Algorithm:

Suppose a transport network with the capacity of each edge is given.

1. Initially, assign the zero flow to each edge of the given network. Also assign the label $(-, \infty)$ to the source s.
2. Scan all those vertices which are adjacent to the source s. Suppose the vertex b is adjacent to s and c (s, b) > f (s, b) then label the vertex b as $(s^+, \Delta b)$ where Δb = c (s, b) - f (s, b). The vertex b is not labeled if c (s, b) = f (s, b).
3. Scan those vertices which are adjacent to labeled vertices. Suppose the vertex q is adjacent to the labeled vertex b. The vertex q is labeled $(b^+, \Delta q)$ where Δq is equal to the smaller of the two quantities Δb and [c (b, q)- f (b, q)] if c (b, q) > f (b, q).

   The vertex q is not labeled if c (b, q) = f (b, q).

   Also the vertex q is labeled $(b^-, \Delta q)$ where Δq is equal to the smaller of the two quantities Δb and f (q, b) if f (q, b) > 0. The vertex q is not labeled if f (q, b) = 0.

   Such a labeling process is not unique. The vertex q might be adjacent to or from more than one labeled vertex. In such case, when a vertex can be labeled in more than one way, an arbitrary choice is to be made.
3. Repeat the step 2 (labeling the vertices that are adjacent to or from the labeled vertices) till we reach to the sink t.
4. If the sink t is labeled with the label $(y^*, \Delta t)$ where y is some labeled vertex, then increase the flow of the edge (y, t) from f (y, t) to f (y, t) + Δ t. Note that the vertex y must be labeled either $(q+, \Delta y)$ or $(q-, \Delta y)$ with $\Delta y \geq \Delta t$ for some vertex q. If y is labeled $(q+, \Delta y)$ then increase the flow in the edge (q, y) from f (q, y) to f (q, y) + Δt. On the other hand, if y is labeled $(q-, \Delta y)$ then decrease the flow in the edge (y, q) from f (y, q) to f (y, q)- Δt. This process is continued back to the source s and the value of the flow in the transport network will be increased by amount Δt. Again start the labeling process to further increase the value of the flow in the network i.e. go to step 2.
5. If the sink t is not labeled, then denote all the labeled vertices by P and all unlabeled vertices by $\bar{P}$. Determine the capacity of the cut $(P, \bar{P})$ which is the value of the maximal flow.

Now we illustrate few examples.

SOLVED EXAMPLES

Example 1: *Determine the maximal flow in the following transport network.*

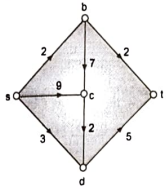

Fig. 7.146

Solution: Step 1: Assign the flow zero to each edge and the label (–,) to the source s.

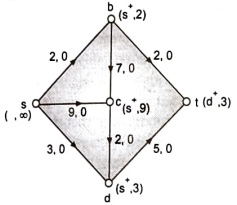

Fig. 7.147

Step 2: The vertices b, c, d are adjacent to the source s. Therefore, we label the vertices b, c, d. For the vertex b, c (s, b) – f (s, b) = 2

Thus the label of the vertex b is $(s^+, 2)$.

Similarly the labels of c and d are $(s+, 9)$ and $(s+, 3)$.

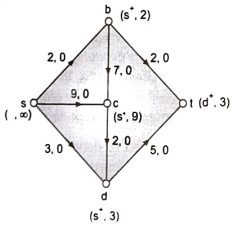

Fig. 7.148

Now the sink t is adjacent to both the vertices b and d. So we can choose any vertex b or d for labelling of sink t. Let us choose the vertex d. For the vertex d, the label is $(s^+, 3)$ and

c (d, t) – f (d, t) = 5 – 0 = 5

Minimum of 3 and 5 is 3 and thus the label of sink t will be $(d^+, 3)$. According to the label of the sink, adjust the flow in the edges (d, t) and (s, d).

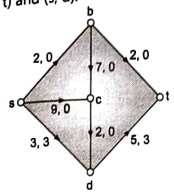

Fig. 7.149

Repeat the step 2. In each pass the new value of the flow is obtained.

Step 3:

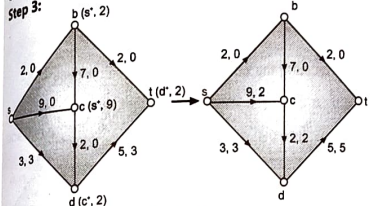

Fig. 7.150

Step 4:

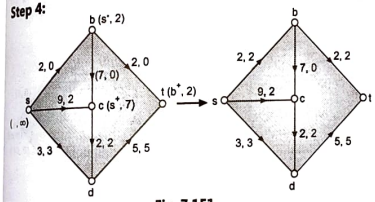

Fig. 7.151

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

Example 2: *Solve the following network problem.* **(Dec. 2014)**

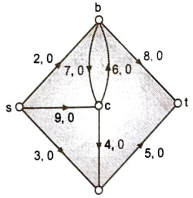

Fig. 7.152

Solution: Different iterations for the maximum flow are given as follows:

Step 1:

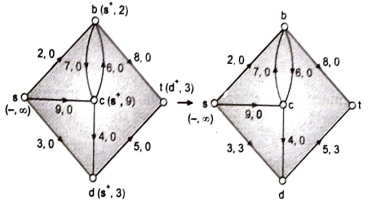

Fig. 7.153

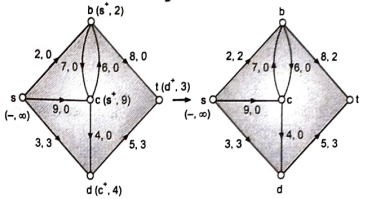

Fig. 7.154

Step 2:

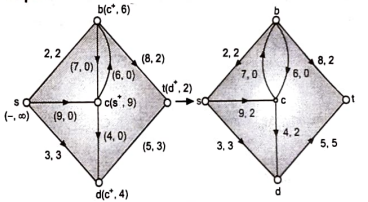

Fig. 7.155

Step 3:

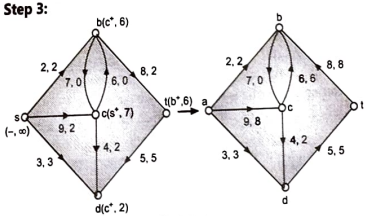

Fig. 7.155

The maximum flow is 13.

Example 3: *Use labeling procedure to find a maximum flow in the transport network shown in the following figure. Determine the corresponding minimum cut.* **(Dec. 2014)**

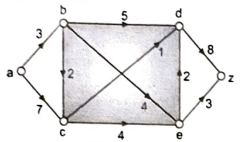

Fig. 7.156

Solution: To find the maximum flow in the given transport network, assign the flow zero to each edge and label (–,) to the source a.

Step 1:

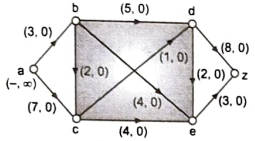

Fig. 7.157

Step 2: Since the vertices b and c are adjacent to the source a, therefore label the vertices b and c as (a+, Δb) and (a+, Δc) respectively, where

$$\Delta b = C(a, b) - f(a, b) = 3$$

$$\Delta c = C(a, b) - f(a, c) = 7$$

Label of b is $(a^+, 3)$ and label of c is $(a^+, 7)$.

Now, the vertices d and e are adjacent to labeled vertices b $(a^+, 3)$ and c $(a^+, 7)$, therefore, we label the vertices d and e as $(b^+, \Delta d)$ and $(c^+, \Delta e)$, where

$$\Delta d = \min(\Delta b, C(b, d) - f(b, d)) = \min(3, 5, -0)$$

$$\Delta d = 3$$

$$\text{Similarly, } \Delta e = \min(\Delta c, C(c, e) - f(c, e)) = \min(7, 4, -0)$$

$$\Delta e = 4$$

Label of d is $(b^+, 3)$ and label of e is $(c^+, 4)$.

Now, the sink z is adjacent to both the vertices d and e, we can choose any vertex d or e to label the sink z. Let us choose the vertex e, which is labeled as (c+, 4). The label of z will be (e+, Δz) where

$$\Delta z = \min(4, 3, -0)$$

$$\Delta z = 3$$

Hence, label of z is $(e^+, 3)$.

The labels of vertices can be shown as follows:

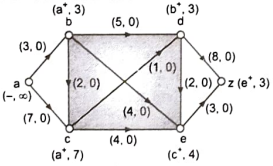

Fig. 7.158

Step 3:

According to the label of the sink z, adjust the flow in the edges (e, z), (c, e) and (a, c).

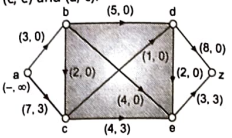

Fig. 7.159

Repeat the step 2. In each pass, the new value of the flow is obtained.

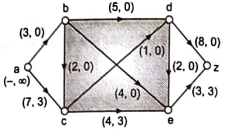

Fig. 7.160

After adjusting the flow, we have

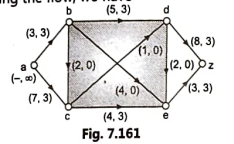

Fig. 7.161

Step 4:

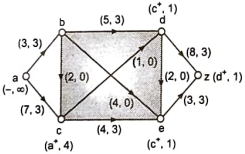

Fig. 7.162

Adjust the flow according to sink z label.

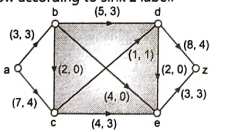

Fig. 7.163

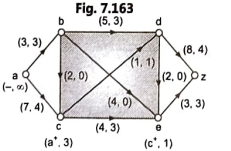

Fig. 7.164

Since the vertex z (sin k) cannot be labeled, we have to stop. The vertices b , d and z cannot be labelled because whether the edges approaching to vertices are saturated or the edges in the opposite direction have flow zero. At this stage, we have minimum cut (P, (P is the set of labelled vertices $P = \{a, c, e\}$, is the set of unlablled vertices, The edges in cut $P\{(a, b), (c, d), (e, z)\}$.

Capacity of the cut is C (a, b) + C (c, d) + C (e, z) = 3 + 1 + 3 = 7.

Hence, the maximum flow in the given transport network = 7.

Example 4: *Find the maximum flow in the following transport network using labelling procedure. Also specify saturated and unsaturated edges.*

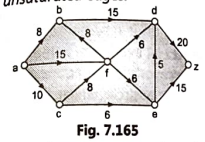

Fig. 7.165

Solution: Various iterations for the maximum using labelling process are given below.

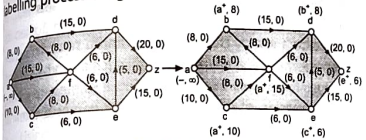

Fig. 7.166 (a)

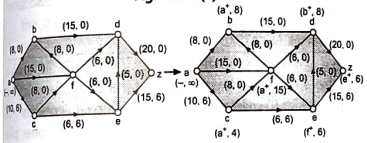

Fig. 7.166 (b)

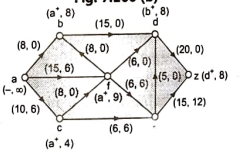

Fig. 7.166 (c)

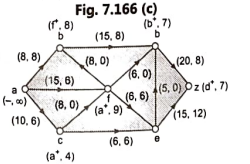

Fig. 7.166 (d)

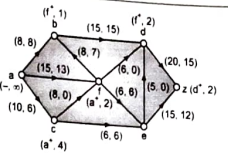

Fig. 7.166 (e)

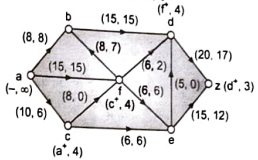

Fig. 7.166 (f)

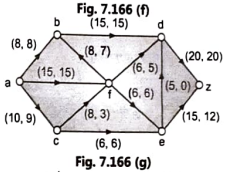

Fig. 7.166 (g)

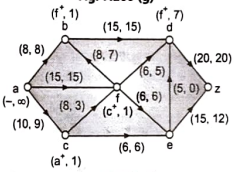

Fig. 7.166 (h)

Since z cannot be labelled, we will stop. Minimum cut = {(c, e), (f, e), (d, z)}.

The capacity of cut is C (c, e) + C (f, e) + C (d, z) = 6 + 6 + 20 = 32.

The maximum flow in the network is 32.

The saturated edges are {(a, b), (b, d), (d, z), (a, f), (c, e), (f, e)}

Unsaturated edges are {(a, c), (c, f), (f, d), (f, b), (e, d), (e, z)}

Example 5: *Find maximum flow in the transport network using labelling procedure. Determine the corresponding minimum cut.* ***(April 2018)***

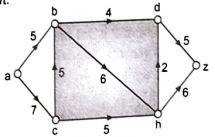

Fig. 7.167

Solution: The maximum flow in the transport network using labelling procedure can be obtained using following steps.

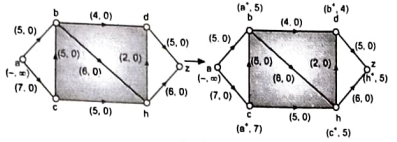

Fig. 7.168

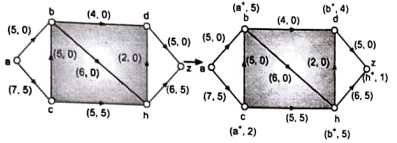

Fig. 7.169

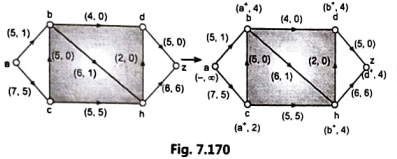

Fig. 7.170

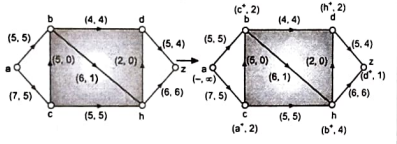

Fig. 7.171

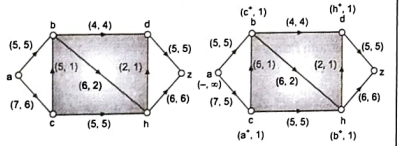

Fig. 7.172

Since Z cannot be labeled so we have to stop.

The minimum cut is where P is set of labeled vertices and is the set of unlabelled vertices.

P = {a, b, c, d, h),

Edges in cut = {(d, z), (h, z)}

Capacity of the minimum cut C (d, z) + C (h, z) = 5 + 6 = 11. Maximum flow in transport work is 11.

7.9 GAME TREE

- In this section, we study about trees useful in analyzing games like chess, checkers and tic-tac-toe, where players take moves alternatively. These trees are called **Game Trees** and are used to develop game playing strategies and computer programs related to games.
- The vertices of a Game Tree represent the positions in the game and edges represent legal moves between the positions (vertices). A path is a sequence of moves (edges) in the game tree. Since game trees are quite large, all symmetric positions of a game are represented by the same vertex. The same position of a game can be represented by different vertices if different sequences of moves lead to this position.
- The starting position is represented by the root of the game tree. Vertex at even level is represented by a box which is a first player's move and a vertex at odd level is represented by a circle which is a second player's move. The final positions of a game are represented by leaves of game tree. Each leaf is assigned a value indicating the pay-off to the first player, if the game terminals in the position represented by this leaf. If terminal vertex represented by a circle with 1 then its indicate a win by the first player and a terminal vertex represented by a box with 1 indicates a win by second player for games of win-lose. Some games may have the provision of draw also. In these games a terminal vertex is labelled 0 with a draw position.
- Now we discuss some of the game trees associated with games like Nim and Tic-Tac-Toe.

7.9.1 Game Nim

- In a general version of game of nim, initially there are n piles of stones. Two players take their turn (called moves) alternatively. A legal move consists of removing one or more stones from any one pile without removing all the stones left player without a legal move loses. That means the player who removes the last stone loses the game. Fig. 7.173 shows a game tree for nim with starting position having two piles of stones containing two and one stone each respectively. Each position (vertex) of the tree is represented by the list of the number of stones in the different piles.
- The order of the piles does not matter. The starting move by the first player (represented by box 21). In Fig. 7.173, after first player's move from starting position can be lead to three possible positions because this first player can remove one stone remaining is the turn of second player (represented circles) for removing the stone at position or remove 2 stones from first pile leaving zero, one stone removing or removing one stone from second pile leaving two, zero stones.

- If he removes any stone from position, no stone will be left and therefore he will lose the game. Because of this reason, the value at is 1 (first player wins). For remaining positions, he can remove stones as they are the legal moves and are obtained. Again next will be the turn of first player and for him no legal moves are left. That means if he removes any stone, no stones will be left in any pile and he loses the game at these positions. These positions are marked with + 1.
- As explained above, we have assigned the values + 1 or 1 to terminal vertices (leaves) of the game.

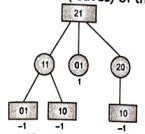

Fig. 7.173 : Game Tree for Nim

- When only one pile with one stone is left, no other legal move is possible, hence such positions are terminal positions. In this game of nim, which is a win-lose game, the terminal vertices with + 1 label represent win for first player and 1 represent win for second player.
- In Fig. 7.173 after first players move from starting position 21 is the turn of second player (Represented by circles) for removing the stones at positions 11, 01 and 20.
- Using minmax strategy, the internal vertices can also be assigned the values which gives rise to the value of the game. This minmax strategy is explained in the next section.

7.9.2 Minmax Strategy for Game Tree

- In the last example of game nim, we have assigned the values + 1 or 1 to terminal vertices. Similarly we can assign the values to internal vertices also when both players follow optimal strategies (Best move). For first player, the optimal strategy is to maximize the payoff and for second player is to minimize this payoff.
- When the first player moves to a position represented by a child with maximum value and the second player moves to a position of a child with minimum value, the strategy used is called **minmax strategy**. When both players follow minmax strategies, the value of the root gives the values of the tree. The value of the vertex (left and internal vertex) in the game tree is defined as follows:
- The value of a leaf in a game tree is a payoff to the first player when the game terminates in the position represented by this leaf.
- The value of an internal vertex of a game tree at an even level is the maximum of the values of its children and the value of an internal vertex at an odd level is the minimum of the values of its children.
- The value of a vertex of the game tree gives the payoff to the first player if both players follows the minimax strategy and play starts from the position represented by this vertex.
- To illustrate this, consider the game of nim with three piles of stones having two, two and one stone respectively. Considering the symmetrical positions equivalent the game gree is shown in Fig. 7.174.

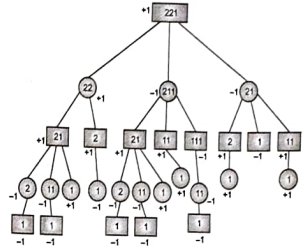

Fig. 7.174 : Game Tree for Game Nim with values of vertices

- In the game tree shown in Fig. 7.174 values of the vertices are calculated using the values of leaves and moving up one level at a time. As shown earlier, the value of the even level. Vertex is the maximum of the values of its children and the value of the odd level vertex is the minimum of the values of its children. Continuing this way, we get the value of the root as + 1. It shows that the first player wins when both players follows a minimax strategy.
- As we have seen in the last example of the game nim, the game tree could be drawn and the value of the tree could be calculated easily because of limited number of moves. For some games like chess, game trees are very large as they have many different possible moves. For chess, the number of vertices estimated is 10^{100}. As the size of this type of game tree is large, it is difficult to determine good strategies and the output of the game. In such cases to determine the values of internal vertices, an **evaluation function** is constructed that assigns each possible game position P, the value E(P) of the position to the first player. By using this function E, the vertices at the lowest level are assigned some values.
- To find the values of other vertices, the minimax strategy can be applied. For example, in the game of Tic-Tac-Toe the evaluation function E, which assigns the position the value No-Nx where No is the number

Solution: The maximum flow in the transport network using labelling procedure can be obtained using following steps.

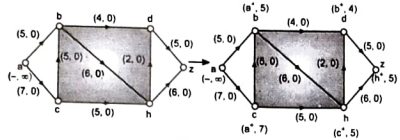

Fig. 7.168

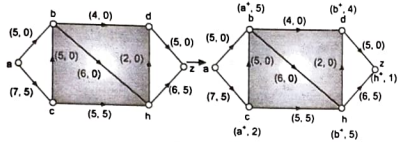

Fig. 7.169

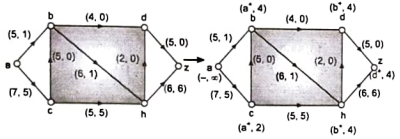

Fig. 7.170

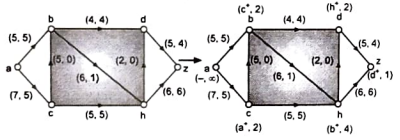

Fig. 7.171

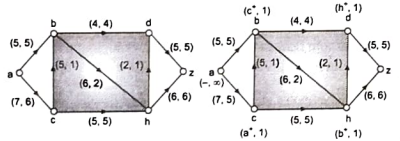

Fig. 7.172

Since Z cannot be labeled so we have to stop.

The minimum cut is where P is set of labeled vertices and is the set of unlabelled vertices.

P = {a, b, c, d, h),

Edges in cut = {(d, z), (h, z)}

Capacity of the minimum cut C (d, z) + C (h, z) = 5 + 6 = 11. Maximum flow in transport work is 11.

7.9 GAME TREE

- In this section, we study about trees useful in analyzing games like chess, checkers and tic-tac-toe, where players take moves alternatively. These trees are called **Game Trees** and are used to develop game playing strategies and computer programs related to games.
- The vertices of a Game Tree represent the positions in the game and edges represent legal moves between the positions (vertices). A path is a sequence of moves (edges) in the game tree. Since game trees are quite large, all symmetric positions of a game are represented by the same vertex. The same position of a game can be represented by different vertices if different sequences of moves lead to this position.
- The starting position is represented by the root of the game tree. Vertex at even level is represented by a box which is a first player's move and a vertex at odd level is represented by a circle which is a second player's move. The final positions of a game are represented by leaves of game tree. Each leaf is assigned a value indicating the pay-off to the first player, if the game terminals in the position represented by this leaf. If terminal vertex represented by a circle with 1 then its indicate a win by the first player and a terminal vertex represented by a box with 1 indicates a win by second player for games of win-lose. Some games may have the provision of draw also. In these games a terminal vertex is labelled 0 with a draw position.
- Now we discuss some of the game trees associated with games like Nim and Tic-Tac-Toe.

7.9.1 Game Nim

- In a general version of game of nim, initially there are n piles of stones. Two players take their turn (called moves) alternatively. A legal move consists of removing one or more stones from any one pile without removing all the stones left player without a legal move loses. That means the player who removes the last stone loses the game. Fig. 7.173 shows a game tree for nim with starting position having two piles of stones containing two and one stone each respectively. Each position (vertex) of the tree is represented by the list of the number of stones in the different piles.
- The order of the piles does not matter. The starting move by the first player (represented by box 21). In Fig. 7.173, after first player's move from starting position can be lead to three possible positions because this first player can remove one stone remaining is the turn of second player (represented circles) for removing the stone at position or remove 2 stones from first pile leaving zero, one stone removing or removing one stone from second pile leaving two, zero stones.

