UNIT- 1 :

LECTURE NO 01

KEYWORDS : Set, Roaster Form, Tabular Form, Set Builder Form
Integers, Whole numbers, Real numbers, Rational numbers, complex numbers, Cardinality, Subset, Interval

Set Theory [R1]

- The theory of sets was developed by German Mathematician "George Canter".

Set [R1, R2]

- A well defined collection of distinct objects is called a Set.
- The objects in a set are called its members or elements.
- We denote sets by Capital Letters, A, B, C, X, Y, Z ... etc.
- The elements of a set are also represented by small letters. a, b, c, x, y, z ... etc.
- If 'a' is an element of a set A, we write $\boxed{a \in A}$ i.e. 'a' belongs to A or 'a' is an element of A.
- If 'a' does not belong to A, it cannot be written as $a \in A$, instead it is denoted as $\boxed{a \notin A}$.
- As mentioned, a set is defined as a 'well defined' collection of objects. By 'well defined' we mean that there exits a rule which helps us in deciding whether a given object belongs to the collection or not.

Principle of Extension [R2]

- Two sets are equal if they contain the same elements, i.e the sets A and B are equal if every element x of A is an element of B and every element y of B is an element of A.
- In such a case, denotion is $\boxed{A = B}$
- Example

① $A = \{a, b, c, d\}$
$B = \{a, b, c, d\}$

*② $A = \{a, b, c, d\}$
$B = \{a, c, b, d\}$

NOTE: * Order of element is not important.

Representation of a Set [R1, R2]

Set Representation

- 1. ROSTER OR TABULAR FORM
- 2. SET BUILDER OR RULE METHOD

1. Roaster or Tabular Form

- In this form, all the elements of a set are listed within braces { } and are seperated by commas.
- Example:

Q. Write the following sets in a Roaster Form

① A = Set of all factors of 12
$\therefore A = \{1, 2, 3, 4, 6, 12\}$

② B = Set of all letters in the word 'Mathematics'
$\therefore$ *$B = \{M, A, T, H, E, I, C, S\}$

NOTE: * The repeated elements are considered only once

2. Set Builder Form or Rule Method

- In this method, a set is defined by specifying a property that elements of the set have in common.
- It is written as $\boxed{A = \{x : x \text{ satisfies the property } P\}}$

i.e. $\underbrace{\text{A is the set of } x}_{\text{set of all } x}$ such that each x satisfies property P.

- Example:

① Write the set $A = \{1,2,3,4,5,6,7,8\}$ in the set-builder form, we have A = set of all natural nos. less than 9.

$\therefore A = \{x ; x \in N \text{ and } x < 9\}$

② Redefine each of the foll. sets using set-builder notation

(a) $A = \{-2,-4,-6, \ldots\}$

$\therefore A = \{x : x = -2n \text{ for all } n \in N\}$

(b) $B = \{0, 3, -3, 6, -6, 9, \ldots\}$

$\therefore B = \{x : x = 3n \text{ for } n \in Z\}$

(c) $C = \{2,3,4,6,8,9,10,12,14,15, \ldots\}$

$\therefore C = \{x : x = 2n \text{ or } x = 3n \text{ for } n \in N\}$

(d) $D = \{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots\}$

$\therefore D = \{x : x = \frac{1}{n} \text{ for } n \in N\}$

(e) $E = \{0, 1, 2, \ldots, 100\}$

$\therefore E = \{x : 0 \leq x \leq 100 \text{ and } x \in Z\}$

Important Sets [R2]

1. N = Set of Positive integers $= Z^+$
   $= \{1, 2, 3, 4, \cdots\}$

2. Z = Set of all integers
   $= \{\cdots, -2, -1, 0, 1, 2, \cdots\}$

3. W = Set of all whole nos.
   $= \{0, 1, 2, 3, 4, \cdots\}$

4. R = Set of Real nos. = Whole nos + Rational nos. + Irrational nos.
   $= \{1, 12.38, -0.8625, \frac{3}{4}, \sqrt{2}, 198\}$

5. Q = Set of Rational nos.
   $= \{5, 1.75, 0.001, -0.1, 0.111\cdots\}$

6. C = Set of Complex nos.
   $= \{1+i, 39+3i, 0.8-2.2i, -2+\pi i, \sqrt{2}+i/2 \cdots\}$

References:
1. Liu and Mohapatra, "Elements of Discrete Mathematics", McGraw Hill.
2. Jean Paul Trembly, R Manohar, "Discrete Mathematical Structures with Application to Computer Science", Mc Graw Hill

UNIT 1 :

KEYWORDS :
set, subset, cardinality

LECTURE NO 02

Cardinal Number of a Set / Cardinality of a Set [R2]

- The no. of distinct elements containing in a finite set A is called Cardinal Number of A.
- Denoted by $\boxed{n(A).}$.
- Example:

Q. Find the cardinality of $A = \{2, 3, 5\}$

$\therefore \boxed{n(A) = 3}$

Types of Sets [R1, R2]

1. UNIVERSAL SET

- In any particular application of Set Theory, all the sets under investigation are likely to be considered as subsets of a particular set.
- This set is called the Universal Set or Universe of Discourse
- Denoted by 'U'.

2. EMPTY SET

- The set with no element is called the Empty Set or Null Set.
- Denoted by 'ϕ' or '$\{\ \}$'

3. NON EMPTY SET

- A set which has atleast one element is called a Non-Empty Set.
- Example: $A = \{16\}$

$A = \{4, 8, 16\}$

4. SINGLETON SET

- A set containing exactly one element is called Singleton Set.
- Example:

a) $\{0\}$ is a singleton set whose element is 0.

b) $\{x : x \in N \text{ and } x^2 - 9 = 0\}$ is a singleton set whose value is $\{3\}$.

5. FINITE SET

- A set is said to be finite if it consists of only finite numbers of elements.
- The number of distinct elements in a finite set A is denoted by $\underbrace{n(A)}_{\text{Cardinality}}$
- Example:

a) $A = \{2, 4, 6, 8, 10\}$. A is a finite set and $n(A) = 5$.

b) The set of all students in 2B.

c) The set of all family members in Building.

6. INFINITE SET

- A set which is not finite is called an Infinite Set
- Example:

a) The set of all points on the arc of a circle.

b) The set of all positive integers, multiple of 5.

c) P = set of all prime numbers

$= \{2, 3, 5, 7, 11, 13, \ldots\}$

Scanned by CamScanner

7. EQUAL SETS

- Two sets A and B are said to be equal, if they have exactly the same elements.
- Denoted by $\boxed{A = B}$.
- If the sets A and B are not equal, then $\boxed{A \neq B}$.
- The elements of a set may be listed in <u>any order</u>, i.e. $\{1,2,3\} = \{2,1,3\} = \{3,2,1\}$ etc.
- The repetion of elements in a set has no meaning. i.e. $\{1,2,3\} = \{1,1,2,3,2\} = \{1,1,1,2,2,3,3,3\}$ etc.

8. EQUIVALENT SETS

- Two finite sets A and B are said to be equivalent if $\boxed{n(A) = n(B)}$.
- Example:

  $A = \{2,3,4\}$ $\quad B = \{7,8,9\}$

  $n(A) = 3$ $\quad n(B) = 3$ $\quad$ ie $\boxed{n(A) = n(B) = 3}$

  $\therefore$ A and B are equivalent.

  But $A \neq B$.

9. DISJOINT SET

- Two sets A and B are said to be disjoint if $\boxed{A \cap B = \phi}$.
- Example:

  $A = \{1,3,5,7,9\}$ $\quad B = \{2,4,6,8\}$

  $A \cap B = \phi$

  $\therefore$ A and B are Disjoint sets.

10. INTERSECTING SETS

- Two sets A and B are said to be intersecting if they are not disjoint.
- Denoted by $\boxed{A \cap B \neq \phi}$
- Example:

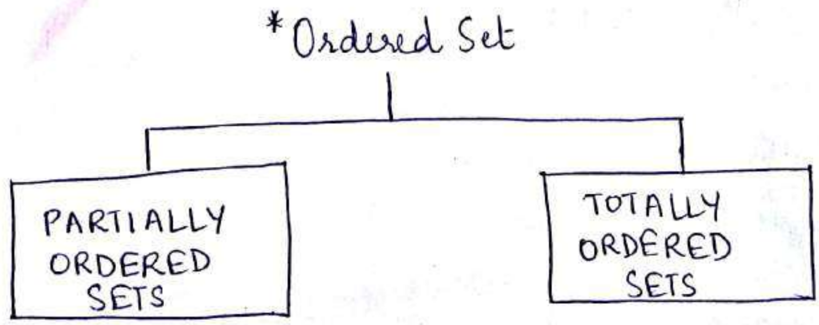
  $A = \{1, 3, 5, 7, 9\}$ $B = \{2, 3, 5, 7, 11\}$

  $A \cap B = \{3, 5, 7\} \neq \phi$

  $\therefore$ A and B are intersecting sets.

11. ORDERED SET

- We define Set as an Unordered Collection of Distinct objects.
- But while entering the elements, if the sequence has some relevance, then the set is said to be an Ordered Set.
- An ordered set is defined as Ordered Collection of Distinct Objects.



12. SUBSET

- A set A is said to be subset of set B, if every element of A is also an element of B.
- Denoted by $\boxed{A \subseteq B}$.
- Example: $A = \{2\}$ $B = \{2, 3\}$ $\therefore A \subseteq B$

NOTE: *If $n(A) = m$, then total no. of Subsets $= 2^m$

13. SUPERSET

- If $A \subseteq B$, then B is called a Superset of A.
- Denoted by $\boxed{B \supseteq A}$
- Example:

  $A = \{2\}$, $B = \{2,3\}$

  Here $A \subseteq B$ and $B \supseteq A$

14. POWER SET

- The set of all subsets of a given set A is called Power Set of A.
- Denoted by 'P(A)'

NOTE: If $n(A) = m$, then $n[P(A)] = 2^m$

References:

1. Liu and Mohapatra, "Elements of Discrete Mathematical", McGraw Hill
2. Jean Paul Trembley, R Manohar, "Discrete Mathematical Structures with Application to Computer Science", McGraw Hill

UNIT 01

LECTURE NO 03

KEYWORDS: Union, Intersection, Difference, Symmetric Difference, Compliment, Ordered Pair, Cartesian Product, Set Laws

Operations on Sets [R1, R2]

1. Union of Sets

- Union of two sets A and B is denoted by $\boxed{A \cup B}$.
- Defined as the set of all those elements which are either in A or in B or in both A and B.
- Example:

$A = \{2, 3, 5, 7\}$ $B = \{1, 2, 4, 8\}$

$\therefore \boxed{A \cup B = \{1, 2, 3, 4, 5, 7, 8\}}$

2. Intersection of Sets

- Intersection of two sets A and B is denoted by $\boxed{A \cap B}$.
- Defined as the set of all those elements which are common to both A and B.
- Example:

$A = \{1, 3, 5, 7, 9\}$ $B = \{2, 3, 5, 7, 11, 13\}$

$\therefore \boxed{A \cap B = \{3, 7, 5\}}$

3. Difference of Sets

- For any sets A and B, their difference is denoted by $\boxed{A - B}$.
- Defined by $\boxed{(A - B) = \{x : x \in A \text{ and } x \notin B\}}$
- Example:

$A = \{1, 2, 3, 6\}$ $B = \{1, 2, 4, 8\}$

$\boxed{\begin{array}{l} A - B = \{3, 6\} \\ B - A = \{4, 8\} \end{array}}$

4. Symmetric Difference of Sets

- For any sets A and B, their symmetric difference is denoted by

$$\boxed{\begin{array}{c} A \Delta B = (A-B) \cup (B-A) \\ \text{OR} \\ A \otimes B = (A-B) \cup (B-A) \end{array}}$$

- Example:

$A = \{-2, 0, 1, 2\}$ $B = \{1, 2, 3, 4\}$

$$A \otimes B = \{(A-B) \cup (B-A)\}$$
$$= \{(-2, 0) \cup (3, 4)\}$$
$$\therefore \boxed{A \otimes B = \{-2, 0, 3, 4\}}$$

5. Complement of Set

- Let U be the Universal Set and let $A \subseteq U$, then, the compliment of A is denoted by $\boxed{A' \text{ or } (U-A)}$.
- Defined by $\boxed{A' = \{x \in U : x \notin A\}}$
- Example:

$U = \{1, 2, 3, 4, 5, 6, 7, 8\}$ $A = \{2, 4, 6, 8\}$

$$\therefore \boxed{A' = \{1, 3, 5, 7\}}.$$

and $(A')' = \{2, 4, 6, 8\}$
$= A$

$$\boxed{\therefore (A')' = A}$$

Scanned by CamScanner

UNIT 01

LECTURE NO 3.A [R3, R4]

Q1. Let $A=\{1,3,5,7,9\}$ and $B=\{2,3,5,7,11,13\}$. Find $A\cap B$.

Solⁿ: $A\cap B = \{1,3,5,7,9\} \cap \{2,3,5,7,11,13\}$

$\boxed{A\cap B = \{3,5,7\}}$

Q2. If $A=\{1,3,5,7,9\}$, $B=\{2,4,6,8\}$ & $C=\{2,3,5,7,11\}$
Find $A\cap B$ and $A\cap C$. What do you conclude?

Solⁿ: We have $A\cap B = \{1,3,5,7,9\} \cap \{2,4,6,8\}$

$\boxed{A\cap B = \phi} \Rightarrow$ A & B are Disjoint Sets

and $A\cap C = \{1,3,5,7,9\} \cap \{2,3,5,7,11\}$

$\boxed{A\cap C = \{3,5,7\} \neq \phi} \Rightarrow$ A & C are Intersecting sets.

