The adjacency matrix of G is given by

$$X = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \end{array} \begin{array}{c} \begin{array}{cccccc} v_1 & v_2 & v_3 & v_4 & v_5 & v_6 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \end{array}.$$

We have the following observations about the adjacency matrix X of a graph G.

1. The entries along the principal diagonal of X are all zeros if and only if the graph has no self-loops. However, a self-loop at the ith vertex corresponds to $x_{ii} = 1$.
2. If the graph has no self-loops, the degree of a vertex equals the number of ones in the corresponding row or column of X.
3. Permutation of rows and the corresponding columns imply reordering the vertices. We note that the rows and columns are arranged in the same order. Therefore, when two rows are interchanged in X, the corresponding columns are also interchanged. Thus two graphs G_1 and G_2 without parallel edges are isomorphic if and only if their adjacency matrices $X(G_1)$ and $X(G_2)$ are related by

$$X(G_2) = R^{-1}X(G_1)R,$$

where R is a permutation matrix.

4. A graph G is disconnected having components G_1 and G_2 if and only if the adjacency matrix $X(G)$ is partitioned as

4. A graph G is disconnected having components G_1 and G_2 if and only if the adjacency matrix $X(G)$ is partitioned as

$$X(G) = \begin{bmatrix} X(G_1) & : & O \\ \cdots & : & \cdots \\ O & : & X(G_2) \end{bmatrix},$$

where $X(G_1)$ and $X(G_2)$ are respectively the adjacency matrices of the components G_1 and G_2. Obviously, the above partitioning implies that there are no edges between vertices in G_1 and vertices in G_2.

5. If any square, symmetric and binary matrix Q of order n is given, then there exists a graph G with n vertices and without parallel edges whose adjacency matrix is Q.

GRAPH ISOMORPHISM

DEFINITION:

Two graphs G_1 and G_2 are said to be isomorphic to each other, if there exists a one-to-one correspondence between the vertex sets which preserves adjacency of the vertices.

Note: If G_1 and G_2 are isomorphic then G_1 and G_2 have,

(i) The same number of vertices.

(ii) The same number of edges

(iii) An equal number of vertices with a given degree.

Note: However, these conditions are not sufficient for graph isomorphism.

ISOMORPHISM AND ADJACENCY:

RESULT 1:

Two graphs are isomorphic if and only if their vertices can be labeled in such a way that the corresponding adjacency matrices are equal.

RESULT 2:

Two simple graphs G1 and G2 are isomorphic if and only if their adjacency matrices A1 and A2 are related $A1=P^{-1} A_2 P$ where P is a permutation matrix.

Note:

A matrix whose-rows are the rows of the unit matrix but not necessarily in their natural order is called permutation matrix.

Example:
Test the Isomorphism of the graphs by considering the adjacency matrices.

Let A1 and. A2 be the adjacency matrices of G1 and G2 respectively.

$$A_1 = \begin{array}{c} \\ u_1 \\ u_2 \\ u_3 \\ u_4 \end{array} \begin{array}{c} \begin{array}{cccc} u_1 & u_2 & u_3 & u_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

$$A_2 = \begin{array}{c} \\ V_1 \\ V_2 \\ V_3 \\ V_4 \end{array} \begin{array}{c} \begin{array}{cccc} V_1 & V_2 & V_3 & V_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

Now $A_1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$

$\sim \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$ (Interchaning Column 3 and Column 4)

$\sim \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$ (Interchaning Row 3 and Row 4)

$\sim A_2$

Since A_1 and A_2 are similar, the corresponding graphs G_1 and G_2 are Isomorphic.

Paths,Reachability and Connectedness:

DEFINTTIONS:

Path:

A Path in a graphi s a sequence v1,v2,v3……vk of vertices each adjacent to the next.ln other words,starting with the vertex v1 one can travel along edges(v1,v2),(v2,v3)..and reach the vertex vk.

Length of the path:

The number of edges appearingi n the sequence of a path is called the length of Path.