- If he removes any stone from position, no stone will be left and therefore he will lose the game. Because of this reason, the value at is 1 (first player wins). For remaining positions, he can remove stones as they are the legal moves and are obtained. Again next will be the turn of first player and for him no legal moves are left. That means if he removes any stone, no stones will be left in any pile and he loses the game at these positions. These positions are marked with + 1.
- As explained above, we have assigned the values + 1 or 1 to terminal vertices (leaves) of the game.

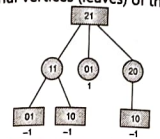

Fig. 7.173 : Game Tree for Nim

- When only one pile with one stone is left, no other legal move is possible, hence such positions are terminal positions. In this game of nim, which is a win-lose game, the terminal vertices with + 1 label represent win for first player and 1 represent win for second player.
- In Fig. 7.173 after first players move from starting position 21 is the turn of second player (Represented by circles) for removing the stones at positions 11, 01 and 20.
- Using minmax strategy, the internal vertices can also be assigned the values which gives rise to the value of the game. This minmax strategy is explained in the next section.

7.9.2 Minmax Strategy for Game Tree

- In the last example of game nim, we have assigned the values + 1 or 1 to terminal vertices. Similarly we can assign the values to internal vertices also when both players follow optimal strategies (Best move). For first player, the optimal strategy is to maximize the payoff and for second player is to minimize this payoff.
- When the first player moves to a position represented by a child with maximum value and the second player moves to a position of a child with minimum value, the strategy used is called **minmax strategy**. When both players follow minmax strategies, the value of the root gives the values of the tree. The value of the vertex (left and internal vertex) in the game tree is defined as follows:
- The value of a leaf in a game tree is a payoff to the first player when the game terminates in the position represented by this leaf.
- The value of an internal vertex of a game tree at an even level is the maximum of the values of its children and the value of an internal vertex at an odd level is the minimum of the values of its children.
- The value of a vertex of the game tree gives the payoff to the first player if both players follows the minimax strategy and play starts from the position represented by this vertex.
- To illustrate this, consider the game of nim with three piles of stones having two, two and one stone respectively. Considering the symmetrical positions equivalent the game gree is shown in Fig. 7.174.

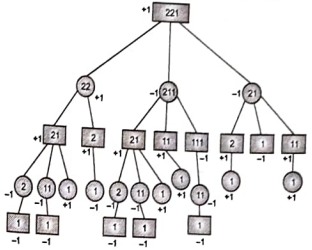

Fig. 7.174 : Game Tree for Game Nim with values of vertices

- In the game tree shown in Fig. 7.174 values of the vertices are calculated using the values of leaves and moving up one level at a time. As shown earlier, the value of the even level. Vertex is the maximum of the values of its children and the value of the odd level vertex is the minimum of the values of its children. Continuing this way, we get the value of the root as + 1. It shows that the first player wins when both players follows a minimax strategy.
- As we have seen in the last example of the game nim, the game tree could be drawn and the value of the tree could be calculated easily because of limited number of moves. For some games like chess, game trees are very large as they have many different possible moves. For chess, the number of vertices estimated is 10^{100}. As the size of this type of game tree is large, it is difficult to determine good strategies and the output of the game. In such cases to determine the values of internal vertices, an **evaluation function** is constructed that assigns each possible game position P, the value E(P) of the position to the first player. By using this function E, the vertices at the lowest level are assigned some values.
- To find the values of other vertices, the minimax strategy can be applied. For example, in the game of Tic-Tac-Toe the evaluation function E, which assigns the position the value No-Nx where No is the number

of files (rows, columns and diagonals) containing no O's (move of second player) minus the number of files (rows, columns and diagonals) containing no X's (move of first player). In Fig. 7.175, No = 1, Nx = 2 and hence No Nx = 1 = E(P).

Fig. 7.175: The value of position P

E(P) = No Nx = 1

- Another method for evaluation of game tree for large tree is Alpha-Beta pruning. It eliminates many calculations by pruning portions of the game tree that cannot affect the value of ancestor vertices. In general, alpha-beta pruning allows us to bypass many vertices in game tree yet still find the values of a vertex. The value obtained is the same as if we had evaluated all vertices.

EXERCISE 7.2

1. Explain the following terms:
   (i) Transport network **(Oct. 2017)**
   (ii) Capacity of a cut
   (iii) Maximal flow
   (iv) Game Tree **(April 2018)**
2. Find the maximal flow in the following network.

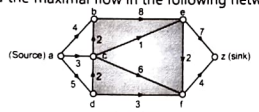

Fig. 7.176

3. Equipment is manufactured at three factories x_1, x_2 and x_3 and is to be shipped to three depots y_1, y_2 and y_3 through the transport network given in the following Fig. 7.177.

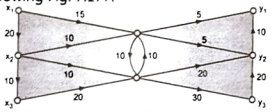

Fig. 7.177

Factory x_1 can make 40 units, factory x_2 can make 20 units and factory x_3 can make 10 units. Depot y_1 needs 15 units, depot y_2 needs 25 units and depot y_3 needs 10 units. How many units should each factory make so that they can be transported to the depots ?

Hint: In order to make this example with a transport network, introduce a source s and a sink z as shown in the following Fig. 7.178. The manufacturing capabilities of the three factories are then used to define the capacities for the edges (s, x_1), (s, x_2) and (s, x_3). For the edges (y_1, z), (y_2, z) and (y_3, z) demands are used as capacities. Apply labelling process to this network to find the value of maximum flow.

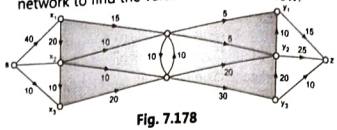

Fig. 7.178

4. Use labelling procedure to find a maximum flow in the transport network shown in Fig. 7.179. Determine the corresponding minimum cut.

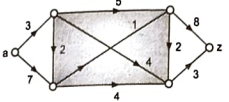

Fig. 7.179

POINTS TO REMEMBER

- A "tree" is a simple connected graph without any circuits.
- A tree with n vertices contains (n – 1) number of edges.
- The eccentricity E(v) of a vertex v in a graph G is the distance from v to the vertex farthest from v in G. i.e.
- A tree in which one vertex (called the root) is distinguished from all the other vertices is known as rooted tree. Trees without any root are called free trees or simply trees.
- A forest is a set of disjoint trees.
- A rooted tree in which every interior node has atmost m sons is called an m-ary tree.
- In a binary tree, every internal vertex has atmost 2 sons.
- A binary tree is a full or regular binary tree if each internal vertex has **exactly** 2 sons.
- If T be any full binary tree and w_1, w_2 ..... w_t be the weights of the terminal vertices (leaves). Then, the weight W of the binary tree is given by

$$W(T) = \sum_{i=1}^{t} w_i l_i$$

where li 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.

- A binary prefix code obtained from an optimal tree is called an **optimal prefix code**.
- Let G be any connected graph. A spanning subgraph of G which is a tree is called a spanning tree of G. i.e. a subgraph of G, which is a tree and contains all the vertices of G is called a spanning tree of G.

ALGEBRAIC STRUCTURES AND CODING THEORY

CHAPTER 8

8.1 INTRODUCTION

- In this chapter, we study sets with additional structure, induced by one or more binary operations on the elements of the set. These discrete structures are called as algebraic systems as they obey a set of rules or axioms which are similar to the rules of addition and multiplication of numbers in elementary algebra. In fact many of these structures are prototype models of mathematical systems, with which we are familiar.
- We first introduce a general algebraic system and discuss its properties. We then concentrate our attention on some special algebraic systems such as semigroups, groups, rings and fields.
- An important application of groups is in coding theory where techniques are developed for detecting and correcting errors in transmitted data. The section on codes discusses some of these techniques in detail.
- Besides coding theory, algebraic systems are also widely applied in the design of computer hardware and development of software especially formal language theory and finite state machines.

8.2 ALGEBRAIC SYSTEM

Let us first define an operation on the elements of a set, such that the resulting element is also an element of the set.

Definition

An n-ary operation on a non-empty set A is a function $f: A^n \to A$, A^n being the product set of A.

Observe the following properties that a binary operation must satisfy.

1. The n-ary operation must be defined for each n-tuple $(a_1, a_2, ..., a_n) \in A$.
2. Since f is a function, only one element of A should be assigned to each n-tuple of A^n.

If n = 1, f is called **Unary,**

if n = 2, f is called **Binary,**

if n = 3, f is called **Ternary** and so on.

Let us consider the following examples.

Examples:

1. The function $f: Z \to Z$, where $f(x) = -x$, is unary,
2. $f: Z \times Z \to Z$, defined as $f(x, y) = x + y$, is binary,
3. $f: Z \times Z \times Z \to Z$, defined as
   $f(x, y, z) = y$; if $x \neq 0$
   $= z$; otherwise,

is ternary.

We now proceed to define an algebraic system.

Definition

An algebraic system is an ordered pair (A, F) where

1. A is a set of elements, called as the **carrier** of the algebra.
2. F is a finite set of m-ary operations on the carrier, m being a variable.

In the notation for an algebraic system, the carrier set A is first specified, followed by the elements of F, which are actually listed, viz (A, f_1) or (A, f_1, f_2) etc.

Examples:

1. Let E = {0, 2, 4, ...}. Then E with the binary operation of addition + represents an algebraic system (E, +).
2. The set of integers Z with the two binary operations of addition + and multiplication x is an algebraic system, and is denoted as (Z, +, x).
3. The set of real numbers R with a single unary operation minus – and two binary operations of addition and multiplication is an algebraic system denoted by (R, –, +, x).
4. For a fixed integer n > 0, let M_n (R) denote the set of all n x n matrices. Then under the binary operation of matrix addition, M_n (R) forms an algebraic system (M_n (R), +).

   Similarly, under matrix multiplication, (M_n (**R**), x) is another algebraic system.

5. Let P(A) denote the power set of a non-empty set A. Then P(A) together with the set operations of union, intersection and complementation forms an algebraic system (P(A), ∪, ∩, –).

6. Let E = {a, b} be a set of symbols, called as the **Alphabets**. A **word** over E is a finite string of symbols a, b, with possible repetitions, e.g. a, aa, abab, etc. Given two words x and y. We can form a new word xy by simply just opposing the symbols of x with those of y in the order xy. For example, if x = aa, y = aba, then xy = aaaba, whereas yx = abaaa. This operation is called as **Concatenation**. If E^* denotes the set of all words over E, then concatenation is a binary operation on E^*.

In what follows, we will deal with algebraic systems, having only binary operations.

8.3 PROPERTIES OF BINARY OPERATIONS

Definition

A binary operation $\cdot$ on A is said to be **Commutative** if $a \cdot b = b \cdot a$, for all elements $a, b \in A$.

Examples:

1. The binary operation of addition on the set of integers is commutative, but the operation of subtraction on the set of integers is not commutative.
2. The binary operation of multiplication on the set of integers is commutative.

Definition

A binary operation $\cdot$ on A is said to be **Associative** if $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, for all elements, $a, b, c \in A$.

Examples:

1. The binary operation of addition on the set of integers is associative, whereas the binary operation of subtraction is not associative.
2. The binary operation of multiplication on the set of integers is associative.

Definition

A binary operation $\cdot$ on A is said to satisfy the **Idempotent** property if $a \cdot a = a$, for all $a \in A$.

Example:

- Let L be a lattice with the operators $\wedge$ (meet) and $\vee$ (join). Then $\wedge$ and $\vee$ are binary operations and we know that

$a \vee a = a$,

$a \wedge a = a$, for all $a \in A$.

Hence both $\wedge$ and $\vee$ satisfy the idempotent property.

8.3.1 Tables of Binary Operations

If $A = \{a_1, a_2, \ldots, a_n\}$ is a finite set, we can define a binary operation on A, by means of a table, is shown below. The entry in the i-th row and j-th column denotes the element $a_i \cdot a_j$.

$\cdot$	a_1	a_2	a_j	a_n
a_1				
a_2				
a_i			$a_i \cdot a_j$	
a_n				

Example:

Let A = {0, 1} and let × denote multiplication. Then we have the binary table

×	0	1
0	0	0
1	0	1

SOLVED EXAMPLES

Example 1: *For each of the following, determine whether $\cdot$ is a binary operation:*

(i) R is the set of real numbers and $a \cdot b = ab$.

(ii) Z^- is the set of positive integers and $a \cdot b = a / b$.

(iii) On Z^- where $a \cdot b = a - b$.

(iv) On R, where $a \cdot b = min\ \{a, b\}$.

(v) On R, where $a \cdot b = a \times |b|$.

(vi) On Z, where $a \cdot b = a^b$.

Solution:

(i) Yes, since f: $\mathbf{R}^2 \to \mathbf{R}$ defined as f(a, b) = ab is a function, with a b ∈ **R**.

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

(1, 2) ∈ $Z^+ \times Z^+$, but 1/2 ∉ Z^+.

(iii) No, since (1, 2) ∈ $Z^+ \times Z^+$ but

$1 - 2 = -1 \notin Z^+$

(iv) Yes, since $\cdot$ is a function, with min {a, b} ∈ **R**.

(v) Yes, since $\cdot$ is a function, with a × |b| ∈ **R**.

(vi) No, since $2 \cdot (-1) = 2^{-1} = \frac{1}{2} \notin Z$.

Example 2: *For each of the following, determine whether the binary operation $\cdot$ is commutative or associative:*

(i) N is the set of natural numbers and $a \cdot b = a + b + 2$, for $a, b \in N$.

(ii) On N, where $a \cdot b = max\ (a, b)$.

(iii) On N, where $a \cdot b = min\ (a, b)$.

(iv) On N, where $a \cdot b = min\ (a, b + 2)$

(v) On R, where $a \cdot b = ab + 2b$.

(vi) On R, where $a \cdot b = ab / 3$.

(vii) On the set of non-zero real numbers, $a \cdot b = a / b$.

(viii) On R, $a \cdot b = a^b$.

Solution:

(i) $\cdot$ is commutative since $a \cdot b = a + b + 2$ and $b \cdot a = b + a + 2$. Hence both are equal.

$a \cdot (b \cdot c) = a \cdot (b + c + 2)$

$= a + (b + c + 2) + 2 = a + b + c + 4.$

$(a \cdot b) \cdot c = (a + b + 2) \cdot c$

$= (a + b + 2) + c + 2$

$= a + b + c + 4$

Hence $\cdot$ is associative.

(ii) $a \cdot b = max\ (a, b) = max\ (b, a) = b \cdot a$. Hence $\cdot$ is commutative.

Let a, b, c ∈ N. Consider $b \cdot c$.

$b \cdot c = max\ \{b, c\}$.

$\therefore \quad b \cdot c = b$; if $b \geq c$

or $\quad = c$; if $c \geq b$

Let us suppose {b, c} = b, so that

$b \cdot c = b$.

Then $a \cdot (b \cdot c) = max\ \{a, b\}$

$= a$; if $a \geq b$

or $\quad = b$; if $b \geq a$

If $a \geq b$, then $a \cdot (b \cdot c) = a$

Then $a \cdot b = max\ \{a, b\} = a$.

Hence $(a \cdot b) \cdot c = max\ \{a, c\} = a$; since $a \geq b$ and $b \geq c$.

Hence if $a \geq b \geq c$, then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Similarly, one can prove $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for other cases.

Hence $\cdot$ is associative.

(iii) $\cdot$ is commutative as well as associative. Proof is similar to (ii).

(iv) $\cdot$ is not commutative since

$2 \cdot 3 = min\ (2, 5) = 2$, whereas,

$3 \cdot 2 = min\ (3, 4) = 3$.

$\cdot$ is also not associative since

$4 \cdot (3 \cdot 1) = 4 \cdot 3 = 4$, while

$(4 \cdot 3) \cdot 1 = 4 \cdot 1 = 3$.

(v) $\cdot$ is not commutative since

$2 \cdot 3 = 6 + 6 = 12$, while

$3 \cdot 2 = 6 + 4 = 10$

Clearly $\cdot$ is also not associative.

(vi) $\cdot$ is commutative and associative.

(vii) $\cdot$ is not commutative; and $\cdot$ is also not associative since $a \cdot (b \cdot c)$

$= a \cdot (b/c) = a\ /b/c = ac / b$; whereas

$(a \cdot b) \cdot c = (a / b) \cdot c = a\ /b/\ c = \frac{a}{bc}$

(viii) $\cdot$ is not commutative since $a^b \neq b^a$.

$\cdot$ is also not associative since,

$(a \cdot b) \cdot c = (a^b)^c = a^{bc}$

whereas $a \cdot (b \cdot c) = a^{b^c}$

Example 3: *Let (A, $\cdot$) be an algebraic system where $\cdot$ is a binary operation such that for any a, b, ∈ A, $a \cdot b = a$.*

(i) Show that $\cdot$ is an associative operation.

(ii) Can $\cdot$ ever be a commutative operation ?

Solution:

(i) $a \cdot (b \cdot c) = a \cdot b = a.\ (a \cdot b) \cdot c$

$= a \cdot c = a.$

Hence $\cdot$ is associative.

(ii) $\cdot$ is commutative only if $a \cdot b = b \cdot a$, i.e. a = b, for all a, b ∈ A. This is possible if A is the singleton set {a} and $a \cdot a = a$, i.e. $\cdot$ is an idempotent operation on A.

Example 4: *Let (A, $\cdot$) be an algebraic system such that for all a, b, c, d ∈ A,*

$a \cdot a = a$,

$(a \cdot b) \cdot (c \cdot d) = (a \cdot c) \cdot (b \cdot d)$

Show that $a \cdot (b \cdot c) = (a \cdot b) \cdot (a \cdot c)$

Solution: Since

$a \cdot a = a$,

$a \cdot (b \cdot c) = (a \cdot a) \cdot (b \cdot c)$.

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

(by the second condition)

Example 5: *Let (A, ·) be an algebraic system such that for all a, b ∈ A,*

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

$(a \cdot b) \cdot b = (b \cdot a) \cdot a.$

(i) Show that $a \cdot (a \cdot b) = a \cdot b$, for all a, b, ∈ A

(ii) Show that $a \cdot a = (a \cdot b) \cdot (a \cdot b)$, for all a, b ∈ A.

(iii) Show that $a \cdot a = b \cdot b$, for all a, b.

(iv) Show that $a \cdot b = b \cdot a$ iff a = b.

(v) Let (A, ·) satisfy the additional condition $a \cdot b = (a \cdot b) \cdot b$, for all a, b ∈ A. Show that · is idempotent and commutative.

Solution:

(i) $a \cdot (a \cdot b) = ((a \cdot b) \cdot a) \cdot (a \cdot b)$,

since $a = (a \cdot b) \cdot a$, (by the first condition)

Now let $c = a \cdot b$.

Then R.H.S. $= (c \cdot a) \cdot c = c$ again by the first condition.

Hence $a \cdot (a \cdot b) = a \cdot b$

(ii) $a \cdot a = ((a \cdot b) \cdot a) \cdot a$

$= (c \cdot a) \cdot a$, putting $a \cdot b = c$

$= (a \cdot c) \cdot c$

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

$= (a \cdot b) \cdot (a \cdot b)$ (by (i))

(iii) $a \cdot a = (a \cdot b) \cdot (a \cdot b)$ (by (ii))

$= c \cdot c$, where $a \cdot b = c$

$= (c \cdot b) \cdot (c \cdot b)$ (by (ii))

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

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

$= (b \cdot a) \cdot (b \cdot a)$ } (by (ii)

$= b \cdot b$ }

(iv) If $a = b$, $a \cdot b = b \cdot a$.

Conversely, let $a \cdot b = b \cdot a$.

Then $a = (a \cdot b) \cdot a = (b \cdot a) \cdot a$

$= (a \cdot b) \cdot b$ (by given condition)

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

$= b$ (by given condition)

(v) $a \cdot a = (a \cdot a) \cdot a$ (by given condition)

$= a$, since $(a \cdot b) \cdot a = a$ for all a, b ∈ A.

To show · is commutative

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

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

$= b \cdot a$ (by given condition.)

Hence · is commutative.

Example 6: *The following table, of a binary operation · is given. Is · commutative ?*

·	a	b	c
a	b	c	a
b	c	b	a
c	a	b	c

Solution: From the table we observe the following:

$a \cdot b = c$, $b \cdot a = c$

$a \cdot c = a$, $c \cdot a = a$

$b \cdot c = a$, $c \cdot b = b$, and $a \neq b$.

Hence · is not commutative.

Example 7: *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) $c \cdot d$ and $d \cdot c$

(ii) $b \cdot d$ and $d \cdot b$

(iii) $a \cdot (b \cdot c)$ and $(a \cdot b) \cdot c$

(iv) Is · commutative, associative ?

Solution:

(i) $c \cdot d = a$, $d \cdot c = a$

(ii) $b \cdot d = c$, $d \cdot b = b$

(iii) $b \cdot c = b$,

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

$a \cdot b = c$. Hence $(a \cdot b) \cdot c = c \cdot c = a$

(iv) · is not commutative, since $b \cdot d \neq d \cdot b$.

· is also not associative, since $a \cdot (b \cdot c) \neq (a \cdot b) \cdot c$.

We shall now study some special algebraic systems.

Example 8: *Consider the following table for a binary operation * on the set {a, b, c, d}.*

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

*(i) Is * associative ?*

(ii) Find the identity element e.

(iii) What is the inverse of b ?

Solution: (i) * is not associative.

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

However, $b * (c * d) = b * d = a$

(ii) Notice that the first column and first row contains the ordered sequence of elements {a, b, c, d}. Hence a is the identity element (i.e. a is left identity as well as right identity).

(iii) Since $b * c = a = c * b$ and also $b * d = a = d * b$, b has two inverse i.e. both c and d are inverse of b.

8.4 SEMI GROUPS

Let (A, ·) be an algebraic system, with a binary operation · on A. Then (A, ·) is called a **Semi Group** if · is associative, i.e.

$a \cdot (b \cdot c) = (a \cdot b) \cdot c$, for all a, b, c ∈ A.

The semigroup is further said to be commutative if · is commutative.

Examples:

1. (Z, +) is a commutative semi group.
2. (Z, ×) is a commutative semi group.
3. For a non-empty set A, (P(A), ∪) is a commutative semi group and so is (P(A), ∩).
4. (Z, −) is not a semi group, since subtraction is not associative.

Definitions

1. An element e in (A, ·) is called as **Left Identity** element if for each element x ∈ A, $e \cdot x = x$.
2. e is called a **Right** identity if $x \cdot e = x$, for all x ∈ A.

A semi group can have more than one left (or right) identity, as seen from the following example.

Example: The algebraic system (A, ·) whose table is given below is a semi group.

·	A	b	c
A	A	b	c
b	a	c	b
c	a	b	c

Since the rows for both the elements a and c are equal to [a b c] it follows that both a and c are left identities. However there is no right identity since none of the columns are equal to [a b c].

Definition

An element e in a semi group (A, ·) is called an **Identity** element if $a \cdot e = e \cdot a = a$, for all a ∈ A, i.e. e is both a left identity and right identity. It is clear that e is unique.

