CHAPTER 8

Graphs

1. Introduction

Graph Theory is a fast growing branch of Mathematics, having its place in several branches of Mathematics, and also of Science, Engineering, Chemistry, Defence etc. In computer engineering it is an unavoidable tool having applications in switching theory, artificial intelligence, computer graphics etc.

For us a graph is different from what you have in mind since school-days. A graph consists of two things vertices and edges. We shall denote the vertices by $v_1, v_2, \ldots$ and edges by $e_1, e_2, \ldots$ and their sets by capital letters V and E. Every edge corresponds to a pair of vertices. We denote this as $e_1 = \{v_1, v_2\}$, $e_2 = \{v_2, v_3\}$ etc.

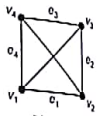


Fig. 8.1

In this chapter we shall first define and illustrate the following terms.

(1) Graph, (2) Vertex, node, point, (3) Edge, curve, line,
(4) Loop, (5) Parallel edges multiple edges, (6) Simple graph,
(7) Multiple graph, (8) Adjacent vertices, (9) Incident edge,
(10) Degree of a vertex, (11) Pendant vertex, (12) Pendant edge.

Then we shall prove some interesting theorems about graphs and shall then define special types of graphs viz.

(1) Complete graph, (2) Regular graph, (3) Planar graph.

2. Basic Terms

Definition 1 : A graph is an ordered pair (V, E) of two sets V and E satisfying the following conditions :

(i) V is a finite non-empty set.

(ii) each $e \in E$ corresponds to a unique unordered pair v_1, v_2 of elements of V.

(M.U. 1998)

Definition 2 : The elements of the set V are called **vertices** of the graph (V, E). A vertex is also referred to as a **node** or a **point**.

Definition 3 : The elements of E are called **edges**. An edge is also referred to as a **curve** or a **line**.

Definition 4 : If an edge starts and ends in the same vertex then it is called a **loop** (or a self loop).

In the graph shown in Fig. 8.2, G_1, e_1 is a loop.

Definition 5 : If two edges have the same starting vertex and the same end vertex they are called **parallel edges or multiple edges.**

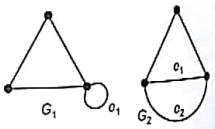


Fig. 8.2

In the above graph G_2, e_1 and e_2 are parallel edges (although they meet at the two ends). It is like joining two cities by two different roads.

Definition 6 : A graph having no loops or parallel edges is called a **simple graph** or (simply) a graph.


Fig. 8.3 (a)

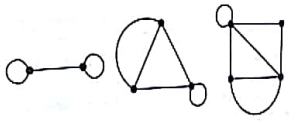


Fig. 8.3 (b)

The graphs shown in Fig. 8.3 (a) are simple graphs. The graphs shown in Fig. 8.3 (b) are not simple graphs.

Example 1 : Prove that in a simple graph having n vertices, there can be at most $n(n-1)/2$ edges.

Sol. : If we are given n vertices, we can join any two of them to get a simple graph. But n vertices can be taken two at a time in ${}^nC_2 = n(n-1)/2$ ways.

Hence, there will be at most $n(n-1)/2$ edges.

In the above graph 8.3 (a), when there are two vertices the number of edges $= 2(2-1)/2 = 1$, when there are three vertices the number of edges $= 3(3-1)/2 = 3$, etc.

Example 2 : Can we have a simple graph with 6 vertices and 16 edges?

Sol. : In a simple graph with 6 vertices there can be at most $6(6-1)/2 = 15$ edges.

Hence, we cannot have a simple graph with 6 vertices and 16 edges.

Example 3 : Show that the maximum degree of any vertex in a simple graph of n vertices is $(n-1)$.

Sol. : Consider a simple graph G (similar to any one shown above in Fig. 8.3 (a)) with n vertices.

As the graph is simple, it has no loops or parallel edges as in graphs of 8.13 (b). Now, consider any vertex of such a simple graph. Each vertex can be adjacent to at most $(n-1)$ vertices. Hence, there will be at most $(n-1)$ edges. Hence, the maximum degree of any vertex is $(n-1)$.

[In Fig. 8.13 (a), In the first graph, there are $(n =)$ two vertices each of degree $((n-1) =) 1$, In the second graph, there are $(n =)$ 3 vertices each of degree $((n-1) =) 2$, In the third graph, there are $(n =)$ 4 vertices each of degree $((n-1) =) 3$.]

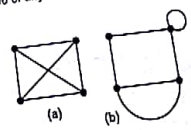


Fig. 8.4

Definition 7 : A graph which is not simple is called a **multigraph.**

In the graphs (Fig. 8.4), G_1 is (a) simple graph and (b) is a multigraph.

3. Adjacency and Incidence

Definition 8 : If there is an edge between two vertices v_1 and v_2 then they are called **adjacent vertices**.

In the graph G, v_1 and v_2, v_2 and v_3 are adjacent vertices but v_1 and v_3, v_2 and v_5 etc. are not adjacent vertices.

Definition 9 : If an edge starts (or ends) from a vertex then the edge is said to be **incident edge** on the vertex.

In the graph shown in Fig. 8.5, the edge e_1 is incident on v_1 or on v_2, the edge e_2 is incident on v_2 or on v_3 etc.

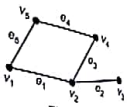


Fig. 8.5

Definition 10 : The number of edges incident (coming or leaving but counted once only) at a vertex is called the **degree** or the **valency** of the vertex. The degree of a vertex v is denoted by $d(v)$.

In the graph G (Fig. 8.5), the degree of the vertex v_1 is 2, of v_2 is 3, of v_4 is 2 and of v_5 is 2.

Definition 11, 12 : If only one edge is incident at a vertex v, then its degree is one and it is called a **pendant vertex** and the corresponding edge is called **pendent edge**.

In a loop, the same edge is incident at v twice; the degree of a loop is **two.**

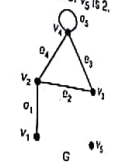


Fig. 8.6

In the graph G, there is no edge incident at v_5 hence v_5 is an isolated vertex; its degree is zero. There is only one edge incident at v_1, hence it is a pendant vertex; its degree is one. The degree of v_3 is two. Since v_4 is a loop and since two more edges are incident at v_4, the degree of v_4 is four.

Theorem 1 (Hand Shaking Lemma) : The sum of degrees of all vertices of any graph is equal to twice number of edges.

Proof : Let $G = (V, E)$ be a graph with m vertices $v_1, v_2, \ldots, v_m$ and n edges $e_1, e_2, \ldots, e_n$ *i.e.*, $V = \{v_1, v_2, \ldots, v_m\}$ and $E = \{e_1, e_2, \ldots, e_n\}$.

If $E = \Phi$ *i.e.* $n = 0$, (See G_1) the degree of each vertex is zero *i.e.*, $d(v_i) = 0$ for all $i = 1, 2, \ldots, m$.

$\therefore \quad \sum d(v_i) = 0.$

The theorem is trivially true.

If $E \neq \Phi$ and if $e \in E$ then e is an edge between two vertices say v_1 and v_2. Clearly, e contributes 1 to $d(v_1)$ and 1 to $d(v_2)$ (See G_2). Thus, each edge contributes precisely '2' to the sum of degrees of all vertices. Since there are n edges in G, the total contribution to the sum of degrees is $2n$.

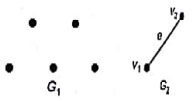


Fig. 8.7

$\therefore \quad \sum d(v_i) = 2n.$

Remark ....

The theorem can also be stated as "The sum of degrees of all vertices of any graph is even".

Note ....

The theorem 1 is also known as **Hand Shaking Lemma.** This is so because if in a party n hard-shakes occur, then as in each handshake two hands are involved, the total number of hands involved in $2n$.

Example : Verify Hand Shaking Lemma for the graph given in Fig. 8.6.

Sol. : In the above graph there are five vertices. $d(v_1) = 1$, $d(v_2) = 3$, $d(v_3) = 2$, $d(v_4) = 4$, $d(v_5) = 0$, and there are ($n =$) 5 edges e_1, e_2, e_3, e_4, e_5.

$\therefore \quad \sum d(v_i) = 1 + 3 + 2 + 4 + 0 = 10$

And $2n = 2(5) = 10$ (n = number of edges). Hence, $\sum d(v_i) = 2n$.

Theorem 2 : In any graph the number of vertices of odd degree is even.

Proof : Let $G = (V, E)$ be a graph. Let $u_1, u_2, \ldots, u_p$ be the vertices of odd degree and $w_1, w_2, \ldots, w_q$ be the vertices of even degree.

We have to show that p is even. Now there are two possibilities $p = 0$, $p \neq 0$.

(i) Let $p = 0$ *i.e.* there is no vertex of odd degree.

But zero is an even integer and hence, the theorem is true.

(See Ex. 1 below)

(ii) Let $p \neq 0$ *i.e.* let there be some vertices of odd degree.

Now, by the above theorem sum of the degrees of all vertices,

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

If we consider p vertices of odd degree and q vertices of even degree separately, then

$$\sum_{i=1}^{n} d(v_i) = \sum_{i=1}^{p} d(u_i) + \sum_{i=1}^{q} d(w_i) = 2n$$

But since $d(w_i)$ is even for each $i = 1, 2, \ldots, q$, then sum, $\sum d(w_i)$ is even. Since the right hand side is even, the first term is also even

$$\therefore \quad \sum_{i=1}^{p} d(u_i) \text{ is even.}$$

But by our supposition $u_1, u_2, \ldots, u_p$ are all odd vertices. If p is odd $\sum_{i=1}^{p} d(u_i)$ (being the sum of odd numbers each of which is odd *e.g.* $3 + 5 + 7 = 15$) will be odd. Hence, $\sum_{i=1}^{p} d(u_i)$ is even is impossible.

Hence, p is even.

Example 1 : Find the number of vertices in a simple graph having n edges and having each vertex of degree 2. **(M.U. 2011, 13, 14)**


Fig. 8.8

Sol. : Since each vertex is of degree 2, from any vertex, we have one edge going out and one edge coming in.

Between two vertices there is only one edge. Since there are thus n edges there will be n vertices.

Example 2 : Find the number of vertices in a simple graph with exactly six edges in which each vertex is of degree 2. **(M.U. 2013, 14)**


Fig. 8.9

Sol. : Let the number of vertices be n. Since each vertex is of degree 2, the sum of the degrees of all vertices = $2n$.

But by theorem 1 above, the sum of degrees of all vertices is equal to twice the number of edges. Since there are by data 6 edges, the sum of the degrees = $2 \times 6 = 12$.

Thus, $2n = 12$ $\therefore$ $n = 6$

Hence, there are 6 vertices. (See Fig. 8.9 on the previous page)

Example 3 : Determine the number of edges in a graph with 6 nodes, 2 of degree 4 and 4 of degree 2. Draw two such graphs. (M.U. 2015)

Sol. : Let there be e edges. Then by theorem 1 above, the sum of degrees of all vertices $= 2e$.

Since there are 2 vertices of degree 4 and 4 vertices of degree 2, the sum of the degree of all vertices

$= (4 \times 2) + (2 \times 4) = 16.$

Hence, $16 = 2e$ $\therefore$ $e = 8$

There will 8 edges in the graph.

Two such graphs are shown in Fig. 8.10.

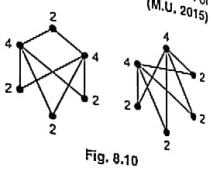


Fig. 8.10

4. Types of Graphs

We shall now consider some special types of graphs.

(1) Complete Graph

Definition : A simple graph of n vertices in which the degree of each vertex is $(n-1)$ is called a **complete graph** and is denoted by K_n.

In other words in a complete graph of n vertices each vertex is connected with any other.

Thus, if $G = (V, E)$ is complete, then

(i) G has no loops.

(ii) G has no multiple edges

(iii) If v_1, v_2 are any two vertices there is precisely one edge between v_1 and v_2.

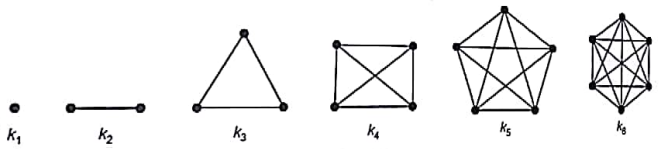


Fig. 8.11

A complete graph with n vertices is denoted by K_n. K stands for completeness and n denotes number of vertices. The above figures show complete graphs K_n for $n = 1, 2, 3, 4, 5, 6$.

A complete graph has the following properties.

Property 1 : Every pair of vertices is adjacent in K_n.

Property 2 : In K_n each vertex has the same degree and that degree is $(n-1)$.

Property 3 : The total number of edges in K_n is $n(n-1)/2$, (where n is the number of vertices).

Proof : Let G be a simple graph with n vertices. Let e be the number of edges in the graph G.

Then by Hand Shaking Lemma

$$d(v_1) + d(v_2) + ... + d(v_n) = 2e$$

But by property (2), (See the previous page) each vertex has the degree $(n-1)$.

$\therefore$ $(n-1) + (n-1) + ... + (n-1) = 2e$

$\therefore$ $n(n-1) = 2e$ $\therefore$ $e = \dfrac{n(n-1)}{2}$

Example 1 : Can a complete graph with 8 vertices have 40 edges excluding self loop. (M.U. 2016)

Sol. : For a complete graph with 8 vertices there are

$\dfrac{8(8-1)}{2} = \dfrac{8 \cdot 7}{2} = 28$ edges.

Hence, there cannot be graph of 8 vertices and 40 edges.

Example 2 : Verify the result that in a complete graph K_m, the number of edges $= n(n-1)/2$ for the graph shown in Fig. 8.10.

Sol. : The above graph is complete because (i) it has no loops, (ii) it has no multiple edges, (iii) each vertex is joined with each of the remaining vertices by a single edge.

Now, there are 10 edges. They are

(1) 4 edges $\{v_1, v_j\}$, $j = 2, 3, 4, 5$

(2) 3 edges $\{v_2, v_j\}$, $j = 3, 4, 5$

(3) 2 edges $\{v_3, v_j\}$, $j = 4, 5$

(4) 1 edges $\{v_4, v_5\}$

Since there are 5 vertices v_1, v_2, v_3, v_4, v_5, $m = 5$.

$\therefore$ Number of edges $= \dfrac{m(m-1)}{2} = \dfrac{5 \times 4}{2} = 10$ as shown.

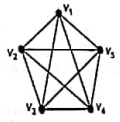
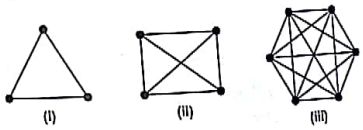


Fig. 8.12

EXERCISE - I

1. Verify that in K_m the number of edges in a graph is $\dfrac{m(m-1)}{2}$ for the following graphs.



(i) (ii) (iii)

2. Find the number of edges in a complete graph with 7 vertices. [Ans. : 21]

3. Find the number of edges in K_{11}. [Ans. : $\dfrac{11 \times 10}{2} = 55$]

(2) Regular Graph

Definition : A graph in which every vertex has the same degree is called a **regular graph**. In other words if the number of edges incident at a vertex is the same, then the graph is called a regular graph. If the common degree of a vertex is r then it is called an r-regular graph or regular graph of degree r.

Clearly, a complete graph of n number of vertices is $(n-1)$-regular graph because in such a graph, we have seen that at each vertex there are $(n-1)$ incident edges. But the converse is not true. A regular graph need not be complete.

The graphs shown below are regular but not complete. In the first and second figure there are two edges incident at each vertex. In the third and fourth figures there are three edges incident at each vertex. In the last figure there are four edges incident at each vertex. But these graphs are not complete because each vertex is not connected with the remaining vertices except (i) and the last is not a simple graph.

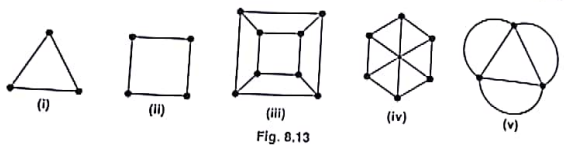


Fig. 8.13

Example 1 : *If r and n are odd natural numbers, then there cannot be an r-regular graph of n vertices.*

Sol. : *If possible let there be an r-regular graph $G = (V, E)$ with n vertices $v_1, v_2, \ldots, v_n$ where r and n both are odd.*

By data $d(v_i) = r$ for all $i = 1, 2, \ldots, n$.

$\therefore \quad \sum d(v_i) = rn$

Since r and n both are odd, rn is an odd natural number.

But by Theorem 1, page 8-3, $\sum d(v_i)$ is an even number. Hence, this is a contradiction.

$\therefore$ There is no r-regular graph with n-vertices where both r and n are odd.

Example 2 : *Can we have a graph in which there are 5 vertices and the degree of each vertex is 3.*

Sol. : *No because of the above result.*

Example 3 : *If $G = (V, E)$ is an r-regular graph with n vertices and m edges then $m = \frac{nr}{2}$.*

Sol. : *Let $V = \{v_1, v_2, \ldots, v_n\}$. Then by Theorem 1, page 8-3, $\sum d(v_i) = 2m$.*

Since G is regular, $d(v_i) = r$, for $i = 1, 2, \ldots, n$

$\therefore \quad \sum d(v_i) = rn \quad \therefore \quad rn = 2m \quad \therefore \quad m = \frac{nr}{2}$.

Example 4 : *Verify the result that for a r-regular graph with n vertices and m edges $m = \frac{nr}{2}$ for the graph shown in Fig. 8.14.*

Sol. : *We have 6 vertices $v_1, v_2, v_3, v_4, v_5, v_6$. There are the following 9 edges.*

3 edges $\{v_1, v_j\}$; $j = 2, 4, 6$

2 edges $\{v_2, v_j\}$; $j = 3, 5$

2 edges $\{v_3, v_j\}$; $j = 4, 6$

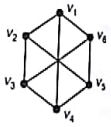


Fig. 8.14

1 edge (v_4, v_5)

1 edge (v_5, v_6)

Degree of each vertex is 3.

$\therefore \quad n = 6, \; m = 9, \; r = 3. \quad \therefore \quad \frac{nr}{2} = \frac{6 \times 3}{2} = 9 = m$

Hence, the $m = \frac{nr}{2}$ is verified.

EXERCISE - II

1. Give an example of an r-regular graph and verify for the same graph the result $m = \frac{nr}{2}$ with usual notation.
2. If a 4 regular graph has 12 edges, find the number of vertices of the graph.

[**Ans. :** $m = \frac{nr}{2} \quad \therefore \; n = \frac{2m}{r} = \frac{2 \times 12}{r} = 6$]

3. Prove that there is no 5 regular graph with 7 vertices.
4. Find a regular graph of degree 3 other than K_4 and $K_{3,3}$.

[**Ans. :** See adjoining figure. This is known as Petersen's graph.]

(3) Bipartite Graph

Definition : a graph $G = (V, E)$ is called bipartite (= of two parts) if it satisfies the following conditions.

(i) V can be expressed as a union of two disjoint sets U and W.

(*i.e.*, $U \cup W = V$ and $U \cap W = \Phi$)

(ii) Every edge in E has one vertex in U and the other in W.

Also the sets U and W are called partitions of V.

Example 1 : *Show that $G = (V, E)$ where $V = \{v_1, v_2, \ldots, v_6\}$ and $E = \{e_i \mid e_i = \{v_1, v_i\}, i = 2, 3, \ldots, 6\}$ is a bipartite graph.*

Sol. : In this graph there are six vertices $v_1, v_2, \ldots, v_6$ and the vertex v_1 is connected to every other vertex v_2, v_3, v_4, v_5, v_6. Thus, we get the Fig. 8.15 (a).

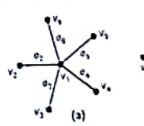


Fig. 8.15

Now, let $U = \{v_1\}$ and $W = \{v_2, v_3, v_4, v_5, v_6\}$

Then $V = U \cup W$ and $U \cap W = \Phi$.

Further each vertex in U is joined with each vertex v_2, v_3, v_4, v_5, v_6 in W. Hence, it is a bipartite graph.

The Fig. 8.15 (b) shows the partitions of this graph.

Example 2 : *Show that the graph given in Fig. 8.16 (a) is bipartite.*

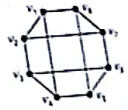


Fig. 8.16 (a)

Sol. : Let $V = \{v_1, v_2, \ldots, v_7\}$.

Also let $U = \{v_1, v_3, v_5, v_7\}$

and $W = \{v_2, v_4, v_6\}$.

Clearly, $V = U \cup W$ and $U \cap V = \Phi$.

Further, every edge has one vertex in U and the other vertex in W. Hence, it is a bipartite graph. The Fig. 8.16 (b) below shows this fact clearly.

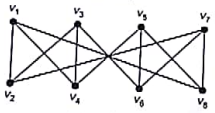


Fig. 8.16 (b)

Example 3 : If G is a simple, bipartite graph with m vertices and n edges show that $m^2 \geq 4n$.

Sol. : Since G is a bipartite graph, let $V = U \cup W$ be its partition. Let there be p vertices in U and q vertices in W, so that G has $p + q$ vertices.

$$\therefore \quad p + q = m \qquad \ldots\ldots\ldots\ldots (1)$$

Since each vertex u in U can be connected to **at the most** q vertices in W as there are q vertices in W by our supposition. Hence, there are at the most pq edges in E.

$$\therefore \quad n \leq pq \qquad \ldots\ldots\ldots\ldots (2)$$

Now, from (1)

$$m^2 = (p+q)^2 = (p-q)^2 + 4pq$$
$$\geq 4pq \geq 4n \qquad [\because (p-q)^2 \geq 0]$$

Example 4 : Determine which of the following graphs are bipartite graphs. Find the partitions of the vertices if yes.

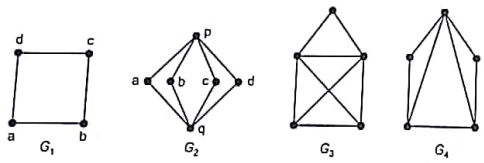


Fig. 8.17 (a)

Sol. : **(i)** In G_1 there are four vertices where a and c (or b and d) are not joined. Let $U = \{a, c\}$, $V = \{b, d\}$. Then $V = U \cup W$ and $U \cap W = \Phi$.

$\therefore$ It is a bipartite graph.

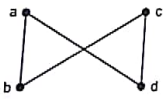


Fig. 8.17 (b)

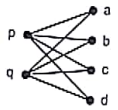


Fig. 8.17 (c)

(ii) In G_2 there 6 vertices and two are joined to the remaining four. We get the Fig. 8.17 (c).

Let $U = \{p, q\}$, $W = \{a, b, c, d\}$. Then $V = U \cup W$ and $U \cap W = \Phi$.

Further each vertex in U is joined with each vertex in W.

Hence, it is a bipartite graph.

(iii) G_3 is not a bipartite graph as the vertices cannot be partitioned as disjoint sets. Further in G_3 there are $m = 5$ vertices and $n = 8$ edges and $m^2 \geq 2n$.

(iv) G_4 is not a bipartite graph as the vertices cannot be partitioned in disjoint sets. Further, note that in G_2 there are $m = 5$ vertices and $n = 7$ edges. Now, $m^2 = 25$ and $2n = 23$, $m^2 \geq 4n$.

Example 5 : Show that there is not bipartite graph with 6 vertices and 10 edges.

Sol. : Such a graph cannot be drawn. Further for this graph $m = 6$ and $n = 10$ and $m^2 \geq 4n$.

Example 6 : Show that a bipartite graph has no loops.

Sol. : Let U and W be the two sets of vertices of the given bipartite graph such that $V = U \cup W$ and $U \cap W = \Phi$ where V is the set of vertices of the given bipartite graph.

Now, suppose $a = \{v, v\}$ is a loop. Hence, $v \in U$ and $v \in W$.

$$\therefore \quad v \in U \cap W.$$

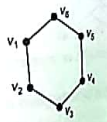
But by definition $U \cap W = \Phi$. This is a contradiction.

$\therefore$ A bipartite graph has no loops.

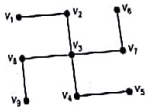
EXERCISE - III

1. Show that the following are bipartite graphs. Draw the graphs again showing the partitions.

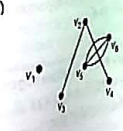
(a)



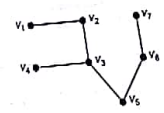
(b)



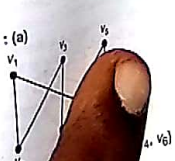
(c)



(d)

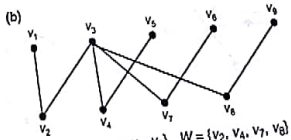


[Ans. : (a)



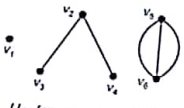
$U = \{v_1, v_3, v_5\}$, $W = \{v_2, v_4, v_6\}$

(b)



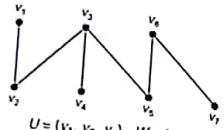
$U = \{v_1, v_3, v_5, v_6, v_8\}$, $W = \{v_2, v_4, v_7, v_8\}$

(c)



$U = \{v_1, v_2, v_3\}$, $W = \{v_3, v_4, v_6\}$

(d)

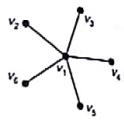


$U = \{v_1, v_3, v_6\}$, $W = \{v_2, v_4, v_5, v_7\}$

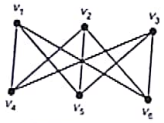
2. Show that there is no bipartite graph with six vertices and ten edges.

3. Construct some bipartite graphs on six vertices. Showing the partitions.

$U = \{v_1\}$,
$W = \{v_2, v_3, v_4, v_5, v_6\}$



$U = \{v_1, v_2\}$, $W = \{v_3, v_4, v_5, v_6\}$



$U = \{v_1, v_2, v_3\}$, $W = \{v_4, v_5, v_6\}$

(4) Complete Bipartite Graph

Definition : $G = (V, E)$ is called **complete bipartite graph** if

(1) G is bipartite, (2) G is simple, (3) If $V = U \cup W$ is the partition of V then every vertex u_i in U is joined to every vertex w_j in W. In other wards there is an edge between every vertex in U and every vertex in W.

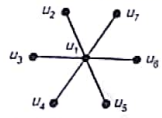
If U has m vertices and W has n vertices, then the complete bipartite graph is denoted by $K_{m, n}$.

Since each of the m vertices in U is adjacent (joined) to each of the n vertices in W, there will be mn edges in $K_{m, n}$. For standardisation we assume that $m \leq n$ in $K_{m, n}$.

Notes ....

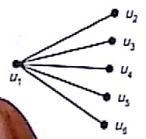
1. Since a complete bipartite graph is simple it has **no loops** and **no multiple edges**.
2. If $u \in U$ and $w \in W$ then there is only one edge between u and w, $e = (u, w) \in E$.

The following are complete bipartite graphs. The graph $K_{1, n}$ is called **star**.



$U = \{u_1\}$
$W = \{u_2, u_3, u_4, u_5, u_7\}$

Fig. 8.18 (a)



8.18 (b)

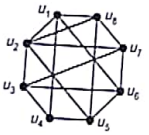
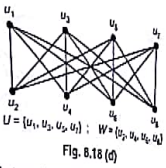


Fig. 8.18 (c)



$U = \{u_1, u_3, u_5, u_7\}$; $W = \{u_2, u_4, u_6, u_8\}$

Fig. 8.18 (d)

3. Clearly $K_{mn} = K_{nm}$. The first graph in (2) is a complete bipartite graph $K_{1, 6}$.
4. Observe the following complete bipartite graphs.

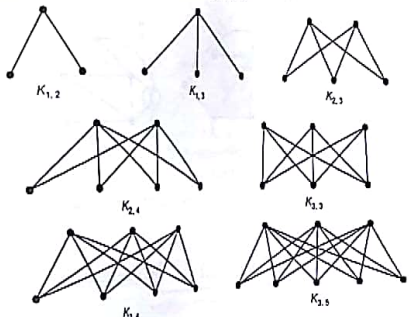


Fig. 8.19

Example : Find a complete bipartite graph which is not regular.

Sol. : A complete bipartite graph $K_{m,n}$ is not regular because each of m vertices in one set is joined with each of n vertices in another set. But the degree of each vertex is not the same, since $m \neq n$. Hence, it is not regular. For example, $K_{2,3}$ is not regular.

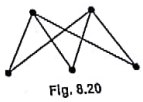


Fig. 8.20

(M.U. 2007, 12, 13, 17)

(5) Planar and Plane Graphs

Definition : If it is possible to draw the diagram of a given graph in such a way that no two edges intersect (except at a vertex) it is called a planar graph.

Definition : The diagram of a graph drawn in such a way that no two edges intersect is called a plane graph.

For example, the graph shown in the Fig. 8.21 (a) is a **planar graph** because (although the two edges e_1 and e_2 cross each other) it is possible to redraw the graph in such a way that the edges e_1 and e_2 do not cross as shown in the Fig. 8.21 (b) which is a plane graph.

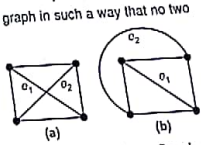


Fig. 8.21 : (a) Planar Graph, (b) Plane Graph.

The graphs shown in Fig. 8.22 (a) and (b) below are plane graphs.

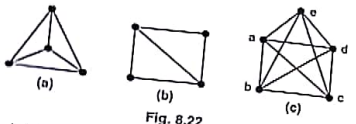


Fig. 8.22

The graph shown in Fig. 8.23 (a) is a planar graph as it can be redrawn as in Fig. 8.23 (b) which is a plane graph.

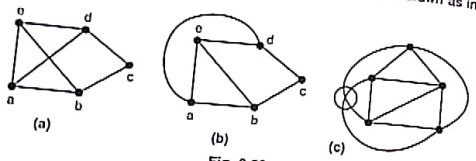


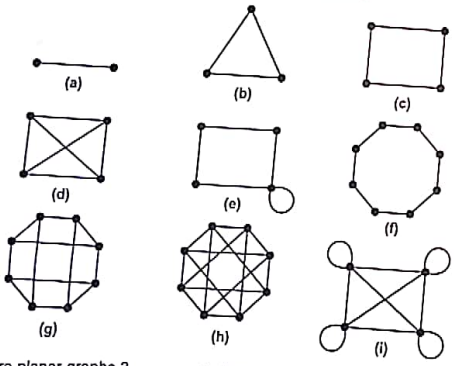
Fig. 8.23

But the graph G shown in Fig. 8.22 (c) is not a planar graph as it cannot be drawn without intersecting edges as shown in Fig. 8.23 (c).

We shall study planar graphs in details in Chapter 16.

EXERCISE - IV

Carefully observe the following graphs and answer the questions.



1. Which are planar graphs ?
2. Which are simple graphs ?

3. Which are regular graphs ?
4. Which are bipartite graph ?
5. Which are complete graphs ?
6. Which are complete bipartite graphs ?

[Ans. : (1) All are planar graphs. (2) Except (e) and (i) all are simple. (3) Except (e) all are regular. (4) (a), (f), (g), (h) are bipartite. (5) (a), (b), (d), (h) are complete. (6) (a), (h) are complete bipartite.]

5. Isomorphism

Consider diagrams G_1 and G_2.

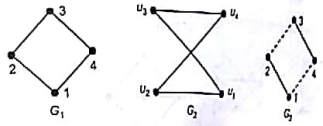


Fig. 8.24

Do they represent the same graph ? If we change the names of vertices in G_2 as $u_1 \to 2$, $u_2 \to 1$, $u_3 \to 3$, $u_4 = 4$, then we see that the second diagram can be redrawn to get the first diagram. Imagine that you "lift" the vertex u_1 and put it on the left. 'Essentially' the two graphs are the 'same' although they 'look' different. Such graphs are called Isomorphic, (iso = same, morph = form).

Definition : Two graphs $G = (V, E)$ and $G' = (V', E')$ are said to be Isomorphic, if there exists a one-to-one correspondence f from V to V' such that if $v_1, v_2 \in V$ and $v_1', v_2' \in V'$ and $f(v_1) = v_1'$, $f(v_2) = v_2'$ then the number of edges between v_1 and v_2 equals the number of edges between v_1' and v_2'. The function f is called an Isomorphism between G and G'. If G and G' are isomorphic we write $G \cong G'$. (M.U. 2000, 01, 09, 14)

Notes ....

(i) If f is an isomorphism between G and G' the f^{-1} is also an Isomorphism.

(ii) If G is isomorphic to G' and G' is isomorphic to G'' then G is isomorphic to G''.

(iii) If $v_1, v_2 \in V$ are adjacent then $v_1', v_2' \in V'$ are also adjacent.

(iv) If $e = \{v_1, v_1\}$ is a loop, then $e' = \{v_1', v_1'\}$ is also a loop.

(v) If $e_1 = \{v_1, v_2\}$ and $e_2 = \{v_2, v_3\}$ are two adjacent edges i.e. e_1, e_2 are two edges incident at a common vertex v_2 then $e_1' = \{v_1', v_2'\}$ and $e_2' = \{v_2', v_3'\}$ are also adjacent edges.

(vi) If $e_1 = \{v_1, v_2\}$, $e_2 = \{v_1, v_2\}$ are parallel edges then $e_1' = \{v_1', v_2'\}$, $e_2' = \{v_1', v_2'\}$ are also parallel edges. In other words if G is a multigraph then G' is also a multigraph.

(vii) $d(v) = d(v')$ for all $v \in V$ i.e. degree of vertex v is equal to the degree of vertex v' under f.

It is not always easy to determine whether two graphs are isomorphic.

If two graphs are isomorphic then,

1. They must have the same number of vertices,
2. They must have the same number of edges.
3. They must have the same degrees of vertices.

If one of the above conditions is not satisfied then the graphs are not isomorphic.

Graphs may satisfy all the above three conditions and yet they may not be isomorphic. For example, see the Ex. 1 (a) below.

4. It may be noted that in addition to the above three conditions 'adjacency' also is an important condition.

Example 1 : Determine whether the following pairs of graph are isomorphic.

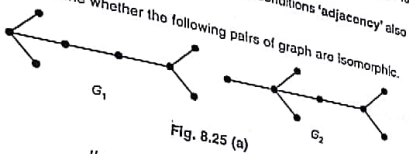


Fig. 8.25 (a)

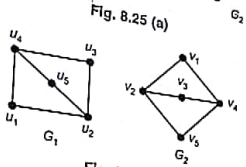


Fig. 8.25 (b)

Sol. : (a) The two graphs G_1, G_2 have eight vertices and seven edges. However, in the first graph G_1, there are four vertices of degree one and in the second graph G_2, there are five vertices of degree one.

Hence, the two graphs are not isomorphic.

(b) The two graphs G_1, G_2 have five vertices and six edges each. Further, in both the graphs there are three vertices of degree two and two vertices of degree three.

We can define one-to-one correspondence f as follows :

$u_1 \rightarrow v_5$, $u_2 \rightarrow v_4$, $u_3 \rightarrow v_1$, $u_4 \rightarrow v_2$, $u_5 \rightarrow v_3$.

This correspondence preserves the adjacency and incidence relationship.

$\therefore$ The graphs are isomorphic.

Note ....

G_2 can be obtained by just terning G_1 through 125°.

Example 2 : Draw all non-isomorphic graphs of (i) 2 vertices, (ii) 3 vertices and state reasons.

Sol. : *(i) All non-isomorphic graphs with two vertices are*

Fig. 8.26 (a)

(ii) All non-isomorphic graphs with three vertices are

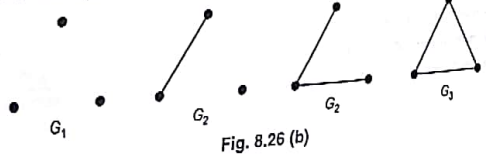


Fig. 8.26 (b)

Example 3 : Find all non-isomorphic connected graphs with four vertices and state reasons.

Sol. : All non-isomorphic connected graphs with four vertices are shown below.

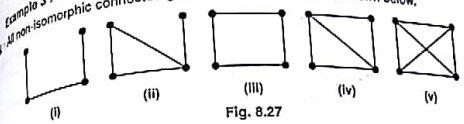


Fig. 8.27

Example 4 : Are the following pairs of graphs isomorphic ? Give reasons ?

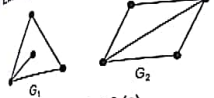


Fig. 8.28 (a)

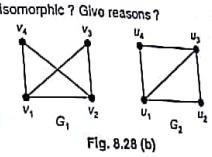


Fig. 8.28 (b)

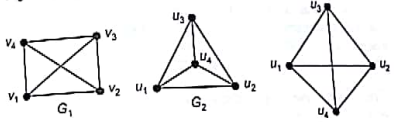


Fig. 8.28 (c)

Sol.: (a) No. Although G_1 and G_2 have 4 vertices both; G_1 has 4 edges and G_2 has 5 edges; G_1 has a pendant vertex, G_2 has not. G_1 has only one vertex with 3 edges while G_2 has two vertices with 3 edges.

(b) Yes. G_1 and G_2 both have 4 vertices; 5 edges; 2 vertices of degree 2 and 2 vertices of degree 3. The correspondence is obtained by lifting v_3 and placing it below v_2. [See Fig. 8.28 (d)]

$\therefore$ $v_1 \rightarrow u_1$, $v_3 \rightarrow u_2$, $v_2 \rightarrow u_3$, $v_4 \rightarrow u_4$.

(c) Yes. G_1 and G_2 both have 4 vertices 4 edges. Each vertex in G_1 and G_2 is of degree 3. The correspondence is obtained if u_4 is pulled down and the figure is rotated through 45°. [See Fig. 8.28 (d)]

$\therefore$ $v_1 \rightarrow u_1$, $v_2 \rightarrow u_4$, $v_3 \rightarrow u_2$, $v_4 \rightarrow u_3$.

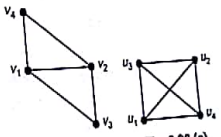


Fig. 8.28 (d) Fig. 8.28 (e)

Example 5 : Are the graphs shown in the Fig. 8.29 Isomorphic ? Give reasons.

Sol. : Yes. Both G and G' have 6 vertices and 9 edges. Each vertex in G and G' is of degree 3. The correspondence is obtained if G is rotated through 45° (in anticlockwise direction) and d and a are interchanged by pushing a up and pulling d down.

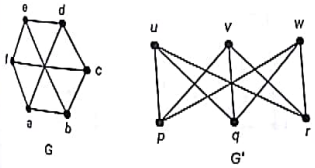


Fig. 8.29

$\therefore$ $e \to u$, $a \to v$, $c \to w$, $f \to p$, $d \to q$, $b \to r$.

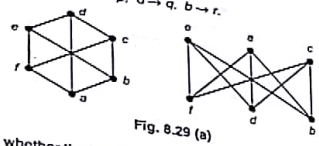


Fig. 8.29 (a)

Example 6 : Find whether the following graphs $G = (V, E)$ and $G^* = (V^*, E^*)$ are isomorphic giving reasons.

(i) $V = \{a, b, c, d\}$, $E = \{(a, b), (a, d), (b, d), (c, d), (c, b), (c, d)\}$

(ii) $V^* = \{1, 2, 3, 4\}$, $E^* = \{(1, 2), (2, 3), (3, 1), (3, 4), (4, 1), (4, 2)\}$

Sol. : **(i)** We shall first draw the diagrams of these graphs which are given in set notation. In E the edge (c, d) occurs twice, indicating that there are two edges between c and d.

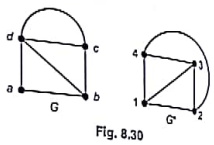


Fig. 8.30

(ii) No. Both graphs G and G^* have 4 vertices and 6 edges. But the degree of vertex a in G is 2 and there is no vertex of degree 2 in G^*. Also in G the degree of vertex d is 4, but there is no vertex of degree 4 in G.

Example 7 : Find whether the graphs shown in Fig. 8.31 are isomorphic.

(M.U. 2000, 14, 15, 17)

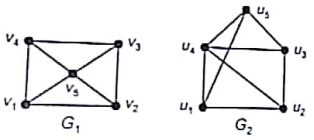


Fig. 8.31

Sol. : We first note that both the graphs have

(1) five vertices (2) eight edges

In G_1 there is one vertex v_5 of degree 4 and the remaining vertices are of degree 3.

In G_2, there is one vertex u_4 of degree 4 and the remaining are of degree 3.

Further, the adjancy property is observed. The vertex with degree 4 is adjacent to the remaining vertices in both the graphs.

Hence, the two graphs are isomorphic.

If you pull u_4 inside and u_5 to the position of u_4, you will get G_1.

The correspondence is

$v_1 \to u_1$, $v_2 \to u_2$, $v_3 \to u_3$, $v_4 \to u_5$ and $v_5 \to u_4$.

Example 8 : Determine whether the following graphs are isomorphic. **(M.U. 2002, 17)**

Sol. : There are 8 vertices in G_1 and 8 vertices in G_2.

Further there are four vertices of degree 3 in G_1 and four vertices of degree 3 in G_2. There are four vertices of degree 2 in G_1 and there are four vertices of degree 2 in G_2.

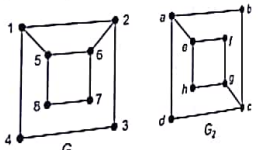


Fig. 8.32

But if $5 \to e$ and $6 \to g$ then although 5 and 6 are adjacent, e and g are not adjacent (See (4), page 8.15]. Thus adjacency is not preserved.

Similarly, if $1 \to a$ and $2 \to c$ although 1 and 2 are adjacent but a and c are not adjacent. Thus, we see that the adjacency is not preserved.

The graphs are not isomorphic.

Example 9 : Determine whether the graphs G_1 and G_2 are isomorphic or not. Justify your answer. **(M.U. 2008)**

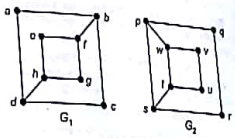


Fig. 8.33

Sol. : We first note the following.

1. Both the graphs have the same number of vertices viz. 8 and the same number of edges 10.
2. In G_1 there are four vertices with degree 3 and in G_2 also there are four vertices with degree 3.
3. But adjancy is not preserved in the two graphs. In G_1 vertex with 3 edges is adjacent to only one vertex with 3 edges (f and b or d and h). But in G_2 a vertex with 3 edges is adjacent to two vertices with edges 3 (p to w and s; w to p and t and so on). Thus, adjacency is not preserved.
4. Hence G_1 and G_2 as above are not isomorphic.

Example 10 : Show that the graphs shown in the Fig. 8.34 are isomorphic.

(M.U. 1998, 2000, 13)

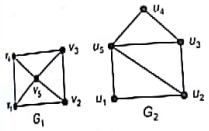


Fig. 8.34

Sol. : We first see that the two graphs have the same number of vertices (5) and the same number of edges (8).

In G_1 there are 4 vertices of degree 3 and one vertex of degree 4. In G_2 also there are 4 vertices of degree 3 and one vertex of degree 4.

Consider the correspondence

$v_1 \to u_1$, $v_2 \to u_2$, $v_3 \to u_3$, $v_4 \to u_4$ and $v_5 \to u_5$.

(If we pull u_5 towards u_2, so that u_4 becomes the vertex of the rectangle G_2 will look like G_1).

Hence, G_1 and G_2 are isomorphic.

Example 11 : Determine whether the following graphs are isomorphic or not. **(M.U. 2005, 07)**

Sol. : We first see that both the graphs have the same number of vertices (6) and the same number of edges (9).

In G_1 all the vertices are of degree 3 and in G_2 also all the vertices are of degree 3.

Consider the correspondence $v_1 \to u_1$, $v_2 \to u_2$, $v_3 \to u_3$, $v_4 \to u_4$, $v_5 \to u_5$, $v_6 \to u_6$.

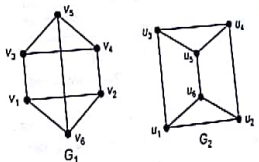


Fig. 8.35

(If we press the edge (v_5, v_6) in G_1 and bring it within the rectangle after making it short, we will get the graph G_2.)

Hence, G_1 and G_2 are isomorphic.

Example 12 : Show that the two graphs shown in the Fig. 8.36 are isomorphic. **(M.U. 2001, 13, 14)**

Sol. : We first see that the two graphs have the same number of vertices (5) and the same number of edges (7).

In G_1 there are 4 vertices of degree 3 and one vertex of degree 2. In G_2 also there are 4 vertices of degree 3 and one vertex of degree 2.

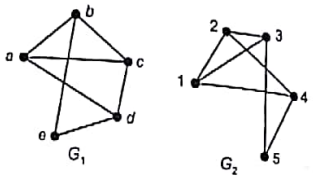


Fig. 8.36

Consider the correspondence $a \to 1$, $b \to 2$, $c \to 3$, $d \to 4$, $e \to 5$.

(If we rotate G_2 keeping the vertex 1 fixed, in clockwise direction such that the edge (1, 3) becomes horizontal, then G_2 will look like G_1.)

Hence, G_1, G_2 are isomorphic.

Example 13 : Show that the graphs shown in the Fig. 8.37 are not isomorphic. **(M.U. 2005)**

Sol. : Both the graphs have 5 vertices. Both the graphs have 6 edges.

But in graph G_2 there is one vertex a' with degree 4 and one vertex e' with degree 1.

There is no vertex with degree 4 and no vertex with degree 1 in G_1.

∴ The graphs are not isomorphic.

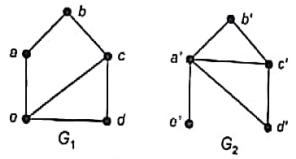


Fig. 8.37

Example 14 : Determine whether the pair of graphs (Fig. 8.38) is isomorphic or not. **(M.U. 2012)**

Sol : We first note that both the graphs have

1. same number of vertices *viz.* 6
2. same number of edges *viz.* 9.

In G, there are two vertices e, f of degree 2, two vertices c and a of degree 3, two vertices b and d of degree 4.

In G', also there are two vertices b' and e' of degree 2, two vertices a' and d' of degree 3, two vertices c' and f' of degree 4.

Yet the two graphs are **not** isomorphic because **the property of adjacency is not observed.**

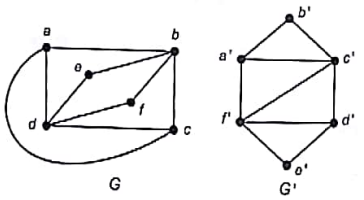


Fig. 8.38

In G, one vertex e (and also f) of degree 2 is adjacent to two vertices d and b of degree 4.

In G', one vertex b' (and also e') of degree 2 is adjacent to the vertex c' with degree 4 but to a' with degree 3.

Hence, the graphs are **not** isomorphic.

Example 15 : Find whether the following graphs (Fig. 8.39) are isomorphic. **(M.U. 2000)**

Sol. : We first note that both the graphs G and G' have

(i) the same number of vertices *viz.* 6

(ii) the same number of edges *viz.* 6

(iii) each vertex in G and G' is of degree 2.

Hence, the two graphs are isomorphic.

G can be obtained from G' by "pulling" the vertex d' up above the vertices c' and e'.

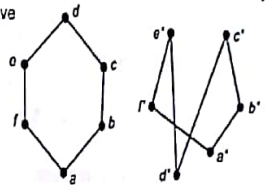


Fig. 8.39

Example 16 : Determine whether the following graphs are isomorphic. **(M.U. 2003, 10, 11)**

Sol. : We first note that G and G' have

(i) the same number of vertices *viz.* 6

(ii) but they do not have the same number of edges. G has 8 edges while G' has 9 edges.

(iii) In G' the vertex c' (and also f') is of degree 4, while in G there is no vertex of degree 4.

Hence, G and G' are **not** isomorphic.

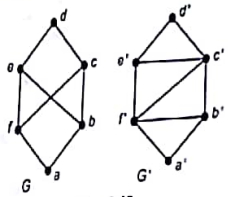


Fig. 8.40

Example 17 : Determine whether the following graphs [Fig. 8.41 (a) and (b)] are isomorphic. **(M.U. 2009)**

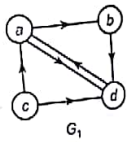


Fig. 8.41 (a)

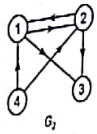


Fig. 8.41 (b)

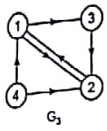


Fig. 8.41 (c)

Sol. : We first observe that

(i) G_1 and G_2 have the same number of vertices, 4.

(ii) G_1 and G_2 have the same number of edges, 6.

(iii) Both G_1 and G_2 have two vertices of degree 4 and two vertices of degree 2.

If we interchange the positions of (2) and (3) in G_2, we get G_3 as shown in the Fig. 8.41 (c).

Hence, the graphs are isomorphic.

Example 18 : Determine the whether the graphs (Fig. 8.42) are isomorphic. **(M.U. 2015)**

Sol. : We first note that G and G' have

(i) the same number of vertices (7)

(ii) the same number of edges (9)

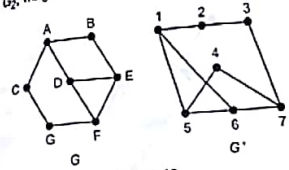


Fig. 8.42

(iii) three vertices of degree two (G has B, C, G ; G' has 2, 3, 4) four vertices of degree three (G has A, D, E, F ; G' has 1, 5, 6, 7)

Also adjacency is preserved.

We can define one-to-one correspondence as follows.

$A \to 1, B \to 2, C \to 3, D \to 6, E \to 5, F \to 7, G \to 4$.

[See Fig. 8.42 (a)]

Hence, the graphs are isomorphic.