Q3. If $A=\{a,b,c,d,e,f\}$, $B=\{c,e,g,h\}$ & $C=\{a,e,m,n\}$

Find (i) $A\cup B$ (ii) $B\cup C$ (iii) $A\cup C$ (iv) $B\cap C$ (v) $C\cap A$ (vi) $A\cap B$

Solⁿ: (i) $A\cup B = \{a,b,c,d,e,f\} \cup \{c,e,g,h\}$

$\boxed{A\cup B = \{a,b,c,d,e,f,g,h\}}$

(ii) $B\cup C = \{c,e,g,h\} \cup \{a,e,m,n\}$

$\boxed{B\cup C = \{a,c,e,g,h,m,n\}}$

(iii) $A\cup C = \{a,b,c,d,e,f\} \cup \{a,e,m,n\}$

$\boxed{A\cup C = \{a,b,c,d,e,f,m,n\}}$

(iv) $B \cap C = \{c, e, g, h\} \cap \{a, e, m, n\}$

$\boxed{B \cap C = \{e\}}$

(v) $C \cap A = \{a, e, m, n\} \cap \{a, b, c, d, e, f\}$

$\boxed{C \cap A = \{a, e\}}$

(vi) $A \cap B = \{a, b, c, d, e, f\} \cap \{c, e, g, h\}$

$\boxed{A \cap B = \{c, e\}}$

Q4. If $A = \{x : x \in N, x \text{ is a factor of } 6\}$ and
$B = \{x : x \in N, x \text{ is a factor of } 8\}$

Then find (i) $A \cup B$ (iii) $A - B$

(ii) $A \cap B$ (iv) $B - A$

Solⁿ: We have

$A = \{x : x \in N, x \text{ is a factor of } 6\}$

$\therefore \boxed{A = \{1, 2, 3, 6\}}$

$B = \{x : x \in N, x \text{ is factor of } 8\}$

$\therefore \boxed{B = \{1, 2, 4, 8\}}$

i) $A \cup B = \{1, 2, 3, 6\} \cup \{1, 2, 4, 8\}$

$\boxed{A \cup B = \{1, 2, 3, 4, 6, 8\}}$

ii) $A \cap B = \{1, 2, 3, 6\} \cap \{1, 2, 4, 8\}$

$\boxed{A \cap B = \{1, 2\}}$

iii) $A - B = \{1, 2, 3, 6\} - \{1, 2, 4, 8\}$

$\boxed{A - B = \{3, 6\}}$

iv) $B - A = \{1, 2, 4, 8\} - \{1, 2, 3, 6\}$

$\boxed{B - A = \{4, 8\}}$

Q5. If $U = \{1,2,3,4,5,6,7,8,9\}$, $A = \{2,4,6,8\}$ & $B = \{2,3,5,7\}$.
Verify that

(i) $(A \cup B)' = (A' \cap B')$

(ii) $(A \cap B)' = (A' \cup B')$

Sol^n: We have

$U = \{1,2,3,4,5,6,7,8,9\}$

$A = \{2,4,6,8\}$

$B = \{2,3,5,7\}$

$\therefore \; A' = U - A = \{1,2,3,4,5,6,7,8,9\} - \{2,4,6,8\}$

$$\boxed{A' = \{1,3,5,7,9\}}$$

$B' = U - B = \{1,2,4,5,6,7,8,9\} - \{2,3,5,7\}$

$$\boxed{B' = \{1,4,6,8,9\}}$$

Algebra of Set Theory [R1, R2]

LAWS OF ALGEBRA OF SETS

1.	Commutative Law	(a) $A \cup B = B \cup A$ (b) $A \cap B = B \cap A$
2.	Associative Law	(a) $(A \cup B) \cup C = A \cup (B \cup C)$ (b) $(A \cap B) \cap C = A \cap (B \cap C)$
3.	Idempotent Law	(a) $A \cup A = A$ (b) $A \cap A = A$
4.	Distributive Law	(a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
5.	Identity Law	(a) $A \cup \phi = A$ (b) $A \cap U = A$ (c) $A \cup U = U$ (d) $A \cap \phi = \phi$
6.	Involution Law	$(A')' = A$
7.	Complement Law	(a) $A \cup A' = U$ (b) $A \cap A' = \phi$ (c) $U' = \phi$ (d) $\phi' = U$
8.	DeMorgan's Law	(a) $(A \cup B)' = A' \cap B'$ (b) $(A \cap B)' = A' \cup B'$

* PROOFS OF LAWS

* SET IDENTITIES.

Ordered Pair [R1]

- An ordered pair (a,b) is built from two objects, a and b.
- As the name suggests, the "order" matters.
- $(a,b) \neq (b,a)$, unless $a=b$.
- For two ordered pairs (a,b) & (c,d), $(a,b) = (c,d)$ iff $a=c$ and $b=d$.
- If we are allowed to choose 'a' from the set A and 'b' from the set B, then the set of all possible ordered pairs that we can create is called the Product Set or the Cartesian Product.

Cartesian Product of Sets [R1]

- Also called as Cross Product or Direct Product.
- Let A and B be two sets, then the cartesian product is denoted by $\boxed{A \times B}$.
- It is the set of all possible ordered pairs whose first component is an element of A and second component is an element of B.

ie. $\boxed{A \times B = \{(a,b) : a \in A \text{ and } b \in B\}}$

- Example:

$A = \{x, y\}$ and $B = \{a, b, c\}$

$A \times B = \{x, y\} \times \{a, b, c\}$

$\boxed{A \times B = \{(x,a), (x,b), (x,c), (y,a), (y,b), (y,c)\}}$

Properties of Cartesian Product [R1, R2]

- For four sets A, B, C and D

(i) $(A \cap B) \times (C \cap B) = (A \times C) \cap (B \times D)$

(ii) $(A - B) \times C = (A \times C) - (B \times C)$

(iii) $(A \cup B) \times C = (A \times C) \cup (B \times C)$

(iv) $A \times (B \cap C) = (A \times B) \cap (A \times C)$

Principle of Duality [R3, R4]

- The principle of duality states that any established result involving sets and complements and operations of union and intersection gives a corresponding dual result by replacing $\cup$ by ϕ and $\cup$ by $\cap$ and vice versa.

UNIT 01

LECTURE NO 3.B

Using the Laws of the Algebra of Sets, prove the laws using definitions. [R3,R4]

1. IDEMPOTENT LAW

(a) $A \cup A = A$

Let x be any arbitrary element of the set A.

ie $x \in A$

So, $x \in A \Rightarrow x \in A$ or $x \in A$

$\Rightarrow x \in A \cup A$

$\therefore A \subseteq (A \cup A)$ ——— (I)

Similarily,

if $x \in (A \cup A) \Rightarrow x \in A$ or $x \in A$

$\Rightarrow x \in A$

$\therefore (A \cup A) \subseteq A$ ——— (II)

From (I) & (II), we get $\boxed{A \cup A = A}$

(b) $A \cap A = A$

Let x be any arbitrary element of set A

ie $x \in A$

So, $x \in A \Rightarrow x \in A$ and $x \in A$

$\Rightarrow x \in A \cap A$

$\therefore A \subseteq (A \cap A)$ ——— (I)

Similarily, $(A \cap A) \subseteq A$ ——— (II)

From (I) & (II), we get $\boxed{A \cap A = A}$

2. ASSOCIATIVE LAW

(a) $(A \cup B) \cup C = A \cup (B \cup C)$

Let x be any arbitary element.

ie $x \in (A \cup B) \cup C$

So, $x \in (A \cup B) \cup C \Rightarrow x \in (A \cup B)$ or $x \in C$

$\Rightarrow (x \in A$ or $x \in B)$ or $x \in C$

$\Rightarrow x \in A$ or $(x \in B$ or $x \in C)$

$\Rightarrow x \in A$ or $x \in (B \cup C)$

$\Rightarrow x \in A \cup (B \cup C)$ ——— (I)

Similarily, $x \in A \cup (B \cup C)$

$x \in A \cup (B \cup C) \Rightarrow x \in A$ or $x \in (B \cup C)$

$\Rightarrow x \in A$ or $(x \in B$ or $x \in C)$

$\Rightarrow (x \in A$ or $x \in B)$ or $x \in C$

$\Rightarrow x \in (A \cup B)$ or $x \in C$

$\Rightarrow x \in (A \cup B) \cup C$ ——— (II)

From (I) & (II), we get

$$\boxed{(A \cup B) \cup C = A \cup (B \cup C)}$$

(b) $(A \cap B) \cap C = A \cap (B \cap C)$

The above law can be proved using the similar identities.

3. COMMUTATIVE LAW

(a) $A \cup B = B \cup A$

Let x be any arbitary element such that $x \in (A \cup B)$

ie $x \in (A \cup B)$

So, $x \in (A \cup B) \Rightarrow x \in A$ or $x \in B$

$\Rightarrow x \in B$ or $x \in A$

$\Rightarrow x \in (B \cup A)$

$\therefore (A \cup B) \subseteq (B \cup A)$ ——— (I)

Similarily, $x \in (B \cup A) \Rightarrow x \in B$ or $x \in A$

$\Rightarrow x \in A$ or $x \in B$

$\Rightarrow x \in (A \cup B)$

$\therefore (B \cup A) \subseteq (A \cup B)$ ——— (II)

From (I) & (II), we get $\boxed{A \cup B = B \cup A}$.

(b) $A \cap B = B \cap A$

Let x be any arbitairy element such that $x \in (A \cap B)$

ie. $x \in (A \cap B)$

So, $x \in (A \cap B) \Rightarrow x \in A$ and $x \in B$

$\Rightarrow x \in B$ and $x \in A$

$\Rightarrow x \in (B \cap A)$

$\therefore (A \cap B) \subseteq (B \cap A)$ ——— (I)

Similairly $x \in (B \cap A) \Rightarrow x \in B$ and $x \in A$

$\Rightarrow x \in A$ and $x \in B$

$\Rightarrow x \in (A \cap B)$

$\therefore (B \cap A) \subseteq (A \cap B)$ ——— (II)

From (I) & (II), we get $\boxed{(A \cap B) = (B \cap A)}$

4. DISTRIBUTIVE LAWS

(a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Let x be any arbitrary element such that $x \in [A \cup (B \cap C)]$

So, $x \in [A \cup (B \cap C)] \Rightarrow x \in A$ or $x \in (B \cap C)$

$\Rightarrow x \in A$ or ($x \in B$ and $x \in C$)

$\Rightarrow$ ($x \in A$ or $x \in B$) and ($x \in A$ or $x \in C$)

$\Rightarrow x \in (A \cup B)$ and $x \in (A \cup C)$

$\Rightarrow x \in (A \cup B) \cap (A \cup C)$

$\therefore A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ —— (I)

Similarily $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$ —— (II)

From (I) & (II), we get

$$\boxed{A \cup (B \cap C) = (A \cup B) \cap (A \cup C)}$$

Similarily (b) $\boxed{A \cap (B \cup C) = (A \cap B) \cup (A \cap C)}$

References:

1. Y. N. Singh, "Discrete Mathematics", Wiley India, New Delhi, First Edition, August 2010.
2. Biswal, "Discrete Mathematics and Graph Theory", PHI.
3. PDF: Sets and Set Operations, "https://people.cs.pitt.edu
4. PDF: Set Operations, "www.maths.manchester.ac.uk

UNIT 01

LECTURE NO. 04

KEYWORDS:
Multiset, Multisubset, Venn Diagrams, Partition of sets

Multiset [R1]

- A collection of object that are not necessarily distinct, is called a Multiset.

Multiplicity of an Element [R1]

- The number of times an element appears in the multiset is called the Multiplicity of that element.
- In fact, we can categorize a pair (A, μ), where A is the generic set and μ is the multiplicity function defined as

$$\mu : A \rightarrow \{1, 2, 3, \ldots\}$$

so that $\mu(a) = k$, where k is the number of times the element is in the multiset.

- Example:

(1) $A = \{a, b, c, c, a, c\}$

then $\mu(a) = 2$
$\mu(b) = 1$
$\mu(c) = 3$

(2) $B = \{a, a, a, b, b, d, d, d, d, e\}$

then $\mu(a) = 3$
$\mu(b) = 2$
$\mu(c) = 0$
$\mu(d) = 4$
$\mu(e) = 1$

Equality of Multiset [R1]

- If the number of occurence of each element is the same in both the multiset, then the multiset are equal.
- Example: $\{a, b, a, a\} = \{a, a, b, a\}$

But $\{a, b, a\} \neq \{a, b\}$

Multisubset [R1]

- A multiset P is said to be a multisubset of Q, if multiplicity of each element in P is less or equal to its multiplicity in Q

- Example: $[1,2,2,3] \subseteq [1,1,1,2,2,3]$

Operations on Multiset [R1]

1] Intersection of Multisets

- If P and Q are multisets, then $P \cap Q$ is defined as the multiset such that for each element $x \in P \cap Q$,

$$\boxed{\mu(x) = \min\{\mu_P(x), \mu_Q(x)\}}$$

- Example: $P = \{1,1,1,2,2,3\}$, $Q = \{1,2,2,2,3,3\}$

$$\therefore \boxed{P \cap Q = \{1,2,2,3\}}$$

2] Union of Multisets

- If P and Q are multisets, then $P \cup Q$ is defined as the multiset such that for each element $x \in P \cup Q$,

$$\boxed{\mu(x) = \max\{\mu_P(x), \mu_Q(x)\}}$$

- Example: $P = \{a,b,b,c\}$, $Q = \{b,c,c,d\}$

$$\boxed{P \cup Q = \{a,b,b,c,c,d\}}$$

3] Difference of Multisets

- Let P and Q be two multisets, then P-Q is defined as the multiset such that for each element $x \in P-Q$,

$$\boxed{\mu(x) = \mu_P(x) - \mu_Q(x)}$$

- Example: $P = \{a,a,a,a,b,b,c,d\}$, $Q = \{a,a,b,d,e\}$

$$\boxed{P-Q = \{a,a,b,c\}}$$

4] Sum of Multisets

- This concept is not defined on Ordinary Set.
- However, for multiset P and Q, we define (A + B) as

$$x \in A+B \Rightarrow \boxed{\mu(x) = \mu_A(x) + \mu_B(x)}$$

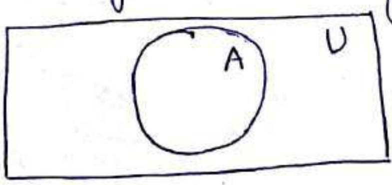
- Example:

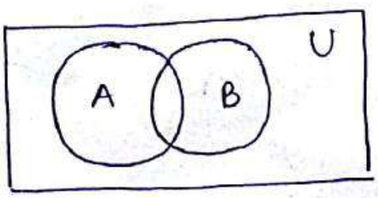
$P = \{a, a, b, b, b, c\} \quad Q = \{a, a, a, b, c, c, d, e\}$

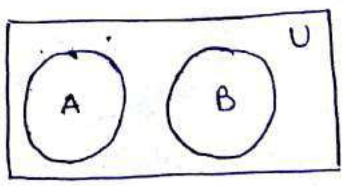
$$\boxed{P + Q = \{a, a, a, a, a, b, b, b, b, c, c, c, d, e\}}$$

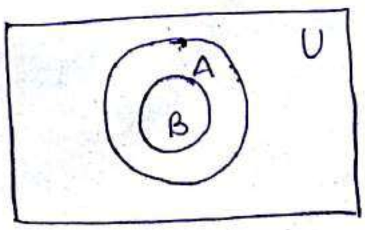
Venn Diagrams [R1]

- In order to express the relationship among sets in perspective, we represent them pictorically by means of diagrams, called Venn Diagram.
- In these diagrams, the Universal Set is represented by a Rectangular Region and its subsets by Circles inside the rectangle.
- We represent disjoint sets by Disjoint Circles and intersecting sets by Intersecting Circles.

