REVISED SYLLABUS
S.Y.B.SC. (I.T.), SEM. -III,
LOGIC AND DISCRETE MATHEMATICS

Unit 1 :

Set Theory : Fundamentals - Sets and subsets, Venn Diagrams, Operations on sets, Laws of Set Theory, Power Sets and Products, Partition of sets, The Principle of Inclusion - Exclusion.

Logic : Propositions and Logical operations, Truth tables, Equivalence, Implications, Laws of Logic, Normal forms, Predicates and quantifiers, Mathematical Induction.

Unit 2 :

Relations, diagraphs and lattices : Product sets and partitions, relations and diagraphs, paths in relations and diagraphs, properties of relations, equivalence and partially ordered relations, computer representation of relations and diagraphs, manipulation of relations, Transitive closure and Warshall's algorithm, Posets and Hasse Diagrams, Lattice.

Unit 3 :

Functions and Pigeon Hole Principle : Definitions and types of functions : injective, subjective and bijective, Composition, identity and inverse, Pigeon hole principle.

Unit 4 :

Graphs and Trees : Graphs, Euler paths and circuits, Hamiltonian paths and circuits, Planner graphs, coloring graphs, Isomorphism of Graphs.

Trees : Trees, rooted trees and path length in rooted trees, Spanning tree and Minimal Spanning tree, Isomorphism of trees, Weighted trees and Prefix Codes.

Unit 5 :

Algebric Structures : Algebraic structures with one binary operation - semi groups, monoids and groups, Product and quotient of algebraic structures, Isomorphism, homomorphism, automorphism, Cyclic groups, Normal sub group, codes and group codes, Algebraic structures with two binary operations - rings, integral domains and fields. Ring homomorphism and Isomorphism.

Unit 6 :

Generating Functions and Recurrence relations : Series and Sequences, Generating Functions, Recurrence relations, Applications, Solving difference equations, Fibonacci.

Books :

Discrete mathematical structures by B Kolman RC Busby, S Ross PHI Pvt. Ltd.

Discrete mathematical structures by R M Somasundaram (PHI) EEE Edition.

Reference :

Discrete structures by Liu, Tata McGraw -Hill.

Digital Logic John M Yarbrough Brooks / cole, Thompson Learning

Discrete Mathematics and its Applications, Kenneth H. Rosen, Tata McGraw - Hill.

Discrete Mathematics for computer scientists and Mathematicians, Joe L. Mott, Abraham

Kandel Theodore P. Baker, Prentice - Hall of India Pvt. Ltd.

Discrete Mathematics With Applications, Susanna S. Epp, Books / Cole Publishing Company.

Discrete Mathematics, Schaum's Outlines Series, Seymour Lipschutz, Marc Lipson, Tata McGraw - Hill.

1

FUNDAMENTALS OF DISCRETE MATHEMATICS

Unit Structure :

1.0 OBJECTIVES

After going through this chapter you will be able to :

- Understand basic tools of discrete mathematics like sets.
- Understand different type of sets.
- Understand different operation on sets.
- Principle of Inclusion- Exclusion.
- Solve different examples on sets, and principle of Inclusion-Exclusion etc.

1.1 INTRODUCTION

Sets are one of the most fundamental concepts in mathematics. It was invented at the end of the 19^{th} century. It is seen as the foundation from which all of the mathematics can be derived. Concept of division of Integers is fundamental to computer arithmetic. Mathematical structures are useful in Number theory. Number theory plays an important role in Computer and Internet security.

1.2 SETS AND SUBSETS

1.2.1 Sets

A set is any well defined collection of distinct objects. Objects could be fans in a class room, numbers, books etc.

For example, collection of fans in a class room collection of all people in a state etc. Now, consider the example, collection of brave people in a class. Is it a set? The answer is no because brave is a relative word and it varies from person to person so it is not a set.

Note : Well-defined means that it is possible to decide whether a given object belongs to given collection or not.

Objects of a set are called as elements of the set. Sets are denoted by capital letters such as A, B, C etc and elements are denoted by small letters x, y, z etc.

If x is an element of set A then we write $x \in \mathrm{A}$ and if x is not an element of A then we write $x \notin \mathrm{A}$.

There are two ways to represent a set one way by listing all the elements of a set separated by a comma enclosed in braces. Another way of specifying the elements of a set is to give a rule for set membership.

For example, $\mathrm{A} = \{\mathrm{e}, \mathrm{t}, \mathrm{a}\}$ can be written as

$\mathrm{A} = \{x \mid x \text{ is a letter in the word 'eat'}\}$

We have following Basic sets of numbers.

(a) $\mathbb{N}$ = set of all Natural numbers.
$= \{1, 2, 3, ...\}$

(b) $\mathbb{W}$ = set of all whole numbers
$= \{0,\ 1,\ 2,\ 3, ...\}$

(c) $\mathbb{Z}$ = set of all Integers
$= \{...., -2, -1, 0, 1, 2, 3, ...\}$

(d) $\mathbb{Q}$ = set of all rational numbers.
$= \left\{ \frac{\mathrm{p}}{\mathrm{q}} / \mathrm{p}, \mathrm{q} \in \mathbb{Z}, \mathrm{q} \neq 0 \right\}$

(e) $\mathbb{R}$ = set of all real numbers.

1.2.2 Some Basic Definitions –

(a) Empty Set : A set without any element. It is denoted by $\varnothing$ or { }

For examples,

$B = \{x \mid x < 1 \quad \text{and} \quad x \in \mathbb{N}\} = \phi$

$C = \{x \mid x \in \mathbb{N} \quad \text{and} \quad x + 1 = 1\} = \phi$

(b) Equal Sets :- Two sets A and B are said to be equal if they have same elements and we write A = B.

For examples,

(1) $A = \{x \mid x$ is a letter in the word 'ate'$\}$

$B = \{y \mid y$ is a letter in the word 'eat'$\}$

$\therefore A = B$

(2) $X = \{-3, 3\}$ and $Y = \left\{x \mid x^2 = 9, x \in \mathbb{Z}\right\}$

i.e. X = Y

(c) Subset :- Set A is said to be a subset of B if every element of A is an element of B and this is denoted by $A \subseteq B$ or $B \supseteq A$. If A is not a subset of B we write $A \not\subseteq B$.

For example,

(1) $A = \{1\}$, $B = \left\{x \mid x^2 = 1, x \in \mathbb{Z}\right\}$ then $A \subseteq B$ and $B \not\subseteq A$

(2) $\mathbb{N} \subseteq \mathbb{W} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$

Note : (1) Every set A is a subset of itself i.e. $A \subseteq A$

(2) If $A \subseteq B$ but $A \neq B$ then we say A is a proper subset of B and we write $A \subset B$. If A is not a proper subset of B then we write $A \not\subset B$.

(3) $\varnothing \subseteq A$ for any set 'A'

(4) A = B iff $A \subseteq B$ and $B \subseteq A$

(d) Finite Set :- A set A with 'n' distinct elements, $(n \in \mathbb{N})$ is called as a finite set.

For example,

(1) $A = \{x \mid x \in \mathbb{N}, 5 \leq x \leq 20\}$

(2) $B = \{y \mid y$ is a hair on some ones head$\}$

(e) Infinite Set :- A set which is not finite is Infinite.

For example,
(1) $A = \{x \mid x \in \mathbb{R}, 1 < x < 2\}$
(2) $\mathbb{N}$
(3) $\mathbb{Q}$

Note : $\varnothing$ is finite.

(f) Cardinality of a set :- The number of elements in a set is called as cardinality of a set and it is denoted by n(A) or |A|.

For example,
(1) A = {1, 2, 3, 4, 5}, |A| = 5
(2) B = $\varnothing$, |B| = 0

(g) Power set :- Let A be a given set. Then set of all possible subsets of A is called as a power set of 'A'. it is denoted by P(A).

For example,
(1) A = {1, 2}
P(A) = {$\varnothing$, {1}, {2}, {1, 2}}

Note : (1) If |A| = m then $|P(A)| = 2^m$

(h) Universal set :- Any larger set which contains some subsets is a universal set. It is denoted by U.

For example,

(1) $\mathbb{R}$ contains $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{W}$ and $\mathbb{N}$.

$\therefore$ $\mathbb{R}$ is a universal set for $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{W}$ and $\mathbb{N}$. Similarly, $\mathbb{Q}$ is universal set for $\mathbb{W}$ and $\mathbb{N}$ and so on.

(2) A CPU consist of hard disk, RAM, ROM, Sound Card etc. It can be treated as a universal set.

(i) Venn diagram :- A pictorial representation of a set is called as Venn diagram. Elements of a set are denoted by dots enclosed in a triangle, a square or a circle.

For example,
(1) A = {a, b, d}

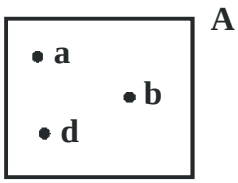


Fig. 1.1

(2) B = {5, 6, 7}

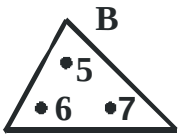


Fig. 1.2

Check your progress :

1. Identify each of the following as true or false.
   (a) A = A (b) $A \subset A$ (c) $A \subseteq A$ (d) $A \subseteq \phi$
   (e) $\phi \subseteq A$ (f) If A {1} then P(A) = $\{\phi, A\}$

2. If A = $\{x, y, 3\}$, then find (a) P(A), (b) |A| (c) |P(A)|

3. Which of the following are empty sets?
   (a) $\{x \mid x \in \mathbb{N}, 1 < x < 2\}$
   (b) $\{x \mid x \in \mathbb{R},\ x^2 = -1\}$
   (c) $\{x \mid x \in \mathbb{W},\ x + 1 = 1\}$
   (d) $\{x \mid x \in \mathbb{Q}, x^2 = 3\}$
4. Draw the Venn diagram for $\mathbb{N} \subseteq \mathbb{W} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

1.3 OPERATION ON SETS

1.3.1 Basic definitions :

(a) **<u>Union of two sets</u>** :- Let A and B be two given sets. Union of A and B is the set consisting of all elements that belong to 'A' or 'B' and it is denoted by $A \cup B$. $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$

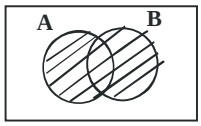
For example,
(1) A = $\{x, y, z\}$, B = $\{2, 5\}$
$A \cup B = \{x, y, z, 2, 5\}$

(2) $A = \mathbb{N}$, $B = \mathbb{Z}$
$A \cup B = \mathbb{N} \cup \mathbb{Z} = \{1, 2, 3, ...\} \cup \{....., -2, -1, 0, 1, 2, ...\}$
$= \{....., -2, -1, 0, 1, 2, ...\} = \mathbb{Z}$

Note : (1) If $A \subseteq B$ then $A \cup B = B$

(2) $A \cup A = A$

(3) $A \cup \phi = A$

(4) 

Shaded region represents $A \cup B$.

Fig. 1.3

(b) **<u>Intersection of two sets :-</u>** Let A and B be two given sets. Intersection of A and B is the set consisting of the elements Present in A and B. (i.e. in both) and it is denoted by $A \cap B$.

$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$

For example,

(1) A = {1, 2, 3}, B = {2, 4, 5} then $A \cap B = \{2\}$

(2) A = {1, 2, 3} and B = { x, y } then $A \cap B = \phi$ such sets whose intersection is empty is called as disjoint sets.

Note : (1) $A \cap A = A$

(2) If $A \subseteq B$ then $A \cap B = A$

(3) $A \cap \phi = \phi$

(4) Shaded region represents $A \cap B$

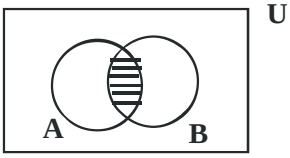


Fig. 1.4

(5) Disjoint sets

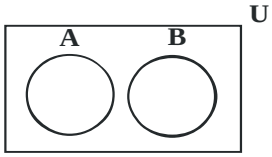


Fig. 1.5

Definition for union and Intersection can be extended to 'n' number of sets. ($n \in \mathbb{N}$)

(c) **<u>Complement of a set</u>** :- Let U be a given universal set and let A be any subset of U. Then complement of a set A in U is set of those elements which are present in U but not in A and it is denoted by A^c or A' or $\bar{A}$.

i.e. $A^c = \{x \mid x \notin A \ \& \ x \in U\}$

For example,

(1) If $A = \mathbb{N}$ and $U = \mathbb{W}$ then $A^c = \{0\}$ but if $U = \mathbb{Z}$ then $A^c = \{...., -2, -1, 0\}$ i.e. complement of a set depends on U.

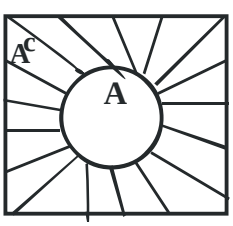


Fig. 1.6

Shaded region is A^c.

(d) Complement of A with respect to 'B' is the set of all elements in B which are not in A and it is denoted by A – B or $A \setminus B$.

i.e. $A - B = \{x \mid x \in A \text{ and } x \in B\}$

Similarly, we can define B – A.

For example,

(1) A = {1, 2, 3} and B = {3, 4, 5}

A – B = {1, 2} and B – A= {4, 5}

(2) A = {1, 2} and B = {3, 4}

A – B = A and B – A = B

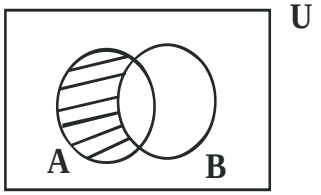


Fig. 1.7

A – B

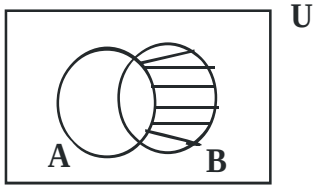
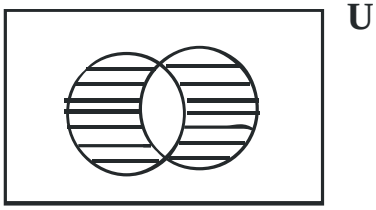


Fig. 1.8

B – A

(e) Symmetric difference of two sets :- Symmetric difference of two sets A and B is the set of elements present in A or in B but not both and it is denoted by $A \oplus B = (A - B) \cup (B - A)$.



A⊕B

Fig. 1.9

Check your progress :

1. If $A = U$ ($U -$ universal set), then (a) A^c, (b) $A \setminus U$, (c) $U \setminus A$, (d) $A \oplus U$

2. If $U = \{x \mid x \in \mathbb{N} \text{ and } x \leq 17\}$ and A = {1, 3, 5, 6}, B = {3, 4, 7, 5, 8}, then (a) A^c, (b) A\B, (c) B\A, (d) $A \oplus B$, (e) B^c, (f) $A \cup B$, (g) $A \cap B$.

1.3.2 Algebraic Properties of set operations

Like Algebraic properties of Real numbers, sets also satisfy some Algebraic Properties with respect to the operations union, intersection etc.

(I) Commutative Properties
- (1) $A \cup B = B \cup A$
- (2) $A \cap B = B \cap A$

(II) Associative Properties
- (3) $A \cup (B \cup C) = (A \cup B) \cup C$
- (4) $A \cap (B \cap C) = (A \cap B) \cap C$

(III) Distributive Properties
- (5) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- (6) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(IV) Idempotent Properties
- (7) $A \cup A = A$
- (8) $A \cap A = A$

(V) Properties of Complement
- (9) $(\overline{A}) = A$
- (10) $A \cup \overline{A} = U$
- (11) $A \cap \overline{A} = \varnothing$
- (12) $\overline{\varnothing} = U$
- (13) $\overline{U} = \varnothing$
- (14) $\overline{A \cup B} = \overline{A} \cap \overline{B}$
- (15) $\overline{A \cap B} = \overline{A} \cup \overline{B}$

} (De Morgan's laws)

Properties (1) to (13) can be proved easily. We will prove (14) and (15) here.

(14) $\overline{A \cup B} = \bar{A} \cap \bar{B}$

Proof : $\overline{A \cup B} = \{x \mid x \notin (A \cup B) \text{ and } x \in U\}$

$= \{x \mid (x \notin A \text{ and } x \in U) \text{ and } (x \notin B \text{ and } x \in U)\}$

$= \{x \mid x \in \bar{A} \text{ and } x \in \bar{B}\}$

$= \bar{A} \cap \bar{B}$

Similarly, we can prove (15).

Example 1: Prove that i) $(A \cup B) \cap (A \cup B^c) = A$ and

ii) $(A \cap B) \cup (A \cap B^c) = A$.

Solution: L.H.S.= $(A \cup B) \cap (A \cup B^c)$

$= A \cup (B \cap B^c)$ (Distributive law)

$= A \cup \phi$ ($B \cap B^c = \phi$ complement law)

$= A$

= R.H.S

Hence $(A \cup B) \cap (A \cup B^c) = A$.

Similarly, we can prove $(A \cap B) \cup (A \cap B^c) = A$.

Example 2: If U = {x\x is a natural number less than 20} is the universal set, A = {1, 3, 4, 5, 9}, B = {3, 5, 7, 9, 12}. Verify that De Morgan's laws.

Solution: De Morgan's laws can be state as i) $\overline{A \cup B} = \bar{A} \cap \bar{B}$,

ii) $\overline{A \cap B} = \bar{A} \cup \bar{B}$.

By listing method,

U = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19},

and A = {1, 3, 4, 5, 9},

$\bar{A}$ = {2, 6, 7, 8, 10, 11, 12, 13,14,15,16,17,18,19},

and B = {3,5,7,9,12},

$\bar{B}$ = {1, 2, 4, 6, 8, 10, 11, 13, 14, 15, 16, 17, 18,19}

$A \cup B$ = {1, 3, 4, 5, 7, 9, 12}

$(\overline{A \cup B})$ = {2, 6, 8, 10, 11, 13, 14, 15, 16, 17, 18, 19}

Also $(\bar{A} \cap \bar{B})$ = {2, 6, 8, 10, 11, 13, 14, 15, 16, 17, 18, 19}

Hence $\overline{A \cup B} = \bar{A} \cap \bar{B}$.

Now $(A \cap B) = \{3, 5, 9\}$,

$(\overline{A \cap B}) = \{1, 2, 4, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19\}$

Also $(\bar{A} \cup \bar{B}) = \{ 1, 2, 4, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19\}$

Hence $\overline{A \cap B} = \bar{A} \cup \bar{B}$.

Example 3: If u={1,2,3,4,5,6,7,8,9,10,11,12} is the universal set.
A={2,3,5,8,10}, and
B={4,5,7,8,9,11}, find.
i). A-B, ii). B-A, iii). $(\overline{A - B})$.

Solution:- i). A-B={2,3,10}
ii). B-A={4,7,9,11}
iii). $(\overline{A - B})$ ={1,4,5,6,7,8,9,11,12}.

1.3.3 Principle of Inclusion – Exclusion (The addition Principle)

Theorem (1) If A and B be two given finite sets, then we have $|A \cup B| = |A| + |B| - |A \cap B|$.

(1) Let A = {a, b, c, d} and B = {e, d, p, q}

$\therefore$ $A \cap B = \{c, d\}$

i.e. |A| = 4, |B| = 4 and $|A \cap B| = 2$

$\therefore$ By addition principle, $|A \cup B| = 4 + 4 - 2 = 6$

Example 4: In a class of 50 students, 25 like Maths and 15 like Physics, 10 like both Maths and Physics. So find (a) How many like Maths or Physics? (b) How many do not like any or the subjects?

Solution : Let m be the set of all those students who likes Maths and 'p' be the set of all those students who likes Physics.

$\therefore$ |M| = 25, |P| = 15 and $|M \cap P| = 10$

(a) No. of students like atleast one subject

$= |M \cup P| = |M| + |P| - |M \cap P|$ (by Addition formula)

$= 25 + 15 - 10$

$= 30$

(b) No. of students do not like any of the two subject

$= 50 - |M \cup P| = 50 - 30 = 20$

Above theorem can be extended to three sets, –

Theorem :- If A, B and C be given finite sets, then $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$

Example 5

In a survey of people it was found that 80 people knew Maths, 60 knew physics, 50 knew chemistry, 30 new Maths and Physics, 20 knew Physics and Chemistry, 15 knew Maths and Chemistry and 10 knew all three subjects. How many people knew?

(a) At least one subject

(b) Maths only

(c) Physics only

(d) Maths and Chemistry only

Solution : Let M, P, C represents respectively, the set of students knowing Maths, Physics and Chemistry.

$\therefore |M| = 80, |P| = 60, |C| = 50, |M \cap P| = 30, |M \cap C| = 15, |P \cap C| = 20, |M \cap P \cap C| = 10$

(a) By addition principle

$|M \cup P \cup C| = |M| + |P| + |C| - |M \cap P| - |M \cap C| - |P \cap C| + |M \cap P \cap C|$

$= 80 + 60 + 50 - 30 - 15 - 20 + 10$

$= 135$

Let's draw the Venn diagram of above situation.

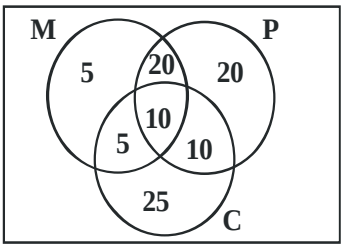


Fig. 1.10

(b) Maths only = 80 – (20 + 10 + 5)

= 80 – 35

= 45

(c) Physics only = 60 – (20 + 10 + 10) = 20

(d) Maths and Chemistry only = 15 – 10 = 5

Example 6: Out of 150 residents a building, 105 speak Marathi, 75 speak Gujarati and 45 speak both Languages. Find the number of

residents who do not speak either of the languages also find the number of residents who speak only Marathi.

Solution:- Let A be the set of resident who speak Marathi.
B the set of resident who speak Gujarati
Given $|U|=150$
$|A|=105$
$|B|=75$
$|A\cap B|=45$
By principal of Inclusion-Exclusion.
$|AUB|=|A|+|B|-|A\cap B|$
$= 105+75-45$
$=135.$
i). Number of resident who do not speak either of language.
$|(AUB)'|=|U|-|AUB|$
$=150-135$
$=15$
ii). The number of resident who speak only Marathi
$=|A|-|A\cap B|$
$=105-45$
$=60.$

Example 7: Out of 240 students in college 130 students are in N.C.C. 110 are in N.S.S. and 80 are in other activity in this 40 are N.C.C. and N.S.S both, 35 are N.C.C and other activity and 30 are N.S.S. and other activity but 20 student are take part in all three.

Find the number of students takes part in
i). Atleast any one.
ii). None of them.
iii). Only N.S.S.
iv). Only other activity.
v). Only N.S.S and N.S.S but not in other activity.

Solution:- Let A be the set of N.S.S students.

B be the set of N.C.C students.

C be the set of other activity student.

Here $|A|=130$, $|B|=110$, $|C|=80$.

$|A\cap B|=40$, $|A\cap C|=30$, $|B\cap C|=35$, $|A\cap B\cap C|=20$.

By principle Inclusion-Exclusion
i). atleast one of them i.e. $|AUBUC|$
$|AUBUC|=|A|+|B|+|C|-|A\cap B|-|B\cap C|-|A\cap C|+|A\cap B\cap C|$
$=130+110+80-40-35-30+20$
$=235.$

ii). None of them i.e. $|(AUBUC)'|$

$|(AUBUC)'| = |U| - |AUBUC|$

$=240-235$

$=5.$

iii). Only N.S.S. i.e.

$= |A| - |A\cap B| - |A\cap C| + |A\cap B\cap C|$

$=130-40-30+20$

$=80.$

iv). Only other activity i.e.

$= |C| - |A\cap C| - |B\cap C| + |A\cap B\cap C|$

$=80-30-35+20$

$=35.$

v). Only N.S.S and N.C.C. but not other activity i.e.

$= |AUB| - |A\cap B\cap C|$

$=40-20$

$=20.$

Example 8: Find the number of integers including both from 1 to 500 that are divisible by,

i). 2 or 3 or 5.

ii). 2 or 3 but not 5.

iii). Only by 5.

Solution:- Here $U=\{1,2,3,\ldots\ldots\ldots\ldots,500\}$

A=the set of numbers in U divisible by 2.

B= the set of numbers in U divisible by 3.

C= the set of numbers in U divisible by 5.

$|U|=250,\ |A| = \left[\frac{500}{2}\right] = 250$

$|B| = \left[\frac{500}{3}\right] = 166$

$|C| = \left[\frac{500}{3}\right] = 100$

$|AUB| = \left[\frac{500}{2\times 3}\right] = \left[\frac{500}{6}\right] = 83$

$|B\cap C| = \left[\frac{500}{15}\right] = 33$

$|C\cap A| = \left[\frac{500}{2\times 5}\right] = 50$

$|A\cap B\cap C| = \left[\frac{500}{2\times 3\times 5}\right] = \left[\frac{500}{30}\right] = 16$

i) $AUBUC|=|A|+|B|+|C|-|A\cap B|-|B\cap C|-|A\cap C|-|A\cap B\cap C|$

= 250+166+100-83-33-50+16

= 366.

ii). 2 or 3 but not by 5.

= | AUB | - | A∩B∩C |

=83-16

=67.

iii). Only by 5.

= | C | - | A∩C | - | B∩C | + | A∩B∩C |

=100-33-50+16

=33.

1.7 LET US SUM UP

This chapter consist of sets and different operations on sets with different examples which helps in better understanding of the concept and able to use in different areas. We saw the principle of inclusion – Exclusion which can be used in different counting problems we saw some concepts of number theory such as division in Integers, sequence etc. which is useful in computer security. At the end we saw definition of a mathematical structure and it is different properties.

1.8 REFERENCES FOR FURTHER READING

a) Discrete structures by Liu.

b) Discrete mathematics its Application, Keneth H. Rosen TMG.

c) Discrete structures by B. Kolman HC Busby, S Ross PHI Pvt. Ltd.

d) Discrete mathematics, schaum's outlines series, seymour Lip Schutz, Marc Lipson, TMG.

1.9 UNIT END EXERCISES

1. Let $A=\left\{x \mid x\in\mathbb{R} \text{ and } x^2+7=0\right\}$, $B=\{x \mid x\in\mathbb{Z}\}$,

$C=\{x \mid x\in\mathbb{R}, 0<x<0.2\}$, $D=\{x \mid x=6q, q\in\mathbb{Z}\}$

$E=\{x \mid x\in\mathbb{R}, x+7=7\}$

Check whether following are True or False.

(i) A is finite, (ii) $B\subseteq A$, (iii) $E=A$, (iv) $E\cup A\subseteq D$,

(v) C is infinite, (vi) $B=\mathbb{Z}$, (vii) $A\subseteq E$, (viii) $B\cap C=A$

2. Prove $A-B=A-(A\cap B)$

3. There are 250 students in a computer Institute of these 180 have taken a course in Pascal, 150 have taken a course in C++, 120 have taken a course in Java. Further 80 have taken Pascal and C++, 60 have taken C++ and Java, 40 have taken Pascal and Java and 35 have taken all 3 courses. So find –

   (a) How many students have not taken any course?

   (b) How many study atleast one of the languages?

   (c) How many students study only Java?

   (d) How many students study Pascal and C++ but not Java?

   (e) How many study only C++ and Java?

4. The students stay in hostel were asked whether they had a textbook r a digest in their rooms. The results showed that 650 students had a textbook, 150 deed not have a textbook, 175 had a digest and 50 had neither a textbook nor a digest. Find, i). the number of students in hostel , ii).How many have a textbook and digest both, iii). How many have only a digest.

5. Prove that $(B^c \cap U) \cap (A^c \cup \emptyset) = (AUB)^c$.

6. Prove that , i).$AU(A \cap B)=A$, ii). $A \cap (AUB)=A$.

7. In a survey of 80 people in Gokuldham 50 of them drink Tea, 40 of them drink Coffee and 20 drink both tea and coffee. Find the number of people who take atleast one of the two drinks also find the number of students who do not take tea or Coffee.

8. In a survey of 60 people, It was found that 25 read magazine. 26 read Times of India and 26 read DNA. Also 9 read both magazine and DNA, 11 read both magazine and times of India , 8 read times of India and DNA and 8 are not reading anything.

   i). Find the number of people who read all three.

   ii). Draw a Vann diagram.

   iii). Determine the number of people who read exactly one magazine.

2

LOGIC

Unit Structure :

2.0 OBJECTIVES

After going through this chapter you will be able to:

- Learn about the propositions related to Logical Operations.
- Learn about negations and various connectors like conjunction, disjunction.
- Learn about Quantifiers and Conditional and bi-conditional statements.
- Solve problems using the method of Mathematical Induction.

2.1 PROPOSITIONS AND LOGICAL OPERATIONS

The statement in English need not always be true or false whereas a statement in Logic is a declarative sentence which is either true or false but not both. Identify the statements among the following sentences.

1. It will rain today.....
2. Mumbai is capital city of Maharashtra.
3. Do you know where is Vijay ?
4. $2 \times 3 - 5 = 1$.
5. $x^2 - 1 = 4$.
6. Come in!

In above, sentences (1), (2) and (4) are statements. (3) is not a statement as it is question,(5) is declarative but depending upon the value of x it is true or false. Sentence (6) is a command and hence not a statement.

2.1.1 Logical connectives and compound statements.

Just as in mathematics variables x, y, z, ... can take real values and can be combined by operations $+,-,\times,\div$, in logic, the variables p, q, r, .. can the replaced by statements. The variable p, q, r, ... are called as propositional variables. For example we can write p : Sonia Gandhi is president of India, q : Newton was a Physicist, r : It will rain today. etc. One can combine propositional variables by logical connectives to obtain more complex statements - compound statement. For example suppose Q Mangoes are ripe, R : Oranges are sour. The statement Q and R means Mangoes are ripe and orange is sour. The truth value of compound statement depends on truth values of statements which are combined and on the logical connectives that are used. In this subsection, we will discuss most commonly used logical connectives.

2.1.2 Negation :

Suppose P is any statement. Then negation of P, denoted by $\sim p$. Thus if P is true then $\sim p$ is false and vice a versa. A table giving truth values of compound statement in terms of compound parts is known as truth table.

p	$\sim p$
T	F
F	T

Strictly speaking not P is not compound statement as it is unary operation.

Example 1 Give negation of

1. p: It is hot.

2. q: 2 is a divisor of 5.

Solution :
1. ~P : It is not the case that it is hot i.e. it is not hot.
2. ~q: 2 is not divisor of 5. Since q is false, $\sim q$ is true.

2.1.3 Conjunction

The next operation is conjunction. If p and q are two statement then conjunction of p and q is the compound statement "p and q". The notation is $p \wedge q$. The operation and is a binary operation on the set of statements. The $p \wedge q$ is true whenever both p and q on true, false otherwise. Thus the truth table is given by

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Example 2 Form the conjunction of p and q.

1. p: I will drive my car q: I will reach the office in time.
2. p: 2 is even q: 11 is odd.
3. p: 2 + 3 + 1 = 6 q: 2 + 3 > 4
4. p: Delhi is capital of India q: Physics is a science subject.

Solution :
1. $p \wedge q$ is "I will drive my car and I will reach office in time".
2. "2 is even and 11 is odd".
3. "2 + 3 + 1 = 6 and 2 + 3 > 4".
4. "Delhi is capital of India and Physics a science subject".

2.1.4 Disjunction

The second logical connective used is disjunction. Disjunction of statements p and q is dented by $p \vee q$,which means p or q. The statement $p \vee q$ is true where p or q or both are true and is false only when both p and q are false.

The truth table for $p \vee q$ is as follows.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Example 3 Form the disjunction of

1. p: Bananaras is on the bank of holy river Ganga. q: Dehra Doon is capital of Uttaranchal.
2. p: Eiffel tower is in London. q: Panama canal connects Atlantic ocean with Pacific ocean.
3. p: Mukesh and Anil are sons of Industrialist Late Dhirubhai Ambani. q: Rajbhavan is official residence of the Governor of Maharashtra.
4. p: $\sqrt{3}$ is rational. q: -10 is odd integer

Solution :
The statement $p \vee q$ is given by

1. Banaras is on the bank of holy river Ganga or Dehradoon is capital of Uttaranchal.
2. Eiffel Tower is in London or Panama canal connects Atlantic ocean with Pacific ocean.
3. Mukesh and Anil are sons of late Industrialist Dhirubhai Ambani or Rajbhavan is official residence of the Governor of Maharashtra.
4. $\sqrt{3}$ is rational or - 10 is odd.

The statements 1, 2 and 3 are true whereas 4 is false since p and q are both false.

Note that in logic we can join two totally unrelated sentences while in English, we do not combine.

In mathematics or in Computer Science, connective or is used in inclusive sense . That is $p \vee q$ is true if true if p is true or q is true or both are true. Consider the statements p: 2 is a prime number and q: 2 is composite. Here the composite statement $p \vee q$ is the statement "2 is prime number or 2 is composite". Since exactly one of p and q can be true, $\vee$ is used in exclusive sense.

A compound statement may have many Components each of which is if self a statement. $p \vee (q \wedge (p \wedge r))$ involves three prepositions p, q and r. The prepositions p, q and r each may be independently true of false. Hence there are in all $2^3 = 8$ possibilities in the truth table of $p \vee (q \wedge (p \wedge r))$. In general, if a statement involves n propositional variable, then there will be 2^n rows in its truth table.

Example 4 Make a truth table if $(p \vee q) \wedge (\sim q)$.

p	q	$p \vee q$	$\wedge$	~q
T	T	T	F	F
T	F	T	T	T
F	T	T	F	F
F	F	F	F	F

2.2 CONDITIONAL STATEMENTS

Observe the following sentences that we use in day to day life:-

1. If it is very hot in summer then there is a chance of early monsoon.

2. If I see you talking then I will give you a punishment.

3. If I am not in a good mood then I will go for swimming.

4. If I take stress then my blood pressure will increase.

Such sentences are called as conditional statements or implication. In logic, a compound statement of the type "If p then q" is called as conditional statement or implication. **p** is called as **hypothesis** or **antecedent** and **q** is called as **conclusion** or **consequent**. The notation for connective if then is denoted by: $p \Rightarrow q$.

Example 5 Write implication for each of the following.

1. p: I have headache q: I will take aspirin.

2. p: I take a walk q: I will reach late.

3. p: 2 divides 10 q: Rajiv will go to movie.

Solution : $p \Rightarrow q$ in each of the case is given by

1. If I have a headache, then I will take Aspirin.

2. If I take a walk then I will be late.

3. If 2 divides 10 then Rajiv will go for a movie.

Note than in 1 and 2 given above, we are assuming that p is cause of q. But in logic, $p \Rightarrow q$ means that if p is true then q will also be true. Hence it is not possible to have p to be true and q is false. Thus $p \Rightarrow q$ is false only when p is true and q is false. In all other possibilities $p \Rightarrow q$ is always true.

The truth table for $p \Rightarrow q$ is as follows.

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Example 6 Determine truth value of the following :

1. If 3 is even then India will win world cup football.
2. If 2 + 5 = 7 then Sonia Gandhi is the prime minister of India.

Solution:

1. This is true sine 3 is even is false. Note that when p is false, p $\Rightarrow$ q is always true for any q.
2. This is false because 2 + 5 = 7 is true and Sonia Gandhi is PM is false.

In mathematics we say p implies q or if p then q, q if p, p is sufficient for q or q is necessary for p. If $p \Rightarrow q$ is the implication ; then the statement $q \Rightarrow p$ is called its **converse** which also is an implication. The **contra-positive** statement of the implication $p \Rightarrow q$ is the statement $\sim q \Rightarrow \sim p$.

Example 7 Give contra-positive and converse of the following statements.

1. If I am hungry then I will eat.
2. If the three sides of a triangle are equal then each angle of the triangle is of measure 60^0.
3. If today is Sunday then I am going for a movie.

Solution

1. Let p be the statement I am hungry and q be the statement I will eat. The converse is If I will eat then I am hungry while contra-positive is the statement If I will not eat then I am not Hungry.
2. If each angle of a triangle is of measure 60^0 then the three sides of the triangle are equal (Converse); If each angle of a triangle is not of measure 60^0 then the triangle is not an isosceles (contra-positive).

3. If I go for a movie then it is Sunday (converse); If I do not go for a movie then it is not a Sunday (contra-positive).

Example 8 : Translate each of the following in verbal language.
p: Hardwork.

q: Success.

(i) $(\sim p) \wedge (\sim q)$, (ii). $p \wedge \sim q$, (iii). $p \rightarrow q$, (iv). $\sim q \rightarrow \sim p$

Solution : (i). No hardwork and no success.
(ii). Hardwork but not success.

(iii). If there is hardwork then there is a success.

(iv). If no success then no hardwork.

2.2.1 Quantifiers

A set can some times be conveniently denoted as {x | P(x)} which means that an element x is in the given set if it satisfies the given property, P(x). For example the set $\{0, \pm 2, \pm 4, \pm 6, ...\}$ can be described by {x | x is an even integer}. The sentence P(x) is called as **predicate** or **propositional function**. Let A = $\{0, \pm 2, \pm 4, \pm 6, ...\}$. Then the sentence P(x) "x is an even integer". Since P(2) is true, $2 \in$ A while $1 \notin$ A as P(1) is not true. The **universal quantification** of a predicate P(x) is the sentence "for all values of x, P(x) is true" and we write this as $\forall x$ P(x). The symbol $\forall$ is called as **universal quantifier**. We now discuss few examples.

Example 8 (a) Suppose P(x): $2x + 1$ is an odd number is a predicate that is true for all real numbers x. Hence the sentence $\forall x$ P(x) is true. (b) Let
Q(x): $x^2 - 9 < 16$. In this case $\forall x$ Q(x) is not true since Q(10) is not true.

A predicate may contain several variables and universal quantification can be applied to each of them. For example $\forall$ x $\forall$ y $\forall$ z (xy)z = x(yz) means that the property that the multiplication is associative is true for all real numbers x,y and z.

The **existential quantification** of a predicate P(x) is the statement "there exist some value of x for which P(x) is true". We write this symbolically as $\exists$ x P(x). The symbol $\exists$ is called as existential quantifier. in English, $\exists$ x can also be described as " there is some x" "there is at least one value of x".

Example 9 Let x and y be any two real numbers.

(a) The statement $\exists x \forall y$ x + y = y is true since real number 0 has the property that 0 + y = y for all real numbers y.

(b) The statement $\forall x \exists y$ x + y = y is not true since for real number 1 there is no real number y such that 1 + y = y.

Let p: $\forall$ x P(x). Then p will be false if there is at least one value of x for which P(x) is false. Thus there is at least one value of x for which $\sim$P(x) is true. Thus p is false if $\exists$ x $\sim$P(x) is true. Let q: $\exists$ x Q(x). Then q is false if there does not exists any value of x for which Q(x) is true i.e. for all values of x, $\sim$Q(x) is true. Thus q is false if $\forall$ x $\sim$Q(x) is true.

Example 10

(a) Let p: For all integers n, 3n-7 a perfect square. Then $\sim$p is the statement. There exists at least one integer n for which 3n - 7 is not a perfect square.

(b) Let q: there exists a real number x such that $2 < \frac{x^2+1}{x^2-1}$. Then $\sim$q is the statement For all real numbers x, $2 \geq \frac{x^2+1}{x^2-1}$.

2.2.2 Bi-conditional

Bi-conditional or equivalence of two statements p and q means both $p \Rightarrow q$ and $q \Rightarrow p$ and is denoted by $p \Leftrightarrow q$. The truth table of $p \Leftrightarrow q$ is given below.

p	q	$r : p \Rightarrow q$	$s : q \Rightarrow p$	$r \wedge s$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Note that $p \Rightarrow q$ is true if either p, q are both true or both false.

Example 11 Compute the truth table of $(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$

p	q	$p \Leftrightarrow q$	$\sim$p	$\sim$q	$\sim q \Rightarrow \sim p$	$(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$
T	T	T	F	F	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

Note that last column of the above table indicates that the statement $(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$ is always true. Such a statement is called as Tautology. A statement that is always false is called as Contradiction or absurdity. Any other statement is called as contingency.

Check Your Progress :

1) Translate each of the following in verbal language.

a) p: Teacher is present

q: student attend the class.

(i) $p \vee q$, (ii) $p \wedge q$, (iii).p→q, (iv).p↔q, (v). q↔p

b) p: 2 is an even number.

q: 2 is a prime number.

r: $2+2=(2)^2$.

(i). p→q, ii). q→p, (iii). p→q, (iv). p→(q ∨r), (v). ~p∧q, (vi). p∨~r, (vii). ~p→(~p∧~r).

2).Write down the following conditional statements in converse contra positive and inverse.

a). If it is a Sunday then it is a holiday.

b). If the teacher is present then students are standing.

c). If you know mathematics them you know logc.

3) Which of the following statements are Tautology, Contradiction or Contingency?

1. $(q \wedge p) \vee (q \wedge \sim p)$
2. $(p \vee q) \vee (\sim p \vee q)$
3. $p \wedge \sim p$

Similar to the mathematical structure [Sets, $\cup, \cap$], one can define a structure on set of proposition with the help of binary operations $\vee, \wedge$ and $\sim$.

The operations for propositions have following properties which we list as theorem. The proofs are very simple and hence are left as an exercise to the reader.

2.3 THEOREM

A. Commutativity

(a) $p \vee q \equiv q \vee p$

(b) $p \wedge q \equiv q \wedge p$

B. Associativity

(a) $(p \vee q) \vee r \equiv p \vee (q \vee r)$

(b) $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

C. Distributivity

(a) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

(b) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

D. Idempotent Property

(a) $p \vee p \equiv p$

(b) $p \vee p \equiv p$

E. Properties of negation

(a) $\sim(\sim p) \equiv p$

(b) $\sim(p \vee q) \equiv (\sim p) \wedge (\sim q)$

(c) $\sim(p \wedge q) \equiv (\sim p) \vee (\sim q)$

F. Properties of implication

(a) $(p \Rightarrow q) \equiv (\sim q \Rightarrow (\sim p))$

(b) $(p \Rightarrow q) \equiv ((\sim p) \vee q)$

(c) $\sim(p \Leftrightarrow q) \equiv ((p \wedge \sim q) \vee (\sim p \wedge q))$

(d) $(p \Leftrightarrow q) \equiv ((p \Rightarrow q) \wedge (q \Rightarrow r))$

Standard way of proving all the above properties is to construct truth table. In some cases one can also use previous results.

2.4 MATHEMATICAL INDUCTION

We now use the ideas developed so far and demonstrate an important technique of proof- Principle of mathematical induction which is an indispensable proof technique, extensively used in mathematics. Suppose P(n) is some statement or property or a formula to be verified where n is an integer. We need to establish the formula P(n) is true for all integers $n \geq n_0$, where n_0 is some fixed integer. This can be achieved as follows. First we establish the validity of $P(n)$ for $n = n_0$. This step is called as **basis step**. Next we show that $P(k) \Rightarrow P(k+1)$ is a tautology i.e. assuming the validity of P(k), we establish the validity of P(k + 1) for any integer $k \geq n_9$. This step is called as **induction step**. Usually some efforts are required to prove induction step. We now use the induction principle and prove many formulas, statements.

Example 12 Prove that $1 + 2 + 3 + \ldots\ldots + n = \frac{n(n+1)}{2}, n \geq 1$.

Solution: Let P(n) denote the formula $1 + 2 + 3 + \ldots\ldots + n = \frac{n(n+1)}{2}$, . $n \geq 1$ In this example, $n_0 = 1$.

Basis step: For n = 1, left hand side of above formula is 1while the right side is $\frac{1(1+1)}{2}$ which also is 1. Thus the formula is true for n = 1 and we have proved the basis step.

Induction step: We now need to establish the validity of the formula P(k+1) whenever P(k) is true for $k \geq 1$. Let $k \geq 1$ be any integer for which P(k) is true. Thus the statement $1 + 2 + 3 + \ldots\ldots + k = \frac{k(k+1)}{2}$. We now wish to prove $1 + 2 + 3 + \ldots\ldots + (k+1) = \frac{(k+1)\left((k+1)+1\right)}{2}$. We can write the right hand side of this as $1 + 2 + 3 + \ldots\ldots + k + (k + 1)$. By induction step we know that $1 + 2 + 3 + \ldots\ldots + k = \frac{k(k+1)}{2}$.

Thus $1 + 2 + 3 + \ldots\ldots + k + (k+1) = \frac{k(k+1)}{2} + (k+1)$. This upon straightforward simplification reduces to $\frac{(k+1)(k+2)}{2}$. This is precisely what we need to establish. We conclude by the principle of mathematical induction that P(n) is true for all positive integers.

Example 13. Prove by the method of induction, that for all $n \in N$,
$1.2.3 + 2.3.4 + 3.4.5 + \ldots\ldots + n\,(n+1)\,(n+2) = \frac{n(n+1)(n+2)(n+3)}{4}$.

Solution:- The result P(n) to be proved is, that for all $n \in N$
$1.2.3 + 2.3.4 + 3.4.5 + \ldots\ldots + n\,(n+1)\,(n+2) = \frac{n(n+1)(n+2)(n+3)}{4}$.

Step.1: For n = 1, L.H.S = 1.2.3 = 6 ;

R.H.S = $\frac{1,2,3,4}{4} = 6$

There for L.H.S = R.H.S for n = 1
There for P(1) is true

Step.2: Let us assume that for some $k \in N$, P(k) is true.
That is, $1.2.3 + 2.3.4 + 3.4.5 + \ldots\ldots + k\,(k+1)$

$(k+2) = \frac{k(k+1)(k+2)(k+3)}{4}$ ……(I)

Then to prove that P (k + 1) is true,
That is, to prove that
1.2.3 + 2.3.4 + 3.4.5 + …….. + k (k + 1) (k + 2) + (k + 1) (k + 2) $(k+3)=\frac{k(k+1)(k+2)(k+3)(k+4)}{4}$

Here
L.H.S = [1.2.3 + 2.3.4 + 3.4.5 + ……+ k (k + 1) (k + 2)] + (k + 1) (k + 2) (k + 3)

= $\frac{k(k+1)(k+2)(k+3)}{4}$ + (k+1) (k + 2) (k + 3)…… [by (I).]

= (k + 1) (k + 2) (k + 3) $\left(\frac{k}{4}+1\right)$

$=\frac{k(k+1)(k+2)(k+3)(k+4)}{4}$

= R.H.S.

There for P (k + 1) is true.

There for by the principal of mathematical induction, the result P (n) is true for all n □ N, that is, 1.2.3 + 2.3.4 + 3.4.5 + ……+ n (n + 1) (n + 2) = $\frac{n(n+1)(n+2)(n+3)}{4}$, for all n ∈ N.

Example 14. Prove by the method of induction, that for all n ∈ N ,

$$\frac{1}{3.5}+\frac{1}{5.7}+\frac{1}{7.9}+.....+\frac{1}{(2n+1)(2n+3)}=\frac{n}{3(2n+3)}$$

Solution:- the result p (n) to be proved is that for all n∈N

$$\frac{1}{3.5}+\frac{1}{5.7}+\frac{1}{7.9}+.....+\frac{1}{(2n+1)(2n+3)}=\frac{n}{3(2n+3)}$$

Step.1. For n=1 L.H.S = $\frac{1}{3.5}$

R.H.S = $\frac{1}{3(2\times1+3)}=\frac{1}{3.5}$

There for L.H.S = R.H.S for n=1 there for P(1) is true.

Step.2. Let us assume that for some k∈N, P (k) is true.

That is, $\frac{1}{3.5}+\frac{1}{5.7}+\frac{1}{7.9}+.....+\frac{1}{(2k+1)(2k+3)}=\frac{k}{3(2k+3)}$ .....(1)

Then to prove that P (k+2) is true,
That is to prove that

$$\frac{1}{3.5}+\frac{1}{5.7}+\frac{1}{7.9}+.....+\frac{1}{(2k+1)(2k+3)}+\frac{1}{(2k+3)(2k+5)}=\frac{k+1}{3(2k+5)}$$

Here
L.H.S

$$=\left[\frac{1}{3.5}+\frac{1}{5.7}+\frac{1}{7.9}+.....+\frac{1}{(2k+1)(2k+3)}\right]+\frac{1}{(2k+3)(2k+5)}$$

$$=\frac{k}{3(2k+3)}+\frac{1}{(2k+3)(2k+5)} \text{ ..... [by (1)]}$$

$$=\frac{1}{2k+3}\left(\frac{k}{3}+\frac{1}{2k+5}\right)=\frac{1}{2k+3}.\frac{2k^2+5k+3}{3(2k+5)}$$

$$=\frac{(k+1)(2k+3)}{3(2k+3)(2k+5)}=\frac{k+1}{3(2k+5)}=R.H.S$$

There for P (k + 1) is true.
There for by the principle of mathematical induction, the result P(n) is true for all n $\in$ N.
That is $\frac{1}{3.5}+\frac{1}{5.7}+\frac{1}{7.9}+.....+\frac{1}{(2n+1)(2n+3)}=\frac{n}{3(2n+3)}$, for all n $\in$ N.

Example 15.

$$\frac{1}{3.4.5}+\frac{2}{4.5.6}+\frac{3}{5.6.7}+.....+\frac{n}{(n+2)(n+2)(n+3)}=\frac{n(n+1)}{6(n+3)(n+4)}$$

Solution:- The result P (n) to be proved is that for all n $\in$ N,

$$\frac{1}{3.4.5}+\frac{2}{4.5.6}+\frac{3}{5.6.7}+.....+\frac{n}{(n+2)(n+2)(n+3)}=\frac{n(n+1)}{6(n+3)(n+4)}$$

Step.1. for n = 1, L.H.S = $\frac{1}{3.4.5}$;

R.H.S = $=\frac{1(1+1)}{6(1.3)(1.4)}=\frac{1}{3.4.5}$

There for L.H.S = R.H.S for n=1 there for P(1) is true.

Step.2. Let us assume that for some k $\in$ N , P (k) is true,

That is

$$\frac{1}{3.4.5}+\frac{2}{4.5.6}+\frac{3}{5.6.7}+.....+\frac{k}{(k+2)(k+3)(k+4)}=\frac{k(k+1)}{6(k+3)(k+4)}$$

……. (I)

Then to prove that P (k + 1) is true,

That is to prove that

$$\frac{1}{3.4.5}+\frac{2}{4.5.6}+\frac{k}{(k+2)(k+3)(k+4)}+\frac{k}{(k+3)(k+4)(k+5)}=\frac{(k+1)(k+2)}{6(k+4)(k+5)}$$

Here L.H.S

$$=\left[\frac{1}{3.4.5}+\frac{1}{4.5.6}+\frac{k}{(k+2)(k+3)(k+4)}\right]+\frac{k+1}{(k+3)(k+4)(k+5)}$$

$$=\frac{k(k+1)}{6(k+3)(k+4)}+\frac{k+1}{(k+3)(k+4)(k+5)}$$ …… [by (1)]

$$=\frac{k+1}{(k+3)(k+4)}\left(\frac{k}{4}+\frac{1}{k+5}\right)$$

$$=\frac{(k+1)\left(k^2+5k+6\right)}{6(k+3)(k+4)(k+5)}$$

$$=\frac{(k+1)(k+2)(k+3)}{6(k+3)(k+4)(k+5)}=\frac{(k+1)(k+2)}{6(k+4)(k+5)}$$

$$=R.H.S$$

There for P (k + 1) is true.

There for by the principle of mathematical induction, the result P(n) is true for all n $\in$ N

That is,

$$\frac{1}{3.4.5}+\frac{2}{4.5.6}+\frac{3}{5.6.7}+.....+\frac{n}{(n+2)(n+2)(n+3)}=\frac{n(n+1)}{6(n+3)(n+4)}$$

For all n $\in$ N.

Example 15. Show that if P(n) given by 1.6 + 2.9 + 3.12 +…….+ n(3n + 3) = $n^3 + 3n^2$+2n+3 is true for n = k then it is true for n = k + 1. Is P(n) true for all n $\in$ N?

Solution:- Let us assume that P(k) is true.

Then 1.6 + 2.9 + 3.12 +……+ k(3k + 3)

$=k^3 + 3k^2 + 2k + 3$

Now we have to prove P(k + 1) is true.

There for to prove that

1.6 + 2.9 + 3.12 +……..+ k(3k + 3) + (k + 1)(3k + 6) = $(k + 1)^3$ + $3(k + 1)^2$ + 2(k + 1) + 3

L.H.S = [1.6 + 2.9 + 3.12 +…..…+ k(3k + 3)] + (k + 1)(3k + 6)

$=(k^3 + 3k^2 + 2k + 3) + 3k^2 + 9k + 6$

$=(k^3 + 3k^2 + 3k + 1) + 3(k^2 + 2k + 1) + 2(k + 1) + 3$

= $(k + 1)^3 + 3(k + 1)^2$+2(k + 1) + 3 = R.H.S

Hence if P (n) is true for n = k, it is also true for n = k + 1.

When n = 1, $n^3 + 3n^2 + 2n + 3 = 1 + 3 + 2 + 3 = 9$

Which is not the same as L.H.S = 1 (6) = 6.

There for P (n) is not true for n = 1.

Hence P (n) is not true for all n $\in$ N.

Example 16 Prove that a set containing n elements, n $\geq$ 1, has 2^n subsets.

Solution : We will prove the result by induction on the size of the set, n. Let P(n) denotes the statement : Number of subsets of a set containing n elements is 2^n. In this problem, n_0 = 1.

Basis step : Since the only subsets of a singleton set x = $\{x_1\}$ are $\varnothing$ and $\{x_1\}$, the formula is true for n = 1. **Induction step:** Suppose P(k), k $\geq$ 1, is true, i.e. any set with k elements has 2^k subsets, k $\geq$ 1. Let X = $\{x_1, x_2, ..., x_{k+1}\}$. Any subset S of X can be classified into two types : (A) $x_{k+1} \in S$; (B) $x_{k+1} \notin S$. We will count these subsets separately. If S is any subset of X of type (A) then S' = S $-\{x_{k+1}\}$ is a subset of X $-$ $\{x_{k+1}\}$ and vice-a-versa. Therefore number of subsets S of the set X of type (A) is same as number of subsets of a set X $-$ $\{x_{k+1}\}$. Since there are k elements in X$-\{x_{k+1}\}$, by induction there are 2^k subsets of X $-\{x_{k+1}\}$. Thus there are 2^k subsets of X of type (A). Any subset S of the set X of type (B) is a subset of X $-$ $\{x_{k+1}\}$ and vice-a-versa. By induction it follows that there are exactly 2^k subsets of X of type (B). Thus number of subsets of the set X containing k + 1 elements is $2^k + 2^k = 2^{k+1}$. The result now follows by the method of induction.

Example 17 Prove that $1+2^n < 3^n, n \geq 2$.

Solution : Let P(n) : $1+2^n < 3^n, n \geq 2$. In this case, $n_0 = 2$.

Basis step : Clearly, $1+2^2 = 5 < 3^2 = 9$, it follows that P(2) is true.

Induction step: Suppose P(k), k ≥ 2 is true. Thus we have $1+2^k < 3^k, k \geq 2$.

Now $1+2^{k+1} = 1+2\times 2^k = 2(1+2^k)-1 < 2(3^k)-1$, by induction. Clearly, $2(3^k)-1 = 3^k + (3^k - 1) < 3^k + 3^k = 3^{k+1}$. Thus P(k + 1) is true. By induction, the result is true for all integers greater than 1.

Example 18 (De Morgan's Laws) Let $A_1, A_2, ..., A_n$ be any n sets. Prove that

1. $$\overline{\left(\bigcap_{i=1}^{n} A_i\right)} = \bigcup_{i=1}^{n} \overline{A_i}, n \geq 1.$$

2. $$\overline{\left(\bigcup_{i=1}^{n} A_i\right)} = \bigcap_{i=1}^{n} \overline{A_i}, n \geq 1.$$

Solution : Let P(n) be the statement that equality holds in(1) for any n sets.

Basis step : The statement is true for n = 1.

Induction step : Suppose P(k) is true. Thus we have

$$\overline{\left(\bigcap_{i=1}^{k} A_i\right)} = \bigcup_{i=1}^{k} \overline{A_i}, n \geq 1.$$

The left-hand side of P(k + 1) is

$$\overline{\left(\bigcap_{i=1}^{k+1} A_i\right)} = \overline{A_1 \cap A_2 \cap ..... \cap A_k \cap A_{k+1}} = \overline{A \cap A_{k+1}}$$

where $A = A_1 \cap A_2 \cap ..... \cap A_k$. By De Morgan's laws for two sets, $\overline{A \cap A_{k+1}} = \overline{A} \cup \overline{A_{k+1}}$. By induction,

$$\overline{A} = \overline{A_1 \cap A_2 \cap ..... \cap A_k} = \overline{\bigcup_{i=1}^{k} A}:$$

Hence P(k + 1) is true. The result now follow by induction.

Example 19 Prove that $3 \mid (n^3 - n)$ for any natural number n.

Solution : Let P(n) denote the statement that $3 \mid (n^3 - n)$ for any natural number n.

Basis step : Clearly, $(1^3 - 1) = 0$ is divisible by 3, it follows that P(1) is true.

Induction step : Suppose $3 \mid (k^3 - k)$, $k \geq 1$, i.e.$(k^3 - k) = 3t$, for some integer t. Since $(k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - k - 1 = (k^3 - k) + 3(k^2 + k)$. By induction, the first term on the right is divisible by 3 and hence it follows that the right side is divisible by 3. We conclude the result by the principle of induction.

2.5 LET US SUM UP

We have learned logical connectives such as negation, conjunction, disjunction. We also have learned about quantifiers, conditional and bi-conditional statement. Finally we have learned a method of proof the principle of mathematical induction.

2.6 UNIT END EXERCISE

Prove the exercise number 1 to 8 by the principle of induction.

1. $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

2. $\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$

3. $\sum_{i=1}^{n} a.r^i = a.\frac{r^n - 1}{r - 1}, r \neq 1$

4. $\sum_{i=1}^{n} 2i = n(n+1), \sum_{i=1}^{n} (2i-1) = n^2$

5. $\sum_{i=1}^{n} (4i - 3) = (2n+1)(n-1)$

6. Prove that sum of first n terms of an arithmetic progression a, a + d, a +

2d, ……..+ [a(n − 1)d] is given by $\frac{n\left[2a+(n-1)d\right]}{2}$.

7. $\frac{1}{1.2}+\frac{1}{2.3}+\frac{1}{3.4}+.....+\frac{1}{n(n+1)}=\frac{n}{n+1}$.

8. $\frac{1}{2}+\frac{2}{2^2}+\frac{3}{2^2}+.....+\frac{n}{2^n}=2-\frac{n+2}{2^n}$.

9. Find a formula for $1^2+3^2+5^2+.....+(2n-1)^2$ and prove it by induction.

10. Prove that $\left(1+\frac{1}{2}\right)^n \geq 1+\frac{n}{2}$.

11. Prove that $n<2^n,\ n\geq 1$.

12. Let $A_1, A_2, ..., A_n$ and B be any sets. Prove by induction the following distributive properties

(a) $\left(\bigcap_{i=1}^{n} A_i\right)\bigcup B=\bigcap_{i=1}^{n}\left(A_i\bigcup B\right), n\geq 1.$

(b) $\left(\bigcup_{i=1}^{n} A_i\right)\bigcap B=\bigcup_{i=1}^{n}\left(A_i\bigcap B\right), n\geq 1.$

13. If A and B are two square matrices of order n such that AB = BA. Prove that $(AB)^n=A^nB^n,\ n\geq 1..$

14. (a) Prove that product of any two consecutive integers is divisible by 2.
(b) Prove that product of any three consecutive integers is divisible by 6.

3

RELATIONS AND IT'S PROPERTIES

Unit Structure

3.0 OBJECTIVES:

After going through this chapter you will be able to :

- Understand the concept and definition of product and partition of a set.
- Understand the different representation of a relation (set theoretical, pictorial and matrix representation).
- Understand the definition of a path in a relation and able to find paths of different length.
- Understand the different properties of binary relation.

3.1 INTRODUCTION:

In day today life we deal with relationships such as an employee and employee number, element and set, a person and his telephone number etc. In mathematics it's looked in more abstract sense such as division of integers, order property of Real numbers and so on. In computer science, a computer programme and variable, computer language and valid statement and so on Relations are useful in computer databases, networking etc.