Fig. 8.42 (a)

Example 19 : Discuss whether the following graphs are isomorphic. (M.U. 1998)

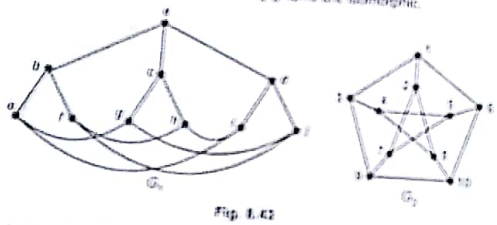


Fig. 8.42

Sol. : We first see that both the graphs have the same number of vertices (10) and the same number of edges (15).

In both the graphs all the 10 vertices are of degree 3.

Also the adjacency is preserved.

Consider the correspondence

$a \to 1, b \to 2, c \to 3, d \to 4, e \to 5, f \to 6, g \to 7, h \to 8, i \to 9, j \to 10$

Hence, the two graphs are isomorphic.

Example 20 : Show that the graphs shown in the Fig. 8.44 are isomorphic. Also find the isomorphism.

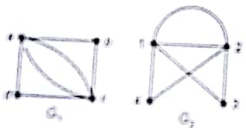


Fig. 8.44

Sol. : Both graphs have 4 vertices and 6 edges.

Each graph has 2 vertices of degree 2 and 2 vertices of degree 4. Also the adjacency is preserved.

Since all the four conditions are satisfied, the two graphs are isomorphic.

The correspondence is $a \to 1, c \to 2, b \to 3, d \to 4$.

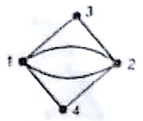


Fig. 8.44 (a)

If we shift the vertex 3 and place it above 1 and 2, we get the Fig. 8.44 (G_1) as shown in Fig. 8.44 (a).

Example 21 : Determine whether the following graphs (Fig. 8.45) are isomorphic. (M.U. 2013)

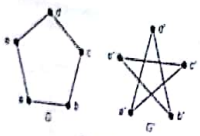


Fig. 8.45

Both graph have 5 vertices. Both graphs have 5 edges. The degree of each vertex is 2.

Also adjacency is preserved.

Hence, the both graphs are isomorphic.

Fig. 8.45 (a)

Left the side $a'c'$, turn it through 180° and place it below the points a', b', such that c' is below a' and d is below b'.

The correspondence is $a \to c', b \to e', c \to b', d \to d', e \to a'$.

Example 22 : Determine whether the following graphs are isomorphic. (M.U. 2017)

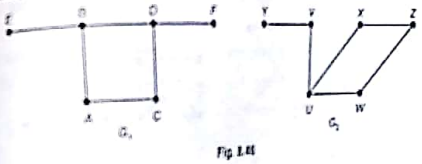


Fig. 8.46

Sol. : Both the graphs have 6 vertices and 8 edges.

But in G_1, there are two vertices of degree 1 and in G_2 there is only one vertex of degree 1.

In G_1 there are two vertices of degree 3 and in G_2 there is only one vertex of degree 3.

Hence, the graphs are not isomorphic.

Example 23 : Find if the following two graphs are isomorphic. (M.U. 2018)

If yes, find one-to-one correspondence between their vertices.

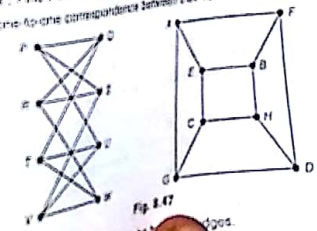


Fig. 8.47

Sol. : Both graphs have 8 vertices. Both graphs ... edges.

In both graphs each vertex is of degree ... conditions are satisfied the graphs are isomorphic.

Also adjacency is preserved. Since ...

(iii) three vertices of degree two (G has B, C G; G' has 2, 3 4) four vertices of degree three (G has A, D, E, F; G' has 1, 5, 6, 7).

Also adjacency is preserved.

We can define one-to-one correspondence as follows.

$A \to 1$, $B \to 2$, $C \to 3$, $D \to 6$, $E \to 5$, $F \to 7$, $G \to 4$.

[See Fig. 8.42 (a)]

Hence, the graphs are isomorphic.

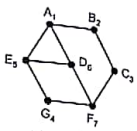


Fig. 8.42 (a)

Example 19 : Discuss whether the following graphs are isomorphic. **(M.U. 1998)**

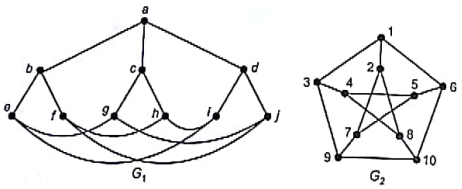


Fig. 8.43

Sol. : We first see that both the graphs have the same number of vertices (10) and the same number of edges (15).

In both the graphs all the 10 vertices are of degree 3.

Also the adjacency is preserved.

Consider the correspondence

$a \to 1$, $b \to 2$, $c \to 3$, $d \to 4$, $e \to 5$, $f \to 6$, $g \to 7$, $g \to 8$, $i \to 9$, $j \to 10$.

Hence, the two graphs are isomorphic.

Example 20 : Show that the graphs shown in the Fig. 8.44 are isomorphic. Also find the isomorphism.

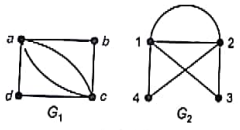


Fig. 8.44

Sol. : Both graphs have 4 vertices and 6 edges.

Each graph has 2 vertices of degree 2 and 2 vertices of degree 4. Also the adjacency is preserved.

Fig. 8.44 (a)

Since all the four conditions are satisfied, the two graphs are isomorphic.

The correspondence is $a \to 1$, $c \to 2$, $b \to 3$, $d \to 4$.

If we shift the vertex 3 and place it above 1 and 2, we got the Fig. 8.44 (G_1) as shown in Fig. 8.44 (a).

Example 21 : Determine whether the adjoining graphs (Fig. 8.45) are isomorphic. **(M.U. 2015)**

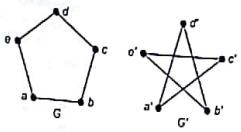


Fig. 8.45

Sol. : Both graph have 5 vertices. Both graphs have 5 edges. The degree of each vertex is 2.

Also adjacency is preserved.

Hence, the both graphs are isomorphic.

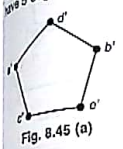


Fig. 8.45 (a)

Lift the side $c'o'$, turn it through 180° and place it below the points a', b', such that c' is below a' and e' is below b'.

The correspondence is $a \to c'$, $b \to e'$, $c \to b'$, $d \to d'$, $e \to a'$.

Example 22 : Determine whether the following graphs are isomorphic. **(M.U. 2017)**

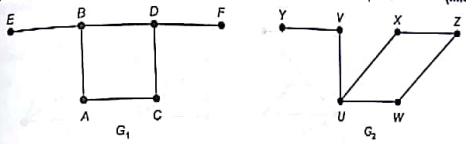


Fig. 8.46

Sol. : Both the graphs have 6 vertices and 6 edges.

But in G_1, there are two vertices of degree 1 and in G_2, there is only one vertex of degree 1.

In G_1 there are two vertices of degree 3 and in G_2 there is only one vertex of degree 3.

Hence, the graphs are not isomorphic.

Example 23 : Find if the following two graphs are isomorphic. If yes, find one-to-one correspondence between their vertices. **(M.U. 2018)**

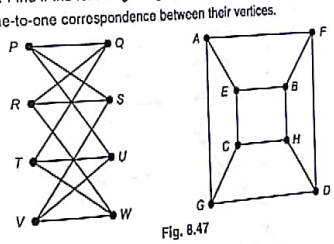


Fig. 8.47

Sol. : Both graphs have 8 vertices. Both graphs have 12 edges.

In both graphs each vertex is of degree three.

Also adjacency is preserved. Since, all the four conditions are satisfied the graphs are isomorphic.

We can obtain the second figure from the first by interchanging the vertices R, S. Also interchanging the vertices T, U and putting them down, so that the vertices V and W are inside the square.

The required correspondence is

$A \to P$, $F \to Q$,
$E \to S$, $B \to R$,
$C \to V$, $H \to W$,
$G \to U$, $D \to T$.

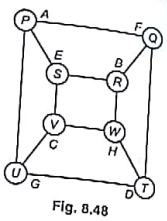
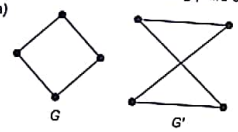


Fig. 8.48

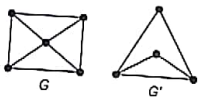
EXERCISE - V

1. Determine whether the following pairs of graphs G and G' are isomorphic. Give reasons.

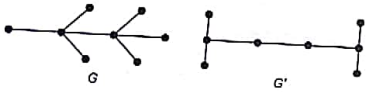
(a)



(b)



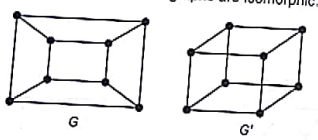
(c)



[Ans. : (a) Yes, (b) Yes, (c) No.]

2. Determine whether the following pairs of graphs are isomorphic. Give reasons.

(a)



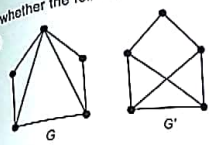
(b)

(c)

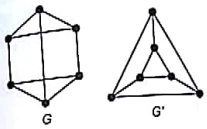
[Ans. : (a) Yes, (b) No, (c) Yes.]

3. Find whether the following pairs of graphs are isomorphic. Give reasons.

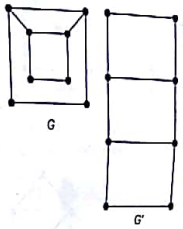
(a)



(b)



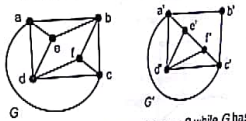
(c)



[Ans. : (a) No, (b) Yes, (c) Yes.]

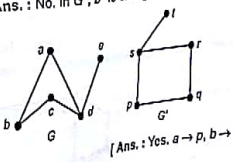
4. Find whether the following graphs are isomorphic. Give reasons.

(i)



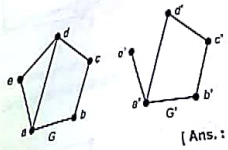
[Ans. : No. In G', b' is of degree 2 while G has no vertex of degree 2]

(ii)



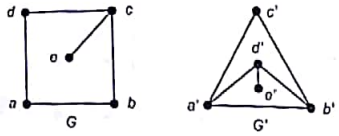
[Ans. : Yes, $a \to p$, $b \to q$, $c \to r$, $d \to s$, $o \to t$]

(iii)



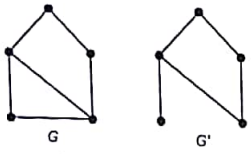
[Ans. : No. In G', o' is a pendant.]

5. Determine whether the following graphs are isomorphic. Give reasons.



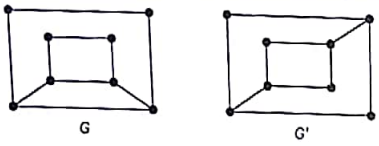
[**Ans.** : No. In G, there is only one vertex of degree 3, while in G', there are 3 vertices of degree 3.]

6. Determine whether the following graphs are isomorphic. Give reasons.



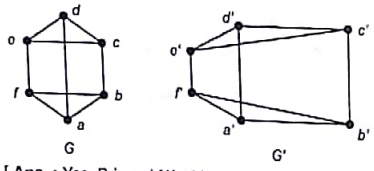
[**Ans.** : No. G' has a pendant while G has no pendendant.]

7. Determine whether the following graphs are isomorphic. Give reasons.



[**Ans.** : No. Adjancy is not preserved.]

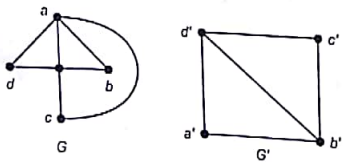
8. Determine whether the following graphs are isomorphic. Give reasons.



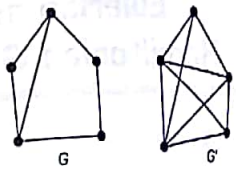
[**Ans.** : Yes. Bring o' f ' inside the square and then stretch it on both sides.]

9. Determine whether the following pairs of graphs are isomorphic. Give reasons.

(a)



(b)



[**Ans.** : (a) No. G has a vertex of degree 4 but G' does not have such a vertex.
(b) No. G' has 3 vertices of degree 4.]

EXERCISE - VI

1. Define the following terms giving illustrations.
   1. Graph **(M.U. 1998)** 2. Loop 3. Multigraph
   4. Adjacent Vertices 5. Incident Edge 6. Adjacent Edges
   7. Degree Of A vertex 8. Isolated Vertex 9. Pendant.
   10. Length Of A Graph.
2. Define the following terms giving illustrations.
   1. Simple Graph 2. Complete Graph 3. Regular Graph
   4. Bipartite Graph **(M.U. 2010)** 5. Complete Bipartite Graph **(M.U. 2010)**
   6. Planar Graph
3. Define and illustrate isomorphism of two graphs. **(M.U. 2000, 01, 05)**
4. State and prove "Hand Shaking Lemma"
5. Prove that the sum of the degrees of all vertices of a graph is equal to twice the number of edges.
6. Prove that in any graph the number of vertices of odd degree is even.
7. Prove that the total number of edges in a complete graph K_n is $n(n-1)/2$ and the degree of each vertex is $n-1$.
8. Explain whether K_4 is a plane graph.

21. Let R be an equivalence relation on set A. prove that the following statements are equivalent. (M.U. 2013)
(i) $a R b$. (ii) $[a] = [b]$. (iii) $[a] \cap [b] \neq \Phi$.

22. Determine whether the relation R defined below on set of all integers is reflexive, symmetric, anti symmetric and / or transitive where $x R y$ if and only if (i) $xy \geq 1$. (ii) $x = y \pmod 7$. (M.U. 2013)
[**Ans.** : Both are equivalence relations. Not antisymmetric.

CHAPTER 4

Posets and Lattices

1. Introduction

We have seen that the relations which are reflexive, symmetric and transitive form a new type of relations called equivalence relations. Similarly, relations which are reflexive, antisymmetric and transitive form a new type of relations called **partial order relations**. Now, we shall study such relations and sets arising from these relations *i.e.* **posets** (Partially Ordered Sets).

2. Partially Ordered Sets (Posets) (M.U. 1999, 2013, 17)

(a) Partial Order Relation

Definition : A relation R on a set A is called a **partial order relation** if R is (i) reflexive, (ii) antisymmetric and (iii) transitive. For example, the relations $\leq$, $\geq$, $\subseteq$ are partial order relations.

(b) Partially Ordered Set

Definition : The set A together with the partial order relation R is called a **partially ordered set** or in brief **poset** and is generally denoted by (A, R) or by $(A, \leq)$ where A denotes the set and R denotes the relation.

(Why such a set is called partially ordered set is explained in Ex. 1, (bottom) page 4-3, 4-4) (M.U. 2001, 07, 10, 13)

Remark ....

Partial order relation can be memorised by its acronym RAT (Reflexive, Antisymmetric, Transitive.)

Example 1 : If S is any set and $\wp$ is its power set (collection of subsets) then the relation $\subseteq$ (is a subset of) is a partial order relation on $\wp$. (M.U. 2004, 13)

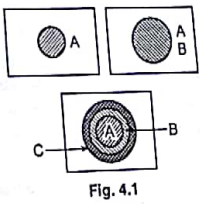


Fig. 4.1

Sol. : Let A, B, C be the elements of $\wp$.

(i) Since $A \subseteq A$, R is reflexive.

(ii) If $A \subseteq B$ and $B \subseteq A$ then $A = B$.
$\therefore$ R is antisymmetric.

(iii) If $A \subseteq B$, $B \subseteq C$ then $A \subseteq C$.
$\therefore$ R is transitive.

$\therefore$ R is a partial order relation on $\wp$.

Example 2 : If Z^+ is the set of positive integers then the relation $\leq$ (less than or equal to) is a partial order relation on Z^+. (M.U. 2008, 11)

Sol. : Let a, b, c be any three natural numbers.

(i) Since $a \le a$, R is reflexive. *e.g.* $3 \le 3$

(ii) If $a \le b$ and $b \le a$ then $a = b$.

$\therefore$ R is antisymmetric.

(iii) If $a \le b$, $b \le c$ then $a \le c$. *e.g.* $2 \le 3$, $3 \le 4$ $\therefore$ $2 \le 4$.

$\therefore$ R is transitive. $\therefore$ R is a partial order relation.

Example 3 : If Z^+ is a set of positive integers then the relation $\ge$ (greater than or equal to) is a partial order relation on Z^+.

Sol. : Prove it.

Example 4 : If Z^+ is a set of positive integers then the relation R of divisibility *i.e.* $a\ R\ b$ if and only if $a \mid b$ (a divides b) is a partial order relation on Z^+. **(M.U. 2011)**

Sol. : Prove it. Or see Ex. 1 page 4-3.

Example 5 : Consider a set of integers Z. Let $a\ R\ b$ if $b = a^r$ for some positive integer r. Show that R is a partial order relation. **(M.U. 2000, 02)**

Sol. : Let $a, b, c \in Z$.

(i) Since $a = a^1$, R is reflexive.

(ii) If $a = b^r$ and $b = a^{r'}$ then $a = b$.

(If $a = b^r$ and $b = a^{r'}$ then $\frac{a}{a^r} = \frac{b^{r'}}{b}$ $\therefore$ $a^{1-r} = b^{r'-1}$. This is true only if $r = 1 = r'$ *i.e.* $a = b$)

$\therefore$ R is antisymmetric.

(iii) If $a = b^r$ and $b = c^{r'}$ then $a = (c^{r'})^r = c^{rr'}$.

$\therefore$ $a\ R\ c$ $\therefore$ R is transitive. $\therefore$ R is a partial order relation.

Example 6 : Consider a set of integers Z. Let $a\ R\ b$ if $a = 2b$. Examine whether R is a partial order relation. **(M.U. 1995)**

Sol. : Let $a, b, c \in Z$.

Since, we cannot have $a = 2a$. $\therefore$ R is not reflexive.

Also, if $a = 2b$ and $b = 2c$, $a = 4c$. $\therefore$ R is not transitive.

$\therefore$ R is **not** a partial order relation.

Example 7 : Define a relation R on the set Z by $a\ R\ b$ if $a - b$ is a non-negative even integer. **(M.U. 2005)** Verify whether R is a partial order relation.

Sol. : Let a, b, c be three integers.

(i) $a - a = 0$ and zero is non-negative even integer.

$\therefore$ $a\ R\ a$ $\therefore$ R is reflexive.

(ii) If $a\ R\ b$ and $b\ R\ a$ then $(a - b)$ is non-negative even integer and $(b - a)$ is also a non-negative even integer. This is possible only if $a - b = 0$.

$\therefore$ $a = b$. $\therefore$ R is anti-symmetric.

(iii) Let $a\ R\ b$ and $b\ R\ c$. Then $a - b = 2n_1$, say, and $b - c = 2n_2$ where n_1 and n_2 are non-negative integers.

$\therefore$ $a - c = 2(n_1 + n_2)$

$\therefore$ $(a - c)$ is an even non-negative integer

$\therefore$ $a\ R\ c$ $\therefore$ R is transitive.

Since R is reflexive, antisymmetric and transitive R is partially ordered.

Example 8 : Let R be a relation on the set of positive integers such that $R = \{(a, b) \mid (a - b)$ is an odd positive integer $\}$. Is R an equivalence relation, a partial order relation? **(M.U. 2000)**

Sol. : (i) $a - a = 0$ and 0 is an odd positive integer.

$\therefore$ R is reflexive.

(ii) Let $a\ R\ b$, then $a - b =$ an odd positive integer, say, $a - b = 2n + 1$.

Then $b - a = -2n - 1$ which is negative and hence $b \not R\ a$.

$\therefore$ R is not symmetric and R is not antisymmetric.

(iii) Let $a\ R\ b$ and $b\ R\ c$.

$\therefore$ $a - b = 2n_1 + 1$ and $b - c = 2n_2 + 1$

$\therefore$ $(a - b) + (b - c) = (2n_1 + 1) + (2n_2 + 1)$

$\therefore$ $a - c = 2n_1 + 2n_2 + 2 = 2(n_1 + n_2 + 1)$, even integer.

$\therefore$ $a \not R\ c$ $\therefore$ R is not transitive.

$\therefore$ R is neither an equivalence relation nor a partially ordered relation.

Example 9 : Consider a relation R on the set of integers defined by $x\ R\ y$ if $y - x = k$ where k is a positive integer. Show that R is a partial order relation. **(M.U. 2009)**

Sol. : Write the solution as in the Ex. No. 7, above.

EXERCISE - I

Give examples of relations R_1, R_2 and R_3 on $A = \{1, 2, 3, 4\}$ with justification such that (i) R_1 is reflexive but not symmetric, (ii) R_2 is transitive, symmetric but not reflexive, (iii) R_3 is a partial order relation. **(M.U. 2001)**

[**Ans. :** (i) $R_1 = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (1, 3)\}$

(ii) $R_2 = \{(2, 3), (3, 2), (2, 2), (3, 3)\}$

(iii) $R_3 = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (1, 4), (1, 3), (2, 4), (3, 4)\}$]

(c) Comparable Elements

Definition : If A is given set and R is a partial order relation on A then the elements a, b of A are said to be **comparable** if $a\ R\ b$ or $b\ R\ a$. This means if $a \not R\ b$ or $b \not R\ a$ then a and b are not comparable.

For example, in a set of Z^+ if R is a relation "is divisible by 3" then the elements 3 and 6 are comparable but 4 and 11 are not comparable.

Example 1 : If Z^+ is a set of positive integers and R is a relation 'a divides b' then prove that R is partial order relation. Show that Z is partially ordered. Find two elements which are not comparable. **(M.U. 2004, 08, 11)**

Sol. : Let $a, b, c \in Z^+$.

(i) Since 'a divides a', R is reflexive.

(ii) If $a \, R \, b$ and $b \, R \, a$ *i.e.* if a divides b and b divides a then $b = a$.

$\therefore$ R is antisymmetric.

(iii) If $a \, R \, b$, $b \, R \, c$ then $a \, R \, c$.

$\therefore$ R is transitive. $\therefore$ R is a partial order relation on Z^+.

Now, in this set 3 and 8 are not comparable elements because 3 does not divide 8 and 8 does not divide 3. Similarly, 2 and 11 are not comparable elements. Thus, in a poset, some elements are related *i.e.* comparable and some elements are not related *i.e.* not comparable. In this sense the set is ordered but **"partially"**.

(d) Total Order Relations or Chains

Definition : If any two elements in a poset are **comparable**, then the partial order is called a **total order** or a **linear order**. In such a situation the relation is called **simple ordering relation** or **linear ordering relation**. The set A together with a total order relation is called **totally ordered set** or **simply ordered set** or a **chain**.

For example, the set {2, 4, 8, 16} with 'divides' as relation is a chain.

Since the most common partial order relations are $\leq$ and $\geq$ on Z or R, a partial order relation is generally denoted by $\leq$ and $\geq$ and the poset is denoted by $(A, \leq)$. Just as by taking complement union or intersecting of two sets we construct new sets, from posets we can construct new posets

Example : Let N be the set of whole numbers.

Find one totally ordered and one partially ordered relation on N such that all elements of N are included in each relation. **(M.U. 2003)**

Sol. : (a) In Ex. 2, page 4-1, we have proved that the relation $\leq$ is a partially ordered relation.

Further, since any two elements are comparable as if a, b are two natural numbers, then $a \leq b$ or $b \leq a$.

Hence, R is a total order relation.

(b) In Ex. 1, page 4-3, we have proved that 'a divides b' is a partially ordered relation. But it is not totally ordered. We have seen that 3 and 8 are not comparable elements as 3 does not divide 8. Similarly, 2 and 11 are not comparable elements.

3. Hasse Diagram

The digraph of a poset can be considerably simplified as follows. For instance, since in a poset the relation is reflexive, we drop the loops around the vertices. Since in a poset R is transitive *i.e.* if $a \, R \, b$ and $b \, R \, c$ then $a \, R \, c$, we drop the edge from a to c. Thus, we drop all edges implied by transitivity. Finally we arrange the whole diagram such that all arrows point upwards and then drop the arrow heads. The resulting diagram is called the **Hasse diagram**, named after the German mathematician Helmut Hasse who first suggested it.

Example 1 : Consider a set $A = \{1, 2, 3, 4, 12\}$ and the relation of divisibility *i.e.* $a \, R \, b$ if a divides b which we denote as $a \mid b$. Show that (A, R) is a poset. Also construct the digraph of the poset and its Hasse diagram. **(M.U. 2003)**

Sol. : Now $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (12, 12), (1, 2), (1, 3), (1, 4), (1, 12), (2, 4), (2, 12), (3, 12), (4, 12)\}$

Let a, b, c be any three elements of A

(i) Since $a \mid a$, R is reflexive.

(ii) If $a \mid b$ and $b \mid a$ then $a = b$.

$\therefore$ R is antisymmetric.

(iii) If $a \mid b$ and $b \mid c$ then $a \mid c$

$\therefore$ R is transitive.

$\therefore$ R is a partial order relation on A.

And (A, R) is a poset. The digraph of the poset is shown in Fig. 4.2.

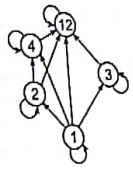


Fig. 4.2

Note : If n is a positive integer then we shall denote the set of all positive divisors of n by D_n. Thus, by this notation $D_4 = \{1, 2, 4\}$, $D_9 = \{1, 3, 9\}$, $D_{12} = \{1, 2, 3, 4, 6, 12\}$, $D_{20} = \{1, 2, 4, 5, 10, 20\}$. (See Ex. 11 (a), page 4-11, Ex. 15, 16, page 4-15, Ex. 21 (i), page 4-17.)

(a) To Construct Hasse Diagram

Step 1 : Delete the loop at each vertex. The result is Fig. 4.3 (a).

Step 2 : Delete the edges implied by the transitivity. For instance, since $1 \to 2$, $2 \to 4$, hence, $1 \to 4$, we delete the edge from 1 to 4. Similarly, we delete edges from 1 to 12, and from 2 to 12. The result is Fig. 4.3 (b).

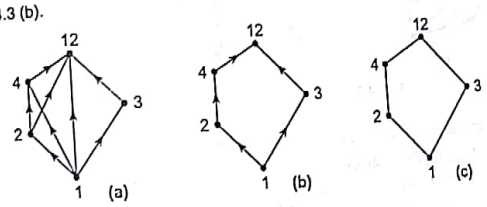


Fig. 4.3

Step 3 : Rearrange the digraph, if necessary, such that all edges go "upward". In the present diagram all the edges are pointing upwards. Hence, we need only to drop the arrow heads. The result is the Hasse diagram shown in Fig. 4.3 (c).

Such a diagram is called **Hasse diagram** which is defined below.

Definition : A **Hasse diagram** of a poset (A, R) is a figure in which

(i) the vertices represent the elements of A.

(ii) there is an upward line from x to y whenever $x \, R \, y$ and $x \neq y$.

(iii) the figure has **least number** of segments that accomplish the property (ii).

Example 2 : Construct the digraph and the Hasse diagram for the poset $(A, |)$ where $A = \{1, 2, 3, 4, 6, 8\}$ and $|$ denotes the divisibility relation.

Sol. : Now, $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (6, 6), (8, 8), (1, 2), (1, 3), (1, 4), (1, 6), (1, 8), (2, 4), (2, 6), (2, 8), (3, 6), (4, 8)\}$

Let a, b, c be any three elements of A

(i) Since $a \mid a$ R is reflexive.

$$M_R = \begin{array}{c} \\ 3 \\ 5 \\ 30 \end{array} \begin{array}{c} \begin{array}{ccc} 3 & 5 & 30 \end{array} \\ \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \end{array}$$

We first find the digraph [Fig. 4.11 (a)].

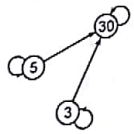


Fig. 4.11 (a)

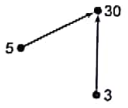


Fig. 4.11 (b)

Fig. 4.11 (c)

Step 1 : Delete all the loops [Fig. 4.11 (b)].

Step 2 : Delete all the edges implied by transitivity. There is none such edge.

Step 3 : Drop the arrow heads [Fig. 4.11 (c)]. The result is Hasse diagram [Fig. 4.11 (c)]. The poset is not a chain because $3 \not\leq 5$. See the definition (d), page 4-4.

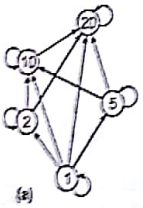
(c) The partial order relation "divides" on the set {1, 2, 5, 10, 20} is

$R = \{(1, 1), (1, 2), (1, 5), (1, 10), (1, 20), (2, 2), (2, 10)$
$(2, 20), (5, 5), (5, 10), (5, 20), (10, 10), (10, 20), (20, 20)\}$

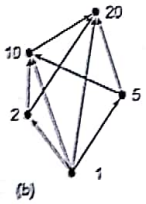
The matrix of the relation is

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 5 \\ 10 \\ 12 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 5 & 10 & 20 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

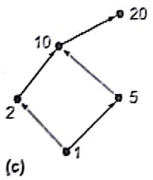
We first find the digraph [Fig. 4.12 (a)].



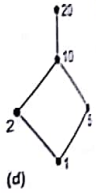
(a)



(b)



(c)



(d)

Fig. 4.12

Step 1 : Delete all the loops [Fig. 4.12 (b)].

Step 2 : Delete all the edges implied by transitivity. Delete the edges from 1 to 10, from 1 to 20, 2 to 20 and from 5 to 20 [Fig. 4.12 (c)].

Step 3 : Drop the arrow heads. The result is the Hasse diagram [Fig. 4.12 (d)]. The poset is not a chain because $2 \not\leq 5$. See the definition (d), page 4-4.

Example 6 : Draw two Hasse diagrams of posets with three elements. **(M.U. 2009)**

Sol. : Let $A = \{1, 2, 3\}$.

Let $R_1 = (A, \leq)$ and $R_2 = (A, \geq)$.

Then both R_1 and R_2 are reflexive, antisymmetric and transitive.

(See Ex. 2, page 4-1 and Ex. 3, page 4-2)

Hence, R_1 and R_2 both are posets.

Their Hasse diagrams are shown in Fig. 4.13 (a) and (b).

(See also Theorem given on page 4-23 and Ex. 1 (c), Ex. 2 of Exercise IV on page 4-24.)

(a) (b)

Fig. 3.13

Example 7 : Construct the Hasse diagram of the following relation R

(a) $A = \{1, 2, 3, 4\}$
$R = \{(1, 1), (1, 2), (2, 2), (2, 4), (1, 3), (3, 3), (3, 4), (1, 4), (4, 4)\}$ **(M.U. 2008)**

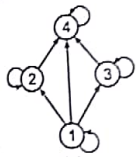
(b) $A = \{1, 2, 3, 4, 5\}$
$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (2, 2), (2, 4), (3, 3), (3, 5), (4, 4), (5, 5)\}$
(M.U. 1996)

Sol. : (a) We first find the digraph [Fig. 4.14 (a)].

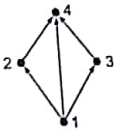
Step 1 : Delete all the loops [Fig. 4.14 (b)].

Step 2 : Delete the edges that are implied by transitivity *i.e.* delete the edge from 2 to 4 [Fig. 4.14 (c)].

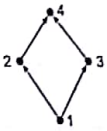
Step 3 : Drop the arrow heads. The result is Hasse diagram [Fig. 4.14(d)].



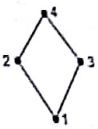
(a)



(b)



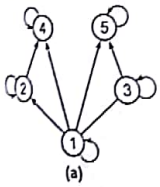
(c)



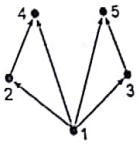
(d)

Fig. 4.14

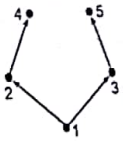
(b) We first find the digraph of the relation [Fig. 4.15 (a)].



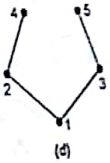
(a)



(b)



(c)



(d)

Fig. 4.15

Step 1 : Delete all the loops [Fig. 4.15 (b)].

Step 2 : Delete the edges that are implied by the transitivity. Delete the edges from 1 to 4 and from 1 to 5 [Fig. 4.15 (c)].

Step 3 : Delete all the arrow heads. The result is the Hasse diagram [Fig. 4.15 (d)].

Example 8 : Let $A = \{a, b, c, d\}$ and R be the relation on A whose matrix is

$$M_R = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

Construct the Hasse diagram of R.

Also prove that R is a partial order. (M.U. 2007) (M.U. 2010)

Sol. : The relation R is

$R = \{(a, a), (a, c), (a, d), (b, b), (b, c), (b, d), (c, c), (c, d), (d, d)\}$

We first find the diagraph of R [Fig. 4.16 (a)].

Step 1 : Delete the loops [Fig. 4.16 (b)].

Step 2 : Delete the edges that are implied by transitivity *i.e.* delete the edge from a to d and from b to d [Fig. 4.16 (c)].

Step 3 : Delete the arrow heads. The result is the Hasse diagram [Fig. 4.16 (d)].

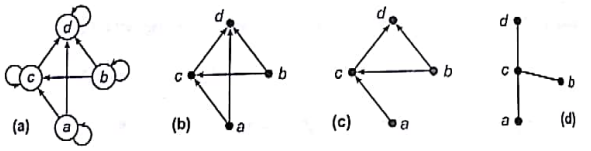


Fig. 4.16

Since R is reflexive, transitive and antisymmetric, it is a poset.

Example 9 : Determine the Hasse diagram of the partial order having the digraph shown in Fig. 4.17. (M.U. 2008)

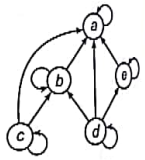


Fig. 4.17

Sol. : Step 1 : First delete the loops [Fig. 4.18 (a)].

Step 2 : Delete the edges implied by transivity *i.e.* delete the edge from c to a and from d to a. [Fig. 4.18 (b) below].

Step 3 : Delete the arrow heads. The result is the Hasse diagram [Fig. 4.18 (c) below].

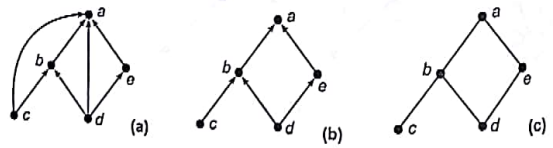


Fig. 4.18

Example 10 : Determine the Hasse diagram of the relation on $A = \{1, 2, 3, 4, 5\}$ whose matrix is shown below.

(a) $M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$ (M.U. 2011, 13)

(b) $M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$ (M.U. 2000, 05)

Sol. : We shall show below the diagrams involved leaving the explanation to you.

(a)

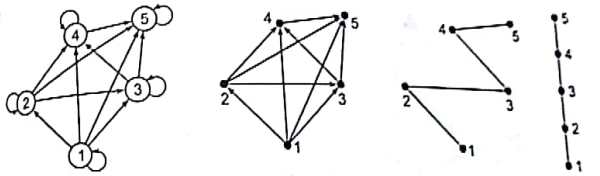


Fig. 4.19

(b)

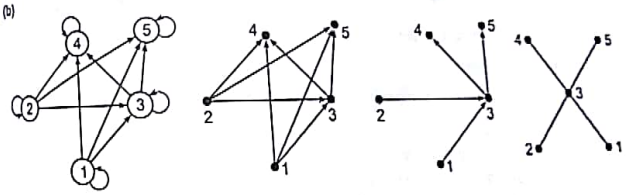


Fig. 4.20

Example 11 : Determine the matrix of the partial order relation of "divisibility" on the following set S. Draw the Hasse diagram of the poset. Indicate those which are chains.

(a) $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$,

(b) $B = \{3, 6, 12, 36, 72\}$

(c) $C = \{2, 4, 8, 16, 32\}$ (M.U. 2003)

Sol. : (a) We show below the matrix of the relation and the diagrams involved in the process of finding the Hasse diagram leaving the explanation to you.

$M_R =$

	1	2	3	5	6	10	15	30
1	1	1	1	1	1	1	1	1
2	0	1	0	0	1	1	0	1
3	0	0	1	0	1	0	1	1
5	0	0	0	1	0	1	0	1
6	0	0	0	0	1	0	0	1
10	0	0	0	0	0	1	0	1
15	0	0	0	0	0	0	1	1
30	0	0	0	0	0	0	0	1

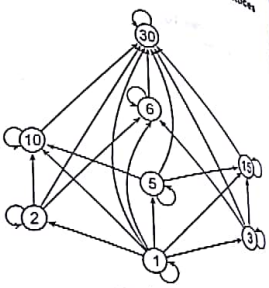


Fig. 4.21 (a)

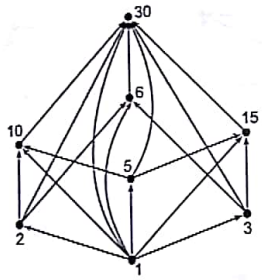


Fig. 3.21 (b)

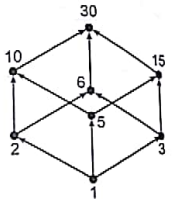


Fig. 4.21 (c)

The poset not a chain.

(b) $M_R =$

	3	6	12	36	72
3	1	1	1	1	1
6	0	1	1	1	1
12	0	0	1	1	1
36	0	0	0	1	1
72	0	0	0	0	1

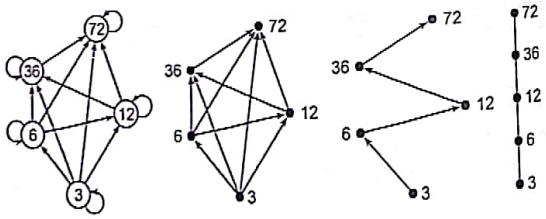


Fig. 4.22

The poset is a chain.

(c) $M_R =$

	2	4	8	16	32
2	1	1	1	1	1
4	0	1	1	1	1
8	0	0	1	1	1
16	0	0	0	1	1
32	0	0	0	0	1

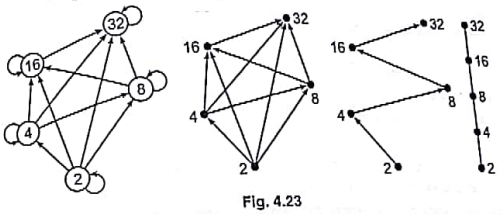
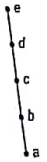


Fig. 4.23

The poset is a chain.



Example 12 : Let $A = \{a, b, c, d, e\}$ and let

$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (b, c), (c, d), (d, e), (a, c), (a, d), (a, e), (b, d), (b, e), (c, e)\}$

Draw the Hasse diagram.

Sol. : The Hasse diagram is as shown in adjoining figure.

Note that the elements are linearly ordered as every pair of A is comparable.

Note that the Hasse diagram of a finitely linearly ordered set is always of the form of this diagram which looks like a chain. Hence, the **finitely linearly ordered set** is called a chain.

Example 13 : Let $A = \{1, 2, 3, 6, 8, 12\}$ and R be the relation of "a divides b". Prove that $(A, |)$ is a poset. Draw the digraph and Hasse diagram of the poset.

Sol. : We leave it to you to write R and the matrix.

The digraph of the poset is shown in Fig. 4.24 (a).

The Hase diagram is shown in Fig. 4.24 (b).

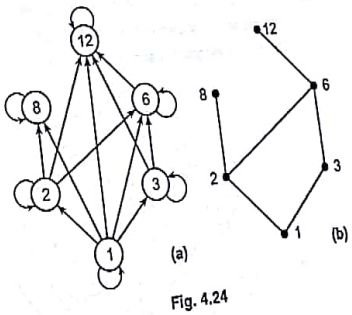


Fig. 4.24

Example 14 : Draw the Hasse diagram of the following sets under the partial order relation 'divides' and indicate those which are chains.

(a) $A = \{2, 4, 12, 24\}$, (b) $B = \{1, 3, 5, 15, 30\}$ **(M.U. 1998, 2016, 18)**

Sol. : We leave it to you to write R and the matrix.

The digraph of the poset is shown in Fig. 4.25 (a).

The Hasse diagram is shown in the Fig. 4.25 (b).

∴ The poset is a chain.

(b) We leave it to you.

The Hasse diagram is shown in the Fig. 4.25 (c).

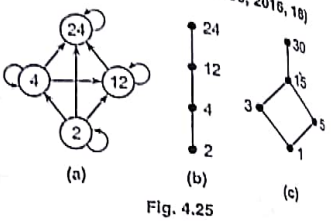


Fig. 4.25

Example 15 : Let $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and R be the relation 'is divisible by'. Obtain the relation matrix and draw the Hasse diagram.

Sol. : The relation matrix and the Hasse diagram are shown in Fig. 4.26.

	1	2	3	5	6	10	15	30
1	1	1	1	1	1	1	1	1
2	0	1	0	0	1	1	0	1
3	0	0	1	0	1	0	1	1
5	0	0	0	1	0	1	1	1
6	0	0	0	0	1	0	0	1
10	0	0	0	0	0	1	0	1
15	0	0	0	0	0	0	1	1
30	0	0	0	0	0	0	0	1

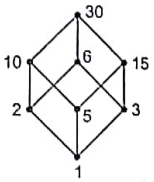


Fig. 4.26

Example 16 : Draw the Hasse diagram of D_{36}. **(M.U. 2006, 09)**

Sol. : We have $A = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$

The digraph is shown in the Fig. 4.27 (a).

The Hasse diagram is shown in the Fig. 4.27 (b).

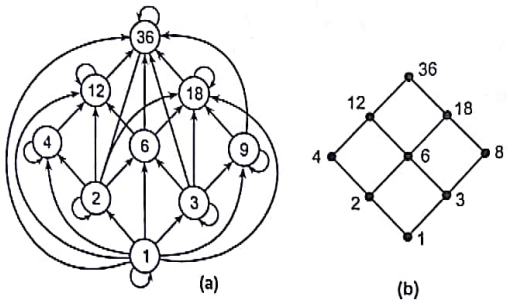


Fig. 4.27

Example 17 : Draw the Hasse diagram for the following set.

$\{(a, b) \mid a \text{ divides } b\}$ on $\{1, 2, 3, 4, 6, 8, 12\}$ **(M.U. 2002)**

Sol. : The matrix of the relation is

M =	1	2	3	4	6	8	12
1	1	1	1	1	1	1	1
2	0	1	0	1	1	1	1
3	0	0	1	0	1	0	1
4	0	0	0	1	0	1	1
6	0	0	0	0	1	0	1
8	0	0	0	0	0	1	0
12	0	0	0	0	0	0	1

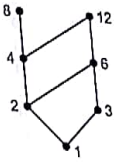


Fig. 4.28

The Hasse diagram is shown in Fig. 4.28.

Example 18 : (a) Let $A = \{1, 2, 3, 4\}$ and R be the relation is 'less than or equal to'. (b) Let $B = \{\Phi, \{a\}, \{a, b\}, \{a, b, c\}\}$ and R be the relation $\subseteq$. Draw the Hasse diagrams. Show that the sets are chains. **(M.U. 2013)**

Sol. : The Hasse diagrams are as shown in Fig. 4.29 (a) and 3.29 (b).

Note : The sets A and B given above are totally ordered.

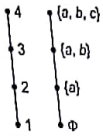


Fig. 4.29

Example 19 : Let $A = \{a, b, c\}$. Show that $(\mathcal{P}(A), \subseteq)$ is a poset and draw its Hasse diagram. **(M.U. 2013, 15, 17)**

Sol. : When $A = \{a, b, c\}$

$\mathcal{P}(A) = \{\Phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

(a) (i) For $\mathcal{P}(A)$, set inclusion $\subseteq$ relation R is reflexive because for every $B \in \mathcal{P}(A)$.

∴ $B \subseteq B$

(ii) If $B \subseteq C$ and $C \subseteq B$, then $B = C$.

∴ R is antisymmetric.

(iii) If $B \subseteq C$ and $C \subseteq D$, then $B \subseteq D$.

∴ R is transitive. ∴ R is a poset.

(b) The partial order relation $\subseteq$ is given below

$R = \{\{\{\Phi\}, \{\Phi\}\}, \{\{\Phi\}, \{a\}\}, \{\{\Phi\}, \{b\}\}, \{\{\Phi\}, \{c\}\}, \{\{\Phi\}, \{a, b\}\}, \{\{\Phi\}, \{a, c\}\},$
$\{\{\Phi\}, \{b, c\}\}, \{\{\Phi\}, \{a, b, c\}\}, \{\{a\}, \{a\}\}, \{\{a\}, \{a, b\}\}, \{\{a\}, \{a, c\}\}, \{\{a\}, \{a, b, c\}\},$
$\{\{b\}, \{b\}\}, \{\{b\}, \{a, b\}\}, \{\{b\}, \{b, c\}\}, \{\{b\}, \{a, b, c\}\}, \{\{c\}, \{c\}\}, \{\{c\}, \{a, c\}\},$
$\{\{c\}, \{a, b, c\}\}, \{\{a, b\}, \{a, b\}\}, \{\{a, b\}, \{a, b, c\}\}, \{\{b, c\}, \{b, c\}\}, \{\{b, c\}, \{a, b, c\}\},$
$\{\{a, c\}, \{a, c\}\}, \{\{a, c\}, \{a, b, c\}\}, \{\{a, b, c\}, \{a, b, c\}\}\}$

(c) The Matrix of the above relation is

$$M_R = \begin{array}{c} \\ \Phi \\ \{a\} \\ \{b\} \\ \{c\} \\ \{a, b\} \\ \{b, c\} \\ \{a, c\} \\ \{a, b, c\} \end{array} \begin{array}{c} \begin{array}{cccccccc} \Phi & \{a\} & \{b\} & \{c\} & \{a, b\} & \{b, c\} & \{a, c\} & \{a, b, c\} \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

(d) The Hasse diagram is shown in Fig. 4.30.

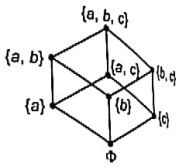


Fig. 4.30

Example 20 : Determine the matrix of the partial order relation of divisibility on the set A. Draw Hasse diagrams of the posets. Indicate those which are chains.

(a) $B = \{3, 6, 12, 36, 72\}$

(b) $C = \{2, 4, 8, 16, 32\}$ **(M.U. 2003)**

Sol. : (b) $B = \{3, 6, 12, 36, 72\}$

$R = \{ (3, 3), (3, 6), (3, 12), (3, 36), (3, 72), (6, 6), (6, 12), (6, 36), (6, 72), (12, 12), (12, 36), (12, 72), (36, 36), (36, 72), (72, 72) \}$

The matrix of the relation is

$$M = \begin{array}{c} \\ 3 \\ 6 \\ 12 \\ 36 \\ 72 \end{array} \begin{array}{c} \begin{array}{ccccc} 3 & 6 & 12 & 36 & 72 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

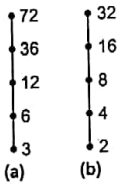


Fig. 4.31

The Hasse diagram is shown in Fig. 4.31 (b).

(b) $C = \{2, 4, 8, 16, 32\}$

$R = \{ (2, 2), (2, 4), (2, 8), (2, 16), (2, 32), (4, 4), (4, 8), (4, 16), (4, 32), (8, 8), (8, 16), (8, 32), (16, 16), (16, 32), (32, 32) \}$

The matrix of the relation is

$$M = \begin{array}{c} \\ 2 \\ 4 \\ 8 \\ 16 \\ 32 \end{array} \begin{array}{c} \begin{array}{ccccc} 2 & 4 & 8 & 16 & 32 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

Both are chains. The Hasse diagram is shown in Fig. 4.31 (b).

Example 21 : Draw the Hasse diagram of the following sets under the partial order relation of divisibility and indicate which are chains.

(i) $A = \{2, 4, 12, 24\}$, (ii) $A = \{1, 3, 5, 15, 30\}$ **(M.U. 1997)**

Sol. : (i) $A = \{2, 4, 12, 24\}$

$R = \{ (2, 2), (2, 4), (2, 12), (2, 24), (4, 4), (4, 12), (4, 24), (12, 12), (12, 24), (24, 24) \}$

The matrix of the relation is

$$M_R = \begin{array}{c} \\ 2 \\ 4 \\ 12 \\ 24 \end{array} \begin{array}{c} \begin{array}{cccc} 2 & 4 & 12 & 24 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

Fig. 3.32

The Hasse diagram is shown in Fig. 4.32. This is a chain.

(ii) $A = \{1, 3, 5, 15, 30\}$

$R = \{ (1, 1), (1, 3), (1, 5), (1, 15), (1, 30), (3, 3), (3, 5), (3, 15), (3, 30), (5, 5), (5, 15), (5, 30), (15, 15), (15, 30), (30, 30) \}$

The matrix of the relation is

$$M_R = \begin{array}{c} \\ 1 \\ 3 \\ 5 \\ 15 \\ 30 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 3 & 5 & 15 & 30 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

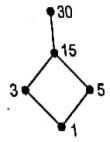


Fig. 4.33

The Hasse diagram is shown in Fig. 4.33.

Example 22 : If P_1 and P_2 are the posets shown in Fig. 4.34 (a). Draw the Hasse diagram of $P_1 \times P_2$ with product partial order.

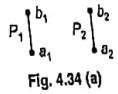


Fig. 4.34 (a)

Sol. : The cartesian product

$$P_1 \times P_2 = \{(a_1, a_2), (a_1, b_2), (b_1, a_2), (b_1, b_2)\}$$

Since $a_1 \le b_1$ and $a_2 \le b_2$, we get the Hasse diagram as shown in Fig. 4.34 (b).