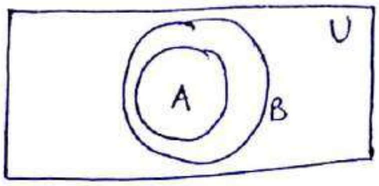
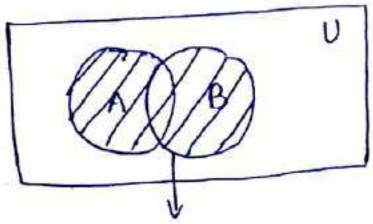
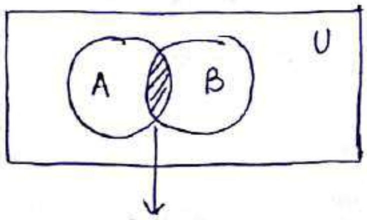
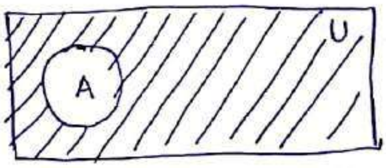
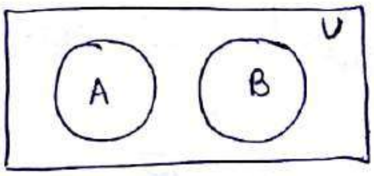
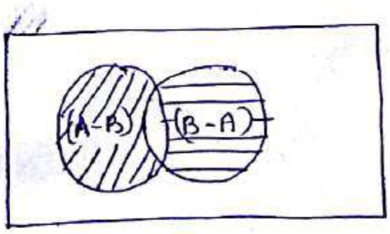








Operations on Venn Diagrams [R1]

SR. NO.	OPERATIONS ON VENN DIAGRAMS	RERESENTATION
1.	Set Inclusion Operation - If A is a proper subset of B	
2.	Union of Two Sets	 A ∪ B
3.	Intersection of Two Sets	 A ∩ B
4.	Complement of a Set	
5.	Disjoint Sets	
6.	Subtraction of Sets	

LECTURE NO. 4.A [R2]

- For a Venn Diagram, the following Laws hold true:

1. $n(A \cup B) = n(A) + n(B) - n(A \cap B)$
2. $n(A \cup B) = n(A) + n(B)$ [when A & B are DISJOINT]
3. $n(A - B) + n(A \cap B) = n(A) \Rightarrow n(B - A) = n(A \cup B) - n(A)$
4. $n(B - A) + n(A \cap B) = n(B)$
5. $n(A - B) + n(A \cap B) + n(B - A) = n(A \cup B)$

Q. Show that for any two sets A and B

$$A - (A \cap B) = A - B$$

Sol^n: Let $x \in A - (A \cap B)$

$\Rightarrow x \in A$ and $x \notin (A \cap B)$

$\Rightarrow x \in A$ and $(x \notin A$ or $x \notin B)$

$\Rightarrow (x \in A$ and $x \notin A)$ or $(x \in A$ and $x \notin B)$

$\Rightarrow (x \in \phi)$ or $(x \in A - B)$

$\Rightarrow x \in \phi$ or $x \in (A - B)$

$\Rightarrow x \in \phi \cup (A - B)$

$\Rightarrow x \in (A - B)$

$\therefore \boxed{A - (A \cap B) = A - B}$ —— (I)

Again let $x \in (A - B)$

$\Rightarrow x \in A$ and $x \notin B$

$\Rightarrow x \in A$ and $x \notin (A \cap B)$

$\Rightarrow x \in A - (A \cap B)$

$\Rightarrow x \in A - (A \cap B)$

$\therefore \boxed{(A - B) \subseteq A - (A \cap B)}$ —— (II)

From (I) & (II), we get $\boxed{A - (A \cap B) = A - B}$

Q. In a group of 60 people, 40 speak Hindi, 20 speak both English and Hindi and all people speak at least one of the two languages. How many people speak only English and not Hindi? How many speak English?

Solⁿ: Let A = set of Hindi speaking
B = set of English speaking

$\therefore n(A) = 40, \; n(A \cap B) = 20, \; n(A \cup B) = 60$

$\therefore$ no. of people that speak only English and not Hindi is

$$n(B-A) = n(A \cup B) - n(A)$$
$$= 60 - 40$$
$$\therefore \boxed{n(B-A) = 20}$$

$\therefore$ no. of people that speak English

$$n(B) = n(B-A) + n(A \cap B)$$
$$= 20 + 20$$
$$\therefore \boxed{n(B) = 40}$$

Q. A class has 175 students. The following description gives the number of students studying one or more of the subjects in the class.

Mathematics = 100
Physics = 70
Physics & Chemistry = 46
Mathematics & Physics = 30
Mathematics & Chemistry = 20
Physics & Chemistry = 23
Mathematics, Physics & Chemistry = 18

Find:

(i) How many students are enrolled in Mathematics alone, Physics alone & Chemistry alone?

(ii) The number of students who have not offered any of these subjects.

Q. Using Laws of sets prove that

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

Sol^n: $(A\cap\bar{B})\cup(\bar{A}\cap B)\cup(\bar{A}\cap\bar{B})$

$= (A\cap\bar{B})\cup[(\bar{A}\cap B)\cup(\bar{A}\cap\bar{B})]$

$= (A\cap\bar{B})\cup[\bar{A}\cap(B\cup\bar{B})]$

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

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

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

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

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

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

Hence Proved

Q. If A and B are two sets such that

$n(A)=27,\ n(B)=35,\ n(A\cup B)=50.$

Find $n(A\cap B)$

Sol^n: $n(A\cup B)=n(A)+n(B)-n(A\cap B)$

$n(A\cap B)=27+35-50$

$\therefore \boxed{n(A\cap B)=12}$

LECTURE NO. 4B

Partitions of sets [R2]

- Let A be a non-empty set
- $S \subseteq P(A)$ is called a partition of A if
  1. $\forall X \in S, X \neq 0$
  2. $\forall X, Y \in S, X = Y$ or $X \cap Y = \phi$
  3. $\bigcup_{X \in S} X = A$

Def^n: Let S be a non-empty set, A partition of S into a non-overlapping, non-empty subsets. Or a partition of S is a collection $\{A_i\}$ of non empty subsets of S such that
a) Each a in S belongs to one of the A_i
b) The sets of $\{A_i\}$ are mutually disjoint i.e $A_i \neq A_j$ Other $A_i \cap A_j = \phi$

- Example:

A = {1, 2, 3, 4, 5, 6}. Check which of the following are the partitions of set A.

		C1	C2	C3
S1.	= {{1,4,5}, {2}, {3,6}}	✓	✓	✓
S2	= {ϕ, {1,2}, {3,4,5,6}}	✗	✓	✓
S3.	= {{1,2,3,4}, {4,5,6}}	✓	✗	✓
S4.	= {{1,2}, {4,5,6}}	✓	✓	✗

$\therefore$ Only S1 is the partition of A.

Q. S = { 1,2,3,4}. Find all the partitions of S.

Q. S = {a, b, c, d}. Find all the partitions of S.

References:

1. Jean Paul Trembley, R Manohar, "Discrete Mathematical Structures" McGraw Hill
2. PDF: Partitions and Counting," https://math.darthmouth.edu

UNIT 01

LECTURE NO. 05

KEYWORDS:
Relations, Domain, Range

Binary Relation [R2]

- Let A and B be sets.
- A binary relation from A to B is a subset of a cartesian product A×B

ie $\boxed{R_{(A,B)} \subseteq A \times B}$

- Example:

$A = \{a, b, c\}$ $B = \{1, 2, 3\}$

$A \times B = \{(a,1), (a,2), (a,3), (b,1), (b,2), (b,3), (c,1), (c,2), (c,3)\}$

$R = \{(a,1), (b,2), (c,2)\}$ is an example of a relation from A to B.

- If R is a relation from A to B, then R is a set of ordered pairs where each first element comes from A and each second element comes from B ie. $\forall a \in A$ and $b \in B$.

- If $(a,b) \in R$, then we say "a is R-related to b" written as $\boxed{aRb}$

If $(a,b) \notin R$, then we say 'a is not R-related to b" written as $\boxed{a \not R b}$ or $\boxed{a R' b.}$

Representing Binary Relations [R1, R2]

- We can represent a binary relation R by a table showing the ordered pairs of R.

- Example:

Let $A = \{0, 1, 2\}$ $\quad B = \{u, v\}$

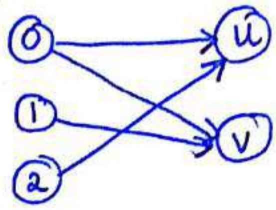
$A \times B = \{(0,u), (0,v), (1,u), (1,v), (2,u), (2,v)\}$

and let $R = \{(0,u), (0,v), (1,v), (2,u)\}$

Table:

R	u	v
0	1	1
1	0	1
2	1	0

Graph/ Pictorical:



Domain and Range of a Relation R [R1, R2]

- **Domain:**

- The domain of a relation R is the set of all first elements of the ordered pairs which belong to R.
- The set $\boxed{\{a \in A : (a,b) \in R \text{ for some } b \in B\}}$ is called the domain of R and is denoted by $\boxed{Dom(R)}$.

- **Range:**

- The range of a relation R is the set of second elements of the ordered pairs which belong to R.
- The set $\boxed{\{b \in B : (a,b) \in R \text{ for some } a \in A\}}$ is called the range of R and is denoted by $\boxed{Ran(R)}$.

NOTE

$$\boxed{\begin{array}{l} {}^{*}Dom(R) \subseteq A \\ Ran(R) \subseteq B \end{array}}$$

- Example:

$A = \{1, 2, 3, 4\}$ $\quad B = \{3, 4, 5, 6\}$

List the elements of each relation R defined below and find domain and range.

a) $a \in A$ is related to $b \in B$ i.e. aRb iff $a < b$.

here $A = \{1,2,3,4\}$ $B = \{3,4,5,6\}$

$A \times B = \{(1,3),(1,4),(1,5),(1,6),(2,3),(2,4),(2,5),(2,6),(3,3),(3,4),(3,5),$
$(3,6),(4,3),(4,4),(4,5),(4,6)\}$

now aRb iff $a < b$

$\therefore R = \{(1,3),(1,4),(1,5),(1,6),(2,3),(2,4),(2,5),(2,6),(3,4),(3,5),$
$(3,6),(4,5),(4,6)\}$

$\therefore$ $\boxed{\begin{array}{l} Dom(R) = \{1,2,3,4\} \\ Range(R) = \{3,4,5,6\} \end{array}}$

b) $a \in A$ is related to $b \in B$ i.e aRb iff a and b are both odd nos.

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

$\therefore$ $\boxed{\begin{array}{l} Dom(R) = \{1,3\} \\ Ran(R) = \{3,5\} \end{array}}$

No. of Distinct Relations [R1]

- To find the total no. of distinct relations from a set A and a set B.
- Let no. of elements of A and B be 'm' and 'n' respectively.
- Then, $\boxed{\text{distinct relations from A to B} = 2^{mn}}$

References

1. Liu and Mohapatra, "Elements of Discrete Mathematics", McGraw Hill
2. Y.N. Singh, "Discrete Mathematical Structures", Wiley India.

UNIT 01

LECTURE NO 06

KEYWORDS:
Diagonal Relation, matrix, Empty Relation, Self Loop, Reflexive, Transitive, Symmetric

Types of Relations [R1, R2]

1. IDENTITY RELATION

- Let A be any set.
- An important relation on A is that of equality.
- It is also called as Diagonal Relation on A.
- Denoted by $\boxed{\Delta_A \text{ or } I_A}$
- $\boxed{I_A = \{(a,a) : a \in A\}}$
- Example:

I_A	x	y	z
x	1	0	0
y	0	1	0
z	0	0	1

$$A = \{x, y, z\}$$

$$A \times A = \{(x,x), (x,y), (x,z), (y,y), (y,z), (z,z)\}$$

the $\boxed{I_A = \{(x,x), (y,y), (z,z)\}}$ is an Identity Relation on A

2. INVERSE RELATION

- Let R be any relation from set A to set B.
- Inverse of R is denoted by $\boxed{R^{-1} \text{ or } R^{I}}$.
- R^{-1} is the relation from B to A which consists of those ordered pairs which when reversed belong to R

i.e $\boxed{(R^{-1})^{-1} = R}$

$$\boxed{\begin{array}{l} \text{i.e. } R^{-1} = \{(b,a) : (a,b) \in R\} \\ \text{also } R^{-1} \subseteq B \times A \end{array}}$$

- Example: $R = \{(1,7), (2,3), (3,8), (4,5)\}$

then $R^{-1} = \{(7,1), (3,2), (8,3), (5,4)\}$

3) N-ARY RELATION

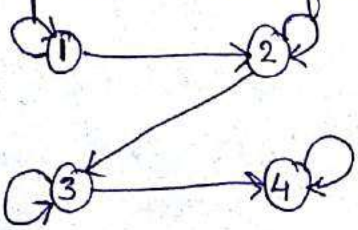
- Let $\{A_1, A_2, \dots A_n\}$ be a finite collection of sets.
- A subset R of $A_1 \times A_2 \times \dots \times A_n$ is called an n-ary relation on $A_1, A_2, \dots, A_n$.
- If $R = \phi$, then R is called void or Empty relation.
- If $R = A_1 \times A_2 \times \dots \times A_n$, then R is called the Universal Relation.
- For n = 1, R is called Unary Relation.
  n = 2, R is called Binary Relation
  n = 3, R is called Ternary Relation

4. REFLEXIVE RELATION

- Let R be an binary relation on a set A.
- R is reflexive iff, $\boxed{\forall a \in A, (a,a) \in R}$
  i.e. R is reflexive if xRx is true.
- Example:
  1. $A = \{1,2,3,4\}$
  $\therefore$ $R1 = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,3), (3,3), (4,4)\}$
  here R is Reflexive.

  2. $A = \{1,2,3,4\}$
  $R2 = \{(1,1), (1,2), (2,2), (2,3), (3,3), (3,4), (4,4)\}$
  is also Reflexive.

- Graphical Representation of R2



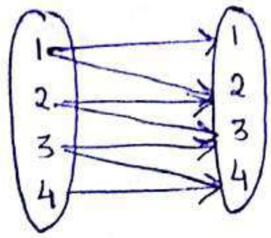
* In a Reflexive Relation, the elements will have SELF LOOP.

