... (2)}$$

for all points (x,y) in D.

Let (x,y_1) and (x,y_2) be in D. It follows from the mean value theorem that

$$|f(x,y_1)-f(x,y_2)|=|y_1-y_2|\left|\frac{\partial f}{\partial y}(x,y_1+\theta(y_2-y_1))\right|$$

for some θ such that $0<\theta<1$. Thus using (2) we have the Lipschitz condition

$$|f(x,y_1)-f(x,y_2)| \le M|y_1-y_2| \qquad \text{..... (3)}$$

for all (x,y_1) and (x,y_2) in D.

The given problem of the differential equation is now converted to an equivalent problem relating to an integral equation as follows.

Let $y=g(x)$ be such that

$$\frac{dy}{dx}=f(x,y) \text{ where } y_0=g(x_0).$$

$$\therefore \frac{dg(x)}{dx}=f(x,g(x)) \qquad \text{..... (4)}$$

or, $dg(x)=f(x,g(x))dx$

Integrating from x_0 to x we have

$$g(x)-g(x_0)=\int_{x_0}^{x} f(t,g(t))\,dt$$

or, $$g(x)=g(x_0)+\int_{x_0}^{x} f(t,g(t))\,dt \qquad \text{..... (5)}$$

We note that differentiation of (5) gives (4) and integration of (4) gives (5). Hence, (4) and (5) are equivalent. So, solution of the integral equation (5) is the required solution of the given differential equation.

We now choose a positive number c such that $Mc<1$. Let us consider the closed subject F of D determined by $F=\{(x,y):|x-x_0|\le c \text{ and } |y-y_0|\le cK\}$.

Let G be the set of all continuous real functions $y=g(x)$ defined on $|x-x_0|\le c$ such that $|g(x)-y_0|\le cK$. Then G is a closed subspace of the complete metric space $C[x_0-c,x_0+c]$ and is therefore itself a complete metric space.

Let $h(x)=y_0+\int_{x_0}^{x} f(t,g(t))\,dt$

Then we have

$$\begin{aligned}|h(x)-y_0| &= \left|\int_{x_0}^{x} f(t,g(t))\,dt\right| \\ &\le \int_{x_0}^{x} |f(t,g(t))|\,dt \\ &\le \int_{x_0}^{x} K\,dt \\ &= K(x-x_0) \\ &= cK\end{aligned}$$

i.e. $|h(x)-y_0|\le cK \therefore h(x)\in G.$

Let $Tg=h$. Then T maps G into itself and is defined as

$$Tg=y_0+\int_{x_0}^{x} f(t,g(t))\,dt \qquad \text{..... (6)}$$

$\therefore$ (5) is nothing but $Tg=g$. So the solution of the given differential equation is the fixed point of T.

Now $|Tg_1 - Tg_2|$

$$= \left| y_0 + \int_{x_0}^{x} (t, g_1(t))dt - y_0 - \int_{x_0}^{x} f(t, g_2(t)dt) \right|$$

$$= \left| \int_{x_0}^{x} \{ f(t, g_1(t)) - f(t, g_2(t)) \} \right|$$

$$\leq \left| \int_{x_0}^{x} |f(t, g_1(t)) - f(t, g_2(t))| dt \right|$$

$$\leq \left| \int_{x_0}^{x} M |g_1(t) - g_2(t)| dt \right| \quad \text{[by (3)]}$$

$$\leq \left| \int_{x_0}^{x} M \left(\sup_{|t-x_0| \leq c} |g_1(t) - g_2(t)| \right) dt \right|$$

$$= d(g_1, g_2) M |(x - x_0)|$$

$$\leq cM\, d(g_1, g_2)$$

Thus $|Tg_1 - Tg_2| \leq cM\, d(g_1, g_2)$.

This is true for all x in $[x_0 - c, x_0 + c]$.

$$\therefore \sup_{|x-x_0| \leq c} |Tg_1 - Tg_2| \leq cM\, d(g_1, g_2)$$

or, $d(Tg_1, Tg_2) \leq cM\, d(g_1, g_2)$.

Since $0 < Mc < 1, T : G \to G$ defined by (6) is a contraction mapping. As G is complete applying Banach fixed point theorem T has a unique fixed point and this unique fixed point is the unique solution of the given differential equation. This completes the proof of the theorem.

Now we show that Banach fixed point theorem can establish the existence and uniqueness of the solution of integral equations.

21.5.3. Theorem.

The Fredholm integral equation

$$f(s) = x(s) - \mu \int_a^b k(s,t) x(t) dt$$

has unique solution if

i) $k(s,t)$ is continuous in both the variables s and t where $a \le s \le b$ and $a \le t \le b$

ii) $|k(s,t)| \le c$ for all $(s,t) \in [a,b] \times [a,b]$

iii) $|\mu| < \frac{1}{c(b-a)}$

iv) $x(t), f(t)$ are continuous in $[a, b]$

Proof.

The given integral equation is

$$f(s) = x(s) - \mu \int_a^b k(s,t)x(t)\,dt \quad \ldots\ldots (1)$$

or, $x(s) = f(s) + \mu \int_a^b k(s,t)x(t)\,dt$

or, $x(s) = Tx(s)$ $\ldots\ldots (2)$

where $Tx(s) = f(s) + \mu \int_a^b k(s,t)x(t)\,dt$ $\ldots\ldots (3)$

Thus the solution of the integral equation (1) is the fixed point of the operator $T : C[a,b] \to C[a,b]$ defined by (3).

Hence the existence and uniqueness of the fixed point of the operator T shows the existence and uniquess of the solution of the given integral equation (1).

Now $d(Tx,Ty) = \max\limits_{s\in[a,b]} |Tx(s) - Ty(s)|$

$$= \max_{s\in[a,b]} \left| f(s) + \mu \int_a^b k(s,t)x(t)\,dt - f(s) - \mu \int_a^b k(s,t)y(t)\,dt \right|$$

$$= |\mu| \max_{s\in[a,b]} \left| \int_a^b k(s,t)\{x(t) - y(t)\}\,dt \right|$$

$$\le |\mu| \max_{s\in[a,b]} \int_a^b |k(s,t)||x(t) - y(t)|\,dt$$

$$\le |\mu| \max_{s\in[a,b]} \int_a^b c \left\{ \max_{u\in[a,b]} |x(u) - y(u)| \right\} dt$$

$$= |\mu| \int_a^b c\, d(x,y)\,dt$$

$$= |\mu| c\, d(x,y)(b-a)$$

$\therefore d(Tx,Ty) \le \alpha\, d(x,y)$ where $\alpha = |\mu| c \cdot (b-a)$

Since $0 < |\mu| c(b-a) < 1$, T is a contraction mapping.

Applying the Banach fixed point theorem we conclude that T has a unique fixed point. Hence the given integral equation has unique solution.

21.5.4. Theorem. The Volterra integral euqation

$$f(s) = x(s) - \mu \int_a^s k(s,t)x(t)\,dt$$

has a unique solution if

i) $f(t), y(t)$ are continuous on $[a, b]$

ii) $k(s, t)$ is continuous on the triangular region $a \le t \le s, a \le s \le b$

Proof. The given Volterra integral equation is

$$f(s) = x(s) - \mu \int_a^s k(s,t)x(t)\,dt \qquad \ldots\ldots (1)$$

or, $$x(s) = f(s) + \mu \int_a^s k(s,t)x(t)\,dt$$

or, $$x(s) = Tx(s) \qquad \ldots\ldots (2)$$

where $$Tx(s) = f(s) + \mu \int_a^s k(s,t)x(t)\,dt \qquad \ldots\ldots (3)$$

From (1), (2) and (3) we see that the solution of the integral equation (1) is the fixed point of the operator $T : C[a,b] \to C[a,b]$ defined by (3).

So the given integral equation (1) has unique solution if the operator T has unique fixed point.

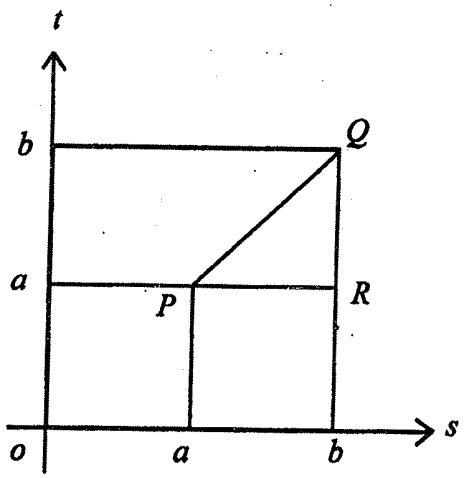
We now show that T has unique fixed point.

Let G be the triangular region PQR defined by

$$G = \{(s,t) : a \le s \le b,\ a \le t \le s\}$$

Since k is continuous on G and G is closed and bounded, it follows that for some positive constant c.

$$|k(s,t)| \le c \text{ for all } (s,t) \in G.$$



We take the metric d as

$$d(x,y)=\max_{a\le t\le b}|x(t)-y(t)|$$

We have $|Tx(s)-Ty(s)|$

$$=\left|f(s)+\mu\int_a^s k(s,t)x(t)dt-f(s)-\mu\int_a^s k(s,t)y(t)dt\right|$$

$$=|\mu|\left|\int_a^s k(s,t)\{x(t)-y(t)\}dt\right|$$

$$\le|\mu|\int_a^s|k(s,t)||x(t)-y(t)|dt$$

$$\le|\mu|\int_a^s c\left\{\max_{a\le u\le b}|x(u)-y(u)|\right\}dt$$

$$=|\mu|\int_a^s c\,d(x,y)dt$$

$$=c|\mu|d(x,y)\cdot(s-a)$$

i.e. $|Tx(s)-Ty(s)|\le c|\mu|(s-a)d(x,y)$ ..... (4)

Using mathematical induction we now show that for any positive integer n

$$|T^n x(s)-T^n y(s)|\le|\mu|^n c^n\cdot\frac{(s-a)^n}{\underline{n}}d(x,y)$$ .....(5)

From (4) we see that the result (5) holds for $n=1$.

Let the result (5) holds for $n = m$. Then

$$|T^m x(s) - T^m y(s)| \le |\mu|^m c^m \cdot \frac{(s-a)^m}{\lfloor m} d(x,y) \qquad \text{.....(6)}$$

Now $|T^{m+1}x(s) - T^{m+1}y(s)|$

$$= |T(T^m x(s)) - T(T^m y(s))|$$

$$= \left| f(s) + \mu \int_a^s k(s,t)(T^m x(t))dt - f(s) - \mu \int_a^s k(s,t)(T^m y(t))dt \right|, \text{ [by (3)]}$$

$$= |\mu| \left| \int_a^s k(s,t)\{T^m x(t) - T^m y(t)\}dt \right|$$

$$\le |\mu| \int_a^s |k(s,t)| |T^m x(t) - T^m y(t)| dt$$

$$\le |\mu| \int_a^s c.|\mu|^m c^m \frac{(t-a)^m}{\lfloor m} d(x,y)dt$$

$$= |\mu|^{m+1} .c^{m+1} .d(x,y). \frac{1}{\lfloor m} . \frac{(s-a)^{m+1}}{m+1}$$

$$\therefore |T^{m+1}x(s) - T^{m+1}y(s)| \le |\mu|^{m+1} .c^{m+1} . \frac{(s-a)^{m+1}}{\lfloor m+1} d(x,y)$$

Hence the relation (5) holds for $n = m + 1$ if it holds for $n = m$. But it holds for $n = 1$. So it holds for n=1+1=2. As it holds for n=2, it holds for n=2+1=3 and then for n=3+1=4 and so on. Thus the relation (5) holds for any positive integer n.

Since $s - a \le b - a$ it follows from (5) that for any positive integer n

$$|T^n x(s) - T^n y(s)| \le |\mu|^n c^n \cdot \frac{(b-a)^n}{\lfloor n} d(x,y)$$

This relation is true for all s and $[a, b]$ and the right hand side is independent of s, so we have

$$\max_{a \le s \le b} |T^n x(s) - T^n y(s)| \le |\mu|^n c^n \frac{(b-a)^n}{\lfloor n} d(x,y)$$

or, $$d(T^n x, T^n y) \le \alpha_n d(x,y) \qquad \text{.....(7)}$$

where $\alpha_n = |\mu|^n c^n . \frac{(b-a)^n}{\lfloor n}$ ..... (8)

As μ and c are fixed numbers, taking n sufficiently large we have from (8) that $0 < \alpha_n < 1$.

Also as $T : C[a,b] \to C[a,b]$ we have for any positive integer n that $T^n : C[a,b] \to C[a,b]$.

Thus for sufficiently large n, T^n is a contraction mapping from the complete metric space $C[a, b]$ to itself. Hence by Banach fixed point theorem T^n has a unique fixed point $\xi(t)$ in $C[a,b]$.

i.e. $T^n \xi = \xi$. ..... (9)

Now $T^n(T\xi) = T^{n+1}\xi = T(T^n\xi) = T\xi$ [by (9)]

i.e. $T\xi$ is also a fixed point of T^n. Since T^n has unique fixed point we have $T\xi = \xi$.

Now we show that ξ is the only fixed point of T.

If possible let $\eta (\neq \xi)$ be another fixed point of T.

Then $T\eta = \eta$. $\therefore T^2\eta = T(T\eta) = T\eta = \eta$

$T^3\eta = T(T^2\eta) = T\eta = \eta$ and so on.

Hence $T^n\eta = \eta$ i.e. $\eta (\neq \xi)$ is another fixed point of T^n.

This is a contradiction since T^n has unique fixed point.

Thus T has unique fixed point and this fixed point is the unique solution of the given integral equation (1).

Hence the proof of the theorem is complete.

21.6. Illustrative Examples.

21.6.1. Example. Let $T : R \to R$ defined by $Tx = 2\left(1 - \frac{x}{5}\right)$. Show that T is a contraction mapping and T has a unique fixed point.

Solution. For any $x \in R$ we have $2\left(1 - \frac{x}{5}\right) \in R$.

So $T : R \to R$. We know that R is a complete metric space with usual metric $d(x, y) = |x - y|$.

Now for any $x, y \in R$ we have $d(Tx,Ty) = |Tx - Ty| = \left|2\left(1-\frac{x}{5}\right) - 2\left(1-\frac{y}{5}\right)\right|$

$$= \frac{2}{5}|x-y| = \frac{2}{5}d(x,y)$$

i.e. $d(Tx,Ty) = \frac{2}{5}d(x,y) \ \forall \ x, y \in R$

Thus T is a contraction mapping. Using Banach fixed point theorem the unique fixed point is given by $x = \frac{10}{7}$.

21.6.2. Example. Let $T : R \to R$ be defined by $Tx = \frac{x}{2}$.

Using Banach fixed point theorem find the fixed point as a limit of the iterative sequence.

Solution. For any $x \in R$ we have $\frac{x}{2} \in R$. $\therefore T : R \to R$.

Again $|Tx - Ty| = \left|\frac{x}{2} - \frac{y}{2}\right| = \frac{1}{2}|x-y|$

$\therefore T$ is a contraction mapping. Since $T : R \to R$ and R is complete, we can apply the Banach fixed point theorem and obtain the fixed point as the limit of the iterative sequence with any point of R as the starting point.

The iterative sequence $\{x_n\}$ with any $x_0 \in R$ as starting point is given by

$$x_1 = Tx_0 = \frac{x_0}{2}$$

$$x_2 = Tx_1 = T\left(\frac{x_0}{2}\right) = \frac{x_0}{2^2}$$

$$x_3 = Tx_2 = T\left(\frac{x_0}{2^2}\right) = \frac{x_0}{2^3} \text{ and so on.}$$

$\therefore$ In general $x_n = \frac{x_0}{2^n}$ and

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} \frac{x_0}{2^n} = 0.$$

Hence $0 \in R$ is the unique fixed point of the operator T. We note that this limit remains same for any $x_0 \in R$.

21.6.3. Example. Give an example of the operator $T : X \to X$ for which $d(Tx, Ty) < d(x, y)$ for all $x, y \in X$ but T is not contraction.

Ans. Let $X = [0, 1[$ and $T : X \to X$ be defined by $Tx = \frac{x^2}{2}$.

Now for any $x, y \in X$ we have

$$d(Tx, Ty) = |Tx - Ty|$$

$$= \left|\frac{x^2}{2} - \frac{y^2}{2}\right|$$

$$= \left|\frac{1}{2}(x+y)(x-y)\right|$$

$$= \frac{1}{2}(x+y)|x-y|$$

$$= \frac{1}{2}(x+y)d(x, y)$$

Since $0 \le x \le 1$ and $0 \le y \le 1$ it follows that $0 \le \frac{x+y}{2} < 1$.

$\therefore d(Tx, Ty) < d(x, y)$. But here there exists no $\alpha, 0 < \alpha < 1$ such that $d(Tx, Ty) \le \alpha\, d(x, y)$. This is because here $\alpha < 1$ and we can always choose x and y such that $\alpha < \frac{x+y}{2} < 1$.

21.6.4. Example. If T is contraction mapping, show that for any positive integer n, T^n is a contraction mapping.

Solution. Let $T : X \to X$ be a contraction mapping.

Then for any $x, y \in X$ we have

$d(Tx, Ty) \le \alpha\, d(x, y)$ where $0 < \alpha < 1$.

Now $d(T^2x, T^2y) = d(T(Tx), T(Ty))$

$$\le \alpha\, d(Tx, Ty)$$

$$\le \alpha^2\, d(x, y)$$

Now $d\left(T^3x, T^3y\right) = d\left(T\left(T^2x\right), T\left(T^2y\right)\right)$

$$\leq \alpha\, d\left(T^2x, T^2y\right)$$

$$\leq \alpha \cdot \alpha^2\, d(x,y)$$

$$= \alpha^3 d(x,y)$$

i.e. $d\left(T_x^3, T_y^3\right) \leq \alpha^3 (x,y)$ and so on.

In general for any positive integer n we have

$$d\left(T_x^n, T_y^n\right) \leq \alpha^n d(x,y)$$

As $0 < \alpha < 1$ we have $0 < \alpha^n < 1$. Hence T^n is a contraction mapping.

21.6.5. Example. Using Banach fixed point theorem determine the solution of system of equations

$$x = \cdot 2x - \cdot 5y + 1 \cdot 3$$

$$y = \cdot 4x + \cdot 3y + \cdot 3$$

with the help of iterative sequence with $X_0 = \begin{bmatrix} 1 \cdot 3 \\ \cdot 3 \end{bmatrix}$ as starting point.

Solution. Here the given system may be written as

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \cdot 2 & -\cdot 5 \\ \cdot 4 & \cdot 3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 1 \cdot 3 \\ \cdot 3 \end{bmatrix}$$

or $X = AX + b$ where $X = \begin{bmatrix} x \\ y \end{bmatrix}, A = \begin{bmatrix} \cdot 2 & -\cdot 5 \\ \cdot 4 & \cdot 3 \end{bmatrix}$ and $b = \begin{bmatrix} 1 \cdot 3 \\ \cdot 3 \end{bmatrix}$.

In A we have $|\cdot 2| + |-\cdot 5| = \cdot 2 + \cdot 5 = \cdot 7 < 1$

and $|\cdot 4| + |\cdot 3| = \cdot 7 < 1$.

$\therefore$ The solution of the given system is the fixed point of the operator T defined by $TX = AX + b$. Also this fixed point is the lim it of the iterative sequence $\left\{T^n X_0\right\}$ with any X_0 as the starting point.

Here $X_0 = \begin{bmatrix} 1.3 \\ .3 \end{bmatrix}$

$$X_1 = AX_0 + b = \begin{bmatrix} .2 & -.5 \\ .4 & .3 \end{bmatrix}\begin{bmatrix} 1.3 \\ .3 \end{bmatrix} + \begin{bmatrix} 1.3 \\ .3 \end{bmatrix} = \begin{bmatrix} .26 - .15 + 1.3 \\ .52 + .09 + .3 \end{bmatrix} = \begin{bmatrix} 1.41 \\ .91 \end{bmatrix}$$

$$X_2 = AX_1 + b = \begin{bmatrix} .2 & -.5 \\ .4 & .3 \end{bmatrix}\begin{bmatrix} 1.41 \\ .91 \end{bmatrix} + \begin{bmatrix} 1.3 \\ .3 \end{bmatrix} = \begin{bmatrix} 1.127 \\ 1.137 \end{bmatrix}$$

$$X_3 = AX_2 + b = \begin{bmatrix} .2 & -.5 \\ .4 & .3 \end{bmatrix}\begin{bmatrix} 1.127 \\ 1.137 \end{bmatrix} + \begin{bmatrix} 1.3 \\ .3 \end{bmatrix} = \begin{bmatrix} .9569 \\ 1.0919 \end{bmatrix}$$

$$X_4 = AX_3 + b = \begin{bmatrix} .2 & -.5 \\ .4 & .3 \end{bmatrix}\begin{bmatrix} .9569 \\ 1.0919 \end{bmatrix} + \begin{bmatrix} 1.3 \\ .3 \end{bmatrix} = \begin{bmatrix} .94543 \\ 1.01033 \end{bmatrix}$$

$$X_5 = AX_4 + b = \begin{bmatrix} .2 & -.5 \\ .4 & .3 \end{bmatrix}\begin{bmatrix} .94543 \\ 1.01033 \end{bmatrix} + \begin{bmatrix} 1.3 \\ .3 \end{bmatrix} = \begin{bmatrix} .983921 \\ .981271 \end{bmatrix}$$

$$X_6 = AX_5 + b = \begin{bmatrix} .2 & -.5 \\ .4 & .3 \end{bmatrix}\begin{bmatrix} .983921 \\ .981271 \end{bmatrix} + \begin{bmatrix} 1.3 \\ .3 \end{bmatrix} = \begin{bmatrix} 1.0061487 \\ 0.9879497 \end{bmatrix}$$

and so on.

We see the sequence $\{X_n\}$ converges to $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$.

$\therefore$ The required solution is $x = 1, y = 1$.

21.7 Summary.

This module is devoted to the theorem of the remarkable Polish mathematician S. Banach. The application of this Banach fixed point theorem are given to solve system of linear algebraic equation, differential euqation and integral equation. Examples are given to explain and to understand the theorem and its applications.

