Unit V

5 Trees

5.1 : Introduction

Q.1 Define tree with examples.

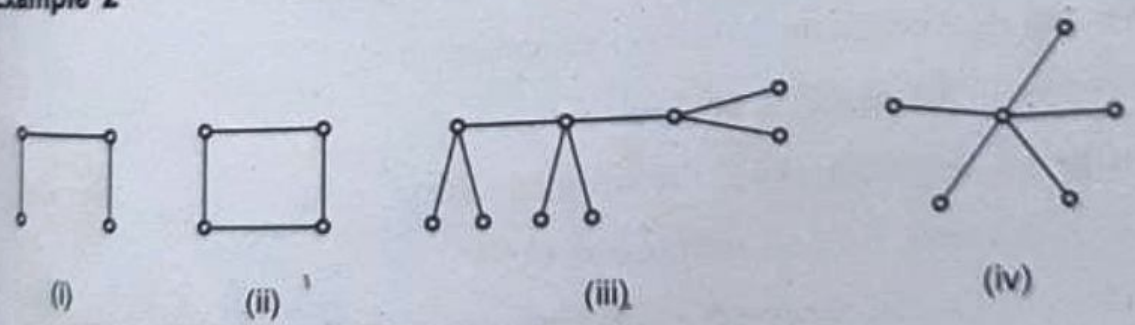
Ans. : A tree is a connected graph without any circuit i.e. tree is a connected acyclic graph. The collection or set of an acyclic graphs. (not necessarily connected) is called a forest.

Examples :

Example 1

All these three graphs are trees. There are unique tree on one vertex, 2 vertices and 3 vertices.

Example 2



Graphs (i), (iii) and (iv) are trees but (ii) is not a tree as it has a cycle.

A) A vertex of degree 1 in a tree is called a **leaf** or a **terminal node.** A vertex of a degree greater than one is called a **branch node** or **internal node.**

e.g. In a tree

c, d and e are leaves or terminal nodes and a, b, c are branch nodes.

B) Some properties of tree are obvious

i) Every edge of a tree is an isthmus. Conversely if every edge in a connected graph G is an isthmus then G is a tree.

ii) Every tree is a simple graph because loops and multiple edges field cycles.

iii) Every tree is a bipartite graph with $n \geq 2$ vertices.

Theorem 1 : A graph G is a tree iff there exists a unique path between every distinct pair of vertices of G.

Proof : Suppose G is a tree. So G is a connected and without circuits. We know that a circuit forms two or more paths. But G has no circuits so it has unique path between every pair of vertices.

Conversely assume that there is a unique path between every pair of vertices in G. This implies that G is a connected and G has no cycles. i.e. G is a connected acyclic graph.

Therefore G is a tree.

Theorem 2 : A graph G on n vertices is a tree iff G is connected and has exactly $n - 1$ edges.

Proof : Suppose graph G is a tree. Therefore is a connected and acyclic graph.

It is sufficient to prove that G has $n - 1$ edges only.

We can prove this by induction principle on n.

For $n = 1$, the result is obvious

Let $n > 1$, consider $G - e'$ for any $e' \in E(G)$

As G is a tree, e' is an isthmus of G.

$\therefore G - e'$ is a disconnected graph with two components say G_1 and G_2.

Now G_1 and G_2 are connected and a cyclic graphs as G_1 and G_2 are subgraph of G.

Let G_1 has n_1 vertices and m_1 edges and G_2 has n_2 vertices and m_2 edges

$\therefore$ By induction principle

$$m_1 = n_1 - 1 \quad \text{and} \quad m_2 = n_2 - 1$$

Therefore the number of edges in G is given by

$$e = (e_1 + e_2) + 1 = n_1 - 1 + n_2 - 1 + 1$$

$$= n_1 + n_2 - 1$$

$$e = n - 1 \qquad (\because n = n_1 + n_2)$$

Hence G has $n - 1$ edges only.

Conversely assume that G is connected graph and has exactly $n - 1$ edges.

Claim : Prove that G is a tree.

It is suffices to prove that G is noncyclic graph.

Suppose G contains a cycle C.

Let P denote the number of vertices in C

$\therefore$ The number of edges in $C = P$

As G is connected graph, the remaining $n - P$ vertices must be connected to vertices in C. To connect each vertex of G which is not in C, we required $n - P$ edges as each edge of G can connect only one vertex to the vertices in C.

Hence the total number of edges in G is given by

$$e = (n - P) + P = n \Rightarrow e = n \text{ which is contradiction}$$

$\therefore$ G has $n - 1$ edges only.

Thus G is a tree.

Theorem 3 : Let G be a graph with n vertices and m edges. If any of the following is true then all are true.

i) G is a tree.

ii) G is connected and $m = n - 1$

iii) G is acyclic graph and $m = n - 1$

iv) Every edge of G is an isthmus and G is connected.

v) There is exactly one path between every pair of vertices in G.

Theorem 4 : A non trivial tree contains at least two vertices of degree 1. (i.e. pendent vertices)

Proof : Let G be a tree with n vertices, so G is connected.

$\therefore \quad d(x) \geq 1 \; ; \; \forall x \in V(G)$

By handshaking lemma

$$\sum_{x \in V(G)} d(x) = 2 \times \text{Number of edges in } G = 2(n-1)$$

Suppose there is no vertex of degree 1.

Then $\quad 2n \leq \sum_{x \in V(G)} d(x) = 2n - 2$

i.e. $2n \leq 2n - 2 \Rightarrow n \leq n - 1$ which is impossible.

Thus there is at least one vertex of degree 1.

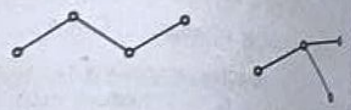
By a similar argument there is one more vertex of degree 1.

Hence every tree has at least two pendent vertices.

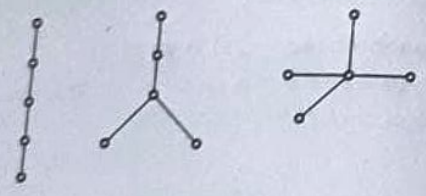
Q.2 Draw all non isomorphic trees on 4 and 5 vertices.

Ans. :

a) Non isomorphic trees on 4 vertices



b) Non isomorphic trees on 5 vertices



Q.3 Under what conditions trees are the complete bipartite graphs.

Ans. : Suppose T is a tree which is the complete bipartite graph.

Let $\quad T = K_{m,n}$

$\therefore$ T has $m + n$ vertices and $(m+n-1)$ edges.

But $K_{m,n}$ has $m \cdot n$ number of edges.

Therefore $\quad mn = m + n - 1$

$$mn - m - n + 1 = 0$$

$$(m-1)(n-1) = 0.$$

$m = 1$ or $n = 1$

or $\quad m = 1$ and any n $\quad$ or $\quad n = 1$ and any m

i.e. Hence $K_{1,n}$ and $K_{m,1}$ are the only complete bipartite graphs. These are known as star graphs.

Thus T is a star graph.

Q.4 a) Is it possible to draw a tree with 10 vertices which has vertices either of degree 1 or 3 ? If possible draw tree. Is it possible to draw same type of tree with 13 vertices ?

b) For which values of n (number of vertices), such type of tree exist ?

Ans. : a) Given that tree T has 10 vertices so it must have 9 edges.

Let x and y be the number of vertices of degree 1 and 3 in T respectively.

$$x + y = 10 \qquad \text{... (Q.4.1)}$$

$\therefore$ By handshaking lemma

$$\sum_{v \in V(T)} d(v) = 2(\text{Number of edges in T})$$

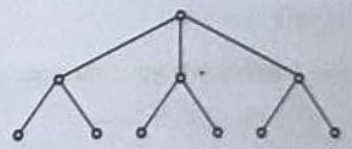
$$x + 3y = 2 \times 9 = 18$$

$$x + 3y = 18 \qquad \text{... (Q.4.2)}$$

Solving equations (Q.4.1) and (Q.4.2) we get

$$y = 4 \quad \text{and} \quad x = 6$$

Therefore there are 6 vertices of degree 1 and 4 vertices of degree 3. Such type of graph is given below.



Now consider a tree with 13 vertices and 12 edges.

By using similar theory, we get

$$x + y = 13 \qquad \text{... (Q.4.3)}$$

$$x + 3y = 24 \qquad \text{... (Q.4.4)}$$

Solving (Q.4.3) and (Q.4.6), we get $3y = 11 \Rightarrow y = \frac{11}{2}$ and $x = \frac{17}{2}$ which is impossible.

Therefore it is not possible to draw such type of tree.

b) Let T be a tree with n vertices.

Let x and y be the number of vertices of degree 1 and 3 respectively. T has n – 1 edges.

Therefore $\quad x + y = n$

By handshaking lemma $\quad x + 3y = 2(n-1)$

$$x + 3y = 2n - 2$$

Equation (Q.4.6) – Equation (Q.4.5) $\Rightarrow 2y = 2n - 2 - n$

$$2y = n - 2$$

$$\Rightarrow \quad y = \frac{n-2}{2} = \frac{n}{2} - 1$$

$$\Rightarrow \quad x = n - y = n - \frac{n}{2} + 1 = \frac{n}{2} + 1$$

i.e. $x = \frac{n}{2} + 1$ and $y = \frac{n}{2} - 1$. These should be non negative integers.

Case 1 : If n is even then $x = \frac{n}{2}$ is odd

and $\frac{n}{2} + 1 = x$ is an even integer

$\frac{n}{2} - 1 = y$ is an even integer

Thus the tree exists with required condition on even number of vertices. $T_2, T_4, T_6, T_8 \ldots T_{2n}$ are such type of trees.

Case 2 : If n is odd then $\frac{n}{2}$ is not an integer there x and y are not an integer.

Hence the required tree does not exist on odd number of vertices.

Q.6 Explain centre of a tree.

Ans. : We know that the distance between two vertices in a connected graph i.e. is a length of the shortest path between that vertices. Before defining centre of a tree first find the distance between vertices of a tree which is defined as follows :

Eccentricity of a Vertex

Let G be a connected graph G and $v \in V(G)$. The eccentricity of a vertex v is denoted by E(v) or e(v) and defined as the distance from v to the vertex farthest from v in G.

i.e. $E(v)$ or $e(v) = \max\{d(v, v_i) \mid \forall v_i \in v(G)\}$

Centre of a Graph

A vertex in a graph G with minimum eccentricity is called a centre of G and it's eccentricity is called as radius of G. It is denoted by r(G).

Q.8 Prove that every tree has either one or two centres.

Ans. :

Proof : Let T be a tree. Then e(v) for a vertex v is at a vertex farthest from v. As T is a tree, it is attained at a pendent vertex.

We know that every non trivial tree has at least two pendent vertices. Now, delete all pendent vertices from G, we get new graph G' which is also a tree. Moreover as one edge at each pendent vertex is removed, the eccentricity of any vertex will be reduced by one. Therefore centres of G will still remain centres of G'. We continue the process with G' until we arrive at K_2 or K_1. K_2 has two centres and K_1 has one centre. Hence the proof.

Q.7 Define cut vertex of a tree.

Ans. : We know that the vertex v whose removal from a connected graph G, disconnects the graph is called as cut vertex of G.

In any tree all vertices except pendent vertices are cut vertices.

Solving (Q.4.3) and (Q.4.4), we get $1y = 11 \Rightarrow y = \frac{11}{2}$ and $x = \frac{15}{2}$ which is impossible.

Therefore it is not possible to draw such type of tree.

b) Let T be a tree with n vertices.

Let x and y be the number of vertices of degree 1 and 3 respectively. T has n – 1 edges.

Therefore $x + y = n$

By handshaking lemma $x + 3y = 2(n-1)$ ...(Q.4.5)

$$x + 3y = 2n - 2 \quad \text{...(Q.4.6)}$$

Equation (Q.4.6) – Equation (Q.4.5) $\Rightarrow 2y = 2n - 2 - n$

$$2y = n - 2$$

$$\Rightarrow \quad y = \frac{n-2}{2} = \frac{n}{2} - 1$$

$$\Rightarrow \quad x = n - y = n - \frac{n}{2} + 1 = \frac{n}{2} + 1$$

i.e. $x = \frac{n}{2} + 1$ and $y = \frac{n}{2} - 1$. These should be non negative integers.

Case 1 : If n is even then $x = \frac{n}{2}$ is odd

and $\frac{n}{2} + 1 = x$ is an even integer

$\frac{n}{2} - 1 = y$ is an even integer

Thus the tree exists with required condition on even number of vertices. $T_2, T_4, T_6, T_8 \ldots T_{2n}$ are such type of trees.

Case 2 : If n is odd then $\frac{n}{2}$ is not an integer there x and y are not an integer.

Hence the required tree does not exist on odd number of vertices.

Q.5 Explain centre of a tree.

Ans. : We know that the distance between two vertices in a connected graph i.e. is a length of the shortest path between that vertices. Before defining centre of a tree first find the distance between vertices of a tree which is defined as follows :

Eccentricity of a Vertex

Let G be a connected graph G and $v \in V(G)$. The eccentricity of a vertex v is denoted by E(v) or e(v) and defined as the distance from v to the vertex farthest from v in G.

i.e. $E(v)$ or $e(v) = \max\{d(v, v_i) / \forall v_i \in v(G)\}$

Centre of a Graph

A vertex in a graph G with minimum eccentricity is called a centre of G and it's eccentricity is called as radius of G. It is denoted by r(G).

Q.6 Prove that every tree has either one or two centres.

Ans. :

Proof : Let T be a tree. Then e(v) for a vertex v is at a vertex farthest from v. As T is a tree, it is attained at a pendent vertex.

We know that every non trivial tree has at least two pendent vertices. Now, delete all pendent vertices from G, we get new graph G′ which is also a tree. Moreover as one edge at each pendent vertex is removed, the eccentricity of any vertex will be reduced by one. Therefore centres of G will still remain centres of G′. We continue the process with G′ until we arrive at K_2 or K_1. K_2 has two centres and K_1 has one centre. Hence the proof.

Q.7 Define cut vertex of a tree.

Ans. : We know that the vertex v whose removal from a connected graph G, disconnects the graph is called as cut vertex of G.

In any tree all vertices except pendent vertices are cut vertices.

Q.8 Define rooted tree and binary tree.

Ans. : A connected acyclic, directed graph is called a directed tree. In other words, a directed graph is said to be a directed tree if it becomes a tree when the directions of the edges are ignored.

Q.9 Define rooted tree.

Ans. : A directed tree is called a **rooted tree** if there is exactly one vertex whose incoming degree is zero and the incoming degree of all other vertices are one.

The vertex with incoming degree 0 is called **the root** of the rooted tree.

The vertex whose outgoing degree is zero is called **leaf** or **terminal node**.

A vertex whose outgoing and incoming degrees are non zero is called **branch note** or an **internal node.** Consider the following example.

Q.10 Define level and height of a tree.

Ans. : A vertex v in a rooted tree is said to be at **level n** if there is a path of length n from the root to the vertex v.

The **height** of the tree is the maximum of the levels of its vertices.

Example

In the given graph G .... a is a root

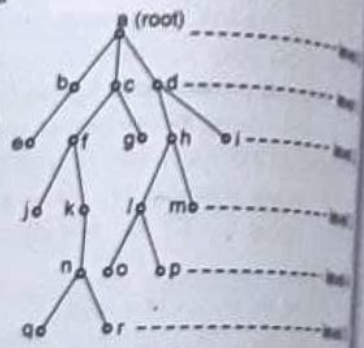
Vertices b, c, d are at level 1

Vertices e, f, g, h and i are at level 2

Vertices j, k, l and m are at level 3

Vertices n, o and p are at level 4

Vertices q and r are at level 5



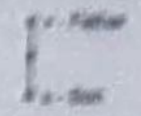
G

The maximum level is 5.

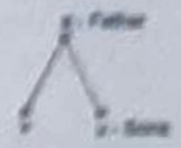
Therefore the height of tree is 5.

Rules for rooted tree : In a rooted tree

i) If the level of a vertex u is greater than the level of vertex v then u is below v.



ii) If vertex u is below vertex v and there is an edge from v to u then u is said to be son of v (or child of v) and v is said to be the father of u (or parent of u) i.e.

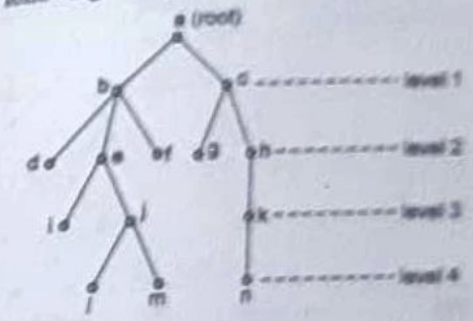


iii) Two vertices u and v are said to be brothers if they are the sons of the same vertex.

iv) A leaf is a vertex without children.

v) If $p = \{a, v_1, v_2, v_3, \ldots, v_{n-1}, b\}$ is a path from a to b then b is called as descendent of a and a is called as ancestor of b.

Consider the following example



From above figure i) a is a root of the tree.

ii) b and c lie at level 1. ∴ b and c are sons of root a i.e. a is father of b and c and b and c are brothers.

iii) b has three sons d, e, f

∴b is a father of d, e, f

c has 2 sons g and h

iv) e has two sons i and j

h has only one son k

v) i has no son j has two sons l and m. So k and l are brothers. k has one son n. n has no brother as n is a leaf.

l, m, n are known as descendent of a and a is ancestor of d, e, f, g, h, i, j, k, l, m, n and so on.

Q.11 Define subtrees.

Ans. : Let T be a rooted tree and $x \in V(T)$.

A vertex x together will all its descendants is called the **subtree** of T rooted at x.

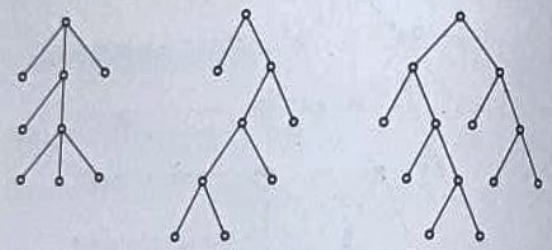
The subtree corresponding to the root node is the **entire tree.** The subtree corresponding to any other node is called a **proper subtree.**

Q.12 Define M-ary trees.

Ans. : A rooted tree in which every interior node has at most m sons is called an **m-ary tree.**

A m-ary tree is said to be **regular m-ary tree** or full m-ary tree if every branch node has exactly m sons.

Consider the following examples.



3 - ary tree 2 - ary tree Full 2 - ary tree

Q.13 A regular m-ary tree with p interior nodes has mp + 1 nodes at all. ☞ **[SPPU : Dec.-09]**

Ans. :

Proof : Let T be a regular m-ary tree with n vertices. Out of n vertices there are p interior vertices or branch nodes.

Therefore there are $t = n - p$ number of sons or leaves in T.

But given graph is regular and p interior nodes.

So the regular m-ary tree will have mp sons.

But root is not a son.

Therefore give tree has total (mp + 1) number of vertices

Hence

$$\boxed{n = mp + 1}$$

5.2 : Binary Tree

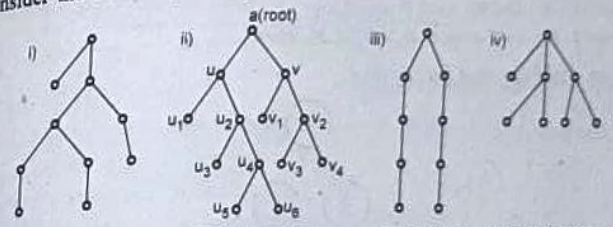
Q.14 Explain binary tree. ☞ **[SPPU : Dec.-09, May-10, 12]**

Ans. : An m-ary tree is known as **binary tree** if every branch node has at most 2 sons.

In other words, a tree in which there is exactly one vertex of degree 2 and each of the remaining vertices of degree or three, is called a binary tree.

A binary tree is called as **regular binary tree** or **full binary tree** if every branch node has exactly 2 sons or zero son.

Consider the following examples



Binary tree Full binary tree Binary tree Not binary tree

In binary trees, instead of referring the first or second subtree of a branch node, we use to the left subtree or right subtree of the node.

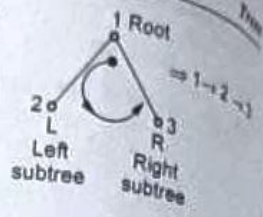
5.3 : Tree Traversal

Q.15 Explain binary tree traversal with examples.

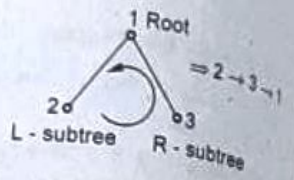
Ans. : Traversing means visiting or processing all the nodes of a tree. A binary tree traversal is the visiting of each node of a tree only once according to some sequence.

There are two types of traversing binary trees.

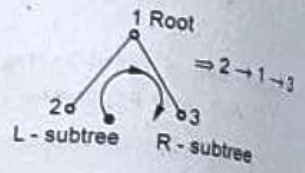
1) Depth-first traversal : In this method, the processing proceeds from the root or the most distant descendent of the first child. There are three types of Depth-First Traversal.



A) Pre order traversal : In this traversal, the root node is traversal first, followed by the left subtree and then the right subtree as shown below.



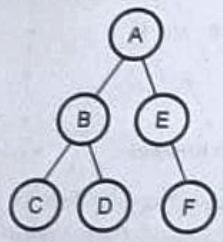
B) Post order traversal : If processes first the left subtree then the right subtree and then at the last root of the tree as shown below.