Cycle or Circuit:

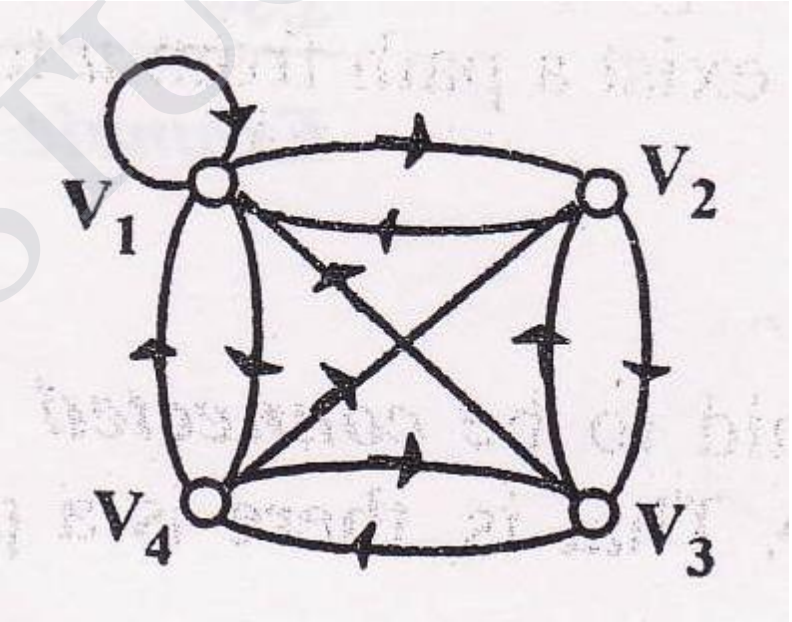
A path which originates and ends in the same node is called a cycle of circuit.

A path is said to be simple if all the edges in the path are distinct.

A path in which all the vertices are traversed only once is called an elmentary Path.

Example I :

Consider the graph:



Then some of the paths originating in node V1 and ending in node v1 are:

P1=(<V1 ,V2> ,<V2V3>)

P2=(<V1 ,V4> ,<V4 ,V3>)

P3 = (<V1 ,V2>,(V2, V4), <V4, V3>)

P4 = (<V1;V2>,<V2,V4>,<V4,V1>,<V1,V2>, <V2,V3>)

P5 = (<V1,V2>,<V2,V4>,<V4,V1 >,<V1,V4>,<V4,V3>)

P6= (<V1,Vl>, (V1,V1), (V1,V2), < V2, V3>)

Here,paths P1P2 and P3 are elementary path.

Path P5 is simple but not elementary.

DEFINITION:

REACHABLE:

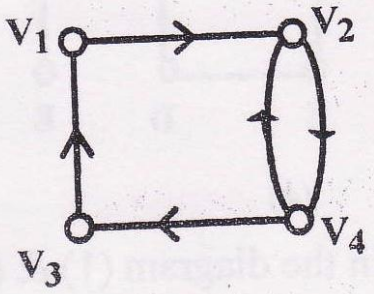
A node v of a simple digraph is-said to ber eachable from the node u of the same graph, if there exist a path from u to v.

Connected Graph :

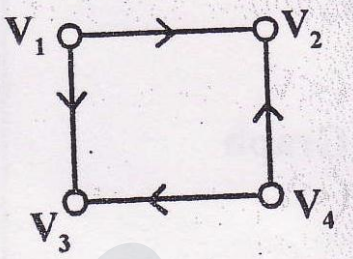
An directed graph is said to be connected if any pair of nodes are reachable from one another that is, there is a path between any pair of nodes.

A graph which is not connected is called disconnected graph.

Example 1 :



Connected Graph



Not Connected Graph

Components of a Graph :

The connected subgraphs of a graph G are called components of the.' graph G.

Theorem :

A simple graph with 'n' vertices and 'k' components can have atmost $\frac{(n-k)(n-k+1)}{2}$ ***edges***

Proof :

Let $n_1, n_2, \ldots\ldots, n_k$ be the number of vertices in each of k components of the graph G.