21.8. Self Assessment Questions

1. Give an example of contraction mapping in an incomplete metric space without having any fixed point.
2. In the real line show that the mapping $Tx = \frac{3x+4}{5}$ has a unique fixed point.

3. Use Banach fixed point theorem to show that the system

$$x = \frac{1}{3}x - \frac{1}{4}y + \frac{1}{4}z - 1$$

$$y = -\frac{1}{2}x + \frac{1}{5}y + \frac{1}{4}z + 2$$

$$z = \frac{1}{5}x - \frac{1}{3}y + \frac{1}{4}z - 2$$

has a unique solution.

4. Give an example to show that the conditions in the Banach fixed point theorem are sufficient conditions for having fixed point.

5. Using Banach fixed point theorem solve the integral equation

$$e^s - \mu(e-1) = x(s) - \mu\int_0^1 x(t)dt, |\mu| < 1$$

6. Use Banach fixed point theorem to show that $x = 0, y = 1$ is the unique solution of the system

$$x = .5x + .4y - .4$$

$$y = .3x + .2y - .8$$

21.9. Suggested books for further readings

1. Introductory Functional Analysis with Applications: Erwin Kreyszig; John Wiley & Sons
2. Functional Analysis with Applications : B. Choudhary and Sudarsan Nanda; Wiley Eastern Limited
3. Elements of Functional Analysis : B.K. Lahiri; World Press
4. Introduction to Functional Analysis for Scientists and Technologists; B.Z. Vulikh; Pergamon Press
5. Elements of Real Analysis : Shanti Narayan and M.D. Raisinghania; S. Chand

---- 0 ----

M.Sc. Course
in
Applied Mathematics with Oceanology
and
Computer Programming

PART-I

Paper-II

Group-B

Module No. - 22

Functional Analysis

(Normal Linear Space and Banach Space)

Module Structure :

22. Normed Linear Space and Banach Space

22.1 Introduction

We are familiar with vectors and vector spaces in two and three dimensions. Two vectors can be added and a vector can be multiplied by a scalar. But in metric space two elements can not be added. In metric space only we have the notion of finding distance between any two elements of it. In a general set, if we have the definition of addition of two elements and multiplication of one element by a scalar obeying similar properties of ordinary vector addition and scalar multiplication then we get a general vector space or a linear space. As the elements of this linear

space behaves like usual vectors in two-three dimensions, they are termed also as vectors.

Also a vector has a length. Extending this notion of length of a vector to a linear space we get the normed linear space. Norm of an element in a linear space is similar to modulus of a vector in a vector space. A linear space equipped with norm is called a normed linear space. A complete normed linear space is called a Banach space. In fact a metric can be defined in a normed linear space with the help of the norm. In a normed linear space we can define linear operator. The theory of normed linear spaces, Banach spaces and the theory of linear operators defined on them play very important role in functional analysis.

21.2. Objectives

In many branches of mathematics vectors and vector spaces play an important role. In this module the vector space is generalized to linear space. The elements of this linear space may be usual three dimensional vectors or sequences of numbers or functions or matrices. These elements can be added and multiplied by scalars. Also the concept of the length of usual vector is introduced through norm defined on this linear space. The elements of linear space thus behaves like vectors in three dimension. The definition of linear space involves a set X and a field F involving two algebraic operations *viz* addition of two elements of X called vector addition and multiplication of one element of X by one element of F called scalar multiplication. This linear space equipped with norm is called as normed linear space and has a vital role in functional analysis.

22.3 Linear Space.

22.3.1. Definition of Linear Space

A linear space over a field F is a set X with mapping $x+y$ of $X \times X$ into X, called addition, and mapping λx of $F \times X$ into X, called scalar multiplication, such that the following axioms are satisfied for all x, y, z in X and λ, μ in F.

i) $(x+y)+z = x+(y+z)$

ii) $x+y = y+x$

iii) there exists an element $0 \in X$, called zero element such that $x+0 = x$

iv) for each $x \in X$, there exists an element $(-x) \in X$, called the additive inverse or the negative of x, such that $x+(-x) = 0$

v) $\lambda(x+y)=\lambda x+\lambda y$

vi) $(\lambda+\mu)x=\lambda x+\mu x$

vii) $\lambda(\mu x)=(\lambda\mu)x$ and

viii) $1x=x$ where 1 is the multiplicative identity of the field F.

The elements of X are called vectors and the elements of F are called the scalars. The linear space is also called vector space.

22.3.2 Examples of Linear Spaces

i) For any positive integer n

$$R^n=\{(x_1,x_2,...,x_n): x_1,x_2,...,x_n\in R\}$$

is a real vector space with respect to addition and scalar multiplication defined as follows:

$$x+y=(x_1,x_2,...,x_n)+(y_1,y_2,...,y_n)$$
$$=(x_1+y_1,x_2+y_2,...,x_n+y_n)$$

and $\lambda x=\lambda(x_1,x_2,...,x_n)=(\lambda x_1,\lambda x_2,...,\lambda x_n)$

where $\lambda\in R$. Here the field is $(R,+,\cdot)$

ii) For any positive integer n

$$C^n=\{(z_1,z_2,...,z_n): z_1,z_2,...,z_n\in C\}$$

is a complex vector space with respect to addition and scalar multiplication defined as follows

$$z+w=(z_1,z_2,...,z_n)+(w_1,w_2,...,w_n)$$
$$=(z_1+w_1,z_2+w_2,...,z_n+w_n)$$

and $\lambda z=\lambda(z_1,z_2,...,z_n)=(\lambda z_1,\lambda z_2,...,\lambda z_n)$

where $\lambda\in C$. Here the field is $(C,+,\cdot)$ where C is the set of all complex numbers.

iii) Let S denote the set of all sequences $\{x_n\}$ of real numbers. Then S is a real linear space under addition and scalar multiplication defined as

$$\{x_n\}+\{y_n\}=\{x_n+y_n\}$$

and $\lambda\{x_n\} = \{\lambda x_n\}$.

Here the field is $(R, +, \cdot)$.

iv) Let S' denote the set of all sequences $\{z_n\}$ of complex numbers. Then S' is a complex linear space under addition and scalar multiplication defined as

$$\{z_n\} + \{w_n\} = \{z_n + w_n\}$$

and $\lambda\{z_n\} = \{\lambda z_n\}$ where λ is any complex number. Here the associated field is $(C, +, \cdot)$ where C is the set of all complex numbers.

v) Let X be any non-empty set and let $F(X)$ denote the set of all real valued functions defined on X. The $F(X)$ is a real vector space with respect to addition and scalar multiplication defined as

$$(f_1 + f_2)(x) = f_1(x) + f_2(x)$$

and $(\lambda f)(x) = \lambda f(x)$ for all $x \in X, \lambda \in R$ and $f, f_1, f_2 \in F(X)$.

vi) Let $C(S)$ be the set of all continuous real functions defined on a compact Hausdorff space S. Then $C(S)$ is a real linear space with respect to addition and scalar multiplication defined as

$$(f_1 + f_2)(x) = f_1(x) + f_2(x)$$

and $(\lambda f)(x) = \lambda f(x)$ for all $x \in S, \lambda \in R$ and $f, f_1, f_2 \in C(S)$.

vi) Let A be the set of all complex functions f analytic on $\{z \in C : |z| < 1\}$ and continuous on $\{z \in C : |z| \le 1\}$. Then A is a complex vector space with respect to addition and scalar multiplication defined as

$$(f_1 + f_2)(z) = f_1(z) + f_2(z)$$

and $(\lambda f)(z) = \lambda f(z)$ for all $\lambda \in C$ and $f, f_1, f_2 \in A$.

viii) Let $C[a, b]$ be the set of all continuous functions defined on the closed interval $[a, b]$. Then $C[a, b]$ is a linear space with addition and scalar multiplication defined as

$$(f_1 + f_2)(x) = f_1(x) + f_2(x)$$

and $(\lambda f)(x) = \lambda f(x)$ for all $\lambda \in R$ and $f, f_1, f_2 \in C[a, b]$.

ix) For fixed real number $p \ge 1$ let ℓ^p be the set of all sequences $\{x_n\}$ such that $\sum_{n=1}^{\infty} |x_n|^p < \infty$. Then ℓ^p is a linear space with respect to addition and scalar multiplication defined as

$$\{x_n\}+\{y_n\}=\{x_n+y_n\}$$

and $\lambda\{x_n\}=\{\lambda x_n\}$.

x) Let P_n be the set of all polynomials of degree $\leq n$. Then P_n is a linear space with respect to addition and scalar multiplication defined as

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$

$$\lambda \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} (\lambda a_i) x^i.$$

xi) Let M be the set of all matrices of order $m \times n$. Then M is a linear space with addition and scalar multiplication as

$$\left[a_{ij}\right]_{m\times n} + \left[b_{ij}\right]_{m\times n} = \left[a_{ij} + b_{ij}\right]_{m\times n}$$

and $\lambda\left[a_{ij}\right]_{m\times n} = \left[\lambda a_{ij}\right]_{m\times n}$.

22.3.3. Definition : Subspace

Let X be a vector space over a field F. A subspace of X is a nonempty subset E of X such that $x+y$ and λx are in E whenever x and y are in E and $\lambda \in F$.

We note that the set $\{0\}$ consisting of just the zero vector is a vector subspace. Also the vector space X itself is a subspace of X. These two subspaces are called trivial subspaces.

22.3.4. Definition : Linear mapping.

Let X and Y be two vector spaces over a field F. A mapping $f : X \to Y$ is called a linear mapping (linear transformation) if

$$f(\lambda_1 x_1 + \lambda_2 x_2) = \lambda_1 f(x_1) + \lambda_2 f(x_2)$$

for all $x_1, x_2 \in X$ and $\lambda_1, \lambda_2 \in F$.

22.3.5. Examples of linear and non-linear mappings

i) The zero mapping $\theta : X \to Y$ defined by

$\theta x = 0$ for all $x \in X$ (right hand 0 is the zero vector of Y) is a linear mapping. It is also called trivial mapping.

This is because for any $\lambda_1, \lambda_2 \in F$ and $x_1, x_2 \in X$

$$\theta(\lambda_1 x_1 + \lambda_2 x_2) = 0 = \lambda_1 0 + \lambda_2 0 = \lambda_1 \theta(x_1) + \lambda_2 \theta(x_2).$$

ii) Let $I : X \to X$ be the identity mapping

$Ix = x.$

Then $I(\lambda_1 x_1 + \lambda_2 x_2) = \lambda_1 x_1 + \lambda_2 x_2 = \lambda_1 I(x_1) + \lambda_2 I(x_2).$

Thus I is a linear mapping.

iii) Let $T : R \to R$ be a mapping defined by

$T(x) = x + \lambda$ where $x \in R$ and λ is a real constant.

Then $T(\lambda_1 x_1 + \lambda_2 x_2) = \lambda_1 x_1 + \lambda_2 x_2 + \lambda$

and $\lambda_1 Tx_1 + \lambda_2 Tx_2 = \lambda_1 (x_1 + \lambda) + \lambda_2 (x_2 + \lambda) = \lambda_1 x_1 + \lambda_2 x_2 + (\lambda_1 + \lambda_2)\lambda.$

$\therefore T(\lambda_1 x_1 + \lambda_2 x_2) \neq \lambda_1 Tx_1 + \lambda_2 Tx_2.$

So T is not a linear mapping.

iv) Let $T : R \to R$ be defined by $Tx = \lambda$ where λ is a fixed real number.

Then $T(\lambda_1 x_1 + \lambda_2 x_2) = \lambda$ and $\lambda_1 Tx_1 + \lambda_2 Tx_2 = \lambda_1 \lambda + \lambda_2 \lambda.$

$\therefore T(\lambda_1 x_1 + \lambda_2 x_2) \neq \lambda_1 Tx_1 + \lambda_2 Tx_2.$

Thus T is not a linear mapping.

22.3.5. Defnition : Linear functional

Let X be a real vector space. A linear functional on X is a linear mapping $T : X \to R$ if for any $\lambda_1, \lambda_2 \in R$ and $x_1, x_2 \in X$ we have

$$T(\lambda_1 x_1 + \lambda_2 x_2) = \lambda_1 Tx_1 + \lambda_2 Tx_2.$$

Let X be a complex vector space. A linear functional on X is a linear mapping $T : X \to C$. This linear

functional is called complex linear functional. The linear functional $T : X \to R$ is called real linear functional.

Note : Any linear mapping $T : R \to R$ or $T : C \to C$ is linear functional.

22.4. Normed Linear Space

We have seen that linear space is an extension of the ordinary vector space. The elements of linear space behaves like vectors. One very important concept associated with vector is its length. In fact, an ordinary vector has length and direction i.e. every vector is associated with a length. This notion of length of a vector is introduced in general linear space through norm.

Thus normed linear space is a linear space associated with the notion of length of each of its element. The formal definition is given below.

22.4.1 Definition. Normed linear space

A norm on a real linear space X is a real function $\| \| : X \to R$ defined on X such that for any $x, y \in X$ and for all $\lambda \in R$ the following properties hold:

i) $\|x\| \geq 0$

ii) $\|x + y\| \leq \|x\| + \|y\|$

iii) $\|\lambda x\| = |\lambda| \, \|y\|$

iv) $\|x\| = 0$ implies $x = 0$.

22.4.2. Properties of norm.

i) $\|0\| = 0$.

Taking $\lambda = 0$ in $\|\lambda x\| = |\lambda| \, \|x\|$ we have

$\|0x\| = |0| \, \|x\|$

or, $\|0\| = 0$

ii) $\|y - x\| = \|x - y\|$

Taking $\lambda = -1$ in $\|\lambda x\| = |\lambda| \, \|x\|$ we get

$\|(-1)x\| = |-1|\,\|x\|$ or, $\|-x\| = \|x\|$

Hence $\|y-x\| = \|(-1)(x-y)\| = |-1|\|x-y\| = \|x-y\|$

iii) $\|\|x\| - \|y\|\| \le \|x-y\|$

We have $\|x\| = \|(x-y)+y\|$

$\le \|x-y\| + \|y\|$

or, $\|x\| - \|y\| \le \|x-y\|$ ..... (1)

Again $\|y\| = \|(y-x)+x\|$

$\le \|y-x\| + \|x\|$

$= \|x-y\| + \|x\|$

or, $\|y\| - \|x\| \le \|x-y\|$ ..... (2)

From (1) and (2) we have

$$\|\|x\| - \|y\|\| \le \|x-y\|$$

22.4.3. Examples of Normed Linear Spaces

i) The n-dimensional Euclidean space R^n of all ordered n-tuples of real numbers $x = (x_1, x_2, ..., x_n)$ is a *nls* with the norm defined by

$$\|x\| = \left(\sum_{j=1}^{n} |x_j|^2 \right)^{1/2}$$

ii) The space C^n of all ordered n-tuples of complex numbers $x = (x_1, x_2, ..., x_n)$ is a *nls* with the norm defined by

$$\|x\| = \left(\sum_{j=1}^{n} |x_j|^2 \right)^{1/2}$$

iii) For real $p \ge 1$ the space ℓ^p of all real sequence $x = \{x_j\}$ such that $\sum_{j=1}^{\infty} |x_j|^p$ is convergent is a *nls* with the norm

$$\|x\| = \left(\sum_{j=1}^{\infty} |x_j|^p \right)^{1/p}$$

iv) The space C of all convergent squences $x = \{x_j\}$ is a *nls* with norm

$$\|x\| = \sup_j |x_j|$$

v) The space C_0 of all null sequences $x = \{x_j\}$ is a *nls* with the norm

$$\|x\| = \sup_j |x_j|$$

vi) The space B of all bounded sequences is a *nls* with the norm

$$\|x\| = \sup_j |x_j|$$

vii) The space $C[a, b]$ of all continuous functions $x = x(t)$ defined on the closed interval $[a, b]$ is a *nls* with the norm

$$\|x\| = \max_{a \le t \le b} |x(t)|.$$

22.4.4. Theorem. Every *nls* is a metric space.

Proof. Let X be a *nls* and $d : X \times X \to R$ be a mapping defined by

$$d(x, y) = \|x - y\|$$

Then i) $d(x, y) \ge 0$.

ii) $d(x, y) = 0 \Rightarrow \|x - y\| = 0 \Rightarrow x - y = 0 \Rightarrow x = y$

and $x = y \Rightarrow x - y = 0 \Rightarrow \|x - y\| = 0 \Rightarrow d(x, y) = 0$

iii) $d(x, y) = \|x - y\| = \|y - x\| = d(y, x)$

iv) $d(x, y) = \|x - y\|$

$= \|(x - z) + (z - y)\|$

$\le \|x - z\| + \|z - y\|$

$= d(x, z) + d(z, y)$

Hence d is a metric and (X, d) is a metric space.

Note : For the *nls* X we have thus $\|x-y\| = d(x,y)$. Putting $y = 0$ we get $d(x,0) = \|x-0\| = \|x\|$. Thus $\|x\|$ is the distance of x from the zero element of the linear space.

The vector space $X(\neq \{0\})$ with the discrete metric d defined by

$$d(x,y) = \begin{cases} 0 \text{ if } x = y \\ 1 \text{ if } x \neq y \end{cases}$$

is a metric space but not a *nls*.

Thus the converse of Theorem 22.4.4 is not true.

22.4.5. Definition : Banach Space

A complete normed linear space is called a Banach space.

The following theorem is a characterisation of a Banach space in terms of series.

22.4.6. Theorem. A *nls* X is complete if and only if every absolutely convergent series in X is convergent.

Proof. Let X be complete *nls* and $\sum_{n=1}^{\infty} x_n$ be any absolutely convergent series. Thus $\sum_{n=1}^{\infty} \|x_n\|$ is convergent.

Let $y_k = \sum_{n=1}^{k} x_n$. $\therefore$ For any positive integer p we have

$$\|y_{k+p} - y_k\|$$

$$= \left\| \sum_{n=1}^{k+p} x_n - \sum_{n=1}^{k} x_n \right\|$$

$$= \left\| \sum_{n=k+1}^{k+p} x_n \right\|$$

$$\leq \sum_{n=k+1}^{k+p} \|x_n\|$$

As $\sum_{n=1}^{\infty} \|x_n\|$ is convergent $\sum_{n=k+1}^{k+p} \|x_n\| \to 0$ as $k \to \infty$.

So, $\|y_{k+p} - y_k\| \to 0$ as $k \to \infty$ i.e. $\{y_n\}$ is a Cauchy sequence in X. Since X is complete, there exists $x \in X$ such that

$$x = \lim_{k\to\infty} y_k = \lim_{k\to\infty} \sum_{n=1}^{k} x_n = \sum_{n=1}^{\infty} x_n$$

Hence the series $\sum_{n=1}^{\infty} x_n$ is convergent.

Conversely, let every absolutely convergent series in X be convergent. We are to prove that X is complete. Let $\{x_n\}$ be any Cauchy sequence in X. Then for each positive integer k, there is a positive integer N_k such that

$$\|x_n - x_m\| < \frac{1}{2^k} \text{ for all } n, m \geq N_k. \qquad \text{..... (1)}$$

We choose N_k such that for each $k \geq 1, N_{k+1} > N_k$.

Let $y_1 = x_{N_1}, y_2 = x_{N_2} - x_{N_1}, y_3 = x_{N_3} - x_{N_2}$ and so on.

Then $\|y_{k+1}\| = \|x_{N_{k+1}} - x_{N_k}\| < \frac{1}{2^k}$, [by (1)].

Now $\sum_{k=1}^{\infty} \frac{1}{2^k}$ is a convergent series.

So $\sum_{k=1}^{\infty} \|y_{k+1}\|$ is also a convergent series. Hence by assumption $\sum_{k=1}^{\infty} y_{k+1}$ is also convergent.

Therefore, there exists $y \in X$ such that

$$\sum_{k=1}^{\infty} y_{k+1} = y$$

So, $\lim_{m\to\infty} \sum_{k=1}^{m} y_{k+1} = y$

or, $\lim_{m\to\infty} \sum_{k=1}^{m} \left(x_{N_{k+1}} - x_{N_k}\right) = y$

or, $\lim_{m\to\infty} x_{N_{m+1}} = y$ ..... (2)

Now $\|x_m - y\| = \|x_m - x_{N_{m+1}} + x_{N_{m+1}} - y\|$

$$\leq \|x_m - x_{N_{m+1}}\| + \|x_{N_{m+1}} - y\|$$

Since $\{x_n\}$ is Cauchy sequence we have using (2)

$$\lim_{m\to\infty}\|x_m - y\| \le 0 \text{ i.e. } \lim_{m\to\infty}\|x_m - y\| = 0 \text{ i.e. } \lim_{m\to\infty} x_m = y \in X.$$

Thus the Cauchy sequence $\{x_n\}$ is convergent. Hence X is complete.

22.5. Illustrative Examples

22.5.1. Example. Show that R^n is a linear space with usual coordinate addition and scalar multiplication.

Solution. Let $x = (x_1, x_2, ..., x_n), y = (y_1, y_2, ..., y_n)$

and $z = (z_1, z_2, ..., z_n)$.

Here addition and scalar multiplication are defined as $x + y = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n)$

and $\lambda x = (\lambda x_1, \lambda x_2, ..., \lambda x_n)$ for any $\lambda \in R$.