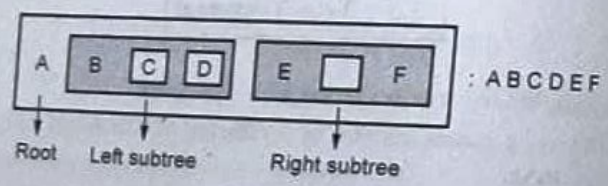
C) In order traversal : It processes the left subtree first then the root and at the last right subtree.

The prefix "in" means root is processed in between the subtrees. It is shown as below.

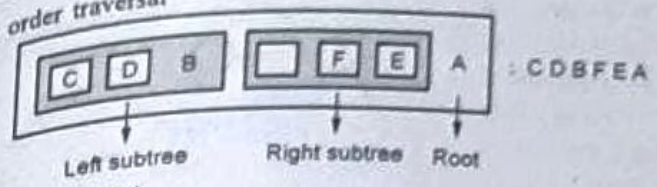
Consider the following binary tree.



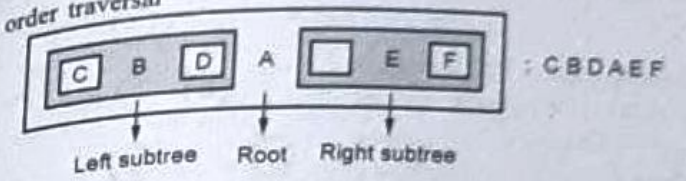
i) Pre order traversal



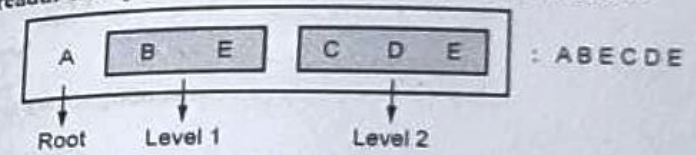
ii) Post order traversal



iii) In order traversal



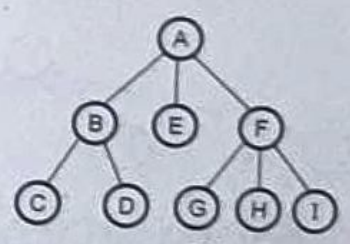
2) Breadth first traversal : In this traversal, the processing proceeds horizontally from the root of all of its children, then to its childre's children and so on until all the nodes have been processed. That is first write node of zero level, then all nodes of level 1 then level 2 and so on. The breadth first process for the above binary is shown below.



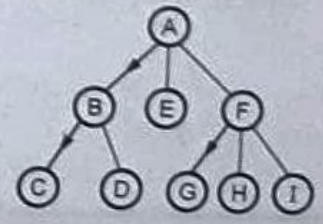
Q.16 Explain conversion of general tree to binary tree.

Ans. : Let us explain the method to convert general tree to binary tree with the help of the following example.

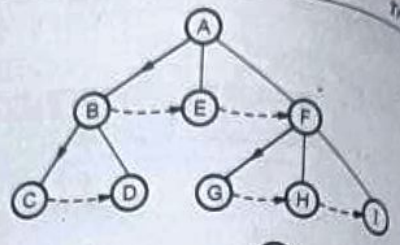
Consider the following steps



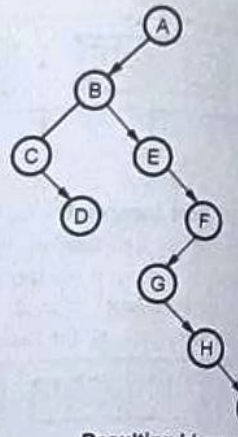
Step 1) To convert it into binary tree, we first identify the branch from the parent to its first or left most child. These branches from each parent become left pointers in the binary tree.



Step 2) Connect sibling, starting with the left most or first child, using a branch for each sibling to its right sibling. They are the right pointers in the binary tree.

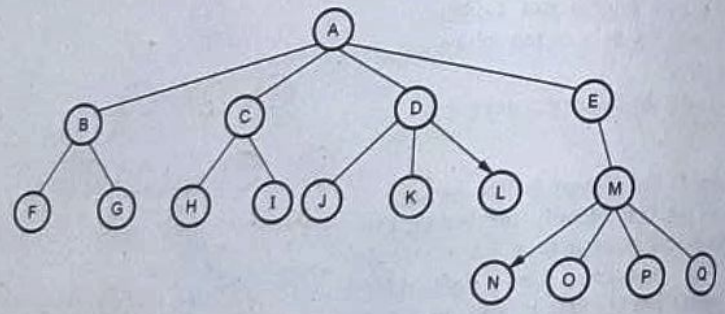


Step 3) Now remove all unneeded branches from the parent to its children. Therefore remove $A \to E$, $B \to D$, $A \to F$, $F \to H$, $F \to I$ we get the following required binary tree.

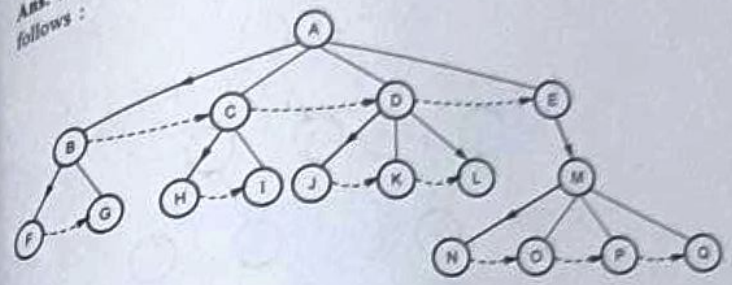


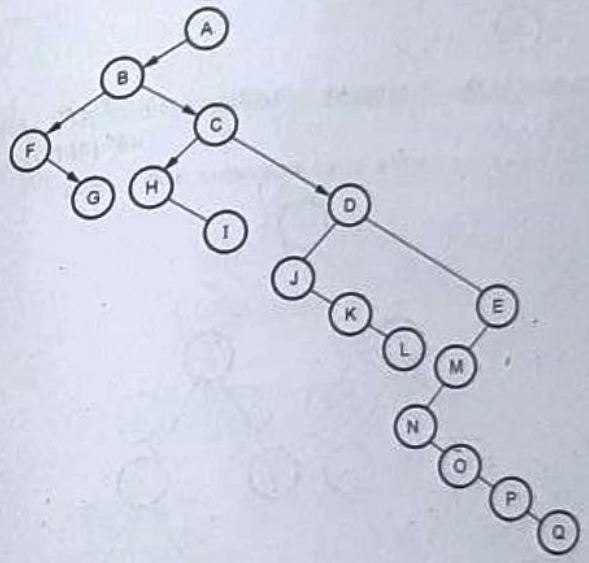
Resulting binary tree

Q.17 Convert the following tree into binary tree. ☞ **[SPPU : Dec.-09]**



Ans. : The steps involve to convert the given tree into binary tree are as follows :



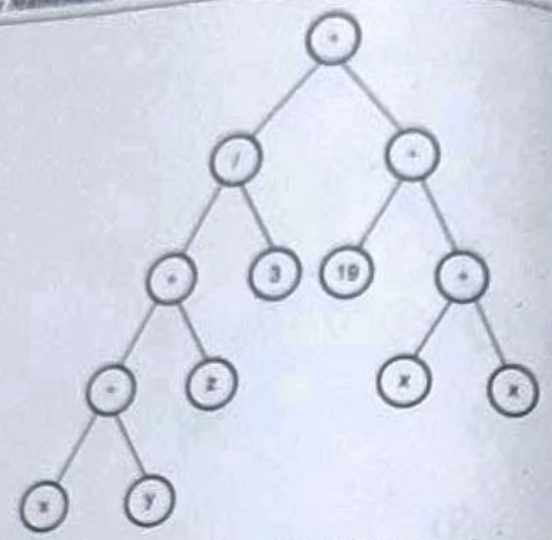


Binary tree

Q.18 Construct the labeled tree of the following algebraic expression ☞ **[SPPU : May-10]**

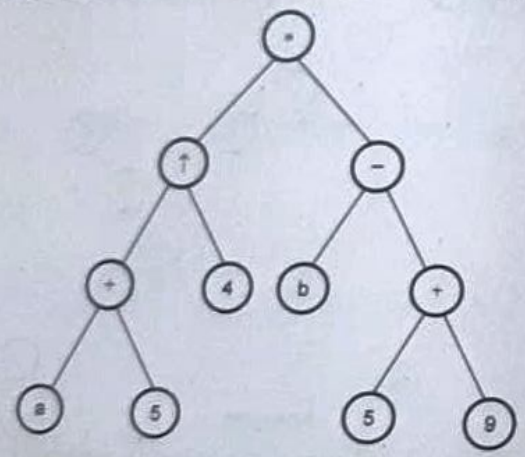
$(((x+y)*z)/3)+(19+(x*x))$

Ans. : The expression tree for the given algebraic expression is given below :

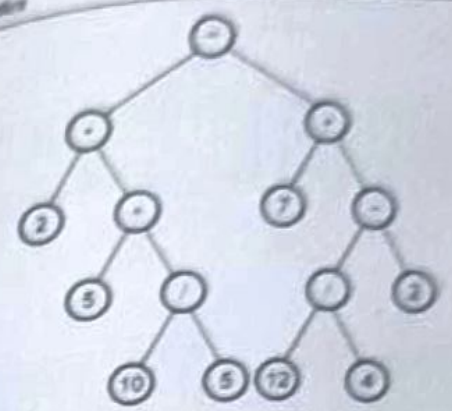


Q.19 Represent the expression $((a+5)\uparrow 4)*(b-(5+9))$ using a binary tree. **[SPPU : May-12]**

Ans. : The binary tree for the given expression is as follows :



Q.20 Write and evaluate the expression tree shown below. **[SPPU : Dec.-09]**

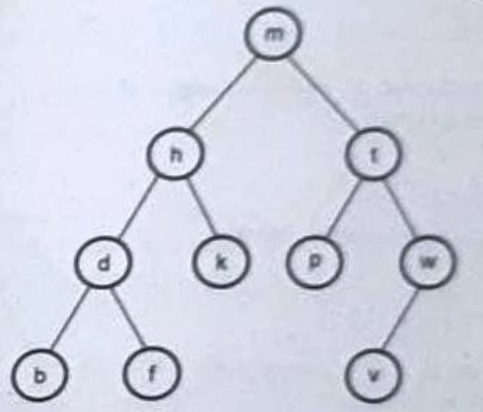


Ans. : The algebraic expression of the given binary tree is,

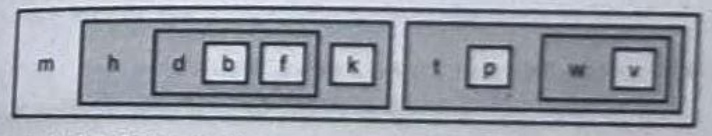
$(2*((5)+(10/5))) - ((7)*(((12/4)-(2))))$

Its value is $2*(5+2)-(7*(3-1)) = 14 - 7 = 14$

Q.21 Find the preorder, postorder and inorder traversal of the following tree. **[SPPU : May-10]**

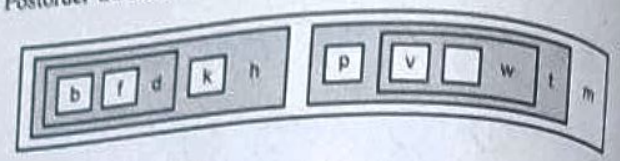


Ans. : i) Preorder traversal



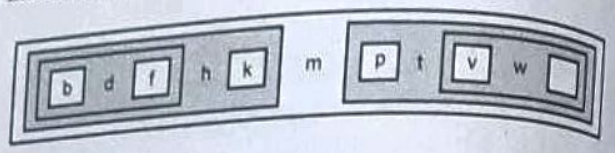
i.e. m b d b f k t p w v

ii) Postorder traversal



i.e. b f d k h p v w t m

iii) Inorder traversal



i.e. b d f h k m p t v w

Out of which 2^h are leaves.

Hence internal vertices $= (2^{h+1}-1)-2^h$

$= 2^h(2-1)-1$

$= 2^h - 1$

Q.22 Find the maximum of possible height of a binary tree with 13 vertices and draw graph.

Ans. :

We have $n = 13$

The maximum possible height of the binary tree is

$$\frac{n-1}{2} = \frac{13-1}{2} = 6$$

The required graph as shown in Fig. Q.22.1.

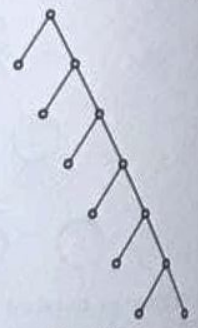


Fig. Q.22.1

Q.23 Define prefix code and binary search trees.

[SPPU : Dec.-12, 14, 15, May-08, 19]

Ans. : 1) A set of sequences is said to be a **prefix code** if no sequences in the set is a prefix of another sequence in the set.

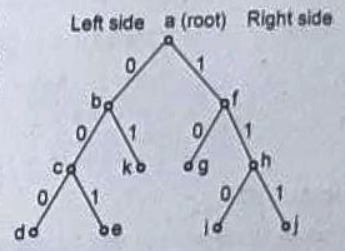
For example the set {000, 001, 01, 10, 11} is a prefix code as no sequence of symbols is present at the beginning of another sequences. All these sequence are distinct.

The set {1, 00, 000, 0001} is not a prefix code because the sequence 00 is the prefix of the sequences 000 and 0001.

A question comes in everyone's mind "How to construct prefix code to a full binary trees ?"

We can solve this question by adding some flavours and binary codes to a full binary trees.

For a given full binary tree, we label the two branches incident from each internal node with 0 and 1. For the left branch we assign 0 and for the right branch we assign 1 of every rooted tree or subtree. Consider the following example of full binary tree.



In given figure root a has 2 sons. Left son is ab and right is af, so assign 0 to ab and 1 to af. Now b has two sons. Assign 0 to left son be and 1 to right son bk. Similarly assign 0 or 1 to every edge of a tree.

Now assign to each leaf, a sequence of 0's and 1's which is the sequence of labels of the edges in the path from the root to the leaf.

For example, d is a leaf and the path a to d is a – b – c – d and their respective labels are 0 – 0 – 0 so the prefix code of d is 000.

For leaf e, path is a – b – c – e and labels 0 – 0 – 1

∴ The prefix code of e is 001

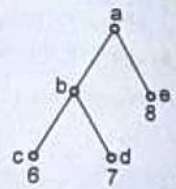
Thus the prefix code of above tree is {000, 001, 01, 10, 110, 111}.

2) Optimal Tree

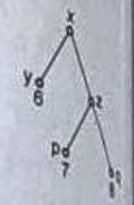
Let T be any full binary tree and $W_1, W_2, W_3, \ldots W_t$ be the weights of the leaves (terminal vertices) then the weight W of the full binary tree is given by

$$W(T) = \sum_{i=0}^{t} W_i l_i$$

Where $l_i = l(i)$ is the length of the path of the leaf i from the root of the tree. The full binary tree is called an optimal tree if its weight is minimum.



T_1



T_2

For example, suppose 6, 7, 8 are the weights of the leaves in a full binary tree as given below.

In T_1, $l(c) = 2$, $l(d) = 2$, $l(e) = 1$

$\therefore$ The weight of T is given by

$$W(T_1) = 6 \times l(c) + 7 \times l(d) + 8 \times l(e)$$
$$= 6 \times 2 + 7 \times 2 + 8 \times 1$$
$$= 12 + 14 + 8 = 34$$

In T_2, $l(y) = 1$, $l(p) = 2$, $l(q) = 2$

$$\therefore \quad W(T_2) = 6 \times 1 + 7 \times 2 + 8 \times 2$$
$$= 6 + 14 + 16 = 36$$

Hence $W(T_1) < W(T_2)$

Thus T_1 is the optimal tree for the weights 6, 7, 8.

Q.24 Explain Huffman algorithm to find an optimal tree.

Ans. : Let $W_1, W_2, W_3, \ldots W_t$ be the weights of the leaves and it is required to construct an optimal binary tree.

The following steps of an algorithm gives the required optimal binary tree.

Step 1 : Arrange the weights in increasing order

Step 2 : Consider two leaves with the minimum weights W_1 and W_2. Replace these two leaves and their father by a leaf. Assign weight $W_1 + W_2$ to this new leaf.

Step 3 : Repeat the step 2 for the weights $W_1, W_2, W_3, \ldots W_t$ until no weight remains.

Step 4 : The tree obtained in this way is an optimal tree for given weights and stop.

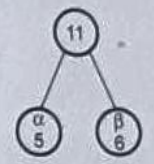
Q.25 For the following set of weights construct optimal binary prefix code. $\alpha - 5, \beta - 6, \gamma - 6, \delta - 11, \in - 20$ **[SPPU : Dec.-14]**

Ans. : Here we use Huffman's coding method.

Step 1 : Sort the weights or frequencies of the given letters in increasing order in a queue.

α	β	γ	δ	$\in$
5	6	6	11	20
↑	↑			

{↑ indicates the first 2 smallest weights}



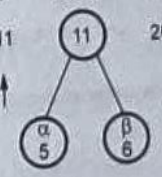
Consider the two symbols with lowest weights say α, β. The root of the first subtree has a weight

$5 + 6 = 11$.

As $6 < 11$, it can not be placed at the beginning. It has to be placed an appropriate position means after δ. The first subtree is given below

Step 2 : Again rewrite sequence of weights in increasing order by replacing and β by new subtree weight as

γ	δ	$\alpha + \delta$	$\in$
6	11	11	20
↑	↑		

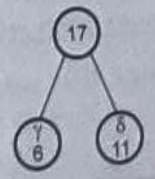


The first two smallest weights are 6 and 11.

$\therefore$ The root of new subtree has a weight

$$6 + 11 = 17$$

The new subtree is as follows



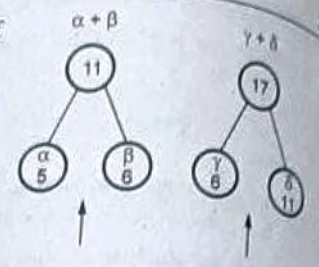
Step 3 : Rewrite sequence of weight in increasing order as

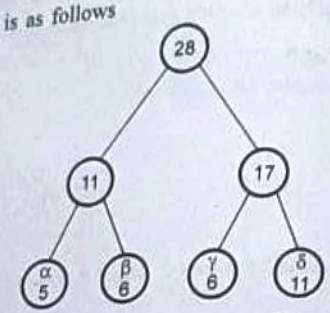
The first two smallest weights are 11 and 17.

∴ The root of new subtree has a weight

$$11 + 17 = 28$$

The new subtree is as follows





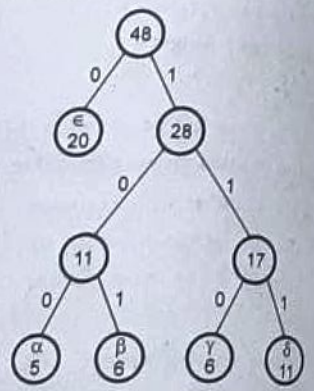
Step 4 : Rewrite the sequence of weights in increasing order

$$\begin{array}{cc} \epsilon & \\ 20 & 28 \\ \uparrow & \uparrow \end{array}$$

The root of new subtree is $20 + 28 = 48$

∴ The new subtree is as follows

This is the optimal binary tree.



Symbols leaves	α	β	γ	δ	ϵ
Binary prefix code	100	101	110	111	0

The weight of the optimal tree is

$$W = 20 \times 1 + 5 \times 3 + 6 \times 3 + 6 \times 3 + 11 \times 3$$

$$= 20 + 5 + 18 + 18 + 33 = \mathbf{104}$$

Q.26 Suppose data items A, B, C, D, E, F, G occur in the following frequencies :

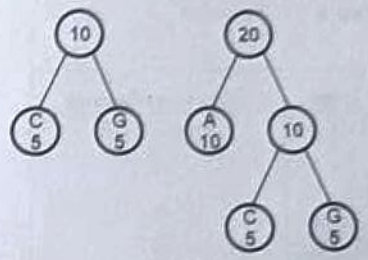
Data Items	A	B	C	D	E	F	G
Weight	10	30	5	15	20	15	05

Construct a Huffman code for the data. What is the minimum weighted path length ? ☞ **[SPPU : May-08, Dec.-14]**

Ans. : Consider the following steps

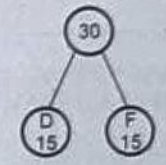
Step 1 : Sequence in increasing order is as follows

$$\begin{array}{ccccccc} C & D & A & D & F & E & B \\ 5 & 5 & 10 & 15 & 15 & 20 & 30 \\ \uparrow & \uparrow & & & & & \end{array}$$



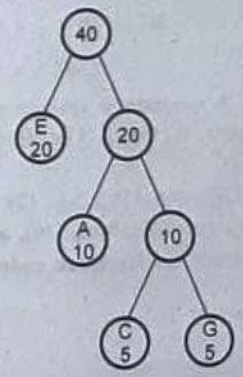
Step 2 : Sequence : D F F

$$\begin{array}{ccccc} 15, & 15, & 20, & 20, & 30 \\ \uparrow & \uparrow & \cdot & & \end{array}$$

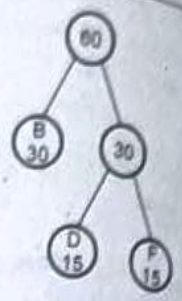


Step 3 : Sequence : E B

$$\begin{array}{cccc} 20, & 20, & 30, & 30 \\ \uparrow & \uparrow & & \end{array}$$

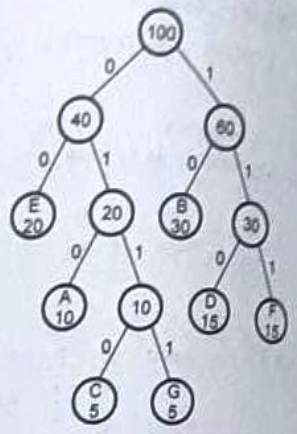


Step 4 : Sequence : B
30, 30, 40
↑ ↑



Step 5 : Sequence : 40, 60
↑ ↑

Items	Binary prefix code
5	0111 or 0110
10	010
15	110 or 111
20	00
30	11



The minimum weight path length for the vertices as follows

$A \to 3,\ B \to 2,\ C \to 4,\ D \to 3,\ E \to 2,\ F \to 3,\ G \to 4$

∴ The minimum weight of tree is

$$W = 10 \times 3 + 30 \times 2 + 5 \times 4 + 15 \times 3 + 20 \times 2 + 15 \times 3 + 5 \times 4 = \mathbf{260}$$

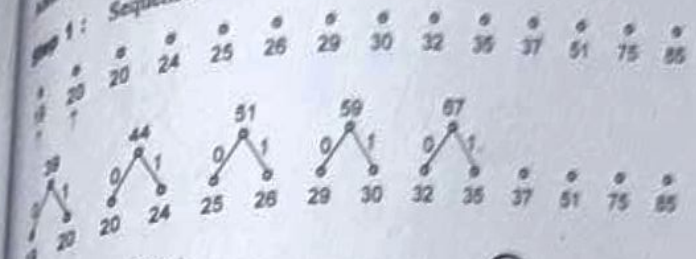
Q.27 A secondary storage media contains information in files with different formats. The frequency of different types of files is as follows.