3.2 PRODUCT SETS AND PARTITIONS:

3.2.1 Product sets

Definition:

Let A and B be two non empty sets. The product set or Cartesian product of A and B, (denoted by $A \times B$) is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$.

Thus, $A \times B = \{(a,b) / a \in A \text{ and } b \in B\}$

[**Note:** an order pair (a, b) is the ordered collection that has 'a' and 'b' in prescribed order, 'a' in first position and 'b' in second position.]

Examples:

(1) Let $A = \{1, 2, 3\}$ and $B = \{x, y\}$

then $A \times B = \{(1, x), (1, y), (2, x), (2, y), (3, x), (3, y)\}$

Similarly, $B \times A = \{(x,1), (y,1), (x, 2), (y, 2), (x, 3), (y, 3)\}$

(2) Let A be the set of all 2 divisions in X^{th} class in some school and B be the set of all 3 courses available.

i.e. $A = \{X, Y\}$, $B = \{C^{++}, \text{ Java, } VB\}$

then

$A \times B = \{(X, C^{++}), (X, \text{ Java}), (X, VB) (Y, C^{++}), (Y, \text{ Java}), (Y, VB)\}$

so there are total 6 categories possible.

Remark:

(1) $A \times B$ and $B \times A$ may or mayn't be equal.

(2) If A and B are finite sets then $|A \times B| = |A|.|B| = |B \times A|$

(3) An ordered pair (a_1, b_1) and (a_2, b_2) are equal iff $a_1 = a_2$ and $b_1 = b_2$.

(4) The idea of Cartesian product of two sets can be extended to 'n' number of sets $A_1, A_2, ..., A_n$, (it's denoted by $A_1 \times A_2 \times ... \times A_n$) and it's defined as, $A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ..., a_n) / a_1 \in A_1, a_2 \in A_2 ... \& \ a_n \in A_n\}$

[$(a_1, a_2, ..., a_n)$ is an ordered 'n' -tuple.]

3.2.2 Partitions

Definition:

A partition of a nonempty set A is a collection $p = \{A_1, A_2, ..., A_n\}$ of nonempty subsets of A such that

(1) $A_1 \cup A_2 \cup A_3 \cup ... \cup A_n = A$

(2) $A_i \cap A_j = \emptyset \ (1 \le i < j \le n)$

$A_1, A_2, A_3, ..., A_n$ are called as blocks or cells of the partition.

Example:

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

(a) Let $A_1 = \{1\}$, $A_2 = \{2, 3\}$ and $A_3 = \{4, 5\}$

Then we have, $A_1 \cup A_2 \cup A_3 = A$

& $A_1 \cap A_2 = \emptyset$, $A_1 \cap A_3 = \emptyset$, $A_2 \cap A_3 = \emptyset$

$\therefore P = \{A_1, A_2, A_3\}$ is a partition of 'A'

(b) Let $A_1 = \{1, 2\}$, $A_2 = \{3\}$, $A_3 = \{4\}$ and $A_4 = \{5\}$

then $P = \{A_1, A_2, A_3, A_4\}$ is a partition of A.

(c) Let $A_1 = \{1, 2\}$, $A_2 = \{2, 3\}$, $A_3 = \{4, 5\}$

then $P = \{A_1, A_2, A_3\}$ is not a partition of A

$\therefore A_1 \cap A_2 \neq \emptyset$

(d) Let $A = \mathbb{Z} =$ set of all 'integers'

E = set of all even integers and

O = set of all odd integers

We have, $E \cap O = \emptyset$ and $E \cup O = A$

$\therefore P = \{E, O\}$ is a partition of A.

Check your progress

1. List all partition of $A = \{a, b, d\}$.
2. Let $A = \{a, b, c, d, e, f, g, h\}$ and $A_1 = \{a\}, A_2 = \{b, c\}, A_3 = \{d, e, f\}$, $A_4 = \{g, h\}$ and $A_5 = \{f, g\}, A_6 = \{a, b, c\}$

   Which of the following are partition of A.

   (a) $\{A_1, A_2, A_3\}$ (b) $\{A_1, A_2, A_3, A_4\}$ (c) $\{A_3, A_4, A_5, A_6\}$

   (d) $\{A_3, A_6, A_4\}$
3. $A \times B = B \times A$ if (a) A is finite (b) A=B

   (c) B is finite
4. If $A = \{x, y, z\}$, $B = \{1, 2, 3\}$ and $C = \{a, b\}$ write down the set $A \times B \times C$.

3.3 RELATIONS AND DIAGRAPHS:

3.3.1 Definition and examples of Relation

Definition:

Let A and B be two non empty sets A relation R from A to B is a subset of $A \times B$.

If $(x, y) \in R$ then we write xRy and If $(x, y) \notin R$ then we write $x \not R y$.

Examples:

(1) Let $A = \{1, 2, 3\}$ & $B = \{x, y, z\}$ then $R = \{(1, x), (1, y), (2, z)\}$ is relation from A to B.

Note: If A=B then instead of saying a relation from A to B we will say a relation on A.

(2) Let $A = B = \{1, 2, 3, 4\}$, Let R be a relation on A defined as xRy iff x > y.

$\therefore R = \{(2,1), (3,1), (3, 2), (4,1), (4, 2), (4, 3)\}$

(3) Let $A = B = \mathbb{R} =$ The set of Real numbers.

Let R be a relation on A such that

xRy iff $x^2 + y^2 = 25$

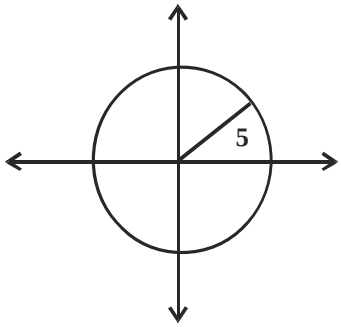


Fig. 3.1

$\therefore R = \left\{(x,\ y) / x^2 + y^2 = 25\right\}$

= The set of all points on the circle centre at origin with radius '5'

We can see, $(3,4) \in R \quad (\because 3^2 + 4^2 = 25)$

but $(3,\ 3) \notin R \quad (\because 3^2 + 3^2 = 18 \neq 25)$

(4) Let $A = \mathbb{N}$, Let 'R' be a relation on 'A' defined as xRy iff 'x' divides 'y'. $R = \{(1, 2), (2, 4), (5, 10), (2, 6), ...\}$

We have 1 R 2 but $2 \not R\ 1$.

3.3.2 Sets related to a relation

Let 'R' be relation from A to B.

Two important sets related to R are the Domain of 'R' [denoted by Dom (R)] and The Range of R [denote by Ran (R)].

We have, Dom (R)= $\{x / (x, y) \in R\} \subseteq A$ i.e. Dom (R) is a subset of 'A' containing first element of the pair (x, y) which belongs to 'R'. Similarly, Ran (R)= $\{y / (x, y) \in R\} \subseteq B$.

For Example:

(1) Let $A = \{1,\ 2,\ 3\}$ and $B = \{x, y\}$ $R = \{(1,\ x), (3,\ y)\}$

Dom (R)= $\{1, 3\} \subseteq A$ and Ran (R)= $\{x, y\} = B$

(2) Let A and B be only two sets and $R = A \times B$.

Then Dom (R) = A and Ran (R) =B

Check your progress

1. Write down the elements of R form $A=\{0,1,2,3\}$ to $B=\{1,2,3\}$, defined as $(a,b)\in R$ iff

   (a) a = b (b) a + b is an even number

   (c) a + b is a multiple of '3' (d) $a \geq b$

2. Find the domain and Range of the relations defined in Q.1.

3.3.3 The matrix of a Relation

A relation between two finite sets can be represented by a Boolean matrix (a matrix which is having entries as '0' or '1')

Let 'R' be a relation from $A=\{a_1, a_2, ..., a_m\}$ to $B=\{b_1, b_2, ..., b_n\}$. (Here the elements of A and B are listed in a particular order). Then relation 'R' can be represented by the *m* x *n* matrix $M_R=[mij]_{m\times n}$, which is defined as,

$$m_{ij}=\begin{cases}1 & \text{if } (a_i, b_j)\in R\\ 0 & \text{if } (a_i, b_j)\notin R\end{cases}$$

The matrix M_R is called as the matrix of a Relation 'R'

Examples:

(1) Let $A=\{1, 2, 3\}$ and $B=\{x, y\}$ and

$$R=\{(1,x),(2,x),(3,y),(1,y),(3,x)\}$$

$$\therefore M_R=\begin{bmatrix}1 & 1\\ 1 & 0\\ 1 & 1\end{bmatrix}_{3\times 2}$$

(2) Let $A=B=\{1, 2, 3, 4\}$

Let 'R' be a relation on 'A' defined as xRy iff $x\leq y$.

$$\therefore R=\{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,3),(3,4),(4,4)\}$$

$$\therefore M_R=\begin{bmatrix}1 & 1 & 1 & 1\\ 0 & 1 & 1 & 1\\ 0 & 0 & 1 & 1\\ 0 & 0 & 0 & 1\end{bmatrix}_{4\times 4}$$

Note: Converse process is also possible i.e. given a matrix with enteries '0' or '1' we can write 'R' related to that matrix.

3.3.4 The Diagraph of a Relation

Just we saw that a relation on finite set 'A' can be represented by a binary matrix. Similarly there is another way of representing a relation using a pictorial representation. Pictorial representation of 'R' is as follows, Draw a small circle for each element of A and label the circle with the corresponding elements of A, (these circles are called as vertices) draw an arrow from vertex a_i to a_j iff a_i R a_j. (these arrows are called as edges)

The resulting pictorial representation is called as Directed graph or diagraph of 'R'.

For example:

(1) Let $A = B = \{1, 2, 3, 4\}$ and $R = \{(1,1), (1, 2), (2, 3), (3, 4), (2, 4), (3,1)\}$

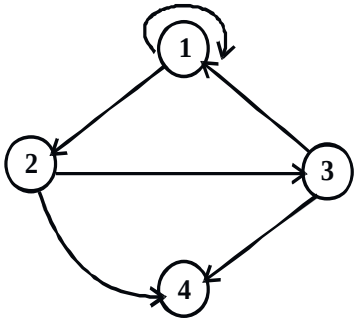


Fig. 3.2

Note:

(1) An edge of the form (a, a) is represented using an arc from the vertex 'a' back to it self. Such an edge is called a loop.

(2) Conversely diagraph can be used to find underlying relation represented by it.

(3) There are two important definitions arising from the diagraph.

(i) In-degree of a vertex = no. of arrows coming towards that vertex and

(ii) Out-degree of a vertex = no. of arrows going away from that vertex

For example (1) for below diagraph

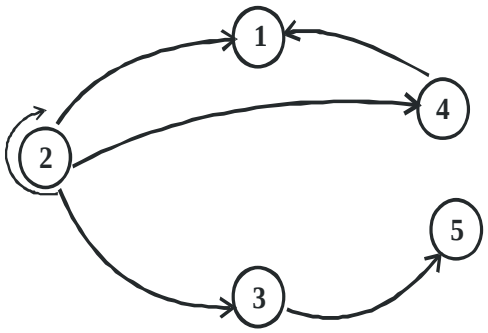


Fig. 3.3

	1	2	3	4	5
In-degree	2	1	1	1	1
Out-degree	0	4	1	1	0

Check your progress

1. Write down the matrix M_R and draw the diagraph for following relations.

   (a) $A = B = \{1, 2, 3, 4\}$, R is such that xRy iff $x \mid y$.

   (b) $A = B = \{1, 2, 3, 4\}$, 'R' is such that xRy iff $x + y \leq 5$

   (c) $A = B = \{1, 2, 4, 6\}$, 'R' is such that xRy iff $x + y$ is a multiple of '2'

2. Write down In-degree and out-degree for each of the vertices in example (1).

3. Let $A = \mathbb{R}$, Give a description of the relation 'R' specified by the shaded region shown below

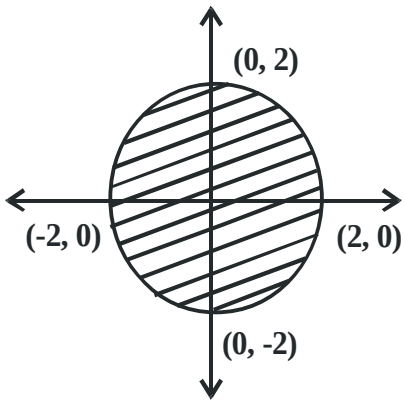


Fig.3.4

3.4 PATHS IN RELATIONS and DIAGRAPHS:

Let A be a given set and let 'R' be a relation on 'A'. A path of length m in R from 'a' to 'b' is a finite sequence. $\pi : a = x_0,\ x_1,\ x_2,\ x_3, ..., x_{m-1},\ x_m = b,$ starting from 'a' and ending to 'b' such that $aRx_1,\ x_1 Rx_2,\ x_2 Rx_3, ..., x_{m-1} R\ b.$

Note: Length of a path is nothing but the number of arrows involved in a path.

For example:

(1) Consider the following diagraph,

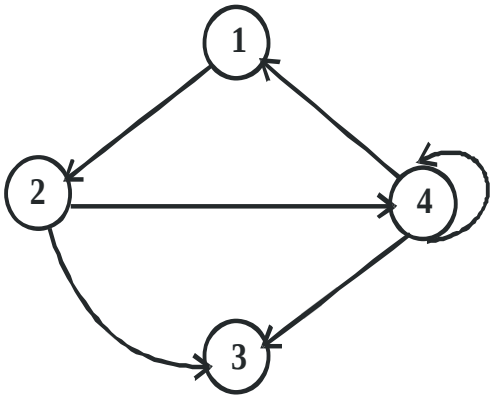


Fig. 3.5

$\pi_1 : 1,\ 2, 4$ is a path of length '2'

$\pi_2 : 1, 2, 4, 1$ is a path of length '3'

$\pi_3 : 4, 4, 3$ is a path of length '2'

$\pi_4 : 4, 4$ is a path of length '1'

Note: a path like $\pi_2 \& \pi_4$ are called as cycles, a cycle is a path which is having same starting and ending vertex.

3.4.1 Paths in a relation 'R' can be used to define new relations.

From above example, It can be seen that paths of length 1 can be identified with the elements of R and vice versa. So 'R' can be replaced by R^1 where '1' stands for set of all order pairs (x, y) for which there exist a path of length 1 from x to y. on similar lines now we can define $R^2,\ R^3, ..., R^n\ (n \in \mathbb{N})$

$R^2 = \{(x,\ y) / \text{if a path of length '2' from 'x' to 'y'}\}.$

$\vdots \qquad\qquad \vdots$

$R^n = \{(x,\ y) / \text{if a path of length 'n' from 'x' to 'y'}\}.$

$\vdots \qquad\qquad \vdots$

Now we may define R^∞ as,

$R^\infty = \{(x,\ y) / \text{if some path from 'x' to 'y'}\}.$

i.e. $\boxed{R^\infty = \bigcup_{i=1}^{\infty} R^i}$

For example:

(1) Consider the following diagraph.

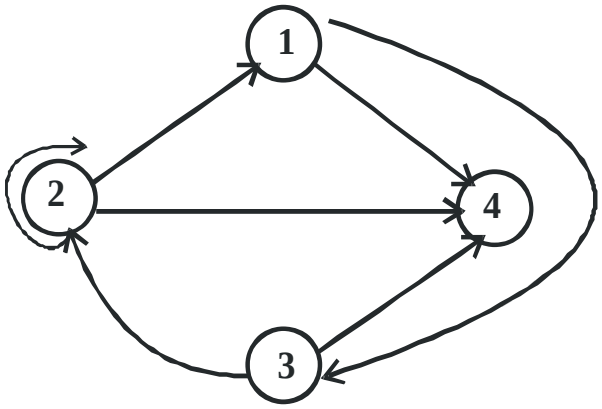


Fig. 3.6

So, $R^1 = \{(2,2), (2,1), (2,4), (3,2), (3,4), (1,4), (1,3)\}$

Now for R^2, we have to find all Paths of length '2'

$\pi_1 : 2, 2, 2 \qquad \pi_2 : 2, 2, 1 \qquad \pi_3 : 2, 2, 4$

$\pi_4 : 3, 2, 2 \qquad \pi_5 : 3, 2, 4 \qquad \pi_6 : 3, 2, 1$

$\pi_7 : 1, 3, 2 \qquad \pi_8 : 1, 3, 4 \qquad \pi_9 : 2, 1, 3$

i.e. $R^2 = \{(2,2,), (2,1), (2,4), (3,2), (3,4), (3,1), (2,3), (1,2), (1,4)\}$

similarly we can find R^3, R^4 and so on.

(2) Consider the diagraph,

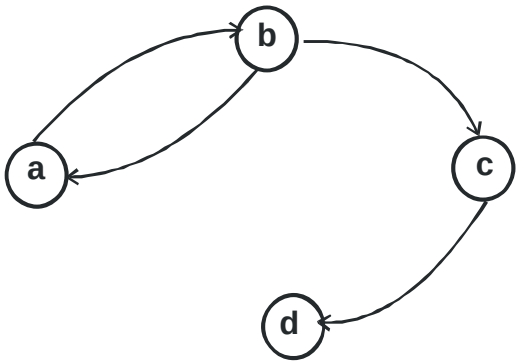


Fig. 3.7

Then, $R^1 = \{(a,b),(b,a),(b,c),(c,d)\}$

$R^2 = \{(a,a),(a,c),(b,b),(b,d)\}$

$R^3 = \{(a,b),(a,d),(b,a),(b,c)\}$

$\vdots \qquad\qquad \vdots$

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

Note: Since 'n' is finite the process of finding $R^1, R^2, R^3, \ldots$ will stop after some finite 'n'.

In fact we can prove that, $R^\infty = R^1 \cup R^2 \cup R^3 \cup \ldots\ldots \cup R^n$, where 'n' is number of elements in the given set 'A'.

3.4.2 Matrix version

If $|R|$ is large, it would be tedious to compute R^∞, or even R^2, R^3 etc. from the set representation of R so we have following matrix version of above concepts.

First we will see some different operations defined on Boolean matrices.

Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be two m x n Boolean matrices.

(1) we define $A \vee B = C = [C_{ij}]$, the join of A and B by,

$$C_{ij} = \begin{cases} 1 & \text{if } a_{ij} = 1 \text{ or } b_{ij} = 1 \\ 0 & \text{if } a_{ij} \text{ \& } b_{ij} \text{ both are } 0 \end{cases}$$

(2) We define $A \wedge B = E = [e_{ij}]$, the meet of A and B

$$e_{ij} = \begin{cases} 1 & \text{if } a_{ij} = 1 \& b_{ij} = 1 \\ 0 & \text{if } a_{ij} = 0 \text{ or } b_{ij} = 0 \end{cases}$$

(3) Let $A = \left[a_{ij}\right]_{m\times p}$ and $B = \left[b_{ij}\right]_{p\times n}$ be two Boolean matrices.

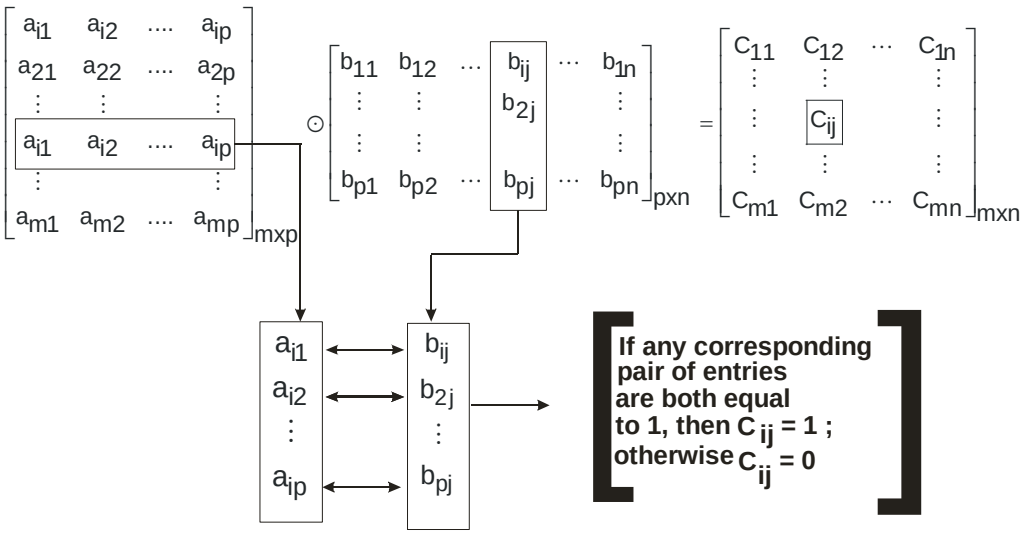
Then Boolean product of A and B, (denoted by $A \odot B$) is the $m \times n$ Boolean matrix $C = [C_{ij}]$ defined by

$$C_{ij} = \begin{cases} 1 & \text{if } a_{ik} = 1 \text{ and } b_{kj} = 1 \text{ for some k, } 1 \le k \le p \\ 0 & \text{otherwise} \end{cases}$$

for eg: Let $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}_{3\times 3}$ & $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}_{3\times 2}$

$$\therefore A \odot B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}_{3\times 2}$$

Note:



We can prove that $\boxed{M_{R^2} = M_R \odot M_R}$ i.e. matrix related with R^2 is nothing but the Boolean product of M_R with M_R similarly. $\boxed{M_{R^n} = M_R \odot M_R \odot .... \odot M_R}$ ('n' times)

For example

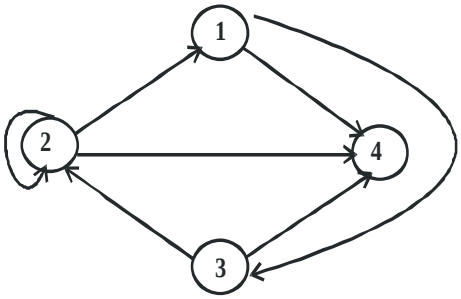


Fig. 3.8

as we saw, $R^2 = \{(2,1), (2,2), (2,4), (3,2), (3,4), (3,1), (1,2), (2,3), (1,4)\}$

$$\therefore M_{R^2} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}_{4\times4} \quad \text{and} \quad M_R = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}_{4\times4}$$

Now let's compute, $M_R \odot M_R = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \odot \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

$$= \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \text{ which is nothing but } M_{R^2}$$

i.e. $M_{R^2} = M_R \odot M_R$ is verified.

Notation: $M_R \odot M_R$ is denoted by $(M_R)^2_{\odot}$

Similarly, $\underbrace{M_R \odot M_R \ldots \odot M_R}_{\text{'n' times}} = (M_R)^n_{\odot}$

i.e. $M_{R^n} = (M_R)^n_{\odot}$, $n \geq 2$

Now, we know that, $R^{\infty} = \bigcup_{i=1}^{\infty} R^i$

i.e. $R^{\infty} = R^1 \cup R^2 \cup R^3 \cup R^4 \cup \ldots$

we can check that If R and S are two relations then $M_{R \cup S} = M_R \vee M_S$.

if we extend this idea we have,

$$M_{R^{\infty}} = M_{R^1} \vee M_{R^2} \vee M_{R^3} \vee M_{R^4} \vee \ldots$$

i.e. $M_{R^{\infty}} = M_{R^1} \vee (M_R)^2_{\odot} \vee (M_R)^3_{\odot} \vee (M_R)^4_{\odot} \vee \ldots$

thus, we got another way of calculating $M_{R^2}, M_{R^3}, \ldots, M_{R^n}, \ldots, M_{R^{\infty}}$ and which in turn gives the sets $R^2, R^3, \ldots, R^n, \ldots, R^{\infty}$.

Check your progress

1. Consider the following diagraph and answer following

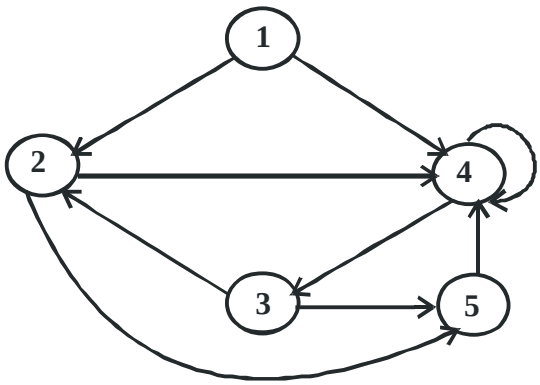


Fig. 3.9

(a) List all paths of length '2'

(b) List of all paths of length '2' starting from '3'

(c) List all cycles

(d) All cycles starting at '1'

2. For example (1) find M_{R^2} and M_{R^3} ?

3. Prove that if R and S are two relations then $M_{R \cup S} = M_R \vee M_S$

3.5 PROPERTIES OF RELATIONS:

3.5.1 Reflexive and Irreflexive Relations

A relation on set 'A' is reflexive if $(x, x) \in R \; \forall \; x \in A$ [or $xRx \; \forall \; x \in A$]

A relation on set 'A' is irreflexive if $(x, x) \notin R \; \forall \; x \in A$ [or $x \not R x \; \forall \; x \in A$]

For e.g. (1) Let $A = \{1, 2, 3, 4\}$ with Relations R,S,T on A.

If $R = \{(1,1), (1, 2), (2, 2), (3, 3), (4, 4), (4, 2)\}$ then 'R' is reflexive.

If $S = \{(1,1), (2,1), (3, 3), (4, 3), (4, 4)\}$ then 'S' is not reflexive. $(\because 2 \not R 2)$ and also 'S' is not irreflexive. $(\because (3,3) \in R \text{ or } (2,2) \in R)$. if $T = \{(1, 2), (2, 3), (3,1)\}$ then T is irreflexive.

Note:

(1) $\Delta = \{(x, x) / x \in A\}$ is called as an equality relation on 'A'.

(2) 'R' is reflexive iff $\Delta \subseteq R$.

(3) 'R' is irreflexive iff $\Delta \cap R = \emptyset$

(4) If $R = \emptyset$, an empty relation then 'R' is not reflexive since $(x, x) \notin R \; \forall \; x \in A$. However, R is irreflexive.

(5) Let 'R' be a reflexive relation on set 'A' then matrix of relation M_R must have diagonal elements as 1.

(6) If 'R' is irreflexive then M_R must have diagonal elements as zero's.

3.5.2 Symmetric, Asymmetric and Antisymmetric relations

(1) A relation on set 'A' is symmetric if whenever $(a, b) \in R$, then $(b, a) \in R$.

(2) A relation on set 'A' is asymmetric if whenever $(a, b) \in R$, then $(b, a) \notin R$.

(3) A relation on set A is antisymmetric if whenever $(a, b) \in R$, & $(b, a) \in R$ then a = b.

For Examples:

(1) Let $A = \mathbb{N}$, 'R' be a relation on 'A' such that xRy iff 'x' divides 'y'.

(a) If xRy (i.e. 'x' divides 'y')

then yRx or $y \not R x$

($\because$ 'y' may or mayn't divide 'x')

For eg: 2 R8 (as 2|8) but $8 \not R 2$ ($\because 8 \times 2$)

$\therefore$ R isn't asymmetric

(b) If a = b = 2 then aRb as well as bRa

$\therefore$ R is not asymmetric

(c) If 'a' and 'b' are such that a/b and b/a

A / b and b / a gives a = b

$\therefore$ R is antisymmetric

(2) Let A = set of all lines in a xy-plane.

(a) If ℓ and m are in A such that ℓ R m then

m R ℓ ($\because \ell$ R m $\Rightarrow \ell \,||\, m \Rightarrow m \,||\, \ell \Rightarrow$ m R ℓ)

$\therefore$ R is symmetric

(b) R is not asymmetric as ℓ R m $\Rightarrow$ mR ℓ

(c) R is not antisymmetric as we can have 2 distinct lines | | to each other butn't equal.

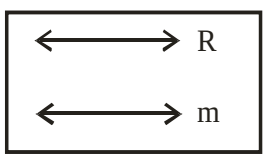


Fig. 3.10

(3) Let $A = \mathbb{N}$, 'R' is a relation such that x R y iff x < y then R is not symmetric but R is asymmetric. ($\because$ x R y $\Rightarrow$ x < y

$\Rightarrow y \not< x$

$\Rightarrow y \not R\ x$)

Notes:

1) The matrix M_R of a symmetric relation satisfies the property that $M_R = M_R^t$ i.e. if $m_{ij} = 1$ then $m_{ji} = 1$ and if $m_{ij} = 0$ then $m_{ji} = 0$

2) The matrix M_R of an asymmetric relation satisfies the property if $m_{ij} = 1$ then $m_{ji} = 0$ and $m_{ii} = 0\ \forall$ i (i.e. diagonal elements are zero)

3) Relation 'R' is antisymmetric means x R y and y R x $\Rightarrow x = y$ contrapositive of this statement is, if $x \neq y \Rightarrow x \not R y$ or $y \not R x$

   i.e. M_R of antisymmetric relation satisfied the property that if $i \neq j$, then $M_{ij} = 0$ or $M_{ji} = 0$

   Similarly for diagraphs we have,

4) The diagraph of symmetric relation has the property that if there an edge from i to j, then there is an edge from j to i.

5) If R is an asymmetric relation, then if there an edge from i to j so there can't be any edge from j to i and there can't be any cycle of length '1'.

6) If 'R' is an antisymmetric relation, then for different i and j there can not be an edge from vertex 'i' to vertex 'j' and an edge from vertex 'j' to vertex 'i'. (we can't say anything if i = j)

3.5.3 Transitive Relations

A relation 'R' on set 'A' is said to be transitive if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$.

[i.e. if xRy and yRz $\Rightarrow$ xRz]

For Example:

(1) Let $A = \{1, 2, 3, 4\}$ and let $R = \{(1,1), (1, 2), (2, 2), (2, 4), (1, 4)\}$ and $S = \{(3, 2), (2,1), (1, 4), (4, 2), (1, 2)\}$ then we can check 'R' is transitive but 'S' is not. [$\because (3, 2)$ & $(2,1) \in S$ but $(3,1) \notin S$]

(2) Let $A = \mathbb{N}$ & Let 'R' be a relation $\leq$. Then, if xRy and yRz i.e. $x \leq y$ & $y \leq z$

We have $x \leq y \leq z \Rightarrow xRz$

$\therefore$ R is transitive.

Notes:

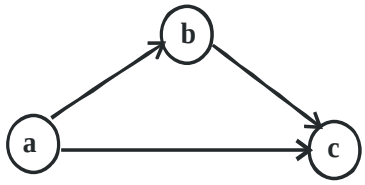
(1) A matrix M_R of relation 'R' has the property, if $m_{ij} = 1$ & $m_{jk} = 1$

Then $m_{ik} = 1$

(2) from above point (1) we can see that if $(M_R)^2_{\odot} = m_R$ then R is transitive but converse is not true.

(3) If there is a path of length '2' from 'a' to 'c' then there has to be a path of length '1' from 'a' to 'c' inorder to have 'R' transitive.

i.e. if (a, c) $\in R^2$ then $(a, c) \in R$



i.e. $R^2 \subseteq R$

$\therefore$ R is transitive iff $R^2 \subseteq R$ **Fig. 3.11**

(4) more generally we have,

'R' is transitive iff $R^n \subseteq R \quad \forall\ n \geq 1$

Check your progress

1. Determine whether the following relation is reflexive, irreflexive, symmetric, asymmetric, antisymmetric or transitive.

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

(a) $R_1 = \{(1,1), (2, 2)\}$

(b) $R_2 = \{(1,1), (2, 3), (3, 2), (2, 2)\}$

(c) $R_3 = \{(2, 3), (3, 2), (2, 2), (3, 4), (4, 3), (3, 3), (4, 4)\}$

(d) $R_4 = \{(2, 3), (3, 2), (1, 4), (4, 2), (1, 2)\}$

2. Determine whether the relation 'R' on the set $A = \{1, 2, 3\}$ whose matrix M_R and Diagraph are given is reflexive, irreflexive, symmetric, asymmetric, antisymmertic or transitive.

(a) $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$

(b)

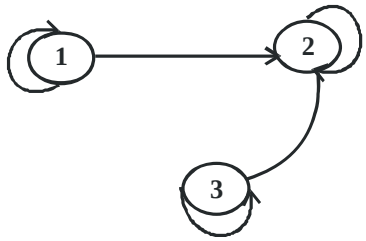


Fig. 3.12

(c) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$

(d)

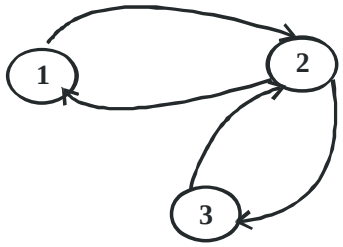


Fig. 3.13

3.6 LET US SUM UP

We started the definition of product sets which is useful in defining relation from one set to other. Then we saw different ways of representing a relation. Which is useful in understanding the concepts in more better way. Then we saw very important definition of a path in a relation and then concepts of paths of different length and then finally matrix version of it. At the end we saw different properties of a relation which is useful in coming chapters.

3.7 REFERENCES FOR FURTHER READING:

(1) Discrete structures by B. Kolman HC Busloy, S Ross PHI Pvt. Ltd.

(2) Discrete mathematics and its application, Keneth H. Rosen TMG.

(3) Discrete structures by Liu.

3.8 UNIT END EXERCISES:

1. Find R^{∞} for the relation 'R' whose diagraph is

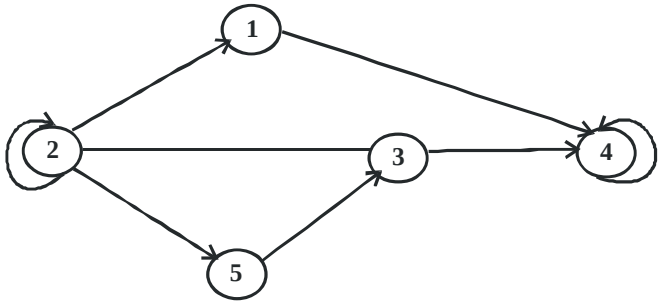


Fig. 3.14

Q.2 Calculate M_{R^4} for a relation $R = \{(1,1), (3,2), (1,4), (2,4)\}$ on set $A = \{1, 2, 3, 4\}$

Q.3 Determine whether following relations are reflexive, irreflexive, symmetric, asymmetric, antisymmetric or transitive.

(a) $A = \mathbb{Z}$, x R y iff x + y is an even number.

(b) $A = \mathbb{R}$, x R y iff $x^2 + y^2 = 9$

(c) $A = \mathbb{N}$, x R y iff $x \leq y$

(d) $A = \mathbb{Z}$, x R y iff $(x - y) \leq 3$

Q.4 Define a relation on $A = \{1, 2, 3, 4\}$ that is

(a) Reflexive butn't symmetric

(b) Transitive butn't reflexive

(c) Antisymmetric and reflexive

(d) irreflexive and transitive

Q.5 Prove that if 'R' is symmetric then R^2 is also symmetric.

4

EQUIVALENCE RELATION AND CLOSURES

Unit Structure

4.0 OBJECTIVES :

After going through this chapter, students will be able to

- Understand the definition of an equivalence relation and able to identify an equivalence relation
- Find the Partition produce by an equivalence relation and vice versa.
- Understand different operations that can be performed on different relations which is useful in finding the closures of a relation.
- Use Warshall's algorithm to find transitive closure.

4.1 INTRODUCTION :

We have already seen the concept of reflexive, symmetric and transitive etc. If a relation is not transitive then it doesn't contain all the pairs that can be linked so we want to make it transitive by adding the remaining pairs with the property that resulting set is smallest set containing given relation. Such a set is called as transitive closure. Also we will see important concept of composition of relations and computer representation of relation and diagraph.

4.2 EQUIVALENCE RELATIONS

4.2.1 Definition :

Let 'R' be a relation on 'A', 'R' is said to be an equivalence relation on A iff 'R' is reflexive, symmetric and transitive.

Examples :

(1) Let A = {1, 2, 3} and R = {(2, 2), (1, 2), (2, 1), (1, 1), (3, 3)} then it's easy to check 'R' is an equivalence relation.

(2) Let A = $\mathbb{N}$ and 'R' be a relation on 'A' such that x R y iff $x+y$ is an even number.

To check whether 'R' is an equivalence relation or not.

(a) Let $x \in A$,

$\therefore\ x + x = 2x = \text{even}$

$\therefore\ x\ R\ x\ \forall x \in A$

$\therefore$ R is reflexive.

(b) Let $x, y \in A$ such that $x\ R\ y$ i.e. $x + y = \text{even}$ i.e. $x + y = 2p,\ p \in \mathbb{N}$

Consider, $y + x = x + y = 2p = \text{even}$

$\therefore\ y + x$ is also an even number.

$\therefore\ y\ R\ x$

$\therefore$ R is symmetric.

(c) Let $x, y, z \in A$ such that $x\ R\ y \Rightarrow x + y = 2p,\ p \in \mathbb{N}$ ---------- (1)

and $y\ R\ z \Rightarrow y + z = 2q,\ q \in \mathbb{N}$ ---------- (2)

(1) + (2) $\Rightarrow$ $x+2y+z=2p+2q$

$\therefore$ $x+z=2p+2q-2y$

$\therefore$ $x+z=2(p+q-y)$

i.e. $x+z=$ even number

$\therefore$ $x\,R\,z$

$\therefore$ R is transitive.

and hence R is an equivalence relation.

(3) Let A = $\mathbb{Z}$ and 'R' be a relation on 'A' such that $x\,R\,y$ iff 'x' divides 'y'. We have 3/6 but 6 X 3.

i.e. 3 R 6 but $6 \not R 3$.

$\therefore$ 'R; isn't symmetric,

$\therefore$ 'R' isn't an equivalence relation.

4.2.2 Equivalence Relation and Partition

Using an equivalence relation we can produce a partition and vice versa. Let 'R' be a given equivalence relation on set 'A'.

Let $a \in A$

We define a set which is equal to $\{x / x\,R\,a,\ x \in A\}$ is called as an equivalence class of 'a'. i.e. [a] = $\{x / x\,R\,a,\ x \in A\}$.

For example,

(1) Let A = {1, 2, 3, 4} and R = {(1, 1), (1, 2), (2, 1), (2, 3), (3, 2), (2, 2), (4, 4), (1, 3), (3, 1), (3, 3)}

Then, [1] = $\{x / x\,R\,1\} = \{1, 2, 3\}$

[2] = {1, 2, 3} and [4] = {4}

Theorem :-

Let 'R' be an equivalence relation on 'A'. Then we have following properties –

(i) $A = \bigcup_{a \in A} [a]$

(ii) Any two equivalence classes are equal or disjoint.

Proof :-

(i) T.P.T. $A = \bigcup_{a \in A} [a]$

[a] = $\{x / x\, R\, a,\ x \in A\} \subseteq A$

$\therefore \bigcup_{a \in A} [a] \subseteq A$ … (1)

Now, let $x \in A$ t.p.t. $x \in \bigcup_{a \in A} [a]$

$\because x \in A \therefore x\, R\, x$ ($\because$ R is reflexive)

$\therefore x \in [x] \subseteq \bigcup_{a \in A} [a]$

$\therefore x \in \bigcup_{a \in A} [a]$ … (2)

By (1) and (2), $A = \bigcup_{a \in A} [a]$

(ii) Let a, b $\in$ A, t.p.t. [a] $\cap$ [b] = $\emptyset$ or [a] = [b]
If [a] and [b] are disjoint then done. So let's consider
[a] $\cap$ [b] $\neq \emptyset$

Let $w \in [a] \cap [b]$

$\Rightarrow w \in [a]$ & $w \in [b]$

$\Rightarrow w\, R\, a$ and $w\, R\, b$

$\Rightarrow a\, R\, w$ and $w\, R\, b$ ($\because$ R is symmetric)

$\Rightarrow a \in [b]$ (by definition)

$\Rightarrow [a] \subseteq [b]$ ($\because a \in [b]$ $\therefore$ a R b and hence every element of [a] is related to b)

Similarly, we can prove, $[b] \subseteq [a]$

$\therefore$ [a] = [b]

$\therefore$ Two equivalence classes are either disjoint or equal. So, from above theorem we can say $p = \{[a] / a \in A\}$ form a Partition of set A.

Note : Above p is denoted as A/R.

Example –

(1) Let A = {1, 2, 3, 4} and R = {(1,1), (1,3), (3,1), (2,2), (4,4)}

[1] = {1, 3}, [2] = {2}, [4] = {4}

$\therefore$ p = {[1], [2], [4]} is a Partition of 'A'.

We can reverse the above Process, i.e. given a Partition we can produce an equivalence relation on a given set. Let 'A' be a given set and let p be a partition of A. define a relation on set 'A' as, x R y iff 'x' and 'y' belongs to same block or cell of the given partition.

T.P.T. R is an equivalence relation.

(a) If $x \in$ A, then it's very obvious x belongs to same block.

$\therefore$ x R x, $\forall x \in$ A

$\therefore$ R is reflexive.

(b) If $x, y \in$ A such that, x R y $\Rightarrow$ x & y belongs to same block

$\Rightarrow$ y & x belongs to same block

$\Rightarrow$ y R x

$\therefore$ R is symmetric.

(c) If $x, y, w \in$ A such that,

$(x$ R y$)$ & $($y R w$) \Rightarrow$ (x and y belongs to same block)

and (y and w belongs to same lock)

$\Rightarrow$ x and w belongs to same block

$\Rightarrow$ x R w

$\therefore$ R is transitive

$\therefore$ R is an equivalence relation.

For example,

(1) Let A = {1, 2, 3, 4} and partition p = {{1}, {2, 3}, {4}}

$\therefore$ R = {(1, 1), (2, 2), (2, 3), (3, 2), (3, 3), (4, 4)}

Check your progress

1. Let A = $\{1, 2, 3, 4, 5, 6, 7, 8\}$ and p = $\{\{1\}, \{2, 3\}, \{4\}, \{5, 6, 7\}, \{8\}\}$ be a partition of A. Find corresponding equivalence relation.

2. Let A = $\{ 1, 2, 3, 4, 5 \}$ and R = $\{(1,1), (2, 2), (1, 2), (2,1), (3,3), (4,4), (3,4), (4,3), (5,5)\}$ be an equivalence relation on 'A'. Find the corresponding Partition.

4.3 OPERATIONS ON RELATIONS :

Let 'R' and 's' be two relations from set 'A' to set 'B'. We have following operations defined on Relations.

(1) Complementary relation of 'R' (denoted as $\overline{R}$)

$\overline{R} = \{(x, y) / (x, y) \notin R\}$

(2) Inverse of a relation 'R' (denoted as R^{-1})

$R^{-1} = \{(x, y) / (y, x) \in R\}$

For example,

(1) Let $A = \{1, 2, 3\}$ and $R = \{(2, 2), (1, 3), (2, 3), (3, 3)\}$

$\overline{R} = \{(1,1), (1, 2), (2,1), (3,1), (3, 2)\}$ and

$R^{-1} = \{(2, 2), (3,1), (3, 2), (3, 3)\}$

(3) $R \cup S = \{(x, y) / (x, y) \in R \text{ or } (x, y) \in S\}$

(4) $R \cap S = \{(x, y) / (x, y) \in R \ \& \ (x, y) \in S\}$

For example,

(1) Let $A = \{1, 2, 3, 4\}$ and $R = \{(1, 2), (1,1), (2, 4), (3, 2)\}$ and

$S = \{(2, 2), (1,1), (3, 2), (3, 4)\}$

$\therefore R \cup S = \{(1,1), (1, 2), (2, 2), (3, 2), (3, 4), (2, 4)\}$ and

$R \cap S = \{(3, 2), (1,1)\}$

Note :-

(1) $M_{R \cup S} = M_R \vee M_S$

$M_{R \cap S} = M_R \wedge M_S$

$M_R{}^{-1} = (M_R)^T$

$M_{\overline{R}} = \overline{M}_R$

[$\overline{M}_R$ complement is a matrix obtained by replacing every '1' by '0' and every '0' by '1'.]

Theorem : Suppose ‘R’ and ‘S’ are relations from ‘A’ to ‘B’

(a) If $R \subseteq S$, then $R^{-1} \subseteq S^{-1}$

(b) If $R \subseteq S$, then $\bar{S} \subseteq \bar{R}$

(c) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$ and $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$

(d) $\overline{R \cap S} = \bar{R} \cup \bar{S}$ and $\overline{R \cup S} = \bar{R} \cap \bar{S}$

(e) R is reflexive iff $\bar{R}$ is irreflexive.

(f) R is symmetric iff $R = R^{-1}$

(g) R is antisymmetric iff $R \cap R^{-1} \subseteq \Delta$

(h) R is asymmetric iff $R \cap R^{-1} \subseteq \emptyset$

(i) $(R \cap S)^2 \subseteq R^2 \cap S^2$

Proof :

(a) Let $(x, y) \in R^{-1}$

$\Rightarrow (y, x) \in R \subseteq S$

$\Rightarrow (x, y) \in S^{-1}$

$\Rightarrow R^{-1} \subseteq S^{-1}$

(b) Let $(x, y) \in \bar{S}$

$\Rightarrow (x, y) \notin S$

$\Rightarrow (x, y) \notin R \quad (\because R \subseteq S)$

$\Rightarrow (x, y) \notin \bar{R}$

$\Rightarrow \bar{S} \subseteq \bar{R}$

(c) $(R \cap S)^{-1} = \{(x, y) / (y, x) \in R \cap S\}$

$= \{(x, y) / (y, x) \in R \text{ and } (y, x) \in S\}$

$= \{(x, y) / (x, y) \in R^{-1} \text{ and } (x, y) \in S^{-1}\}$

$= R^{-1} \cap S^{-1}$

Similarly, other one.

(d) $\overline{R \cap S} = \{(x, y) / (x, y) \notin R \cap S\}$

$= \{(x, y) / (x, y) \notin R \text{ or } (x, y) \notin S\}$

$= \{(x, y) / (x, y) \notin \overline{R} \text{ or } (x, y) \notin \overline{S}\}$

$= \{(x, y) / (x, y) \in \overline{R} \cup \overline{S}\}$

$= \overline{R} \cup \overline{S}$

(e), (f), (g) and (h) are easy to check

(i) Let $(x, y) \in (R \cap S)^2$ means w such that $x(R \cap S)w$ and $w(R \cap S)y$

$x(R \cap S)w \Rightarrow (x, w) \in R \cap S$ and

$w(R \cap S)y \Rightarrow (w, y) \in R \cap S$

i.e. (x, w) *and* $(w, y) \in R$ *and* (x, w) *and* $(w, y) \in S$

$\Rightarrow (x, y) \in R^2$ *and* $(x, y) \in S^2$

$\Rightarrow (x, y) \in R^2 \cap S^2$

$\therefore (R \cap S)^2 \subseteq R^2 \cap S^2$

Check your progress

1. Verify $M_{R \cup S} = M_R \vee M_S$, $M_{R \cap S} = M_R \wedge M_S$, $M_R{}^{-1} = (M_R)^T$, $M_{\overline{R}} = \overline{M}_R$ for relations.

   R = {(1, 1), (1, 2), (2, 4), (3, 2)} and S = {(2, 2), (2, 4), (1,1), (4, 3)} on set A = {1, 2, 3, 4}

2. Compute $R \cup S$, $R \cap S$, $\overline{R}$, $\overline{S}$, R^{-1}, S^{-1} for R = {(1, 2), (2, 2), (3, 2)} and S = {(1, 3), (2, 3), (3, 3), (2, 1)} on set A = {1, 2, 3}.

4.4 CLOSURES

If ‘R’ is some relation on ‘A’ that doesn’t have some important relational properties like reflexivity, symmetry and transitivity. It’s natural to ask a question like can we make it reflexive, symmetric and transitive by adding some pair in it and we

want to add as few new pairs as possible, so we want to find smallest relation that contains given relation and posses the property we desire. Such a smallest relation is called as closures of a given relation.

4.4.1 Reflexive and Symmetric closures

Reflexive closure :-

Let 'R' be a given relation on 'A'. Then reflexive closure of 'R' is the smallest reflexive relation containing 'R' and it's denoted by R^r.

Note : (1) If R itself is reflexive then $R^r = R$

(2) $R^r = R \cup \Delta$

For example,

(1) Let A = {1, 2, 3} and R = {(1, 1), (1, 3), (2, 3), (3, 1)}

$\therefore R^r = \{(1,1), (1,3), (2,3), (3,1), (2,2), (3,3)\}$

Symmetric closure :-

Let 'R' be a given relation on set 'A'. Then symmetric closure of 'R' is the smallest symmetric relation containing 'R' and it's denoted by R^s.

Note : (1) If R itself is symmetric then $R^s = R$

(2) $R^s = R \cup R^{-1}$

For example,

(1) If $A = \{x, y, z\}$ and $R = \{(x, x), (x, y), (z, z), (y, z)\}$ then

$R^s = \{(x, x), (x, y), (y, x), (z, z), (y, z), (z, y)\}$

Check your progress

1. Let 'R' be a relation whose matrix is $\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}_{4\times4}$.

   Find the reflexive and symmetric closures of 'R'.

2. Let ‘R’ be a relation whose diagraph is

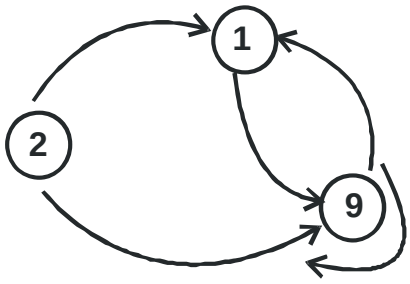


Fig. 4.1

Find the reflexive and symmetric closures of ‘R’.

4.4.2 Transitive Closure

Definition : Let ‘R’ be a relation on ‘A’. The transitive closure of ‘R’ is the smallest transitive relation that contains ‘R’. It’s denoted by R^T.

As compare to reflexive and symmetric closures it’s little bit difficult to find transitive closure because we don’t have a formula for it but we have following results and an algorithm for finding the transitive closure.

Result :-

(1) Let ‘R’ be a relation on A. Then R^∞ is transitive closure of ‘R’.

For example,

(1) Let A = {1, 2, 3, 4} and R = {(1, 1), (1, 2), (2, 3), (3, 4)} we know that if, |A| = m, then $R^\infty = R^1 \cup R^2 \cup .... \cup R^m$.

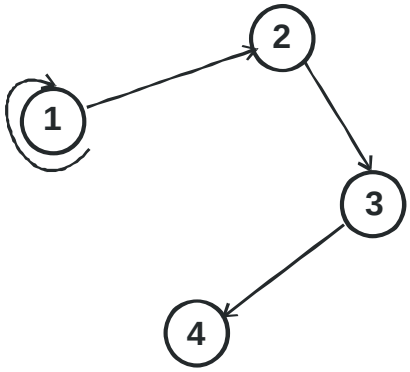


Fig. 4.2

$\because$ |A| = 4

$\therefore$ $R^{\infty} = R^1 \cup R^2 \cup R^3 \cup R^4$

$R^1 = \{(1,1), (1,2), (2,3), (3,4)\}$

$R^2 = \{(1,2), (1,3), (1,1), (2,4)\}$

$R^3 = \{(1,1), (1,2), (1,4), (1,3)\}$ and

$R^4 = \{(1,1), (1,2), (1,4), (1,3)\}$

$\therefore$ $R^{\infty} = \{(1,1), (1,2), (1,3), (1,4), (2,4), (2,3), (3,4)\}$

$\therefore$ Transitive Closure = $R^T = R^{\infty}$

The above graphical method is impractical for large sets and relations and it is not systematic and also It would be more time consuming and costly for large set.

But we have a more efficient algorithm for computing transitive closure called as 'Warshall's Algorithm'.

Warshall's Algorithm :-

Let 'R' be a relation on a set $A = \{a_1, a_2, ..., a_n\}$. If $x_1, x_2, x_3, ..., x_n$ is a Path in R, then any vertices other than x_1 & x_m are called interior vertices of the Path. Now, for $1 \le k \le n$, we define a Boolean matrix W_k as follows. W_k has a '1' in position (i, j) iff there is a path from a_i to a_j in 'R' whose interior vertices, if any, come from the set $\{a_1, a_2, ..., a_k\}$.

So, it follows that W_n has a '1' in position (i, j) iff some Path in 'R' connects a_i with a_j, i.e. $W_n = M_{R\infty}$. If we define W_0 to be m_R, then we will have a sequence $W_0, W_1, ..., W_n = M_{R\infty}$. Now, we will see how to compute matrix W_k from the previous matrix W_{k-1} this procedure is called as 'Warshall's Algorithm'.

Step – I Let $W_0 = M_R$.

Step – II Suppose we have calculated W_{k-1}, now to calculate W_k.

Step – III List the locations $p_1, p_2, \ldots$ in column 'k' of W_{k-1}, where the entry is '1', and the locations $q_1, q_2, \ldots$ in row k of W_{k-1}, where the entry is '1'.

Step – IV Put 1's in all the positions (p_i, q_j) of W_k (if they are not already there.)

For example,

(1) Let A = {1, 2, 3, 4} and R = {(1, 1), (1, 2), (2, 3), (3, 4)} as earlier.

Now, we will use Warshall's Algorithm to find R^{∞}.

(1) $W_0 = M_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}_{4\times 4}$

(2) To computer W_1 consider Ist column and Ist row of W_1 where 1's are present.

$W_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

Column	Row
1	1
	2

So fill the positions (1, 1) and (1, 2) by 1's if not present already.

(3) To compute W_2 consider IInd column and IInd row of W_1 where 1's are present.

$W_2 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

Column	Row
1	3

So fill (1, 3) by '1'.

(4) To compute W_3, consider IIIrd column and IIIrd row of W_2 where 1's are present.

$$W_3 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Column	Row
1	4
2	

So fill (1, 4) and (2, 4) by 1's.

(5) To compute W_4, consider IVth column and IVth row of W_3 where 1's are present.

$\therefore\ W_4 = W_3 = M_{R\infty}$

Column	Row
1	No
2	1's
3	

So, no new entries.

$\therefore\ R^T = R^\infty = \{(1,1), (1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$

Note :

(1) Warshall's Algorithm gives another method to calculate R^∞.

(2) Warshall's Algorithm relatively faster then other methods. (in the sense of time taken)

Check your progress

1. Let A = {1, 2, 3, 4} and matrix of Relation 'R; is,

$$M_R = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Find R^∞ using (a) Warshall's Algorithm
(b) Diagraph

2. Let A = { x, y, z, w} and matrix of Relation 'R' is,

$$M_R = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = W_0$$

Compute $W_1,\ W_2,\ W_3$ as in Warshall's algorithm.

4.5 COMPOSITION :

Let A, B, C be given sets. Let 'R' be a relation from A to B and 'T' be a relation from 'B' to 'C' then we can define a new relation from 'A' to 'C' called as composition of 'R' and 'T' [denoted by (TOR)]

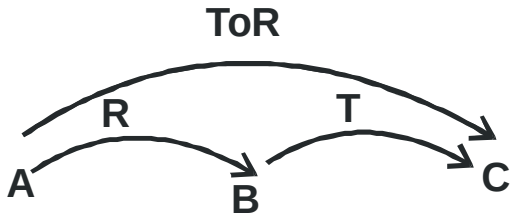


Fig. 4.3

Definition : Let $x \in A$ and $y \in c$, then $x(TOR)y$ means there exist $w \in B$ such that (x R w) and (w T y).

For example,

(1) Let A = {1, 2, 3, 4} and

R = {(1, 1), (2, 3), (1, 4)} and T = (2, 2), (2, 3), (3, 4)}

$(2, 3) \in R$ and $(3, 4) \in T \Rightarrow (2, 4) \in TOR$

$\therefore$ TOR = {(2, 4)}

In terms of Matrices,

If M_R is a matrix related to 'R' and

If M_T is a matrix related to 'T' and

M_{TOR} is a matrix related to (TOR).

Then we have, $M_{TOR} = M_R \odot M_T$

For example,

(1) Let A = {1, 2, 3} and let R and T be relations on 'A' whose matrices

are $M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ and $M_T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$ then we see that,

$(1,1) \in R$ *and* $(1,1) \in T \Rightarrow (1,1) \in TOR$
$(1,3) \in R$ *and* $(3,1) \in T \Rightarrow (1,1) \in TOR$
$(1,3) \in R$ *and* $(3,3) \in T \Rightarrow (1,3) \in TOR$
$(2,1) \in R$ *and* $(1,1) \in T \Rightarrow (2,1) \in TOR$
$(2,2) \in R$ *and* $(2,2) \in T \Rightarrow (2,2) \in TOR$
$(2,2) \in R$ *and* $(2,3) \in T \Rightarrow (2,3) \in TOR$
$(2,3) \in R$ *and* $(3,1) \in T \Rightarrow (2,1) \in TOR$
$(2,3) \in R$ *and* $(3,3) \in T \Rightarrow (2,3) \in TOR$
$(3,2) \in R$ *and* $(2,2) \in T \Rightarrow (3,2) \in TOR$
$(3,2) \in R$ *and* $(2,3) \in T \Rightarrow (3,3) \in TOR$

$$\therefore M_{TOR} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

We can check that, $M_{TOR} = M_R \odot M_T$ so this formula gives an easy way to compute ToR (by using M_{TOR})

Note : (1) If R = T then we have $ToR = R^2$ and
$M_{TOR} = M_{R^2} = M_R \odot M_R$.

(2) If we have relation R, T, S such that,

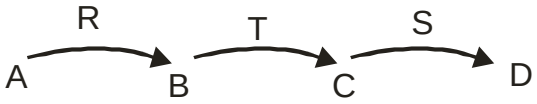


Fig. 4.4

then $To(SoR) = (ToS) \circ R$ [i.e. composition is associative]

(3) In General, $RoS \neq SoR$

(4) $(SoR)^{-1} = R^{-1} \circ S^{-1}$

Check your progress

1. A = B = C , A = { *x* , y, z, w} and R and T be two relations such that

$$M_R = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \textit{ and } M_T = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

then compute (ToR) and (RoT)

2. Give an example of relations R and T such that RoT $\neq$ ToR.

4.6 COMPUTER REPRESENTATION OF RELATIONS AND DIAGRAPHS :

We know that a Relation 'R' on set 'A' can be represented by an n X n matrix M_R, if |A| = n. The matrix M_R has entries that are '0' or '1'. Then one of the easier way of representing 'R' in a computer is by an n X n array having 0's and 1's stored in each location. Thus, if A = {1, 2} and R = {(1, 1), (2, 1), (2, 2)}, then $M_R = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and these data would be represented by a two dimensional array MR, where $MR[1,1] = 1, MR[1,2] = 0, MR[2,1] = 1,$ MR [2, 2] = 1 (MR means matrix related to 'R')

An another way of storing data for relations and diagraphs is by using the linked list idea of computer programming. A liked list will be constructed that contains all the edges of the diagraph, that is, the ordered pairs of numbers that determine those edges. The data can be represented by two arrays, TAIL and HEAD, giving the beginning vertex and end vertex, respectively for all edges.

If we are making these edge data into a linked list, then we need an array NEXT of pointers from each edge to the Next edge.

Consider the relation whose diagraph is

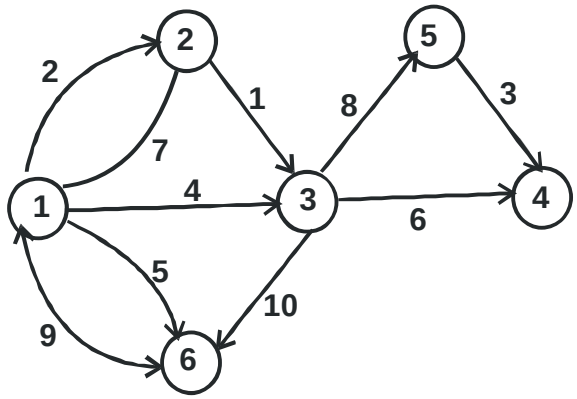


Fig. 4.5

The vertices are the integers ‘1’ to ‘6’ and we arbitrarily number the edges as shown in above diagraph. If we wish to store the diagraph in liked – list form so that the logical order coincides with the numbering of edges. We can use a scheme mentioned below.