Then we have

i) $(x+y)+z = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n) + (z_1, z_2, ..., z_n)$

$= ((x_1 + y_1) + z_1, (x_2 + y_2) + z_2, ..., (x_n + y_n) + z_n)$

$= (x_1 + (y_1 + z_1), x_2 + (y_2 + z_2), ..., x_n + (y_n + z_n))$

$= (x_1, x_2, ..., x_n) + (y_1 + z_1, y_2 + z_2, ..., y_n + z_n)$

$= x + (y + z)$

ii) $x + y = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n)$

$= (y_1 + x_1, y_2 + x_2, ..., y_n + x_n)$

$= y + x$

iii) $0 = (0, 0, ..., 0) \in X$

$x + 0 = (x_1 + 0, x_2 + 0, ..., x_n + 0) = (x_1, x_2 ..., x_n) = x.$

iv) $-x = (-x_1, -x_2, ..., -x_n) \in X$ and

$x + (-x) = (x_1 - x_1, x_2 - x_2, ..., x_n - x_n) = (0, 0, ..., 0) = 0.$

v) $\lambda(x + y)$

$= \lambda(x_1 + y_1, x_2 + y_2, ..., x_n + y_n)$

$$= (\lambda x_1 + \lambda y_1, \lambda x_2 + \lambda y_2, ..., \lambda x_n + \lambda y_n)$$
$$= (\lambda x_1, \lambda x_2, ..., \lambda x_n) + (\lambda y_1, \lambda y_2, ..., \lambda y_n)$$
$$= \lambda(x_1, x_2, ..., x_n) + \lambda(y_1, y_2, ..., y_n)$$
$$= \lambda x + \lambda y$$

vi) $(\lambda + \mu)x$

$$= (\lambda + \mu)(x_1, x_2, ..., x_n)$$
$$= ((\lambda + \mu)x_1, (\lambda + \mu)x_2, ..., (\lambda + \mu)x_n)$$
$$= (\lambda x_1 + \mu x_1, \lambda x_2 + \mu x_2, ..., \lambda x_n + \mu x_n)$$
$$= (\lambda x_1, \lambda x_2, ..., \lambda x_n) + (\mu x_1, \mu x_2, ..., \mu x_n)$$
$$= \lambda(x_1, x_2, ..., x_n) + \mu(x_1, x_2, ..., x_n)$$
$$= \lambda x + \mu x$$

vii) $\lambda(\mu x)$

$$= \lambda(\mu(x_1, x_2, ..., x_n))$$
$$= \lambda(\mu x_1, \mu x_2, ..., \mu x_n)$$
$$= (\lambda(\mu x_1), \lambda(\mu x_2), ..., \lambda(\mu x_n))$$
$$= ((\lambda\mu)x_1, (\lambda\mu)x_2, ..., (\lambda\mu)x_n)$$
$$= (\lambda\mu)(x_1, x_2, ..., x_n)$$
$$= (\lambda\mu)x$$

viii) Here the multiplicative identity of the field is 1 and

$$1x = 1(x_1, x_2, ..., x_n)$$
$$= (1x_1, 1x_2, ..., 1x_n)$$
$$= (x_1, x_2, ..., x_n)$$
$$= x$$

Thus R^n is a linear space.

22.5.2. Example. Show that the set of all $m \times n$ matrices is a linear space with matrix addition and scalar multiplication.

Solution. Let $A=[a_{ij}]_{m\times n}, B=[b_{ij}]_{m\times n}$ and $C=[c_{ij}]_{m\times n}$ and $\lambda, \mu \in R$.

The matrix addition and scalar multiplication are defined as

$A+B=[a_{ij}+b_{ij}]_{m\times n}$ and $\lambda A=[\lambda a_{ij}]_{m\times n}$

We have

i) $(A+B)+C=[a_{ij}+b_{ij}]+[c_{ij}]=[(a_{ij}+b_{ij})+c_{ij}]$

$=[a_{ij}+(b_{ij}+c_{ij})]=[a_{ij}]+[b_{ij}+c_{ij}]=A+(B+C)$

ii) $A+B=[a_{ij}+b_{ij}]=[b_{ij}+a_{ij}]=B+A$

iii) Let 0 be zero matrix of order $m \times n$. Then

$A+0=[a_{ij}+0]=[a_{ij}]=A$

iv) We know, $-A=[-a_{ij}] \therefore A+(-A)=[a_{ij}+(-a_{ij})]=0$

v) $\lambda(A+B)=\lambda[a_{ij}+b_{ij}]=[\lambda(a_{ij}+b_{ij})]=[\lambda a_{ij}+\lambda b_{ij}]$

$=[\lambda a_{ij}]+[\lambda b_{ij}]=\lambda[a_{ij}]+\lambda[b_{ij}]=\lambda A+\lambda B$

vi) $(\lambda+\mu)A=(\lambda+\mu)[a_{ij}]=[(\lambda+\mu)a_{ij}]=[\lambda a_{ij}+\mu a_{ij}]$

$=[\lambda a_{ij}]+[\mu a_{ij}]=\lambda[a_{ij}]+\mu[a_{ij}]=\lambda A+\mu A$

vii) $\lambda(\mu A)=\lambda\{(\mu)[a_{ij}]\}=\lambda\{[\mu a_{ij}]\}$

$=[\lambda(\mu a_{ij})]=[(\lambda\mu)a_{ij}]=(\lambda\mu)[a_{ij}]=(\lambda\mu)A$

ix) $1A=1[a_{ij}]=[1a_{ij}]=[a_{ij}]=A$

Thus the set of all $m \times n$ matrices is a linear space with respect to matrix addition and scalar multiplication.

22.5.3. Example. Show that the transformation $T: R^3 \to R^2$ defined by $T(x_1, x_2, x_3) = (x_1, x_2)$ for all $x_1, x_2, x_3 \in R$ is a linear transformation.

Solution : Let $x = (x_1, x_2, x_3)$ and $y = (y_1, y_2, y_3)$ be any elements of R^3 and $\lambda, \mu \in R$.

Now $T(\lambda x + \mu y)$

$$= T\left[\lambda(x_1, x_2, x_3) + \mu(y_1, y_2, y_3)\right]$$

$$= T\left[(\lambda x_1 + \mu y_1, \lambda x_2 + \mu y_2, \lambda x_3 + \mu y_3)\right]$$

$$= (\lambda x_1 + \mu y_1, \lambda x_2 + \mu y_2)$$

$$= (\lambda x_1, \lambda x_2) + (\mu y_1, \mu y_2)$$

$$= \lambda(x_1, x_2) + \mu(y_1, y_2)$$

$$= \lambda T(x_1, x_2, x_3) + \mu T(y_1, y_2, y_3)$$

$$= \lambda Tx + \mu Ty$$

22.5.3. Example. Show that the transformation $T: R^3 \to R^2$ defined by $T(x_1, x_2) = (0, x_2)$ is a linear transformation

Solution. Let $x = (x_1, x_2), y = (y_1, y_2)$ be elements of R^2 and $\lambda, \mu \in R$.

Now $T(\lambda x + \mu y)$

$$= T\left[\lambda(x_1, x_2) + \mu(y_1, y_2)\right]$$

$$= T\left[(\lambda x_1 + \mu y_1, \lambda x_2 + \mu y_2)\right]$$

$$= (0, \lambda x_2 + \mu y_2)$$

$$= (0, \lambda x_2) + (0, \mu y_2)$$

$$= \lambda(0, x_2) + \mu(0, y_2)$$

$$= \lambda T(x_1, x_2) + \mu T(y_1, y_2)$$

$$= \lambda Tx + \mu Ty.$$

22.5.4. Example Let X be the linear space of all bounded continuous real functions $f(x)$ defined on the closed interval $I=[a, b]$. Prove that the mapping $T: X \to R$ defined by

$$T(f)=\int_a^b f(x)dx \text{ is a linear functional.}$$

Solution. Here $T(f)=\int_a^b f(x)dx$.

Let $f, g \in X$ and $\lambda, \mu \in R$. Then

$$T(\lambda f+\mu g)=\int_a^b (\lambda f+\mu g)(x)dx$$

$$=\int_a^b [\lambda f(x)+\mu g(x)]dx$$

$$=\lambda\int_a^b f(x)dx+\mu\int_a^b g(x)dx$$

$$=\lambda Tf+\mu Tg$$

22.5.5. Example : Let R^n be n-dimensional real linear space and $T: R^n \to R$ be defined by

$T(x_1, x_2, ..., x_n)=b_1x_1+b_2x_2+...+b_nx_n$ for all $(x_1, x_2, ..., x_n) \in R^n$ where

$b_1, b_2, ..., b_n$ are fixed real members. Show that T is a linear functional.

Solution. $x=(x_1, x_2, ..., x_n), y=(y_1, y_2, y_n) \in R^n$ and $\lambda, \mu \in R$.

Then $T(\lambda x+\mu y)$

$$=T[\lambda(x_1, x_2, ..., x_n)+\mu(y_1, y_2, ..., y_n)]$$

$$=T[(\lambda x_1+\mu y_1, \lambda x_2+\mu y_2, ..., \lambda x_n+\mu y_n)]$$

$$=b_1(\lambda x_1+\mu y_1)+b_2(\lambda x_2+\mu y_2)+....+b_n(\lambda x_n+\mu y_n)$$

$$=\lambda(b_1x_1+b_2x_2+...+b_nx_n)+\mu(b_1y_1+b_2y_2+...+b_ny_n)$$

$$=\lambda Tx+\mu Ty.$$

Hence T is a linear functional.

22.5.6 Example. Prove that R^n is a *nls* with the norm

$$\|(x_1, x_2, ..., x_n)\|=\sum_{j=1}^{n}|x_j|$$

Solution. Let $x=(x_1,x_2,...,x_n), y=(y_1,y_2,...,y_n)$ be any member of R^n and λ be any real number.

i) Then $\|x\|=\|(x_1,x_2,...,x_n)\|=\sum_{j=1}^{n}|x_j|\geq 0$

ii) $\|x+y\|$

$=\|(x_1,x_2,...,x_n)+(y_1,y_2,...,y_n)\|$

$=\|(x_1+y_1,x_2+y_2,...,x_n+y_n)\|$

$=\sum_{j=1}^{n}|x_j+y_j|$

$\leq\sum_{j=1}^{n}(|x_j|+|y_j|)$

$=\sum_{j=1}^{n}|x_j|+\sum_{j=1}^{n}|y_j|$

$=\|x\|+\|y\|$

Thus $\|x+y\|\leq\|x\|+\|y\|$

iii) $\|\lambda x\|=\|\lambda(x_1,x_2,...,x_n)\|=\|(\lambda x_1,\lambda x_2,...,\lambda x_n)\|$

$=\sum_{j=1}^{n}|\lambda x_j|=|\lambda|\sum_{j=1}^{n}|x_j|=|\lambda|\|x\|$

iv) $\|x\|=0\Rightarrow\|(x_1,x_2,...,x_n)\|=0\Rightarrow\sum_{j=1}^{n}|x_j|=0\Rightarrow|x_j|=0$ for $j=1, 2, ..., n$

$\Rightarrow x_j=0$ for $j=1, 2, ...n$

$\Rightarrow(x_1,x_2,...,x_n)=(0,0,...,0)$

$\Rightarrow x=0$

Hence the result.

22.5.7 Example. Prove that $C[a,b]$ is a *nls* with the norm

$\|x(t)\|=\max_{a\leq t\leq b}|x(t)|$.

Solution. Let $x = x(t), y = y(t)$ and λ be any real number.

Then we have

i) $\|x\| = \|x(t)\| = \max_{a \le t \le b} |x(t)| \ge 0$

ii) $\|x+y\| = \|x(t)+y(t)\|$

$$= \max_{a \le t \le b} |x(t)+y(t)|$$

$$\le \max_{a \le t \le b} \{|x(t)|+|y(t)|\}$$

$$\le \left\{\max_{a \le t \le b} |x(t)|\right\} + \left\{\max_{a \le t \le b} |y(t)|\right\}$$

$$= \|x\| + \|y\|$$

Thus $\|x+y\| \le \|x\| + \|y\|$

iii) $\|\lambda x\| = \|\lambda x(t)\| = \max_{a \le t \le b} |\lambda x(t)| = \max_{a \le t \le b} |\lambda| |x(t)|$

$$= |\lambda| \max_{a \le t \le b} |x(t)| = |\lambda| \, \|x\|$$

iv) $\|x\| = 0 \Rightarrow \max_{a \le t \le b} |x(t)| = 0 \Rightarrow x(t) = 0 \forall t \in [a,b]$

$$\Rightarrow x = 0$$

Hence $\|x\| = \max_{a \le t \le b} |x(t)|$ is a norm of the linear space $C[a, b]$ i.e. $C[a, b]$ is a *nls*.

Note: In module 21 we have already shown that $C[a, b]$ is complete. Hence $C[a, b]$ is a complete *nls* i.e. a Banach space.

22.6. Summary. In this module a very important part of functional analysis *viz.* normed linear space has been defined. A complete normed linear space is called Banach space. Some theorems have been deduced and examples are given to illustrate them.

22.7. Self Assessment Questions

1. Show that the set of all real numbers is a real linear space.

2. Show that the set of all complex numbers is a complex linear space.
3. Show that for any positive integer n the set C^n of all n-tuples $(z_1, z_2, ..., z_n)$ is a complex linear space.
4. Show that the set S of all sequences $\{x_n\}$ of real numbers is a real linear space with the scalar multiplication and addition as

   $$\lambda\{x_n\} = \{\lambda x_n\} \text{ and } \{x_n\} + \{y_n\} = \{x_n + y_n\}$$
5. Show that the set P_n of all polynomials of degree $\leq n$ is a linear space.
6. Show that the set of all real valued functions of real variables is a linear space with the usual point wise addition and scalar multiplication.
7. Show that the mapping $T : R^3 \to R^2$ defined by

   $T(x_1, x_2) = (kx_1, kx_2)$ where k is a fixed constant is a linear mapping.
8. Show that the operator $T : R^2 \to R^2$ defined by

   $T(x_1, x_2) = (x_2, x_1)$ is a linear transform.
9. Show that the operator $T : R^2 \to R^2$ defined by

   $T(x_1, x_2) = (x_1, 0)$ is a linear operator.
10. Let P be the real linear space of the polynomials $p(x)$ with real coefficients defined on the closed interval [0,1]. Show that the mapping $T : P \to P$ defined by $T\,p(x) = \dfrac{dp(x)}{dx}$ is a linear mapping.
11. Show that R^n is a *nls* with

    $$\|(x_1, x_2, ..., x_n)\| = \left(\sum_{j=1}^{n} |x_j|^2\right)^{1/2} \text{ as norm.}$$
12. Show that R^n is a *nls* with

    $\|(x_1, x_2, ..., x_n)\| = \max_j |x_j|$ as norm.
13. Show that the set of all null sequences $\{x_n\}$ is a *nls* with norm as $\|\{x_n\}\| = \sup_n |x_n|$
14. Show that the set of all convergent sequences $\{x_n\}$ is a *nls* with the norm as $\|\{x_n\}\| = \sup_n |x_n|$.

22.8. Suggested Books for further reading :

1. Functional Analysis with Application: B Choudhary and Sudarsan Nanda; Wiley Eastern Limited
2. Elements of Functional Analysis: B.K. Lahiri; World Press
3. Introductory Functional Analysis with Applications: Erwin Kreyszig; John Wiley & Sons
4. Introduction to Functional Analysis for Scientists and Technologists: B.Z. Vulikh; Pergamon Press
5. Functional Analysis : J.N. Sharma & A.R. Vasishtha; Krishna Prakashan Mandir.

---- 0 ----

M.Sc. Course
in
Applied Mathematics with Oceanology
and
Computer Programming

PART-I

Paper-II Group-B

Module No. - 23

Functional Analysis

(Basic Theorems of Nomed Linear Space and Banach Space)

Module Structure :

23.1 Introduction

The four theorems viz Hahn-Banach theorem, Open mapping theorem, Closed graph theorem and Uniform boundedness theorem are considered as the cornerstone of functional analysis and so they are called as fundamental theorems of functional analysis. The Hahn-Banach theorem is an extension theorem for linear functional. This theorem is one of the most important theorem in connection with bounded linear operators. This theorem characterizes

the extent to which values of linear functional can be preassigned. This theorem was discovered by H. Hahn (1927) and was rediscovered in more general form by S. Banach (1929). In an extension problem a mathematical object defined on a subset M of a given set X is considered and the aim is to extend the object from M to the entire set X in such a way that certain basic properties of the object continue to hold for the extended object. In the Hahn-Banach theorem, the object to be extended is a linear functional defined on a subspace M of a linear space X and has a certain boundedness property formulated in terms of sublinear functional.

The second fundamental theorem is the open mapping theorem. In this theorem we need open mapping and complete normed linear space. The open mapping theorem exhibits the reason why completeness of *nls* are more satisfactory than incomplete *nls*. This theorem gives conditions under which a bounded linear operator is an open mapping. This theorem also gives conditions under which the inverse of a bounded linear operator is bounded.

The third fundamental theorem of functional analysis is the closed graph theorem. The closed linear operators have practical importance and so analysts have to use these operators frequently. Closed graph theorem is connected with closed linear operators defined with domain and range as Banach spaces. This theorem gives the sufficient conditions under which a closed linear operator on a Banach space is bounded.

The fourth and last fundamental theorem is the Uniform boundedness theorem or unifrom boundedness principle. This theorem was discovered by S. Banach and H. Steinhaus (1927) and is of great importance. In functional analysis there are many instances of results related to this theorem. This theorem also requires the completeness of normed linear space.

All these four fundamental theorems characterize some of the most important properties of Banach spaces which normed linear spaces may not have in general.

The open mapping theorem, the closed graphy theorem and uniform boundedness theorem are obtained from a common source viz. Baire's category theorem. Baire's category theorem has various other applications also in functional analysis. However in this module we only state this Baire's category theorem and use it to prove these important theorems.

23.2. Objectives

The objective of this module is to study the four fundamental theorems of functional analysis viz Hahn-Banach theorem, Open mapping theorem, Closed graphy theorem and Uniform boundedness theorem. Throughout analysis many instances are there related to these fundamental theorems. Applications of Hahn-Banach theorem are given here in details. Other theorems and related results are discussed.

22.3. Bounded Linear Transformation

22.3.1. Definition. Bounded linear transformation

Let X and Y be normed linear spaces and $T : X \to Y$ be a linear operator. The linear operator T is said to be bounded if there is a positive real number M such that

$$\|Tx\| \leq M \|x\| \quad \text{for all } x \in X.$$

We note that the norm $\|x\|$ is of the space X and the norm $\|Tx\|$ is of the space Y. For simplicity we denote both norms by the same symbol $\|\cdot\|$. Also we note that if $\|x\| \leq k$ then $\|Tx\| \leq Mk$. Thus a bounded linear operator maps a bounded set to a bounded set.

It is very important to remember that the definition of bounded function in real analysis is different from this definition. In real analysis the range of a bounded function is bounded but here image of any bounded set is bounded.

22.3.2. Definition. Norm of a bounded linear operator

Let $T : X \to Y$ be a bounded linear operator from *nls* X to *nls* Y. Then there exists $M>0$ such that

$$\|Tx\| \leq M \|x\| \text{ for all } x \in X.$$

For all $x \neq 0$ we thus have $\frac{\|Tx\|}{\|x\|} \leq M$. This shows that $\sup_{x \neq 0} \frac{\|Tx\|}{\|x\|}$ exists. Norm of T is defined as

$$\|T\| = \sup_{x \neq 0} \frac{\|Tx\|}{\|x\|}$$

(It is called norm of T as we shall soon prove that it satisfies all axioms of norm)

As $\|T\|$ is the supremum of all $\frac{\|Tx\|}{\|x\|}$, we have for all non zero $x \in X$, $\frac{\|Tx\|}{\|x\|} \leq \|T\|$ i.e. $\|Tx\| \leq \|T\| \|x\|$.

For $x = 0$ we have $Tx = T0 = 0 \therefore \|Tx\| = 0$. Also $\|x\| = \|0\| = 0. \therefore \|Tx\| = \|T\| \|x\|$ for $x = 0$.

Thus $\|Tx\| \leq \|T\| \|x\|$ for all $x \in X$.

Hence if $T : X \to Y$ is a bounded linear operator then we have

$$\|Tx\| \leq \|T\| \|x\| \text{ for all } x \in X.$$

An alternative definition of $\|T\|$ is given below.

Definition. Norm of a bounded linear operator $T : X \to Y$ may be defined as

$$\|T\| = \sup_{\|x\|=1} \|Tx\|.$$

This is because

$$\|T\| = \sup_{x \neq 0} \frac{\|Tx\|}{\|x\|} = \sup_{x \neq 0} \left\| \frac{1}{\|x\|} Tx \right\| = \sup_{x \neq 0} \left\| T\left(\frac{x}{\|x\|} \right) \right\| \text{ (as } T \text{ is linear)}$$

$$= \sup_{\|x'\|=1} \|Tx'\| \text{ where } x' = \frac{x}{\|x\|}$$

$$= \sup_{\|x\|=1} \|Tx\|$$

22.3.3 Examples of Linear Operators

1. Let X be a *nls*. The identity operator $I : X \to X$ defined by $Ix=x$ for all $x \in X$ is a bounded linear operator as $\|Ix\| = \|x\| = 1\|x\|$ for all $x \in X$.

2. Zero operator defined $\theta : X \to X$ by $\theta x = 0$ for all $x \in X$ is a bounded linear operator as

$$\|\theta x\| = \|0\| = 0 < 1\|x\| \text{ for all } x \in X.$$

3. Let X be a *nls* of all polynomials defined on [0, 1] with norm given by $\|x\| = \max_{0 \le t \le 1} |x(t)|$. Let T be the differentiation operator T defined on X by $Tx(t) = \frac{dx(t)}{dt}$. Then T is linear but not bounded. This is shown below.

Let $x_n(t) = t^n$ where n is positive integer.

Then $\|x_n\| = \max_{0 \le t \le 1} |x_n(t)| = \max_{0 \le t \le 1} |t^n| = 1$

and $Tx_n(t) = \frac{dx_n(t)}{dt} = \frac{dt^n}{dt} = nt^{n-1}$

$$\therefore \|Tx_n\| = \max_{0 \le t \le 1} |nt^{n-1}| = n$$

Thus $\sup_{\|x_n\|=1} \|Tx_n\| = \sup_n n$.

So $\sup_{\|x_n\|=1} \|Tx_n\|$ does not exist. Hence T is not bounded.

4. Let the integral operator

$T : C[0,1] \to C[0,1]$ be defined by

$Tx(t) = \int_0^1 k(t,s)x(s)ds$ where k (t, s) is a given continuous function on the closed square $[0,1]\times[0,1]$.

Then T is linear. We show that T is bounded.

Here $k(t,s)$ is continuous function on the closed square $[0,1]\times[0,1]$. So it is bounded i.e. there exists $M>0$ such that $|k(t,s)| \le M$ for all $(t,s) \in [0,1]\times[0,1]$.