Exe (20), bin (75), bat (20), jpeg (85), dat (51), doc (32), sys (26), c (19), cpp (25), bmp (30), avi (24), prj (29), 1st (35), zip (37).

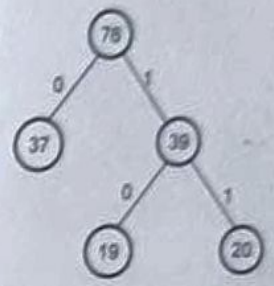
Construct the Huffman code for this. ☞ **[SPPU : May-15, Dec.-15]**

Sol. : Consider the following steps

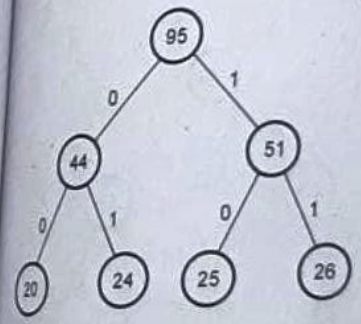
Step 1 : Sequence :



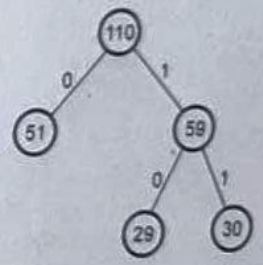
Step 2 : Sequence :
37, 39, 44, 51, 51, 59, 67, 75, 85
↑ ↑



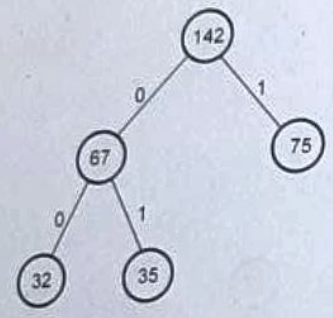
Step 3 : Sequence :
44, 51, 51, 59, 67, 75, 76, 85
↑ ↑



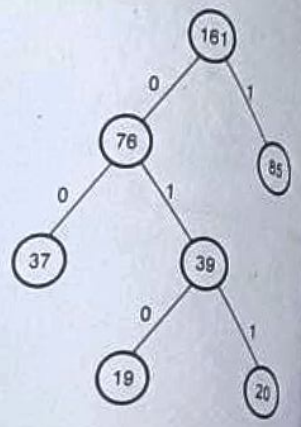
Step 4 : Sequence :
51, 59, 67, 75, 76, 85, 95
↑ ↑



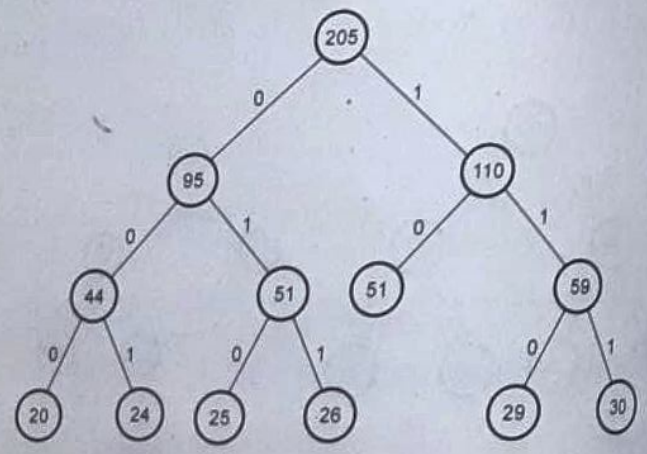
Step 5 : Sequence :
67, 75, 76, 85, 95, 100
↑ ↑



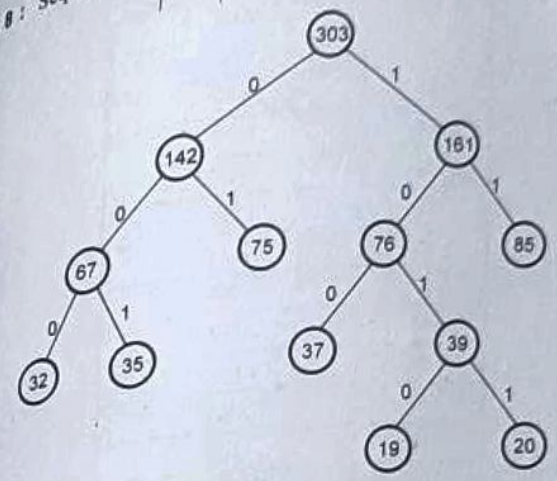
Step 6 : Sequence :
76, 85, 95, 110, 142,
↑ ↑



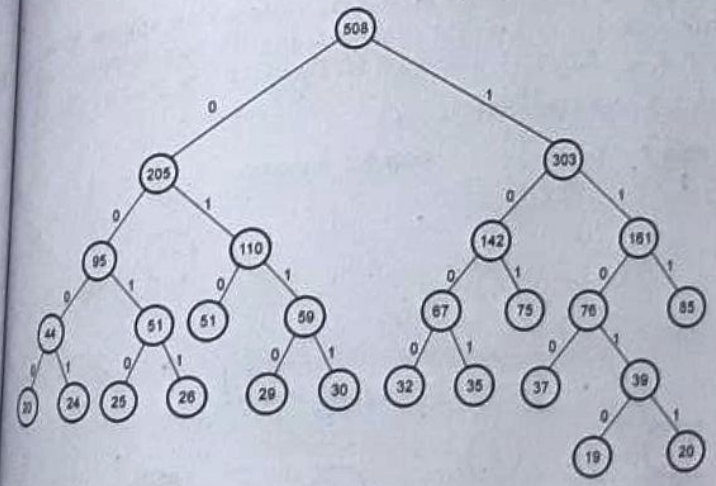
Step 7 : Sequence : 95, 110, 142, 161,
↑ ↑



Step 8 : Sequence : 142, 161, 205
↑ ↑



Step 9 : Sequence : 205, 303,
↑ ↑

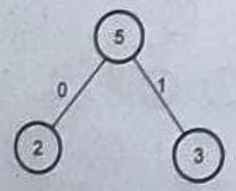


Numbers	Binary prifix codes
20	0000
24	0001
25	0010
26	0011
51	010
29	0110
30	0111
32	1000
35	1001
75	101
37	1100
19	11010
20	11011
85	111

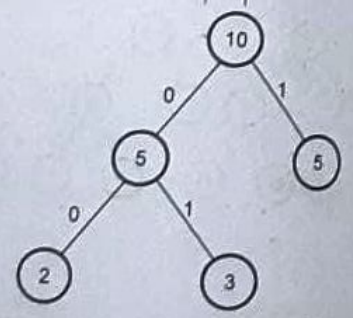
Q.28 For the following sets of weights, construct an optimal binary prefix code. For each weight in the set, give the corresponding code word i) 2, 3, 5, 7, 9, 13 ii) 8, 9, 10, 11, 13, 15, 22 ☞ **[SPPU : Dec.-12]**

Ans. : Consider the following steps.

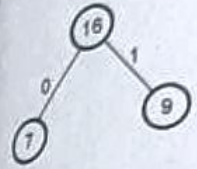
i) Step 1 : Sequence : 2, 3, 5, 7, 9, 13



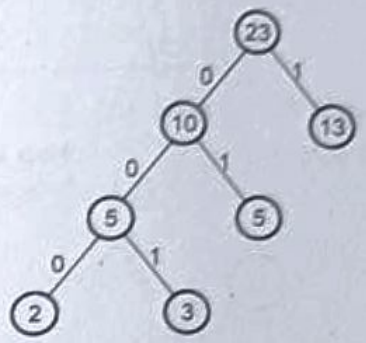
Step 2 : Sequence : 5, 5, 7, 9, 13,



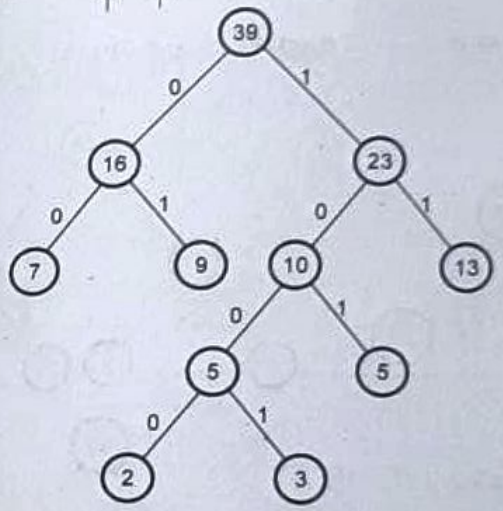
Step 3 : Sequence : 7, 9, 10, 13



Step 4 : Sequence : 10, 13, 16,



Step 5 : Sequence : 16, 23

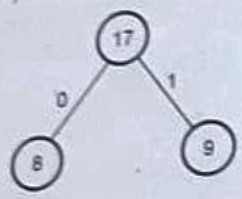


Symbols	Binary prefix code
7	00
9	01
2	1000

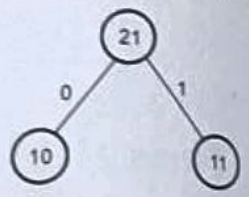
3	1001
5	101
13	11

ii) Consider the following steps

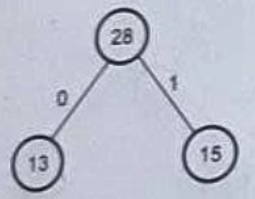
Step 1 : Sequence :
8, 9, 10, 11, 13, 15, 22
↑ ↑



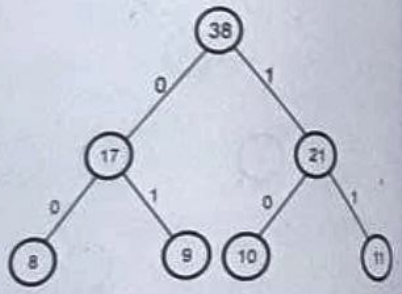
Step 2 :
Sequence : 10, 11, 13, 15, 17, 22
↑ ↑



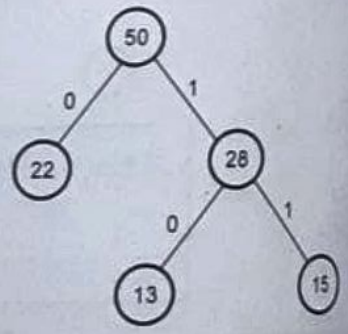
Step 3 : Sequence :
13, 15, 17, 21, 22,
↑ ↑



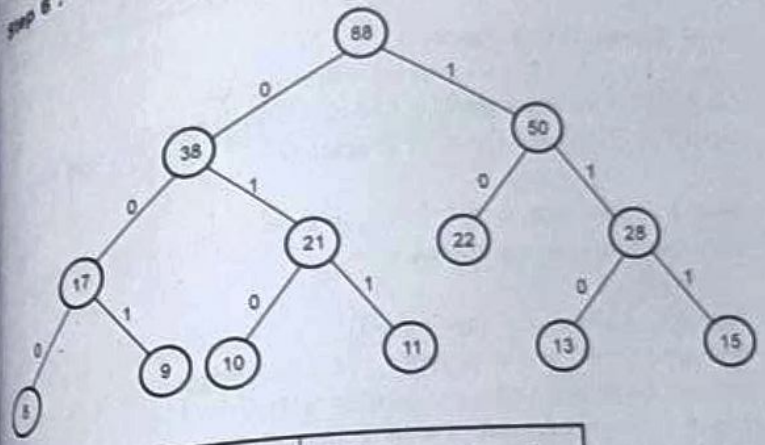
Step 4 : Sequence : 17, 21, 22, 28,
↑ ↑



Step 5 : Sequence : 22, 28, 38
↑ ↑



Step 6 : Sequence : 38, 50
↑ ↑



Symbols	Binary prefix code
8	000
9	001
10	010
11	011
22	10
13	110
15	111

5.4 : Spanning Trees

Q.29 Define spanning trees.

[SPPU : Dec.-11, 13, 14, 15, May-05, 14, 15]

Ans. : A spanning subgraph T of a connected graph G is said to be **spanning tree** of G if T is a tree. In other words, A subgraph T of a graph G is said to be spanning tree if V(T) = V(G).

5.5 : Kruskal's and Prim's Algorithm

Q.30 Explain Prim's algorithm.

Ans. : Let G(V, E) be a connected weighted graph.

To construct minimum spanning tree of G consider the following steps.

Step 1 : Select any vertex v_o in graph G.

Set $T = \{v_o, \phi\}$

Step 2 : Find edge $e_i = (v_o, v_i)$ in E such that its one end vertex is $v_o \in T$ and its weight is minimum.

$\therefore$ New set $T = \{\{v_0, v_1\}, \{e_i\}\}$

Step 3 : Choose next edge $e_k = (v_k, v_j)$ in such a way that it's one end vertex $v_k \in T$ and other vertex $v_j \notin T$ and weight of e_k is as small as possible. Again join vertex v_j and edge e_k to T.

Step 4 : Repeat the step 3 until T contains all the vertices of G. The set T will give the minimum spanning tree of the graph G.

Q.31 Explain Kruskal algorithm.

Ans. : Let G(V, E) be a weighted connect graph.

Consider the following steps.

Step 1 : Pick up an edge e_i of G such that its weight $W(e_i)$ is minimum.

(If there are more edges of the minimum weight then select all those edges which do not form a circuit).

Step 2 : If edges $e_1, e_2, \ldots, e_n$ have been chosen then pick an edge e_{n+1} such that

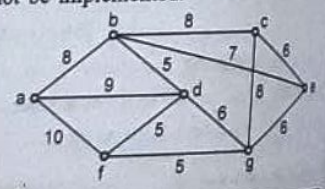
i) $e_{n+1} \neq e_i$ for $i = 1, 2, \ldots n$

ii) The edges $e_1, e_2, \ldots, e_n, e_{n+1}$ do not form a circuit.

iii) $W(e_{n+1})$ is as small as possible subject to condition (ii).

Step 3 : Stop when step two cannot be implemented.

Q.32 Find the minimum spanning tree for the graph given in the figure using Prim's algorithm.



☞ **[SPPU : Dec.-14]**

Ans. : Consider the following steps for the construction of the minimum spanning tree.

Step 1 : Select $a \in G$ as a starting vertex

$T = \{\{a\}, \phi\}$

$\therefore$

Step 2 : Vertex a is adjacent to vertices b, d and f. Among these edges minimum weight is $\{a, b\} = 8$

$T = \{\{a, b\}, \{e_1\}\}$

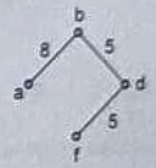
$\therefore$

Step 3 : Vertex a is adjacent to f, d.

Vertex b is adjacent to c, d, e

The minimum weight is of an edge $\{b, d\} = 5$

$T = \{\{a, b, d\}, \{e_1, e_2\}\}$



$\therefore$

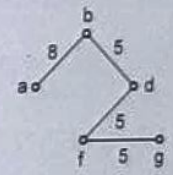
Step 4 : Vertex a is adjacent to f and $af = 10$

Vertex b is adjacent to c, e and $bc = 8$, $be = 7$

Vertex d is adjacent to f and g and $df = 5$, $dg = 6$

Among all these weights minimum is $5 = df$

$T = \{\{a, b, d, f\}\{e_1, e_2, e_3\}\}$



$\therefore$

Step 5 : Vertex is adjacent to b, d, f but all are in T.

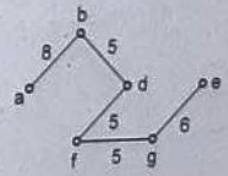
Vertex b is adjacent to c and e

Vertex d is adjacent to g.

Vertex f is adjacent to g

Among all these edges minimum weight is of fg.

$\therefore$ $T = \{\{a, b, d, f, g\}\{e_1, e_2, e_3, e_4\}\}$



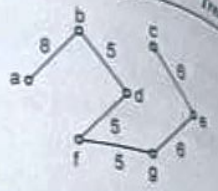
Step 6 : Vertex g is adjacent to c and e

Vertex b is adjacent to c and e

Among these edges the minimum weight is $ge = 6$

$\therefore T = \{\{a, b, d, f, g, e\}\{e_1, e_2, e_3, e_4, e_5\}\}$

Step 7 : Now only one vertex is remaining.



The vertex C is adjacent to b, e, g.

The minimum weight is ec = 6

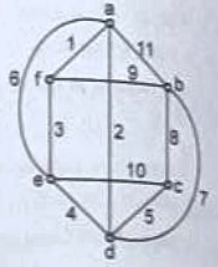
$\therefore \quad T = \{\{a, b, d, f, g, e, c\}\{e_1, e_2, e_3, e_4, e_5, e_6\}\}$

The graph obtained is the minimum spanning tree of weight

$= 8 + 5 + 5 + 5 + 6 + 6 = 35$

Q.33 Determine minimum spanning tree for the given graph by Prism's algorithm.

☞ [SPPU : May-14]



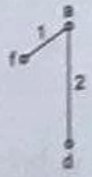
Ans. : Consider the following steps for the construction of the minimum spanning tree.

Step 1 : Starting with vertex a

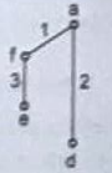
$T = \{\{a\}, \phi\}$

Step 2 : $T = \{\{a, f\}, e_1\}$

Step 3 : $T = \{\{a, f, d\}, \{e_1, e_2\}\}$

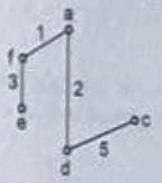


Step 4 : $T = \{\{a, f, d, e\}, \{e_1, e_2, e_3\}\}$



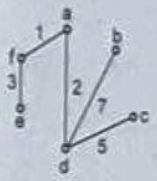
Step 5 :

$T = \{\{a, f, d, e, c\}, \{e_1, e_2, e_3, e_4\}\}$



Step 6 :

$T = \{\{a, f, d, e, c, b\}, \{e_1, e_2, e_3, e_4, e_5\}\}$

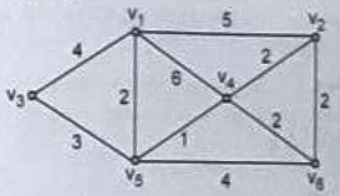


The graph obtained is the minimum spanning tree of weight

$= 1 + 2 + 1 + 5 + 7 = 18$

Q.34 Find the minimum spanning tree for graph given below by Kruskal's algorithm.

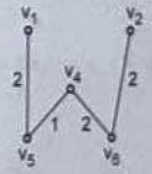
☞ [SPPU : Dec.-13]



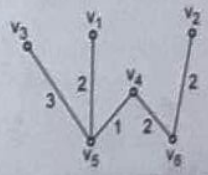
Ans. : Consider the following steps for the construction of the minimum spanning tree.

Step 1 : The minimum weight in given graph is 1, so select an edge $\{v_4, v_5\}$

Step 2 : The minimum weight is 2 in remaining graph. There are four edges of weight 2. These edges form a circuit so select edges which do not form a circuit with selected edge. We select three edges $\{v_5, v_1\}, \{v_4, v_6\}, \{v_6, v_2\}$



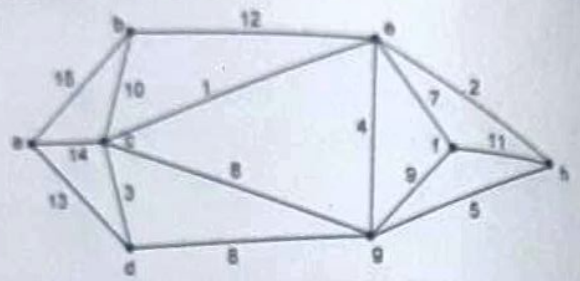
Step 3 : The minimum weight is 3 in the remaining graph so select $\{v_5, v_3\}$



The graph obtained is the minimum spanning tree of weight

$$= 3 + 2 + 1 + 2 + 2 = 10$$

Q.35 Obtain the minimum spanning tree for the following graph. Obtain the total cost of minimum spanning tree.