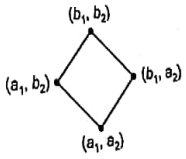


Fig. 4.34 (b)

Example 23 : If P_1 and P_2 are the posets given in Fig. 4.35 (a) and 4.35 (b). Draw the Hasse diagram of $P_1 \times P_2$. **(M.U. 1997, 2013)**

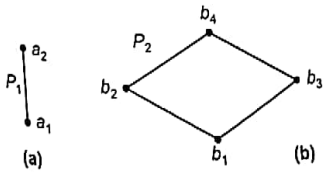


Fig. 4.35

Sol. : The cartesian product

$P_1 \times P_2 = \{ (a_1, b_1), (a_1, b_2), (a_1, b_3), (a_1, b_4), (a_2, b_1), (a_2, b_2), (a_2, b_3), (a_2, b_4) \}$

Since, $a_1 \le a_2$, $b_1 \le b_2$, $b_1 \le b_3$, $b_2 \le b_4$, $b_3 \le b_4$, we get the Hasse diagram as shown in Fig. 4.35 (c).

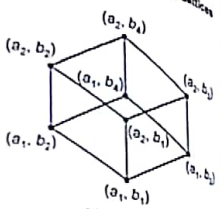


Fig. 4.35 (c)

Example 24 : Given the posets $(D_4, \le)$ and $(D_9, \le)$ under the usual notation of divisibility, draw the Hasse diagram of $L = D_4 \times D_9$ under the product partial order. **(M.U. 2015)**

OR - Draw Hasse diagram of D_{36}. **(M.U. 2006, 09, 14)**

OR - Consider the lattices $L_1 = \{1, 2, 4\}$, $L_2 = \{1, 3, 9\}$ under divisibility. Draw the lattice $L_1 \times L_2$. **(M.U. 2014)**

Sol. : Let us denote the two posets by P_1 and P_2, the set of divisors of 4 and 9 and R is $\le$.

$\therefore \quad P_1 = \{1, 2, 4\}, \qquad P_2 = \{1, 3, 9\}$

The Hasse diagrams of P_1 and P_2 are shown in Fig. 4.36 (a) and Fig. 4.36 (b).

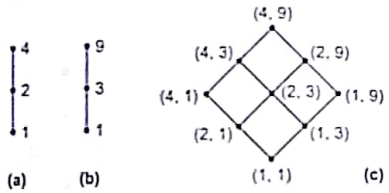


Fig. 4.36

The cartesian product

$P_1 \times P_2 = \{(1, 1), (1, 3), (1, 9), (2, 1), (2, 3), (2, 9), (4, 1), (4, 3), (4, 9)\}$

In Hasse diagram of $P_1 \times P_2$, we must have $a_1 \le a_2$, $b_1 \le b_2$ for all a's and b's, we get the Hasse diagram of $P_1 \times P_2$ as shown in Fig. 4.36 (c) above.

EXERCISE - II

1. Let $S = \{a, b, c\}$ and $A = \mathcal{P}(S)$. Draw the Hasse diagram of the poset A with the relation $\subseteq$ (set inclusion).

[Ans. : $A = \mathcal{P}(S)$

$= \{\Phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}\}$.

See Fig. 4.37]

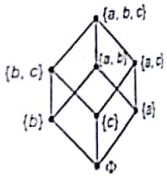


Fig. 4.37

2. Draw Hasse diagrams of the following relations.

(i) $R_1 = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (2, 2), (2, 3), (2, 4), (2, 5), (3, 3), (3, 4), (3, 5), (4, 4), (4, 5), (5, 5)\}$

(ii) $R_2 = \{(1, 1), (1, 3), (1, 4), (1, 5), (2, 2), (2, 3), (2, 4), (2, 5), (3, 3), (3, 4), (3, 5), (4, 4), (4, 5)\}$

(M.U. 2013) [Ans. : See Ex. 10, page 4-11]

3. Let $A = \{1, 2, 3, 4\}$, $R = \{(1, 1), (1, 2), (2, 2), (2, 4), (1, 3), (3, 3), (3, 4), (1, 4), (4, 4)\}$. Draw Hasse diagram. Show that it is a poset.

[Ans. : See Fig. 4.38]

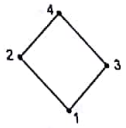


Fig. 4.38

4. Determine the Hasse diagram of the relation on $A = \{a, b, c, d, e\}$ whose matrix is shown below.

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array} \begin{array}{c} \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

[Ans. : Same as in solved Ex. 12, page 4-12. See Hasse diagram of Ex. 12, page 4-12]

5. Draw the Hasse diagram of the relation on $A = \{a, b, c, d, e\}$ whose matrix is

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array} \begin{array}{c} \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

[Ans. : Same as in solved Ex. 4, page 4-6. See Fig. 4.9 (b), page 4-7]

6. Let $A = \{a, b, c, d, e\}$ and

$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, c), (a, e), (b, c), (b, d), (b, e), (c, e), (d, e)\}$.

Prove that (A, R) is a poset. Draw its digraph and Hasse diagram.

[Ans. :

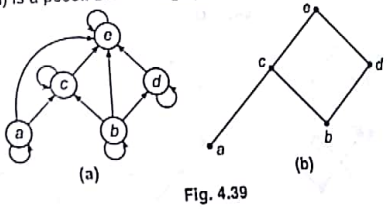


Fig. 4.39

7. Let $A = \{1, 2, 3, 4, 6, 8, 12, 24\}$ and R be the relation of 'is divisible by' *i.e.* $a \, R \, b$ means $a \mid b$. Draw the Hasse diagram.

(M.U. 1996) [Ans. : See Fig. 4.40]

8. Let $A = \{2, 4, 8, 16, 32\}$ and R be the relation of 'd is divisible by' *i.e.* $a \, R \, b$ if $a \mid b$. Draw the Hasse diagram. Is it linearly ordered ?

[Ans. : See Fig. 4.41. Yes]

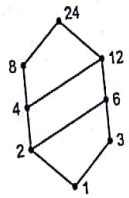


Fig. 4.40

Fig. 4.41

9. Draw the Hasse diagram of the relation R.

(a) $A = \{1, 5, 6, 30\}$
$R = \{(1, 1), (1, 5), (5, 5), (5, 30), (1, 6), (6, 6), (6, 30), (1, 30), (30, 30)\}$

(b) $A = \{1, 2, 3, 4, 5\}$
$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (2, 4), (3, 5), (2, 2), (3, 3), (4, 4), (5, 5)\}$

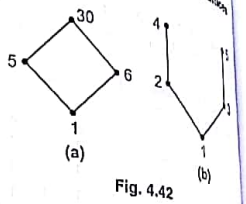


Fig. 4.42

(M.U. 1996) [**Ans. :** See Fig. 4.42 (a) and (b)]

10. Let $A = \{2, 3, 6, 12, 24, 36\}$ and R be the relation 'is divisible by' *i.e.* $a\ R\ b$ means $a \mid b$. Obtain the relation matrix and draw Hasse diagram. **(M.U. 2005, 07, 17)**

[**Ans. :**

	2	3	6	12	24	36
2	1	0	1	1	1	1
3	0	1	1	1	1	1
6	0	0	1	1	1	1
12	0	0	0	1	1	1
24	0	0	0	0	1	0
36	0	0	0	0	0	1

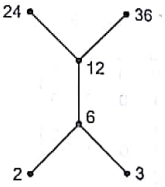


Fig. 4.43

11. Let $A = \{3, 4, 12, 24, 48, 72\}$ and the relation $\leq$ be $a\ R\ b$ if a divides b. Obtain the Hasse diagram. [**Ans. :** M_R not given. For Hasse diagram see Fig. 4.44]

12. Let $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$ and the relation $\leq$ be $a\ R\ b$ if a divides b. Obtain the relation matrix and draw the Hasse diagram.

[**Ans. :** M_R not given. For Hasse diagram see Fig. 4.45]

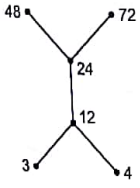


Fig. 4.44

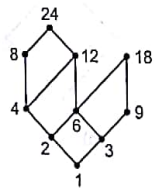


Fig. 4.45

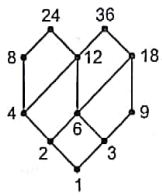


Fig. 4.46

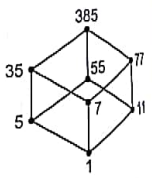


Fig. 4.47

13. Let $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36\}$ and the relation $\leq$ be $a\ R\ b$ if a divides b. Obtain the matrix of the relation and Hasse diagram.

[**Ans. :** M_R not given. For Hasse diagram See Fig. 4.46 above.]

14. Draw Hasse diagram for D_{385}. [**Ans. :** For Hasse diagram See Fig. 4.47 above]

15. Let $A = \{1, 2, 3, 4, 6, 12\}$ and R be the relation 'is divisible by'. Obtain the relation matrix and draw Hasse diagram.

[**Ans. :**

	1	2	3	4	6	12
1	1	1	1	1	1	1
2	0	1	0	1	1	1
3	0	0	1	0	1	1
4	0	0	0	1	0	1
6	0	0	0	0	1	1
12	0	0	0	0	0	1

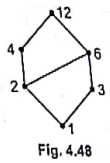


Fig. 4.48

16. Let $A = \{1, 3, 5, 9, 15, 45\}$ and R be the relation 'is divisible by'. Obtain the relation matrix and draw Hasse diagram.

[**Ans. :**

	1	3	5	9	15	45
1	1	1	1	1	1	1
3	0	1	0	1	1	1
5	0	0	1	0	1	1
9	0	0	0	1	0	1
15	0	0	0	0	1	1
45	0	0	0	0	0	1

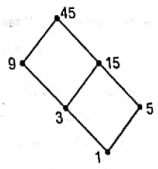


Fig. 4.49

17. Draw Hasse diagrams of D_{72} and D_{105}. **(M.U. 2014)**

[**Ans. :** Hasse diagram of $D_{72} = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72\}$ [Fig. 4.50 (a)]

Hasse diagram of $D_{105} = \{1, 3, 5, 7, 15, 21, 35, 105\}$ [Fig. 4.50 (b)]

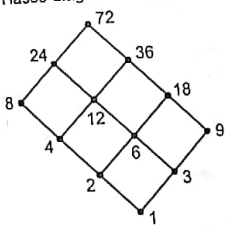


Fig. 4.50 (a)

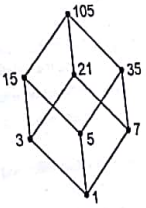
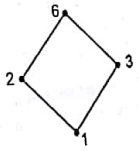


Fig. 4.50 (b)

18. Let $A = \{1, 2, 3, 6\}$,
$B = \{1, 2, 3, 6, 7, 14, 21, 42\}$
R be the relation 'is divisible by'. Draw Hasse diagram for the two sets. Show that they are posets.

[**Ans. :** See Fig. 4.51 (a) and 3.51 (b).]



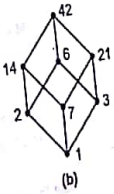


Fig. 4.51

19. If P_1 and P_2 are the posets given in Fig. 4.52 below. Draw the Hasse diagram of $P_1 \times P_2$.

[**Ans. :** Similar to Fig. 4.51 (a)]

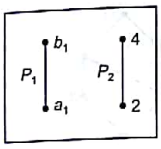


Fig. 4.52

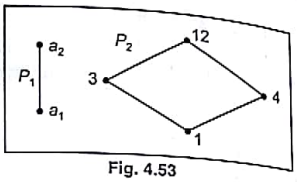


Fig. 4.53

20. If P_1 and P_2 are the posets given in Fig. 4.53 above. Draw the Hasse diagram of $P_1 \times P_2$.

[**Ans. :** Similar to Fig. 4.51 (b)]

(b) To Find the Relation From a Hasse Diagram

To solve the converse of the above problem *i.e.* to find the relation from the Hasse diagram we reverse the above steps.

(i) Put a loop at each vertex of the given Hasse diagram.

(ii) Join the vertices which are connected through intermediate points.

(iii) Put upward arrows for all segements.

(iv) The vertices connected as above are related.

(v) Write the relation set.

Example 1 : Find the relation set R for the Hasse digram shown in Fig. 4.54 (a).

Sol. : 1. Put a loop at each vertex.

2. Since a is connected to c and c is connected to d, join a to d. Since b is connected to c and c is connected to e, join b to e. Similarly, join a to e and b to d. (Do not connect ed. Why? For the same reason do not connect ab. This is so because arrow head showing the relationship go upwards only.)

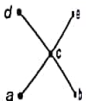


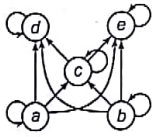
Fig. 4.54 (a)

3. Now put an arrow head on each segement.

4. Two elements which are thus connected by a line segment with an arrow head are related.

In this way we get the following matrix of the relation.

$$M_R = \begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array} \begin{array}{c} \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$



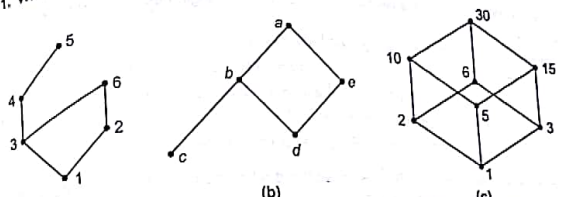
From this matrix, we get the following relation.

$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, c), (a, d), (a, e), (b, c), (b, d), (b, e), (c, d), (c, e)\}$

(**Note** that since a Hasse digram is related to a poset, R is **not symmetric.**)

EXERCISE - III

1. Write the relation set corresponding to the following Hasse diagrams.



(a) (b) (c)

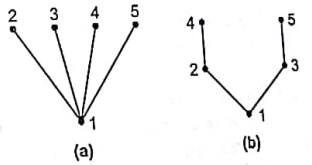
Fig. 4.55

[**Ans. :** (a) { (1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (1, 2), (1,3), (1, 4), (1, 5), (1, 6), (2, 6), (3, 4), (3, 5), (3, 4), (4, 5) }

(b) { (*a*, *a*), (*b*, *b*), (*c*, *c*), (*d*, *d*), (*e*, *e*), (*b*, *a*), (*c*, *b*), (*c*, *a*), (*c*, *b*), (*d*, *b*), (*d*, *a*), (*d*, *e*), (*e*, *a*) }

(c) {(1, 1), (2, 2), (3, 3), (5, 5), (6, 6), (10, 10), (15, 15), (30, 30), (1, 2), (1, 3), (1, 5), (1, 6), (1, 10), (1, 15), (1, 30), (2, 6), (2, 10), (2, 30), (3, 6), (3, 15), (3, 30), (6, 30), (10, 30), (15, 30) }]

2. Determine the matrix of the partial order whose Hasse digram are given below.



(a) (b)

Fig. 4.56

[**Ans. :** (a)

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

(b)

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

(c) Dual of Poset

Theorem : If R is a partial order relation on A then R^{-1} *i.e.* the inverse relation is also a partial order on A *i.e.* if (A, R) is a poset then (A, R^{-1}) also is a poset. **(M.U. 2004)**

Proof : Since R is a partial order on A, by definition, **(M.U. 2009)**

(i) R is reflexive *i.e.* $a\ R\ a$.

(ii) R is antisymmetric *i.e.* if $a\ R\ b$ and $b\ R\ a$ then $a = b$.

(iii) If $a\ R\ b$ and $b\ R\ c$ then $a\ R\ c$ transmitivity.

Also by definition R^{-1} is a relation obtained by interchanging the order of the elements in R *i.e.*, $b\ R^{-1}\ a$ if $a\ R\ b$.

Hence, if $a\ R\ a$, then $a\ R^{-1}\ a$ *i.e.*, R^{-1} is reflexive.

If $a\ R\ b$ and $b\ R\ a$ imply $a = b$ then $b\ R^{-1}\ a$ and $a\ R^{-1}\ b$ imply $a = b$.

If $a\ R\ b$ and $b\ R\ c$ imply $a\ R\ c$ then $b\ R^{-1}\ a$ an $c\ R^{-1}\ b$ *i.e.*, ($c\ R^{-1}\ b$ and $b\ R^{-1}\ a$) imply $c\ R^{-1}\ a$

$\therefore$ R^{-1} is also an partial order relation.

Thus, if (A, R) is a poset then (A, R^{-1}) is also a poset. (See Ex. 6, page 4-9)

Definition : The poset (A, R^{-1}) is called the **dual** of the poset (A, R) and the partial order R^{-1} is called **dual** of the partial order R. (M.U. 2009)

Example : From the Hasse diagram given in Fig. 4.57 (a), find the poset and construct the Hasse diagram of its dual.

Sol. : As discussed earlier [in (b), page 4-22] from a given Hasse diagram we obtain the poset by (i) putting the loop on every element (ii) by putting the upward arrows.

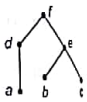


Fig. 4.57 (a)

We shus get the poset shown in Fig. 4.57 (b).

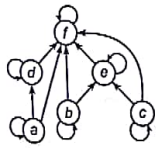


Fig. 4.57 (b)

From the diagram of Fig. 4.57 (b), we get the following partial order relation.

$R = \{ (a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (a, d), (d, f), (a, f), (b, e), (e, f), (b, f), (c, e), (c, f) \}$

The dual of the partial order relation R is obtained by reversing the order of the elements. Hence,

Dual of $R = R^{-1}$

$= \{ (a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (d, a), (f, d), (f, a), (e, b), (f, e), (f, b), (e, c), (f, c) \}$

The Hasse diagram of dual of R is obtained by reversing the order of elements which means by **turning the Hasse diagram of R upside down.** [Fig. 4.57 (c)]

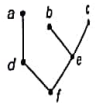
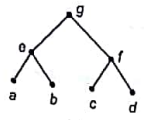


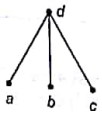
Fig. 4.57 (c)

EXERCISE - IV

1. Find the partial order relation from the following Hasse diagrams and obtain the Hasse diagrams of their duals.

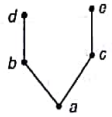


(a)



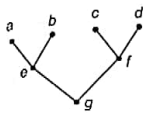
(b)

(c)

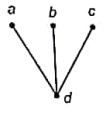


(d)

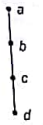
[Ans. :



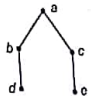
(a)



(b)



(c)



(d)

2. Prove that on the set of integers $\leq$ is a partial order relation and prove that $\geq$ is its dual. Further prove that both partial order relations are chains.

(d) Product Partial Order

If $(A, \leq_1)$, $(B, \leq_2)$ are posets then partial order $\leq_3$ defined on the cartesian product $A \times B$ by $(a, b) \leq_3 (a', b')$ where $a \leq_1 a'$ in A and $b \leq_2 b'$ in B is called the **product partial order.** (See Ex. 22, 23, 24 on page 4-17 and 4-18)

Theorem : If $(A, \leq_1)$ and $(B, \leq_2)$ are posets then $(A \times B, \leq_3)$ is a poset with partial order $\leq_3$ defined by

$(a, b) \leq_3 (a', b')$ where $a \leq_1 a'$ in A and $b \leq_2 b'$ in B.

Proof : We have to prove that the relation $\leq_3$ is (i) reflexive, (ii) anti-symmetric and (iii) transitive in $(A \times B)$.

(i) If $(a, b) \in A \times B$ then clearly $(a, b) \leq_3 (a, b)$ because $a \leq_1 a$ in A and $b \leq_2 b$ in B.

$\therefore$ $\leq_3$ is reflexive in $A \times B$.

(ii) Let $(a, b) \leq_3 (a', b')$ and $(a', b') \leq_3 (a, b)$ where $a, a' \in A$ and $b, b' \in B$.

By definition of product partial order given above

$a \leq_1 a'$ and $a' \leq_1 a$ in A ..... (1)

and $b \leq_2 b'$ and $b' \leq_2 b$ in B. ..... (1)

Since, A and B are posets the relations $\leq_1$ and $\leq_2$ are antisymmetric in A and B.

$\therefore$ From (1), we get, $a = a'$, $b = b'$.

$\therefore$ $\leq_3$ is antisymmetric in $A \times B$.

(iii) Let $(a, b) \leq_1 (a', b')$ and $(a', b') \leq_2 (a'', b'')$ where $a, a', a'' \in A$ and $b, b', b'' \in B$.

$\therefore$ $a \leq_1 a'$, $b \leq_2 b'$ and $a' \leq_1 a''$, $b' \leq_2 b''$.

Since $a \leq_1 a'$ and $a' \leq_1 a''$ and since A is a poset by transitivity property

$a \leq_1 a''$.

Since, $b \leq_2 b'$, $b' \leq_2 b''$ and since B is a poset by transitivity property

$b \leq_2 b''$.

Hence, $(a, b) \leq_3 (a'', b'')$

$\therefore$ $\leq_3$ is transitive in $A \times B$.

$\therefore$ $(A \times B, \leq_3)$ is a poset.

Example 1 : Let $A = \{2, 3, 4, 6, 9, 12, 24\}$ and $S = A \times A$. A relation R is defined on S as $(a, b)\ R\ (a', b')$ if and only if $a \mid a'$ and $b \leq b'$. Show that (S, R) is a poset. (M.U. 2004)

Sol. : By the above theorem if $A = \{2, 3, 4, 6, 9, 12, 24\}$ with the relation a divides b is a poset and if $A = \{2, 3, 4, 6, 9, 12, 24\}$, with the relation a is less than b is a poset then $A \times B$ with $(a, b)\ R\ (a', b')$ where R is

Hence, we need to prove only that (i) $(A, |)$ is a poset and (ii) $(A, \leq)$ also is a poset.

Now, the Hasse diagram of $(A, |)$ and $(A, \leq)$ are shown in Fig. 4.58.

It can be seen from the Hasse diagrams that both $(A, |)$ and $(A, \leq)$ are posets.

Hence, by the above theorem $(A \times B, \leq')$ is also a poset.

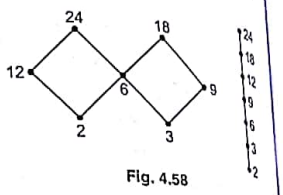


Fig. 4.58

Example 2 : See also Ex. 23, page 4-17.

4. Isomorphism

Definition : Let $(A, \leq)$ and $(B, \leq')$ be two posets and let a function $f : A \to B$ be a one-to-one correspondence between A and B such that for $a, b \in A$ and $f(a), f(b) \in B$, we have $a \, R \, b$ if and only if $f(a) \, R' \, f(b)$ *i.e.* $a \leq b$ if and only if $f(a) \leq' f(b)$.

The function f then is called an **isomorphism** from $(A, \leq)$ to $(B, \leq')$.

Further, if $f : A \to B$ is an isomorphism then the posets A and B are called **isomorphic posets.**

Example 1 : Let $A = \{1, 2, 3, 6\}$ and $B = \{1, 5, 6, 30\}$ and R be the relation 'a divides b' for both sets. Find the isomorphism between A and B, if it exists.

Sol. : Hasse diagrams of the two relations are shown in Fig. 4.59.

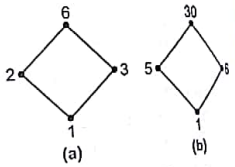


Fig. 4.59

If we define $f : A \to B$, by $f(1) = 1$, $f(2) = 5$, $f(3) = 6$ and $f(6) = 30$, we see that f is a one-to-one correspondence between A and B such that $a \, R \, b$ if and only if $f(a) \, R_1 \, f(b)$. Hence, f is an isomorphism.

If we compare the Hasse diagrams of the two posets we see that, they have the same form or shape. Hence, the name iso (similar) morphism (form) shape.

Example 2 : Let A be the set Z^+ of positive integers $\{1, 2, 3, 4, ...\}$ and let $\leq$ be the usual partial order relation on A. Let A' be the set of positive even integers $\{2, 4, 6, 8, ...\}$ and let $\leq'$ be the usual partial order relation on A'. Show that the function $f : A \to A'$ given by

$$f(a) = 2a$$

is an isomorphism for $(A, \leq)$ to $(A', \leq')$.

Sol. : We first note that f is one to one because if $f(a) = f(b)$ then $2a = 2b$, $\therefore a = b$. Further, Dom $(f) = A$, so f is everywhere defined. Also if $c \in A'$ then $c = 2a$ for some $a \in Z^+$. Therefore, $c = f(a)$. Hence, f is onto. Therefore, f is a one-to-one correspondence.

Now, if a and b are elements in A then $a \leq b$, if and only if $2a \leq 2b$.

$\therefore$ f is an isomorphism.

Example 3 : Let $A = \{1, 2, 3, 6\}$ and let $\leq$ be the relation 'is divisible by'. Let $A = \wp(\{a, b\}) = \{\Phi, \{a\}, \{b\}, \{a, b\}\}$ and let $\leq'$ be the relation $\subseteq$, is a subset of '. Let $f : A \to A'$ be defined by

$f(1) = \Phi$, $f(2) = \{a\}$, $f(3) = \{b\}$, $f(b) = \{a, b\}$.

Show that f is an isomorphism.

Sol. : Since every element of A is associated to one and only one element of A' and conversely every element of A' is associated with one and only one element of A, f is a one-to-one correspondence.

Further, if a and b are elements of A *i.e.* a divides b then $f(a) \subseteq f(b)$ and conversely if $f(a) \subseteq f(b)$ then a divides b.

$\therefore$ f is an isomorphism.

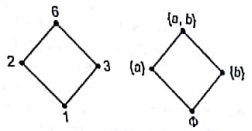


Fig. 4.60

The Hasse diagrams of the posets are shown in Fig. 4.60.

Example 4 : Let $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and let $\leq$ be the relation 'is divisible by'. Let $A' = \wp(\{a, b, c\}) = \{\Phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ and let $\leq'$ be the relation is 'a subset of'

If $f : A \to A'$ is defined by

$f(1) = \Phi$, $f(2) = \{a\}$, $f(3) = \{b\}$, $f(5) = \{c\}$, $f(6) = \{a, b\}$,

$f(10) = \{a, c\}$, $f(15) = \{b, c\}$, $f(30) = \{a, b, c\}$.

Show that f is an isomorphism.

Sol. : The Hasse diagrams for $(A, \leq)$ and $(A', \leq')$ are given in Fig. 4.77 on page 4-34 and in Fig. 4.79 (c) on page 4-36.

You can prove the result as above.

EXERCISE - V

1. Let $A = \{3, 6, 9, 36\}$ and R be 'a divides b'. Let $B = \wp(a, b) = \{\Phi, \{a\}, \{b\}, \{a, b\}\}$. Find the isomorphism between A and B.

[Ans. : $f(3) = \Phi$, $f(6) = \{a\}$, $f(9) = \{b\}$, $f(36) = \{a, b\}$. Hasse diagrams are similar to the above diagrams of Ex. 3. **]**

2. Let $A = \{1, 2, 3, 4, 6, 8, 12, 24\}$ and R be relation 'a divides b', $B = \wp(a, b, c)$ and R be the relation $\subseteq$.

Find the isomorphism between A and B. **[Ans. :** $f(1) = \Phi$, $f(2) = \{a\}$ etc. For figure of poset A see Fig. 4.22 and for figure of poset B see Fig. 4.19 **]**

3. Let $A = \{1, 2, 3, 6, 7, 14, 21, 42\}$ and R be the relation of divisibility. $B = \wp(a, b, c)$ and R be the relation of set inclusion $\subseteq$.

Find the isomorphism between A and B. **[Ans. :** Similar to the above. **]**

5. Extremal Elements of Posets

(M.U. 2008)

Certain elements of a poset are of special importance. We shall discuss these elements now and the importance of role played by them later. In this section and here after we shall denote the poset by $(A, \leq)$ where A is the set and $\leq$ is the partial order relation.

(M.U. 2008)

(a) Maximal and Minimal Elements

Definition 1 : An element $a \in A$ is called a **maximal element** of the poset A if there is no element $c \in A$ such that $a < c$.

In other words, an element a in a partially ordered set A is said to be **maximal** if no other element **succeeds** A *i.e.* if $a \leq x$ then $a = x$.

Definition 2 : An element $b \in A$ is called a **minimal element** of the poset A if there is no element $c \in A$ such that $c < b$.

In other words, an element b in a partially ordered set A is said to be **minimal** if no other element **precedes** b *i.e.* if $y \leq b$ then $y = b$.

We shall show below (Fig. 4.61) maximal and minimal elements of some posets diagrammatically.

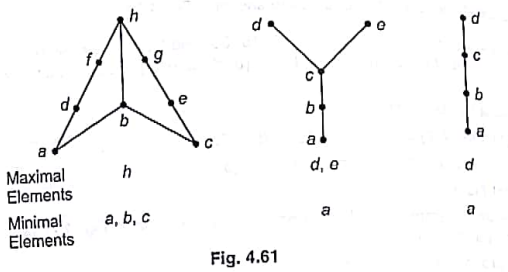


Fig. 4.61

Example 1 : Consider $A = \{ x \mid x \text{ is real and } 0 \leq x < 2\}$ with usual partial order $\leq$.

Then 0 is the minimal element. There is no maximal element. (This is so because $2 \notin A$)

Example 2 : Consider $A = \{ x \mid x \text{ is real and } 0 < x \leq 2\}$ with usual partial order $\leq$. **(M.U. 2008)**

Then 2 is the maximal element. There is no minimal element. (This is so because $0 \notin A$)

Example 3 : Consider $A = \{ x \mid x \text{ is real and } 0 \leq x \leq 2 \}$.

Then 0 is the minimal elements and 2 is the maximal element.

Example 4 : Let A be the poset of non-negative real numbers with usual partial order relation $\leq$ (less than or equal to).

Then 0 is the minimal element of A and there is no maximal element.

Example 5 : Let A be the poset of non-positive real numbers with usual partial order relation $\leq$

Then 0 is the maximal element and there is no minimal element.

Example 6 : Consider the poset Z with usual partial order relation $\leq$ (less than or equal to).

There is no minimal element of Z, there is no maximal element of Z.

Example 7 : In Ex. 2 page 4-5 the poset A has two maximal elements 6 and 8 and one minimal element 1.

Example 8 : In Ex. 10 page 4-20, there are two minimal elements 2 and 3 and two maximal elements 24 and 36.

Example 9 : Let $S = \{2, 4, 6, 12, 20\}$ be ordered by the relation of divisibility. Draw Hasse diagram and find the maximal and minimal elements of S.

Sol. : 12 and 20 are maximal elements. 2 is the minimal element.

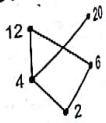


Fig. 4.62

Example 10 : Let $S = \{2, 3, 4, 16\}$ be ordered by the relation of divisibility. Draw Hasse diagram and find the maximal and minimal elements.

Sol. : 3 and 16 are maximal elements. 2 and 3 are minimal elements.

Note that 3 is both maximal and minimal element because 3 is not comparable with any other element.

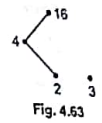


Fig. 4.63

Example 11 : Find the maximal and mimal element of the poset shown in Fig. 4.64.

Sol. : d and g are maximal elements, a and b are minimal elements.

We note the following properties of maximal and minimal elements of posets.

1. A poset may have **more than one maximal element** and more than one **minimal elements.**
2. A poset **need not have any maximal element** or any minimal **element.**
3. A poset may **have a maximal element but no minimal** elements or a **minimal element but no maximal** elements.

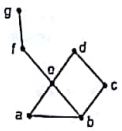


Fig. 4.64

Theorem 1 : Every **finite** non-empty poset $(A, \leq)$ has at least one minimal element. (Note 'finite')

Proof : We accept the theorem without proof.

Theorem 2 : Every **finite** non-empty poset $(A, \leq)$ has at least one maximal element. (Note 'finite')

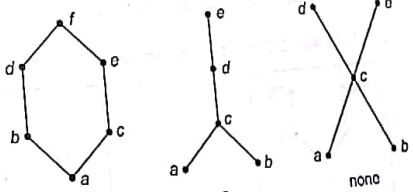
Proof : We accept the theorem without proof.

(M.U. 2008)

(b) Greatest and Least Elements

Let A be a finite non-empty poset. An element $a \in A$ is called a **greatest element** of A if $x \leq a$ for all $x \in A$. An element $a \in A$ is called a **least element** of A if $a \leq x$ for all $x \in A$.

We show below greatest and least elements of some posets diagrammatically.



Greatest element :	f	o	none
Least element :	a	none	none

Fig. 4.65

Example 1 : Let $S = \{a, b, c, d\}$ and let $A = \mathcal{P}(S)$ be the power set of S and $\leq$ be the relation is a subset of '.

Since Φ is a subset of every set of $\mathcal{P}(S)$, Φ is the least element.

Since $\{a, b, c, d\}$ is the superset of every set $\mathcal{P}(S)$, $\{a, b, c, d\}$ is the greatest element.

Example 2 : Let $A = \{1, 2, 3, 4, 6, 12, 24\}$ with partial order of divisibility.

Since 1 divides every element of A, 1 is the least element. Since every element divides 24, 24 is the greatest element.

Example 3 : Let $A = \{2, 3, 6, 12, 24, 36\}$ with partial order of divisibility.

Since 2, 3 are not comparable A has no least element. Similarly, 24, 36 are not comparable. Hence, A has no the greatest element (See Fig. 4.43, page 4-20).

Uniqueness : The greatest element of a poset, if it exists is **unique**. Similarly, the least element, if it exists, is **unique**.

Theorem 3 : A poset has at most one greatest element and one least element.

Proof : We accept it without proof.

The greatest element of a poset, if it exists, is often called the **unit element** and is denoted by *I*. The least element of a poset, if it exists, is often called the **zero element** and is denoted by 0.

EXERCISE - VI

Find the maximal and minimal elements in each poset if they exist. (Ex. 1 to 8).

1.

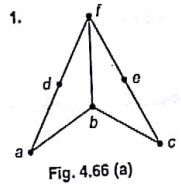


Fig. 4.66 (a)

2.

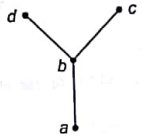


Fig. 4.66 (b)

3.

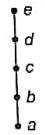


Fig. 4.66 (c)

[**Ans. :** (1) Minimal a, b, c ; maximal f, (2) minimal a ; maximal d, c.
(3) minimal a ; maximal e.]

4. $(A, \leq)$, A is the set of positive even integers. [**Ans. :** minimal 2, no maximal]

5. $(A, |)$, A is the set $\{2, 5, 6, 12, 20\}$ and $|$ is the relation of divisibility. Draw also Hasse diagram.

[**Ans. :** Max. 12, 20, Min. 2. For Hasse diagram see Fig. 4.67 (a)]

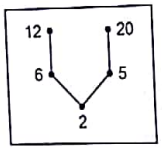


Fig. 4.67 (a)

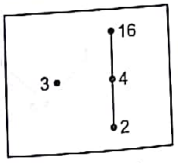


Fig. 4.67 (b)

6. $(A, |)$, A is the set $\{2, 3, 4, 16\}$. Draw Hasse diagram.

[**Ans. :** Max. 3, 16, Min. 3, 2. For Hasse diagram see Fig. 4.67 (b)]

7. $(A, \leq)$, A is the set of negative even integers. [**Ans. :** No minimal, maximal - 2]

8. $(A, \leq)$, A is the set of (negative and positive) integers. [**Ans. :** No maximal, no minimal]

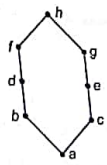
9. Find the least and the greatest elements of the poset (i) in Ex. 5. (ii) $A = \{2, 4, 6, 8, 12, 18, 24, 36, 72\}$ with partial order of divisibility.

[**Ans. :** (i) least 2, no greatest.
(ii) least 2, greatest 72.]

10. Find the greatest and the least elements of the given posets (Fig. 4.68). **(M.U. 2007)**

[**Ans. :** (a) Least a, greatest h ;
(b) No least elements, greatest f.]

(a)



(b)

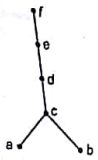


Fig. 4.68

(c) Supremum and Infimum (LUB and GLB) (M.U. 1996, 98)

Consider a poset A and a subset B of A.

Definition 4 : An element $a \in A$ is called an **upper bound** of B if $b \leq a$ for all $b \in B$.

In other words a is an upper bound of B if a **succeeds every element** b of B.

Definition 5 : An element $a \in A$ is called a **lower bound** of B if $a \leq b$ for all $b \in B$.

In other words a is a lower bound of B if a precedes every element b of B.

Definition 6 : Let A be a poset and B be a subset of A. An element $a \in A$ is called a **least upper bound (LUB)** or **supremum** of B if a is an upper bound of B and $a \leq a'$ where a' is an upper bound.

In other words, if an upper bound of B precedes every other upper bound of B then it is called a least upper bound of B.

Definition 7 : Let A be a poset and B be a subset of A. An element $a \in A$ is called a greatest lower bound (GLB) or **infimum** of B if a is a lower bound of B and $a' \leq a$ if a' is a lower bound.

In other words if a lower bound of B succeeds every other lower bound of B then it is called a greatest lower bound of B.

Example 1 : Consider the poset $A = \{a, b, c, d, e, f, g, h\}$ whose Hasse diagram is shown in Fig. 4.69. Find all upper and lower bounds of the following subsets of A (i) $B_1 = \{a, b\}$, (ii) $B_2 = \{d, c\}$. **(M.U. 2004)**

Sol. : (i) It is clear that since there are no elements in A below a, b, B_1 has no lower bound.

Also since c, d, e, f, g, h are above *i.e.* succeed a, b the upper bounds of B_1 are c, d, e, f, g, h.

(ii) Since the elements a, b, c in A are below *i.e.* precede d, e the lower bounds of B_2 are a, b, c.

Since the elements f, g, h are above *i.e.* succeed d, e, the upper bounds of B_2 are f, g, h.

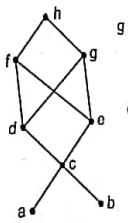


Fig. 4.69

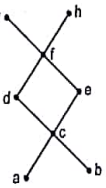


Fig. 4.70

Example 2 : Consider the poset

$A = \{a, b, c, d, e, f, g, h\}$

whose Hasse diagram is shown in Fig. 4.70. Find all upper bounds and lower bounds of $B = \{c, d, e\}$.

Sol. : Since f, g, h succeed every element of B. f, g, h are the upper bounds of B.

Since a, b precede every element of B. a, b are the lower bounds of B.

From Ex. 1 and Ex. 2, we see that an upper or a lower bounds of B may or may not belong to B.

Example 3 : Consider $A = \{1, 3, 5, 7, 15, 21, 35, 105\}$ and let R be the relation 'a divides b'. Find all upper and lower bounds of $B_1 = \{3, 7\}$, $B_2 = \{3, 5\}$. **(M.U. 2014)**

OR Draw Hasse diagram of D_{105}.

Sol. : The Hasse diagram is given in Fig. 4.71.

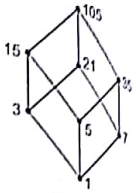


Fig. 4.71

Since 21 and 105 succeed both 3, 7 the upper bounds of B_1 are 21, 105.

Since 15 and 105 succeed both 3, 5 the upper bounds of B_2 are 15, 105.

Since 1 precedes both 3 and 7, the lower bound of B_1 is 1.

Similarly, the lower bound of B_2 is 1.

Example 4 : Let A be the poset considered in Ex. 1. Let the subsets B_1 and B_2 be defined as in the same example. Find least upper bound and greatest lower bound of (i) B_1 and (ii) of B_2

Sol. : **(i)** Since B_1 has no lower bound it has no greatest lower bound.

Since c precedes all other upper bounds d, e, f, g, h we have LUB = c.

(ii) Since c succeeds all other lower bounds a, b we have GLB = c.

Upper bounds of B_2 are f, g, h. But f, g are not comparable. We therefore, say that B_2 has no least upper bound.

Example 5 : Find the greatest lower bound and the least upper bound of the sets {3, 9, 12} and {1, 2, 4, 5, 10} if they exist in the poset $(Z, /)$ where / is the relation of divisibility.

(M.U. 2005, 09)

Sol. : **(a)** We have set $A = \{3, 9, 12\}$.

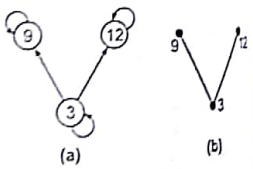
The relation R is, $R = \{(3, 3), (3, 9), (3, 12), (9, 9), (12, 12)\}$

$$\therefore M_R = \begin{array}{c} \\ 3 \\ 9 \\ 12 \end{array} \begin{array}{c} \begin{array}{ccc} 3 & 9 & 12 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{array}$$

We shall now find the Hasse diagram of R.

The digraph of R is as shown in Fig. 4.72 (a).

There is no transitivity. Removing the loop we get the Hasse diagram as shown in Fig. 4.72 (b).



(a) (b)

Fig. 4.72

The GLB is 3. LUB does not exist.

(b) We have $A = \{1, 2, 4, 5, 10\}$. The relation R is

$R = \{(1, 1), (1, 2), (1, 4), (1, 5), (1, 10), (2, 2), (2, 4), (2, 10), (4, 4), (5, 5), (5, 10), (10, 10)\}$

$$\therefore M_R = \begin{array}{c} \\ 1 \\ 2 \\ 4 \\ 5 \\ 10 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 4 & 5 & 10 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

We shall now find Hasse diagram of R.

The digraph is as shown in Fig. 4.73 (a).

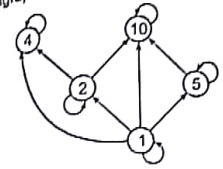


Fig. 4.73 (a)

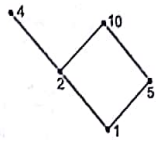


Fig. 4.73 (b)

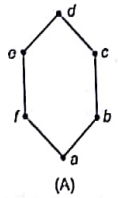
Deleting the transitivity and the arrow-heads, we get the Hasse diagram as given in Fig. 4.73 (b).

The GLB is 1, LUB does not exist.

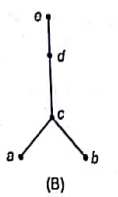
Example 6 : Find the GLB and LUB for the following posets whose Hasse diagram are shown in Fig. 4.74.

Sol. : (i) In (A), a is the GLB and d is LUB.

(ii) In (B), a is the LUB, GLB does not exit.



(A)



(B)

Fig. 4.74

Example 7 : Find the lower bounds and upper bounds of the subsets

(i) $\{a, b, c\}$, (ii) $\{j, h\}$, (iii) $\{a, c, d, f\}$

in the poset with Hasse diagram shown in the Fig. 4.75.

Also find GLB and LUB of $\{b, d, g\}$. **(M.U. 2005, 09)**

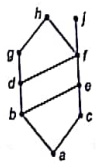


Fig. 4.75

Sol. : (i) For the subset $\{a, b, c\}$ lower bound is a and upper bounds are e, f, h and j.

(ii) For the subset $\{j, h\}$ lower bounds are f, e, c, d, b, a and there is no upper bound.

(iii) For the subset $\{a, c, d, f\}$ lower bound is a and upper bounds are f, j, h.

(iv) For the subset $\{b, d, g\}$ GLB is b and LUB is g.

(d) Isomorphism And Extremal Elements

From the definition of isomorphism given in § 4, page 4-26 and from the definitions of extremal elements, given in § 5 the following results follow.

If $(A, \leq)$ and $(B, \leq_1)$ are isomorphic posets under the isomorphism $f : A \to B$ then :-

(a) If a is a maximal (minimal) element of A then $f(a)$ is a maximal (minimal) element of B.

(b) If a is the greatest (least) element of A then $f(a)$ is the greatest (least) element of B.

(c) If a is an upper bound (lower bound, the least upper bound, the geatest lower bound) of a subject S of A, then $f(a)$ is an upper bound (lower bound, the least upper bound, the greatest lower bound) of the corresponding subset $f(S)$ of B.

(d) If every subset of A has a least upper bound (greatest lower bound) then every subset of B has a least upper bound (greatest lower bound).

EXERCISE - VII

Find (i) all upper bounds, (ii) all lower bounds, (iii) the least upper bound, (iv) the greatest lower bound of B for the given poset A.

1. Consider the poset $A = \{a, b, c, d, e, f, g, h\}$ whose Hasse diagram is shown in Fig. 4.59, page 4-31. Let $B = \{c, d, e\}$. [**Ans. :** (i) f, g, h ; (ii) a, b, c ; (iii) f ; (iv) c]

2. Consider the poset $A = \{a, b, c, d, e, f\}$ whose Hasse diagram is shown in Fig. 4.76. Let $B = \{b, c, d\}$.

[**Ans. :** (i) d, e, f ; (ii) b, a ; (iii) d ; (iv) b]

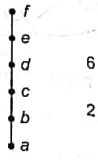


Fig. 4.76

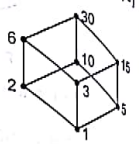


Fig. 4.77

3. Let A = the set of real numbers and R be the relation $\leq$. Let $B = \{ x \mid x$ is a real number and $2 < x < 3\}$. [**Ans. :** (i) $\{ x \mid x \in [3, \infty)\}$; (ii) $\{x \mid x \in (-\infty, 2)\}$; (iii) 3 ; (iv) 2]

4. Let A = the set of real numbers and R be the relation $\leq$. Let $B = \{x \mid x$ is a real number and $2 \leq x < 3\}$.

[**Ans. :** (i) $\{ x \mid x \in [3, \infty)\}$; (ii) $\{x \mid x \in (-\infty, 2)\}$; (iii) 3 ; (iv) 2]

5. Let $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$. Let R be the relation 'a divides b'. $B = \{10, 15\}$. Also draw Hasse diagram. [**Ans. :** (i) 30 ; (ii) 1, 5 ; (iii) 30 ; (iv) 5. For Hasse diagram see Fig. 4.77]

6. Lattices

(M.U. 2005, 07, 13)

Lattice is a mathematical structure with two binary operations called join and meet which frequently appear in computing and its mathematical applications.

We first define two new terms **join** and **meet** with reference to a poset L.

Definitions : Let A be a poset $(L, \leq)$. Let a, b be two elements $\in L$. Now, we define

$a \vee b$ (read as 'a join b') as LUB of a and b.

$a \wedge b$ (read as 'a meet b') as GLB of a and b.

Theorem : Let L be a poset $(A, \leq)$ and let $a, b \in A$ then

(i) If a and b have a LUB then this LUB is unique.

(ii) If a and b have a GLB then this GLB is unique.

Proof : We prove the theorem by reductio-ad-absurdum method.

(i) Let if possible the elements a, b have two distinct LUB's l_1 and l_2.

Then by definition of LUB $a \leq l_1$ and $b \leq l_1$

and $a \leq l_2$ and $b \leq l_2$

But, since l_1 is a LUB $l_1 \leq l_2$. Also since l_2 is a LUB $l_2 \leq l_1$.

By antisymmetric property of $\leq$, $l_1 = l_2$.

But this contradicts our hypothesis.

$\therefore$ LUB of a, b is unique.

(ii) We can prove the part (ii) in the same way.

Definition : A poset $(L, \leq)$, in which **every pair** $\{a, b\}$ of two elements of L has a **least upper bound** (LUB) **and** a **greatest** lower bound (GLB), is called a **lattice.** (M.U. 2005, 07, 13)

We denote LUB $(\{a, b\})$ by $a \vee b$ and call it the **join** of a and b. Also we denote GLB $(\{a, b\})$ by $a \wedge b$ and call it the **meet** of a and b. Since a lattice is an algebraic system with binary operations $\vee$ and $\wedge$ it is denoted by $[L, \vee, \wedge]$.

It may be noted that a totally ordered set is trivially a lattice but not all partially ordered sets are lattices.

As illustrations we show below two lattices diagrammatically.

Illustration 1 :

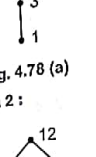


Fig. 4.78 (a)

$\vee$	1	3	6	12
1	1	3	6	12
3	3	3	6	12
6	6	6	6	12
12	12	12	12	12

LUB

$\wedge$	1	3	6	12
1	1	1	1	1
3	1	3	3	3
6	1	3	6	6
12	1	3	6	12

GLB

Illustration 2 :

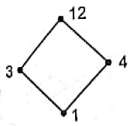


Fig. 4.78 (b)

$\vee$	1	3	4	12
1	1	3	4	12
3	3	3	12	12
4	4	12	4	12
12	12	12	12	12

LUB

$\wedge$	1	3	4	12
1	1	1	1	1
3	1	3	1	3
4	1	1	4	4
12	1	3	4	12

GLB

Example 1 : Let S be any set and $\mathcal{P}(S)$ be its power set. Let '$\subseteq$ is a subset of' *i.e.* $\subseteq$ be the relation. Prove that $(\mathcal{P}(S), \subseteq)$ is a lattice when (i) $S = \{a\}$, (ii) $S = \{a, b\}$, (iii) $S = \{a, b, c\}$.

Sol. : We have already proved that $(\mathcal{P}(S), \subseteq)$ is a partial ordered set. (Ex. 1 page 4-1.)

(i) Let $S = \{a\}$, $\mathcal{P}(S) = \{\Phi, \{a\}\}$ and R be set inclusion $\subseteq$. Now, by definition (page 4-31) of LUB *i.e.* join $\vee$ of a, b is the upper bound of a, b which precedes every other upper bound. From the Hasse diagram given below, we see that $\{a\}$ precedes every upper bound of $\{\Phi, \{a\}\}$ (in fact there is none.) Thus, in this case the **least upper bound** is the **union.**

Similarly, the greatest lower bound of $\{\Phi, \{a\}\}$ is the lower bound which succeeds all other lower bound. Now, Φ succeeds every lower bound of $\{\Phi, \{a\}\}$ (in fact there is none). Thus, in this case the **greatest lower bound** is the **intersection.**

Considering the union of Φ and $\{a\}$, we get the Table No. 1 and considering the intersection of Φ and $\{a\}$, we get the Table No. 2.

Fig. 4.79 (a)

$\vee$	Φ	$\{a\}$
Φ	Φ	$\{a\}$
$\{a\}$	$\{a\}$	$\{a\}$

Table No. 1

$\wedge$	Φ	$\{a\}$
Φ	Φ	Φ
$\{a\}$	Φ	$\{a\}$

Table No. 2

Since $(\mathcal{P}(S), \subseteq)$ is a poset and every pair of elements of $\mathcal{P}(S)$ has an LUB and a GLB, it is a lattice.