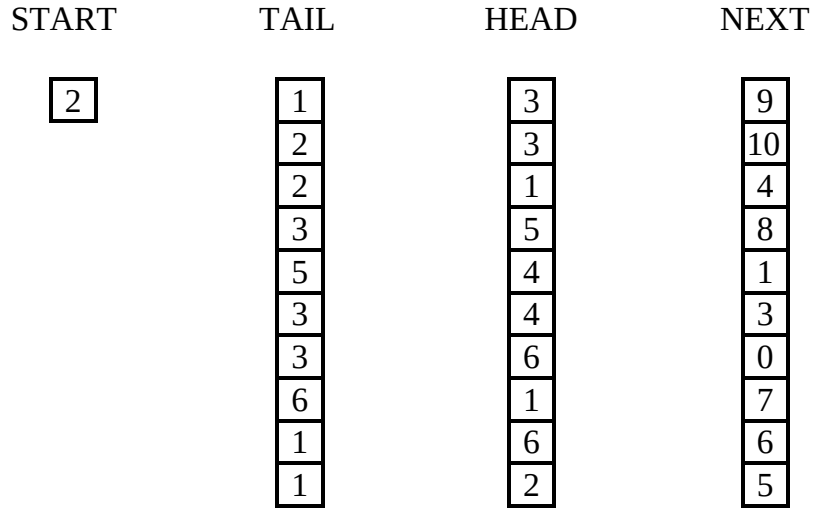


Fig. 4.6

START contains 2, the index of the first data item, the edge (2, 3) [this edge is labeled with a ‘1’ in fig : 5.6]. This edge is stored in the second entries of TAIL and HEAD, respectively. Since NEXT [2] contains 10, the next edge is the one located in position 10 of TAIL and HEAD, that is, (1, 2).

NEXT [10] contains 5, so we go to next to data position 5, which contains the edge (5, 4). This process continues until we reach edge (3, 6) in data position 7. This is the last edge, and this fact is indicated by having NEXT [7] contains ‘0’. We use ‘0’ as a pointer, indicating the absence of any more data.

If we trace through this process, we will see that we encounter the edges in exactly the order corresponding to their numbering. We can arrange, in a similar way, to pass through the edges in any desired order.

But this scheme and the numerous equivalent variations of it have important disadvantages. In many algorithms, it’s efficient to locate a vertex and then immediately begin to investigate the edges that begin or end with this vertex. This is not possible in general with the mechanism shown in fig : 2. So we have modification of it. We use an additional linear array VERT having one position for

each vertex in the diagraph. For each vertex I, VERT [I] is the index, in TAIL and HEAD, of the first edge we wish to consider leaving vertex I as shown below.

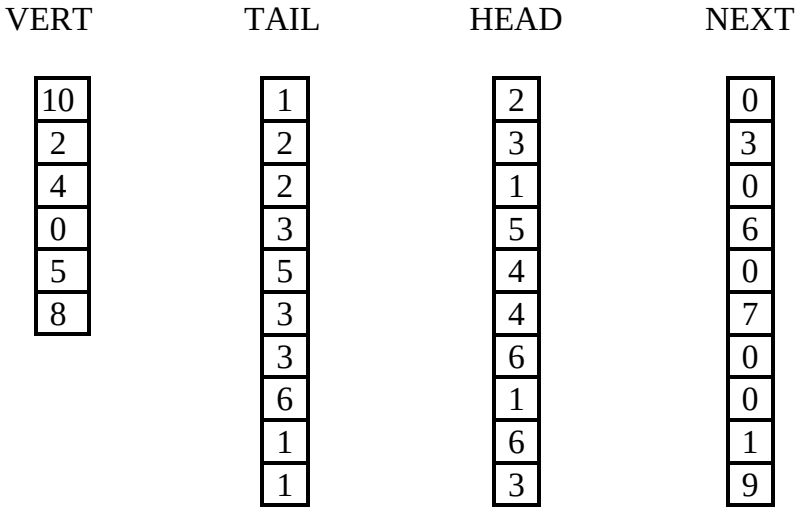


Fig. 4.7

In Fig. 4.5, the first edge could be taken to edge with the smallest number labeling it. Thus VERT, like NEXT, contains pointers to edges. For each vertex I, we must arrange the pointers in NEXT so that they link together all edges leaving I, starting with the edge pointed to by VERT [I]. The last of these edges is made to point to zero in each case. In a sense, the data arrays TAIL and HEAD really contain several linked lists of edges, one for each vertex.

In Fig. 4.7 we can see that VERT [1] contains 10, so the first edge leaving vertex 1 must be stored in the tenth data position. This is edge (1, 3). Since NEXT [10] = 9, the next edge leaving vertex '1' is (1, 6) located in data position '9'. Again NEXT [9] = 1, which points us to the edge (1, 2) in data position 1. Since NEXT [1] = 0, we have come to the end of those edges that begin at vertex '1'. The order of the edges choosen here differs from the numbering in Fig. 1.

We then proceed to VERT [2] and get a pointer to position '2' in the data. This contains the first edge leaving vertex 2, and we can follow the pointers to visit all edges coming from vertex 2. Note that VERT [4] = 0, signifying that there are no edges beginning at vertex '4'.

So we have seen at least two methods for storing the data for a relation or diagraph, one using the matrix of the relation and one

using linked lists. There are number of factors which determines the choice of method to be used for storage and an analysis shows that matrix storage method is 'n' times faster than the linked list method in most cases.

4.7 LET US SUM UP :

We saw the definition of an equivalence relation and method to produce partition using an equivalence relation and vice versa. Then we saw the different operations that can be performed on relations and how some of them can be used to find closures. Then we saw different method for computing transitive closures with an important method Warshall's Algorithm. At the end we saw two important concepts, composition of relations and computer representation of relation and diagraph.

4.8 REFERENCES FOR FURTHER READING :

(1) Discrete structures by B. Kolman Hc Busby, S Ross PHI Pvt. Ltd.

(2) Discrete mathematics and it's Application Keneth H. Rosen TMG.

(3) Discrete structures by Liu.

4.9 UNIT END EXERCISES

Q.1 Let A = $\mathbb{R} \times \mathbb{R}$, define the following relation 'R' on A : (a, b) R (c, d) iff $a^2 + b^2 = c^2 + d^2$ show that 'R' is an equivalence relation.

Q.2 Let A = { x, y, z, w} and 'R' be a relation on 'A' defined by,

$$M_R = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$ compute a partition produce by 'R'.

Q.3 Let A = {1, 2, 3, 4,… 12} and let 'R' and 'S' be the following relations on A : x R y iff $2 | (x - y)$ and $x \subseteq y$ iff $3 | (x - y)$.

Compute –

(a) $\overline{R}$ (f) S^{-1}

(b) $\overline{S}$ (g) $M_{R \cup S}$

(c) $R \cup S$ (h) $M_{R \cap S}$

(d) $R \cap S$ (i) $M_{R^{-1}}$

(e) R^{-1} (j) $M_{\overline{S}}$

Q.4 Find the transitive closure of a relation whose matrix is

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

by (a) computing R^{∞} (b) using Warshall's Algorithm

Q.5 Let A = {1, 2, 3, 4} and let R and S be the relations on 'A' such that

$$M_R = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \text{ and } M_S = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

use Warshall's Algorithm to compute the transitive closure of $R \cup S$.

Q.6 If A = {1, 2, 3, 4} and let R and S be the relations on 'A' such that

$$M_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \text{ and } M_S = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Find (a) M_{RoR}, (b) M_{RoS}, (c) SoR, (d) RoS.

5

PARTIAL ORDER SETS AND LATTICES

Unit Structure

5.0 OBJECTIVES:

After going through this chapter students will be able to understand:

- The definition of partially order sets and example based on it.
- Idea of Hasse diagram and able to represent the diagraph of a poset in more efficient way.
- The concept of Isomorphism and which is useful in classification of Posets.
- The concept of maximal, minimal elements, the greatest and least element, upper and lower bound of a subset and finally the concept of LUB and GLB.
- The concept of Lattices and different properties of a Lattice.

5.1 INTRODUCTION:

We use relations to order some or all of the elements of sets. For example we order words using the relation, containing pair of words (x, y) where ‘x’ comes before ‘y’ in the dictionary. We schedule projects using the relation consisting of pairs (x, y) where x and y are tasks in project such that x must be completed before y

begins. When we add all the pairs of the form (x, x) to these relations we get partial order. (Practical definition afterwards). These structures are useful in set theory, algebra, sorting and searching, in the construction of logical representations for computer circuits.

5.2 DEFINITION AND EXAMPLES:

Definition: Let 'R' be a relation on set A. then 'R' is said to be partial order if 'R' is (a) reflexive (b) antisymmetric and (c) transitive.

The set A with partial order 'R' is called as partial order set or poset and It's denoted as (A, R)

For example

(1) Let $A = \mathbb{N}$ and 'R' be a relation on 'A' such that x R y iff $x \leq y$.

It's easy to check 'R' is reflexive, ant symmetric and transitive.

$\therefore$ R is a partial order.

$\therefore (\mathbb{N}, \leq)$ is a poset.

(2) Let $S = \{1, 2, 3\}$ and $A = P(S)$

$\therefore A = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, S\}$

Let R be a relation on A defined as x R w iff $x \subseteq w$

(a) Let $x \in A$,

$\because x \subseteq x$

$\therefore$ xRx $\quad \forall\ x \in A$

$\therefore$ R is reflexive

(b) Let $x, w \in A$ such that x R w and w R x

$xRw \Rightarrow x \subseteq w$ (1)

and $wRx \Rightarrow w \subseteq x$ (2)

$\therefore w = x$ from (1) and (2)

$\therefore$ R is antisymmetric

(c) Let x, w, $z \in A$ such that x R w and w R z

$x\ R\ w \Rightarrow x \subseteq w$ (1)

and $wRz \Rightarrow w \subseteq z$ (2)

From (1) and (2) we have, $x \subseteq w \subseteq z \;\; \therefore x \subseteq z \;\; \therefore x\, R\, z$

$\therefore R$ is transitive

$\therefore R$ is partial order

$\therefore (A, R)$ is a poset

(3) Above example can be extended to any finite set as well as for an infinite set

(4) Let $A = \mathbb{N}$, & $'R'$ be a relation on 'A' such that x R y iff x divides y.

It's easy to check (A, R) is a poset.

(5) Let $A = \mathbb{N}$ and 'R' be a relation on A such that x R y iff x < y. Then 'R' isn't a partial order. ($\because R$ isn't reflexive $\because 3 \not R 3$) $\therefore (A, <)$ isn't a poset.

Note:

(1) Let 'R' be a partial order then R^{-1} is also a partial order.

R^{-1} is called as the dual of R and the set (A, R^{-1}) is called the dual of the poset (A, R)

For example (a) dual of $(\mathbb{N}, \leq)$ is $(\mathbb{N}, \geq)$.

(2) IF (A, R) is a poset, the elements x and y of A are said to be comparable if x R y or y R x. The important observation is that two elements in a poset may not be comparable.

For example 2 and 7 in $\mathbb{N}$ with divisibility relation are not comparable ($\because 2 \nmid 7$ & $7 \nmid 2$)

(3) If every pair of elements in a poset is comparable, we say that 'A' is a linearly ordered and the partial order is called a linear order and we say 'A' is a chain.

Check your progress

1. Determine whether relation 'R' is a partial order on the set 'A'.

(a) $A = \mathbb{N}$, and $x\, R\, y$ iff $x + y$ is an even number.

(b) $A = \mathbb{N}$, and $x\, R\, y$ iff $x \geq y$

5.3 HASSE DIAGRAMS:

Result: The diagraph of a partial order has no cycle of length greater than '1' (except at loops)

With the help of above result we can simplify the diagraph of a partial order, simplified diagram is called as Hasse diagram.

Procedure for finding Hasse diagram:

1) Draw the diagram of given partial order so that all the arrows are pointing in upward direction.

2) Remove all cycles of length '1' (i.e. loop at each of the vertex)

3) Eliminate all edges that are implied by the transitive property i.e. (a R b) and (b R c) then aRc so remove the edge from 'a' to 'c'

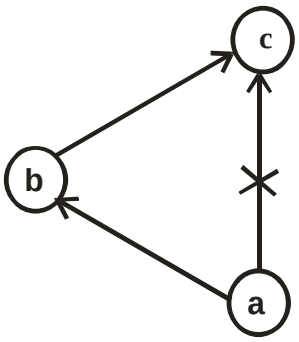


Fig. 5.1

4) Replace arrows by line segments and circles by dots.

For example:

(1) Let $A = \{1,\ 2,\ 4,\ 5,\ 10,\ 20\}$ with relation of divisibility.

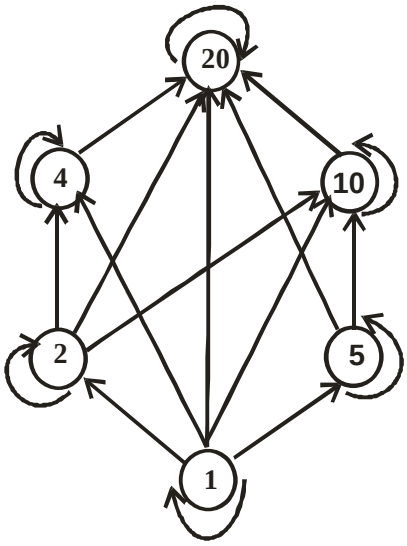


Fig. 5.2

Diagraph

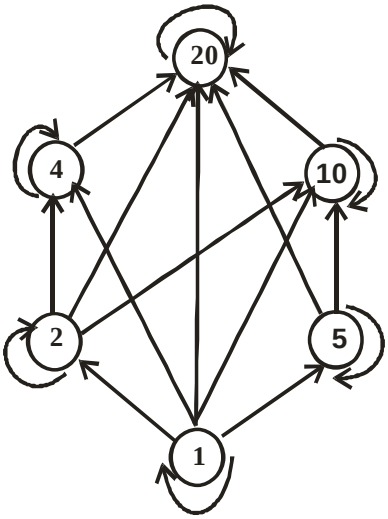


Fig. 5.3 Step: 1

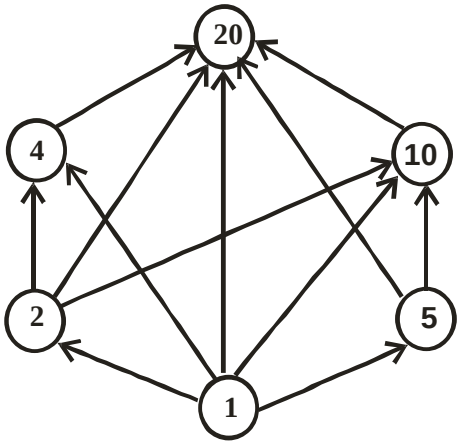


Fig. 5.4 Step: 2

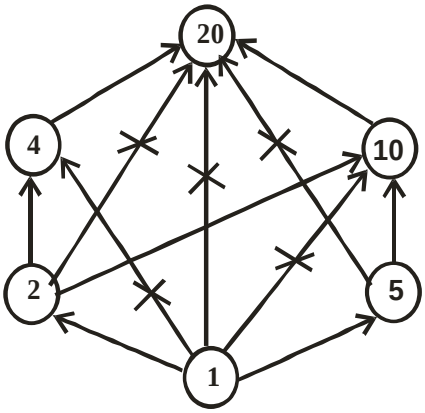


Fig. 5.5 Step: 3

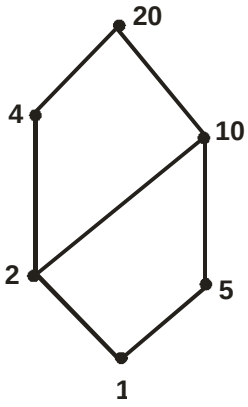


Fig. 5.6 Step: 4

Hasse diagram

(2) Let $S = \{1, 2, 3\}$ and $A = P(S) = \{0, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\} S\}$ with relation of contain $(\subseteq)$

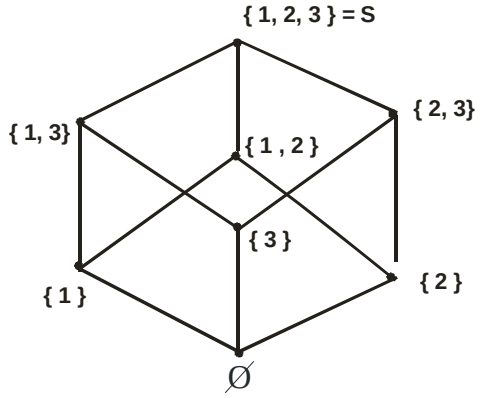
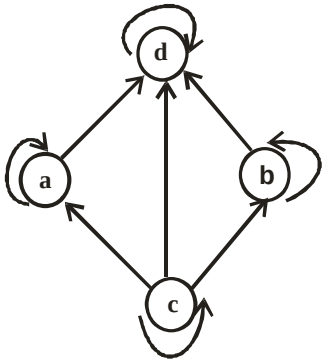


Fig. 5.7 Hasse diagram

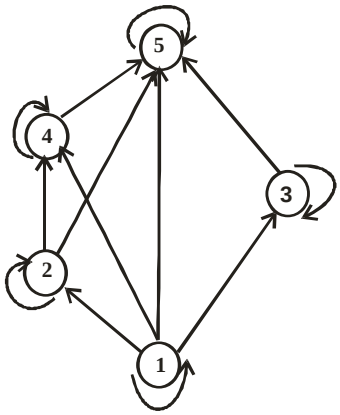
Check your progress:

Draw Hasse diagram of following diagraphs.



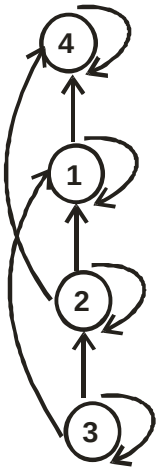
(a)

Fig. 5.8



(b)

Fig. 5.9



(c)

Fig. 5.10

5.4 ISOMORPHISM :

Let (A, R) and (B, T) be two Posets. Then (A, R) and (B, T) are said to be Isomorphic if $\mathcal{F}$ a function 'f' from 'A' to 'B' such that

(a) f is bijective

(b) 'f' preserves partial order. [i.e. for any a, b in 'A', we have $a\ R\ b$ iff $f(a)\ T\ f(b)$]

Note :- If (A, R) and (B, T) are Isomorphic then such a 'f' is called as an Isomophism from 'A' to 'B'.
For example,

(1) Let (A, R) = $(\mathbb{N}, \leq)$

(B, T) = (set of all even natural numbers, $\leq$)

Define f : (A, R) $\rightarrow$ (B, T) as f(m) = 2m

(a) Let a, b $\in$ A such that f(a) = f(b)

$\Rightarrow$ 2a = 2b

$\Rightarrow$ a = b

$\therefore$ f is one one.

(b) Let b $\in$ B

$\therefore$ b = 2q $(q \in \mathbb{N})$

Take a = q

$\therefore$ f(a) = f(q) = 2q = b true $\forall\ b \in B$

$\therefore$ f is onto.

$\therefore$ f is bijective.

Now, Let a, b $\in$ A such that $a\ R\ b \Rightarrow a \leq b$

$\Rightarrow 2a \leq 2b$

$\Rightarrow f(a) \leq f(b)$

$\therefore$ f preserves partial order.

$\therefore$ f is an Isomorphism.

$\therefore$ (A, R) and (B, T) are Isomorphic.

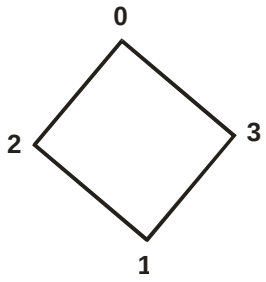
5.5 EXTERNAL ELEMENTS OF PARTIALLY ORDERED SETS :

Let (A, R) be a given poset.

An element $a \in A$ is called a maximal element of A if there is no element 'x' (except 'a') in A such that $a \, R \, x$.

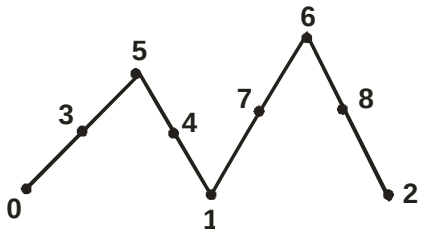
Similarly, an element $b \in A$ is called a minimal element of A if there is no element 'x' (except 'b') in A such that $x \, R \, b$.

For example,
(1) Consider the Hasse diagrams of some posets as shown below.



(a)

Fig. 5.11
Maximal element = 0
Minimal element = 1



(b)

Fig. 5.12
Maximal elements = 5, 6
Minimal elements = 0, 1, 2

(2) Consider a poset $(\mathbb{N}, \leq)$, minimal element = 1, maximal element doesn't exist.

(3) Consider a poset $(\mathbb{Z}, \leq)$ minimal and maximal doesn't exist.

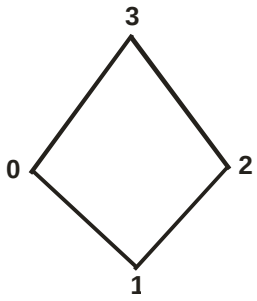
Result :-

Let 'A' be a finite non empty poset, then A has atleast one maximal and atleast one minimal element.

An element a $\in$ A is called a greatest element of 'A' if $x \, R \, a$ $\forall x \in A$ and an element b $\in$ A is called a least element of 'A' if bRx $\forall x \in A$.

For example,

(1)



Greatest element = 3

Least element = 1 **Fig. 5.13**

(2) Poset $(\mathbb{N},\leq)$ greatest element doesn't exist least element = 1

(3)

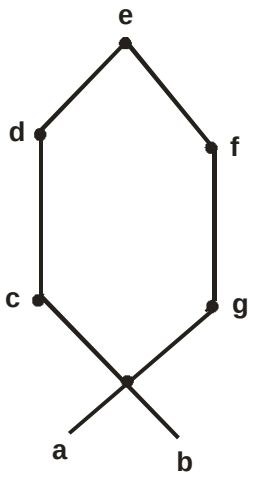


Fig. 5.14

Greatest element = e

Least element doesn't exist

(4)

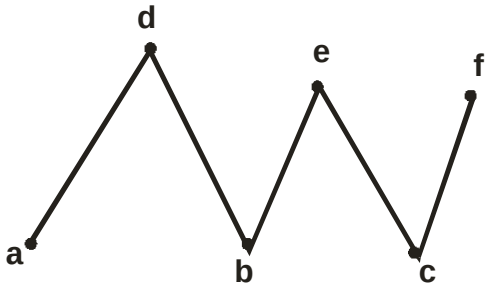


Fig. 11.15

Greatest as well as least element doesn't exist.

Result :-

A poset has at most one greatest and at most one least element.

Note :

(1) Greatest element is denoted by I and it's also called as unit element

(2) Least element is denoted by '0' and it's also called as zero element.

Consider a poset (A, R) and a subset 'B' of 'A'. An element 'u' of A is said to be an upper bound of B if bRu $\forall b \in B$.

An element 'ℓ' of A is said to be a lower bound of B if ℓ R b $\forall$ b $\in$ B.

For example,

(1) Consider the following poset and find the upper and lower bounds of (a) $B_1 = \{2, 5, 7\}$ (b) $B_2 = \{1, 3\}$ (c) $B_3 = \{3, 2, 7, 4\}$

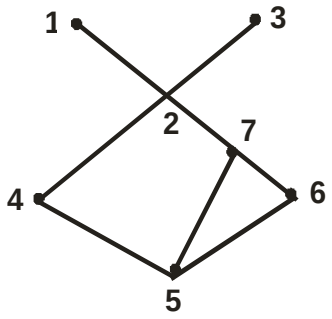


Fig.5.16

For B_1, Upper bounds are 1, 2, 3
Lower bound is 5

For B_2, No upper bounds
Lower bounds are 2, 7, 4, 5, 6

For B_3, Upper bound is 3
Lower bounds are 5, 6

Note : 1) A subset 'B' of a poset may or mayn't have upper or lower bounds.
2) It can have more than one upper or lower bounds.

3) Upper or lower bound may or mayn't belong to given subset.

Let 'A' be a poset and 'B' a subset of 'A'.

1) An element are u $\in$ A is called a least upper bound of 'B', $\left[\text{L}\cup\text{B}(\text{B})\right]$
   (a) If 'u' is an upper bound of 'B'.
   (b) If w is any other upper bound of 'B' then u R w,

Similarly,

2) An element l $\in$ A is called a greatest lower bound of 'B', $\left[\text{GLB}(\text{B})\right]$
   (a) If '*l*' is a lower bound of 'B'.
   (b) If 't' is any other lower bound of 'B' then t R *l*.

For example,

(1) Consider the following poset

(a) for a subset B = {e, d, h}
Upper bounds = a, c, b
Lower bounds = h, f, g
$\text{L}\cup\text{B}(\text{B})$ = h
$\text{GLB}(\text{B})$ = does not exist (as 'a' and 'c' are not comparable)

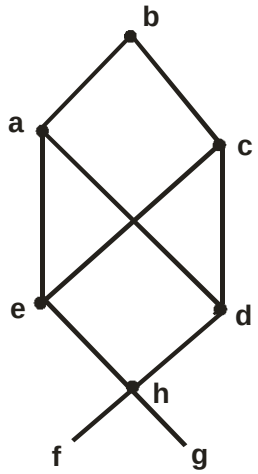


Fig. 5.17

(b) For a subset D = {a, d. f. g}
Upper bounds = a, b $\text{L}\cup\text{B}$ = a
No lower bounds GLB = does not exist

(c) For a subset E = {a, e, d}
Upper bounds = a, b $L \cup B = a$
Lower bounds = h, f, g GLB = h

Result :

Suppose that (A, R) and (B, T) are Isomorphic posets under the Isomorphism f : $A \to B$

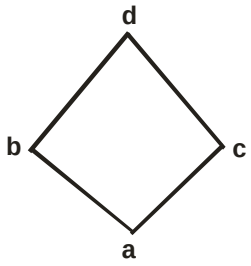
(a) If 'a' is a maximal (minimal) element of (A, R), then f(a) is a maximal (minimal) element of (B, T).

(b) If 'a' is the greatest (least) element of (A, R), then f(a) is the greatest (least) element of (B, T)

(c) If 'a' is an upper bound (lower bound, least upper, upper bound, greatest lower bound) of a subset 'D' of A, then f(a) is an upper bound (lower bound, least upper bound, greatest lower bound) for the subset f(D) of B.
[Notation : if D = {1, 2, 3} then f(D) = {f(1), f(2), f(3)}]

(d) If every subset of (A, R) has a $L \cup B$ (GLB), then every subset of (B, T) has a $L \cup B$ (GLB).

For example,
(1)



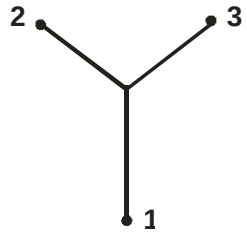


Fig. 5.18 **Fig. 5.19**

This two posets are not Isomorphic as first one have a greatest element but second one not.

(2) Consider the posets, A = {1, 2, 3, 6} with divisibility relation and $S = \{1, 2\}$, A = P(S) with contain relation

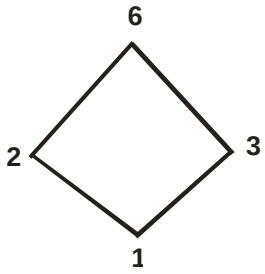


Fig. 5.20

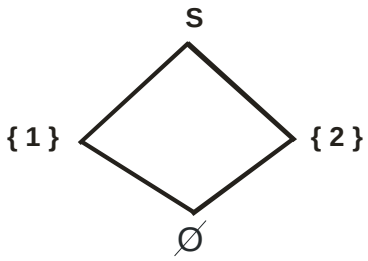


Fig. 5.21

So these two posets are Isomorphic under the Isomorphism 'f' which is defined as, f(1) = □, f(3) = {2}, f(2) = {1}, f(4) = S and they satisfy all conditions stated in above result.

Check your progress

1. Consider the poset,

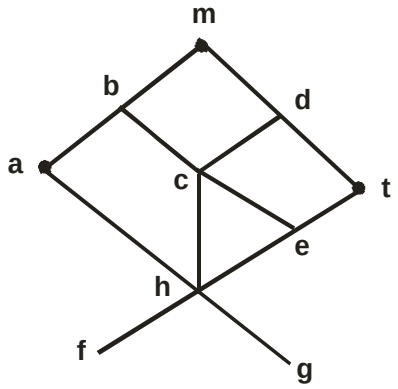


Fig. 5.22

(a) Find maximal, minimal, greatest and least element if exist.

(b) For following subsets find

(i) All upper bounds

(ii) All lower bounds

(iii) The least upper bound

(iv) The greatest lower bound

1) $B_1 = \{a, c, h\}$

2) $B_2 = \{h, f, g, e\}$

3) $B_3 = \{a, d, e, f\}$

4) $B_4 = \{b, c, h, e\}$

2. Check whether following posets are Isomorphic if yes find the corresponding Isomorphism.

I

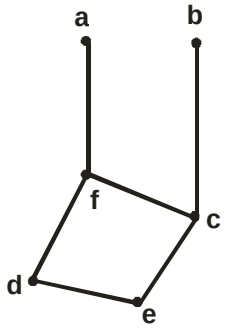


Fig. 5.23

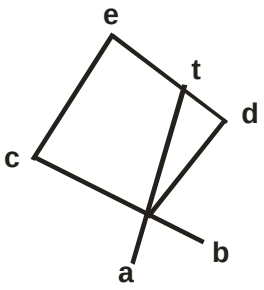


Fig. 5.24

II

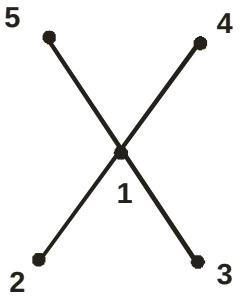


Fig. 5.25

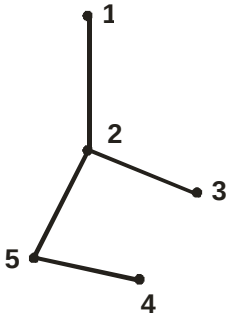


Fig. 5.26

III

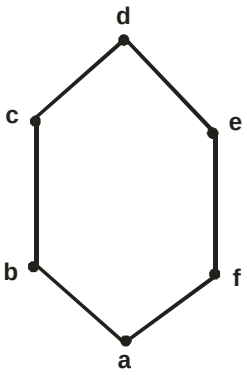


Fig. 5.27

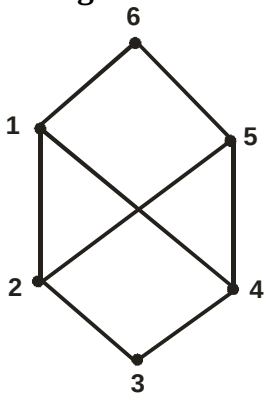


Fig. 5.28

3. Find maximal, minimal, greatest and least element if exist.
   (a) A = $\mathbb{Z}$ with usual partial order $\leq$.
   (b) A = $\{ x / x \in \mathrm{R} \quad and \quad 0 < x < 1\}$ with usual partial order $\leq$
   (c) A = $\{ x / x \in \mathrm{R} \quad and \quad 0 \leq x < 1\}$ with usual partial order $\leq$
   (d) A = $\{ x / x \in \mathrm{R} \quad and \quad 0 \leq x \leq 1\}$ with usual partial order $\leq$

5.6 LATTICES

5.6.1 Definition

A lattice is a poset (L, R) in which every subset consisting of two elements has a least upper bound $(L \cup B)$ and greatest lower bound (GLB).

Notation :- If a set is {a, b} then $L \cup B(\{a, b\})$ is denoted by $a \vee b$ and it's called as join of 'a' and 'b'. Similarly, GLB ({a, b}) is denoted by $a \wedge b$ and it's called as meet of 'a' and 'b'.

For example
(1) Consider a poset,

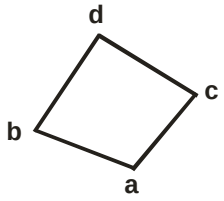


Fig. 5.29

$\vee$	a	b	c	d
a	a	b	c	d
b	b	b	d	d
c	c	d	c	d
d	d	d	d	d

$\wedge$	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	a	c	c
d	a	b	c	d

So, from the table of join and meet we can see $L \cup B$ and GLB of any subset with two elements exist.
$\therefore$ it's a Lattice.

(2) Consider a poset,

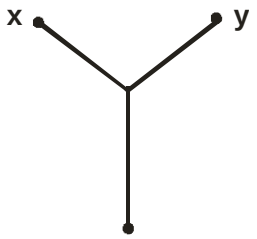


Fig. 5.30

Since $L \cup B(\{x, y\})$ doesn't exist.
$\therefore$ it's not a lattice.

(3) Let 'S' be a given set and L = P(S). Consider 'L' with relation contain $(\subseteq)$

We know that $(L, \subseteq)$ is a poset.

Let x, y $\in$ L, then $x \vee y = X \cup Y$ and $X \wedge Y = X \cap Y$

and which exist in L. (as they are subsets of 's')

$\therefore$ $(L, \subseteq)$ is a lattice.

(4) Consider the poset ($\mathbb{N}$, divisibility relation),

Let $x, y \in \mathbb{N}$,

then $x \vee y = L C M (x, y)$ and $x \wedge y = G C D (x, y)$

(5) Let $n \in \mathbb{N}$,

Let D_n = set of all positive divisors of 'n', then it can be proved D_n with divisibility relation is a poset.

For example,

If n = 20, then $D_{20} = \{1, 2, 4, 5, 10, 20\}$

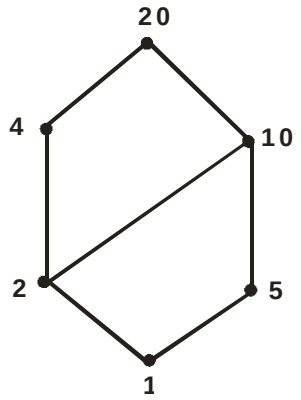


Fig. 5.31
Hasse diagram of D_{20}

is a Lattice. [it can be proved similarly as in example (1).]

Check your progress

1. Check whether following Hasse diagrams are lattice or not?

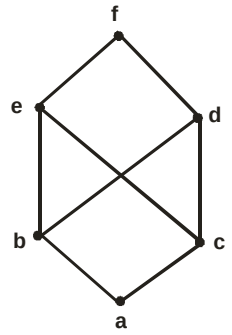


Fig. 5.32

(a)

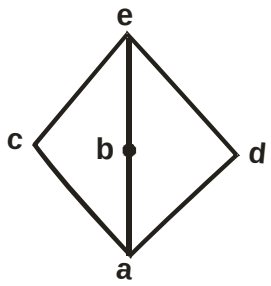


Fig. 5.33

(b)

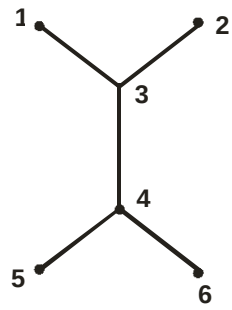


Fig. 5.34

(c)

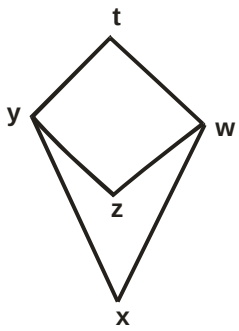


Fig. 5.35

(d)

5.6.2 Isomorphic Lattices

Let (L_1, R_1) and (L_2, R_2) be two given posets. A function $f : L_1 \to L_2$ is said to be an isomorphism if

(1) 'f' is bijective

(2) f preserves the Lattice properties. [i.e. if a, $b \in L_1$ then $f(a \vee b) = f(a) \vee f(b)$ and $f(a \wedge b) = f(a) \wedge f(b)$]

Note : (L_1, R_1) and (L_2, R_2) are said to be Isomorphic Lattices.

For example,

(1) $(D_6$, divisibility) and $\left(P(\{1, 2, 3\}), \subseteq\right)$ are Isomorphic Lattices.

5.6.3 Properties of Lattices

Theorem :-

Let (L, R) be a lattice, then for every ‘a’ and ‘b’, ‘c’ in ‘L’,

(1) $a \vee b = b$ iff $a \, R \, b$

(2) $a \wedge b = a$ iff $a \, R \, b$

(3) $a \wedge b = a$ iff $a \vee b = b$

(4) $a \vee a = a$

(5) $a \wedge a = a$ } Indempotent Properties

(6) $a \vee b = b \vee a$

(7) $a \wedge b = b \wedge a$ } Commutative Properties

(8) $a \vee (b \vee c) = (a \vee b) \vee c$

(9) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ } Associative Properties

(10) $a \vee (a \wedge b) = a$

(11) $a \wedge (a \vee b) = a$ } Absorption Properties

Proof :-

(1) Assume $a \vee b = b$

$\because$ $a \, R \, (a \vee b)$

$\therefore$ $a \, R \, b$

Conversely, if a R b, since b R b, b is an upper bound of ‘a’ and ‘b’. So, by definition of least upper bound we have $(a \vee b) \, R \, b$. Since, $a \vee b$ is an upper bound, $b \, R \, (a \vee b)$, so $a \vee b = b$.

(2) and (3) proof similar to (1).

(4) and (5) follows from definition of $L \cup B$ and GLB.

(6) $a \vee b = L \cup B \, (\{a, b\})$

$= L \cup B \, (\{b, a\})$

$= b \vee a$

(7) Proof similar to (6)

(8) From definition of $L \cup B$, we have $a \, R \, (a \vee (b \vee c))$ and

$(b \vee c) \, R \, (a \vee (b \vee c))$ and also $b \, R \, (b \vee c)$ and $c \, R \, (b \vee c)$ so by transitivity, $b \, R \, (a \vee (b \vee c))$ and $c \, R \, (a \vee (b \vee c))$ thus, $a \vee (b \vee c)$ is an upper bound of a and b, so by definition of $L \cup B$ we have, $(a \vee b) \, R \, (a \vee (b \vee c))$.

Since, $a \vee (b \vee c)$ is an upper bound of $a \vee b$ and c, we obtain $((a \vee b) \vee c) \, R \, (a \vee (b \vee c))$

Similarly, $(a \vee (b \vee c)) \, R \, ((a \vee b) \vee c)$

By antisymmetry of R, we have $(a \vee b) \vee c = a \vee (b \vee c)$

(9) Proof Similar to (7)

(10) Since, $(a \wedge b) \, R \, a$ and a R a, we have 'a' is an upper bound of $a \wedge b$ and 'a' so $a \vee (a \wedge b) \, R \, a$.
On the other hand, by definition of $L \cup B$, we have $a \, R \, (a \vee (a \wedge b))$, so $a \vee (a \wedge b) = a$

(11) Proof is similar to (10).

5.7 LET US SUM UP

We started the concept of partial order set (poset), a set with some special properties of a relation, defined on a set. Then we saw if a given relation is a partial order then diagraph of a partial order can be represented in better way, so that we can retrieve more and more properties of a given poset. Then we had seen a concept of Isomorphism, which divides the space of Lattices in different groups. Then we saw the concept of maximal, minimal elements, upper bounds, lower bounds, GLB and $L \cup B$ of a subset of a given poset. GLB and $L \cup B$ concepts are useful in defining Lattice which in turn useful in defining Boolean Algebra (which we will be seeing in the next chapter).

5.8 UNIT END EXERCISES

1. Determine whether the following relation 'R' is a partial order or not on a given set.

   (a) A = $\mathbb{Z}$, a R b iff a + b is even.

   (b) A = $\mathbb{Z}$, a R b iff a = b.

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

   (a) $\begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ (b) $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$

3. Draw the Hasse diagram of Poset with partial order divisibility) and determine which posets are linearly ordered.

   (a) A = {1, 2, 3, 4, 6, 9, 12, 36}

   (b) A = {3, 6, 12, 36, 72}

4. A is the set of all 2 X 2 Boolean matrices and the relation 'R' is defined as M R N iff $m_{ij} \le n_{ij}$, $1 \le i \le 2$, $1 \le j \le 2$.

   (a) Find maximal and minimal elements of A

   (b) Find the greatest and least element if exist of A.

   (c) Find all upper and lower bounds of $B = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \right\}$

   (d) Find GLB and L $\cup$ B of above set 'B'.

5. Draw the Hasse diagram of D_{30}, D_{36}, D_{42}.

6. Determine whether following Hasse diagram represents a Lattice or not.

(*i*)

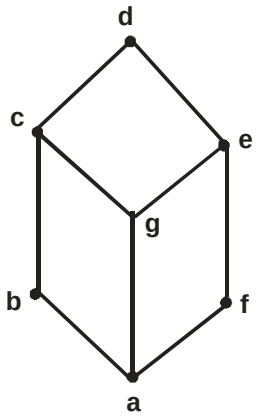


Fig. 5.36

(*ii*)

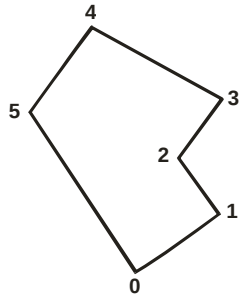


Fig. 5.37

(*iii*)

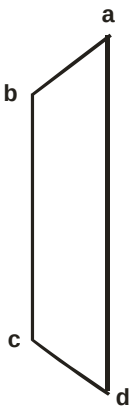


Fig. 5.38

(*iv*)

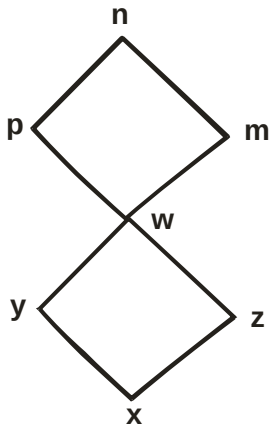


Fig. 5.39

5.9 REFERENCES FOR FURTHER READING

(1) Discrete structure by B. Kolman, Hc Busby, S. Ross PHI Pvt. Ltd.

(2) Discrete structures by Liu.

(3) Discrete mathematics and it's Apprlications Keneth H. Rosen TMG.

❖❖❖❖

6

FUNCTION

Unit Structure

6.0 OBJECTIVES:

- A function is the central to the study of physics and enumeration.
- In computer implementation of any program output of any program can be considered as a function of the input.
- Binary operations have applications in the study algebraic structures.

6.1 INTRODUCTION:

A function was the heart of the scientific revolution of the seventeenth century. To understand the general use of function we must study their properties in the general, which is what we do in this chapter.

The reader is no doubt familiar with function of the form $y = f(x)$ for instance, if $f(x) = x^2 - 2$, $x = 2$ and $y = f(2)$ then the value of y is 4.

6.2 FUNCTIONS:

Definition: Let X and Y are non-empty sets. A function f form X to Y if for each element of $a \in X$ exactly one element $b \in Y$ (called the image of a under f) such that a is in relation f to b, then is called function or mapping from X to Y.

If f is a function (mapping) from X to Y we write

$f : X \to Y$ Or $X \xrightarrow{f} Y$.

Suppose f is a any function from X to Y. Here set X is called **domain** of the function f, and set Y is called **co-domain** of function f. The **image** of a function $f : X \to Y$ is the set $f(X) = \{ f(a) / a \in X \}$. The **pre-image** or inverse image of the function $f : X \to Y$ is the set $f^{-1}(b) = \{a / f(a) \in Y\}$.

The **range** of a function $f : X \to Y$ as the image of its domain. i.e. set $f(X)$.

For the function $y = f(x)$, y is also known as the output corresponding to the input x.

Note: Every element $a \in X$ has an image, but it is not necessary that every element $b \in Y$ also has pre-image in X.

Example-1. State whether the following are the function or not. If $X = \{p, q, r, s\}$ and $Y = \{1, 2, 3, 4\}$. Give reasons and also find the range of the function.

(i) $f = \{(p,1), (q,2), (r,2)\}$.

(ii) $g = \{(p,1), (q,3), (r,2), (q,4)\}$.

(iii) $h = \{(p,1), (q,3), (r,2), (s,4)\}$.

Solution.

(i) Since the element $s \in X$ do not have image in Y, therefore f is not a function from X to Y.

(ii) The element $q \in X$ it has two different images in Y i.e. 3 and $4 \in Y$. Therefore g is not a function from X to Y.

(iii) By definition of function, each element of X has exactly one image in Y. Therefore h is a function from X toY. So range of $h = h(X) = \{1, 2, 3, 4\} = Y$.

Example-2. Let the function $f: X \to \mathbb{R}$ be defined by $f(x) = x^3 + 3x + 2$. If $X = \{-1, 0, 1, 2\}$ then find range of f.

Solution.

Given that f is the function from $X \to \mathbb{R}$. By definition of range we have to find image of each element of X.

$f(-1) = (-1)^3 + 3(-1) + 2 = -2$

$f(0) = (0)^3 + 3(0) + 2 = 2$

$f(1) = (1)^3 + 3(1) + 2 = 6$

$f(2) = (2)^3 + 3(2) + 2 = 16$

Thus the range of f is the set $\{-2, 2, 6, 16\}$.

6.3 TYPES OF FUNCTION:

Definition: A function $f: X \to Y$ is said to be **injective** or **(one–one or monomorphism)** if $x_1, x_2 \in X: f(x_1) \neq f(x_2) \Rightarrow x_1 \neq x_2$ or equivalently $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

Definition: A function $f: X \to Y$ is said to be **surjective** or **(Onto, or epimorphism)**, if every $y \in Y$ such that $y = f(x)$ for some $x \in X$.

A function that is injective and surjective is said to be **bijective**, if $f: X \to Y$ is a bijective function we may write $f: X \simeq Y$. For e.g. Let the function $f: X \to Y$ is defined by

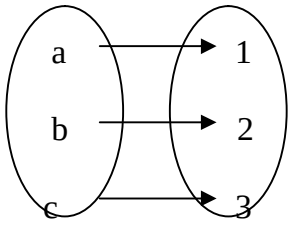


Fig.6.1

Here $f(a) = 1, f(b) = 2, f(c) = 3$.

$\therefore$ $f(x_1) \neq f(x_2) \Rightarrow x_1 \neq x_2$

f is injective. (I)

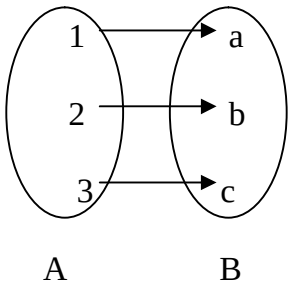
$\because \forall$ $y \in Y$ $\exists$ $x \in X$ So that $f(x) = y$.

$\therefore$ f is surjective. (II)

from I and II we say that
f is bijective.

e.g. If $f : A \to B$, defined by $f(1) = a, f(2) = a, f(3) = b$. Where $A = \{1,2,3\}, B = \{a,b,c\}$. Then check whether the function is bijective or not?

Solution: If $f : A \to B$, defined by $f(1) = a, f(2) = a, f(3) = b$. Where $A = \{1,2,3\}, B = \{a,b,c\}$.



Here, $f(1) = f(2)$ but $1 \neq 2$.
$\therefore$ $f : A \to B$ is not injective.

$\therefore$ $f : A \to B$ is not bijective.
.

Example-3 If function $f : \mathbb{R} \to \mathbb{R}$ is defined by $f(x) = 3x - 1$ then prove that f is bijective.

Solution. We first show that f is injective i.e.
$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$
So we assume that

$f(x_1) = f(x_2)$

$\therefore 3x_1 - 1 = 3x_2 - 1$

$\therefore 3x_1 = 3x_2$ (Adding 1 both side)

$\therefore x_1 = x_2$ (Dividing both side by 3)

$\therefore$ Thus f is injective. (I)

Now to show that f is surjective.

Let y be a real number. We must find value of x such that $f(x) = y$. Thus we must find x such that $y = 3x - 1$ solving,

$$\therefore x = \frac{y+1}{3} \in \mathbb{R}$$

$\therefore$ Thus f is surjective. (II)

from I and II we say that

$\therefore$ f is bijective.

6.4 IDENTITY FUNCTIONS

Definition: A function f on X is said to be **identity function** if $f(x) = x$ for every $x \in X$. It is denoted by I_x and leaves every input unchanged. For e.g. Let $X = \{1,2,3\}$ and $f = \{(1,1),(2,2),(3,3)\}$ which can be written in equation $f(1) = 1$, $f(2) = 2$, $f(3) = 3$ is an identity function of X.

Theorem 6.1. Let $f : X \to Y$ for each subset $A \subseteq Y$,

$f(f^{-1}(A)) \subseteq A$.

Proof. Let $b \in f(f^{-1}(A))$

$\Rightarrow f(a) = b$ for some $a \in f^{-1}(A)$

$\Rightarrow b \in A$

$\Rightarrow f(f^{-1}(A)) \subseteq A$.

Theorem 6.2.If f is function form X onto Y then $f(f^{-1}(A)) = A$.

Proof. Above theorem 4.1 we prove that $f(f^{-1}(A)) \subseteq A$.

For opposite inclusion let $b \in A$ then there exist some element $a \in X$ such that $f(a) = b$ because f onto.

$f(a) = b \in A \Rightarrow a \in f^{-1}(A)$

$\Rightarrow f(a) \in f(f^{-1}(a))$

$\Rightarrow b \in f(f^{-1}(A))$

$A \subseteq f(f^{-1}(A))$

Hence $f(f^{-1}(A)) = A$.

Theorem 6.3. Let function $f : X \to Y$ for each subset $A \subseteq X$;

Then $A \subseteq f^{-1}(f(A))$.

Proof: Let $f : X \to Y$ for each subset $A \subseteq X$.

Let $a \in A \Rightarrow f(a) \in f(A)$

$\Rightarrow a \in f^{-1}(f(A))$ (By definition of pre-image)

$\Rightarrow A \in f^{-1}(f(A))$.

Hence $A \subseteq f^{-1}(f(A))$.

Theorem.6.4. If f is one-to-one function from X onto Y, then
$A = f(f^{-1}(A))$.

Proof. In above theorem we prove that $A \subseteq f^{-1}(f(A))$.

Let $a \in f(f^{-1}(A)) \Rightarrow f(a) = f(A)$
$\Rightarrow f(a) = f(a')$ For some $a' \in A$.
$\Rightarrow a = a'$ Since f is one-to-one.
$\Rightarrow a \in A$
$\Rightarrow f(f^{-1}(A)) \subseteq A$.

Hence $A = f(f^{-1}(A))$.

6.5 COMPOSITE FUNCTION

Definition: Let $f: X \to Y$ and $g: Y \to Z$ then the composite of the function f and g denoted by (gof) is a function of $X \to Z$ given by $(gof): X \to Z$ such that $(gof)(x) = g[f(x)], \forall x \in X$.

For e.g. Let $X = \{p, q, r\}$, $Y = \{1, 2, 3\}$ and $Z = \{c, d, e\}$. Let $f: X \to Y$ and $g: Y \to Z$ be defined by $f = \{(p, 2), (q, 1), (r, 3)\}$ and $g = \{(1, d), (2, c), (3, e)\}$. Then the composite function $(gof): X \to Z$ may be computed in the following manner: $(gof)(p) = g[f(p)] = g(2) = c$,
$(gof)(q) = g[f(q)] = g(1) = d$, $(gof)(r) = g[f(r)] = g(3) = e$.
Thus $(gof): X \to Z$ is given by $(gof) = \{(p, c), (q, d), (r, e)\}$.

Example-4: Let $f: \mathbb{R} \to \mathbb{R}$ is defined by $f(x) = x + 1, \forall x \in \mathbb{R}$,
And the function $g: \mathbb{R} \to \mathbb{R}$ is defined by $g(x) = x^2, \forall x \in \mathbb{R}$.
Find gof and fog.

Solution: Let the composite function $gof: \mathbb{R} \to \mathbb{R}$ is given by $(gof)(x) = g[f(x)] = g(x+1) = (x+1)^2$. And the composite function $fog: \mathbb{R} \to \mathbb{R}$ is given by $(fog)(x) = f[g(x)] = f(x^2) = x^2 + 1$.
$\therefore gof \neq fog$
Remark; In general the composite function is not commutative.

Theorem 6.5. If $f: W \to X$, $g: X \to Y$ and $h: Y \to Z$, then
$(hog)of = ho(gof)$.

Proof. It is clear that $(hog)of$ and $ho(gof)$ is the function from W to Z. This two function will be equal if they have the same image to each element $x \in W$.

Now, $((hog)of)(x) = (hog)(f(x))$
$= h(g(f(x)))$
$= h(gof(x))$
$= (ho(gof))(x)$
Which shows that $(hog)of = ho(gof)$.

6.6 INVERSE FUNCTION

Definition: Let $f: X \to Y$ be a one-to-one function. The **inverse** of function denoted by f^{-1}, is the set of $f^{-1} = \{(y,x)/(x,y) \in f\}$.
This, if $f: X \to Y$ is a one-to-one function, then $f(x) = y \Rightarrow x = f^{-1}(y)$ for $x \in X$ and $y \in Y$.

Theorem 6.6. The inverse of a one-to-one and onto function is unique.

Proof. Let $f: X \to Y$ be one-to-one and onto function. Let $g: Y \to X$ and $h: Y \to X$ be two different inverse function of f.
Then for $x_1, x_2 \in X$ there exists $y \in Y$ such that $g(y) = x_1$, $h(y) = x_2$.
$\therefore g(y) = x_1 \Rightarrow y = f(x_1)$ $\because$ g is the inverse of f.

$\therefore h(y) = x_2 \Rightarrow y = f(x_2)$ $\because$ h is the inverse of f.
Then it follows that $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. $\because$ f is one-to-one.
$\Rightarrow g(y) = h(y)$ For $y \in Y$.
Hence the inverse of a one-to-one and onto function is unique.

Theorem 6.7. The inverse of a one to one function is one to one and onto.

Proof. Let $f: X \to Y$ be one-to-one and onto function.
Then for $x_1, x_2 \in X$ there exists $y_1, y_2 \in Y$ such that $f(x_1) = y$ and $f(x_2) = y_2 \Rightarrow x_1 = f^{-1}(y_1)$ and $x_2 = f^{-1}(y_2)$.
Now for $y_1, y_2 \in Y$,
$f^{-1}(y_1) = f^{-1}(y_2) \Rightarrow x_1 = x_2$
$\Rightarrow f(x_1) = f(x_2)$
$\Rightarrow y_1 = y_2$
This proves that f^{-1} is one-to-one.

Again since f is onto, then for $y \in Y$ there exists some $x \in X$ such that $f(x) = y \Rightarrow x = f^{-1}(y)$ $\because$ f is one-to-one
This proves f^{-1} is onto.

Example-5 If function $f:\mathbb{R}\to\mathbb{R}$ be defined by $f(x)=2x+3$ for every $x\in\mathbb{R}$, has its inverse (f is invertible). Find formula for f^{-1}.

Solution: Let $f:\mathbb{R}\to\mathbb{R}$ be defined by $f(x)=2x+3$ for if $x_1,x_2\in\mathbb{R}$ then $f(x_1)=f(x_2)\Rightarrow 2x_1+3=2x_2+3$

$\Rightarrow 2x_1=2x_2$ (Adding -3 both side)

$\Rightarrow x_1=x_2$ (Divide by 2 both side)

This proves that f is one-to-one. (f is injective) I

Again, if $y\in\mathbb{R}$, $y=f(x)\Rightarrow y=2x+3$

$$\Rightarrow x=\frac{y-3}{2}$$

Thus for $x\in\mathbb{R}$ there exists $\frac{1}{2}(y-3)\in\mathbb{R}$ such that

$$f\left(\frac{1}{2}(y-3)\right)=2\left(\frac{1}{2}(y-3)\right)+3$$

$$=y-3+3=y.$$

This proves that f is onto. (f is surjective) II

$\therefore$ From I and II we say that f is bijective.

$\therefore$ f^{-1} is exists and it is defined by

$$f^{-1}(y)=\frac{1}{2}(y-3)\in\mathbb{R}.$$

Example.6. If each functions f and g is one-to-one then function gof is one-to-one.

Solution: Let $f:X\to Y$ and $g:Y\to Z$ is one-to-one function.

Let $x_1,x_2\in X$ then $gof(x_1)=gof(x_2)$

$\Rightarrow g(f(x_1))=g(f(x_2))$

$\Rightarrow f(x_1)=f(x_2)$ $\because$ (g is one-to-one)

$\Rightarrow x_1=x_2$ $\because$ (f is one-to-one)

Hence function gof is one-to-one.

Examlpe.7. If each function f and g is onto then function gof is onto.

Solution: Let $f:X\to Y$ and $g:Y\to Z$ is onto function.

By definition of composite function $gof:X\to Z$ .To prove that gof is onto we have to prove that every element $z\in Z$ is an image element for some $x\in X$ under gof . Since g is onto $\exists$ $y\in Y$ such that $g(y)=z$. Again f is onto $\exists$ $x\in X$ such that $f(x)=y$.

Now, $gof(x)=g(f(x))=g(y)=z$.

Hence function gof is onto.

Example.8. Let A and B be two non-empty sets. Let $f : A \to B$ be the function then prove that, If A_1 and A_2 subset of A so that $A_1 \subseteq A_2$ then $f(A_1) \subseteq f(A_2)$. Is the converse true?

Solution: Let $y \in f(A_1)$ $\exists$ $x \in A_1$ such that $y = f(x)$.
Since $A_1 \subseteq A_2$, $x \in A_2$ such that $y = f(x)$.
$\therefore f(x) \in f(A_2) \Rightarrow y \in f(A_2)$
$\Rightarrow f(A_1) \subseteq f(A_2)$.
But the converse is not true.
To show that the converse is not true we give counter example.
Let $f : A \to B$ be the function. $f(a) = 1$, $f(b) = 1$, $f(c) = 2$
$\therefore A = \{a, b, c\}$, $B = \{1, 2\}$
Let $A_1 = \{a, c\}$ and $A_2 = \{a, b\}$ be the subset of A.
$\therefore f(A_1) = \{1, 2\}$ and $f(A_2) = \{1, 2\}$.
$\Rightarrow f(A_1) = f(A_2)$
$\Rightarrow f(A_1) \subseteq f(A_2)$ But $\Rightarrow A_1 \not\subset A_2$.

EXERCISE 6.1

1. Decide whether or not the following are functions from A to B where $A = \{a, b, c, d, e\}$ and $B = \{p, q, r, s\}$. If they are function, give the range of each. If they are not tell, why?
(i) $f = \{(a, p), (c, q), (e, s), (d, r)\}$.
(ii) $g = \{(a, t), (e, s), (c, p), (b, r)(a, s), (d, p)\}$.
(iii) $h = \{(a, p), (b, s), (c, t), (d, q), (e, r)\}$.

2. Each of the following formulas defines a function from $\mathbb{R}$ to $\mathbb{R}$. Find the range of each of the function.
(i) $f(x) = x^3$.
(ii) $g(x) = \sin x$.
(iii) $h(x) = x^2 + 1$.

3. Let $\mathbb{Q}$ be the set of rational numbers. Let $f : \mathbb{Q} \to \mathbb{Q}$ be defined by $f(x) = 2x + 3, x \in \mathbb{Q}$. Show that f is bijective. Also find a formula that the inverse function f^{-1}.

4. Prove the following two result for a finite set T:
(i) If f maps T onto T then f is one-to-one.
(ii) If f is a one- to-one mapping of T into itself, then f is onto.

5. Let $X = \mathbb{R} - \{3\}$ and $Y = \mathbb{R} - \{1\}$ where $\mathbb{R}$ is the set of real numbers. Let the function $f : X \to Y$ be defined by $f(x) = \frac{x-2}{x-3}$ is this function is bijective?

6. Prove that identity function of set T into itself is one-to-one and onto.

7. If $f : X \to Y$ and $g : Y \to Z$ be two one-to-one and onto function, then $gof : X \to Z$ is also one-to-one and onto also Show that $(gof)^{-1} : Z \to X = (f^{-1}og^{-1})Z \to X$.

6.7 BINARY OPERATION

The basic idea underlying the definition of an algebraic structure is that of a set with a binary operation. Suppose we have a set A of objects with the property that any pair of them x and y, can be combined in some way to form an objects z. This can be expressed by the equation

$$x * y = z$$

Where the $*$ indicates a binary operation. The word binary signifying here that two objects are involved. The most familiar examples are the arithmetical operation like + and $\times$ defined on the set of integers $\mathbb{Z}$.