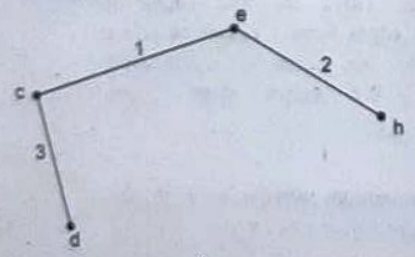
☞ **[SPPU : May-15, Dec.-18]**

Ans. : Using Kruskal algorithm, the minimum spanning tree is obtained as follows :

Step 1 : Minimum weight in a given graph is 1 associated with edge (a, c)

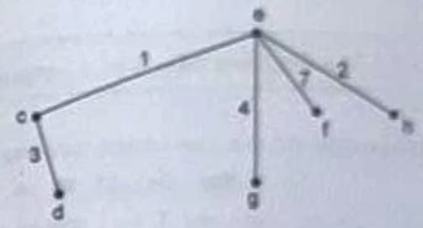
Step 2 : Minimum weight = 2

Step 3 : Minimum weight = 3

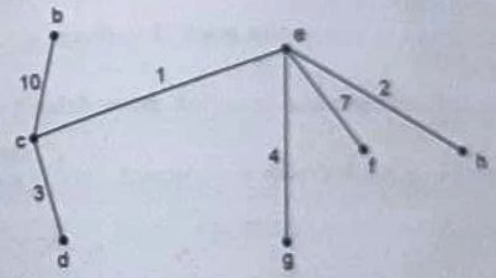


Step 4 : Minimum weight = 4

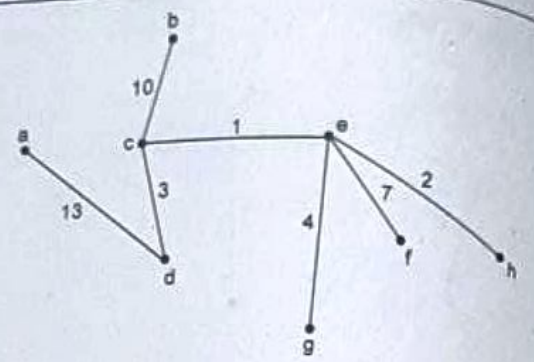
Step 5 : Minimum weight = 7



Step 6 : Minimum weight = 10



Step 7 : Minimum weight = 13



The obtained graph is the minimum spanning tree of the given graph. Its total cost is 40.

5.6 : The Maxflow Min Cut Theorem

Q.36 Explain fundamental circuits and cutsets with examples.

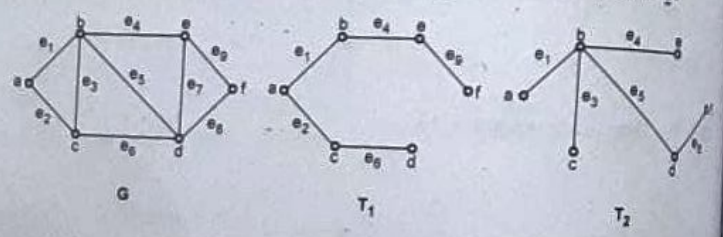
☞ [SPPU : Dec.-07, 12, 14, 15, May-07, 18]

Ans. : Let G be a connected graph and T be a spanning tree of G. An edge of a tree is called a **branch.** An edge of G which is not in T is called chord of T. T + e contains a unique circuit called fundamental circuit of G with respect to T.

A fundamental circuit of a connected graph G is always with respect to a spanning tree of G.

Therefore the different spanning trees will have different fundamental circuits.

Consider the following graph G with two spanning trees T_1 and T_2.



In graph G, vertex set V(G) = {a, b, c, d, e, f}

Edge set $E(G) = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9\}$

A) For Spanning Tree T_1 :

Branches of T_1 are e_1, e_2, e_4, e_6, e_9

Chords of T_1 are e_3, e_5, e_4, e_8

Consider, the following table of chords and corresponding fundamental circuits.

Chords	Corresponding Fundamental Circuits
e_3	$\{e_1, e_2, e_3\}$
e_5	$\{e_1, e_2, e_6, e_5\}$
e_7	$\{e_1, e_2, e_4, e_6, e_7\}$
e_8	$\{e_1, e_2, e_4, e_6, e_9, e_8\}$

B) For Spanning Tree T_2

Branches of T_2 are e_1, e_3, e_5, e_4, e_8

Chords of T_2 are e_2, e_4, e_6, e_7, e_9

Consider the following table of chords and corresponding fundamental circuits.

Chords	Corresponding Fundamental Circuits
e_2	$\{e_1, e_3, e_2\}$
e_6	$\{e_3, e_5, e_6\}$
e_7	$\{e_4, e_5, e_7\}$
e_9	$\{e_4, e_5, e_8, e_9\}$

Fundamental Cutsets

Let T be k spanning tree of a connected graph G. Since every edge e of a tree is an isthmus or bridge, T-e splits into two components say T_1 and T_2. But

$V(T) = V(T_1) \cup V(T_2) = V(G)$

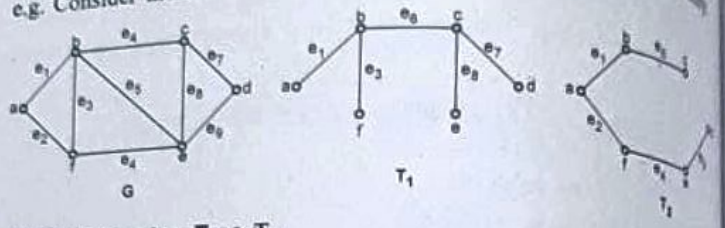
The set E of edges of G which join a vertex in $V(T_1)$ to a vertex in $V(T_2)$ is a cutset of G.

A cutset of G obtained in this manner is called a fundamental cutset of G with respect to T. To each edge of edge there is a fundamental cutset and

every fundamental cutset is obtained in this way. Thus the number of fundamental cutsets of G w.r.t. T is the number of branches of T.

Theorem : Let G be a connected graph with n vertices then its spanning tree has n – 1 edges and there are n – 1 fundamental cutsets only.

e.g. Consider the following and its spanning tree.



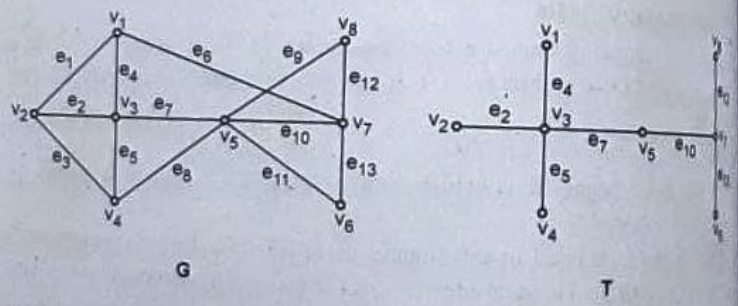
A) For Spanning Tree T_1

Branches of T_1 are e_1, e_3, e_6, e_7, e_8

Consider the following table

Branches T_1	Corresponding Fundamental Cutset
e_1	$\{e_1, e_2\}$
e_3	$\{e_3, e_2, e_4\}$
e_6	$\{e_6, e_5, e_4\}$
e_7	$\{e_7, e_9\}$
e_8	$\{e_8, e_4, e_9, e_5\}$

Q.37 Find the fundamental system of cutset for the graph G shown below w.r.t. the spanning tree T. ☞ **[SPPU : May-15, Dec.-12, 15]**

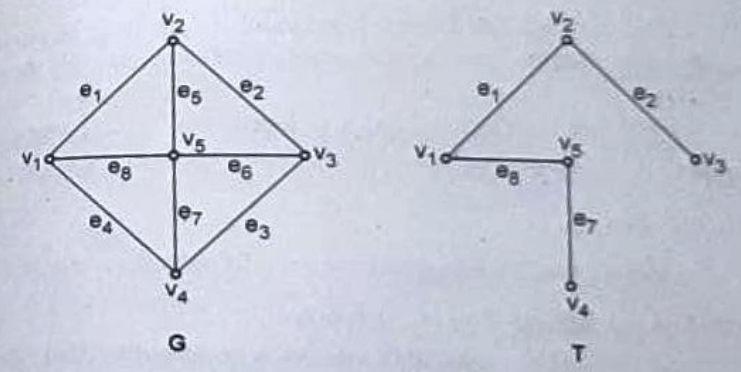


Ans. : The spanning tree T has 7 branches $\{e_2, e_4, e_5, e_7, e_{10}, e_{12}, e_{13}\}$. Therefore are seven fundamental cutsets of G w.r.t. T which are given below :

Branch	Fundamental Cutset
e_2	$\{e_2, e_1, e_3\}$
e_4	$\{e_4, e_1, e_6\}$
e_5	$\{e_5, e_3, e_8\}$
e_7	$\{e_7, e_6, e_8\}$
e_{10}	$\{e_{10}, e_8, e_9, e_{11}\}$
e_{12}	$\{e_{12}, e_9\}$
e_{13}	$\{e_{13}, e_{11}\}$

Q.38 Find the fundamental cutsets and fundamental circuits of the following graph w.r.t. given spanning tree.

☞ **[SPPU : May-07, Dec.-07, 14]**



Ans. : Here the spanning tree has 4 branches e_1, e_2, e_7, e_8. Therefore there are 4 fundamental cutsets corresponding to each branch of T which are given below.

Branch	Corresponding Fundamental Cutset
e_1	$\{e_1, e_5, e_8, e_3\}$
e_2	$\{e_2, e_8, e_3\}$
e_7	$\{e_7, e_3, e_4\}$
e_8	$\{e_8, e_4, e_5, e_6, e_3\}$

The chords of T are c_3, c_4, c_5, c_6

Therefore there are 4 fundamental circuits corresponding to each chord of T which are given below :

Chord	Corresponding Fundamental Cutset
e_3	$\{e_1, e_2, e_7, e_8, e_3\}$
e_4	$\{e_4, e_7, e_8\}$
e_5	$\{e_5, e_1, e_8\}$
e_6	$\{e_6, e_1, e_2, e_8\}$

Q.39 Explain labelling procedure for finding maximum flow in the network.

Ans. :

1) The source a is labelled $(-, \infty)$. It means that (out from nowhere) the source can supply can infinite amount of material to the other vertices.

2) A vertex b that is adjacent from a is labelled $(a^+, \Delta b)$, where Δb is equal to $w(a, b) - \phi(a, b)$.

if $w(a, b) > \phi(a, b)$;

i.e. $\Delta b = w(a, b) - \phi(a, b)$ [if $w(a, b) > \phi(a, b)$]

The vertex is not labelled if $w(a, b) = \phi(a, b)$

3) Scan and label all the remaining vertices adjacent to a. Also scan and label all the vertices adjacent to labelled vertices.

Suppose vertex q is adjacent to labelled vertex b, then q is labelled as $(b^+, \Delta q)$

where $\Delta q = \min(\Delta b, [w(b, q) - \phi(b, q)])$

if $w(b, q) > \phi(b, q)$

Vertex q is not labelled if $w(b, q) = \phi(b, q)$

We can also label vertex q as $(\bar{b}, \Delta q)$ where

$$\Delta q = \min[\Delta b, \phi(q, b)] \quad \text{if} \quad \phi(q, b) > 0$$

4) Repeat step 3 till we reach to sink z.

5) If we repeat this labelling procedure, two cases shall arise while labelling the sink z.

Case I :

i) Sink z is labelled, say with a label $(y^+, \Delta z)$ [z is never labelled $(y^-, \Delta z)$]

ii) Vertex y can be labeled as $(q^+, \Delta y)$ or $(q^-, \Delta y)$ for some adjacent vertex q.

iii) If y is labelled $(q^+, \Delta y)$ (q^+ means increase in flow) then we increase the flow in edge (q, y) to $\phi(q, y)$ to Δz. Similarly for the label $(q^-, \Delta y)$ we decrease the flow in edge (q, y) to $\phi(q, y) - \Delta y$.

iv) This process is continued back to source a till the value of flow is increased by amount Δz.

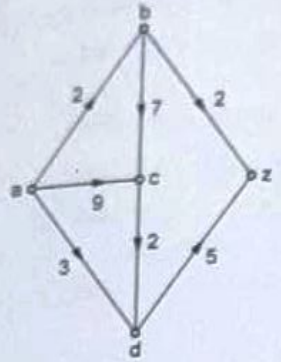
v) Again start the labelling procedure to further increase value of flow in the network.

Case II :

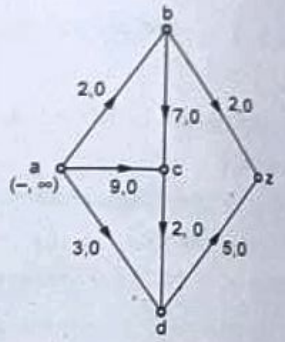
i) If the sink z is not labelled, then denote all labelled vertices as P and all unlabelled vertices as $\bar{P}$.

ii) The fact that sink z is not labeled means flow each edge directed from vertices of P to vertices of $\bar{P}$. is equal to capacity of cut $(P, \bar{P})$ is thus maximum flow.

Q.40 Determine the maximal flow in the following transport network. **[SPPU : Dec.-12, May-14]**



Ans. : Step 1 : Assign the flow zero to each edge and the label $(-, \infty)$ to the source a.



Step 2 : The vertices b, c, d are adjacent to the source a.

Therefore, we label the vertices b, c, d.

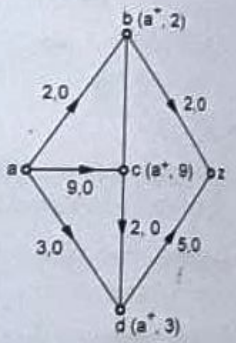
For the vertex b

$$w(a, b) - \phi(a, b) = 2$$

i.e. $\Delta b = 2$

Similarly $\Delta c = 9$ and $\Delta d = 3$

Now sink z is adjacent to both vertices b and d, so we arbitrarily choose vertex d and label.



sin z as $(d^+, 5)$ as

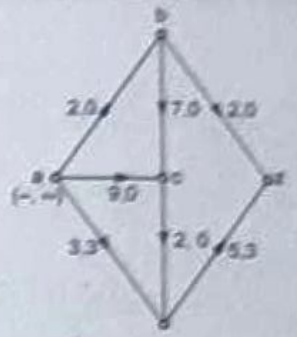
$$w(d, z) - \phi(d, z) = 5 - 0 = 5$$

and $\Delta z =$

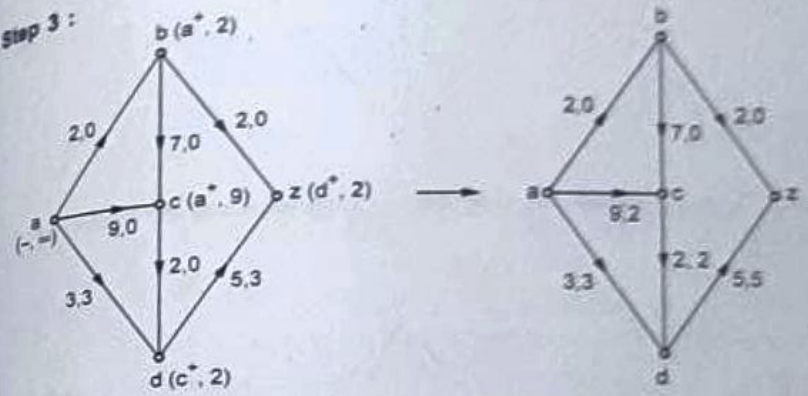
$\min\{\Delta d, \{w(d, z) - \phi(d, z)\}$

$= \min\{3, 5\} = 3$

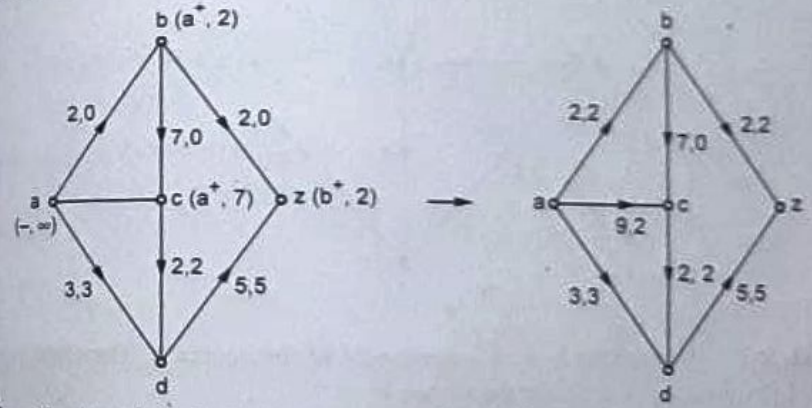
According to label of sink, we now adjust flow of edge (d, z) and edge (b, d)



Step 3 :



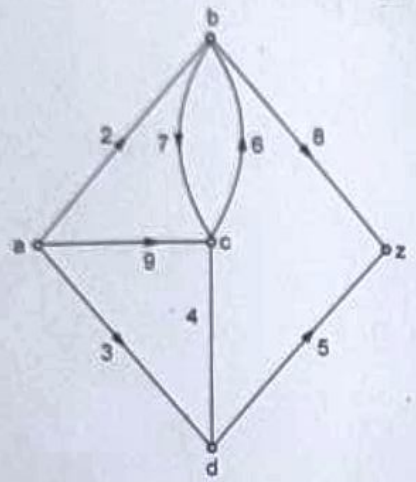
Step 4 :



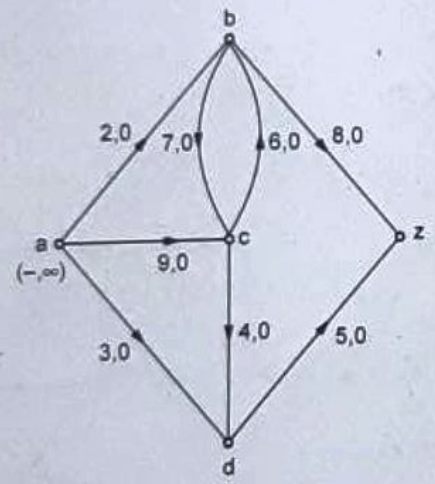
From the step 4, it is clear that the maximum flow is 7.

Q.41 Determine the maximal flow in the flowing transport network.

[SPPU : Dec.-13]



Ans. : Step 1 : Assign the flow zero to each edge and the label $(-, \infty)$ to the source a.

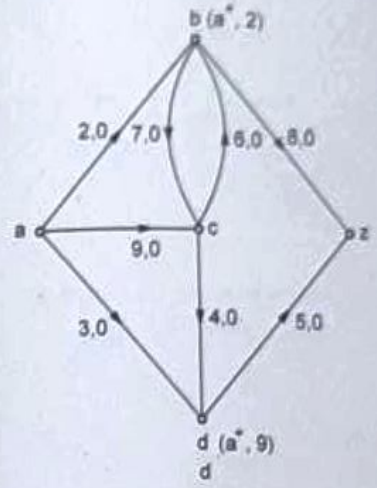


Step 2 : The vertices b, c, d are adjacent to the source a. Therefore, we label the vertices b, c, d for the vertex b.

$w(a, b) - \phi(a, b) = 2$

i.e. $\Delta b = 2$,

Similarly $\Delta c = 9$, $\Delta d = 3$



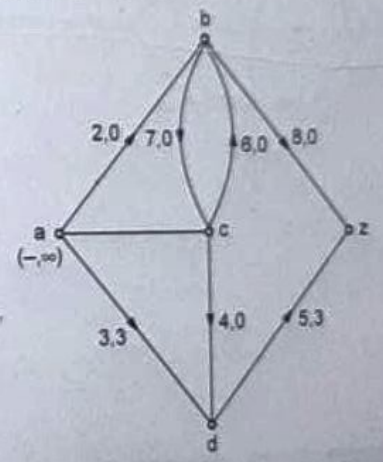
Now sink z is adjacent to both vertices b and d, so we can choose any vertex b or d for labelling of sink z. Let us choose the vertex d. The label of sink z is $(d^+, 5)$ as $w(d, z) - \phi(d, z) = 5 - 0 = 5$

and

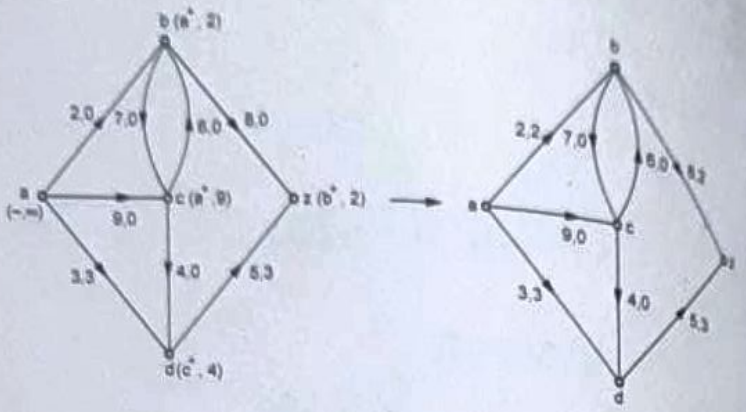
$\Delta z = \min\{\Delta d, w(d, z) - \phi(d, z)\}$

$= \min\{3, 5\} = 3$

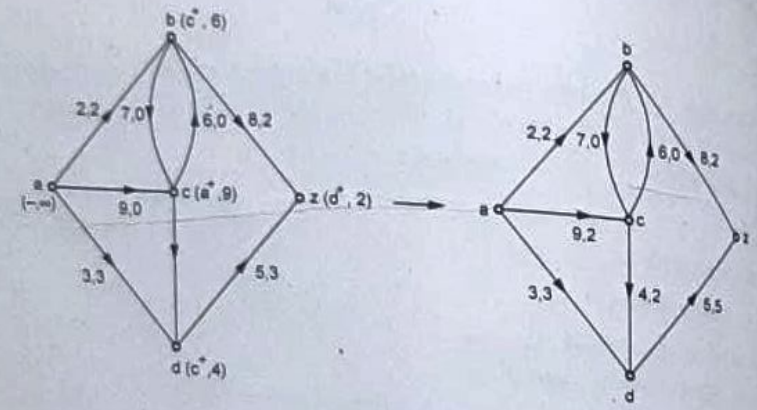
According to label of sink, we now adjust flow of edge (d, z) and edge (a, d)



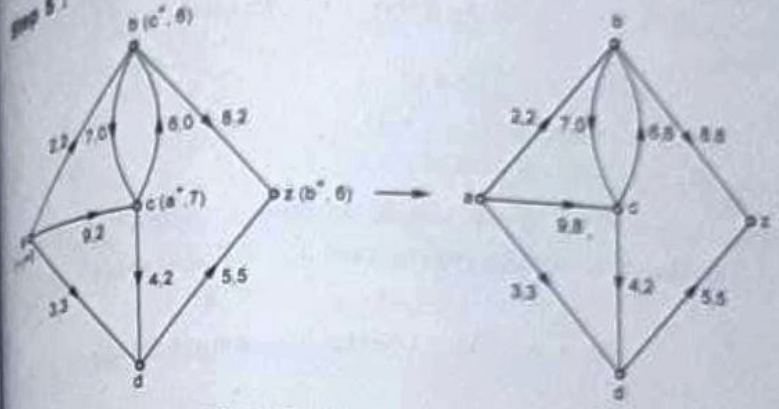
Step 3 :



Step 4 :



Step 5 :



Q.42 Using the labelling procedure to find maximum flow in the transport network in the following figure. Determine the corresponding minimum cut.