Note ....

As noted above, the LUB of two subsets of the power set $\mathcal{P}(S)$ of the set S is obtained by taking the union of the subsets. e.g. LUB ({a}, {b}) is {a, b}. Similarly, the GLB of two subsets of $\mathcal{P}(S)$ is obtained by taking the intersection of the subsets. e.g. GLB ({a}, {b}) is Φ. Thus, the join, **is equivalent to union ∪ and the meet ∧ is equivalent to the intersection of ∩ two subsets of** $\mathcal{P}(S)$. This is why join is denoted by ∨ for (union ∪) and the meet is denoted by ∧ (intersection ∩)

(II) When $S = \{a, b\}$, $\mathcal{P}(S) = \{\Phi, \{a\}, \{b\}, \{a, b\}\}$. Its Hasse diagram and operation tables for ∨ and ∧ are given below.

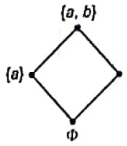


Fig. 4.79 (b)

∨	Φ	{a}	{b}	{a, b}
Φ	Φ	{a}	{b}	{a, b}
{a}	{a}	{a}	{a, b}	{a, b}
{b}	{b}	{a, b}	{b}	{a, b}
{a, b}	{a, b}	{a, b}	{a, b}	{a, b}

Table No. 1

∧	Φ	{a}	{b}	{a, b}
Φ	Φ	Φ	Φ	Φ
{a}	Φ	{a}	Φ	{a}
{b}	Φ	Φ	{b}	{b}
{a, b}	Φ	{a}	{b}	{a, b}

Table No. 2

Since $(\mathcal{P}(S), \subseteq)$ is a poset and every pair of elements in $\mathcal{P}(S)$ has an LUB and a GLB, it is a lattice.

(III) When $S = \{a, b, c\}$,

$\mathcal{P}(S) = \{\Phi, \{a\}, \{b\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$.

Its Hasse diagram is shown in Fig. 4.79 (c).

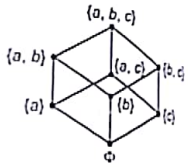


Fig. 4.79 (c)

The operation tables for ∨ *i.e.* union and ∧ *i.e.* intersection of two sets are given below.

∨	Φ	{a}	{b}	{c}	{a, b}	{a, c}	{b, c}	{a, b, c}
Φ	Φ	{a}	{b}	{c}	{a, b}	{a, c}	{b, c}	{a, b, c}
{a}	{a}	{a}	{a, b}	{a, c}	{a, b}	{a, c}	{a, b, c}	{a, b, c}
{b}	{b}	{a, b}	{b}	{b, c}	{a, b}	{a, b, c}	{b, c}	{a, b, c}
{c}	{c}	{a, c}	{b, c}	{c}	{a, b, c}	{a, c}	{b, c}	{a, b, c}
{a, b}	{a, b}	{a, b}	{a, b}	{a, b, c}	{a, b}	{a, b, c}	{a, b, c}	{a, b, c}
{a, c}	{a, c}	{a, c}	{a, b, c}	{a, c}	{a, b, c}	{a, c}	{a, b, c}	{a, b, c}
{b, c}	{b, c}	{a, b, c}	{b, c}	{b, c}	{a, b, c}	{a, b, c}	{b, c}	{a, b, c}
{a, b, c}	{a, b, c}	{a, b, c}	{a, b, c}	{a, b, c}	{a, b, c}	{a, b, c}	{a, b, c}	{a, b, c}

∧	Φ	{a}	{b}	{c}	{a, b}	{a, c}	{b, c}	{a, b, c}
Φ	Φ	Φ	Φ	Φ	Φ	Φ	Φ	Φ
{a}	Φ	{a}	Φ	Φ	{a}	{a}	Φ	{a}
{b}	Φ	Φ	{b}	Φ	{b}	Φ	{b}	{b}
{c}	Φ	Φ	Φ	{c}	Φ	{c}	{c}	{c}
{a, b}	Φ	{a}	{b}	Φ	{a, b}	{a}	{b}	{a, b}
{a, c}	Φ	{a}	Φ	{c}	{a}	{a, c}	{c}	{a, c}
{b, c}	Φ	Φ	{b}	{c}	{b}	{c}	{b, c}	{b, c}
{a, b, c}	Φ	{a}	{b}	{c}	{a, b}	{a, c}	{b, c}	{a, b, c}

Since $(\mathcal{P}(S), \subseteq)$ is a poset and every pair of elements in $\mathcal{P}(S)$ has a LUB and GLB, it is a lattice.

Example 2 : Show that the set of all divisions of 70 form a lattice. **(M.U. 1995, 2015)**

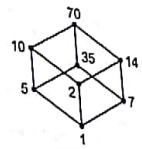


Fig. 4.80

Sol. : The set of all divisions is the set $A = \{1, 2, 5, 7, 10, 14, 35, 70\}$

The Hasse diagram of the poset is shown in Fig. 4.80.

As in the above example, we got the following tables.

∨	1	2	5	7	10	14	35	70
1	1	2	5	7	10	14	35	70
2	2	2	10	14	10	14	70	70
5	5	10	5	35	10	70	35	70
7	7	14	35	7	70	14	35	70
10	10	10	10	70	10	70	70	70
14	14	14	70	14	70	14	70	70
35	35	70	35	35	70	70	35	70
70	70	70	70	70	70	70	70	70

∧	1	2	5	7	10	14	35	70
1	1	1	1	1	1	1	1	1
2	1	2	1	1	2	2	1	2
5	1	1	5	1	5	1	5	5
7	1	1	1	7	1	7	7	7
10	1	2	5	1	10	2	5	10
14	1	2	1	7	2	14	7	14
35	1	1	5	7	5	7	35	35
70	1	2	5	7	10	14	35	70

Since every pair of elements has a LUB and GLB the set is a lattice.

Example 3 : Let $A = \{1, 3, 5, 15, 30, 60, 90, 180\}$ with the relation of divisibility. Draw Hasse diagram. Determine whether it is a lattice. **(M.U. 2011)**

Sol. : The Hasse diagram of the relation is shown in the Fig. 4.81.

It is a lattice.

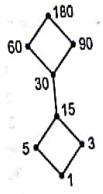


Fig. 4.81

Example 4 : Let $L = \{1, 2, 3, 6\}$ and R be the relation 'is divisible by'. Prove that L is a lattice.

Sol. : The relation matrix and Hasse diagram are as shown below.

$$\begin{array}{c|cccc} & 1 & 2 & 3 & 6 \\ 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 1 & 0 & 1 \\ 3 & 0 & 0 & 1 & 1 \\ 6 & 0 & 0 & 0 & 1 \end{array}$$

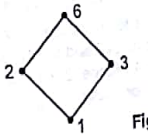


Fig. 4.82

Using the matrix M_R, we can show that (L, R) is a poset (Left to you as an exercise).

In the first problem we saw that if A is the power set of A and the relation is set inclusion then the LUB or the join $\vee$ of two elements is the union and the GLB or the meet of two elements is the intersection.

Now, we shall see what $\vee$ and $\wedge$ mean when A is a set of positive integers and the relation is "a divisible by".

By applying the definition and also from the above figure, we see that LUB of 2 and 3 is 6, of 2 and 6 is 6 etc.

Thus, LUB in this case means the lowest common multiple (LCM) present in the set of the two numbers. Thus, so far as numbers are concerned the LUB or the join $\vee$ means the LCM present in the set.

Similarly, from the definition and also from the above figure, we see that the GLB of 2 and 6 is 2, of 2 and 1 is 1, of 2 and 3 is 1 etc.

Thus, GLB in this case means the greatest common divisor (GCD) present in the set.

Hence, the join $\vee$ of a, b means the LCM *i.e.* **the lowest common multiple of a, b** *i.e.* **the smallest number which is divisible by a and b both and which is present in A.** The meet $\wedge$ of a, b means, the GCD *i.e.* **the greatest common divisor of a, b** *i.e.* **the largest number that divides a and b both and which is present A.**

With these considerations, we get the following tables. The operation table for $\vee$ and $\wedge$ are given below.

$\vee$	1	2	3	6
1	1	2	3	6
2	2	2	6	6
3	3	6	3	6
6	6	6	6	6

$\wedge$	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

Since (L, R) is a poset and every pair of elements of L has an LUB and a GLB, it is a lattice.

Example 5 : Let $L = \{1, 2, 3, 5, 30\}$ and R be the relation 'is divisible by'. Prove that L is a lattice.

Sol. : The relation matrix and Hasse diagram are shown below.

$$\begin{array}{c|ccccc} & 1 & 2 & 3 & 5 & 30 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 1 & 0 & 0 & 1 \\ 3 & 0 & 0 & 1 & 0 & 1 \\ 5 & 0 & 0 & 0 & 1 & 1 \\ 30 & 0 & 0 & 0 & 0 & 1 \end{array}$$

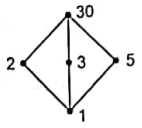


Fig. 4.83

Using matrix M_R, we can show that (L, R) is a poset (Left to you as an exercise).

Now, while preparing the tables for $\wedge$ and $\wedge$ we have to see that l.c.m. and g.c.d. of elements a, b **must be present in A.** Thus, l.c.m. of 2 and 5 is 10 but it is not present in A. However, 30 is also l.c.m. of 2 and 5 which is present in A. Hence, $2 \vee 5 = 30$. Similarly, we find that $3 \vee 5 = 30$, $2 \vee 3 = 30$. Thus, we get the following table for $\vee$ and $\wedge$.

The operation tables for $\vee$ and $\wedge$ are given below.

$\vee$	1	2	3	5	30
1	1	2	3	5	30
2	2	2	30	30	30
3	3	30	3	30	30
5	5	30	30	5	30
30	30	30	30	30	30

$\wedge$	1	2	3	5	30
1	1	1	1	1	1
2	1	2	1	1	2
3	1	1	3	1	3
5	1	1	1	5	5
30	1	2	3	5	30

Since (L, R) is a poset and every pair of elements of L has an LUB and a GLB it is a lattice.

Note : If n is a positive integer then D_n denotes the set of all divisors of n. For example, D_3 denotes the set of all divisors of 3 *i.e.* $D_3 = \{1, 3\}$, D_4 denotes the set of all divisors of 4 *i.e.* $D_4 = \{1, 2, 4\}$.

The posets associated with the relation of divisibility are denote by $(D_3, \leq)$, $(D_4, \leq)$ etc. The relation $\leq$ is the relation of Divisibility.

Example 6 : Prove that $(D_8, \leq)$ and $(D_{10}, \leq)$ are lattices. Show their Hasse diagrams.

Sol. : (a) We have $D_8 = \{1, 2, 4, 8\}$. The Hasse diagram is shown in the Fig. 4.84 (a).

(b) We have $D_{10} = \{1, 2, 5, 10\}$. The Hasse diagram is shown in the Fig. 4.84 (b).

It is left to you to prepare the tables for $\wedge$ and $\vee$ and show that these are lattice.

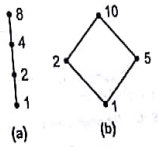


Fig. 4.84

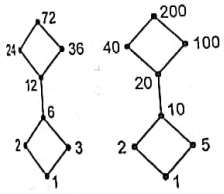


Fig. 4.85

Fig. 4.86

Example 7 : Draw the Hasse diagram of the poset $A = \{1, 2, 3, 6, 12, 24, 36, 72\}$ under the relation of divisibility. Is it a lattice?

Sol. : The Hasse diagram is shown in Fig. 4.85.

It is a lattice.

Example 8 : Draw the Hasse diagram of the poset $A = \{1, 2, 5, 10, 20, 40, 100, 200\}$ under the relation of divisibility. Is it lattice?

Sol. : The Hasse diagram is shown in Fig. 4.86.

It is a lattice.

Example 9 : Draw the Hasse diagram of the poset $A = \{1, 3, 4, 12, 24, 48, 72, 144\}$ under the relation of divisibility. Is it lattice?

Sol. : The Hasse diagram is shown in Fig. 4.87.

It is a lattice.

Example 10 : Let $A = \{1, 2, 3, 4, 6, 8, 12, 24\}$ with the relation of divisibility. Draw Hasse diagram. Determine whether it is a lattice.

Sol. : The Hasse diagram is shown in Fig. 4.88.

The poset is a lattice.

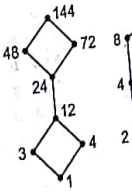


Fig. 4.87

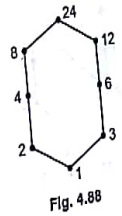


Fig. 4.88

Example 11 : Draw the Hasso diagrams of the lattices having 2^n elements for $n = 1, 2, 3$. (M.U. 2000)

Sol. : For $n = 0, 1, 2, 3$ the Lattices have $2^n = 1, 2, 4, 8$ elements. The corresponding Lattice are shown below.

n	Elements	Lattice
0	1	
1	2	
2	4	
3	8	

Fig. 4.89

Example 12 : Determine whether the posets with the Hasse diagram [Fig. 8.90 (a) and (b)] are lattices or not. (M.U. 2003, 06, 12)

Sol. : We shall prepare the tables of LUB and GLB for both sets.

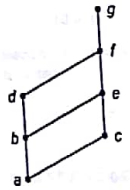


Fig. 8.90 (a)

(a) LUB

$\vee$	a	b	c	d	e	f	g
a	a	b	c	d	e	f	g
b	b	b	e	d	e	f	g
c	c	e	c	f	e	f	g
d	d	d	f	d	f	f	g
e	e	e	e	f	e	f	g
f	f	f	f	f	f	f	g
g	g	g	g	g	g	g	g

GLB

$\wedge$	a	b	c	d	e	f	g
a	a	a	a	a	a	a	a
b	a	b	a	b	b	b	b
c	a	a	c	a	c	c	c
d	a	b	a	d	b	d	d
e	a	b	c	b	e	e	e
f	a	b	c	d	e	f	f
g	a	b	c	d	e	f	g

Since every pair of elements has a LUB and GLB, the poset (A) is a lattice.

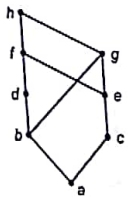


Fig. 8.90 (b)

(b) LUB

$\vee$	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	b	g	d	f	f	g	h
c	c	g	c	f	e	f	g	h
d	d	d	f	d	f	f	h	h
e	e	f	e	f	e	f	g	h
f	f	f	f	f	f	f	h	h
g	g	g	g	h	g	h	g	h
h	h	h	h	h	h	h	h	h

GLB

$\wedge$	a	b	c	d	e	f	g	h
a	a	a	a	a	a	a	a	a
b	a	b	a	b	a	b	b	b
c	a	a	c	a	c	a	c	c
d	a	b	a	d	a	d	b	d
e	a	a	c	a	e	e	e	e
f	a	b	c	d	e	f	–	
g								
h								

Since GLB of (f, g) does not exist, the poset is **not** a lattice.

Example 13 : Draw Hasso diagram of the relation of divisibility on the set $A = \{2, 4, 12, 16\}$ and check if it is a lattices. (M.U. 2009, 11)

Sol. : The relation

$R = \{(2, 2), (2, 4), (2, 12), (2, 16), (4, 4), (4, 12), (4, 16), (12, 12), (16, 16)\}$

The matrix of the relation and Hasso diagram (Fig. 4.91) is shown below.

$$M_R = \begin{array}{c} \\ 2 \\ 4 \\ 12 \\ 16 \end{array} \begin{array}{c} \begin{array}{cccc} 2 & 4 & 12 & 16 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

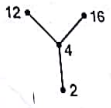


Fig. 4.91

Since there is no LUB for 12 and 16 R is not a lattice.

Example 14 : Determine whether the following Hasso diagram represents a lattice. (M.U. 2008)

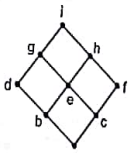


Fig. 4.92

Sol. : LUB

$\vee$	a	b	c	d	e	f	g	h	i
a	a	b	c	d	e	f	g	h	i
b	b	b	e	d	e	h	g	h	i
c	c	e	c	g	e	f	g	h	i
d	d	d	g	d	g	i	g	i	i
e	e	e	e	g	e	h	g	h	i
f	f	h	f	i	h	f	i	h	i
g	g	g	g	g	g	i	g	i	i
h	h	h	h	i	h	h	i	h	i
i	i	i	i	i	i	i	i	i	i

GLB

$\wedge$	a	b	c	d	e	f	g	h	i
a	a	a	a	a	a	a	a	a	a
b	a	b	a	b	b	a	b	b	b
c	a	a	c	a	c	c	c	c	c
d	a	b	a	d	b	a	d	b	d
e	a	b	c	b	e	c	e	e	e
f	a	a	c	a	c	f	c	f	f
g	a	b	c	d	e	c	g	e	g
h	a	b	c	b	e	f	e	h	h
i	a	b	c	d	e	f	g	h	i

Since every pari of elements has a LUB and GLB, the relation is a lattice.

Example 15 : Determine whether the posets with the following Hasse diagrams (Fig. 4.93) are lattices or not. **(M.U. 2013)**

Sol. : Both Hasse diagrams are lattices because every pair of elements has GLB and LUB.

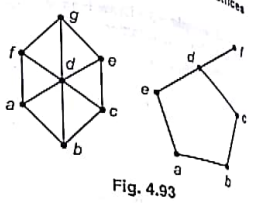


Fig. 4.93

Example 16 : Determine whether the posets represented by the Hasse diagrams (Fig. 4.94) are lattices. **(M.U. 2002)**

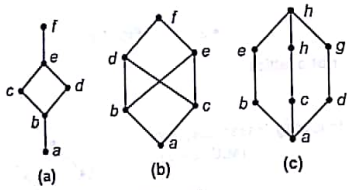


Fig. 4.94

Sol. : (i) Fig. 4.94 (a) is a lattice as every pair has a LUB and GLB.

(ii) Fig. 4.94 (b) is not a lattice as LUB of (b, c) and GLB of (d, e) do not exist.

(iii) Fig. 4.94 (c) is a lattice as every pair has a LUB and GLB.

Example 17 : Let D_m denote the set of divisors of a positive integer m. **(M.U. 2008, 15)**

For $m = 36$, prove that D_m is a lattice under the relation 'a divides b' i.e. $(D_m, \leq)$ is a lattice.

Sol. : We see that $D_m = \{1, 2, 3, 4, 6, 12, 18, 36\}$. Its Hasse diagram is shown in the Fig. 4.95.

We leave it you to prepare the tables for (LUB) $\vee$ and (GLB) $\wedge$.

Example 18 : Draw the Hasse diagram of D_{60}.

Check if it is a lattice. **(M.U. 2010, 11, 12, 15)**

Sol. : The Hasse diagram of D_{60} is shown in Fig. 4.96.

Proof is left to you.

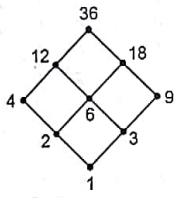


Fig. 4.95

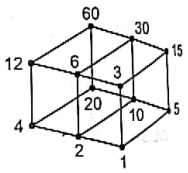


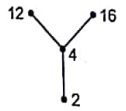
Fig. 4.96

Example 19 : Check whether $A = \{2, 4, 12, 16\}$ and $B = \{3, 4, 12, 24\}$ are lattices under divisibility. **(M.U. 2009, 11)**

Draw their Hasse diagrams.

Sol. : (a) The Hasse diagram is shown below.

The operation tables for $\vee$ and $\wedge$ are given below.



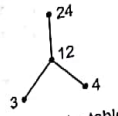
$\vee$	2	4	12	16
2	2	4	12	16
4	4	4	12	16
12	12	12	12	—
16	16	16	—	16

$\wedge$	2	4	12	16
2	2	2	2	2
4	2	4	4	4
12	2	4	12	4
16	2	4	4	16

We see from the table that LUB of (12, 16) [and of (16, 12)] does not exist. Hence, it is not a lattice. Hence, it is not a lattice.

(b) The Hasse diagram is shown below.

The operation tables for (LUB) $\vee$ and (GLB) $\wedge$ are given below.



$\vee$	3	4	12	24
3	3	12	12	24
4	12	4	12	24
12	12	12	12	24
24	24	24	24	24

$\wedge$	3	4	12	24
3	3	—	3	3
4	—	4	4	4
12	3	4	12	12
24	3	4	12	24

We see from the table that GLB of (3, 4) [and of (4, 3)] does not exist. Hence, it is not a lattice.

Example 20 : Prove that the following posets are not lattices. Draw also the Hasse diagram.

(a) $L = \{a_1, a_2, a_3, a_4, a_5, a_6\}$
$R = \{(a_1, a_3), (a_1, a_4), (a_1, a_5), (a_1, a_6), (a_3, a_4), (a_3, a_5), (a_3, a_6), (a_4, a_5), (a_4, a_6), (a_2, a_3), (a_2, a_4), (a_2, a_5), (a_2, a_6)\}$

(b) $L = \{a_1, a_2, a_3, a_4, a_5\}$
$R = \{(a_1, a_2), (a_1, a_4), (a_1, a_5), (a_2, a_4), (a_2, a_5), (a_1, a_3), (a_3, a_4), (a_3, a_5)\}$

(c) $L = \{a_1, a_2, a_3, a_4, a_5, a_6\}$
$R = \{(a_1, a_2), (a_1, a_4), (a_1, a_6), (a_2, a_4), (a_2, a_6), (a_1, a_3), (a_1, a_5), (a_3, a_5), (a_3, a_6), (a_5, a_6), (a_2, a_5), (a_3, a_4)\}$

Sol. : (a) The LUB of a_5 and a_6 does not exists. Also the GLB of a_1 and a_2 does not exist. Hence, L is not a lattice. Hasse diagram is shown in Fig. 4.97 (a).

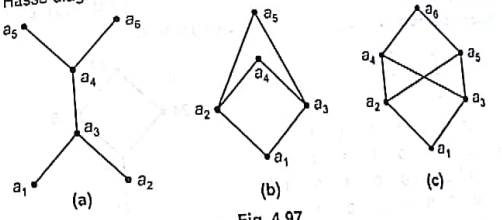


Fig. 4.97

(b) The LUB of a_2 and a_3 does not exist. Also GLB of a_4 and a_5 does not exist. Hence, L is not a lattice. Hasse diagram is shown in Fig. 4.97 (b).

(c) The LUB of a_2 and a_3 does not exist. Also GLB of a_4 and a_5 does not exist. Hence, L is not a lattice. Hasse diagram is shown in Fig. 7.97 (c).

Example 21 : For the set $X = \{2, 3, 6, 12, 24, 36\}$, a relation $\leq$ is defined by $x \leq y$ if x divides y. Draw Hasse diagram for $(x, \leq)$. Answer the following :

(i) What are maximal and minimal elements?

(ii) Give one example of chain and antichain.

(iii) Is the poset lattice? **(M.U. 2017)**

Sol. : For Hasse diagram see Fig. 4.43, page 4-20.

(i) Maximal elements are 24 and 36.

Minimal elements are 2 and 3.

(ii) { 2, 6, 12, 24 }, { 3, 6, 12, 36 } are chains.
{ 2, 3 }, { 24, 36 } are antichains.

(iii) Since the set {2, 3} has no GLB and set {24, 36} has no LUB.
It is not a lattice.

Example 22 : Show that the set of all divisions of 70 form a lattice.

Sol. : The Hasse diagram of L is as shown in Fig. 4.98.

Since every pair of elements of L has a LUB and GLB, it is a lattice.

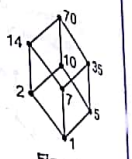


Fig. 4.98

Example 23 : Determine whether the Hasse diagram [Fig. 4.99 (a) and (b)] define a lattice. **(M.U. 1995, 2000)**

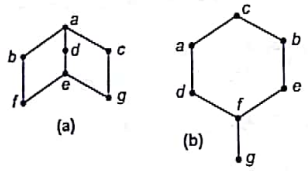


Fig. 4.99

Sol. : (i) Since GLB of (f, g) does not exist, it is not a lattice.

(ii) Each pair of elements has LUB and GLB. Hence, it is a lattice.

Example 24 : Draw the Hasse diagram of the poset A = { 2, 3, 6, 12, 24, 36, 72 } under the relation of divisibility. Is it a lattice? **(M.U. 2001, 05, 06, 07, 09, 14)**

Sol. : The relation "is divisible by" is given by the following matrix.

$$R = \begin{array}{c} \\ 2 \\ 3 \\ 6 \\ 12 \\ 24 \\ 36 \\ 72 \end{array} \begin{array}{c} \begin{array}{ccccccc} 2 & 3 & 6 & 12 & 24 & 36 & 72 \end{array} \\ \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

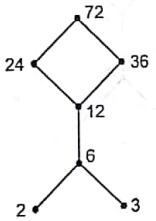


Fig. 4.100

The Hasse diagram is as shown in Fig. 4.100.

It is easy to see from the figure that there is no GLB to the pair (2, 3).

Hence, it is not a lattice.

Example 25 : Consider chains of divisors of 4 and 9 *i.e.*, L_1 = { 1, 2, 4 } and L_2 = {1, 3, 9} and partial order 'division' on L_1 and L_2. Draw the lattice $L_1 \times L_2$. **(M.U. 2003, 06, 09, 12, 14, 15)**

Sol. : Same as Ex. 24, page 4-18.

Example 15 : Let L_1 and L_2 be the lattices as shown in Fig. 4.101. Draw the Hasse diagram of $L_1 \times L_2$. **(M.U. 1997, 99)**

Sol. : Same as Ex. 23, page 4-17.

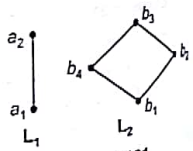


Fig. 4.101

7. Dual in a Lattice

Consider the two statements (1) $a \vee a = a$, (2) $a \wedge a = a$. **(M.U. 2009)**

It can be seen that statement (2) can be obtained from (1) by changing $\vee$ by $\wedge$ and statement (1) can be obtained from (2) by changing $\wedge$ by $\vee$. Such statements are called duals of each other.

Definition : The dual of any statement in a lattice $(L, \vee, \wedge)$ is defined to be the statement obtained by interchanging $\vee$ and $\wedge$.

For example, (1) Dual of $a \vee b = b \vee a$ is $a \wedge b = b \wedge a$.

(2) Dual of $a \vee (b \vee c) = (a \vee b) \vee c$ is $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

Principal of Duality

If a statement is true in a lattice $(L, \vee, \wedge)$ then its dual is also true in $(L, \vee, \wedge)$.

This is called the **principal of duality.**

Theorem : Let L be a lattice. Then the following properties hold.

1. **Idempotent properties** : $a \vee a = a$ and $a \wedge a = a$
2. **Commutative properties** : $a \vee b = b \vee a$ and $a \wedge b = b \wedge a$
3. **Associative properties** : $a \vee (b \vee c) = (a \vee b) \vee c$ and $a \wedge (b \wedge c) = (a \wedge b) \wedge c$
4. **Absorption properties** : $a \vee (a \wedge b) = a$ and $a \wedge (a \vee b) = a$

Proof : (1) By definition of LUB and GLB, LUB {(a, a)} = a and GLB ([a, a]) = a. Hence, $a \vee a = a$ and $a \wedge a = a$.

(2) Since in the definition of LUB and GLB of a, b the order does not enter,

GLB ({a, b}) = GLB ({b, a}).

$\therefore$ $a \vee b = b \vee a$ and $a \wedge b = b \wedge a$.

(3) By the definition LUB a is less than or equal to the LUB of a and $(b \vee c)$.

$\therefore$ $a \leq a \vee (b \vee c)$

By the same reasoning

$b \vee c \leq a \vee (b \vee c)$

Also $b \leq (b \vee c)$ and $c \leq (b \vee c)$

Since $b \leq (b \vee c)$ and $b \vee c \leq a \vee (b \vee c)$

By transitivity $b \leq a \vee (b \vee c)$

Since $c \leq (b \vee c)$ and $b \vee c \leq a \vee (b \vee c)$

By transitivity $c \leq a \vee (b \vee c)$

Now, $a \leq a \vee (b \vee c)$ and $b \leq a \vee (b \vee c)$

This means $a \vee (b \vee c)$ is an upper bound of a and b.

Hence, by definition of LUB $a \vee b \leq a \vee (b \vee c)$.

Now, $a \vee b \leq a \vee (b \vee c)$ and $c \leq a \vee (b \vee c)$

This means $a \vee (b \vee c)$ is an upper bound of $a \vee b$ and c. .....(1)

Hence, by definition of LUB, $(a \vee b) \vee c \leq a \vee (b \vee c)$ .....(2)

Similarly, we can prove that, $a \vee (b \vee c) \leq (a \vee b) \vee c$

Since, L is a poset having the property of antisymmetry from (1) and (2), we get

$(a \vee b) \vee c = a \vee (b \vee c)$.

Similarly we can prove that (or it follows from the principle of duality)

$a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

(4) By definition of GLB of a and b, $a \wedge b$ is less than or equal to a.

$\therefore\ a \wedge b \leq a$ but $a \leq a$.

$\therefore$ a is an upper bound of $a \wedge b$ and a. Hence, LUB of a and $a \wedge b$ is less than or equal to a.

$\therefore\ a \vee (a \wedge b) \leq a$

By definition of LUB the LUB of a and $a \wedge b$ is greater than or equal to a ..... (3)

$\therefore\ a \leq a \vee (a \wedge b)$

From (3) and (4), we get $a \vee (a \wedge b) = a$. ..... (4)

Similarly, we can prove that (or it follows from the principle of duality)

$a \wedge (a \vee b) = a$.

Example 1 : For any a, b, c, d in a lattice $(L, \leq)$, if $a \leq b$ and $c \leq d$, show that (i) $a \vee c \leq b \vee d$ and (ii) $a \wedge c \leq b \wedge d$. (M.U. 1998)

Sol. : By data $a \leq b$ and by definition of LUB $b \leq b \vee d$.

$\therefore$ By transitivity, $a \leq b \vee d$ ..... (i)

By data $c \leq d$ and by definition of LUB $d \leq b \vee d$.

$\therefore$ By transitivity, $c \leq b \vee d$ ..... (ii)

By (i) and (ii) $b \vee d$ is an upper bound of a, c.

By definition of LUB, $a \vee c \leq b \vee d$.

Similarly, we can prove that $a \wedge c \leq b \vee d$.

Example 2 : Let $(A, \leq)$ be a poset. Let $\leq_R$ be a binary relation on A such that for a and b in A, $a \leq_R b$ if and only if $b \leq a$.

(i) Show that $\leq_R$ is a partially ordering relation.

(ii) Show that if $(A, \leq)$ is a lattice then $(A, \leq_R)$ is also a lattice.

Sol. : (a) Since $\leq$ is a poset, we have

(i) $a \leq a$ (Reflexivity).

(ii) If $a \leq b$ and $b \leq a$, then $a = b$ (Antisymmetry).

(iii) If $a \leq b$, $b \leq c$, then $a \leq c$ (Transitivity)

Now, for every a in A, $a \leq a$. Hence, $a \leq_R a$. $\therefore\ \leq_R$ is reflexive.

Further, let $a \leq_R b$ and $b \leq_R a$. $\because\ a \leq_R b$ we have $b \leq a$.

$\because\ b \leq_R a$ we have $a \leq b$.

But since $\leq$ is antisymmetric if $b \leq a$ and $a \leq b$, then $a = b$.

Hence, if $a \leq_R b$ and $b \leq_R a$, then $a = b$.

$\therefore$ R is antisymmetric.

Further if $a \leq_R b$ and $b \leq_R c$, then $b \leq a$ and $c \leq b$.

This means $c \leq b$ and $b \leq a$.

Hence, $c \leq a$ $\therefore\ a \leq_R c$. $\therefore\ \leq_R$ is transitive. $\therefore\ (A, \leq_R)$ is a poset.

(b) Since $(A, \leq)$ is a lattice for every two elements a, b in A, GLB $= g$ and LUB $= l$ exist in A.

Consier $\{a, b, g, l\}$. Since g is GLB of a, b, $g \leq a$ and $g \leq b$.

$\therefore\ a \leq_R g$ and $b \leq_R g$ $\therefore$ g is the LUB of a, b.

Also since l is LUB of a, b, $a \leq l$ and $b \leq l$.

$\therefore\ l \leq_R a$ and $l \leq_R b$.

Hence, l is GLB of a, b. Hence, for a, b, GLB and LUB exist.

$\therefore\ (A, \leq_R)$ is also a lattice.

8. Product Partial Order

Theorem : If $(L_1, \leq)$ and $(L_2, \leq)$ are lattices, then $(L, \leq)$ is a lattice, where $L = L_1 \times L_2$ and the partial order $\leq$ of L is the product partial order. (M.U. 2003)

Proof : Let us denote the join and meet in L_1 by $\vee_1$ and $\wedge_1$ respectively and the join and meet in L_2 by $\vee_2$ and $\wedge_2$ respectively.

We have proved as theorem on page 4-25 that $(L, \leq)$ is a poset. Now, we need to prove that if (a_1, b_1) and $(a_2, b_2) \in L$ then $(a_1, b_1) \vee (a_2, b_2)$ and $(a_1, b_1) \wedge (a_2, b_2)$ are in L.

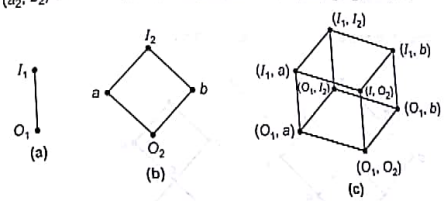


Fig. 4.102

It can be easily seen that since $a_1 < b_1$ and $a_2 < b_2$,

$(a_1, b_1) \vee (a_2, b_2) = (a_1 \vee a_2, b_1 \vee b_2)$

and $(a_1, b_1) \wedge (a_2, b_2) = (a_1 \wedge a_2, b_1 \wedge b_2)$

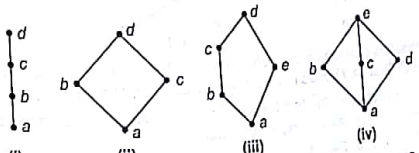
Hence, $(L, \leq)$ is a lattice.

For example, if L_1, L_2 are the lattices shown in Fig. 4.102 (a) and (b) then $L = L_1 \times L_2$ is the lattice shown in Fig. 4.102 (c).

(See also Examples 22, 23, 24 on page 4-17 and 4-18.)

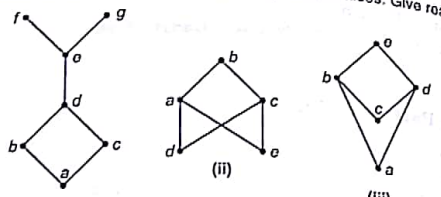
EXERCISE - VIII

1. State whether the following Hasse diagrams represent lattices.



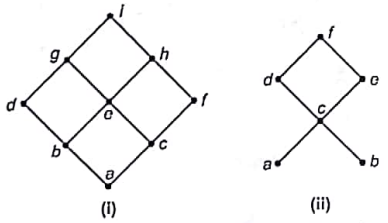
[**Ans. :** All the diagrams represent lattices]

2. State whether the following Hasse diagrams represent lattices. Give reasons.



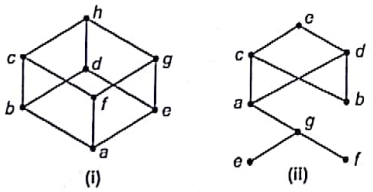
[**Ans. :** (i) The LUB of $\{f, g\}$ does not exists. It is not a lattice. (ii) The GLB of $\{a, c\}$ does not exist. Also the LUB of $\{d, e\}$ does not exist. It is not a lattice. (iii) The GLB of $\{b, d\}$ does not exist. It is not a lattice.]

3. Determine whether the following Hasse diagrams represent a lattice. Give reasons. (M.U. 2002)



[**Ans. :** (i) Yes. It is a lattice since each pair has a LUB and a GLB. (ii) No. It is not a lattice since GLB of $\{a, b\}$ does not exist.]

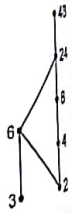
4. Determine whether following Hasse diagrams represent a lattice. Give reasons. (M.U. 2000, 2015)



[**Ans. :** (i) Yes. It is a lattice since each pair has a LUB and GLB. (ii) No. It is not a lattice, since GLB of $\{b, f\}$ does not exist. Also GLB of $\{e, f\}$ does not exist.]

5. Draw Hasse diagrams for the following poset under the relation R 'is divisible by' and determine whether it represents lattice.

$L = \{2, 3, 4, 6, 8, 24, 48\}$ (M.U. 2000)

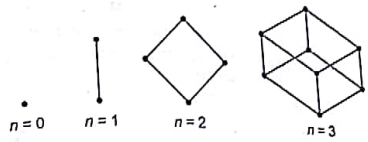


[**Ans. :** See adjoining figure.

It is not a lattice since the GLB of $\{2, 3\}$ does not exist.]

6. Draw Hasse diagrams of lattices having 2^n elements for $n = 0, 1, 2, 3$. (M.U. 1999)

Ans. :



7. Draw the Hasse diagram for $A = \{1, 3, 5, 15, 30\}$ and R is "a divides b". Check it is a lattice.

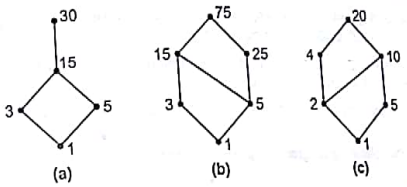
[**Ans. :** For Hasse diagram see Fig. (a) below ; Yes]

8. Draw Hasse diagram for $(D_{75}, \leq)$ and check whether it is a lattice.

[**Ans. :** $D_{75} = \{1, 3, 5, 15, 25, 75\}$; Yes. See Fig. (b) below.]

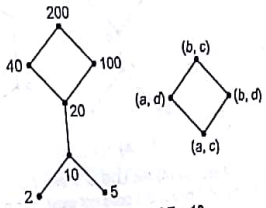
9. Draw Hasse diagram for $(D_{20}, \leq)$ and check if it is a lattice. (M.U. 2010, 12, 13)

[**Ans. :** $D_{20} = \{1, 2, 4, 5, 10, 20\}$; Yes. See Fig. (c) below.]



10. If $L_1 = \{a, b\}$ and $L_2 = \{c, d\}$ are lattices under usual relation $\leq$ in that order draw the Hasse diagram of $L_1 \times L_2$.

[**Ans. :** See adjoining figure.]



Answer of Ex. 10

11. Is the poset

$A = \{2, 5, 10, 20, 40, 100, 200\}$

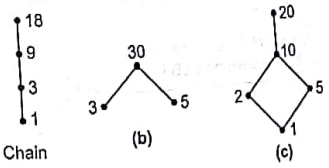
a lattice under the relation of divisibility ?

[**Ans. :** No]

12. Draw Hasse diagrams of the following sets under partial ordering relation 'divides' and indicate which are chains. (M.U. 2000)

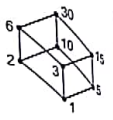
(a) $\{1, 3, 9, 18\}$, (b) $\{3, 5, 30\}$, (c) $\{1, 2, 5, 10, 20\}$.

[**Ans. :**



13. Draw the Hasse diagram for $L = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and let the relation R be 'is divisible by'. Determine whether it is a lattice.

(M.U. 2010, 12, 13)

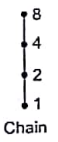


[Ans. : Hasse diagram shown in adjoining figure. Yes. It is a lattice.]

14. Draw the Hasse diagrams of the following sets under partial order relation divides and indicate which are chains.

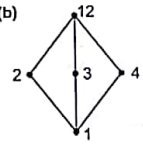
(a) {1, 2, 4, 8}, **(b)** {1, 2, 3, 4, 12}, **(c)** {1, 3, 5, 15}

[Ans. : (a)

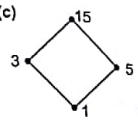


Chain

(b)

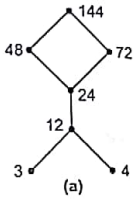


(c)

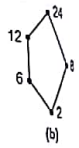


15. Is the poset $L = \{3, 4, 12, 24, 48, 72, 144\}$ under the relation of divisibility a lattice ? Draw the Hasse diagram.

[Ans. : Hasse diagram shown in adjoining figure (a). Not a lattice since the GLB of {3, 4} does not exist.]



(a)

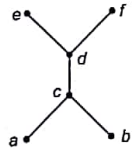


(b)

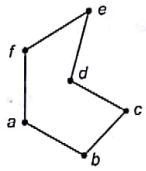
16. Is the poset $L = \{2, 6, 8, 12, 24\}$ under the relation of divisibility a lattice ? Draw the Hasse diagram.

[Ans. : Hasse diagram shown in above figure (b). It is a lattice.]

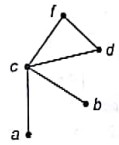
17. Which of the following diagrams represent lattice.



(A)



(B)

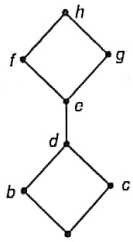


(C)

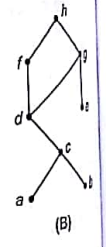
[Ans. : In (A) the LUB of e and f does not exist. Also the GLB of a and b does not exist. It is not a lattice. In (C) In the LUB of a, b does not exist. (B) is a lattice.]

18. Determine whether the following Hasse diagrams represent lattices.

[Ans. : (A) is a lattice, a distributive lattice. (B) is not a lattice. a, b have no GLB. d, e have no GLB.]



(A)



(B)

9. Special Types of Lattices

(1) **Sub-lattice**

Let $(L, \leq)$ be a lattice. A non-empty subset S of L is called a **sub-lattice** if for each $a \in S$ and $b \in S$, $a \vee b \in S$ and $a \wedge b \in S$.

In other words, if S is a non-empty subset of a lattice L such that every pair $\{a, b\}$ of two elements of S has a LUB and a GLB (*i.e.* S is a lattice) then S is called a sub-lattice.

Example 1 : Let $L = \{1, 2, 4, 5, 10, 20\}$ and $S = \{1, 4, 5, 20\}$. Let the relation be 'is divisible by'. Show that S is a sub-lattice.

Sol. : The Hasse diagram of L is as shown in Fig. 4.103 (a) below. It is easy to see that L is a lattice.

The Hasse diagram of S is as shown in Fig. 4.103 (b) below.

S is also a lattice. $\therefore$ S is a sub-lattice.

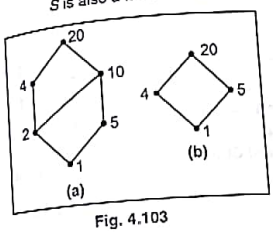


Fig. 4.103

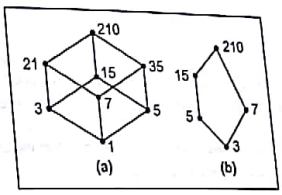


Fig. 4.104

Example 2 : Let $L = \{1, 3, 5, 7, 15, 21, 35, 210\}$ and $S = \{3, 5, 7, 15, 210\}$. Let the relation be 'is divisible by'. Show that S is a sub-lattice.

Sol. : The Hasse diagram of L is as shown in Fig. 4.104 (a) above. It is easy to see that L is a lattice.

The Hasse diagram of S is as shown in the Fig. 4.104 (b) above. It is easy to see that S is also a lattice.

$\therefore$ S is a sub-lattice.

Example 3 : Let $L = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and $S = \{1, 2, 3, 6, 10, 30\}$. Let the relation be 'is divisible by'. Show that S is a sub-lattice.

Sol. : The Hasse diagram of L is shown (Fig. 4.26) In Ex. 15, page 4-13. The Hasse diagram of S is as shown in Fig. 4.105. Since S is a lattice. S is a sub-lattice.

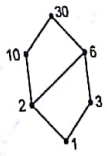
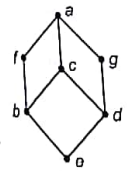
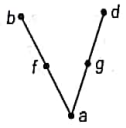


Fig. 4.105

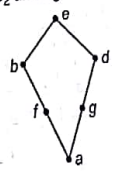
Example 4 : Consider the lattice L given in (a) below. Let S_1 be the poset (b), S_2 be the poset (c) and S_3 be the poset (d). Determine whether S_1, S_2 and S_3 are sub-lattices.



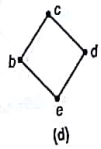
(a)



(b)



(c)



(d)

Fig. 4.106

Sol. : **(i)** The partially ordered subset S_1 shown in (b) is **not** a lattice since the LUB of $\{b, d\}$ does not exist.

(ii) The partially ordered subset S_2 shown in (c) is **not** a sub-lattice because the GLB of $\{b, d\}$ is c in the given set L and it does not belong to S_2.

(However, if we consider the poset S_2 independently, it is a lattice.)

(iii) The partially ordered subset S_3 shown in (d) is a sub-lattice.

Example 5 : Let $L = \mathcal{P}(A)$ be the lattice of all subsets of A under the relation of $\subseteq$ set inclusion. Let S be a subset of A.

Prove that $\mathcal{P}(S)$ is a sub-lattice.

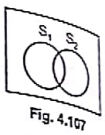


Fig. 4.107

Sol. : Let us consider any two subsets S_1 and S_2 of S. Then it is easy to see that $S_1 \cup S_2 \subseteq \mathcal{P}(S)$ and $S_1 \cap S_2 \subseteq \mathcal{P}(S)$ *i.e.* LUB of S_1 and S_2 and GLB of S_1 and S_2 belong to $\mathcal{P}(S)$. [Fig. 4.107]

Hence, $\mathcal{P}(S)$ is a sub-lattice.

Example 6 : Let $L = \{1, 2, 4, 8, 16, 32\}$ and $S = \{2, 8, 16\}$. Let the relation be "is divisibly by". Prove that S is a sub-lattice.

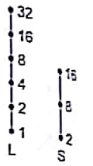


Fig. 4.108

Sol. : $S = \{2, 8, 16\}$ under the relation "is divisibly by" is a chain as shown in the Fig. 4.108.

Further every pair of elements of S has the LUB and GLB.

Hence, S is a sub-lattice.

Example 7 : Let $(L, \leq)$ be a lattice in which $L = \{a_1, a_2, \ldots, a_8\}$. Diagram of $(L, \leq)$ is given in the Fig. 4.109.

Let $S_1 = \{a_1, a_2, a_4, a_8\}$, $S_2 = \{a_3, a_5, a_7, a_8\}$, $S_3 = \{a_1, a_2, a_4, a_8\}$ be the subsets of L. Which of the above subsets $(S_1, \leq)$, $(S_2, \leq)$, $(S_3, \leq)$ are sublattices? (M.U. 2003)

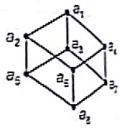
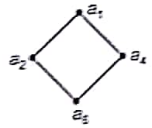


Fig. 4.109

Sol. : **(i)** The Hass diagram of $(S_1, \leq)$ is shown in the following left figure.



$\vee$	a_1	a_2	a_4	a_8
a_1	a_1	a_1	a_1	a_1
a_2	a_1	a_2	a_1	a_2
a_4	a_1	a_1	a_4	a_4
a_8	a_1	a_2	a_4	a_8

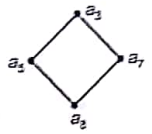
LUB

$\wedge$	a_1	a_2	a_4	a_8
a_1	a_1	a_2	a_4	a_8
a_2	a_2	a_2	a_8	a_8
a_4	a_4	a_8	a_4	a_8
a_8	a_8	a_8	a_8	a_8

GLB

$\therefore$ S_1 is a sublattice.

(ii) The Hass diagram of $(S_2, \leq)$ is shown in the following left figure.



$\vee$	a_3	a_5	a_7	a_8
a_3	a_3	a_3	a_3	a_3
a_5	a_3	a_5	a_3	a_5
a_7	a_3	a_3	a_7	a_7
a_8	a_3	a_5	a_7	a_8

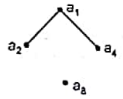
LUB

$\wedge$	a_3	a_5	a_7	a_8
a_3	a_3	a_5	a_3	a_8
a_5	a_5	a_5	a_8	a_8
a_7	a_7	a_8	a_7	a_8
a_8	a_8	a_8	a_8	a_8

GLB

$\therefore$ S_2 is a sublattice.

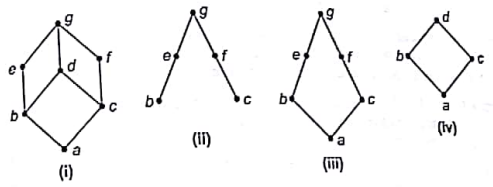
(iii) The Hasse diagram of $(S_3, \leq)$ is shown in the figure.



Since GLB of $a_2 \wedge a_4$ $(= a_6)$ does not belong to S_3, it is not a lattice.

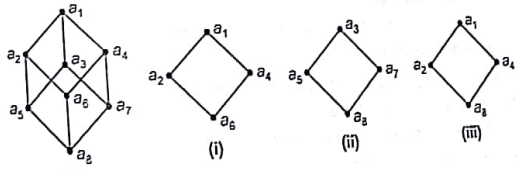
EXERCISE - IX

1. Given the lattice $(L, \leq)$ where $L = \{a, b, c, d, e, f, g\}$ shown in (i), examine whether $S_1 = \{b, c, e, f, g\}$ shown in (ii), $S_2 = \{a, b, c, e, f, g\}$ shown in (iii) and $S_3 = \{a, b, c, d\}$ shown in (iv) are sub-lattices.



[**Ans. :** **(i)** S_1 is not a sub-lattice as the GLB of $\{b, c\}$ does not exist. **(ii)** S_2 is not a sub-lattice as the LUB of $\{b, c\}$ is d in L, it does not belong to S_2. However, if we consider the poset S_2 independently, it is a lattice. **(iii)** S_3 is a sub-lattice.]