Then $n_1 + n_2 + \ldots\ldots + n_k = n = |V(G)|$

$$\sum_{i=1}^{k} n_i = n \qquad \ldots (1)$$

Now, $$\sum_{i=1}^{k} (n_i - 1) = (n_1 - 1) + (n_2 - 1) + \ldots\ldots + (n_k - 1)$$

$$= \sum_{i=1}^{k} n_i - k$$

$$\sum_{i=1}^{k} (n_i - 1) = n - k$$

Squaring on both sides

$$\left[\sum_{i=1}^{k} (n_i - 1)\right]^2 = (n-k)^2$$

$$(n_1 - 1)^2 + (n_2 - 1)^2 + \ldots\ldots + (n_k - 1)^2 \leq n^2 + k^2 - 2nk$$

$$n_1^2 + 1 - 2n_1 + n_2^2 + 1 - 2n_2 + \ldots + n_k^2 + 1 - 2n_k \leq n^2 + k^2 - 2nk$$

DEFINITION:

Unilaterally Connected:

A simple digraph is said to be unilaterally connected if for any pair of nodes of the graph atleast one of the node of the pair is reachable from the node.

Strongly Connected:

A simple digraph is said to be strongly connected if for any pair of nodes of the graph both the nodes of the pair are reachable from the one another.

Weakly Connected:

We call a digraph is weakly.connected if it is connected.as an undirected graph in which the direction of the edges is neglected.

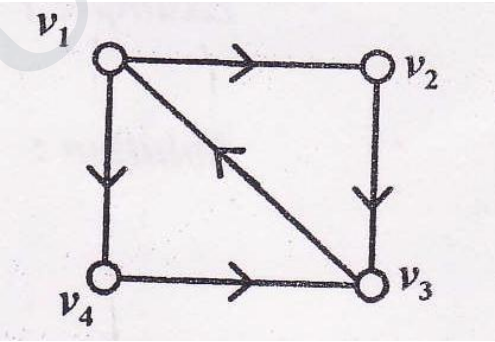
Note:

1.A unilateraaly connected digraph is weakly connectedbut a weakly connected digraph is not necessarily unilaterally connected.

2.A strongly connected digraph is both unilaterally and weakly connected.

EXAMPLE:

For example consider the graph:



It is strongly connected graph.

For,

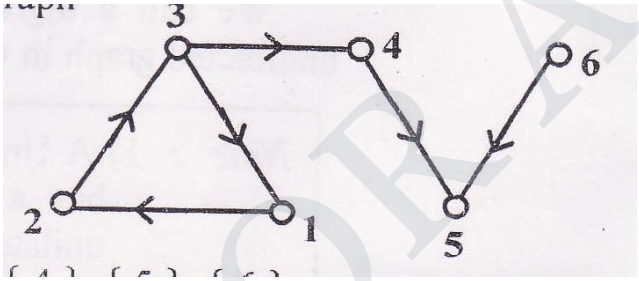
The possible pairs of vertices of the graph are (v1 v2), (v1 v3), (v1 V4), (V2 V3) and (v2 V4)

(1) Consider the pair (v1 v2)

Then there is a path from v1 to v2,via v1-> v2 and path from v2-> v1,via v2->v3->v1
(2) Consider the pair (v1 v3)
There is a path from v1 to v3, via v1 -> v2-> v3 and path from v3 to v1 via v3 -> v1.
similarly we can prove it for the remaining pair of vertices,each vertices is reachable from other.
Given graph is strongly connected

DEFINITION:

For a simple digraph maximal strongly connected subgraph is called strong component.
For the digraph:



{1,2,3},{4},{5},{6} are strong component.

The possible Hamilton cycles are
(l) A-B-C-D-A
(2) A-D-C-B-A
(3) B->C-D-A-B
(4) B-A-D-C-B
(s) C-D-A-B-C
(6) C-B-A-D-C
(7) D-A-B-C-D
(S) D-C-B-A-D
(Since all the vertices appeares exactly once),but not all the edges.
Since,G 1 contains Hamiltonian cycle,G 1- is a Hamiltonian graph.
(2) G2 contains Hamiltonian paths,namely
(1) A-> B-C-D
(2) A -> B-D-C
(3) D->C-B-A etc.