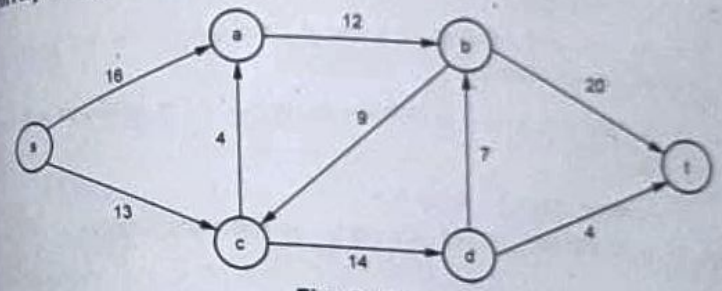


Fig. Q.42.1

Ans. : Assign the flow zero to each edge and $(-,\infty)$ to the source s.

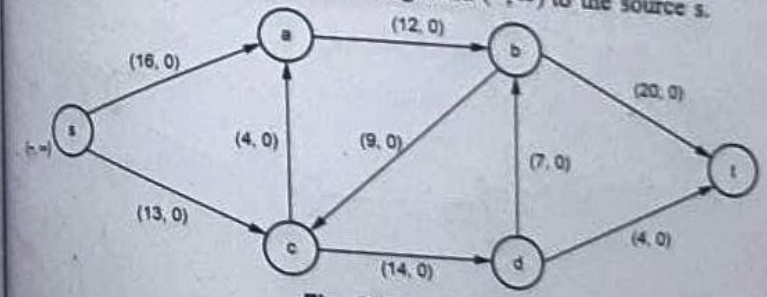


Fig. Q.42.1 (a)

Step 2 : Since, vertices a and c are adjacent to source s. Therefore, label the vertices a and c as $(s^+, \Delta a)$ and $(s^+, \Delta c)$ respectively.

Where,

$$\Delta a = ((s-a)-f(s,a)) = 16$$

$$\Delta c = ((s-c)-f(s,c)) = 13$$

Label of a is $(s^+, 16)$ and label of c is $(s^+, 13)$

Now vertices b and d are adjacent to labelled vertices $(s^+, 16)$ and $(s^+, 13)$. Therefore, label the vertices b and d as $(a^+, \Delta b)$ and $(c^+, \Delta d)$

Where,

$$\Delta b = \min(\Delta a, c(a,b)-f(a,b)) = \min(16, 12-0)$$

$$= 12$$

Similarly, $\Delta d = 13$

Lable b is $(a^+, 12)$ and d is $(c^+, 13)$

Now t is the sink and adjacent to b and d , we can choose any vertex b or d to label the sink t.

Lets, choose vertex d, which is labelled as $(c^+, 13)$. The label of t will be $(d^+, \Delta t)$ where

$$\Delta t = \min(13, 4-0) = 4$$

Hence, label of t is $(d^+, 4)$. It is shown in the following diagram.

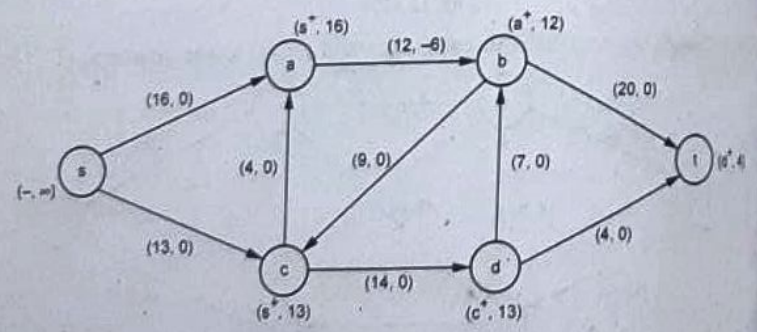


Fig. Q.42.1 (b)

Now adjust the flow in the edges

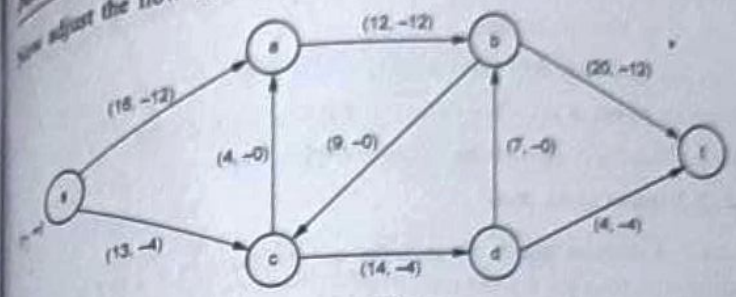


Fig. Q.42.1 (c)

Now adjust the flow in the edges s–c, c–d, d–b and label the nodes

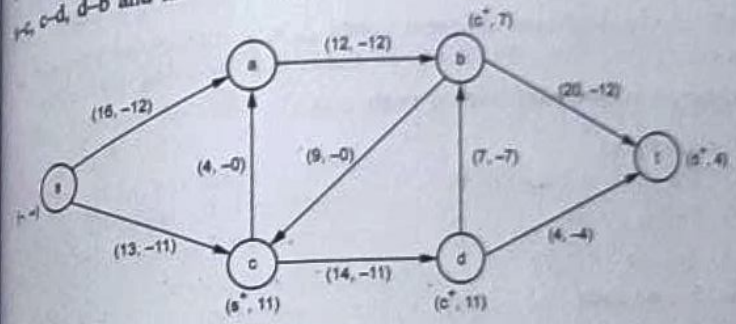


Fig. Q.42.1 (d)

Now adjust the flow in the edges b–t

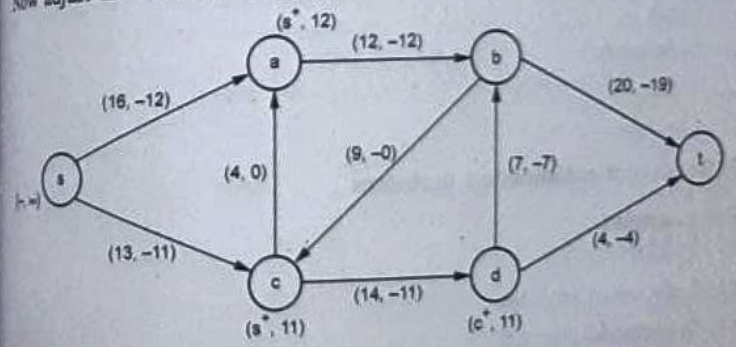


Fig. Q.42.1 (e)

We have to stop here.

P is set of labelled vertices

{s,a,c,d} and unlabelled vertices {b,t} .

Capacity of cut is $c(a+b)+(d,b)+c(d,t) = 12+7+4 = 23$

Hence, maximum flow in the network = 23.

Q.43 Explain game tree.

Ans. : A directed graph whose nodes are positions in a game and edges are moves, is called a game tree.

The complete game tree for a game is the game tree starting at the initial position and containing all possible moves from each position. The complete tree is the same tree as that obtained from the extensive form game representation.

We look at using trees for game planning, in particular the problems of searching game trees. We classify all games into following three types.

1) Single player path finding problems :

For examples :

a) Travelling salesman problem

b) Sliding puzzle

c) Hamiltonian paths

d) Rubik's cude

2) Two player games :

For examples :

a) Chess

b) Badminton

c) Tennis

d) Checkers

3) Constraint satisfication problems :

For examples :

a) Sudoku

b) Eight queen problem

c) Mathematical puzzles

d) Four queen problem

Each game consists of a problem space, an initial state and a set of goal states.

A problem space is a mathematical abstraction in a form of a tree :

- The root represents current state
- Nodes represent states of the game
- Edges represents moves
- Leaves represent final states (Win, loss or draw)

For example, in the 8-puzzle game

- Nodes : The different permentations of the tiles.
- Edges : Moving the black file up, down, right or left.

Minimax :

We consider game with two players in which one players gains are the result of another players losses so called zero sum games.

The minimax algorithm is a specialized search algorithm which returns the optimal sequence of moves for a player in an zero sum game.

In the game tree that result from the algorithm, each level represents a move by either of two players, say A and B player. The minimax algorithm explores the entire game tree using a depth-first search.

At each node in the tree where A-player has to move, A-player would like to play the move that miximizes the payoff. Thus, A-player will assign the maximum score amongst the children to the node where max makes a move. Similarly, B-player will minimize the pay off to A-player. The maximum and minimum scores are taken at alternating levels of the tree, Since A and B alternate turns. The minimax algorithm computes the minimx decision for the leaves of the game tree and than backs up through the tree to give the final value to the current state.

END...

Unit VI

6 Algebraic Structures and Coding Theory

6.1 : Algebraic Structure

Q.1 Define binary operation. [SPPU : Dec.-05]

Ans. : Binary operation : I) Let A be any non empty set. A function $f: A \times A \to A$ is called the binary operation on the set A.

'$*$' is a binary operation on the set A iff $a * b \in A \ \forall\ a, b \in A$ and $a * b$ is unique.

II) An n-ary operation on a set $A \neq \phi$ is a function $f: A \times A \times \ldots \times A$ (n times) $\to A$ i.e. $f: A^n \to A$

The n-ary operation is defined for each n-tuple $(a_1, a_2, \ldots a_n) \in A$ for $a_2 \in A$

If n = 1 then f is called unary operation

If n = 2 then f is called binary operation

If n = 3 then f is called ternary operation

Examples

1) A function $f: \Re \to \Re$ such that $f(x) = x$; $\forall x \in \Re$ then f is a unary operation.
2) A function $f: \Re \times \Re \to R$ such that $f(x, y) = x + y$ then f is a binary operation.
3) A function $f: Z \times Z \times Z \to Z$ such that $f(x, y, z) = x + y + z$. then f is a ternary operation.

Properties of binary operations

I) Commutative property

A binary operation '$*$' on A is said to be commutative if $a * b = b * a$, for all $a, b \in A$. e.g. $x + y = y + x$ and $x \times y = y \times x$ for all $x, y \in \Re$

$\therefore$ '+' and '×' are commutative binary operations on $\Re$

But '−' is not commutative on $\Re$

II) Associative property :

A binary operation '$*$' on set A is said to be associative if $a * (b * c) = (a * b) * c$; $\forall$ a, b, c $\in$ A

e.g. '+' and '×' are associative on the set of real numbers '−' is not associative on $\Re$

III) Idempotent

A binary operation '$*$' on set A is said to be idempotent if $a * a = a$; for all $a \in A$

e.g.

1) 1 is idempotent element in $\Re$ w.r.t. binary operation 'X'.
2) 0 is idempotent element in $\Re$ w.r.t. '+'.
3) 1 is not idempotent element in $\Re$ w.r.t. '+'.

Q.2 For each of the following, determine whether $*$ is a binary operation.

i) R is the set of real numbers and $a * b = ab$

ii) z^+ is the set of positive integers and $a * b = a/b$.

iii) On z^+ where $a * b = a - b$. iv) On R, where $a * b = \min\{a, b\}$

v) On R, where $a * b = a \times |b|$ vi) On z, where $a * b = a^b$.

Ans. : i) Yes, since $f: R^2 \to R$ defined as f(a, b) = ab is a function, with $a\ b \in R$.

ii) No, since $(a, b) \in z^+ \times z^+$ does not imply that $a * b = a/b \in z$

$(1, 2) \in z^+ \times z^+$, but $1/2 \notin z^+$

iii) No, since $(1, 2) \in z^+ \times z^+$ but

iv) Yes, since, $*$ is a function with $\min\{a, b\} \in R$

v) Yes, since $*$ is a function with $a \times |b| \in R$

vi) No, since $2 * (-1) = 2^{-1} = \frac{1}{2} \notin z$

Q.3 Determine whether or not following operations on the set of integers Z are associative. i) Division ii) Exponentiation

[SPPU : Dec.-05, Marks 3]

Ans. : i) Division on the set of integers is not associative as

$(a/b)/c \neq a/(b/c)$

ii) Exponentiation on the set of integers is not associative as

$(a^b)^c \neq a^{(b^c)}$

Q.4 Consider the binary operation * defined on the set A = {a, b, c, d} by the following table.

*	A	b	c	d
a	a	c	b	d
b	d	a	b	c
c	c	d	a	a
d	d	b	a	c

Find i) $c*d$ and $d*c$ ii) $b*d$ and $d*b$
iii) $a*(b*c)$ and $(a*b)*c$ iv) Is * commutative, associative ?

Ans. :

i) $c*d = a$ $\quad$ $d*c = a$

ii) $b*d = c$ $\quad$ $d*b = b$

iii) $b*c = b$ $\quad$ $a*(b*c) = a*b = c$

$a*b = c$ $\quad$ Hence $(a*b)*c = c*c = a$

iv) * is not commutative, since $b*d \neq d*b$

* is also not associative, since $a*(b*c) \neq (a*b)*c$

Q.5 Define Groupoid, semigroup, monoid with examples.

[SPPU : Dec.-06, 13]

Ans. : 1. Groupoid : A non empty set k with binary operation '*' is called groupoid if the binary operation '*' satisfies $\forall a, b \in G, a*b \in G$
In other words, every algebraic structure is groupoid.

e.g. $(\Re, +)$, $(\Re, -)$, $(Z, +)$, $(Z, \times)$ are groupoids.

2. Semigroup : A non empty set G with binary operation '*' is called a semigroup if it satisfies the following properties.

$a*(b*c) = (a*b)*c$; $\forall a, b, c \in G$

i.e. '*' is associative in G

A semigroup is said to be commutative if * is commutative.

e.g. i) $(\Re, +)$, $(N, +)$, $(Z, +)$ are commutative semigroups.

ii) $(\Re, \times)$, $(Z, \times)$ are commutative semigroups.

iii) $(Z, -)$ is not a semigroup as '–' is not associative.

[SPPU : Dec.-13]

3. Monoid

Let G be a non empty set and * be a binary operation on G. (G, *) is called monoid if.

i) Associative property : $a*(b*c) = (a*b)*c$; $\forall a, b, c \in G$

ii) Existence of identity : $\exists$ an element $e \in G$ such that $e*a = a*e = a$; $\forall a \in G$

The element 'e' is called the identity element.

Example 1 : $(\Re, +)$ is a monoid as $a + b \in \Re$ $\forall a, b \in \Re$

i.e. $(\Re, +)$ is closed

and $a + (b + c) = (a + b) + c$

and $0 + a = a + 0 = a$, $\quad \forall a \in \Re$

0 is the identity element in $\Re$ w.r.t. '+'.

Example 2 : $(C, +)$, $(C, \times)$, $(Z, +)$, $(Z, \times)$, $(Q, +)$ are monoids.

Example 3 : $(N, \times)$ is a monoid but $(N, +)$ is not monoid as $0 \notin N$

Q.6 Show that the algebraic system (A, +) is a monoid, where A is the set of integers and '+' is a binary operation giving addition of two integers.

[SPPU : Dec.-06, Marks 4]

Ans. : Let A be the set of all integers and '+' defined on A.

i) Closure property : $a + b \in A$; $\forall a, b, \in A$ as $a + b$ is an integer.

ii) Associative property :

$a + (b + c) = (a + b) + c$; $\forall a, b, c \in A$

iii) Existence of identity element :

For any $a \in A$, $\exists$ $0 \in A$ such that

$a + 0 = 0 + a = a$

Therefore (A, +) is a monoid.

6.2 : Group and Abelian Group

Q.7 Define group and abelian group.

☞ [SPPU : Dec.-08,09,10,12, May-14, Marks 4]

Ans. : Let G be a non empty set equipped with a binary operation $*$. $(G, *)$ is called a group if it satisfies the following postulates or axioms.

i) Associativity : $a*(b*c) = (a*b)*c$; $\forall\, a, b, c \in G$

ii) Existence of the identity : For any $a \in G$, $\exists\, e \in G$

s.t. $\quad a*e = e*a = a$,

An element e is called the identity element in $(G, *)$

iii) Existence of the inverse :

For all $a \in G$, $\exists\, b \in G$ such that

$$a*b = b*a = e$$

Then b is called the inverse of a in $(G, *)$

$\therefore \quad b = a^{-1}$

Abelian Group or Commutative Group :

A group $(G, *)$ is called an Abelian group if

$$a*b = b*a \quad ; \quad \forall\, a, b \in G$$

i.e. $*$ is commutative in $(G, *)$

Q.8 Explain properties of group with proof.

☞ [SPPU : Dec.10, Marks 2]

Ans. : I) The identity element in a group is unique.

Proof : Suppose e_1 and e_2 are two identity elements in group G.

We have, $e_1 e_2 = e_1$; if e_2 is identity element in G.

and $\quad e_1 e_2 = e_2$; If e_1 is identity element in G.

$\Rightarrow \quad e_1 e_2 = e_1 = e_2$. Hence the identity element in group G is unique.

II) The inverse of each element in group G is unique.

☞ [SPPU : Dec.-10, Marks 4]

Let a be any element of a group G and let e be identity element in group G.

Suppose b and c are two inverses of a in G.

$\therefore \quad ba = ab = e$ and $ac = ca = e$

$$b = be = b\,(ac)$$

$$b = (ba)\,c$$

$$b = ac$$

$$b = c$$

Hence, the inverse of each element is unique.

III) The inverse of an inverse of the element is the original element. i.e. If the inverse of a is a^{-1} then $(a^{-1})^{-1} = a$.

Proof : Let $e \in G$ be the identity element of the group G.

Let $a \in G$.

We have, $a^{-1}a = e$

$(a^{-1})^{-1}(a^{-1})a = (a^{-1})^{-1}\, e$ — (Multiplying by $(a^{-1})^{-1}$)

$(a^{-1})^{-1}(a^{-1})\, a = (a^{-1})^{-1}$ — ($\because$ Associativity of e identity)

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

$a = (a^{-1})^{-1}$ Hence, the proof

IV) Prove that the inverse of the product of two elements of a group G is the product of the inverses taken in reverse order. i.e. $(ab)^{-1} = b^{-1}a^{-1}$, $\forall\, a ; b \in G$.

Proof : Let a^{-1} and b^{-1} be the inverses of a and b in a group G respectively. Let e be the identity in G. Then $a^{-1}a = a\,a^{-1} = e$ and $b^{-1}b = b^{-1}b = e$

Consider, $\quad (ab)(b^{-1}a^{-1}) = a\,(bb^{-1})\,a^{-1}$ ($\because$ Associativity)

$= a\,(e)\,a^{-1}$ ($\because bb^{-1} = e$)

$= (ae)\,a^{-1} = aa^{-1} = e$ ... (1)

Similarly, $\quad (b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)\,b = b^{-1}(e)\,b$

$= b^{-1}b = e$ ... (2)

From equation (1) and equation (2), $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab)$

$b^{-1}a^{-1}$ is the inverse of ab

$$(ab)^{-1} = b^{-1}a^{-1}$$

V) Prove that the cancellation laws hold in a group.i.e. If a, b, c $\in$ G then $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$.

Proof : Let a be any element in G and e be the identity element of a group G.

Now we have, $ab = ac$

Permultiplying by a^{-1} we get,

$$a^{-1}(ab) = a^{-1}(ac)$$

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

$$eb = ec \quad \ldots (\because \text{Associativity})$$

$$b = c \quad \ldots (\because aa^{-1} = e)$$

Similarly, $ba = ca$

$\Rightarrow \quad (ba)a^{-1} = (ca)a^{-1} \Rightarrow be = ce$

$\Rightarrow \quad b = c$

Hence, the proof

VI) If a, b are any elements of a group G then equation ax = b and ya = b have unique solutions in G.

Proof : Let $a \in G$

$\therefore \exists\, a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$

$a, a^{-1} \in G$ and $b \in G \Rightarrow a^{-1}b \in G$.

Now substituting $a^{-1}b$ for x in the L.H.S. given equation, we get,

$$ax = a(a^{-1}b) = (aa^{-1})b = eb = b$$

Thus, $\quad x = a^{-1}b$ is the solution of $ax = b$

Let us suppose that x_1 and x_2 are two solutions of $ax = b$.

$\therefore \quad ax_1 = b$ and $ax_2 = b$

$\Rightarrow \quad b = ax_1 = ax_2 \Rightarrow x_1 = x_2$

Hence solution is unique.

Similarly prove for $ya = b$.

Q.9 If set Q_1 of all rational numbers other than 1 with $a * b = a + b - ab$. Show that (G, *) is a group.