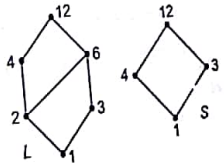
2. Given the lattice $(L, \leq)$ where $L = \{a_1, a_2, a_3, \ldots, a_8\}$ as shown in (a), $S_1 = \{a_1, a_2, a_4, a_8\}$ as shown in (i), $S_2 = \{a_3, a_5, a_7, a_8\}$ as shown in (ii), $S_3 = \{a_1, a_2, a_4, a_8\}$ as shown in (iii). Examine whether S_1, S_2 and S_3 are sub-lattices.



[**Ans. :** **(i)** S_1 is a sub-lattice, **(ii)** S_2 is a sub-lattice, **(iii)** S_3 is not a sub-lattice as the GLB of $\{a_2, a_4\}$ is a_6 in L and it does not belong to S_3. However, if we consider S_3 independently then it is a lattice.]

3. Let $L = \{1, 2, 3, 4, 6, 12\}$ and $S = \{1, 3, 4, 12\}$. Let the relation be 'is divisible by'. Show that S is a sub-lattice.

[See adjoining figure.]



4. Let $S = \{a, b, c\}$ and let $L = \mathcal{P}(S)$ the set of all subsets of S be a lattice under the relation of $\subseteq$, set inclusion. Let $T = \{a, b\}$. Prove that $\mathcal{P}(T)$ is a sub-lattice of L where $\mathcal{P}(T)$ is the set of all subsets of T.

5. Show that a subset of a linearly ordered poset is a sub-lattice.

(**Hint :** Let a, b be any two elements of the poset. Then either $a \, R \, b$ or $b \, R \, a$. Let $a \, R \, b$ then $a \wedge b = a$ and $a \vee b = b$. Hence, the result.)

(2) Isomorphism

The essence of the concept of iso (same) morphism (shape) is given by the following definition.

Two algebraic systems are called **isomorphic** if there exists a translation rule between them so that any true statement in one system can be translated into a true system in another system. The translation rule is called an **isomorphism.**

We have already studied isomorphism between posets on page 4-26 Since a lattice also is a poset the idea of isomorphism can be extended to lattices also as follows.

Isomorphic Lattices : If L_1 and L_2 are two lattices such that there is a function $f : L_1 \to L_2$ such that (i) f is one-to-one, (ii) f is onto, (iii) $f(a \wedge b) = f(a) \wedge f(b)$, (iv) $f(a \vee b) = f(a) \vee f(b)$ for all $a, b \in L_1$ then the lattices L_1 and L_2 are called **isomorphic.**

Example 1 : Let $A = \{1, 2, 4, 8\}$ and let divisibility be the partial order ($\leq$) on A. Let $A' = \{0, 1, 2, 3\}$ and less than or equal to be the partial order ($\leq'$) on A'. Show that A, A' are isomorphic lattices. **(M.U. 1999)**

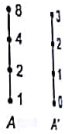


Fig. 4.110

Sol. : The Hasse diagrams are shown in the adjoining figure.

Clearly, A and A' are lattices.

Let the function f be $f(1) = 0$, $f(2) = 1$, $f(4) = 2$, $f(8) = 3$. It is easy to see that (i) f is one-to-one, (ii) f is onto.

Now, GLB of $\{2, 4\}$ *i.e.* $2 \wedge 4$ is 2 and $f(2) = 1$ *i.e.* $f(2 \wedge 4) = 1$. And $f(2) = 1$, $f(4) = 2$ and GLB of $\{1, 2\}$ is 1.

$\therefore \quad f(2) \wedge f(4) = 1 \qquad \therefore \quad f(2 \wedge 4) = f(2) \wedge f(4)$

Similarly, we can prove that,

$f(a \wedge b) = f(a) \wedge f(b)$ and $f(a \vee b) = f(a) \vee f(b)$ for each pair $a, b \in A$.

Hence, A_1, A_2 are isomorphic lattices.

Example 2 : Let $A = \{1, 2, 3, 6\}$ and $\leq$ be the relation 'is divisible by'.

Let $A = \mathcal{P}(\{a, b\}) = \{\Phi, \{a\}, \{b\}, \{a, b\}\}$.

Let $f : A \to A'$ be defined by $f(1) = \Phi$, $f(2) = \{a\}$, $f(3) = \{b\}$, $f(6) = \{a, b\}$.

Show that A, A' are isomorphic lattices.

Sol. : Refer to Ex. 3 page 4-26 (Fig. 4.60). Clearly f is a one-to-one correspondence.

From the Hasse diagram we can easily, prove that $f(a \wedge b) = f(a) \wedge f(b)$ and $f(a \vee b) = f(a) \vee f(b)$ for each pair of elements $a, b \in A$.

Hence, A, A' are isomorphic lattices.

Example 3 : Let $A = \{1, 2, 5, 7, 10, 14, 35, 70\}$ and $\leq$ be the relation 'is divisible by'. Let $A' = \mathcal{P}(\{a, b, c\}) = \{\Phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ and let $\leq'$ be the relation 'is a subset of'.

If $f : A \to A'$ is defined by

$f(1) = \Phi$, $f(2) = \{a\}$, $f(7) = \{b\}$, $f(5) = \{c\}$, $f(10) = \{a, c\}$,

$f(14) = \{a, b\}$, $f(35) = \{b, c\}$, $f(70) = \{a, b, c\}$.

Show that A, A' are isomorphic lattices.

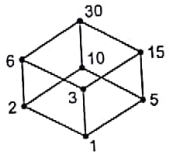
(See Fig. 4.98 on page 4-44 and Fig. 4.79 (c) on page 4-36)

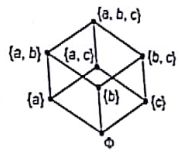
Sol. : Prove it.

Example 4 : Let $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and $\leq$ be the partial order relation of divisibility on A. Let $A' = \mathcal{P}(S)$ where $S = \{a, b, c\}$ be another poset with partial order relation $\subseteq$.

Show that $(A, \leq)$ and $(A', \subseteq)$ are isomorphic. **(M.U. 2007)**

Sol. : We have $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and R is the relation of divisibility. We have seen that it is a lattice (Ex. 13, page 4-50) and its Hasse diagram is shown below.





Also we have $A' = \mathcal{P}(S)$ where $S = \{a, b, c\}$ and R is the relation of set inclusion $\subseteq$. We have seen that it is a lattice (page 4-36) and its Hasse diagram is shown above.

We can define $f : A \to A'$ as

$f(1) = \Phi$, $f(2) = \{a\}$, $f(3) = \{b\}$, $f(5) = \{c\}$, $f(6) = \{a, b\}$,

$f(10) = \{a, c\}$, $f(15) = \{b, c\}$, $f(30) = \{a, b, c\}$.

From Hasse diagram we see that

$f(a \wedge b) = f(a) \wedge f(b)$ and $f(a \vee b) = f(a) \vee f(b)$ for every a and b.

Hence, A, B are isomorphic.

Example 5 : Let $A = \{2, 4, 8, 12, 36\}$ and $B = \{3, 6, 9, 12, 24\}$ and let $\leq$ be the relation of divisibility.

Are the lattices isomorphic ? **(M.U. 2008)**

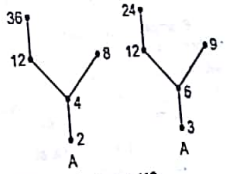


Fig. 4.112

Sol. : Yes. Let us define $f(2) = 3$, $f(4) = 6$, $f(8) = 9$, $f(12) = 12$, $f(36) = 24$.

From Hasse diagram, we see that

$f(a \wedge b) = f(a) \wedge f(b)$.

If $a = 2$, $b = 4$ then $f(a) = f(2) = 3$, $f(b) = f(4) = 6$, $f(a) \wedge f(b) = 3 \wedge 6 = 3$ and $a \wedge b = 2 \wedge 4 = 2$ and $f(2) = 3$.

Similarly, we can prove that $f(a \vee b) = f(a) \vee f(b)$ for any a and b.

Hence, A and B are isomorphic.

EXERCISE - X

1. Let $A = \{1, 2, 3, 4\}$ and $\leq$ be the relation 'is less than'. $A' = \{3, 6, 9, 12\}$ and $\leq'$ be the relation 'is less than'. If $f : A \to A'$ is given by $f(a) = 3a$, prove that A and A' are isomorphic lattices.

2. Let $A = \{1, 3, 4, 12\}$ and $\leq$ be the relation 'is divisible by'. Let $A' = \{1, 4, 5, 20\}$, $\leq'$ be the relation 'is divisible by'. If $f : A \to A'$ is given by $f(1) = 1$, $f(3) = 4$, $f(4) = 5$, $f(12) = 20$, prove that A and A' are isomorphic lattices.

3. Let $A = \{1, 3, 5, 15\}$ and $\leq$ be the relation 'is divisible by'. Let $A' = \{1, 2, 3, 6\}$ and $\leq'$ be the relation 'is divisible by'. If $f : A \to A'$ is given by $f(1) = 1$, $f(3) = 2$, $f(5) = 3$, $f(15) = 6$, prove that A and A' are isomorphic lattices.

4. Let $A = \{1, 3, 5, 7, 15, 21, 35, 105\}$ and $\leq$ be the relation 'is divisible by'. Let $A' = \mathcal{P}(\{a, b, c\}) = \{\Phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ and let $\leq'$ be the relation 'is a subset of'. If $f : A \to A'$ is given by

$f(1) = \Phi$, $f(3) = \{a\}$, $f(5) = \{b\}$, $f(7) = \{c\}$, $f(15) = \{a, b\}$,

$f(21) = \{a, c\}$, $f(35) = \{b, c\}$, $f(105) = \{a, b, c\}$.

Show that A and A' are isomorphic lattices. (See Ex. 3, Fig. 4.71, page 4-31; and Fig. 4.79 (c) on page 4-36.)

5. Let $S = \{a, b, c\}$ and $L = \mathcal{P}(S)$. Prove that $(L, \subseteq)$ is a lattice and that it is isomorphic with D_{42}.

(Hint : See Fig. 4.79 (c) page 4-36 and Fig. 4.51 (b), page 4-21.) **(M.U. 2004)**

6. Let $S = \{a, b, c\}$ and $L = \mathcal{P}(S)$. Prove that $(L, \subseteq)$ is isomorphic with D_{30}.

7. Let $A = \{2, 3, 5, 7, 15, 21, 35, 210\}$ and $\leq$ be the relation 'is divisible by'. Let $A' = \mathcal{P}(\{a, b, c\}) = \{\Phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$ and $\leq'$ be the relation 'is a subset of'. If $f : A \to A'$ is given by

$f(1) = \Phi$, $f(3) = \{a\}$, $f(5) = \{c\}$, $f(7) = \{b\}$, $f(15) = \{a, c\}$,

$f(21) = \{a, b\}$, $f(35) = \{b, c\}$, $f(210) = \{a, b, c\}$.

Show that A and A' are isomorphic lattices.

[See Fig. 4.104 (a), page 4-51; Fig. 4.79 (c), page 4-36]

8. Show that D_{30} and D_{42} are isomorphic. **(M.U. 2006)**

---

(3) Distributive Lattices **(M.U. 2000, 14, 16)**

Definition : A lattice L is called **distributive** if for **any** elements a, b, c of L the following distributive properties are satisfied. *i.e.*, $\vee$ distributes over $\wedge$ and $\wedge$ distributes over $\vee$.

(a) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

(b) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Example 1 : Let L be the power set $\mathcal{P}(A)$ of A and R be the relation 'is a subset of'. L is a distributive lattice.

Sol. : Consider $A = \{a, b, c\}$ then $L = \mathcal{P}(A) = \{\Phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}\}$. If R is the relation 'is a subset of' the Hasse diagram is shown in adjoining figure.

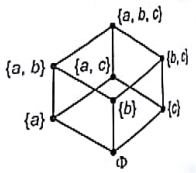


Fig. 4.113

The LUB $\{\{a\}, \{b\}\} = \{a, b\}$

i.e. LUB $\{\{a\}, \{b\}\} = \{a\} \cup \{b\}$.

The GLB $\{\{a\}, \{b\}\} = \Phi$

i.e. GLB $\{\{a\}, \{b\}\} = \{a\} \cap \{b\}$.

Thus, the join and meet correspond to union and intersection and since union and intersection satisfy distributive property L is a distributive lattice.

Example 2 : Consider the lattice shown in Fig. 4.114. Show that it is distributive.

Sol. : Consider the three elements a, b, c.

$a \vee b = b$, $b \vee c = e$, $a \vee c = c$

$a \wedge b = a$, $b \wedge c = a$, $a \wedge c = a$

Now, $a \wedge (b \vee c) = a \wedge e = a$

and $(a \wedge b) \vee (a \wedge c) = a \vee a = a$

Also $a \vee (b \wedge c) = a \vee a = a$

$(a \vee b) \wedge (a \vee c) = b \wedge c = a$

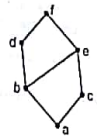


Fig. 4.114

In this way we can show that distributive property is satisfied for any three elements of a, b, c.

$\therefore$ L is a distributive lattice.

Note ...

There are 12 triples to be checked.

Example 3 : Show that the lattices whose Hasse diagrams are given below (Fig. 4.115) are not distributive. **(M.U. 2001, 03, 09)**

Sol. : For (i) $b \vee d = d$, $b \vee c = c$, $d \vee c = e$

$b \wedge d = b$, $b \wedge c = a$, $d \wedge c = a$

Now, $d \wedge (b \vee c) = d \wedge e = d$

$(d \wedge b) \vee (d \wedge c) = b \vee a = b$

$\therefore$ The distributive property is **not** satisfied.

Hence, the lattice is **not** distributive.

For (ii) $b \vee c = e$, $b \wedge d = a$, $c \vee d = e$

$b \wedge c = a$, $b \wedge d = a$, $c \wedge d = a$

Now, $d \wedge (c \vee d) = d \wedge e = d$

$(b \wedge c) \vee (b \wedge d) = a \vee a = a$

$\therefore$ The distributive property is **not** satisfied.

Hence, the lattice is **not** distributive.

For (iii), we see that

$a \wedge (b \vee c) = a \wedge f = a$

and $(a \wedge b) \vee (a \wedge c) = a \vee a = a$

$\therefore$ $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

But $b \vee (d \wedge e) = b \wedge a = a$

and $(b \vee d) \wedge (b \vee c) = d \wedge f = d$.

$\therefore$ The distributive property is **not** satisfied.

Hence, the lattice is **not** distributive.

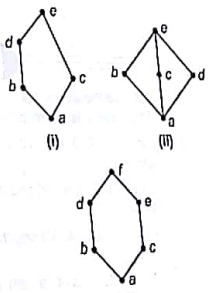


Fig. 4.115

Notes ...

1. For a distributive lattice L, it is necessary that the property of distributivity must be satisfied for all $a, b, c \in L$. Note Ex. 3(iii) carefully.
2. The following theorem which we accept without proof is highly useful to show that a given lattice is non-distributive.

"A lattice is non-distributive if and only if it contains a sub-lattice which is isomorphic to one of the first two lattices of Example 3 above.

Example 4 : Show that in a distributive lattice $(A, \leq)$ if $a \wedge x = a \wedge y$ and if $a \vee x = a \vee y$ then $x = y$. **(M.U. 1995)**

Sol. : By definition of LUB y is less than or equal to the LUB of y and $y \wedge a$.

$\therefore \quad y \leq y \vee (y \wedge a)$. But $y \wedge y = y$

$\therefore \quad y \leq (y \wedge y) \vee (y \wedge a) = y \wedge (y \vee a)$ [By distributivity]

But $y \vee a = a \vee x$ [Data]

$\therefore \quad y \leq y \wedge (a \vee x) = (y \wedge a) \vee (y \wedge x)$

But $y \wedge a = a \wedge x$ [Data]

$\therefore \quad y \leq (a \wedge x) \vee (y \wedge x) = x \wedge (a \vee y)$ [By distributivity]

By definition of GLB x is greater than or equal to the GLB of x and $a \vee x$.

But $a \vee x = a \vee y$ [Data]

$\therefore$ x is greater than or equal to x and $a \vee y$.

$\therefore \quad x \wedge (a \vee y) \leq x \quad \therefore \quad y \leq x$.

Similarly, we can prove that

$x \leq y \quad \therefore \quad x = y$.

EXERCISE - XI

1. Let L be the power set $\mathcal{P}(A)$ of A where $A = \{a, b\}$. Let R be the relation 'is a subset of'. Show that L is a distributive lattice.
2. Let $L = \{1, 2, 3, 4, 6, 12\}$ and the relation be 'is divisible by'. Show that L is a distributive lattice.
3. Let $L = \{1, 2, 3, 4, 12\}$ and the relation be 'is divisible by'. Show that L is not a distributive lattice. **(M.U. 2006)**
4. Let $L = \{1, 2, 3, 5, 30\}$ and the relation be 'is divisible by'. Show that L is not a distributive lattice.
5. Let $L = \{1, 2, 3, 4, 9, 36\}$ and the relation be 'is divisible by'. Show that L is not a distributive lattice.
6. Let $L = \{1, 3, 5, 12, 20, 60\}$ and the relation be 'is divisible by'. Show that L is not a distributive lattice.
7. Let $L = \{1, 3, 5, 6, 10, 60\}$ and the relation be 'is divisible by'. Show that L is not a distributive lattice.
8. Let $L = \{1, 3, 5, 6, 9, 15, 45\}$ and the relation be 'divisible by'. Show that L is not a distributive lattice. **(M.U. 2008)**
9. Show that the lattices shown in Fig. 4.116 are not distributive.

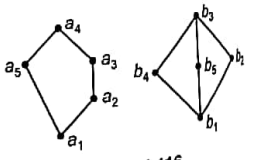


Fig. 4.116

(4) Bounded Lattice

A lattice L is said to be **bounded** if it has a **greatest element** and a **least element**.

Example 1 : The lattice $L = \{1, 2, 3, 4, \ldots, 10\}$ under partial order $\leq$ is bounded since its least element is 1 and greatest element is 10.

Example 2 : The lattice $L = \mathcal{P}(S)$ of all subsets of S is bounded since Φ is its least element and S is its greatest element.

(5) Complement of an element **(M.U. 1999, 2000)**

Let L be a bounded lattice with greatest element 1 and least element 0. Let an element $a \in L$. An element $\overline{a}$ belonging to L is called **complement** of a if

LUB $(\{a, \overline{a}\})$ *i.e.* $a \vee \overline{a} = 1$ and GLB $(\{a, \overline{a}\})$ *i.e.* $a \wedge \overline{a} = 0$

Note that $\overline{0} = 1$ and $\overline{1} = 0$ where bars denote the complement.

Remarks ....

1. Some authors use dash (') to denote the complement. A lattice L is called **complemented** if it is bounded and if **every element of L** has a complement.
2. Note that if a is a complement of b then b is a complement of a. The relation is symmetric.

Example 1 : Let $S = \{a, b, c\}$ and $L = \mathcal{P}(S) = \{\Phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$. Let the relation be 'is a subset of '. Show that every element has a complement.

Sol. : If $A \subset L$ then the complement set $\overline{A}$ of A is the complement of A since $A \vee \overline{A} = A \cup \overline{A} = S$ and $A \wedge \overline{A} = A \cap \overline{A} = \Phi$ and S is the greatest element and Φ is the least element. (See Fig. 4.79 (c), page 4-36).

The list of complements of all elements is given below.

Element	:	Φ	$\{a\}$	$\{b\}$	$\{c\}$	$\{a,b\}$	$\{b,c\}$	$\{a,c\}$	$\{a,b,c\}$
Complement	:	$\{a,b,c\}$	$\{b,c\}$	$\{a,c\}$	$\{a,b\}$	$\{c\}$	$\{a\}$	$\{b\}$	Φ

Example 2 : Consider the lattices given in the Fig. 4.93. List the complements of all elements.

Sol. : Using the definition, we find that

For (i)

Element	:	0	b	a	c	1
Complement	:	1	c	c	a,b	0

For (ii)

Element	:	0	a	b	c	1
Complement	:	1	b,c	a,c	a,b	0

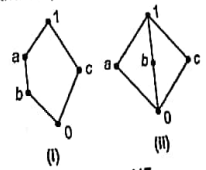


Fig. 4.117

Theorem : Let L be bounded distributive lattice. Show that the complement of an element of L if exists is unique. **(M.U. 1999, 2005, 06, 07, 09, 10, 16)**

Sol. : Let $a \in L$ and let a have a complement. We shall prove the result by reductio-ad-absurdum method.

Let, if possible a_1 and a_2 be the complements of a. ..... (1)

By definition of complement

$a \vee a_1 = 1$ and $a \vee a_2 = 1$

$a \wedge a_1 = 0$ and $a \wedge a_2 = 0$

Since, 0 is the least element, the LUB of $\{a_1, 0\} = a_1$.

$\therefore \quad a_1 = a_1 \vee 0 = a_1 \vee (a \wedge a_2)$ [By (2)] ..... (2)

$= (a_1 \vee a) \wedge (a_1 \vee a_2)$ [By distributivity]

$= 1 \wedge (a_1 \vee a_2)$ [By (1)]

Since, 1 is the greatest element, the GLB $\{a_1 \vee a_2, 1\}$ is $a_1 \vee a_2$ ..... (3)

i.e. $1 \wedge (a_1 \vee a_2) = a_1 \vee a_2$.

$\therefore \quad a_1 = a_1 \vee a_2$ [By (2) and (3)]

Similarly, arguing in the same way, we can prove that ..... (4)

$a_2 = a_1 \vee a_2$

Hence, from (4) and (5), we gat $a_1 = a_2$. ..... (5)

Example 3 : Let $L = \{1, 2, 4, 5, 10, 20\}$ and the relation be 'is divisible by'. List the complements of all elements of L. **(M.U. 2006, 07, 12, 13)**

Sol. : [See Fig. 4.118 below.]

Element	:	1	4	5	2	10	20
Complement	:	20	5	4	No compl.	No compl.	1

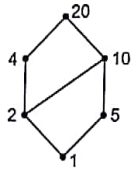


Fig. 4.118

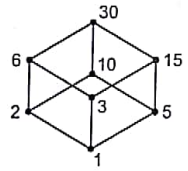


Fig. 4.119

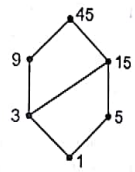


Fig. 4.120

Example 4 : Let $L = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and the relation be 'is divisible by'. List the complements of all elements of L. **(M.U. 2010, 12, 13)**

Sol. : [See Fig. 4.119 above]

Element	:	1	2	5	3
Complement	:	30	15	6	10

Example 5 : Let $L = \{1, 3, 5, 9, 15, 45\}$ and the relation be 'is divisibly by'. List the complements of all elements of L. **(M.U. 2006)**

Sol. : [See Fig. 4.120 above]

Element	:	1	3	5	9	15	45
Complement	:	45	No Compl.	9	5	No. Compl.	1

Note ....

In Ex. 2, we find that **some elements can have more than one** complement. In Ex. 3, we find that **some elements may not have a** complement.

However, **if L is a distributive bounded lattice** then **if an element has a complement, then it is unique.** (See Theorem page 4-59 at the bottom)

EXERCISE - XII

1. Let $S = \{a, b\}$ and $L = \mathcal{P}(S) = \{\Phi, \{a\}, \{b\}, \{a, b\}\}$. Let the relation be 'is a subset of'. Show that every element has a complement. (See Fig. 4.60 on page 4-26)

Ans. :

Element	:	Φ	$\{a\}$	$\{b\}$	$\{a, b\}$
Complement	:	$\{a, b\}$	$\{b\}$	$\{a\}$	Φ

2. Let $L = \{1, 2, 3, 6\}$ and the relation be 'is divisible by'. Write the complements of the elements of L (See Fig. 4.60 on page 4-26)

Ans. :

Element	:	1	2	3	6
Complement	:	6	3	2	1

3. Let $L = \{1, 2, 3, 5, 30\}$. Let the relation be 'is divisible by'. Write the complements of the elements of L. (See Fig. 4.83, page 4-38) **(M.U. 2013, 18)**

Ans. :

Element	:	1	2	3	5	30
Complement	:	30	3, 5	2, 5	2, 3	1

4. Let $L = \{1, 2, 3, 4, 12\}$. Let the relation be 'is divisible by'. Write the complements of elements of L (See Fig. 4.3 (c), page 4-5)

Ans. :

Element	:	1	2	3	4	12
Complement	:	12	3	2, 4	3	1

5. Let $L = \{2, 6, 8, 12, 24\}$. Let the relation be 'is divisible by'. Write the complements of elements of L. (Draw figure similar to the above figure)

Ans. :

Element	:	2	6	12	8	24
Complement	:	24	8	8	6, 12	2

6. Let $L = \{2, 3, 5, 7, 15, 21, 35, 105\}$. Let the relation be 'is divisible by'. Write the complements of elements of L. (Draw figure similar to Fig. 4.71 page 4-32)

Ans. :

Element	:	2	3	5	7
Complement	:	105	35	21	15

7. Let $L = \{1, 2, 3, 4, 6, 12\}$. Let the relation be 'is divisible by'. Write the complements of L. (See Fig. 4.48, page 4-21)

Ans. :

Element	:	1	2	3	4	6
Complement	:	12	No compl.	4	3	No compl.

8. Let $L = \{1, 2, 3, 6, 10, 30\}$. Let the relation be 'is divisible by'. Write the complements of L (See Fig. 4.105, page 4-51)

Ans. :

Element	:	1	2	3	6	10
Complement	:	30	No compl.	10	No compl.	3

9. Find the complement of each element in D_{42}. **(M.U. 1999, 2000, 05, 07, 14)**

(D_{42} denotes the set of all positive divisors of 42)

(**Hint :** $L = \{1, 2, 3, 6, 7, 14, 21, 42\}$ and Hasse diagram is given in Fig. 4.51 (b), page 4-21)

Ans. :

Element	:	1	2	3	6
Complement	:	42	21	14	7

(6) Complemented Lattice

A lattice L is called **complemented** if it is bounded and if every element of L has atleast one complement.

Example 1 : Let $S = \{a, b, c\}$ and $L = \mathcal{P}(S)$ with 'set inclusion' as the relation.
As seen earlier (Ex. 1, page 4-59), L is bounded and each element has a complement.
$\therefore$ L is a complemented lattice.

Example 2 : Let $L = \{1, 2, 3, 5, 6, 10, 15, 30\}$ with 'divisibility' relation.
As seen earlier (Ex. 4, page 4-60), L is bounded and each element has a complement.
$\therefore$ L is a complemented lattice.

Example 3 : Let $L = \{1, 2, 3, 6, 7, 14, 21, 42\}$ with 'divisibility' relation.
As seen earlier (Ex. 9, page 4-61), L is bounded and each element has a complement.
$\therefore$ L is a complemented lattice.

Example 4 : Let $L = \{1, 2, 3, 5, 30\}$ with 'divisibility' relation.
As seen earlier (Ex. 3, page 4-61), L is bounded and each element has a complement.
$\therefore$ L is a complemented lattice.

Example 5 : Let $L = \{1, 2, 4, 5, 10, 20\}$ with divisibility relation.
As seen earlier (Ex. 3, page 4-60), the elements 2, 10 have no complements.
$\therefore$ L is not a complemented lattice.

EXERCISE - XIII

1. In the previous Exercise - XI, page 4-58 show that the lattices given in Ex. 1, 2, 3, 4, 5, 8 and 9 are complemented, while those given in Ex. 7 and 8 are not complemented.
2. Show that the lattice shown in Fig. 4.121 is neither distributive nor complemented. (M.U. 1998)
3. Show that the lattice shown in Fig. 4.122 is distributive but not complemented. (M.U. 2002, 07)
4. Show that the lattice shown in Fig. 4.123 is neither distributive nor complemented. (M.U. 2002, 07)

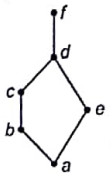


Fig. 4.121

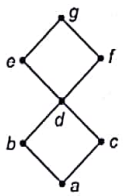


Fig. 4.122

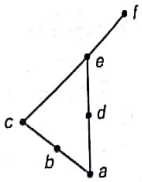
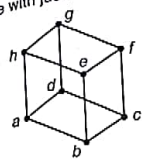


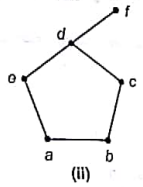
Fig. 4.123

EXERCISE - XIV

State with justification which of the following are lattices. (M.U. 2013)



(i)



(ii)

[Ans. : (i) Yes, (ii) No]

Theory

1. Define partial order relation. (M.U. 1997, 2001)
2. Define dual of a poset with an example. (M.U. 2009)
3. Define POSET and Hasse Diagram. (M.U. 2010, 13)
4. Define the terms for a subset B of a poset A -
   (i) upper bound, (ii) least upper bound, (iii) lower bound, (iv) greatest lower bound.
   Give one example of each. (M.U. 1996)
5. Explain the terms : (i) Posets, (ii) Lattice. (M.U. 1999, 2013, 17)
   (iii) Extremal elements. (M.U. 2008)
5. Define distributive Lattice and complemented Lattice. (M.U. 1999)
   Give an example. (M.U. 2014, 16)
6. Let L be a distributive Lattice. Show that if a complement exists then it is unique. (M.U. 1999, 2009)
7. For a given set S, let $P(S)$ denote the power set of A. Consider the relation $A\ R\ B$ if $A \subseteq B$. Show that R is a partial order relation.
8. If L is a bounded and distribution lattice then prove that the complement is unique if it exists. (M.U. 2004)

CHAPTER 10

Some Algebraic Structures

1. Introduction

In this chapter we shall define groups, rings, fields and prove some of their elementary properties. These concepts are as basic to Modern Mathematics as the operations of addition and multiplication are to school mathematics. In fact the basic operations in arithmetic are generalised in Modern Mathematics to abstract level.

2. Binary Operation

(a) Definition : Let A be a non-empty set. A function $f : A \times A \to A$ is called a **binary** operation.

Examples of Binary Operation

It should be noted that since a binary operation is a function, one and only one element of A is assigned to one ordered pair of $A \times A$. Further, we shall denote binary operations by $*$ or $(+)$ instead of f. Since, a binary operation is a function to each $(a, b) \in A \times A$, there exists a unique element $a * b \in A$. We describe this property by saying that A is closed under $*$.

Example 1 : Let $A = Z$ and $a * b$ be $a + b$. Then $*$ is a binary operation on Z.

Example 2 : Let $A = Z^+$ and $a * b$ be $a - b$.

Then $*$ is not a binary operation on Z^+ since $a - b$ may not be an element of A for some a, b in A. *e.g.* $3 * 7 = 3 - 7 = -4$ does not belong to Z^+.

Example 3 : Let $A = R$ and $a * b$ be a / b.

Then $*$ is not a binary operation on R since a / b may not be an element of R for some a, b in A. *e.g.* $5 * 0 = 5 / 0 \notin A$.

However, if $A = R - \{0\}$ then $a * b = a / b$ is a binary operation.

Example 4 : Let L be a lattice and $a * b$ be $a \wedge b$ (GLB of a, b).

Then $a * b$ is a binary operation because for every ordered pair a, b of L, there exists a unique $a \wedge b$.

Example 5 : Let L be a lattice $a * b$ be $a \vee b$ (LUB of a, b).

Then $a * b$ is a binary operation for the reason given above.

(b) Identity and Inverse

Definition : Given a non-empty set A and a binary operation $\oplus$ if there is an element $e \in A$, such that for **every** $a \in A$, $a \odot e = e \odot a = a$, then e is called the **identity** element for the operation $\odot$.

For example, in the set of real numbers, zero is identity element for usual addition because $a + 0 = 0 + a = a$ for every $a \in R$.

In the set of real numbers, unity is identity element for usual multiplication because $a \times 1 = 1 \times a = a$ for every $a \in R$.

Definition : Given a non-empty set A and a binary operation $\odot$ if A has an identity element e and if for any two element $a, b \in S$, $a \odot b = b \odot a = e$, then b is called the **inverse** of a and is denoted by a^{-1}.

Example : "If a binary operation in Q^+ (set of positive rational numbers) is defined by $a \odot b = ab / 2$ then 2 is an identity and $4/a$ is the inverse of a under $\odot$".

State true or false with proper justification. **(M.U. 2004)**

Sol. : If e is an identity element under $\odot$, we must have

$$a \odot e = e \odot a = a$$

But by data, $a \odot e = \frac{ae}{2}$

$\therefore \frac{ae}{2} = a \quad \therefore e = 2$ is identity.

If b is the inverse of a, we must have

$$a \odot b = b \odot a = 2 \quad \text{(identity)}$$

But by data, $a \odot b = \frac{ab}{2}$

$\therefore \frac{ab}{2} = 2 \quad \therefore b = \frac{4}{a} \quad \therefore a^{-1} = \frac{4}{a}$

Hence, the statement is true.

3. Properties of Binary Operations

1. Commutativity

Definition : A binary operation on set A is called commutative if

$$\boxed{a * b = b * a} \quad \text{for all element } a \text{ and } b \text{ of } A.$$

Example 1 : The binary operation of usual addition in Z is commutative ?

Example 2 : The binary operation of usual subtraction (division) on Z is not commutative.

2. Associativity

Definition : A binary operation $*$ on a set A is said to be **associative**, if

$$\boxed{a * (b * c) = (a * b) * c} \quad \text{for all } a, b, c \in A.$$

Example 1 : Is the binary operation of usual addition on Z associative ?

Sol. : Because $a + (b + c) = (a + b) + c$ for all $a, b, c \in Z$, the operation of addition is associative.

Example 2 : Show that the relation $*$ given by $a * b = a^b$ on the set of natural numbers is a binary operation. Is it associative? **(M.U. 2005, 07)**

Sol. : If a and b are natural numbers, then a^b is also a natural numbers.

Hence, $a * b$ is binary.

Since, $a^{b^c} \neq a^{c^b}$, the operation is not associative.

Example 3 : Is the binary operation of usual subtraction (division) on Z associative ? Commutative ? (M.U. 2003)

Sol. : Because $a-(b-c) \neq (a-b)-c$ e.g. $5-(6-4)=5-(2)=3$ and $(5-6)-4=-1-4=-5$, the usual subtraction is not associative on Z.

Also $5-8 \neq 8-5$.

It is not commutative on Z.

Example 4 : Is the operation $*$ on $A=\{a, b, c\}$ defined by the adjoining table associative ?

*	a	b	c
a	a	a	c
b	a	b	a
c	c	a	c

Sol. : Although $(a * c) * b = c * b = a$ and $a * (c * b) = a * a = a$ but $a * (b * c) = a * a = a$ and $(a * b) * c = a * c = c$, the operation $*$ is not associative.

Example 5 : Is the operation $a * b = a \times |b|$, associative on R ?

Sol. : Because $(a * b) * c = (a \times |b|) * c = a \times |b| \times |c|$

and $a * (b * c) = a * (b \times |c|) = a \times |b \times |c|| = a \times |b| \times |c|$

We see that $*$ is associative. (But note that $*$ is not commutative).

Example 6 : Is the operation $a * b = ab / 5$ on R associative ?

Sol. : Because $(a * b) * c = (ab / 5) * c = abc / 25$

and $a * (b * c) = a * (bc / 5) = abc / 25$,

the operation $*$ is associative. (Note that $*$ is also commutative.)

Example 7 : Let L be a lattice and let $a * b = a \wedge b$ (the greatest lower bound). Then $*$ is associative.

Sol. : Since $(a * b) * c = (a \wedge b) \wedge c$ and $a * (b * c) = a \wedge (b \wedge c)$

But, $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.

Hence, the result.

Similarly, we can prove that $a * b = a \vee b$ (the least upper bound of a and b) is also associative.

EXERCISE - I

1. Show that o given by $a \circ b = a^b$ is a binary operation on the set of natural numbers. (M.U. 2005, 07)

2. Verify whether the following binary operations are commutative and associative.

   (a) Usual subtraction / division on Z. [**Ans. :** Neither commutative nor associative]

   (b) $a * b = a + b + 3$ on Z^+. [**Ans. :** Commutative and Associative]

   (c) $a * b = a / b$ on non-zero real numbers. [**Ans. :** Neither commutative, nor associative]

   (d) $a * b = ab$ on Z. [**Ans. :** Commutative and Associative]

   (e) $a * b$ = maximum (minimum) of a and b on R. [**Ans. :** Commutative and Associative]

   (f) $a * b = ab / 7$. [**Ans. :** Commutative and Associative]

   (g) $a * b = ab + 3b$ on R. [**Ans. :** Neither Commutative nor Associative]

3. Consider the set $A = \{0, 1, 2, 3\}$. Give one example for each of the following.

   (i) A relation R on A that is neither symmetric, nor anti-symmetric.

   (ii) A relation R on A that is symmetric, transitive but not reflexive.

   (iii) A binary operation on A that is commutative but not associative. (M.U. 2005)

*	0	1	2	3
0	1	2	3	0
1	2	3	2	2
2	3	2	0	2
3	0	2	2	1

[**Ans. :** (i) $R = \{(1, 3), (1, 0), (2, 0), (0, 1)$.

(ii) $R = \{(0, 1), (1, 0), (1, 2), (2, 1), (2, 3), (3, 2), (0, 0), (1, 3), (3, 1)\}$]

(iii) See adjoining Table.

4. Semi-Group

(M.U. 2000, 10, 13)

(a) Definition

A non-empty set S together with a (i) binary and (ii) associative operation, $*$ is called a semi-group.

We denote the semi-group by $(S, *)$. Thus, a non-empty set S is a semi-group if

(i) $*$ is binary *i.e.* $a * b \in S$ for every $a, b \in S$.

(ii) $*$ is associative *i.e.* $a * (b * c) = (a * b) * c$ for every $a, b, c \in S$.

Definition : A semi-group $(S, *)$ is called commutative semi-group if $*$ is commutative.

Thus, $(S, *)$ will be a commutative semi-group if $*$ is (i) binary, (ii) associative and (iii) commutative.

Examples of Semi-groups

Example 1 : $(Z, +)$ is a commutative semi-group.

Example 2 : If A is a set and $\mathcal{P}(A)$ is its power set then $\mathcal{P}(A)$ with the operation of union is a commutative semi-group.

Example 3 : Prove that the set Q of rational numbers with the binary operation $*$ defined by $a * b = a + b - ab$; $a, b \in Q$ is a semi-group. Is it commutative ? (M.U. 2005)

Sol. : With usual multiplication addition and subtraction for any two rational numbers $a * b = a + b - ab$ belongs to Q. Hence, $*$ is a binary operation.

Now, $(a * b) * c = (a + b - ab) * c$

$= (a + b - ab) + c - (a + b - ab) * c$

$= a + b - ab + c - ac - bc + abc$

$= a + b + c - ab - bc - ca + abc$.

Also, $a * (b * c) = a * (b + c - bc) = a + (b + c - bc)$

$= a + b + c - bc - ab - ac + abc$

$= a + b + c - ab - bc - ca + abc$.

Hence, $*$ is associative.

Further $b * a = b + a - ba = a + b - ab$

$\therefore$ $*$ is also commutative.

Hence, $a * b = b * a$.

Example 4 : Let $Z_n = \{0, 1, 2, ..., (n-1)\}$ and * be the operation on Z_n such that $a * b$ = the remainder when ab is divided by n.

(a) Construct the table for the operation * when $n = 4$.

(b) Show that $(Z_4, *)$ is a semigroup.

(M.U. 1997, 99, 2017)

Sol. : (a) We have $Z_4 = \{0, 1, 2, 3\}$ and $a * b$ = remainder when ab is divided by 4.

With this understanding, we get the adjoining table.

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(b) **(i)** From the table it is clear the Z_n is closed under * because $a * b$ belongs to Z_n.

(ii) Now consider associativity. Let $a = 1$, $b = 2$, $c = 3$ then using the table we see that

$$(a * b) * c = 2 * 3 = 2$$
$$a * (b * c) = 1 * 2 = 2$$
$$\therefore \quad (a * b) * c = a * (b * c)$$

It can be verified for all the elements.

Hence, * is associative. Hence, $(Z_n, *)$ is a semigroup for any n.

Example 5 : Let $(A, *)$ be a semigroup. Consider a binary operation + on A such that for x and y in A, $x + y = x * a * y$ where a is in A.

Show that + is an associative operation. (M.U. 1997)

Sol. : To prove associativity, we shall prove that

$$(x + y) + z = x + (y + z) \quad \text{where } x, y, z \in R$$

Now, L.H.S. $= (x + y) + z = (x * a * y) + z$

$= (x * a * y) * a * z = x * a * y * a * z$

And R.H.S. $= x + (y + z) = x + (y * a * z)$

$= x * a * (y * a * z) = x * a * y * a * z$

$\therefore$ L.H.S. = R.H.S.

$\therefore$ + is an associative operation.

(b) Product of Semi-groups

Let $(S_1, *_1)$ and $(S_2, *_2)$ be two semi-groups. We can obtain a new semi-group $S = S_1 \otimes S_2$ called the product of S_1 and S_2 as follows.

(i) The elements of S come from $S_1 \times S_2$ *i.e.* if the ordered pair (a, b) is an element S, then $a \in S_1$ and $b \in S_2$.

(ii) The operation * on S is defined on the two components as

$$(a, b) * (a', b') = (a *_1 a', b *_2 b') \quad [\text{See Ex. 1, page 10-11}]$$

5. Monoid (M.U. 2000, 10)

(a) Definition : A semi-group $(S, *)$ which has identity is called a monoid.

Thus, we can say that there are semi-groups which have identity (in which case we call them monoids) and there are semi-groups without identity element.

(b) Theorem : The identity element of a semi-group is unique.

Proof : If possible let e' be another identity element of the semi-group $(S, *)$. Since e' is an identity, $a * e' = e' * a = a$ for each a.

In particular, let $a = e$. $\therefore \quad e * e' = e' * e = e$ ..... (1)

Also since e is an identity, $a * e = e * a = a$ for each a.

In particular let $a = e'$, $\therefore \quad e' * e = e * e' = e$ ..... (2)

From (i) and (ii), it follows that $e = e'$.

$\therefore$ The identity element is unique.

Examples of Monoid

Example 1 : The semi-group $(Z, +)$ is a monoid because 0 is the identity element.

But note that the semi-group $(Z^+, +)$ is not a monoid as it has no identity element.

Example 2 : The semi-group $(Z^+, \times)$ is a monoid because 1 is its identity element.

Example 3 : Let S be a finite set. Let $F(S)$ be the set of all functions $f : S \to S$ and let * be operation of composition of functions.

$F(S)$ is a monoid because * is associative and identity function is the identity of this semi-group.

Example 4 : Verify that if A is any set then the power set $\mathcal{P}(A)$ with the operation of union is a monoid.

Sol. : As seen before in Ex. 2, page 10-4 for union $(\mathcal{P}(A), \cup)$ is a commutative semi-group.

If Φ is the null-set then Φ is the identity element because

$$\Phi * A = \Phi \cup A = A \quad \text{and} \quad A * \Phi = A \cup \Phi = A$$

Hence, $(\mathcal{P}(A), \cup)$ is a monoid.

Note that $\mathcal{P}(S)$ with * as intersection of two subsets of $\mathcal{P}(S)$ is also a monoid with $\mathcal{P}(S)$ itself as identity. It is also commutative.

Example 5 : If $a * b = a$ and S is the set of all positive integers $Z^+ = \{1, 2, 3, ...\}$, verify whether $(S, *)$ is a semi-group or a monoid.

Sol. : Since for every a, b, $a * b = a$ is in S, * is binary.

Further, $(a * b) * c = a * c = a$ and $a * (b * c) = a * b = a$

$\therefore$ * is associative.

Hence, $(S, *)$ is a semi-group.

But $a * 1 = a$ and $1 * a = 1$.

Hence, $(S, *)$ has no identity element. $\therefore$ $(S, *)$ is not a monoid.

6. Isomorphism, Automorphism And Homomorphism

We have already studied isomorphism between two posets. In general, two algebraic systems are called isomorphic if they preserve special characteristics of the system. We shall now consider isomorphism between two semi-groups.

Isomorphism

Definition : Let $(S, *)$ and $(S', *')$ be two semi-groups. A function $f : S \to S'$ is called an isomorphism from $(S, *)$ to $(S', *')$ if f is one-to-one and onto and if

$$f(a * b) = f(a) *' f(b) \quad \text{for all } a, b \text{ in } S.$$

Note carefully the * on the left side and *' on the right side.

Theorem 1 : If $(S, *)$ and $(S', *')$ are two semi-groups and if $f : S \to S'$ is a isomorphism from $(S, *)$ to $(S', *')$ then $f^{-1} : S' \to S$ is also an isomorphism from $(S', *')$ to $(S, *)$.

Proof : Since by definition of isomorphism, f is a one-to-one correspondence hence f^{-1} exists and is a one-to-one correspondence from $(S', *')$ to $(S, *)$.

Let a' and b' be any two elements of S'. Since f is onto there exist elements a and b in S such that $f(a) = a'$ and $f(b) = b'$.

$\therefore \quad a = f^{-1}(a')$ and $b = f^{-1}(b)$

Now, $f^{-1}(a' *' b') = f^{-1}(f(a) *' f(b)) = f^{-1}(f(a * b))$

[$\because$ f is a isomorphism $f(a * b) = f(a) *' f(b)$ by definition above.]

$\therefore \quad f^{-1}(a' *' b') = (f^{-1} \circ f)(a * b)$

$= a * b = f^{-1}(a') * f^{-1}(b')$

Hence, f^{-1} is an isomorphism.

Procedure To Prove An Isomorphism

To prove an isomorphism between two semi-groups $(S, *)$ and $(S', *')$ we shall follow the following procedure.

(i) **Step 1 :** We define the function $f : S \to S'$ with domain of $f = S$.

(ii) **Step 2 :** We shall show that f is one-to-one.

(iii) **Step 3 :** We shall show that f is onto.

(iv) **Step 4 :** We shall show that $f(a * b) = f(a) *' f(b)$.

Example 1 : Let S be the set of all even integers. Show that the semi-groups $(Z, +)$ and $(S, +)$ are isomorphic. **(M.U. 2016)**

Sol. : We shall follow the above procedure.

Step 1 : We define the function $f : Z \to S$ where $f(a) = 2a$.

Step 2 : Suppose $f(a_1) = f(a_2)$. Then $2a_1 = 2a_2$. Hence, f is one-to-one.

Step 3 : Suppose b is an even integer.

Then $a = b/2 \in Z$ and $f(a) = f(b/2) = 2(b/2) = b$. Hence, f is onto.

Step 4 : We have $f(a + b) = 2(a + b) = 2a + 2b$

$= f(a) + f(b)$

Hence, $(Z, +)$ and $(S, +)$ are iso-morphic semi-groups.

Example 2 : Let R^+ be the set of all positive real numbers. Show that the function $f : R^+ \to R$ defined by $f(x) = \log x$ is an isomorphism from the semigroup $(R^+, \times)$ to the semigroup $(R, +)$ where $\times$ and $+$ are the usual multiplication and addition respectively. **(M.U. 2004, 05)**

Sol. : Step 1 : The function is defined by $f(x) = \log x$.

Step 2 : If $f(a_1) = f(a_2)$, then $\log a_1 = \log a_2$

$\therefore \quad a_1 = a_2$. f is one-to-one.

Step 3 : Suppose b is a real number then

$e^b \in R$ and $f(e^b) = \log e^b = b \in R^+$.

$\therefore$ Each element of R is an f-image of some element of R^+.

$\therefore$ f is onto.

Step 4 : We have $f(ab) = \log ab = \log a + \log b = f(a) + f(b)$

$\therefore$ f is an isomorphism.

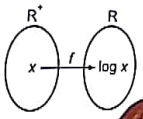


Fig. 10.1

Example 3 : Let $S = \{a, b, c\}$ and $S' = \{p, q, r\}$ and consider the following operations.

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*'$	p	q	r
p	r	p	q
q	p	q	r
r	q	r	p

Let $f(a) = q$, $f(b) = p$, $f(c) = r$. Show that S and S' are isomorphic.

Sol. : Step 1 : The function f is defined by $f(a) = q$, $f(b) = p$, $f(c) = r$.

Step 2 : Clearly f is one-to-one.

Step 3 : Clearly f is onto.

Step 4 : Now, from the first table above since $a * b = b$

$f(a * b) = f(b) = p$

Also, since $f(a) = q$, $f(b) = p$,

$f(a) *' f(b) = q *' p = p$ $\therefore$ $f(a * b) = f(a) *' f(b)$

This can be shown to be true for all possible products of a, b and c. In fact we can obtain the table of operation $*$ on $f(a)$, $f(b)$ and $f(c)$ by replacing in the first table, the images of a, b, c i.e. by replacing a by $f(a) = q$, b by $f(b) = p$ and c by $f(c) = r$. Thus, we get

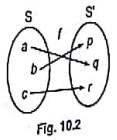


Fig. 10.2

$*$	q	p	r
q	q	p	r
p	p	r	q
r	r	q	p

Interchanging the first and second rows we get the left table. Then interchanging the first and second columns we get the table on the right which is the same as the table given for $*'$ on S'. This shows that S and S' are isomorphic.

$*$	q	p	r
p	p	r	q
q	q	p	r
r	r	q	p

$*$	p	q	r
p	r	p	p
q	p	q	r
r	q	r	p

Example 4 : Let $S = \{a, b, c, d\}$ and $S' = \{p, q, r, s\}$ and consider the following operations.