We cannot find Hamiltonian cycle in G2.
Therefore G2 is not a Hamiltonian graph

Properties :

(1) A Hamiltonianc irbuitc ontainsa Hamiltonian path but a graph , Containing a Hamiltonian path need not have a Hamiltonian cycle.
(2) By deleting any one edge from Hamiltonian cycle,we can get Hamiltonian path.
(3) A graph may contain more than one Hamiltonian cycle.
(4) A complete graph k_n, will always have a Hamiltonian cycle, when n>=3

Note :

We don't have simple necessary and sufficient criteria for the existence of Hamiltonian cycles. However, we have many theorems that give sufficient conditions for the existence of Hamiltonian cycles.
Also, certain properties can be used to show that a graph
Has no Hamiltonian cycle.F or example a, graph with a vertex of degree one cannot have a Hamiltonian cycle, since in a Hamiltonian cycle each vertex is incident with two edges in the cycle.

3.4 EULER GRAPH & HAMILTON GRAPH:

Example:Explain Konisberg bridge problem.Repersent the problem by mean of graph.Does the problem have a solution?

Solution: There are two islands A and B formed by a river.They are connected to each other and to the river banks C and D by means of 7-bridges

The problem is to start from any one of the 4 land areas.A,B,C,D, walk across each bridge exactly once and return to the starting point.(without swimmimg across the river)

This problem is the famous Konisberg bridge problem.

When the situation is represented by a graph,with vertices representating the land areas the edges representing the bridges,the graph will be shown as fig:

Theorem:

In a simple digraph,G=(V,E) every node of the digraph lies in exactly one strong component.

Proof:

Let v € V(G) and S be the set of all those vertices of G which are mutually reachable with v.

The problem is to find whether there is an Eulerian circuit or cycle(i.e.a circuit containing every edge exactly once) in a graph.

Here, we can not find a Eulerian circuit.Hence,Konisberg bridge problem has no solution .

EULER GRAPH:

Definition: Euler path:

A path of a graph G is called an Eulerian path,if it contains each edge of the graph exactly once.

Eulerian Circuit or Eulerian Cycle:

A circuit or cycle of a graph G is called an Eulerian circuit or cycle,if it includes each of G exactly once.

(Here starting and ending vertex are same).

An Eulerian circuit or cycle should satisfies the following conditions.

(1)Starting and ending points(vertices) or same.

(2)Cycle should contain all the edges of the graph but exactly once.

Eulerian Graph or Euler Graph:

Any graph containing an Eulerian circuit or cycle is called an Eulerian graph.

Theorem:

A connected graph is Euler graph(contains Eulerian circuit) if and only if each of its vertices is of even degree.

Proof:

Let G be any graph having Eulerian circuit(cycle) and let "C" be an Eulerian circuit of G with origin(and terminus) vertex as u.Each time a vertex as an internal of C,then two of the edges incident with v are accounted for degree.

We get,for internal vertex v € (G)

d(v)=2+2*{number of times u occur inside V

=even degree.

Conversely, assume each of its vertices has an even degree.

Claim: G has an Eulerian circuit.Support not, i.e.,Assume G be a connected graph which is not having an Euler circuit with all vertices of even degree and less number of edges.That is ,any degree having less number of edges than G,then it has an Eulerian circuit.Since each vertex of G has degree atleast two,therefore G contains closed path.Let C be a closed path of maximum possible length in G.If C itself has all the edges of G,then C itself an Euler circuit in G.

By assumption,C is not an Euler circuit of G and G-E© has some component G' with |E(G')|>0.C has less number of egdes than g, therefore C itself ia an Eulerian,and C has all the vertices of even degtee,thus the connected graph G' also has all the vertices of even degree.Since |E(G')|< |E(G)|,therefore G' has an Euler circuit C'.Bec ause G is connected,there is vertex v in both C and C'. Now join C and C' and transverse all the edges of C and C' with commen vertex v,we get CC' is a closed path in G and E (C C') > E (C), which is not possible for the chioices of C.

G has an Eulerian circuit.

G is Euler graph.

4.0 Introduction

In this unit we shall embark on the study of the algebraic object known as a group which serves as one of the fundamental building blocks for the subject today called abstract algebra.

4.1 ALGEBRAIC SYSTEMS - DEFINITIONS - EXAMPLES - PROPERTIES

Definition 1: Algebraic system or Algebra

A system consisting of a set and one or more n-ary operations on the set will be called an algebraic system or simply an algebra.

We shall denote an algebraic system by $(S, f_1, f_2, \ldots)$ where S is a nonempty set and $f_1, f_2, \ldots$ are operations on S.