Definition: Given a set of element A, then a binary operation $*$ on the set A is a rule of combination which assigns to each ordered pair of element $a, b \in A$ a unique element $c \in A$. We write symbolically that $c = a * b$.

Example.9. Let $\mathbb{N}$ be the set of all natural numbers then the operation of addition on the set $\mathbb{N}$ is a binary operation for if $a, b \in \mathbb{N}$ then so is c where $c = a + b$.

Example.10. Let A be the of all odd integers then the operation of addition on the set A is not a binary operation for if $a, b \in A$ then $c \notin A$ where $c = a + b$.

Remark: Addition, Multiplication are the binary operation in $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

Subtraction is binary operation in $\mathbb{Z}, \mathbb{R}$. Division is not a binary operation.

6.8 PROPERTIES OF BINARY OPERATION

Commutative: A binary operation * on a set of element A is said to be commutative, if and only if, for $a, b \in A$,

$$a * b = b * a$$

Associative: A binary operation * on a set of element A is said to be associative, if and only if, for every $a, b, c \in A$,

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

Distributive: A binary operation * on a set of element A is said to be distributive over the binary operation on the same set A elements if and only if for every $a, b, c \in A$,

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

Identity element: An element e in a set A is said to be a identity element with respect to the binary operation * on A if and only if for every $a \in A$,

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

Inverse element: An element b is in a set A is said to be inverse element of an element $a \in A$ with respect to the binary operation *, if and only if,

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

Example.11. Check the following operation is commutative and associative. $a * b = a + b - 10$, For every $a, b \in \mathbb{Z}$.

Solution: For every $a, b \in \mathbb{Z}$.

(i) $a * b = a + b - 10$
$= b + a - 10$
$= b * a$

$\therefore$ '*' is a commutative.

(ii) $a * (b * c) = a * (b + c - 10)$
$= a + b + c - 10 - 10$
$= a + b + c - 20$ I

$(a * b) * c = (a + b - 10) * c$
$= a + b - 10 + c - 10$
$= a + b + c - 20$ II

From I and II we say that,

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

$\therefore$ '*' is an associative.

Example.12. The binary operation * on the set of all real numbers are defined by $a*b=|a-b|$. Show that the * is commutative but not associative.

Solution: Since $a*b=|a-b|$

$$=|b-a|$$

$$=b*a$$

$\therefore$ '*' is a commutative.

Again,

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

$$=||a-b|-c|$$

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

$$=|a-|b-c||$$

If $a=1,b=2,c=5$ then

$$(a*b)*c=||1-2|-5|=|1-5|=4$$

$$a*(b*c)=|1-|2-5||=|1-3|=2$$

$\therefore$ '*' is not associative.

Example.13. A binary operation * is defined on $\mathbb{Q}-\{0\}$ as $a*b=\frac{ab}{9}.\ \forall a,b\in\mathbb{Q}-\{0\}$

Show that the * is closed under commutative, associative and also find identity and inverse element of the binary operation.

Solution: For $\forall a,b,c\in\mathbb{Q}-\{0\}$,

(i) $a*b=\frac{ab}{9}=\frac{ba}{9}=b*a$

$\therefore$ '*' is a commutative.

(ii) $(a*b)*c=\left(\frac{ab}{9}\right)*c=\frac{\left(\frac{ab}{9}\right)c}{9}=\frac{abc}{81}$

$$a*(b*c)=a*\left(\frac{bc}{9}\right)=\frac{a\left(\frac{bc}{9}\right)}{9}=\frac{abc}{81}$$

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

$\therefore$ '*' is associative.

(iii) Let e be an identity element in $\mathbb{Q}-\{0\}$ with respect to '*'.

$a*e=a$

$\therefore \frac{a*e}{9}=a$

$\therefore e=9 \qquad \because 9\in\mathbb{Q}-\{0\}, a\neq 0$

$\therefore e=9$ be an identity element in $\mathbb{Q}-\{0\}$ with respect to '*'.

(iv) Let b be an inverse element in $\mathbb{Q}-\{0\}$ with respect to '*'.

$a*b=e$

$\therefore a*b=9 \qquad \because e=9$

$\therefore \frac{ab}{9}=9$

$\therefore b=\frac{81}{a}$

$\therefore b=\frac{81}{a}$ be an inverse element in $\mathbb{Q}-\{0\}$ with respect to '*'.

Exercise 6.2

1. Check whether the following binary operation defined on corresponding set is commutative or associative.

(i) $a*b=2a-b$ for $a,b\in\mathbb{Z}$

(ii) $a*b=a+b-3$ for $a,b\in\mathbb{Z}$

(iii) $a*b=|2a-3b|$ for $a,b\in\mathbb{R}$

(iv) $a*b=a^2b$ for $a,b\in\mathbb{R}$

2. Find identity and inverse of element in $\mathbb{Z}$.
Where $a*b=a+b-10$, $\forall a,b\in\mathbb{Z}$.

3. A binary operation * is defined as $a*b=\frac{a^2b^2}{4}, \forall a,b\in\mathbb{Q}-\{0\}$,
Show that * is commutative and associative also find identity and inverse element in $\mathbb{Q}-\{0\}$ with respect to '*'.

6.9 REVIEW

In this chapter we have covered the following points:

- Function and term related to function (range, image, Pre-image).
- Injective function, surjective function and bijective function.
- Identity function, composite function, inverse function.
- Binary operation and their property.

6.10 UNIT END EXERCISE

1. Define the term give example of each term.: function, range of function, Image of function, pre-image of the function.

2. Explain all the of function with their definition and counter example.

3. Decide whether or not the following are functions from A to B where $A=\{p,q,r,s,t,u\}$ and $B=\{a,b,c,d\}$. If they are function, give the range of each. If they are not tell, why?
(i). $f=\{(p,a),(q,b),(s,c),(r,d)\}$
(ii) $g=\{(t,a),(s,a),(p,c),(r,b)(s,d)\}$.
(iii) $h=\{(p,a),(s,b),(t,d),(q,c)\}$.

4. Each of the following formulas defines a function from $\mathbb{R}$ to $\mathbb{R}$. Find the range of each of the function.
(i) $f(x)=x^3+2$.
(ii) $g(x)=\cos\theta$.
(iii) $h(x)=x^3+5x-6$.

5. Find the image set of the function $f:\mathbb{R}\to\mathbb{R}$ defined by $f(x)=\dfrac{3x}{x^2+1}$.

6. Let $\mathbb{Q}$ be the set of rational numbers. Let $f:\mathbb{Q}\to\mathbb{Q}$ be defined by $f(x)=9x-4$, $x\in\mathbb{Q}$. Show that f is bijective. Also find a formula that the inverses function f^{-1}.

7. Let $X=\mathbb{R}-\left\{\dfrac{5}{2}\right\}$ and $Y=\mathbb{R}-\{0\}$ where $\mathbb{R}$ is the set of real numbers. Let the function $f:X\to Y$ be defined by $f(x)=\dfrac{1}{2x-5}$ is this function is bijective?

8. Show that $f:\mathbb{R}\to\mathbb{R}$ is given by $f(x)=|x|$ are neither injective nor surjective.

9. Let the functions $f:\mathbb{Z}^+\to\mathbb{R}, f(x)=\dfrac{2}{x+1}$, $g:\mathbb{Z}\to\mathbb{Z}, g(x)=x^2+3$ and $h:\mathbb{R}\to\mathbb{R}, h(x)=3x+2$ then determine the following composite function (i) hog, (ii) fog, (iii) gof, (iv) foh, (v) hof, (vi) goh.

10. Let $f:\mathbb{R}\to\mathbb{R}$ and $g:\mathbb{R}\to\mathbb{R}$ be two function given by $f(x)=|x|+x$ for all $x\in\mathbb{R}$ and $g(x)=|x|-x$ for all $x\in\mathbb{R}$. Find *fog* and *gof* .

11. Let $f:A\to B$ be a function. If $B_2\subseteq B_1\subseteq B$, then show that $f^{-1}(B_2)\subseteq f^{-1}(B_1)$.

12. Check whether the following binary operation defined on corresponding set is commutative or associative.

(i) $a*b=a^b b^a$ for $a,b\in\mathbb{Z}$

(ii) $a*b=2a+2b-8$ for $a,b\in\mathbb{Z}$

(iii) $a*b=2^{ab}$ for $a,b\in\mathbb{R}$

(iv) $a*b=ab+a+b$ for $a,b\in\mathbb{R}$

13. Find identity and inverse of element in $\mathbb{Z}$ .Where $a*b=a+b-3$, $\forall a,b\in\mathbb{Z}$.

7

PIGEONHOLE PRINCIPLES

Unit structure:

7.0 OBJECTIVE

After going through this chapter you will be able to:

- learn different counting techniques like Pigeonhole Principle
- define cardinality of sets
- learn about the properties related to cardinality of sets

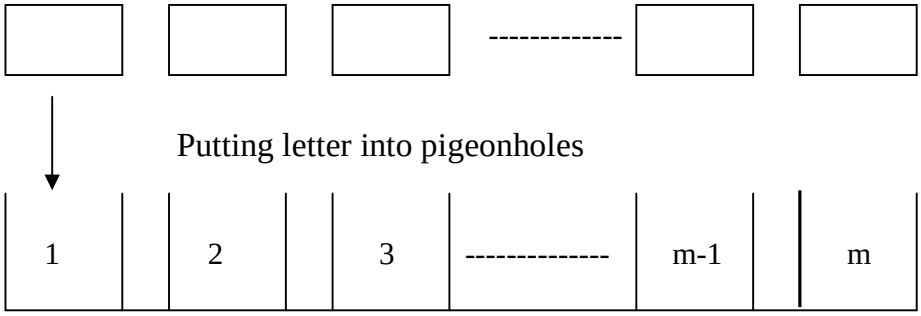
7.1 INTRODUCTION

This chapter dedicated to the study of 'size' of sets and also we show how one can efficiently do the counting in a variety of situations. We represent the basic principle of counting which is easily derived and extremely useful. We know that some sets are not finite there for **Cantor** gives cardinality of infinite sets in 1870's and 1881's.

Suppose there are 7 peoples working in an office and a pile of 8 letters is delivered. Each letter is addressed to are of the people in the office, and letter are put in the appropriate pigeonholes. Then we know for sure that some are is going to be lucky and get more then one letter. Generally it seen obvious that **if** $n > m$ **and** n **letters are put into** m **pigeonholes then one pigeonhole will receive more then one letter.**

If the statement is obvious then so also must be its cantrapositive, because that is logically equivalent to it. The cantrapositive is: if every pigeonhole receives at most one letter, then $n \leq m$.

Now we can formulate a purely mathematical form of this principle we suppose that the letters are numbered $1, 2, 3, 4 - - - -, n$ and the pigeonholes are numbered $1, 2, 3, 4 - - - -, m$ for each letter the address tells us which pigeonhole should receive it. Thus in mathematical terms we have a rule for assigning letters to pigeonholes that is a function from set $\mathbb{N}_n$ to the set $\mathbb{N}_m$. The condition that every pigeonhole receives at most one letter is equivalent to the condition that this function is an injection.



Thus the cantra positive from the original statements essentially: if a function $\mathbb{N}_n \to \mathbb{N}_m$ is an injection.

Then it must follow that $n \leq m$. Now we know that what we have to prove.

Theorem : 7.1 Let m be a natural number then the following statements true for every natural number n if there is an injection from $\mathbb{N}_n$ to the set $\mathbb{N}_m$ then $n \leq m$.

Proof : We use the principle of induction. The statement is true when $n = 1$, since $1 \leq m$ for any natural number m. The induction hypothesis is that the statement is true when n taking a specific value $k \geq 1$. We have to deduce that it is true when $n = k + 1$.

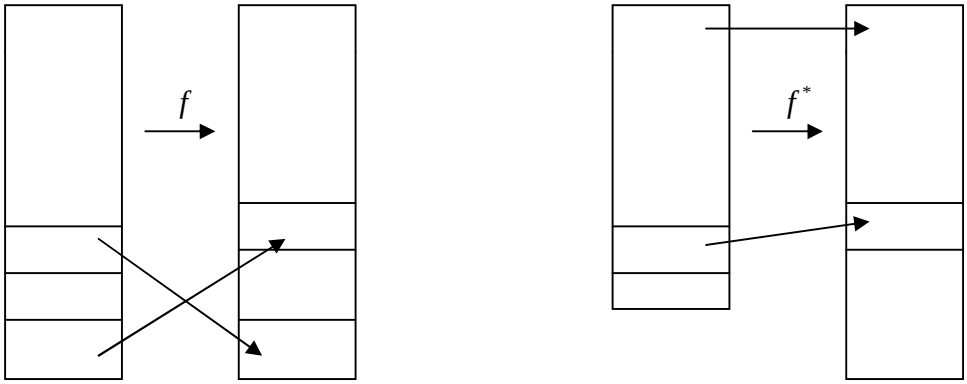
Suppose that $f : \mathbb{N}_n \to \mathbb{N}_m$ is an injection. Since $k + 1 \geq 2$ it follows that m can not be 1. So $m = s + 1$ for some natural number s. In order to show that $k + 1 \leq m = s + 1$. We construct an injection $f : \mathbb{N}_k \to \mathbb{N}_s$ and uses the induction hypothesis conclude that $k \leq s$. There are two cases:

(I) Case:1: Suppose that $f(x) \neq s+1$ for all $x \in \mathbb{N}_k$. Then let be the injection defined by $f^*(x) = f(x)$ for all $x \in \mathbb{N}_k$.

(II) Case:2: Suppose that there is an $x \in \mathbb{N}_k$ such that $f(x) = s+1$. Then $f(k+1) = y$. Where (since f is injection) $y \neq s+1$ in this case defined f^* as follows.

$$f^*(x) = y, \quad f^*(z) = f(z) \ \ (z \neq x).$$

It is easy to check f^* is an injection $\mathbb{N}_n$ to $\mathbb{N}_m$.



The theorem is contrapositive from the original statement:
If $n > m$ **then there is no injection from** $\mathbb{N}_n \to \mathbb{N}_m$

7.2 PIGEONHOLE PRINCIPLE

We represent the basic principle of counting which is easily derived and extremely useful.

Statement: If there n-pigeons to be placed in m-pigeonhole where $m < n$. Then there is at least one pigeonhole which receives more then one pigeon.

Pigeonhole Principle

Here is a simple consequence of the pigeonhole principle.

In one set 13 or more people there are at least two whose birthdays fall in the same month.

In this case we have to think of putting the people in to pigeonhole. it can be January, February, March and so on. Since there are 13 people and only 12 pigeon holes one of the pigeonhole must contain at least two people.

That this intuitively obvious result can be quite useful is illustrated by the following example.

Example 1:

If eight people are chosen in any way what so ever at least two of them will have been born on the same day of the week.

Solution :

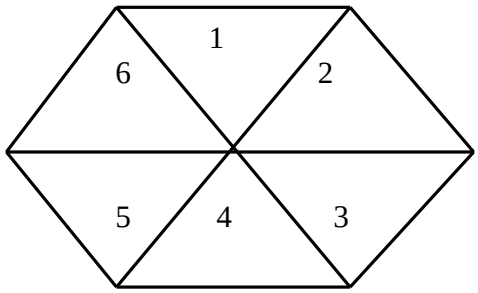
Here each person (pigeon) is assigned the day of the week (pigeonhole) on which he and she was born since there are eight people and only seven days of the week, the pigeonhole principle. Tells us that at least two people must be assigned to the same day.

Example 2:

Consider the area shown it is bounded by a regular hexagon. Whose sides have length 1units. Show that if any seven points are chosen with in this area then two of them must be on further apart then 1 unit.

Solution:

Suppose that the area is divided in to six equilateral triangles. As shown in figure 1.1



If seven points are chosen we can assign each one to a triangle that contains it.

If the point belongs to several triangles, assigns it arbitrarily to one of them. The seven points one assigned to six triangles so by

pigeonhole principle, at least two points must belong to the same triangle. These two can not be more then 1 unit apart.

Example 3 :

Five points are located inside a square whose sides are of length 2. Show that two of the points are within a distance $\sqrt{2}$ of each other.

Solution :

Divide up the square into four square regions of area 1 unit. as indicated in figure 1.2.

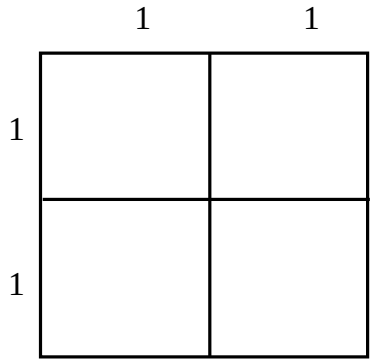


fig.1.2

By Pigeonhole principle, it follows that at least one of these regions will contain at least two points. The result now follows since two points in a square of radius 1.can not be further apart then length of the diagonal of the square is which (**by Pythagoras theorem**) $\sqrt{2}$.

Example 4 :

Show that if any five numbers from 1 to 8 are chosen, then two of then will add to 9.

Solution :

Constructs four different sets each contains two numbers that add to 9, as follows $A_1 = \{1,8\}, A_2 = \{2,7\}, A_3 = \{3,6\}, A_4 = \{4,5\}$ each of the five numbers chosen will be assigned to the set that contains it .Since there are only four sets. The pigeonhole principle tells that two of the chosen numbers will be assigned to the same set. These two numbers will add to 9.

Example 5 :

Fifteen children together gathered 100 nuts. Prove that some pair of children gathered the same numbers of nuts.

Solution :

Now to prove that we use method of contradiction.

Suppose all the children gathered a different numbers of nuts. Then the fewest total number is $0+1+2+3+4+5+6+----+14=105$, but this is more then 100. Which is contradiction to our assumption. There fore at least pair of children gathered same number of nuts.

Example 6 :

Show that in any set of 10 integers there are at least pair of integers who have same remainder when divided by 9.

Solution :

Set of 10 integers, when it divide by 9, lie in the same residue classes of modulo 9. i.e. the remainder is 0,1,2,3,4,5,6,7,8. Here there will be 9 remainder and 10 integers. There fore by pigeonhole principle, at least one integer has same remainder.

Example 7 :

Any 7 numbers are chosen from 1-12. Show that,

(i). Two of them will add to 13.

(ii). There are two respectively prime integers.

(iii). There are two integers such that 1 is a multiple of the other.

Solution :

(i). We form the box different sets (boxes) each containing two integers from 1-12 with their sum as 13 as follows.

{1, 12}	{4, 9}
{2, 11}	{5, 8}
{3, 10}	{6, 7}

These six sets are the boxes and the 7 integers chosen from 1-12 are objects each of these 7 integers will be arranged if the set that contains it since there are only 6 boxes and 7 objects By Pigonhole principle, two of the selected numbers will be arranged to the same box, hence there sum will be 13.

(ii). Two numbers are said to be relatively prime if their G.C.D is 1.

We form 6 different boxes containing two integers form 1-12 such that they are respectively prime as follows,

{1, 2}	{7, 8}
{3, 4}	{9, 10}
{5, 6}	{11, 12}

Since each set contains consecutive integers.

∴ They are relatively prime each of these 7 integers will be assigned to the set that contain it these 6 sets are boxes and 7 integers are chosen from 1-12 are objects.

Since there are only 6 boxes and 7 objects 6 < 7.

By pigeonhole principle selected numbers will be arranged to the same box that is their exists two numbers which are relatively prime.

(iii). Let A_1, A_2,…….A_7 be seven chosen numbers from 1-12.

We known that any integers n can be written in the form n = 2^km where k ≥ 0 km. is an odd number.

$$1 = 2^0 \cdot 1$$

$$2 = 2^1 \cdot 1$$

$$3 = 2^0 \cdot 3$$

$$4 = 2^2 \cdot 1$$

$$5 = 2^0 \cdot 5$$

$$6 = 2^1 \cdot 3$$

$$7 = 2^0 \cdot 7$$

$a_1 = 2^{k1}\ x_1$, $a_2 = 2^{k2}\ x_2$……. $a_7 = 2^{k7}\ x_7$

Where $k_i \geq 0$.

X_i is an odd integer……..i=1,2,…….,7.

Each a_i is assigned to the odd integer x_i where x_i is such that $a_i = 2^{kl}.a_i$.

Where $k_i \geq 0$.

Corresponding to u chosen integer a_1, a_2,…….,a_7 we have 7 odd integers.

x_1, x_2,…….,x_7 but we have only 6 odd integers from 1-12.

∴By Pigonhole principle a_i's corresponding to the same x_i.

i.e.7i ,j such that I ≠ j

$1 \leq i \leq 7$

$1 \leq j \leq 7$ and $x_i = x_j$

$a_i = 2^{ki}.x_i$

$a_j = 2^{kj}.x_j$

$a_j = 2^{kj}.x_i$ [xi = xj]

if xi= xj then $2^{kj}/2^{ki}$

$= 2^{kj_{xi}}/2^{ki_{xi}}$

$= a_j/a_i$

a_i is a multiple of a_j.

if $x_i \geq x_j$ then $2^{kj}/2^{ki}$

$= 2^{kj_{xi}}/2^{ki_{xi}}$

$= a_j/a_i$

a_j is a multiple of a_i.

There for their exist two integers such that one is a multiple of another.

Example 8.Show that in any set of 12 integers there are 2 whose difference is divisible by 11.

Solution :-

Let A_1, A_2,…….A_{12} be 12 selected integers by division algorithm, 7 unique q_i and r_i.
s.t. $A_i = q_i + r_i$ where $0 \leq r_i \leq 11$
i.e. $0 \leq r_i \leq 10$
each q_i is assigned to its remainder r_i.
A_1, A_2,…….A_{12} corresponds to r_1, r_2,…….r_{12} but use have only 11

Remainders {0,1,2,……,10}
When a no. is divided by 11
∴The remainders are 12 i.e. r_1, r_2,…….r_{12} but possible remainders are 11.
i.e. 0,1,……..11
∴By Pigonhole principle, two remainders are same i.e.i , j

s.t.i ≠ j, $r_i = r_j$ $1 \leq i \leq 12$,
$1 \leq j \leq 12$

$a_i = 11q_i + r_i$
$a_j = 11q_j + r_j$
$= 11q_j + r_i$ ($r_i = r_j$)
i.e. $11/a_i - a_j$

∴two whose difference is divisible by 11.

Two whose difference is a multiple of 11.

7.3 THE EXTENDED PIGEONHOLE PRINCIPLE

If there n-pigeons are assigned to m-pigeonholes, then one of the pigeonhole must contain at least $\left[\frac{(n-1)}{m}\right]+1$ pigeons.

Proof: If each contain number more then $\left[\frac{(n-1)}{m}\right]$ pigeons, then there are at most $\left[\frac{(n-1)}{m}\right] \le m\frac{(n-1)}{m} = n-1.$

A pigeon in all this contradicts our assumption. So one of the pigeonholes must contain at least $\left[\frac{(n-1)}{m}\right]+1$ pigeons.

Example 9: Show that if 30 dictionaries in a library contains a total of 61,327 pages, then one of the dictionaries must have at least 2045 pages.

Solution: Let the pages be the pigeons and the dictionaries are the pigeonholes. Assigns each to the dictionaries in which it appears then by the extended pigeonhole principle are dictionary must contain at least $\left[\frac{(61,327-1)}{30}\right]+1=\frac{61,326}{30}+1=2045$ pages.

Example 10: Show that if any 29 people are selected then one may choose subset of 5. So that all 5 were born on the same day of the week.

Solution: Assign each person to the day of week on which he and she was born. Then $n=29$ persons are being assigned to $m=7$ pigeonholes. By the extended pigeonholes principle at least $\left[\frac{(n-1)}{m}\right]+1=\left[\frac{(29-1)}{7}\right]+1=\frac{28}{7}+1=5$ persons.

There fore 5 persons must have been born on the same day of the week.

Check Your Progress :

1. Show that if there are seven numbers from 1 to 12 are chosen then two of them will add to 13.

2. Let T be an equilateral triangle whose sides has length 1 unit. Show that if any five point are chosen lying on inside T. Then two of them will be more then $\frac{1}{2}$ unit apart.
3. Show that if any Eight positive integer are chosen two of them will have the same remainder when divided by 7.
4. Show that if seven colors are used to paint 50 bicycles at least eight bicycles must have the same colors.
5. All 82 entering student of a certain high school take courses in English, History, Maths and science. If three section of each of these four subjects. Show that there are two students that have all four classes together.
6. Nineteen points are chosen inside a regular hexagon whose side length 1. Prove that two of these points may be chosen whose distance them is less then $\frac{1}{\sqrt{3}}$.
7. In any group of 15 people there are at least three born on the same day of the week?

7.4 LET US SUM UP

In this chapter we have covered the following points:

- If $m < n$ then there cannot be an injection from $\mathbb{N}_n$ to $\mathbb{N}_m$.
- Pigeon hole Principle.
- Extended Pigeonhole Principle and Application of pigeon hole principle.

7.5 UNIT END EXERCISES

1. Prove that, if $m < n$ then there cannot be an injection from $\mathbb{N}_n$ to $\mathbb{N}_m$.
2. Write the statement of pigeon hole principle and explain with example.
3. 10 people want to go to the movies, and there are only 7 cars, then at least more then one person in the same car.
4. Prove that among the 51 positive integers less then 100. There is a pair whose sum is 100.

5. There are 33 students in the class and sum of their ages 430 year. Is it true that one can find 20 students in the class such that sum of their ages greater 260?
6. Show that in any set X of people, there are two members of X who have the same number of friends in X.
7. Seven darts are thrown onto a circular dartboard of radius 10units. Can we show that there will always be two darts which are at most 10 units apart?
8. Nineteen darts are thrown onto a dartboard which is shaped as a regular hexagon with side length of 1 unit. Can we prove that there are two darts within $\frac{\sqrt{3}}{3}$ units of each other?
9. How many friends must you have to guarantee that at least five of them will have birthdays in the same month?
10. Show that there must be at least 90 ways to choose six numbers from 1 to 15 so that all the choices have the same sum.

8

GRAPH THEORY-I

Unit Structure :

8.0 OBJECTIVES

- Fundamental concepts of graphs
- Types of graphs
- Isomorphism of graphs
- Concept of connectedness in graph

8.1 INTRODUCTION

Graph theory is a subject where no previous knowledge is assumed. In this subject the focus is on understanding the structure of graphs and the techniques used to analyse problems in Graph theory. This subject have many applications in different areas right from computing to social sciences and to natural sciences. One of the standard ways of maintaining a graph in the memory of computer is by means of its adjacency matrix. In simple words a graph is collection of points and a collection of pairs of points (edges). Some of the graphs look like.

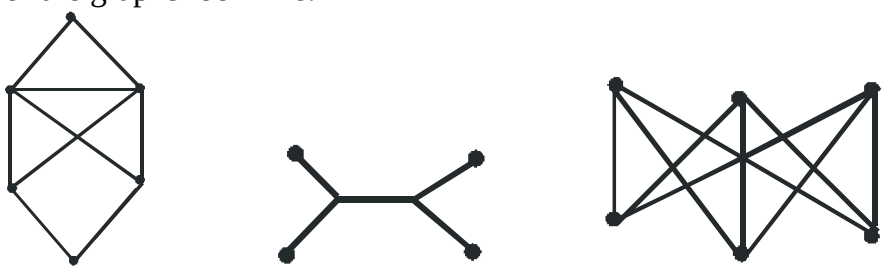


Fig. 8.1

8.2 APPLICATION OF GRAPHS

A graph can be used to represent almost any physical situation involving discrete objects and relationship among them. Some of examples given below are from among hundreds of application.

1. Konigsberg Bridge Problem :-

This exciting problem is said to have given birth to graph theory. The city of Konigsberg is located on the Pregel river in Prussia. The city occupied the island of Kneiphopf (A) plus areas on both banks. These regions were linked by seven bridges as shown below in Fig 8.2 (a). The citizens of Konigsberg had a problem to start from their home, cross every bridge exactly once and return home. This problem was represented using dots for land masses and curves for bridges Fig. 8.2 (b).

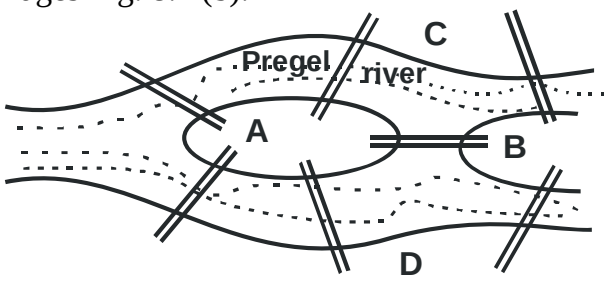


Fig. 8.2 (a)
The bridges of Konigsberg

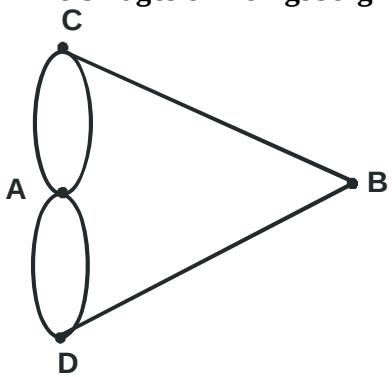


Fig. 8.2 (b)
Graphical representation of Konigsberg bridge problem

Euler first represented this situation by means of graph and proved that the solution for this problem does not exist using Eulerian graphs.

2. Travelling salesman problem :-

This problem is stated as follows : A salesman is required to visit a number of cities during a trip. Given the distance between the cities, in what order should he travel so that he travels as minimum as possible?

In the graph theory, the cities are represented by vertices and the roads by edges. There is a real number associated with each edge e_i in a graph. Such a graph is called weighted graph. $w(e_i)$ is weight of edge e_i.

This problem amounts to finding minimum weight Hamiltonian circuit in a weighted Hamiltonians graph. No efficient algorithm for solving this problem is known. However, it is possible to obtain reasonably good but not necessarily optimal solution.

3. Four colour problem :-

The four colour problem is a partitioning problem. Partitioning is applicable in many practical problems such as coding theory, partitioning of logic in digital computers and state reduction of sequential machines.

This problem is related to colouring of a map. A map is a partition of the plane into connected region. Can we colour the regions of given map using atmost four colours so that neighbouring regions have different colours?

In graph theory, the vertex is considered as a region and an edge represents regions sharing a boundary. The problem is whether the resulting graph have chromatic number atmost 4. A graph can be drawn in a plane without crossing edges, such graphs are planar graphs.

The four colour problem was posed in 1852 and was settled by Appel and Haken in 1972. A computer free proof of this problem is still to be found.

8.3 BASIC DEFINITIONS AND TYPES OF GRAPH :

The Fig. 8.3. Shows some of the graphs.

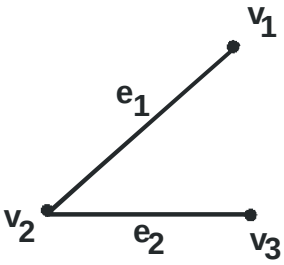


Fig. 8.3.1 (a)

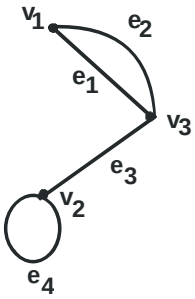


Fig. 8.3.1 (b)

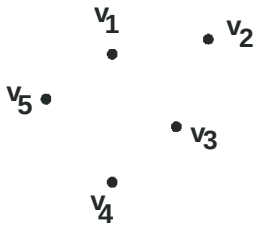


Fig. 8.3.1 (c)

In Fig. 8.3.1 (a) there are points v_1, v_2, v_3 and the line segments e_1, e_2. Line segment e_1 joins points v_1 and v_2 while line segment e_2 joins points v_2 and v_3.

In Fig. 8.3.1 (b) point v_2 is joined to itself by a loop e_4. There are multiple line segments between points v_1 and v_3. In Fig. 8.3.1 (c). There are no line segments but the points v_1, v_2, v_3, v_4, v_5.

All the above figures are the examples of graphs. Each graph consists of certain number of points called vertices and some pairs of points joined by line segments which are called as edges.

8.3.1 Definition : Graph, order and size of graph

A graph G is a pair (V, E) where V is nonempty finite set of vertices and E is family of unordered pairs of elements of V called edges. V is vertex set of G, E is edge set of G. The number of elements in V is called order of G. It is denoted by |V|. The number of edges in graph G is called size of G and denoted by |E|.

In Fig.8.3.1 (a), $V = \{v_1, v_2, v_3\}$, $E = \{e_1, e_2\}$, $|V| = 3$ & $|E| = 2$.

In Fig. 8.3.1 (b), $V = \{v_1, v_2, v_3\}$, $E = \{e_1, e_2, e_3, e_4\}$, $|V| = 3$ and $|E| = 4$

In Fig. 8.3.1 (c), $V = \{v_1, v_2, v_3, v_4, v_5\}$, $E = \emptyset$ (empty), $|V| = 5$ and $|E| = 0$

8.3.2 Definition : Simple graph, Multigraph, Directed graph

A simple graph *G (V, E)* consists of V, a nonempty set of vertices and E, a set of unordered pairs of distinct elements of V called edges. Fig. 8.3.2 (a).

A multigraph G(V, E) consists of set V of vertices, a set E of edges including multiple edges and loops. Fig. 8.3.2 (b).

A directed graph G(V, E) consists of V, nonempty set of vertices and E which is family of ordered pairs of elements of V which are directed edges. Fig. 8.3.2 (c).

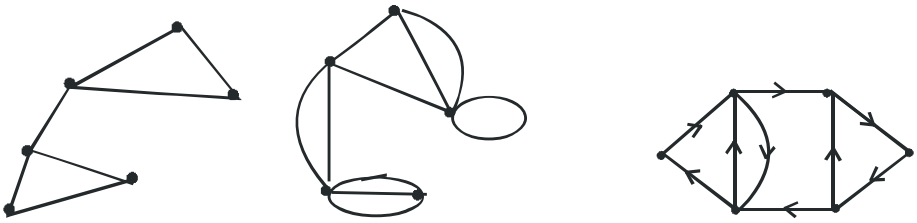


Fig. 8.3.2 (a) Simple Graph **Fig. 8.3.2 (b) Multiple Graph** **Fig. 8.3.2 (c) Directed Graph**

8.3.3 Definition : Incidence, Adjacent, Degree, Pendant vertex

See the Fig. 8.3.1 (a) the edge e_1 joins vertices v_1 and v_2. The vertices v_1 and v_2 are called end vertices of edge e_1. The edge e_1 is said to be incident on vertex v_1 and vertex v_2. The vertices v_1 and v_2 are adjacent vertices. Thus, two vertices are said to be adjacent if they are the end vertices of the same edge. Similarly, two nonparallel edges are said to be adjacent if they are incident on a common vertex. In Fig. 8.3.1 (a), e_1 and e_2 are adjacent edges.

- The number of edges incident on vertex v, with self loop counted twice is called degree, d(v), of vertex v. In Fig. 8.3.1(a) $d(v_2) = 2$. In Fig. 8.3.1(b) $d(v_2) = 3$.
- The vertex having no incident edge is called an isolated vertex. Isolated vertices are vertices with zero degree. A graph with all isolated vertices is called null graph. Fig.8.3.1 (c).
- The vertex of degree one is called pendant vertex. In Fig. 8.3.1(a), vertices v_1 and v_3 are pendant vertices.

Theorem 8.3.1 :

The Handshaking Theorem

The sum of degrees of all vertices in graph G is twice the number of edges in G.

Proof :-
Let G be a graph with e edges and n vertices $v_1, v_2, ..., v_n$. To show

that $\sum_{i=1}^{n} d(v_i) = 2e$ $\rightarrow$ (3.1)

Each edge contributes two degrees to the sum of degree of vertices as each edge is incident with exactly two vertices. This means that the sum of degrees of the vertices is twice the number of edges. A loop at a vertex also counted twice.

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

For example consider the graph in fig. 8.3.3

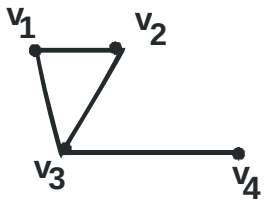


Fig. 8.3.3

$d(v_1) + d(v_2) + d(v_3) + d(v_4)$
$= 2 + 2 + 3 + 1 = 8 = 2 \times 4$ = twice the number of edges.

Theorem 8.3.2 :
The number of vertices of odd degree in a graph is always even.

Proof :-
Consider the vertices of odd degrees and even degrees separately. The sum of degrees of all vertices is even i.e. $\sum_{i=1}^{n} d(v_i) = 2e$, in a graph G with n vertices $v_1, v_2, ..., v_n$ and number of edges e.

Also, $\sum_{i=1}^{n} d(v_i) = \sum_{odd} d(v_i) + \sum_{even} d(v_k)$ $\rightarrow$(3.2)

The left side of equation 3.2 is expressed as sum of two sums, each sum taken over vertices of odd and even degrees respectively.

Since $\sum_{i=1}^{n} d(v_i) = 2e$ and the second expression on right hand side i.e. $\sum_{\text{even}} d(v_k) = \underset{\text{(say)}}{2s}$, both are even,

we get $\sum_{\text{odd}} d(v_i) = 2e - \sum_{\text{even}} d(v_k)$

$= 2e - 2s$

$= 2\,(e - s)$

i.e. $\sum_{\text{odd}} d(v_i) =$ an even number $\rightarrow (3.3)$

Thus, because of equation 3.3, each $d(v_i)$ is odd.

The total number of terms in the sum must be even, to make the sum an even number. Hence the theorem.

Types of Graphs

(a) Complete Graphs :

A simple graph in which every pair of distinct vertices is adjacent is called a <u>complete</u> graph. Denote complete graph on n-vertices by k_n.

Note :

1) In K_n, every vertex is adjacent to all the remaining (n – 1) vertices.

2) The degree of each vertex of K_n is n – 1.

Some examples of complete graphs.

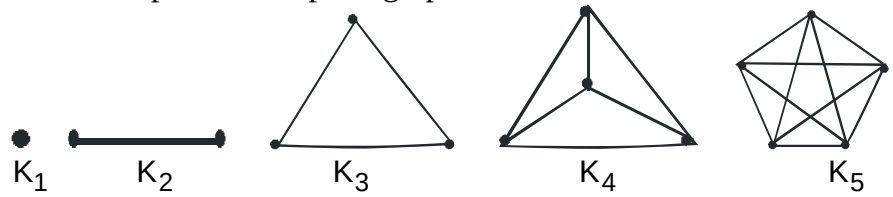


Fig. 8.3.4.1 complete graphs

(b) Regular Graphs :

If all the vertices in a graph G are of the same degree, then G is called regular graph. If degree of each vertex is 'n' then G is said to be regular of degree 'n'.

Remark :
(1) All the complete graphs are regular.
(2) A regular graph of degree 3 is known as cubic graph.

The graph of Fig.8.3.4.2 is Petersen's graph. In this graph there are ten vertices and degree of each vertex is 3. It is also an example of cubic graph.

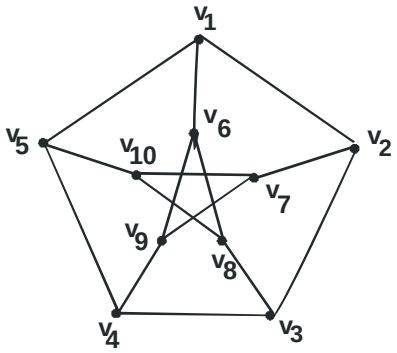
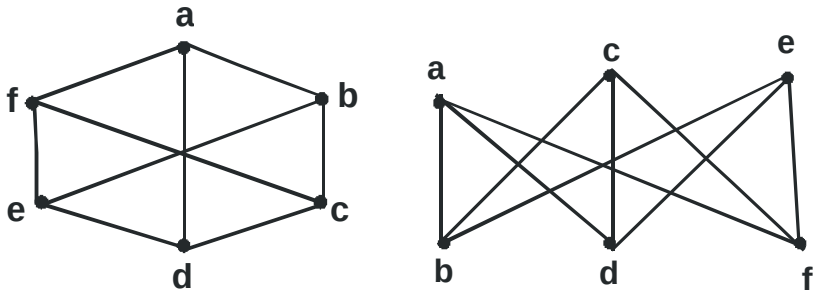


Fig. 8.3.4.2 Petersen's Graph

(c) Bipartite Graph: If the vertex set V of a graph G can be partitioned into two disjoint subjects say V_1 and V_2 such that any edge in G joins a vertex of V_1 to a vertex of V_2, then G is called bipartite graph.



(a) Here $V_1 = \{a, c, e\}$, $V_2 = \{b, d, f\}$

(b) Here $V_1 = \{a, c, e\}$, $V_2 = \{b, d, f\}$

Fig. 8.3.4.3 Bipartite Graphs

Remark :

(1) In bipartite graph, it is not necessary that every vertex in V_1 is adjacent with every vertex in V_2. But if it is so and G is simple graph then G is called complete bipartite graph. A complete bipartite graph is denoted by Km,n where $|V_1| = m$ and $|V_2| = n$.

(2) Km,n has mn edges as each vertex in v_1 joins every vertex in V_2. The Fig. 7.3.4.3 shows $K_{3,3}$ graph.

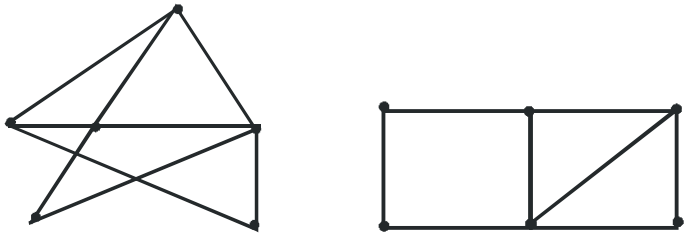
(3) The graph $K_{1,n}$ is known as star. For example, Fig. 7.3.4.4 is Star Graph $K_{1,7}$.

Fig. 8.3.4.4
Star Graph; $K_{1,7}$

Check your progress :

1. Draw all simple graphs on one, two, three and four vertices.

2. Describe the graph G in the diagram i.e.
   i) Find vertex set V(G) and |V(G)|
   ii) Find edge set E(G) and |E(G)|
   iii) Find the degree of each vertex.
   iv) Verify Handshaking theorem for given graphs.

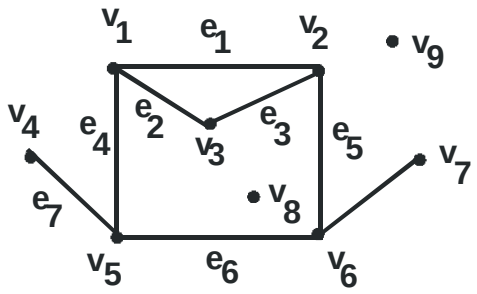


(a) **(b)**

3. Draw a simple graph, multiple graph and directed graph on seven vertices.

4. Show that number of odd degree vertices in a graph is always even.

5. Consider the graph in following diagram.



Find (i) end vertices of edges e_5, e_4, e_3

ii) edge incident on vertices v_1 and v_2, v_4 and v_5, v_2 and v_3

iii) pair of adjacent vertices (any three)

iv) pair of adjacent edges (any three)

v) isolated vertices

vi) pendant vertices

6. Draw following graphs

i) K_4

ii) K_5

iii) Regular graph of degree three

iv) Petersen's graph

v) $K_{2,3}$

vi) $K_{5,3}$

7. Justify whether the following statements are True or False.

i) A circle with radius one and centre at origin is a graph.

ii) In a simple graph on 'p' vertices the degree of each vertex is atmost p_{-1}.

iii) There does not exist a graph on give vertices whose degrees are 4, 1, 2, 2, 3.

iv) The number of vertices of odd degree is odd.

v) There does not exist a complete graph on n (n > 2) vertices which is bipartite graph.

8.4 SUBGRAPHS AND ISOMORPHISM

A) Subgraphs

8.4.1 Definition :

A graph H is called a subgraph of a graph G if all the vertices and the edges of H are also vertices and edges of G. In other words, $V(H) \subseteq V(G)$ and $E(G) \subseteq E(H)$.

For example,

Consider Petersen's graph P given in Fig. 8.3.4.2. The following graphs P_1, P_2, P_3 are subgraphs of P.

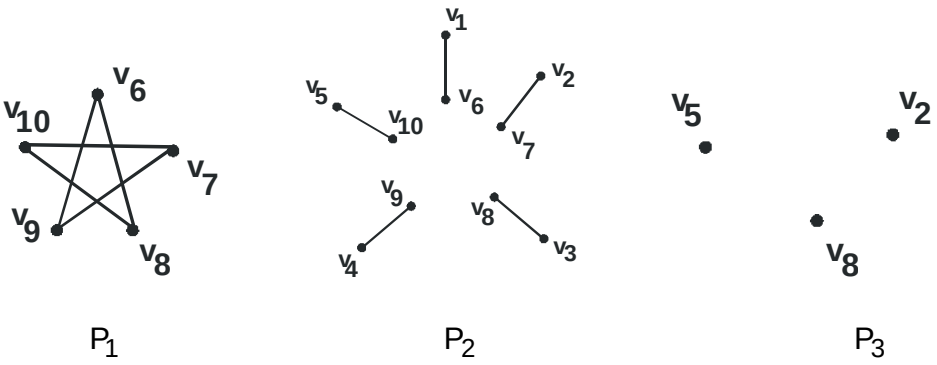


Fig. 8.4.1
Subgraphs of Petersen's Graph

The graph P_0 is not a subgraph of P as shown in Fig. 8.4.2 because the edge set of P_0 is not contained in E(P).

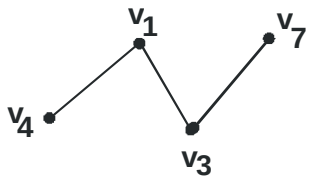


Fig. 8.4.2
Graph which not subgraph of Petersen's Graph

Note : Subgraph of bipartite graph is bipartite, because all the edges in the subgraph are edges of original graph.

8.4.2 Definition :

A subgraph H of a graph G is called <u>spanning subgraph</u> of G if H contains all the vertices of G. In other words $V(G) = V(H)$.

Let G be a graph as shown in Fig. 8.4.3, then graphs H_1, H_2, H_3 of Fig. 8.4.4 are spanning subgraphs of G.

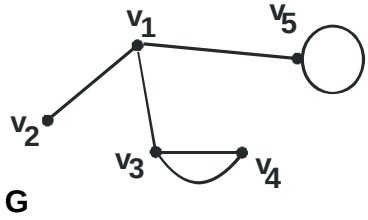
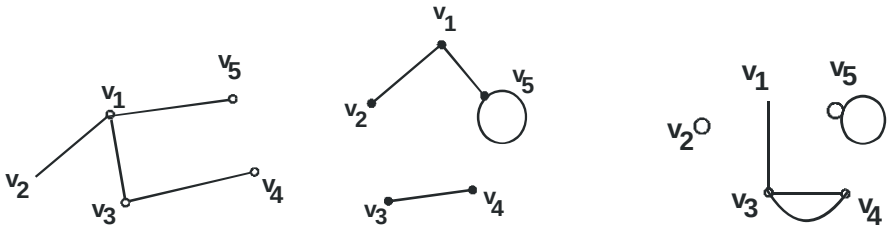


Fig. 8.4.3



H_1 H_2 H_3

Fig. 8.4.4
Spanning subgraphs

8.4.3 Definition :

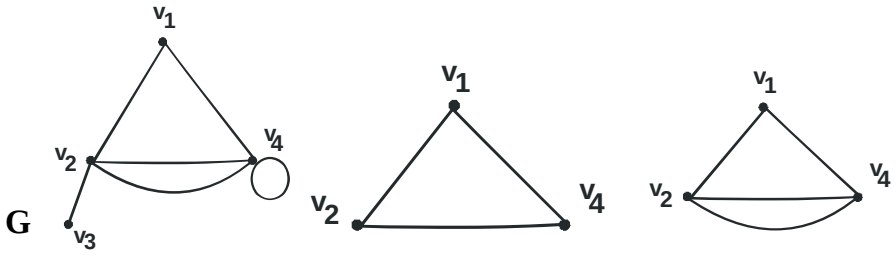
Let G be graph with vertex set V. Let any set S be subset of V, the induced subgraph <S> is defined as the maximal subgraph of G with vertex set S.

Note : There is no subgraph of G with vertex set S that contains <S> properly.

Example :

1) Consider Petersen's graph P in Fig.8.3.4.2 and its subgraphs shown in fig. 8.4.1. In this case P_1 is subgraph of P induced by $S = \{v_6, v_7, v_8, v_9, v_{10}\}$ i.e. $P_1 = <S>$. Note that P_2 is not an induced subgraph of G.

2) Consider Fig. 8.4.5 (a). If we take $S = \{v_1, v_2, v_4\}$ then <S> = H_1 is not induced subgraph because the graph has vertex set S but $H_1 \subsetneqq H_2$ i.e. H_1 is not a maximal subgraph of G with vertex set S. Thus, H_2 is induced subgraph of G.



(a) H_1 (b) H_2 (c)

Fig. 8.4.5
Induced subgraph

B) Isomorphisms of Graphs

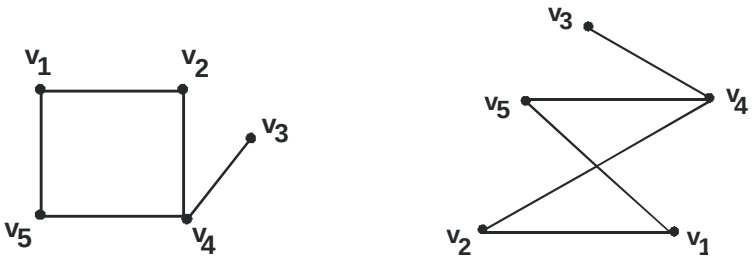
8.4.4 Definition :

Two graphs G_1 and G_2 are said to be isomorphic if there exists a one-one and onto map $T: V(G_1) \to V(G_2)$ such that if $v_1, v_2 \in V(G_1)$, then the number of edges joining v_1 and v_2 is also the same as the number of edges joining $T(v_1)$ and $T(v_2)$.

Note that isomorphism of two graphs preserves adjacency and non-adjacency of any two vertices.

Example :

Consider following two graphs G_1 and G_2 in Fig. 7.4.6.



G_1 G_2

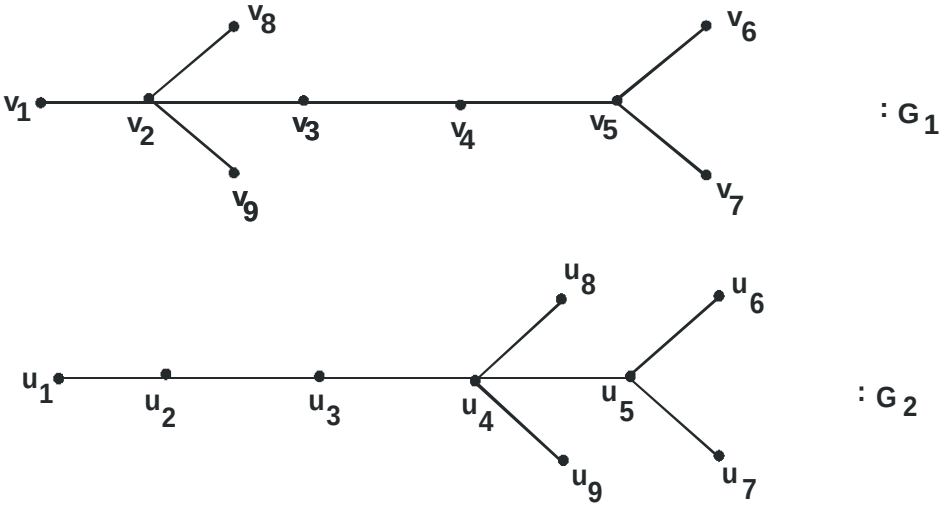
Fig. 8.4.6
Isomorphic graphs

Define a map from $V(G_1)$ to $V(G_2)$ as follows : $v_1 \mapsto u_1$, $v_2 \mapsto u_2$, $v_3 \mapsto u_3$, $v_4 \mapsto u_4$, $v_5 \mapsto u_5$. This map is an isomorphism. G_1 and G_2 are isomorphic graphs.

Remarks :

Two isomorphic graphs have the same number of vertices, same number of edges and also same number of vertices of given degree. However, these conditions are only necessary not sufficient. For example, consider graphs G_1 and G_2 given in fig. 7.4.7. They have same number of vertices, same number of edges and also each of them have exactly one vertex of degree three and four, two vertices of degree two and five vertices of degree one. Yet, they are <u>not isomorphic</u> because under the isomorphism, v_2 and v_5 are not adjacent in G_1 where as in G_2, u_4 and u_5 are adjacent. $d(v_2) = 3$ and $d(u_4) = 3$

$d(v_5) = 3$ and $d(u_5) = 3$ Thus, $v_5 \mapsto u_4$ and $v_5 \mapsto u_5$



Fir. 8.4.7 Non-isomorphic Graphs

C) Matrix representation of Graphs

Graphs can also be represented by matrices. This method is most suitable for computer processing. The two representations of graphs using matrix is by incidence matrix and adjacency matrix.

8.4.5 Definition : Incidence matrix

Consider graph G without loops. Let $V = \{v_1, v_2, ... v_m\}$ and $E = \{e_1, e_2, ..., e_n\}$ Define m x n matrix I(G) as follows :

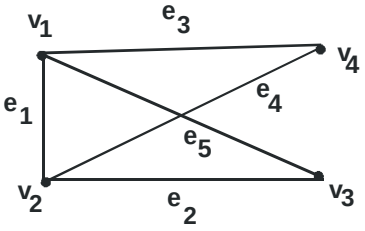
$I(G) = [aij]_{m \times n}$

where aij = 1, if e_j is incident at v_i

= 0, otherwise

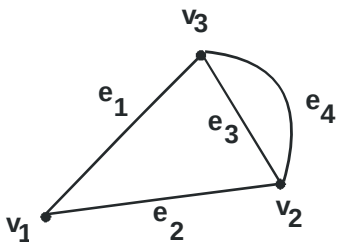
Example of incidence matrix :

Consider graphs and its incidence matrix, in Fig. 8.4.8



G

$$I(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$



$$I(H) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array} \begin{array}{c} \begin{array}{cccc} e_1 & e_2 & e_3 & e_4 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

Fig. 8.4.8 Incidence matrix

Note :

1) Incidence matrix is defined for graphs without loops.
2) All entries in incidence matrix is ‘zero’ or ‘one’. Such matrix is called binary matrix.
3) There are exactly two ones in each column.
4) The sum of the entries in any row is the degree of the corresponding vertex.
5) A row corresponding to a vertex of degree zero contains all zeros.
6) Two graphs G_1 and G_2 are isomorphic if and only if their incidence matrices $I(G_1)$ and $I(G_2)$ differ only by permutation of its rows and columns.

8.4.6 Definition : Adjacency matrix

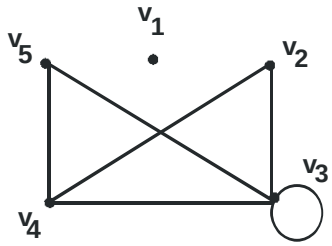
Let G be a graph with n vertices, say $\{v_1, v_2, \ldots v_n\}$ and not having multiple edges. Then the matrix $A(G) = [x_{ij}]$ of order n $\times$ n,

called the adjacency matrix of G is defined as the matrix whose ijth entry is given by,

$x_{ij} = 1$, if there is an edge joining ith and jth vertices.
$= 0$, otherwise

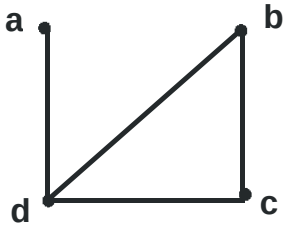
Example of Adjacency matrix:

Consider graphs and their adjacency matrix, in Fig 8.4.9



G

$$A(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$



H

$$A(H) = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

Fig. 8.4.9 Adjacency matrix

Note :

1) Adjancency matrix is a symmetric square matrix with entries either zero or one.

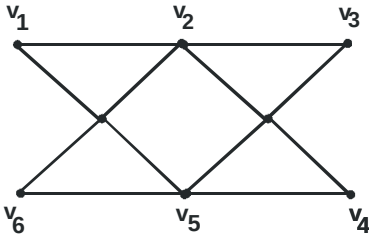
2) If G has no loops then the sum of the entries along any row or any column is the degree of the corresponding vertex.

3) If G_1 and G_2 are graphs without multiple edges then G_1 is isomorphic to G_2 if and only if $A(G_1)$ can be obtained from $A(G_2)$ by applying permutation of rows and of corresponding columns.

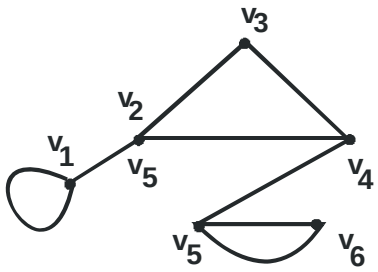
Check your progress

1. Draw a bipartite graph whose subgraph is bipartite.

2. Draw any two spanning subgraphs of following graphs.



(a)

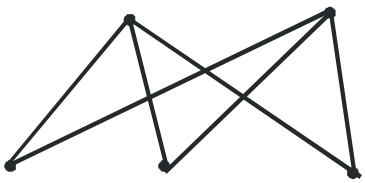


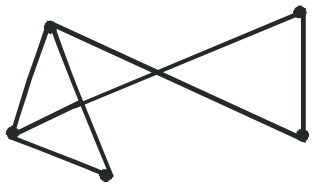
(b)

3. Draw any two induced subgraphs of the graphs given in Exercise 2.

4. Give any two examples of non-isomorphic graphs.

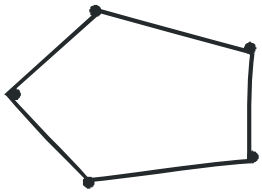
5. Prove that following graphs are not isomorphic.

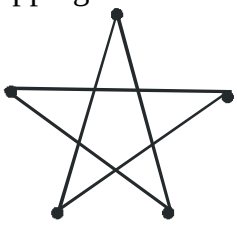




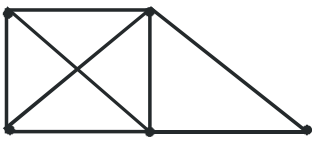
6. Determine whether given pair of graphs are isomorphic. If not, then justify. If isomorphic then show mapping.

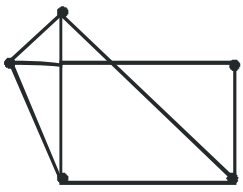
a)



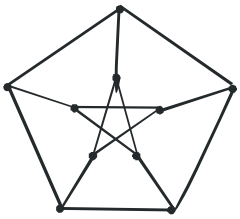


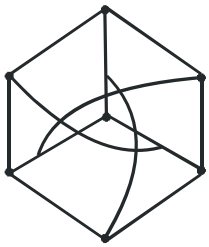
b)





c)





7. Show that there are four non-isomorphic simple graphs on three vertices.

8. Draw graphs corresponding to following incidence matrix.

i)

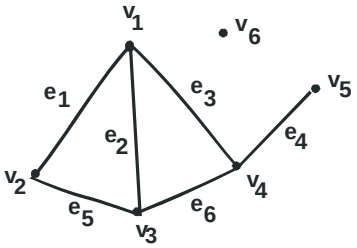
	e1	e2	e3	e4
v1	1	1	0	0
v2	0	1	1	1
v3	1	0	1	1

ii)

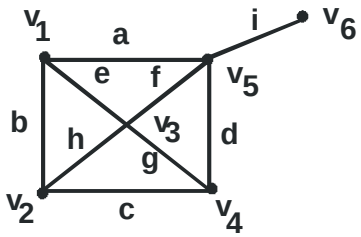
	a	b	c	d	e	f	g	h
v_1	0	0	0	1	0	1	0	0
v_2	0	0	0	0	1	1	1	1
v_3	0	0	0	0	0	0	0	1
v_4	1	1	1	0	1	0	0	0
v_5	0	0	1	1	0	0	1	0
v_6	1	1	0	0	0	0	0	0

9. Write incidence matrix for simple graphs

i)



ii)

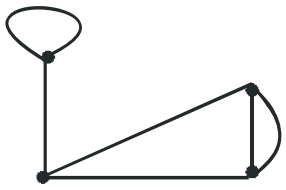


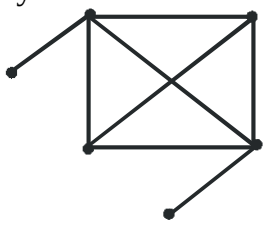
10. Draw Graph with given adjacency matrix.

i) $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$

ii) $\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$

11. Represent given graphs using adjacency matrix.

i) 

ii) 

12. Justify whether following statements are true or false.

i) There are eleven non-isomorphic simple graphs on four vertices.

ii) Let H be subgraph of G. If u.v are non adjacent vertices in H then they are also non-adjacent in G.

iii) If H is induced subgraph of G and if two vertices are not adjacent in H then they are also not adjacent in G.

iv) Subgraph of subgraph of G is a subgraph of G.

v) An induced spanning subgraph of G is G itself.

vi) Adjacency matrix is symmetric square matrix.

vii) Incidence matrix is defined for graphs with loops.

viii) A row corresponding to a vertex of degree zero in incidence matrix contains all non zero entries.