Now $|x(t)| \le \max_{0\le t\le 1} |x(t)| = \|x\|$. ..... (1)

Hence $\|Tx\| = \max_{0\le t\le 1} \left| \int_0^1 k(t,s)x(s)ds \right|$

$\le \max_{0\le t\le 1} \int_0^1 |k(t,s)||x(s)|ds$

$\le \max_{0\le t\le 1} \int_0^1 M\|x\|ds$ [by (1)]

$= M\|x\|$

i.e. $\|Tx\| \le M\|x\|$ for all $x \in C[0,1]$.

Thus T is bounded.

We now only state the following important theorem which shows that in a finite dimensional *nls* boundedness of linear operator is always assured.

22.3.4. Theorem. If a normed linear space X is finite dimensional, then every linear operator on X is bounded.

We now prove the following theorem which asserts that for a linear transformation continuity and boundedness are equivalent. Also, we show that for a linear transformation continuity at one point assures the continuiity at every point.

22.3.5. Theorem. Let $T : X \to Y$ be a linear operator where X and Y are normed linear spaces. Then prove that

i) T is continuous if and only if T is bounded

ii) If T is continuous at a single point of X then it is continuous at every other points of X.

Proof.

i) Let $T : X \to Y$ be bounded linear operator and x_0 be any point of X. Then $\sup_{x \neq 0} \frac{\|Tx\|}{\|x\|}$ exists and is $\|T\|$.

Also we have

$$\|Tx\| \leq \|T\| \|x\| \text{ for all } x \in X.$$

For any given $\varepsilon > 0$ we take $\delta = \frac{\varepsilon}{\|T\|}$

Now, $\|Tx - Tx_0\|$

$= \|T(x - x_0)\|$ [as T is linear]

$\leq \|T\| \|x - x_0\|$ [as T is bounded].

Thus for $\|x - x_0\| < \delta$ we get $\|Tx - Tx_0\| \leq \|T\| \delta = \varepsilon$.

This shows that T is continuous at x_0. But x_0 is arbitrary.

Hence T is continuous over X.

Conversely, we assume that T is continuous over X.

Then T is continuous at any arbitrary point $x_0 \in X$.

$\therefore$ For given $\varepsilon > 0$ there is a $\delta > 0$ such that

$\|Tx - Tx_0\| < \varepsilon$ whenever $\|x - x_0\| < \delta$.

Let y be any point of X and we choose x as

$$x = x_0 + \frac{\delta y}{\|y\|}.$$

Then $\|x - x_0\| = \left\| \frac{\delta y}{y} \right\| = \delta \left(\frac{\|y\|}{\|y\|} \right) = \delta$

$$\therefore \|Tx - Tx_0\| < \varepsilon$$

or, $\|T(x - x_0)\| < \varepsilon$

or, $\left\| T\left(\frac{\delta y}{\|y\|} \right) \right\| < \varepsilon$

or, $\left\| \frac{\delta}{\|y\|} Ty \right\| < \varepsilon$

or, $\frac{\delta}{\|y\|} \|Ty\| < \varepsilon$

or, $\|Ty\| < \frac{\varepsilon}{\delta} \|y\|$

This is true for all $y \in X$. Hence T is bounded.

ii) Let T be continuous at the particular point ξ of X. Then from the proof of second part of (*i*) of follows that T is bounded over X. Hence from the first part of (*i*) we conclude that T is continuous over X.

However, a direct proof of (*ii*) is as follows.

Let T be continuous at the particular point ξ of X and x be any point of X. Let $\{x_n\}$ be any sequence converging to x i.e. $x_n \to x$ as $n \to \infty$.

Then $x_n - x + \xi \to \xi$ as $n \to \infty$.

Since T is continuous at ξ we have

$$T(x_n - x + \xi) \to T\xi \text{ as } n \to \infty$$

Now T is linear.

So $Tx_n - Tx + T\xi \to T\xi$ as $n \to \infty$

or, $Tx_n \to Tx$ as $n \to \infty$

i.e. T is continuous at x. Since x is any point of X, T is continuous on X.

22.3.6 Theorem. If X and Y are normed linear spaces, then $B(X, Y)$, the set of all bounded linear transformations from X into Y, is a normed linear space with pointwise linear operations.

Proof. Here $B(X, Y)$ is the set of the bounded linear transformations from X into Y. The vector addition and scalar multiplications are here given by

$$(T_1 + T_2)x = T_1x + T_2x$$

$$(\lambda T)x = \lambda(Tx)$$

Then we have

i) $\left[(T_1 + T_2) + T_3\right]x = (T_1 + T_2)x + T_3x = T_1x + T_2x + T_3x$

$$= T_1x + (T_2 + T_3)x = [T_1 + (T_2 + T_3)]x$$

$$\therefore (T_1 + T_2) + T_3 = T_1 + (T_2 + T_3)$$

ii) $(T_1 + T_2)x = T_1x + T_2x = T_2x + T_1x = (T_2 + T_1)x$

$\therefore T_1 + T_2 = T_2 + T_1$

iii) For the zero operator θ we have

$(T + \theta)x = Tx + \theta x = Tx + 0 = Tx$

$\therefore T + \theta = T$

iv) For T we have $(-T)$ such that

$[T + (-T)]x = Tx + (-T)x = Tx - Tx = 0 = \theta x$

$\therefore T + (-T) = \theta$

v) $[\lambda(T_1 + T_2)]x = \lambda[(T_1 + T_2)x] = \lambda(T_1x + T_2x)$

$= \lambda(T_1x) + \lambda(T_2x) = (\lambda T_1)x + (\lambda T_2)x$

$= (\lambda T_1 + \lambda T_2)x$

$\therefore \lambda(T_1 + T_2) = \lambda T_1 + \lambda T_2$

vi) $[(\lambda + \mu)T]x = (\lambda + \mu)(Tx) = \lambda(Tx) + \mu(Tx)$

$= (\lambda T)x + (\mu T)x = (\lambda T + \mu T)x$

$\therefore (\lambda + \mu)T = \lambda T + \mu T.$

vii) $[\lambda(\mu T)]x = \lambda[(\mu T)x] = \lambda[\mu(Tx)] = (\lambda\mu)Tx = [(\lambda\mu)T]x$

$\therefore \lambda(\mu T) = (\lambda\mu)T$

viii) For the scalar 1 we have

$(1T)x = 1(Tx) = Tx$

$\therefore 1T = T.$

Hence $B(X, Y)$ is a linear space.

We now show that for $T \in B(X, Y)$ $\sup_{\|x\|=1} \|Tx\|$

is the norm of T i.e. $\|T\| = \sup_{\|x\|=1} \|Tx\|$ ..... (1)

From (1) we have obviously $\|T\| \geq 0$.

For $T_1, T_2 \in B(X,Y)$ we have

$$\|T_1 + T_2\|$$

$$= \sup_{\|x\|=1} \|(T_1 + T_2)x\|$$

$$= \sup_{\|x\|=1} \|T_1 x + T_2 x\|$$

$$\leq \sup_{\|x\|=1} \{\|T_1 x\| + \|T_2 x\|\}$$

$$\leq \sup_{\|x\|=1} \|T_1 x\| + \sup_{\|x\|=1} \|T_2 x\|$$

$$= \|T_1\| + \|T_2\|$$

$$\therefore \|T_1 + T_2\| \leq \|T_1\| + \|T_2\|$$

Again for any scalar λ and $T \in B(X,Y)$ we have

$$\|\lambda T\|$$

$$= \sup_{\|x\|=1} \|(\lambda T)x\|$$

$$= \sup_{\|x\|=1} \|\lambda (Tx)\|$$

$$= \sup_{\|x\|=1} |\lambda| \, \|Tx\|$$

$$= |\lambda| \sup_{\|x\|=1} \|Tx\|$$

$$= |\lambda| \, \|T\|$$

Lastly, let $\|T\| = 0$. Then $\sup_{x \neq 0} \frac{\|Tx\|}{\|x\|} = 0$

This implies $\|Tx\| = 0$ for all $x \neq 0$

or, $Tx = 0$ for all $x \neq 0$

Now $To = 0 \therefore Tx = 0$ for all $x \in X$. So $T = \theta$.

Hence $B(X, Y)$ is a normed linear space.

22.3.7. Thoerem. If Y is a Banach space then so is $B(X, Y)$

Proof. Let Y be complete. We are to show that $B(X, Y)$ is complete.

Let $\{T_n\}$ be any Cauchy sequence in $B(X, Y)$.

Now for each $x \in B(X,Y)$ we have

$\|T_m x - T_n x\| = \|(T_m - T_n)x\| \le \|T_m - T_n\| \, \|x\| \to 0$ as $m, n \to \infty$.

$\therefore \{T_n x\}$ is a Cauchy sequence in Y for each $x \in X$.

Since Y is complete, there is $y \in Y$ such that $T_n x \to y \in Y$ as $n \to \infty$. Thus for each $x \in X$ there is $y \in Y$ such that $T_n x \to y$ as $n \to \infty$. This determines an operator $T : X \to Y$ such that $Tx = y$. So we have $T_n x \to Tx$ for each $x \in X$. .....(1)

Now, $T_n(\lambda_1 x_1 + \lambda_2 x_2) = \lambda_1 T_n x_1 + \lambda_2 T_n x_2$.

Taking limit as $n \to \infty$ we have

$$T(\lambda_1 x_1 + \lambda_2 x_2) = \lambda_1 T x_1 + \lambda_2 T x_2.$$

Hence T is linear. We now show that T is bounded.

We have $\|T_m\| - \|T_n\| \le \|T_m - T_n\| \to 0$ as $m, n \to \infty$

i.e. $\{\|T_n\|\}$ is a Cauchy sequence of real numbers.

As set of all real numbers is complete $\{\|T_n\|\}$ is convergent and so it is bounded. Let $\|T_n\| \le M$ for all n.

..... (2)

From (1) $Tx = \lim_{n\to\infty} T_n x$

$$\therefore \|Tx\| = \left\|\lim_{n\to\infty} T_n x\right\| = \lim_{n\to\infty} \|T_n x\| \quad [\because \|\cdot\| \text{ is continuous}]$$

$$\le \lim_{n\to\infty} \|T_n\| \, \|x\|$$

$$\le M \, \|x\| \text{ [by (2)]}$$

This is true for all $x \in X$. Hence T is bounded. Thus $T \in B(X,Y)$.

We now show that $\lim_{n\to\infty} T_n = T$.

For $\|x\| = 1$ we have

$$\|T_n x - T_m x\| = \|(T_n - T_m)x\| \leq \|T_n - T_m\| \, \|x\| = \|T_n - T_m\| \quad \text{..... (3)}$$

Since $\{T_n\}$ is Cauchy, for given $\varepsilon > 0$ there exist n_0 such that

$$\|T_n - T_m\| < \varepsilon \text{ for all } m, n \geq n_0$$

$\therefore$ For $m, n \geq n_0$ we have from (3)

$$\|T_n x - T_m x\| < \varepsilon \quad \text{..... (4)}$$

Keeping n fixed and letting $m \to \infty$ we get from (4) using (1)

$$\|T_n x - Tx\| < \varepsilon \text{ for all } n \geq n_0 \text{ and for all } \|x\| = 1 \quad \text{..... (5)}$$

Now $\|T_n - T\| = \sup_{\|x\|=1} \|(T_n - T)x\| = \sup_{\|x\|=1} \|T_n x - Tx\|$

Thus by (5) we have $\|T_n - T\| < \varepsilon$ for all $n \geq n_0$.

$\therefore \lim_{n \to \infty} T_n = T$ i.e. the Cauchy sequence $\{T_n\}$ is convergent in $B(X, Y)$. Hence $B(X, Y)$ is complete.

Remark : From above theorem it follows that $B(X)$, the set of all bounded linear operators from *nls* X into X is a *nls*. Also if X is a Banach space then $B(X)$ is also so. Since the set of real numbers is complete we have X^*, the set of all bounded linear functionals defined on a *nls* X, is a Banach space.

We note that X^* is always a Banach space even if X is not complete. The Banach space X^* is called the congujate or dual space of X.

22.4. Hahn-Banach Theorem

Hanh-Banach theorem is one of the most fundamental theorem in functional analysis. We have seen that X^* is a Banach space. But if X is a non zero normed linear space, an important and natural question arises whether there are any nonzero element in X^*. This question is answered by the Hahn-Banach theorem in the affirmative. So this theorem yields the existence of nontrivial continuous linear functional on a normed linear space. A large portion of functional analysis is developed with the help of this theorem. Also, it is an indispensable tool in the proofs of

many important theorems of functional analysis. There are several forms of this famous theorem. Here we state without proof the extended form.

22.4.1. Definition. Sublinear Functional

Let X be a real vector space. A real valued function p defined on X is called a sublinear functional if

$$p(x+y) \leq p(x)+p(y)$$

and $p(\lambda x) \leq \lambda p(x)$

for all $x, y \in X$ and all positive real number λ.

We now state the Hahn Banach theorem.

22.4.2. Hahn-Banach Theorem : Let X be a real linear space and let M be a linear subspace of X. Let p be a sublinear functional defined on X and f be a linear functional defined on M such that $f(x) \leq p(x)$ for every $x \in M$. Then there is a linear functional g defined on X such that $g(x) = f(x)$ for all $x \in M$ and $g(x) \leq p(x)$ for all $x \in X$.

There are many consequences of this Hahn-Banach theorem. Some of them are proved here.

22.4.3. Theorem. Let X be a real normed linear space and let M be a linear subspace of X. If $f \in M^*$ then there is a $g \in E^*$ such that $f(x) = g(x)$ for all $x \in M$ and $\|g\| = \|f\|$.

Proof. We define a functional p on X by

$$p(x) = \|f\| \, \|x\|$$

Then for $x, y \in X$ and any real number λ we have

$$\begin{aligned} p(x+y) &= \|f\| \, \|x+y\| \\ &\leq \|f\|(\|x\|+\|y\|) \text{ [by triangle inequality]} \\ &= \|f\| \, \|x\| + \|f\| \, \|y\| \\ &= p(x) + p(y) \end{aligned}$$

i.e. $p(x+y) \leq p(x)+p(y)$

and $p(\lambda x) = \|f\| \|\lambda x\|$

$= \|f\| |\lambda| \|x\|$

$= |\lambda| p(x)$

Thus p is a sublinear functional on X.

For any $x \in M$ we have

$f(x) \le |f(x)| \le \|f\| \|x\|$ [as f is linear bounded functional]

$= p(x)$

$\therefore f(x) \le p(x)$ for every $x \in M$.

Therefore, by Hahn-Banach theorem there exists a linear functional g defined on X such that

$g(x) = f(x)$ for all $x \in M$

and $g(x) \le p(x)$ for all $x \in X$.

From $g(x) \le p(x)$ we have

$g(x) \le \|f\| \|x\|$ for all $x \in X$.

$\therefore g(-x) \le \|f\| \|-x\|$

or, $-g(x) \le \|f\| \|x\|$ for all $x \in X$.

Thus $|g(x)| \le \|f\| \|x\|$ for all $x \in X$

This shows that g is bounded functional on X and $\|g\| \le \|f\|$ ..... (1)

Also $\|g\| = \sup\{|g(x)| : x \in X, \|x\| = 1\}$

$\ge \sup\{|g(x)| : x \in M, \|x\| = 1\}$

$= \sup\{|f(x)| : x \in M, \|x\| = 1\}$ [$\because f(x) = g(x)$ for all $x \in M$]

$= \|f\|$

i.e. $\|g\| \ge \|f\|$ ..... (2)

From (1) and (2) we have $\|g\| = \|f\|$.

This completes the proof of the theorem.

22.4.4. Theorem. Let X be a real normed linear space and M be linear subspace of X. If $z \in X$ and $dist(z, M) = d > 0$ then show that there exists $g \in X^*$ such that $g(M) = \{0\}, g(z) = d$ and $\|g\| = 1$.

Proof. Let $M_1 = \{x + \alpha z : x \in M, \alpha \in R\}$.

We now show that M_1 is a linear subspace of X.

Let $x_1 + \alpha_1 z, x_2 + \alpha_2 z \in M_1$.

Then $(x_1 + \alpha_1 z) + (x_2 + \alpha_2 z)$

$= (x_1 + x_2) + (\alpha_1 + \alpha_2) z \in M_1$

and $\lambda(x + \alpha z) = (\lambda x) + (\lambda\alpha) z \in M_1$

The zero element of X is $o + oz$ and so belongs to M_1

If $x + \alpha z \in M_1$ then $(-x) + (-\alpha) z \in M_1$ such that $(x + \alpha z) + \{(-x) + (-\alpha) z\}$

$= o + oz$

$= 0$

Lastly $1(x + \alpha z) = 1x + (1\alpha) z = x + \alpha z$.

Thus M_1 is a linear subspace of X.

We define the functional f on M_1 by

$$f(x + \alpha z) = \alpha d. \qquad \text{..... (1)}$$

Then $f[(x_1 + \alpha_1 z) + (x_2 + \alpha_2 z)]$

$= f[(x_1 + x_2) + (\alpha_1 + \alpha_2) z]$

$= (\alpha_1 + \alpha_2) d$ [by (1)]

$= \alpha_1 d + \alpha_2 d$

$= f(x_1 + \alpha_1 z) + f(x_2 + \alpha_2 z)$ [by(1)]

and $f[\lambda(x + \alpha z)]$

$= f[(\lambda x) + (\lambda\alpha) z]$

$= (\lambda\alpha) d$

$= \lambda(\alpha d)$

$= \lambda f(x + \alpha z)$

$\therefore$ f is a linear functional on M_1.

We now show that f is bounded linear functional on M_1.

For any $x+\alpha z \in M_1$ where $x+\alpha z \neq 0$ we have

$$\frac{|f(x+\alpha z)|}{\|x+\alpha z\|} = \frac{|\alpha d|}{\|x+\alpha z\|} = \frac{|\alpha| d}{\|x+\alpha z\|} = \frac{d}{\frac{1}{|\alpha|}\|x+\alpha z\|}$$

$$= \frac{d}{\left\|\frac{1}{\alpha}(x+\alpha z)\right\|} = \frac{d}{\left\|\frac{x}{\alpha}+z\right\|} = \frac{d}{\left\|z-\left(-\frac{x}{\alpha}\right)\right\|} \quad \text{..... (2)}$$

Now $x+\alpha z$ is any element of M_1, so x is any element of M and α is any scalar. Hence $-\frac{x}{\alpha}$ is any element of M

Since $dist(z, M) = d$, we have $\left\|z-\left(\frac{x}{\alpha}\right)\right\| \geq d$.

This gives $\frac{d}{\left\|z-\left(-\frac{x}{\alpha}\right)\right\|} \leq 1 \;\; \therefore \frac{|f(x+\alpha z)|}{\|x+\alpha z\|} \leq 1.$

So, $\sup\left\{\frac{f(x+\alpha z)}{\|x+\alpha z\|} : x+\alpha z \in M_1, x+\alpha z \neq 0\right\}$ exists.

Hence f is bounded linear functional on M_1 i.e. $f \in M^*$.

From (2) we have

$$\|f\| = \sup\left\{\frac{f(x+\alpha z)}{\|x+\alpha z\|} : x+\alpha z \in M_1, x+\alpha z \neq 0\right\}$$

$$= \sup\left\{\frac{d}{\left\|z-\left(-\frac{x}{\alpha}\right)\right\|} : -\frac{x}{\alpha} \in M\right\}$$

$$= \frac{d}{d}$$

$= 1$ i.e. $\|f\| = 1$ ..... (3)

For any $x \in M$ we have

$f(x)$

$= f(x + oz)$

$= od$

$= o \quad \therefore f(M) = \{O\}$ ..... (4)

Also $f(z)$

$= f(0+1z)$

$= 1d$

$= d$ i.e. $f(z) = d$ ..... (5)

Thus X is a real *nls*, M_1 is a linear subspace of X and $f \in M^*$. Hence there is a $g \in X^*$ such that

$f(x) = g(x)$ for all $x \in M_1$

and $\|f\| = \|g\|$. [follows from Theorem 22.4.3]

Now $M \subset M_1$. $\therefore g(M) = f(M) = \{0\}$ [by(4)]

Since $z \in M_1$ we have $g(z) = f(z) = d$ [by(5)]

Using (3) we have $\|g\| = \|f\| = 1$.

Hence the theorem.

We are now in a position to answer the famous question of existence of nonzero element in X^* when X is a nonzero normed linear space.

22.4.5. Theorem. If X is a nonzero normed linear space, then there exists a nonzero element in X^*.

Proof. Let X be a nonzero normed linear space.

Let z be a nonzero element of X.

Let M be the trivial subspace of X i.e . $M = \{0\}$.

Then $dist(z, M) = \|z - 0\| = \|z\| = d$ (say).

Now in the proof of Theorem 22.4.4 just taking M=$\{0\}$ we have the proof of this theorem.

22.4.6. Theorem. Let X be a normed linear space and z be a nonzero element of X. Then there exists a functional $g \in E^*$ such that $g(z) = \|z\|$ and $\|g\| = 1$.

Proof. Taking $M = \{0\}$, the trivial subspace of X, and following the proof of Theorem 22.4.4 we get the proof of this theorem.

23.5. Open Mapping Theorem

One of the four fundamental theorems of functional analysis is Open mapping theorem. It is connected with the mapping which maps open set to open set. As open sets play vital role in functional analysis this mapping and hence the Open mapping theorem has become fundamental theorem of functional analysis. In fact this theorem has many important applications. It states conditions under which a bounded linear operator is an open mapping. This theorem also gives conditions under which the inverse of a bounded linear operator is bounded.

23.5.1. Definition. Let X and Y be metric spaces. Then the mapping $T : X \to Y$ is called an open mapping if for every open set in X the image is an open set in Y i.e. if image of every open set is open.

Note : We should note that a continuous mapping $T : X \to Y$ has the property that for every open set in Y, the inverse image is an open set in X. A continuous mapping may or may not be open mapping e.g. $T : R \to R$ defined by $Tx = 2x + 1$ is continuous as well as open mapping. On the other hand $T : R \to R$ defined by $Tx = \sin x$ is continuous but not open mapping since $(0, 2\pi)$ is an open set but its image is not an open set, it is the closed set $[-1, 1]$.