$*$	a	b	c	d
a	a	b	c	d
b	b	a	a	c
c	b	d	d	c
d	a	b	c	d

$*'$	p	q	r	s
p	p	q	r	s
q	q	p	p	r
r	q	s	s	r
s	p	q	r	s

Let $f(a) = p$, $f(b) = q$, $f(c) = r$, $f(d) = s$. Show that f is an isomorphism.

Sol. : Step 1 : The function is defined by $f(a) = p$, $f(b) = q$, $f(c) = r$, $f(d) = s$.

Step 2 : Clearly f is one-to-one.

Step 3 : Clearly f is onto.

Step 4 : Now $a * b = b$. $\therefore$ $f(a * b) = f(b) = q$

Since $f(a) = p$ and $f(b) = q$

$f(a) *' f(b) = p *' q = q$ $\therefore$ $f(a * b) = f(a) *' f(b)$

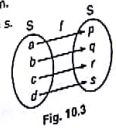


Fig. 10.3

This can be shown to be true for all possible products of a, b, c and d.

Hence, f is isomorphic.

Theorem 2 : Let $(S, *)$ and $(S', *')$ be monoids with identity elements e and e' respectively. Let $f : S \to S'$ be an isomorphism from $(S, *)$ to $(S', *')$. Prove that $f(e) = e'$. (M.U., 2003)

Proof : Let b be any element of S'.

Since f is onto there is an element a in S such that b is the image of a i.e. $f(a) = b$.

Now, $b = f(a) = f(a * e) = f(a) *' f(e)$

because S and S' are **isomorphic.**

But $f(a) = b$. ..... (1)

$\therefore$ From (1), we get $b = b *' f(e)$

Similarly, since $a = e * a$

$b = f(a) = f(e * a) = f(e) *' f(a)$ ..... (2)

because S and S' are isomorphic.

$\therefore$ $b = f(e) *' b$

From (2) and (3), we see that $f(e)$ is the identity element of S'. ..... (3)

But since identity element is unique, we get, $f(e) = e'$.

Corollary : If $(S, *)$ and $(S', *')$ are two semi-groups such that S has an identity element while S' does not have the identity element then $(S, *)$ and $(S', *')$ cannot be isomorphic.

Proof : For isomorphism of two semi-groups we must have, for all a, b, S,

$$f(a * b) = f(a) *' f(b)$$

If we take $b = e$, the identity element in S, then we must have,

$$f(a * e) = f(a) *' f(e) = f(a) *' e'$$

where, e' is the identity element of S' by the above theorem.

Since, by data e' does not exist, S and S' cannot be isomorphic.

Example : Let Z be the set of all integers and S' be the set of all even integers. If X is the usual multiplication then prove that (Z, X) and (S, X) are semi-groups which are not isomorphic.

Sol. : We can easily prove that (Z, X) and (S', X) are semi-groups because multiplication is binary and associative in both Z and S'.

But $Z = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ has multiplicative identity 1

and $S' = \{\ldots, -6, -4, -2, 2, 4, 6, \ldots\}$ has no multiplicative identity.

Hence, by the above corollary (Z, X) and (S', X) are not isomorphic.

Automorphism

Definition : An isomorphism from a semigroup $(S, *)$ to $(S, *)$ itself is called an automorphism (auto = self) on $(S, *)$.

Example 1 : Let $S = \{a, b, c, d\}$ and consider the following operations $*$.

*	a	b	c	d
a	a	b	c	d
b	b	a	a	c
c	b	d	d	c
d	a	b	c	d

Let $f(a) = d$, $f(b) = c$, $f(c) = b$ and $f(d) = a$.

Show that f is an automorphism.

Step 1 : The function is defined by

$f(a) = d$, $f(b) = c$, $f(c) = b$, $f(d) = a$.

Step 2 : Clearly f is one-to-one.

Step 3 : Clearly f is onto.

Step 4 : From the table

$a * b = b$ $\therefore$ $f(a * b) = f(b) = c$

Since $f(a) = d$, $f(b) = c$

$f(a) * f(b) = d * c = c$ $\therefore$ $f(a * b) = f(a) * f(b)$

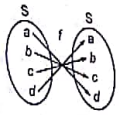


Fig. 16.4

This can be shown to be true for all products of a, b, c and d.

Hence, f is isomorphic.

$\therefore$ $(S, *)$ is an automorphism.

If we drop the conditions of one-to-one and onto from the definition of isomorphism we get another property, called homomorphism of the algebraic structures of two semi-groups.

Homomorphism

Definition : Let $(S, *)$ and $(S', *')$ be two semi-groups. A function $f : S \to S'$ is called a homomorphism from $(S, *)$ to $(S', *')$ if

$$\boxed{f(a * b) = f(a) *' f(b)}$$ for all a, b in S.

Further if f is also onto S' is called a **homomorphic image** of S.

We note that for isomorphism as well as for homomorphism, the image of the product is equal to the product of the images

i.e., $f(a * b) = f(a) *' f(b)$

And the difference is that, in isomorphism f is one-to-one and also onto.

Theorem 3 : Let $(S, *)$ and $(S', *')$ be monoids with identity elements e and e' respectively. Let $f : S \to S'$ be homomorphism from $(S, *)$ to $(S', *')$.

Prove that $f(e) = e'$.

Proof : Similar to the proof of Theorem 2, page 10-9 and as such is left to you.

Theorem 4 : If f is a homomorphism from a commutative semi-group $(S, *)$ onto a semi-group $(S', *')$ then $(S', *')$ is also commutative.

Proof : Let s_1' and s_2' be any two elements of S'. Since f is onto there exist two elements s_1 and s_2 in S whose images are s_1' and s_2' respective i.e. $f(s_1) = s_1'$ and $f(s_2) = s_2'$.

$\therefore$ $s_1' *' s_2' = f(s_1) *' f(s_2)$

$= f(s_1 * s_2) = f(s_2 * s_1)$

[$\because$ $(S, *)$ is a commutative semi-group.]

$= f(s_2) *' f(s_1)$

$= s_2' *' s_1'$

$\therefore$ $(S', *')$ is also commutative.

Example 1 : Let $S = N \times N$. Let $*$ be the operation on S defined by $(a, b) * (a', b') = (a + a', b + b')$. Further, let $f : (S, *) \to (Z, +)$ defined by $f(a + b) = a - b$. Show that $(S, *)$ is a semi-group and f is a homomorphism. (M.U. 2004)

Sol. : (a) Let $x = (a, b)$, $y = (c, d)$, $z = (e, f)$ where $a, b, c, d, e, f \in N$.

(i) $x * y = (a, b) * (c, d)$

$= (a + c, b + d)$

But $a + c \in N$ and $b + d \in N$

$\therefore \quad (a + c, b + d) \in N \times N$. $*$ is binary.

(ii) $x(yz) = (a, b) * [(c, d) * (e, f)]$

$= (a, b) * (c + e, d + f)$

$= [a + (c + e), b + (d + f)]$

$(xy) z = [(a, b) * (c, d)] * (e, f)$

$= (a + c, b + d) * (e, f)$

$= [(a + c) + e, (b + d) + f]$

But as $a, b, c, d, e, f \in N$.

$a + (c + e) = a + c + e = (a + c) + e$

$b + (d + f) = b + d + f = (b + d) + f$

$\therefore$ $*$ is associative. Hence, $(S, *)$ is a semi-group.

(b) Further, we have

$f(x * y) = f(a + c, b + d)$

$= (a + c) - (b + d) = (a - b) + (c - d)$

$= f(a, b) + f(c, d) = f(x) + f(y)$

But $f : S \to Z$ is not onto. Hence, f is homomorphism.

Example 2 : Let $S = N \times N$ and $*$ be the operation on S defined by $(a, b) * (a', b') = (aa', bb')$. Show, that $(S, *)$ is a semi-group. If f is defined by $f : (S, *) \to (Q, *)$ by $f(a, b) = a / b$, show that f is homomorphism.

Sol. : Left to you.

If $x = (a, b)$, $y = (c, d)$, $z = (e, f)$, note that

$f(x * y) = f(ac, bd) = (ac) / (bd)$

$= (a / b) (c / d) = f(x) \times f(y)$.

7. Group

(M.U. 2000, 01, 10, 17)

Definition : An ordered pair $(G, *)$ is called a **group**, if G is a non-empty set and $*$ is a binary **operation** on G satisfying the following axioms.

$G1$: For all $a, b, c \in G$, $a * (b * c) = (a * b) * c$.

(*i.e.*, $*$ **is associative** in G.)

$G2$: There exists an element $e \in G$, such that $e * a = a * e = a$ for all $a \in G$. The element e is called **identity** for $*$.

(*i.e.*, **Identity** e for $*$ exists in G.)

$G3$: For every $a \in G$ there exists an element $b \in G$ such that $a * b = b * a = e$. The element b is called the **inverse** of a and is denoted by a' or by a^{-1}.

(*i.e.*, for every element in G **inverse** exists.)

Abelian or Commutative Group : A group $(G, *)$ is called commutative or Abelian if $a * b = b * a$ for all $a, b \in G$. (M.U. 2002)

Most of the groups that we shall be dealing with are commutative *i.e.* Abelian groups. But all groups are not commutative. If M is the set of non-singular $n \times n$ matrices then the set forms a non-commutative group under multiplication. You might have noticed that in general $A \times B = B \times A$ where A and B are non-singular square matrices of the same order.

Examples of Groups

Example 1 : Let $G = \{ x \mid x$ is a real number$\}$ and $a * b = a + b$, the usual addition. Then $(G, *)$ is an Abelian group with 0 as identity and $-a$ as a^{-1}.

Example 2 : Let $G = \{x \mid x$ is a rational number excluding zero$\}$ and $a * b = a \times b$, the usual multiplication.

G is group with 1 as identity and q / p as inverse of p / q.

Example 3 : Let $G = \{0, \pm 1, \pm 2, ...\}$ and $a * b = a + b$ the usual sum of Integers. Then $(G, *)$ is an Abelian group with 0 as identity and $-a$ is a^{-1}.

Example 4 : Let $G = \{ x \mid x$ a non-zero real number $\}$ and $a * b = a \times b$, the usual multiplication. Then $(G, *)$ is an Abelian group with 1 as identity and $1/a$ as a^{-1}.

Example 5 : Let $G = \{ z \mid z$ is a complex number $\}$ and $a * b = a + b$, the addition of complex numbers. Then $(G, *)$ is an Abelian group with $0 + i0$ an identity and $-x - iy$ as the inverse of $x + iy$.

Example 6 : Let $G = \{ z \mid z$ is a non-zero complex number $\}$ $a * b = a \times b$, the multiplication of complex numbers. Then $(G, *)$ is an Abelian group with $1 + i \cdot 0$ as identity and $(x - iy) / (x^2 + y^2)$ as inverse of $x + iy$.

Example 7 : Let $G = \{ z \mid z = e^{i\theta} \}$ and $a * b = a \times b$ usual multiplication of complex numbers. Then $(G, *)$ is an Abelian group with e^{i0} as unity and $e^{-i\theta}$ as inverse of $e^{i\theta}$.

Example 8 : Let $G = \{1, -1\}$ and $a * b = a \times b$ with usual multiplication. Then $(G, *)$ is a group with 1 as identity and each element is inverse of itself.

Examples of Non-Commutative Groups

Example 1 : Let $G = \{ M \mid M$ is a 2×2 non-singular matrix $\}$ and $A * B$ be the usual matrix multiplication. Then $(G, *)$ is a group but **not** an Abelian group. (We shall discuss this problem in detail on page 10-18 in Ex. 12.)

Example 2 : Let $G = \{ (a, b) \mid (a, b)$ is an ordered pair of real numbers, $a \neq 0 \}$ and $(a, b) * (c, d) = (ac, bc + d)$. Then $(G, *)$ is a group but **not** an Abelian group. (See Ex. 11, page 16-17).

To prove that G is a group

Example 1 : Prove that $G = \{1, -1, i, -i\}$ is a group under usual multiplication $*$ of complex numbers. (M.U. 2002, 05)

Sol. : The adjoining table shows the result of multiplication of elements of G.

$*$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	1

Since for every pair $a, b \in G$ there exists a unique element $a * b$ in G, $*$ is a binary operation in G.

G 1 : Since multiplication of complex numbers is associative, the multiplication * is associative in G.

G 2 : From the first column (or row) we see that 1 is an identity element. Hence, $1 \in G$ is an identity element.

G 3 : Since $1 * 1 = 1$, $(-1) * (-1) = 1$, $(i) * (-i) = 1$, $(-i) \times (i) = 1$, inverse exists for every elements in G. We have $1^{-1} = 1$, $-1^{-1} = -1$, $i^{-1} = -i$, $-i^{-1} = i$.

Hence, G is a group under multiplication.

Example 2 : Prove that the set of cube-roots of unity is a group under multiplication of complex numbers. **(M.U. 2005)**

Sol. : We know that the three cuberoots of unity are $1, \omega, \omega^2$, where $\omega = e^{2\pi i/3}$, $\omega^2 = e^{4\pi i/3}$.

*	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

The multiplication table is given on the right. The table shows that G is closed under *.

G 1 : Since multiplication of complex numbers is associative, multiplication is associative in G.

G 2 : From the first row (or column) we find that 1 is the identity element.

G 3 : Since the identity element 1 appears in each row (column) each element has its inverse

$\therefore \quad (1)^{-1} = 1, \quad (\omega)^{-1} = \omega^2, \quad (\omega^2)^{-1} = \omega.$

$\therefore$ Cube-roots of unity is a group under multiplication.

Example 3 : Prove that the set of real numbers is a group under * defined by

$$a * b = a + b - 2.$$

Sol. : Since for every $a, b \in R$, there exists a unique element $a * b = a + b - 2$ in R, * is a binary operation in R.

G 1 : $(a * b) * c = (a + b - 2) * c = (a + b - 2) + c - 2$

$= a + b + c - 4$

And $a * (b * c) = a * (b + c - 2) = a + (b + c - 2) - 2$

$= a + b + c - 4$

$\therefore \quad (a * b) * c = a * (b * c)$ for all $a, b, c \in R$.

$\therefore \quad *$ is associative in R.

G 2 : To find identity e, consider $a * e = a$

But $a * e = a + e - 2$

$\therefore \quad a + e - 2 = a \quad \therefore \quad e = 2.$ $\therefore$ 2 is the identity element.

G 3 : To find inverse of a. Let b be the inverse. Then $a * b = e = 2$

$\therefore \quad a + b - 2 = 2 \quad \therefore \quad b = 4 - a.$

$\therefore \quad 4 - a$ is the inverse of a. $\therefore$ Hence, G is a group under *.

Example 4 : Determine whether the following set together with the binary operation * is a semi-group, monoid or a group. Justify your answer.

(a) Set of real numbers with $a * b = a + b + 2$. **(M.U. 2000)**

(b) The set of $m \times n$ matrices under the operation of multiplication.

Sol. : (a) Since for every $a, b \in R$, there exists a unique element $a * b = a + b + 2$ in R, * is a binary operation.

G1 : $(a * b) * c = (a + b + 2) * c = (a + b + 2) + c + 2 = a + b + c + 4$

and $a * (b * c) = a * (b + c + 2) = a + (b + c + 2) + 2 = a + b + c + 4$

$\therefore \quad (a * b) * c = a * (b * c) \quad \therefore$ * is associative in R.

G2 : To find identity, consider $a * e = a$.

$\therefore \quad a + e + 2 = a \quad \therefore \quad e = -2$

$\therefore \quad -2$ is the identity element.

G3 : To find the inverse. Let b be the inverse of a. Then by definition of the inverse

$a * b = e \quad \therefore \quad a + b + 2 = -2 \quad \therefore \quad a + b = -4 \quad \therefore \quad b = -4 - a$

Hence, $-4 - a$ is the inverse of a.

$\therefore \quad G$ is a group under *.

(b) If A and B are two $m \times n$ matrices, then we know that AB is not defined.

$\therefore$ The operation of multiplication is not binary and hence the set of $m \times n$ matrices under multiplication is not a monoid, a subgroup or a group.

Example 5 : Let G be the set of rational numbers different from 1.

Let $a * b = a + b - ab$ for all $a, b \in G$. Prove that $(G, *)$ is a group. **(M.U. 2005, 13, 18)**

Sol. : Let $a, b \in G$. We shall prove that $a * b = a + b - ab$ is a rational number different from 1 by reduction-ad-absurdum method.

If possible, let $a + b - ab = +1$

$\therefore \quad a - b + b - ab = 0 \quad \therefore \quad (a - 1) - b(a - 1) = 0$

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

Hence, $a = +1$, $b = +1$ which is absurd since $a, b \in G$, the set of rational numbers different from 1.

$\therefore \quad a * b$ is a rational number different from 1 *i.e.* $a * b \in G$.

$\therefore \quad *$ is a binary operation.

G 1 : $a * (b * c) = a * (b + c - bc) = a + (b + c - bc) - a(b + c + bc)$

$= a + b + c - bc - ab - ac - abc$

And $(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b + ab)c$

$= a + b + c - ab - ac - bc - abc.$

Hence, $a * (b * c) = (a * b) * c. \quad \therefore \quad *$ is associative.

G 2 : Now $a * 0 = a + 0 + a\,0 = a$

Also $0 * a = 0 + a + 0\,a = a \quad \therefore \quad 0 \in G$ is the identity element.

G 3 : For a given $a, b \in G$ consider the equation $a * b = 0$

i.e., $a + b - ab = 0. \quad \therefore \quad b = -\dfrac{a}{1 - a}.$

Since $a * b = a + b - ab = 0$, b is the inverse of G. Since $a \in G$, $a \neq 1$.

$\therefore \quad b$ is rational. Further $b = -\dfrac{a}{1 - a} \neq 1$ because if $b = -\dfrac{a}{1 - a} = 1$

i.e., $-a = 1 - a$ *i.e.*, $0 = 1$ which is absurd.

Hence, b is different from one.

$\therefore\ b = -\frac{a}{1-a} \in G$ $\therefore$ b is the inverse of a.

$\therefore\ a^{-1} = -\frac{a}{1-a}$. Hence, G is a group under $*$.

Example 6 : Prove that if G is the set of all subsets of A, a non-empty set A and $*$ the operation of union, then $(G, *)$ is not a group. **(M.U. 2001)**

Sol. : If A, B are the subsets of A then $A \cup B$ is also a subset of A.

$\therefore$ G is closed under $*$.

G 1 : $A \cup (B \cup C) = (A \cup B) \cup C$.

$\therefore$ $*$ is associative.

G 2 : If Φ denotes empty set.

$A \cup \Phi = A$ and $\Phi \cup A = A$ $\therefore$ $\Phi \in G$ is identity element.

G 3 : But the inverse of a set $A \in G$ does not exist because we cannot find a non-empty set B such that $A \cup B = \Phi$.

$\therefore$ Inverse does not exist. $\therefore$ $(G, *)$ is not a group.

Example 7 : Let G be a set of all square matrices of type $\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$ where $m \in Z$. Prove that G is a group under multiplication. Is it a Abelian group ? **(M.U. 2002, 03)**

Sol. : Let $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$

$\therefore\ AB = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix} \in G$

$\therefore$ Multiplication is binary operation.

G 1 : Since matrix multiplication is associative, multiplication in the example is associative.

G 2 : Let $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$AI = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$. Also $IA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$

$\therefore$ I is identity element.

G 3 : Since $|A| = 1 \neq 0$, inverse of A exists for every $A \in G$.

$\therefore$ $(G, *)$ is a group under multiplication.

Now, $AB = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$ as seen above and $BA = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$

$\therefore$ $AB = BA$. $\therefore$ $(G, *)$ is an Abelian group.

Example 8 : Let G be the set of complex numbers for which $|z| = 1$. Is $(G, *)$ a group where $*$ is multiplication of complex numbers ? **(M.U. 2002)**

Sol. : Let $z_1 = x_1 + iy_1$, $z_2 = x_2 + iy_2$ where $|z_1| = 1$, $|z_2| = 1$ *i.e.* $x_1^2 + y_1^2 = 1$, $x_2^2 + y_2^2 = 1$.

Now, $z_1 z_2 = (x_1 + iy_1)(x_2 + iy_2) = (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_2)$

$\therefore$ $|z_1 z_2|^2 = (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2$

$= x_1^2x_2^2 + y_1^2y_2^2 - 2x_1x_2y_1y_2 + x_1^2y_2^2 + x_2^2y_1^2 + 2x_1x_2y_1y_2$.

$= x_1^2x_2^2 + x_1^2y_2^2 + y_1^2x_2^2 + y_1^2y_2^2$

$= x_1^2(x_2^2 + y_2^2) + y_1^2(x_2^2 + y_2^2)$

$= (x_1^2 + y_1^2)(x_2^2 + y_2^2) = 1 \times 1 = 1$

$\therefore$ $|z_1 z_2| = 1$

$\therefore$ $*$ is a binary operation.

G 1 : Multiplication of complex numbers is associative.

$\therefore$ $*$ is associative.

G 2 : For any complex number $z = x + iy$, $(x + iy)(1 + i0) = x + iy$

$\therefore$ $(1 + i0)$ whose modulus 1 is the identity element.

G 3 : Let $z = x + iy$ and $z^{-1} = x - iy$

$\therefore$ $z * z^{-1} = (x + iy)(x - iy) = x^2 + y^2 = 1$

$\therefore$ For every $z \in G$ the inverse exist.

$\therefore$ Further, since for complex numbers $z_1 z_2 = z_2 z_1$

$\therefore$ $(G, *)$ is an Abelian group.

Example 9 : If R is the set of all real numbers other than zero and if $a * b = 2ab$, prove that $(R, *)$ is an Abelian group. **(M.U. 2002, 03, 08, 14)**

Sol. : Since $a * b = 2ab \in R$, $*$ is a binary operation in R.

G 1 : $a * (b * c) = a * (2bc) = 2a(2bc) = 4abc$

And $(a * b) * c = (2ab) * c = 2(2ab)(c) = 4abc$.

$\therefore$ $*$ is associative.

G 2 : Let $a * e = a$ $\therefore$ $2ae = a$ $\therefore$ $e = \frac{1}{2}$

Now, $a * \frac{1}{2} = 2a * \frac{1}{2} = a$, $\frac{1}{2} * a = 2 * \frac{1}{2}a = a$.

$\therefore$ $\frac{1}{2}$ is identity element.

G 3 : Let $a * b = e = \frac{1}{2}$ $\therefore$ $2ab = \frac{1}{2}$ $\therefore$ $b = \frac{1}{4a}$

Hence, $\frac{1}{4a}$ is the inverse of a *i.e.* $a^{-1} = \frac{1}{4a}$.

$\therefore$ For every $a \in R$, inverse exists.

Further, $a * b = 2ab$ and $b * a = 2ab$.

$\therefore$ $a * b = b * a$. $\therefore$ $(R, *)$ is an Abelian group.

Example 10 : Let G be the set of all non-zero real numbers and let $a * b = \frac{ab}{2}$. Show that $(G, *)$ is an Abelian group. **(M.U. 2003, 09, 14)**

Sol. : Since $a * b = \frac{ab}{2}$ and $\frac{ab}{2} \in R$, If $a, b \in R$, $*$ is a binary operation in R.

G 1 : $a * (b * c) = a * \frac{bc}{2} = \frac{a(bc)}{4} = \frac{abc}{4}$ and $(a * b) * c = \frac{ab}{2} * c = \frac{(ab)c}{4} = \frac{abc}{4}$.

$\therefore$ $*$ is associative.

G 2 : Let $a * e = a$ $\therefore$ $\frac{ae}{2} = a$ $\therefore$ $ae = 2a$ $\therefore$ $e = 2$

Now, $a * 2 = \frac{a2}{2} = a$

$\therefore$ 2 is identity element.

G 3 : Let $a * b = e = 2$ $\therefore$ $\frac{ab}{2} = 2$ $\therefore$ $ab = 4$ $\therefore$ $b = \frac{4}{a}$

$\therefore$ $\frac{4}{a}$ is the inverse of a *i.e.*, $a^{-1} = \frac{4}{a}$.

Further $a * b = \frac{ab}{2}$ and $b * a = \frac{ba}{2}$,

$\therefore$ $a * b = b * a$ $\therefore$ $(R, *)$ is an Abelian group.

Example 11 : Determine whether the set A of all ordered pairs (a, b) of real numbers $(a \neq 0)$ under $*$ defined by $(a, b) * (c, d) = (ac, bc + d)$ is an Abelian group. **(M.U. 2003)**

Sol. : If a, b, c, d are real number, we have

$(a, b) * (c, d) = (ac, bc + d)$ and $ac \in R, bc + d \in R$.

$\therefore$ $*$ is a binary operation.

G 1 : Consider

$$[(a, b) * (c, d)] * (e, f) = (ac, bc + d) * (e, f)$$
$$= (ace, bce + de + f)$$
$$(a, b) * [(c, d) * (e, f)] = (a, b) * [(ce, de + f)]$$
$$= (ace, bce + de + f)$$

$\therefore$ $[(a, b) * (c, d)] * (e, f) = (a * b) * [(c, d) * (e, f)]$

$\therefore$ $*$ is associative.

G 2 : Let $(a, b) * (x, y) = (a, b)$ so that (x, y) is identity element.

$\therefore$ $(ax, bx + y) = (a, b)$

This equality will hold if $x = 1$ and $y = 0$.

$\therefore$ $(1, 0)$ is identity element.

G 3 : Let $(a, b) * (x, y) = (1, 0)$

$\therefore$ $(ax, bx + y) = (1, 0)$ $\therefore$ $ax = 1,\ bx + y = 0$

$\therefore$ $x = \frac{1}{a},\ y = -bx = -\frac{b}{a}$ $\therefore$ $(a, b)^{-1} = (x, y) = \left(\frac{1}{a}, -\frac{b}{a}\right)$.

It can be verified that

$$(a, b)\left(\frac{1}{a}, -\frac{b}{a}\right) = \left(1, \frac{b}{a} - \frac{b}{a}\right) = (1, 0)$$

Further, $(a, b) * (c, d) = (ac, bc + d)$ and $(c, d) * (a, b) = (ca, da + b)$

$\therefore$ $(a, b) * (c, d) \neq (c, d) * (a, b)$

$\therefore$ $(R, *)$ is a group but **not** a Abelian group.

Example 12 : Let M be the set of all 2×2 non-singular matrices. Prove that M is a non-commutative group under usual multiplication of matrices. Is M a group under addition of matrices ? Is M a group under matrix multiplication if the condition of non-singularity is removed ? **(M.U. 2007)**

Sol. : If $A, B \in M$ then clearly AB is defined and is a 2×2 matrices. Further, $(AB)^{-1} = B^{-1} A^{-1}$. Since the inverse of AB exists, AB is non-singular.

$\therefore$ Multiplication is a binary operation on M.

G 1 : The matrix multiplication is associative.

G 2 : The identity matrix is $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. It is non-singular.

Also $I \in M$, $AI = A = IA$ for all $A \in M$.

G 3 : By definition of a non-singular matrix, for $A \in M$ there exist A^{-1} $(\in M)$ the inverse of A is such that

$AA^{-1} = A^{-1}A = I$. $\therefore$ M is a group under multiplication.

Now, to demonstrate that it is a non-abelian group, let

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

Since $|A| = |B| = -1$, both A, B are non-singular.

But $AB = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and $BA = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$\therefore$ $AB \neq BA$. $\therefore$ G is **not** Abelian.

For the last part, let $A \in M$ be any matrix. Then $|A| \neq 0$. Also $|-A| = -|A| \neq 0$.

$\therefore$ $(-A)$ is also a non-singular matrix. But $(A) + (-A) = 0$. Hence, the determinant of the sum is zero. The sum is not non-singular and does **not** belong to M *i.e.* M is not closed under addition.

$\therefore$ M is not a group under addition (where M is the set of **non-singular** matrices.)

If M is any matrix then $(M, \times)$ is not a group because inverse does not exist always.

Example 13 : Prove that the set of matrices $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$ where α is real, forms a group under usual matrix production. Is the group Abelian ? **(M.U. 1997, 98, 2004, 05)**

Sol. : Let $A_\alpha, A_\beta \in G$.

$$\therefore\ A_\alpha * A_\beta = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$$
$$= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} = A_{\alpha+\beta} \in G$$

$\therefore$ $*$ is a binary operation.

G 1 : We know that matrix multiplication is associative.

G 2 : The unit matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix}$ is identity element.

G 3 : Since $|A_\alpha| = \cos^2\alpha + \sin^2\alpha = 1$, A_α is non-singular, inverse exists.

$$A^{-1} = \frac{1}{|A_\alpha|}\text{adj. } A = \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} = \begin{bmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{bmatrix} = A_{(-\alpha)} \in G$$

Further, matrix multiplication is commutative.

$\therefore$ $(A_\alpha, \cdot)$ is an Abelian group.

Example 14 : Let $(G, \cdot)$ be a group. Prove that G is an Abelian group if and only if $(a \cdot b)^2 = a^2 \cdot b^2$ where a^2 stands for $a \cdot a$. (M.U. 1999, 2002, 08, 14, 16)

Sol. : **(i)** Let $(G, \cdot)$ be an Abelian group.

Hence, $a \cdot b = b \cdot a$.

Now, consider ..... (1)

$$\begin{aligned} (a \cdot b)^2 &= (a \cdot b) \cdot (a \cdot b) \\ &= (a \cdot b) \cdot (b \cdot a) \\ &= a \cdot (b \cdot b) \cdot a \qquad [\text{By (1)}] \\ &= a \cdot b^2 \cdot a = a \cdot a \cdot b^2 \qquad [\text{By (1)}] \\ &= a^2 \cdot b^2. \end{aligned}$$

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

Pre-multiplying by a^{-1} and post-multiplying by b^{-1}.

$$a^{-1} \cdot (a \cdot b)^2 \cdot b^{-1} = a^{-1} \cdot (a^2 \cdot b^2) \cdot b^{-1}$$

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

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

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

$\therefore$ $b \cdot a = a \cdot b$. $\therefore$ G is an Abelian group.

Example 15 : If $(G, \cdot)$ is an Abelian group, then prove that $(a \cdot b)^n = a^n \cdot b^n$ where $a, b \in G$. (M.U. 2001, 13, 15)

Sol. : We shall prove the result by the method of mathematical induction.

Step 1 : By data $(a \cdot b)^1 = a^1 \cdot b^1$ $\therefore$ $a \cdot b = a \cdot b$.

$\therefore$ The result is true for $n = 1$.

Step 2 : Let the result be true for $n = k$.

$\therefore$ $(a \cdot b)^k = a^k \cdot b^k$.

Now, multiply both sides by $a \cdot b$.

$\therefore$ $(a \cdot b)^k \cdot (a \cdot b) = a^k \cdot b^k \cdot a \cdot b$

$\therefore$ $(a \cdot b)^{k+1} = a^k \cdot a \cdot b^k \cdot b$ [$\because$ $G, \cdot$ is an Abelian group]

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

Hence, the result is true for $n = k + 1$.

Step 3 : Since it is true for $n = 1$, by step 2, it is true for $n = 2$ and since it is true for $n = 2$ again by step 3, it is true for $n = 3$ and so on.

It is true for all n.

Example 16 : Prove that a set of 2×2 rook matrices form a group under matrix multiplication. Is the group abelian ?

Sol. : A rook matrix is a square matrix which has only two elements, 0 and 1 such that each row or each column has exactly one 1.

Obviously there will be only two 2×2 rook matrices given below.

$$M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

There will be four products of the above matrices.

$$M_1 \cdot M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = M_1$$

$$M_1 \cdot M_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = M_2$$

$$M_2 \cdot M_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = M_2$$

$$M_2 \cdot M_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = M_1$$

Thus, we have the following multiplication table.

$\cdot$	M_1	M_2
M_1	M_1	M_2
M_2	M_2	M_1

The table show that M_1 is the identity element.

G 1 : Since there are only two elements, $\cdot$ is trivially associative.

G 2 : M_1 is the identity element.

G 3 : Since $M_1 \cdot M_1 = M_1$ (Identity), M_1 is the inverse of M_1.

Since $M_2 \cdot M_2 = M_1$ (Identity), M_2 is the inverse of M_2.

Further, since $M_2 \cdot M_1 = M_1 \cdot M_2$. $\therefore$ $(M, \cdot)$ is an Abelian Group.

Example 17 : Prove that a set of bijective functions from A to A where $A = (1, 2)$ is a group under composition of functions. Is it Abelian ?

Sol. : Let $A = (1, 2)$ then we have the following two bijective functions on A.

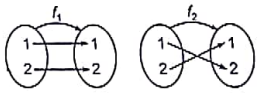


Fig. 10.5

We can obtain four compositions from f_1 and f_2 viz. $f_1 \circ f_1$, $f_1 \circ f_2$, $f_2 \circ f_1$, $f_2 \circ f_2$. Now, prove the remaining part as above.

Example 18 : Prove that z_4 where z_4 denotes the set of integers z modulo 4 is a group under addition but is not a group under multiplication.

Sol. : We first prepare the addition and multiplication tables.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(1) For $(z_4, \oplus)$ se seo that

(i) $\oplus$ is associative.

For example, $(1 \oplus 2) \oplus (3) = 3 \oplus 3 = 2$

and $1 \oplus (2 \oplus 3) = 1 \oplus 1 = 2$

(ii) 0 is the identity element.

This, can be seen to be true from the first row or the first column.

$0 + 0 = 0, \quad 1 + 0 = 1, \quad 2 + 0 = 2, \quad 3 + 0 = 3.$

(iii) Additive inverse exists for each element

$0^{-1} = 0, \quad 1^{-1} = 3, \quad 2^{-1} = 2, \quad 3^{-1} = 1$

Hence, $(z_4, \oplus)$ is a group.

(2) For $(z_4, \otimes)$, we see that multiplicative inverse does not exist.

For example, $2 \times 0 = 0, \quad 2 \times 1 = 2, \quad 2 \times 2 = 0, \quad 2 \times 3 = 2$

The product of 2 with no element of z_4 is unity.

Hence, 2^{-1} does not exist. $\therefore$ $(z_4, \otimes)$ is not a group.

In general, if z_m denotes the set of integers modulo m, then z_m is a group under addition but it is not a group under multiplication.

However, if U_m denotes a reduced residue system modulo m which consists of those integers which are relatively prime to m (*i.e.* which are not factors or multiples of factors of m), then U_m is a group under multiplication. See the next example.

Example 19 : Show that $U_{12} = \{1, 5, 7, 11\}$ which denotes the reduced residue system modulo 12 is a group under multiplication.

Sol. : We first prepare the multiplication table.

$\otimes$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

(1) $(u_{12}, \otimes)$ is associative.

For example, $5 \times (7 \times 11) = 5 \times (5) = 1$

and $(5 \times 7) \times 11 = (11) \times 11 = 1$

(2) 1 is the identity element.

This is clear from the first row or from the first column.

(3) Every element has the inverse and the element itself is its inverse.

This is so because all diagonal elements are unity.

$\because \quad 5 \otimes 5 = 1, \quad 5^{-1} = 5$

$\because \quad 7 \otimes 7 = 1, \quad 7^{-1} = 7$

Similarly, $1^{-1} = 1, \quad 11^{-1} = 11.$

Hence, $(u_{12}, \otimes)$ is a group.

Example 20 : Let $S = \{ x \mid x \text{ is real and } x \neq 0, x \neq -1 \}$.

Consider the following functions $f_i : S \to S, \ i = 1, 2, \ldots\ldots, 6$

$$f_1(x) = x, \ f_2(x) = \frac{1}{x}, \ f_3(x) = 1 - x, \ f_4(x) = \frac{x}{1-x}, \ f_5(x) = \frac{1}{1-x}, \ f_6 = \frac{x-1}{x}.$$

Show that $G = \{ f_1, f_2, f_3, \ldots\ldots, f_6 \}$ is a group under the operation of composition. Give the multiplication table for G. **(M.U. 2003, 05, 15)**

Sol. : We shall first obtain $f_i \circ f_j$ for all i and j.

$$f_1 \circ f_1 = f_1 \circ (x) = x = f_1 \qquad f_1 \circ f_2 = f_1 \circ \left(\frac{1}{x}\right) = \left(\frac{1}{x}\right) = f_2$$

$$f_1 \circ f_3 = f_1 \circ (1 - x) = 1 - x = f_3 \qquad f_1 \circ f_4 = f_1 \circ \left(\frac{x}{1-x}\right) = \frac{x}{1-x} = f_4$$

$$f_1 \circ f_5 = f_1 \circ \left(\frac{1}{1-x}\right) = \frac{1}{1-x} = f_5 \qquad f_1 \circ f_6 = f_1 \circ \left(\frac{x-1}{x}\right) = \frac{x-1}{x} = f_6$$

Further, $f_2 \circ f_1 = f_2 \circ (x) = \frac{1}{x} = f_2$

$$f_2 \circ f_2 = f_2 \circ \left(\frac{1}{x}\right) = \frac{1}{1/x} = x = f_1, \qquad f_2 \circ f_3 = f_2 \circ (1 - x) = \frac{1}{1-x} = f_5$$

$$f_2 \circ f_4 = f_2 \circ \left(\frac{x}{x-1}\right) = \frac{x-1}{x} = f_6$$

$$f_2 \circ f_5 = f_2 \circ \left(\frac{1}{1-x}\right) = \frac{1}{1/(1-x)} = 1 - x = f_3$$

$$f_2 \circ f_6 = f_2 \circ \left(\frac{x-1}{x}\right) = \frac{1}{(x-1)/x} = \frac{x}{x-1} = f_4$$

Further since $f_3 = 1 - x$,

$$f_3 \circ f_1 = f_3 \circ (x) = 1 - x = f_3$$

$$f_3 \circ f_2 = f_2 \circ \left(\frac{1}{x}\right) = 1 - \frac{1}{x} = \frac{x-1}{x} = f_6$$

$$f_3 \circ f_3 = f_3 \circ (1 - x) = 1 - (1 - x) = x = f_1$$

$$f_3 \circ f_4 = f_3 \circ \left(\frac{x}{x-1}\right) = 1 - \frac{x}{x-1} = \frac{-1}{x-1} = \frac{1}{1-x} = f_5$$

$$f_3 \circ f_5 = f_3 \circ \left(\frac{1}{1-x}\right) = 1 - \frac{1}{1-x} = \frac{-x}{1-x} = \frac{x}{x-1} = f_4$$

$$f_3 \circ f_6 = f_3 \circ \left(\frac{x-1}{x}\right) = 1 - \frac{x-1}{x} = \frac{1}{x} = f_2$$

Also since $f_4 = \frac{x}{x-1}$,

$$f_4 \circ f_1 = f_4 \circ (x) = \frac{x}{x-1} = f_4$$

$$f_4 \circ f_2 = f_4 \circ \left(\frac{1}{x}\right) = \frac{1/x}{(1/x) - 1} = \frac{1}{1-x} = f_5$$

$$f_4 \circ f_3 = f_4 \circ (1-x) = \frac{1-x}{(1-x)-1} = \frac{1-x}{-x} = \frac{x-1}{x} = f_6$$

$$f_4 \circ f_4 = f_4 \circ \left(\frac{x}{x-1}\right) = \frac{x/(x-1)}{x/(x-1)-1} = x = f_1$$

$$f_4 \circ f_5 = f_4 \circ \left(\frac{1}{1-x}\right) = \frac{1/(1-x)}{1/(1-x)-1} = \frac{1}{x} = f_2$$

$$f_4 \circ f_6 = f_4 \circ \left(\frac{x-1}{x}\right) = \frac{(x-1)/x}{(x-1)/x-1} = \frac{x-1}{-1} = 1-x = f_3$$

To find $f_5 \circ f_1$ ..... $f_5 \circ f_6$ and $f_6 \circ f_1$ ..... $f_6 \circ f_6$ is left to you.

Now we shall see the following.

G_1 : Associativity

$$f_2 \circ f_3 = f_2 \circ (1-x) = \frac{1}{1-x}, \qquad f_1 \circ (f_2 \circ f_3) = f_1 \circ \left(\frac{1}{1-x}\right) = \frac{1}{1-x}$$

Also, $f_1 \circ f_2 = f_2 \circ \frac{1}{x} = \frac{1}{x}$ $\quad \therefore \ (f_1 \circ f_2) \circ f_3 = (f_1 \circ f_2) \circ (1-x) = \frac{1}{1-x}$

Hence, $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$ $\quad \therefore$ $\circ$ is associative in G.

G_2 : Identity

From the above calculations, we find that f_1 is the identity.

G_3 : Inverse

From the above calculations, we see that every element has an inverse.

For instance inverse of f_1 is f_1, inverse of f_2 is f_2, inverse of f_3 is f_3 and so on. Hence, G is a group under composing.

You can prepare the multiplication table.

Example 21 : Write down all permutations taken 3 at a time of the elements of the set {1, 2, 3}.

Show that this set of permutations of the elements of {1, 2, 3} forms a group under the composition of permutations. **(M.U. 1997, 99, 2000)**

Sol. : The permutations of the elements of the set {1, 2, 3} are

(i) (1, 2, 3); (ii) (1, 3, 2); (iii) (2, 1, 3);

(iv) (2, 3, 1); (v) (3, 1, 2), (vi) (3, 2, 1).

With $A = \{1, 2, 3\}$ we define the six (functions) permutations as follows.

$P_1(A) = 1, 2, 3;$ $P_2(A) = 1, 3, 2;$ $P_3(A) = 2, 1, 3;$

$P_4(A) = 2, 3, 1;$ $P_5(A) = 3, 1, 2;$ $P_6(A) = 3, 2, 1.$

$P_1(A)$ means keeping the same order

e.g., if $A = \{3, 2, 1\}$ then $P_1(A) = 3, 2, 1.$

$P_6(A)$ means interchanging the first and the last elements

e.g., if $A = \{3, 2, 1\}$ as above, then $P_6(A) = \{1, 2, 3\}$.

Let us denote the set of six permutations (functions) by P.

$\therefore \quad P = \{ P_1(A), P_2(A), ..., P_6(A) \}$

With $A = \{1, 2, 3\}$ and P_i defined as above we consider the following.

G_1 : Associativity

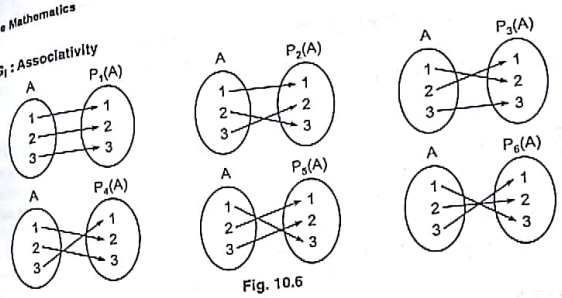


Fig. 10.6

We have, if $A = \{1, 2, 3\}$, then

$P_1(A) = \{1, 2, 3\}$, $P_2(A) = \{1, 3, 2\}$, $P_3(A) = \{2, 1, 3\}$

$P_1(A) \circ P_2(A) = \{1, 3, 2\}$ [$\because$ P_1 maintains the order]

Thus, if $A = \{1, 2, 3\}$, $P_1(A) \cdot P_2(A) = \{1, 3, 2\}$.

$P_1 \circ P_2$ interchanges the last two.

But $P_3(A) = 2, 1, 3.$

$\therefore \ (P_1 \circ P_2) \circ P_3 = 2, 3, 1$

Now, $P_2(A) \circ P_3(A) = 2, 3, 1$ [$\because$ P_2 interchange the last two]

$\therefore \ P_1 \circ (P_2 \circ P_3) = 2, 3, 1$ [$\because$ P_1 maintains the order]

$\therefore \ (P_1 \circ P_2) \circ P_3 = P_1 \circ (P_2 \circ P_3)$

$\therefore$ $\circ$ is associative.

G_2 : Identity

Since, if $A = \{1, 2, 3\}$, $P_1(A) = \{1, 2, 3\}$, we see that P_1 maintains the order

$\therefore \ P_1 \circ P_2 = P_2, \ P_1 \circ P_3 = P_3, \ ....., \ P_1 \circ P_k = P_k.$

G_3 : Inverse

We see that $P_1 \circ P_1 = P_1$

$P_2 \circ P_2 = P_2 \circ (1, 3, 2) = (1, 2, 3)$

$= P_1$ [$\because$ P_2 interchanges the last two elements]

$P_3 \circ P_3 = P_3 \circ (2, 1, 3) = (1, 2, 3)$ [$\because$ P_3 interchanges the first two elements]

and so on.

Each function is the inverse of itself. $\therefore$ $(G, \circ)$ is a group.

Example 22 : Let Q be the set of all positive rational numbers which can be expressed as $2^a 3^b$ where a, b are integers.

Prove that $(Q, *)$ is a group where $*$ is usual multiplication. **(M.U. 2002, 06, 12)**

Sol. : We have $2^{a_1} 3^{b_1} * 2^{a_2} 3^{b_2} = 2^{a_1+a_2} 3^{b_1+b_2} = 2^a 3^b$

$\therefore$ G is closed under $*$.

G_1 : Associativity

Consider $(2^{a_1}3^{b_1})*(2^{a_2}3^{b_2}*2^{a_3}3^{b_3}) = (2^{a_1}3^{b_1})*(2^{a_2+a_3}3^{b_2+b_3})$

$= 2^{a_1+a_2+a_3}3^{b_1+b_2+b_3} = 2^a 3^b$

Again $(2^{a_1}3^{b_1}*2^{a_2}3^{b_2})*2^{a_3}3^{b_3} = (2^{a_1+a_2}3^{b_1+b_2})*2^{a_3}3^{b_3}$

$= 2^{a_1+a_2+a_3}3^{b_1+b_2+b_3} = 2^a 3^b$

$\therefore$ $(G, *)$ is associative.

G_2 : Identity

If $a = 0, b = 0$, $2^0 3^0 = 1$

$\therefore$ $(2^a 3^b)*(2^0 3^0) = 2^a 3^b \cdot 1 = 2^a 3^b$ $\therefore$ $2^0 3^0$ is an identity.

G_3 : Inverse

Consider $(2^a 3^b)\times(2^{-a}3^{-b}) = 2^{a-a}3^{b-b} = 2^0 3^0 = 1$

$\therefore$ $2^{-a}3^{-b}$ is the inverse of $2^a 3^b$. $\therefore$ $(Q, *)$ is a group.

Example 23 : If S is a non-empty set, prove that the $P(S)$ (power set of S) with $*$ where $A * B$ is defined as symmetric difference is an Abelian group. (M.U. 2006)

Sol. : Clearly, if $A, B \in S$, then $A * B$ also belongs to S.

$\therefore$ $P(S)$ is closed under $*$.

G_1 : Associativity

$(A * B) = \{x \mid x$ belongs to A or $B\}$

$(A * B) * C = \{x \mid x$ belongs to A or B or $C\}$

$(B * C) = \{x \mid x$ belongs to B or $C\}$

$A * (B * C) = \{x \mid x$ belongs to A or B or $C\}$

$\therefore$ $(A * B) * C = A * (B * C)$

$\therefore$ $*$ is associative.

G_2 : Identity

Φ is an identity element.

$A * \Phi = \{x \mid x$ belongs to A or $\Phi\}$

$= \{x \mid x$ belongs to $A\}$ [$\because$ Φ has no elements]

$\therefore$ $A * \Phi = A$ for each A.

G_3 : Inverse

Since $A * \overline{A} = \{x$ belong to A or $\overline{A}\}$

$= \Phi$ [$\because$ No element belongs to A and $\overline{A}$ simultaneously]

$\therefore$ $\overline{A}$ is the inverse of A.

G_4 : Commutativity

Clearly $A * B = B * A$

$\therefore$ $(G, *)$ is an Abelian group.

Example 24 : Let $(A, *)$ be a monoid such that for every $x \in A$, $x * x = e$ where e is the identity (*i.e.*, every element is its own inverse). Show that $(A, *)$ is an Abelian group. (M.U. 2000, 01)

OR If every element in a group is its own inverse then the group is Abelian. (M.U. 2013, 15)

Sol. : (i) Since $(A, *)$ is a monoid, $*$ is associative over A.

(ii) Since $(A, *)$ is a monoid, it has an identity element.

(iii) Since $x * x = e$ and e is the identity element, for every x, its inverse exists and every element is its inverse.

$\therefore$ $(A, *)$ is a group.

Since by data e is the identity $x * e = e * x = x$ ..... (1)

But by data $y * y = e$ ..... (2)

Let us denote $y * y = b$.

Then from (2), $b = e$ and then from (1), $x * b = b * x$ for all $x \in A$.

$\therefore$ $(A, *)$ is an Abelian group

(a) **Congruence Relation** (M.U. 2009)

Definition : If m is any positive integer and if a, b are any integers then a is said to be **congruent to b modulo m** if m divides $(a - b)$ (*i.e.* if $\left(\frac{a-b}{m}\right)$ has zero remainder).

We write this as $a \equiv b \pmod m$. If the remainder is not zero we write it as $a' \not\equiv b' \pmod m$. For example,

(i) $81 \equiv 21 \pmod 5$ $\because$ 5 divides $81 - 21 = 60$.

(ii) $58 \equiv 16 \pmod 7$ $\because$ 7 divides $58 - 16 = 42$.

(iii) $34 \not\equiv 12 \pmod 3$ $\because$ 3 does not divide $34 - 12 = 22$.

(iv) $25 \not\equiv 7 \pmod 4$ $\because$ 4 does not divides $25 - 7 = 18$.

Theorem : Congruence modulo m is an equivalence relation in Z.

Proof : Let m be a positive integer.

(i) If a is any integer $a - a = 0$, is divisible by m.

$\therefore$ $a \equiv a \pmod m$ (Reflexivity)

(ii) If $a \equiv b \pmod m$ *i.e.* if $(a - b)$ is divisible by m then $(b - a) = -(a - b)$ is also divisible by m.