Examples:

1. The semi group (Z, +) has the identity element which is the number 0.
2. The semi group (Z, ×) has the identity element which is the number 1.
3. The semi group (N, +) has no identity element, where the set N is the set of natural numbers, excluding 0.

Definition

A **Monoid** is a semi group (A, ·) that has an identity element.

Examples:

1. Let E = {0, 2, 4, 6, ...}. Then (E, +) is a monoid, with the number 0 as the identity element.
2. Let E^* be the set of all words over the alphabet set E = {a, b}. Let concatenation be the binary operation. The empty word Λ is the identity for E^*. Hence E^* under concatenation is a monoid.

Definition

Let (A, ·) be an algebraic system, and let B be a subset of A. Then B is said to be closed under ·, if for any elements b, c ∈ B, b · c is also in B.

Definition

Let (A, ·) be a semi group and let B be a non-empty set of A, such that B is closed under ·. Then (B, ·) is itself a semi group and is called a **Sub Semi Group** of (A, ·).

Definitions

Let (A, ∘) be a monoid, and let B be a non-empty subset of A. Then (B, ∘) is called a **Sub Monoid** of (A, ∘) if

(i) B is closed under ∘.

(ii) The identity element e ∈ B.

Example:

Let E = {0, 2, 4, 6, ...}. Then (E, +) is a sub monoid of (Z, +).

The concepts of semi groups and monoids are used in finite state machines.

Definitions

Let (A, ∘) be a monoid with identity element e. Let B be a non-empty subset of A. Then the monoid generated by B, denoted by $< B >$ is defined as follows:

1. $e \in < B >$, and if $b \in B$, then b also is in $< B >$, that is $B \subseteq < B >$.
2. $< B >$ is closed under ∘.
3. The only elements of $< B >$ are those obtained from steps (1) and (2).

SOLVED EXAMPLES

Example 1: *Find the smallest submonoid of (Z, +) generated by the set {– 4, 6}.*

Solution: Let B = {– 4, 6}. Then $< B >$ is obtained as follows:

(i) $0, 6, -4 \in < B >$.

(ii) If $x, y \in < B >$, then $x + y \in < B >$.

(iii) $< B >$ contains only the elements obtained from steps (i) and (ii).

Hence $< B >$ = {0, 6, – 4, 2, – 2, 4, 8, – 6, 10, ...}

= {..., – 6, – 4, – 2, 0, 2, 4, 6, 8, 10, ...}

= set of even integers.

(ii) Let E = {a, b} and B = {aa, bbb}.

Find the submonoid of E^* generated by B.

$< B >$ = {∧, aa, bbb, aabbb, bbbaa, aaaa, bbbbbb, ...}.

(iii) Let A = {a, b, c, d} and let C(A) denote the set of all functions on A. Let f: A → A be defined by the following diagram.

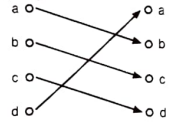

Fig. 8.1

Find the submonoid of (C(A), ∘), where ∘ denotes composition of functions, generated by f.

Solution: The identity element is 1_A. Consider $fof = f^2$ which is defined by the following diagram.

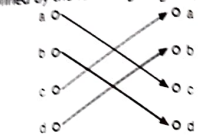

Fig. 8.2

$fofof = f^3$ is defined as

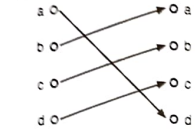

Fig. 8.3

f^4 is defined as

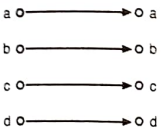

Fig. 8.4

$\therefore \quad f^4 = 1_A$

Hence the submonoid generated by f is the set $\{1_A, f, f^2, f^3\}$.

Example 2: *Show that the set of integers of the form 3m + 1 is closed under multiplication. Is this set a submonoid of (Z, ×)?*

Solution: Let $B = \{ n \in Z \mid n = 3m + 1 \}$.

Let $r, s \in B$, then $r = 3m + 1$ and $s = 3n + 1$ for $m, n \in Z$.

then $rs = (3m + 1)(3n + 1)$

$= 9mn + 3n + 3m + 1$

$= 3(m + n + 3mn) + 1$

$= 3t + 1$, where $t = m + n + 3mn$.

Hence B is closed under ×.

Since the identity element 1 can be written as $1 = 30 + 1$, $1 \in B$. Hence B is a sub monoid of (Z, ×).

Example 3: *(i) Determine the sub monoid of (Z, +) generated by 6 and 9.*

(ii) Submonoid of (Z, +) generated by – 3 and 5.

Solution:

(i) Let S = {6, 9}

then $< S >$ = {0, 6, 9, 12, 15, 18, 21, 24, ...}

(ii) Let S = {– 3, 5}.

then $< S >$ = {0, –3, 5, 2, –1, –2, 4, 7, – 4, 1, 3, ...}

= {..., –3, –2, –1, 0, 1, 2, 3, ...}

= Z

Example 4: *Let A = {a, b}. Which of the following tables define a semigroup of A ? Monoid on A ?*

(i)

·	a	B
a	a	B
b	a	A

(ii)

·	a	b
a	a	b
b	b	b

(iii)

·	a	B
a	b	A
b	a	B

(iv)

·	a	b
a	a	b
b	b	a

Solution: (i) · is not associative. Consider b · (a · b) = b · b = a. On the other hand (b · a) · b = a · b = b. Therefore (A, ·) is not a semi group and hence not a monoid.

(ii) a · (b · b) = a · b = b

(a · b) · b = b · b = b

a · (a · b) = a · b = b

(a · a) · b = a · b = b

a · (b · a) = a · b = b

(a · b) · a = b · a = b

Similarly · is associative for the remaining combinations.

The identity element is a. Hence (A, ·) is not only a semi group, but it is also a monoid.

(iii) a · (a · b) = a · a = b

(a · a) · b = b · b = b

Similarly checking for other combinations, one can show that · is associative. The identity element is b. Hence (A, ·) is not only a semi group, but it is also a monoid.

(iv) a · (b · a) = a · b = b

(a · b) · a = b · a = b

Similarly one can verify that · is associative for other combinations as well.

Hence (A, ·) is a semi group. Note that a · b = b = b · a, and a · a = a.

Hence the identity element is a.

Hence (A, ·) is also a monoid.

Example 5: *Let A = {a, b}. Write the operation table for the semigroup (P(A), ∪).*

Solution: P(A) = {∅, A, {a}, {b}}

∪	∅	A	{a}	{b}
∅	∅	A	{a}	{b}
A	A	A	A	A
{a}	{a}	A	{a}	A
{b}	{b}	A	A	{b}

Example 6: Prove that the intersection of two subsemigroups of a semigroup (S, ·) is a subsemigroup of (S, ·).

Solution: Let S_1, S_2 be subsemigroups of S. We have only to show that $S_1 \cap S_2$ is closed under ·. Let $x, y \in S_1 \cap S_2$. Then $x, y \in S_1$ and $x, y \in S_2$. Since S_1 and S_2 are subsemigroups, $x \cdot y \in S_1$ and $x \cdot y \in S_2$ which means that $x \cdot y \in S_1 \cap S_2$. Hence $S_1 \cap S_2$ is closed under ·. Therefore $(S_1 \cap S_2, \cdot)$ is a subsemigroup.

Example 7: *Prove that the intersection of two submonoids of a monoid (S, ·) is a submonoid of (S, ·).*

Solution: Let S_1 and S_2 be submonoids of S. Then by the above example $(S_1 \cap S_2, \cdot)$ is a subsemigroup. We have only to prove the identity element is in $S_1 \cap S_2$ which is obvious. Hence $(S_1 \cap S_2, \cdot)$ is a submonoid.

Example 8: *Show that the set of all idempotents in a commutative monoid S is a submonoid of S.*

Solution: Recall an element $x \in S$ is called an idempotent if $x \cdot x = x$. Let T be the set of all idempotents in S. Then $e \in T$ since $e \cdot e = e$. We have only to prove that T is closed under ·. For $x, y \in T$ consider $(x \cdot y) \cdot (x \cdot y)$.

$= ((x \cdot y) \cdot x) \cdot y$ (by associativity of ·)

$= (y \cdot (x \cdot x)) \cdot y$

(using both commutativity and associativity)

$= (y \cdot x) \cdot y$

$= x \cdot (y \cdot y)$

$= x \cdot y$

We have thus shown that $x \cdot y$ is an idempotent element, and hence $x \cdot y \in T$. T is therefore closed under · and is hence a submonoid of S.

Example 9: *Let Z_n denote the set of integers {0, 1, 2,..., n − 1}. Let Θ be binary operation on Z_n such that*

$a \ \Theta b$ = *the remainder of ab divided by n.*

(i) Construct the table for the operation Θ for n = 4.

(ii) Show that (Z_n, Θ) is a semigroup for any n.

Solution: (i) Z_4 = {0, 1, 2, 3}.

Θ	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(ii) Let $a \Theta b = r$, where

$$ab = pn + r \quad \ldots (1)$$

Then $(a \Theta b) \Theta c = r \Theta c$

$$= s, \text{ where } rc = qn + s \quad \ldots (2)$$

Let $b \Theta c = t$, where $bc = ln + t$ ... (3)

$a \Theta (b \Theta c) = a \Theta t = k$, where $at = mn + k$ ... (8.4)

We have to prove $s = k$.

Now $a(bc) = a(ln + at) = aln + mn + k$ ... (5)

Also $(ab)c = (pn + r)c = pnc + rc$

$$= pnc + qn + s \quad \ldots (6)$$

Now since equations (5) and (6) are equal, it follows that k = s.

Hence $(a \Theta b) \Theta c = a \Theta (b \Theta c)$.

Hence (Z_n, o) is a semigroup for any n.

Example 10: *Let (A, ·) be a semigroup. Let a be an element in A. Consider a binary operation ∗ on A such that for every $x, y \in A$, $x * y = x \cdot a \cdot y$.*

Show that ∗ is an associative operation.

Solution: $(x * y) * z = (x \cdot a \cdot y) * z$

$$= x \cdot a \cdot y \cdot a \cdot z$$

Now $x * (y * z) = x * (y \cdot a \cdot z)$

Hence $(x * y) * z = x * (y * z)$

therefore ∗ is an associative operation.

Example 11: *Let ((a, b), ·) be a semigroup where*

$a \cdot a = b$. *Show that*

(i) $a \cdot b = b \cdot a$

(ii) $b \cdot b = b$.

Solution: (i) $a \cdot b = a \cdot (a \cdot a) = (a \cdot a) \cdot a$ (as · is associative)

$$= b \cdot a$$

(ii) Since (A, ·) is closed under ·, $a \cdot b = a$ or $a \cdot b = b$.

Let us first assume $a \cdot b = a$.

Then by associativity property of ·,

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

$\Rightarrow \quad a \cdot a = b \cdot b$

$\Rightarrow \quad b = b \cdot b$

Next assume $a \cdot b = b$.

Then $a \cdot (a \cdot b) = (a \cdot a) \cdot b$

$\Rightarrow \quad a \cdot b = b \cdot b$

$\Rightarrow \quad b = b \cdot b$

Hence in either case $b \cdot b = b$.

Hence the result is proved.

Example 12: *Consider the algebraic system (Q, ·), where Q is set of rational numbers and · is binary operation defined by $a \cdot b = a + b - ab$, $\forall a, b \in Q$.*

Determine whether · is associative.

Solution: Let a, b, c ∈ Q.

Consider $(a \cdot b) \cdot c$. Let $a \cdot b = p$.

Then $p = a + b - ab$. Now $(a \cdot b) \cdot c$

$$= p \cdot c = p + c - pc$$

$$= (a + b - ab) + c) - (a + b - ab)c \quad \ldots (1)$$

Now, $a \cdot (b \cdot c) = a \cdot q$ (say)

$$= a + q - aq, \text{ (where } q = b + c - bc)$$

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

$$= a + b + c - bc - ab - ac + abc \quad \ldots (2)$$

Since equations (1) and (2) are equal, it follows that · is associative.

8.5 GROUPS

A **Group** (G, ·) is a monoid, with identity e, such that for every element $a \in G$ there exists an element $a^{-1} \in G$, called as the inverse of a, such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Thus a group is a set G together with a binary operation · on G such that

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all a, b, c ∈ G (i.e. · is **Associative**)
2. There is a un5que element e in G such that $a \cdot e = e \cdot a$, for a ∈ G. (**Identity** element)
3. For each a ∈ G, there exists an element $a^{-1} \in G$, such that $a \cdot a^{-1} = a^{-1} \cdot a = e$. (**Inverse** element)

Definition

A group (G, ·) is called an **Abelian** group if $a \cdot b = b \cdot a$, for all a, b ∈ G.

Examples:

1. The set of all integers Z with the operation of addition is a group. The identity element is the number 0 and for every n ∈ Z, its inverse is (− n).
2. The set $Q^* = Q - \{0\}$ of non-zero rational numbers is a group under multiplication. The identity element is the number 1 and inverse of each element p/q ∈ Q^* is q/p.
3. The set of all **non zero** real numbers under the operation of multiplication is a group, with the number 1 as the identity element; and inverse of each number a is 1/a.

   The next is a very important example of a group.
4. Let n be any positive integer (n > 0). For elements x, y ∈ Z, define a relation ≡ on them as $x \equiv y$ or x = y (mod n) if x − y is divisible by n. The relation is an equivalence relation and for each element x ∈ Z, we obtain the corresponding equivalence class [x].

   There are in all n distinct equivalence classes. Let Z_n denote the set of all equivalence classes; Z_n is called as a set of **Residue Classes Modulo n**, where [x] = [y] implies x = y (mod n).

   For any two elements [x], [y] ∈ Z_n define [x] + [y] = [x + y]. One can easily see that + is both associative and commutative. The identity element is [0], and for each [x] ∈ Z_m, its inverse is [m − x], since [x] + [m − x] = [x + m − x] = [m] = [0]. Thus (Z_m, +) is an abelian group.
5. If p is a prime number, then $Z_p - \{0\} = Z_p^*$ is a multiplicative abelian group where the multiplication · is defined naturally as

   $[x] \cdot [y] = [x \cdot y]$.

   However, for a non-prime number Z_m^* is not a group.

   Consider $Z_4^* = \{[1], [2], [3]\}$. Z_4 is not a group since [2] · [2] = [4] = [0] ∉ Z_4^*. Hence Z_4^* is not closed under ·, and therefore it is not a group.

   We give below the group tables for Z_3 and Z_4 under +.

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

(Z_3, +)

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[2]
[3]	[3]	[0]	[1]	[2]

(Z_4, +)

6. Let A = {a, b, c} and let F denote the set of functions from A to A, which are given below.

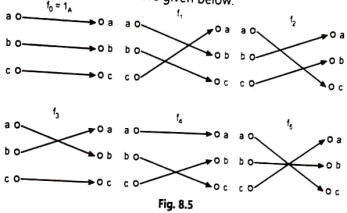

Fig. 8.5

The set (F, ·), where · denotes composition forms, a group. The group table is given below.

·	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_2	f_0	f_5	f_3	f_4
f_2	f_2	f_0	f_1	f_4	f_5	f_3
f_3	f_3	f_4	f_5	f_0	f_1	f_2
f_4	f_4	f_5	f_3	f_2	f_0	f_1
f_5	f_5	f_3	f_4	f_1	f_2	f_0

This group is non-abelian, since $f_1 \cdot f_3 = f_5$ and $f_3 \cdot f_1 = f_4$.

- **The Permutation Group (Group of Symmetries of a Triangle):** Consider an equilateral triangle (Fig. 8.6) with vertices 1, 2, 3. Since the triangle is determined by its vertices, a symmetry of the triangle is a **permutation** of the vertices. We describe the various symmetries of this triangle.

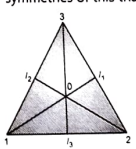

Fig. 8.6

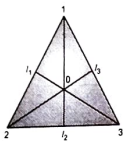

Fig. 8.7

$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ is the identity permutation, that keeps the vertices undisturbed.

Next consider the anti-clockwise rotation f_2 of the triangle about 0 through 120°. (Fig. 8.7). Then

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

Next obtain an anti-clockwise rotation f_3 about 0 through 240°, which is the permutation

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

Finally, there is an anti-clockwise rotation about 360° which is the same as f_1.

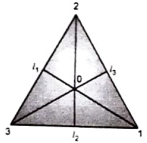

Fig. 8.8

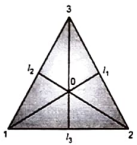

Fig. 8.9

We also obtain three additional symmetries of the triangle g_1, g_2 and g_3 by reflecting about the lines l_1, l_2 and l_3 respectively. We denote these reflections by the following permutations.

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

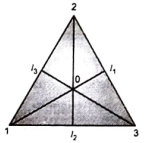

Fig. 8.10

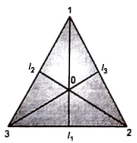

Fig. 8.11

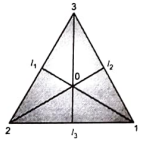

Fig. 8.12

We denote the set of all these permutations by $S_3 = \{f_0, f_1, f_2, g_1, g_2, g_3\}$. S_3 is a non-abelian group of order 6, under composition $\cdot$, with f_1 as the identity element.

$\cdot$	f_0	f_1	f_2	g_1	g_2	g_3
f_0	f_0	f_1	f_2	g_1	g_2	g_3
f_1	f_1	f_2	f_0	g_3	g_1	g_2
f_2	f_2	f_0	f_1	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_0	f_1	f_2
g_2	g_2	g_3	g_1	f_2	f_0	f_1
g_3	g_3	g_1	g_2	f_1	f_2	f_0

Group table of S_3

- If $(G, \cdot)$ and $(G', \cdot')$ are groups then $(G \times G', \cdot)$ is a group with group operation defined by

  $(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot' b_2)$, called as the **Product** group.

The following is an example of a product group.

Let $G = G' = Z_2$. For simplicity of notation, let us denote the equivalence class [0] by $\bar{0}$ and [1] by $\bar{1}$. Then the multiplication table for the product group $Z_2 \times Z_2$ is given below.

$\cdot$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

Definition

Let $(G, \cdot)$ be a group. The order of G is the cardinality of G, denoted by $|G|$.

Examples:

1. The group $(Z, +)$ is of infinite order.
2. The group $(Z_m, +)$ is of finite order viz. m.

Definition

Let $(G, \cdot)$ be a group. Let $a \in G$. The order of a is the **smallest** positive integer n such that $a \cdot a \cdot \ldots \cdot a = a^n = e$. If no such value of n exists for a, then a is said to be of infinite order.

Examples:

1. In $(Z, +)$, every number $n \neq 0$ is of infinite order.
2. In $(Z_4, +)$, order of [1] is 4, order of [2] is 2, order of [3] is 4.

8.6 BASIC PROPERTIES OF A GROUP

Uniqueness of Identity and Inverse

Theorem :

Let $(G, \cdot)$ be a group, then

Identity element e of G is unique.

Every element $x \in G$ has a unique inverse x^{-1} in G.

Proof:

Suppose there exists an element e' is G, with the same property as x.

Then $x \cdot e' = e' \cdot x = x$, for all $x \in G$.

In particular, for $x = e$, we have $e \cdot e' = e' \cdot e = e'$. But since e is also an identity,

$$e \cdot e' = e' \cdot e = e.$$

Hence $e = e'$.

Let an element $y \in G$, such that for all $x \in G$, $x \cdot y = y \cdot x = e$ premultiplying by x^{-1}, we have $x^{-1} \cdot (x \cdot y) = x^{-1} \cdot (y \cdot x) = x^{-1} \cdot e = x^{-1}$.

Using the associativity of $\cdot$, we have $(x^{-1} \cdot x) \cdot y = x^{-1}$ which implies $y = x^{-1}$.

Cancellation Laws:

1. **Left Cancellation Law:** For $a \in G$, $a \cdot x = a \cdot y$ implies $x = y$; and
2. **Right Cancellation Law:** For $a \in G$, $x \cdot a = y \cdot a$ implies $x = y$.

Proof: Left as an exercise.

8.7 CYCLIC GROUP

A group $(G, \cdot)$ is said to be a cyclic group if there exists an element $a \in G$ such that every element of G can be written as some power of a, viz a^k, for some integer k. By a^k, we mean $a \cdot a \cdot a \cdot \ldots \cdot a$ (k times). We then say that G is generated by a or a is a generator of G.

A cyclic group is abelian, since for any two elements $a^r, a^s \in G$, $a^r \cdot a^s = a^{r+s} = a^{s+r} = a^s \cdot a^r$.

Examples:

1. The group $(Z_2, +)$ is cyclic generated by the equivalence class [1].

   In general, the group $(Z_m, +)$ is a cyclic group of order m, generated by [1].

2. Let S be the unit circle and let ρ_0 be a rotation of the circle through an angle $2\pi/n$. Then the set of rotations $\{\rho_0, \rho_0^2, \rho_0^3, \ldots, \rho_0^n\}$ forms a cyclic group of order n, under the operation composition of functions.

The following theorem is significant, as it describes, completely, the structure of finite cyclic groups.

Theorem:

Let G be a cyclic group of order n. Then n is the smallest positive integer such that $a^n = e$, where a is a generator of G.

Proof:

Consider the subset $\{a, a^2, \ldots\}$ of G. Since G is finite, the power of a must terminate at some stage.

Hence there exists positive integers r and s such that $a^r = a^s$.

Assume $r > s$. Then $a^{(r-s)} = e$.

Since there exists atleast (at least) one element with this property, choose m least such that $a^m = e$.

Now $m \leq n$, since otherwise order of g is greater than n.

We shall show $m = n$.

Suppose $m < n$.

Then for any k such that $m < k \leq n$, by division algorithm $k = pm + q$, where $0 \leq q < m$.

Then $a^k = a^{pm+q} = (a^p)^m \cdot a^q = a^q$.

Since $q < m$, $a^q \in \{a, a^2, \ldots, a^m\}$.

Since a is a generator for G, this means $G \subset \{a, a^2, \ldots, a^m\}$, which is absurd.

Hence $m < n$ and therefore $m = n$.

8.8 SUBGROUPS

Subgroups are subsets of a group G, which inherit the group structure of G.

Definition

Let H be a non-empty subset of a group G. Then H is said to be a **Subgroup** of $(G, \cdot)$ if H is itself a group under $\cdot$.

The singleton set {e} is a subgroup of G.

The following theorem gives necessary and sufficient conditions for a subset to be a subgroup.

Theorem:

A non-empty subset H of $(G, \cdot)$ is a subgroup iff

(i) $a, b \in H$ implies $a \cdot b \in H$, i.e. H is closed under $\cdot$.

(ii) $a \in H$ implies $a^{-1} \in H$.

Proof:

Let H be a subgroup of G, then (i) and (ii) are satisfied.

Conversely, let conditions (i) and (ii) hold.

We have to show that H satisfies the group axioms.

For a, b, c ∈ H, a ∘ (b ∘ c) = (a ∘ b) ∘ c holds for G and hence for H.

Hence the associative law holds for H.

Also by condition (ii) every element in H has an inverse in H.