We now state without proof the following Lemma which we need for the proof of the open mapping theorem.

23.5.3. Lemma. Open Unit Ball

A bounded linear operator T from a Banach space X onto a Banach space Y has the property that the image $T(B_0)$ of the open unit ball $B_0 = B(0,1) \subset X$ contains an open ball about $0 \in Y$.

23.5.4 Open Mapping Theorem

A bounded linear operator T from a Banach space X onto a Banach space Y is an open mapping. Hence if T is bijective then T^{-1} is continuous and bounded.

Proof. We are to prove that image of every open set is open. Let A be any open set of X. We have to show that $T(A)$ is an open set in Y.

Let $y = Tx \in T(A)$. Here A is open and $x \in A$. Therefore A contains an open ball with centre x.

Hence $A - x$ contains an open ball with centre 0.

Let the radius of this ball be r.

$\therefore A - x$ contains the open ball $B(0, r)$

Hence $\frac{1}{r}(A - x)$ contains the open unit ball $B(0; 1)$.

Then the Lemma 22.5.3. implies that $T\left[\frac{1}{r}(A - x)\right]$ contains an open ball about 0. Using linear property of T, it follows that $\frac{1}{r}T(A - x)$ contains an open ball about 0

$\Rightarrow T(A - x)$ contains an open ball about 0

$\Rightarrow T(A) - Tx$ contains an open ball about 0

$\Rightarrow T(A)$ contains an open ball about Tx.

Since Tx is arbitrary, $T(A)$ is open.

Hence T is an open mapping.

Finally, let T be bijective. Then $T^{-1} : Y \to X$ exists. Let $T^{-1} = S$. Then $S^{-1} = T$. We shall show that S is continuous.

Here $S : Y \to X$.

Let G be any open set in X. Then the inverse image of G by S is the set $S^{-1}(G)$ i.e. $T(G)$.

Since T is an open mapping and G is an open set, we have $T(G)$ is an open set i.e. $S^{-1}(G)$ is an open set.

Thus inverse image of any open set in X by S i.e. by T^{-1} is an open set in Y. Hence T^{-1} is continuous.

We now show that T^{-1} is linear.

Let y_1, y_2 be any elements of Y and $T^{-1}y_1 = x_1, T^{-1}y_2 = x_2$.

Then $Tx_1 = y_1$ and $Tx_2 = y_2$. Since T is linear for any scalars α, β we have

$$T(\alpha x_1 + \beta x_2) = \alpha Tx_1 + \beta Tx_2 = \alpha y_1 + \beta y_2$$

$$\Rightarrow T^{-1}(\alpha y_1 + \beta y_2) = \alpha x_1 + \beta x_2 = \alpha T^{-1} y_1 + \alpha T^{-1} y_2$$

Hence T^{-1} is linear.

We know that any linear continuous mapping is bounded. Here T^{-1} is linear and continous. So, T^{-1} is bounded.

23.6. Closed Graph Theorem

Closed graph theorem is connected with closed linear operator. This theorem states sufficient condition under which a closed linear operator on a Banach space is bounded.

We first define graph of an operator and then defined closed linear operator.

23.6.1. Definition. Graph of an Operator

Let X and Y be metric spaces. Then the graph of the operator $T : X \to Y$ is the subset $G(T)$ of $X \times Y$ defined by

$$G(T) = \{((x, y) : x \in X, y = Tx)\}.$$

23.6.2. Theorem. If X and Y are normed linear spaces, then $X \times Y$ is also a normed linear space with the two algebraic operations as

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

$$\lambda(x, y) = (\lambda x, \lambda y)$$

and the norm as

$$\|(x, y)\| = \|x\| + \|y\|.$$

Proof. Left as an exercise.

22.6.3. Definition. Closed Linear Operator

Let X and Y be normed linear spaces $T : X_1 \to Y$ be a linear operator with domain $X_1 \subset X$. Then T is called a closed linear operator if its graph

$$G(T) = \{(x, y) : x \in X_1, y = Tx\}$$

is closed in the normed linear space $X \times Y$.

23.6.4. Closed Graph Theorem.

Let X and Y be Banach spaces and $T : X_1 \to Y$ be a closed linear operator, where $X_1 \subset X$. Then if X_1 is closed in X, then the operator T is bounded.

Proof. Here X and Y are Banach spaces. We first show that XxY is also a Banach space. We know that XxY is a normed linear space with the algebraic operations and norm defined by

$$(x_1, y_1)+(x_2, y_2)=(x_1+x_2, y_1+y_2)$$

$$\lambda(x, y)=(\lambda x, \lambda y)$$

and $\|(x, y)\|=\|x\|+\|y\|$.

Let $\{(x_n, y_n)\}$ be any Cauchy sequence in XxY.

Then for given $\varepsilon > 0$ there is positive integer n_0 such that

$$\|(x_m, y_m)-(x_n, y_n)\| < \varepsilon \text{ for all } m, n \geq n_0.$$

$$\|(x_m - x_n, y_m - y_n)\| < \varepsilon \text{ for all } m, n \geq n_0$$

$$\Rightarrow \|x_m - x_n\| + \|y_m - y_n\| < \varepsilon \text{ for all } m, n \geq n_0$$

$$\Rightarrow \|x_m - x_n\| < \varepsilon \text{ and } \|y_m - y_n\| < \varepsilon \text{ for all } m, n \geq n_0$$

$\Rightarrow \{x_n\}$ and $\{y_n\}$ are Cauchy sequences in X and Y respectively.

Now X and Y are complete. Hence there are $x \in X$ and $y \in y$ such that $x_n \to x$ and $y_n \to y$ as $n \to \infty$.

Since $x \in X$ and $y \in Y$ we have $(x, y) \in X \times Y$

Now $\|(x_n, y_n)-(x, y)\| = \|x_n - x\| + \|x_n - y\| \to 0$ as $n \to \infty$

$\therefore (x_n, y_n) \to (x, y)$ as $n \to \infty$. i.e. the Cauchy sequence $\{(x_n, y_n)\}$ is convergent in XxY. Hence XxY is complete *nls*. i.e. a Banach space.

Now $T : X_1 \to Y$ is a closed linear operator. So the graph $G(T)$ is closed in XxY. Also X_1 is closed in X.

Hence both $G(T)$ and X_1 are complete.

We now consider the mapping

$$P : G(T) \to X_1 \text{ by}$$

$$P(x, Tx) = x.$$

We show now that P is linear. We have for any scalars λ_1, λ_2

$$P\{\lambda_1(x_1,Tx_1)+\lambda_2(x_2,Tx_2)\}$$
$$=P\{(\lambda_1x_1,\lambda_1Tx_1)+(\lambda_2x_2,\lambda_2Tx_2)\}$$
$$=P\{(\lambda_1x_1+\lambda_2x_2,T(\lambda_1x_1)+T(\lambda_2x_2))\}$$
$$=P\{(\lambda_1x_1+\lambda_2x_2,T(\lambda_1x_1+\lambda_2x_2))\}$$
$$=\lambda_1x_1+\lambda_2x_2$$
$$=\lambda_1P(x_1,Tx_1)+\lambda_2P(x_2,Tx_2)$$

This implies that P is linear. P is also bounded because

$$\|P(x,Tx)\|=\|x\|\le\|x\|+\|Tx\|=\|(x,Tx)\|.$$

Also $P(x_1,Tx_1)=P(x_2,Tx_2)$

$$\Rightarrow x_1=x_2.$$

$\therefore$ P is one-to-one. Obviously, it is onto. Thus P is bijective.

Hence $P^{-1}:X_1\to G(T)$ exists and is given by

$$P^{-1}(x)=(x,Tx)$$

Since $G(T)$ and X_1 are complete, applying Open Mapping Theorem we see that P^{-1} is bounded. Hence there exists positive constant M such that

$$\|P^{-1}(x)\|\le M\|x\| \quad \text{for all } x\in X_1$$

or, $\|(x,Tx)\|\le M\|x\|$ for all $x\in X_1$

Now for any $x\in X_1$ we have

$$\|Tx\|\le\|Tx\|+\|x\|=\|(x,Tx)\|\le M\|x\|.$$

Hence T is bounded.

23.7. Uniform Boundedness Theorem

This theorem is the fourth fundamental theorem of functional analysis. There are many important applications of this theorem. This theorem shows that under certain hypothesis the pointwise boundedness of bounded linear operators implies boundedness in some stronger sense, namely, uniform boundedness. Before we state and prove this famous theorem, we state Baire's Category theorem which is needed for the proof of this fundamental theorem.

23.7.1. Definition. Category.

A subset M of a metric space X is said to be

i) nowhere dense (or rare) in X if its closure $\bar{M}$ has no interior point.

ii) of first category (or meager) in X if M is the union of countably many sets each of which is nowhere dense in X.

iii) of the second category (or nonmeager) in X if M is not of first category in X.

We now state (without proof) the Baire's Category Theorem.

23.7.2. Baire's Category Theorem

If a metric space X is complete then it is of the second category i.e. nonmeager in itself. Hence if X is complete and

$$X = \bigcup_{k=1}^{\infty} A_k \text{ where } A_k \text{ is closed for each } k = 1, 2, \ldots$$

then at least one A_k contains a nonempty open subset.

Using this Baire's Category theorem we shall now state and prove the fourth fundamental theorem of functional analysis viz. Uniform Boundedness Theorem.

23.7.3. Theorem. Uniform Boundedness Theorem.

Let $\{T_n\}$ be a sequence of bounded linear operators $T_n : X \to Y$ from a Banach space X into a normed linear space Y such that $\{\|T_n x\|\}$ is bounded for every $x \in X$. Then the sequence of norms $\{\|T_n\|\}$ is bounded.

Proof. Here $\{\|T_n x\|\}$ is bounded for every $x \in X$. So there exist M_x dependent on x such that

$$\|T_n x\| \leq M_x \text{ for all } n = 1, 2, 3, \ldots \quad \ldots\ldots\ldots\ldots (1)$$

For every positive integer k we define A_k by

$$A_k = \{x : \|T_n x\| \leq k \text{ for all } n = 1, 2, \ldots\} \quad \ldots\ldots\ldots\ldots (2)$$

We now show that A_k is closed for each positive integer k.

Let ξ be any limit of A_k and the sequence $\{x_j\}$ of A_k converges to ξ. Then from the definition of A_k it follows that $\|T_n x_j\| \le k$ for each j. Now T_n and norm function are continuous.

So, as $j \to \infty$ this gives $\|T_n \xi\| \le k$. This implies that $\xi \in A_k$.

Hence A_k is closed subset of X.

From (1) and (2) it follows that each $x \in X$ belongs to some A_k. Hence $X = \bigcup_{k=1}^{\infty} A_k$.

Since X is complete, each A_k is closed and $X = \bigcup_{k=1}^{\infty} A_k$

Baire's Category theorem implies that some A_k contains an open ball, say, $B_0 = B(x_0; r) \subset A_{k_0}$ .....(3)

Let x be any non zero element of X.

We set $z = x_0 + \left(\frac{r}{2\|x\|}\right)x.$ .....(4)

Then $\|z - x_0\| = \frac{r}{2} < r$. $\therefore z \in B_0$ i.e. $z \in A_{k_0}$ [by (3)].

So, $\|T_n z\| \le k_0$ for all $n = 1, 2, ...$

Again $x_0 \in B_0 \subset A_{k_0}$ i.e. $x_0 \in A_{k_0}$. So $\|T_n x_0\| \le k_0$ for all $n = 1, 2, ...$

Now for all $n = 1, 2, ...$ we have

$$\|T_n x\|$$

$$= \left\| T_n \left\{ \frac{2\|x\|}{r}(z - x_0) \right\} \right\|, \text{ [by (4)]}$$

$$= \frac{2\|x\|}{r} \|T_n z - T_n x_0\|$$

$$\le \frac{2\|x\|}{r} (\|T_n z\| + \|T_n x_0\|)$$

$$\le \frac{2\|x\|}{r} (k_0 + k_0)$$

i.e. $\|T_n x\| \leq \left(\frac{4k_0}{r}\right)\|x\|$ for all $n = 1, 2, ...$

$$\Rightarrow \frac{\|T_n x\|}{\|x\|} \leq \frac{4k_0}{r} \quad \text{for all } n = 1, 2, ...$$

$$\Rightarrow \sup_{x \neq 0} \frac{\|T_n x\|}{\|x\|} \leq \frac{4k_0}{r} \quad \text{for all } n = 1, 2, ...$$

$$\Rightarrow \|T_n\| \leq \frac{4k_0}{r} \text{ for all } n = 1, 2, ...$$

Hence the sequence of norms $\{\|T_n\|\}$ is bounded.

23.8. Summary

All four fundamental theorems of functional analysis are introduced in this module. These theorems are related with bounded linear transformations. We define this transformation first over *nls* and then define its norm. Examples are given and related theorem are studied to have a clear understanding of this operator. The Hahn-Banach theorem is stated and its applications are shown. The other three fundamental theoresm are also proved.

23.9. Self Assessment Questions

1. Let N be a real normed linear space and suppose $f(x) = 0$ for all $f \in N^*$. Prove that $x = 0$.
2. Let N and N' be normed linear spaces and let T be a linear transformation of N into N'. If T is continuous at $x_1 \in N$ then show that T is continuous at $x_2 \in N, (x_2 \neq x_1)$.
3. Let T be a linear transformation of a normed linear space X into another normed linear space Y. Show that T is bounded if and only if T maps bounded set in X into bounded set in Y.
4. If T is a bounded linear operator such that its inverse T^{-1} exists, prove that T^{-1} is also continuous.
5. If T is the function on R^2 defined by

   $$T(x, y) = (x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta)$$

   then show that T is bounded linear transformation.

6. If T is a bounded linear functional on a *nls* X and $\{x_n\}$ is Cauchy in X, then show that $\{Tx_n\}$ is a Cauchy sequence.

23.10. Suggested books for further reading

1. Functional Analysis with Applications: B. Chaudhary and Sudarsan Nanda; Wiley Eastern Limited.
2. Elements of Functional Analysis : B.K. Lahiri; World Press.
3. Introductory Functional Analysis with Applications : Erwin Kreyszig; John Wiley & Sons.
4. Functional Analysis : J.N. Sharma, A.R. Vasishtha; Krishna Prakashan Mandir.

----- 0 ------

M.Sc. Course
in
Applied Mathematics with Oceanology
and
Computer Programming

PART-I

Paper-II

Group-B

Module No. - 24

Functional Analysis

(Inner Product Space and Hilbert Space)

Module Structure :

24.1 Introduction

The linear space is a generalization of vector space of two and three dimensions. The concept of length of a vector has been introduced in terms norm in a linear space. In a vector space of usual vector one more important notion is there viz the notion of dot product. With the help of dot product the concept of orthogonality can be introduced. This concept of dot product is missing is normed linear space. Hence the question arises whether the

dot product and orthogonality can be introduced in arbitrary linear space. In fact, we show in this module that this can be done and thus we define an inner product in a linear space. A linear space equipped with inner product will be called an inner product space. It is shown here that the normed linear space is a special case of inner product space. Though we have first discussed the normed linear space (Module 22) and then inner product space (Module 24), historically the notion of inner product space was introduced before the notion of normed linear space.

24.2. Objectives

We begin with the axiomatic definition of inner product space introduced by the famous mathematician J. Von Neumann. A complete inner product space is called a Hilbert space in the name of the great German mathematician D. Hilbert. The modern developments in Hilbert spaces are concerned largely with the theory of operators on the spaces. The whole theory was initiated by the work of D. Hilbert (1912) on integral equations. The currently used geometrical notation and terminology is analogous to that the Euclidean geometry. The generalization of the notions of parallelogram law, Pythagorean theorem, Bessels inequality, Fourier series etc. have been discussed. The decomposition of any element of the Hilbert space uniquely as the sum of two elements one from the closed subspace and another from its complement is very important and interesting. The unique representation of bounded linear functional on a Hilbert space in terms of inner product is realy amazing. The notion of adjoint operator and theorems relating to it have been studied.

24.3. Inner-Product Space

24.3.1. Definition. Inner product space

Let X be a linear space over the complex field C. Then X is called an inner product space if there exists a function $(,): X \times X \to C$ which satisfies the following conditions :

i) $(x,y) = \overline{(y,x)}$ for $x, y \in X$

ii) $(\lambda x + \mu y, z) = \lambda(x,z) + \mu(y,z)$ *for* $\lambda, \mu \in C, x, y, z \in X$

iii) $(x,x) \geq 0$ for all $x \in X$

iv) $(x,x) = 0$ if and only if $x = 0$.

Taking $y = x$ in (*i*) we get $(x,x) = \overline{(x,x)}$ for all $x \in X$.

This shows that (x,x) is a real number.

Also we have

$$(x, \lambda y + \mu z) = \overline{(\lambda y + \mu z, x)} \text{ [by } (i)\text{]}$$

$$= \overline{\lambda (y,x) + \mu (z,x)} \text{ [by } (ii)\text{]}$$

$$= \bar{\lambda} \overline{(y,x)} + \bar{\mu} \overline{(z,x)}$$

$$= \bar{\lambda} (x,y) + \bar{\mu} (x,z) \text{ [by } (i)\text{]}$$

Thus $(\alpha x + \beta y, \mu z + \gamma v)$

$$= \alpha (x, \mu z + \gamma v) + \beta (y, \mu z + \gamma v)$$

$$= \alpha\bar{\mu} (x,z) + \alpha\bar{\gamma} (x,v) + \beta\bar{\mu} (y,z) + \beta\bar{\gamma} (y,v)$$

Taking $\lambda = o = \mu$ we get from (i) that $(ox + oy, z) = o(x,y) + o\,(y,z)$

or, $(o, z) = o + o$ or, $(o, z) = 0$ for any $z \in X$.

Thus $(o, x) = 0 = (x, o)$ for any $x \in X$.

24.3.2. Examples of inner-product spaces

i) R^n is a real inner-product space with the inner product

$$(x,y) = \sum_{j=1}^{n} x_j y_j$$

where $x = (x_1, x_2, ..., x_n), y = (y_1, y_2, ..., y_n)$ and x_j, y_j are real numbers.

ii) C^n is a complex inner product space with the inner product

$$(x,y) = \sum_{j=1}^{n} x_j \bar{y}_j$$

where $x = (x_1, x_2, ..., x_n), y = (y_1, y_2, ..., y_n)$ and x_j, y_j are complex numbers.

iii) The sequence space l_2 is an inner product space with the inner product

$$(x,y) = \sum_{j=1}^{\infty} x_j \bar{y}_j$$

where $x = \{x_j\}, y = \{y_j\}$ and x_j, y_j are real or complex numbers.

iv) The set of all real numbers R is an inner product space with the inner product

$$(x, y) = xy$$

Here we note that the inner product is the ordinary product.

24.3.3. Theorem (Cauchy-Schwarz inequality)

If X is an inner product space and $x, y \in X$, then $|(x,y)|^2 \leq (x,x)(y,y)$

Proof. For $y = 0$ we have $(x,y) = (x,0) = 0$ and $(y,y) = (0,0) = 0$

$\therefore |(x,y)|^2 = 0 = (x,x)(y,y)$ i.e. the inequality holds.

Let $y \neq 0$ and $\lambda \in C$. Then we have

$$0 \leq (x - \lambda y, x - \lambda y) = (x,x) - \bar{\lambda}(x,y) - \lambda(y,x) + \lambda\bar{\lambda}(y,y)$$

$$\therefore (x,x) - \bar{\lambda}(x,y) - \lambda\overline{(x,y)} + |\lambda|^2 (y,y) \geq 0$$

This is true for any $\lambda \in C$. Taking $\lambda = \dfrac{(x,y)}{(y,y)} [\because y \neq 0]$ we get

$$(x,x) - \frac{\overline{(x,y)}}{(y,y)}(x,y) - \frac{(x,y)}{(y,y)}\overline{(x,y)} + \frac{|(x,y)|^2}{(y,y)^2}(y,y) \geq 0$$

or, $$(x,x) - \frac{2|(x,y)|^2}{(y,y)} + \frac{|(x,y)|^2}{(y,y)} \geq 0$$

or, $$(x,x) \geq \frac{|(x,y)|^2}{(y,y)}$$

or, $$|(x,y)|^2 \leq (x,x)(y,y).$$

A linear space x becomes a *nls* if it is possible to define a norm in X, the same linear space becomes an inner product space if it is possible to define an inner product is it. So question arises whether a linear space can be both *nls* as well as inner product space. The following theorem gives the answer.

24.3.4. Theorem. Every inner product space is a normed linear space.

Proof. Let X be an inner product space. Then for every $x \in X$ we know that (x,x) is a real number and is non negative. We define a function $f : X \to R$ by $f(x) = (x,x)^{1/2}$ and show that this satisfies all axions of norm function.

We have

i) $f(x) = (x,x)^{1/2} \geq 0$

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

$= (x,x)+(y,y)+\overline{(x,y)}+(x,y)$

$= (x,x)+(y,y)+2$ real part of (x,y)

$\leq (x,x)+(y,y)+2|(x,y)|$

$\leq (x,x)+(y,y)+2(x,x)^{1/2}(y,y)^{1/2}$ [by Cauchy-Schwarz inequality]

$= \left[(x,x)^{1/2}+(y,y)^{1/2}\right]^2$

i.e. $(x+y, x+y)^{1/2} \leq (x,y)^{1/2}+(y,y)^{1/2}$

i.e. $f(x+y) \leq f(x)+f(y)$

iii) For any $\lambda \in C$ we have

$(\lambda x, \lambda x) = \lambda\bar{\lambda}(x,x) = |\lambda|^2 (x,x)$

or, $(\lambda x, \lambda x)^{1/2} = |\lambda|(x,x)^{1/2}$

or, $f(\lambda x) = |\lambda| f(x)$

iv) $(x,x)^{1/2} = 0$

$\Rightarrow (x,x) = 0$

$\Rightarrow x = 0$

Thus $f(x)$ satisfies all axioms of norm function and so we denote it by $\|x\|$ i.e. $\|x\| = f(x) = (x,x)^{1/2}$. Hence every inner product space is a normed linear space with norm defined by $\|x\| = (x,x)^{1/2}$.