$\therefore$ If $a \equiv b \pmod m$, then $b \equiv a \pmod m$ (Symmetry)

(iii) If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $(a - b)$ is divisible by m and $(b - c)$ is divisible by m.

$\therefore$ The sum $(a - b) + (b - c) = a - c$ is also divisible by m.

$\therefore$ If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$ (Transitivity)

$\therefore$ Congruence is an equivalence relation.

Remarks ....

(i) If a is congruent to an integer in the set $S = \{0, 1, 2, ..., (m-1)\}$ then that integer is **unique**. In other words a cannot be congruent to two integers of the set S.

(ii) If $a \equiv b \pmod m$ then a and b when divided by m leave the same remainder.

(iii) The set obtained from Z modulo m is denoted by Z_m, the operation of addition on Z_m is denoted by $+_m$ and operation of multiplication on Z_m is denoted by $\times_m$.

Example 1 : Find a set of three real numbers that is closed under addition modulo 2 and multiplication modulo 2. (M.U. 1998, 2001)

Sol. : Consider the set { −1, 0, 1 } and prepare the two tables addition modulo 2 and multiplication modulo 2.

$+_2$	−1	0	1
−1	0	−1	0
0	−1	0	1
1	0	1	0

$\times_2$	−1	0	1
−1	1	0	−1
0	0	0	0
1	−1	0	1

Example 2 : Prove that the set $A = \{0, 1, 2, 3, 4, 5\}$ is a finite Abelian group under addition modulo 6. **(M.U. 2004, 05, 07, 09, 13, 16)**

Sol. : We first prepare the table of addition modulo 6 denoted by $\oplus$.

From the table, it is obvious that $\oplus$ is a binary operation.

***G* 1 :** From the table we see that $\oplus$ is associative.

e.g., $2 \oplus (3 \oplus 5) = 2 \oplus (2) = 4$ and $(2 \oplus 3) \oplus 5 = (5) \oplus 5 = 4$.

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	6 = 0
2	2	3	4	5	6 = 0	7 = 1
3	3	4	5	6 = 0	7 = 1	8 = 2
4	4	5	6 = 0	7 = 1	8 = 2	9 = 3
5	5	6 = 0	7 = 1	8 = 2	9 = 3	10 = 4

***G* 2 :** The first column or the first row shows that 0 is the identity for $\oplus$.

***G* 3 :** The positions of 0 the additive inverse in every row (and every column) show that every element of A has the additive inverse. *e.g.,* $1 \oplus 5 = 0$.

Hence, inverse of 1 is 5 and inverse of 5 is 1.

Also $\because\ 3 \oplus 3 = 0 \quad \therefore\ (3)^{-1} = 3$

Further, $2 \oplus 4 = 0 \quad \therefore\ (2)^{-1} = 4$ etc.

$\therefore$ *G* is a group under addition modulo 6.

***G* 4 :** Further $a \oplus b = b \oplus a$. *e.g.,* $4 \oplus 5 = 3$ and $5 \oplus 4 = 3$

$\therefore\ 4 \oplus 5 = 5 \oplus 4. \quad \therefore$ *G* is an Abelian group.

Example 3 : Prove that $A = \{ 1, 2, 3, 4, 5, 6 \}$ is a finite Abelian group under multiplication modulo 7. **(M.U. 2010, 11, 12, 14, 15, 17, 18)**

Sol. : We first prepare the table of multiplication modulo 7 denoted by $\otimes$. From the table it is clear that $\otimes$ is a binary operation.

$\otimes$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

***G* 1 :** From the table, we see that $\otimes$ is associative.

e.g. $2 \otimes (3 \otimes 5) = 2 \otimes 1 = 2$

and $(2 \otimes 3) \otimes 5 = 6 \otimes 5 = 2$

***G* 2 :** The first column (or the first row) show that 1 is the identify for $\otimes$.

***G* 3 :** The positions of the multiplicative identity 1 in every row (and every column) show that every element of A has the multiplicative inverse.

e.g. $2 \otimes 4 = 1$ and $4 \otimes 2 = 1$

$\therefore\ (2)^{-1} = 4$ and $(4)^{-1} 2$

$\therefore$ *G* is a group modulo 7.

***G* 4 :** Further, $a \otimes b = b \otimes a$

e.g. $4 \otimes 5 = 6$ and $5 \otimes 4 = 6$

$\therefore$ *G* is an Abelian Group.

Example 4 : Let Z_4 *i.e.*, $G = \{ 0, 1, 2, 3 \}$. (i) Prepare the composition table with respect to X_4. (ii) Is it a group ? **(M.U. 2008)**

Sol. : X_4 denotes the operation of multiplication modulo 4 and composition table means the table in which this operation is shown. (See the adjoining table.)

From the table, we see that *G* is closed under the operation X_4 as all elements in the adjoining table are elements of *G*.

X_4	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

***G* 1 :** From the table, we see that $\otimes$ is associative.

e.g., $2 \otimes (3 \otimes 1) = 2 \otimes (3) = 2 \otimes 3 = 2$

and $(2 \otimes 3) \otimes 1 = 2 \otimes (1) = 2 \otimes 2 = 2$

***G* 2 :** From the second row (or second column) we see that, 1 is the identity element.

$0 \otimes 1 = 0, \quad 1 \otimes 1 = 1, \quad 2 \otimes 1 = 3, \quad 3 \otimes 1 = 3$

***G* 3 :** In the row (or column) of 2, we see that, $2 \otimes 0 = 0, 2 \otimes 1 = 2, 2 \otimes 2 = 0, 2 \otimes 3 = 2$. Thus, we do not get an identity element and hence, 2 does **not** have a inverse.

$\therefore$ *G* under multiplication modulo 4 is not a group.

(b) Residue Classes

Since congruence is an equivalence relation, it partitions Z, the set of integers into disjoint equivalence classes called the **residue classes modulo** m. The residue class of a is the set of integers which are congruent to a modulo m. The residue class of a is denoted by $[a]$. Thus, $[a] = \{x \mid x \in Z \text{ and } x \equiv a\}$.

For example, if $m = 5$, we have

$[0] = \{ \ldots, -10, -5, 0, 5, 10, \ldots \}$

$[1] = \{ \ldots, -9, -4, 1, 6, 11, \ldots \}$

$[2] = \{ \ldots, -8, -3, 2, 7, 12, \ldots \}$

$[3] = \{ \ldots, -7, -2, 3, 8, 13, \ldots \}$

$[4] = \{ \ldots, -6, -1, 4, 9, 14, \ldots \}$

(c) Congruence Relation On Semi-group

Definition : An equivalence relation R on the semi-group $(S, *)$ is called a **congruence relation on the semi-group** if $a\ R\ a'$ and $b\ R\ b'$, then $(a * b)\ R\ (a' * b')$.

Example : Consider the semi-group $(Z, +)$ and the relation R defined by $a\ R\ b$ if and only if $a \equiv b \pmod 3$.

Prove that R is a congruence relation on the semi-group S.

Sol. : Considering the above definition we have to prove that if $a, a', b, b' \in S$ and if $a \; R \; b$ and $a' \; R \; b'$, then $(a * a') \; R \; (b * b')$ *i.e.* we have to prove that if $a \equiv a' \pmod 3$ and $b \equiv b' \pmod 3$ then $a + b \equiv a' + b' \pmod 3$. Now, since $a \equiv a' \pmod 3$, $(a - a') = 3m$ say and since $b \equiv b' \pmod 3$, $(b - b') = 3n$, say, where m and n are integers.

$\therefore \quad a - a' + b - b' = 3m + 3n$

$\therefore \quad (a + b) - (a' + b') = 3\,(m + n)$

$\therefore \quad (a + b) \equiv (a' + b') \pmod 3$

Hence, the result.

(d) Cyclic Group

Definition : A group $(G, *)$ is said to be a **cyclic group** if there exists an element $a \in G$ such that every element of G can be written as some power of a *viz.* a^k for some integer k where by a^k we mean $a \times a \times a \ldots\ldots a$ (k times). (M.U. 2000, 13)

Then G is said to be generated by a or a generates G.

A cyclic group is always Abelian because commutativity is observed,

$\because$ if $a^r, a^s \in G$, then $a^r \times a^s = a^s \times a^r$.

Example 1 : The cube roots of unity form a cyclic group under multiplication of complex numbers.

Sol. : In Example 2, page 10-13, we have proved that the cube roots of unity is a group under multiplication.

Now, we shall prove that it is cyclic *i.e.*, every element of the group $1, \omega, \omega^2$ can be expressed as integral power of some element $a \in G$.

We note that $\omega^0 = 1, \; \omega^1 = \omega, \; \omega^2 = \omega^2$.

Thus, the element $1, \omega, \omega^2$ are expressed as 0^{th}, 1^{st} and 2^{nd} power of ω. Hence, the group is cyclic with ω as a generator.

Also, $(\omega^2)^0 = 1, \; (\omega^2)^1 = \omega^2, \; (\omega^2)^2 = \omega^4 = \omega^3 \cdot \omega = \omega$.

Thus, $1, \omega, \omega^2$ are expressed as 0^{th}, 1^{st} and 2^{nd} power of ω^2.

Hence, the group is cyclic with ω^2 as a generator.

Example 2 : Prove that the group $G = \{0, 1, 2, 3, 4, 5\}$ is a finite, abelian, cyclic group under addition modulo 6.

Sol. : We have proved in Example 2, page 10-27 that G is an Abelian group.

Now, we shall prove that it is a cyclic group *i.e.*, every element of the group G can be expressed as integral power of some element $a \in G$.

We note that $1^1 = 1, \quad 1^2 = 1 +_6 1 = 2, \quad 1^3 = 1 + 1_6 \; 1^2 = 1 +_6 2 = 3,$

$1^4 = 1 +_6 1^3 = 1 +_6 3 = 4, \quad 1^5 = 1 +_6 1^4 = 1 +_6 4 = 5,$

$1^6 = 1 +_6 1^5 = 1 +_6 5 = 0.$ [See the table on page 10-27]

Hence, $G = \{1^6, 1^1, 1^2, 1^3, 1^4, 1^5\}$.

$\therefore$ G is a cyclic group with 1 as a generator.

(It can be shown that 5 is another generator.)

(e) Subgroup (M.U. 2002, 04, 05, 10)

Definition : Let H be a subset of group G, such that

(i) the identity element e of G belongs to H.

(ii) if a, b belong to H then $a * b$ also belongs to H.

(iii) if $a \in H$ then $a^{-1} \in H$. Then H is called a **subgroup** of G.

In short a subgroup is a subset of G having all the properties of a group.

Illustrations : (i) Let G be the group of all non-zero complex numbers $a + ib$ where a, b are real under multiplication.

Let $H = \{a + ib \mid a^2 + b^2 = 1\}$ then H is a subgroup of G.

(ii) Let G be the group of 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that $ad - bc \neq 0$ under matrix multiplication.

Let $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \; ad \neq 0 \right\}$, then H is a subgroup of G.

Example 1 : Consider the group Z of integers under addition.

Let $H = \{\ldots\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\ldots\}$ where m is a positive integer.

Show that H is a subgroup of Z.

Sol. : (i) The identity of element of G is 0 and 0 belongs to H.

(ii) If km and lm are any two elements of H, then

$(km + lm) = (k + l)\,m$ is also an element of H.

(iii) If km is an element of H, then its negative (inverse) km is also an element of H.

$\therefore$ H is a subgroup.

Example 2 : Find the subgroups of $(Z_5, \oplus)$ where $\oplus$ is the operation addition modulo 5. (M.U. 1998)

Sol. : The operation addition modulo 5 is given by the adjoining table.

Addition Modulo 5

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

From the first row and first column we see that 0 is the identity element.

$\because$ $1 \oplus 4 = 0$, inverse of 1 is 4.

$\because$ $4 \oplus 1 = 0$, inverse of 4 is 1.

Also $2 \oplus 3 = 0$, inverse of 2 is 3.

and $3 \oplus 2 = 0$, inverse of 3 is 2.

Hence, we consider two subgroups of $(Z_5, \oplus)$ viz. $G_1 = \{0, 1, 4\}$ and $G_2 = \{0, 2, 3\}$.

Now, by definition of subgroup H is a subgroup if

(i) the identity element e belongs to H.

(ii) If a, b belongs to H then $a \oplus b$ belongs to H.

(iii) if a belongs to H then a^{-1} belongs to H.

The above properties are satisfied by $\{0, 1, 4\}$ and $\{0, 2, 3\}$ under $\oplus$ and hence they are subgroups.

Example 3 : Consider the set $A = \{1, 2, 3, 4, 5, 6\}$ under the multiplication modulo 7.

(i) Construct the multiplication table.

(ii) Find the inverses of 2, 3, 5 and 6.

(iii) Prove that A is a cyclic group.

(iv) Find the subgroups generated by {3, 4} and {2, 3} and state their orders. **(M.U. 1999, 2000, 16)**

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Sol. : (i) The multiplication tables is given by the adjoining table.

From the first column and the first row we see that 1 is the identity element.

(ii) From the table we see that $2 * 4 = 1$ and $4 * 2 = 1$.

$\therefore$ Inverse of 2 is 4.

Also since $3 * 5 = 1$ and $5 * 3 = 1$ $\therefore$ Inverse of 3 is 5.

Since $5 * 3 = 1$ and $3 * 5 = 1$ $\therefore$ Inverse of 5 is 3.

Since $6 \times 6 = 1$, inverse of 6 is 6.

(iii) We observe that

$3^1 = 3$, $3^2 = 9_7 = 2$, $3^3 = 27_7 = 6$,

$3^4 = 81_7 = 4$, $3^5 = 243_7 = 5$, $3^6 = 729_7 = 1$.

Thus, each element of A can be written as 3^k.

Hence, $(H, *$ is a cyclic a group) and 3 is its generator.

(iv) The subgroup generated by {3, 4} is denoted by $\langle \{3, 4\} \rangle$.

Clearly the elements (3, 4) belong to the subgroup $\langle \{3, 4\} \rangle$.

The inverse of 3 is 5 and inverse of 4 is 2 and they belong to the subgroup $\langle \{3, 4\} \rangle$.

The identity element 1 belongs to the subgroup.

Thus, the elements 1, 2, 3, 4, 5 belong to the subgroup $\langle \{3, 4\} \rangle$.

Let us check whether the remaining element 6 also belongs to the subgroup.

Now, since $4 \in \langle \{3, 4\} \rangle$ and $5 \in \langle \{3, 4\} \rangle$

$4 * 5$ must belong to the subgroup.

But $4 * 5_7 = 6$. Hence, $6 \in \langle \{3, 4\} \rangle$

$\therefore$ The subgroup of {3, 4} is {1, 2, 3, 4, 5, 6} the set A. Its order *i.e.* the number of elements is 6.

Similarly, you can prove that the subgroup of {2, 3} is the set A itself.

Example 4 : Let G be a reduced system modulo 15 *i.e.*, $G = \{1, 2, 4, 7, 8, 11, 13, 14\}$ (*i.e.*, the set of integers between 1 and 15 which are relatively prime to 15 *i.e.* the integers which are not the factors of 15 or the multiples of the two factors 3, 5 from 1 to 15).

Then, G is a group under multiplication modulo 15.

(1) Construct the multiplication table.

(2) Find 2^{-1}, 7^{-1}, 11^{-1}.

(3) Is G cyclic ?

(4) Find the order and the sub-groups generated by 2, 7, 11.

Sol. : (a) To prepare the multiplication table we find the remainder when the product of any two elements ab is divided 15. We thus get the following table.

$\otimes$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

From the first row (or the column), we find that 1 is the identity element.

(b) Since 1 is the multiplicative identity b is the inverse of a if $a \otimes b = 1$.

From the table, we find that $2^{-1} = 8$, $7^{-1} = 13$, $11^{-1} = 11$.

(c) Since $2^2 = 4$, $2^3 = 8$, $2^4 = 1$, the sub-group generate by $2 = \{1, 2, 4, 8\}$.

The number of elements in this group *i.e.* the order of this group $|2| = 4$.

Since $7^2 = 7 * 7 = 4$, $7^3 = (7 * 7) * 7 = 4 * 7 = 13$, $7^4 = (7 * 7) * 7 = 13 * 7 = 1$, the sub-group generated by $7 = \{1, 4, 7, 13\}$. The number of elements in the sub-group *i.e.*, $|7| = 4$.

Since $11^2 = 1$, the sub-group generate by 11 is {1, 11} and $|11| = 2$.

(d) Since no element generates G, G is not cyclic.

Example 5 : Consider $G = \{1, 5, 7, 11, 13, 17\}$ a reduced system modulo 18 (*i.e.* the set of integers between 1 and 18 which are relatively prime to 18). Then G is a group under multiplication.

(i) Construct the multiplication table.

(ii) Find 5^{-1}, 7^{-1}, 17^{-1}

(iii) Find the order and the sub-groups generated by 5, 7, 17.

(iv) Is G cyclic ?

Sol. : (i) The multiplication table is as shown in adjoining table.

$\otimes$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

1 is the identity.

(ii) $5^{-1} = 11$, $7^{-1} = 13$, $17^{-1} = 17$.

(iii) Now $5^2 = 5 \otimes 5 = 7$,

$5^3 = 5 \otimes 5 \otimes 5 = 7 \otimes 5 = 17$,

$5^4 = 17 \otimes 5 = 13$,

$5^5 = 13 \otimes 5 = 11$,

$5^6 = 11 \otimes 5 = 1$

$\therefore$ Sub-group of $5 = \{1, 5, 7, 11, 13, 17\} = G$ and $|5| = 6$.

i.e., the number of elements in sub-group of 5 is 6. Hence, the order is 6.

Since $7^2 = 7 \otimes 7 = 13$, $7^3 = 13 \otimes 7 = 1$.

Sub-group of $7 = \{1, 7, 13\}$ and $|7| = 3$

Since $17^2 = 17 \otimes 17 = 1$, sub-group of $17 = \{1\}$ and $|17| = 1$.

(iv) The group G is cyclic. Sub-group of $5 = G$.

(f) Coset

Definition : Let $(G, *)$ be group and H be a subgroup of G. If a, b are two elements of G and if $a * b^{-1} \in H$, then we say that "a is congruent to b modulo H". It is written as "$a \equiv b \bmod H$". (M.U. 2001)

It can be easily verified that this congruence relation is an equivalence relation (See Ex. 1 below). Since this congruence relation is an equivalence relation on G it partitions G into equivalent classes called cosets.

Definition : Let $(G, *)$ be group and H be a subgroup of G.

If a is an element of G then the set $Ha = \{ h * a \mid h \in H \}$ is called the right coset of H.

If a is an element of G, then the set $aH = \{ a * h \mid h \in H \}$ is called the left coset of H.

a is called the representative element of the coset aH or Ha.

(g) Normal Subgroup

Definition : A subgroup H of G is said to be normal if for every $a \in G$ we have $aH = H$. (M.U. 2002, 05, 07, 10, 13)

A subgroup of an Abelian group is normal.

Example 1 : Prove that "congruence modulo H" is an equivalence relation.

Sol. : By definition of "Congruence modulo H" $a\ R\ b$ means $a * b^{-1} \in H$.

(i) R is reflexive

$\because\ a * a^{-1} = e$ and $e \in H \quad \therefore\ R$ is reflexive.

(ii) R is symmetric

$\because\ a\ R\ b \quad \therefore\ a * b^{-1} = \in H$

Since, $(a * b^{-1}) \in H$, $(a * b^{-1})^{-1} \in H$

$\therefore\ b * a^{-1} \in H \quad \therefore\ R$ is symmetric.

(iii) R is transitive

If $a\ R\ b$ then $a * b^{-1} \in H$

If $b\ R\ c$ then $b * c^{-1} \in H$

$\therefore\ (a * b^{-1}) * (b * c^{-1}) \in H$

$\therefore\ a * (b^{-1} * b) * c^{-1} \in H$

$\therefore\ a * e \times c^{-1} \in H$

$\therefore\ a * c^{-1} \in H \quad \therefore\ a\ R\ c\ \therefore\ R$ is transitive.

Hence, R is an equivalence relation.

Example 2 : Find all cosets of the sub-group $H = 3 \cdot Z$ of the group $(Z, +)$.

Sol. : We have $Z = \{ \ldots, -4, -3, -2, -1, 0, 1, 2, 3, \ldots \}$

and $H = 3 \cdot Z = \{-7, -6, -3, 0, 3, 6, \ldots \}$

Now, $H + 0 = \{ \ldots, -6, -3, 0, 3, 6, \ldots \} = H$

$H + 1 = \{ \ldots, -5, -2, 1, 4, 7, \ldots \} = H_1$

$H + 2 = \{ \ldots, -4, -1, 2, 5, 8, \ldots \} = H_2$

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

But $H + 3 = H + 0$.

Hence, H, $H + 1$, $H + 2$ are the only three distinct right cosets of H in Z.

Further all these cosets partition the set Z into three disjoint subsets such that

$H \cup H_1 \cup H_2 = Z$

Further, since G is abelian, H is abelian and $ah = ha$. Hence, every right coset is equal to the left coset.

$\therefore\ H + 1 = 1 + H, \qquad H + 2 = 2 + H.$

Example 3 : Find all the cosets of the sub-group $H = 2 \cdot Z$ of the sub-group $(Z, +)$ in Z.

Sol. : Left to you.

Example 4 : Let $G = Z_6$. Find the left and right cosets of $H = \{[0], [3]\}$.

Is H a normal subgroup of the group Z_6.

Sol. : The group Z_6 is abelian because $a + b = b + a$ for $a, b \in Z_6$

e.g., $1 + 2 = 3$ and $2 + 1 = 3$.

Now, left coset of $H = \{[0], [3]\}$ with respect to a in the set Z_6 is

$aH = \{ a * b \mid h \in H \}$

$\therefore\ 0H = \{0 + 0, 0 + 3\} = \{0, 3\},$

$1H = \{1 + 0, 1 + 3\} = \{1, 4\},$

$2H = \{2 + 0, 2 + 3\} = \{2, 5\},$

$3H = \{3 + 0, 3 + 3\} = \{3, 0\},$

$4H = \{4 + 0, 4 + 3\} = \{4, 1\},$

$5H = \{5 + 0, 5 + 3\} = \{5, 2\}.$

The table of Z_6 (Here + stands for $+_6$)

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Now, the right coset of $H = \{[0]_6, [3]_6\}$ with respect to a in the set is

$Ha = \{ h * a \mid h \in H \}$

$\therefore\ H0 = \{0 + 0, 3 + 0\} = \{0, 3\}, \qquad H1 = \{0 + 1, 3 + 1\} = \{1, 4\},$

$H2 = \{0 + 2, 3 + 2\} = \{2, 5\}, \qquad H3 = \{0 + 3, 3 + 3\} = \{3, 0\},$

$H4 = \{0 + 4, 3 + 4\} = \{4, 1\}, \qquad H5 = \{0 + 5, 3 + 5\} = \{5, 2\}.$

Clearly, we have

$0H = H0,\ 1H = H1,\ 2H = H2,\ 3H = H3,\ 4H = H4,\ 5H = H5.$

$\therefore\ H$ is a normal subgroup of Z_6.

Example 5 : Let $G = Z_8$. Determine the left cosets of $H = \{[0], [4]\}$ in G. (M.U. 2005)

Sol. : The table of Z_8 (Here + stands for $+_8$)

$+_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Now, left coset of $H = \{[0], [4]\}$ with respect to a in the Z_8 is

$aH = \{ a * h \mid h \in H \}$

$\therefore$ $0H = \{0 + 0, 0 + 4\} = \{0, 4\}$, $1H = \{1 + 0, 1 + 4\} = \{1, 5\}$,
$2H = \{2 + 0, 2 + 4\} = \{2, 6\}$, $3H = \{3 + 0, 3 + 4\} = \{3, 7\}$,
$4H = \{4 + 0, 4 + 4\} = \{4, 0\}$, $5H = \{5 + 0, 5 + 4\} = \{5, 1\}$
$6H = \{6 + 0, 6 + 4\} = \{6, 2\}$, $7H = \{7 + 0, 7 + 4\} = \{7, 3\}$.

Example 6 : Let $G = Z_8$. Determine all right cosets of $H = \{[0], [4]\}$ in G.

Sol. : Left to you.

(h) Product Group

Definition : If G_1 and G_2 are groups and $G = G_1 \times G_2$ then G is called a product group under the operation defined by

$$(a_1, b_1) * (a_2, b_2) = (a_1 * a_2, b_1 * b_2)$$

Example : Let $G_1 = G_2 = Z_2$. If $\bar{0}$ denotes the equivalence class [0], and $\bar{1}$ denotes the equivalence class [1], then the multiplication table for the product group $G_1 \times G_2$ is given by

	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

(i) Quotient

(M.U. 2000)

We know that an equivalence relation R defined on a set A induces a partition of A denoted by A / R. In the same way the equivalence relation R, mod m induces a partition of the set S of the semi-group $(S, *)$ which we denote by S / R. S / R is called **quotient.**

Example : If A is the set of natural numbers and R is the relation defined by $a \, R \, b$ if $a \equiv b \pmod 5$, then prove that $(A / R, \oplus)$ is a group where A / R denotes the quotient group induced on A by R and $\oplus$ the addition on residue classes *i.e.* $[a] \oplus [b] = [a + b]$.

Sol. : The partition induced on A by the relation $a \equiv b \pmod 5$ is given by

$[0] = \{ \ldots, -10, -5, 0, 5, 10, \ldots \} = [5] = [10] = \ldots$
$[1] = \{ \ldots, -9, -4, 1, 6, 11, \ldots \} = [1] = [6] = \ldots$
$[2] = \{ \ldots, -8, -3, 2, 7, 12, \ldots \} = [2] = [7] = \ldots$
$[3] = \{ \ldots, -7, -2, 3, 8, 13, \ldots \} = [3] = [8] = \ldots$
$[4] = \{ \ldots, -6, -1, 4, 9, 14, \ldots \} = [4] = [9] = \ldots$

Thus, we have $A / R = \{ [0], [1], [2], [3], [4] \}$ and $[a] \oplus [b] = [a + b]$

e.g., $[2] \oplus [3] = [2 + 3] = [5]$

With this understanding we can prepare the following table for $\oplus$ on A / R.

$\oplus$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

From this table it is clear that $\oplus$ is a binary operation.

G1 : Associativity

$[a] \oplus ([b] \oplus [c]) = [a] \oplus [b + c]$
$= [a + (b + c)] = (a + b + c)$ [By associativity in A]

Similarly, $([a] \oplus [b]) \oplus [c] = a + b + c$.

This proves associativity.

G2 : From the first row (column) we see that [0] is the identity for $\oplus$.

G3 : Since in each row and column we find the identity element, every element has its inverse.

$[0]^{-1} = [0]$, $[1]^{-1} = [4]$, $[2]^{-1} = [3]$

because $[0] \oplus [0] = [0]$, $[1] \oplus [4] = [0]$, $[2] \oplus [3] = [0]$.

Hence, $(A / R, \oplus)$ is a group.

Definition : If R is a congruence relation defined on a semi-group $(S, *)$ or on a group $(G, *)$ and if $(S / R, \odot)$ or $(G / R, \odot)$ is the corresponding quotient semi-group or group defined as above, then the function $f_R : S \to S / R$ or $f_R : G \to G / R$ defined by $f_R(a) = [a]$ is an **homomorphism** called **natural homomorphism.**

Example 1 : Find the natural homomorphism $f_R : G \to G / R$ for the set A of natural numbers and the relation R defined by $a \, R \, b$ is $a \equiv b \pmod 5$.

Sol. : From the table given the previous page, it is clear that the natural homomorphism is given by

$0 \to [0]$, $1 \to [1]$, $2 \to [2]$, $3 \to [3]$, $4 \to [4]$.

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Example 2 : Consider the following semigroup defined on $S = \{a, b, c, d\}$ by the operation * given by the adjoining table.

Show that $R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a), (c, d), (d, c)\}$ is an equivalence relation.

Find the quotient semi-group $(S / R, \odot)$ induced by R.

Find the operation table for $(S / R, \odot)$. Find the natural homomorphism $f_R : S \to S / R$.

(M.U. 2006)

Sol. : It is easy to prove that R is an equivalence relation and is left to you as an exercise.

The partition S / R induced by R is

a	c
b	d

because every element in the block is related to the elements in the same block.

We denote this as congruence classes. $[a] = \{a, b\}$, $[c] = \{c, d\}$

Now, by definition $[a] \odot [b] = [a * b]$

From the given table, we find that

$[a] \odot [a] = [a * a] = [a]$, $[a] \odot [c] = [a * c] = [c]$,
$[c] \odot [a] = [c * a] = [c]$, $[c] \odot [c] = [c * c] = [a]$.

Hence, we get the table.

*	[a]	[c]
[a]	[a]	[c]
[c]	[c]	[a]

The natural homomorphism (from partion table).

$(a) \to [a]$, $(b) \to [a]$, $(c) \to [c]$, $(d) \to [c]$.

Example 3 : Consider the monoid $S = \{a, b, c, d\}$ with the operation $*$ defined by the adjoining table.

*	a	b	c	d
a	d	b	c	a
b	c	b	c	b
c	b	b	c	c
d	a	b	c	d

Consider the congruence relation

$R = \{(d, d), (d, a), (a, d), (a, a), (b, b), (b, c), (c, b), (c, c)\}$

(i) Write operation table of the quotient monoid S / R.

(ii) Find the natural homomorphism $f_R : S \to S / R$.

Sol. : You can easily prove that R is an equivalence relation.

The partition S / R is given by $[d] = \{a, d\}$, $[b] = \{b, c\}$. Further d is the identity element of $*$. From the given table, we find that,

a	b
d	c

$[a] \circledast [a] = [a * a] = [d] = [a]$

$[a] \circledast [b] = [a * b] = [b]$

$[b] \circledast [a] = [b * a] = [c] = [b]$

$[b] \circledast [b] = [b * b] = [b]$

Hence, we get the table.

*	[a]	[b]
[a]	[a]	[b]
[b]	[b]	[b]

The natural homomorphism is (from partion table)

$(a) \to [a]$, $(d) \to [a]$, $(b) \to [b]$, $(c) \to [b]$.

8. Elementary Properties of A Group

(a) Theorem 1 : In a group $(G, *)$,

(i) **identity is unique,** **(M.U. 2000, 05)**

(ii) **inverse of every element is unique.** **(M.U. 2002, 04)**

(iii) $(a^{-1})^{-1} = a$ for all $a \in G$.

(iv) $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$. **(M.U. 2003, 04, 05, 06, 12)**

Proof : (i) We have proved this property for semi-groups (See theorem in § 5, page 10-5).

Now, we shall prove it for Group.

Uniqueness of Identity Element

Proof : If possible let e and e' be two distinct identity elements in a group $(G, *)$.

Since e' is an identity, $a * e' = e' * a = a$ for each a.

In particular let $a = e$, $\therefore e * e' = e' * e = e$ ..... (i)

Also since e is an identity, $a * e = e * a = a$ for each a.

In particular, let $a = a'$, $\therefore a' * a = a * a' = e$ ..... (ii)

From (i) and (ii), it follows that $e = a'$.

$\therefore$ The identity element is unique.

(ii) If possible let b and b' be two distinct inverses of $a \in G$ in G.

Now, $b = b * e$ (By definition of Identity)

$= b * (a * b')$ (Since $a * b' = e$)

$= (b * a) * b'$ (Since $*$ is associative)

$= e * b'$ (Since $b * a = e$)

$= b'$ (Since e is identity)

$\therefore b = b'$

This contradicts our hypothesis.

$\therefore$ Inverse is unique.

(iii) Let $a^{-1} = c$. $\therefore c * a = a^{-1} * a = e$.

Also $a * c = a * a^{-1} = e$ $\therefore c^{-1} = a$ $\therefore (a^{-1})^{-1} = a$.

(iv) Let $c = a * b$, $d = b^{-1} * a^{-1}$.

$\therefore c * d = (a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$

$= a * e * a^{-1} = a * a^{-1} = e$.

Similarly, $d * c = e$ $\therefore c^{-1} = d$

$\therefore (a * b)^{-1} = b^{-1} * a^{-1}$.

Remark ....

Since identity is unique in a group, we shall call it ***the*** identity. Similarly, for the same reason we shall call ***the*** inverse of an element.

Theorem 2 : (Cancellation Laws) : In a group $(G, *)$ if $a, b, c \in G$, then

(i) $a * b = a * c$ implies $b = c$. [Left cancellation law] **(M.U. 2008)**

(ii) $b * a = c * a$ implies $b = c$. [Right cancellation law] **(M.U. 1997, 99, 2009)**

Proof : (i) If $a * b = a * c$ then by multiplying both sides on the left by a^{-1}, we get

$a^{-1} * (a * b) = a^{-1} * (a * c)$

$\therefore (a^{-1} * a) * b = (a^{-1} * a) * c$

$\therefore e * b = e * c$ $\therefore b = c$.

(ii) Similarly, $(b * a) * a^{-1} = (c * a) * a^{-1}$ leads us as above to $b = c$.

Theorem 3 : (Solution of equations) : For any two elements a, b in a group $(G, *)$.

(i) the equation $a * x = b$ has a unique solution.

(ii) the equation $y * a = y$ has a unique solution. **(M.U. 1998, 2005)**

Proof : *(i) Existence of solution :* Since a^{-1} exists in a group, we multiply the given equation on the left by a^{-1}.

$\therefore (a^{-1}) * (a * x) = a^{-1} * b$

$\therefore a^{-1} * b = (a^{-1} * a) * x = e * x = x$

$\therefore x = a^{-1} * b$ is a solution.

(ii) Uniqueness of solution : If x_1 and x_2 are two distinct solutions of $a * x = b$, we have

$a * x_1 = b$ and $a * x_2 = b$ $\therefore$ $a * x_1 = a * x_2$

$\therefore$ By cancellation law $x_1 = x_2$.

If y_1 and y_2 are distinct solution of $y * a = b$, we have

$y_1 * a = b$ and $y_2 * a = b$. $\therefore$ $y_1 * a = y_2 * a$

$\therefore$ By cancellation law $y_1 = y_2$.

Example 1 : Find the solution of $(3 * x) * 4 = 3 * 4$ in the group $(G, *)$ given in Example 9 on page 10-16. **(M.U. 2002, 03)**

Sol. : Consider $(3 * x) * 4 = 3 * 4$

By data $2\,(3 \times x) * 4 = 2\,(3 \times 4)$ $\therefore$ $6x * 4 = 24$

$2\,(6x \times 4) = 24$ $\therefore$ $48x = 24$ $\therefore$ $x = 1/2$.

Example 2 : Find the solution of $5 * x = 2$

(i) in the group of real numbers under the binary operation $a * b = a + b - 1$

(ii) in the group of rational numbers different from -3 under the binary operation

$$a * b = a + b + \frac{ab}{3}.$$

Sol. : (i) Since $a * b = a + b - 1$, $5 * x = 2$ gives

$5 + x - 1 = 2$ $\therefore$ $x = 2 - 4 = -2$.

(ii) Since $a * b = a + b + \frac{ab}{3}$, $5 * x = 2$ gives

$$5 + x + \frac{5x}{3} = 2 \quad \therefore \quad \frac{8x}{3} = -3 \quad \therefore \quad x = -\frac{9}{8}.$$

Example 3 : Prove that if $a^2 = a$, $a \in G$, then $a = e$ where e is an identity of the group G. **(M.U. 1997)**

Sol. : Since $a^2 = a$, $a^{-1}(a^2) = a^{-1}a$

$\therefore$ $(a^{-1}a)\,a = e$ $\therefore$ $a = e$.

Example 4 : If in a group every element is its inverse, prove that the group is Abelian. Give an example of such a group. Is the converse true ? Give an example if it is not.

Sol. : Let $a, b \in G$. Then by data $a^{-1} = a$, $b^{-1} = b$.

Since, it is a closed binary operation

$ab \in G$ $\therefore$ $(ab) = (ab)^{-1}$

Now, $ab = (ab)^{-1} = b^{-1} \cdot a^{-1}$ [By (iv) of Theorem 1 of § 8, page 10-37]

$\therefore$ $ab = ba$ [By data]

Hence, G is an Abelian group.

The following is the example of such a group

Let G be the set of residue classes [1], [3], [5], [7] modulo 8 under multiplication. We see from the table that every element is its own inverse.

To demonstrate that the converse is not true, we have to give an example of an Abelian group in which a^{-1} is not a.

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Now, the set of all rational numbers (without zero) is an Abelian group under usual multiplication. But a^{-1} is not a. For example, 2^{-1} is 1/2 but it is not 2.

Hence, the converse is not true.

Similar Example : Another example of the above type of group *i.e.* of a group in which every element is its inverse, is : The set $\{1, -1\}$ under multiplication. The multiplication table is as shown in the right side.

×	1	−1
1	1	−1
−1	−1	1

EXERCISE - II

1. Let G be the set of all non-zero real numbers and let $a * b = \frac{ab}{2}$.

   Show that $(G, *)$ is a Abelian group. Find the solution of $3 * x = 2$ in G. **(M.U. 2009, 14)** [Ans. : 4 / 3]

2. Prove that the set of all $m \times n$ matrices forms a group under addition.

3. Prove that the set of all $n \times n$ non-singular matrices forms a non-commutative group.

4. Prove that the set of the following four matrices forms a commutative group under multiplication

   $$\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}.$$ **(M.U. 2003, 04, 05)**

5. Prove that the set of the following six matrices forms a group under multiplication

   $$\begin{bmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{bmatrix}, \begin{bmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{bmatrix} \text{ for } \theta = 0, \frac{2\pi}{3}, \frac{4\pi}{3}.$$

6. Prove that the set of all points on the unit circle $|z| = 1$ is a group under multiplication.

   (**Hint :** If $z_1 = e^{i\theta_1}$, $z_2 = e^{i\theta_2}$, $z_1 z_2 = e^{i(\theta_1 + \theta_2)} = 1 = e^{i0}$ is an identity and $e^{-i\theta}$ is the inverse of $e^{i\theta}$.)

7. Show that $G = \{1, 2, 3, 4\}$ is an Abelian group under multiplication modulo 5.

8. Show that $S = \{1, 2, 3, 4, 5\}$ is not a group under multiplication modulo 6.

9. Prove that the set M of all 2×2 non-singular matrices is a group under multiplication. But M is not a group under addition.

10. Show that $(G, *)$ where $G = \{0, 1, 2, 3, 5\}$ and $*$ is multiplication modulo 6 (addition modulo 6) is an Abelian group. **(M.U. 1997)**

11. Prove that the set of all matrices $\begin{bmatrix}a & 0\\0 & b\end{bmatrix}$ where $a \neq 0$, $b \neq 0$ are real numbers is a group under matrix multiplication. **(M.U. 1997)**

12. Show the set $G = \{0, 1, 2\}$ is a group under addition modulo 3 but is not a group under usual addition.

13. Show that the set $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ where the functions are defined by

    $$f_1(x) = x, \quad f_2(x) = 1 - x, \quad f_3(x) = \frac{x}{x-1},$$

    $$f_4(x) = \frac{1}{x}, \quad f_5(x) = \frac{1}{1-x}, \quad f_6(x) = 1 - \frac{1}{x}.$$

Suppose b is a positive real number *i.e.* $b \to G'$.

Then $b = e^a$ $\therefore$ $a = \log b$.

and $f(a) = f(\log b) = e^{\log b} = b$. $\therefore$ f is onto.

Now, $f(a *_1 b) = f(a + b) = e^{a+b}$

$= e^a \cdot e^b = f(a) *_2 f(b)$

$\therefore$ f is an isomorphism.

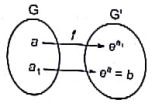


Fig. 10.8

Example 3 : Let R^+ be the set of all positive real numbers. Show that the function $f : R^+ \to R$ defined by $f(x) = \ln x$ is an isomorphism of the semi-group $(R^+, \times)$ to the semi-group $(R^+, +)$ where $\times$ and $+$ are ordinary multiplication and addition respectively. **(M.U. 2004, 05)**

Sol. : **(i)** Since $f(x) = \ln x = \log_e x$ if $f(a) = f(b)$ *i.e.*, $\log a = \log b$, then $a = b$.

$\therefore$ f is one-to-one.

(ii) If $c \in R$, then $e^c \in R$ and $f(e^c) = \log e^c = c \log e = c \in R^+$

$\therefore$ f is onto.

(iii) Now, $f(a \times b) = \log(a \times b) = \log a + \log b = f(a) + f(b)$

$\therefore$ f is an isomorphism.

Example 4 : Show that the additive group Z_4 is isomorphic to multiplicative group of non-zero elements of Z_5. **(M.U. 2006)**

Sol. : We have the following tables for the additive group G of Z_4 and multiplicative group of G' of (non-zero) Z_5.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Now, we write the table of × taking the second column last and second row last.

×	1	3	4	2
1	1	3	4	2
3	3	4	2	1
4	4	2	1	3
2	2	1	3	4

Clearly, now we can see that $G \to G'$ where the mapping is $0 \to 1$, $1 \to 3$, $2 \to 4$, $3 \to 2$ is a isomorphism.

Example 5 : If ω denotes the cube root of unity, show that $G = \{1, \omega, \omega^2\}$ is isomorphic to $(Z_3, +_3)$.

Sol. : We have the following tables for × and +.

×	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω^2

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

Clearly, $G \to G'$ where the mapping is $1 \to 0$, $\omega \to 1$ and $\omega^2 \to 2$ is an isomorphism.

Example 6 : *Show that* $(G, \times)$ *where* $G = \{1, -1, i, -i\}$ *and* $(Z_4, +_4)$ *are isomorphic.*

Sol. : *We first prepare the following tables for* × *and* +.

×	1	−1	i	$-i$
1	1	−1	i	$-i$
−1	−1	1	$-i$	i
i	i	$-i$	−1	1
$-i$	$-i$	i	1	−1

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Clearly $G \to G'$ where the mapping is $1 \to 0$, $-1 \to 2$, $i \to 1$ and $-i \to 3$ is a isomorphism.

Example 7 : If a function f is an isomorphism from a semi-group $(S, *)$ to another semi-group $(T, *')$, show that f^{-1} is also an isomorphism from $(T, *')$ to $(S, *)$. **(M.U. 2002, 15)**

Sol. : Since $f : S \to T$ is an isomorphism, f is one-to-one from S to T. ..... (1)

i.e., $f(a * b) = f(a) *' f(b)$ for all a, b in S.

$\therefore$ f^{-1} exists and is also one to one from T to S.

Now, suppose a', b' are elements of T.

Since f is onto we can always find elements a, b in S, such that

$f(a) = a'$, $f(b) = b'$

Hence, $a = f^{-1}(a')$ and $b = f^{-1}(b')$

Now, $f'(a' *' b') = f^{-1}[f(a) *' f(b)]$

$= f^{-1}[f(a * b)]$ [By (1)]

$= a * b$

$= f^{-1}(a') * f^{-1}(b')$

$\therefore$ Hence, f^{-1} is an isomorphism.

Example 8 : Show that if a function f is an isomorphism from a group $(G, *)$ to another group $(G', *')$ then show that f^{-1} is also an isomorphism from $(G, *')$ to $(G, *)$. **(M.U. 2006)**

Sol. : Left to you.

Example 9 : If f is homomorphism from a commutative semigroup $(S, *)$ onto a semigroup $(T, *')$ then prove that $(T, *')$ is also commutative. **(M.U. 2002, 08, 13)**

Sol. : Let t_1 and t_2 be any two elements of T.

Since f is homomorphic there exist s_1 and s_2 in S, such that $t_1 = f(s_1)$ and $t_2 = f(s_2)$.

Hence, $t_1 *' t_2 = f(s_1) *' f(s_2)$

$= f(s_1 * s_2)$

$= f(s_2 * s_1)$ [$\because$ s is a commutative group]

$\therefore$ $t_1 *' t_2 = f(s_2) *' f(s_1)$

$= t_2 *' t_1$

$\therefore$ $(T, *')$ is also commutative.

Example 10 : Let $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and consider the partial order relation $\leq$ of divisibility on A *i.e.* $a \leq b$ if a / b. Let $A' = P(S)$ where $S = \{e, f, g\}$ be the poset with partial order relation $\subseteq$ (is a subset of). **(M.U. 2007)**

Prove that $(A, \leq)$ and $(A', \subseteq)$ are isomorphic.

Sol. : Hasse diagram of the partial order relation of divisibility on A is shown in Fig. 10.9 (a) below.

is its inverse. We shall denote an element of the group B^n by $(b_1, b_2, \ldots, b_n)$ or by $b_1, b_2, \ldots, b_n$. We shall say that the order of the group B^n is n.

In order to reduce the possibility of error in transmission *i.e.* the possibility of receiving a different word than the word sent we define a new function called encoding function.

(a) Encoding Function

Definition : If an integer $n > m$ and if there is one to one correspondence $e : B^m \to B^n$ then e is called an (m, n) **encoding function.** In this way every word in B^m is represented by a word in B^n. If $b \in B^m$ then $e(b)$ is called the **code word** representing b.

Since $n > m$ there will be some more 0's and 1's in $e(b)$ than in b. These additional zeros and ones help us to detect and correct the errors as seen earlier in an example.

Weight : If a word $x \in B^n$ then the number of 1's x is called the weight of x and is denoted by $|x|$.

Example 1 : Find the weights of each of the following words in B^5.

(i) $x = 00100$ (ii) $x = 01010$ (iii) $x = 00000$ (iv) $x = 11110$

Sol. : (i) $|x| = 1$, (ii) $|x| = 2$, (iii) $|x| = 0$, (iv) $|x| = 4$.

(b) Parity Check Code

Definition : The encoding function $e : B^m \to B^{m+1}$ is called **parity** $(m, m+1)$ **check code,** if $b = b_1, b_2, \ldots, b_m \in B^m$ define

$$e(b) = b_1\, b_2 \ldots b_m\, b_{m+1} \quad \text{where } b_{m+1} = \begin{cases} 0, & \text{if } |b| \text{ is even} \\ 1, & \text{if } |b| \text{ is odd} \end{cases}$$

The encoding function defined above enables us to detect an error. We first observe that $b_{m+1} = 0$ if and only if the number of 1's in b is an even number *i.e.* every code word $e(b)$ has even weight. A single error in transmission of a code word will change the received word to a word of odd weight and as such can be detected. Similarly, $b_{m+1} = 1$ if and only if the number of 1's in b is an odd number *i.e.* every code word $e(b)$ has odd weight. A single error in transmission of a code word will change the received word to a word of even degree and thus error can be detected.

Example 1 : Consider the (3, 4) parity check code. For each of the following received words, determine whether an error will be detected.

(i) 0100, (ii) 1100

Sol. : **(i)** Since $x_1 = 0100$, $|x_1| = 1$

Since $|x_1|$ is odd, the last digit should have been 1 but it is zero and hence there is an error.

$\therefore$ The error is detected.

(ii) Since $x_1 = 1100$, $|x_1| = 2$.

Since $|x_1|$ is even, the last digit should have been zero and it is zero.

$\therefore$ The error cannot be detected.

Example 2 : Consider the (3, 4) parity check code for $m = 3$.

$e(b) = x$ $e(000) = 0000$ $e(001) = 0011$

$e(010) = 0101$ $e(011) = 0110$ $e(100) = 1001$

$e(101) = 1010$ $e(110) = 1100$ $e(111) = 1111$

Can you detect an error if $b = 001$ *and* $e(b) = 0111$?

Sol. : Since $b = 001$, $e(b) = 0111$.

But by data $c(b) = 0111$ and $|x_1| = 3$. Hence, odd number of errors (at least one) has occurred.

It should be noted that **if the received word is of even weight then we cannot conclude that the code word was transmitted correctly,** since this encoding function does not detect even number of errors. Still the parity check is widely used.

EXERCISE - III

1. Find the weights of the words given below.

(i) 1011 (ii) 1110 (iii) 0110 (iii) 01101 (iv) 010101 (v) 111111

[**Ans. :** (i) 3, (ii) 3, (iii) 2, (iv) 3, (v) 3, (vi) 6.]

2. Consider (3, 4) parity check code. For each of the following received words find whether an error will be detected.

(i) 0010 (ii) 1001 (iii) 1101 (iv) 1010 (v) 1111 (vi) 0011

[**Ans. :** (i) Yes, (ii) No, (iii) Yes, (iv) No, (v) No, (vi) No.]

3. Consider the (6, 7) parity check code. For each of the following received words, find whether an error will be detected.

(i) 1101010 (ii) 011111 (iii) 1010011 (iv) 1001101

[**Ans. :** (i) No, (ii) Yes, (iii) No, (iv) No.]

11. Group Codes

So far we have not made use of the fact that $(B^n, \oplus)$ is a group. Now we shall consider an encoding function e that makes use of this property. First we shall define the term group code.

(a) Group Code **(M.U. 1999, 2000, 05)**

Definition : An (m, n) coding function $e : B^m \to B^n$ is called a **group code** if

$$e(B^m) = \{ e(b) \mid b \in B^m \}$$
$$= \text{Range } (e)$$

is a subgroup of B^n.

To prove that a given encoding function is a group code we have to show that (i) the identity element of B^n is in N. (ii) if x, y belong to N then $x \oplus y$ belongs to N, (iii) if x is in N then its inverse is in N.

We need not check (iii) because every element of B^n is its inverse.

Example 1 : Show that the (2, 5) encoding function $e : B^2 \to B^5$ defined by

$e(00) = 00000$, $e(01) = 01110$, $e(10) = 10101$, $e(11) = 11011$

is a group code. **(M.U. 2002, 04, 06, 07, 09, 14, 16, 18)**

Sol. : Let $N = \{00000, 01110, 10101, 11011\}$. We have to show that N is a subgroup of B^5. We shall now prepare the following table for B^5.