It remains to show that the identity element e ∈ H.

Now by condition (ii) $a \in H$ implies $a^{-1} \in H$.

Hence $a \circ a^{-1} = a^{-1} \circ a = e \in H$, by condition (i).

Thus the theorem is proved.

For a finite group however, condition (ii) becomes redundant as proved in the following theorem.

Theorem:

If H is a non-empty finite subset of a group G and H is closed under multiplication, then H is a subgroup of G.

Proof:

It is enough to show that whenever $a \in H$, $a^{-1} \in H$.

Suppose $a \in H$, then $a^2, a^3, \ldots, a^m \in H$, as H is closed under ∘.

This means that the infinite set $\{a, a^2, \ldots, a^m, \ldots\}$ is a subset of H, which is finite.

This is possible only if the elements are repeated.

Hence for some s, t, $s > t$, $a^s = a^t$.

By cancellation law, this implies $a^{s-t} = e$.

Hence $e \in H$.

Since $s-t-1 \geq 0$, $a^{s-t-1} \in H$ and $a^{-1} = a^{s-t-1}$, as $a \circ a^{s-t-1} = a^{s-t} = e$.

Thus $a^{-1} \in H$, it is proved.

Examples:

1. For a positive integer n, let $H = nZ = \{nx \mid x \in Z\}$. Then (H, +) is a subgroup of (Z, +).
2. Let $H = \{[0], [4]\}$ in $(Z_8, +)$. H is then a subgroup of Z_8.
3. Let G be the group of all 2 × 2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad - bc \neq 0$, under matrix multiplication. Let $H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, ad \neq 0 \right\}$. H is then a subgroup of G.
4. Let G be the group of all non-zero complex numbers a + ib (a, b real) under multiplication. Let $H = \{a + ib \mid a^2 + b^2 = 1\}$. Then H is a subgroup of G.

8.9 COSETS

In this section, we shall see that a subgroup H defines an equivalence relation on a group G, so that G is partitioned into equivalence classes called as cosets.

Definition

Let (G, ∘) be a group and let H be a subgroup of G. For a, b ∈ G, we say a is congruent to b modulo H, written as $a \equiv b \bmod H$, if $a \circ b^{-1} \in H$. One can easily see that the congruence relation is an equivalence relation on G. It therefore partitions G into equivalence classes called as **Cosets** of H. The set of these equivalence classes is also called as the **Quotient** set of G by H.

Definition

Let H be a subgroup of a group (G, ∘). For a ∈ G, define

$Ha = \{h \circ a \mid h \in H\}$. Then Ha is called a **right coset** of H in G.

Similarly, $aH = \{a \circ h \mid h \in H\}$ is called a left coset of H in G.

a is called as the representative element of the coset aH or Ha. If $a \in H$, then $Ha = aH = H$.

Again one can easily show that the cosets are precisely the equivalence classes formed through the congruence relation.

Hence the right cosets of H in G partition G into disjoint subsets. Likewise, the left cosets of H in G yield a partition of G into disjoint subsets.

The concept of cosets as equivalence classes leads to the following theorem, known as Lagrange's theorem, which gives an important relationship between a group and its subgroup.

Theorem (Lagrange):

The order of a subgroup of a finite order divides the order of the group.

Proof:

Let (G, ∘) be a finite group of order n and let H be a subgroup of G of order m.

Consider a right coset Ha $a \in G$. If $a \in H$, then $Ha = H$, which means that number of elements in Ha is the same as the order of H, which means that m/n.

Next let $a \in G$ but $a \notin H$.

Then for any two distinct elements $h_1, h_2 \in H$, $h_1 \circ a \neq h_2 \circ a$.

Hence distinct elements in Ha correspond to distinct elements in H and vice versa.

This means that each right (left) coset contains exactly m elements.

Since the right (left) cosets partition G into disjoint subsets, each containing m elements, it follows that since order of G is n, we must have n/m cosets.

This proves that m divides n.

Remarks :

From Lagrange's theorem, we deduce the following:

- Any group of prime order has only the trivial group {e} as its proper subgroup.
- Consider the permutation group $(S_3, 0)$ described in S_3 has subgroups of order 3 and order 2.

Finding these subgroups is left as an exercise.

8.10 NORMAL SUB-GROUPS

- We have seen that a subgroup H of G induces an equivalence relation on G, so that G can be partitioned into equivalence classes. Our aim now, is to impose a group structure on the set of equivalence classes, so as to form the quotient group. For this, we must first define the product of two equivalence classes, so that this product is compatible with the group operation on G.
- Let H be a subgroup of G, and let Ha, Hb be right cosets of H in G. We want to define Ha ∘ Hb.
- A natural way, that suggests itself is Ha ∘ Hb = Hab. However, this definition makes sense only if Ha = aH. Then for $h_1, h_2 \in H$, $(h_1 \circ a) \circ (h_2 \circ b) = h_1 \circ h_3 \circ a \circ b \in Hab$.
- Hence subgroups in which the right and left cosets are one and the same form an important class of subgroups called as normal subgroups. More formally, we have the following definition of a normal subgroup.

Definition

A subgroup H of G is said to be a **Normal** subgroup of G if for every $a \in G$, aH = Ha.

Examples:

1. A subgroup of an abelian group is normal. For example, nZ is normal in Z (n > 0).
2. Consider the symmetric group $(S_3, 0)$, Then $H = \{f_0, g_2\}$ is a subgroup of S_3. But H is not normal in S_3. Consider $f_1 H = \{f_1, g_1\}$. But $Hf_1 = \{f_1, g_3\}$ since $f_1 H \neq H f_1$, it follows that H is not normal in S_3.

   However consider $K = \{f_0, f_1, f_2\}$. Note that $f_2 = f_1^2$, so that $K = \{f_0, f_1, f_1^2\}$. One can show that every right coset of K in G is equal to a left coset of K is G and vice versa. Hence k is normal in G.

8.11 QUOTIENT GROUP

Let N be a normal subgroup of G. Then G/N is the set of cosets of N in G.

For two coset elements $g_1 N$, $g_2 N \in G/N$ define an operation ∘ on G/N as $g_1 N \circ g_2 N = (g_1 \circ g_2) N$. Note that the operation ∘ on G/N is induced by the operation ∘ in G. (We use the same symbol for both the operations).

With this operation, G/N is a group, with identity element eN. The inverse of each element $g_1 N$ is naturally $g_1^{-1} N$.

The other group axioms, one can easily verify.

8.12 HOMOMORPHISM OF GROUPS

While discussing quotient group, we have implicitly related elements of G and G/H by associating g with g = gH.

In other words, we have defined a function ϕ: G → G/H where

$$\phi(g) = gH.$$

Note that $\phi(g_1 \circ g_2) = \phi(g_1) \circ \phi(g_2)$.

A function characterised by this property is defined below.

Definition

Let (G, ∘) and (G', ∘') be two semigroups, then a function $\phi : (G, \circ) \to G', \circ')$ is called a homomorphism of G and G' if for every a, b ∈ G, $\phi(a \circ b) = \phi(a) \circ' \phi(b)$.

In particular if G and G' are groups, then ϕ is called a group homomorphism.

We have the following theorem which shows that under a group homomorphism, identity is mapped onto identity, and inverse onto inverse.

Theorem:

Let ϕ be a homomorphism of G into G', where G and G' are groups. Then

(i) $\phi(e) = e'$ is the identity element of G'.

(ii) $\phi(g^{-1}) = \phi(g)^{-1}$, for all g ∈ G.

Proof:

For any $g \in G$.

$\phi(g) * e' = \phi(g) * \phi(e)$

$= \phi(g * e) = \phi(e * g) = \phi(g)$.

Similarly one can prove $e' * \phi(g) = \phi(g)$.

Hence e' is the identity element of G'.

(ii) For any $g \in G$, $\phi(g) * \phi(g^{-1})$

$= \phi(g * g^{-1}) = \phi(e) = e'$.

Similarly one can prove $\phi(g^{-1}) * \phi(g) = e'$.

Hence $\phi(g^{-1}) = (\phi(g))^{-1}$

Definition

Let $\phi: G \to G'$ be a homomorphism of semigroups (or groups). Then ϕ is called an **isomorphism** if ϕ is one-one and onto (i.e. injective as well as surjective).

If $G' = G$, then ϕ is called an automorphism.

Examples:

The homomorphism $\phi: Z \to Z$ such that $\phi(n) = -n$ is an automorphism of the group $(Z, +)$.

1. Define $\phi: Z \to Z_m$, where $\phi(n) = [n]$. Then ϕ is a homomorphism of groups $(Z, +)$ and $(Z_m, +)$.
2. The mapping $\pi: Z \to Z|_{mZ}$, where $\pi(n) =$ coset $n + mZ$ is a homomorphism.
3. The following example plays an important role in the transmission of information in coded form, in coding theory.

   Consider $\phi: Z_2 \times Z_2 \to Z_2 \times Z_2 \times Z_2$ given by $\phi(a, b) = (a, b, a + b)$.

   Note that $\phi(0, 0) = (0, 0, 0)$, $\phi(1, 0) = (1, 0, 1)$, $\phi(0, 1) = (0, 1, 1)$, $\phi(1, 1) = (1, 1, 0)$. Clearly ϕ is one-one and onto. Hence ϕ is an isomorphism.
4. Let $Z_5^* = Z_5 - \{0\}$. Then Z_5^* is a group under multiplication.

   Consider the group $(Z_4, +)$ and define a mapping $\phi: (Z_4, +) \to (Z_5^*, \times)$ as $\phi([0]) = [1]$, $\phi([1]) = [2]$, $\phi([3]) = [3]$, $\phi([2]) = [4]$.

   Obviously, ϕ is one-one and onto mapping. One can also verify that ϕ is a homomorphism, by the following method:

   Consider the group tables of $(Z_4, +)$ and $(Z_5^*, \times)$.

$(Z_4, +)$

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$(Z_5^*, \times)$

×	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

In $(Z_4, +)$ replace [0] by [1], [1] by [2], [2] by [4] and [3] by [3] and rewrite the table as

+	[1]	[2]	[4]	[3]
[1]	[1]	[2]	[4]	[3]
[2]	[2]	[4]	[3]	[1]
[4]	[4]	[3]	[1]	[2]
[3]	[3]	[1]	[2]	[4]

Then change + to × and rearrange the rows and columns, so that we obtain

×	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[4]	[3]	[1]	[4]	[2]
[3]	[4]	[3]	[2]	[1]

This table is same as $(Z_5^*, \times)$. Hence it follows that $(Z_5^*, \times)$ is isomorphic to $(Z_4, +)$.

- Let $(A, *)$ be the semigroup whose table of operation is given below.

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

Then the function $f: A \to A$ given by

$f(a) = d$

$f(b) = c$

$f(c) = b$

$f(d) = a$.

is an automorphism of $(A, *)$. f is one-one and onto and one can verify that for any elements $x, y \in A$, $f(x * y) = f(x) * f(y)$.

For example $f(a * b) = f(b) = c$ by definition of f, and also $f(a) * f(b) = d * c = c$.

Hence $f(a * b) = f(a) * f(b)$.

SOLVED EXAMPLES

Example 1: *In each of the following determine whether the set together with the binary operation is a group. If it is a group, determine if it is abelian, specify the identity and inverse of an element a.*

*(i) Z, where * is ordinary multiplication.*

*(ii) Z, where * is subtraction.*

(iii) Q, the set of all rational numbers under the operation of addition.

(iv) Q, the set of all rational numbers under the operation of multiplication.

(v) R, under the operation of multiplication.

Solution: (i) $(Z, *)$ is not a group since the inverses of elements of Z do not exist in Z.

(ii) * is not associative, hence $(Z, *)$ is not a group.

(iii) $(Q, +)$ is an abelian group, with 0 as the identity element.

(iv) $(Q, \times)$ is not a group since the element 0 does not possess an inverse.

(v) $(R, \times)$ is not a group, since the element 0 does not possess an inverse.

Example 2: *Let A = {a, b, c, d} be a group under the operation * defined in the table given below. Find the identity element of the group and find the inverse of each element in the group. Solve the equation $b * x = d$.*

*	A	B	c	d
a	c	D	a	b
b	d	a	b	c
c	a	b	c	d
d	b	c	d	a

Solution: Identity element is c, since $a * c = c * a = a$, $b * c = c * b = b$, $c * c = c$, $d * c = c * d = d$.

Since $a * a = c$ a is the inverse of itself. $b * d = c = d * b$. Hence inverse of b is d, and inverse of d is b. Since $b * a = d$, $x = a$.

Example 3: *Solve the following equations in $(Z_{12}, +)$*

(i) [5] + x = [2], (ii) [7] + x = [5].

Solution: $Z_{12} = \{[0], [1], [2], \ldots\ldots, [11]\}$ identity element is the equivalence class [0].

(i) $[5] + x = [2]$

$\Rightarrow [5] + x = [14]$, since for any element $[y] \in Z_{12} > [y] = [y + 12]$

$\therefore x = [14] - [5] = [9]$

(ii) $[7] + x = [5]$

$\Rightarrow [7] + x = [17]$

$\Rightarrow x = [17 - 7] = [10]$

Example 4: *Find the order and inverse of each element in $(Z_{12}, +)$.*

Solution: The following table gives the elements and their inverses.

Element	Inverse
[0]	[0]
[1]	[11]
[2]	[10]
[3]	[9]
[4]	[8]
[5]	[7]
[6]	[6]

The following table gives the elements and their orders.

Element	Order of the Element
[0]	1
[1]	12
[2]	6
[3]	4
[4]	3
[5]	12
[6]	2
[7]	12
[8]	3
[9]	4
[10]	6
[11]	12

Example 5: *Let $(A, *)$ be a monoid such that for every x in A, $x * x = e$, where e is the identity element. Show that $(A, *)$ is an abelian group.*

Solution: Since $x * x = e$, for all $x \in A$, every element is its own in inverse in A. Hence $(A, *)$ is a group. Let $a, b \in A$.

Consider $(a * b) * (b * a) = a * (b * b) * a = a * e * a = a * a = e$.

Similarly, $(b * a) * (a * b) = e$.

Hence $b * a$ is the inverse of $a * b$. Since a group has unique inverse, it follows that

$a * b = b * a$.

Example 6: *Let (A, ·) be a group. Show that (A, ·) is an abelian group if and only if $a^2 \cdot b^2 = (a \cdot b)^2$.*

Solution: Let (A, ·) be an abelian group. Then $a \cdot b = b \cdot a$, for all $a, b \in A$.

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

$= a \cdot (a \cdot b) \cdot b$ (· is associative)

$= a \cdot (b \cdot a) \cdot b$ (· is commutative)

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

$= (a \cdot b)^2$

Conversely, let $a^2 \cdot b^2 = (a \cdot b)^2$.

To show A is abelian we have

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

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

premultiply by a^{-1} and postmultiply by b^{-1}. Then

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

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

$\Rightarrow \quad a \cdot b = b \cdot a$, for all $a, b \in A$.

Hence (A, ·) is an abelian group.

Example 7: *Let G be a finite group with identity e, and let a be an arbitrary element of G. Prove that there exists a non-negative integer n such that $a^n = e$.*

Solution: Let $|G| = m$, and $a \in G$. Consider $a, a^2, a^3, \ldots, a^m, a^{m+1}$. There are $m + 1$ elements. But since $|G| = m$, this means that $a^{m+1} = a^k (1 \le k \le m)$.

Hence it follows that $a^{m+1-k} = e$. Putting $n = m + 1 - k$, we obtain $a^n = e$.

Example 8: *Let $(Z^+, \bullet)$ denote the group of positive integers under multiplication $\bullet$, and let $H = \{3^k \mid k \in Z\}$. Is H a subgroup of $(Z^+, \bullet)$?*

Solution: First we have to show H is closed under $\bullet$. Let $3^{k_1}, 3^{k_2} \in H$.

Then $3^{k_1} \cdot 3^{k_2} = 3^{k_1 + k_2} \in H$. Hence H is closed under $\bullet$.

Next let $3^{k_1} \in H$. Then by definition 3^{-k_1} is also in H.

Hence H is a subgroup of $(Z^+, \cdot)$.

Example 9: *Let G be an abelian group with identity e and let $H = \{x \mid x^2 = e\}$. Show that H is a subgroup of G.*

Solution: Let x, $y \in H$, then $x^2 = e$, $y^2 = e$. Consider $(xy)^2 = (xy)(yx) = x^2 y^2 = e$ using the fact that G is abelian. Hence H is closed under the group operation. By definition of H, every element x of H is its own inverse. Hence H is a subgroup.

Example 10: *Let G be a group with identity e. Show that the function $f: G \to G$ defined by $f(a) = e$, for all $a \in G$, is a homomorphism.*

Solution: We have to show that for all $a, b \in G$, $f(a \cdot b) = f(a) \cdot f(b)$.

Now $f(a \cdot b) = e$.

Also $f(a) \cdot f(b) = e \cdot e = e$.

Hence f is a homomorphism.

Example 11: *Let G be a group. Show that the function $f: G \to G$, defined by $f(a) = a^2$ is a homomorphism iff G is abelian.*

Solution: Let G be abelian, and let $a, b \in G$.

Then $f(ab) = (ab)^2 = abab$

$= aabb = a^2 b^2 = f(a) \cdot f(b)$.

Hence if G is abelian, f is a homomorphism.

Conversely, let f be a homomorphism. We have to show G is abelian.

Let $a, b \in G$.

$f(ab) = f(a)\ f(b)$

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

$\Rightarrow \quad abab = aabb$. Premultiply this equation by a^{-1} and b^{-1}.

Then $a^{-1} abab^{-1} = a^{-1} aabbb^{-1}$

$\Rightarrow \quad ebae = eabe$

$\Rightarrow \quad ba = ab$, i.e. G is abelian.

Example 12: *Let $G = \{e, a, a^2, a^3, a^4, a^5\}$ be a group under the operation of $a^i a^j = a^r$, where $i + j = r \pmod 6$. Prove that G and Z_6 are isomorphic.*

Solution: $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$,

Define $f: G \to Z_6$ as follows

$e \to [0]$

$[1] \to [a]$

$[2] \to [a^2]$

$[3] \to [a^3]$

$[4] \to [a^4]$

$[5] \to [a^5]$.

$\therefore \quad f([i] + [j]) = a^r$, where $i + j = r \pmod 6$

f is clearly an isomorphism.

Example 13: *Find the subgroup of $(Z_4, +)$ generated by [2]. Subgroup generated by [3] ?*

Solution: Subgroup $H_1 = \{[2], [0]\}$.

$H_2 = \{[3], [2], [1], [0]\} = Z_4$

Example 14: *Find the right cosets of $\{[0], [3], [6], [9]\}$ of $(Z_{12}, +)$.*

Solution: $H = \{[0], [3], [6], [9]\}$

We obtain the following distinct right cosets

$H_0 = \{[0], [3], [6], [9]\}$

$H_1 = \{[1], [4], [7], [10]\}$

$H_2 = \{[3], [6], [9], [0]\}$

$H_3 = \{[5], [8], [11], [2]\}$

$H_4 = \{[6], [9], [0], [3]\}$

$H_6 = \{[8], [11], [2], [5]\}$

$H_7 = \{[9], [0], [3], [6]\}$

$H_8 = \{[11], [2], [5], [8]\}$

Example 15: *The set $H = \{f_0, f_1, f_2\}$ is a subgroup of $(S_3, 0)$. Find the left coset of H.*

Solution:

$$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$g_1 H = \{g_1, g_2, g_3\}$

$g_2 H = \{g_2, g_3, g_1\}$

$g_3 H = \{g_3, g_1, g_2\}$

Example 16: *Find the subgroups of*

(i) Z_8 (ii) $Z_2 \times Z_2$

Solution: (i) The group table for Z_8 under addition is given below:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{7}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$

The following are the subgroups of $(Z_8, +)$

$H_1 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$ and

$H_2 = \{\bar{0}, \bar{4}\}$

H_1 and H_2 are closed under group operation.

(ii) The group table for $(Z_2 \times Z_2, +)$ is given below:

+	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

The following are subgroups of $Z_2 \times Z_2$

$H_1 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1})\}$

$H_2 = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0})\}$

$H_3 = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{1})\}$

One can verify that H_1, H_2, H_3 are all closed under group operation. (cf. Theorem 8.7.3).

Example 17: *Let G be a group; for a fixed element G, let $G_x = \{a \in G: ax = xa\}$. Show that G_x is a subgroup of G for all $x \in G$.*

Solution: One of the conditions for G_x to be a subgroup is that G_x should be closed under multiplication. Let a, $b \in G_x$, we have to prove that $ab \in G_x$. Now $ax = xa$, $bx = xb$.

$\therefore \quad (ab)x = a(bx)$

$= a(xb) = (ax)(b) = (xa)(b)$

$= x(ab)$.

Also it is clear that $e \in G_x$. It only remains to show that $x^{-1} \in G_x$. For this consider $e = a \Rightarrow x^{-1}(xa) = a \Rightarrow x^{-1}(ax) = a \Rightarrow (x^{-1}a)(xx^{-1}) = ax^{-1}$.

i.e. $(x^{-1}a)(e) = x^{-1}a = ax^{-1}$

Hence, G_x is a subgroup of G.

Example 18: *G is a group and there exists two relatively prime positive integers m and n such that $a^m b^m = b^m a^m$ and $a^n b^n = b^n a^n$ for all $a, b \in G$. Prove that G is abelian.*

Solution: Since m and n are relatively prime, there exist integers p, q such that $mp + nq = 1$. First we shall show that, $\forall\ a, b \in G$.

$(a^m b^n)^{pm} = (b^n a^m)^{pm}$ and

Similarly,

$(a^m b^n)^{2n} = (b^n a^m)^{2n}$

Note that:

$$(a^m b^n)^{pm} = a^m (b^n a^m)(b^n a^m) \ldots (b^n a^m)\, b^n \quad (pm - 1) \text{ times}$$
$$= a^m (b^n a^m)^{pm-1} \cdot b^n$$
$$= a^m (b^n a^m)^{pm} (b^n a^m)^{-1} \cdot b^n$$
$$= a^m (b^m a^n)^{pm} a^{-m} b^{-n} \cdot b^n$$
$$= (b^n a^m)^{pm} a^m a^{-m} \quad (\because a^m b^m = b^m a^m, \ \forall\, a, b \in G).$$

Similarly,

$$(a^m b^n)^{qn} = (b^n a^m)^{qn}$$
$$\therefore \quad a^m b^n = (a^m b^n)^{pm \cdot qn}$$
$$= (a^m b^n)^{pm} (a^m b^n)^{qn}$$
$$= (b^n a^m)^{pm} (b^n a^m)^{qn}$$
$$= (b^n a^m)^{pm \cdot qn} = b^n a^m, \ \forall\, a, b \in G$$

Now consider,

$$ab = a^{pm \cdot qn}\, b^{pm \cdot qn}$$
$$= a^{pm} \cdot a^{qn} \cdot b^{pm} \cdot b^{qn} = a^{pm}$$
$$= a^{pm} (a^q)^n (b^p)^m b^{qn}$$
$$= apm\ bpm\ aqn\ bqn$$
$$= bpm\ apm\ bqn\ aqn$$
$$= bpm\ bqn\ apm\ aqn$$
$$= (b)pm + qn\ (a)pm + qn$$
$$= b^1 a^1 = ba$$

Example 19: *Show that {1, 2, 3} under multiplication modulo 4 is not a group but that {1, 2, 3, 4} under multiplication modulo 5 is a group.*

Solution: Let, $G_1 = \{1, 2, 3\}$. Multiplication Table for G_1 is

X_4	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

$0 \notin G_1$, closure property is not satisfied, hence G_1 is not a group.