8.5 OPERATIONS ON GRAPHS

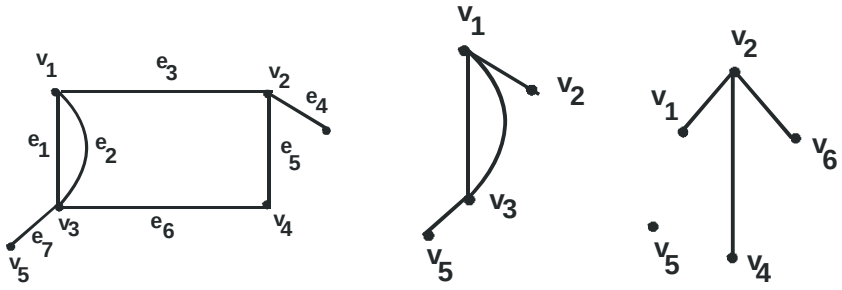
8.5.1 Removal of vertex or edge

Let G be a graph with $V = \{v_1, v_2, ..., v_n\}$. The removal of vertex v_i results in a subgraph G^l of G consisting of all vertices of G except v_i and all edges of G which are not incident with v_i. $G^l = G - v_i$ is maximal subgraph of G with vertex set,

$$S = \{v_1, v_2, ..., v_{i-1}, v_{i+1}, ..., v_n\}$$

Example :

Consider the graphs $G - v_4$ and $G - v_3$ obtained by removing vertex v_4 and vertex v_3 respectively in Fig. 7.5.1.



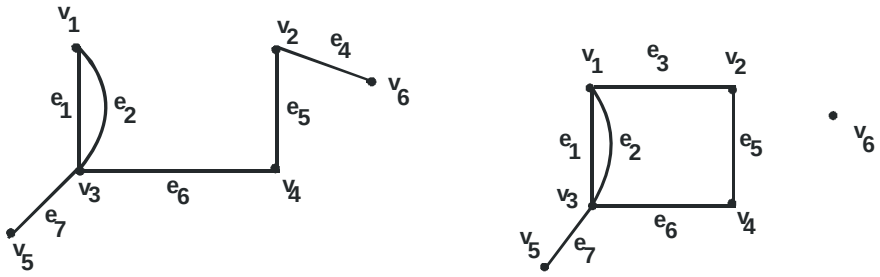
G $G - v_4$ $G - v_3$

FIG. 8.5.1(a) Removal of vertex

If $E(G) = \{e_1, e_2, ..., e_k\}$ then removal of an edge say e_i from G results in graph G^I where $V(G) = V(G^I)$ and $E(G^I)$ contains all edges of G except e_i.

Example :

$G - e_3$ and $G - e_4$ are two graphs obtained by deleting edge e_3 and edge e_5 respectively from graph G given in Fig. 8.5.1.



$G - e_3$ $G - e_4$

Fig. 8.5.1(b) Removal of edge

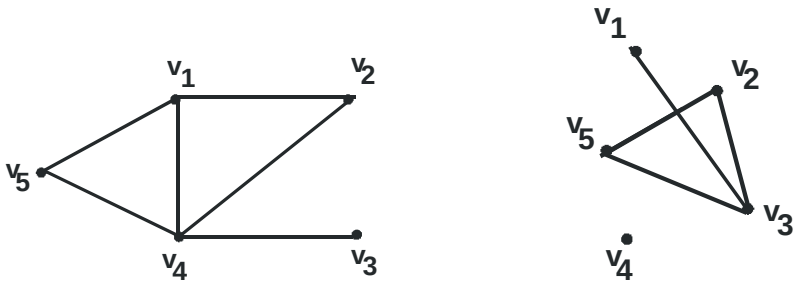
Note : When a vertex is removed or deleted all edges incident on that vertex is removed but when a edge is removed we do not remove vertices incident at that edge.

8.5.2 Complement of a graph

Let $G = (V(G), E(G))$, then complement of G is graph $\bar{G}$ with vertex set V(G) where in two vertices are adjacent if and only if they are not adjacent in G.

Example :

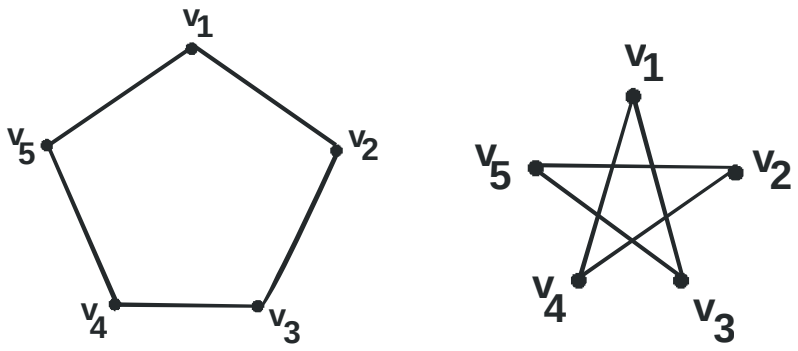
See Fig. 8.5.2(a) for graph G and its complement.



G $\overline{G}$: Complement of G

Fig. 8.5.2(a) Complement of a graphs

A graph G is <u>self complementary</u> if it is isomorphic to its complement $\overline{G}$ as shown in Fig. 8.5.2(b).



G $\overline{G}$

Fig. 8.5.2(b) Self complementary Graphs

G and $\overline{G}$ in Fig. 8.5.2(b) are isomorphic under the map $v_1 \mapsto v_1$, $v_2 \mapsto v_3$, $v_5 \mapsto v_4$, $v_3 \mapsto v_5$, $v_4 \mapsto v_2$.

8.5.3 Union of two graphs

Let $G_1(V_1, E_1)$ and $G_2(V_2, E_2)$ be two graphs. The union $G_1 \cup G_2$ of G_1 and G_2 is defined as graph where vertex set is $V_1 \cup V_2$ and edge set is $E_1 \cup E_2$.

Example :

Union of two graphs i.e. illustrated in Fig. 7.5.3.

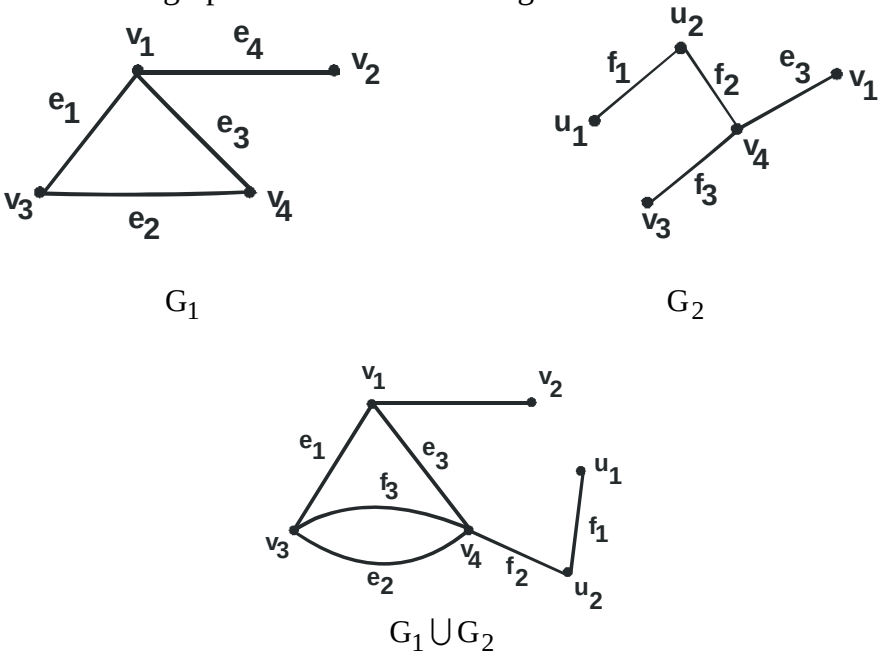


Fig. 8.5.3 Union of two graphs

8.5.4 Intersection of two graph

Let $G_1(V_1, E_1)$ and $G_2(V_2, E_2)$ be two graphs then the intersection $G_1 \cap G_2$ of G_1 and G_2 is graph consisting of only those vertices and edges which are both in G_1 and G_2.

Example :

Illustration of $G_1 \cap G_2$ is G_2 as shown in Fig. 7.5.3.

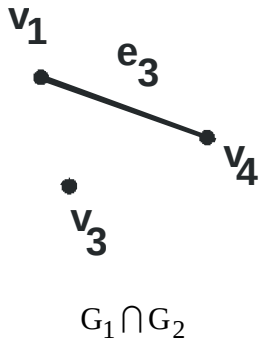


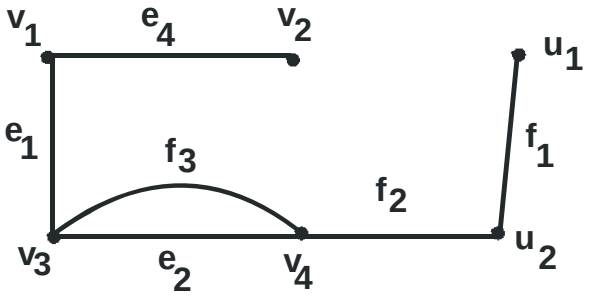
Fig. 8.5.4 Intersection of graph

8.5.5 Ring sum of two graphs

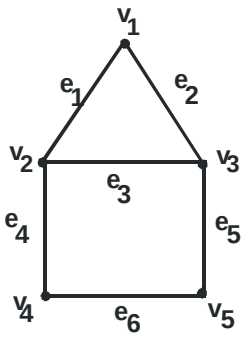
The ring sum of graphs $G_1(V_1, E_1)$ and $G_2(V_2, E_2)$ is consisting of vertex set $V_1 \cup V_2$ and edges that are either in G_1 or in G_2 but not in both and is denoted by $G_1 \oplus G_2$.

Example :

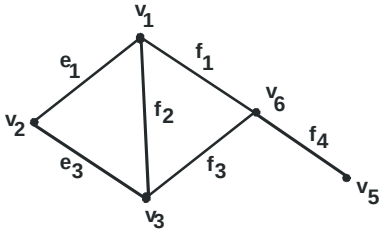
Taking G_1 and G_2 from Fig. 8.5.3, the ring sum $G_1 \oplus G_2$ is



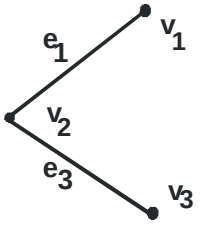
Following is one more example which shows $G_1 \cap G_2$, $G_1 \cup G_2$ and $G_1 \oplus G_2$. Fig. 8.5.5(a)



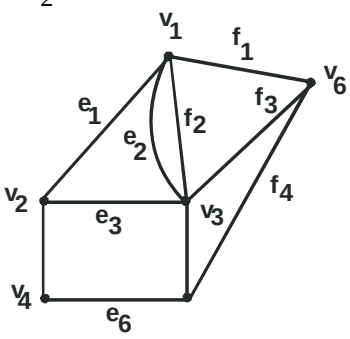
G_1



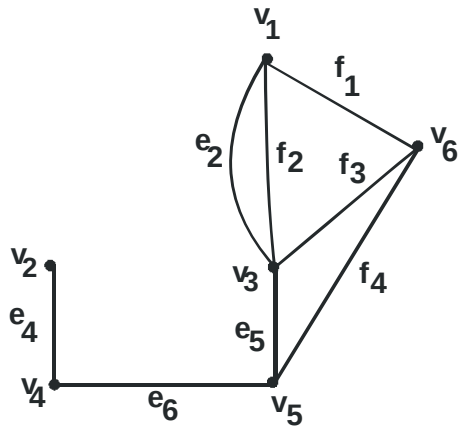
G_2



$G_1 \cap G_2$



$G_1 \cup G_2$



$G_1 \oplus G_2$

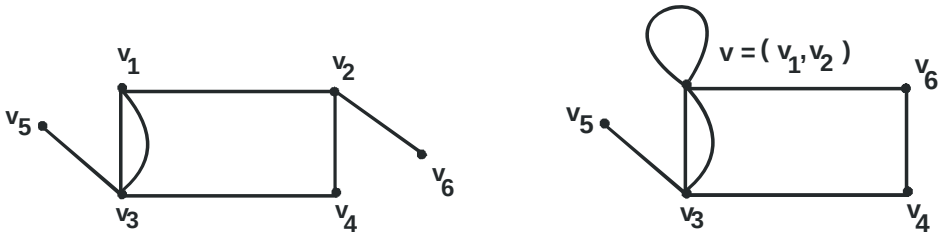
Fig. 8.5.5(a) Intersection, Union and ringsum of two graphs

8.5.6 Fusion and Contraction

A pair of vertices v_1 and v_2 in graph G is said to be fused if the two vertices are replaced by single vertex v such that every edge that was adjacent to either v_1 or v_2 or both is adjacent to the new vertex v. The fusion does not alter the number of edges in the graph but number of vertices is reduced by one.

Example :

Fig. 8.5.6.1(b) is graph obtained by fusion of vertices v_1 and v_2 in Fig. 8.5.6.1(a).



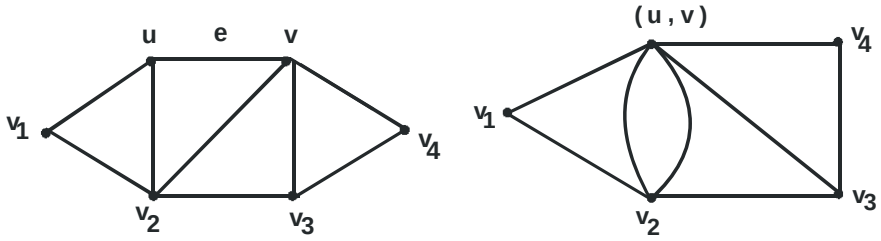
(a) **(b)**

Fig. 8.5.6.1 Fusion of vertices

Contraction of an edge in a graph is obtained by taking an edge with end vertices u and v, and contracting it. In other words, removing e and identifying u and v in such a way that the resulting vertex is incident to those edges (other than e) which were originally incident to u or v.

Example :

Fig. 8.5.6.2(b) is a graph obtained by contraction of an edge e in graph of Fig. 8.5.6.2(a).



(a) **(b)**

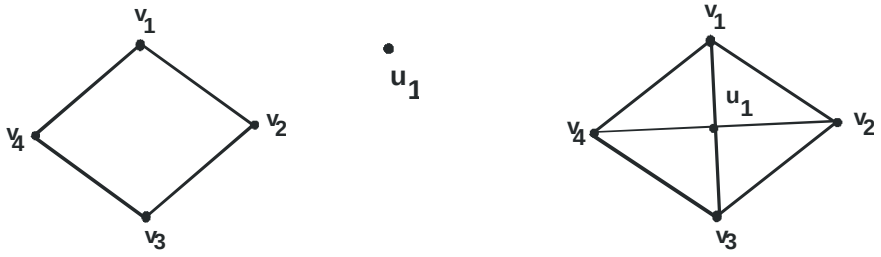
Fig. 8.5.6.2 Contraction of an edge

8.5.7 Sum of two graphs

Let $G_1(V_1, E_1)$ and $G_2(V_2, E_2)$ be two graphs where $V_1 \cap V_2 = \varnothing$ then sum of G_1 and G_2 denoted by $G_1 + G_2$ is defined as graph whose vertex set is $V_1 \cup V_2$ and consisting of all edges, which are in G_1 and G_2, and the edges obtained by joining each vertex of G_1 to each vertex of G_2.

Example :

Fig. 8.5.7 show the sum $G_1 + G_2$.



G_1 G_2 $G_1 + G_2$

Fig. 8.5.7 Sum of two graphs

8.5.8 Line graph

The line graph L(G) is a simple graph G whose vertices are in one-one correspondence with the edge of G, two vertices of L(G) being adjacent if and only if corresponding edges of G are adjacent.

Example :

See Fig. 8.5.8.

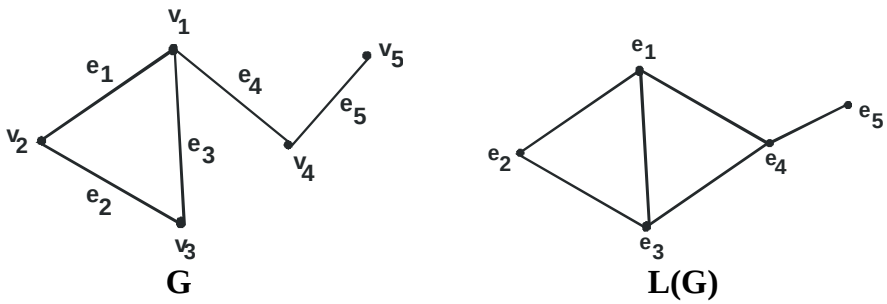


Fig. 8.5.8 Line Graph

8.5.9 Cartesian product of G_1 and G_2

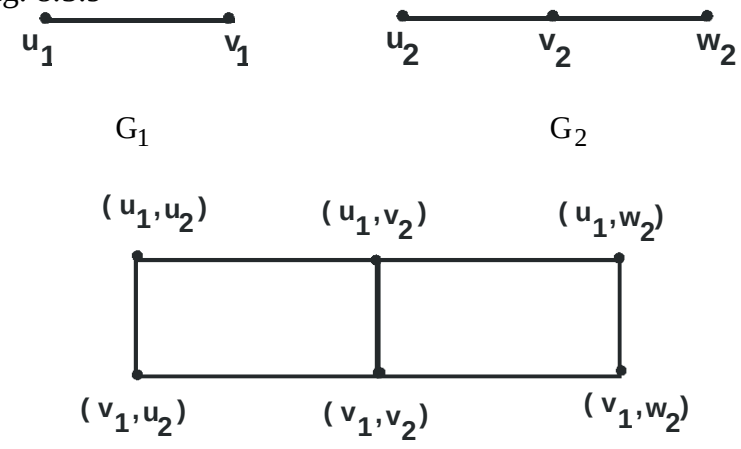
Let $G_1(V_1, E_1)$ and $G_2(V_2, E_2)$. Then carterian product of G_1 and G_2. $G_1 \times G_2$ is graph with vertex set V specified by putting u adjacent to v if and only if

i) $u_1 = v_1$ and $u_2 v_2 \in E_2$ or

ii) $u_2 = v_2$ and $u_1 v_1 \in E_1$

Example :

See Fig. 8.5.9



$G_1 \times G_2$

Fig. 8.5.8 Cartesian product of graphs

Remark :

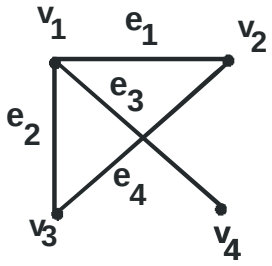
If $V_1 = \{u_1, v_1\}$ and $V_2 = \{u_2, v_2, w_2\}$ then cartesan product of sets $V_1 \times V_2$ is

$V_1 \times V_2 = \{(u_1, u_2), (u_1, v_2), (u_1, w_2), (v_1, u_2), (v_1, v_2), (v_1, w_2)\}$ The points in $V_1 \times V_2$ are vertices of $G_1 \times G_2$.

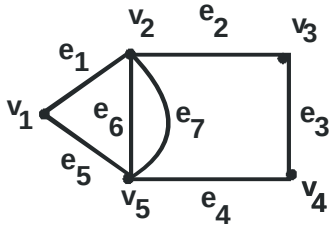
At this juncture, let us take a break and do some problems and check if we have understand the basic concepts of graphs.

Check your progress

1. Consider the graphs given below



G_1



G_2

Draw the graph

i) $G_1 - v_2$

ii) $G_1 - v_1$

iii) $G_2 - v_5$

iv) $G_2 - v_3$

v) $G_1 - e_4$

vi) $G_1 - e_3$

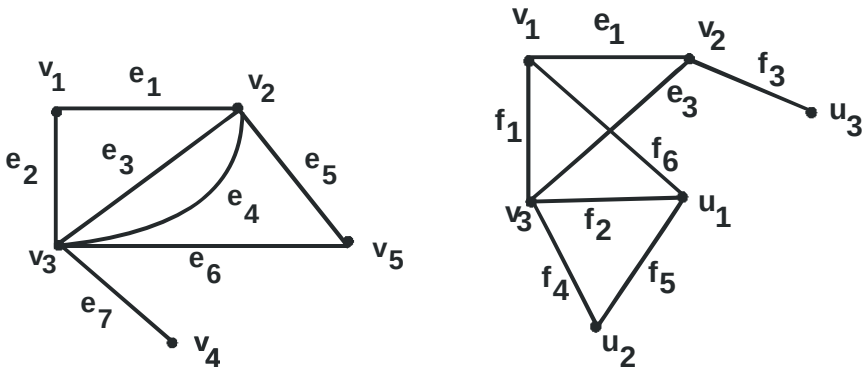
vii) $G_2 - e_3$

viii) $G_2 - e_7$

2. Draw a graph which is self complementary.

3. Draw complement of graphs given in exercise 7.5.1.

4. Draw the graphs $G_1 + G_2$ if G_1 and G_2 are given as follows :



G_1 G_2

5. Draw the graph obtained by fusion of vertices v_1 and v_2 in graphs given in exercise 7.5.1.

6. Draw the graph obtained by contracting the edge e_1 in the graphs given in exercise 7.5.1.

7. Let $G_1(V_1, E_1)$ and $G_2(V_2, E_2)$ be two graphs with $V_1 = \{u_1, v_1\}$, $E_1 = \{u_1, v_1\}$ while $V_2 = \{u_2, v_2\}$, $E_2 = \{u_2, v_2\}$. Draw the graph of Cartesian product of G_1 and G_2.

8. Justify whether following statements are True or False.

   i) The ring sum of two complete graphs is complete.

   ii) If G, H, K are simple graphs then $G \cup (H \oplus K) = (G \cup H) \oplus (G \cup K)$

   iii) The complement of every graph and its line graph are isomorphic.

   iv) Adjacency matrix of simple graph and its complement is different.

   v) G_1 and G_2 is regular if $G_1(V_1, E_1)$, $G_2(V_2, E_2)$ are two graphs with $|V_1| = 3$, $|E_1| = 2$, $|V_2| = 4$ and $|E_2| = 3$.

8.6 LET US SUM UP

In this chapter, we have learnt basic concepts of graph theory to start with. The understanding of graph theory starts with this basic concepts as vertex, edge, edge set and vertex set. The different operations on graph lead to a big family of graph. Isomorphism of graphs tells vs about graphs which are isomorphic.

8.7 REFERENCES

1. Discrete Mathematical structures by Kolamn, Busby and Ross. Pearson education.
2. Introduction to graph theory by Douglas B. West.
3. Discrete Mathematics and its applications by Kenneth. H.Rosen. McGraw Hill edition.
4. Graph theory by Frank Harary. Narosa Publication.
5. Discrete Mathematics by Norman Priggs. Oxford.

9

GRAPH THEORY-II

Unit Structure :

9.0 OBJECTIVES :

After going through this chapter you will be able to:

- find walks, paths and circuit in a graph
- understand Eulerian graphs and circuits
- understand Hamiltonian graphs and circuits
- know about colouring the graphs

9.1 INTRODUCTION :

We have seen in earlier chapter, different operation of graphs and different types of graphs. In this chapter we are actually perform operation on graphs, so as to get circuit with a particular condition imposed on the edges and vertices of a graph joining. The edges and vertices in continuity we get a cycle or circuit. We can colour the edges and vertices of graph with different colours and can also find minimum number of colours required to colour a graph.

9.2 WALKS, PATHS AND CIRCUITS

Consider the following graphs.

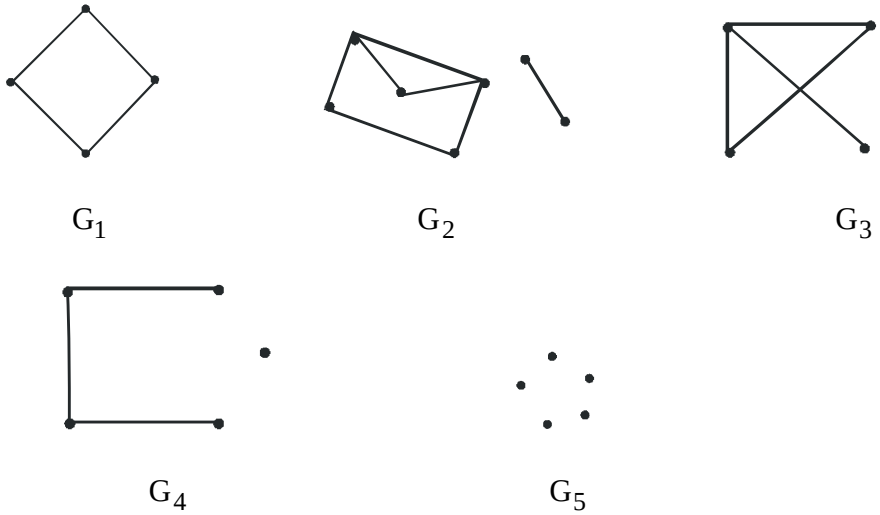


Fig. 9.1

In Fig. 9.1, observe graphs G_1 and G_3. We can travel from one vertex to another just by traversing the edges. This is not possible in case of the graphs G_2, G_4, G_5 as there is some vertex from which the edge is not there to another vertex. At this stage we are in position to make some more definitions.

Definition 9.1 :

A walk in a graph is defined as a finite alternating sequence of vertices and edges, beginning and ending with vertices such that each edge is incident with the vertices preceding and following it and occurs exactly once.

Definition 9.2 :

The vertices at the beginning and at the ending of a walk are called terminal vertices. Wherever terminal vertices are same, we call the walk as a closed walk. A open walk is one which is not closed.

Definition 9.3 :

A open walk in which no vertex is repeated is called a path.

Definition 9.4 :

A closed walk in which no vertex is repeated is called a circuit or a cycle.

Definition 9.5 :

The number of edges in a walk is called the length of the walk.

Let us illustrate all the definitions from 9.1 to 9.5 with help of graph in Fig. 9.2.

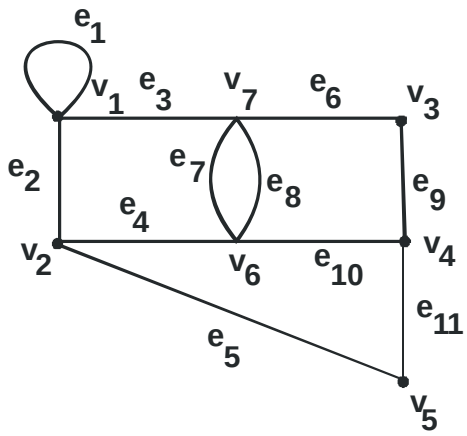


Fig. 9.2 A closed walk

An open walk :

$v_7\ e_3\ v_1\ e_1\ v_1\ e_2\ v_2\ e_5\ v_5\ e_{11}\ v_4\ e_{10}\ v_6\ e_4\ v_2$. This is not a path as vertex v_1 and v_2 are repeated. The length of the walk is 7.

The closed walk :

$v_7\ e_7\ v_6\ e_8\ v_7\ e_6\ v_3\ e_9\ v_4\ e_{10}\ v_6\ e_4\ v_2\ e_2\ v_1\ e_3\ v_7$. The length of this walk is 8. This is not a circuit as vertex v_6 and v_7 are repeated.

The path :

$v_5\ e_{11}\ v_4\ e_{10}\ v_6\ e_7\ v_7\ e_6\ v_3$. Length of the path is 4.

The circuit or cycle :

$v_7\ e_7\ v_6\ e_{10}\ v_4\ e_9\ v_3\ e_6\ v_7$. The length of cycle is 4.

Lemma 9.1:

Every uv walk contain uv path. u and v are terminal vertices.

Proof : The proof is by induction on the length ℓ of a uv walk say W.

Step 1: Suppose $\ell = 0$. It means the length of walk W is zero. It means W contains single vertex u (=v). This vertex is u v path of length zero.

Step 2: Suppose $\ell \geq 1$ and the result holds for walks of length less than ℓ.

Step 3: If W has no repeated vertex then its vertices and edges form a uv path. If W has repeated vertex w then delete all the edges and vertices appearing between w. This gives a smaller uv walk say W. W is contained in W.

As length of W is less than ℓ, induction hypothesis holds and W is contained in W.

Theorem 9.2:

Let G be a graph with adjacency matrix A. $V(G) = \{v_1, v_2, ..., v_n\}$ then the number of different paths of length r from v_i to v_j, where r is positive integer equals to ijth entry of A^n.

Example 1:

Find the number of paths from a to c for the graph in Fig. 8.3 of length 3.

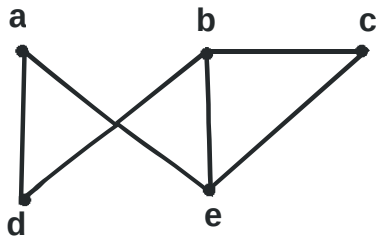


Fig. 9.3

Solution : Adjacency matrix A corresponding to graph in Fig. 9.3 is

$$A = \begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array} \begin{array}{c} \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix} \end{array} \quad \text{then} \quad A^3 = \begin{bmatrix} 0 & 1 & 2 & 4 & 5 \\ 1 & 2 & 4 & 5 & 6 \\ 2 & 4 & 2 & 2 & 4 \\ 4 & 5 & 2 & 0 & 1 \\ 5 & 6 & 4 & 1 & 2 \end{bmatrix}$$

We find A^3 as we want to find path of length 3.

Number of paths between vertices a and c is the $(1, 3)^{th}$ entry of A^3. $(1, 3)^{th}$ entry of A^3 is two.

$\therefore$ The paths of length 3 between the vertices a and c are two.

Check your progress

1) List all the different paths between vertices 5 and 6 in following Figure 8.4. Give the length of each path.

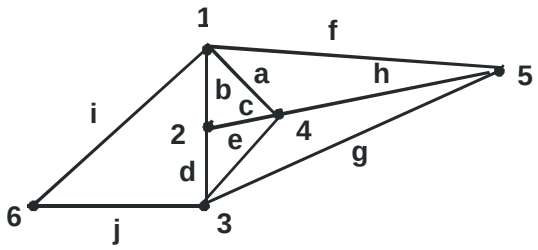


Fig. 9.4

2) List atleast four cycles in graph given in Fig. 8.4.

3) Show that every uv-walk contains a uv-path.

4) Find the number of paths from vertex 1 to 3 for the graph in Fig. 9.5 of length 3.

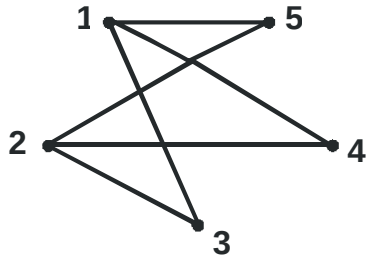


Fig. 9.5

5) Judge whether true or false.
   1) Any uv-walk contains a uv-path.
   2) The union of any two distinct uv-walks contains a circuit.
   3) The union of any two distinct uv-path contains a circuit.

6) List all the paths that begin at vertex 2 in Fig. 8.4.
7) List all the circuits that begin at vertex 3 in Fig. 8.5.

8) In the following graph

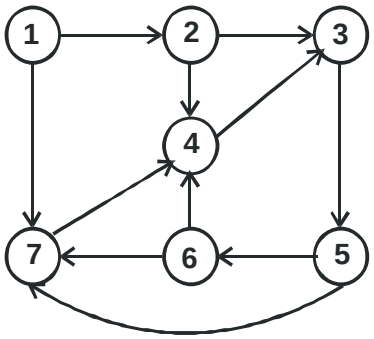


Fig. 9.6

i) List all paths of length 2 starting from vertex 2 and 5.
ii) Find the cycle at vertex 7 & 4.
iii) List all paths of length 1.
iv) List all paths of length 3.

9.3 CONNECTED AND DISCONNECTED GRAPHS

A graph is connected if we can reach any vertex from any other vertex by traversing along the edges. As seen in Fig. 8.1 G_1 and G_3 are connected while G_2, G_4, G_5 are disconnected. A disconnected graph consists of two or more connected graphs. Each of connected parts in disconnected graph is the component of the graph. More formally let us give definition of all these.

Definition 9.6:

A graph G with $u, v \in V(G)$ is said to be connected if G has a uv path otherwise G is said to be disconnected.

Definition 9.7 :

A disconnected graph is not a single piece. Each single piece in a disconnected graph is called a component. A component is maximal connected subgraph of given disconnected graph. For example, in Fig.9.1, G_2 has two components.

H_1 :  and H_2 : 

G_4 has two components say K_1 and K_2

K_1 :  K_2 : 

G_5 has five components each having a single vertex.

Theorem 9.3:

A graph G is connected if and only if given any pair u, v of distinct vertices, there is a path from u to v in G.

Proof : Let G be disconnected. Then G is expressed as a disjoint union of subgraphs. Choose two vertices u and v which belong to two of these different subgraphs say G_1 and G_2. Since G is union of mutually disjoint subgraphs, we cannot find an edge which is incident to vertices in G_1 and G_2. Hence we cannot find a path from u to v. This is a contradiction. G, therefore cannot be expressed as union of mutually disjoint subgraphs.

$\therefore$ G is connected.

Conversely, assume that G is connected and there are two vertices in G such that there is no path between them. Let u & v be these vertices. Denote by G_1 the induced subgraph formed by all those vertices w of G such that there is uw path in G. Let G_2 denote the complement of G_1. Then G is union of these two mutually disjoint subgraphs i.e. G is disconnected. This is contradiction. Hence we cannot find a pair of vertices such that there is no path between them.

Theorem 9.4:

Let G be a simple graph on n vertices. If G has k – components then the number q of edges of G satisfies the inequality,

$$(n-k) \le q \le \frac{1}{2}(n-k)(n-k+1)$$

Check your progress

1) Draw complete graph on seven vertices. Is this graph connected?

2) Give an example of a regular, connected graph on six vertices which is not complete.

3) Construct a graph with 8 vertices 16 edges and degree of each vertex 4.

4) Judge whether the following are true or false.
   i) A graph G is connected if and only if it has exactly one component.
   ii) Complement of connected graph is connected.
   iii) Subgraph of a connected graph is also connected.
   iv) If G is graph on 5 vertices and G has two components then number of edges of G is atmost 12.

5) Let u and v be any two vertices of a connected graph G. Show that there exists a uv – walk containing all vertices of G.

6) Draw a simple (p, q) graph G to show that G contains unique circuit iff G is connected & p = q.

7) Which connected graphs can be both regular and bipartite?

8) Give an example of regular connected graph on six vertices that is not complete.

9) Give an example of a graph on five vertices with exactly two components.

10) Give an example of a graph that is regular but not complete, with each vertex having degree three.

11) Give an example of a graph with seven vertices and exactly three components.

9.4 EULER GRAPHS :

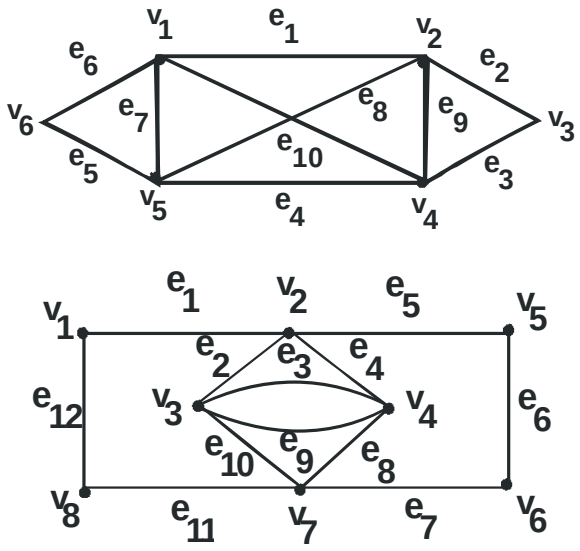
In this section we consider the task to travel a path using each edge of the graph exactly once. The problem is to draw a figure without lifting the pencil from the paper and without retracing a line.

Definition 9.8:

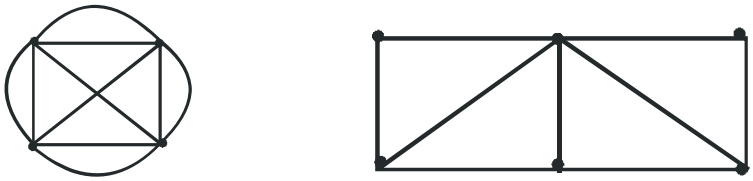
A path containing all the edges in a graph is called an **Eulerian path**.

Example 2 :

The figure 8.4.1 shows examples of Eulerian graphs and non Eulerian graphs.



(a) Eulerian graphs



(b) Non – Eulerian Graphs

Fig. 9.4.1

Definition 9.9:

A closed walk containing all the edges in a graph is called an Eulerian circuit.

A graph is Eulerian graph, if it has a closed walk containing all the edges.

In Fig. 9.4.1(a) graph G_1 is Eulerian because it contains Eulerian circuit $v_1\ e_1\ v_2\ e_2\ v_3\ e_3\ v_4\ e_4\ v_5\ e_5\ v_6\ e_6\ v_1\ e_7\ v_5\ e_8\ v_2\ e_9\ v_4\ e_{10}\ v_1$.

In Fig. 9.4.1(a) graph G_2 is Eulerian because it contains Eulerian circuit

$v_1\ e_1\ v_2\ e_2\ v_3\ e_3\ v_4\ e_4\ v_2\ e_5\ v_5\ e_6\ v_6\ e_7\ v_7\ e_8\ v_4\ e_9\ v_3\ e_{10}\ v_7$
$e_{11}\ v_8\ e_{12}\ v_1$.

Lemma 9.5:

If every vertex of a graph G has degree atleast 2, then G contains a cycle.

Theorem 9.6: Characterisation of Eulerian graph :

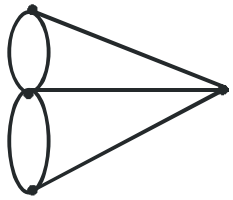
A connected graph G is Eulerian if and only if every vertex of G is of even degree.

Corollary 9.7:

Let G be connected with exactly two odd vertices say u and v. then there is a uv walk in G that contains all edges of G.

Proof : Let G' be the graph obtained from G, by adding an edge joining u and v. The degree of each vertex in G' is even and therefore it has Eulerian walk beginning with u and ending with u. Any Eulerian walk for G' must contain the edge uv. Otherwise, G itself would be Eulerian and u as well as v will be of even degree which is a contradiction. Let therefore, $v \to u \to v_1 \to v_2 \to ..... \to v_i \to v$, be Eulerian walk of G'. Then the walk $u \to v_1 \to v_2 \to .... \to v_i \to v$ got by removing edge uv is required uv walk in G.

Remark: As mentioned in 7.2 about application of graphs, the Konigsberg bridge problem was to find an Eulerian walk in Eulerian graph. Euler proved that it is impossible to get Eulerian walk in the given graph. Therefore, there is no solution to Konigsberg bridge problem.

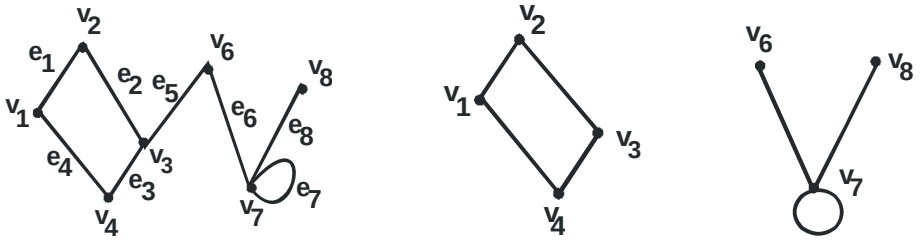


Next, we give an algorithm that produces an Euler circuit for a connected graph with no vertices of odd degree.

Definition 9.10:

An edge is called a bridge or cut – edge in a connected graph if deleting it would create a disconnected graph.

See Fig. 8.4 for an example of a bridge. The edge e_5 is a bridge. Remove e_5 to get disconnected graph $G - e_5$.



G $G - e_5$

Fig. 9.4.2 A bridge or cut-edge

Algorithm 9.11 : Fleury's algorithm

Let G be an Eulerian graph and v be any vertex of G. Starting from v, we traverse the edges of G subject to following conditions

1. Erase an edge that is traversed
2. Erase the isolated vertices, if any.
3. Traverse a bridge only if there is no other alternative.

The procedure is possible and finally we arrive at an empty set. The successive sequence of edges which were removed will form an Eulerian walk for G.

Example 3: To illustrate Fleury's algorithm.

Use Fleury's algorithm to construct Euler circuit for the graph in Fig. 9.4.3.

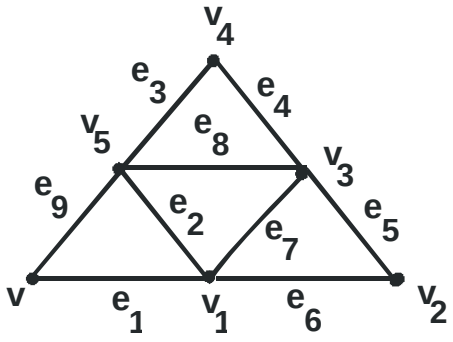
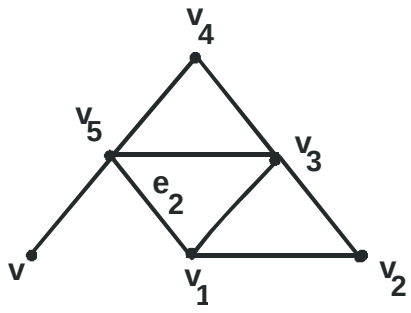


Fig. 9.4.3

Start with vertex v.

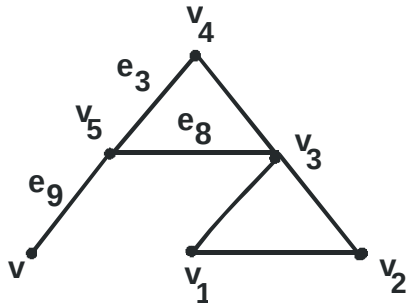
Step 1 : Traverse any edge incident at v say e_1

Step 2 : Erase the edge that is traversed. The graph will now look like this



Step 3 : Traverse the edge e_2.

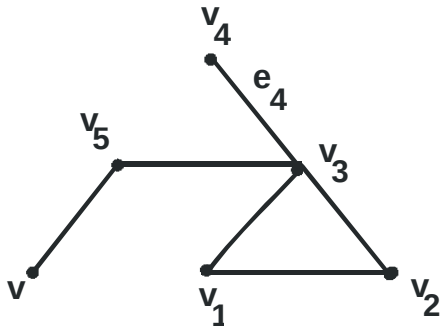
Step 4 : Erase edge e_2 the graph will now be



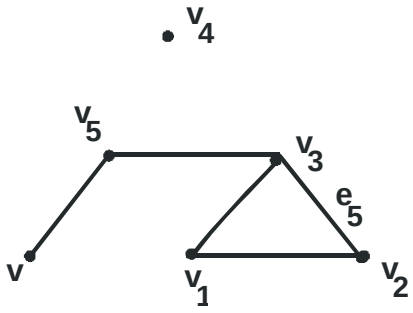
At v_5 we have three choices for edges viz, e_3, e_8, e_9. But edge e_9 is bridge. Thus, by condition 3 of the algorithm we cannot traverse this edge.

Step 5 : Traverse edge e_3.

Step 6 : Erase edge e_3. The graph will be



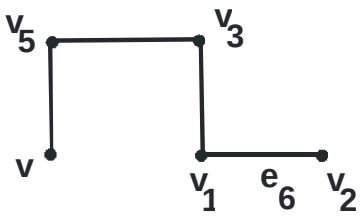
Step 7 : Traverse e_4 and erase e_4 to get graph.



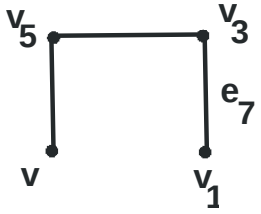
Though e_4 was bridge but we had no alternative.

Step 8 : Erase vertex v_4.

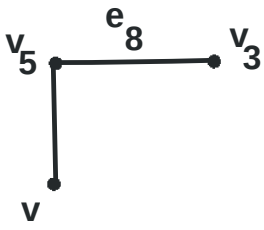
Step 9 : Traverse e_5 and erase e_5 to get the graph.



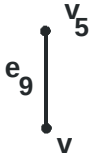
Step 10 : Traverse e_6 and erase e_6 to get the graph. Also remove vertex v_2.



Step 11 : Traverse e_7, erase e_7 and remove v_1 to get,



Step 12 : Traverse e_8, erase e_8 and remove v_3 to get



Step 13 : Traverse e_9, erase e_9 and remove v_5. The graph left is single vertex.

Step 14 : Remove $\overset{\bullet}{v}$ v .

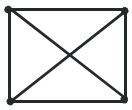
The sequence of edges erased in order were $e_1, e_2, e_3, e_4, e_5, e_6,$ e_7, e_8, e_9. Thus we get Eulerian circuit $v \to v_1 \to v_5 \to v_4 \to v_3 \to v_2 \to v_1 \to v_3 \to v_5 \to v$ observe that each edge of G is traversed exactly once. However, the vertex may be traversed more than once. The graph should remain connected at every step.

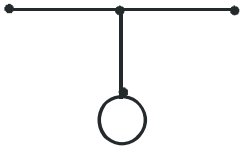
Check your progress

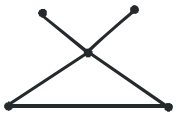
1) Make adjacency and incidence matrix of any one Eulerian graph. What can you say about them?

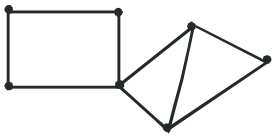
2) Draw a Eulerian graph on 6-vertices.

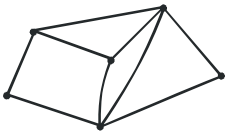
3) Which of the following graphs have an Eulerian circuit, an Eulerian path but not an Eulerian circuit or neither? Give reason for your choice.

a) 

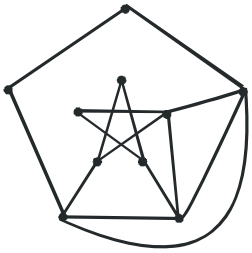
b) 

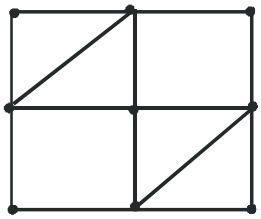
c) 

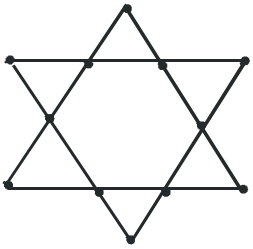
d) 

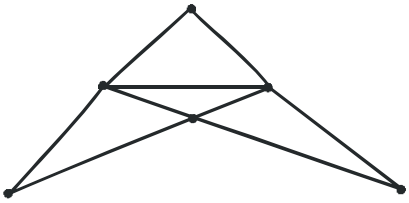
e) 

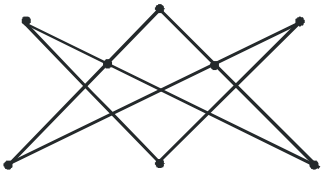
4) Use Fleury's algorithm to find an Eulerian path for the following graphs :

a) 

b) 

c) 

d) 

e) 

5) Judge whether the following are true or false.

i) Eulerian graph is connected.

ii) K_n is Eulerian if and only if n is even.

iii) $K_{m,n}$ is Eulerian if and if m and n are even.

iv) Line graph of Eulerian graph is Eulerian.

v) Petersen's graph is Eulerian graph.

9.5 HAMILTONIAN GRAPHS :

We have seen the walks which include all the edges of the graph. Now we see the graph which contains paths that contain each vertex of the graph. These graphs were named after Sir William Rowan Hamilton who introduced such graphs.

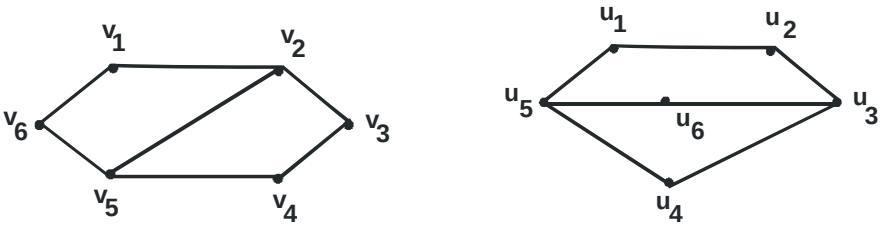
Definition 9.11:

A cycle which passes through each vertex of the graph called Hamiltonian cycle or circuit. We say Hamiltonian cycle spans the graph. A Hamiltonian path is a path that contains each vertex exactly once. A graph having a Hamiltonian cycle is called Hamiltonian graph.

Note : Hamiltonian graph contains a closed path that includes all the vertices of the graph.

Example 4 :

Consider the graphs in Fig. 8.5.1.



(a) **(b)**

Fig. 9.5

The graph of Fig. 9.9.1(a) is Hamiltonian graph. The Hamiltonian cycle is $v_1 \to v_2 \to v_3 \to v_4 \to v_5 \to v_6 \to v_1$.

The graph of Fig. 9.9.1(b) is not Hamiltonian graph. However, the walk $v_6 \to v_3 \to v_4 \to v_5 \to v_1 \to v_2$ is the path that includes all the vertices but it is not closed.

Example 5 :

Any complete graph K_n has Hamiltonian cycle. Hence K_n is Hamiltonian graph.

Note : If G is graph on n vertices and G has Hamiltonian circuit then G must have atleast n edges.

Remark : 1) It is not always possible to determine a Hamiltonian path or cycle.

2) If there is Hamiltonian path or circuit in a graph then there is no efficient way found to trace it, unlike, Eulerian path or cycle.

Some observations of Hamiltonian graphs are as follows :

Theorem 9.8 :

If G is Hamiltonian then for every non empty proper subset S of V(G), $W(G - S) \leq |S|$ where W(H) denotes number of components of any graph H and |S| denotes number of elements of S.

Proof : Let C be Hamiltonian cycle of G. If S is any proper non – empty subset of V(C) = V(G). If G = C, we are through. Otherwise G can only be C with more edges. But the addition of edges to C can only decrease the number of components of C – S.

Therefore, $W(G - S) \leq W(C - S)$

i.e. $W(G - S) \leq |S|$

Remark : The above theorem is useful in showing that some graphs are non-Hamiltonian. For example, the complete bipartite graph $K_{m,n}$ where $m \neq n$ is non-Hamiltonian. Let (V_1, V_2) be partition of vertex set $K_{m,n}$ where $|V_1| = m$. The graph $Km, n - V_1$ is totally disconnected with n – vertices as its components. Thus, $W(Km, n - V_1) = n \not\leq m = |V_1|$

Note : The converse of theorem 7.9.4 is not true. For example, the Petersen's graph satisfies the condition of the theorem but is not Hamiltonian.

Theorem 9.9 :

A Hamilton graph contains no cut-vertices.

Theorem 9.10:

Let G be simple graph with n vertices. Suppose a and v is a pair of non – adjacent vertices such that $\deg.(v) + \deg.(u) \geq n$. Then G is Hamiltonian. The proof of above two theorems is omitted but from it we can prove the following :

Corollary 9.11 :

G has Hamiltonian cycle, if each vertex has degree greater than or equal to $n/2$.

Proof : The sum of the degrees of any two vertices of G is $n/2 + n/2 = n$. Thus, all conditions of theorem 7.9.6 are satisfied. Hence, G has Hamiltonian cycle i.e. G is Hamiltonian graph.

Theorem 9.12 :

Let G be a graph with n-edges. Then G has Hamiltonian cycle if $m \geq \frac{1}{2}\left(n^2 - 3n + 6\right)$ where n is number of vertices of G.

Proof : Suppose u and v are non-adjacent vertices of G.

Let H be the graph obtained by deleting vertices u and v along with any edges having u or v as end point. Then H has n – 2 vertices. The number of edges of H is m – deg(u) – deg (v). [If u and v were adjacent then one edge less will be removed] The maximum number of edges H could possibly have is ${}^{n-2}C_2$. This happens if there is an edge connecting every distinct pair of vertices.

Thus, the number of edges of H is atmost ${}^{n-2}C_2$.

$$
\begin{aligned}
{}^{n-2}C_2 &= \frac{(n-2)!}{2!\left(\overline{n-2}-2\right)!} \quad = \frac{(n-2)!}{2!(n-4)!} \\
&= \frac{(n-2)(n-3)}{2} \\
&= \frac{1}{2}\left(n^2 - 5n + 6\right)
\end{aligned}
$$

Therefore, $m - \deg(u) - \deg(v) \leq \frac{1}{2}(n^2 - 5n + 6)$

$$\Rightarrow \deg(u) + \deg(v) \geq m - \frac{1}{2}(n^2 - 5n + 6)$$

Given that $m \geq \frac{1}{2}(n^2 - 3n + 6)$

Therefore, $\deg(u) + \deg(v) \geq \frac{1}{2}(n^2 - 3n + 6) - \frac{1}{2}(n^2 - 5n + 6)$

$= \frac{1}{2}(n^2 - 3n + 6 - n^2 + 5n - 6)$

$= \frac{1}{2}(2n)$

$= n$

The condition of theorem 9.10 is satisfied and G has Hamiltonian cycle.

Remark : The converse of theorem 9.10 and theorem 8.12 is not true. Example, consider the graph G in Fig. 9.5.2. |V(G)| = n = 8. Each vertex has degree 2. If u and v are vertices of G then $\deg(u) + \deg(v) = 4$.

Fig. 9.5.2

The total number of edges is 8. The conditions in the theorem is not satisfied still we can find a Hamiltonian cycle in G.

Definition 9.12 :

A graph G is called a weighted graph if there is a positive real number associated with each edge of G. The real number is called the weight of the corresponding edge. The weight of subgraph H of a weighted graph is defined as the sum of weights of all edges of H.

Travelling Salesman Problem :

As mentioned in 9.2 about the application of graph, the traveling salesman problem is to find a minimum weight Hamiltonian cycle in a weighted Hamiltonian graph.

No efficient algorithm for solving the traveling salesman problem is known. However, it is possible to obtain a reasonably good but not necessarily optimal solution. One such method is given below. First find Hamiltonian cycle G. Then search for another Hamiltonian cycle of smaller weight as follows :

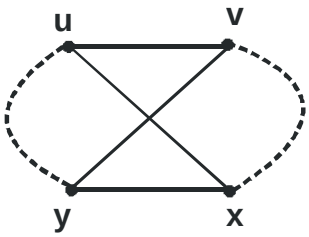


Fig. 9.5.3

Let $\{u, v\}$ and $\{x, y\}$ be two non adjacent edges in C such that the vertices u, v, x and y occur in that order in C. See Fig. 8.5.3 If $\{u, x\}$ and $\{v, y\}$ are edges and $w(u, x) + w(y, v) < w(u, v) + w(x, y)$ then replace edges (u,v) and (x, y) in C by edges (u, x) and (v,y). The resulting cycle C' would be Hamiltonian and will be of less weight than C. continue above process with C', until one gets reasonably good Hamiltonian cycle.

Note : The initial Hamiltonian cycle itself may be chosen such that it has comparatively small weight.

Example 6 :

Find the Hamiltonian cycle of minimal weight for the following graph 9.5.4.

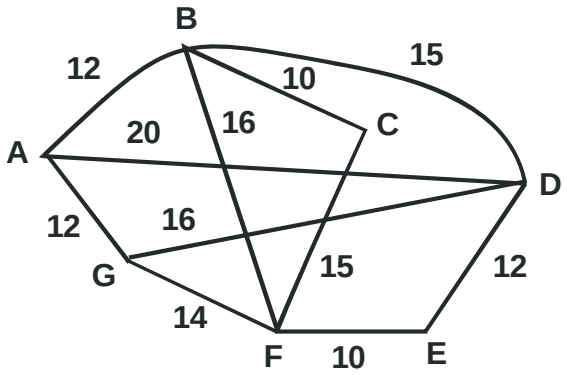


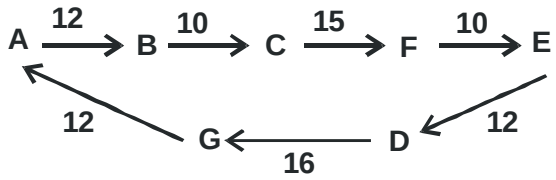
Fig. 9.5.4 Hamiltonian circuit

Consider vertex A vertex. Vertices B, G and D are adjacent to A. w(A,B)=12, w(A,D) = 20 and w(A,G)=12. We have to choose minimum weight. Let us consider edge AB with weight 12. As we reach B there are two choices either C or D. Min {w(B,C), w(B,D)} = w(B,C)=10. So we reach C with w(B,C) = 10. C is adjacent to F and w(C,F) = 15. At F there are three choices either B, G or E.

Min {w,(F,B), w(F,G), w(F,E)}

= w(F,E) = 10.

Thus, we take vertex E. So far we have traversed as follows : $A \xrightarrow{12} B \xrightarrow{10} C \xrightarrow{15} F \xrightarrow{10} E$. From E we reach D, w(E,D) = 12. From D we have to go to G, as B is already traversed. From G we reach A back again. Thus, the Hamiltonian cycle of minimal weight for the graph in Fig 8.5.4 is



The weight of this cycle is 87 as

w(AB) + w(BC) + w(CF) + w(FE) + w(ED) + w(DG) + w(GA)

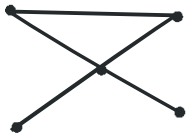
= 12+10+15+10+12+16+12

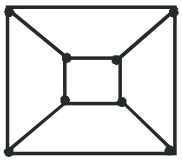
= 87

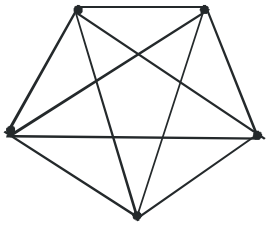
Check your progress

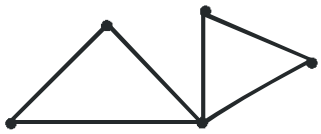
1) Give two Hamiltonian circuits in K_5 that have no edges in common.
2) Give example of Hamiltonian graph which is not Eulerian.
3) How many distinct Hamiltonian cycles are there in K_4 and K_6?
4) Show that there are only three Hamiltonian graphs on 6-vertices, C_6, K_6 and $K_{3,3}$.
5) Give one example of an Eulerian graph which is not Hamiltonian.
6) Justify whether true or false.
   i) Every Hamiltonian graph is connected.
   ii) An induced subgraph of Hamiltonian graph is Hamiltonian.
   iii) A simple graph which is both Hamiltonian and Eulerian is necessarily a cycle.