Note. Using this norm function the Cauchy-Schwarz inequality may be put in the form

$$|(x, y)| \leq \|x\| \, \|y\|.$$

We know that every normed linear space is a metric space with the metric $d(x, y) = \|x - y\|$. As every inner product space is normed linear space and as every normed linear space is a metric space, it follows that every inner product space is a metric space with metric $d(x, y) = \|x - y\| = (x - y, x - y)^{1/2}$

We now define Hilbert space.

24.3.5. Definition. Hilbert Space

A complete inner product space with the metric defined by $d(x, y) = (x - y, x - y)^{1/2}$ is called a Hilbert space.

As every inner product space is normed linear space it follows that every complete inner product space is complete normed linear space i.e. every Hilbert space is a Banach space. We have proved that the norm function defined in a normed linear space is a continuous function. In the same manner it is now shown that the inner product function defined in an inner product space is also a continuous function. Thus we have the following theorem.

24.3.6. Theorem. In an inner product space, the inner product function is a continuous functioin.

Proof. Let X be an inner product space and x, y be any elements of X. Let $\{x_n\}$ and $\{y_n\}$ be sequences in X such that $x_n \to x \in X$ and $y_n \to y \in X$ as $n \to \infty$.

Then we have

$$\begin{aligned}
&|(x_n, y_n) - (x, y)| \\
&= |(x_n, y_n) - (x_n, y) + (x_n, y) - (x, y)| \\
&= |(x_n, y_n - y) + (x_n - x, y)| \\
&\leq |(x_n, y_n - y)| + |(x_n - x, y)| \\
&\leq \|x_n\| \|y_n - y\| + \|x_n - x\| \|y\| \text{ [by Cauchy Schwarz inequality]} \\
&\to \|x\| \cdot 0 + 0 \|y\| \text{ as } n \to \infty
\end{aligned}$$

Hence $|(x_n, y_n)-(x,y)| \to 0$ as $n \to \infty$

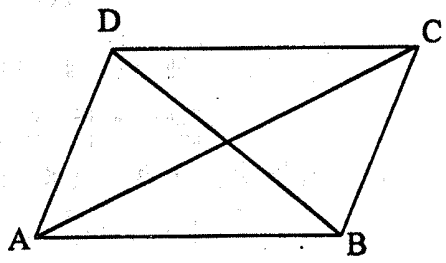
i.e. $(x_n, y_n) \to (x,y)$ as $n \to \infty$

This shows that inner product function is a continuous function.

In elementary geometry, we know that the sum of the squares of the sides of a parallalogram is equal to the sum of the squares of its diagonals i.e. if $ABCD$ is a parallelogram then we have

$$AB^2 + BC^2 + CD^2 + DA^2 = AC^2 + BD^2$$

or, $2(AB^2 + BC^2) = AC^2 + BD^2$.



This law is known as parallelogram law.

This parallelogram law is also true for ordinary vectors as

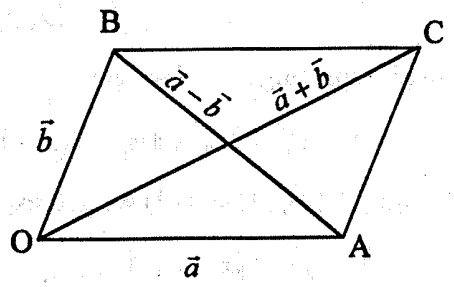
$$|\vec{a}+\vec{b}|^2 + |\vec{a}-\vec{b}|^2 = 2\left(|\vec{a}|^2 + |\vec{b}|^2\right)$$

Geometrically this gives

$$|\overrightarrow{OC}|^2 + |\overrightarrow{BA}|^2 = 2\left(|\overrightarrow{OA}|^2 + |\overrightarrow{OB}|^2\right)$$

or, $OC^2 + AB^2 = 2(OA^2 + OB^2)$

Now we state and prove parallegram law for inner product space



24.3.7. Theorem. If x and y are elements of an inner product space X, then

$$\|x+y\|^2 + \|x-y\|^2 = 2\left(\|x\|^2 + \|y\|^2\right)$$

Proof. We have

$$\|x+y\|^2 + \|x-y\|^2$$
$$= (x+y, x+y) + (x-y, x-y)$$
$$= (x,x)+(x,y)+(y,x)+(y,y)+(x,x)-(x,y)-(y,x)+(y,y)$$
$$= 2(x,x)+2(y,y)$$
$$= 2\left(\|x\|^2 + \|y\|^2\right).$$ Hence the theorem.

24.3.8. Theorem. If x and y are elements of an inner product space X then prove that

$$(x,y)=\frac{1}{4}\left\{\|x+y\|^2-\|x-y\|^2+i\|x+iy\|^2-i\|x-iy\|^2\right\}$$

(This is called Polarization identity)

Proof. We have

$$\|x+y\|^2=(x+y,x+y)=(x,x)+(x,y)+(y,x)+(y,y)$$
$$=\|x\|^2+\|y\|^2+(x,y)+(y,x) \quad \ldots\ldots\ldots (1)$$

In (1) replacing y by $-y$ we get

$$\|x-y\|^2=\|x\|^2+\|-y\|^2+(x,-y)+(-y,x)$$
$$=\|x\|^2+\|y\|^2-(x,y)-(y,x) \quad \ldots\ldots\ldots (2)$$

In (1) replacing y by iy we get

$$\|x+iy\|^2=\|x\|^2+\|iy\|^2+(x,iy)+(iy,x)$$
$$=\|x\|^2+|i|^2\|y\|^2-i(x,y)+i(y,x)$$
$$=\|x\|^2+\|y\|^2-i(x,y)+i(y,x) \quad \ldots\ldots\ldots (3)$$

In (3) replacing i by $-i$ we get

$$\|x-iy\|^2=\|x\|^2+\|y\|^2+i(x,y)-i(y,x) \quad \ldots\ldots\ldots (4)$$

From (1), (2), (3) and (4) we get respectively

$$\|x+y\|^2=\|x\|^2+\|y\|^2+(x,y)+(y,x)$$
$$-\|x-y\|^2=-\|x\|^2-\|y\|^2+(x,y)+(y,x)$$
$$i\|x+iy\|^2=i\|x\|^2+i\|y\|^2+(x,y)-(y,x)$$
$$-i\|x-iy\|^2=-i\|x\|^2-i\|y\|^2+(x,y)-(y,x)$$

Adding we get, $\|x+y\|^2-\|x-y\|^2+i\|x+iy\|^2-i\|x-iy\|^2=4(x,y)$

i.e. $(x,y)=\frac{1}{4}\left[\|x+y\|^2-\|x-y\|^2+i\|x+iy\|^2-i\|x-iy\|^2\right]$.

We have seen that every inner product space is a normed linear space. Is its converse true? Not always.

Under certain condition a normed linear space becomes an inner product space, and that condition is the holding of parallelogram law. We now state and prove this theorem.

24.3.9. Theorem. A Banach space is a Hilbert space if and only if the parallelogram low holds.

Proof. For simplicity, we consider the Banach space to be real. We suppose that in this Banach space parallelogram law holds. We introduce an inner product in X by

$$(x,y)=\frac{1}{4}\left[\|x+y\|^2-\|x-y\|^2\right] \qquad \text{..... (1)}$$

We now verify one by one the axioms of inner product.

We have $(y,x)=\frac{1}{4}\left[\|y+x\|^2-\|y-x\|^2\right]=\frac{1}{4}\left[\|x+y\|^2-\|x-y\|^2\right]=(x,y)$

Also $(x,x)=\frac{1}{4}\left[\|x+x\|^2-\|x-x\|^2\right.$

$$=\frac{1}{4}\left[\|2x\|^2-0=\|x\|^2\geq 0\right.$$

Now $(x,x)=0\Rightarrow\|x\|^2=0\Rightarrow\|x\|=0\Rightarrow x=0.$

Also when $x=0$ then $\|x\|=0\Rightarrow\|x\|^2=0\Rightarrow(x,x)=0$

It remains to show that

$$(x_1+x_2,y)=(x_1,y)+(x_2,y)$$

and $(\lambda x,y)=\lambda(x,y)$ where λ is a scalar.

By parallelogram low, we have

$$\|u+v+w\|^2+\|u+v-w\|^2=2\|u+v\|^2+2\|w\|^2$$

and $\|u-v+w\|^2+\|u-v-w\|^2=2\|u-v\|^2+2\|w\|^2$

On subtraction, we get

$$\|u+v+w\|^2+\|u+v-w\|^2-\|u-v+w\|^2-\|u-v-w\|^2=2\|u+v\|^2-2\|u-v\|^2$$

Using (1) we get $(u+w,v)+(u-w,v)=2(u,v)$

This is true for any u, v, w in X.

taking $w=u$ we have $(2u,v)+(0,v)=2(u,v)$

or, $(2u,v)=2(u,v)\left[\because (0,v)=\frac{1}{4}\left[\|0+v\|^2-\|0-v\|^2\right]=0\right]$

$\therefore (u+w,v)+(u-w,v)=(2u,v)$

Let x_1, x_2, y be elements in X. Setting $u+w=x_1, u-w=x_2$ and $v=y$ we obtain

$(x_1,y)+(x_2,y)=(x_1+x_2,y)$ ..... (2)

We now show that $(\lambda x,y)=\lambda(x,y)$

where λ is a scaler. ..... (3)

In (2) we take $x_1=x_2=x$ and obtain

$2(x, y) = (2x, y)$

Now $3(x, y) = 2(x, y) + (x, y) = (2x, y) + (x, y) = (2x+x, y) = (3x, y)$

$4(x, y) = 3(x, y) + (x, y) = (3x, y) + (x, y) = (3x+x, y) = (4x, y)$

and so on.

In general we thus have by induction that

$n(x, y) = (nx, y)$ when n is any positive integer.

In (1) taking $-x$ for x we have $(-x,y)=\frac{1}{4}\left[\|-x+y\|^2-\|-x-y\|^2\right]=-\frac{1}{4}\left[\|x+y\|^2-\|x-y\|^2\right]=-(x,y)$.

If n is any negative integer, let $n=-m$. Then m is a positive integer. Hence

$(nx, y) = (-mx, y) = -(mx, y) = -m(x, y) = n(x, y)$.

So $(\lambda x,y)=\lambda(x,y)$ is true for any integer λ, positive or negative.

If λ is any rational number, let $\lambda=\frac{p}{q}$.

Then

$$p(x,y)=(px,y)=\left(q\left(\frac{p}{q}x\right),y\right)=q\left(\frac{px}{q},y\right)$$

or, $\frac{p}{q}(x,y)=\left(\frac{p}{q}x,y\right)$. Thus (3) is true for any rational λ.

Finally, let λ be any real number. Then there exists a squence r_n of rational numbers such that $r_n \to \lambda$ as $n \to \infty$.

Now for each r_n we have

$$r_n(x,y)=(r_n x,y) \qquad \text{.....(4)}$$

We have

$$|r_n(x,y)-\lambda(x,y)|=|(r_n-\lambda)(x,y)|=|r_n-\lambda|(x,y)\to 0 \text{ as } n\to\infty.$$

$$\therefore r_n(x,y)\to\lambda(x,y) \text{ as } n\to\infty. \qquad \text{.....(5)}$$

Again

$$|(r_n x,y)-(\lambda x,y)|=|(r_n x-\lambda x,y)|$$

$$=\left|((r_n-\lambda)x,y)\right|=\frac{1}{4}\left|\|(r_n-\lambda)x+y\|^2-\|(r_n-\lambda)x-y\|^2\right|$$

$$\to\frac{1}{4}\left|\|0+y\|^2-\|0-y\|^2\right| \text{ as } n\to\infty$$

$$\therefore(r_n x,y)\to(\lambda x,y) \text{ as } n\to\infty \qquad \text{.....(6)}$$

In (4) letting $n\to\infty$ and using (5) and (6) we get

$\lambda(x,y)=(\lambda x,y)$ i.e. (3) is true for any real λ.

This proves the theorem.

Note: In case the Banach space is complex we have to take the inner product of x, y as

$$(x,y)=\frac{1}{4}\left[\|x+y\|^2-\|x-y\|^2+i\|x+iy\|^2-i\|x-iy\|^2\right]$$

We now introduce uniformly convex space and prove a related theorem.

24.3.10. Definition. Uniformly Convex Space

Let X be a normed linear space. Suppose for all $\varepsilon>0$ and $x,y\in X$ such that $\|x\|=\|y\|=1$ and $\|x-y\|>\varepsilon$ imply that $\left\|\frac{1}{2}(x+y)\right\|\le 1-\delta$ where $\delta=\delta(\varepsilon)$ is independent of x and y and $0<\delta<1$. Then X is said to be uniformly convex.

The following theorem shows that every inner product space is uniformly convex.

24.3.11. Thorem. Every inner product space is uniformly convex.

Proof. Let X be any inner product space and $\varepsilon>0$.

Let $x,y\in X$, $\|x\|=\|y\|=1$ and $\|x-y\|>\varepsilon$.

Using parallelogram law we have

$$\left\|\frac{x}{2}+\frac{y}{2}\right\|^2+\left\|\frac{x}{2}-\frac{y}{2}\right\|^2=2\left(\left\|\frac{x}{2}\right\|^2+\left\|\frac{y}{2}\right\|^2\right)$$

or, $$\left\|\frac{x+y}{2}\right\|^2=\frac{1}{2}\|x\|^2+\frac{1}{2}\|y\|^2-\frac{1}{4}\|x-y\|^2$$

$$<\frac{1}{2}+\frac{1}{2}-\frac{\varepsilon^2}{4}$$

$$=1-\left(\frac{\varepsilon}{2}\right)^2$$

Thus, we can find a number $\delta=\left(\frac{\varepsilon}{2}\right)^2, 0<\delta<1$, such that

$$\left\|\frac{x+y}{2}\right\|\leq 1-\delta.$$

This completes the proof of the theorem.

24.4. Orthogonal and Orthonormal Sets

The inner product in an inner-product space is similar to scalar product or dot product in ordinary three dimensional vector space. As the dot product gives the measure of angle in between two vectors, the inner product in an *ips* also gives a measure of angle in between two elements of it. Similar to dot product two elements of an *ips* will be orthogonal if the inner product between them is zero. This notion of orthogonality is introduced here.

24.4.1. Definition. Orthogonal elements

Two elements x and y in an inner product space X are said to be orthogonal if the inner product between them is zero i.e. if $(x, y) = 0$. It is denoted by $x \perp y$.

24.4.2. Definition. Orthogonal Set

A subset S of an inner product space X is said to be orthogonal set if $x \perp y$ for all $x, y \in S$ and $x \neq y$.

24.4.3. Definition. Orthonormal Set

A subset S of an inner product space X is said to be orthonormal if $x \perp y$ for all $x \neq y; x, y \in S$ and $\|x\| = 1$ for every $x \in S$.

We now show that the famous Pythagorean theorem is true for an inner product space.

24.4.4. Theorem. Pythagorean theorem.

If $\{x_1, x_2, ..., x_n\}$ is an orthogonal subset of an inner product space then

$$\|x_1 + x_2 + ... + x_n\|^2 = \|x_1\|^2 + \|x_2\|^2 + ... + \|x_n\|^2.$$

Proof. We have

$$\|x_1 + x_2 + ... + x_n\|^2$$
$$= (x_1 + x_2 + ... + x_n, x_1 + x_2 + ... + x_n)$$
$$= (x_1, x_1) + (x_1, x_2) + ... + (x_1, x_n)$$
$$+ (x_2, x_1) + (x_2, x_2) + ... + (x_2, x_n)$$
$$... \quad ... \quad ... \quad ... \quad ... \quad ... \quad ... \quad ...$$
$$... \quad ... \quad ... \quad ... \quad ... \quad ... \quad ... \quad ...$$
$$+ (x_n, x_1) + (x_n, x_2) + ... + (x_n, x_n)$$
$$= (x_1, x_1) + 0 + ... + 0$$
$$+ 0 + (x_2, x_2) + ... + 0$$
$$... \quad ... \quad ... \quad ... \quad ... \quad ... \quad ...$$
$$.... \quad ... \quad ... \quad ... \quad ... \quad ... \quad ...$$
$$+ 0 + 0 + ... + (x_n, x_n) \left[\because (x_i, x_j) = 0 \text{ for all } i \neq i\right]$$
$$= (x_1, x_1) + (x_2, x_2) + ... + (x_n, x_n)$$
$$= \|x_1\|^2 + \|x_2\|^2 + ... + \|x_n\|^2.$$

24.4.5. Definition. Complete orthogonal (or orthonormal) set

An orthogonal (or orthonormal) set $\{e_i\}$ in the inner product space X is said to be complete if it is impossible to adjoin a vector e to $\{e_i\}$ such that $\{\{e_i\}, e\}$ is an orthogonal (or orthonormal) set.

Note : It can be proved that every norzero inner product space X contains a complete orthonormal set.

The following theorem shows the importance of complete orthonormal set in an inner product space.

24.4.6. Theorem.

Let $\{e_i\}$ be a nonvoid arbitrary orthonormal set in an inner product space X. Then the following four conditions are equivalent :

i) $\{e_i\}$ is complete

ii) $x \perp e_i$ for all $i \Rightarrow x = 0$

iii) $x \in X \Rightarrow x = \sum_i (x, e_i) e_i$

iv) $x \in X \Rightarrow \|x\|^2 = \sum_i |(x, e_i)|^2$

Proof. Let (*i*) be true i.e. $\{e_i\}$ be complete. We are to prove (*ii*). If possible let (*ii*) be false. Then there exists $x \in X, x \neq 0$ such that $x \perp e_i$ for all i. Now we define e by $e = x/\|x\|$. Then $\{\{e_i\}, e\}$ is an orthonormal set which properly contains $\{e_i\}$. This contradicts the completeness of $\{e_i\}$. Hence (*ii*) is true. Therefore (*i*) implies (*ii*).

Let (*ii*) be true i.e. $x \perp e_i$ for all $i \Rightarrow x = 0$.

Now for any e_j of $\{e_i\}$ we have for any $x \in X$

$$\begin{aligned}
&\left(x - \sum (x, e_i) e_i, e_j\right) \\
&= (x, e_j) - \sum (x, e_i)(e_i, e_j) \\
&= (x, e_j) - (x, e_j)(e_j, e_j) \left[\because (e_i, e_j) = 0 \forall i \neq j\right] \\
&= (x, e_j) - (x, e_j) \left[\because (e_j, e_j) = 1\right] \\
&= 0
\end{aligned}$$

Thus $x-\sum(x,e_i)e_j \perp e_j$ for all j.

Hence by (*ii*) we have $x-\sum(x,e_i)e_i=0$

i.e. $x=\sum(x,e_i)e_i$. So (*iii*) is true.

$\therefore$ (*ii*) implies (*iii*).

Let (*iii*) be true i.e. for any $x\in X$ we have $x=\sum(x,e_i)e_i$

Then $\|x\|^2$

$=(x,\ x)$

$$=\left(\sum_i(x,e_i)e_i,\sum_i(x,e_j)e_j\right)$$

$$=\sum_i\left[\sum_j(x,e_i)\overline{(x,e_j)}(e_i,e_j)\right]$$

$$=\sum_i(x,e_i)\overline{(x,e_i)}(e_i,e_i)\left[\because(e_i,e_j)=0 \text{ for all } i\neq j\right]$$

$$=\sum_i(x,e_i)\overline{(x,e_i)}\left[\because(e_i,e_i)=1\right]$$

$$=\sum_i|(x,e_i)|^2$$

Hence (*iii*) implies (*iv*).

Finally, let (*iv*) be true. We are to show that (*i*) is true. If possible, let (*i*) be not true i.e. $\{e_i\}$ be not complete.

Then there exists $e\in X$ with $\|e\|=1$ such that $\{\{e_i\},e\}$ is an orthonormal set. Then $e\perp e_i$ for all i.

i.e. $(e,e_i)=0$ for all i ..... (1)

Since (*iv*) is true we have

$$\|e\|^2=\sum_i|(e,e_i)|^2$$

$$=\sum_i|0|^2 \text{ [by (1)]}$$

$$=0$$

i.e. $\|e\|=0$.

This is a contraction, as $\|e\| = 1$.

Hence (*i*) is true. Thus (*iv*) implies (*i*).

This completes the proof.

Remarks.

i) The series $x = \sum_i (x, e_i) e_i$ is known as Fourier series of x and (x, e_i) are called Fourier coefficients of x.

ii) The identity $\|x\|^2 = \sum_i |(x, e_i)|^2$ is known as Parseval's identity.

In the following theorem we prove the Bessel's inequality.

24.4.7. Theorem. If $\{e_1, e_2, ..., e_n\}$ is a finite orthonormal set in an inner product space X and x is any element of X, then

$$\sum_{i=1}^{n} |(x, e_i)|^2 \leq \|x\|^2 \text{ and}$$

$$x - \sum_{i=1}^{n} (x, e_i) e_i \text{ is orthogonal to } e_j \text{ for all } j = 1, 2, ..., n.$$

Proof. We have

$$0 \leq \left\| x - \sum_{i=1}^{n} (x, e_i) e_i \right\|^2$$

$$= \left(x - \sum_{i=1}^{n} (x, e_i) e_i, x - \sum_{j=1}^{n} (x, e_j) e_j \right)$$

$$= (x, x) - \left(x, \sum_{j=1}^{n} (x, e_j) e_j \right) - \left(\sum_{i=1}^{n} (x, e_i) e_i, x \right)$$

$$+ \left(\sum_{i=1}^{n} (x, e_i) e_i, \sum_{j=1}^{n} (x, e_j) e_j \right)$$

$$= (x, x) - \sum_{j=1}^{n} \overline{(x, e_j)} (x, e_j) - \sum_{i=1}^{n} (x, e_i)(e_i, x)$$

$$+\sum_{i=1}^{n}\left[\sum_{j=1}^{n}(x,e_i)\overline{(x,e_j)}(e_i,e_j)\right]$$

$$=\|x\|^2-\sum_{j=1}^{n}|(x,e_j)|^2-\sum_{i=1}^{n}(x,e_i)\overline{(x,e_i)}+\sum_{i=1}^{n}(x,e_i)\overline{(x,e_i)}(e_i,e_i)\ \left[\because (e_i,e_j)=0 \text{ for all } i\neq j\right]$$

$$=\|x\|^2-\sum_{j=1}^{n}|(x,e_j)|^2-\sum_{j=1}^{n}|(x,e_i)|^2+\sum_{i=1}^{n}|(x,e_i)|^2\ \left[\because (e_i,e_i)=1\right]$$

$$=\|x\|^2-\sum_{j=1}^{n}|(x,e_j)|^2$$

or, $\sum_{j=1}^{n}|(x,e_j)|^2\leq\|x\|^2$

This inequality is known as Bessel's inequality.