Let $G_2 = \{1, 2, 3, 4\}$

Multiplication Table for G_2 is

X_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

G_2 is closed under multiplication. Multiplication is associative.

For example, $2 \times (3 \times 4) = 2 \times 2 = 4$ and $(2 \times 3) \times 4 = 1 \times 4 = 4$.

The rows and columns when interchanged yield the same elements, so that G_2 is commutative. From table the inverses of 1, 2, 3, 4 are 1, 3, 2, 4 respectively. Hence, G_2 is an abelian group under X_5.

Example 20: *Show that (A, +) is a group where A = {... −4a, −3a, −2a, 0, a, 2a, 3a, 4a, ...}*

Solution: $A = \{na \mid n \in Z\}$

(i) + is associative

$(x + y) + z = (n_1 + n_2)\, a + n_3\, a = (n_1 + n_2 + n_3)\, a$

$x + (y + z) = n_1 a + (n_1 a + n_3 a) = (n_1 + n_2 + n_3)\, a$

(ii) $x + 0 = na + 0 = na = x$

(iii) If $x = na$, $-x = -na$.

$x + (-x) = (n - n)\, a = 0a = 0$

Hence (A, +) is a group.

Example 21: *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.*

Solution: (i) * is associative, since

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

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

(ii) $e = 2$ since $a * 2 = \frac{2a}{2} = a = 2 * a$.

(iii) For each $a \in G$,

$$a^{-1} = \frac{4}{a}, \text{ because } a * a^{-1} = a * \left(\frac{4}{a}\right)$$

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

$$a^{-1} * a = \left(\frac{4}{a}\right) * a = \frac{4a}{2a} = 2$$

(iv) $a * b = \frac{ab}{2} = b * a$, i.e. * is commutative.

Hence, (G, •) is an Abelian group.

Example 22 : *Consider an algebraic system (G, •), where G is the set of all non-zero real numbers and • is a binary operation defined by a • b = ab/4. Show that (G, •) is an abelian group.*

Solution : Similar lines, as the above example. 21.

Example 23: *Consider an algebraic system (Q, •), where Q is set of rational numbers and • is binary operation defined by a • b = a + b − ab; ∀ a, b ∈ Q. Determine whether (Q, •) is a group.*

Solution: We have shown that ∀ is associative . Suppose (Q, •) is a group, let us find the identity element e.

Let $a \neq 1 \in Q$. Then $a * e = a \Rightarrow a + e - ae = a \Rightarrow a(1 - a) = 0 \Rightarrow e = 0$.

Hence the number 0 must be the identity element if (Q, •) where to be a group. Let '1'' be inverse of 1. Then $1 * 1' = 0 \Rightarrow 1 + 1' - 1 \cdot 1' = 0 \Rightarrow 1 + 1' - 1' = 0 \Rightarrow 1 = 0$ observed. Hence the number 1 has no inverse in (Q, •). Hence, (Q, •) is not a group. If we remove 1 from Q, i.e. consider $Q = Q - \{1\}$, then (Q, •) becomes a group with identity element 0 and inverse of every element a, given by $\frac{a}{1-a}$.

Example 24 : *Prove that every cyclic group is an abelian group.*

Solution : By definition of a cyclic group (G, •), every element of G can be expressed as a^k, where a is a generator of G and k is any positive integer. Let $x, y \in G$; then $x = a^r$, $y = a^s$ for some positive integer r and s.

Therefore, $x * y = a^r * a^s = a^{r+s} = a^{s+r} = a^s * a^r = y * x$.

This proves that (G, •), where G is a cyclic group is abelian.

Example 25 : *Show that if N is a normal subgroup of (G, •) then (G, N, •) is a group.*

Solution : G/N is the set of cosets $\{gN \mid g \in G\}$.

For elements $g_1, g_2 \in G$, $g_1 N * g_2 N = g_1 g_2 N$, as $gN = Ng$ $\forall\, g \in G$, as N is normal subgroup of G. (G/N, •) satisfies the following group axioms.

(i) $(g_1 N * g_2 N) * g_3 N = g_1 N * (g_2 N * g_3 N)$ (Associative law)

(ii) The identity element is $eN = N$ as

$$gN * eN = g(N * e) * N$$
$$= g(N) * N = g(N) * N = gN$$

(iii) For each $GN \in G/N$, inverse is given by $g^{-1}N$ as

$$gN * g^{-1}N = g * g^{-1} N$$
$$= eN = N$$

8.13 RINGS, INTEGRAL DOMAINS AND FIELDS

8.13.1 Rings

So for we have discussed groups which are algebraic structures with a single binary operation. We now turn our attention to algebraic structures, with two binary operations, called **Rings.** We shall denote these binary operations by + and · respectively. In analogy with numbers, + is called addition and · multiplication.

Definition

An algebraic structure (R, +, ·) is called a ring if

1. (R, +) is an abelian group.
2. Associativity of multiplication holds: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. The left distributive law

$a \cdot (b + c) = a \cdot b + a \cdot c$, and the right distributive law

$(b + c) \cdot a = b \cdot a + c \cdot a$ are satisfied by + and ·.

Definition

A ring R is said to be commutative ring if $a \cdot b = b \cdot a$, for all $a, b \in R$.

Definition

A ring R is said to be a ring with **unit** element if there exists an element, denoted by the symbol 1 such that $a \cdot 1 = 1 \cdot a = a$, for all $a \in R$.

Examples:

1. (Z, +, ·) is a ring, where Z is the set of integers, + and · are the usual addition and multiplication respectively. It is a commutative ring with unit element, the integer 1.
2. Z_m, the set of integers modulo m is a commutative ring with unit element (1) under addition and multiplication (modulo m).
3. The set of even integers including 0, under addition and multiplication is a commutative ring with no unit element.
4. The set of m × m matrices over the real numbers, is a non-commutative ring but with unit element (the identity matrix), under matrix addition and multiplication.
5. Other common examples are the set of rational, real and complex numbers, which however form a special class of rings called as fields.

For a ring R, we shall denote the additive identity by 0 and the multiplicative unit element by 1.

Basic Properties

If R is a ring with identity 0 and unit element 1, then following are true, for all elements a, b ∈ R.

(i) $a \cdot 0 = 0 \cdot a = 0$.

(ii) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$.

(iii) $(-a) \cdot (-b) = a \cdot b$

(iv) unit element is unique

(v) $(-1) \cdot a = -a$

(vi) $(-1) \cdot (-1) = 1$.

Proof:

(i) $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ by left distributive law. Hence it follows by cancellation law, $a \cdot 0 = 0$.

(ii) Consider $a \cdot (-b) + a \cdot b = a \cdot (-b + b)$ (left distributive

$= a \cdot 0 = 0$

Hence by uniqueness of inverse, it follows that

$a \cdot (-b) = -(a \cdot b)$

One can prove similarly that

$(-a) \cdot b = -(a \cdot b)$

(iii) $(-a) \cdot (-b) = -((-a) \cdot (b))$

$= a \cdot b$. Since $-(-a) = a$.

(iv) Suppose there exists another element 1' with the same property of 1, then $1 \cdot 1' = 1' \cdot 1 = 1$, since 1' is unit element. Since 1 is also a unit element, $1 \cdot 1' = 1' \cdot 1 = 1'$.

This implies 1 = 1', i.e. unit element, if it exists, is unique.

(v) and (vi) follow from (ii) and (iii) respectively.

The above theorem tells us that we can freely compute with negative and 0, as we do in the case of numbers.

Subring: Analogous to the concept of subgroup of a group, we introduce that of a subring in a ring.

Definition

A subset $R \subseteq S$, where $(S_1, +, \cdot)$ is a ring, is called a subring of S if $(R, +, \cdot)$ is a ring with the operations + and · restricted to elements of R.

Examples:

1. The ring of even integers is a subring of the ring of integers. More generally for any positive integer n, the set

$$nZ = \{ nm \mid m \in Z \} \text{ is a subring of } Z.$$

2. The set of rationals is a subring of the ring of real numbers.

8.13.2 Ring Homomorphism

Let $(R, +, \cdot)$ and $(S, +', \cdot')$ be rings. A mapping $\phi: R \to S$ is called a **Ring Homomorphism,** if for any a, b ∈ R.

(i) $\phi(a + b) = \phi(a) +' \phi(b)$

(ii) $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

If ϕ is one-one and onto, it is called as a ring **Isomorphism.**

One can easily verify that $\phi(0) = 0'$ and $\phi(-a) = -\phi(a)$, for every a ∈ R.

Definition

Let $(R, +, \times)$ and $(S, +', \psi')$ be rings, with identities 0 and 0' respectively. Let f: R → S be a ring homomorphism. Then **kernel** of f is defined as the set $\{x \in R \mid f(x) = 0'\}$.

We denote kernel of f as ker (f) or ker f.

Example:

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 if is a homomorphism.

(ii) Determine the kernel of f.

Solution:

(i) $f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} + \begin{bmatrix} c & d \\ d & c \end{bmatrix}\right)$

$= f\left(\begin{bmatrix} a+c & b+d \\ b+d & a+c \end{bmatrix}\right)$

$= (a + c) - (b + d)$

$= (a - b) + (c - d)$

$= f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) + f\left(\begin{bmatrix} c & d \\ d & c \end{bmatrix}\right)$

Also

$f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ d & c \end{bmatrix}\right) = f\begin{bmatrix} ac + bd & ad + bc \\ bc + ad & bd + ac \end{bmatrix}$

$= (ac + bd) - (ad + bc)$

$= (ac - bc) + (bd - ad)$

$= (a - b)(c - d)$

$= f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) \cdot f\left(\begin{bmatrix} c & d \\ d & c \end{bmatrix}\right)$

(ii) $\ker(f) = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} ; a - b = 0 \right\}$

i.e. $\left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} ; a \in Z \right\}$.

Examples:

- The mapping $\phi: Z \to Zn$ defined by $m \to [m]$, is a ring homomorphism.

Similar to the concept of a normal subgroup in groups, we have the concept of an **ideal** in ring R.

Definition

A non-empty set I of a ring R is called an **ideal** in R if

(i) I is a subgroup of R, under addition.

(ii) For every a ∈ I, $a \cdot x = x \cdot a$, for all x ∈ R.

Examples:

1. If Z is the set of integers, then the set nZ is an ideal in the ring $(Z, +, \cdot)$.

For an ideal I in R, the quotient group R/I becomes a ring in a natural way.

For elements x + I, y + I in R / I, we define $(x + I) \cdot (y + I) = xy + I$, x, y ∈ R.

The routine verification of the various ring axioms, is left as an exercise. The ring R/I is called the **Quotient Ring** of R.

The mapping $\phi: R \to R / I$ defined as $\phi(x) = x + I$ is a ring homomorphism, details to be worked out as an exercise.

8.13.3 Zero Divisors

Let R be a commutative ring. Then a ≠ 0 ∈ R is called a zero divisor if there exists b ≠ 0 ∈ R, such that $a \cdot b = 0$.

Examples:

1. [2] is a zero divisor in $(Z_4, +, \cdot)$, since [2], [2] = [2·2] = [4] = 0.
2. In the quotient ring Z/6Z, (2 + 6Z) (3 + 6Z) = 0 + 6Z. Hence 2 + 6Z and 3 + 6Z are zero divisors.

8.13.4 Integral Domains and Fields

Definition:

Let R be a commutative ring. Then R is called an **Integral Domain** if it has no zero divisors.

Definition

Let R be a commutative ring with unit element. If every non-zero element has a multiplicative inverse, then R is called a field. A field is an integral domain, since if a, b ∈ R, then $a \cdot b = 0$ implies $(a^{-1} \cdot a) \cdot (b \cdot b^{-1}) = (a^{-1} \cdot 0) \cdot b^{-1} = 0$ which further implies $1 \cdot 1 = 0$, which is not true, since $1 \cdot 1 = 1$.

Examples:

The ring of rational numbers, the ring of real numbers are standard examples of fields, as each non-zero element possesses its multiplicative inverse.

A field is an integral domain. However, not every integral domain is a field. The following theorem tells us which of them are fields.

Theorem:

A finite integral domain is a field.

Proof:

Let D be a finite integral domain.

We must show that D possesses the unit element 1 and for every $a \neq 0$ in D, $a^{-1} \in D$.

Since D is finite, let $x_1, x_2, \ldots, x_n$ be distinct elements of D.

Let $a \neq 0 \in D$.

Then the elements $a \cdot x_1, a \cdot x_2, \ldots, a \cdot x_n$ are all in D.

We claim that these elements are all distinct.

Suppose not, then $a \cdot x_i = a \cdot x_j$, for $x_i, x_j \in D$.

This means that $a \cdot (x_i - x_j) = 0$.

Since D is an integral domain, this implies $x_i - x_j = 0$, i.e. $x_i = x_j$.

Hence our claim is valid.

Since D contains exactly n elements, we must have $a = a \cdot x_k$ for some $x_k \in D$.

We prove what x_k is the unit element of D. Let $y \in D$.

Then $y = a \cdot x_i$, for some $x_i \in D$. Hence $y \cdot x_k$

$= (a \cdot x_i) \cdot x_k = x_i \cdot (a \cdot x_k)$

$= x_i \cdot a = y$.

Hence we have shown that D contains a unit element $1 = x_k$.

Since $1 \in D$, $1 = a \cdot x_j$, for some x_j, for any $a \neq 0 \in D$.

Hence every non-zero element has a multiplicative inverse in D.

This completes the proof.

SOLVED EXAMPLES

Example 1: *Find the multiplicative inverse of each non-zero element in $(Z_7, +, \cdot)$.*

Solution: (i) Table is

×	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[6]	[5]	[4]	[3]	[2]	[1]

(ii) The elements and their inverses are given below.

Element	Inverse
[1]	[1]
[2]	[4]
[3]	[5]
[4]	[2]
[5]	[3]
[6]	[6]

Example 2: *Show that* $S = \{a + b\sqrt{2} ; a, b \in Z\}$ *for the operations +, × is an integral domain but not a field.*

Solution: We have

$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$

$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2}$

Clearly S is a commutative ring with unit element 1.

We have to prove S is an integral domain.

Let $(a + b\sqrt{2})(c + d\sqrt{2}) = 0$

This implies

$ac + 2bd = 0$ ... (1)

and $bc + ad = 0$ ... (2)

Suppose $a = 0$; then $bd = bc = 0$.

$\therefore$ 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 (1) by d gives

$acd + 2bd^2 = 0$ ... (3)

From (2), $ad = -bc$

Hence, substituting this in equation (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 exist in S, for $(2 + \sqrt{2})(c + d\sqrt{2}) = 1$

$\Rightarrow 2c + 2d = 1 \Rightarrow c + d = \frac{1}{2}$

Absurd, since c, d $\in$ Z.

Example 3: *If R is a ring such that* $a^2 = a$, $\forall a \in R$, *prove that*

(i) $a + a = 0$, $\forall a \in R$.

(ii) R is a commutative ring.

Solution: (i) Let $b = -a$, i.e. inverse of a.

We have to prove $a = b$.

Consider, $a - b = (a - b)(a - b)$

i.e. $a - b = a^2 - ba - ab + b^2$

$= a - ba - ab + b$

$= (a + b) - ba - ab$

$= 0 - ba - ab = -ba - ab$ ... (1)

Now,

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

$= a^2 + ba + ab + b^2$

$= a + ba + ab + b$

$= (a + b) + ba + ab$

$= 0 + ba + ab$ ... (2)

$\therefore$ $ba + ab = 0$

Hence, $a - b = 0$, i.e. $a = b$.

(ii) We have to prove that R is commutative. For any elements $a, b \in R$,

$a + b = (a + b)(a + b)$

$= a^2 + ba + ab + b^2$

$= a + ba + ab + b$

$\therefore$ $ba + ab = 0$

or $ab = -ba$

By (1) every element is its own inverse. Hence, $-ba = ba$.

$\therefore$ $ab = ba$, i.e. R is commutative.

EXERCISE - 8.1

1. For each of the following, determine whether the binary operation is associative or commutative.
   (i) on **R**, where $a \cdot b = a\sqrt{b}$
   (ii) on Z^+, where $a \cdot b = ab + 1$
   (iii) on a lattice A, where $a \cdot b = a \vee b$
   (iv) on the set of all n × n Boolean matrices, under matrix addition.
   (v) on the set of all prime numbers, under multiplication.

2. In each of the following, complete the table, so that the binary operation $\cdot$ is associative.

(i)

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

(ii)

*	A	b	c	d
a	a	b	c	d
b	b	a	c	d
c	–	–	–	–
d	D	c	c	d

3. Let A be a set with n elements.
   (i) How many binary operations can be defined on A ?
   (ii) How many commutative binary operations can be defined on A ?
4. Let A = {a, b, c}. For each of the binary operation $\cdot$ defined on A, by the corresponding tables, determine whether $\cdot$ is associative or commutative. Determine also whether $\cdot$ has a right or left identity.

(i)

*	A	b	c
A	B	c	a
b	c	a	b
c	a	b	c

(ii)

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

5. Let G be a group with identity e. Show that if $x^2 = x$ for some x in G, then $x = e$.
6. Let G be a group. Show by mathematical induction that if $ab = ba$, then $(ab)^n = a^n b^n$ for $n \in Z^+$.
7. Let G be a group of integers under the operation of addition and let $H = \{3k \mid k \in Z\}$. Is H a subgroup of G ?
8. Let G be a group and let $H = \{x \mid x \in G \text{ and } xy = yx \text{ for all } y \in G\}$. Prove that H is a subgroup of G.
9. If H and K are subgroups of a group G, then show that $H \cap K$ is also a subgroup. Is $H \cup K$ a subgroup ?
10. Prove that the function $f(x) = |x|$ is a homomorphism from the group G of non-zero real numbers under multiplication to the group G^+ of positive real numbers under multiplication.
11. Is the set {{0}, {3}, {5}} a subgroup in $(Z_6, +)$?
12. Find the subgroup of $(Z_{12}, +)$ generated by the set {[6], [9]}.
13. Find the left cosets of the subgroup {[0], [3], [6], [9]} of $(Z_{12}, +)$.
14. Which elements of $(Z_{12}, +)$ generate a proper cyclic subgroup ?
15. Show that the set H = {0, 4, 8} is a subgroup of $(Z_{12}, +)$. Find its left cosets.
16. Show that if $(G, \cdot)$ is a cyclic group, then every subgroup of $(G, \cdot)$ is cyclic.
17. Let $(G, \cdot)$ be a group of prime order p. Show that G is a cyclic group. Deduce that the groups $(G, \cdot)$ and $(Z_p, +)$ are isomorphic.
18. Which of the following are rings ?
   (i) The set Q^* of positive rational numbers under addition and multiplication.
   (ii) Let p be a prime, and let Q_p be the set of rational numbers of the form $\left\{x : x = m \mid p^n \ldots, m \in Z\right\}$ under addition and multiplication.
   (iii) The subset {[0], [2], [4]} of $(Z_6, +)$.
19. Find all the subgroups of (i) Z_8, (ii) $Z_2 \times Z_2$.
20. Show that in the ring $(Z_6, +)$ both S = {[0], [2], [4]} and T = {[0], [3]} are subrings.
21. Write the operation tables for $(Z_2^2, +, \times)$. Is Z_2^2 a ring, integral domain, field ?

22. Show that the following rings are not isomorphic
    (i) $(3Z, +, \times)$ and $(4Z, +, \times)$.
    (ii) $(Z_2 \times Z_2, +, \cdot)$ and $(Z_4, +, \cdot)$.
23. Prove that $Z_2 \times Z_3$ is a commutative ring with unity. Find all zero divisors of $Z_2 \times Z_3$.
24. We are given the ring $(\{a, b, c, d\}, +, \cdot)$ whose operations are given below:

+	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

·	a	b	c	d
a	a	a	a	a
b	a	c	a	c
c	a	a	a	a
d	a	c	a	c

    Is it a commutative ring ? Does it have an identity ? What is the zero of this ring ? Find the additive inverse of each of its elements.
25. Prove that the ring $(Z_5, +, \cdot)$ is a field. Is $(Z_6, +, \cdot)$ a field ?
26. Prove that the set of numbers of the form $a + b\sqrt{2}$, where a, b are rational numbers, is a field.
27. Prove that the four matrices $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ form a field, where the entries $0, 1 \in Z_2$.
28. Let $R = \{0°, 60°, 120°, 180°, 240°, 300°\}$ and $\cdot$ = binary operation so that for a and b in R, a $\cdot$ b is overall angular rotation corresponding to successive rotations by a and then by b. Show that $(R, \cdot)$ is group.
29. Let Z_n be the set of integers $\{0, 1, 2, ..., n-1\}$. Let $\oplus$ be a binary operation on Z_n such that
$$a \oplus b = \begin{cases} a + b, & \text{if } a + b < n \\ a + b - n; & \text{if } a + b \geq n \end{cases}$$
    Let $\odot$ be a binary operation on Z_n such that $a \odot b$ = the remainder of and divided by n. Show that $(Z_n, \oplus)$ is abelian group and $(Z_n, \oplus, \odot)$ is a ring.
30. Define homomorphism and normal subgroups with example.
31. Define with example (with respect to group).
    (i) Isomorphism and Homomorphism
    (ii) Automorphism.
    (iii) Group
    (iv) Permutation group
    (v) Subgroup
    (vi) Normal subgroup
    (vii) Algebraic system with two binary operations
32. Define congruence classes with respect to groups. Define Abelian group. Show that $<Z_6, +>$ is Abelian group.
33. Define Abelian group, subgroup, power subgroup and normal subgroup with example.
34. Define subgroup of a group. Z is a group of integers under addition, H is the subset of Z consisting of all multiples of a positive integer m, that is
    $H = \{..., -3m, -2m, -m, 0, n, 2m, 3m, ...\}$. Show that H is a subgroup of Z.
35. Let $R = \{0°, 60°, 120°, 180°, 240°, 300°\}$ and $\cdot$ binary operation so that for a and b in R, a $\cdot$ b is overall angular rotation corresponding to successive rotations by a and then by b. Show that $(R, \cdot)$ is a group.
36. Show that $G = \{1, 5, 7, 11\}$ is a group under multiplication modulo 12.
37. Show that the set of cube roots of unity forms a group under multiplication.
38. Explain group Homomorphism and Isomorphism of groups. Take suitable example. **(Nov./Dec. 14)**
39. Explain the terms :
    (i) Homomorphism of group.
    (ii) Automorphism of group. **(May 15)**
40. Prove that $\{(a + b\sqrt{2}), +, \cdot\}$, where $a, b \in R$ is an integral domain. **(Nov./Dec. 14)**

8.14 GROUP CODES

- Developing technologies in various fields necessitate the transmission of large amount of data from one place to another. Specific examples are telecommunication over phone, satellite communication over the large distances and data transmission between the computers and other instrumentation systems.
- In transmitting the data, interferences such as noises from external sources may cause an error in transmission so that a received data is different from the transmitted one. The noise may be human link, lightning, thermal noise, imperfection of equipments etc. It is therefore important to detect and correct the error in the data transmitted through the communication channel.