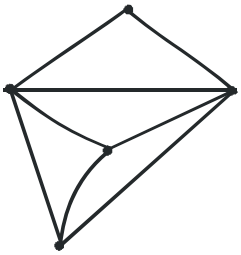
7) Which of the following graphs have Hamiltonian circuit, a Hamiltonian path but no Hamiltonian circuit, or neither. Trace the circuit if graph has Hamiltonian circuit.

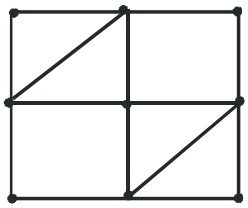
a) 

b) 

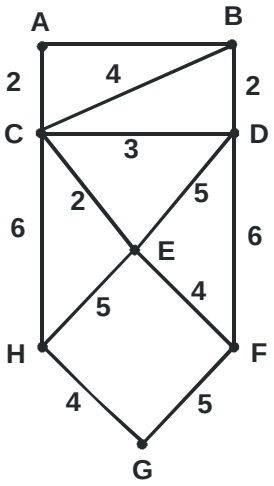
c) 

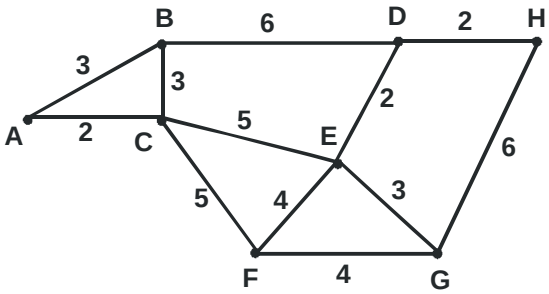
d) 

e) 

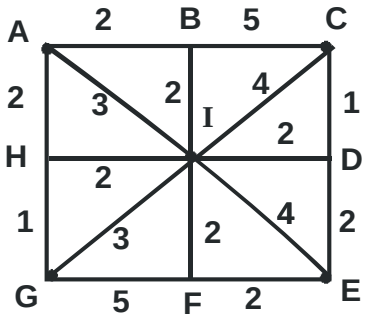
f) 

8) Find a minimal weight Hamiltonian circuit for the graphs given below.

a) 

b) 

c)



9.6 COLOURING OF GRAPHS :

Definition 9.13 :

Consider a graph G. A vertex colouring or colouring of G is an assignment of colours to the vertices of G such that adjacent vertices have different colours.

A graph is said to be k-colourable if the vertices of G are coloured using atmost k-colours such that adjacent vertices receive different colours.

The chromatic number denoted by $\chi(G)$ of a graph G is the minimum number of colours needed to colour G.
Note : If a graph is k-colourable then it is (k+1) – colourable.

Examples :

1) Kp is p-colourable..As each pair of vertices is adjacent. $\chi(Kp) = p$. Consider K_4 in Fig. 8.6.1

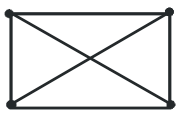


Fig. 9.6.1 Chromatic number of K_4 is 4.

$$\chi(K_4) = 4$$

2) $\overline{Kp}$ is complement of Kp. It is disconnected graph with p components as vertices. $\overline{Kp}$ is 1-colourable $\chi(\overline{Kp}) = 1$. As shown in Fig. 8.6.2, $\overline{K_4}$ is 1-colourable and $\chi(\overline{K_4}) = 1$.

Fig. 9.6.2 Chromatic number of $\overline{K}_4$ is one.

3) Consider bipartite graph $K_{m,n}(V_1, V_2)$ with m-vertices in V_1 and n-vertices in V_2. No two vertices of V_1 and V_2 are adjacent. But every vertex of V_1 is adjacent to each vertex of V_2. Therefore, every vertex of V_1 can be coloured by colour α and all vertices of V_2 can be coloured by colour β. Thus $\chi(K_{m,n}) = 2$. Consider $K_{2,3}$ as in Fig. 9.6.3.

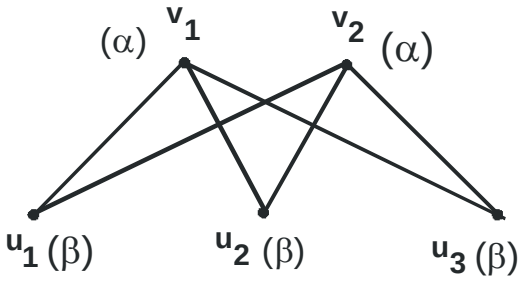
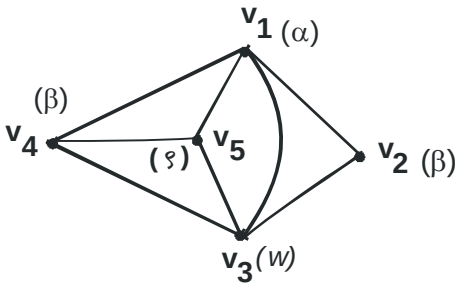


Fig. 9.6.3 : Colouring of $K_{2,3}$

$V_1 = \{v_1, v_2\}; V_2 = \{u_1, u_2, u_3\}$, Chromatic number of $K_{2,3}$ is two.

Theorem 9.13 : Graph G is 2-colourable iff G is bipartite

4) Consider the graph G in Fig. 9.6.4.



G

Fig. 9.6.4

Let vertex v_1 be coloured by colour α. Then v_4 and v_5 must receive two distinct colours say β and ऽ different from α. Now, vertex v_3 is adjacent to v_1, v_4 and v_5. Therefore, it cannot

have colour α, β, γ. Hence v_3 will receive colour ω. The vertex which is to be coloured is v_2. v_2 can receive colour β as it is not adjacent to v_4. Thus, atleast 4 colours are necessary to colour the graph. Hence $\chi(G) = 4$.

Definition 9.13 :

A graph is called planar graph if it can be drawn in a plane so that no two edges of graph cross.

The crossing is said to occur in a graph it two edges meet in a point which is not a vertex.

The figure 9.6.5 shows an example of planar and non-planar graph.

(a) Non-planar Graph **(b) Planar Graph**

Fig. 9.6.5

In Fig. 9.6.5(a) edges v_2v_4 and v_1v_3 cross each other. In Fig. 9.6.5(b) two edges wherever they meet they meet only at their end points. The graphs (a) and (b) are isomorphic.

Theorem 14 : Every planar graph is 6-colourable.

Theorem 15 : (Heawood) Every planar graph is 5-colourable.

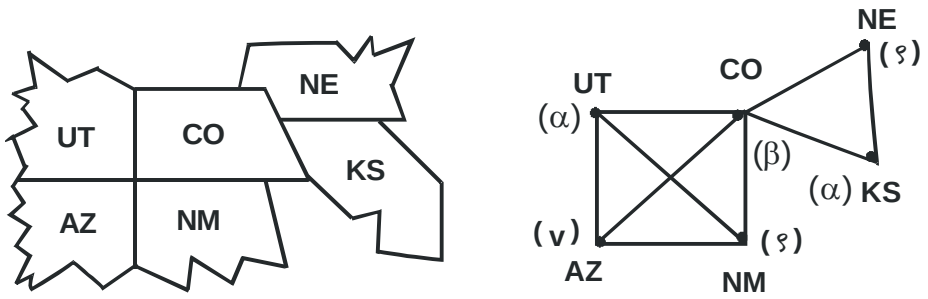
Theorem 16 : (four colour theorem) Every planar graph is 4-colourable.

Note : The proof of theorem 4 was given by computer computations. A computer free proof of this theorem is still to be found. Appel and Haken have solved four colour theorem by using computers.

Application of colouring of graph :

The colouring of graphs were used to solve map-colouring problem. The colouring of map means to colour each region (or country or state or province) so that no two distinct regions sharing a

common border have the same colour. The map-colouring problem is to find the smallest number of colours used to colour the map. Each region will be considered as vertex and an edge will be common boundary shared by two regions. For example, consider the map given in Fig. 7.10.6 and its graphical representation with colouring.



(a) Map G **(b) Graph of map G**

$\chi(G) = 4$

Fig. 9.6.6

Definition 9.14 :

Given an integer $\lambda > 0$, we denote by $P_G(\lambda)$ as the number of different λ- colourings of graph G. We call $P_G(\lambda)$ as chromatic polynomial of G.

Example :

1) Consider simple trivial graph K_1. K_1 is graph with one vertex. We can colour K_1 with any of given λ colour. Therefore, $P_{K_1}(\lambda) = \lambda$.

2) Consider graph K_2, a graph with two incident vertices u and v. We can colour vertex u with λ colours but v will carry the colour which is not given to u. So total colourings of v are $(\lambda - 1)$ – colourings. Thus, total colourings of K_2 given by $P_{K_2}(\lambda) = \lambda(\lambda - 1)$.

3) In General, $P_{K_n}(\lambda) = \lambda(\lambda - 1)$ --------- $(\lambda - n + 1)$.

4) Consider the line graph L_4 as shown in Fig.9.6.7.

Fig. 9.6.7 Line graph L_4

Suppose there are λ- colours. The first vertex can be coloured by any λ colours. The second vertex adjacent to first can be coloured by any $(\lambda-1)$ - colours. 3rd vertex can be coloured by any $(\lambda-1)$ colours not used for second vertex. Similarly, the 4th vertex can be coloured by any $(\lambda-1)$ - colours. By multiplication principle of counting, the total number of colourings is $\lambda(\lambda-1)^3$. Thus, $P_{L_4}(\lambda)=\lambda(\lambda-1)^3$.

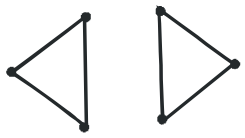
Theorem 9.17:

Let $G_1, G_2, ..., G_K$ be components of disconnected graph G. Then $P_G(\lambda)=P_{G_1}(\lambda).P_{G_2}(\lambda),....,P_{G_K}(\lambda)$, where R.H.S. is product of chromatic polynomials of each component.

Example:

Consider graph G in Fig.9.10.8. It has two components each of which is K_3. The chromatic polynomial of K_3 is $\lambda(\lambda-1)(\lambda-2)$.

$\therefore P_G(\lambda)=\lambda^2(\lambda-1)^2(\lambda-2)^2$



G

Fig. 9.6.8

As $\chi(G)=3$, the number of distinct ways to colour G using 3 – colours is $P_G(3)=3^2(3-1)^2(3-2)^2$

$= 9(2)^2(1)^2$

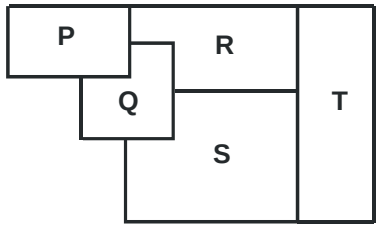
$= 9\times 4$

$= 36$

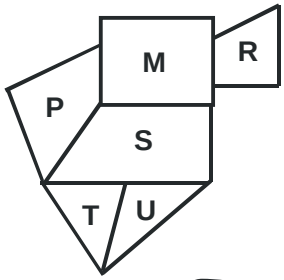
Check your progress

1) Construct a graph for the following maps.

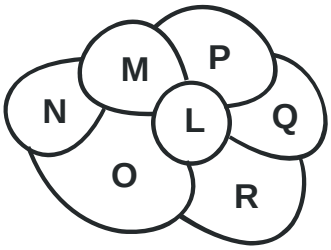
a)



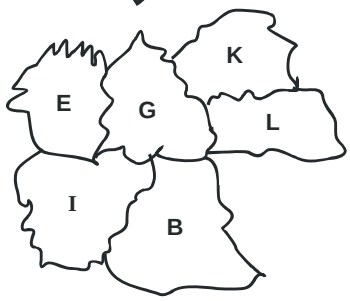
b)



c)



d)

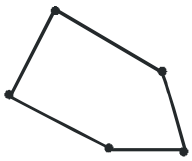


2) Find the chromatic number for the following graphs.

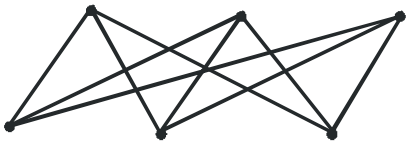
a)

b)

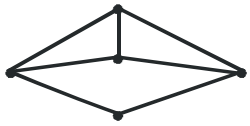
c)



d)



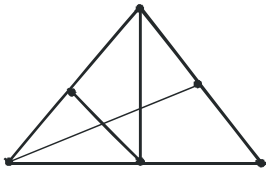
e)



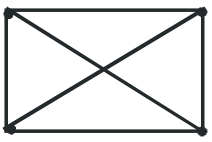
3) Find the chromatic polynomial P_G for the graphs given in Exercise 2.

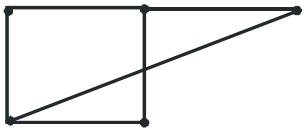
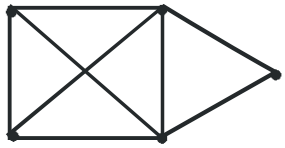
4) Determine whether the given graphs are planar? If so, draw it so that no edges cross.

a)



b)



c)  d) 

5) Find P_G and $X(G)$ for the graph drawn in Exercise 1.

6) Give example of a connected graph on five vertices that is (a) planar (b) not planar.

7) What is $X(G)$ for a bipartite graph G? Justify.

8) Judge whether following is true or false.

   i) The chromatic number of any cycle is 2.

   ii) The chromatic number of bipartite graph is 2.

   iii) For each integer $p > 0$ there is a graph which is p-colourable.

   iv) The chromatic number of Petersen's graph is 4.

   v) Any two graphs with same chromatic number are isomorphic.

9.7 LET US SUM UP :

In unit 8, we have seen interesting graphs like Eulerian graphs and Hamiltonian graphs. We have also leant simple methods to find Eulerian circuit and Hamiltonian circuit. As colouring of graphs also is a field where not much work is done, we have tried to learn basic concepts of colouring a graphs.

9.8 REFERENCES

1. Discrete Mathematical structures by Kolamn, Busby and Ross. Pearson education.
2. Introduction to graph theory by Douglas B. West.
3. Discrete Mathematics and its applications by Kenneth. H.Rosen. McGraw Hill edition.
4. Graph theory by Frank Harary. Narosa Publication.
5. Discrete Mathematics by Norman Priggs. Oxford.

❖❖❖❖

10

TREES

Unit Structure

10.0 OBJECTIVES

After going through this chapter students will be able to understand:

- Know about tree in graph theory, its properties and characterisation
- Find minimal spanning trees
- Know about directed and undirected trees

10.1 INTRODUCTION :

One of the most important topic in study of Graph Theory is Trees. Many applications rangeing from family tree to computer science management tree is dealt with the study of trees.

The first use of trees by German Mathematician Karl Georg Christian von Staudt was done in 1847 in his work on projective Geometry and by German physicist Gustav Robert Kirchhoff in the same year in his paper on electrical networks. The word tree for a particular graph was first used by Arthur Cayley.

In this unit we are going to study trees and its properties first. Then we study labeled trees; spanning trees, rooted and binary trees. The wide range of application of trees in different field has created a revolution in study of trees.

A graph of an undirected tree T will have a single line without arrows. While the edge of directed tree will have arrows showing the direction of edge.

10.2 CHARACTERISATION OF TREES :

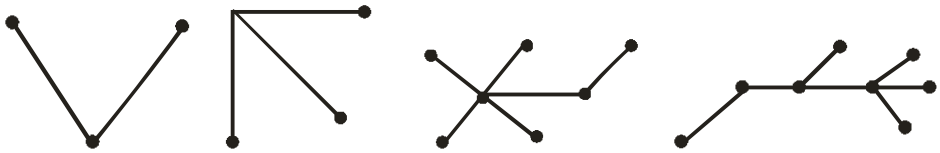
To start with we have to first understand basic definitions related to trees.

10.2.1 Definition : A connected graph which contains no circuits is called a tree.

We can also frame a definition which uses set theory notation. Let A be a set and T be relation on A then we say that T is a tree if there is a vertex v_0 in A with the property that there exists a unique path in T from v_0 to every other vertex in A but no path from v_0 to v_0.

Remark : Tree is a connected acyclic graph.

Some examples of trees is given in figure 10.2.1.



(a) **(b)** **(c)** **(d)**

Fig. 10.2.1

10.2.2 Properties of Trees

Let T be a graph on n vertices then –

1. There is one and only one path between every pair of vertices in a tree.
2. T has n vertices and n – 1 edges.
3. T is connected and has n – 1 edges.

4. T is connected and every edge is cut-edge.
5. T is minimally connected graph.
6. T has n-vertices, n – 1 edges and no circuits.
7. In a tree with $n \geq 2$, there are atleast two vertices of degree one.

10.2.3 Definition : A pendant vertex is defined as a vertex of degree one.

Example : In the graph given below in Fig. 9.2.2 v_0 is the pendant vertex. There are more than one, pendant vertex in any tree.

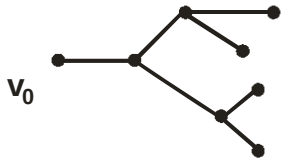


Fig. 10.2.2

10.2.4 Definition : The initial vertex v_0 considered when we start drawing a tree is called root vertex. A tree in which there is root vertex is called rooted tree. In rooted tree the root vertex is clearly distinguished from remaining vertices. Denote tree T with root vertex v_0 as (T, v_0). Examples of rooted trees are given in Fig. 10.2.3.

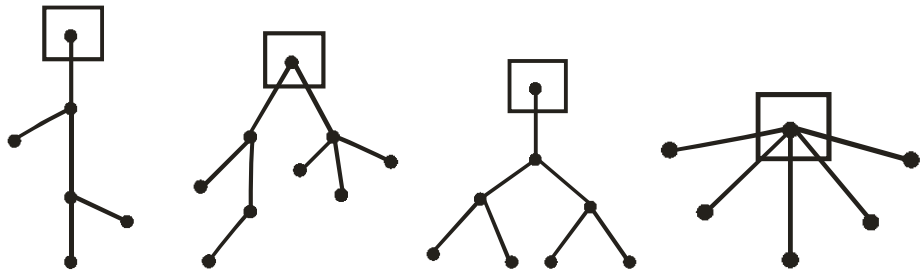


Fig. 10.2.3 Rooted trees

10.2.5 Definition : A binary tree is defined as a tree in which there is exactly one vertex of degree two and each of remaining vertices are of degree one or three.

Examples of binary trees are given in Fig. 9.2.4.

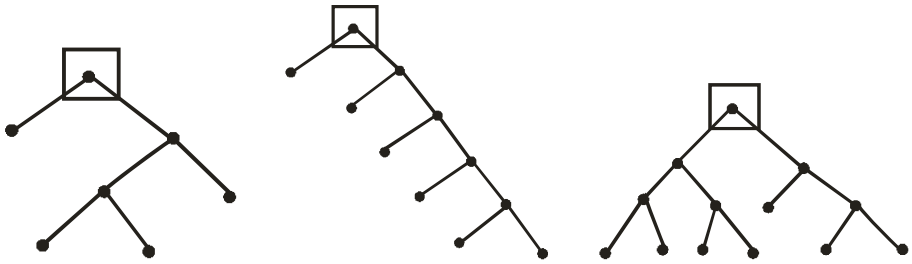


Fig. 10.2.4 : Binary Trees

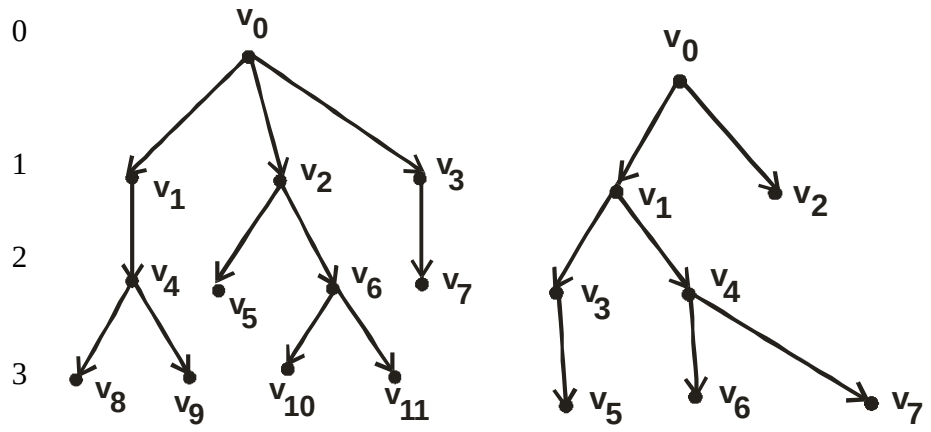
Note that every binary tree is a rooted tree.

10.2.6 Theorem 1 : Let T be a tree with root vertex v_0 then,

a) There are no cycles in T.
b) v_0 is the only root of T.
c) Each vertex in T, other than v_0 has in-degree one and v_0 has in-degree zero.

10.2.7 Levels in a tree

Consider the trees given below in the figure 10.2.5. We start with vertex v_0 the root vertex. No edges enter v_0.



(a) T_1 (b) T_2

Fig. 10.2.5 : Levels in a tree

Several edges may leave v_0. These edges are drawn in downward direction. The vertex v_0 is said to be at level 0. The edges starting at v_0 will terminate into the vertices which will be called as level 1 vertices. v_0 is sometimes called parent of vertices

in level 1 while vertices in level 1 are called the offspring of v_0. The edges having a vertex at level 1 are drawn downwards. The vertices at which the edges drawn from level 1 vertices terminates are called vertices at level 2. The offspring of any one vertex are sometimes called siblings. The largest level number of a tree is called the height of the tree. The vertices of the tree that have no offspring are called the leaves of the tree. All the vertices of tree that can be reached by a path beginning at any vertex v are called descendants of vertex v. If T is rooted tree with vertex v_0 and v is any vertex of T other than v_0 then the tree with root vertex v is called subtree of tree T beginning at v. Denote subtree of tree (T, v_0) as T(v).

In figure 10.2.5(a) T_1 has vertex v_0 at level 0. Level 1 vertices are v_1, v_2, v_3. Level 2 vertices are v_4, v_5, v_6, v_7. Level 3 vertices are v_8, v_9, v_{10}, v_{11}. The height of tree T_1 is 3. The vertices v_8, v_9, v_{10}, v_{11} are leaves of tree T_1. The offsprings of v_0 are v_1, v_2, v_3. The offspring of v_2 are v_5 and v_6. The vertices v_5 and v_6 are siblings of v_2. The descendants of v_2 are v_{10} and v_{11}. The subtree of T_1 beginning at v_2 is given in figure 10.2.6. The height of subtree is 2.

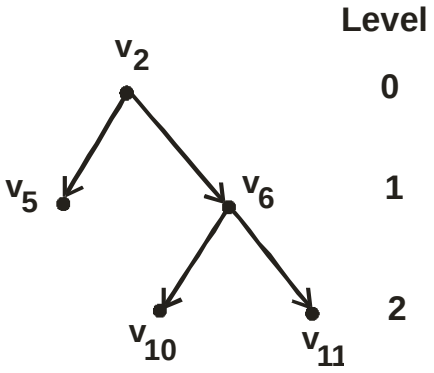
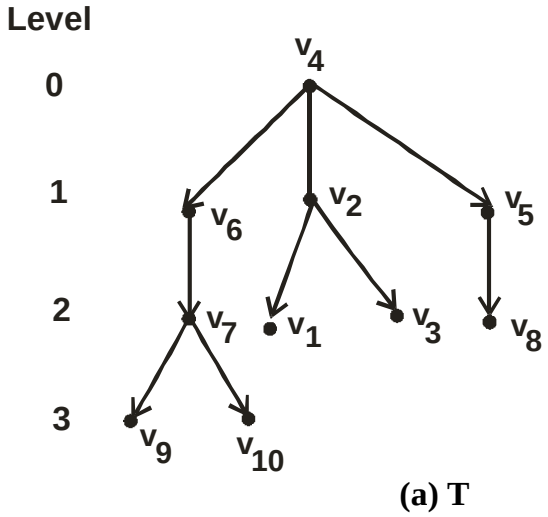


Fig. 10.2.6 : Subtree of T_1

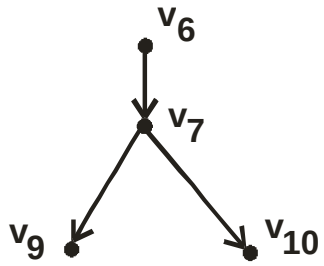
Example : Draw a tree T with vertex set $\{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9, v_{10}\}$ and edge set $\{(v_2, v_3), (v_2, v_1), (v_4, v_5), (v_4, v_6), (v_5, v_8), (v_6, v_7), (v_4, v_2), (v_7, v_9), (v_7, v_{10})\}$. Show that T is a tree and identify the root. Draw one subtree of T. Write height of T.

Solution : T is a tree with root vertex v_4 as there is path from v_4 to every vertex in tree T. There are no cycles. Height of tree T is 3.



(a) T

Subtree of T is



(b)

Fig. 10.2.7 Subtree of T

10.3 LABELED TREES

It is sometimes useful to ℓabel the vertices of tree for a particular purpose. The set of vertices of tree is not important but emphasis is given on the label which is attached to vertices of tree. Such a tree where labels are given to each vertex is called labeled tree.
Some examples of labeled trees.

10.3.1 Label tree representing algebraic – expression.

Consider the algebraic expression.

$$\left(4 \div \left(3 \times x\right)\right) + \left(\left(2 - x\right) + \left(5 + x\right)\right)$$

The labeled tree for this expression is shown in Fig. 10.3.1.

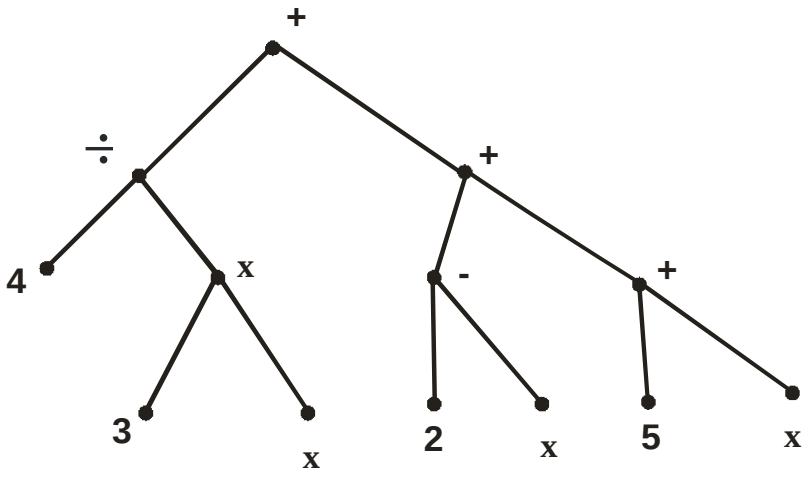


Fig. 10.3.1 : Labeled tree for algebraic expression

While drawing such tree, we try to find the central operator. The central operator is the operation which is inbetween two numbers or expressions. As shown in the example. '+' is central operator of expression $\left(4 \div \left(3 \times x\right)\right)$ and $\left(\left(2 - x\right) + \left(5 + x\right)\right)$. '$\div$' is central operator of number 4 and expression $\left(3 \times x\right)$ while '+' is central operator of expression $\left(2 - x\right)$ and $\left(5 + x\right)$. Similarly, '-' is central operator of 2 and x; '+' is central operator of 5 and x; 'x' is central operator of 3 and x. Each vertex has only one label either a operation sign or the number.

10.3.2 Positional tree : It is a type of labeled tree. The vertices are labeled so as to show the position of offspring. While drawing a positional tree we have to imagine that the n – offspring positions for each vertex are arranged symmetrically below the vertex and we place in its appropriate position each offspring that actually occurs.

We do not label the root vertex in these trees as root vertex is not a offspring. Suppose we choose three offspring positions then each vertex will have offsprings placed at these 3 – positions only. If any offspring is not present then that position will not be shown.

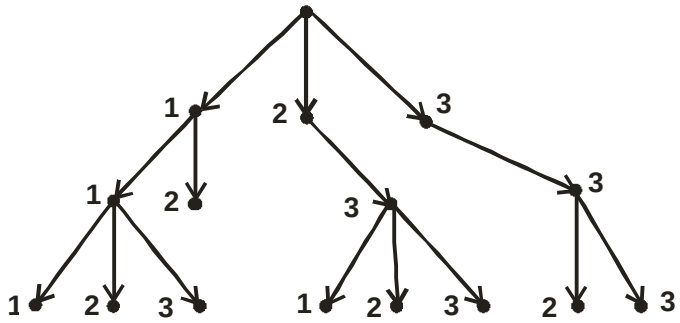


Fig. 10.3.2 A positional 3 - tree

As shown in figure 10.3.2 the first offspring – 1 from any vertex v if it exists is edge drawn from v sloping to its left. The offspring – 2 from vertex v if it exists is drawn vertically downward from v while offspring – 3 from vertex v if it exists, is drawn to the right of vertex v dropping downloads.

10.3.3 Labeled graph : A graph in which every vertex is assigned a unique name or label (no two vertices have the same label) is called a labeled graph.

Whenever we are counting the total number of distinct labeled graphs on certain number of vertices the two differently labeled graphs are counted separately even though they are isomorphic. Note that the number of distinct labeled trees with n vertices $(n \geq 2)$ is n^{n-2}. For example, consider labeling of trees on 4 – vertices. There are 16 trees on 4 – vertices that carry distinct labels. Some of these labeled trees on 4 – vertices are shown in Fig. 9.3.3.

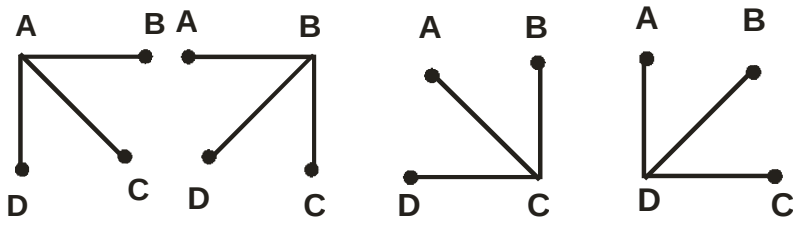


Fig. 10.3.3 : Labeled trees

The trees in figure 10.3.3 are isomorphic but are different labeled trees.

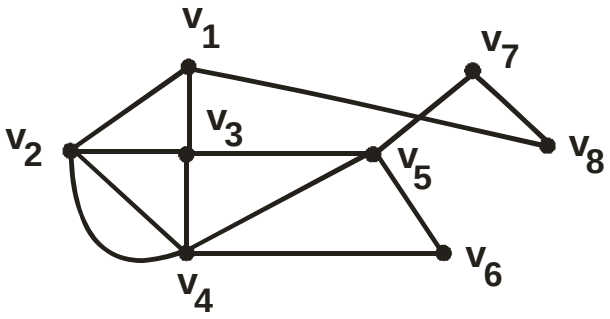
9.4 MINIMAL SPANNING TREES :

Here we see how are can associate tree to a connected graph.

Definition 10.4.1 : Let G be a connected graph then a spanning tree T of G is a subgraph of G which is a tree and which contains all the vertices of G.

Example : Consider graph G and its spanning tree in figure 10.4.1(a) and 10.4.1(b) respectively.

a)



b)

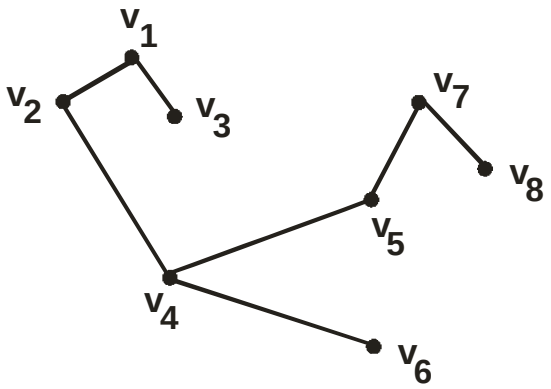


Fig. 10.4.1 : Spanning tree

We remove the edges of a graph G which forms cycle and get a tree.

Definition 10.4.2 : A minimal spanning tree in a connected weighted graph is a spanning tree that has the smallest possible sum of weight of its edges.

There are two algorithm for constructing minimal spanning trees. Both proceed by successively adding edges of smallest weights, from those edges with a specified property that have not already been used.

10.4.3 Prim's algorithm : Let G be a graph with n-vertices.

Step 1 Choose a vertex v_1 of G. Let $V = \{v_1\}$ and $E = \{\ \}$

Step 2 Choose a nearest neighbour v_i of V that is adjacent to v_j, $v_j \in V$ and for which the edge (v_i, v_j) does not form a cycle with members of E. Add v_j to v and edge $v_i\, v_j$ to E.

Step 3 Repeat step - 2 until |E| = n – 1 , Then v contains all n vertices of G and E contains all the edges of minimal spanning tree T.

Example : The small town of social circle maintains a system of walking trails between the recreational areas in town. The system for the same is shown in Fig. 10.4.2. The system is a weighted graph. The weights represent the distances in kilometers between sites.

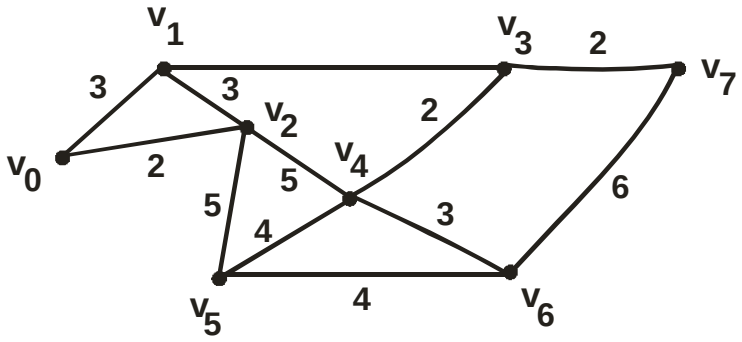


Fig. 10.4.2

Using Prim's algorithm we begin with vertex v_0. The nearest neighbour to v_0 is v_2 who is 2 – km away from v_0. So we select edge $v_0\, v_2$ first. Fig. 9.4.2(a). Consider set $\{v_0, v_2\}$. The vertex v_1 is the nearest neighbour. We can either choose $v_0\, v_1$ or $v_2\, v_1$ as next edge. Let us choose $v_2\, v_1$. Then vertex set will be $\{v_0, v_2, v_1\}$ and edges set will be $\{v_0\, v_2, v_2\, v_1\}$. Fig. 9.4.2(b). Here we cannot choose edge $v_0\, v_1$ as it will make a cycle so next vertex we choose is v_5 and edge $v_2\, v_5$ to get $\{v_0, v_2, v_1, v_5\}$ and edge set $\{v_0, v_2, v_2\, v_1, v_2\, v_5\}$. Continue in this manner and finally get minimal spanning tree shown Fig. 10.4.2.

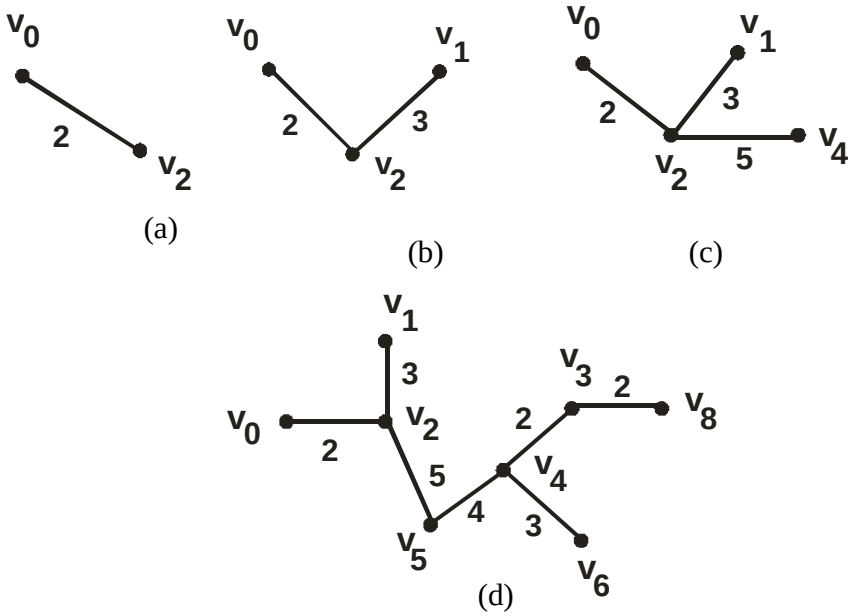


Fig. 10.4.2: Minimal spanning tree using Prim's algorithm

Thus total weight of the spanning tree which is minimal is 2 + 3 + 5 + 4 + 2 + 3 + 2 = 21. Thus, the bicycle path of minimum length for the system is of 21 km.

Note that for the same graph shown in Fig. 10.4.2. We can find minimal spanning tree using Prim's algorithm beginning with vertex v_4. Here also bicycle path is 21 km, long as seen in Fig. 10.4.3.

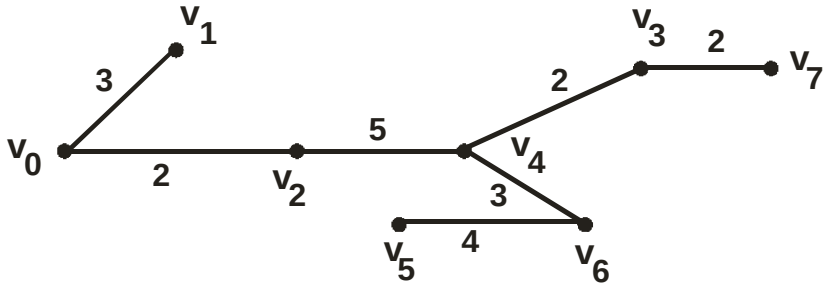


Fig. 10.4.3 Minimal Spanning Tree

10.4.4 Kruskal's algorithm : Let G be a connected graph with n vertices and let $S = \{ e_1, e_2, ..., e_k \}$ be set of weighted edges of G.

Step 1 Choose edge e_1 in S of least weight. Let $E = \{ e_1 \}$. Replace S with $S - \{ e_i \}$.

Step 2 Select edge e_i in S of least weight that will not make a cycle with edges of E. Replace E with $E \cup \{e_i\}$ and S with $S - \{ e_i \}$.

Step 3 Repeat step - 2 until $|E| = n - 1$.

Since G has n vertices, the n – 1 edges in E will give spanning tree T.

Example : Consider the graph given in Fig. 10.4.3.

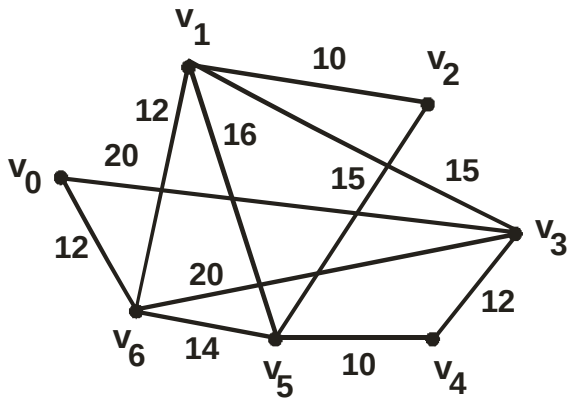
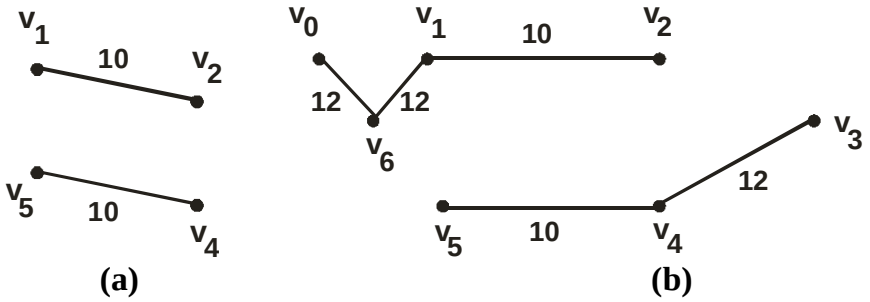
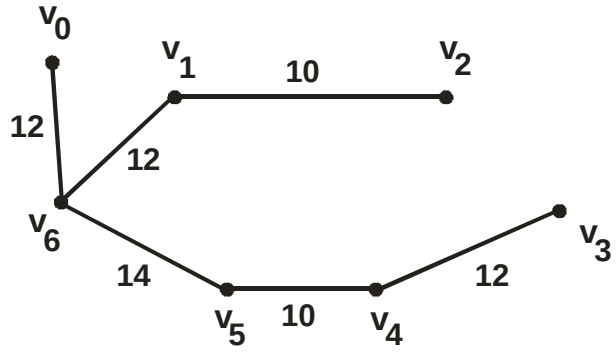


Fig. 10.4.3

Initially choose edges with minimum weight. In Fig. 10.4.3, they are edges $v_1 v_2$ and $v_5 v_4$. Both of these are selected. Fig. 10.4.4 (a) Next there are three edges of weight 12. All these edges can be added without creating a cycle. Fig. 10.4.4 (b) Edge of weight 14 is remaining edge of least weight. Adding this edge given us six edges for 7 – vertex graph, so a minimal spanning tree is found as shown in Fig. 10.4.4 (c).





(c)

Fig. 10.4.4 Minimum spanning tree by Kruskal's algorithm

10.4.5 Application of minimal spanning tree

Suppose that n cities $v_1, v_2, ..., v_n$ are to be connected through a network of roads. The cost C_{ij} of building a direct road between v_i and v_j is given. Then the problem is to find the least expensive network that connects all n cities together. Thus the problem of connecting n – cities with a least expensive network is a problem of finding a shortest spanning tree in a connected weighted graph of n vertices.

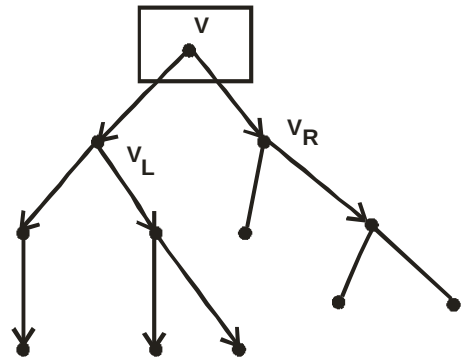
10.5 TREES SEARCHING :

Sometimes it is necessary to consider each vertex of a tree T exactly once in some specific order. When we reach a particular vertex and wish to perform computation at that vertex then that application is represented by the tree. By visiting a vertex, we mean performing particular task at that vertex.

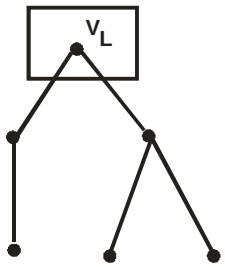
The process of visiting each vertex of a tree in some specific order is called searching the tree or tree search.

In this topic we will consider searches on binary positional trees. We know that in a binary positional tree, each vertex has two offsprings. Denote these offspring as v_L and v_R where v_L denotes left offspring and v_R denotes right offspring. If a binary tree is not positional then it can be labeled in such a way that it becomes positional.

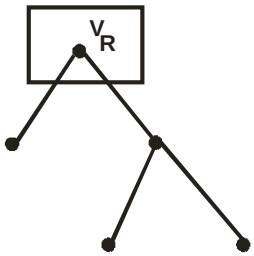
10.5.1 Definition : Let T be positional binary tree with root vertex v then if v_L exists then the subtree $T(v_L)$ will be called the left subtree of T and if v_R exists then the subtree $T(v_R)$ is called right subtree of T. See Fig. 10.5.1.



(a)
Positional binary tree T



(b)
Left subtree $T(v_L)$



(c)
Right subtree $T(v_R)$

Fig. 10.5.1 Subtree

Note : 1) $T(v_L)$ if it exists is a positional binary tree with root v_L

2) $T(v_R)$ if it exists is a positional binary tree with root v_R

10.5.2 Methods of tree searching

There are three methods of searching. They are :

1) Preorder Search
2) Inorder Search
3) Postorder Search

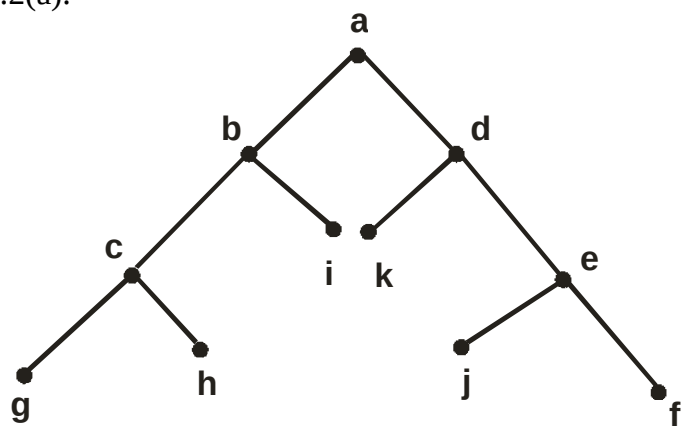
We will discuss these three methods of tree searching in detail.

10.5.2.1 Preorder Search

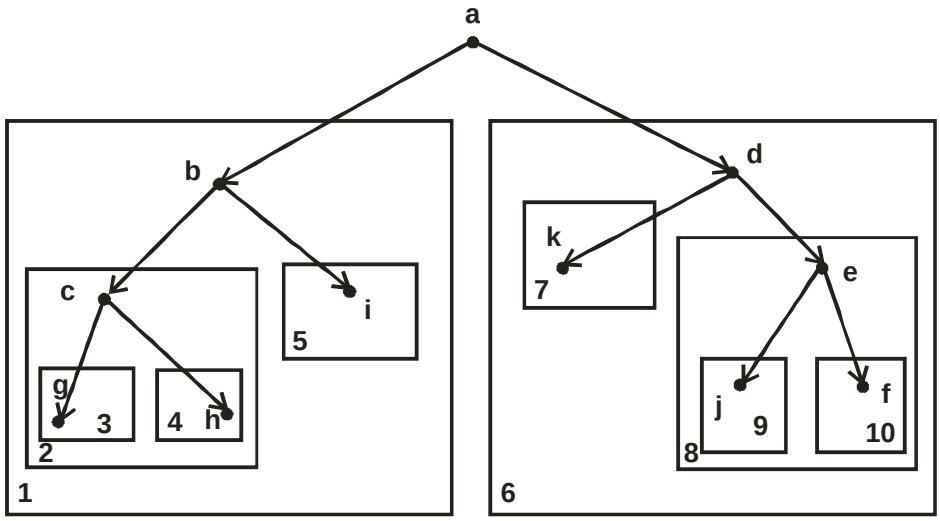
Preorder search of a tree consists of following three steps :

1) Visit the root
2) Search the left subtree if it exists
3) Search the right subtree if it exists

Exercise : Use preorder search and find all subtrees of given tree t in Fig. 10.5.2(a).



(a) Tree T for preorder search



(b) Subtrees of T after preorder search

Fig. 10.5.2 a b c g h i d k e j f

Procedure : According to preorder search applied to T, first the root is visited and 'a' will be printed. Then the left subtree starting at 'b' will be considered. The boxes represents the subtrees in the order of their search. The next vertex that will be printed will be 'b'. At 'b' the left subtree begin at 'c'. Thus, next printed vertex will be 'c'. After 'c' comes 'g' and 'h'. All the subtrees towards left of vertex 'a' are searched. Now, we proceed to right subtrees of vertex 'a'. The order in which search gives the vertex are 'd' then 'k' then 'e' then 'j' then 'f'. Thus, the preorder search gives us tree T as "a b c g h i d k e j f".

10.5.2.1(a) : Polish form or prefix of algebraic expression

Consider the parenthesized expression
$(p+q)\times(r-(s\div d))$

Fig. 10.5.3(a) shows the labeled positional binary tree representation of this expression.

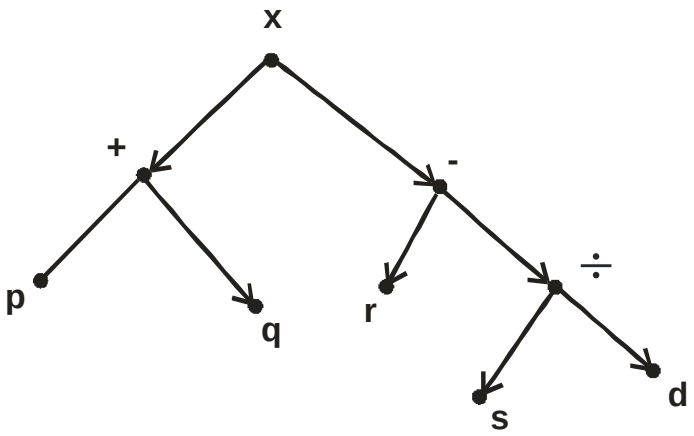


Fig. 10.5.3(a) Labeled positional binary tree

We can apply preorder search to this tree as shown in Fig. 10.5.3(b).

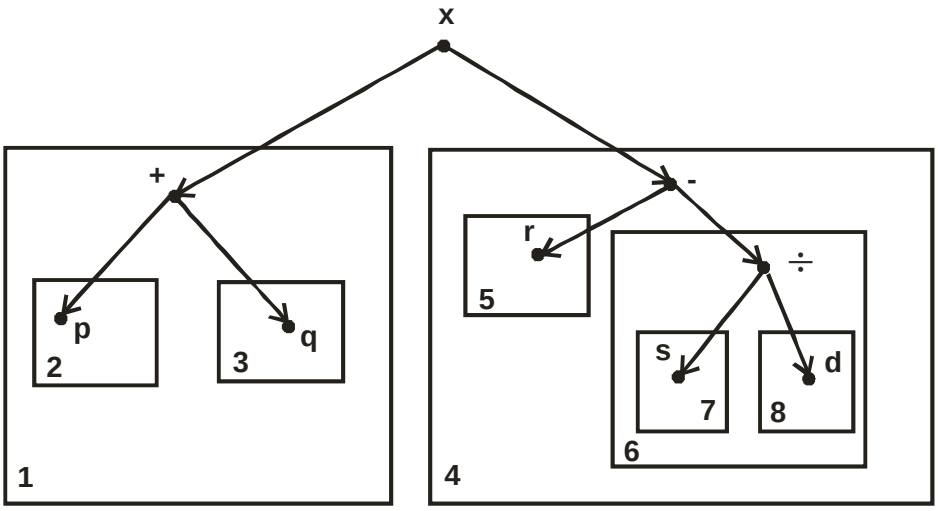


Fig. 10.5.3(b) Tree "x + pq – r ÷ sd"

The preorder search gives the string "x + pq – r ÷ sd". This is polish form of the given expression ((p + q) × (r – (s ÷d)). The boxes shows the order of getting the subtrees.

10.5.2.2 Inorder Search

Inorder search of tree consists of following steps.

1) Search left subtree $\left(T\left(v_L\right), v_L\right)$ if it exists
2) Visit the root, v.
3) Search the right subtree $\left(T\left(v_R\right), v_R\right)$ if it exists.

Exercises : Use inorder search and find all the subtree of tree T given in Fig. 10.5.2(a).

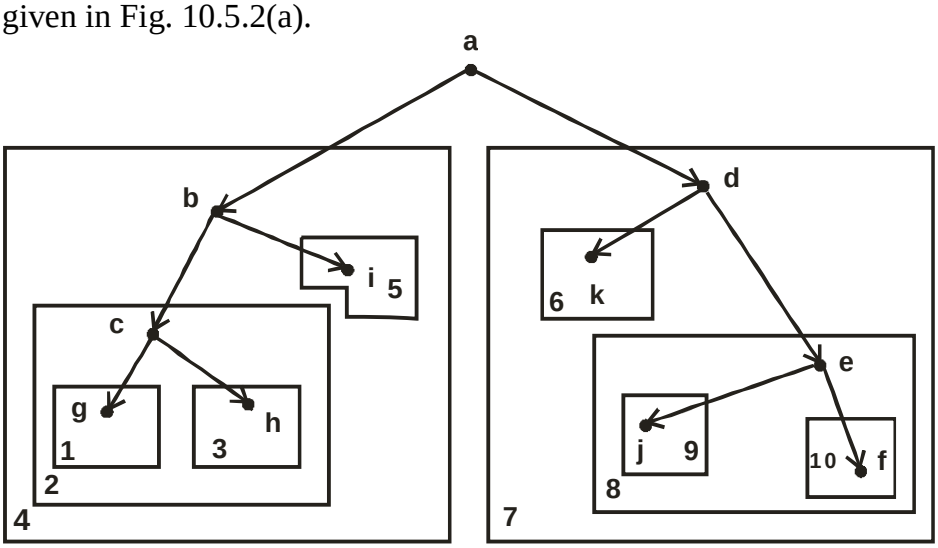


Fig. 10.5.4 Inorder search

First, search subtree 1 in Fig. 10.5.2(a). This requires us to search subtree 2 and this in turn requires us to search subtree 3. As before, a search of tree simply prints the label of the vertex.

Thus, symbol 'g' is printed first. The root of g is 'c', so next printed vertex is 'c'. Right of 'c' is 'h', so next vertex is 'h' which is printed. Now, the next subtree begins at 'b', and right of it is 'i'. The vertex which will be printed after 'c' will be 'b' and 'i'. The left subtree of 'a' is complete. Start with the innermost vertex of right subtree. Subtree in box 6, gives vertex 'k', then comes root 'd' and then vertex 'f'. Now vertex 'f' is to right of root 'e'. Finally the inorder search will give the tree with following order of vertices, "g c h b i a k d j e f".

10.5.2.2(a) Infix notation for algebraic expression

The labeled positional binary tree given in Fig. 10.5.3(a) is considered for the expression $(p+q)\times(r-(s\div d))$. When inorder search is applied to this tree we get the string.

"$p+q\times r-s\div d$"

This is infix notation for algebraic expression.

10.5.2.3 Postorder Search

Postorder search of tree consists of following steps :

1) Search for left subtree $\left(T\left(v_L\right), v_L\right)$ if it exists.
2) Search for right subtree $\left(T\left(v_R\right), v_R\right)$ if it exists.
3) Visit the root v.

Exercise : Use postorder search and find all the subtree of tree T given in Fig. 10.5.2(a).

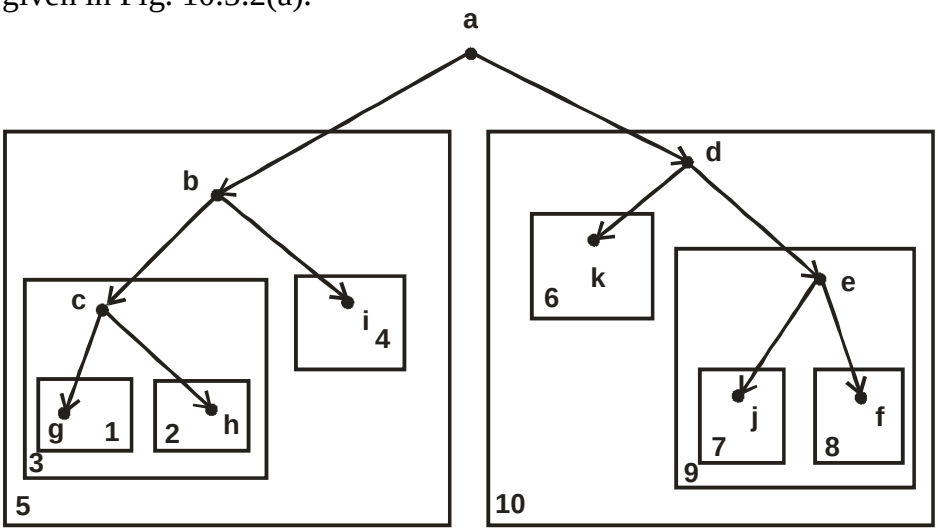


Fig. 10.5.5 Postorder Search

When we begin the search we see that subtree 3 and subtree 4 must be searched, before vertex 'c' is printed, if Fig. 10.5.2(b) is considered for post – order search.

Thus the order in which the vertices will be considered in the postorder search can be given by : "g h c i b k j f e d a".

10.5.2.3(a) Reverse polish form or postfix for algebraic expression

When postorder search is applied to tree of the expression $(p+q)\times(r-(s\div d))$ we get the string " $pq+rsd\div-x$ "

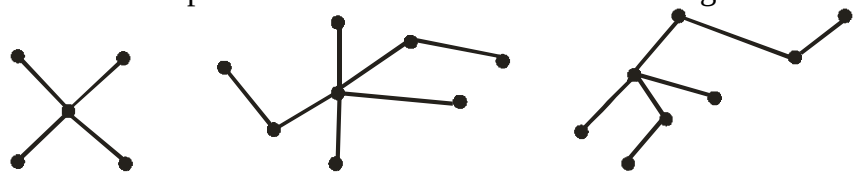
This is the <u>postfix</u> or <u>Reverse Polish</u> form of the algebraic expreesion.

<u>Note</u> that in a preorder search the order is root, left and right. For the inorder search the order is left, root, right while in postorder search the order is left, right, root.

10.6 DIRECTED AND UNDIRECTED TREES :

The trees with directed edges are of great importance in many applications such as electrical network analysis, game theory, theory of languages, computer programming and counting problems. One of the rooted tree with directed edges is called arborescence.

An undirected tree is simply a tree when all the edges are made bidirectional. We donot use arrows for the edges in undirected tree. Some examples of undirected trees is shown in Fig. 9.6.1.



(a) **(b)** **(c)**

Fig. 10.6.1 Undirected trees

Note that if T is an undirected tree then it is connected and acyclic. The converse also holds. Thus any connected and cyclic graph is a undirected tree. Some more properties of directed and undirected trees are discussed in section 10.2.

9.7 EXERCISES :

1) Draw a tree with vertex set V and edge set E. Also find root if exists.
   a) V = {a, b, c, d, e, f}; E = {(a, b), (c, e), (f, a), (f, c), (f, d)}
   b) V = {1, 2, 3, 4, 5, 6}; E = {(1, 2), (1, 3), (4, 5), (4, 6)}
2) List all the level – 3 vertices and all the leaves of Fig. 10.2.5(a) and 10.2.5(b).
3) Consider following Fig. 10.7.1.

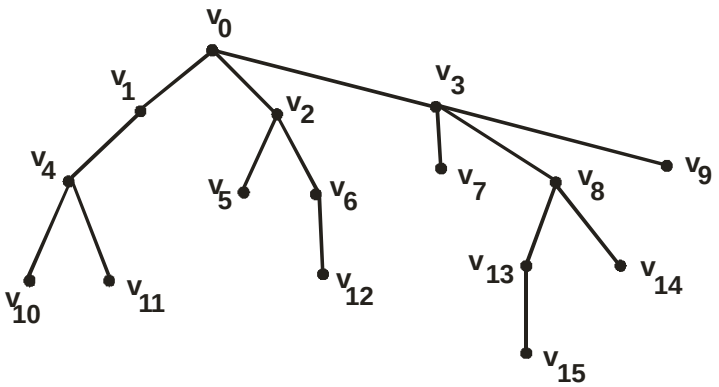


Fig. 10.7.1 $T(v_0)$

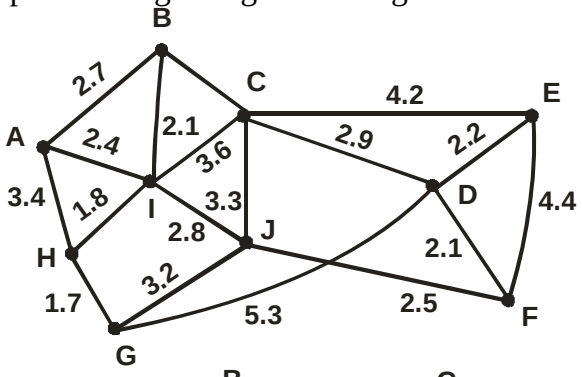
a) Find siblings of v_8.
b) Find descendants of v_8.
c) Compute tree $T(v_2)$ and $T(v_3)$.
d) What is height of $T(v_0)$ and $T(v_3)$?.
e) List all level – 4 vertices if exists.
f) List all leaves.