[SPPU : Dec.-09, Marks 4]

Ans. : We have, $a * b = a + b - ab, \forall\, a, b \in G$.

i) Closure property : Let $a, b \in Q_1$, $a \neq 1$, $b \neq 1 \therefore ab \neq 1$.

$\therefore \quad a * b = a + b - ab \neq 1$ and $a * b \in Q_1$

Q_1 is closed w.r.t. *

ii) Associativity : Let $a, b, c \in Q_1$.

$(a * b) * c = (a + b - ab) * c = (a + b - ab + c - (a + b - ab)c$

$= a + b - ab + c - ac - bc - abc \quad \ldots (Q.9.1)$

$a * (b * c) = a * (b + c - bc) = a + b + c - bc$

$= a(b + c - bc) = a + b + c - bc - ab - ac + abc \quad \ldots (Q.9.2)$

From equation (Q.9.1) and equation (Q.9.2)

$(a * b) * c = a * (b * c)$

* is associative

iii) Existence of the identity : Let e be the identity element in Q_1

$$a * e = a$$

$$a + e = ae = a$$

$$e - ae = 0$$

$$e(1 - a) = 0 \quad \text{(But } a \neq 1)$$

$$e = 0$$

0 is the identity element.

iv) Existence of the inverse : Let $a \in Q_1$, $a \neq 1$.

Suppose $b \in Q_1$ is the inverse of a.

$$a * b = e$$

$$a + b - ab = 0$$

$$a + b(1 - a) = 0$$

$$b(1 - a) = -a$$

$$b = \frac{-a}{1-a} = \frac{a}{a-1} \neq 1 \text{ and } b \in Q_1.$$

The inverse exist for all a in Q_1.

Thus, $(Q_1, *)$ is a group.

Q.10 If $S = \{(a, b) \mid a \neq 0, a, b, \in \Re\}$ and $(a, b) * (c, d) = (ac, bc + d)$ then show that G is a group but not abelian group w.r.t.*

Ans. : i) Closure property : Let $(a, b)(c, d) \in S$; $a \neq 0$; $c \neq 0$

$\therefore ac \neq 0$.

$(a, b) * (c, d) = (ac, bc + d) \in S$

ii) Associativity : Let (a, b), (c, d) and $(e, f) \in S$

Consider

$[(a, b) * (c, d)] * (e, f) = [ac, bc + d) * (e, f) = ([ac]e, [bc + d]e + f)$

$= (ace, bce + de + f) \quad \ldots (Q.10.1)$

and $(a, b) * [(c, d) * (e, f)] = (a, b) * [ce, de + f] = [ace, b(ce) + de + f]$

$= (ace, bce + de + f)$ ...(Q.10.2)

From equation (Q.10.1) and equation (Q.10.2) $*$ is associative operation.

iii) Existence of the identity : Let $(a, b) \in S$ and $(x, y) \in S$, $x \neq 0$

Consider, $(a, b) * (x, y) = (a, b)$

$(ax, bx + y) = (a, b)$

$\Rightarrow \quad ax = a$ and $bx + y = b$

$\Rightarrow \quad x = 1$ and $b + y = b$

$\Rightarrow \quad y = 0$

Similarly, $(x, y) * (a, b) = (a, b)$

$(1, 0)$ is the identity element in S.

iv) Existence of the inverse : Let (a, b) and $(c, d) \in S$.

$(a, b) * (c, d) = (1, 0)$

$(ac, bc + d) = (1, 0)$

$\Rightarrow \quad ac = 1$

and $\quad bc + d = 0$

$\therefore \quad c = \frac{1}{a}$

and $\quad d = -bc = -\frac{b}{a}$ and $c \neq 0$

Thus $\left(\frac{1}{a}, -\frac{b}{a}\right)$ is the inverse of (a, b) in S.

Thus $(S, *)$ is a group.

Consider, $(a, b) * (c, d) = (ac, bc + d)$

and $(c, d) * (a, b) = (ca, da + b)$

$\Rightarrow \quad (a, b) * (c, d) \neq (c, d) * (a, b)$

Thus, $(S, *)$ is not an abelian group.

Q.11 If $G = \left\{\begin{bmatrix} x & x \\ x & x \end{bmatrix} \middle/ x \text{ is non zero real number}\right\}$. Show that G is an abelian group w.r.t. matrix multiplication.

Ans : i) Closure property :

$A = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$ and $B = \begin{bmatrix} y & y \\ y & y \end{bmatrix} \in G$

Let

$AB = \begin{bmatrix} x & x \\ x & x \end{bmatrix}\begin{bmatrix} y & y \\ y & y \end{bmatrix} = \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} \in G$

ii) Associativity : We know that any matrix multiplication is associative.

iii) Existence of the identity : Let $E = \begin{bmatrix} e & e \\ e & e \end{bmatrix}$ such that

$AE = A \Rightarrow$

$\begin{bmatrix} x & x \\ x & x \end{bmatrix}\begin{bmatrix} e & e \\ e & e \end{bmatrix} = \begin{bmatrix} e & e \\ e & e \end{bmatrix}$

$\Rightarrow \quad \begin{bmatrix} 2xe & 2xe \\ 2xe & 2xe \end{bmatrix} = \begin{bmatrix} e & e \\ e & e \end{bmatrix}$

$\Rightarrow \quad 2xe = e$

$\Rightarrow \quad 2x = 1$

$\Rightarrow \quad x = \frac{1}{2}$

$\Rightarrow \quad E = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$ is the identity element of G.

iv) Existence of the inverse : Let $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \in G$ and

$B = \begin{bmatrix} y & y \\ y & y \end{bmatrix} \in G$ such that $AB = E$

$\Rightarrow \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$

$\Rightarrow \quad 2xy = \frac{1}{2}$

$\Rightarrow \quad xy = \frac{1}{4}$

$\Rightarrow \quad y = \frac{1}{4x}$

$$A^{-1} = \begin{bmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{bmatrix}$$

v) Commutative property :

We have, $AB = BA = \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} \in G$

Thus G is an abelian group w.r.t. matrix multiplication.

Q.12 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.

☞[SPPU : Dec.-08]

Ans. : i) Closure property : Let $a, b \in G$.

$$a * b = \frac{ab}{2} \in G \text{ as } ab \neq 0$$

ii) Associativity : Let $a, b, c \in G$

Consider $\quad a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{a(bc)}{4} = \frac{abc}{4}$

$$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{(ab)c}{4} = \frac{abc}{4}$$

$\Rightarrow$ * is associative in G.

iii) Existence of the identity : Let $a \in G$ and $\exists$ e such that

$$a * e = \frac{ae}{2} = a$$

$\Rightarrow \quad ae = 2a$

$\Rightarrow \quad e = 2$

$\therefore$ 2 is the identity element in G.

iv) Existence of the inverse : Let $a \in G$ and $b \in G$ such that $a * b = e = 2$

$\Rightarrow \quad \frac{ab}{2} = 2$

$\Rightarrow \quad ab = 4$

$b = \frac{4}{a}$

$\therefore$ The inverse of a is $\frac{4}{a}$, $\forall a \in G$.

v) Commutativity : Let $a, b \in G$

$a * b = \frac{ab}{2}$

and $\quad b * a = \frac{ba}{2} = \frac{ab}{2}$

$\therefore$ * is commutative

Thus, (G, *) is an abelian group.

Q.13 Show that the set $G = \{1, w, w^2\}$ where w is the cube root of unity is a group with respect to multiplication.

☞[SPPU : Dec.-12, Marks 6]

Ans. : Consider the following composition table of G.

	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

i) Closure property : From table all elements belong to G.

$\therefore$ G is closed w.r.t. multiplication.

ii) Associativity : As all elements of G are complex numbers and multiplication of complex numbers is associative.

$\therefore$ (G, x) is associative.

iii) Existence of the identity : From the composition table

$$1\,(1) = 1\,,\ 1\,(w) = 1\,,\ 1\,(w^2) = w^2$$

$\therefore$ 1 is multiplicative identity in G.

iv) Existence of the inverse : From table, the inverses of 1, w, w^2 are 1, w^2, w respectively. Thus (G, x) is a group.

Q.14 Let (A, *) be a group. Show that (A, *) is abelian group if $a^2 * b^2 = (a * b)^2$

☞[SPPU ; Dec.-12, Marks 4]

Ans. : Let (A, *) be an abelian group.

$$a * b = b * a$$

Consider,

$$a^2 * b^2 = (a * a) * (b * b)$$
$$= a * (a * b) * b$$
$$= a * (b * a) * b = (a * b) * (a * b) \quad (* \text{ is associative})$$
$$a^2 * b^2 = (a * b)^2$$

Conversely suppose

$$a^2 * b^2 = (a * b)^2$$

$$\text{L.H.S.} = a^2 * b^2 = (a * a) * (b * b) = a * (a * b) * b \quad \text{(Q.14.1)}$$

$$\text{R.H.S.} = (a * b)^2 = (a * b) * (a * b) = a * (b * a) * b$$

Equation (Q.14.1) $\Rightarrow$

$$a * (a * b) * b = a * (b * a) * b$$

By cancellation laws,

$$a * b = b * a$$

$\Rightarrow$ (A, *) is an abelian group.

Q.15 Show that the set of all idempotents in a commutative monoid S is a submonoid of S.

[SPPU : Dec.-12, Marks 4]

Ans. : We know that an element $x \in S$ is called an idempotent if $x * x = x$.

Let T be the set of all idempotents in S.

i) For any $x, y \in T$, Consider

$$(x * y) * (x * y) = ((x * y) * x) * y = (y * (x * x)) * y = (y * x) * y$$
$$= (x * y) * y = x * (y * y) = x * y$$

$\therefore$ $x * y \in T$ for all $x, y \in T$

T is closed w.r.t. '*'

ii) Associativity, Let $x, y, z \in T \subseteq S$

$\therefore$ $x * (y * z) = (x * y) * z$ in T

* is associative in T

iii) Existence of the identity :

Let e be the identity element in S

As $e * e = e$ $\therefore$ $e \in T$

$\therefore$ e is the identity element in T.

$\therefore$ T is a monoid

Thus T is a submonoid of S.

Q.16 Prove that the set Z of all integers with binary operation * defined by $a * b = a + b + 1$ such that $\forall\, a, b \in Z$ is an abelian group :

[SPPU : May-14, Marks 4]

Ans. : We have $a * b = a + b + 1$, $\forall\, a, b \in Z$

i) Closure property

For $a, b \in Z \Rightarrow a + b + 1 \in Z \Rightarrow a * b \in Z$

$\therefore$ Z is closed w.r.t. *

ii) Associative : Let $a, b, c \in Z$

$$(a * b) * c = (a + b + 1) * c$$
$$= a + b + 1 + c + 1 = a + b + c + 2 \quad \text{... (Q.16.1)}$$

and $a * (b * c) = a * (b + c + 1)$

$$= a + b + c + 1 + 1 = a + b + c + 2 \quad \text{... (Q.16.2)}$$

From equation (Q.16.1) and equation (Q.16.2) $(a * b) * c = a * (b * c)$

$\therefore$ * is associative in Z

iii) Existence of the identity :

Let e be the identity in Z

$\therefore$ For any $a \in Z$, $a * e = e * a = a$

$$\Rightarrow a + e + 1 = a$$
$$\Rightarrow e + 1 = a$$
$$\Rightarrow e = -1 \text{ is the identity element in } Z$$

iv) Existence of the inverse :

Let $a \in Z$. Suppose $b \in Z$ is the inverse of a in Z

$\therefore$ $a * b = e$

$$a + b + 1 = -1$$
$$a + b = -2$$
$$b = -a - 2 \in Z$$

$\therefore$ The inverse exists for all $a \in Z$

Thus (Z, *) is a group.

Now consider $a * b = a + b + 1$ $\quad (\because a + b = b + a)$

$= b + a + 1 = b * a \;,\; \forall\, a, b \in \mathbf{Z}$

$\therefore$ * is commutative in $\mathbf{Z}$

$\therefore (\mathbf{Z}, *)$ is an abelian group.

Q.17 Define modulo m **[SPPU : Dec.-11, May-08]**

Ans. : I) Let and b are any integers and m is a fixed positive integer then the addition modulo m denoted by $a +_m b$ and defined as $a +_m b = r$; $0 \le r \le m$

Where r is the least non negative remainder when a + b is divided by m.

e.g. $5 +_3 9 = 2$ as $5 + 9 = 14$ and $14 = 3 \times 4 + 2$

$15 +_5 25 = 0$ as $15 + 25 = 40$ and $40 = 5 \times 8 + 0$

II) Let a and b be any integers and m is a fixed positive integer. Then the multiplication modulo m is denoted by $a \times_m b$ and defined as

$$a \times_m b = r \;;\; 0 \le r \le m$$

Where r is the least non negative remainder when a × b is divided by m.

e.g. $3 \times_4 5 = 3$ as $3 \times 5 = 15$ and $15 = 4 \times 3 + 3$

$9 \times_6 4 = 0$ as $9 \times 4 = 36$ and $36 = 6 \times 6 + 0$

III) If a and be are any two integers such that a − b is divisible by a fixed positive integer m, is called "a congruent to b modulo m".

It is denoted by $a \equiv b \pmod m$

Q.18 Show that $(z_6, +)$ is an abelian group. **[SPPU : May-08]**

Ans. : Let z_6 be the set of residue classes modul o6.

$\therefore \quad z_6 = \{[0], [1], [2], [3], [4], [5]\}$

Or $\quad z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

Consider the following table

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\boxed{\bar{0}}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\boxed{\bar{0}}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\boxed{\bar{0}}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\boxed{\bar{0}}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\boxed{\bar{0}}$	$\bar{1}$	$\bar{2}$	$\bar{1}$
$\bar{5}$	$\bar{5}$	$\boxed{\bar{0}}$	$\bar{1}$	$\bar{2}$	$\bar{8}$	$\bar{4}$

i) Closure Property : Every element of a table belongs to z_6

$\bar{a} + \bar{b} \in z_6 \qquad \forall\, \bar{a}, \bar{b} \in z_6$

$\therefore$ + is closed in z_6

ii) Associativity : By table, for any $\bar{a}, \bar{b}, \bar{c} \in z_6$

$\bar{a} + (\bar{b} + \bar{c}) = (\bar{a} + \bar{b}) + \bar{c}$

$\therefore$ + is associative in z_6

iii) Existence of the Identity : By observing the first row and the first column, such that

For any $\quad \bar{a} \in z_6, \exists\, \bar{0} \in z_6$

$\bar{a} + \bar{0} = \bar{0} + \bar{a} = \bar{a}$

$\therefore \bar{0}$ is the identity element in z_6.

iv) Existence of the Inverse

From table, identify the identity elements

As $\bar{0} + \bar{0} = \bar{0}$, $\quad \bar{0}$ is the inverse of $\bar{0}$

As $\bar{1} + \bar{5} = \bar{5} + \bar{1} = \bar{0}$, $\quad \bar{1}$ is the inverse of $\bar{5}$ and $\bar{5}$ is the inverse of $\bar{1}$

As $\bar{2} + \bar{4} = \bar{4} + \bar{2} = \bar{0}$, $\quad \bar{2}$ is the inverse of $\bar{4}$ and $\bar{4}$ is the inverse of $\bar{2}$

As $\bar{3} + \bar{3} = \bar{0}$, $\quad \bar{3}$ is the inverse of $\bar{3}$

$\therefore$ Every element of z_6 has inverse in z_6.

v) Commutative Property

From table, For all $\bar{a}, \bar{b} \in z_6$

$\bar{a} + \bar{b} = \bar{b} + \bar{a}$

$\therefore$ + is commutative in z_6.

Hence $(z_6, +)$ is an abelian group.

Q.19 Let z = {0, 1, 2, 3, 4, ... (n − 1)} and '◊' be a binary operation such that $a \lozenge b$ = remainder of abelian when divided by n. Construct a table for n = 4,

Is $(z_4, \lozenge)$ is groupoid, monoid, semigroup and abelian group ? **[SPPU : Dec.-11]**

Ans. : We have $z_4 = \{0, 1, 2, 3\}$

Table of z_4 is

$\Diamond$	0	1	2	3
0	$\boxed{0}$	0	0	0
1	0	1	2	3
2	0	2	$\boxed{0}$	2
3	0	3	2	1

i) From table, for any $a, b \in z_4$, $a \Diamond b \in z_4$

$\therefore$ $(z_4, \Diamond)$ is a groupoid and $\Diamond$ is a binary operation in z_4 i.e. $\Diamond$ is closed in z_4.

ii) Semigroup : By table for any $a, b, c, \in z_4$

$$a \Diamond (b \Diamond c) = (a \Diamond b) \Diamond c$$

$\therefore$ $\Diamond$ is associative in z_4

OR Let $a \Diamond b = r$ and $b \Diamond c = t$

$\therefore$ $ab = 4p + r$ and $bc = 4l + t$

$\therefore$ $(a \Diamond b) \Diamond c = r \Diamond c = s$ where $rc = 4q + s$

$a \Diamond (b \Diamond c) = a \Diamond t = k$ where $at = 4m + k$

Prove that $s = k$

$$a(bc) = 4al + at = 4al + 4m + k$$

$$(ab)c = (4p + r)c = 4pc + rc = 4pc + 4q + s \quad \cdots (Q.19.1)$$

Equations (Q.19.1) and equation (Q.19.2) are equal $\cdots (Q.19.2)$

$$\Rightarrow 4al + 4m + k = 4pc + 4q + s$$

$$\Rightarrow k = s$$

Hence $(a \Diamond b) \Diamond c = a \Diamond (b \Diamond c)$

Thus $(z_4, \Diamond)$ is a semigroup

iii) Monoid

By observing the first row and the first column of table

For any $a \in z_4$, $\exists$ $0 \in z_4$ such that

$$a + 0 = 0 + a = a$$

$\therefore$ 0 is the identity element in z_4

Thus from (i), (ii) and (iii), $(z_4, +)$ is a monoid.

iv) Existence of the inverse

From table, identify the identity elements.

x is the inverse of 3 in z_4 and $x \Diamond 3 = 4$ if $3x = 4m + r$

$$x \Diamond 3 = 0$$

$$\therefore \quad 3x - 4m = 0$$

$$\therefore \quad 3x = 4m$$

$$\Rightarrow \quad x = \frac{4m}{3} \quad \text{which is an integer}$$

$$\Rightarrow \quad m = 1, 2, \quad x \text{ is not an integer}$$

For $m = 3$, $x = 4$ which is an integer

For $x = 4 \notin z_4$

But

Thus 3 does not have inverse in z_4

$\therefore$ $(z_4, \Diamond)$ is not a group

Hence $(z_4, \Diamond)$ is not an abelian group.

Q.20 Define permutation group

Ans. : I) Let $S = \{1, 2, 3, \ldots, n\}$ be a finite set with n distinct elements. If $f : S \to S$ is a bijective function then f is called a permutation of degree n.

Let $f(a_1) = b_1$, $f(a_2) = b_2$, $f(a_3) = b_3$, $\ldots f(a_n) = b_4$

Then the permutation is denoted by

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ b_1 & b_2 & b_3 & \ldots & b_n \end{pmatrix} \begin{matrix} \to \text{Elements in Domain} \\ \to \text{Elements in Co-domain} \end{matrix}$$

II) The permutation corresponding to the identity function is called the identity permutation

$$I = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ b_1 & b_2 & b_3 & \ldots & b_n \end{pmatrix}$$

III) If $f_1 = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ b_1 & b_2 & b_3 & \ldots & b_n \end{pmatrix}$ and $f_2 = \begin{pmatrix} b_1 & b_2 & b_3 & \ldots & b_n \\ c_1 & c_2 & c_3 & \ldots & c_n \end{pmatrix}$

Then the product of two permutations is given by

$$f_1 f_2 = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ c_1 & c_2 & c_3 & \dots & c_n \end{pmatrix}$$

(To write product use $a_1 \to b_1 \to c_1 \Rightarrow a_1 \to c_1$ and so on)

6.3 : Subgroup

Q.21 Define Complexes and subgroups

Ans. : 1) Complex of a group : Let $(G, *)$ be a group. Any non empty subset of a group G is called a complex of the group.

e.g. $H_1 = \{1, 2, 3, 4, 5\}$, $H_2 = \{1, 2, 3, \dots\}$, $H_3 = Z$

are complexes of a group $(\Re +)$

2. Subgroup

Let $(G, *)$ be a group. A non empty subset H of a group G, is said to be subgroup of G if $(H, *)$ itself is a group.

Examples

1) $(Z, +)$ is a subgroup of $(\Re +)$
2) $(\Re +)$ is a subgroup of $(\mathbb{C}, +)$
3) $(N, +)$ is not a subgroup of $(Z, +)$
4) $(\Re_0, \cdot)$ is a subgroup of $(\mathbb{C}_0, \cdot)$
5) $(\{1\}, \cdot)$ is a subgroup of $(Q_0, \cdot)$, $(\Re_0, \cdot)$, $(\mathbb{C}, \cdot)$
6) $(\Re +)$ is a subgroup of $(\Re, +)$

Note :

1) $\{e\}$ and $\{G\}$ are subgroups of group G : These subgroups are called improper subgroups.
2) Subgroups which are not improper are called proper subgroups.

Q.22 Explain properties of subgroup with proof.

Ans. : Theorem I) : Prove that the identity of a subgroup is the same as that of the group.

Let H be a subgroup of the group G.

Let e and e' be the identities of G and H respectively.