For the second part we have for any $e_j\ (j=1,2,...,n)$

$$\left(x-\sum_{i=1}^{n}(x,e_i)e_i,e_j\right)$$

$$=(x,e_j)-\sum_{i=1}^{n}(x,e_i)(e_i,e_j)$$

$$=(x,e_j)-(x,e_i)(e_i,e_j)\left[\because (e_i,e_j)=0 \text{ for all } i\neq j\right]$$

$$=(x,e_j)-(x,e_j)\left[\because (e_j,e_j)=1\right]$$

$$=0$$

Hence $x-\sum_{i=1}^{n}(x,e_i)e_i$ is orthogonal to e_j for all $j=1,2,...n$.

This proves the theorem.

24.5. Riesz representation theorem

Before proving Riesz representation theorem we first prove the following important theorem as a consequence of parallelogram law. This theorem has several applications.

24.5.1. Theorem. If M is a non empty, closed and convex set in a Hilbert space X, then there exists a unique element in M of smallest norm.

Proof. Let $d = \inf\{\|x\| : x \in M\}$. Then there exists a sequence $\{x_n\}$ in M such that $\|x_n\| \to d$ as $n \to \infty$. Using parallelogram law we get

$$\left\|\frac{x_n}{2}+\frac{x_m}{2}\right\|^2+\left\|\frac{x_n}{2}-\frac{x_m}{2}\right\|^2=2\left\|\frac{x_n}{2}\right\|^2+2\left\|\frac{x_m}{2}\right\|^2$$

or, $$\left\|\frac{x_n-x_m}{2}\right\|^2=\frac{1}{2}\|x_n\|^2+\frac{1}{2}\|x_m\|^2-\left\|\frac{x_n+x_m}{2}\right\|^2 \quad \text{..... (1)}$$

Since M is convex and $x_n, x_m \in M$, we have $\frac{x_n+x_m}{2} \in M$.

Hence $\left\|\frac{x_n+x_m}{2}\right\|^2 \geq d^2$. Thus (1) becomes

$$\frac{1}{4}\|x_n-x_m\|^2 \leq \frac{1}{2}\|x_n\|^2+\frac{1}{2}\|x_m\|^2-d^2$$

or, $$\|x_n-x_m\|^2 \leq 2\|x_n\|^2+2\|x_m\|^2-4d^2$$

Taking limit this gives

$$\lim_{n,m\to\infty}\|x_n-x_m\|^2 \leq 2d^2+2d^2-4d^2$$

or, $$\lim_{n,m\to\infty}\|x_n-x_m\|^2 \leq 0$$

or, $$\lim_{n,m\to\infty}\|x_n-x_m\|^2 = 0$$

or, $$\lim_{n,m\to\infty}\|x_n-x_m\| = 0$$

i.e. $\{x_n\}$ is a Cauchy sequence in M.

Now M is a closed subset of the complete space X. So M is complete, hence there exists an element $x \in M$ such that $\lim_{n\to\infty} x_n = x$.

As the norm function is continuous we have

$$\|x\| = \left\|\lim_{n\to\infty} x_n\right\| = \lim_{n\to\infty}\|x_n\| = d$$

Thus we get the element x in M with smallest norm. We now show that this element is unique.

If possible, let there be another y in M such that $\|y\| = d$.

Therefore, $x \neq y, x, y \in M$ and $\|x\| = \|y\| = d$.

Applying parallelogram law we get

$$\left\|\frac{x-y}{2}\right\|^2 = 2\left\|\frac{x}{2}\right\|^2 + 2\left\|\frac{y}{2}\right\|^2 - \left\|\frac{x+y}{2}\right\|^2$$

$$\leq \frac{d^2}{2} + \frac{d^2}{2} - d^2 \left[\text{as} \left\|\frac{x+y}{2}\right\| \geq d\right]$$

$$= 0$$

or, $\|x-y\| = 0$

or, $x-y = 0$

or, $x = y$.

This is a contradiction as $x \neq y$.

Hence the element in M possessing smallest norm is unique. This completes the proof of the theorem.

Using this theorem we shall now prove the famous decomposition theorem. For this we need the following definitions.

24.5.2. Definition. Orthogonal Complement

Let M be a subset of a Hilbert space X. The orthogonal complement of M is the set of the elements of X which are orthogonal to every element of M. It is denoted by $M^{\perp}$.

We have the following results.

i) For every subset M of the Hilbert space, the orthogonal complement $M^{\perp}$ is always a closed subspace of X

ii) If $M = \{0\}$ then $M^{\perp} = X$

iii) If $M = X$ then $M^{\perp} = \{0\}$

iv) If $M \neq \{0\}$ then $M^{\perp} \neq X$

v) Orthogonal complement of $M^{\perp}$ is M i.e. $\left(M^{\perp}\right)^{\perp} = M$.

We now prove the following decomposition theorem.

24.5.3. Theorem. If M is a closed subspace of a Hilbert space X and $x \in X$, then there exists unique element y in M and z in $M^{\perp}$ such that $x = y + z$.

Proof. Let x be any element of X. We define the set S by

$$S = \{x - w : w \in M\}.$$

Since M is closed subspace of X, it follows that S is a non empty closed convex subset of X. Hence from theorem 24.5.1. there exists a unique element in S of the smallest norm. Let this unique element be z.

Since $z \in S$, there is $y \in M$ such that $z = x - y$ ..... (1)

Now let u be an element in M of norm one. Then

$$\begin{aligned} & z - (z, u)\, u \\ = \; & x - y - (z, u)\, u \\ = \; & x - \{y + (z, u)\, u\} \end{aligned} \quad \text{..... (2)}$$

Since $y \in M, u \in M$ and M is a subspace it follows that $y + (z,u)u \in M$. Hence from (2), $z - (z,u)u \in S$.

Since z has smallest norm in S we get

$$\|z\| \le \|z - (z,u)u\|$$

or, $$\|z\|^2 \le \|z - (z,u)u\|^2$$

$$= (z - (z,u)u, z - (z,u)u)$$

$$= (z,z) - (z,(z,u)u) - ((z,u)u, z) + ((z,u)u, (z,u)u)$$

$$= \|z\|^2 - \overline{(z,u)}(z,u) - (z,u)(u,z) + (z,u)\overline{(z,u)}(u,u)$$

$$= \|z\|^2 - |(z,u)|^2 - (z,u)\overline{(z,u)} + (z,u)\overline{(z,u)} \quad \left[\because (u,u) = \|u\|^2 = 1\right]$$

$$= \|z\|^2 - |(z,u)|^2$$

or, $|(z,u)|^2 \leq 0$

or, $|(z,u)| \leq 0$

or, $|(z,u)| = 0.$

This implies that $(z, u) = 0$. Thus for any element u of M with unit norm we have $(z, u) = 0$.

Let v be any non-zero element of M. Then $v/\|v\|$ is an element of M with unit norm.

$$\therefore \left(z, \frac{v}{\|v\|}\right) = 0 \quad \text{or,} \quad \frac{1}{\|v\|}(z,v) = 0 \text{ or, } (z,v) = 0$$

Hence $z \perp v$ for any $v \in M$. This means $z \perp M$ i.e. $z \in M^{\perp}$.

Thus from (1) we have $x = y + z$ where $z \in M$ and $z \in M^{\perp}$.

For the uniqueness, let there be $y'(\neq y)$ in M and $z'(\neq z)$ in $M^{\perp}$ such that $x = y' + z'$.

Then $x = y + z = y' + z'$ where $y, y' \in M$ and $z, z' \in M^{\perp}$.

We have then $y - y' - z' - z$. Since M and $M^{\perp}$ are subspaces, $y - y' \in M$ and $z' - z \in M^{\perp}$. But $y - y' = z' - z$.

Therefore, $y - y' \in M \cap M^{\perp}$ and $z' - z \in M \cap M^{\perp}$.

As $M \cap M^{\perp} = \{0\}$ we see $y - y' = 0$ and $z' - z = 0$ i.e. $y = y'$ and $z = z'$.

This is a contradiction as $y' \neq y$ and $z' \neq z$.

Hence the theorem.

We are now in a position to prove Reisz representation theorem.

24.5.4. Theorem. Riesz represntation theorem.

If f is a bounded linear functional on a Hilbert space X, then there is a unique $y \in X$ such that $f(x) = (x, y)$ for every $x \in X$.

Proof. Since f is bounded linear functional, it is continuous.

Let M denote the kernel of f i.e. $M = \{x \in X : f(x) = 0\}$.

Hence M is a closed subspace of X.

If $M = X$, then $f(x) = 0$ for all $x \in X$. Thus we have $f(x) = 0 = (x, 0)$ for every $x \in X$. This proves the theorem.

If $M \neq X$, there exist $x' \in X - M$ and $M^{\perp} \neq \{0\}$. For this x' we have by Theorem 24.5.3 unique $y \in M$ and $z \in M^{\perp}$ such that $x' = y + z$. Since $z \notin M$ we have $f(z) \neq 0$.

Let x be any element of X.

Then we have as $f(z) \neq 0$

$$f\left(x - \frac{f(x)}{f(z)} z\right) = f(x) - \frac{f(x)}{f(z)} f(z) = f(x) - f(x) = 0$$

Therefore $x - \frac{f(x)}{f(z)} z \in M$. Since $z \in M^{\perp}$ we have

$$\left(x - \frac{f(x)}{f(z)} z, z\right) = 0$$

or, $(x, z) - \frac{f(x)}{f(z)} (z, z) = 0$

or, $f(x)\,(z, z) = f(z)\,(x, z)$

or, $f(x) = \frac{f(z)(x, z)}{(z, z)}$

or, $f(x) = \frac{f(z)}{\|z\|^2} (x, z)$

or, $f(x) = \left(x, \frac{\overline{f(z)}}{\|z\|^2} z\right)$

or, $f(x) = (x, y)$ where $y = \frac{\overline{f(z)}}{\|z\|^2} z$

Thus $f(x) = (x, y)$ for every $x \in X$.

If possible let there exists $y' (\neq y)$ such that $f(x) = (x, y')$ for every $x \in X$. Then $(x, y) = (x, y')$ for every $x \in X$

or, $(x, y-y')=0$ for every $x \in X$.

choosing $x = y-y'$ we have $(y-y', y-y')=0$ i.e. $y-y'=0$

i.e. $y = y'$. This is a contradiction as $y' \neq y$.

Hence the representation is unique. This completes the proof of the theorem.

24.6. Bounded Linear Operators on Hilbert Space

There are remarkable results relating bounded linear operators in Hilbert spaces. We shall first prove a theorem on the basis of which adjoint operator is defined. This theorem is an outcome of direct application of the Riesz representative theorem.

Let $B(X)$ be the set of all bounded linear operators from a Hilber space X to itself.

24.6.1. Theorem. If $T \in B(X)$ then there exists $S \in B(X)$ such that

$(Tx, y) = (x, Sy)$ for all $x, y \in X$.

Proof. For a fixed $y \in X$, we define the functional $\phi : X \to C$ by $\phi(x) = (Tx, y)$ for all $x \in X$.

Now for $x_1, x_2 \in X$ and $\lambda_1, \lambda_2 \in C$ we have

$$\begin{aligned}\phi(\lambda_1 x_1 + \lambda_2 x_2) &= (T(\lambda_1 x_1 + \lambda_2 x), y) \\ &= (\lambda_1 Tx_1 + \lambda_2 Tx_2, y) \quad [\because T \text{ is linear}] \\ &= \lambda_1 (Tx_1, y) + \lambda_2 (Tx_2, y) \\ &= \lambda_1 \phi(x_1) + \lambda_2 \phi(x_2)\end{aligned}$$

This shows that ϕ is linear.

Again, $|\phi(x)| = |(Tx, y)|$

$\leq \|Tx\| \|y\|$ [by Cauchy Schwarz inequality]

$\leq \|T\| \|x\| \|y\|$ [$\because T$ is bounded and linear]

$\therefore |\phi(x)| \leq M \|x\|$ for all $x \in X$ where $M = \|T\| \|y\|$.

Thus $\phi : X \to C$ is a bounded linear functional on X.

Therefore, by Riesz representation theorem, there exists a unique $z \in X$, such that $\phi(x) = (x, z)$ for all $x \in X$.

This process gives a unique z corresponding to fixed y of X.

i.e. this process defines an operator, say S, such that $Sy = z$.

Hence for all $x, y \in X$ we have

$$(Tx, y) = (x, Sy) \qquad \text{..... (1)}$$

We now show that this $S : X \to X$ is linear.

For $y_1, y_2 \in X$ and $\lambda_1, \lambda_2 \in C$ we have

$$\begin{aligned}(x, S(\lambda_1 y_1 + \lambda_2 y_2)) &= (Tx, \lambda_1 y_1 + \lambda_2 y_2) \\ &= \bar{\lambda}_1 (Tx, y_1) + \bar{\lambda}_2 (Tx, y_2) \\ &= \bar{\lambda}_1 (x, Sy_1) + \bar{\lambda}_2 (x, Sy_2) \\ &= (x, \lambda_1 Sy_2) + (x, \lambda_2 Sy_2) \\ &= (x, \lambda_1 Sy_1 + \lambda_2 Sy_2)\end{aligned}$$

or, $(x, S(\lambda_1 y_1 + \lambda_2 y_2) - \lambda_1 Sy_1 - \lambda_2 Sy_2) = 0.$

This is true for all $x \in X$. Hence taking

$x = S(\lambda_1 y_1 + \lambda_2 y_2) - \lambda_1 Sy_1 - \lambda_2 Sy_2$ it follows that

$S(\lambda_1 y_1 + \lambda_2 y_2) - \lambda_1 Sy_1 - \lambda_2 Sy_2 = 0$

i.e. $S(\lambda_1 y_1 + \lambda_2 y_2) = \lambda_1 Sy_1 + \lambda_2 Sy_2.$

Therefore, S is linear. We now show that S is bounded.

In (1) putting $x = Sy$ we have

$$(TSy, y) = (Sy, Sy)$$

or, $\|Sy\|^2 = (T(Sy), y)$

$\leq \|T(Sy)\| \|y\|$ [by Cauchy Schwarz inequality]

$\leq \|T\| \|Sy\| \|y\|$ [as T is bounded linear]

$\therefore \|Sy\| \leq \|T\| \|y\|$ for all $y \in X$.

Hence $S : X \to X$ is a bounded linear operator i.e. $S \in B(X)$.

If possible, let there be another $S' \in B(X)$ such that $(Tx, y) = (x, S'y)$ for all $x, y \in X$.

Then we have

$(x, Sy) = (x, S'y)$ for all $x, y \in X$

or, $(x, Sy - S'y) = 0$ for all $x, y \in X$.

Choosing $x = Sy - S'y$ we have

$(Sy - S'y, Sy - S'y) = 0$ for all $y \in X$

$\Rightarrow Sy - S'y = 0$ for all $y \in X$

$\Rightarrow Sy - S'y$ for all $y \in X$

$\Rightarrow S = S'$

This is a contradiction. Hence S is unique.

This completes the proof.

24.6.2. Definition Adjoint Operator

Let $T \in B(X)$. The there exists a unique $T^* \in B(X)$ such that $(Tx, y) = (x, T^*y)$ for all $x, y \in X$. This T^* is called the adjoint of T.

The following theorem gives some properties of adjoint operators.

24.6.3. Theorem. For $T, T_1, T_2 \in B(X)$ and $\lambda \in C$ the following properties are true

i) $(T_1 + T_2)^* = T_1^* + T_2^*$

ii) $(\lambda T)^* = \bar{\lambda} T^*$

iii) $(T_1, T_2)^* = T_2^* T_1^*$

iv) $T^{**} = (T^*)^* = T$

v) $\|T^*\| = \|T\|$

vi) $\|T^* T\| = \|T\|^2$

Proof. We first note that if $(x, y) = (x, z)$ for all $x, y, z \in X$ then $y = z$. This is proved as follows

$$(x, y) = (x, z)$$
$$\Rightarrow (x, y) - (x, z) = 0$$
$$\Rightarrow (x, y - z) = 0$$

As this is true for all x, choosing $x = y - z$ we get $(y - z, y - z) = 0$

This implies that $y - z = 0$ or, $y = z$.

i) For any $x, y \in X$ we have

$$\begin{aligned}\left(x, (T_1 + T_2)^* y\right) &= \left((T_1 + T_2)x, y\right) \\ &= (T_1 x + T_2 x, y) \\ &= (T_1 x, y) + (T_2 x, y) \\ &= \left(x, T_1^* y\right) + \left(x, T_2^* y\right) \\ &= \left(x, T_1^* y + T_2^* y\right) \\ &= \left(x, \left(T_1^* + T_2^*\right) y\right).\end{aligned}$$

This is true for any $x, y, \in X$. Hence $(T_1 + T_2)^* y = \left(T_1^* + T_2^*\right) y$.

This is true for all $y \in X$.

Therefore, $(T_1 + T_2)^* = T_1^* + T_2^*$

ii) For any $x \in X$ and $\lambda \in C$ we have

$$\begin{aligned}\left(x, (\lambda T)^* y\right) &= \left((\lambda T)x, y\right) \\ &= \lambda (Tx, y) \\ &= \lambda \left(x, T^* y\right) \\ &= \left(x, \bar{\lambda} T^* y\right)\end{aligned}$$

Therefore $(\lambda T)^* y = \bar{\lambda} T^* y = \left(\bar{\lambda} T^*\right) y$. This is true for all $y \in X$.

Hence $(\lambda T)^* = \bar{\lambda} T^*$

iii) For any $x, y \in X$. we have

$$\begin{aligned}\left(x,(T_1T_2)^* y\right) &= \left((T_1T_2)x, y\right)\\ &= \left(T_1(T_2x), y\right)\\ &= \left(T_2x, T_1^* y\right)\\ &= \left(x, T_2^*\left(T_1^* y\right)\right)\\ &= \left(x, T_2^*T_1^* y\right)\end{aligned}$$

This is true for all $x, y, \in X$. Therefore $\left(T_1T_2\right)^* y = \left(T_1^*T_2^*\right)y$. This is true for all $y \in X$.

Hence $\left(T_1T_2\right)^* = T_2^*T_1^*$

iv) For $x, y, \in X$, we have

$$\begin{aligned}\left(x, T^{**}y\right) &= \left(x, \left(T^*\right)^* y\right)\\ &= \left(T^*x, y\right)\\ &= \left(\overline{y, T^*x}\right)\\ &= \left(\overline{Ty, x}\right)\\ &= (x, Ty)\end{aligned}$$

This is true for all $x, y, \in X$. So $T^{**}y = Ty$.. This is true for all $y \in X$.

Hence $T^{**} = T$.

v) For any $x, y, \in X$ we have

$(Tx, y) = \left(x, T^*y\right)$.

Putting $x = T^*y$ we get,

$$\left(T\left(T^*y\right), y\right) = \left(T^*y, T^*y\right)$$

or, $$\left(T^*y, T^*y\right) = \left(T\left(T^*y\right), y\right)$$

or, $$\left\|T^*y\right\|^2 \le \left\|T\left(T^*y\right)\right\|\|y\|$$ [by Cauchy Schwarz inequality]

or, $\|T^*y\|^2 \le \|T\| \|T^*y\| \|y\|$ [$\because$ T is bounded and linear]

or, $\|T^*y\| \le \|T\| \|y\|$

or, $\|T^*\| \le \|T\|$ ..... (1)

Again

$T = T^{**}$

$\therefore \|T\| = \|T^{**}\|$

or, $\|T\| = \|(T^*)^*\|$

or, $\|T\| \le \|T^*\|$ [using (1)] ..... (2)

From (1) and (2) we have $\|T^*\| = \|T\|$

vi) For $T, T^* \in B(X)$ and $x \in X$ we have

$\|(T^*T)x\|$

$= \|T^*(Tx)\|$

$\le \|T^*\| \|Tx\|$ [$\because$ T^* is bounded and linear]

$\le \|T^*\| \|T\| \|x\|$ [$\because$ T is bounded and linear]

Hence $\|T^*T\| \le \|T^*\| \|T\|$

But $\|T^*\| = \|T\|$. Therefore,

$\|T^*T\| \le \|T\|^2$ ..... (1)

For $x \in X$ we have

$\|Tx\|^2 = (Tx, Tx)$

$= (x, T^*Tx)$

$\le \|x\| \|T^*Tx\|$ [by Cauchy Schwarz inequality]

$= \|x\| \|(T^*T)x\|$

$$\leq \|x\| \left\|(T^*T)\right\| \|x\|$$

$$\therefore \|Tx\|^2 \leq \left\|T^*T\right\| \|x\|^2$$

or, $\|Tx\| \leq \left\|T^*T\right\|^{1/2} \|x\|$

Hence $\|T\| \leq \left\|T^*T\right\|^{1/2}$

or, $\|T\|^2 \leq \left\|T^*T\right\|$ ..... (2)

From (1) and (2) $\|T\|^2 = \left\|T^*T\right\|$

This completes the proof.

Some important operators are defined below.

24.6.4. Definitions. Let $T \in B(X)$. Then

i) T is called self adjoint or hermitian if $T = T^*$

ii) T is called normal if $T^*T = TT^*$

iii) T is called unitary if $T^*T = TT^* = I$ (identity operator)

iv) T is called positive operator if $(Tx, x) \geq 0$ for all $x \in X$

We now prove some theorems relating the above defined operators.