4) Construct tree for algebraic expression
   a) $17 + (6 - 2) - (x - (y - 4))$
   b) $3 - (x + (6 \times 4 \div (2 - 3)))$
   c) $(x \div y) \div ((x \times 3) - (z \div 4))$

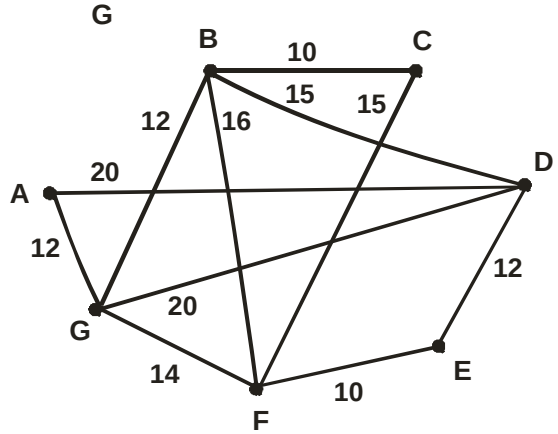
5) Make a 'family' tree that shows the descendants of one of your great grandfather.

6) How many distinct positional 3 – trees are there with height 2? Draw them.

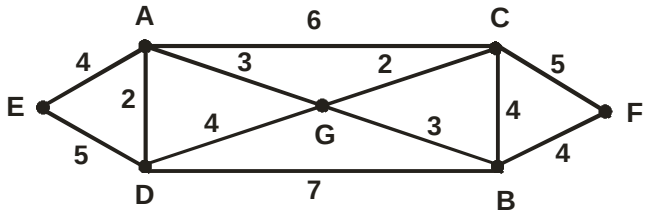
7) Use Prim's algorithm to find minimal spanning tree for following graphs and beginning at vertex given.

a) 

, at vertex F

b) 

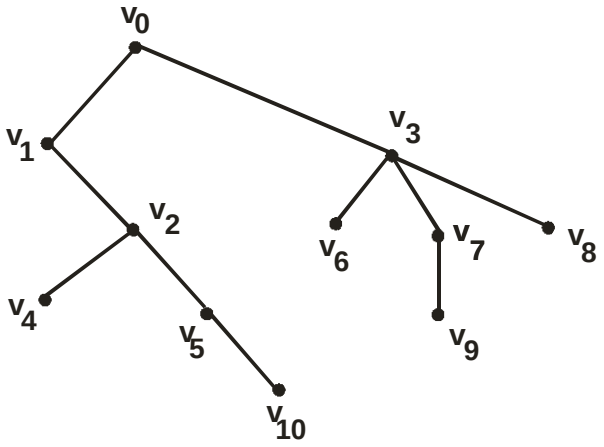
, at vertex G

c) 

, at vertex E.

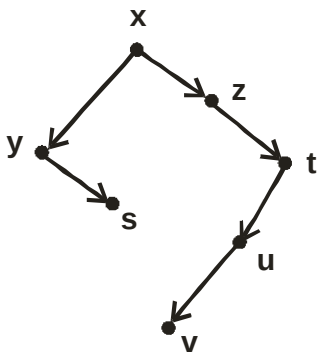
8) Use Krushkal's algorithm to find minimal spanning tree for the graphs given in Exercise 7.

9) Refer following tree and answer.

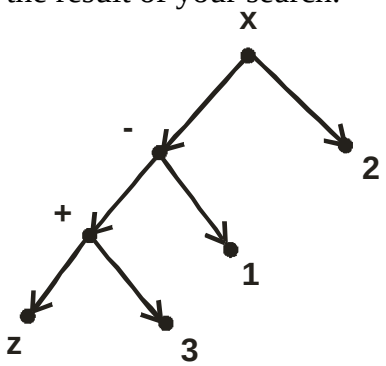


a) What is height of the tree?
b) List the leaves of T.
c) How many subtrees of T condition v_4?
d) List the siblings of v_7.

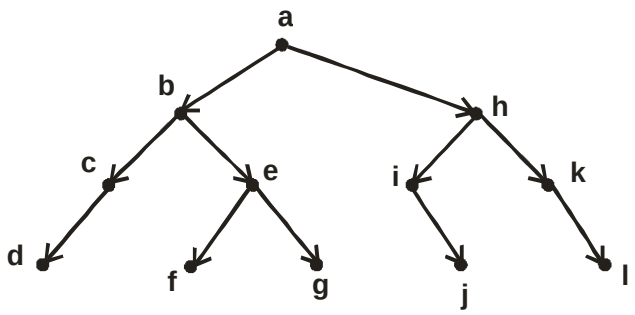
10) For the graphs given below perform
i) Preorder search
ii) Inorder search
iii) Post order search and write the result of your search.



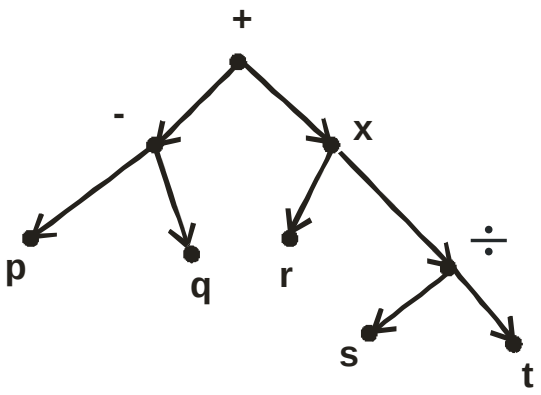
(a)



(b)



(c)



(d)

10.8 LET US SUM UP

In this chapter, we have learnt the structure of trees and its properties we have also seen different ways of searching trees in a graph. One can also find the spanning tree using the Prim's and Kruskal's algorithm. The trees are very useful models for different situations in computer science.

10.9 REFERENCES FOR FURTHER READING

1. Discrete Mathematical structures by Kolamn, Busby and Ross. Pearson education.
2. Introduction to graph theory by Douglas B. West.
3. Discrete Mathematics and its applications by Kenneth. H.Rosen. McGraw Hill edition.
4. Graph theory by Frank Harary. Narosa Publication.
5. Discrete Mathematics by Norman Priggs. Oxford.

11

SEMI-GROUPS AND GROUPS

Unit Structure :

11.0 OBJECTIVES

After going through this chapter students will be able to:

- about binary operations
- Algebraic structures like semi-groups and groups will be known
- Operations like product and quotient of these algebraic structure will be known

11.1 INTRODUCTION

Semi-groups and groups are mathematical structures. Semi-groups help in the study of finite state machines. While studying group structure we develop an understanding for coding theory. To study groups and semi-groups some knowledge of set theory and number system is required.

In this chapter we are going to discuss following topics.

- What are binary operations?
- The structure called semi-group, their products and quotients.
- The group structure and its product and quotient.

11.2 BINARY OPERATION

Binary operation is basic tool to study discrete mathematics. A collection of objects with operations defined on them and the properties associated with the operation together gives us a system which we call mathematical structure or system. An operation that combines two objects is a binary operation. Binary operation is a function with certain properties. A set with binary operation is a set in which an abstract product is defined such that the product of two elements of the set is again an element of the set.

11.2.1 Definition 1: A binary operation on set G is defined as a function $f : G \times G \to G$. If a and b $\in$ G then $f(a, b) \in G$.

Remark : A binary operation is a rule which assigns to each ordered pair of element of *G*, a unique element of *G*.

Notation : We use the symbol $a * b$ to denote *f* (a, b).

11.2.2 Examples of binary operation :

1. Let G = $\mathbb{Z}$ = The set of integers.
   Define $*$: G $\times$ G $\to$ G as $a * b = a + b$
   Since $a + b \in \mathbb{Z} = G$, $*$ is binary operation on $\mathbb{Z}$.

2. Let G = $\mathbb{R}$ = set of real numbers.
   Define $*$: $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$ as $a * b = a \div b$

Then $*$ is not binary operation, since it is not defined for every pair of elements of $\mathbb{R}$. For example; $3 \in \mathbb{R}$ and $0 \in \mathbb{R}$ but $3 \div 0$ is not defined.

3. Let G = $\mathbb{Z}^+$ = set of positive integers, where $*$ is defined as $a * b = a - b$.
$*$ is not binary operation since it is not defined for every pair of elements of $\mathbb{Z}^+$. For example; $2 \in \mathbb{Z}^+$, $3 \in \mathbb{Z}^+$ but $2 - 3 = -1 \notin \mathbb{Z}^+$.

4. Let G = $\mathbb{Z}$, be set of integers
   Define $*$: G $\times$ G $\to$ G as $a * b = a + b - ab$

Then $*$ is binary operation. Note that if G = $\mathbb{Z}^+$ = set of positive integers then $*$ defined above will not be binary operation as $2 \in \mathbb{Z}^+$, $3 \in \mathbb{Z}^+$ but $2 * 3 = 2 + 3 - 2.3 = 2 + 3 - 6 = -1 \notin \mathbb{Z}^+$.

5. Let M be set of all $n \times n$ Boolean matrices.

A Boolean matrix is $n \times n$ matrix whose entries are zero or one. Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be $n \times n$ Boolean matrices. Define $A \vee B$, the **join** of A and B, by $C = [c_{ij}]$ where

$$c_{ij} = \begin{cases} 1 & \text{if } a_{ij} = 1 \quad \text{or} \quad b_{ij} = 1 \\ 0 & \text{if } a_{ij} \text{ and } b_{ij} \text{ both are } 0 \end{cases}$$

Define $A \wedge B$, the **meet** of A and B by $D = [d_{ij}]$ where

$$d_{ij} = \begin{cases} 1 & \text{if } a_{ij} \text{ and } b_{ij} \text{ are both } 1 \\ 0 & \text{if } a_{ij} = 0 \quad \text{or} \quad b_{ij} = 0 \end{cases}$$

Let M be set of Boolean matrices. Let G = M. Define $*$ on M as follows : For A, B $\in$ M; $A * B = A \vee B$. The $*$ is a binary operation. If $*$ is defined as $A * B = A \wedge B$ then, again $*$ is binary operation.

11.2.3 Properties of binary operation :

1. **Definition 2:** A binary operation on a set G is said to be closed if $a * b \in G$ for all elements a and b in G. We say $*$ satisfies closure property.

Note : Whenever $*$ is binary operation, it always hold closure property and we say G is closed with respect to $*$.

2. **Definition 3:** A binary operation on set G is said to be commutative if $a * b = b * a$ for all a, b $\in$ G. We say $*$ satisfies commutative property.

3. **Definition 4:** A binary operation $*$ on a set G is said to be associative if $a * (b * c) = (a * b) * c$ for all a, b, c $\in$ G. We say $*$ satisfies associative property.

4. **Definition 5:** A binary operation $*$ on a set G is said to be idempotent if $a * a = a$ for all $a \in G$. We say $*$ satisfies idempotent property.

To summaries properties of binary operation we have following table where $*$ is binary operation on a set G and $*$ satisfies properties for a, b, c $\in$ G.

1. $a * b \in G$	Closure Property
2. $a * a = a$	Idempotent Property
3. $a * b = b * a$	Commutative Property
4. $a * (b * c) = (a * b) * c$	Associative Property

Table No. 11.1

Examples based on definition 2 to 5.

1. Let G = $\mathbb{Z}$ and a $*$ b = a + b, $\forall$ a, b $\in$ $\mathbb{Z}$, Then $*$ satisfies closure property as a $*$ b = a + b $\in$ $\mathbb{Z}$.
$*$ satisfies commutative property because a $*$ b = a + b while b $*$ a = b + a and a $*$ b = a + b = b + a = b $*$ a.

Also, $(a * b) * c = (a + b) * c$
$= (a + b) + c$
$= a + (b + c)$ $[\because$ *+ is associative in* $\mathbb{Z}]$
$= a + (b * c)$
$= a * (b * c)$

$\therefore$ * holds associative property. Now, 2 * 2 = 2 + 2 = 4 $\neq$ 2, hence * does not satisfy idempotent property.

2. Let L be a lattice. Define a $*$ b = $a \wedge b$ (greatest lower bound of a and b) Then $*$ satisfies all four properties.

$a * b = a \wedge b \in L$, $\therefore$ $*$ holds closure property
$a * a = a \wedge a = a$, $\therefore$ $*$ holds idempotent property
$a * b = a \wedge b = b \wedge a = b * a$ $\therefore$ $*$ holds commutative property

$(a * b) * c = (a \wedge b) \wedge c$
$= a \wedge (b \wedge c)$
$= a * (b * c)$, $\therefore$ $*$ holds associative property

3. Let $G = \mathbb{R}$ and * be defined as, $a * b = ab + 2b$

Then a $*$ b $\in \mathbb{R}$, hence $*$ holds closure property.
$a * a = a.a + 2a = a\,(a + 2) \neq a$, hence $*$ does not hold idempotent property.

$a * b = ab + 2b$ and
$b * a = ba + 2a$
Since $a * b \neq b * a$, $*$ is not commutative on $\mathbb{R}$.

$(a * b) * c$
$= (ab + 2b) * c$
$= (ab + 2b) \,.\, c + 2c$
$= abc + 2bc + 2c$ and

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

$= abc + 2ac + 2bc + 4c$

Thus, $(a * b) * c \neq a * (b * c)$ and hence $*$ is not associative on $\mathbb{R}$.

4. Consider the set G = {a, b, c, d} with binary operation $*$ defined by 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

i) $c * d = a$ and $d * c = a$

Thus, $c * d = d * c$

ii) $b * d = c$ and $d * b = b$

Thus, $b * d \neq d * b$

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

$= c$

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

$\therefore a * (b * c) \neq (a * b) * c$

From (ii), $*$ is not commutative.

and from (iii), $*$ is not associative.

Check your progress

1. Determine whether $*$ is binary operation. If it is determine whether $*$ is closed, idempotent, commutative and associate on given set.
   a) On $\mathbb{Z}$ where $a * b = 2a + b$
   b) On $\mathbb{R}^+$ where $a * b = a / b$
   c) On $\mathbb{Z}$ where $a * b = a - b$
   d) On lattice L where $a * b = a \vee b$
   (least upper bound of a and b)
2. Consider binary operation $*$ defined on set G = {a, b, c} given by following table.

$*$	a	b	c
a	b	c	b
b	a	b	c
c	c	a	b

   a) Is $*$ commutative?
   b) Compute $a * (b * c)$ and $(a * b) * c$
   c) Is $*$ associative?

11.3 SEMI-GROUPS

Definition 6 : Algebraic Structure

A nonempty set G with one or more binary operations is called an algebraic structure.

If $*$ is binary operation on G then (G, $*$) is an algebraic structure.

Examples of algebraic structure

1. The set $\mathbb{N}$: set of natural numbers is algebraic structure with respect to binary operation +. Thus we denote ($\mathbb{N}$, +) is an algebraic structure.
2. ($\mathbb{Z}$, +) : set of integers with binary operation + is an algebraic structure.
3. ($\mathbb{R}$, + , $\circ$) : set of real numbers with binary operations + and $\circ$, is an algebraic structure.

Definition 7: Semi-group :

An algebraic structure (G, $*$) is called a semi-group if the binary operation $*$ is associative in G. Thus, if a, b, c $\in$ G, then (a $*$ b) $*$ c = a $*$ (b $*$ c).

Definition 8: Commutative Semi-group :

The semi-group (G, $*$) is said to be commutative if $*$ is commutative.

Examples of Semi-group :

1. ($\mathbb{N}$, +) : Set of natural numbers with respect to binary operation + is semi group as + satisfies associative property i.e. $\forall$ a, b, c $\in$ $\mathbb{N}$, (a + b) + c = a + (b + c)

2. ($\mathbb{Z}$, +) : set of integers with binary operation + is commutative semi-group because + is associative and commutative in $\mathbb{Z}$.

Definition 9: Identity element:

An element e in a semi group (G, $*$) is called the identity element if e $*$ a = a $*$ e = a $\forall$ a $\in$ G. (read $\forall$ as 'for all')

Note that identity element is unique. Otherwise if it is not unique then there exist another identity element i such that i $*$ a = a $*$ i = a.

Thus if a = e then; i $*$ e = e $*$ i = e (1)
Also, if a = i then; e $*$ i = i $*$ e = i (2)

From (1) and (2) we get e = i. Thus, identity element if it exists is unique.

Definition 10: Monoid

A monoid is a semigroup $(G, *)$ that has an identity element.

Examples of Monoid

1. $(\mathbb{Z}, +)$: Set of integers with binary operation + is monoid. Here; 0 is identity element as $0 + a = a + 0 = a \ \forall\ a \in \mathbb{Z}$.

2. Let S be fixed non empty set and let S^S be set of all functions $f : S \to S$. If f and g are elements of S^S, define $f * g = f \circ g$, the composite function. Then $(S^S, *)$ is a semigroup which is not commutative and is a monoid since S^S has identity element 1_S, i.e. $\forall\ f \in S^S;\ 1_S * f = f * 1_S = f$

Definition 11: Sub semi-group

Let $(G, *)$ be a semi-group. Let H be subset of G. If H is closed under binary operation $*$ then $(H, *)$ is called sub-semi-group of $(G, *)$

Definition 12: Sub monoid

Let $(G, *)$ be a monoid with identity element e. If H be nonempty subset of G. If H is closed under binary operation $*$ and $e \in H$, then $(H, *)$ is called submonoid.

Note : 1) Subsemigroup of a semigroup is itself a semigroup.
2) Submonoid of a monoid is itself a monoid.

Examples of submonoid

1. If $(G, *)$ is a semigroup, then $(G, *)$ is subsemigroup of $(G, *)$. Similarly if $(G, *)$ is a monoid then $(G, *)$ is submonoid of $(G, *)$. If $T = \{e\}$ then $(T, *)$ is also a submonoid of monoid $(G,*)$.
2. Let H be set of all even integers then (H, X) is a sub semigroup of $(\mathbb{Z}, X)$ where 'x' is binary operation multiplication. But (H, X) is not a submonoid of $(\mathbb{Z}, X)$ because 1 is identity element of $\mathbb{Z}$ which does not belong to H.

Group Theory

A group is formally defined as below. We denote the binary operation as **"0" or "*"** until or otherwise specified.

Definition: Let G be a non-empty set and 0 be a binary operation on G. We say that (G, 0) is a group if the following **four properties** are satisfied.

1. G. is **closed** with respect to '*' i.e .,for all a , b in G the element a * b is a uniquely defined element of G
2. G. is **associative** with respect to '*'
   i.e., for all a , b , c in G a * (b*c) = (a*b) *c
3. **Identity** element **exists** in G for '*'
   i.e., if there exists 'e' such that a * e = e * a = a $\forall$ a in G.
4. **Inverse exists** for **each element** in G with respect to '0'
   i.e., for each a in G there exists an element a^{-1} in G such that $a * a^{-1} = a^{-1} * a = e$ (where e is identity element of G)

Example 1: Set of all non-zero rational numbers from a group under ordinary multiplication.

Solution: Let Q* is the set of all non-zero rational numbers.

Closure law: Let a , b ∈ Q*
a . b also belongs to Q* (Product of two rational numbers is a ational number)

Q* is closed with respect to multiplication.
Q* satisfies fist condition of a group

Associative law: Let $a,b,c \in Q^*$ let $a = \frac{u}{x}, b = \frac{v}{y}$ and $c = \frac{w}{3}$

Consider $a \cdot b = \frac{u}{x} \cdot \frac{v}{y} = \frac{uv}{xy}; (a.b).c = \left(\frac{uv}{xy}\right) \cdot \frac{w}{z} = \frac{(uv)w}{(xy)z} = \frac{u(vw)w}{x(yz)}$

(∴ (uv)w = u(vw) and (xy)z = x(yz) where u,v,w,x,y,z ∈ Z and satisfies associative law)

$$= \frac{u}{x} \cdot \left(\frac{v}{y} \cdot \frac{w}{z}\right)$$

$$= a(b.c)$$

From the above example it is clear that (a . b) . c = a .(b.c) and it si true ∀a , b , c∈Q*

Q* is associative with respect to multiplication.

Existence of Identity: since 1 is a rationa1 number 1 ∈Q*
Let a ∈Q*
We have a.1 = a = 1.a
So 1 is the identity element of Q* which exists in Q*

Existence of Inverse: To prove existence of inverse, let $a = \frac{p}{q}$ be an element Q* There exists $\frac{q}{p} \in Q^*$ such that $\frac{p}{q} \cdot \frac{q}{p} = 1$

That shows $\frac{q}{p}$ is the inverse of $\frac{p}{q}$ and it is true for all a $\in$Q*
Hence inverse exists for such element of Q* and inverse of a denoted by 1/a or a^{-1}.

Q* satisfies all four properties of a group, Q* is a group under multiplication (Q*, .) is a group

Properties of a Group :

Abelian Group: In addition to the above mentioned four properties of a group if it also satisfies another property called commutative property , i.e.,a*b = b*a $\forall$ a , b $\in$ G

The group is calles either **Abelian group or commutative group**. A group which is not abelian is calles as non-abelian group

Example 3: C = { a + ib / a,b $\in$**R**} C is an abelian group with two addition.

Addition is defined on C as $(a_1 + i\, b_1) + (a_2 + i\, b_2) = (a_1 + a_2) + (b_1 + b_2)$

Commutative Property
Let x , y $\in$*C* where $x = a_1 + i\, b_1$ and $y = a_2 + i\, b_2$, a_1 , a_2 , b_1 , $b_2 \in$R

$X + y = (a_1 + i\, b_1) + (a_2 + i\, b_2)$
$= (a_1 + a_2) + i(b_1 + b_2)$

Since addition two real number satisfies the commutative law.

$a_1 + a_2 = a_2 + a_1$ and $b_1 + b_2 = b_2 + b_1$
$= (a_2 + a_1) + i(b_2 + b_1)$
$= (a_2 + i\, b_2) + (a_1 + i\, b_1)$
$= y + z$

C satisfies the commutative law with respect to **addition.**
(*C* , +) is an abelian group or (*C* , +) is a **commutative group.**
Set of complex number also forms an **abelian group** with respect to **multiplication.**
(Leftas an exercise)

Commutative Law : $a,b \in Q \;\; a*b = \frac{ab}{5} = \frac{ba}{5} = b*A\left(\because ab = ba\right)$

Hance Q_+ is an abelian group with respect to *.

Example 4: G = {1, -1} is an abelian group under multiplication.

.	1	-1
1	1	-1
-1	-1	1

From the above table, it is clear that (G , .) satisfies both closure, associative property ,and abelian property with 1 being identity and -1 is its own inverse

Addition modulo "m"

We shall now define a new type of addition called "addition modulo "and is denoted by $a +_m b$ where a and b are integers and 'm' is a fixed positive integers.

By definition , $a +_m b = r \; 0 \leq r < m$ where r is the least non-negative remainder when a + b is devided by m and we read itas a addition modulo m b.

Example 5: If a = 7; b = 8 then add 7 and 8 gives 15 divide by 2 the remainder is 1.

$7 +_2 8 = 1$

If a = 5 and b = 6 add 5 and 6 gives 11 divide by 3 we get the remainder is 2.

$5 +_3 6 = 2$

Note: If a and b are two integers such that a-b divisible by fixed positive integer 'm' we write a = b (mod m) and we read it as "a is congruent to b modulo m"

Note: It can be easily seen that $a +_m b = b +_m c$ (take any example and try it in your own)

Example 6: prove that the set G = { 0, 1, 2, 3, 4, 5} is a finite abelian group of group of order '6' with respect to addition modulo '6'.

From the composition table as shown below

$+_6$	0	1	2	3	4	5
0	$0+_6 0=0$	$0+_6 1=1$	$0+_6 2=2$	$0+_6 3=3$	$0+_6 4=4$	$0+_6 5=5$
1	$1+_6 0=1$	$1+_6 1=2$	$1+_6 2=3$	$1+_6 3=4$	$1+_6 4=5$	$1+_6 5=0$
2	$2+_6 0=2$	$2+_6 1=3$	$2+_6 2=4$	$2+_6 3=5$	$2+_6 4=0$	$2+_6 5=1$
3	$3+_6 0=3$	$3+_6 1=4$	$3+_6 2=5$	$3+_6 3=0$	$3+_6 4=1$	$3+_6 5=2$
4	$4+_6 0=4$	$4+_6 1=5$	$4+_6 2=0$	$4+_6 3=1$	$4+_6 4=2$	$4+_6 5=3$
5	$5+_6 0=5$	$5+_6 1=0$	$5+_6 2=1$	$5+_6 3=2$	$5+_6 4=3$	$5+_6 5=4$

From the above table we see that all entries in the composite table are the element of G.

That shows G is closed under addition modulo 6.("+6".)
To prove G is associative, let a = 2 b = 4 c=1
Consider $2+_6 (4+_6 1) = 2+_6 5 = 1$
$(2+_6 4) +_6 1 = 0+_6 1 = 1$
$2+_6 (4+_6 1) = (2+_6 4) +_6 1$ and it is true $\forall$ a , b , c $\in$G
G is associative under addition modulo 6 ('$+_6$".)

Existence of identity : let a $\in$ G $a +_6 0 = 0+_6 a = a \ \forall$ a $\in$G.
0 is the identity element in G.

Existence of inverse: from the above table,

$0+_6 0=0$
$1+_6 5=0$
$2+_6 4=0$
$3+_6 3=0$
$4+_6 2=0$
$5+_6 1=0$

Inverse of 0 is 0 , inverse of 1 is 5 , inverse of 2 is 4 , inverse of 3 is 3 , inverse of 4 is 2 , inverse of 5 is 1 => inverse exists for each element of G and belongs to G

=> G is a group with respect to the binary operation $+_6$.
Commutative Law : $a +_6 b = b +_6 a \ \forall$ a, b $\in$ G.
If a = 2 b = 4 $2+_6 4 = 0 = 4+_6 2$.
(G, $+_6$) is an abelian group)

Note: The set of first m non-negative forms an abelian hroup with respect to addition modulo 'm'

Finite and identity Group: If the set G contains a finite number of element then the group then the group (G, *) is called a finite group. Otherwise the group (G, *) is called as *Infinite* group

Order of a group: Another natural characteristic of a group G is the number of element it contains. We call it as order of a group and is denoted by O(G).

Example 10: Let G = {1, -1} is a group
Then *O*(G) = 2**.**

If G is a group containing the set of all integers or set of all natural numbers, then ***O***(G) is infinite.

Order of an element of a group: If G is a group and a ∈ G. The order of a is the least positive integer m such that $a^m = e$.

So, to find the order of a group element compute a,a^2,a^3,.. until you reach the identity for the first time. See the following example.

In the group { 1 , -1 , I , -i} 1 is identity element i^1 =I , i^2 = -1 , i^3 = -I , i^4 = 1 , i^5 =I , i^6 = -1 , i^7 = -I , i^8 = 1. Identity appeared twice at i^4 and i^8 , but o (i) = 4 (∴ it is the least)

If such integer does not exists we say that the order of a is infinity. We use the notation ***O*** (a) for the order of a.

Co-prime

Two number are said to be co prime if they do not have any common factory except '1'. If a are co primes then there exists two integers x , y such that xa + by = 1.

Example:-7.

On a group G, O (a) = 18, State that the orders of a^6, a^{15}, a^{-7}.

Solution:- $O(a) = n$

$$O\left(a^k\right) = \frac{n}{(n,k)}$$

1) O (a) = 18

$$O\left(a^6\right) = \frac{18}{(18,6)} = \frac{18}{6} = 3$$

2) O (a) = 18

$$O\left(a^{15}\right)=\frac{18}{(18,15)}=\frac{18}{2}=6$$

3) O (a) = 18

$$O\left(a^{-7}\right)=\frac{18}{(18,7)}$$

Now $O\left(a^{-7}\right)$

$O\left(a^{-7}\right)=O\left(a^{7}\right)$ O (a^{-7}) = O (a^{7}) (the order of element of group is same as its inverse)

$$O\left(a^{-7}\right)=\frac{18}{(18,7)}=18.$$

Example 11: Find the order of such element of the group G = {1, 2, 4, 7, 8, 11, 13, 14} the composition being multiplication modulo 15.

Solution: Identity element of G = 1:***O*** (1) =1

To Find the order of 2,$2x_{15}2x_{15}2 = 4x_{15}2=8$

$2x_{15}2x_{15}2 = 4x_{15}2=8$

$2x_{15}2x_{15}2x_{15}2 = 8x_{15}2=$**1(identity)**

Hence ***O***(2) = 4

To Find the order of 4,$4x_{15}4$ =1(identity)

Hence ***O***(4) = 2

To Find the order of 7,$7x_{15}7 = 4$

$7x_{15}7x_{15}7 = 13$

$7x_{15}7x_{15}7x_{15}7 = 13x_{15}7 =$ **1(identity)**

Similarly, we can compute the order of 8,11,13,14.

Sub Group :

Sub Group: In general we are not interested in a subset of a group G. but certain subset of elements in a group is itself a group. This situation arises so often that we introduce a special name to describe it, called sub group. See the following definition for a subgroup.

Definition: A non-empty subset H of a group G is said to be a subgroup of G if H itself is a group, with respect to the same binary operation defined on G.

Every subgroup of G is a complex of G every complex is not always a subgroup.

Example 12: Q*under multiplication is a proper subgroup of R* under multiplication.

Example 13: Additive group of even integer is a subgroup of the additive group of all integers.

Two-Step Subgroup Test:

Theorem: A non-empty subset of H of a group G is a subgroup of G if and only if

i. a,b ∈H implies ab ∈H
ii. a ∈H implies that a^{-1} ∈ H

Theorem: A non-empty subset of H of a group G is a subgroup of G if and only if a , b ∈H => ab^{-1} ∈H.

One-Step Subgroup Test

Example 14 : See the example to under stand one-step subgroup Test.

G be the group of non-zero complex numbers under multiplication.

H = {a+ib/a^2+b^2 = 1,a∈R b∈R} is a sub group of G.

Let x , y ∈H where x = a + ib and y = c + id

Inverse of $y = \frac{1}{C+id} = \frac{C-id}{C^2+d^2}$

we have $xy^{-1} = (a + ib) \frac{C-id}{C^2+d^2} = ac+bd +i(bc-ad)/c^2 + d^2$

real part of $xy^{-1} = \frac{ac-id}{C^2+d^2}$

imaginary part of $xy^{-1} = \frac{bc-ad}{C^2+d^2}$

consider $\left(\frac{ac+bd}{C^2+d^2}\right)_2 + \left(\frac{bc-ad}{C^2+d^2}\right)_2$

$$= \frac{a^2c^2+b^2d^2+2abcd+b^2c^2+a^2d^2-2abcd}{\left(c^2+d^2\right)}$$

$$= \frac{\left(a^2+b^2\right)\left(c^2+d^2\right)}{\left(c^2+d^2\right)} = \frac{1.1}{1} = 1$$

Xy^{-1} ∈H , hence H is a subgroup of G.

Example 15: Let Z be the group of all integers

Let H_1 = {…..-6,-4,-2, 0, 2, 4, 6…}
H_2 = {…..-12,-9,-6,-3, 0, 3, 6, 9, 12…} be two subgroups of Z.

$H_1 \cup H_2$ = { -12, -9, -6, -4, -3, -2, 0, 2, 3, 4, 6, 9,…}
Since -2 $\in H_1 \cup H_2$, -3 $\in H_1 \cup H_2$ but -2 + -3 $\notin H_1 \cup H_2$
$H_1 \cup H_2$, is not closed under '+'.
$\therefore$ $H_1 \cup H_2$, is not subgroup of (Z, +).

Example 16 : G = {1, -1} is a group
H = {-1} is a subset of G.
H^{-1} = {-1}
$H = H^{-1}$ but H is not a group since identity does not exists.
$\therefore$ H is not a subgroup of G.

Check your progress

1. Show that AB is a sub-group of G if and only if AB = BA.
2. When does the semi-group form a group?
3. Prove that the set {0, 1, 2, 3, 4, 5} is a finite abelian group of order 6 with respect to addition modulo 6.
4. Show that the set $G = \{a + b\sqrt{2} : a, b \in Q\}$ is a group with respect to addition.

11.7 LET US SUM UP

In this chapter we have learnt the details of algebraic structures semi-group and groups. The examples of semi-group and group are varying because of the properties related to the structure. The study of semi-groups and groups will make the study of finite state machines and coding theory simpler.

11.8 UNIT END EXERCISE

Q.1 Show that the set of all positive rational numbers forms an abelian group under the composition defined by $a * b = \frac{ab}{2}$.

Q.2 Show that set IN of all natural numbers is not a group with respect addition.

Q.3 Find the order of the elements of the group $(z_4, + 4)$.

Q.4 Find the order of the elements of the group ({1, w, w^2}, .). Where w isa cube root of 1.

Q.5 Prove that the fourth roots of unity form an abelian group under multiplication.

Q.6 Prove that the set {0, 1, 2, 3, 4} is a finite Abelian group of order 5 under addition modulo 5 as composition.

Q.7 Check whether (Z, -) is semi-group or not. Where "-" denotes integer subtraction.

Q.8 Check whether (Z, +) and (Z, .) are monoids or not.

Q.9 Show that the set of matrices $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$, where $\alpha \in IR$, forms a group under matrix multiplication.

Q.10 Show that the integer multiples of 5 form a sub-group of the additive group of integers.

11.9 REFERENCES FOR FURTHER READING

1. University Algebra by N.S. Gopalkrishnan.

2. Contemptary Algebra by Gallian.

3. Discrete mathematics by Kenneth and Rosen.

4. Discrete mathematical structures by Kolman, Busby and Ross.

5. Modern Algebra by Vasishtha.

12

NORMAL SUBGROUP

Unit Structure

12.0 OBJECTIVES :

After going through this chapter students will be able to know:

- Operations like product and quotient of these algebraic structures.
- Isomorphism, Homomorphism and Automorphism group.
- Generators of Cyclic group.
- Normal sub-group.
- Coding and Encoding of group.

12.1 INTRODUCTION :

After having all the basic property of group and sub-group, we now begin our journey with more detail about group study. In this we are going to discuss about product of group and quotients group, isomorphic group, homomorphic group, automorphic group. In group theory cyclic group are the simplest group also it is very interesting. In previous chapter we learn about sub-group, now here we discuss about cosets and normal sub-group.

12.2 PRODUCT AND QUOTIENTS OF GROUPS :

12.6.1 **Definition :** If G_1 and G_2 are groups then the product of G_1 and G_2 denoted as $G_1 \times G_2$ is a group with binary operation defined by $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$

Examples 1: Let $G_1 = G_2 = \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$, $\bar{0}$ is notation for [0] find $G_1 \times G_2$.

Solution: $G = G_1 \times G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$

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

Composition table for $\mathbb{Z}_2 \times \mathbb{Z}_2$ is

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

Note that in $(\mathbb{Z}_2, +)$, $\bar{1} + \bar{1} = \bar{2} = \bar{0}$. G is group of order four.

12.3 HOMOMORPHISM

Group of Homomorphism: Till now we have seen the notion of a group and various type of group. Now we see the relation between two groups by introducing "Homomorphism". A relation between groups G and G, is generally exhibited in terms of a structure relating map from G to G_1.

Let G and G_1, be two groups. We are interested in a map that relates the group structure of G to the group structure of G_1, and this map often gives us information about the structure of G_1 from known structural properties of G, or information about the structure of G from known structural properties of G_1

We known that the group structure is determined by its binary operation. We now define such a structure relating map for groups, and then point out how the binary operations of G and G_1 are related by such a map.

Definition: Let G and G_1 be groups. A map $f : G \rightarrow G_1$ is said to be Homomorphism

If $f(ab) = f(a)\, f(b)$ for all $a , b \in G$.

Note: If the operation in G is denoted by '*' and the operation in G_1 is '.' The above condition for Homomorphism means the following.
$f(aob) = f(a) . f(b)$.

12.3.1 Properties of Homomorphism

Let G and G_1 be two groups. e and e_1 be the identity element of G and G_1 respectively. If f is Homomorphism from G to G_1 then $f(e) = e_1$

Range of Homomorphism: G and G_1 are two groups and f is homomorphism from G to G_1. The set of all f images of G in G_1 is called range of homomorphism.
It can be written as $f(G) = \{ f(a) / a \in G\}$

12.3.2 Types of Homomorphism

Onto Homomorphism: Let G and G_1 be two groups and f is a mapping from G onto G_1.
If $f(ab) = f(a)\, f(b)$ $\forall$ a, b $\in$ G then f is said to be a **Homomorphism from G onto G_1.**
In some books it is referred as **epimorphism**.

Endomorphism: A homomorphism of a group into itself is called an endomorphism.

Monomorphism: If the homomorphism is one-one it is called monomorphism.

Example 2: Let G be the additive of integers and G_1 be the multiplicative group. Show that $f : G \rightarrow G_1$
a function defined as $f(m) = e^m$ is a homomorphism

Solution: Let $m , n \in G$; $f(m) = e^m \in G_1$ and $f(n) = e^n \in G_1$
m+n $\in$ G (G is additive group)
$f(m+n) = e^{m+n} = e^m e^n = f(m) f(n)$
f is homomorphism from G to G_1.

12.4 ISOMORPHISM

Isomorphism: A function f from G to G_1. Is said to be isomorphism, if
1. $f : G \rightarrow G_1$ is one-one
2 . f: $G \rightarrow G_1$ is onto

3. $f: G \to G_1$ is homomorphism.
Says distinct element in G have distinct f - images in G_1
Says $\forall X \in G_1 \exists a \in G$ such that $f(a) = x$.
Says image of the product is same as product of images.

Note: in the above definition, we have denoted the operation as multiplication. We can use different symbols to denote the compositions.

Note: There may exists more than one isomorphism from G onto G_1.

Example 3: Let G be the multiplication group of all positive real numbers, and G_1 be the additive group of all real numbers. The mapping defined by $f : G \to G_1$ such that $f(x) = \log x$ .is isomorphism from G to G_1

Solution: : $G \to G_1 = \log x$

To prove f is one – one

Let $x_1, x_2 \in$ and $f(x_1) = f(x_2)$

$\Rightarrow \text{Log } x_1 = \log x_2$

$\Rightarrow e^{\log x_1} = e^{\log x_2}$

$\Rightarrow x_1 = x_2$

$\Rightarrow f$ is one – one from G to G_1

To prove f is on-to

For any real number $y \in G_1$ e^y is a positive real number such that $e^y \in G$

$f(e^y) = \log e^y = y \in G_1$

$\therefore$ Each element of G_1 is the f - image of some element in G.

i.e. f is on-to.

To prove f as homomorphism.

Consider $x,y \in G$ where $f(x) = \log x : f(y) = \log y$

Then $f(xy) = \log(xy)$

$= \log(x) + \log(y)$

$= f(x) + f(y)$

f is homomorphism from G to G_1

$\therefore$ f is isomomorphism from G to G_1

Example 4: There exists isomomorphism from an additive group of integers.
G = {….,-3, -2, -1, 0, 1, 2, 3…} to another additive group
G_1 = {….,-3m, -2m, -m, m, 1m, 2m, 3m…} where m is any fixed integers not equal to zero.
Solution: Define mapping $f : G \to G_1$ such that $f(x) = mx$
To prove f is one- one : let $x_1, x_2 \in G$ and $f(x_1) = f(x_2)$
$mx_1 = mx_2$ (from the definition of f)
$x_1 = x_2$
f is one – one from G to G_1
To prove f is onto: for any element $y \in G_1$ $\exists$ $y/m \in G$ such that $f(y/m) = m(y/m) = y \in G_1$
$\Rightarrow$ each element of G_1 is the f - image of some element in G.
i.e., f os on-to.
To prove f as n=homomorphism.
Consider x,y $\in$ G where $f(x) = mx$: $f(y) = my$
$f(x + y) = m(x+y)$
$= mx + my$
$= f(x) + f(y)$
f is homomorphism
$\therefore$ f Is isomorphism from G to G_1

12.5 AUTOMORPHISM OF A GROUP

Definition: If $f : G \to G$ is an isomorphism from a group G to itself, then f is called an automorphism of G.

Example 5: If G is an additive group of complex number, show that $f : G \to G$ such that f(Z) = pZ where p is a non-zero complex number, an automorphism of G.

Solution: G is an automorphism if $f : G \to G$ is an isomorphism.
To prove f is one-one.
Let $Z_1, Z_2 \in G$ and $f(Z_1) = f(Z_2)$
$PZ_1 = pZ_2$
$Z_1 = Z_2$
f is one-one.
To prove f is onto.
For any element $Z \in G$ there exists $Z/p \in G$ such that $f(Z/p) = p.(Z/p) = Z$.
Each element of G is the f- image of some element in G.
There fore f is onto.
To prove f is homomorphism.

Consider $f(Z_1 + Z_2) = p(Z_1 + Z_2) = pZ_1 + pZ_2 = f(Z_1) + f(Z_2)$
f is an homomorphism.
There fore f is isomorphism from G to G.
Hence $f : G \to G$ is an automorphism.

12.6 CYCLIC GROUP

Cyclic group: In the group theory, cyclic group are the simplest are the simplest among all group all groups. Because of this cyclic groups possess interesting properties. With the help of cyclic group we can find answer for some of the difficult questions in group theory. Now let us see what do we mean by a cyclic group?
The formal definition of a cyclic group is given below.

Definition: A group G is called *cyclic if for some* a ∈ G, every element x ∈ G is of the from such that a^n
Where n is some integer. The element 'a' is called a generator of G.
A cyclic group G generated by a can be represented as G = <a>
If G is a group with respect to the binary operation addition, cyclic group is defined as G = { na / n ∈ Z}

Example 6: G = {1, -1} is a cyclic group generated by -1 (∴ $1 = (-1)^{2,}$ $-1 = (-1)^1$)

12.6.1 Cyclic Subgroup: *A subgroup H of a group G is called a* ***cyclic subgroup*** *if H is a cyclic group.*

Note: If a is a generator of a cyclic group G then a^{-1} is also a generator

Let G be a cyclic group generated by a.

Then for every x ∈G there exists an integer, such that $x = a^m$

$= (a^{-1})^{-m}$

∴ Every x can be expressed as integral power of a^{-1}

i.e.,a^{-1} is also a generator of G.

12.7 COSETS

Definition: If G is a Group and H is a subgroup of G. let a ∈ G Then

Ha = {ha : h∈H} is called right coset of H in G generated by a.

And the set aH = {ah: h ∈ H} is called left coset of H in G generated of a.

Example 7: Let G = { a, b, c, d, e, f} is a group. And H = { b, c, e} be the subgroup of G.

Solution: a ∈ G : Ha = { ba, ca , ea}

d ∈ G : Hd = { bd, cd , ed} are some right coset of H in G.

c ∈ G : Hc = { bc, cc , ec}

The set aH = { ah : h ∈ H} is called left coset of H in G generated by a.

a ∈ G : aH = { ab, ac , ae}

d ∈ G : Hd = { db, dc , de} are some right coset of H in G.

c ∈ G : Hc = { cb, cc , ce}

Note: If G is an abelian group then **aH = Ha**

Example 8: Let G be the additive group of integers, and H is a subset of group of G where element of H are obtained by multiplying each element of G by 2.

Solution:
Clearly (H, +) is a subgroup of (G, +).

Now G = {…..-3,-2,-1, 0, 1, 2, 3…}

H = {…..-6,-4,-2, 0, 2, 4, 6…}

1 ∈ G and 1 + H = {…..-5,-3,-1, 1, 3, 5, 7…}

Example 9: Let G= <a> a cyclic group of order 15. List all the cosets of $<a^5>$ in G.

Solution: Let G = <a> a cyclic group of order 15.

i.e. G = {e, a, a_1, a_2, ……., a_{14}}

H is a subgroup of G.

H = {e, a^5, a^{10}}

The left cosets of $<a^5>$ are

aH = {a, a^6 , a^{11}}, a^2H = {a^2, a^7, a^{12}}, a^3 H = {a^3, a^8,a^{13}},

a^4 H = {a^4,a^9,a^{14}} .

Remark: A coset may not essentially a subgroup

Remark: If e is the identity in G, it is also identity in H. Then eH = {eh/h ∈ H} = H

12.7.1 Normal Subgroup

If G is a group and H is a subgroup of G, it is not always true that aH = Ha for all a in G. If it happens i.e.,if Ha = aH $\forall$ a in G we call H as normal subgroup. And it is denoted by H $\trianglelefteq$ G.

Definition: If G is a group and H is a subgroup of G.If Hx = xH $\forall$ x$\in$G then H is called a normal subgroup.

Note: Every normal subgroup but every subgroup need not be a normal subgroup.

Importer and proper normal subgroups: G is a group then G , {e} are subgroup of G and they are also normal subgroups of G. These two subgroups are called trivial or importer subgroups of "G"

The normal subgroup of G other than these two subgroups are called proper normal subgroups of G.

For example H = {1,-1} is a normal subgroup of multiplicative group of none zero real numbers.

Example :- Show that every subgroup of an Abelian group is normal.

Solution :- Let G be an abelian and H a subgroup of G. Let x be any element of G and H any element of H.

So, $xhx^{-1} = xx^{-1}$

$=h$ […G is Abelian $\Rightarrow x^{-1}h = hx^{-1}$]

$=eh$

$\Rightarrow h \in H$.

Hence $x \in G$,

$\Rightarrow h \in H$

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

So H is normal in G.

Example :- Given that H = { I, (12)(13) (34)} is a subgroup of A_4. Show that (243)H = (142)H and (132)H = (234)H but (234)(132)H $\neq$ (142)(234)H. Is H a normal subgroup of Ah? Justify your answer.

Solution :- H = { I, (12)(34)} is a subgroup of Ah.

A_4 = { I, (12)(34)(13)(24)(23)(14)(123)(132)(142)(124)}

To show that (243)H = (142)H

(243)(12)(34) = (142)

(243)H = {(243)(142)}

(142)H = i.e. (142)I and (142)(12)(34)

(142)H = {(142)(243)}
….. (243)H = (142)H
To show that (132)H = (234)H
(132)H = (132)I
(132)(12)(34) = {(132), (234)}
(234I = (234)
(234)(12)(34) = (132)
(234)H = {(234)(132)}
…. (132)H = (234)H
To show that (234)(134)H ≠ (142)(234)H
(234)(132)H = (234)(132)
(234)(132)(12)(34) = I
(142)(243)(12)(34) = (124)
Thus (243)(132)H ≠ (142)(243)H
…GH = HG
… H is normal subgroup A_4.

12.8 CODE AND GROUP CODE

Word : A sequence of 0's and 1's is called a word.
e.g. 1101, 101, 00100 are words.

Code : A collection of words used to represent different messages is called code.

Codeword : A word in a code is called codeword.

Block of code : A code consisting of words having same length is called block of code.

Let B = {0, 1} then $B \times B = \{00, 01, 10, 11\} = B^2$ i.e. B^2 contains words of length 2, and it contains 4 elements or codes. Number of elements in the set is called cardinality of the set and it is denoted by two vertical bar.

$\therefore$ Number of elements in set $B^2 = |B^2| = 4$. Also |B| = 2.

$\therefore |B^2| = |B \times B| = |B| \times |B| = 2 \times 2 = 2^2$

$\therefore |B^2| = 2^2 = 4$

Similarly

$B^3 = B \times B \times B$ = {000, 001, 010, 011, 100, 101, 110, 111},

$|B^3| = |B \times B \times B| = |B| \times |B| \times |B| = 2 \times 2 \times 2 = 2^3 = 8$

$\therefore$ The set B^m is collection of codes of length m and it contains 2^m codes.

$\therefore$ $|B^m| = 2^m$

Weight : Let $x \in B^n$ then weight of x is number of 1's in x and it is denoted by w(x).

e.g. i) x = 1101 $\in B^4$ $\therefore$ w(x) = 3
ii) x = 110010 $\in B^6$ $\therefore$ w(x) = 3
iii) x = 11 $\in B^2$ $\therefore$ w(x) = 2
iv) x = 0000 $\in B^4$ $\therefore$ w(x) = 0

$x \oplus y$: (Read as x ring sum y). Let x, y $\in B^n$, then $x \oplus y$ is a sequence of length n that has 1's in those position x and y differ and 0's in those positions x and y are the same.

i.e. The operation + is defined as

0 + 0 = 0 0 + 1 = 1
1 + 1 = 0 1 + 0 = 1

e.g.

i) $x, y \in B^3$, x = 101, y = 110

x =	1	0	1
y =	1	1	0
$x \oplus y$ =	0	1	1

$\therefore$ $x \oplus y$ = 011 and $w(x \oplus y) = 2$

ii) $x, y \in B^6$, x = 110100, y = 111111

x =	1	1	0	1	0	0
y =	1	1	1	1	1	1
$x \oplus y$ =	0	0	1	0	1	1

$\therefore$ $x \oplus y = 001011$ and $w(x \oplus y) = 3$

iii) $x, y \in B^7$, x = 1010001, y = 0001010

$\therefore$ $x \oplus y$ = 1011011 and $w(x \oplus y) = 5$

Distance : The distance between x and y is the weight of $x \oplus y$. i.e. $w(x \oplus y)$, it is denoted by d(x, y). The distance between two words is exactly the number of positions at which they differ.

$\therefore$ d(x, y) = $w(x \oplus y)$.

It is also called Hamming distance. **Minimum distance**: Let $x, y \in B^n$ then minimum distance = min. {d(x, y) : $x, y \in B^n$ }.

Let $x_1, x_2, ..., x_n$ are the code words, let any x_i, i = 1, 2, … n is a transmitted word and y be the corresponding received word. Then $y = x_k$ if $d(x_k, y)$ is the minimum distance for k = 1, 2, …n. This criteria is known as the minimum – distance criterion.

Encoding function : Let m < n (m, $n \in N$, N is set of natural numbers) then an one to one function $e : B^m \to B^n$ is called an (m, n) encoding function. i.e. for $x \in B^m$ we have $y \in B^n$ such that e(x) = y.

Detection of errors : Let $e : B^m \to B^n$ (m < n) is an encoding function then if minimum distance of e is (k + 1) then it can detect k or less than k errors.

Correction of errors : Let $e : B^m \to B^n$ (m < n) is an encoding function then if minimum distance of e is (2k + 1) then it can correct k or less than k errors.

Example 1 : Let e is (2, 4) encoding function defined as

e(00) = 0000 e(01) = 1011

e(11) = 1100 e(10) = 0110

i) Find minimum distance,

ii) How many errors can e detect,

iii) How many errors can e correct.

Solution :

Let $x_0 = 0000$, $x_1 = 1011$, $x_2 = 0110$, $x_3 = 1100$

i) $w(x_0 \oplus x_1) = w(x_1) = 3$

$w(x_0 \oplus x_2) = w(x_2) = 2$

$w(x_0 \oplus x_3) = w(x_3) = 2$

$w(x_1 \oplus x_2) = w(1101) = 3$

$w(x_1 \oplus x_3) = w(0111) = 3$

$w(x_2 \oplus x_3) = w(1010) = 2$

$\therefore$ Minimum distance of e = 2.

Note that minimum distance is not unique. There are three pairs having distance 2.

ii) $\therefore$ k + 1 = 2 $\therefore$ k = 1,

$\therefore$ e can detect 1 or less than 1 i.e. 0 errors.

iii) $\therefore$ 2k + 1 = 2 $\therefore$ k = $\frac{1}{2}$

$\therefore$ e can correct $\frac{1}{2}$ or less than $\frac{1}{2}$ errors, i.e. e can correct 0 errors.

Example 2 : Let e is (3, 8) encoding function defined as

e(000) = 00000000 e(011) = 01110001

e(010) = 10011100 e(110) = 11110000

e(001) = 01110010 e(101) = 10110000

e(100) = 01100101 e(111) = 00001111

i) Find minimum distance.

ii) How many errors can e detect?

iii) How many errors can e correct?

Solution :

Let x_0 = 00000000, x_1 = 10011100, x_2 = 01110010, x_3 = 01100101, x_4 = 01110001, x_5 = 11110000, x_6 = 10110000, x_7 = 00001111.

i) $w(x_0 \oplus x_1) = w(x_1) = 4$, $w(x_0 \oplus x_2) = w(x_2) = 4$,

$w(x_0 \oplus x_3) = w(x_3) = 4$, $w(x_0 \oplus x_4) = w(x_4) = 4$,

$w(x_0 \oplus x_5) = w(x_5) = 4$, $w(x_0 \oplus x_6) = w(x_6) = 3$,

$w(x_0 \oplus x_7) = w(x_7) = 4$

Similarly, $w(x_1 \oplus x_2) = w(11101110) = 6$,

$w(x_1 \oplus x_3) = 6$, $w(x_1 \oplus x_4) = 6$, $w(x_1 \oplus x_5) = 4$, $w(x_1 \oplus x_6) = 3$,

$w(x_1 \oplus x_7) = 4$, $w(x_2 \oplus x_3) = 4$, $w(x_2 \oplus x_4) = 2$, $w(x_2 \oplus x_5) = 2$,

$w(x_2 \oplus x_6) = 3$, $w(x_2 \oplus x_7) = 6$, $w(x_3 \oplus x_4) = 2$, $w(x_3 \oplus x_5) = 4$,

$w(x_3 \oplus x_6) = 5$, $w(x_3 \oplus x_7) = 4$, $w(x_4 \oplus x_5) = 2$, $w(x_4 \oplus x_6) = 3$,

$w(x_4 \oplus x_7) = 6$, $w(x_5 \oplus x_6) = 1$, $w(x_5 \oplus x_7) = 8$, $w(x_6 \oplus x_7) = 7$

$\therefore$ The minimum distance of e = 1.

ii) $\therefore$ k + 1 = 1 $\therefore$ k = 0

$\therefore$ e can detect 0 or less than 0 errors i.e. 0 errors.

iii) $\therefore$ 2k + 1 = 1 $\therefore$ k = 0

$\therefore$ e can correct 0 or less than 0 errors. i.e. 0 errors.

Example 3 : Compute

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \oplus \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Solution :

$$\begin{bmatrix} 1+1 & 1+0 & 0+0 \\ 0+1 & 1+0 & 1+1 \\ 1+0 & 0+0 & 0+1 \\ 0+1 & 0+1 & 0+0 \end{bmatrix} \oplus \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$\because$ Same digit sum = 0, opposite digit sum = 1

Example 4 : Let B = {0, 1} and + is defined on B as follows.

+	0	1
0	0	1
1	1	0

Then show that (B, +) is a group.

Solution :

Addition is associative. Here B is set of bits and the operation of on B is +. $\therefore$ B with operation + is associative.

Also 0 + 1 = 1 and 0 + 0 = 0

$\therefore$ $0 \in B$ is an identity element. Here inverse of each element is itself. Since 0 + 0 = 0. $\therefore$ $0^{-1} = 0$

and 1 + 1 = 0 $\therefore$ $1^{-1} = 1$

$\therefore$ Inverse of each element exists.

$\therefore$ (B, +) is a group.

Three Cartesian product of groups is again a group.

$\therefore$ $B^n = B \times B \times B \ldots \text{n times} \ldots \times B$ with + operation defined as $(x_1, x_2, ..., x_n) \oplus (y_1, y_2, ..., y_n) = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n)$ is also a group. Here identity element is $(0, 0, \ldots 0) \in B^n$ and every element is its own inverse.

$\therefore$ $\left(B^n, \oplus\right)$ is a group. Let $A \subseteq B^n$ such that $(A, \oplus)$ is a group then A is subgroup of B^n. Now we will see the encoding which uses this property of B^n.

Check Your Progress :

1. Let $e : B^2 \to B^6$ is an (2.6) encoding function defined as
   e(00) = 000000 e(01) = 011101
   e(11) = 111111 e(10) = 001110
   i) Find minimum distance.
   ii) How many errors can e detect?
   iii) How many errors can e correct?

2. Let e is (2, 5) encoding function defined as
   e(00) = 00000 e(01) = 11011
   e(11) = 11100 e(10) = 00101
   i) Find minimum distance.
   ii) How many errors can e detect?
   iii) How many errors can e correct?

Answers :

1. i) Minimum distance of e = 2.
   ii) Function can detect 1 or 0 errors.
   iii) Function can correct 0 errors.
2. i) Minimum distance of e = 2.
   ii) Function can detect 1 or 0 errors.
   iii) Function can correct 0 errors.

GROUP CODES:

An (m, n) encoding function $e : B^m \to B^n \, (m < n)$ is called a group code if range of e is subgroup of B^n. i.e. (Ran.(e), $\oplus$) is a group. Since Ran.(e) $\subseteq B^n$ and if (Ran.(e), $\oplus$) is a group then Ran.(e) is a subgroup of B^n.

If an encoding function $e : B^m \to B^n \, (m < n)$ is a group code, then the minimum distance of e is the minimum weight of a non zero codeword.

Example 5 : Show that an (3, 7) encoding function $e : B^3 \to B^7$ defined by

e(000) = 0000000 e(011) = 0111110
e(001) = 0010110 e(101) = 1010011
e(010) = 0101000 e(110) = 1101101
e(100) = 1000101 e(111) = 1111011

is a group code. Hence find minimum distance.

Solution : Let

x_0 = 0000000 x_4 = 1000101

x_1 = 0010110 x_5 = 1010011

x_2 = 0101000 x_6 = 1101101

x_3 = 0111110 x_7 = 1111011

$\therefore$ Ran.(e) = $\{x_0, x_1, ..., x_7\}$

$x_0 \oplus x_0 = x_0$, $x_0 \oplus x_1 = x_1$, $x_2 \oplus x_7 = 1010011 = x_5$ like this we can compute and this we will present in table.

The composition Table is,

$\oplus$	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_0	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_1	x_1	x_0	x_3	x_2	x_5	x_4	x_7	x_6
x_2	x_2	x_3	x_0	x_1	x_6	x_7	x_4	x_5
x_3	x_3	x_2	x_1	x_0	x_7	x_6	x_5	x_4
x_4	x_4	x_5	x_6	x_7	x_0	x_1	x_2	x_3
x_5	x_5	x_4	x_7	x_6	x_1	x_0	x_3	x_2
x_6	x_6	x_7	x_4	x_5	x_2	x_3	x_0	x_1
x_7	x_7	x_6	x_5	x_4	x_3	x_2	x_1	x_0

Like in Example 4 we can verity that (Ran.(e), $\oplus$) is group and Ran.(e) $\subset B^7$.

$\therefore$ Ran.(e) is subgroup of B^7.

$\therefore$ $e : B^3 \to B^7$ is a group code.

The minimum distance of a group code is the minimum weight of non zero code word.

Consider $w(x_0) = 0$, $w(x_1) = w(x_4) = 3$, $w(x_2) = 2$, $w(x_5) = 4$, $w(x_3) = w(x_6) = 5$, $w(x_7) = 6$.

$\therefore$ Minimum distance = 2.

Example 6 : Show that an (2, 5) encoding function $e : B^2 \to B^5$ defined as

e(00) = 00000 e(10) = 10101

e(01) = 01110 e(11) = 11011

is a group code. Hence find minimum distance and also find how many errors can e detect?

Solution :

$x_0 = 00000$, $x_1 = 01110$, $x_2 = 10101$, $x_3 = 11011$

$\therefore$ Ran.(e) = $\{x_0, x_1, x_2, x_3\}$

$\therefore$ The composition Table

$\oplus$	x_0	x_1	x_2	x_3
x_0	x_0	x_1	x_2	x_3
x_1	x_1	x_0	x_3	x_2
x_2	x_2	x_3	x_0	x_1
x_3	x_3	x_2	x_1	x_0

Addition is associative

$\therefore$ (Ran.(e), $\oplus$) is associative. We can see that the first row is same as heading row.

$\therefore$ x_0 is identity element. Also $x_0 \oplus x_0 = x_0$, $\therefore$ $x_0^{-1} = x_0$.

$x_2 \oplus x_2 = x_0$. $\therefore$ $x_2^{-1} = x_2$ so on. i.e. inverse of each element exists which is itself.

$\therefore$ $(\text{Ran.(e)}, \oplus)$ is a group and since Ran.(e) $\subset B^5$.

$\therefore$ Ran.(e) is subgroup of B^5.

$\therefore$ $e : B^2 \to B^5$ is a group code.

Consider,

$w(x_0) = 0$, $w(x_1) = w(x_2) = 3$, $w(x_3) = 4$.

The minimum distance of a group code is the minimum weight of nonzero code word.

$\therefore$ Minimum distance = 3.

Here k + 1 = 3, k = 2.

$\therefore$ e can detect 2 or less than 2 errors. i.e. e can detect 0, 1 or 2 errors.