Now, $a \in H \Rightarrow e' a = a$ ... [$\because$ e' is identity of H]

also $a \in H \Rightarrow a \in G \Rightarrow ea = a$ [$\because$ e is identity of G]

$e'a = ea$

$\therefore$ in G we have, $e' = e$ ... [by right cancellation law in G]

Theorem II) : Prove that the inverse of any element of a subgroup is the same as the inverse of the same regarded as an element of the group.

Let H be a subgroup of the group G.

Let e be the identity of G as well as of H.

Let $a \in H$, suppose b is the inverse of a in H and c is the inverse of a in G. Then we have,

$ba = e$

and $ca = e$

$\therefore$ in G we have, $ba = ca \Rightarrow b = c$

Theorem III) : Prove that the order of any element of a subgroup is the same as the order of the element regarded as a member of the group.

Let H be a subgroup of the group G.

Let $a \in H$, But $a \in G$ and $a^n = e$ in G.

$a^n = e$ in H also. Hence the proof.

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

Suppose H is a subgroup of G.

Let $a \in H$, $b \in H$. Now each element of H must possess inverse because H itself is a group.

$b \in H \Rightarrow b^{-1} \in H$

Further H must be closed with respect to multiplication i.e. the composition in G.

$\therefore a \in H, b^{-1} \in H \Rightarrow ab^{-1} \in H$

i) The condition is sufficient. Now it is given that $a \in H$, $b \in H \Rightarrow ab^{-1} \in H$. We have to prove that H is a subgroup of G.

ii) Existence of identity :

We have $a \in H$, $a \in H \Rightarrow aa^{-1} \in H$ ... By given condition

$\Rightarrow e \in H$

Thus the identity e is an element of H.

iii) Existence of inverse :

Let a be any element of H. Then by the given condition, we have,

$e \in H, a \in H \Rightarrow ea^{-1} \in H \Rightarrow a^{-1} \in H.$

Thus each element of H possesses inverse.

iv) Closure property : Let a, b ∈ H. Then as shown above

$b \in H \Rightarrow b^{-1} \in H$. Therefore applying the given condition we have,

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

v) Associativity : The elements of H are also the elements of G. The composition in G is associative. Therefore, it must also be associative in H.

Hence H itself is a group for the composition in G. Therefore, H is a subgroup of G.

Theorem V) : If H_1 and H_2 are two subgroups of a group G, then $H_1 \cap H_2$ is also a subgroup of G.

Let H_1 and H_2 be any two subgroups of G. Then $H_1 \cap H_2 \neq \phi$ Since at least the identity element e is common to both H_1 and H_2.

In order to prove that $H_1 \cap H_2$ is a subgroup it is sufficient to prove that

$a \in H_1 \cap H_2, b \in H_1 \cap H_2 \Rightarrow ab^{-1} H_1 \cap H_2$

Now, $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ and $a \in H_2$

$a \in H_1 \cap H_2 \Rightarrow b \in H_1$ and $b \in H_2$

But H_1, H_2 are subgroups.

$\therefore$ $a \in H_1, b \in H_1, \Rightarrow ab^{-1} \in H_1$

$a \in H_2, b \in H_2 \Rightarrow ab^{-1} \in H_2$

Finally $ab^{-1} \in H_1, ab^{-1} \in H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$

Thus, we have shown that, $a \in H_1 \cap H_2, b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$

Hence $H_1 \cap H_2$ is a subgroup of G.

Theorem VI) : Show that the union of two subgroups is a subgroup if and only if one is contained in the other.

Suppose H_1 and H_2 are two subgroups of a group G.

Let $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Then $H_1 \cup H_2 = H_2$ or H_1.

But H_1, H_2 are subgroups and therefore, $H_1 \cup H_2$ is also a subgroup.

Conversely suppose $H_1 \cup H2$ is a subgroup. To prove that $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Let us assume that H_1 is not a subset of H_2 and H_2 is also not a subset of H_1.

Now H_1 is not a subset of $H_2 \Rightarrow \exists\, a \in H_1$ and $a \notin H_2$ ... (Q.22.1)

and H_2 is not a subset of $H_1 \Rightarrow \exists\, b \in H_2$ and $B \notin H_1$ ... (Q.22.2)

From equation (Q.22.1) and (Q.22.2).

We have, $a \in H_1 \cup H_2$ and $b \in H_1 \cup H_2$

Since $H_1 \cup H_2$ is a subgroup, therefore $ab = c$ (say) is also an element of $H_1 \cup H_2$.

But $ab = c \in H_1 \cup H_2 \Rightarrow ab = c \in H_1$ or H_2

Suppose $ab = c \in H_1$

Then $b = a^{-1} c \in H_1$,

... [$\because H_1$ is a subgroup. $\therefore a \in H_1 \Rightarrow a^{-1} \in H_1$]

But from (Q.22.2), we have $b \in H_1$. Thus we get the contradiction.

Again suppose $ab = c \in H_2$

Then, $a = cb^{-1} \in H_2$

... [$\because H_2$ is a subgroup, therefore $b \in H_2, \Rightarrow b^{-1} \in H_2$]

But from (Q.22.1), we have $a \notin H_2$. Thus here also we get a contradiction.

Hence either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Q.23 Is union of two subgroups is a subgroup? If not, give example.

Ans. : The union of two subgroups is not necessarily a subgroup.

Let $H_1 = \{...., -4, -2, 0, 2, 4, 6, ...\}$

$H_2 = \{...., -6, -3, 0, 3, 6, ...\}$ are subgroup of $(Z, +)$

Now $H_1 \cup H_2 = \{-6, -4, -3, -2, 0, 2, 3, 4, 6, ...\}$

$2, 3 \in H_1 \cup H_2$ but $2 + 3 = 5 \notin H_1 \cup H_2$

$\therefore$ + is not binary operation on $H_1 \cup H_2$

$\Rightarrow H_1 \cup H_2$ is not a subgroup of G.

Q.24 Define cosets with example.

Ans. : Let (G, ∗) be a group and H be any subgroup of G.

Let a ∈ G be any element, then the set

$H*a = \{h*a / \forall h \in H\}$ is called a right coset of H in G.

and $a*H = \{a*h / \forall h \in H\}$ is called a left coset of H in G.

Note :

1) $H*a$ and $a*H$ are subsets of G.

2) If $(G, *)$ is an abelian group then $H*a = a*H$ in G.

e.g. 1) Let $(\mathbf{Z}, +)$ is a group and

$$H = \{\ldots, -10, -5, 0, 5, 10, \ldots\} \text{ is a subgroup of } G = \mathbf{Z}$$

$\therefore$ For $1 \in \mathbf{Z}$, $H+1 = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$

$3 \in \mathbf{Z}$, $H+3 = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$

$5 \in \mathbf{Z}$, $H+5 = \{\ldots, -5, 0, 5, 10, \ldots\} = H$

are right cosets of H in G.

Q.25 Order of an element of a group

Ans. : Let $(G, \cdot)$ be a group. The smallest positive integer is called the order of an element $a \in G$ if

$$a^n = e(\text{identity element in } G)$$

If is denoted by $o(a) = n$.

If no such positive number exists, then we say that a is of infinite order or zero order.

Note :

1) For the order of the group is the number of distinct elements in G.

2) The order of the identity element is 1 i.e. $o(e) = 1$

3) In a group G, $o(a) = o(a^{-1})$; $\forall a \in G$

4) In a group G, $o(a) \le o(G)$

Q.26 Define cyclic group.

Ans. : A group G is called a cyclic group if $\exists$ at least one element $a \in G$ such that every element $x \in G$ can be written as $x = a^m$ where m is some integer.

The element a is called the generator of G and denoted by $G = \langle a \rangle$

Example 1 : Four fourth roots of unity form a cyclic group with respect to multiplication.

$$G = \{1, -1, i, -i\}$$

We have $(i)^1 = i$, $(i)^2 = -1$, $(i)^3 = -i$, $(i)^4 = 1$

$\therefore$ i is the generator of $G \Rightarrow G$ is a cyclic group.

Moreover, $(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1$

$\therefore$ $-i$ is also generator of G

$$G = \langle i \rangle = \langle -i \rangle$$

Q.27 Define normal subgroups.

Ans. : A subgroup H of a group $(G, *)$ is said to be a normal subgroup of G if for all $g \in G$ and for all $h \in H$

$g*h*g^{-1} \in H$ (We may write $g\,h\,g^{-1} \in H$)

Every group G possesses at least two normal subgroups namely $\{e\}$ and G. These groups are called improper normal subgroups.

Simple group : A group G is said to be simple group if it has only two normal subgroups, $\{e\}$ and G.

Notes :

1) Every subgroup of an abelian group is normal.

2) The intersection of normal subgroups is a normal subgroup.

Q.28 Define quotient groups. ☞[SPPU : Dec.-14. 15, May-15]

Ans. : Let $(G, *)$ be a group and N be a normal subgroup of G. Let G/N be the collection of all cosets of N in G.

$$G/N = \{N*a / a \in G\}$$

$(G/N, *)$ is called the quotient group or factor group.

Q.29 Prove that $(G/N, *)$ is a group. ☞[SPPU : Dec.-15, May-15]

Ans. : Let $(G, *)$ be a group and N is the normal subgroup at G

$\therefore$ $G/N = \{N*a / \forall a \in G\}$

Theorem :

1) Closure property : Let $a, b \in G$, $\therefore N*a, N*b \in G/N$

$(N*a)*(N*b) = N*(a*N)*b$ ($\because$ N is normal)

$= N*(N*a)*b = (N*N)*(a*b)$

$= N*c$ ($\because N*N = N$ and $a*b = c \in G$)

$\therefore (N*a)*(N*b) \in G/N$

$\therefore$ G/N is closed w.r.t. *

2) Associativity : Let $a, b, c \in G$ and $N*a$, $N*b$ and $N*c \in G/N$

$\therefore (N*a)*[(N*b)*(N*c)] = N*a*[N*(b*c)]$

$= N*a*(b*c)$ by (1)

$= N*(a*b)*c)$ by (1)

$= (N*(a*b))*(N*c) = [(N*a)*(N*b)]*(N*c)$ (* is associative in G)

$= [(N*a)*(N*b)]*(N*c)$

Thus * is associative in G/N

3) Existence of the identity :

We have

$N = N*e \in G/N$ and for any $N*a \in G/N$

$(N*a)*(N*e) = N*(a*e)$ (by (1))

$= N*a$

$\therefore$ $N*e = N$ is the identity element in G/N.

4) Existence of the inverse : Let $a \in G$, $N*a \in G/N$

$\therefore \exists\, a^{-1} \in G$ and $N*a^{-1} \in G/N$ such that

$(N*a)*(N*a^{-1}) = N*(a*a^{-1}) = N*e = N$

Hence $N*a^{-1}$ is the inverse of $N*a$ in G/N

Thus (G/N, *) is a group, known as quotient group.

Q.30 Prove lagranges theorem : The order of each subgroup of a finite group is a divisor of the order of the group.

Ans. : Let G be a group of finite order n. Let H be a subgroup of G and let O (H) = m. Suppose $h_1, h_2 \ldots h_m$ are the m members of H.

Let $a \in G$. Then Ha is a right coset of H in G and we have

$$Ha = \{h_1a, h_2a, \ldots\ldots, h_m a\}$$

Ha has m distinct members, since $h_i a = h_j a \Rightarrow h_i = h_j$.

Therefore each right coset of H in G has m distinct members. Any two distinct right cosets of H in G are disjoint i.e. they have no element in common. Since G is a finite group, the number of distinct right cosets of H in G will be finite, say equal to K. The union of these K distinct right cosets of H in G is equal to G.

Thus, if $Ha_1, Ha_2, \ldots\ldots Ha_k$ are the K distinct right cosets of H in G, then

$$G = Ha_1 \cup Ha_2 \cup \ldots\ldots\ldots\ldots \cup Ha_k$$

$\therefore$ The number of elements in G = The number of elements in Ha_1 + The number of elements in Ha_2 + ... + The number of elements in Ha_k

$\therefore$ [$\because$ two distinct right cosets are mutually disjoint]

$O(G) = Km \Rightarrow n = Km$

$K = \frac{n}{m} \Rightarrow$ m is a divisor of n

$\therefore$ O (H) is a divisor of O (G).

Q.31 Prove the order of every element of a finite group is a divisor of the order of the group.

Ans. : Suppose G is a finite group of order n.

Let $a \in G$ and O (a) = m. Prove that m is a divisor of n.

Let $H = \{\ldots\ldots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, \ldots\ldots\}$ be the subset of G consisting of all integral powers of a.

We know that H is a subgroup of G.

We have to show that H contains only m distinct elements and that they are $a, a, a^2, a^3, \ldots\ldots, a^m = e\ a^o$

Let $1 \le r \le m$, $1 \le s \le m$, and $r > s$.

then $a^r = a^s \Rightarrow a^r a^{-s} = a^s a^{-s} \Rightarrow a^{r-s} \Rightarrow a^0 \Rightarrow a^{r-s} = e$

Thus there exists a positive integer $r - s$ less than m such that $a^{r-s} = e$.

m is the least positive integer such that $a^m = e$.

$\therefore$ $a^r \neq a^s$

$\therefore a, a^2, a^3, \ldots\ldots, a^m = a^0 = e$ are all distinct elements of H.

Now suppose at is any element of H where t is any integer.

By division algorithm,

We have, $t = mp + q$ ... [p and q are some integers, $0 \le q < m$]

We have, $a^t = a^{mp+q} = a^{mp} a^q = (a^m)^p a^q = a^q$ ... $(0 \le q < m)$

$\therefore a^q$ is one of the m element $a, a^2, \ldots\ldots, a^m = a^0$

Hence, H has only m distinct elements. Thus order of H is m.

By Lagrange's theorem m is a divisor of n.

Q.32 Prove that if G is a finite group of order n and $a \in G$, then $a^n = e$.

Ans. : In a finite group, the order of each element is finite.
Let $O(a) = m$. The subset H of G consisting of all integral powers of a is a subgroup of G and the order of H is m.
By Lagrange's theorem, m is a divisor of n.

Let $k = \frac{n}{m}$ then $n = mk$

Now, $a^n = a^{mk} = (a^m)^k = e^k$

$= e$ ... $O(a) = m \Rightarrow a^m = e$

6.4 : Cyclic Group

Q.33 Prove that every cyclic group is an abelian group.

[SPPU : Dec.-14, Marks 3]

Ans. : Let $G = \{a\}$ be a cyclic group generated by a.
Let x, y be any two elements of G. Then there exist integers r and s such that $x = a^r$, $y = a^s$.

Now, $xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx$

Thus, we have, $xy = yx \ \forall \ x, y \in G$.
Therefore G is abelian.

Q.34 Prove that If a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Let $G = \{a\}$ be a cyclic group generated by a.
Let a^r be any element of G, where r is some integer.
as $a^r = (a^{-1})^{-r}$
$\therefore -r$ is also some integer.
$\therefore$ Each element of G, is generated by a^{-1}
Thus, a^{-1} is also a generator of G.

Q.35 Prove that every group of order 3 is cyclic.

OR Prove that every group of prime order is cyclic.

Ans. : Suppose G is a finite group whose order is a prime number P, then to prove that G is a cyclic group. As an integer P is said to be a prime number if $P \neq 0$, $P \neq \pm 1$, and if the only divisors of P are $\pm 1, \pm P$.

G is a group of prime order, therefore G must contain at least 2 elements.
So 2 is the least positive prime integer.
There must exist an element $a \in G$ such that $a \neq e$, the identity element e.
Since a is not the identity element, therefore $O(a)$ is definitely ≥ 2.
Let $O(a) = m$. If H is the cyclic subgroup of G generated by a then

$O(H) = O(a) = m$.

By Lagrange's theorem m must be divisor of P.
But P is prime and $m \geq 2$. Hence $m = P$
$\therefore H = G$. Since H is cyclic. Therefore G is cyclic and a is a generator of G.

Q.36 Prove that every subgroup of a cyclic group is cyclic.

Ans. : Suppose $G = \{a\}$ is a cyclic group generated by a. If $H = G$ or $\{e\}$, then obviously H is cyclic. So let H be a proper subgroup of G. The elements of H are integral powers of a. If $a^s \in H$, then the inverse of a^s, i.e. $a^{-s} \in H$.
$\therefore$ H contains elements which are positive as well as negative integral powers of a.
Let m be the least positive integer such that $a^m \in H$.
Then we shall prove that $H = \{a^m\}$
i.e. H is cyclic and is generated by a^m.
Let a^t be any arbitrary element H.
By division algorithm,
there exist integers q and r such that $t = mq + r$, $0 \leq r < m$.

Now, $a^m \in H \Rightarrow (a^m)^q \in H$ ... by closure property

$\Rightarrow a^{mq} \in H \Rightarrow (a^{mq})^{-1} \in H \Rightarrow a^{-mq} \in H$

Also, $a^t \in H$ $a^{-mq} \in H \Rightarrow a^t q^{-mq} \in H \Rightarrow a^{t-mq} \in H \Rightarrow a^r \in H$.
Now m is the least positive integer such that $a^m \in H$ and $0 \leq r < m$.
Therefore r must be equal to 0. Hence $t = mq$.

$\therefore \quad a^t = a^{mq} = (a^m)^q$

Thus every element $a^t \in H$ is of the form $(a^m)q$.
Therefore H is cyclic and a^m is a generator of H.

Q.37 Define the subgroup of a group. Let (G, 0) be a group. Let H = {a | a ∈ G and aob = boa for all b in G}. Show that H is normal subgroup of G.

Ans. : Let (G, x) be a group. A non empty subset H of a group G is said to be a subgroup of G if (H, *) itself is a group.

Given that, $H = \{a \mid a \in G \text{ and } a \circ b = b \circ a ; \forall b \in G\}$

Let $a, b \in H \Rightarrow a \circ x = x \circ a$ and $b \circ x = x \circ b, \forall x \in G$.

$$\Rightarrow (b \circ x)^{-1} = (x \circ b)^{-1}$$
$$\Rightarrow x^{-1} \circ b^{-1} = b^{-1} \circ x^{1}$$
$$\Rightarrow b^{-1} \in H.$$

Now, $(a \circ b^{-1}) \circ x = a \circ (b^{-1} \circ x)$ ... (Q.37.1)

$= a \circ (x \circ b^{-1})$ [∵ o is associative]

$= (a \circ x) \circ b^{-1}$ [∵ use (1) or $b^{-1} \in H$]

$= (x \circ a) \circ b^{-1} = x \circ (a \circ b^{-1})$ [∵ $a \in H$]

$\Rightarrow \quad a \circ b^{-1} \in H$

Therefore H is a subgroup of group G.

Let $h \in H$ and $g \in G$ and any x in G.

Consider,

$(g \circ h \circ g^{-1}) \circ x = (g \circ g^{-1} \circ h) \circ x$

$= (e \circ h) \circ x = h \circ x = x \circ h$ [∵ $h \in H$]

$= x \circ (h \circ g \circ g^{-1}) = x \circ (g \circ h \circ g^{-1})$ (∵ $h \in H$)

$\Rightarrow g \circ h \circ g^{-1} \in H$ for any $g \in G$ (∵ $h \in H$)

∴ H is a normal subgroup of G.

Q.38 Show that the four permutations I, (a b), (c d), (a b) (c d) on four symbols a, b, c, d form a finite abelian group with respect to the multiplication.

Ans. : Let

$$f_1 = I = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$$

$$f_2 = (a\ b) = \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix}$$

$$f_3 = (c\ d) = \begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix}$$

$$f_4 = (a\ b)\ (c\ d) = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}$$

$$G = \{f_1, f_2, f_3, f_4\}$$

Consider the multiplication table

X	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

(i) **Closure property :** All elements of table belong to G. (G, x) is closed w.r.t. x.

(ii) **Multiplication** of permutations is associative.

(iii) $f_1 = I$ is the identity element in G.

(iv) In G, $f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$ and $f_4^{-1} = f_4$

(v) Multiplication table is symmetric about main diagonal ∴ (G, x) is commutative.

Hence (G, x) is an ablein group of order 4.

6.5 : Homomorphism and Isomorphism

Q.39 Define homomorphism of groups with properties.

[SPPU : Dec.-15, 14, 12, 11, May-15]

Ans. : Let $(G_1, *)$ and (G_2, o) be two groups. A function $f : (G_1, *) \to (G_2, o)$ is said to be homomorphism.

If $f(a * b) = f(a) \circ f(b)$ for all $a, b \in G_1$.

i.e. $a * b$ in $G_1 \to f(a) \circ f(b)$ in G_2

A homomorphism from G to itself is called as endomorphism.

Properties of Group Homomorphism.

Let $f : G_1 \to G_2$ be group homomorphism and $((G_1, *)$ and $(G_2 * o)$ are groups then

i) $f(e_1) = (e_2)$

ii) $f(a^{-1}) = [f(a)]^{-1}$

Proof : 1) Let $a \in G_1$ and $f(a) \in G_1$ and e_2 is the identity element in G_2.

$\therefore$ $f(a) o e_2 = f(a) = f(a * e_1)$

$f(a) o e_2 = f(a) o f(e_1)$

$\Rightarrow f(e_1) = e_2$

2) Let $a \in G_1$ then $a^{-1} \in G$

and $e_2 = f(e_1) = f(a * a^{-1})$

$e_2 = f(a) o f(a^{-1})$ (f is homomorphism)

$\Rightarrow$ $f(a^{-1}) = [f(a)]^{-1}$

Q.40 Define isomorphism of groups.

[SPPU : Dec.-13, 12, 11, 10, May-08, 10]

Ans. : Let $(G_1, *)$ and (G_2, o) be two groups. A function $f : (G_1, *) \to (G_2, o)$ is said to be isomorphism.

If i) f is a homomorphism from $G_1 \to G_2$, ii) f is bijective function.