Definition 2 : Algebraic structure

The operations and relations on the set S define a structure on the elements of S, an algebraic system is called an algebraic structure.

Example : Let I be the set of integers. Consider the algebraic system $(I, +, \times)$ where + and $\times$ are the operations of addition and multiplication on I.

A list of important properties

(A-1) For any $a, b, c \in I$

$$(a + b) + c = a + (b + c) \qquad \text{(Associativity)}$$

(A-2) For any $a, b \in I$

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

(A-3) There exists a distinguished element $0 \in I$ such that for any $a \in I$

$$a + 0 = 0 + a = a$$ (Identity element)

Here $0 \in I$ is the identity element with respect to addition

(A-4) For each $a \in I$, there exists an element in I denoted by $-a$ and called the negative of a such that

$$a + (-a) = 0$$ (Inverse element)

(M-1) For any $a, b, c \in I$

$$(a \times b) \times c = a \times (b \times c)$$ (Associativity)

(M-2) For any $a, b \in I$

$$a \times b = b \times a$$ (Commutativity)

(M-3) There exists a distinguished element $1 \in I$ such that for any $a \in I$

$$a \times 1 = 1 \times a = a$$ (Identity element)

(D) For any $a, b, c \in I$

$$a \times (b + c) = (a \times b) + (a \times c)$$ (Distributivity)

The operation $\times$ distributes over $+$.

(C) For $a, b, c \in I$ and $a \neq 0$

$$a \times b = a \times c \Rightarrow b = c$$ (Cancellation property)

The algebraic system $(I, +, \times)$ should have been expressed as $(I, +, \times, 0, 1)$ in order to emphasize the fact that 0 and 1 are distinguished elements of I.

Definition 3 : Homomorphism

If $\{X, \circ\}$ and $\{Y, *\}$ are two algebraic systems, where $\circ$ and $*$ are binary (n-ary) operations, then a mapping $g : X \to Y$ satisfying

$g(x_1 \circ x_2) = g(x_1) * g(x_2) \ \forall \ x_1, x_2 \in X$ is called a homomorphism

$= [a_1 (E_1 \cap E_2) a_1'] \wedge [a_2 (E_1 \cap E_2) a_2']$

$= (a_1 E_1 a_1')$ and $(a_1 E_2 a_1') \wedge (a_2 E_1 a_2')$ and $(a_2 E_2 a_2')$

$= (a_1 E_1 a_1') \wedge (a_2 E_1 a_2')$ and $(a_1 E_2 a_1') \wedge (a_2 E_2 a_2')$

$= (a_1 * a_2) E_1 (a_1' * a_2')$ and $(a_1 * a_2) E_2 (a_1' * a_2')$

$= (a_1 * a_2) (E_1 \cap E_2) (a_1' * a_2')$

$= (a_1 * a_2) E (a_1' * a_2')$

Hence, E is a congruence relation on A.

Example 2. Let $f : S \to T$ be a homomorphism from (S, $*$) to (T, Δ) and $g : T \to P$ is also a homomorphism from (T, Δ) to (P, ∇), then g o f : S → P is a homomorphism from (S, $*$) to (P, ∇).

Solution : As $g \circ f\ (S_1 * S_2) = g\ (f\ (S_1 * S_2))$

$= g\ (f\ (S_1\ \Delta f\ (S_2))$ [Since f is [homomorphism]

$= g\ (f\ (S_1 \nabla g\ (f\ (S_2)))$ [Since g is homomorphism]

$= g \circ f\ (S_1) \nabla g \circ f\ (S_2)$

$= g \circ f : S \to T$ is a homomorphism

Example 3. Let (A, $*$) and (B, Δ) be two algebra systems and g be homomorphism from A → B. Let (A_1, $*$) be subalgebra of (A, $*$). Then show that an the homomorphic image of (A_1, $*$) is a subalgebra of (B, Δ)

Solution : Let g be an homomorphism from A to B. Then for any two elements $a_1, a_2 \in A$.

$g\ (a_1 * a_2) = g\ (a_1)\ \Delta\ g\ (a_2)$. Let A_1 be a subset of A. As g is homomorphism from A to B, for any two elements, a_i, $a_j \in A_1 \subseteq A$.