Check your progress :

1. Show that an (2, 4) encoding function $e : B^2 \to B^4$ defined by

   e(00) = 0000 e(01) = 0011

   e(11) = 1110 e(10) = 1101

   is a group code.

12.9 LET US SUM UP

In this chapter we have learned that

- The product of G_1 and G_2 denoted as $G_1 \times G_2$.
- Homomorphism of a group, its property and types of homomorphism.
- Isomorphism of a group.
- Automorphism of a group.
- Cyclic group and its generators.
- Cosets and normal sub-group and Quotient group.

12.10 UNIT END EXERCISE

Q.1 Define normal subgroup and give one example.

Q.2 If (C, +) be a group, f:C→C define by f(Z) = $\bar{Z}$ for every Z ∈ C, $\bar{Z}$ being conjugate of Z, then show that f is Automorphism.

Q.3 Show that A = ({0, 1, 2, 3, 4, 5}, $+_6$) is cyclic.

Q.4 Show that multiplicative group G = {1, -1, i, -i } is cyclic.

Q.5 Let (Z, +) be the group of integers and N = {3n / n ∈ Z} then N is a normal subgroup of Z.

Q.6 If G = {1, -1, i, -i } is a group and G'= ({0, 1, 2. 3}, $+_4$) is another group then show that gG is isomorphism to G'.

Q.7 If $f : R^+ \to R$ defined by f(x) = log(x) for every x ∈ R^+ then show that f is isomorphism. Where R^+ and R are multiplicative group.

Q.8 Prove that all finite group of order 2 are isomorphism.

Q.9 Mapping $f : G \to G$ defined by f(x) = x^{-1}, for all x ∈ G on a group (G, *) is an automorphism if and only if (G, *) is abelian.

Q.10 Show that the group ({0, 1, 2, 3,……..n-1}, t_n) is a cyclic group.

Q.11Show that (U_n, .) is a cyclic group of n^{th} roots of unity under multiplication.

Q.12 If H is subgroup of G and if x ∈ G implies that x^2 ∈ H, then prove that H is a normal subgroup of G.

Q.13 Compute $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \oplus \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$.

Q.14 Find weights of the given words a) 001110, b) 0000, c) 111, d) 100100110.

Q.15 Find the distance between x and y

i) x = 00111101, y = 00110010

ii) x = 1010001100, y = 0000111100

Answers :

13 $\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

14 a) 3 b) 0 c) 3 d) 4

15. i) 4 ii) 4

12.11 REFERENCES FOR FURTHER READING

1. University Algebra by N.S. Gopalkrishnan.

2. Contemptary Algebra by Gallian.

3. Discrete mathematics by Kenneth and Rosen.

4. Discrete mathematical structures by Kolman, Busby and Ross.

5. Modern Algebra by Vasishtha.

13

RINGS

Unit Structure

13.0 OBJECTIVES :

After going through this chapter students will be able to:

- Algebraic structures with two binary operations.
- Definition of ring and its property.
- Zero divisor and integral domain.
- Fields.
- Ring of homomorphism.
- Ring of isomorphism.

13.1 INTRODUCTION :

Groups were studied in the previous chapters, and the definition of group involves a single binary operation with respect to addition or multiplication. The distributive laws interlink the two operators addition and multiplication. This leads us to the study of one such algebraic system equipped with two binary operations called as rings.

Ring is the second algebraic system. The abstract concept of Rings has its origin from the set of integers. The algebra of rings follows the pattern already laid out for group. Only difference is algebraic structures with two binary operations.

13.2 ALGEBRAIC STRUCTURES WITH TWO BINARY OPERATIONS.

An algebraic structure is a nonempty set together with one or more binary operation on that set.

Addition and multiplication are both binary operations on the set R of real numbers is called algebraic structure with two binary operations. It is denoted by (R,+, .).

13.2.1 Rings

Definition: A ring R is a non-empty set with two binary operations denoted by '+' and . with respect to the following conditions.

- R is an abelian group with respect to +,i.e.,
  - I. $a + (b + c) = (a + b) + c \ \forall\ a,b,c \in R$
  - II. there exists $0 \in R$ such that $a + 0 = a = 0 + a \ \forall\ a \in R$
  - III. For each $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0 = (-a) + a$
  - IV. $a + b = b + a \ \forall\ a, b \in R$
- R is a semi group for i.e., $a.(b.c) = (a.b).c \ \forall\ a, b, c \in R$
- Multiplication distributes over assition, i.e.,
  - I. $a.(b + c) = a.b + a.c \ \forall\ a,b,c \in R$
  - II. $(b + c).a = b.a + c.a \ \forall\ a,b,c \in R$

Note: we write a.b as ab.

Now let us see one example that satisfies the above-described axioms.

Example 1: Set of even integers is a ring with respect to usual addition and multiplications of integers.

Solution: Let E be the set of even integers i.e.,

$$E = \{2x : x \in Z\}$$

Let $a, b \in E$ where $a = 2m$ and $b = 2n$

$$a+b = 2m + 2n = 2(m+n) \in E \ (\therefore\ m+n \in Z)$$

$\therefore$ E is closed with respect to addition.

Let a, b, c ∈ E where a = 2m, b = 2n, c = 2p

a+(b+c)=2m+(2n+2p)=2m+2(n+p)=2[(m+n)+p]
=(2m+2n)+2p=(a+b)+c

∴ *E is associative with respect to addition.*

Since 0 ∈ Z, O = 2.0 ∈ E

Consider a + O = 2m+2.0 = 2(m+0) = 2m = a

∴ O is the identity element in E.

For m ∈ Z there exists –m ∈ Z and 2.(-m) ∈ E.

Let –a =2.(-m)

Consider a + (-a) = 2m +2.(-m)

= 2(m+(-m))

= 2.0

= O =(-a) +a

∈ (-a) is the inverse of a.

∴ *Inverse exists for each element in E.*

For a, b, ∈ E then a + b = 2m + 2n = 2(n+m) (sum of integers is commutative) = 2n + 2m

= b + a

E is commutative with respect to addition.

(E, +) is *an abelian group*.

Consider a, b, c ∈ Z where a = 2m,b = 2n, c = 2p

a(bc)= 2m(2n.2p) =2m,(4np) = 8 mnp

(ab)c = (2m.2n.)2p =(4mn)2p = 8 mnp

a(bc) = (ab).c ∀ a,b,c ∈ E

E is associative with respect to multiplication.

Consider a.(b+c) = 2m.(2n 2p)

= 2m. 2n + 2m.2p

= a.b + a.c

Similarly, (b + c).a = b.a + c.a

∴ Distributive laws hold in E.

∴ Hence (E, +, .) is a ring.

Example 2: Show that the set of all rational numbers is a ring with respect to ordinary addition and multiplication.

Solution: Let Q be the set of all rational numbers.

1) (Q, +) is abelian.

Closure: Let a, b ∈ Q then a + b ∈ Q

because sum of two rational numbers is a rational number.

Associative: Let a, b, c ∈ Q then (a + b) + c = a + (b + c)

because associative law for addition holds.

Existence of Identity: 0 ∈ Q and 0 + a = a + 0 = a for every a ∈ Q

i.e. 0 is additive identity in Q.

Existence of inverse: for every a ∈ Q, -a ∈ Q and a + (-a) = 0

Hence, additive inverse in Q exists for each element in Q.

Commutative: Let a, b ∈ Q then a + b = b + a

because addition is commutative for rational.

2) (Q, .) is a semi group.

Closure : Since the product of two rational numbers is a rational number.

a, b ∈ Q then a .b ∈ Q

Associativity: Multiplication in Q is associative.

3) Multiplication is left as well as right distributive over addition in the set of rational numbers. i.e.

a.(b + c) = a.b + a.c

(b + c).a = b.a + c.a for every a, b,c ∈ Q .

Hence, (Q, +, .) is a ring.

13.3.1 Ring with unity

A ring need not have an identity under multiplication, when a ring other than {0} has an identity under multiplication; we say that the *Ring is with unity.*

Definition: R is called a ring with unity element if there exists 1 ∈ R such that a1 = a = 1a for all a $\neq$ 0 ∈ R.

Note: A Ring with unity contains at least elements 0 and 1.

Commutative Ring

In a ring, multiplication need not be commutative, when it sis, we say that the ring is *commutative*.

Definition: A Ring R is said to be commutative if ab = ba $\forall$ a, b ∈R.

Example 3: Let the addition and multiplication in Q$\sqrt{2}$ be defined as x = a + b$\sqrt{2}$ and y = c + d$\sqrt{2}$

$\in Q(\sqrt{2})$ x + y $(a + c) + (b + d)\sqrt{2}$

xy = $(ac + 2bd) + (ad + bc)\sqrt{2}$ is a commutative ring with unity.

Solution: $Q(\sqrt{2}) = \{a + b\sqrt{2} / a, b \in Q\}$

$X = a + b\sqrt{2}$ and $y = c + d\sqrt{2} \in Q(\sqrt{2})$

$x + y = (a + c) + (b + d)\sqrt{2}$ since a + c and b + d belong to Q

$x + y \in Q\sqrt{2}$.

$\therefore$ $\mathbf{Q}\sqrt{2}$ is closed with respect to addition.

For $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$ $z = e + f\sqrt{2}$ where a, b, c, d, e, f $\in Q\sqrt{2}$

We have, $x + (y+z) = a + b\sqrt{2} + ((c + d\sqrt{2}) + (e + f\sqrt{2}))$

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

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

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

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

$= (x + y) +$

$\therefore$ $Q\sqrt{2}$ is *Associative with respect to* ***Addition.***

Since 0 is a rational number $0 + 0\sqrt{2} \in Q\sqrt{2}$

Consider $(a + b\sqrt{2}) + (0 + 0\sqrt{2}) = (a + 0) + (b + 0)\sqrt{2}$

$= a + b\sqrt{2}$

Similarly $(0 + 0\sqrt{2}) + (a + b\sqrt{2}) = a + b\sqrt{2}$.

Hence $0 + 0\sqrt{2}$ is the identity existing in $Q\sqrt{2}$

For a, b $\in$ Q, -a, -b $\in$ Q hence $(-a) + (-b)\sqrt{2}) \in Q\sqrt{2}$

Consider $a + b\sqrt{2} + ((-a) + (-b)\sqrt{2}) = (a + (-a) + b + (-b)\sqrt{2}) = 0 + 0\sqrt{2}$

Similarly $(-a) + (-b)\sqrt{2} + (a + b\sqrt{2}) = 0 + 0\sqrt{2}$.

Hence $(-a) + (-b)\sqrt{2}$ is the inverse of $a + b\sqrt{2}$

Inverse exists for each element in $Q\sqrt{2}$.

$X = a + b\sqrt{2}$ and $y = c + d\sqrt{2} \in Q(\sqrt{2})$ where a, b, c, d $\in$ Q

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

Since addition of rational numbers is commutative.

a + c = c + a and b + d = d + b

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

$\therefore$ $Q\sqrt{2}$ is **commutative** with respect to **Addition.**

$(Q\sqrt{2}, +)$ is an **Abelian group.**

Example 4 : Let (G, *) be an arbitrary commutative group and Hom G be the set of all homomorphisms from (G, *) onto itself. Then show that (Hom G, +, .) is a ring with unity, where the operation + defined by

(f + g)(a) = f(a)*g(a), a ∈ G, for every f, g ∈ Hom G, and ∈ denotes the functional composition.

Solution:

Closure : For every f, g ∈ Hom G, and a, b ∈ G,

(f, g)(a * b) = f(a * b) * g(a * b)
= (f(a) * f(b)) *(g(a) * g(b))
=(f(a) * g(a) * f(b) * g(b))
= (f + g)(a) * (f + g)(b),

So that the sum f + g ∈ Hom G.

Associative : For every f, g, h ∈ Hom G, and a ∈ G,

We have ((f + g) + h) (a) = (f + g)(a) * h(a)
= ((f(a) * g(a)) * h(a)
= f(a) * ((g(a) * h(a))
= f(a) * (g + h)(a)
= (f + (g+h))(a).

Thus (f + g) + h = f + (g + h).

Existence of identity : For every f ∈ Hom G, there exists constant mapping Z which map all elements of G on e, the identity of (G, *) such that

(f +Z)(a) = f(a) * Z(a) = f(a) * e = f(a).

Thus f +Z = f ∈ Z is an identity in Hom G, that is, the mapping Z in Hom G is the Zero element.

Existence of inverse: For every f ∈ Hom G, ∈ -f ∈ Hom G defined by $(-f)(a) = f(a)^{-1}$, such that , For every a ∈ G,

$(f +(-f))(a) = f(a) * f(a)^{-1} = e = Z(a)$.

Which implies that f +(-f) = Z, therefore inverse also exists.

Commutative property: For every f, g ∈ Hom G, a ∈ G, we have

(f + g)(a) = f(a) * g(a) = g(a) * f(a) = (g +f)(a).

Thus (f +g) = f + g,

Hence (Hom G, +) is commutative group.

Similarly we prove that (Hom G, ∈) is a semi-group with identity.

Now to prove that (Hom G, +, ∈) is a ring with unity there remains to show that ∈ is distributive over +.

f∈ (g + h)(a) = f(g + h) a) = f(g(a) * h(a)) = f(g(a)) * f(h(a)) = (f∈g)(a) * (f∈h)(a).

Therefore f∈ (g + h) = (f∈g) + (f∈h), similarly, we can prove right distributive law.

Thus (Hom G, +, .) is a ring with unity.

13.4 ZERO DIVISORS

There are some properties, which are not true in a general ring. We know that product of two integers is zero, if one among them is zero, but this may no longer be true in any ring R of 2 x 2 matrices we have $\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$; even through $\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$ are non-zero and their product is zero in R.

Definition: Let R be a ring and a ∈ R, b ∈ R both are non-zero but their product

ab = 0 . Then we say that **a, b are zero divisors.**

13.4.1 Integral Domain

Definition: A commutative Ring, with unity is an integral domain if it has no zero divisors and it is donated by the symbol.

For example: The Ring of integrals, rational Numbers, and real numbers and complex numbers is all integral domain.

13.5 FIELD

Definition: A commutative Ring R with unit element $i \neq 0$ in which every non-zero element has an inverse with respect to multiplication am called a **field.**

Example 5: Set of Gaussian integers is an integer's domain but not a field.

Solution: Set of Gaussian integers Z(i) = {a + ib/a, b∈Z)}

Let x , y ∈ Z(i)

Where x = a + ib and y = c + id where a, b, c, d ∈Z

x + y = (a + c) + (b + d) I = $a_i + ib_1$ = a + c and b_1 = b + d ∈ Z.

x . y = (ac – bd) + (ad + bc) I

= $a_2 + ib_2$ where a_2 = ac – bd, b_2 = ad + bc ∈Z.

∴ +, . are binary operation in Z(i).

Since the element of Z(i) are integers,

We have that

1. Addition and multiplication are commutative in Z(i)
2. Addition and Multiplication are associative in Z(i)
3. Multiplication is distributive over addition in Z(i)

Clearly, zero element 0 = 0 + 0_i ∈ Z and unit element 1 = 1 + 0_i ∈ Z

Further, for every x = a + b ∈Z(i), x, y = 0 ∈ x = 0 since x , y are integers.

Z(i) is without zero divisors.

Hence Z(i) is an integral domain

Let $m = 3 + 4i \in Z(i)$ and $n = \frac{3}{25} - i\frac{4}{25}$

So that $m.n = \left([9/25] + [16/25]\right) + i\left([(-12)/25] + [12/25]\right) = 1 + 0i$

But n ∈ Z(i), because 3/25 and 4/25 ∈ Z.

So every non-zero element of Z(i) is not invertible

Hence Z(i) is not a field.

13.6 RING HOMOMORPHISM

In groups, one way to discover information about a group is to examine its interaction with other groups by way of homomorphism. Now we show that just as a group homomorphism preserves the group operation, a ring homomorphism preserves the ring operations.

Definition: A ring homomorphism *f* from a ring R to another ring R_1 is a mapping from R to R_1 that preserves the two ring operations; that is, for all a, b in R

$$f(a + b) = f(a) + f(b)$$
$$f(ab) = f(a)\, f(b).$$

Example: Let $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} / a,b,c \in Z \right\}$. Prove or disprove that the map $\phi : IR \to Z$ defined by $\phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right) = a$ is a ring homomorphism.

Solution: $\phi : IR \to Z$ defined by $\phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right) = a$.

Let $A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$

$$\phi(A+B) = \phi\left(\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}\right)$$

$$= \phi\left(\begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ 0 & c_1 + c_2 \end{bmatrix}\right)$$

$$= a_1 + a_2$$
$$= \phi(A) + \phi(B)$$

$$\phi(AB) = \phi\left(\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}\right)$$

$$= \phi\left(\begin{bmatrix} a_1a_2 & a_1b_1 + b_1c_2 \\ 0 & c_1c_2 \end{bmatrix}\right)$$

$$= a_1\, a_2$$
$$= \phi(A)\phi(B)$$

$\phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right) = a$ is a ring homomorphism.

13.7 ISOMORPHISM

Definition: A homomorphism *f*:R → R_1 is called an isomorphism if, *f* is both one-one and onto mapping.

Propertied of homomorphism: Let $f : R \to R_1$ be a homomorphism of a ring R into the ring R_1 and $0 \in R$, $0_1 \in R_1$ be the zero element of R and R_1 then

$f(0) = 0_1$

$f(-a) = -f(a) \ \forall\ a \in R$

$f(a-b) = f(a) - f(b) \ \forall\ a, b \in R$

Example :- Consider the sings . $S = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} / a,b \in IR \right\}$ and show that the map $\phi\ (a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ is a ring isomorphism.

Solution :- $\phi : C \to M_2[IR]$

$$\phi(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}.$$

To show that ϕ is homomorphism

A = a+bi B = c+di

ϕ (A+B) = ϕ [a+c+bi+di]

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

$$= \phi(a+b) + d(c+di)$$

$$\phi(A \cdot B) = \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & (ac+bd) \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$$

$$= = \phi(A).\phi(B)$$

To show that ϕ is 1-1

$\phi(A) = \phi(B)$

$\phi(a+bi) = \phi(c+di)$

$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$

a = c, b = d $\in$ a+bi = c+di

To show that ϕ is onto

For any $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} (-M_2(IR)$

There exists at b, c $\in$ C such that

$\phi(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$

Hence, the map $\phi\ (a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ is a ring isomorphism.

13.8 LET US SUM UP

In this chapter we have learned

- Algebraic structures with two binary operation.
- Definition of ring.
- Commutative ring and ring with zero divisor.
- Integral domains and fields.
- Ring homomorphism and isomorphism.

13.9 UNIT END EXERCISE

Q.1 Prove that the set I of all integers with ordinary addition and multiplication as the compositions forms a ring.

Q.2 Show that the set of number given by x +y$\sqrt{5}$, where x and y are integers is a ring with ordinary addition and multiplication as the two compositions.

Q.3 If E denotes the set of all even integers, then prove that {E, +, .} is a commutative ring, where a.b = $\frac{ab}{2}$ and + is the usual addition.

Q.4 Show that the set of number of the form x +y $\sqrt{2}$, x and y are rational numbers is a field.

Q.5 Show that Z[$\sqrt{5}$], the set of complex numbers x +y $\sqrt{5}$ where x, y are integers, ia an integral domain.

Q.6 Let 'R' is ring with unity 'e'. $f : Z \to R$ is a mapping defined by $f(x) = xe \quad \forall x \in Z$. Prove that f is ring of homomorphism.

Q.7 Let f be the function from the integer Z onto the even integers given by f(x) = 2x for all

x ∈ Z. Prove that f is not a homomorphism.

13.10 REFERENCES FOR FURTHER READING

1. University Algebra by N.S. Gopalkrishnan.
2. Contemptary Algebra by Gallian.
3. Discrete mathematics by Kenneth and Rosen.
4. Discrete mathematical structures by Kolman, Busby and Ross.
5. Modern Algebra by Vasishtha.

❖❖❖❖

14

RECURRENCE RELATION

Unit Structure

14.0 OBJECTIVES

After going through this chapter you will be able to:

- Series and sequences.
- Generating function.
- Recurrence relation.
- The first order linear homogeneous recurrence relations.
- The second order homogeneous linear recurrence relations.
- The non-homogeneous relations.
- The method of generating functions.
- Applications.

14.1 INTRODUCTION:

We all know that the mathematical induction is a proof technique that verifies a formula or assertion by inductively checking its validity for increasing values of n. In a similar way, a recurrence relation is a counting technique that solves an

enumeration problem by recursively computing the answer for successively larger values of n.

The concept of a generating function is one of the most useful and basic concepts in the theory of combinatorial. The power of the generating function rests upon its ability nor only to solve the kinds of problems have we considered so far but also to aid us in new situations where additional restrictions may be involved.

14.2 SEQUENCES:

A sequence is an ordered list of objects. A sequence is denoted by $\{a_n\}$, where a_n represents n^{th} term of the sequence $(n \in \mathbb{N})$. If the list terminates after some steps then we say sequence is finite otherwise it is called as an infinite sequence.

Example:

(1) 3, 4, 5, 6, 7, 8, 9 is a finite sequence, in this $a_1 = 3$, $a_2 = 4$ and so on.
(2) 1, 4, 9, 16, 25,… is an infinite sequence, in this $a_1 = 1$, $a_2 = 4$, $a_3 = 9, ...$
(3) -1, 1, -1, 1,… is also an infinite sequence $a_1 = -1$, $a_2 = 1$, $a_3 = -1$
(4) 1, 3, 7,… is an infinite sequence.

In example (1) we can see that $a_2 = a_1 + 1$, $a_3 = a_2 + 1$ and so on i.e. $a_{n+1} = a_n + 1$, where $a_1 = 3$ and $n \le 7$. Similarly in (4) we have, $a_{n+1} = 2a_n + 1$, where $a_1 = 1$.

A formula, like above is called as recursive formula, where next term depends on previous term. A recursive formula must have a starting value (i.e. a_1).

But in example (2), we have $a_1 = (1)^2$, $a_2 = (2)^2$, $a_1 = (3)^2$ and so on i.e. $a_n = (n)^2$ means value of $'a'_{n+1}$ does not depend on $'a'_n$ such a formula is called as Explicit formula. Similarly in (3), $a_n = (-1)^n$ value of a_n it is position number.

The set corresponding to a given sequence is the set of all distinct elements of a given sequence.

It can be finite or infinite.

For e.g. (1) for $a_n = (-1)^n$, corresponding set = {-1, 1}.

(2) for $a_n = n + 1$, corresponding set = {2, 3, 4,……}

The difference between set and sequence is, in a set order of the elements is not important but in a sequence order of the elements is important.

A set is called countable if it is elements can be arranged in order first, second, third etc. i.e. it is the set corresponding to some sequence for example, set of Natural numbers, set of rational etc.

A set which is not countable is called as an uncountable set. For example, set of Real Numbers.

Check your progress :

1. Write a formula for n^{th} term and identify it is recursive or explicit.

(a) $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$ (b) $1, 0, 1, 0, 1, 0, \ldots$

(c) 3, 6, 9,… (d) 2, 5, 10, 17, 26

(e) 5, 25, 125,…

14.3 SERIES

An expression of the form $a_1 + a_2 + a_3 + \ldots\ldots + a_n + \ldots\ldots\ldots$ which is the sum of the elements of the sequence $\{a_n\}$ is called a series. If the series contains a finite number of elements, it is called finite series, otherwise called an infinite series.

If $S_n = a_1 + a_2 + a_3 + \ldots\ldots + a_n$, then S_n is called the sum of n terms of the series and is denoted by the Greek letter sigma $\sum$.

Thus $S_n = \sum_{i=1}^{n} a_n$.

Example 1: Find the sum of first 20 natural numbers.

Solution: To find sum of first 20natural numbers.

i.e $S_n = 1 + 2 + 3 + 4 + \ldots..+20$.

Here first term = a = 1 and the common difference = d =1

Bye arithmetic progression,

$S_n = \frac{n}{2}[2a + (n-1)d]$

$= \frac{20}{2}[2(1) + (20-1)1]$

$= 10[2 + 19] = 210$.

Check your progress:

1. Find the sum of the series 2+4+6+8+10+……+38.
2. Find the sum of the series 3+5+7+9+11+……+53.
3. Find the sum of the series 3+7+11+15+…….+73.

14.4 FIBONACCI SEQUENCE:

The Fibonacci sequence is a set of numbers that starts with a one and a zero, followed by a one , and proceed based on the rule that each number is equal to the sum of the preceding two numbers is called Fibonacci number and the sequence obtained is called Fibonacci sequence.

If Fibonacci sequence is denoted by F(n), where n is the first term in the sequence, the following equation obtains for n=0,where first two term are defined as 0 and 1 by convention.

F(0) = 0, 1, 1, 2, 3, 5, 8, 13, …….

14.5 GENERATING FUNCTIONS

Now we see some important polynomial expansions, which are often used in this chapter.

Polynomial Identities

1. $\frac{1-x^{n+1}}{1-x} = 1+x+x^2+x^3+.....+x^n$
2. $\frac{1}{1-x} = 1+x+x^2+x^3+.....$
3. $(1+x)^n = 1+\binom{n}{1}x+\binom{n}{2}x^2+\binom{n}{3}x^3+.....+\binom{n}{n}x^n$

Definition: Let $a_0, a_1, a_2,.....$ be a sequence of real numbers. The function

$$f(x) = a_0 + a_1x + a_2x^2 +_{.....} = \sum_{i=0}^{\infty} a_i r^i$$

is called the ordinary generating function or generating function for the given sequence.

Example 2: Find the generating function for the binomial theorem .

Solution: For any $n \in Z^+$

$$(1+x)^n = \binom{n}{0}+\binom{n}{1}x+\binom{n}{2}x^2+.....+\binom{n}{n}x^n.$$

So $(1+x)^n$ is the generating function for the sequence

$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots\ldots\ldots\ldots, \binom{n}{n}$

$f(x) = (1+x)^n$ is the generating function for $a^r = C(n,r)$, the number of ways to select an r-subset of n-set.

Example 3: Find the coefficient of x^5 of generating function $(1-2x)^{-7}$.

Solution : Using the generating function for Maclaurin series.

We write $(1-2x)^{-7} = (1+y)^{-7} = \sum_{r=0}^{\infty} \binom{-7}{r} (-2x)^r$ where y = -2x.

Consequently, the coefficient of x^5 is

$$\binom{-7}{5}(-2x)^5 = (-1)^5 \binom{7+5-1}{5}(-32)$$

$$= \binom{11}{5}(32) = 14,784.$$

Check your progress:

1. Find the generating function for Maclaurin series. [hint $f(x) = (1+x)^{-n}$]
2. Find the generating function for $\frac{(1-x^{n+1})}{(1-x)}$.
3. Determine the coefficient of x^8 of generating function $\frac{1}{(x-3)(x-2)^5}$.

14.6 RECURRENCE RELATION

A recurrence relation is a recursive formula that counts the number of ways to do a procedure involving n objects in terms of the number of ways to do it with fewer objects. That is if a, is the number of ways to do the procedure with r objects, for r=0, 1, 2,……, then a recurrence relation is an equation that expresses a_n as some function of preceding a_k ‘ s, k < n. A formal definition is given after the following example.

A boy has a staircase of n stairs to climb. Each step it takes can cover either one stair or two stairs. Find the number of different ways for the boy to climb staircase.

We solve this using recurrence relation.

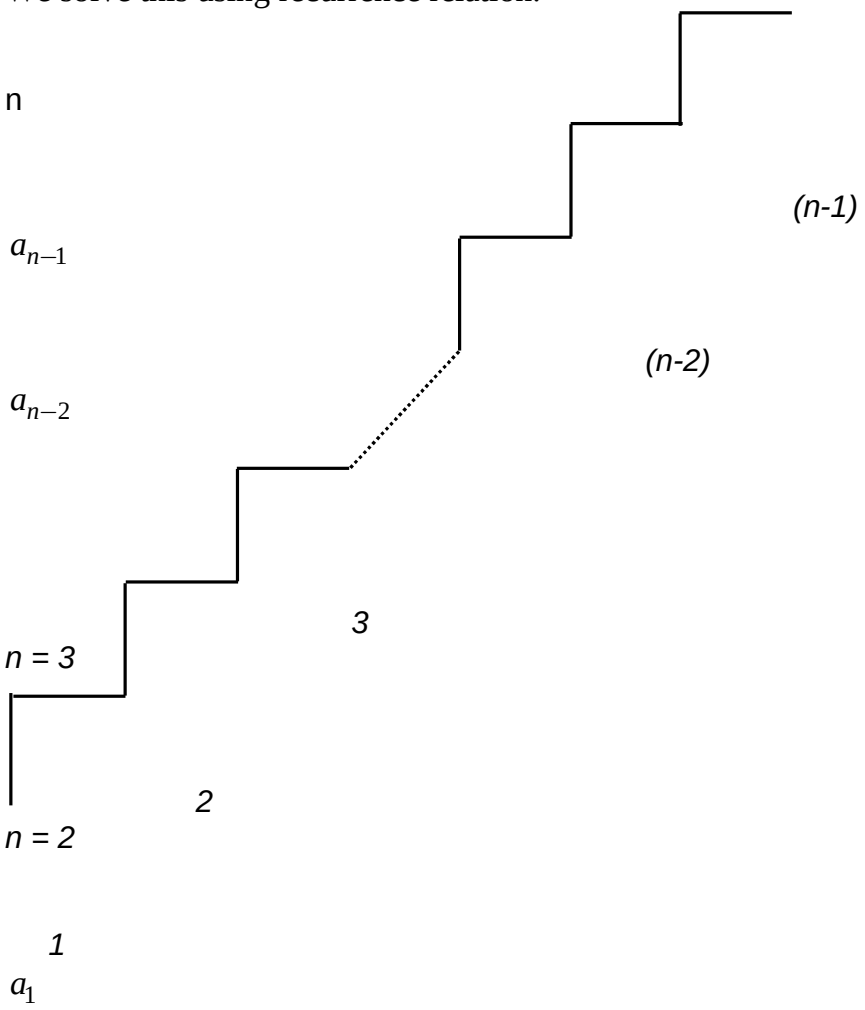


Fig 14.1

Let a_n be the number of different ways the boy can climb a staircase with n stairs.
Thus
a_1=1, [one step can be climbed in only one way]
a_2=2, [1+1 that is in two steps or both stairs in single step]
a_3=3, [1+1+1, 1+2 and 2+1]
etc.
to compute a_n, the boy can reach n th stair with or without using n-1 th stair using n-1 th stairs he has a_{n-2} ways without using n-1 th stair (as the has to use n-2 th stair) he has a_{n-2} ways.
Thus

$a_n = a_{n-1} + a_{n-2.}$

These numbers are well known Fibonacci numbers. Where n th term is some of previous two terms such dependency gives us recurrence relation which can be formally defined as:

"A recurrence relation is a relation among the sequence (a_n), n=0, 1, 2,….., of the form $f(n, a_1, a_2, \ldots, a_n) = 0$ for all $n \geq k$. "
Three simple example could be
$a_n - a_{n-1}\, a_{n-2} = 0, \quad n \geq 2, \qquad (1)$
$a_n - a_{n-1} = n, \quad n \geq 1, \qquad (2)$
$a_n - a_1 a_{n-1} - a_2 a_{n-2} - \ldots - a_{n-1}\, a_1 = 0, \quad n \geq 3. \qquad (3)$
is a linear homogeneous recurrence relation with constant coefficients,
is a linear non-homogeneous recurrence relation with constant coefficients,
is a non-linear recurrence relation, and a formal definition is below.
Let $k \in Z^+$ and $C_n (\neq 0)$, C_{n-1}, C_{n-2},……, $C_{n-k} (\neq 0)$ be real number.
If a_n, for $n \geq 0$, is a discrete function , then
$C_n a_n + C_{n-1} a_{n-1} + C_{n-2} a_{n-2} + \ldots + C_{n-k} a_{n-k} = f(n), \quad n \geq k$,

Is a linear recurrence relation with constant coefficient of order k. when f(n) = 0 for all $n \geq 0$, the relation is called homogeneous; it is non homogenous.

14.6.1 THE FIRST – ORDERED LINEAR RECURRENCE RELATION

A linear homogeneous recurrence relation of the form,
$a_n = \alpha a_{n-1}$
is called the first order homogeneous linear recurrence relation, where α is a constant.
Since a_n depends only on its immediate predecessor, the relation is said to be first-order.
Now the above relation may be defined as the "first – order linear homogenous recurrence relation with constant coefficients.

General solution
The general solution of the recurrence relation
$$a_n = \alpha\, a_{n-1} \qquad (4)$$

where α is a constant, $n \geq 1$, and $a_0 = A$, is unique and is given by
$$a_n = A\alpha^{\,n} \qquad (5)$$
The expression $a_0 = A$ is called the initial condition .
Thus the solution $a_n = A\alpha^{\,n}$, $n \geq 1$, defines a discrete function whose domain is the set **N** of all natural numbers.

Example 4: Solve the recurrence relation $a_{n+1} = 3a_n$, $n \geq 0$, $a_0 = 5$.

Solution:
The first four terms of this sequence are

$a_0 = 5$,
$a_1 = 3a_0 = 3(5) = 15$,
$a_2 = 3a_1 = 3(3a_0) = 3^2(5)$, and
$a_3 = 3a_2 = 3(3^2(5)) = 3^3(5)$.

By using induction, we can easily verify that, the general solution is

$a_n = 5(3^n)$ for each $n \geq 1$.

In the general solution, the value of a_n is a function of n and there is no longer any dependence on prior terms of the sequence, once the value of a_0 is known.

Example 5: Solve the recurrence relation $a_n = 7a_{a-1}$, where $n \geq 1$ and $a_2 = 98$.

Solution:

This is an alternative from of the recurrence relation $a_{a+1} = 7\ a_n$ for $n \geq 0$ and $a_2 = 98$.

From the above formula, we have the general solution $a_n = a_a\,(7)^n$

Since $a_2 = 98 = a_0\,(7^2)$. This gives $a_0 = 2$.

Hence the general solution $a_n = 2(7)^n$, $n \geq 0$, is unique.

Example 6: A bank pays 6% annual interest on savings, compounding the interest monthly. If a person deposits 1000/- , how much will this deposit be worth a year later?

Solution:

We solve the above problem using the recurrence relation concept as follows.

Let P_n be the deposit at the end of n months.

Given

$P_0 = 1000$,

The rate of interest per annum is 6%, so the monthly rate = 6/12% = 0.005.

Now the recurrence relation for the deposit is,

$$P_{n+1} = P_0 + 0.005P_n = P_N(1.005)$$

Where $0.005P_n$ is the interest earned on P_n at the end of n the month.

The general solution for the recurrence relation is

$$P_n = P_0\,(1.005)^n$$

Consequently the deposit at the end of 12 months is

$$P_{12} = P_0(1.005)^{12}$$
$$= 1000(1.005)^{12}$$
$$= 1061.68$$

14.6.2 Special Cases

Conversion of Non Liner to Linear: In a linear relation there are no products such as $a_n a_{n-1}$…, (see equation (1) in the definition of recurrence relation at the beginning of this chapter) which appears in the non-linear relation, $a_{n+1} - 3a_n a_{n-1} = 0$. However , there are times when a nonlinear recurrence relation can be transformed into a linear one by a suitable algebraic substitution.

Example 7: Find a_8 if $a^2_{n+1} = 6a^2_n$, where $a_n > 0$ for $n \geq 0$, and $a_0 = 2$.

Solution:

Given the recurrence relation
$a^2_{n+1} = 6a^2_n$, where $a_n > 0$ for $n \geq 0$, and $a_0 = 2$ (6)
is not a linear one in a_n
But we transform (6) into linear with the substitution.
$b_n = a^2_n$,
Then the new relation
$b_{n+1} = 6b_n$ for $n \geq 0$, and $b_0 = 4$, (7)
is a linear relation
Now the general solution for the new recurrence relation (7) can be computed using the general solution method discussed in this section 3.1.
Comparing (6) with equation (4), we observe that
$\alpha = 6$ and the general solution is
$`b_n = (\alpha)^n b_0 = (6)^n 4$.
Therefore $a_n = 2(\sqrt{6})^n$ for $n \geq 1$.
Consequently $a_8 = 2(\sqrt{6})^8 = 2592$.

Example 8: Find a_{12}, if $a_{n+1}{}^2 = 5a_n{}^2$, where $a_n > 0$ for $n \geq 0$ and $a_0 = 2$.

Solution:

This is a non-linear recurrence relation. This can be converted into linear by letting $b_n = a_n{}^2$. This gives the new relation $b_{n+1} = 5b_n$ for $n \geq 0$, and $b_0 = 4$ which is linear.

The general solution is $b_n = 4(5)^n$.

Therefore, $a_n = 2(\sqrt{5})^n$ for $n \geq 0$.

Hence $a_{12} = 2(\sqrt{5})^{12} = 31{,}250.6$

14.6.3 Non Homogeneous Relations: The general first order linear recurrence relation.

With constant coefficients has the form $a_{n+1} + ca_n = f(n)$, $n \geq 0$ where c is a constant and f(n) is a function on the set N of Non negative integers.

Where $f(n) = 0$ for all $n \in N$, the relation is called homogeneous; otherwise it is called non homogeneous. So far, we have dealt only with homogeneous relations. Now we shall solve a non-homogeneous relation.

Example 9: Find a recurrence relation and solve it for the following sequence.

Solution:

0, 2, 6, 12, 20, 30, 42…

Hear $a_0 = 0$, $a_1 = 2$, $a_2 = 6$, $a_3 = 12$, $a_4 = 20$, $a_5 = 30$, $a_6 = 42$, and we observe that

$a_1 - a_0 = 2$,
$a_2 - a_1 = 4$,
$a_3 - a_2 = 6$,
$a_4 - a_3 = 8$,
$a_5 - a_4 = 10$,
$a_6 - a_5 = 12$,

These calculations suggest the recurrence relation.

$a_n - a_{n-1} = 2n$, $n \geq 1$, $a_0 = 0$

To solve this relation, we proceed in a slightly different manner from the method we used in the previous examples. Consider the following n equation:

$a_1 - a_0 = 2$,
$a_2 - a_1 = 4$,
….
….
….
$a_n - a_{n-1} = 2n$,

By adding the above n equations we get,

$a_1 - a_0 = 0 + 2 + 6 + 8 + \ldots + 2n$
$= 2(1 + 2 + 3 + \ldots + n)$
$= 2[n(n+1)/2] = n^2 + n$

Therefore the general solution is

$a_n = n^2 + n.$

With variable coefficients

We have seen and discussed various types of recurrence relations, which are with constant coefficients. Now we see an example of the type with variable coefficients in this section ***"First order recurrence relations".***

Example 10: Solve the relation $a_n = n.a_{n-1}$, when $n \geq 1$ *and* $a_0 = 1$

Solution: We solve this problem by proceeding as above but differ in a small manner.

Given the recurrence relation.

$a_n = n.a_{n-1}$, when $n \geq 1$ *and* $a_0 = 1$

The first terms of the relation are

$a_0 = 1,$

$a_1 = 1, a_0 = 1,$

$a_2 = 2, a_1 = 2.1,$

$a_3 = 3, a_2 = 3.2.1,$

$a_4 = 4, a_3 = 4.3.2.1,$

$a_5 = 5, a_4 = 5.4.3.2.1,$

Therefore, $a_n = n!$ And the solution is the discrete function a_n, which counts the number or permutations of n objects, $n \geq 0$.

We have seen the same counting principal in chapter 1 of this book in the permutations section.

14.6.5 THE SECOND – ORDER LINEAR HOMOGENEOUS RECURRENCE RELATION WITH CONSTANT COEFFICIENTS

Hear we talk about the relations of particular case in which $k = 2$, discussed in section 3.1, equation (3).

The relation of the from

$$C_n a_n + C_{n-1} a_{n-1} + C_{n-2} a_{n-2} = 0 \text{ , } n \geq 2 \qquad (8)$$

Is called the linear recurrence homogeneous relation with constant coefficients of order 2.

General Solution

As per our discussion 3.1, we found the general solution of the form

$$a_n = cr^n \qquad (9)$$

Where $c \neq 0$, $r \neq 0$.

Substituting (9) in (8) we get

$$C_n cr^n + c_{n-1} cr^{n-1} + c_{n-2} cr^{n-2} = 0 \qquad (10)$$

Which becomes

$$C_n r^2 + c_{n-1} r + C_{n-2} = 0. \qquad (11)$$

a quadratic equation of degree two called the ***characteristic equation***.

Let the roots of the characteristic equation be r_1, r_2. Then the following cases arise: roots may be

a. Distinct i.e. $r_1 \neq r_2$,
b. Complex Conjugates or
c. Equal.

Note that to determine the unique solution of a second order linear homogeneous recurrence relation with constant coefficients we need to have two initial conditions, that is the value of a_n for at least two values of n.

Case (I) Roots are Distinct

Let the distinct roots be r_1, r_2 and $r_1 \neq r_2$. Since the general solution of (8) is

$a_n = cr^n$, where r is the root of equation (10), we have

$a_n - r_1^n$ and $a_n = r_2^n$ are both solutions to (8), and linearly independent.

Therefore the general solution in this case is

$$a_n = c_1 r_1^n + c_2 r_2^n$$

Where c_1, c_2 are arbitrary constants.

Note that the solutions $a_n = r_1^n$ and $a_n = r_2^n$ linearly independent when the following condition is satisfied.

For $c_1, c_2 \in R$, if $c_1 r_1^n + c_2 r_2^n = 0$ for all $n \in N$, then $c_1 = c_2 = 0$.

We may find the unique solution by using the initial conditions and eliminating the arbitrary constants.

Example 11: Solve the recurrence relation $a_n + a_{n-1} - 6a_{n-2} = 0$, where $n \geq 2$ and $a_0 = -1$ and $a_1 = 8$.

Solution:

Given the recurrence relation

$$a_n + a_{n-1} - 6a_{n-2} = 0, \text{ where } n \geq 2 \qquad (12)$$

On substituting the general solution $a_n = cr^n$, $c,r \neq 0$ and $n \geq 2$ in (12) we obtain

$$cr^n + cr^{n-1} - 6cr^{n-2} = 0$$

and the corresponding characteristic equation is

$$r^2 + r - 6 = 0.$$

Solving the characteristic equation.

$$r^2 + r - 6 = 0$$
$$\Rightarrow (r + 3)(r - 2) = 0$$
$$\Rightarrow r = 2, -3.$$

Since we have two distinct real roots, the general solution is

$$a_n = c_1(2)^n + c_2(-3)^n$$

Where c_1 c_2 are arbitrary constants.

The arbitrary constants are determined using the initial conditions as follows:

$$-1 = a_0$$
$$= c_1(2)^0 + c_2(-3)^0$$
$$= c_1 + c_2 \quad (13)$$
$$8 = a_1$$
$$= c_1(2)^1 + c_2(-3)^1$$
$$= 2c_1 - 3c_2 \quad (14)$$

Solving (13) and (14) we find the values of the arbitrary constants as

$c_1 = 1$, $c_2 = -2$.

Case (II) Complex Roots

Let the complex roots be r_1, r_2. Since the general solution of (8) is

$a_n = cr^n$, where r is the root of equation (10),

$a_n = r_1^n$ and $a_n = r_2^n$ are both solutions to (8), and linearly independent as in the case(I). Therefore the general solution in this case is

$$a_n = c_1 r_1^n + c_2 r_2^n$$

Where c_1, c_2 are arbitrary constants.

Since r_1, r_2 are complex roots (complex conjugates), let these roots be

$r_1 = a + ib$ and $r_2 = a - ib$. now re writing the general solution we get

$$a_n = c_1(a + ib) + c_2(a - ib) \quad (15)$$

We may find the unique solution by using the initial conditions and eliminating the arbitrary constants. And the linearly independence as is case (I)

Note that the solution contains no complex numbers.

This is demonstrated in the following example.

Example 12: Solve the recurrence relation $a_n = 2(a_{n-1} - a_{n-2})$, where $n \geq 2$ and $a_0 = 1$, $a_2 = 2$.

Solution:

Let the general solution be

$a_n = cr^n$, for $c, r \neq 0$.

Substituting the solution in the given recurrence relation we get the characteristic equation.

$r^2 - 2r + 2 = 0$.

Solving the above equation we obtain the roots are

$r = 1 \pm i$.

Now we have two independent solutions $(1 + i)^n$ and $(1 - i)^n$.

Therefore the general solution is

$a_n = c_1(1 + i)^n + c_2(1 - i)^n$.

Where c_1, c_2 are arbitrary complex constants.

Using preliminary concept of complex analysis we rewrite the general solution without complex numbers and eliminate the arbitrary constants using the initial conditions as follows.

$1 + i = \sqrt{2}(\cos(\pi / 4) + i \sin(\pi / 4))$

and

$1 + i = \sqrt{2}(\cos(\pi / 4) + i \sin(\pi / 4)) = \sqrt{2}(\cos(\pi / 4) - i \sin(\pi / 4))$

These yields

$a_n = c_1(1 + i)^n + c_2(1 - i)^n$

$= c_1(\sqrt{2}(\cos(\pi / 4) + i \sin(\pi / 4)))^n + c_2(\sqrt{2}(\cos(\pi / 4) - i \sin(\pi / 4)))^n$

$= (\sqrt{2})^n(c_1(^n(\cos(n\pi / 4) + i \sin(n\pi / 4))) + c_2((\cos(n\pi / 4) - i \sin(n\pi / 4))))$

$= (\sqrt{2})^n(k_1 \cos(n\pi / 4) + k_2 \sin(n\pi / 4))$.

Where $k_1 = c_1 + c_2$ and $k_2 = (c_1 - c_2)^i$.

$1 = a_0 = k_1 \cos 0 + k_2 \sin 0 = k_1$.

$2 = a_2 = \sqrt{2}(\cos(\pi / 4) + k_2 \sin(\pi / 4)) = 1 + k_2$.

Therefore

$k_1 = 1, k_2 = 1$.

The solution for the given initial conditions is then given by

$a_2 = (\sqrt{2})^n (\cos(n\pi / 4) + \sin(n\pi / 4)), \quad n \geq 0$.

Case (III) Repeated Roots

Let the r_1, r_2 and $r_1 = r_2$, in this case we say that the root of multiplication 2. Since the general solution of (8) is $a_n = cr^n$, where r is the root if equation (10), we have $a_n = \frac{n}{2}$ are both solution to (8). But these two solutions are not linearly independent and we say

these are dependent solution since one solution is obtained from the other by just multiplying with 1, i.e. multiples of each other.

To find the general solution in this case is we need one more independent solution.

Let the independent solution be $f(n)\ r^n$ where $f(n)$ is not a constant. Substituting this into the given relation yields a general solution of the from

$$a_n = c_1 r^n + c_2 n r^n,$$

And we see this in the example below.

Example 13: Solve the recurrence relation $a_{n+2} = 4a_{n+1} - 4a_n$, where $n \geq 0$ and $a_0 = 1$, $a_1 = 3$.

Solution:

First we find the characteristic equation of the given relation by letting the general solution be $a_n = cr^n$, c, $r \neq 0$. This yields the characteristic equation

$$r^2 - 4r + 4 = 0.$$

Solving the above equation we find roots, r = 2,2 the repeated roots. Now the two dependent solutions are 2^n and 2^n.

Let the independent solution be

$$f(n)\ 2^n$$

Where $f(n)$ is not a constant.

$$f(n+2)2^{n+2} = 4\, f(n+1)2^{n+1} - 4\, f(n)2^n$$

or

$$f(n+2) = 2\, f(n+1) - f(n).$$

Assuming that the general solution is $f(n) = an + b$, for arbitrary constants a, b, with $a \neq 0$. Hear we choose $a = 1$, $b = 0$.

Therefore we find that $f(n) = n$ satisfies the above equation. So $n2^n$ is a second independent solution.

Now the general solution is of the form

$$a_n = c_1 2^n + c_2 n 2^n$$

Using the initial condition, $a_0 = 1$, $a_1 = 3$ we find that

$$a_n = 2^n + (1/2)n2^n\ ,\ n \geq 0.$$

14.6.6 THE NON-HOMOGENEOUS RECURRENCE RELATION

A general form of the non homogeneous first and second order relations are

$$a_n + C_{n-1}a_{n-1} = f(n), \qquad n \geq 1,\ C_{n-1} \neq 0. \qquad (16)$$

$$a_n + C_{n-1}a_{n-1} + C_{n-2}a_{n-2} = f(n), \qquad n \geq 2,\ C_{n-2} \neq 0. \qquad (17)5$$

Where $C_{n-1,}\ C_{n-2}$ are constants and $f(n)$ is not identically zero.

General solution

There is no general method for solving non-homogeneous relation, for certain functions $f(n)$ we shall find a successful technique.

A Special Case

When $C_{n-1} = -1$ in equation (16) we have

$a_1 = a_0 + f(1)$

$a_2 = a_1 + f(2) = a_0 + f(1) + f(2)$

$a_3 = a_2 + f(3) = a_0 + f(1) + f(2) + f(3)$

. . .

$$a_n = a_0 + f(1) + f(2) + f(3) + \ldots + f(n) = a0 + \sum_{i=1}^{i=n} f(i).$$

We can solve this type relation in terms of n, if we can find s suitable summation formula for $\sum_{i=1}^{i=n} f(i)$.

Example 14: Solve the recurrence relation $a_n - a_{n-1} = 3n^2$, where $n \geq 1$ and $a_0 = 7$.

Solution: Hear $f(n) = 3n^{2,}$ so the general solution is

$$a_n = a_0 + \sum_{i=1}^{i=n} f(i).$$

$$= 7 + 3\sum_{i=1}^{i=n} i^2.$$

$$= 7 + \frac{n(n+1)(2n+1)}{2}$$

Method of undetermined coefficients

This relies on associated homogeneous relation obtained by replacing $f(n)$ with zero.

Let $a_n^{(h)}$ denote the general solution for the associated homogenous, relation and $a_n^{(p)}$ be a solution of the given non-homogeneous relation, the term $a_n^{(p)}$ is called the particular solution. Then

$an = a_n^{(h)} + a_n^{(p)}$ is the general solution of the given relation. We use the form $f(n)$ to suggest a form for $a_n^{(p)}$

Here is the procedure to find general solution in which $f(n) = kr^n$, k is a constant. Consider the non-homogeneous first – order relation.

$$a_n + C_{n-1}a_{n-1} = kr^{n,} \quad n \geq 1,\ C_{n-1} \neq 0.$$

If rn is not a solution of the associated homogeneous relation.

$a_n + C_{n-1}a_{n-1} = 0$, then

$a_n^{(p)} = Ar^n$,

Where A is a constant. When r^n is a solution of the associated homogenous relation.

$a_n^{(p)} = Bnr^n$,

For B a constant.

Now consider the case of the non-homogeneous second – order relation

$a_n + C_{n-1}a_{n-1} + C_{n-2}a_{n-2} = kr^n, \qquad n \geq 2, C_{n-2} \neq 0$

Here we find that

a. $a_n^{(p)} = Ar^n$, A is a constant, if r^n is not a solution of the associated homogenous relation;

b. $a_n^{(p)} = Bnr^n$, B is a constant, if $a_n^{(h)} = c_1r^n + c_2r^n$, where $r_1 \neq r$; and

c. $a_n^{(p)} = Cnr^n$, C is a constant, when $a_n^{(h)} = (c_1 + c_2n)r^n$.

Example 15: Solve the recurrence relation $a_n - 3a_{n-1} = 5(7^n)$, where $n \geq 1$ and $a_0 = 2$.

Solution:

Given the non homogenous relation

$a_n - 3a_{n-1} = 5(7^n)$,

(18)

and

$f(n) = 5(7)^n$.

The corresponding homogenous relation is

$a_n - 3a_{n-1} = 0$.

(19)

Solving (19), the general solution for the homogenous relation is

$a_n^{(h)} = c(3^n)$.

Let the particular solution of (18) be

$a_n^{(p)} = c(3^n)$.

A is a constant and

$f(n) = kr^n = 5(7)^n$

Now we have

$a_n^{(h)} = A\,(7^n)$

Placing the particular solution in (18), we find that

$A(7n)- 3A(7n-1) = 5(7n), n \geq 1$

$\Rightarrow \quad 7A – 3A = 5(7)$

$\Rightarrow \quad A = 35/4,$

And

$a_n^{(p)} = (35 / 4)7n$

$= (5 / 4)^{n+1}$, $n \geq 0$.

The general solution is $a_n = c(3^n) + (5 + 4)7^{n+1}$

Using the initial condition a_0=2 now, we find the value of the arbitrary constant c,

$2= a0$

$= c + (5 / 4) (7)$

$\Rightarrow \quad c = - 27 / 4.$

Finally the unique general solution is

$an =(5/4)7^{n+1} – (1/4)(3^{n+3}), n \geq 0.$

Example 16:

Solve the recurrence relation $a_n – 3a_{n-1} = 5(3^n)$, where $n \geq 1$ and $a_0 = 2$.

Solution: Given the non homogenous relation

$a_n – 3a_{n-1} = 5(3^n),$

(20)

And

$f(n) = 5(3)^n$

(21)

The corresponding homogenous relation is

$a_n – 3a_{n-1} = 0.$

Solving (21), the general solution for the homogenous relation is

$a_n^{(h)} = c(3^n)$

Here $a_n^{(h)}$ and $f(n)$ are not linearly independent. As a result $a_n^{(p)}$ of the form $Bn(3^n)$. Substituting the particular solution in the given relation we get

$Bn(3^n) = 3B(n-1) (3^{n-1}) = 5(3^n)$

Or

$Bn – B(n-1) = 5.$

Therefore $B = 5$.

Hence

$a_n = a_n^{(h)} + a_n^{(p)} = (c + 5n)3^n$, $n \geq 0$.

With $a_0 = 2$, the general solution is

$an = (2 + 5n)3^n$

14.7 THE METHOD OF GENERATING FUNCTION

The title of this topic itself indicates that the assistance of **"Generating Function"** in solving recurrence relation is involved. Now we demonstrate the procedure to solve a given recurrence relation with the help of generating function in the following example in a systematic procedure.

Example 17: Solve the recurrence relation

$$a_{n+2} - 5a_{n+1} + 6a_n = 2,\ n \geq 0.$$
$$a_0 = 3, a_1 = 7$$

Step 1

Multiply the given relation by x^{n+2}, because $n+2$ is largest subscript in the relation. This gives us

Step 2

Sum all the equations represented by the result in step (1) and we get

$$\sum_{n=0}^{\infty} a_{n+2}\, x^{n+2} - 5\sum_{n=0}^{\infty} a_{n+1}\, x^{n+2} + 6\sum_{n=0}^{\infty} a_n\, x^{n+2} = 2\sum_{n=0}^{\infty} x^{n+2}$$

Step 3

In order to have each of the subscripts on a match the corresponding exponent on x, we rewrite the equation in step (2) as

$$\sum_{n=0}^{\infty} a_{n+2}\, x^{n+2} - 5x\sum_{n=0}^{\infty} a_{n+1}\, x^{n+1} + 6x_2\sum_{n=0}^{\infty} a_n\, x^n = 2x^2\sum_{n=0}^{\infty} x^n$$

Step 4

Let $f(x) = \sum_{n=0}^{\infty} a_n\, x^n$ be the generating function for the solution. The equation in step (3) now takes the form

$$\left(f(x) - a_0 - a_1 x - 5x\right)\left(f(x) - a_0 + 6x^2\right) f(x) = \frac{2x^2}{1-x}$$

Or

$$\left(f(x) - 3 - 7x - 5x\right)\left(f(x) - 3 + 6x^2\right) f(x) = \frac{2x^2}{1-x}$$

Step 5

Solving for $f(x)$ we have

$$\left(1 - 5x + 6x^2\right) f(x) = 3 - 8x + \frac{2x^2}{1-x}$$
$$= \frac{3 - 11x + 10x^2}{1-x}$$

Form which it follows that

$$f(x) = \frac{3-11x+10x^2}{\left(1-5x+6x^2\right)(1-x)}$$

$$= \frac{(3-5x)(1-2x)}{(1-3x)(1-2x)(1-x)}$$

$$= \frac{3-5x}{(1-3x)(1-x)}$$

Partial fraction decomposition gives us

$$f(x) = \frac{2}{1-2x} + \frac{1}{1-x}$$

$$= 2\sum_{n=0}^{\infty}(3x)^n + \sum_{n=0}^{\infty}(x)^n$$

Consequently, $a_n = 2(3^n) + 1$, $n \geq 0$,

Check your progress:

1. The number of bacteria in a culture is 1000, and this number increases 250% every two hours. Use a recurrence relation to determine the number of bacteria present after one day.

2. If a person invests Rs.100 at 6% interest compounded quarterly, how many months, must he wait for his money to double? (He cannot withdraw his money before the quarter is up.)

3. A person invested the stock profits he received 15 years ago in an account that paid 8% interest compounded quarterly. If his account now had Rs.7218.27 in it, what was his initial investment?

4. Using generating functions solve the recurrence relation

   $a_n - 3a_{n-1} = n$, $n \geq 0$, $a_0 = 1$.

5. Solve the recurrence relation

   $a_{n+2} = a_{n+1} + a_n$, $n \geq 0$, $a_0 = 0$, $a_1 = 1$

6. Solve the recurrence relation

   $a_{n+2} - 4a_n + 3a_n = -200$, $n \geq 0$, $a_0 = 3000$, $a_1 = 3300$.

14.8 LET SUM UP:

In this chapter, we have learnt the following.

- Sequences and series.
- Generating function and Example base on Binomial and Maclaurin series.
- A recurrence relation is a relation among the sequence (a_n), n = 0, 1, 2, …, of the form $f(n, a_1, a_2, \ldots, a_n) = 0$ for all $n \geq k$.
- A linear homogenous recurrence relation of the form,

  $$a_n = \alpha a_{n-1}$$

  is called the first order homogenous linear recurrence relation, where α is a constant.
- The general solution of the recurrence relation $a_n = \alpha a_{n-1}$ where α is a constant, $n \geq 1$, and $a_0 = A$, is unique and is given by $a_n = A\alpha^n$.
- A general form of the non homogenous first and second order relation are

  $$a_n + C_{n-1}a_{n-1} = f(n),\ n \geq 1,\ C_{n-1} \neq 0$$

  $$a_n + C_{n-1}a_{n-1} + C_{n-2}a_{n-2} = f(n), \qquad n \geq 2,\ C_{n-2} \neq 0,$$

  Where $C_{n-1}C_{n-2}$ is constants and $f(n)$ is not identically zero.
- Solving various recurrence relations and the method of generating function.

14.9 UNIT END EXERCISE:

1. Determine the coefficient x^7 of generating function $(1+3x)^{-9}$.
2. Solve $a_r - a_{r-1} - a_{r-2} = -30$ given $a_0 = 20, a_1 = -5$.
3. Solve $a_r - 2a_{r-1} + a_{r-2} = 0$.
4. Solve $a_r - 2a_{r+1} + a_{r+2} = 3$ with $a_0 = 2, a_1 = 5$.
5. Solve the recurrence relation $a_n+a_{n-1}-6a_{n-2}=0$, $n\geq 2$, and $a_0=-1$ and $a_1=8$.
6. Solve the recurrence relation $a_{n+2}=4a_{n+1}-4a_n$ for $n\geq 2$, $a_0=1$, $a_1=3$.
7. Solve the recurrence relation $a_n-3a_{n-1}=5(7^n)$ for $n\geq 1$ and $a_0=2$.
8. Solve the recurrence relation $a_n-3a_{n-1}=5(3^n)$ for $n\geq 1$ and $a_0=2$.
9. Solve the relation $a_{n+2}-5a_{n+1}+6a_n=2$, $n\geq 0$, $a_0=3$, $a_1=7$.
10. Determine the coefficient x^6 of generating function $(1-5x)^8$.

14.10 REFERENCES:

1. Discrete structures by Liu.
2. Discrete mathematics its Application, Keneth H. Rosen TMG.
3. Discrete structures by B. Kolman HC Busby, S Ross PHI Pvt. Ltd.
5. Discrete mathematics, schaum's outlines series, seymour Lip Schutz, Marc Lipson, TMG.