- Matrix Representation of R2

R2	1	2	3	4
1	1	1	0	0
2	0	1	1	0
3	0	0	1	1
4	0	0	0	1

* In a Reflexive Relation, the diagonal elements of the matrix will be 1.
* A relation R is Reflexive iff it has 1 in every position on its main diagonal.

- Pictorical Representation of R2



* xRx in a Reflexive Relation.

5. IRREFLEXIVE RELATION

- Let R be a Binary Relation on a set A.
- R is irreflexive iff $\boxed{\text{for all } x \in A,\ (x,x) \notin R}$
- Example :

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

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

here R is Irreflexive.

- Matrix representation of R

R	1	2	3	4
1	0	1	1	1
2	1	0	1	1
3	1	1	0	1
4	1	1	1	0

* A relation R is Irreflexive iff it has 0 in every position on its main diagonal.

6. NON REFLEXIVE RELATION

- Let R be a binary relation on set A.
- R is neither reflexive, nor irreflexive iff there is $x \in A$ such that $(x,x) \in R$ and there is $y \in A$ such that $(y,y) \notin R$.

7. SYMMETRIC RELATION

- A relation R on a set A is symmetric if whenever $(a,b) \in R$ then $(b,a) \in R$ ie

$$\boxed{\text{if } aRb \Rightarrow bRa}$$

- Example:

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

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

here R is Symmetric.

8. ASYMMETRIC RELATION

- A relation R on a set A is Asymmetric if whenever $(a,b) \in R$ then $(b,a) \notin R$ ie.

$$\boxed{\text{if } aRb \not\Rightarrow bRa}$$

- Example:

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

$R1 = \{(1,3), (3,1), (2,3)(3,2)\}$

here R1 is not Asymmetric.

$R2 = \{(1,3), (3,1), (2,3)\}$

here R2 is not asymmetric.

- R is not asymmetric if there exists a pair of elements a and b in A such that aRb and bRa ie $(a,b) \in R$ and also $(b,a) \in R$ (even for $x=y$)

Scanned by CamScanner

9. ANTISYMMETRIC RELATION

- A relation R on a set A is antisymmetric if whenever $\boxed{aRb \text{ and } bRa \text{ then } a=b}$ $\forall\ a,b \in A$.

- Example:

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

$R1 = \{(1,1),(2,2)\}$

here R1 is Antisymmetric relation

$R2 = \{(1,1),(1,2),(3,2),(3,3)\}$

here R2 is Antisymmetric relation.

10. TRANSITIVE RELATION

- A relation R on a set A is transitive if whenever aRb and bRc, then aRc ie

$\boxed{\text{if whenever } (a,b),(b,c) \in R \text{ then } (a,c) \in R}$

- Thus R is not transitive if there exist $a,b,c \in A$ such that $(a,b),(b,c) \in R$ but $(a,c) \notin R$.

- Example:

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

$R1 = \{(1,1),(1,2),(2,3)\ (1,3),(4,4)\}$

here R1 is Transitive relation.

$R2 = \{(1,1),(1,2),(2,1),(2,2),(3,3),(4,4)\}$

here R2 is Transitive relation

$R3 = \{(1,3),(2,1)\}$

here R3 is not Transitive relation.

11. UNIVERSAL RELATION

- A relation R in a set A is called universal relation if $\boxed{R = A \times A}$

- Example: if $A = \{1,2\}$ then $R = \{(1,1),(1,2),(2,1),(2,2)\}$

12 EQUIVALENCE RELATION

- Let A be a non empty set and R be a relation defined on A.
- Then R is said to be Equivalence Relation if it is

(i) REFLEXIVE ie $aRa \ \forall a \in A$.

(ii) SYMMETRIC ie. if $aR_b \Rightarrow bR_a \ \forall a, b \in A$.

(iii) TRANSITIVE ie aRb and $bRc \Rightarrow aRc \ \forall a, b, c \in A$.

Equivalence Classes [R1, R2]

- Consider an equivalence relation R on a set A. The equivalence class of an element $a \in A$ is the set of elements of A to which element a is related.
- Denoted by $[a]$ or $\bar{a}$.
- Rank of relation R is the no. of distinct equivalence classes.
- Example:

1) Let $A = \{a, b, c\}$

$R = \{(a,a), (b,b), (c,c), (a,b), (b,a)\}$ where R is clearly an equivalence relation.

Find equivalence classes of the elements of A.

Sol^n: $[a] = \{a, b\}$

$[b] = \{b, a\} = [a]$ $\qquad \therefore \boxed{\text{Rank of } R = 2}$

$[c] = \{c\}$

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

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

Determine the equivalence classes and find rank of R.

$[1] = \{1, 2, 3\}$

$[2] = \{1, 2, 3\} = [1]$ $\qquad \therefore \boxed{\text{Rank of } R = 2}$

$[3] = \{3, 2, 1\} = [1]$

$[4] = \{4\}$

LECTURE NO. 6A

Operations on Relations [R3, R4]

1. COMPLEMENT OF A RELATION

- Consider a relation R from set A to B.
- The complement of relation R denoted by $\bar{R}$ or R' is a relation from A to B such that

$$\boxed{\bar{R} = \{(a,b) : (a,b) \notin R\}}$$

- i.e $\boxed{\bar{R} = (A \times B) - R}$
- Example:
Let R be a relation from X to Y, where $X = \{1,2,3\}$ and $Y = \{8,9\}$ and $R = \{(1,8), (2,8), (1,9), (3,9)\}$. Find the complement of R

Now,

First $X \times Y = \{(1,8), (1,9), (2,8), (2,9), (3,8), (3,9)\}$

$\therefore \bar{R} = (X \times Y) - R = \{(2,9), (3,8)\}$

$$\boxed{\therefore \bar{R} = \{(2,9), (3,8)\}}$$

2. INVERSE OF A RELATION/INVERSE RELATION

* Refer Pg 13, Unit 1

3. INTERSECTION OF RELATIONS

- If R and S are two relations, then intersection of R&S is denoted by $R \cap S$
- Example: $R = \{(1,1), (2,2), (3,3), (4,4), (3,4), (4,3)\}$
$S = \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,1)\}$

Then $\boxed{R \cap S = \{(1,1), (2,2), (3,3), (4,4)}$

4. UNION OF RELATIONS

- If R and S are the two relations then union of R & S is denoted by $R \cup S$

- Example: $R = \{(1,1),(2,2),(3,3),(4,4),(3,4),(4,3)\}$

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

Then $\boxed{R \cup S = \{(1,1),(2,2),(3,3),(4,4),(1,2),(2,1),(3,4),(4,3)\}}$

References:

1. Liu and Mohapatra, "Elements of Discrete Mathematics", McGraw Hill.
2. Jean Paul Trembley, R Manohar, "Discrete Mathematical Structures with application to Computer Science," McGraw Hill
3. PDF: operations on Relations," www.inf.ed.ac.uk"
4. PDF: Operations on Relations," faculty.simpson.edu"

UNIT 01

LECTURE NO 07

KEYWORDS:
Composition, Reflexive, Symmetric, Transitive, Equivalence.

Composition of Relations [R1, R2]

- Let A, B & C be sets, and let R be a relation from A to B and let S be a relation from B to C.

  i.e. $R \subseteq A \times B$

  $S \subseteq B \times C$

- Then R & S give rise to a relation from A to C.
- It is denoted by RoS and is defined by

  RoS exists if for some $b \in B$ we have aRb and bSC.

  i.e. $RoS = \{(a,c) : \text{there exists } b \in B \text{ for which } (a,b) \in R \text{ and } (b,c) \in S\}$

- Then this relation RoS is called the composition of R and S.
- It is sometimes denoted by RS.
- Suppose R is a relation on a set A i.e. R is a relation from a set A to itself, then the composition is denoted as RoR or R^2.

- Thus R^n is defined for all +ve n.

Methods to find Composition of Relations [R2]

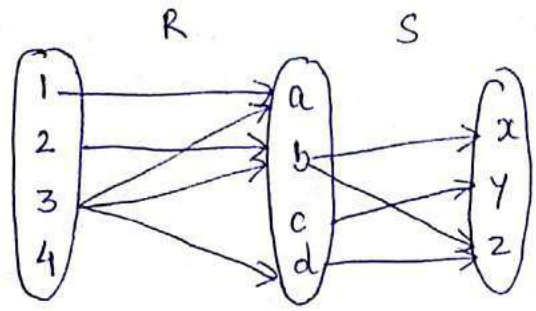
METHOD 01

$R = \{(1,a), (2,d), (3,a), (3,b), (3,d)\}$

$S = \{(b,x), (b,z), (c,y), (d,z)\}$

$\therefore$ $\boxed{RoS = \{(2,z), (3,x), (3,z)\}}$

METHOD 02



$$\therefore \boxed{R \circ S = \{(2,z), (3,x), (3,z)\}}$$

METHOD 03

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

$$M_S = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{array}$$

$$M_R \times M_S = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$$

$$\therefore \boxed{R \circ S = \{(2,z), (3,x), (3,z)\}}$$

Closure Properties [R2]

1. REFLEXIVE CLOSURE

- Let R be a relation on a set A. Then $R \cup \Delta_A$ is the reflexive closure of R.
- Example: let $A = \{1,2,3,4\}$
  & $R = \{(1,1), (1,3), (2,4), (3,1), (3,3), (4,3)\}$

  now to make R reflexive

  $$\Delta_A = \{(2,2), (4,4)\}$$

  ∴ Reflexive Closure of R is

  $$\boxed{R \cup \Delta_A = R \cup \{(2,2), (4,4)\}}$$

2. SYMMETRIC CLOSURE

- Let R be a relation on a set A. Then $R \cup R^{-1}$ is the symmetric closure of R.
- Example:
  $R = \{(1,1), (1,3), (2,4), (3,1), (3,3), (4,3)\}$

  now to make R symmetric

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

  ∴ Symmetric Closure of R is

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

3. TRANSITIVE CLOSURE

- Let R be a relation on a set A. Then $R \cup R^T$ is the transitive closure of R.
- Example: Let $A = \{1,2,3,4\}$

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

  now to make R transitive, find R^T

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

$\therefore$ Transitive Closure of R is

$$\boxed{R^* = R \cup R^T = \{(1,2), (2,3), (3,3), (1,3)\}}$$

Equivalence Relations [R1]

- Consider a non-empty set S. A relation R on S is an equivalence relation if R is reflexive, symmetric and transitive.
- i.e. R is an equivalence relation on S if it has the following three properties:

1. For every $a \in S$, aRa.
2. If aRb, then bRa.
3. If aRb and bRc, then aRc.

References :-

1. PDF : Operations on Relation, "www.inf.ed.ac.uk"
2. PDF : Operations on Relation, "faculty.simpson.edu"

UNIT 01

LECTURE NO. 08

KEYWORDS:
Domain, Co-domain, Function

Functions [R1]

- When to each element of set A, we assign a unique element of set B; the collection of such assignments is called a function from A into B.

- Set A is called the domain of the function, and the set B is called the codomain.

- It is usually denoted by

$$\boxed{f : A \rightarrow B}$$

read as : "f is a function from A into B."

- A function $f : A \rightarrow B$ is a relation from A to B (i.e. a subset of $A \times B$) such that each $a \in A$ belongs to a unique ordered pair (a, b) in f.
- $f^{-1} = \{(b, a) : (a, b) \in f\}$ is called the inverse mapping of f.
- Example:

  $f(x) = x^2$ ie f assigns or sends each real no. to its square

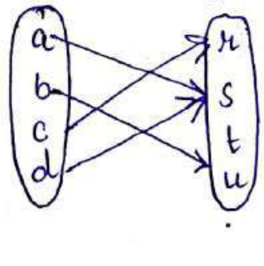
  ie. $x \rightarrow x^2$

  $y = x^2$

  Can also be represented as $f^{-1}(x^2)$ in inverse mapping.

Image of function f [R1]

- If $f(x) = y$, then y is called f-image of x & x is called pre image of y in A.
- Image of f is also called as Range of f.
- consider the figure:



$\therefore f(a) = s$

$f(b) = u$

$f(c) = r$

$f(d) = s$

$\therefore$ $\boxed{\text{Image of } f = \{r, s, u\}}$

*Refer Pg 18.1

Types of Functions [R1]

1. IDENTITY FUNCTION

- Let A be any set.
- The function from A to A which assigns to each element that element itself, is called Identity function
- It is denoted as I_A

$$\boxed{\therefore I_A(a) = a}$$

- Example:

$f(a) = a$

$f(b) = b$

$f(c) = c$ etc.

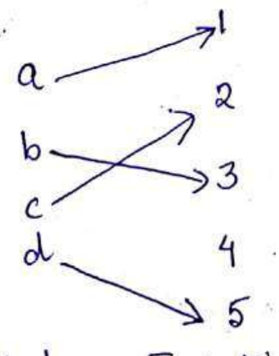
- It is one-to-one and onto. Every element of A is its f-image

2. EQUAL FUNCTIONS

- Two functions are equal when
  1. Their domains are equal
  2. Their co-domains are equal
  3. And they map each element in their common codomain.
- Two functions f and g defined on the same domain A if $f(x) = g(x)\ \forall\ x \in A$, represented as $f = g$.
- Example: let $A = \{2,3\}$, $B = \{2,4,5,9\}$. let $f(x) = x^2$ and $g(x) = \{(2,4),(3,9)\}$, then $f = g$ because they have same domain and are mapped to same image element

3. ONE-TO-ONE FUNCTIONS

- A function f is said to be one-to-one, if for each pair of distinct elements of A, their f-images (in B) are also distinct. ie. $f: A \to B$ is one-to-one if for $x_1, x_2 \in A$, $(x_1 \neq x_2)$



- All domain elements are covered

- It is also called as Injective Function.