$g\ (a_i * a_j) = g\ (a_i)\ \Delta\ g\ (a_j)$ and $g\ (A_1) \subseteq g\ (A) \subseteq B$. Therefore the image of A_1 and g forms an algebraic system with operation Δ, which becomes a subalgebra of B.

4. Given two algebraic system $(W, +)$ and $(Z_4, +_4)$ where W is the set of all non-negative integers and $+$ is the usual addition operation defined on W. Then show that there is a homomorphism from W to Z_4.

5. Let $(W, +)$ be an algebraic system of non-negative integers, where $+$ is the usual addition. Define an equivalence relation R on W such that $n_1 R n_2$ if and only if either $n_1 - n_2$ or $n_2 - n_1$ is divisible by 5. Show that R is an equivalence relation and that the homomorphism g defined from $(W, +)$ to Z_5 by $g(i) = [i]$ is the natural homomorphism associated with R.

4.2 Semi groups and Monoids - Groups - Subgroups- Homomorphisms

Definition 1 : Semi-group : [A.U N/D 2014]

A non-empty set S, together with a binary operation $*$ is called a semi-group if $*$ satisfies the following conditions.

(i) Closure : $\forall\ a, b \in S \Rightarrow a * b \in S$

(ii) Associative : $\forall\ a, b, c \in S,\ a * (b * c) = (a * b) * c$

Example : $(Z, \cdot)$ is a semi-group.

i.e., set of integers under multiplication operation is a semi-group.

Definition 2 : Monoid : [A.U N/D 2014]

A non-empty set M, together with a binary operation $*$ is called a monoid if $*$ satisfies the following conditions

(i) Closure : $\forall\ a, b \in M \Rightarrow a * b \in M$

(ii) Associative : $\forall\ a, b, c \in M \Rightarrow a * (b * c) = (a * b) * c$

(iii) Identity : $\forall\ a \in G, \exists\ e \in G$

s.t. $a * e = e * a = a$

Example : $(Z, +)$ is a monoid.

Definition 3 : Group :

A non-empty set G, together with a binary operation $*$ is said to form a group, if it satisfies the following conditions.

(i) Closure : $\forall\ a, b \in G \Rightarrow a * b \in G$

(ii) Associative : $\forall\ a, b, c \in G \Rightarrow a * (b * c) = (a * b) * c$

(iii) Identity : $\forall\ a \in G, \exists\ e \in G$, s.t. $a * e = e * a = a$

(iv) Inverse : $\forall\ a \in G, \exists\ a^{-1} \in G$, s.t. $a * a^{-1} = a^{-1} * a = e$

Example : $(Z, +)$ is a group.

Definition 4 : Abelian group :

A group $(G, *)$ is said to be an abelian group or commutative group if $a * b = b * a,\ \forall\ a, b \in G$

Example : 1. $(Z, +)$ is an abelian group.

2. S_3 is a non-abelian group.

Definition 5 : Subgroup :

A non-empty subset H of a group G $(H \subseteq G)$ is a subgroup of G iff $a, b \in H \Rightarrow ab^{-1} \in H$

Example : $(Z, +)$ is a subgroup of group $(R, +)$

Definition 6 : Order of a group :

Let G be a group under the binary operation $*$. The number of elements in G is called the order of the group G and is denoted by $O(G)$

Note : If the $O(G)$ is finite, then G is called a finite group, otherwise it is called an infinite group.

Definition 7 : Semi-group homomorphism

Let (S, $*$) and (T, Δ) be any two semigroups. A mapping g : S→T such that for any two elements $a, b \in S$.

$$g(a * b) = g(a)\ \Delta\ g(b)$$

is called a semigroup homomorphism.

Illustraion :

1. $G = \{-1, 1\}$ is a cyclic group generated by -1, since $(-1)^1 = -1$ and $(-1)^2 = 1$. Thus $G = (-1)$
2. $G = \{-1, 1, i, -i\}$ is a cyclic group, where $G = <i>$. Notice that $i^1 = i$, $i^2 = -i$, $i^3 = -i$, $i^4 = 1$. Also $G = <i>$.

Definition 12 : Permutation :

Any one-to-one mapping of a set S onto S is called a permutation of S.

Definition 13 : Even and odd permutation

A permutation of a finite set is called **even** if it can be written as a product of an even number of transpositions, and it is called **odd** if it can be written as a product of an odd number of transpositions.