- A device that can be used to improve the efficiency of the communication channel is an **Encoder** which transforms the incoming message in such a way that the presence of noise on the transformed message is detectable. The use of encoder requires that a **Decoder** be employed to transform the encoded message into their original form that is acceptable to the receiver. Therefore, it is possible to detect the distortion due to the noise in the channel and then correct the message by using proper encoder and decoder devices. A general structure of data communication system is shown in Fig. 8.13.

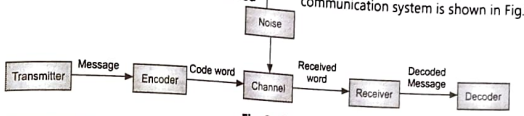

Fig. 8.13

- When messages, originally expressed in some language, are transformed into another language such that these messages can be transformed back again, then such messages are said to be **'Coded'.** More formally, a **code is a collection of words that are to be used to represent distinct messages.** A word in a code is also called a **Code Word.**
- The process of passing from a message word to its corresponding code word is referred so an **Encoding** which is done by encoder and the reverse process called **Decoding** is done by decoder.
- There are many examples of codes like morse code which is used in telegraphy, ASCII (American Standard Code for Information Interchange), EBCDIC (Extended Binary Coded Decimal Interchange Code) etc. In most of the applications, the communication channel uses **Binary Code** in which each code word is represented by a string of digits which is either 0 or 1 i.e. a word over the alphabet {0, 1} (binary alphabet). These words are also called **Binary Words** and their digits are called **Bits.** The communication channel which uses binary code is referred as **Binary Channel.** The number of bits in the binary word is called the length of the **Binary Word.** A **Block Code** is a code consisting of words that are of the same length.
- We now illustrate the essential features of error detection and correction in the following examples.
- Suppose that words to be transmitted through a binary channel are all the members of the set of binary words of length 3 i.e. of B^3, where $B^3 = \{000, 001, 010, 100, 110, 101, 011, 111\}$. Suppose that the word 010 is transmitted and that an error occurs in the third digit so that the received word is 011. The receiver cannot detect this error because 011 is a member of the set B^3 of words which we might expect to receive. Further, if we cannot detect the error, there is no question of correcting it. This example highlights one property that to detect errors, an incorrectly transmitted word must **not** be the member of the set of words which are expecting to receive.
- Consider another example in which the words for transmission are members of the set {111, 100, 001, 010}. Suppose the received word is 011. This word is not the member of the set of words. Hence, the receiver will come to know that an error has occurred, but he cannot determine at which place it is occurred. Considering the probability of one error, the transmitted word can be 111 or 010 or 001. In this case, a single error can be detected but cannot be corrected. Note that two errors cannot (be) detected because errors in any two digits of a word result in another member of the set.
- From above examples it is clear that the error detection and correction both depend upon the words in the set of possible transmitted words being sufficiently different from one another the codes with error detecting and correcting properties have a mathematical structure, known as **Group Structure** described. We now present this group structure of codes with some definitions.
- Let S_n denote the set of all binary words of length n. Let $\oplus$ be a binary operation on S_n such that for any x, y $\in S_n$, where
$$x = (x_1, x_2, ..., x_n) \text{ and } y = (y_1, y_2, ..., y_n),$$
$$x \oplus y = (x_1 \oplus y_1, x_2 \oplus y_2, ..., x_n \oplus y_n) \quad ... (8.1)$$

where the operation ⊕ denotes the addition modulo 2 on {0, 1} and is given by the following table:

⊕	0	1
0	0	1
1	1	0

Table for operation ⊕

For example, suppose x = (10101) and y = (00100) then x ⊕ y = (10001).

- The algebraic structure $(S_n, \oplus)$ is a group in which n tuple of 0's (000 ... 0) is an identity and each element is its own inverse. In general, any code which is a group under the operation ⊕ is called a **Group Code.** Group code was introduced by Hamming and is very useful in binary encoding techniques.

8.14.1 Weight and Hamming Distance

Let x be a word in S_n. We define the **weight** of **x**, denoted by **w(x)**, to be the **number of ones in x**. Thus the weight of (01011) is 3.

Similarly w (11001001) = 4

Let $x = (x_1, x_2, ..., x_n)$ and $y = (y_1, y_2, ..., y_n)$ be any two elements of $(S_n, \oplus)$ where, $x_i, y_i \in (0, 1)$ for all i. The **Hamming Distance** or simply **Distance** between x and y, denoted by d (x, y), is the number of co-ordinates for which all x_i and y_i are different. For example, if x = (001101) and y = (111110), the two words x and y have different first, second, fifth and sixth digits i.e. they are different in total 4 places. Hence d (x, y) = 4. In terms of weights, the distance between x and y is given by

$$d(x, y) = w(x \oplus y). \quad \ldots (8.2)$$

The Hamming distance satisfies a number of useful mathematical properties, namely, that for all x, y, z ∈ S_n,

$$d(x, y) \geq 0$$

$$d(x, y) = 0 \Leftrightarrow x = y \quad \ldots (8.3)$$

$$d(x, y) = d(y, x)$$

$$d(x, z) \leq d(x, y) + d(y, z).$$

Now we define the minimum distance of a code. The **Minimum Distance of a Code** is defined to be the minimum of all the distances between distinct pair of code words. As an example,

let x = (10001), y = (01000) and z = (10101).

The distances are d (x, y) = 3, d (x, z) = 1 and d (y, z) = 4. Therefore, the minimum distance between the words x, y and z is 1.

With the help of weight and minimum distance, as described above, a combination of errors can be detected and corrected. The following theorems give criteria for determining the capability for error detection and error correction in a code.

Theorem: The minimum weight of the **Non Zero** code words in a group code is equal to its minimum distance.

Theorem: A code can detect all combinations of k or fewer errors if and only if the minimum distance between any two code words is at least k + 1.

Theorem : A code can correct all combinations of k or fewer errors if and only if the minimum distance between any two code words is at least 2k + 1.

For example, suppose a code contains only two words of length 3, C = {(000), (111)}. The minimum weight of the nonzero code word is 3 and thus according to the minimum distance is also 3. From this code can detect any combinations of two errors or one error it can correct only one error.

8.14.2 Generation of Codes by using Parity Checks

- The first complete error detecting and error correcting encoding procedure (was) developed by Hamming in 1950. This procedure has been frequently used in computer systems and it is very popular.
- Hamming constructed the codes, called **Hamming Codes,** by introducing redundant digits 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. The later digits are called **Parity Checks.**
- Hamming's single error detecting codes can be described as follows. 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 1s. Such an encoding procedure is called an **Even Parity Check.** An **Odd Parity Check** can also be used by making the entire message containing an odd number of 1s. For example, the message {00, 01, 10, 11} become {000, 011, 101, 110} when a single even parity check digit is added. For odd parity check it becomes {001, 010, 100, 111}. Hamming developed an error-correcting method, based on these parity checks, which enabled the detection of the position of erroneous digits. For codes

involving check digits, the distance between each pair of code words is **not** necessarily the same so that the factor determining the error detecting and error correcting capabilities of the code is the minimum of the distances between pair of code words.

- The code words of length n in which information is contained in m digits (m < n) and the remaining k = n – m digits are parity checks, can be generated by using a k × n matrix H. This matrix H is called a **Parity Check Matrix** where elements are zeros and ones. A single error correcting code of length n generated by H will have k parity check bits given by

$$2^k \geq n + 1.$$

or $$2^k \geq (m + k) + 1$$

or $$m \leq 2^k - k - 1 \quad \ldots (8.4)$$

- The information digits m in the code word is given by 8.13.4. The number of code words generated by H is $2^m = 2^{n-k}$ and the code generated in this way is called **Hamming code.**

For example, consider the parity check matrix.

$$H = \begin{pmatrix} 11\ 10\ 100 \\ 11\ 01\ 010 \\ 10\ 11\ 001 \end{pmatrix} \quad \ldots (8.5)$$

- It is of order 3 × 7 and it will generate a code word of length 7 in which 3 digits are parity checks. Each code word will have m = 7 – 3 = 4 information bits. Also H will generate $2^4 = 2^{(7-3)} = 16$ code words.
- The parity check matrix H of order k × n can be partitioned into two submatrices Q and I_k as follows:

$$H = (Q \mid I_k) \quad \ldots (8.6)$$

where I_k is a k × k identity matrix and Q is any arbitrary k × m matrix chosen in such a way that H generates a single error correcting code (described later on). We will now show that the matrix H always defines a group code.

Theorem :

Let H be a parity check matrix which consists of k rows and n columns. Then the set of words $x = (x_1, x_2, ..., x_n)$ which belong to the following set

$$C = \{x : x H^t = 0 \pmod 2\}$$ is a group code under the operation ⊕ (addition modulo 2), where H^t is the transpose of the matrix H.

Proof:

We know that C is group code if it is a group under the operation ⊕ (addition modulo 2).

Let x, y, ∈ C ⇒ $x \cdot H^t = 0$ and $y \cdot H^t = 0$.

Consider $(x \oplus y) \cdot H^t = (x \cdot H^t) \oplus (y \cdot H^t) = 0 \Rightarrow (x \oplus y) \in C$.

Hence C is closed under the operation ⊕.

For associativity,

$(x \oplus y) \oplus z = (x_1 \oplus y_1, x_2 \oplus y_2, \ldots x_n \oplus y_n) \oplus (z_1, z_2, \ldots z_n)$

$= (x_1 \oplus y_1 \oplus z_1, x_2 \oplus y_2 \oplus z_2 \ldots x_n \oplus y_n \oplus z_n)$

and $x \oplus (y \oplus z) = x \oplus (y_1 \oplus z_1, y_2 \oplus z_2 \ldots\ldots y_n \oplus z_n)$

$= (x_1 \oplus y_1 \oplus z_1, x_2 \oplus y_2 \oplus z_2 \ldots\ldots x_n \oplus y_n \oplus z_n)$

Hence $x \oplus (y \oplus z) = (x \oplus y) \oplus z$.

Observe that $0 \cdot H^t = 0$.

Hence 0 ∈ C.

Also x ⊕ 0 = x.

Therefore, identity element is 0 ∈ C. Lastly,

$x \oplus x = (x_1 \oplus x_1, x_2 \oplus x_2 \ldots\ldots x_n \oplus x_n)$

$= (0, 0 \ldots\ldots 0)$

Hence, every element in C is its own inverse.

From above, we conclude that (C, ⊕) is a group and hence a group code. Also, since C ⊆ S_n, therefore (C, ⊕) is a subgroup of $(S_n, \oplus)$. It means that **not all** the words of length n are code words. Only some of them belong to C.

The above theorem indicates that any solution of $x \cdot H^t = 0$ in which $x = (x_1, x_2, \ldots x_n)$ is a code word generated by H. We now give the statement of the theorem without any proof which enables us to determine the minimum weight and hence the minimum distance of a group code.

Theorem: The parity check matrix H generates a code word of weight q iff there exists a set of q columns of H such that their k-tuple sum is zero.

With the help we can determine the error detecting and error correcting capability of the code. That the minimum weight of a code generated by H is simply the minimum number of columns of H that have a zero sum. Since the minimum weight is equal to the minimum distance in a code, the number of errors detected and corrected can be found out . As an example in the following parity check matrix H, where

$$H = \begin{pmatrix} 1\,1\,0\,1\,0\,0 \\ 1\,0\,1\,0\,1\,0 \\ 1\,1\,1\,0\,0\,1 \end{pmatrix} \quad \ldots (8.7)$$

The sum of columns

$$h_1 = \begin{pmatrix}1\\1\\1\end{pmatrix},\ h_2 = \begin{pmatrix}1\\0\\1\end{pmatrix}$$

and $$h_4 = \begin{pmatrix}0\\1\\0\end{pmatrix} \text{ is } \begin{pmatrix}1\\1\\1\end{pmatrix} \oplus \begin{pmatrix}1\\0\\1\end{pmatrix} \oplus \begin{pmatrix}0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix}$$

That is the minimum number of columns that have zero sum is 3. Hence, the minimum weight of the code is 3 and thus, the minimum distance is 3. Therefore, according to, the code can detect 2 or less errors and correct only single error. Furthermore, the matrix H of order 3 × 6 will generate the code words x of length 6, where $x = (x_1\ x_2\ x_3\ x_4\ x_5\ x_6)$ in which the last 3 digits, namely x_4, x_5 and x_6 are parity checks and the remaining 3 digits x_1, x_2 and x_3 are information bits. According to the theorem 8.13.4 the code words generated are the solutions of the equation $x \cdot H^t = 0$ (mod 2).

$$\text{or} \quad (x_1\ x_2\ x_3\ x_4\ x_5\ x_6)\begin{pmatrix}1&1&1\\1&0&1\\0&1&1\\1&0&0\\0&1&0\\0&0&1\end{pmatrix} = (0\ 0\ 0)$$

This system reduces to the following three equations:

$$\begin{aligned} x_1 + x_2 + x_4 &= 0\\ x_1 + x_3 + x_5 &= 0\\ x_1 + x_2 + x_3 + x_6 &= 0\\ \Rightarrow \quad x_4 &= -(x_1 + x_2)\\ x_5 &= -(x_1 + x_3)\\ x_6 &= -(x_1 + x_2 + x_3) \end{aligned}$$

As $(-1) \equiv 1 \pmod 2$, the above equations become

$$\left.\begin{aligned} x_4 &= x_1 + x_2\\ x_5 &= x_1 + x_3\\ x_6 &= x_1 + x_2 + x_3 \end{aligned}\right\} \quad \ldots (8.8)$$

By giving possible values 0 or 1 to information digits x_1, x_2 and x_3, we can calculate the values of parity check bits x_4, x_5 and x_6 by using equations in 8.8 and thus, we can determine all possible code words generated by H in 8.8. There are all together $2^3 = 8$ code words generated by H. These code words are given in the following table:

x_1	x_2	x_3	x_4	x_5	x_6
0	0	0	0	0	0
0	0	1	0	1	1
0	1	0	1	0	1
0	1	1	1	1	0
1	0	0	1	1	1
1	0	1	1	0	0
1	1	0	0	1	0
1	1	1	0	0	1

Table for single error correcting code with m = 3, n = 3.

Thus, the single error correcting code generated by H is C = {(000000), (001011), (010101), (011110), (100111), (101100), (110010), (111001)}.

In short, the encoding procedure is described as follows:

For the parity check matrix H, of order k × n, the length of the code words generated will be n and the number of parity check bits will be k. The information digits will be m = (n – k). The number of code words generated is $2^m = 2^{n-k}$. Following steps are involved in generating these code words:

Step 1: Find the system of equations from $x \cdot H^t = 0$, where H^t denotes the transpose of the parity check matrix H.

Step 2: Find the values of parity check bits in terms of information digits from the equation obtain in the step 1.

Step 3: Give value 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 detected 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. The number of errors detected and corrected them can be found out.

8.14.3 Decoding

- For group codes, there is an efficient way to determine the transmitted word corresponding to a received word according to the minimum distance decoding criteria. Basic group theory is involved in this decoding process.
- Let (C, ⊕) be a group code. Suppose the code words transmitted contain n binary digits in which the first m digits contain the information part and the last k digits

are parity check bits. Let $(S_n, \oplus)$ be the set of all n tuples, where (C, ⊕) is a subgroup of $(S_n, \oplus)$. Suppose the code word $x \in C$ being transmitted through the noisy channel and the received word is y. Let e be the error in the received word y, where e consists of 1s in digit position in which an error occurs.

Then $x \oplus e = y$, where $y \in S_n$.

- Since the operation ⊕ is addition modulo 2, therefore, $x = e \oplus y$. This shows that the transmitted code word x is closed to y in terms of Hamming distance i.e. the error e should be of least weight.
- To determine the error with the least weight, we use the concept of cosets of the subgroup C of S_n.
- We know that the set of all left cosets (or right cosets) of C in S_n forms a partition in S_n. Consider the element $y \in S_n$. Clearly, y is in the left coset $y \oplus C$. Among all the elements of $y \oplus C$, we can determine the element 'a' with the least weight. Such an element is called a **Coset Leader**. Thus for each coset, we have a coset leader. For the coset C itself, 0 is the coset leader. Since C has 2^m elements, the number of cosets will be $r = 2^{n-m}$. Hence all together, the coset leaders are 0, a_1, a_2 ..... a_{r-1}.
- If a_1 is a coset leader, then the elements of the coset $a_1 \oplus C$ are given $a_1 \oplus x$, where $x \in C$. Furthermore, the element of C which is closed to $a_1 \oplus x$ is x. Thus, if the received word is $a_1 \oplus x$ then, the transmitted code word is x. The steps of constructing a decoding table will now be described.

Step 1: List the code words of C, starting with 0 as the first elements.

Step 2: Choose any word $a_1 \in S_n$ not in the first row of minimum weight.

List the coset $a_1 \oplus C$ as the second row by putting a_1 under 0 and $a_1 \oplus x$ under x for each $x \in C$.

Step 3: From these words of S_n not in the first and second row, choose a_2 of minimum weight and list the coset $a_2 \oplus C$ as in step 2 to get the third row.

Step 4: Continue in this way until all the cosets are listed and every element of S_n appears exactly once.

The decoding table has the form

0	X	x'	x"	.....
a_1	$a_1 \oplus x$	$a_1 \oplus x'$	$a_1 \oplus x"$	.....
a_2	$a_2 \oplus x$	$a_2 \oplus x'$	$a_2 \oplus x"$	.....
.	.	.	.	.....
.	.	.	.	.....
.	.	.	.	.....

In this table, the left most column denotes the coset leader and the top row denotes the code words generated. A received word 'y' can be decoded by first finding y in a row of the decoding table. Suppose y is in $(i + 1)^{th}$ row of the decoding table. Then the decoded word x is given by

$$x = a_i \oplus y$$

where a_i is the coset leader of $(i + 1)^{th}$ row. Also if no error has occurred in transmission, then the coset leader will be 0. For example, consider the matrix H in equation 8.16.7. The single error correcting code of length n = 6 with m = 3 generated by H is given by C = {(000000), (001011), (010101), (011110), (100111), (101100), (110010), (111001)} which is described earlier. The decoding table for this code is given in the following table.

000000	001011	010101	011110	100111	101100	110010	111001
100000	101011	110101	111110	000111	001100	010010	011001
010000	011011	000101	001110	110111	111100	100010	101001
001000	000011	011101	010110	101111	100100	111010	110001
000100	001111	010001	011010	100011	101000	110110	111101
000010	001001	010111	011100	100101	101110	110000	111011
000001	001010	010100	011111	100110	101101	110011	111000
000110	001101	010011	011000	100001	101010	110100	111111

Decoding Table

Now suppose, the received word is 001100 then, the transmitted word will be 101100. If 111000 is received then the word transmitted is 111001.

SOLVED EXAMPLES

Example 1: *Find the Hamming distances between the code words of C = {(0000), (0101), (1011), (0111)}.*

Solution: Let x = (0000), y = (0101), z = (1011) and t = (0111). The Hamming distance between the code words is the number of places in which they are different. Thus, the distances between x, y, z and t are

$$d(x, y) = 2,\ d(x, z) = 3,\ d(x, t) = 3$$

$$d(y, z) = 3,\ d(y, t) = 1,\ d(z, t) = 2$$

Example 2: *Given the parity check matrix*

$$H = \begin{pmatrix}1&1&0&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{pmatrix}$$

Find the minimum distance of the code generated by H. How many errors it can detect and correct ?

Solution: Consider the columns $h_1 = \begin{pmatrix}1\\0\\1\end{pmatrix}$, $h_2 = \begin{pmatrix}1\\1\\0\end{pmatrix}$ and $h_3 = \begin{pmatrix}0\\1\\1\end{pmatrix}$ of H.

The sum of these three columns is $\begin{pmatrix}1\\0\\1\end{pmatrix} \oplus \begin{pmatrix}1\\1\\0\end{pmatrix} \oplus \begin{pmatrix}0\\1\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix}$.

Hence, the minimum weight of the code is 3 which is equal to its minimum distance. Now, the code can detect k errors or less if its minimum distance is k + 1. Therefore, the code generated by H can detect 2 errors or less. Also it can correct k errors if the minimum distance is 2k + 1. In this case, the code can correct only single error. Therefore it is a single error correcting code.

Example 3: *Find the number of code words generated by the parity check matrix H . Also find all the code words generated.*

Solution: The parity check matrix

$$H = \begin{pmatrix}1&1&0&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{pmatrix}$$

It is of order 3 x 6. Hence, the length of the code words is 6 in which last 3 digits are parity check bits. The information digits are 6 – 3 = 3. The matrix H will generate $2^3 = 8$ code words. They are the solutions of

$$x \cdot H^t = 0$$

$$\Rightarrow (x_1 x_2 x_3 x_4 x_5 x_6) \begin{pmatrix}1&0&1\\1&1&0\\0&1&1\\1&0&0\\0&1&0\\0&0&1\end{pmatrix} = (0\ 0\ 0)$$

or

$$x_1 + x_2 + + x_4 = 0$$
$$x_2 + x_3 + x_5 = 0$$
$$x_1 + + x_3 + x_6 = 0$$

$\Rightarrow$

$$x_4 = x_1 + x_2$$
$$x_5 = x_2 + x_3$$
$$x_6 = x_1 + + x_3$$

By giving different combinations of 0 and 1, we get the following code words:

x_1	x_2	x_3	x_4	x_5	x_6
0	0	0	0	0	0
0	0	1	0	1	1
0	1	0	1	1	0
0	1	1	1	0	1
1	0	0	1	0	1
1	0	1	1	1	0
1	1	0	0	1	1
1	1	1	0	0	0

Hence the code C ={(000000), (001011), (010110), (011101), (100101), (101110), (110011), (111000)}.

Example 4: *Suppose the code C is given by C = {(0000), (0011), (1101), (1110)} in which the parity check bits k = 2. What is the transmitted code word if the received word is 1001 ?*

Solution: Here, the code C contains the words of length 4 in which 2 digits are parity checks. Hence the remaining m = 4 – 2 = 2 digits are information digits. Therefore, the number of cosets in the decoding table will be $2^2 = 4$. They are listed below:

0000	0011	1101	1110
1000	1011	0101	0110
0100	0111	1001	1010
0010	0001	1111	1100

The received word 1001 will be decoded as 1101.