If $f : G_1 \to G_2$ is an isomorphism of groups then G_1 and G_2 are called as isomorphic groups and denoted by $G_1 \cong G_2$.

An isomorphism from G to itself is called as automorphism of group G.

Q.41 Let G be a group with identity e show that a function $f : G \to G$ defined by $f(a)\ \forall = e, a \in G$ is a homomorphism (Endomorphism).

[SPPU : May-08, 10, Marks 3]

Ans. : We have $f : G \to G$ and $f(a) = e, \forall a \in G$.

Let $a, b \in G \Rightarrow f(a), f(b) \in G$

$\therefore$ $f(a * b) = e$ (as $a * b \in G$)

$= e * e = f(a) * f(b)$

$\therefore$ f is a homomorphism.

Q.42 Explain homomorphism and antomorphism of groups with examples.

[SPPU : Dec.-11, 12, 13, Marks 3]

Ans. : Refer Q.39 and Q.40 for definition.

1) The homomorphism $f : (Z, +), (Z, +)$ such that $f(n) = -n$ is an antomorphism of group.

2) The homomorphism $f : (R_o, o) \to (R_o, o)$ such that $f(x) = x;\ \forall x \in \Re_o$ is an antomorphism of groups.

Q.43 Let $\Re$ be the additive group of real numbers and $\Re +$ be the multiplicative group of positive real numbers. Prove that the mapping $f : (R, +) \to (\Re, X)$ defined by $f(x) = e^x, \forall x \in \Re$ is an isomorphism of $\Re$ onto $\Re$

[SPPU : Dec.-10, Marks 4]

Ans. : If x is any real number, then e^x is always positive real number and e^x is unique. Therefore, $f : \Re \to R_+$ is a function such that $f(x) = e^x$.

Let $x_1, x_2 \in \Re$ then $f(x_1) = f(x_2)$

$\Rightarrow$ $e^{x1} = e^{x2} \Rightarrow x_1 = x_2$

$\therefore$ f is one to one mapping.

For any $y \in \Re$ then $\log y \in \Re$ such that

$f(\log y) = e^{\log y} = y$

$\therefore$ f is onto.

Now for any $x_1, x_2 \in \Re$

Consider, $f(x_1 + x_2) = e^{x1+x2} = e^{x1 \times x2} = f(x_1) \times f(x_2)$

$\therefore$ f preserves compositions in $\Re$ and $\Re +$

$\therefore$ f is an isomorphism of $\Re$ onto $\Re +$.

Hence $\Re \cong \Re$

6.6 : Rings

Q.44 Define rings, integral domains and fields.

[SPPU : Dec.-08, 10, 11, 12, 13, 14, May-14]

Ans. : 1. Rings

Let R be a non empty set equipped with two binary operations called addition and multiplication and denoted by '+' and '·' respectively.

An algebraic structure (R,+, ·) is called a ring if it satisfies following axioms.

1) (R, +) is an abelian group i.e.

i) **Closure property :** for $a, b \in R$, $a + b \in R$

ii) **Associativity :** for $a, b, c \in R$, $a + (b + c) = (a + b) + c$

iii) **Existence of the identity :** For any $a \in R$, $\exists\ 0 \in R$ s.t.,
$a + 0 = 0 + a = a$.

$\therefore$ 0 is called as the additive identity element of ring.

iv) **Existence of the inverse :** for each $a \in R$, $\exists\ -a \in R$
Such that $a + (-a) = -a + a = 0$
$-a$ is called the additive inverse of a

v) **Commutative property :** For $a, b \in R$
$a + b = b + a$

2) $(R, \cdot)$ is semigroup i.e.

i) **Closure property :** $\forall a, b \in R$, $a \cdot b \in R$

ii) **Associativity :** for $a, b, c \in R$,
$a \cdot (b \cdot c) = (a \cdot b) \cdot c$

3) Multiplication distributes over addition $\forall a, b, c \in R$

i) $a \cdot (b + c) = a \cdot b + a \cdot c$ (Right distributive law)

ii) $(a + b) \cdot c = a \cdot c + b \cdot c$ (Left distributive law)

2. Commutative ring : A ring $(R, +, \cdot)$ is said to be commutative ring if $\forall\ b \in R$, $a \cdot b = b \cdot a$

3. Ring with unity : A ring $(R, +, \cdot)$ is said to be ring with unity if $\forall\ a \in R$, $\exists$, $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$.

Examples :

1) $(\mathbf{Z}, +, \cdot)$ is a commutative ring with unity.

2) $(2\mathbf{Z}, +, \cdot)$ is a commutative ring without unity where $2\mathbf{Z}$ = set of even integers.

3) The set of $n \times n$ matrices over real numbers with respect to usual matrix addition and multiplication is a non commutative ring with unity.

4. Properties of a ring : If $(R, +, \cdot)$ is a ring with identity 0 and unit element 1 then following are true for all $a, b, c \in R$.

i) $a \cdot 0 = 0 \cdot a = 0$

ii) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

iii) $(-a)(-b) = a \cdot b$

iv) Unit element is unique

5. Subring : Let $(R, +, \cdot)$ be a ring. A non empty subset S of R is said to be subring of R if $(S, +, \cdot)$ is a ring. e.g. $(\mathbf{Z}, +, \cdot)$ is a subring of $(\mathbf{R}, +, \cdot)$.

6. Zero divisors : Let $(R, +, \cdot)$ be a commutative ring. An element $a \neq 0$ in R is said to be zero divisor if $\exists\ b \neq 0$ in R such that $a \cdot b = 0$.

A ring $(R, +, \cdot)$ is said to be without zero divisors.

if $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$, $\forall a, b \in R$.

e.g. 1) $\bar{2}$ is a zero divisor in $(\mathbf{Z}_4, +, \cdot)$ as $\bar{2} \cdot \bar{2} = \bar{4} = 0$

2) $(M_{2\times 2}\ \Re, +, \cdot)$ is a ring with zero divisors.

as $$A \cdot B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0 \text{ but } A \neq 0 \text{ and } B \neq 0$$

3) $(\mathbf{Z}, +, \cdot)$ is a ring without zero divisors i.e. $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$.

7. Integral domain

A commutative ring with zero divisors is called an integral domain.

e.g. 1) $(\Re, +, \cdot)$, $(\mathbf{Z}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are integral domains.

2) $(\mathbf{Z}_4, +, \cdot)$ is a ring with zero divisors

$\therefore$ It is not integral domain.

8. Field

A commutative ring with unity in which every non zero element possesses their mulplicative inverse, is called as field.

A field is an integral domain.

e.g. 1) $(\Re, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(Q, +, \cdot)$ are fields.

2) $(\mathbf{Z}, +, \cdot)$ is integral domain but not field.

9. Ring homomorphism

Let $(R, +, *)$ and $(S, +', \xi *')$ be two rings.

A function $\phi : R \to S$ is called a ring homomorphism

If for any $a, b \in R$

i) $\phi(a + b) = \phi(a) +' \phi(b)$

ii) $\phi(a * b) = \phi(a) *' \phi(b)$

If ϕ is bijective then it is called as a ring isomorphism.

The kernal of ring homomorphism is defined as the set $\{a \in R \mid \phi(x) = 0\}$

It is denoted by ker (ϕ) or ker ϕ.

Q.45 Let $R = \left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix} : a, b \in z\right\}$ f is the mapping that takes $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ to a – b.

i) Show that f is a homomorphism. ii) Find Kernel of f.

Ans. : i) $f = \left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} + \begin{bmatrix} c & d \\ d & c \end{bmatrix}\right) = f\left(\begin{bmatrix} a+c & b+d \\ b+d & a+c \end{bmatrix}\right) = (a+c)-(b+d)$ **[SPPU : Dec.-08]**

$$= (a-b)+(c-d) = f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) + f\left(\begin{bmatrix} c & d \\ d & c \end{bmatrix}\right)$$

Also $f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right)\cdot\left(\begin{bmatrix} c & d \\ d & c \end{bmatrix}\right) = f\begin{bmatrix} ac+bd & ad+bc \\ bc+ad & bd+ac \end{bmatrix} = (ac+bd)-(ad+bc)$

$$= (ac-bc)+(bd-ad) = (a-b)(c-d)$$

$$= f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right)\cdot f\left(\begin{bmatrix} c & d \\ d & c \end{bmatrix}\right)$$

ii) Ker $f = \left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix} : a-b=0\right\}$ i.e. $\left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} ; a \in z\right\}$

Q.46 Show that $S = \{a+b\sqrt{2}; a, b \in z\}$ for the operations +, × is an integral domain but not a field.

Ans. : We have, **[SPPU : Dec.-14]**

$$(a+b\sqrt{2})+(c+d\sqrt{2}) = (a+c)+(b+d)\sqrt{2}$$

$$(a+b\sqrt{2})+(c+d\sqrt{2} = (ac+2bd)+(bc+ad)\sqrt{2}$$

Clearly S is commutative ring with unit element 1.

We have to prove S is an integral domain.

Let $(a+b\sqrt{2})(c+d\sqrt{2}) = 0$

$$ac + 2bd = 0 \quad \ldots (Q.46.1)$$

$$bc + ad = 0 \quad \ldots (Q.46.2)$$

Suppose $a = 0$; then $bd = bc = 0$

either $b = 0$ or both $d = c = 0$

Hence, if $a = 0$, $a+b\sqrt{2} = 0$

or $c+d\sqrt{2} = 0$

Assume $a \neq 0$. Multiplying equation (Q.46.1) by d

we have, $acd + 2bd^2 = 0 \quad \ldots (Q.46.3)$

From equation (Q.46.2)

$$ad = -bc$$

Hence substituting this value in equation (Q.46.3)

We have, $-bc^2 + 2bd^2 = 0$

$\Rightarrow b(2d^2 - c^2) = 0$

$\therefore b = 0$ or $c^2 = 2d^2$, i.e. $c = \sqrt{2}\,d$

Since c is an integer, $c^2 = 2d^2$ is true only if $c = d = 0$

Hence if $c^2 \neq 2d^2$, $b = 0$. But $b = 0$ implies $a = 0$

Hence, in any case either $a + b\sqrt{2} = 0$ or $c + d\sqrt{2} = 0$

Hence, S is an integral domain.

To show that S is not a field consider the element $2+\sqrt{2}$. It's multiplicative inverse does not exit in S, for $(2+\sqrt{2})(c+d\sqrt{2}) = 1$

$$\Rightarrow \quad 2c + 2d = 1 \Rightarrow c + d = \frac{1}{2}$$

Absurd, since $c, d \in z$.

Q.47 Let $z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Let R is a relation under the operations addition modulo 7 and multiplication modulo 7. Does this system form a ring ? It is a commutative ring ? **[SPPU : Dec.-11]**

Ans. : Consider the following tables,

Table 1 :

$\times_7$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	0
2	0	2	4	6	1	3	5	0
3	0	3	6	2	5	1	4	0
4	0	4	1	5	2	6	3	0
5	0	5	3	1	6	4	2	0
6	0	6	5	4	3	2	1	0
7	0	0	0	0	0	0	0	0

Table 2 :

$+_7$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	0	1
2	2	3	4	5	6	0	1	2
3	3	4	5	6	0	1	2	3
4	4	5	6	0	1	2	3	4
5	5	6	0	1	2	3	4	5
6	6	0	1	2	3	4	5	6
7	0	1	2	3	4	5	6	0

I) S.T. $(z_8, +_7)$ is an abelian group.

i) From table 2, all element are in z_8 $\therefore$ z_8 is closed w.r.t. $+_7$

ii) Associativity : for all a, b c $\in z_8$.

$a +_7 (b +_7 c) = (a +_7 b) +_7 c$

iii) By observing the first row of table 2. 0 is the additive identy in z_8.

6.7 : Group Codes

Q.48 Explain Group Code

Ans : Let S_n be the set of all binary words of length n. Let $\oplus$ be a binary operation on S_n such that for all x, y $\in S_n$ where

$x = (x_1, x_2, \ldots, x_n)$ & $y = (y_1, y_2, \ldots, y_n)$

$x \oplus y = (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n)$

Where the operation $\oplus$ denotes the addition modulo 2 on {0, 1} and is given by the following table.

$\oplus$	0	1
0	0	1
1	1	0

The algebraic structure $(S_n, \oplus)$ forms a group in which n tuple of 0's (0, 0, 0, ..., 0) is the identity and each element is its own inverse. In general, any code which is a group under the operation $\oplus$ is called a group code. Group code was first introduced by Hamming and it is very useful in binary encoding techniques.

e.g. if $x = (1\ 0\ 1\ 0\ 1)$ and $y = (0\ 1\ 1\ 0\ 0)$

then $x \oplus y = (1\ 1\ 0\ 0\ 1)$

Q.49 Define hamming Distance **[SPPU : Dec.-11, Dec.-15]**

Let x be a word is S_n. The weight of x is denoted by w(x) and defined as

$$w(x) = \text{Number of one's in } x$$

e.g. $w(0\ 0\ 1\ 0\ 1) = 2$, $w(0\ 0\ 0) = 0$, $w = (1\ 1\ 1\ 1) = 4$

Let $x = (x_1, x_2, \ldots, x_n)$ $y = (y_1, y_2, \ldots, y_n)$ be any two elements in $(S_n, \oplus)$. The Hamming distance between x and y is denoted by d(x,y) and defined as

d (x, y) = The number of co-ordinates at which x_i and y_i are different.

e.g. If $x = (1\ 0\ 1\ 1\ 0\ 1)$

$$y = (0\ 1\ 1\ 1\ 1\ 0)$$
$$\downarrow\downarrow \quad \downarrow\downarrow$$
different

$\therefore$ $d(x, y) = 4$, as x and y have first second, fifth, sixth positions different)

Now $x \oplus y = (1\ 1\ 0\ 0\ 1\ 1)$

$w(x \oplus y) = 4 = d(x, y)$

Thus for any $x, y \in S_n$, $d(x, y) = w(x \oplus y)$

Properties of Hamming Distance :

Let $x, y, z \in (S_n, \oplus)$ then

i) $d(x, y) \geq 0$

ii) $d(x, y) = 0$ iff $x = y$

iii) $d(x, y) = d(y, x)$

iv) $d(x, z) \leq d(x, y) + d(y, z)$

The minimum distance of a code is the minimum of all the distances between district pair of code words.

e.g. Let $x\ (1\ 1\ 0\ 1\ 1\ 0)$, $y = (0\ 0\ 1\ 1\ 1\ 1)$, $z = (1\ 0\ 1\ 0\ 1\ 0)$

$\therefore$ $d(x, y) = 4$, $d(y, z) = 3$, $d(x, z) = 3$

Out of 4, 3, 3, minimum is 3.

Therefore the minimum distance between the words x, y, z is 3

By using the weight and minimum distance, a combination of errors can be detected and corrected.

Theorem 1) The minimum weight of the non zero code words in a group code is equal to its minimum distance.

Theorem 2) A code can detect all combinations of k or fewer errors iff the minimum distance between any two code words is at least k +1,

Theorem 3) A code can correct all combinations of k or fewer errors iff the minimum distance between any two code words is at least 2k+1.

For example, Let a code containing words of length 3

$c = \{(0, 0, 0), (1, 1, 1)\}$, c contains only two words.

The minimum weight of non zero code word is 3.

$\therefore$ By theorem 1, the minimum distance is also 3.

By theorem 2, this code can detect any combination of two errors or one error. And by theorem 3, this code can correct only one error.

Q.50 Explain generation of codes by using parity checks

Ans. : In 1950, Hamming developed the first complete error detecting and error correcting encoding procedure. This procedure has been frequently used in computer systems.

Hamming constructed the codes, called Hamming codes by introducing redundant digit called parity digits. In a message, that is n digits long, m digits ($m < n$) are used to represent the information part of the message and the remaining $k = n - m$ digits are used for the detection and correction of errors. These K digits are called parity checks.

Hamming single error detecting codes can be described as follows.

i) The actual message is contained in the first (n–1) digits of a code word of length n and the last digit position is set to 0 or 1 so as to make the entire message contain an even numbers of 1's. such an encoding procedure is called a even parity check.

ii) Odd parity check can be used by making the entire message containing an odd no. of 1's. e.g. In even parity check {00, 10, 11}

becomes {000, 101, 110} In odd parity check { 00, 01, 10, 11}

becomes {001, 010, 100, 111}

The code words of length n in which information is contained m digits ($m < n$) and remaining $k = n - m$ digits are parity checks, can be generated by using $k \times n$ matrix H. This matrix is called parity check matrix, where elements are from set {0, 1} A single error correcting code of length n generated by H with k parity check is given by

$$2^k \geq n + 1 = (k + m) + 1$$

$$\therefore \quad m \leq 2^k - k - 1$$

The number of code words generated by H is $2^m = 2^{n-k}$ and the code generated in this way called the Hamming code.

Theorem 1 : Let H be a parity check matrix which consists of k rows and n columns. Then the set of words $x = (x_1, x_2, x_3, \ldots x_n)$ which belongs to the following set.

$C = \{ x \mid xH^t = 0 \pmod 2 \}$ is a group code under the operation $\oplus$ (addition modulo 2) where H^t = Transpose of matrix H.

Theorem 2 : The parity check matrix H generates a code word of weight q iff $\exists$ a set of columns of H such that their k - tuple sum is zero.

For the parity check matrix H of order $k \times n$.

Where n = Length of code word

k = Number of parity check bits

The information digits will be $m = n - k$. The number of code words generated is $2^m = 2^{n-k}$. Consider the following steps for the generation of code words.

Step 1 : Find the system of equations from $x \cdot H^t = 0$.

Step 2 : Find the values of parity check bits interms of information digits from the equations obtained in step 1.

Step 3 : Give values 0 or 1 to information digits and calculate the values of parity check bits according to step 2. The binary words obtained in this way will be the required code words generated by H.

To find the number of errors defected and corrected first find the columns of H whose sum (addition modulo 2) is zero. The number of these columns is equal to the minimum weight of the code and which is equal to the minimum distance of the code.

Q.51 Find the minimum distance of an encoding function $e : B^2 \to B^5$ given as .

e (0 0) = 00000, e (0 1) = 1 0 0 1 1, e (1 0) = 0 1 1 1 0, e (1 1) = 1 1 1 1 1.

Ans. : **[SPPU : Dec.-06]**

d [e (0 0), e (0 1)] = 3 d [e (0 0), e (1 1)] = 5

d [e (0 0), e (0 1)] = 3 d [e (0 0), e (1 0)] = 3

d [e (0 1), e (1 0)] = 4 d [e (0 1), e (1 1)] = 2

d [e (1 0), e (1 1)] = 2

The minimum along all distances is 2.

Thus the minimum distance of an encoding is 2.

Q.52 What is Hamming function (distance) ? Find the distance between the code words of C = { (0 0 0 0), (0 1 0 1), (1 0 1 1), (1 1 1)} Rewrite the message by adding even parity check bit and parity check bit. **[SPPU : Dec.-11, Marks 5]**

Ans. : Refer Q.50 for the definition. We have

d [e (0 0 0 0), e (0 1 0 1)] = 2 d [e (0 0 0 0), e (1 0 1 1)] = 3

d [e (0 0 0 0), e (0 1 1 1)] = 3 d [e (0 1 0 1), e (1 0 1 1)] = 3

d [e (0 1 0 1), e (0 1 1 1)] = 1 d [e (1 0 1 1), e (0 1 1 1)] = 2

Even parity check bit of c is

{(0 0 0 0 0), (0 1 0 1 0), (1 0 1 1 1), (0 1 1 1 1)}

Odd parity check bit of c is

{(0 0 0 0 1), (0 1 0 1 1), (1 0 1 1 0), (0 1 1 1 0)}

Q.53 Given the parity check matrix $H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$ **find the minimum distance of code generated by H. How many errors can it detect and correct.** **[SPPU : Dec.-15, Marks 5]**

Ans. : From the given matrix H, select minimum number of column whose sum is zero.

$\therefore$ Consider columns $h_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$, $h_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$, $h_3 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$

The sum of these columns

$$h_1 \oplus h_2 \oplus h_3 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

Hence the minimum weight of the code is 3 which is equal to its minimum distance.

We know that the code can detect all combinations of k or fever errors iff the minimum distance between any two code words is at least k +1.

Here minimum distance is $3 = k+1 \Rightarrow k = 2$.

$\therefore$ This code can detect 2 or less errors.

Also it can correct k errors if the minimum distance is 2k + 1

$\therefore \quad 2k + 1 = 3 \Rightarrow k = 1$

This code can correct only one error.

Therefore this is a single error correcting code.

Q.54 Find the number of code words generated by the parity check matrix H given by $H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$ **find all the code words generated.**

[SPPU : Dec.-12, Marks 5]

Ans. : The parity check matrix is

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}_{3\times 6}$$

H is of order 3×6. Hence the length of the code word is 6 in which three digits are parity check bits. The information digits are

$$M = n - k = 6 - 3 = 3$$

$\therefore$ The matrix H will generate. $2^m = 8$ code words.

They are the solution of $x \cdot H^t = 0$.

$$[x_1\ x_2\ x_3\ x_4\ x_5, x_6] \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [0\ \ 0\ \ 0]$$

$$\Rightarrow \begin{aligned} x_1 + x_2 + \quad + x_4 + \quad &= 0 \\ x_2 + x_3 + \quad + x_5 + \quad &= 0 \\ x_1 + \quad + x_3 + \quad + x_6 &= 0 \end{aligned}$$

$$\Rightarrow \begin{aligned} x_4 &= x_1 + x_2 \\ x_5 &= x_2 + x_3 \\ x_6 &= x_1 + \quad + x_3 \end{aligned}$$

By giving different combinations of 0 and 1 to x_1, x_2, x_3, we get the following code words.

END...