4.2(a) Semi-group and Monoids

Theorem 1 : The composition of semi-group homomorphism is also a semi-group homomorphism.

Proof :

Let $(S, *)$, (T, Δ) and $(V, \oplus)$ be semi-groups

Let $a, b \in S$

Define : $f : S \to T$ be semi-group homomorphism

$$\Rightarrow f(a * b) = f(a) \Delta f(b) \quad \ldots (1) \text{ where } f(a), f(b) \in T$$

Define : $g : T \to V$ be semi-group homomorphism

$$\Rightarrow g[f(a) \Delta f(b)] = g\left(f(a)\right) \oplus g\left(f(b)\right) \quad \ldots (2)$$

where $g\left(f(a)\right), g\left(f(b)\right) \in V$

To prove : $g \circ f : S \to V$ is a semi-group homomorphism

Proof : $g \circ f(a * b) = g[f(a * b)]$

$= g[f(a) \Delta f(b)]$ by (1)

$= g[f(a)] \oplus g[f(b)]$ by (2)

$$= (g \circ f)(a) \oplus (g \circ f)(b)$$

Hence, $g \circ f : S \to V$ is a semi-group homomorphism.

Note : $g \circ f(a) = g\left(f(a)\right)$

Definition : Semi-group endomorphism :

A homomorphism of a semi-group into itself is called a semi-group endomorphism.

Theorem 2. The set of all semi-group endomorphisms of a semi-group is a semi-group under the operation of left composition

Proof : Let F be the set of all semi-group homomorphism

$f : S \to S$ where $(S, *)$ is a semigroup.

To prove : (F, o) is a semi-group with binary operation o, the left composition of mapping.

Proof :

(i) Closure : $\forall f, g \in F \Rightarrow f \circ g \in F$

(ii) Associative : $\forall f, g, h \in F, \forall a \in S$

$$(f \circ g) \circ h\,(a) = f \circ g\left(h\,(a)\right)$$
$$= f\left(g\,(h\,(a))\right)$$
$$= f\left(g \circ h\,(a)\right)$$
$$= f \circ (g \circ h)\,(a)$$
$$\Rightarrow (f \circ g) \circ h = f \circ (g \circ h)$$

$\therefore (F, o)$ is a semi-group.

Note : Infact (F, o) is a monoid, because the identity mapping I is the identity under o. Thus (F, o, I) is a monoid. Therefore the set of all semigroup homomorphisms of a semigroup is a monoid.

Theorem 3. Let $(S, *)$ be a given semi-group. There exists a homomorphism $g : S \to S^S$, where $(S^S, \circ)$ is a semi-group of functions from S to S under the operation of (left) composition.

[A.U N/D 2011]

Proof : For any $a \in S$

We define a function $f_a : S \to S$,

defined by $f_a(b) = a * b, \quad \forall\ b \in S$

$$\therefore f(a) \in S^S$$

Now, we define $g : S \to S^S$ by

$$g(a) = f_a, \quad \forall\ a \in S$$

Let $a, b \in S$, then $a * b \in S$

$$g(a * b) = f_{a*b}$$

$$f_{a*b}(c) = (a * b) * c, \ \forall\ c \in S$$

$$= f_a(b * c)$$

$$= f_a\left(f_b(c)\right)$$

$$= f_a \circ f_b(c)$$

$$\Rightarrow \quad f_{a*b} = f_a \circ f_b$$

$$\Rightarrow \quad g(a * b) = g(a) \circ g(b)$$

Hence, the proof.

Theorem 4. Let X be a set containing n elements, let X^* denote the free semigroup generated by X, and let (S, $\oplus$) be any other semigroup generated by any n generators ; then there exists a homomorphism $g : X^* \to S$.

Proof : Let Y be the set of n generators of S. Let $g : X \to Y$ be a one-to-one mapping given by $g(x_1) = y_i$ for $i = 1, 2, \ldots n$. Now for any string

$$\alpha = x_1, x_2, \ldots x_m$$

of X^*, we define

$$g(\alpha) = g(x_1) \oplus g(x_2) \oplus \ldots \oplus g(x_m)$$

From this definition it follows that for a string $\alpha\beta \in X^*$,