Q. If the function $f: R \to R$ be defined by $f(x) = x^2$, then find out (i) $f^{-1}(9)$ (ii) $f^{-1}(-9)$ and (iii) $f^{-1}(9, 16)$

Solⁿ: $f: R \to R$, $f(x) = x^2$, $x \in R$

i) $f^{-1}(9) = \{x \in R : f(x) = 9\}$
$= \{x \in R : x^2 = 9\}$
$= \{x \in R : x = \pm 3\}$
$= \{3, -3\}$

ii) $f^{-1}(-9) = \{x \in R : f(x) = -9\}$
$= \{x \in R : x^2 = -9\}$
$= \{x \in R : x = \pm 3i\}$
$= \phi$ as $\pm 3i \notin R$

iii) $f^{-1}(9, 16) = \{x \in R : f(x) = 9, f(x) = 16\}$
$= \{x \in R : x^2 = 9, x^2 = 16\}$
$= \{x \in R : x = \pm 3, x = \pm 4\}$
$= \{3, -3, 4, -4\}$

Q. If the map $f: C \to C$ is given by $f(x) = x^2$, then find $f^{-1}(-5)$

Solⁿ: $f^{-1}(-5) = \{z \in C : f(z) = -5\}$
$= \{x \in C : z = \pm i\sqrt{5}\}$
$= \{i\sqrt{5}, -i\sqrt{5}\}$

Difference between a Relation and Function

- Let A and B be two sets and f be a function from A to B. f is a subset of $A \times B$ such that each $x \in A$ appears in one and only one ordered pair belonging to f.
- In contrast, a relation between A & B is just an arbitary subset of $A \times B$.

- Example: let $A = \{a, b, c\}$ and $B = \{2, 3, 4, 8\}$ then

i) the subset R of $A \times B$ given by

$R = \{(a,2), (b,2), (c,8)\}$ is a function from A to B

ii) the subset S of $A \times B$ given by

$S = \{(a,2), (a,4), (b,3), (c,8)\}$ is a relation but not a function because the same element $a \in A$ is associated with two elements $2, 4 \in B$.

iii) the subset T of $A \times B$ given by

$T = \{(a,4), (b,8)\}$ is a relation but not a function because an element $c \in A$ is not associated with any element of B.

7. <u>Many - to One Mapping</u> (from Pg 19)

- A mapping $f: A \rightarrow B$ is many - to - one mapping if two or more different elements in A have same f-image in B.

- Example: The mapping $\{-2, 2, 3, 4\} \rightarrow \{4, 9, 16\}$ defined by $f(x) = x^2$ is many - to - one because two different elements in A (ie $-2, 2$) have same f-image.

$-2 \rightarrow 4$

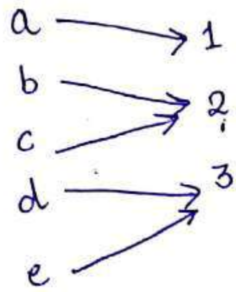
$2 \rightarrow 4$

$3 \rightarrow 9$

$4 \rightarrow 16$

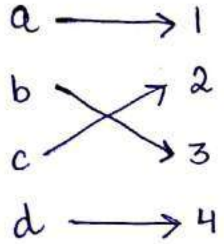
4. ONTO FUNCTIONS

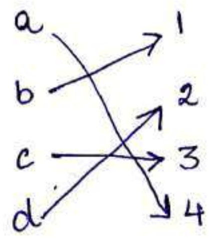
- A function from A to B is called onto iff for every $b \in B$ there is an element $a \in A$ such that $f(a) = b$
- All codomain are covered ie. every element in B has its pre-image in A
- It is also called a Surjective.



5. BIJECTIVE FUNCTION

- A function f is called a Bijection if it is both one-to-one and onto.

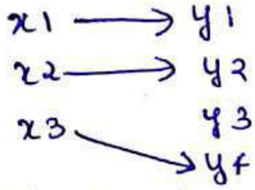




- It is also called Invertible Function.

6. INTO FUNCTION

- If $f: A \rightarrow B$ be a mapping such that at least one element of B is not a ~~pre~~ image of any element of the set A, then the mapping f is said to be an into mapping or A into B mapping.



7. Many to One Mapping (Refer Pg 18.1)

Functions on Real Numbers [R1]

Let f1 and f2 be functions from A to R (real no.), then f1 + f2 and f1 * f2 are also functions from A to R defined by

- $(f1 + f2)(x) = f1(x) + f2(x)$
- $(f1 * f2)(x) = f1(x) * f2(x)$

- Example:

$$f1(x) = x-1$$
$$f2(x) = x^3+1$$

then

$$(f1+f2)(x) = x^3+x$$
$$(f1 \times f2)(x) = x^4 - x^3 + x - 1$$

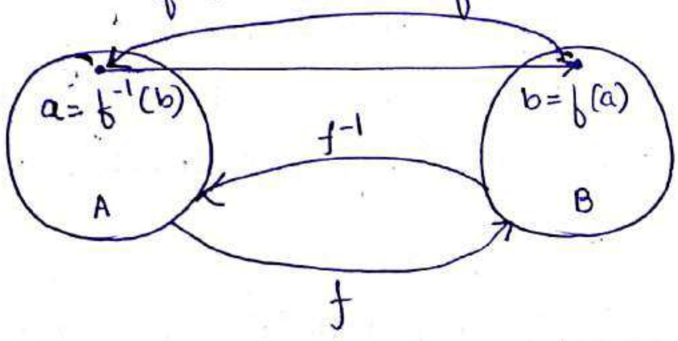
7. INCREASING & DECREASING FUNCTIONS

- Suppose that f is a function whose domain & codomain are subsets of the real nos.
- Then f is called
  - increasing if $f(x) \leq f(y)$
  - strictly increasing if $f(x) < f(y)$
  - decreasing if $f(x) \geq f(y)$
  - strictly decreasing $f(x) > f(y)$

whenever x & y are in the domain of f and $x<y$.

8. INVERSE FUNCTION

- Let f be a one-to-one or bijective correspondance from A to B.
- The inverse function of f is the function f^{-1} that assigns to $b \in B$ the unique element $a \in A$ with $f(a) = b$
- Hence, when $f(a) = b$, then $f^{-1}(b) = a$.



- Example1:

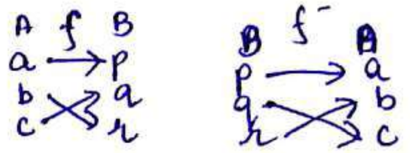
  $A = \{1,2,3\}$ and I_A be the identity functions:

  $I_A(1) = 1$ then $I_A^{-1}(1) = 1$

  $I_A(2) = 2$ $I_A^{-1}(2) = 2$

  $I_A(3) = 3$ $I_A^{-1}(3) = 3$

  $\therefore$ The inverse of I_A is I_A.



- Example 2:

9. MATHEMATICAL FUNCTIONS

   1. FLOOR AND CEILING FUNCTIONS.
   2. INTEGER AND ABSOLUTE VALUE FUNCTIONS.
   3. REMAINDER AND MODULAR FUNCTIONS.
   4. EXPONENTIAL FUNCTIONS
   5. LOGARITHMIC FUNCTIONS
   6. RECURSIVE FUNCTIONS.

Recursively Defined Functions [R1]

- A recursively functions calls itself.
- A function f is recursively defined if it at-least one value of $f(x)$ is defined in terms of another value, $f(y)$, where $x \neq y$.
- This definition must have the following properties so that it may not be circular
  - (i) There must be certain arguments called Base Values for which the function does not refer to itself
  - (ii) Each time the function refers to itself, the argument of function must be a closure to a base value.

- Example :

Let x and y be positive integer and function f is defined as

$$f(x,y) = \begin{cases} 0 \\ f(x-y,y)+1 & \text{if } y \leq x \end{cases}$$

$\therefore$ for $f(t,8) = 0$

$$\begin{aligned}
\text{for } f(20,5) &= f(20-5,\ 5)+1 \\
&= f(15,5)+1 \\
&= f[(15-5),5) + 1] + 1 \\
&= f(10,5)+2 \\
&= f[((10-5),5)+2]+1 \\
&= f(5,5)+3 \\
&= f[((5-5),5)+3]+1 \\
&= f(0,5)+4 = 0+4 = \underline{\underline{4}}
\end{aligned}$$

Even and Odd Functions [R1]

- A function is said to be

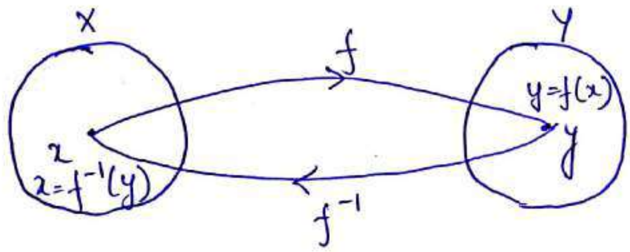
(i) Even if $f(-x) = f(x)\ \forall x$

(ii) Odd if $f(-x) = -f(x)\ \forall x$

Inverse Function (Inverse Mapping) (Repeated from Pg 19)

- Let $f: X \to Y$ be one-to-one onto mapping. Let $y \in Y$, since f is onto, there exists $x \in X$ such that $f(x) = y$
- Again since f is one-to-one, this is the only element of X such that $f(x) = y$.
- Thus, for each $y \in Y$, there is a unique $x \in X$ such that $f(x) = y$.
- This mapping from Y to X is called Inverse of f; denoted by f^{-1}.

$$\therefore \boxed{f(x) = y \iff f^{-1}(y) = x}$$



Operations on Functions [R1]

1. ADDITION

- $(f+g)x = f(x) + g(x)$, $f+g$ will be defined only for those value of x for which both f and g are defined.

$$\therefore \boxed{D(f+g) = D_f \cap D_g}$$

where D_f = Domain of $f(x)$
D_g = Domain of $g(x)$

2. SUBTRACTION

- $(f-g)x = f(x) - g(x)$

$$\therefore \boxed{D(f-g) = D_f \cap D_g}$$

Scanned by CamScanner

Ackermann Function

- In computability theory, the Ackermann function, named after Wilhelm Ackermann, is one of the simplest and earliest-discovered examples of a total computable function that is not primitive recursive.

- All primitive recursive functions are total and computable, but the Ackermann function illustrates that all total computable functions are primitive recursive.

- Ackermann function is defined as follows:

$$A(m,n) = \begin{cases} n+1 & \text{if } m=0 \\ A(m-1,1) & \text{if } m>0 \text{ and } n=0 \\ A(m-1, A(m,n-1)) & \text{if } m>0 \text{ and } n>0. \end{cases}$$

- Its values grows rapidly, even for small inputs.

- Ackermann Function deals with positive integers $\{0,1,2\ldots\}$

- Example

1) $A(0,5)$

Sol^n: $A(m,n) = n+1$ (if $m=0$)

here $m=0$

$\therefore A(0,5) = 5+1 = \underline{\underline{6}}$.

2) $A(1,2)$

Sol^n: $A(m,n) = A(m-1, A(m,n-1))$ (if $m>0$ and $n>0$)

here $m>0$ and $n>0$

$\therefore A(1,2) = A(1-1, A(1,2-1))$

$= A(0, A(1,1))$

$= A(0, A(1-1, A(1, 1-0)))$ (here $m>0, n>0$)

$= A(0, A(0, A(1,0)))$

$= A(0, A(0, A(1-1, 1)))$

$= A(0, A(0, A(0,1)))$

$= A(0, A(0, (1+1)))$

$= A(0, A(0,2))$

$= A(0, (2+1))$

$= A(0, 3)$

$= 3+1$

$= \underline{\underline{4}}$

UNIT 01

LECTURE NO. 09

KEYWORDS:
Function, Relation, Natural nos, Peano's Axioms,

Difference between Relation & Function [R1, R2] (Refer Pg 18.1)

- The usual definition is that a function $A \to B$ is a subset of $A \times B$ such that for every $a \in A$ there is exactly one $b \in B$ such that (a,b) is in the function i.e. $a \in A$ appears in one and only one ordered pair belonging to f.
- In contrast, a relation between A & B is just an arbitary subset of $A \times B$.

Natural Numbers

Peano's Axioms [R2]

- The most basic mathematical system is the set to N (natural nos.) of positive integers.
- The positive integer can be defined by a set of axioms, known as Peano's Axioms.

P1: There exists a natural number 1 ie $1 \in N$.

P2: There exists an *injective mapping *One-to-One
$f: N \to N$. If $n \in N$ then $f(n) = n+1$ successor of n.

P3: There exists no number $n \in N$ such that $f(n) = 1$.

P4: If A be any subset of N such that $1 \in A$ and $n \in A \Rightarrow f(n) \in A$ then $A = N$.

REMARK

* 1. Axiom P1 asserts that N is non empty.
2. Axiom P2 asserts that $f(m) = f(n) \Rightarrow m = n$.
3. Axiom P3 asserts that the natural no. 1 is a non successor.
4. Axiom P4 leads to the important principle known as Principle of Mathematical induction.

Basic Properties of Natural Nos. [R1]

- We denote the set of positive integers by N and set of integers by Z or I

ie $N = \{1, 2, 3, \ldots\}$

$Z = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- The simple rules concerning addition & multiplication of these integers are given as

i) Commutative Laws for Multiplication & Addition

$$\boxed{a+b = b+a \quad \& \quad ab = ba}$$

ii) Associative laws for multiplication and addition

$$\boxed{(a+b)+c = a+(b+c) \quad \& \quad (ab)c = a(bc)}$$

iii) Distributive Law:

$$\boxed{a \cdot (b+c) = ab + ac}$$

iv) Additive identity 0 and multiplicative identity 1.

$$\boxed{\begin{array}{l} a+0 = 0+a = a \\ a \cdot 1 = 1 \cdot a = a \end{array}}$$

v) Additive Inverse of a is (-a)

$$\boxed{a + (-a) = (-a) + a = 0}$$

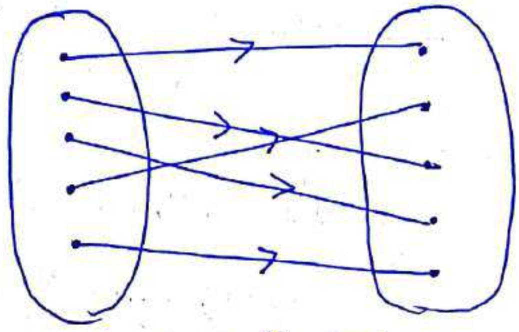
Reference:

1. Liu and Mohapatra, "Elements of Discrete Mathematics", McGraw Hill
2. PDF: Introduction, Natural Numbers, Real Numbers, "www.math.ucla.edu"

Types of Functions

1. One-to-One / Injective Function

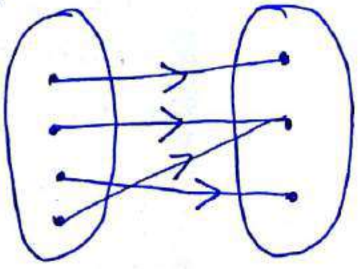
- A function $f: A \to B$ is said to be injective if whenever a and b are elements of A such that $a \neq b$, then $f(a) \neq f(b)$.
- i.e. distinct elements of A are mapped into distinct element of B.