We prepare the following table by using the table (A) given on page 10-46 *i.e.*, by using $0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 0$ and $1 + 1 = 0$.

For example, $01110 + 10101 = 11011$; $11011 + 01110 = 10101$

$\oplus$	00000	01110	10101	11011
00000	00000	01110	10101	11011
01110	01110	00000	11011	10101
10101	10101	11011	00000	01110
11011	11011	10101	01110	00000

(i) From the diagonal elements of the above table we see that the identity (00000) of B^5 is in N.

(ii) From the table we see that if x, y belong to N then $x \oplus y$ also belongs to N.

(iii) Every element is its inverse.

$\therefore$ N is a subgroup of B^5 and the given encoding function is a group code.

Example 2 : Consider (3, 6) encoding function defined below.

e (000) = 000000, e (001) = 000110, e (010) = 010010,
e (011) = 010100, e (100) = 100101, e (101) = 100011,
e (110) = 110111, e (111) = 110001.

Show that the encoding function is a group code. **(M.U. 1998)**

Sol. : Let N = {000000, 000110, 010010, 010100, 100101, 100011, 110111, 11000}

We have to show that N is a subgroup of B^6.

We shall now prepare the following table for B^6.

$\oplus$	000000	000110	010010	010100	100101	1000111	110111	110001
000000	000000	000110	010010	010100	100101	100011	110111	110001
000110	000110	000000	010100	010010	100011	100101	110001	110111
010010	010010	010100	000000	000110	110111	110001	100101	100011
010100	010100	010010	000110	000000	110001	110111	100011	100101
100101	100101	100011	110111	110001	000000	000110	010010	010100
100011	100011	100101	110001	110111	000110	000000	010100	010010
110111	110111	110001	100101	100011	010010	010100	000000	000110
110001	110001	110111	100011	100101	010100	010010	000110	000000

(i) From the diagonal elements of the above table we see that the identity (000000) of B^6 is in N.

(ii) From the table we see that if x, y belong to N then $x \oplus y$ belongs to N.

(iii) Every element is its inverse.

$\therefore$ N is a subgroup of B^6 and the given encoding function is a group code.

(b) Hamming Distance

Definition : If x, y are words in B^m then the weight of $x \oplus y$ *i.e.* $|x \oplus y|$ is called the **Hamming distance** between x and y and is denoted by $\delta(x, y)$.

In other words, the distance between $x = x_1, x_2, \ldots, x_m$ and $y = y_1, y_2, \ldots, y_m$ is the number of values of i such that $x_i \neq y_i$ *i.e.* the number of positions in which x and y differ. The weight of $x \oplus y$ helps us to find the number of different positions.

Example 1 : Find the distance between x and y where

(i) x = 110110, y = 000101; (ii) x = 001100, y = 010110

Sol. : $x \oplus y$ is obtained from the table

+	0	1
0	0	1
1	1	0

for every digit.

(i) $x \oplus y = \begin{array}{r} 110110 \\ 000101 \\ \hline 110011 \end{array}$ $\therefore$ $|x \oplus y| = 4$

(ii) $x \oplus y = \begin{array}{r} 001100 \\ 010110 \\ \hline 011010 \end{array}$ $\therefore$ $|x \oplus y| = 3$

Example 2 : Find the distance between x and y where

(i) x = 1100010, y = 1010011; (ii) x = 0100100, y = 0011010 **(M.U. 1996)**

Sol. : As explained above.

(i) $x \oplus y$ = 0110001 $\therefore$ $|x \oplus y| = 3$

(ii) $x \oplus y$ = 0111110 $\therefore$ $|x \oplus y| = 5$

(c) Theorem (Properties of Hamming Distance)

Let x, y, z be elements of B^m, then

(a) $\delta(x, y) = \delta(y, x)$

(b) $\delta(x, y) \geq 0$

(c) $\delta(x, y) = 0$ if and only if $x = y$

(d) $\delta(x, y) \leq \delta(x, z) + \delta(z, y)$

Sol. : (i) By definition, $\delta(x, y) = |x \oplus y|$

By the same definition, $\delta(y, x) = |y \oplus x|$

Since $|x \oplus y| = |y \oplus x|$ an integer $\delta(x, y) = \delta(y, x)$

(ii) Since $\delta(x, y) = |x \oplus y|$ $\delta(x, y) \geq 0$

(iii) Clearly, $\delta(x, x) = 0$

(iv) For a, b in B^m $|a \oplus b| \leq |a| + |b|$ ..... (1)

Since at any position where a and b differ one of them must contain a 1.

Further, if $a \in B^m$ then $a \oplus a = \overline{0}$, the identity element in B^m.

$$\therefore \quad \delta(x, y) = |x \oplus y| = |x \oplus \overline{0} \oplus y|$$
$$= |x \oplus z + z \oplus y|$$
$$\leq |x \oplus z| + |z \oplus y| \quad \text{[By (1)]}$$
$$\therefore \quad \delta(x, y) \leq \delta(x, z) + \delta(z, y)$$

(d) Minimum Distance

(M.U. 1998, 99, 2011)

Definition : Let $e : B^m \to B^n$ be a coding function. The minimum of the distance between all pairs of distinct code words is called the **minimum distance** of the code.

Symbolically, $\min\left\{[\delta(e(x), e(y))] / x, y \in B^m\right\}$ is called the minimum distance of the code.

Example 1 : Consider the following (2, 5) encoding function e.

$$\left.\begin{aligned} e(00) &= 00000 \\ e(10) &= 00111 \\ e(01) &= 01110 \\ e(11) &= 11111 \end{aligned}\right\} \text{ Code words}$$

Find the minimum distance of the code. **(M.U. 2010)**

Sol. : If we denote these words as x, y, z and u is then

$\delta(x, y) = 3$, $\delta(x, z) = 3$, $\delta(x, u) = 5$,

$\delta(y, z) = 2$, $\delta(y, u) = 2$, $\delta(z, u) = 2$.

$\therefore$ Minimum distance of $e = 2$.

(c) Theorem

An (m, n) coding function $e : B^m \to B^n$ can detect k or less errors if and only if its minimum distance is at least $k + 1$.

We shall accept this theorem without proof but will illustrate it through an example.

Example 1 : Consider the (2, 4) encoding function. How many errors can it detect ?

$$\left.\begin{aligned} e(00) &= 0000 \\ e(10) &= 0110 \\ e(01) &= 1011 \\ e(11) &= 1100 \end{aligned}\right\} \text{ Code words}$$ **(M.U. 1998, 2008)**

Sol. : Let x, y, z, u denote the words. Then the distances are given by

$\delta(x, y) = \delta(0000, 0110) = 2$, $\delta(x, z) = \delta(0000, 1011) = 3$,

$\delta(x, u) = \delta(0000, 1100) = 2$, $\delta(y, z) = \delta(0110, 1011) = 3$,

$\delta(y, u) = \delta(0110, 1100) = 2$, $\delta(z, u) = \delta(1011, 1100) = 3$.

$\therefore$ Minimum distance = 2 $\therefore$ $k + 1 = 2$ $\therefore$ $k = 1$

The code will detect 1 or less errors.

Example 2 : Consider (2, 6) encoding function $e : B^2 \to B^6$ defined as

$e(0, 0) = 000000$, $e(0, 1) = 011110$,

$e(1, 0) = 101010$, $e(1, 1) = 111000$

(i) Find the minimum distance of the code.

(ii) How many errors can be detect ? **(M.U. 2006, 08, 11, 12)**

Sol. : *(i)* If we denote the words by x, y, z and u then

$\delta(x, y) = \delta(000000, 011110) = 4$, $\delta(x, z) = \delta(000000, 101010) = 3$,

$\delta(x, u) = \delta(000000, 111000) = 3$, $\delta(y, z) = \delta(011110, 101010) = 3$,

$\delta(y, u) = \delta(011110, 111000) = 3$, $\delta(z, u) = \delta(101010, 111000) = 3$.

$\therefore$ The minimum distance is 3. Since the minimum distance is 3,

$k + 1 = 3$ $\therefore$ $k = 2$.

The coding function can detect $k = 2$ or less errors.

Example 3 : Consider the following (3, 8) encoding function $e : B^3 \to B^8$ defined by

$$\left.\begin{aligned} e(000) &= 00000000 \\ e(001) &= 10111000 \\ e(010) &= 00101101 \\ e(011) &= 10010101 \\ e(100) &= 10100100 \\ e(101) &= 10001001 \\ e(110) &= 00011100 \\ e(111) &= 00110001 \end{aligned}\right\} \text{ Code words}$$

How many errors can e detect ? **(M.U. 2003, 06, 11, 12)**

Sol. : There will be ${}^8C_2 = 28$ pairs of code words. The minimum distance is 3. By the above theorem if minimum distance is $k + 1 = 3$, then the coding function can detect $2 = k$ or less errors.

Example 4 : Show that (3, 7) encoding function e defined below is a group code.

$e(000) = 0000000$, $e(001) = 0010110$, $e(010) = 0101000$,

$e(011) = 0111110$, $e(100) = 1000101$, $e(101) = 1010011$,

$e(110) = 1101101$, $e(111) = 1111011$

How many errors can it detect ? **(M.U. 2005, 07)**

Sol. :

$\oplus$	0000000	0010110	0101000	0111110	1000101	1010011	1101101	1111011
0000000	0000000	0010110	0101000	0111110	1000101	1010011	1101101	1111011
0010110	0010110	0000000	0111110	0101000	1010011	1000101	1111011	1101101
0101000	0101000	0111110	0000000	0010110	1101101	1111011	1000101	1010011
0111110	0111110	0101000	0010110	0000000	1111011	1101101	1010011	1000101
1000101	1000101	1010011	1101101	1111011	0000000	0010110	0101000	0111110
1010011	1010011	1000111	1111011	1101101	0010110	0000000	0111110	0101000
1101101	1101101	1111011	1000101	1010011	0101000	0111110	0000000	0010110
1111011	1111011	1101101	1010011	1000101	0111110	0101000	0010110	0000000

(I) From the diagonal elements of the above table we see that (0000000) is an identity and it belongs to N.

(II) From the table we also see that if x, y belong to N then $x \oplus y$ belongs to N.

(III) Every element is its inverse.

$\therefore$ N is a subgroup of B^7 and the given encoding function is a group code. The minimum distance is 2. Hence, the code can detect 1 or less errors.

Example 5 : Consider the following (3, 9) encoding function e.

$e(000) = 000000000$, $e(001) = 011100101$, $e(010) = 010101000$,
$e(011) = 110010001$, $e(100) = 010011010$, $e(101) = 111101011$,
$e(110) = 001011000$, $e(111) = 110000111$.

Find the minimum distance. How many error can it detect ? (M.U. 2002)

Sol. : It can be seen that the minimum distance is 3.

Hence, e can detect 2 or less errors.

EXERCISE - IV

1. Consider the (3, 6) encoding function $e : B^3 \to B^6$ defined by
   $e(000) = 000000$, $e(001) = 001100$, $e(010) = 010011$,
   $e(011) = 011111$, $e(100) = 100101$, $e(101) = 101001$,
   $e(110) = 110110$, $e(111) = 111010$.
   Show that the encoding function is a group code.
2. Find the minimum distance of the following (2, 4) encoding function
   $e(00) = 0000$, $e(10) = 0110$, $e(01) = 1011$, $e(11) = 1100$. [Ans. : 2]
3. Consider the following (2, 6) encoding function e.
   $e(00) = 000000$, $e(10) = 101010$, $e(01) = 011110$, $e(11) = 111000$
   (a) Find the minimum distance of e. (b) How many errors will e detect ?
   (M.U. 2008) [Ans. : (a) 2, (b) 1]

12. Mod-2 Boolean Product

Definition : If $D = [d_{ij}]$ is an $m \times p$ Boolean matrix (matrix whose elements are 0 and 1) and $E = [e_{ij}]$ is a $p \times n$ Boolean matrix then we define a product $D * E$ called the mod-2 Boolean product as the $m \times n$ matrix F where

$$f_{ij} = d_{i1} \cdot e_{1j} + d_{i2} \cdot e_{2j} + \ldots\ldots + d_{ip} \cdot e_{pj}, \quad 1 \le i \le m, 1 \le j \le n$$

Example 1 : Find the mod-2 Boolean product of the following two Boolean matrices

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Sol. : First we note that

+	0	1
0	0	1
1	1	0

and

×	0	1
0	0	0
1	0	1

We take the product of the above matrices as usual and use the above results.

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1\cdot1+1\cdot1+0\cdot0 & 1\cdot0+1\cdot1+0\cdot1 \\ 0\cdot1+1\cdot1+1\cdot0 & 0\cdot0+1\cdot1+1\cdot1 \end{bmatrix} = \begin{bmatrix} 1+1+0 & 0+1+0 \\ 0+1+0 & 0+1+1 \end{bmatrix}$$

(But 1 + 1 = 1 and 1 + 1 = 0.)

Hence, we get

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

We thus note that if an odd number of corresponding pairs consist of two 1's then the product is 1 and if an even number of corresponding pairs consist of two 1's then the product is zero.

Mod-2 Boolean product in general terms is shown below.

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1p} \\ a_{21} & a_{22} & \cdots & a_{2p} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ip} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mp} \end{bmatrix} * \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ b_{p1} & b_{p2} & \cdots & b_{pj} & \cdots & b_{pn} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{bmatrix}$$

$$\begin{bmatrix} a_{i1} \\ a_{i2} \\ \vdots \\ a_{ip} \end{bmatrix} \longleftrightarrow \begin{bmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{pj} \end{bmatrix} \longrightarrow \boxed{\begin{array}{l} \text{If an odd number of} \\ \text{corresponding pais consists} \\ \text{of two 1's, then } c_{ij} = 1 \text{ and} \\ \text{if an even number of} \\ \text{corresponding pairs consists} \\ \text{of two 1's, then } c_{ij} = 0 \end{array}}$$

(b) Parity Check Matrix

Definition : Let $m < n$ and $r = n - m$. An $n \times r$ Boolean matrix H given by

$$H = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1r} \\ h_{21} & h_{22} & \cdots & h_{2r} \\ \vdots & \vdots & \cdots & \vdots \\ h_{m1} & h_{m2} & \cdots & h_{mr} \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \quad \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \quad \text{..... (A)}$$

$n - m = r$ rows

where last r rows form the $r \times r$ identity matrix is called a **parity check matrix.**

The parity check matrix H defined above is used to define an encoding function $e_H : B^m \to B^n$ as illustrated in the following examples.

If $b = b_1, b_2, \ldots\ldots, b_m$, ... (1)

let $x = e_H(b) = b_1\, b_2 \ldots\ldots b_m\, x_1\, x_2 \ldots\ldots x_r$

where, $x_1 = b_1 \cdot h_{11} + b_2 \cdot h_{21} + \ldots + b_m \cdot h_{m1}$

$x_2 = b_1 \cdot h_{12} + b_2 \cdot h_{22} + \ldots + b_m \cdot h_{m2}$

. . . . . .

. . . . . .

$x_r = b_1 \cdot h_{1r} + b_2 \cdot h_{2r} + \ldots + b_m \cdot h_{mr}$ ..... (2)

Example 1 : Consider the parity matrix H given by

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$ ..... (B)

Determine the group code $e_H : B^2 \to B^5$. **(M.U. 2008, 09, 10)**

Sol. : Since $B = (0, 1)$, we have $B^2 = (00, 01, 10, 11)$. [See (I), page 10-46]

From (1) and (2) above, we get

$e_H(00) = 00\ x_1\ x_2\ x_3$ ..... (3)

where $x_1\ x_2\ x_3$ are given by the following equations

$x_1 = b_1\ h_{11} + b_2\ h_{21}$

$x_2 = b_1\ h_{12} + b_2\ h_{22}$ ..... (C)

$x_3 = b_1\ h_{13} + b_2\ h_{23}$

But from the given matrix H, [Comparing (A) and (B)]

$h_{11} = 1,\ h_{12} = 1,\ h_{13} = 0;\quad h_{21} = 0,\ h_{22} = 1,\ h_{23} = 1,$

$h_{31} = 1,\ h_{32} = 0,\ h_{33} = 0;\quad h_{41} = 0,\ h_{42} = 1,\ h_{43} = 0;$

$h_{51} = 0,\ h_{52} = 0,\ h_{53} = 1.$

and from (3), $b_1 = 0,\ b_2 = 0.$

Putting these values in (C), we get

$x_1 = 0 \cdot 1 + 0 \cdot 0 = 0;\quad x_2 = 0 \cdot 1 + 0 \cdot 1 = 0;\quad x_3 = 0 \cdot 0 + 0 \cdot 1 = 0$

$\therefore\ e\,(00) = 00\ x_1\ x_2\ x_3 = 00000$ where $b_1 = 0,\ b_2 = 0$

Further, $e\,(10) = 10\ x_1\ x_2\ x_3$ where $(b_1 = 1,\ b_2 = 0)$

$x_1 = 1 \cdot 1 + 0 \cdot 0 = 1,\quad x_2 = 1 \cdot 1 + 0 \cdot 1 = 1;\quad x_3 = 1 \cdot 0 + 0 \cdot 1 = 0$

$\therefore\ e\,(10) = 10110$

Again $e\,(01) = 01\ x_1\ x_2\ x_3$ where $(b_1 = 0,\ b_2 = 1)$

$x_1 = 0 \cdot 1 + 1 \cdot 0 = 0;\quad x_2 = 0 \cdot 1 + 1 \cdot 1 = 1;\quad x_3 = 0 \cdot 0 + 1 \cdot 1 = 1$

$\therefore\ e\,(01) = 01011$

Lastly $e\,(11) = 11\ x_1\ x_2\ x_3$ where $(b_1 = 1,\ b_2 = 1)$

$x_1 = 1 \cdot 1 + 1 \cdot 0 = 1;\quad x_2 = 1 \cdot 1 + 1 \cdot 1 = 0;\quad x_3 = 1 \cdot 0 + 1 \cdot 1 = 1$

$\therefore\ e\,(11) = 11101$

$\therefore$ The group code function $e_H : B^2 \to B^5$ is

$e\,(00) = 00000,\qquad e\,(01) = 01011,$

$e\,(10) = 10110,\qquad e\,(11) = 01011.$

Example 2 : Consider the parity matrix X given by

$$H = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Determine (2, 5) group code function $e_H : B^2 \to B^5$.

Sol. : Since $B = (0, 1)$, we have $B^2 = (00, 01, 10, 11)$.

As in Example 1, from (1) and (2), page 10-54 and 10-55, we get

$e_H(0\,0) = 0\,0\ x_1\ x_2\ x_3$ where $b_1 = 0,\ b_2 = 0$ ..... (3)

where x_1, x_2, x_3 are given by the following equations,

$x_1 = b_1\ h_{11} + b_2\ h_{21}$

$x_2 = b_1\ h_{12} + b_2\ h_{22}$ ..... (A)

$x_3 = b_1\ h_{13} + b_2\ h_{23}$

But from the given matrix H,

$h_{11} = 0,\quad h_{12} = 1,\quad h_{13} = 1,\quad h_{21} = 0,\quad h_{22} = 1,\quad h_{23} = 1,$

$h_{31} = 1,\quad h_{32} = 0,\quad h_{33} = 0,\quad h_{41} = 0,\quad h_{42} = 1,\quad h_{43} = 0,$

$h_{51} = 0,\quad h_{52} = 0,\quad h_{53} = 1$ and from (3), $b_1 = 0,\ b_2 = 0.$

Putting these values in (A), we get

$x_1 = 0 \cdot 0 + 0 \cdot 0 = 0,\ x_2 = 0 \cdot 1 + 0 \cdot 1 = 0,\ x_3 = 0 \cdot 1 + 0 \cdot 1 = 0.$

Hence, from (3), we get

$e\,(0\,0) = 0\,0\,0\,0\,0$ where $b_1 = 0,\ b_2 = 0.$

Further, $e\,(0\,1) = 0\,1\ x_1\ x_2\ x_3$ where $b_1 = 0,\ b_2 = 1.$

$x_1 = 0 \cdot 0 + 1 \cdot 0 = 0,\ x_2 = 0 \cdot 1 + 1 \cdot 1 = 1,\ x_3 = 0 \cdot 1 + 1 \cdot 1 = 1.$

$\therefore\ e\,(0\,1) = 0\,1\,0\,1\,1$

Further, $e\,(1\,0) = 1\,0\ x_1\ x_2\ x_3$ where $b_1 = 1,\ b_2 = 0.$

$x_1 = 1 \cdot 0 + 0 \cdot 0 = 0,\ x_2 = 1 \cdot 1 + 0 \cdot 1 = 1,\ x_3 = 1 \cdot 1 + 0 \cdot 1 = 1.$

$\therefore\ e\,(1\,0) = 1\,0\,0\,1\,1$

Further, $e\,(1\,1) = 1\,1\ x_1\ x_2\ x_3$ where $b_1 = 1,\ b_2 = 1.$

$x_1 = 1 \cdot 0 + 1 \cdot 0 = 0,\ x_2 = 1 \cdot 1 + 1 \cdot 1 = 0,\ x_3 = 1 \cdot 1 + 1 \cdot 1 = 0.$

$\therefore\ e\,(1\,1) = 1\,1\,0\,0\,0$

Hence, the group code function, $e_H : B^2 \to B^5$ is

$e\,(0\,0) = 0\,0\,0\,0\,0,\qquad e\,(0\,1) = 0\,1\,0\,1\,1,$

$e\,(1\,0) = 1\,0\,0\,1\,1,\qquad e\,(1\,1) = 1\,1\,0\,0\,0.$

Example 3 : Let $H = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ be parity check matrix. **(M.U. 2015)**

Determine the group code $e_H : B^2 \to B^5$.

Sol. : Since $B = \{0, 1\}$, we have $B^2 = \{00, 01, 10, 11\}$.

As in Example 2, from (1) and (2), page 10-54 and 10-55, we got

$e_H(0\,0) = 0\,0\,x_1\,x_2\,x_3$ where $b_1 = 0, b_2 = 0$ ..... (3)

where x_1, x_2, x_3 are given by the following equations,

$x_1 = b_1 h_{11} + b_2 h_{21}$

$x_2 = b_1 h_{12} + b_2 h_{22}$ ..... (A)

$x_3 = b_1 h_{13} + b_2 h_{23}$

But from the given matrix H,

$h_{11} = 1, \quad h_{12} = 0, \quad h_{13} = 0, \quad h_{21} = 1, \quad h_{22} = 1, \quad h_{23} = 0,$

$h_{31} = 0, \quad h_{32} = 1, \quad h_{33} = 1, \quad h_{41} = 1, \quad h_{42} = 0, \quad h_{43} = 0,$

$h_{51} = 0, \quad h_{52} = 1, \quad h_{53} = 0, \quad h_{61} = 0, \quad h_{62} = 0, \quad h_{63} = 1$

and from (3), $b_1 = 0, b_2 = 0$.

Putting these values in (A), we get

$x_1 = 0 \cdot 1 + 0 \cdot 1 = 0, \quad x_2 = 0 \cdot 0 + 0 \cdot 1 = 0, \quad x_3 = 0 \cdot 0 + 0 \cdot 0 = 0.$

Hence, from (3), we get

$e(0\,0) = 0\,0\,0\,0\,0$ where $b_1 = 0, b_2 = 0$.

Further, $e(0\,1) = 0\,1\,x_1\,x_2\,x_3$ where $b_1 = 0, b_2 = 1$.

$x_1 = 0 \cdot 1 + 1 \cdot 1 = 1, \quad x_2 = 0 \cdot 0 + 1 \cdot 1 = 1, \quad x_3 = 0 \cdot 0 + 1 \cdot 0 = 0.$

$\therefore \quad e(0\,1) = 0\,1\,1\,1\,0$ where $b_1 = 0, b_2 = 1$.

Further, $e(1\,0) = 1\,0\,x_1\,x_2\,x_3$ where $b_1 = 1, b_2 = 0$.

$x_1 = 1 \cdot 1 + 0 \cdot 1 = 1, \quad x_2 = 1 \cdot 0 + 0 \cdot 1 = 0, \quad x_3 = 1 \cdot 0 + 0 \cdot 0 = 0.$

$\therefore \quad e(1\,0) = 1\,0\,1\,0\,0$ where $b_1 = 1, b_2 = 0$.

Further, $e(1\,1) = 1\,1\,x_1\,x_2\,x_3$ where $b_1 = 1, b_2 = 1$.

$x_1 = 1 \cdot 1 + 1 \cdot 1 = 0, \quad x_2 = 1 \cdot 0 + 1 \cdot 1 = 1, \quad x_3 = 1 \cdot 0 + 1 \cdot 0 = 0.$

$\therefore \quad e(1\,1) = 1\,1\,0\,1\,0$ where $b_1 = 1, b_2 = 1$.

Hence, the group code function, $e_H : B^2 \to B^5$ is

$e(0\,0) = 0\,0\,0\,0\,0, \quad e(0\,1) = 0\,1\,1\,1\,0,$

$e(1\,0) = 1\,0\,1\,0\,0, \quad e(1\,1) = 1\,1\,0\,1\,0.$

Example 4 : Let $H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ be a parity check matrix. ..... (D)

Determine the group code $e_H : B^3 \to B^6$. **(M.U. 2002, 04, 07, 14, 15, 18)**

Sol. : Since $B = \{0, 1\}$ [See (I), page 10-46]

$B^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$

$\therefore \quad e(000) = 000\,x_1\,x_2\,x_3$

where x_1, x_2, x_3 are given by the following equations.

$x_1 = b_1 h_{11} + b_2 h_{21} + b_3 h_{31}$

$x_2 = b_1 h_{12} + b_2 h_{22} + b_3 h_{32}$

$x_3 = b_1 h_{13} + b_2 h_{23} + b_3 h_{33}$ ..... (E)

But from the given matrix H, [Comparing (A), page 10-54 and (D)]

$h_{11} = 1, \quad h_{12} = 0, \quad h_{13} = 0,$

$h_{21} = 0, \quad h_{22} = 1, \quad h_{23} = 1,$

$h_{31} = 1, \quad h_{32} = 1, \quad h_{33} = 1$

and $b_1 = 0, b_2 = 0, b_3 = 0$.

Putting these values in (E), we get

$x_1 = 0 \cdot 1 + 0 \cdot 0 + 0 \cdot 1 = 0; \quad x_2 = 0 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 = 0;$

$x_3 = 0 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 = 0 \quad \therefore \; e(000) = 000000$

Further $e(001) = 001\,x_1\,x_2\,x_3$ where

$x_1 = 0 \cdot 1 + 0 \cdot 0 + 1 \cdot 1 = 1, \quad x_2 = 0 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 = 1;$

$x_3 = 0 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 = 1 \quad \therefore \; e(001) = 001111$

And $e(010) = 010\,x_1\,x_2\,x_3$ where

$x_1 = 0 \cdot 1 + 1 \cdot 0 + 0 \cdot 1 = 0; \quad x_2 = 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 = 1;$

$x_3 = 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 = 1 \quad \therefore \; e(010) = 010011$

And $e(011) = 011\,x_1\,x_2\,x_3$ where

$x_1 = 0 \cdot 1 + 1 \cdot 0 + 1 \cdot 1 = 1; \quad x_2 = 0 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 0;$

$x_3 = 0 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 0 \quad \therefore \; e(011) = 011100$

And $e(100) = 100\,x_1\,x_2\,x_3$ where

$x_1 = 1 \cdot 1 + 0 \cdot 0 + 0 \cdot 1 = 1, \quad x_2 = 1 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 = 0;$

$x_3 = 1 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 = 0 \quad \therefore \; e(100) = 100100$

And $e(101) = 101\,x_1\,x_2\,x_3$ where

$x_1 = 1 \cdot 1 + 0 \cdot 0 + 1 \cdot 1 = 0; \quad x_2 = 1 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 = 1;$

$x_3 = 1 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 = 1 \quad \therefore \; e(101) = 101011$

And $e(110) = 110\,x_1\,x_2\,x_3$ where

$x_1 = 1 \cdot 1 + 1 \cdot 0 + 0 \cdot 1 = 1; \quad x_2 = 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 = 1,$

$x_3 = 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 = 1 \quad \therefore \; e(110) = 110111$

Lastly $e(111) = 111\,x_1\,x_2\,x_3$ where

$x_1 = 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 1 = 0; \quad x_2 = 1 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 0;$

$x_3 = 1 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 0 \quad \therefore \; e(111) = 111000$

Hence, the group code function, $e_H : B^3 \to B^6$ is

$e(000) = 000000, \quad e(001) = 001111,$

$e(010) = 010011, \quad e(011) = 011100,$

$e(100) = 100100, \quad e(101) = 101011,$

$e(110) = 110111, \quad e(111) = 111000.$

EXERCISE - V

1. Let $H = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ be a parity check matrix.

Find the (2, 5) group code function $e_H : B^2 \to B^5$.

[**Ans. :** $e(00) = 00000$, $e(01) = 01011$, $e(10) = 10011$, $e(11) = 11000$]

13. Maximum Likelihood Decoding Technique

It is natural to expect a decoding function when an encoding function is given. When an (m, n) encoding function $e : B^m \to B^n$ is given we can find (n, m) decoding function $d : B^n \to B^m$ associated with e.

Definition : The technique used to find d from e is known as **maximum likelihood technique.**

Without going into theoretical part of maximum likelihood technique we shall learn the procedure of obtaining maximum likelihood decoding function with e.

Procedure To Prepare Decoding Table

1. In the first row write all given encoded words starting from 000 ... 00.
2. Then in the first column write the words with weight 1 viz. 00001, 00010, 00100 and so on.
3. Then take the sum of the word on the left and the word at the top and write it in the table and in this way fill up the table.
4. Underline the word to be decoded and find the column.
5. Note the word at the top in that column.
6. Decode that word and thus get the required result.

The following examples will make the procedure easy to understand.

Example 1 : Consider (2, 5) group encoding function $e : B^2 \to B^5$ defined by

$e(00) = 00000$, $e(01) = 01110$, $e(10) = 10101$, $e(11) = 11011$

Decode the following words relative to maximum likelihood function

(i) 11110, (ii) 10011, (iii) 10100. **(M.U. 2007, 17)**

Sol. : We first prepare the blank table in which in the first row we write encoded words 00000, 01110, 10101 and 11011.

In the first column we write the words with minimum weight 1 *i.e.* we write in the first column,

00001, 00010, 00100, 01000, 10000.

Blank Decoding Table

00000	01110	10101	11011
00001			
00010			
00100			
01000			
10000			

Now we take the sum of the words in 2nd, 3rd and 4th column and the word in each row successively.

Thus, we have 01110 + 00001 = 01111, we enter this sum under 01110. Then we take the sum 10101 + 00001 = 10100 and enter it under 10101 and continuing in this way we fill up the table and get the following.

Decoding Table

00000	01110	10101	11011
00001	01111	<u>10100</u>	11010
00010	01100	10111	11001
00100	01010	10001	11111
01000	00110	11101	<u>10011</u>
10000	<u>11110</u>	00101	01011

(i) The received word 11110 is in the second column and is underlined. The word at the top in its column is 01110.

Since by data $e(01) = 01110$, we decode 11110 as 01 *i.e.*, $d(1110) = 01$.

(ii) The received word 10011 is in the fourth column and is underlined. The word at the top in its column is 11011

Since by data $e(11)$ is 11011, we decode 10011 as 11 *i.e.*, $d(10011) = 11$.

(iii) The received word 10100 is in the third column and is underlined. The word at the top is 10101.

Since by data $e(10) = 10101$, we decode 10100 as 10 *i.e.*, $d(10100) = 10$.

Example 2 : Consider (2, 6) group encoding function $e : B^2 \to B^6$ defined by

$e(00) = 000000$; $e(01) = 011110$; $e(10) = 101101$; $e(11) = 110011$.

Decode the following relative to maximum likelihood decoding function.

(i) 001110, (ii) 111101, (iii) 110010 **(M.U. 2012)**

Sol. : We first prepare a blank table in which we write encoded words 000000, 011101, 101101, 110011 in the first row. Now we write the words with minimum weight in the first column and prepare a blank table.

Decoding Table

000000	011110	101101	110011
000001	011110	101100	<u>110010</u>
000010	011100	101111	110001
000100	011010	101001	110111
001000	010110	100101	111011
010000	<u>001110</u>	<u>111101</u>	100011
100000	111110	001101	010011

As explained in the previous example, we get

$d(001110) = 01$, $d(111101) = 10$, $d(110010) = 11$.

Example 3 : Let $H = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$ be a parity check matrix.

Decode the following words relative to maximum likelihood decoding function.

(i) 0101, (ii) 1010, (iii) 1101 **(M.U. 2003, 07)**

Sol. : First we compute the encoding function $e_H : B^2 \to B^4$.

We have $B^2 = \{00, 01, 10, 11\}$

$e(00) = 00\ x_1\ x_2$

$\therefore\ x_1 = 0 \cdot 1 + 0 \cdot 1 = 0, \quad x_2 = 0 \cdot 1 + 0 \cdot 0 = 0$

$\therefore\ e(00) = 0000$

Next $e(01) = 01\ x_1\ x_2$

$\therefore\ x_1 = 0 \cdot 1 + 1 \cdot 1 = 1, \quad x_1 = 0 \cdot 1 + 1 \cdot 1 = 0$

$\therefore\ e(01) = 0110$

Next $e(10) = 10\ x_1\ x_2$

$\therefore\ x_1 = 1 \cdot 1 + 0 \cdot 1 = 1, \quad x_1 = 1 \cdot 1 + 0 \cdot 0 = 1$

$\therefore\ e(10) = 1011$

Next $e(11) = 11\ x_1\ x_2$

$\therefore\ x_1 = 1 \cdot 1 + 1 \cdot 1 = 0, \quad x_1 = 1 \cdot 1 + 1 \cdot 1 = 1$

$\therefore\ e(11) = 1101$

Now prepare the decoding table.

In the first row of the table write all the encoded words *viz.* 0000, 0110, 1011, 1101.

Decoding Table

0000	0110	1011	1101
0001	0111	1010	1100
0010	0100	1001	1111
1000	1110	0011	0101

(i) Now, the received word is 0101 which can be found in 4th column. The word at the top is 1101.

Since $e(11) = 1101$, we decode 0101 as 11.

(ii) The second received word is 1010 which can be found in the third column. The word at the top is 1011.

Since $e(10) = 1011$, we decode 1010 as 10.

(iii) The third received word is 1101 which is located in the fourth column. The word at the top is the same *viz.* 1101.

Since $e(11) = 1101$, we decode 1101 as 11.

Example 4 : *Consider the parity check matrix H given by*

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Decode the following words relative to the maximum likelihood decoding function associated with e_H : 01111, 11001 **(M.U. 1999, 2009)**

Sol. : We first compute encoding function $e_H : B^2 \to B^5$.

Now, $B^2 = \{00, 01, 10, 11\}$

(i) $e(00) = 00\ x_1\ x_2\ x_3$

$x_1 = 0 \cdot 1 + 0 \cdot 0 = 0; \quad x_2 = 0 \cdot 1 + 0 \cdot 1 = 0;$

$x_3 = 0 \cdot 0 + 0 \cdot 1 = 0$

$\therefore\ e(00) = 00000$

(ii) $e(01) = 01\ x_1\ x_2\ x_3$

$x_1 = 0 \cdot 1 + 1 \cdot 0 = 0; \quad x_2 = 0 \cdot 1 + 1 \cdot 1 = 1,$

$x_3 = 0 \cdot 0 + 1 \cdot 1 = 1$

$\therefore\ e(01) = 01011$

(iii) $e(10) = 10\ x_1\ x_2\ x_3$

$x_1 = 1 \cdot 1 + 0 \cdot 0 = 1; \quad x_2 = 1 \cdot 1 + 0 \cdot 1 = 1;$

$x_3 = 1 \cdot 0 + 0 \cdot 1 = 0$

$\therefore\ e(10) = 10110$

(iv) $e(11) = 11\ x_1\ x_2\ x_3$

$x_1 = 1 \cdot 1 + 1 \cdot 0 = 1; \quad x_2 = 1 \cdot 1 + 1 \cdot 1 = 0; \quad x_3 = 1 \cdot 0 + 1 \cdot 1 = 1$

$\therefore\ e(11) = 11101$

Now, we construct the decoding table.

Decoding Table

00000	01011	10110	11101
00001	01010	10111	11100
00010	01001	10100	11111
00100	01111	10010	11001
01000	00011	11110	10101
10000	11011	00110	01101

(i) The received word 01111 is in the second column and is underlined. The word at the top in its column is 01011.

Since $e(01) = 01011$, we decode 01111 as 01 *i.e.* $d(01111) = 01$.

(ii) The received word 11001 is in the fourth column and is underlined. The word at the top in the fourth column is 11101.

Since $e(11) = 11101$, we decode 11001 as 11 *i.e.* $d(11001) = 11$.

Example 4 : Consider the (2, 5) group encoding function $e : B^2 \to B^5$ defined by

$e(0\ 0) = 00000, \quad e(0\ 1) = 01110,$

$e(1\ 0) = 10101, \quad e(1\ 1) = 11011.$

Decode the following words relative to maximum likelihood decoding function

(i) 11110, (ii) 10011, (iii) 10100. **(M.U. 2007, 10)**

Sol. : We first prepare the decoding table.

Decoding Table

00000	01110	10101	11011
00001	01111	10100	11010
00010	01100	10111	11001
00100	01010	10001	11111
01000	00110	11101	10011
10000	11110	00101	01011

(i) The received word 1 1 1 1 0 is in the second column. The word at the top is 0 1 1 1 0.
Since, by data $e(0\,1) = 0\,1\,1\,1\,0$, we decode 1 1 1 1 0 as 0 1
i.e., $d(1\,1\,1\,1\,0) = 0\,1$.

(ii) The received word 1 0 0 1 1 is in the last column. The word at the top is 1 1 0 1 1
Since, by data $e(1\,1) = 1\,1\,0\,1\,1$, we decode 1 0 0 1 1 as 1 1
i.e., $d(1\,1\,0\,1\,1) = 1\,1$.

(iii) The received word 1 0 1 0 0 is in the third column. The word at the top is 1 0 1 0 1.
Since, by data $e(1\,0) = 1\,0\,1\,0\,1$, we decode 1 0 1 0 1 as 1 0
i.e., $d(1\,0\,1\,0\,1) = 1\,0$.

Example 5 : Let $H = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ be the parity check matrix.

Decode the following words relative to maximum likelihood decoding function e_H.
(i) 0 1 1 0 0 1 (ii) 1 0 1 0 0 1 (iii) 1 1 0 1 0 (M.U. 2009, 14)

Sol. : We first compute encoding function $e_H : B^3 \to B^6$.
Since $B = \{0, 1\}$, we have $B^3 = \{000, 001, 010, 100, 101, 110, 111\}$

Now, $e(0\,0\,0) = 0\,0\,0\,x_1\,x_2\,x_3$
$\therefore\ x_1 = 0 \cdot 1 + 0 \cdot 1 + 0 \cdot 0 = 0$
$x_2 = 0 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 = 0$
$x_3 = 0 \cdot 0 + 0 \cdot 0 + 0 \cdot 1 = 0$ $\therefore\ e(0\,0\,0) = 0\,0\,0\,0\,0\,0$.

Now, $e(0\,0\,1) = 0\,0\,1\,x_1\,x_2\,x_3$
$\therefore\ x_1 = 0 \cdot 1 + 0 \cdot 1 + 1 \cdot 0 = 0$
$x_2 = 0 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 = 1$
$x_3 = 0 \cdot 0 + 0 \cdot 0 + 1 \cdot 1 = 1$ $\therefore\ e(0\,0\,1) = 0\,0\,1\,0\,1\,1$

Now, $e(0\,1\,0) = 0\,1\,0\,x_1\,x_2\,x_3$
$\therefore\ x_1 = 0 \cdot 1 + 1 \cdot 1 + 0 \cdot 0 = 1$
$x_2 = 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 = 1$
$x_3 = 0 \cdot 0 + 1 \cdot 0 + 0 \cdot 1 = 0$ $\therefore\ e(0\,1\,0) = 0\,1\,0\,1\,1\,0$.

Now, $e(0\,1\,1) = 0\,1\,1\,x_1\,x_2\,x_3$
$\therefore\ x_1 = 0 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 = 1$
$x_2 = 0 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 0$
$x_3 = 0 \cdot 0 + 1 \cdot 0 + 1 \cdot 1 = 1$ $\therefore\ e(0\,1\,1) = 0\,1\,1\,1\,0\,1$.

Now, $e(1\,0\,0) = 1\,0\,0\,x_1\,x_2\,x_3$
$\therefore\ x_1 = 1 \cdot 1 + 0 \cdot 1 + 0 \cdot 0 = 1$
$x_2 = 1 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 = 0$
$x_3 = 1 \cdot 0 + 0 \cdot 0 + 0 \cdot 1 = 0$ $\therefore\ e(1\,0\,0) = 1\,0\,0\,1\,0\,0$.

Now, $e(1\,0\,1) = 1\,0\,1\,x_1\,x_2\,x_3$
$\therefore\ x_1 = 1 \cdot 1 + 0 \cdot 1 + 1 \cdot 0 = 1$
$x_2 = 1 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 = 1$
$x_3 = 1 \cdot 0 + 0 \cdot 0 + 1 \cdot 1 = 1$ $\therefore\ e(1\,0\,1) = 1\,0\,1\,1\,1\,1$.

Now, $e(1\,1\,0) = 1\,1\,0\,x_1\,x_2\,x_3$
$\therefore\ x_1 = 1 \cdot 1 + 1 \cdot 1 + 0 \cdot 0 = 0$
$x_2 = 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 = 1$
$x_3 = 1 \cdot 0 + 1 \cdot 0 + 0 \cdot 1 = 0$ $\therefore\ e(1\,1\,0) = 1\,1\,0\,0\,1\,0$.

Now, $e(1\,1\,1) = 1\,1\,1\,x_1\,x_2\,x_3$
$\therefore\ x_1 = 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 = 0$
$x_2 = 1 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 0$
$x_3 = 1 \cdot 0 + 1 \cdot 0 + 1 \cdot 1 = 1$ $\therefore\ e(1\,1\,1) = 1\,1\,1\,0\,0\,1$

Decoding Table

000000	001011	010110	011101	100100	101111	110010	111001
000001	001010	010111	011100	100101	101110	110011	111000
000010	001001	010100	011111	100110	101101	110000	111011
000100	001111	010010	011001	100000	101011	110110	111101
001000	000011	011110	010101	101100	100111	111010	110001
010000	011011	000110	001101	110100	111111	100010	101001

(i) Now, the received word is 011001. The word at the top is 011101
Since $e(011) = 011101$. We decode 011001 as 011.
i.e., $d(011001) = 011$.

(ii) The received word is 101001. The word at the top is 111001
Since $e(111) = 111001$. We decode 1110011 as 111.
i.e., $d(111001) = 111$.

(iii) The received word is 111010. The word at the to is 110010.
Since $e(110) = 110010$. We decode 111010 as 110.
i.e., $d(111010) = 111$.

Example 6 : Consider the (3, 5) group encoding function $e : B^3 \to B^5$ defined by

$e(000) = 00000$, $e(100) = 10011$, $e(001) = 00110$,
$e(101) = 10101$, $e(010) = 01001$, $e(110) = 11010$,
$e(011) = 01111$, $e(111) = 11100$.

Decode the following words relative to maximum likelihood decoding function,

(a) 11001, (b) 01010, (c) 00111. **(M.U. 2009, 10, 13, 15)**

Sol. :

Decoding Table

00000	00110	01001	01111	10011	10101	11010	11100
00001	00111	01000	01110	10010	10100	11011	11101
00010	00100	01011	01101	10001	10111	11000	11110
00100	00010	01101	01011	10111	10001	11110	11000
01000	01110	00001	00111	11011	11101	10010	10100
10000	10110	11001	11111	00011	00101	01010	01100
10001	10111	11000	11110	00010	00100	01011	01101
10010	10100	11011	11101	00001	00111	01000	01110

(i) The received word 11001 is in the third column and is underlined. The word at the top in its column is 01001.

Since by data $e(010) = 01001$, we decode 11001 as 010

i.e., $d(11001) = 010$

(ii) The received word 01010 is in the seventh column and is underlined. The word at the top is 11010.

Since by data $e(110) = 11010$ we decode 01010 as 110

i.e., $d(01010) = 110$

(iii) The received word 00111 is in the second column and is underlined. The word at the top in its column 00110.

Since by data $e(001) = 00110$ we decode 00111 as 001

i.e., $d(00111) = 001$.

EXERCISE - VI

1. Consider the (3, 6) encoding function $e : B^3 \to B^6$ defined by
   $e(000) = 000000$, $e(001) = 001100$, $e(010) = 010011$,
   $e(011) = 011111$, $e(100) = 100101$, $e(101) = 101001$,
   $e(110) = 110110$, $e(111) = 111010$.
   Decode the following word 000101. **[Ans. : 100]**
2. Consider the (3, 6) group encoding function $e : B^3 \to B^6$ defined by
   $e(000) = 000000$, $e(001) = 000110$, $e(010) = 010010$,
   $e(011) = 010100$, $e(100) = 100101$, $e(101) = 100011$,
   $e(110) = 110111$, $e(111) = 110001$.
   Decode (i) 110010, (ii) 101101, (iii) 101011. **[Ans. : (i) 010, (ii) 100, (iii) 101]**

3. Let $H = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ be a parity check matrix.

Decode the following words relative to a maximum likelihood decoding function c_H.

(i) 011 001, (ii) 101001, (iii) 111010. **(M.U. 1997, 2005, 14)**

[Ans. : (i) 011, (ii) 111, (iii) 110]

EXERCISE - VII

Theory

1. Define a group. What is a commutative group ? Give an example of a group which is not commutative. **(M.U. 1998)**
2. In a group $(G, *)$, prove that
   (i) identity is unique **(M.U. 1997)**
   (ii) inverse is unique. **(M.U. 2002)**
   (iii) $(a^{-1})^{-1} = a$ for all $a \in G$.
   (iv) $(a^{-1} * b^{-1}) = b^{-1} * a^{-1}$ for all $a, b \in G$.
3. State and prove that in a group, left cancellation and right cancellation laws hold. **(M.U. 1999)**
4. Define Homomorphism and Isomorphism of groups. **(M.U. 1999)**
   Give an example of each. **(M.U. 2003)**
5. Give examples of binary operations $*_1$, $*_2$, $*_3$ and $*_4$ on Z such that
   (i) $*_1$ is commutative but not associative.
   (ii) $*_2$ is associative but not commutative.
   (iii) $*_3$ is neither associative nor commutative.
   (iv) $*_4$ is both associative and commutative. **(M.U. 2001)**

   [Ans. : (i) $a * b = \frac{a+b}{2}$ is commutative but not associative.
   (ii) $a * b = a \times |b|$ is associative but not commutative.
   (iii) Usual subtraction or usual division is neither associative, nor commutative.
   (iv) Usual addition or multiplication is both associative and commutative. **]**
6. State with justification whether the following statement is true or false.
   Both addition and multiplication are binary operations on $A = \{-1, 0, 1\}$. **(M.U. 2001)**
   [Ans. : Prepare + and × tables. + is not binary; × is *. **]**
7. Give examples of the following with proper justification.
   (i) An Abelian group having 6 elements.
   (ii) Binary operation on Z which is commutative but not associative. **(M.U. 2002)**

   [Ans. : (i) Let $G = \{0, 1, 2, 3, 4, 5\}$ and let * be addition modulo 5. Then $A(G, *)$ is an Abelian group.

(ii) Let • be defined on Z as $a \bullet b = ab + |a| + |b|$. Then • is commutative but not associative.]

8. State true or false with proper justification.

(i) If $S = \{[2], [4], [6], [8]\}$ then S has no identity element under multiplication modulo 10. (Where [2], [4], ... denote the set of integers congruent to 2, 4, ... modulo 10).

(ii) Inverse of an element in a group is unique.

(iii) Field cannot have finite number of elements. **(M.U. 2002)**

[Ans. : (i) Prepare the table for $A = \{2, 4, 6, 8\}$ multiplication modulo 10. From the third column (under 10) we see that 6 is the identity element. Hence, false.

(ii) True.

(iii) False.]

9. Give an example of (i) Non-abelian group, (ii) Abelian group of order 4. **(M.U. 1998)**

[Ans. : (i) G is the set of rational numbers different from 1

$a \bullet b = a + b - ab$.

(ii) $G = \{1, 2, 3, 4\}$ is an Abelian group under multiplication modulo 5.]

10. State true or false :- If • is a binary operation on real numbers as $a \bullet b = \frac{a+b}{2}$ then it is associative. **(M.U. 2002) [Ans. : False]**

11. Explain congruence relation with an example. **(M.U. 2009)**

12. Define the following terms with proper illustrations

(1) Semigroup	**(M.U. 199, 2000, 09, 10, 16)**
(2) Monoid	**(M.U. 1999, 2000, 09, 10, 16)**
(3) Group	**(M.U. 2000, 01, 09, 10, 16)**
(4) Congruence Relation	**(M.U. 2009, 13)**
(5) Commutative Group	**(M.U. 2002)**
(6) Cyclic Group	**(M.U. 1999, 2000)**
(7) Subgroup	**(M.U. 2001, 02, 04, 05, 10)**
(8) Coset	**(M.U. 1998, 2001)**
(9) Normal Subgroup	**(M.U. 2000, 02, 05, 07, 10)**
(10) Quotient Group	**(M.U. 2000)**
(11) Isomorphism	**(M.U. 1999)**
(12) Group Codes	**(M.U. 1999, 2000, 05)**
(13) Minimum distance of an encoding function	**(M.U. 1998, 99)**

✣ ✣ ✣