Example 5: *Find the minimum distance of an encoding function e: $B^2 \rightarrow B^5$ given as*

e (0, 0) = 00000
e (01) = 10011
e (10) = 01110
e (11) = 11111

Solution: As we know, the distance d (x, y) between two code words x and y is the number of places for which all x_i and y_i are different.

$\therefore$ d (e (00), e (01) = 3
d (e (00), e (1, 0)) = 3
d (e (0, 0), e (11)) = 5
d (e (01), e (1, 0)) = 4
d (e (01), e (11)) = 2
d (e (10), e (11)) = 2

The minimum distance among all the distance is 2. Hence, the minimum distance of an encoding function is 2.

EXERCISE - 8.2

1. Explain the functions of encoder and decoder.
2. What is a group code ?
3. Define the weight and Hamming distance of the code. Also write the properties of Hamming distance.
4. Describe even parity checks and odd parity checks.
5. Explain Hamming codes.
6. Prove that the solutions of the equation $x \cdot Ht = 0$ (mod 2) form a group code under the operation $\oplus$ (addition modulo 2).
7. What is the relation between the minimum weight and minimum distance of a code ? How can you find the minimum weight of code generated by a k x n parity check matrix H ?
8. Write the code words generated by H,
   where, $H = \begin{pmatrix}1&0&1&1&1&0&0\\1&1&1&0&0&1&0\\0&1&1&1&0&0&1\end{pmatrix}$
   If the received word is (0101000), what is the transmitted word ?
9. Find the minimum distance of an encoding function e: B2 $\rightarrow$ B5 given as:
   e (00) = 00000
   e (01) = 10011
   e (10) = 01110
   e (11) = 11111

8.14.4 Polynomial Rings and Cyclic Codes

Let (R, +, ·) be a ring and let x denote an indeterminate, a formal symbol which is not an element of R. We shall now describe the algebraic structure (R [x], +, •), generated by (R, +, •) and x.

An element f (x) $\in$ R [x] is of the form $a_0 + a_1 x + \ldots + a_n x^n$, where $a_i \in R$, $0 \le i \le n$.

Note that x^i actually denotes $x \cdot x \cdot \ldots \cdot x$ (i-times) and $a_i x^i$ means $a_i \cdot x^i$. For convenience of writing, we usually drop the multiplication symbol.

The element f (x) is called a polynomial and hence R [x] is the set of all polynomials with coefficients in R. If $a_n \neq 0$, a_n is called as the leading coefficient of f (x) and then f (x) is said to be of degree n. The term a_0 (coefficient of x^0) is called as the constant term of f (x).

If $g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_m x^m$ is also a polynomial in x over R, then f (x) = g (x) if m = n and $a_i = b_i$, $\forall\ 0 \le i \le n$.

It is an easy matter to show that (R[x], + , .) is closed under + and •.

Suppose, $f(x) = a_0 + a_1 x + \ldots + a_m x^m$

and $g(x) = b_0 + b_1 x + \ldots + b_n x^n$

Let n $\ge$ m. Then,

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1) x + \ldots + (a_m + b_m) x^m + b_{m+1} x^{m+1} + \ldots + b_n x^n$$

and $f(x)\, g(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_p x^p$

where, $c_i = (a_0 b_i + a_1 b_{i-1} + \ldots + a_i b_0)$

and $p = m + n$

The ring properties of R [x] are basically inherited from R. Hence it is just a matter of routine to verify the associative and distributive laws and as such left to the reader.

The ring R [x] is called as the ring of polynomials over R.

Examples:

1. Over the ring (Z_6, +, .) the expression $5x^2 + 3x - 2$ is a polynomial of degree 2 with leading coefficient 5. Since [4] = [–2] in Z_6, this polynomial can also be written as $5x^2 + 2x + 4$.
2. Consider the polynomials $1 + 2x + x^2$ and $2 - x + 2x^2$ in Z_3 [x]. Then their product is $2x^4 + 3x^3 + 2x^2 + 3x + 2$. Since [3] = [0], it is same as $2x^4 + 2x^2 + 2$. Sum of the polynomials is $3 + x + 3x^2 = x$.
3. Consider $f(x) = x^2 + 3x + 2 \in Z_6$ [x]
   Then f (1) = 1 + 3 + 2 = 6 = 0
   f (2) = 4 + 6 + 2 = 12 = 0
   f (4) = 16 + 12 + 2 = 30 = 0
   f (5) = 25 + 15 + 2 = 42 = 0

Consequently f (x) has 4 roots.

Note that in this case degree of the polynomial and the number of roots are not correlated a departure from what we are accustomed to. This surprising contradiction is due to the fact that the ring Z_6 has zero divisors.

In view of the last example above, we are naturally interested only in those polynomial rings, where a polynomial of degree n has atmost n roots. This is true in the case of a polynomial ring F[x] where F is a field.

We now state the Division Algorithm for a polynomial ring over a field.

Division Algorithm: Let f (x), g (x) ∈ F [x], with f (x) ≠ 0. Then there exist unique polynomials q (x), r (x) ∈ F [x] such that

$$g(x) = q(x) f(x) + r(x)$$

where r (x) = 0 or degree r (x) < degree f (x)

Examples:

1. Let f (x) = $3x^2 + 4x + 2$ and g (x) = $4x^4 + 3x^3 + 2x^2 + 3x + 2$ be polynomials in Z_5 [x]. We apply long division.

$$\begin{array}{r} 3x^2 + 2x + 1 \\ 3x^2 + 4x + 2 \overline{)\ 4x^4 + 3x^3 + 2x^2 + 3x + 2} \\ 4x^4 + 2x^3 + x^2 \\ \hline x^3 + x^2 + 3x + 2 \\ x^3 + 3x^2 + 4x \\ \hline 3x^2 + 4x + 2 \\ 3x^2 + 4x + 2 \\ \hline 0 \end{array}$$

Here r (x) = 0 and g (x) = $(3x^2 + 4x + 2)(3x^2 + 2x + 1)$

2. Consider f (x) = $x^2 + 3x + 1$, g (x) = $2x^4 + x^3 + 3x + 4$ in Z_5 [x] and apply long division of g (x) by f (x).

$$\begin{array}{r} 2x^2 + 3 \\ x^2 + 3x + 1 \overline{)\ 2x^4 + x^3 + 3x + 4} \\ 2x^4 + x^3 + 2x^2 \\ \hline 3x^2 + 3x + 4 \\ 3x^2 + 4x + 3 \\ \hline 4x + 1 \end{array}$$

$\therefore$ g (x) = $(2x^2 + 3)(x^2 + 3x + 1) + 4x + 1$

In the discussion that now follows, the concept of division algorithm will be very much needed.

Let (F, +, •) be a field and let F_n [x] denote the set of polynomials of degree **strictly less than n** in F (x). Let p (x) be a given polynomial of degree n in F [x].

Define the two binary operations ⊕ and x on F_n [x] as follows:

For f (x), g (x) ∈ F_n [x], define

f (x) ⊕ g (x) = f (x) + g (x) (as in F (x))

f (x) x g (x) = the remainder obtained after dividing f(x) · g(x) by p(x)

Under the two operations defined above the algebraic structure (F_n [x], ⊕, x) becomes a ring.

This ring is called as the ring of polynomials modulo p (x).

For example, if F = Z_2 is field of integers modulo 2, there will be in all 2 × 2 polynomials in F_2 [x] viz. 0, 1, x, H_x.

On the other hand, if F = Z_3, then any polynomial in F_2 [x] being of the type $a_0 + a_1 x$, where a_i = 0, 1, or 2, there will be totally 3 × 3 = 9 polynomials.

SOLVED EXAMPLES

Examples 1: *Let F = Z_2. Construct the ring of polynomials modulo 1 + x + x^2.*

Solution: Here n = 2 and hence we consider F_2 [x], whose elements are 0, 1, x, 1 + x.

We give below the tables for both the operations.

⊕	0	1	X	1 + x
0	0	1	X	1 + x
1	1	0	1 + x	x
x	x	1 + x	0	1
1 + x	1 + x	X	1	0

For multiplication, consider x·x = x^2. We divide x^2 by 1 + x + x^2 and find the remainder, which is 1 + x. In other words,

$$x^2 = 1(1 + x + x^2) + (1 + x)$$

Similarly, $x(1 + x) = x^2 + x = 1(x^2 + x + 1) + 1$

$$1 + x^2 = 1(1 + x + x^2) + x$$

Hence the table is as follows:

⊙	0	1	X	1 + x
0	0	0	0	0
1	0	1	X	1 + x
x	0	x	1 + x	1
1 + x	0	1 + x	1	x

Example 2: *Let F = Z_3, the field of integers modulo 3. Construct the ring of polynomials modulo 2 + 2x + x^2.*

Solution: The elements of F_2 [x] are 0, 1, 2, x, 2x, 1 + x, 2 + x, 1 + 2x, 2 + 2x, in all 9 elements. As in the previous example we have to consider addition and multiplication. For instance,

$(1 + x) \oplus (2 + x) = 3 + 2x = 2x$

$(2 + x) \oplus (1 + 2x) = 3 + 3x = 0$

Likewise, addition of other elements will be obtained.

For product, consider first the ordinary product.

For example,

$(1 + x)(1 + 2x) = 1 + 3x + 2x^2$

$= 1 + 2x^2$

We have to divide $1 + 2x^2$ by the given polynomial $2 + 2x + x^2$ and take the remainder.

Now,

$$\begin{array}{r} 2 \\ 2 + 2x + x^2 \overline{)\ 1 + 2x^2} \\ 4 + 4x + 2x^2 \\ \hline 0 + 2x \end{array}$$

$\therefore (1 + x) \cdot (1 + 2x) = 2x$

Similarly $(2 + x)^2 = 4 + 4x + x^2 = 1 + x + x^2$

Now,

$$\begin{array}{r} 1 \\ 2 + 2x + x^2 \overline{)\ 1 + x + x^2} \\ 2 + 2x + x^2 \\ \hline 2 + 2x \end{array}$$

Hence, $(2 + x) \cdot (2 + x) = 2(1 + x)$

In the same manner we can show the addition and multiplication operations of other elements.

The polynomial rings discussed above enable us to construct a class of codes known as **Cyclic** codes.

Recall that a block code is a set of code words of the same length.

A block code of length n is called a cyclic code if for every code word $a_0 a_1 a_2 \ldots a_{n-1}$, the sequence $a_{n-1} a_0 a_1 a_2 \ldots a_{n-2}$ is also a code word. For example,

C = {0000, 11001, 11100, 01110, 00111, 10011}

is a cyclic code of length 4.

Let us now see how to generate cyclic codes.

Let (F, +, •) be the field of integers modulo 2.

For every binary sequence $a_0 a_1 \ldots a_{n-1}$, we consider the associated polynomial

$a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} \in F[x]$

Let p (x) be the polynomial $1 + x^n$ and consider the ring (F_n [x], ⊕, ⊙), ring of polynomials modulo p (x). Let I be any ideal in (F_n [x], ⊕, ⊙). Then the polynomials in I constitute a cyclic code. This is proved as follows:

Let $f(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$

be any element in I. Then by definition of an ideal x ⊙ f (x) should also be an element in I. Now,

x ⊙ f (x) = remainder of $\dfrac{x \cdot (a_0 + a_1 x + a_2 x^2 + \equiv + a_{n-1} x^{n-1})}{1 + x^n}$

= remainder of $\dfrac{(a_0 x + a_1 x^2 + \ldots a_{n-1} x^n)}{1 + x^n}$

$= a_{n-1} + a_0 x + a_1 x^2 + \ldots + a_{n-2} x^{n-1}$

This corresponds to the code word $a_{n-1}\, a_0\, a_1 \ldots a_{n-2}$.

Thus the polynomials in I generate a cyclic code.

Conversely let I denote a set of polynomials corresponding to the code words in a cyclic code. Hence if $b_0 b_1 b_2 \ldots b_{n-1}$ is a code word, then $b_0 + b_1 x + \ldots + b_{n-1} x^{n-1} \in I$.

Further as shown above $x \odot (b_0 + b_1 x + \ldots + b_{n-1} x^{n-1})$

$= b_{n-1} + b_0 x + \ldots + b_{n-2} x^{n-1}$

which corresponds to the code word $b_{n-1}\, b_0 \ldots b_{n-2}$.

Hence by definition of I,

$x \odot (b_0 + b_1 x + \ldots + b_{n-1} x^{n-1}) \in I$

Similarly for any i, $x^i \odot (b_0 + b_1 x + \ldots + b_{n-1} x^{n-1}) \in I$.

It is also clear that (I, ⊕) is an abelian group. Hence it is proved that I is an ideal in (F_2 [x], ⊕, ⊙).

Example 3: *Let F = Z_2 and p (x) = 1 + x^2*

Consider the ring of polynomials modulo p (x) viz. (F_2 [x], ⊕, ⊙).

The elements of F_2 [x] are 0, 1, x, 1 + x.

Consider the cyclic code {00, 11}.

The ideal corresponding to the cyclic code is {0 + 0x, 1 + x}.

Note the operations

x ⊙ (1 + x) = 1 + x

(1 + x) ⊙ (1 + x) = 0

Example 4: *Assuming f(t) has an integer root, find the roots of f(t) = $t^3 - t^2 - 11t - 10$.*

Solution: Product of roots = 10; hence probable integer roots are factors of 10 viz. ± 1, ± 2, ± 5, ± 10.

By synthetic division, t = − 2 is a root of f(t). Hence, by factorization,

$f(t) = (t + 2)(t^2 - 3t - 5)$

Therefore, the other two roots are $\dfrac{3 \pm \sqrt{29}}{2}$.

Example 5: *Find the roots of f(t) = $2t^4 - 11t^3 + 33t^2 - 19t - 65$, given that t = 2 + 3i is one root.*

Solution: If t = 2 + 3i is one root, its conjugate 2 − 3i is also a root of f(t). Hence, the quadratic polynomial

$g(t) = t^2 - (2 + 3i + 2 - 3i)\, t + (2 + 3i)(2 - 3i)$

$= t^2 - 4t + 13$ is a factor of f(t).

Hence, by division, we can write

$f(t) = g(t)(2t^2 - 3t - 5)$

Solving

$2t^2 - 3t - 5 = 0$, we obtain

$t = \dfrac{3 \pm \sqrt{9 + 40}}{2}$, i.e. t = − 2 or 5

Hence, roots of f(t) are 2 + 3i, 2 − 3i, −2 and 5.

EXERCISE - 8.3

1. Find the quotient and remainder when
   (i) $x^3 + x^2 + 1$ is divided by $x^2 + x + 1$ in $Z_2[x]$.
   (ii) $x^5 + x^4 + 2x^3 + x^2 + 4x + 2$ is divided by $x^2 + 2x + 3$ in $Z_5[x]$.
2. Let F be a field. Show that the polynomial f (x) has an inverse in F (x) if and only if f (x) is a non-zero constant polynomial.
3. Compute the sum and product of the polynomials in $Z_5[x]$.
   (i) $2x^3 + 4x^2 + x + 3$ and $x^2 + 3x + 2$
   (ii) $x^4 + 2x^3 + x^2 + 1$ and $2x^3 + 4x^2 + 3x + 1$
4. Show that in $Z_7[x]$, $(x + 1)^7 = x^7 + 1$
5. Let $F = Z_2$. Construct the ring of polynomials modulo $x^3 + 1$, $(F_3[x], \oplus, x)$. Determine all ideals in $F_3[x]$ and find the corresponding cyclic codes.
6. Suppose $f(t) = t^3 - 2t^2 - 6t - 3$, where f(t) has integer roots. Find the roots of f(t). **(May 05)**

8.15 GALOIS THEORY

The general problem of solvability of polynomial equations led to the development of Galois Theory. It is well known from the fundamental theorem of algebra that a polynomial of degree n has n roots. The question was whether these roots could be determined by some suitable formula, obtained through operations of addition, multiplication, division, subtraction and taking n^{th} roots (radicals). While it was possible for linear, quadratic, cubic and biquadratic (n = 1, 2, 3, 4), polynomials, the complete solution continued to baffle the mathematicians for nearly two hundred years, from sixteenth to eighteenth centuries. Then in 1830, a young French Mathematician Evariste Galois (1811-1832) came up with a remarkable theory, which proved that all polynomials of degree $n \geq 5$ cannot be solved by radicals. This theory, which connects field theory and graph theory, came to be called as Galois Theory.

8.15.1 Preliminary Concepts

Recall the definition of a field.

Definition : Let F be a commutative ring with unit element 1. If for every element $a \in F$, $a \neq 0$, there exists $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$, then F is a field.

Standard Examples :

1. **Q :** Field of rational numbers, **R :** Field of real numbers, **C :** Field of complex numbers; these are also called **Number Fields.**
2. $\mathbf{Z_p}$ **:** The ring of integers modulo p, where p is a prime number, is a **finite** field (containing only finitely many elements).

Subfield :

Definition : Let K be a field. A subfield is a sub-ring $F \subseteq K$ such that if $x \in F$, $x \neq 0$, then $x^{-1} \in F$.

Examples :

1. Q is a subfield of **R**.
2. $Q[\sqrt{2}] \cdot \{a + b\sqrt{2} / a, b \in Q\}$ is a **Field Containing** Q as a **subfield.**

Extension Field :

Definition : Let F be a field. A field K which contains F as a subfield is called as an **Extension Field** of F.

Algebraic Element :

Definition : Let K be an extension of a field F.

Then an element $\alpha \in K$ is said to be **Algebraic Over F** if it is the root of some non-zero polynomial with coefficients in F.

Since the coefficients are from a field, we may assume that the leading coefficient of the polynomial is 1, i.e. the polynomial is **Monic**, i.e. of the type

$$x^n + a_{n-1} x^{n-2} + \ldots + a_1 x + a_0, \; a_i \in F$$

Example 1 : Consider the field extension **R** over **Q**. Then $\sqrt{2} \in \mathbf{R}$ is algebraic over Q, since it satisfies the equation $x^2 - 2 = 0$.

Adjoining $\sqrt{2}$ to Q, we get the field extension $Q(\sqrt{2})$ over Q.

If an element α is not algebraic over F, it is called **Transcendental**.

Example 2 : The real number $\sqrt{2} + \sqrt{3}$ is algebraic over $Q(\sqrt{2})$ as it is a root the polynomial.

$$x^2 - 2\sqrt{2}\, x - 1 = 0$$

Adjoining the number $\sqrt{2} + \sqrt{3}$ to $Q(\sqrt{2})$, the obtain we field extension $Q(\sqrt{2}, \sqrt{3})$ over $Q(\sqrt{2})$, i.e. we have a **Tower** or chain of field extensions

$$Q \subseteq Q(\sqrt{2}) \subseteq Q(\sqrt{2}, \sqrt{3})$$

If K is an extension field of F, F(α) is the **smallest field** containing F, which is **generated by an element** $\alpha \in K$.

Irreducible Polynomial :

Consider an extension field K over F. Assume that an element $\alpha \in K$ is algebraic over F. Let f(x) be the monic polynomial of **lowest** degree having α as a root. This polynomial is then called as the irreducible polynomial for α over F.

Examples :

1. The polynomial $x^2 - 2$ is irreducible for the element $\sqrt{2}$ over Q.
2. Let F = Q(i) and let α be the complex number $\sqrt{i} = \frac{1}{2}\sqrt{2}\,(1 + i)$. The irreducible polynomial for α over Q is $x^4 + 1$, but is reducible over F, since it can be factorized as $(x^2 + i)(x^2 - i)$. The irreducible polynomial for α over F is $x^2 - i$.
   Degree of a field extension.

Definition : Let $\alpha \in K$ be algebraic over F.

Then the **Degree** of the field extension F(α) over F is the degree of the irreducible polynomial of α over F. It is denoted as [F(α) : F].

Examples :

1. $[Q(\sqrt{2}) : Q] = 2$.
2. $[Q(\sqrt{i}) : Q] = 4$, whereas $[Q(\sqrt{i}) : Q(i)] = 2$.

Note that $[Q(\sqrt{i}) : Q] = [Q(\sqrt{i}) : Q(i)]\,[Q(i) : Q]$

Another interpretation of degree of a field extension

An extension field K over a field F is a vector space over F. The dimension of K as a F vector space is called the degree of the extension. If K is a finite dimensional vector space over F, then K over F is called a finite extension. If K = F(α), where α is algebraic over F, of degree n, then every element of K can be written as a polynomial expression $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{n-1}\alpha^{n-1}$, i.e. the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ forms a basis for K over F.

An important property (without proof).

Theorem:

If $F \subset K \subset L$ are field, then

$$[L : F] = [L : K]\,[K : F]$$

Example :

1. Let $\alpha = \sqrt[3]{5}$, $\beta = 1 + \sqrt{2}$. Let $L = Q(\alpha, \beta)$. Then $[L : Q] = 6$.
   $[L : Q(\alpha)] = 2$ and $[Q(\alpha) : Q] = 3$
   Hence it is verified that :
   $[L : Q] = [L : Q(\alpha)]\,[Q(\alpha) : Q]$

8.15.2 Galois Group and Galois Extension

The development of Galois theory was based on an interesting discovery that the roots of a polynomial can be associated with a group of permutations. Let us see how this is done, by considering certain extensions of degree 2.

Consider an extension K over F of degree 2, generated by an element $\alpha \in K$, which is not in F. Let f(x) be the irreducible monic polynomial of degree 2, satisfied by α, let $f(x) = x^2 + bx + c$. if β is the second root of f(x), then we know that $\alpha + \beta = -b$ and $\alpha\beta = c$. We observe that on interchanging α and β in the above equations, the equations will still be valid. This is due to the equation being symmetrical in α and β. Consider the following permutations on α and β :

P_0 = identity permutation

and $P_1 = \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}$

Observe that :

$$P_1 \circ P_1 = \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \alpha & \beta \end{pmatrix} = P_0$$ Denote $P_1 \circ P_1$ by P_1^2,

we notice

that the set $\{P_0, P_1\}$ forms the group S_2.

S_2 is **a Cyclic Group** of order 2.

The permutation group infact defines an isomorphism :

$\sigma : F(\alpha) \to F(\beta)$ such that : $\sigma(\alpha) = \beta$

But since $\beta = -\alpha - c$, it belongs to F(α), and conversely α also is in F(β). Therefore,

F(α) = F(β). This infact shows that σ is an automorphism of F(α), which **Fixes** F, i.e. $\sigma(x) = x \forall\, x \in F$, σ is called a **F-Automorphism** of K = F(α). The group called as the automorphism group of K is called as the **Galois Group** (of order 2) and is denoted as G(K|F), where the notation K|F denotes the extension field K over F. The corresponding extension K|F is called as **Galois** extension of K over F.

We now formally define a Galois extension.

Definition : A finite field extension K|F is called a Galois extension if the order of the Galois group is equal to the degree of the extension.