24.6.5. Theorem. For any $T \in B(X), T^*T$ is a positive operator.

Proof. For $x \in X$ we have

$$\left(T^*Tx, x\right) = \left(T^*\left(Tx\right), x\right) = \left(Tx, Tx\right) = \|Tx\|^2 \geq 0$$

Hence T^*T is a positive operator.

24.6.6. Theorem. The operator $T \in (B)(X)$ is self adjoint if and only if (Tx, x) is a real number for every $x \in X$. In particular, every positive operator is self adjoint.

Proof. Let T be self adjoint i.e. $T^* = T$.

Then for any $x \in X$ we have

$$(Tx, x) = (x, T^* x)$$

$$= (x, Tx) \left[\because T^* = T\right]$$

$$= \overline{(Tx, x)}$$

Hence (Tx, x) is a real number.

Conversely, let (Tx, x) be a real number for every $x \in X$.

We have

$$(T(x+y), x+y) - (T(x-y), x-y) + i(T(x+iy), x+iy) - i(T(x-iy), x-iy)$$

$$= (Tx, x) + (Tx, y) + (Ty, x) + (Ty, y)$$

$$- (Tx, x) + (Tx, y) + (Ty, x) - (Ty, y)$$

$$+ i[(Tx, x) + (Tx, iy) + (T(iy), x) + (Tiy, iy)]$$

$$- i[(Tx, x) - (Tx, iy) + (T(iy), x) + (Tiy, iy)]$$

$$= 2(Tx, y) + 2(Ty, x)$$

$$+ i(Tx, x) + i \cdot \bar{i}(Tx, y) + i^2 (Ty, x) + i \cdot (Ty, y)$$

$$- i(Tx, x) + i\bar{i}(Tx, y) + i^2 (Ty, x) - i \cdot (Ty, y)$$

$$= 4(Tx, y)$$

i.e. $(T(x+y), x+y) - (T(x-y), x-y) + i(T(x+iy), x+iy) - i(T(x-iy), x-iy) = 4(Tx, y)$ ..... (1)

Taking conjugate and noting that (Tx, x) is real for all $x \in X$ i.e. $\overline{(Tx, x)} = (Tx, x)$ for all $x \in X$ we have

$$(T(x+y), (x+y)) - (T(x-y), (x-y)) - i(T(x+iy), x+iy)$$

$$+ i(T(x-iy), x-iy) = 4\overline{(Tx, y)} = 4(y, Tx)$$

Interchanging x and y we get

$$(T(y+x), y+x) - (T(y-x), y-x) - i(T(y+ix), y+ix) + i(T(y-ix), y-ix) = 4(x, Ty)$$

or, $(T(x+y), x+y) - (T(x-y), x-y) - i(iT(x-iy), i(x-iy)) + i(-iT(x+iy), -i(x-iy)) = 4(x, Ty)$

or, $(T(x+y),x+y)-(T(x-y),x-y)-i\cdot i\,\overline{i}\,(T(x-iy),x-iy)$

$$+i(-i)\overline{(-i)}(T(x+iy),x+iy)=4(x,Ty)$$

or, $(T(x+y), x+y) - (T(x-y), x-y) - i\,(T(x-iy), x-iy) + i\,(T(x+iy), x+iy) = 4(x, Ty)$ ..... (2)

From (1) and (2) we see that

$(Tx, y) = (x, Ty)$ for all $x, y \in X$.

This shows that $T = T^*$ and therefore T is self-adjoint.

24.6.7. Theorem. If T_1 and T_2 are self adjoint, then T_1T_2 is self adjoint if and only if $T_1T_2 = T_2T_1$

Proof. Let T_1 and T_2 be self adjoint i.e.

$$T_1^* = T_1 \text{ and } T_2^* = T_2 \qquad \text{..... (1)}$$

We first assume that T_1T_2 is self adjoint

i.e. $(T_1T_2)^* = T_1T_2$

From this we have

$$T_2^*T_1^* = T_1T_2$$

or, $T_2T_1 = T_1T_2$ [by (1)].

Now we assume that

$$T_2T_1 = T_1T_2$$

Using (1) we get from this

$$T_2^*T_1^* = T_1T_2$$

or, $(T_1T_2)^* = T_1T_2$

i.e. T_1T_2 is self adjoint.

This completes the proof of the theorem.

24.6.8. Theorem. If T_1 and T_2 are normal operators such that each commutes with the adjoint of the other, then T_1+T_2 and T_1T_2 are normal.

Proof. We have $T_1T_1^* = T_1^*T_1$ and $T_2T_2^* = T_2^*T_2$ ..... (1)

$T_1^*T_2 = T_2T_1^*$ and $T_1T_2^* = T_2^*T_1$ ..... (2)

We are to show that and T_1+T_2 and T_1T_2 are normal.

Now $(T_1+T_2)(T_1+T_2)^*$

$= (T_1+T_2)(T_1^*+T_2^*)$

$= T_1T_1^* + T_1T_2^* + T_2T_1^* + T_2T_2^*$ ..... (3)

and $(T_1+T_2)^*(T_1+T_2)$

$= (T_1^*+T_2^*)(T_1+T_2)$

$= T_1^*T_1 + T_1^*T_2 + T_2^*T_1 + T_2^*T_2$

$= T_1T_1^* + T_2T_1^* + T_1T_2^* + T_2T_2^*$ [by (1) and (2) ..... (4)

From (3) and (4) we have

$(T_1+T_2)(T_1+T_2)^* = (T_1+T_2)^*(T_1+T_2)$

i.e. T_1+T_2 as normal.

Again,

$(T_1T_2)(T_1T_2)^*$

$= T_1T_2\,T_2^*T_1^*$

$= T_1(T_2T_2^*)T_1^*$

$= T_1(T_2^*T_2)T_1^*$ [by (1)]

$= (T_1T_2^*)(T_2T_1^*)$

$= (T_2^*T_1)(T_1^*T_2)$ [by (2)]

$= T_2^*(T_1T_1^*)T_2$

$= T_2^*(T_1^*T_1)T_2$ [by (1)]

$= (T_2^*T_1^*)(T_1T_2)$

$= (T_1T_2)^*(T_1T_2)$

Hence T_1T_2 is normal.

24.6.9. Theorem. If $T \in B(X)$ is such that $(Tx, x) = 0$ for all x, then $T = 0$.

Proof. For any $x, y \in X$ and $\alpha, \beta \in C$ we have by hypothesis

$$(T(\alpha x + \beta y), \alpha x + \beta y) - |\alpha|^2 (Tx, x) - |\beta|^2 (Ty, y) = 0$$

or, $$(\alpha Tx + \beta Ty, \alpha x + \beta y) - |\alpha|^2 (Tx, x) - |\beta|^2 (Ty, y) = 0$$

or, $$\alpha\bar{\alpha}(Tx, x) + \alpha\bar{\beta}(Tx, y) + \beta\bar{\alpha}(Ty, x) + \beta\bar{\beta}(Ty, y) - |\alpha|^2 (Tx, x) - |\beta|^2 (Ty, y) = 0$$

or, $$|\alpha|^2 (Tx, x) + \alpha\bar{\beta}(Tx, y) + \beta\bar{\alpha}(Ty, x) + |\beta|^2 (Ty, y) - |\alpha|^2 (Tx, x) - |\beta|^2 (Ty, y) = 0$$

or, $$\alpha\bar{\beta}(Tx, y) + \bar{\alpha}\beta(Ty, x) = 0$$

If $\alpha = 1, \beta = 1$, we get $(Tx, y) + (Ty, x) = 0$ ..... (1)

If $\alpha = i, \beta = 1$, we get $i(Tx, y) - i(Ty, x) = 0$

or, $(Tx, y) - (Ty, x) = 0$ ..... (2)

Adding (1) and (2) we have $2(Tx, y) = 0$

or $(Tx, y) = 0$

This is true for all $x, y \in X$. Taking $y = Tx$ we have

$(Tx, Tx) = 0$ for all $x \in X$

i.e. $Tx = 0$ for all $x \in X$

i.e. $T = 0$.

This completes the proof.

24.6.10. Theorem. $T \in B(X)$ is normal if and only if $\|T^*x\| = \|Tx\|$ for all $x \in X$

Proof. Let $\|T^*x\| = \|Tx\|$ for all $x \in X$

$$\therefore \|T^*x\|^2 = \|Tx\|^2 \text{ for all } x \in X$$

or, $$(T^*x, T^*x) = (Tx, Tx) \text{ for all } x \in X$$

or, $$(TT^*x, x) = (T^*Tx, x) \text{ for all } x \in X$$

or, $$((TT^* - T^*T)x, x) = 0 \text{ for all } x \in X$$

or, $TT^* - T^*T = 0$

or, $TT^* = T^*T$

Hence T is normal.

Again let T be normal i.e. $TT^* = T^*T$

Therefore, $TT^* - T^*T = 0$

$\therefore (TT^* - T^*T)x = 0x$ for all $x \in X$

or, $(TT^* - T^*T)x = 0$ for all $x \in X$.

So $((TT^* - T^*T)x, x) = (o, x) = 0$ for all $x \in X$

or, $(TT^*x - T^*Tx, x) = 0$ for all $x \in X$

or, $(TT^*x, x) - (T^*Tx, x) = 0$ for all $x \in X$

or, $(TT^*x, x) = (T^*Tx, x)$ for all $x \in X$

or, $(T^*x, T^*x) = (Tx, Tx)$ for all $x \in X$

or, $\|T^*x\|^2 = \|Tx\|^2$ for all $x \in X$

or, $\|T^*x\| = \|Tx\|$ for all $x \in X$.

Hence the theorem.

24.6.11. Theorem. If $T \in B(X)$ is normal then $\|T\|^2 = \|T^2\|$

Proof. We known the result that if T is normal then

$$\|T^*x\| = \|Tx\| \text{ for all } x \in X \qquad \ldots\ldots\ldots\ldots (1)$$

Let T be normal.

Then taking x as Tx we have from (1)

$$\|T^*(Tx)\| = \|T(Tx)\|$$

or, $\|(T^*T)x\| = \|T^2x\|$

$\therefore \sup_{\|x\|=1} \|(T^*T)x\| = \sup_{\|x\|=1} \|T^2x\|$

or, $\|(T^*T)\| = \|T^2\|$

or, $\|T\|^2 = \|T^2\|$ [by Theorem 24.6.3.]

This completes the proof of the theorem.

24.7. Illustrative Examples

24.7.1. Example : Let X be a normed linear space and let F denote C or R. Then the mappings $T : X \times X \to X$ and $T' : F \times N \to N$ defined by $T(x,y) = x + y$ and $T'(\alpha, x) = \alpha x$ are continuous.

In other words the vector addition and scalar multiplication are continuous.

Solution : Let $\{x_n\}$ and $\{y_n\}$ be sequences in X and $\{\alpha_n\}$ a sequence in F such that

$x_n \to x, y_n \to y, \alpha_n \to \alpha$ as $n \to \infty$ where $x \in X, y \in X$ and $\alpha \in F$ ..... (1)

Now $\|T(x_n, y_n) - T(x,y)\|$

$= \|(x_n + y_n) - (x + y)\|$

$\leq \|x_n - x\| + \|y_n - y\|$

$\to 0$ as $n \to \infty$ [by (1)]

Hence $T(x_n, y_n) \to T(x,y)$ as $n \to \infty$

Again $\|T'(\alpha_n, x_n) - T'(\alpha, x)\|$

$= \|\alpha_n x_n - \alpha x\|$

$= \|\alpha_n x_n - \alpha_n x + \alpha_n x - \alpha x\|$

$= \|\alpha_n (x_n - n) + (\alpha_n - \alpha) x\|$

$\leq |\alpha_n| \|x_n - x\| + |\alpha_n - \alpha| \|x\|$

$\to 0$ as $n \to \infty$ [by (1)]

Hence shows that T and T' are continuous.

24.7.2. Example. Let X and Y be normed linear spaces and let $T : X \to Y$ be a linear continuous transformation. Show that the Kernel of T is a closed linear subspace.

Solution : The Kernel of T is defined as

$$Ker(T) = \{x : x \in X, Tx = 0\}$$

Let $x, y \in Ker(T)$ and α, β be scalars.

Then $Tx = 0$ and $Ty = 0$.

Now $T(\alpha x + \beta y) = \alpha Tx + \beta y$ [as T is linear]

$$= \alpha 0 + \beta 0$$

$$= 0$$

$$\therefore \alpha x + \beta y \in Ker(T).$$

This shows that $Ker(T)$ is a linear subspace of X.

We now show that $Ker(T)$ is closed.

Let x be any limit point of $Ker(T)$. Then there exists a sequence $\{x_n\}$ in $Ker(T)$ such that $x_n \to x$ as $n \to \infty$.

Since T is continuous we have $Tx_n \to Tx$ as $n \to \infty$.

But $Tx_n = 0$ for all n. So $Tx = 0$ i.e. $x \in Ker(T)$

Hence $Ker(T)$ is closed.

Thus $Ker(T)$ is a closed linear subspace of X.

24.7.3. Example

Let S be a non-empty subset of a Hilbert space X. Then the orthogonal complement $S^{\perp}$ is a closed linear subspace of X.

Solution. By definition we have $S^{\perp} = \{x \in X : (x, y) = 0 \text{ for all } y \in S\}$

Since $(0, y) = 0$ for all $y \in S$, we have $0 \in S^{\perp}$ i.e. $S^{\perp}$ is non empty.

Let $x_1, x_2 \in S^{\perp}$ and α, β be be scalars.

Then $(x_1, y) = 0$ and $(x_2, y) = 0$ for all $y \in S$.

We have $(\alpha x_1 + \beta x_2, y) = \alpha(x_1, y) + \beta(x_2, y) = \alpha \cdot 0 + \beta \cdot 0 = 0$

Therefore $\alpha x_1 + \beta x_2 \in S^{\perp}$. Hence $S^{\perp}$ is a subspace of X.

Now we show that $S^{\perp}$ is closed.

Let x be any limit point of $S^{\perp}$. Then there exists a sequence $\{x_n\}$ in $S^{\perp}$ such that $x_n \to x$ as $n \to \infty$.

Since $x_n \in S^{\perp}$ for all n, we have $(x_n, y) = 0$ for all n.

We know that inner product is a continous mapping.

So $\lim_{n\to\infty}(x_n, y) = \left(\lim_{n\to\infty} x_n, y\right)$

or, $\lim_{n\to\infty} 0 = (x, y)$

or, $(x, y) = 0$. This is true for all $y \in S$.

Hence $x \in S^{\perp}$.

This shows that $S^{\perp}$ is closed linear subspace of X.

24.7.4. Example. If M_1, M_2 are non-empty subsets of a Hilbert space X and $M_1 \subset M_2$ then $M_2^{\perp} \subset M_1^{\perp}$.

Solution. Here $M_1 \subset M_2$. Let x be any element of $M_2^{\perp}$.

Now $x \in M_2^{\perp}$

$\Rightarrow x$ is orthogonal to every element in M_2

$\Rightarrow x$ is orthogonal to every element in M_1 as $M_1 \subset M_2$

$\Rightarrow x \in M_1^{\perp}$

Therefore $M_2^{\perp} \subset M_1^{\perp}$.

24.7.5. Example. Prove that an orthonormal set in a Hilbert space is linearly independent.

Solution. Let $\{e_1, e_2, ..., e_n\}$ be any orthonormal set in the Hilbert space X.

Then $(e_i, e_j) = 0$ for all $i \neq j$.

$= 1$ for $i = j$ ..... (1)

Let $\sum_{j=1}^{n} \alpha_j e_j = 0$. ..... (2)

For any k, where $1 \le k \le n$, we have

$$\left(\sum_{j=1}^{n} \alpha_j e_j, e_k\right)$$

$$= \sum_{j=1}^{n} (\alpha_j e_j, e_k)$$

$$= \sum_{j=1}^{n} \alpha_j (e_j, e_k)$$

$= \alpha_k$ [by (1)]

Again using (2) we have $\left(\sum_{j=1}^{n} \alpha_j e_j, e_k\right) = (0, e_k) = 0$

Hence $\alpha_k = 0$. This is true for all $k = 1, 2, ..., n$. This shows that $\{e_1, e_2, ...e_n\}$ are linearly independent.

24.7.6. Example. Show that in an inner product space, $x \perp y$ if and only if we have $\|x + \lambda y\| = \|x - \lambda y\|$ for all scalars λ.

Solution. Let $\|x + \lambda y\| = \|x - \lambda y\|$ for all scalars λ.

Then $\|x + \lambda y\|^2 = \|x - \lambda y\|^2$

or, $(x + \lambda y, x + \lambda y) = (x - \lambda y, x - \lambda y)$

or, $(x,x) + \bar{\lambda}(x,y) + \lambda(y,x) + \lambda\bar{\lambda}(y,y) = (x,x) - \bar{\lambda}(x,y)$

$$-\lambda(y,x) + \lambda\bar{\lambda}(y,y)$$

or, $2\bar{\lambda}(x,y) + 2\lambda(y,x) = 0$

or, $\bar{\lambda}(x,y) + \lambda\overline{(x,y)} = 0$

This is true for all λ. Taking $\lambda = (x,y)$ we have

$$\overline{(x,y)}(x,y) + (x,y)\overline{(x,y)} = 0$$

or, $(x,y)\overline{(x,y)} = 0$

or, $|(x,y)|^2 = 0$

or, $|(x,y)| = 0$

or, $(x,y) = 0$

or, $x \perp y$.

Conversely, let $x \perp y$ i.e. $(x,y) = 0$.

Then for any λ we have

$$\|x+\lambda y\|^2 - \|x-\lambda y\|^2$$

$$= (x,x) + \bar{\lambda}(x,y) + \lambda(y,x) + \lambda\bar{\lambda}(y,y) = (x,y) - \bar{\lambda}(x,y) + \lambda(y,x) - \lambda\bar{\lambda}(y,y)$$

$$= 2\bar{\lambda}(x,y) + 2\lambda(y,x)$$

$$= 0 + 0$$

$$= 0$$

or, $\|x+\lambda y\|^2 = \|x-\lambda y\|^2$

or, $\|x+\lambda y\| = \|x-\lambda y\|$.

24.8. Summary

Inner product space is the most natural generalization of Euclidean space. In this module we have studied many important theorems and properties of inner product space. The main concept of *ips* is the orthogonal concept. The Riesz representation theorem and the generalization of Pythagorean theorem have been studied. Properties of bounded linear operators on Hilbert space have been discussed. Finally, theorems relating to adjoint of bounded linear operator have been studied. Examples are given to have a clear concept and notion of this important space.

24.9. Self Assessment Questions.

1. In the space of all complex numbers, show that $(z_1, z_2) = z_1\bar{z}_2$ defines an inner product.
2. Prove the Appollonius identity

$$\|z-x\|^2 + \|z-y\|^2 = \frac{1}{2}\|x-y\|^2 + 2\left\|z - \frac{1}{2}(x+y)\right\|^2$$

in an innder product space by direct calculation and also by parallelogram law.

3. If $\|x+\lambda y\| = \|x-\lambda y\|$ is true for all scalar λ then show that $x \perp y$. Interprete the result geometrically. Is the converse true?
4. If in an inner product space $(x, u) = (x, v)$ for all x, show that $u = v$.
5. Show that $x \perp y_n$ for all n and $x_n \to x$ as $n \to \infty$ together imply $x \perp y$.
6. Show that for a sequence $\{x_n\}$ in an inner product space the conditions $\|x_n\| \to \|x\|$ and $(x_n, x) \to (x, x)$ imply convergence $x_n \to x$.
7. Let $T : X \to X$ be a bounded linear operator on a complex inner product space X. If $(Tx, x)=0$ for all $x \in X$, show that $T = 0$. Show that this result is not true in the case of real inner product space.
8. Show that the space $C[a, b]$ is a Banach space but not a Hilbert space.

   Hints: For $x = x(t) = 1$, $y = y(t) = \dfrac{t-a}{b-a}$ parallelogram law does not hold.
9. Let X denote the space of all real valued continuous functions on $[0, 2\pi]$. Show that X is an *ips* with inner product defined by $(x, y) = \int_0^{2\pi} x(t)y(t)dt$. Show also that $\{e_n(t)\}$ where $e_0(t) = \dfrac{1}{\sqrt{2\pi}}$ and $e_n(t) = \dfrac{\cos nt}{\sqrt{\pi}}, n = 1, 2, \ldots$ is an orthonormal sequence in X.
10. Let x, y be non zero elements of a Hilbert space X. Show that $\|x+y\| = \|x\| + \|y\|$ holds if and only if $y = \lambda x$ where λ is a scalar.
11. If X is a real inner product space and if $\|x+y\|^2 = \|x\|^2 + \|y\|^2$ then show that $x \perp y$. Show further that this is not necessarily true in a complex *ips*.

24.10. Suggested Books for further reading :

1. Introductory Functional Analysis with Applications: Erwin Kreyszig; John Wiley & Sons
2. Functional Analysis with Applications : B. Choudhary and Sudarsan Nanda; Wiley Eastern Limited
3. Elements of Functional Analysis : B.K. Lahiri; World Press
4. Introduction to Functional Analysis for Scientists and Technologists: B.Z. Vulikh; Pergamon Press
5. Functional Analysis : J.N. Sharma & A.R. Vasishtha; Krishna Prakashan Mandir.

---- 0 ----

"Learner's Feed-back"

After going through the Modules / Units please answer the following questionnaire.
Cut the portion and send the same to the Directorate.

To
The Director
Directorate of Distance Education,
Vidyasagar University
Midnapore - 721 102

1. The modules are : (give ✓ in appropriate box)
   ☐ easily understandable; ☐ very hard; ☐ partially understandable.

2. Write the number of the Modules/Units which are very difficult to understand :
   .....
   .....
   .....

3. Write the number of Modules / Units which according to you should be re-written :
   .....
   .....
   .....

4. Which portion / page is not understandable to you? (mention the page no. and portion)
   .....
   .....
   .....
   .....

5. Write a short comment about the study material as a learner.
   .....
   .....
   .....
   .....
   .....

.....
(Full Signature of the Learner)

Date : .....

Enrolment No. .....

Phone / Mobile No. .....


BINOY BADAL DINESH BHAVAN
DIRECTORATE OF DISTANCE EDUCATION