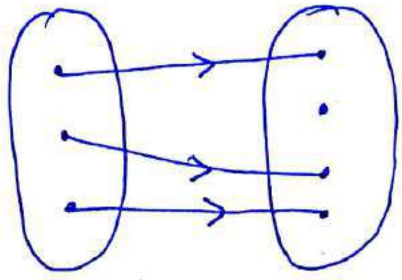
one-to-one

2. Surjective / Onto Function

- A function $f: A \to B$ is called onto or surjective function if for any value 'y' in B there is atleast one element 'x' in A for which $f(x) = y$. i.e.
- i.e. for every element of B is the image of some element in A.
- In order to check whether $f(x) = y$ from a set A to set B is onto or not, write x in terms of y. If for every $y \in B$, $x \in A$, it is onto.



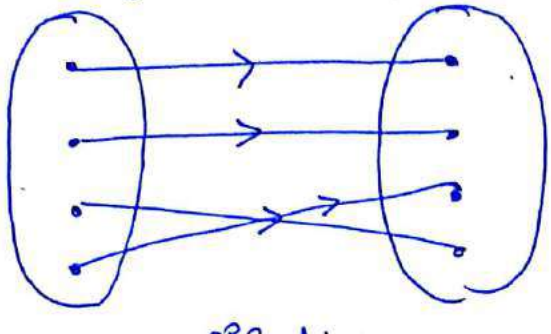
onto



not onto

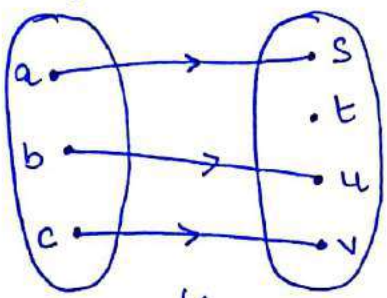
3. Bijective Function

- A function that is both injective and surjective is called a bijection or one-to-one correspondance.

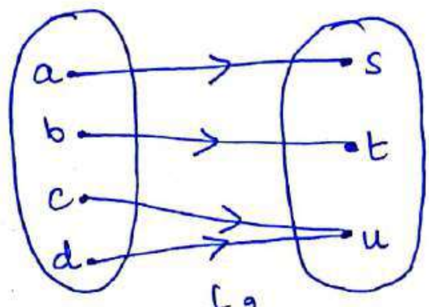


Bijective

Q] Define the functions f1, f2, f3 and f4 by the diagrams shown in the following figure.

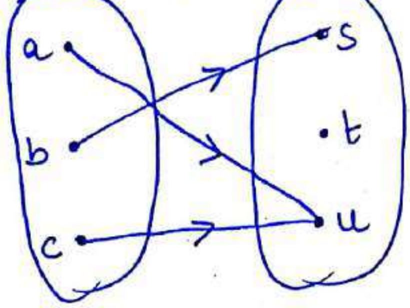


f1

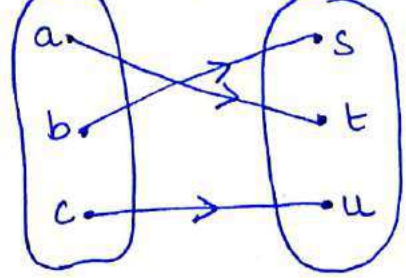


f2

f3



f4



Sol^n: • f1 is one-to-one, but it is on onto because there is no value of x such that $f_1(x) = t$.

• f2 is onto but it is not injective because $f_2(c) = f_2(d)$.

- The function f_3 is neither one-to-one nor onto.
- The function f_4 is both ~~iss~~ one-to-one and onto.

Q] Show that the function $f: R \to R$ defined as $f(x) = 2x+3$ for all $x \in R$ is both injective and surjective function.

Sol^n. First we show that f is injective

Let $x_1, x_2 \in R$ ie $x_1 \neq x_2$

$$\Rightarrow 2x_1 \neq 2x_2$$

$$\Rightarrow 2x_1 + 3 \neq 2x_2 + 3$$

$$\Rightarrow f(x_1) \neq f(x_2)$$

ie. if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$

$\therefore f$ is injective.

Now, we show that f is surjective

Let $y = 2x+3$ be any element in R, then

$$x = \frac{y-3}{2} \in R$$

$$f(x) = f\left(\frac{y-3}{2}\right)$$

$$= 2\left(\frac{y-3}{2}\right) + 3$$

$$= y - 3 + 3$$

$$= y$$

i.e. for every element $y \in R$, there exists an element $x \in R$ such that $f(x) = y$.

$\therefore f$ is surjective.

Q] Show that there exists one-to-one mapping from $A \times B$ to $B \times A$. Is it onto also?

Solⁿ: Let $(x, y) \in A \times B$

$(y, x) \in B \times A$

Suppose $f : (A \times B) \rightarrow (B \times A)$

i.e $f(x, y) = (y, x)$

Let (x_1, y_1) and $(x_2, y_2) \in (A \times B)$

if $f(x_1, y_1) = f(x_2, y_2)$

$\Rightarrow (y_1, x_1) = (y_2, x_2)$

$\Rightarrow y_1 = y_2$ and $x_1 = x_2$

Hence f is one-to-one.

- It will be onto since every element of co-domain will be f-image of at least one element of its domain.

Q] If $f : R^+ \rightarrow R^+$ and $g : R^+ \rightarrow R^+$ are defined by the formula $f(x) = \sqrt{x}$ and $g(x) = 3x + 1 \ \forall \ x \in R^+$, find fog and gof. Is fog = gof?

Solⁿ: $f \circ g(x) = f(g(x)) = f(3x+1) = \sqrt{(3x+1)}$

$g \circ f(x) = g(f(x)) = g(\sqrt{x}) = 3\sqrt{x} + 1$

$\therefore f \circ g(x) \neq g \circ f$

Scanned by CamScanner

Q] If $f: R \to R$ and $g: R \to R$ defined by $f(x) = x^3 - 4x$, $g(x) = \frac{1}{(x^2+1)}$, $h(x) = x^4$, find the following composition functions.

a) $(f \circ g \circ h)(x)$

b) $(g \circ g)(x)$

c) $(h \circ g \circ f)(x)$

d) $(g \circ h)(x)$

Sol^n: a) $(f \circ g \circ h)\, x = f(g(h(x)))$

$$= f(g(x^4))$$

$$= f\left(\frac{1}{(x^4)^2+1}\right) = f\left(\frac{1}{x^8+1}\right)$$

$$= \left(\frac{1}{x^8+1}\right)^3 - 4\left(\frac{1}{x^8+1}\right)$$

$$\boxed{(f \circ g \circ h)\, x = (x^8+1)^{-3} - 4(x^8+1)^{-1}}$$

b) $g \circ g(x) = g(g(x))$

$$= g\left(\frac{1}{x^2+1}\right)$$

$$= \frac{1}{\left(\frac{1}{x^2+1}\right)^2 + 1} = \frac{1}{\frac{1}{(1+x^2)^2} + 1}$$

$$\boxed{g \circ g(x) = \frac{(1+x^2)^2}{1+(x^2+1)^2}}$$

Similarily

c) $\boxed{(h \circ g \circ f)(x) = [(x^3 - 4x)^2 + 1]^{-4}}$

d) $\boxed{(g \circ h)(x) = (x^8+1)^{-1}}$

9] Let $f: R \to R$ be defined by

$$f(x) = \begin{cases} x^2+1 & \text{if } x > 0 \\ 2x+1 & \text{if } x \leq 0. \end{cases}$$

Let $g: R \to R$ be defined by

$$g(x) = \begin{cases} x^3 & \text{if } x > 0 \\ 3x-7 & \text{if } x \leq 0 \end{cases}$$

then find the composition $g \circ f$ for both cases.

Sol^n: $g \circ f(x) = g(f(x))$

For $x > 0$, $g(f(x)) = g(x^2+1) = (x^2+1)^3$

$x \leq 0$, $g(f(x)) = g(2x+1) = 3(2x+1) - 7$

$= 6x + 3 - 7$

$= 6x - 4$

Q] Let $X = \{a, b, c\}$. Define $f : X \to X$ such that $f = \{(a,b), (b,a), (c,c)\}$

Find i) f^{-1}, (ii) f^2 (iii) f^3 (iv) f^4

Solⁿ: here $f = \{(a,b), (b,a), (c,c)\}$

i) $f^{-1} = \{(b,a), (a,b), (c,c)\}$

ii) $f^2 = f \circ f$

$= \{(a,b), (b,a), (c,c)\} \circ \{(b,a), (a,b), (c,c)\}$

$$\boxed{f^2 = \{(a,a), (b,b), (c,c)\}}$$

iii) $f^3 = f \circ f^2$

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

$= \{(a,b), (b,a), (c,c)\} \circ \{(a,a), (b,b), (c,c)\}$

$$\boxed{f^3 = \{(a,b), (b,a), (c,c)\}}$$

iv) $f^4 = f \circ f^3$

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

$= \{(a,b), (b,a), (c,c)\} \circ \{(a,b), (b,a), (c,c)\}$

$$\boxed{f^4 = \{(a,a), (b,b), (c,c)\}}$$

Q] Suppose that $f: R \rightarrow R$ is the bijection given by $f(x) = 3x-1$. Let y be an element of co-domain of f. Find $f^{-1}(y)$

Solⁿ: w.k.t. $f(x) = y$

since $f(x) = 3x-1$ (given)

$\therefore y = 3x-1$ if $f(x) = y$, then $x = f^{-1}(y)$

$\Rightarrow x = \frac{y+1}{3}$

$\therefore \boxed{f^{-1}(y) = \frac{y+1}{3}}$

Q] Let $f: R \rightarrow R$ be defined by $f(x) = 2x-3$. Now f is one-to-one & onto, hence f has an inverse function f^{-1}. Find the formula for f^{-1}.

Solⁿ: w.k.t $f(x) = y$

since $f(x) = 2x-3$ (given)

$\therefore y = 2x-3$ if $f(x) = y$, then $x = f^{-1}(y)$

$\Rightarrow x = \frac{y+3}{2}$

$\therefore \boxed{f^{-1}(y) = \frac{y+3}{2}}$

Q]

KEYWORDS:
Mathematical Induction

LECTURE NO. 10

Mathematical Induction [R1]

PRINCIPLE OF MATHEMATICAL INDUCTION

- Let $P(n)$ be a statement involving the natural nos. n. To prove that $P(n)$ is true for all natural number $n \geq a$, we proceed as follows.

  i) Verify $P(n)$ for $n = a$
  ii) Assume the result for $n = K > a$
  iii) Using result (i) & (ii), prove that $P(K+1)$ is true.

- This is known as the First Principle of Mathematical Induction.
- If $P(n)$ is true for $n=1$ (i.e for $a=1$) $P(n)$ is true for all $n \in N$.
- Sometimes the above procedure will not work. Then we consider the alternative principle called the <u>Second Principle of Mathematical Induction</u>, given as

  i) $P(n)$ is true for $n = a$.
  ii) Assume that $P(n)$ for $a \leq n \leq k$
  iii) Prove $P(n)$ for $n = k+1$.

REMARK

* The second principle of mathematical induction is useful to prove recurrence relation which involves three successive terms eg:

$$\boxed{pT_{n+1} = qT_n + nT_{n-1}}$$

Scanned by CamScanner

Example:

Prove by induction

$$1+2+3+4+\cdots+n = \frac{n(n+1)}{2} \quad \forall n \in N$$

LECTURE NO. 10. A

Mathematical Induction [R2, R3, R4]

⇒ The Basic Principle

- An analogy of the principle of Mathematical Induction is the game of dominoes.
- Suppose the dominoes are lined up properly, so that when one falls, the successive one will fall.
- Now by pushing the first domino, the second will fall; when the second falls, the third will fall; and so on.
- We can see that all dominoes will ultimately fall.
- So the basic principle of mathematical Induction is as follows.
- To prove that a statement holds for all positive integer n, we first verify that it holds for $n=1$, and then if it holds for a certain natural number k, it holds for $k+1$.

THEOREM 1: PRINICIPLE OF MATHEMATICAL INDUCTION

Let $P(n)$ denote a statement involving a variable n. Suppose;

(1) $P(1)$ is true;

(2) If $P(K)$ is true for some positive integer k, then $P(K+1)$ is also true.

The $P(n)$ is true for all positive integers n

⇒ Variations to the Basic Principle

THEOREM 2: PRINCIPLE OF MATHEMATICAL INDUCTION, VARIATION 1

Let $P(n)$ denote a statement involving a variable n.

Suppose

1. $P(k_0)$ is true for some positive integer k_0;
2. If $P(k)$ is true for some positive integer $k \geq k_0$, then $P(k+1)$ is also true.

Then $P(n)$ is true for all positive integers $n \geq k_0$

Example: Prove that $2^n > n^2$ for all natural numbers $n \geq 5$.

Sol^n: First we check that $2^5 = 32 > 5^2 = 25$, so the inequality holds for $n = 5$.

now, Suppose $2^k >$ .. is true for some integer $k \geq 5$

Then
$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &> 2k^2 \\ &> (k+1)^2 \end{aligned}$$

The last inequality holds since $2k^2 - (k+1)^2 = (k-1)^2 - 2 > 0$ whenever $k \geq 5$.

Hence, if the inequality holds for $n = k$, it also holds for $n = k+1$.

Scanned by CamScanner

THEOREM 3: PRINCIPLE OF MATHEMATICAL INDUCTION, VARIATION 2

Let $P(n)$ denote a statement involving a variable n.

Suppose

1. $P(1)$ and $P(2)$ are true;
2. If $P(k)$ and $P(k+1)$ are true for some positive integer k, then $P(k+2)$ is also true.

Then $P(n)$ is true for all positive integers n

Example: Let $\{a_n\}$ be a sequence of natural numbers such that $a_1 = 5$, $a_2 = 13$ and $a_{n+2} = 5a_{n+1} - 6a_n$ for all natural numbers n. Prove that $a_n = 2^n + 3^n$ for all natural numbers.

THEOREM 4: PRINCIPLE OF MATHEMATICAL INDUCTION, VARIATION 3

Let $P(n)$ denote a statement involving a variable n.
Suppose

1. $P(1)$ and $P(2)$ are true;
2. If $P(K)$ is true for some positive integer k, then $P(K+2)$ is also True.

Then $P(n)$ is true for all positive integers. n.

Example: Prove that for all natural number n, there exist distinct integers x, y, z for which $x^2+y^2+z^2=14^n$.

THEOREM 5: PRINCIPLE OF MATHEMATICAL INDUCTION, VARIATION 4

Let $P(n)$ denote a statement involving a variable n.
Suppose

1. $P(1)$ is true;
2. If for some positive integer k, $P(1), P(2), \ldots, P(k)$ all are true, then $P(k+1)$ is also true.