Examples :

1. Consider Q the field of rational numbers. Let $\alpha = 1 + \sqrt{2}$ and let K = Q(α). The irreducible polynomial for α over Q is $x^2 - 2x - 1$. Let $\beta = 1 - \sqrt{2}$, the other root of the polynomial. Define the mapping.
   $\sigma : K \to K$ as
   $\sigma(a + b\alpha) = a + b\beta$, $a, b \in Q$
   It is clear that σ is an automorphism of K and since σ is identity on Q, it is called a Q-automorphism of K.
   The degree of the extension K|Q is 2 and the order of the automorphism group of K is also 2, as $\sigma^2 = 1$ (identity mapping under composition).
   Hence Q(α)/Q is a Galois extension with G(Q (α)/Q) = {1, σ}.
   In the next example, we will consider the permutation group to construct the galois group.

Example : Biquadratic Extension :

Consider the irreducible polynomial $f(x) = x^4 - 7x + 10$, over Q; roots are $\pm\sqrt{2}$ and $\pm\sqrt{5}$.

Let $\alpha = \sqrt{2}$, $\beta = -\sqrt{2}$, $\gamma = \sqrt{5}$, $\delta = -\sqrt{5}$.

The following are some of the equations involving then :

$$\alpha\beta + \gamma\delta = -7$$
$$\alpha\delta - \gamma\beta = 0$$
$$\alpha\beta\gamma\delta = 10$$

Consider the permutation group S_4 on the 4 symbols α, β, γ, δ. There are in all 24 permutations, out of which we will consider for our purpose the following 4 permutations :

1. The identity permutation :

$$\rho_0 = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \alpha & \beta & \gamma & \delta \end{pmatrix}$$

The above equations are preserved by this permutation since $\alpha \leftrightarrow \alpha, \beta \leftrightarrow \beta, \gamma \leftrightarrow \gamma, \delta \leftrightarrow \delta$.

2. $$\rho_1 = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \beta & \alpha & \delta & \gamma \end{pmatrix}$$

By this permutation α is interchanged with β, γ with δ. The equations are still valid as

$$\beta\alpha + \delta\gamma = -7$$
$$\beta\gamma - \delta\alpha = -\sqrt{10} - (-\sqrt{10}) = 0$$
$$\beta\alpha\delta\gamma = 10$$

3. $$\rho_2 = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \delta & \gamma & \beta & \alpha \end{pmatrix}$$

The equations are converted into the equations

$$\delta\gamma + \beta\alpha = -5 - 2 = -7$$
$$\delta\alpha - \beta\gamma = 0$$
$$\delta\gamma\beta\alpha = 10$$

which are still true.

4. $$\rho_3 = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \gamma & \delta & \alpha & \beta \end{pmatrix}$$

$$\gamma\delta + \alpha\beta = -2 - 5 = -7$$
$$\gamma\beta - \alpha\delta = -\sqrt{10} - (-\sqrt{10}) = 0$$
$$\phi\delta\alpha\beta = 10$$

Hence, we consider the above four permutations to form the Galois group of order 4.

Now note that :

$$\rho_1 \cdot \rho_2 = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \beta & \alpha & \delta & \gamma \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \delta & \gamma & \beta & \alpha \end{pmatrix} = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \gamma & \delta & \alpha & \beta \end{pmatrix} = \rho_3$$

$$\text{Also, } \rho_2 \cdot \rho_1 = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \delta & \gamma & \beta & \alpha \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \beta & \alpha & \delta & \gamma \end{pmatrix} = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \gamma & \delta & \alpha & \beta \end{pmatrix} = \rho_3$$

$$\text{Also } \rho_1^2 = \rho_1 \cdot \rho_1 = \rho_0 = \rho_2^2$$

These permutations in turn give rise to the following automorphism defined on the extension field $K = Q(\sqrt{2}, \sqrt{5})$ which fix the element of Q.

σ : $K \to K$
$\sqrt{2} \leftrightarrow -\sqrt{2}$
$\sqrt{5} \leftrightarrow -\sqrt{5}$

τ : $K \to K$
$\sqrt{2} \leftrightarrow -\sqrt{5}$
$-\sqrt{2} \leftrightarrow +\sqrt{5}$

$\sigma\tau$: $K \to K$ $(\sigma \cdot \tau = \tau \cdot \sigma)$
$\sqrt{2} \leftrightarrow \sqrt{5}$
$-\sqrt{2} \leftrightarrow -\sqrt{5}$

Hence, the Galois group G (K/Q) consists of the set $\{1, \sigma, \tau, \sigma\tau\}$, satisfying the conditions : $\sigma^2 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma$.

This is called as the Klein group of order 4.

The next example concerns a finite field.

Example : Consider the field Z_2. The polynomial $x^2 + x + 1$ is irreducible over Z_2. Let α be a root of the polynomial and consider the extension $Z_2(\alpha)$ over Z_2. The other root is $\beta = 1 + \alpha$. Hence, $Z_2(\alpha)$ is a field of 4 elements i.e. $\{0, 1, \alpha, 1 + \alpha\}$.

Consider the mapping $\sigma : Z_2(\alpha) \to Z_2(\alpha)$ such that $\sigma(\alpha) = 1 + \alpha$.

Clearly σ is a automorphism of $Z_2(\alpha)$, with $\sigma(0) = 0$, $\sigma(1) = 1$.

Hence, $Z_2(\alpha)/Z_2$ is a Galois extension with the Galois group being a cyclic group of order 2, generated by σ.

In the ensuing article we will discuss some important properties of finite fields.

8.15.3 Finite Fields

A finite field contains only finitely many elements. For any prime p, Z_p (or F_p) is one such field, it is called as **Prime Field**. It can be shown that a finite field contains one of the prime fields as a subfield. A finite field can be considered as a finite dimensional vector space over its prime subfield F_p. Let $[K : F_p] = n$. Then the number of elements in K will be p^n. It is usual to denote a field with q elements as F_q.

Fields with number of elements as 6, 10, 12, 14, 18, 20 ... **do not exist**.

Important properties of finite fields are stated in the form of a theorem, which is given below :

Theorem :

Let p be a prime and let $q = p^n$, with $n \geq 1$. Then

There exists a field of order q.

Any two fields of order q are isomorphic.

Let K be a field of order q; then the multiplicative group $K - \{0\}$ is a cyclic group of order $q - 1$.

The elements of K are roots of the polynomial $x^q - x$, which has distinct roots and factorizes into linear factors in K.

Every irreducible polynomial of degree n in $F_p[x]$ is a factor of $x^q - x$. The irreducible factors of $x^q - x$ in $F_p[x]$ are precisely the irreducible polynomials in $F_p[x]$ whose degree divides n.

A field K of order q contains a subfield of order p^k if and only if k divides n.

Note : K is said to be a **Splitting Field** for $x^q - x$ (property iv). Since the field was introduced by Galois, it is called as a Galois field and is also denoted as GF(q).

SOLVED EXAMPLES

Example 1 : Let p = 2 and n = 2. Consider the polynomial $x^4 - x = x(x - 1)(x^2 + x + 1)$. The polynomial $x^2 + x + 1$ is irreducible over Z_2 by properly (iii) If α is a root of the polynomial, the other root is $1 + \alpha$. The splitting field or the Galois field GF(4) is the field $Z_4(\alpha)$ which consists of the elements 0, 1, α, $1 + \alpha$.

Let p = 2, n = 3 $\therefore q = 2^3 = 8$.

The field F_8 has degree 3 over F_2 (or Z_2). Its elements are the eight roots of the polynomial.

$x^8 - x = x(x - 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ in $Z_2[x]$.

Both $x^3 + x + 1$ and $x^3 + x^2 + 1$ are irreducible polynomials of the same degree over Z_2. Hence, we can choose any one of them. Let us choose $x^3 + x + 1$. Let α^2 be a root of $x^3 + x + 1$.

Then, $F_8 = \{0, 1, \alpha, \alpha^2, 1 + \alpha, 1 + \alpha^2, \alpha + \alpha^2, 1 + \alpha + \alpha^2\}$

The corresponding Galois group consists of the automorphisms

$\rho_0 : x \to x$
$\rho_1 : x \to x^2$
$\rho_2 : x \to x^4$

It is noted that $\rho_1^2 = \rho_2$ and $\rho_1^3 = \rho_0$ as $\rho_1^3 : x \to x^8 = x$.

Example 2

Let p = 3, n = 2, $\therefore$ q = 9. Consider the polynomial

$$x^9 - x = x(x^8 - 1) = x(x^4 - 1)(x^4 + 1)$$

One of the irreducible factors is $x^2 + 1$.

Now, $x^4 + 1 = x^4 + 1 + 3 = x^4 + 4$
$= (x^2 + 2)^2 - 4x^2$
$= (x^2 - 2x + 2)(x^2 + 2x + 2)$
$= (x^2 + x + 2)(x^2 + 2x + 2)$ $(-2 = 1 \text{ in } F_9)$

Hence, we have two more irreducible factors $x^2 + x + 3$ and $x^2 + 2x + 2$.

1. Consider irreducible polynomial $f(x) = x^2 + 1$ and let α be a root of f(x). If we consider α as a generator for the non-zero multiplication group we obtain only 4 elements, since $\alpha^2 = 1$, $\alpha^3 = 2\alpha$, $\alpha^4 = 1$.
   Hence, we have to select some other non-zero element of F_9 which will give the required set of 8 elements.
   Consider $1 + \alpha \in F_9$.
   Now, $(1 + \alpha)^2 = 1 + 2\alpha + \alpha^2 = 2\alpha$
   $(1 + \alpha)^3 = 2\alpha + 1$, $(1 + \alpha)^4 = 2$, $(1 + \alpha)^5 = 2\alpha + 2$,
   $(1 + \alpha)^5 = \alpha$, $(1 + \alpha)^7 = \alpha + 2$, $(1 + \alpha)^8 = 1$.
   Hence, $1 + \alpha$ is the required generator for the cyclic group of order 8,
   i.e. $\{\alpha + 1, 2\alpha, 2\alpha + 1, 2, 2\alpha + 2, \alpha, \alpha + 2, 1\}$
2. However for the irreducible polynomial $x^2 + x + 2$, it is found that α, where α is a root of $x^2 + x + 2$ is a generator.
   There is no known method or procedure for finding the generator (primitive element) for the non-zero elements of K (which forms a multiplicative cyclic group of finite order). Even for small primes p, we can find one, only by trial and error.

Examples :

1. Consider the Galois field GF(7). We find that powers of 3 generate the non-zero elements. $3^0 = 1$, $3^1 = 3$, $3^2 = 9 \equiv 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$.Hence we obtain the set {1, 3, 2, 6, 4, 5, 1} which gives the multiplicative group,
2. For the Galois field GF(11), 2 is a generator for the non-zero elements. The powers of 2, in sequence, are 1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1.

POINTS TO REMEMBER

- An n-ary operation on a non-empty set A is a function $f : A^n \to A$, A^n being the product set of A.
- An algebraic system is an ordered pair (A, F) where
  1. A is a set of elements, called as the **Carrier** of the algebra.
  2. F is a finite set of m-ary operations on the carrier, m being a variable.
- A binary operation $\cdot$ on A is said to be **Commutative** if $a \cdot b = b \cdot a$, for all elements $a, b \in A$
- A binary operation $\cdot$ on A is said to be **Associative** if $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, for all elements, $a, b, c \in A$.
- A binary operation $\cdot$ on A is said to satisfy the **Idempotent** property if $a \cdot a = a$, for all $a \in A$.
- Let $(A, \cdot)$ be an algebraic system, with a binary operation $\cdot$ on A. Then $(A, \cdot)$ is called a **Semi Group** if $\cdot$ is associative, i.e.
  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, for all $a, b, c \in A$.
- An element e in $(A, \cdot)$ is called as **Left Identity** element if for each element $x \in A$, $e \cdot x = x$. is called a **Right** identity if $x \cdot e = x$, for all $x \in A$.
- An element e in a semigroup $(A, \cdot)$ is called an **Identity** element if $a \cdot e = e \cdot a = a$, for all $a \in A$, i.e. e is both a left identity and right identity. It is clear that e is unique.
- Let $(A, \cdot)$ be a monoid, and let B be a non-empty subset of A. Then $(B, \cdot)$ is called a **Sub Monoid** of $(A, \cdot)$ if
  1. B is closed under $\cdot$.
  2. The identity element $e \in B$.

- Let (A, $\cdot$) be a monoid with identity element e. Let B be a non-empty subset of A. Then the monoid generated by B, denoted by < B > is defined as follows:
  1. $e \in <B>$, and if $b \in B$, then b also is in < B >, that is $B \subseteq <B>$.
  2. < B > is closed under $\cdot$.
  3. The only elements of < B > are those obtained from steps (i) and (ii).
- A group (G, $\cdot$) is called an **Abelian** group if $a \cdot b = b \cdot a$, for all $a, b \in G$.
- Let (G, $\cdot$) be a group. The order of G is the cardinality of G, denoted by |G|.
- Let (G, $\cdot$) be a group. Let $a \in G$. The order of a is the **Smallest** positive integer n such that $a \cdot a \cdot \ldots \cdot a = a^n = e$. If no such value of n exists for a, then a is said to be of infinite order.
- A group (G, $\cdot$) is said to be a cyclic group if there exists an element $a \in G$ such that every element of G can be written as some power of a, viz a^k, for some integer k. By a^k, we mean $a \cdot a \cdot a \ldots \cdot a$ (k times). We then say that G is generated by a or a is a generator of G.
- Let H be a non-empty subset of a group G. Then H is said to be a **Sub Group** of (G, $\cdot$) if H is itself a group under $\cdot$.
- Let H be a subgroup of a group (G, $\cdot$). For $a \in G$, define

  $Ha = \{ h \cdot a \mid h \in H \}$. Then Ha is called a **Right Coset** of H in G.

  Similarly, $aH = \{ a \cdot h \mid h \in H \}$ is called a left coset of H in G. a is called as the representative element of the coset aH or Ha. If $a \in H$, then Ha = aH = H.
- A subgroup H of G is said to be a **Normal** subgroup of G if for every $a \in G$, aH = Ha.
- Let (G, $\cdot$) and (G', $\cdot'$) be two semigroups, then a function $\phi : (G, \cdot) \to (G', \cdot')$ is called a homomorphism of G and G' if for every $a, b \in G$, $\phi(a \cdot b) = \phi(a) \cdot' \phi(b)$. In particular if G and G' are groups, then ϕ is called a group homomorphism.
- Let $\phi: G \to G'$ be a homomorphism of semigroups (or groups). Then ϕ is called an **Isomorphism** if ϕ is one-one and onto (i.e. injective as well as surjective).
- If G' = G, then ϕ is called an automorphism.
- An algebraic structure (R, +, $\cdot$) is called a ring if
  1. (R, +) is an abelian group.
  2. Associativity of multiplication holds: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
  3. The left distributive law

     $a \cdot (b + c) = a \cdot b + a \cdot c$, and the right distributive law

     $(b + c) \cdot a = b \cdot a + c \cdot a$ are satisfied by + and $\cdot$.
- A ring R is said to be commutative ring if $a \cdot b = b \cdot a$, for all $a, b \in R$.
- A ring R is said to be a ring with **unit** element if there exists an element, denoted by the symbol 1 such that $a \cdot 1 = 1 \cdot a = a$, for all $a \in R$.
- A subset $R \subseteq S$, where $(S_1, +, \cdot)$ is a ring, is called a subring of S if (R, +, $\cdot$) is a ring with the operations + and $\cdot$ restricted to elements of R.
- Let (R, +, $\cdot$) and (S, $+'$, $\cdot'$) be rings. A mapping $\phi: R \to S$ is called a **Ring Homomorphism,** if for any $a, b \in R$.
  1. $\phi(a + b) = \phi(a) +' \phi(b)$
  2. $\phi(a \cdot b) = \phi(a) \cdot' \phi(b)$.

  If ϕ is one-one and onto, it is called as a ring **Isomorphism.** One can easily verify that $\phi(0) = 0'$ and $\phi(-a) = -\phi(a)$, for every $a \in R$.
- Let (R, +, $\times$) and (S, $+'$, ψ') be rings, with identities 0 and 0' respectively. Let f: R $\to$ S be a ring homomorphism. Then **kernel** of f is defined as the set $\{x \in R \mid f(x) = 0'\}$.

  We denote kernel of f as ker (f) or ker f.
- A non-empty set I of a ring R is called an **Ideal** in R if
  1. I is a subgroup of R, under addition.
  2. For every $a \in I$, $a \cdot x = x \cdot a$, for all $x \in R$.
- Let R be a commutative ring with unit element. If every non-zero element has a multiplicative inverse, then R is called a field. A field is an integral domain, since if a, b $\in$ R, then $a \cdot b = 0$ implies $(a^{-1} \cdot a) \cdot (b \cdot b^{-1}) = (a^{-1} \cdot 0) \cdot b^{-1} = 0$ which further implies

  $1 \cdot 1 = 0$, which is not true, since $1 \cdot 1 = 1$.

MODEL QUESTION PAPERS FOR
Mid-Semester Examination (2019 Pattern)

Time : 1 Hour **Maximum Marks : 30**

Instructions to the candidates:

(i) Answer Q. No. 1 or 2, Q. No. 3 or 4.

(ii) Assume suitable data wherever necessary.

(iii) Figures to the right indicate full marks.

(iv) Draw neat and labelled diagram wherever necessary.

1. (a) It was found that in first year of computer science of 80 students, 50 know Cobol, 55 know 'C' and 46 know Pascal language. It was also known that 37 know 'C' and Cobol, 28 know 'C' and Pascal, 25 know Pascal and Cobol languages. 7 students, however, know none of the languages. **[5]**

Find:

(i) How many know all the three languages?

(ii) How many know exactly two languages?

(b) Show that $(11)^{n+2} + (12)^{2n+1}$ is divisible by 133, for any positive integer n. **[5]**

(c) Write the following statements in symbolic form using propositions: **[5]**

(i) Indians will win the world-cup if their fielding improves.

(ii) If I am not in a good mood or I am not busy, then I will go for a movie.

(iii) If you know Object Oriented Programming and Oracle, then you will get a job.

(iv) I will score good marks in the exam if and only if I study hard.

(v) Program is readable only if it is well structured.

OR

2. (a) In a set of integers 1 to 500, find how many integers are divisible by 3 or 5 or 11. **[5]**

(b) Show that $1 + 2 + 2^2 + 2^3 + \ldots + 2^n = 2^{n+1} - 1$ where n is a natural number. **[5]**

(c) Explain in brief with examples: **[5]**

(i) Countably Infinite Set

(ii) Power Set

3. (a) Set A = {1, 2, 3, 4}, B = {1, 4, 6, 8, 9}; The relation R is defined from A to B such that aRb iff $b = a^2$ where $a \in A$ and $b \in B$. Find the domain and range of R. Also find therelation matrix and digraph of R. **[5]**

(b) Relation R is defined on set A = {2, 3, 4, 6} where, a R b if a divides b. Show that R is apartial order relation and draw its Hasse diagram. **[5]**

(c) The function f(x) = 2x + 3, g(x) = 3x + 4, h(x) = 4x for $x \in R$, where R is a set of real numbers. Find functions compositions gof, fog, foh, hof and goh. **[5]**

OR

4. (a) Set X = {1, 2, ... 7} and R = {(x, y) | x – y is divisible by 3}. Show that R is an equivalence relation. Draw the graph of R. **[5]**

(b) If set A={1, 2, 3, 4} and R = {(1, 2), (2, 4), (1, 3), (3, 2)}. Find the transitive closure of R by Warshall's algorithm. **[5]**

(c) Explain in brief with examples: **[5]**

(i) Lattice (ii) Partial Order Relation

End-Semester Examination (2019 Pattern)

Time : 2 1/2 Hours **Max. Marks : 70**

N.B. : (i) Answer Q. No. 1 or 2, Q. No. 3 or 4, Q. No. 5 or 6, Q. No. 7 or 8.
(ii) Assume suitable data wherever necessary.
(iii) Figures to the right indicate full marks.
(iv) Draw neat and labelled diagram wherever necessary.

1. (a) A and B are members of a club with a membership of 30. In how many ways can a committee of 10 be formed if
(i) A must be included in the committee?
(ii) A or B should be included but not both? **[6]**

(b) How may four-digit numbers are there formed from the digits 1, 2, 3, 4, 5 (with possible repetition) that are divisible by 4? **[6]**

(c) From a group of 12 mathematicians and 9 physicists, a committee of 8 is to be formed including two physicists. In how many ways can the committee be chosen so that atleast 5 mathematicians are on the committee? **[6]**

OR

2. (a) Suppose that repetitions are not permitted, then how many 4 digit numbers can be formed from the six digits 1, 2, 3, 5, 7, 8? How many such numbers are less than 4000? **[6]**

(b) How many arrangements of the word INSTRUCTOR are there in which there are exactly two consonants between successive pairs of vowels? **[6]**

(c) Five fair coins are tossed and the results are recorded.
(i) How many different sequences of heads and tails are possible?
(ii) How many of the sequences have exactly one head?
(iii) How many of the sequences have at the most 3 heads? **[6]**

3. (a) Explain the following in brief : **[6]**
(i) Bipartite graph
(ii) Planar graph
(iii) Eulerian Graph

(b) Find under what conditions $K_{m, n}$ the complete bipartite graph will have an eulerian circuit. **[6]**

(c) Find whether following pairs of graphs shown below are isomorphic or not. **[5]**

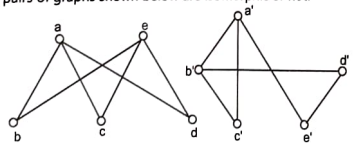

Fig. 1

OR

4. (a) Explain the following in brief : **[6]**
(i) Adjacency matrix of undirected graph.
(ii) Spanning subgraph
(iii) Colouring of graph

(b) For the following graph, find the shortest path between a and e using Dijkstra's Algorithm. **[6]**

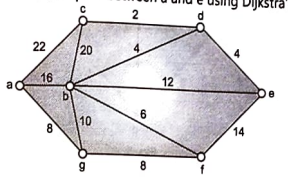

Fig. 2

(c) Use nearest neighbour method to find the Hamiltonian circuit starting from the vertex 'a' in the following graph. Find its weight. **[5]**

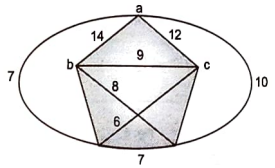

Fig. 3

5. (a) Define the following terms with examples: **[6]**
(i) Rooted tree
(ii) Optimal binary tree
(iii) Height of the tree.

(b) Find the preorder, postorder and inorder traversals of the following tree: **[6]**

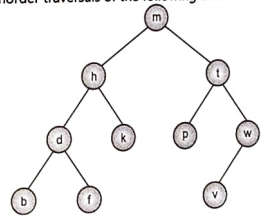

Fig. 4

(c) Suppose data items A, B, C, D, E, F, G occur in the following frequencies respectively 10, 30, 5, 15, 20, 15, 5. Construct a Huffman code for the data. What is the minimum weighted path length ? **[6]**

OR

6. (a) Explain
(i) Binary search tree
(ii) Subtree
(iii) Regular m-ary tree **[6]**