Then $P(n)$ is true for all positive integers n.

Example: Let $a_1, a_2, \ldots$ be a sequence of real numbers satisfying $a_{i+j} \leq a_i + a_j$ for all $i, j = 1, 2, \ldots$
Prove that $a_1 + \frac{a_2}{2} + \frac{a_3}{3} + \cdots + \frac{a_n}{n} \geqslant a_n$

THEOREM 6: BACKWARD INDUCTION

Let $P(n)$ denote a statement involving a variable n.

Suppose

1. $P(n)$ is true for infinitely many natural numbers n;
2. If $P(K)$ is true for some positive integer $K>1$, then $P(K-1)$ is also true.

Then $P(n)$ is true for all positive integers n.

EXAMPLE: AM-GM Inequality

Prove that for positive integers $a_1, a_2, \dots a_n$,

$$\frac{a_1 + a_2 + \dots + a_n}{n} \geq \sqrt[n]{a_1, a_2 \dots a_n}$$

ie AM is always greater than or equal to GM

References:

1. Jean Paul Tremblay, R Manohar, "Discrete Mathematics" McGraw Hill
2. PDF: Mathematical Induction, "https://cims.nyu.edu"
3. PDF: Mathematical Induction, sequences and series, "www-history.mcs.st-and.ac.uk"
4. PDF: Mathematical Induction, "https://cseweb.ucsd.edu".

KEYWORDS:
Binary Operations, Algebraic Structures, Group, Order of Group

UNIT-2

LECTURE NO. 01

Binary Operations [R1]

- let G be a non empty set. Then $G \times G = \{(a,b) : a \in G, b \in G\}$.
- If $o : G \times G \to G$, then o is said to be a Binary Operation on the set G.
- Denoted by $\boxed{a \circ b}$ for ordered pair (a,b).
- Often we use symbols $+, \times, \cdot, \circ, *, \oplus, \cup, \cap, \wedge, \vee$ etc. to denote binary operations on a set.
- Thus '+' is a binary operation on G iff

$$\boxed{a+b \in G \ \forall \ a,b \in G \text{ and } a+b \text{ is unique}}$$

- Similary, other operation can be defined.
- Properties of Binary Operations

1. ASSOCIATIVE LAW

An operation $*$ on a set A is said to be associative if for any elements a, b, c in A, we have

$$\boxed{(a*b)*c = a*(b*c)}$$

2. COMMUTATIVE LAW

A binary operation $*$ on the elements of the set is commutative iff for any two elements $a, b \in A$, we have

$$\boxed{a*b = b*a}$$

3. IDENTITY ELEMENTS

An element 'e' in a set A is called an Identity Element w.r.t the binary operation $*$ if for any element 'a' in A.

$$\boxed{a*e = e*a = a}$$

If $\boxed{a*e=a}$, then e is called the Right Identity Element for an operation on a set A.

Similarily if $\boxed{e*a=a}$, then e is called the Left Identity Element.

Suppose e is the left identity and f is the right identity for an operation on set A. Then $\boxed{e=f}$.

4. INVERSE ELEMENT

Consider a set A having the identity element 'e' w.r.t the binary operation $*$. If corresponding to each element $a \in A$ there exists an element $b \in A$ such that

$$\boxed{a*b = b*a = e}$$

then 'b' is said to be the inverse of 'a' and is usually denoted by a^{-1}.

5. CANCELLATION LAWS

A binary operation $*$ on a set A is said to satisfy Left Cancellation Law if

$$\boxed{a*b = a*c \Rightarrow b=c}$$

and $*$ is said to satisfy Right Cancellation Law if

$$\boxed{b*a = c*a \Rightarrow b=c}$$

Algebraic Structures [R2]

- Also called as Mathematical Structures.
- A non-empty set G equipped with some operations and some propertities is called an Algebraic Structures.
- If $*$ is an operation on G then $(G, *)$ is an algebraic structure.
- Examples: $(N,+)$, $(R,+,\times)$.

Group [R1, R2]

- Let G be a non-empty set together with some operation $*$ then algebraic structure $(G,*)$ is said to be a group if following four conditions are satisfied:

1. G1: CLOSURE PROPERTY

   If $a \in G, b \in G$, then $a*b \in G \ \forall a,b \in G$.

2. G2: ASSOCIATIVE PROPERTY

   If $a,b,c \in G$, then $a*(b*c) = (a*b)*c \ \forall a,b,c \in G$.

3. G3: EXISTENCE OF IDENTITY

   There exists $e \in G$, such that $a*e = e*a = a \ \forall a \in G$.

4. G4: EXISTENCE OF INVERSE

   Every element of G has an inverse i.e. for every $a \in G$ there exists $b \in G$ such that $a*b = b*a = e$ as b is called the inverse of a and b is written as $(a^{-1}) = b$.

- A group with addition binary operation is known as Additive Group and that with multiplication binary operation is known as Multiplicative Group.

- Types of Group

1. ABELIAN GROUP

A group G is said to be abelian group, if it satisfies the commutative property. i.e.

G5: Commutativity

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

Abelian Group is also called as Commutative Group.

2. GROUPOID

An algebraic structure (G,*) is said to be a groupoid, if it satisfies the closure property only.

3. SEMI-GROUP

An algebraic structure (G,*) is said to be a semi group if it satisfies the closure and associative properties.

i.e. a groupoid is said to be a semi-group if it is associative.

4. MONOID

An algebraic structure is said to be monoid, if it satisfies closure, associative and existence of Identity Properties.

GROUPOID	G1
SEMI-GROUP	G1, G2
MONOID	G1, G2, G3
GROUP	G1, G2, G3, G4
ABELIAN GROUP	G1, G2, G3, G4, G5

5. SUB-SEMIGROUP

Let $(A, *)$ be a semigroup and B be a subset of A, then $(B, *)$ is called a Subsemigroup of $(A, *)$ if B is closed under the operation $*$.

i.e. $\boxed{\forall a, b \in B,\ a * b \in B}$

6. FREE SEMIGROUP (Beyond Syllabus)

- Let A be a non-empty set.
- A word w on A is a finite sequence of its elements

eg: $u = ababbbb = abab^4$ is a word on $A = \{a, b, c\}$

- The length of a word w, denoted by $\boxed{L(w)}$ is the number of elements in w

eg: $\boxed{L(u) = 8}$

- Let $v = baccaaaa = bac^2a^2$ be another word on A.
- The concatenation of words u and v on a set A, written as $u * v$ or uv, is the word obtained by writting down the elements of u followed by the elements of v.
- Now let $F = F(A)$ denote the collection of all words on A under the operation of concatenation.
- For any words u, v, w, the words $(u, v)w$ and $u(v, w)$ are identical ie. Associative.
- Thus F is a semigroup, it is called the 'Free Semigroup' on A and the elements of A are called the Generators of G.

- *General Properties of a Group (* Refer Lec no 1.C Pg 3.6)

THEOREM 1

The identity element in a group is unique.

THEOREM 02

The inverse of each element of a group is unique.

THEOREM 03

The inverse of the product of two elements of a group G is the product of the inverse taken in the reverse order i.e. $(ab)^{-1} = b^{-1}a^{-1}$.

THEOREM 04

For every element 'a' in a group G, prove that $(a^{-1})^{-1} = a$.

THEOREM 05

Cancellation Law : If a,b,c are any elements of G, then

$$ab = ac \Rightarrow b = c$$

$$ba = ca \Rightarrow b = c$$

- Order of an Element of a Group

• Let G be a group.

• By the order of the element $a \in G$, we mean the least positive integer 'n' such that $a^n = e$, where e is the identity element in G.

• If there does not exist an integer 'n' satisfying $a^n = e$ then we can say that the element $a \in G$ is of infinite order or zero order.

• The order of an element 'a' is denoted by o(a).

Q. Find the order of each element of the multiplicative group $G = \{1, -1, i, -i\}$

Solⁿ: W.k.t for multiplicative group; $\boxed{e = 1}$

$\therefore$ $o(1) = 1$

$o(-1) = 2$

$o(i) = 4$

$o(-i) = 4$

LECTURE NO 1.A [R1, R2]

Q1. Consider the set $A = \{-1, 0, 1\}$. Determine whether A is closed under
(i) Addition
(ii) Multiplication

Solⁿ: (i) Addition

+	-1	0	1
-1	-2	-1	0
0	-1	0	1
1	0	1	2

-2, 2 donot belong to set A
∴ A is not closed under addition

(ii) Multiplication

x	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

All the elements of $a*b$ belong to set A.
∴ A is closed under multiplication

Q2. Consider set $A = \{1, 3, 5, 7, 9, \ldots\}$ the set of odd integers. Determine whether A is closed under
(i) Addition (ii) Multiplication

Solⁿ: (i) Addition

+	1	3	5	7 ...
1	2	4	6	8 ...
3	4	6	8	10 ...
5	6	8	10	12 ...
7	8	10	12	14 ...
⋮	⋮	⋮	⋮	⋮

Not Closed

(ii) Multiplication

x	1	3	5	7 ...
1	1	3	5	7 ...
3	3	9	15	21 ...
5	5	15	25	35 ...
7	7	21	35	49 ...
⋮	⋮	⋮	⋮	⋮

Closed

Q3. Consider binary operation $*$ on Q, the set of rational nos, defined by $\boxed{a*b = a+b-ab}$ $\forall a,b \in Q$

Determine whether $*$ is associative.

Sol^n: Let us assume some elements $a,b,c \in Q$, then by definition

$$(a*b)*c = (a+b-ab)*c$$
$$= a+b-ab+c-(a+b-ab)c$$
$$\therefore \boxed{(a*b)*c = a+b+c-ab-ac-bc+abc} \quad \text{— I}$$

now

$$a*(b*c) = a*(b+c-bc)$$
$$= a+b+c-bc-a(b+c-bc)$$
$$\therefore \boxed{a*(b*c) = a+b+c-ab-bc-ac+abc} \quad \text{— II}$$

from I & II, we get

$$\boxed{(a*b)*c = a*(b*c)}$$

Hence Proved

Q4. Consider the binary operation $*$ on Q, the set of rational nos. defined by

$\boxed{a*b = a^2+b^2}$ $\forall a,b \in Q$

Determine whether $*$ is commutative

Sol^n: $a*b = a^2+b^2$ — I

$b*a = b^2+a^2 = a^2+b^2$ — II

from I & II, we get

$$\boxed{a*b = b*c}$$

Q5. Consider the binary operation $*$ on Q, defined by

$$\boxed{a * b = \frac{ab}{2}} \quad \forall\, a, b \in Q$$

Determine whether $*$ is
(i) Associative
(ii) Commutative

Sol^n: (i) Associative Property

we have,

$$a * b = \frac{ab}{2} \quad \text{---}$$

$$(a * b) * c = \frac{(a * b)c}{2}$$

$$= \frac{\left[\frac{ab}{2}\right]c}{2} = \frac{abc}{4} \quad \text{--- I}$$

$$a * (b * c) = \frac{a(b * c)}{2}$$

$$= \frac{a\left[\frac{bc}{2}\right]}{2} = \frac{abc}{4} \quad \text{--- II}$$

from I & II, we get $\boxed{(a * b) * c = a * (b * c)}$

(ii) Commutative Property

$$a * b = \frac{ab}{2} \quad \text{--- I}$$

$$b * a = \frac{ba}{2} = \frac{ab}{2} \quad \text{--- II}$$

from I & II, we get $\boxed{(a * b) = b * a}$

Hence Proved

UNIT 02

LECTURE 1.B [R2]

Q. Prove that $e_1' = e_1''$ where e_1' is a Right Identity and e_1'' is a left Identity of Binary Operation.

PROOF W.k.t e_1' is the right identity

$$\therefore \boxed{e_1'' * e_1' = e_1''} \quad \text{———} \quad \mathrm{I}$$

W.k.t e_1'' is the left identity

$$\therefore \boxed{e_1'' * e_1' = e_1'} \quad \text{———} \quad \mathrm{II}$$

From I & II, we get

$$\boxed{e_1' = e_1''}$$ Hence Proved.

Q. Consider the Binary Operation $*$ on I_+, the set of +ve integers defined by

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

Determine the identity for the binary operation $*$, if it exists.

Solⁿ: Let us assume that e be a +ve integer no, then

LEFT IDENTITY

Let $e \,\&\, a \in I_+$

$\boxed{e * a = a}$ — I (By Defⁿ.)

$\boxed{e * a = \frac{ea}{2}}$ — II (Given in Q)

from I & II, we get

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

$$\therefore \boxed{e = 2}$$

RIGHT IDENTITY

Let $e, a \in I_+$

$\boxed{a * e = a}$ — I (By Defⁿ.)

$\boxed{a * e = \frac{ae}{2}}$ — II (Given in Q.)

from I & II, we get

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

$$\therefore \boxed{e = 2}$$

Q. Consider the set $A = \{1, 2, 3\}$ and a binary operation $*$ on the set A defined by $a*b = 2a + 2b$. Represent operation $*$ as a table on A.

Solⁿ:

$*$	1	2	3
1	4	6	8
2	6	8	10
3	8	10	12

Q. Let Z be the set of Integers, show that operation $*$ on Z defined by $a*b = a+b+1 \;\forall a, b \in Z$ satisfies

(i) Closure Property

(ii) Associative Property

(iii) Commutative Property

(iv) Find Identity element if any

(v) Find Inverse element if any

Solⁿ: Let $Z = \{\ldots\ldots -2, -1, 0, 1, 2, 3, \ldots\}$

(i) Closure Property

$*$	-1	0	1
-1	-1	0	1
0	0	1	2
1	1	2	3

Since all the elements of Composition table belong to Z

$\therefore$ It satisfies Closure Property.

(ii) Associative Property $(a*b)*c = a*(b*c)$

LHS

$= (a*b)*c$

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

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

$= a+b+c+2$

$\therefore \boxed{(a*b)*c = a+b+c+2}$ — (I)

R.H.S

$= a*(b*c)$

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

$= a+b+c+1+1$

$= a+b+c+2$

$\therefore \boxed{a*(b*c) = a+b+c+2}$ — (II)

From (I) & (II), we get

It satisfies Associative Property

(iii) Commutative Property $(a*b) = (b*a)$

L.H.S

$= a*b$

$= a+b+1$

$\therefore \boxed{a*b = a+b+1}$ — (I)

R.H.S

$= b*a$

$= b+a+1$

$= a+b+1$

$\therefore \boxed{b*a = a+b+1}$ — (II)

From (I) & (II), we get
it satisfies Commutative Property.

iv) Identity Element

If e is the Identity element for $*$

then $\boxed{a*e = a}$ — (I) (By Defn)

also $\boxed{a*e = a+e+1}$ — (II) (Given in Q)

from (I) & (II), we get

$a+e+1 = a$

$e+1 = 0$

$\therefore \boxed{e = -1}$ and $-1 \in Z$ $\therefore$ Identity element exists.

v) Inverse Element

Let a have its inverse as b. Then

$a*b = e$ (by defn)

$\therefore \boxed{a*b = -1}$ — (I) (from above iv)

also $\boxed{a*b = a*b+1}$ — (II) (Given in Q)

from (I) & (II), we get

$a*b*1 = -1$

$a+b = -2$

$\boxed{b = -(2+a)}$

for different values of a, b will change and it belongs to Z $\therefore$ Inverse Exists.

Q. Consider an algebraic structure $(A, *)$ where $A = \{1, 3, 5, 7, 9, \ldots\}$, the set of all +ve odd integers and $*$ is a binary operation for addition & multiplication. Determine whether $(A, *)$ is a semi group?

Sol^n: For an algebraic structure to be a Semi Group, it should satisfy G1: Closure Property & G2: Associative Property.

(i) G1: Closure Property

+	1	3	5	7	9 ...
1	2	4	6	8	10 ...
3	4	6	8	10	12 ....
5	6	8	10	12	14 ....
7	8	10	12	14	16 ...
9	10	12	14	16	18 ...
⋮	⋮	⋮	⋮	⋮	⋮

For '+' operation the elements of composition table are +ve i.e. they do not belong to A
i.e. Closure property is not satisfied
$\boxed{\therefore (A, *) \text{ is not a Semi Group}}$

×	1	3	5	7	9 ...
1	1	3	5	7	9 ...
3	3	9	15	21	27 ...
5	5	15	25	35	45 ...
7	7	21	35	49	63 ...
9	9	27	45	63	81 ...
⋮	⋮	⋮	⋮	⋮	⋮

For 'x' operation the elements of composition table are -ve ie they belong to A
ie. $\boxed{\text{Closure property is satisfied}}$ — (I)

(ii) Associative Property $(a*b)*b = a*(b*c)$

for '+'

LHS: let $a=1, b=3, c=5$

$(a+b)+c = (1+3)+5$
$= 9$

RHS

$a+(b+c) = 1+(3+5)$
$= 9$

Associative property is satisfied but not Closure for '+'

for 'x'

LHS: Let $a=1, b=3, c=5$

$(a \times b) \times c = (1 \times 3) \times 5$
$= 15$

RHS:

$a \times (b \times c) = 1 \times (3 \times 5)$
$= 15$

$\boxed{\text{Associative Property is satisfied}}$ — (II)

From (I) & (II) $(A, *)$ is a Semi Group for

Q. Consider the algebraic structure $(\{0,1\}, *)$, where $*$ is a multiplication operation. Determine whether $(\{0,1\}, *)$ is a semigroup or not?

Sol^n: For an algebraic structure to be a semigroup, it should satisfy G1: Closure Property and G2: Associative Property.

i) Closure Property

$\times$	0	1
0	0	0
1	0	1

Since all the elements of composition table belong to $\{0,1\}$

$\therefore$ $\boxed{\text{Closure Property is satisfied}}$ — (I)

ii) Associative Property

Since there are only two elements so associativity is always satisfied.

$\therefore$ $\boxed{\text{Associative Property is satisfied}}$ — (II)

from (I) & (II), we get $(\{0,1\}, *)$ is a semi group.

Q. Let $(A,*)$ be a semigroup. Show that for a, b, c in A if $a*c = c*a$ and $b*c = c*b$, then $(a*b)*c = c*(a*b)$

Proof: LHS

$(a*b)*c = a*(b*c)$ ($\because$ $*$ is associative)

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

$= (a*c)*b$ ($\because$ $*$ is associative)

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

$= c*(a*b)$ ($\because$ $*$ is associative)

$=$ R.H.S

Hence Proved.

Congruence Relation

- An equivalence relation R on the semigroup $(S, *)$ is called a Congruence Relation if

$$\boxed{aRa' \ \& \ bRb' \Rightarrow (a*b)\ R\ (a'*b')}$$

Product of Semigroup (Theorem)

If $(S1,*)$ and $(S2,*)$ are Semigroups, then $(S1 \times S2, *)$ is a semigroup where $*$ is defined by

$$\boxed{(s_1', s_2') * (s_1'', s_2'') = (s_1' * s_1'', s_2' * s_2'')}$$

Q. Consider the set Z^+ of non-negative integers. Check whether the operation $*$ defined by $a*b = a^2+b$ $\forall a,b \in Z^+$ is associative or not.

Sol^n: Associative Property $a*(b*c) = (a*b)*c$

$$\text{LHS} = a*(b*c)$$

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

$$\boxed{\text{LHS} = a^2+b^2+c} \quad \text{——} \ \text{I}$$

$$\text{RHS} = (a*b)*c$$

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

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

$$\boxed{\text{RHS} = a^4+b^2+2a^2b+c} \quad \text{——} \ \text{II}$$

From I & II, we get

$$\text{LHS} \neq \text{RHS}$$

$\therefore$ $*$ does not satisfy Associative Property.

UNIT 02

LECTURE NO. 1.C [R1, R2]

*General Properties of a Group

THEOREM 1

The identity element in a group is unique.

PROOF

Let us suppose that $a \in G$ and e, e' be the two identities in G.

i.e $e \in G, a \in G \Rightarrow \boxed{ae = a}$ —— (I)

$e' \in G, a \in G \Rightarrow \boxed{ae' = a}$ —— (II)

From (I) & (II), we get

$$ae = ae'$$

$$\therefore \boxed{e = e'}$$

Hence Proved.

THEOREM 2

The inverse of each element of a group is unique

PROOF

Let $a \in G$ and $e \in G$ and let b & c be two inverses of a in G.

i.e. $a \in G, b \in G, e \in G \Rightarrow \boxed{ab = e}$ —— (I)

$a \in G, c \in G, e \in G \Rightarrow \boxed{ac = e}$ —— (II)

From (I) & (II), we get

$$ab = ac$$

$$\therefore \boxed{b = c}$$

Hence Proved

THEOREM 3

The inverse of the product of two elements of a group G is the product of the inverse taken in the reverse order ie $(ab)^{-1} = b^{-1}a^{-1}$

PROOF

Let $a, b \in G$

If a^{-1}, b^{-1} are the inverses of a and b respectively

so, $\left.\begin{aligned} a^{-1}.a = a.a^{-1} = e \\ b^{-1}.b = b.b^{-1} = e \end{aligned}\right\}$ where e is the Identity Element —— I

Now,

$$
\begin{aligned}
(ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} && \text{(Associative Law)} \\
&= a.e.a^{-1} && \text{(From I)} \\
&= a.a^{-1} && (e=1 \text{ for } x) \\
&= e. && \text{(from I)} \quad \text{—— II}
\end{aligned}
$$

$$
\begin{aligned}
(b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}.a)b && \text{(Associative Law)} \\
&= b^{-1}.e.b && \text{(From I)} \\
&= b^{-1}.b && (e=1 \text{ for } x) \\
&= e && \text{(From I)} \quad \text{—— III}
\end{aligned}
$$

From II & III we have proved that $b^{-1}a^{-1}$ is both right & left inverse element of ab.

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

Hence Proved.

THEOREM 4

For every element 'a' in a group G, prove that $(a^{-1})^{-1} = a$.

PROOF

Let e be the identity element of the group G.

Let $b \in G$ ~~then~~ $b^{-1} \in G$. also $\boxed{b.b^{-1} = e}$ —— (I)

$\therefore$ if $a \in G$ then $a^{-1} \in G$

Replace b by a^{-1} in equ^n (I), we get

$$(a^{-1})[(a^{-1})]^{-1} = e \quad \text{—— (II)}$$

Multiplying (II) by a on both sides

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

$$(aa^{-1})(a^{-1})^{-1} = a \qquad (\because a \cdot e = a)$$

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

$$\boxed{(a^{-1})^{-1} = a}$$

Hence Proved.

THEOREM 5 CANCELLATION LAW

If a, b, c are any elements of G, then

$ab = ac \Rightarrow b = c$ [LEFT CANCELLATION LAW]

$ba = ca \Rightarrow b = c$ [RIGHT CANCELLATION LAW]

PROOF

Let $a \in G \Rightarrow a^{-1} \in G$

now $ab = ac$ —— (I)

Multiplying (I) by a^{-1} on both sides

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

$$(a^{-1}a)b = (a^{-1}a)c \quad \text{[Associative Law]}$$

$$e \cdot b = e \cdot c$$

$$\therefore \boxed{b = c}$$

now $ba = ca$ —— (II)

Multiplying (II) by a^{-1} on both sides

$$(ba)a^{-1} = (ca)a^{-1}$$

$$b(aa^{-1}) = c(aa^{-1}) \quad \text{[Associative law]}$$

$$b.e = c \cdot e$$

$$\therefore \boxed{b = c}$$

Hence Proved.

Q. Let $(G,*)$ be a group. If $(G,*)$ is an Abelian group, then show that $a^3*b^3=(a*b)^3$ for all a and b in G.

Solⁿ: Suppose $(G,*)$ is an Abelian Group, then $\boxed{a*b=b*a}$ $\forall a,b\in G$ — (I)

now $\boxed{(a*b)^3=(a*b)^2*(a*b)}$ —— (II)

now
$$
\begin{aligned}
(a*b)^2 &= (a*b)*(a*b)\\
&= a*(b*a)*b\\
&= a*(a*b)*b \qquad [\text{from (I)}]\\
&= (a*a)*(b*b)
\end{aligned}
$$
$$\boxed{(a*b)^2=a^2*b^2} \text{ —— (III)}$$

Substituting (III) in (II), we get
$$
\begin{aligned}
(a*b)^3 &= (a^2*b^2)*(a*b)\\
&= [(a^2*b)*b]*(a*b)\\
&= (a^2*b)*(b*a)*b\\
&= (a^2*b)*(a*b)*b \qquad [\text{from (I)}]\\
&= a^2*(a*b)*(b*b)\\
&= a^2*(a*b)*b^2\\
&= (a^2*a)*(b*b^2)
\end{aligned}
$$
$$\therefore \boxed{(a*b)^3=a^3*b^3}$$

Hence Proved

References:

1. Liu and Mohapatra, "Elements of Discrete Mathematics", McGraw Hill
2. Jean Paul Trembley, R Manohar, "Discrete Mathematical Structures with Application to Computer Science", McGraw Hill

UNIT 02

KEYWORDS:
Subgroup, Cyclic Group

LECTURE NO. 02

Subgroup [R1, R2]

- Let G be a group, then any non-empty subset H of G is called the complex of the group G.
- A non-empty subset H of a group $(G,*)$ is said to be a subgroup if $(H,*)$ is also a group i.e., if $(G,*)$ is a group then the complex which satisfies all the axioms of the group is said to be Subgroup.
- All subgroups are complexes but all complexes are not subgroup.
- We know, every set is a subset of itself. Therefore, if G is a group, then G is a subgroup of G.
- Also, if e is the identity element of G, then the subset of G containing only identity element is also a subgroup of G.
- These two subgroups $(G,*)$ and $(\{e\},*)$ of the group $(G,*)$ are called improper or trivial subgroups, others are called proper or non-Trivial subgroups.

THEOREM 01

The identity element of a subgroup is the same as that of the group.

THEOREM 02

A non empty subset H of a group G is a subgroup of G iff

(i) $a \in H$, $b \in H \Rightarrow a*b \in H$

(ii) $a \in H \Rightarrow a^{-1} \in H$ where a^{-1} is the inverse of a in G.

THEOREM 03

The necessary and sufficient condition for a non-empty subset H of a group $(G, *)$ to be a subgroup is $a \in H, b \in H \Rightarrow a * b^{-1} \in H$ where b^{-1} is the inverse of b in G.

THEOREM 04

The intersection of any two sub-groups of a group $(G, *)$ is again a subgroup of $(G, *)$

THEOREM 05

Union of two subgroups is not necessarily a subgroup.

Cyclic Groups [R1, R2]

- A group G is called cyclic if for some $a \in G$, every element $x \in G$ is of the form a^n, where n is some integer.
- The element 'a' is then called a generator of G. $i^2 = 1$ $i^4 = 1$

  - Example: multiplicative Group $G = \{1, -1, i, -i\}$ is cyclic. where i is a generator such that $G = \{i, i^2, i^3, i^4\}$
  $-i$ is a generator such that $G = \{-i, (-i)^2, (-i)^3, (-i)^4\}$
- Example:

  The multiplicative group $G = \{1, -1, i, -i\}$ is cyclic where i & $-i$ are generator of G.

- If H is a cyclic group generated by 'a' subject to all powers of a are distinct, then $H = \langle a \rangle$ is an <u>infinite cyclic group</u>.

- Example: The group $(G, +_6)$ is a cyclic group where $G = \{0, 1, 2, 3, 4, 5\}$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	[illegible]

$(1)^0 = 0$
$(1)^1 = \cancel{1+_61} = 1$
$(1)^2 = 1 +_6 1 = 2$
$(1)^3 = 1 +_6 1^2 = 1 +_6 1 +_6 1 = 2 +_6 1 = 3$
$(1)^4 = 1 +_6 1^3 = 1 +_6 3 = 4$
$(1)^5 = 1 +_6 1^4 = 1 +_6 4 = 5$

$(2)^0 = 0$
$(2)^1 = 2$
$(2)^2 = 2 +_6 2 = 4$
$(2)^3 = 2 +_6 2^2 = 2 +_6 4 = 0$

References:

1. Liu and Mohapatra, "Elements of Discrete Mathematics," McGraw Hill.
2. Jean Paul Trembley, R Manohar, "Discrete Mathematical Structures with Applications to Computer Science," McGraw Hill

KEYWORDS:
Cosets, Normal Subgroup

LECTURE NO. 03

Cosets [R1]

- Suppose G is a group and H is any subgroup of G.
- Let 'a' be any element of G, then the set $\boxed{Ha = \{ha : h \in H\}}$ is called Right Coset of H in G generated by 'a'.
- Similarily, the set $\boxed{aH = \{ah : a \in H\}}$ is called Left Coset of H in G generated by a.
- If e is the identity element of G, then $\boxed{He = H = eH}$

∴ in this case, H itself is a right as well as left coset.

- Since H is a subgroup of G, then there exists $e \in H$. So that if Ha is a right coset of H in G then ea is an element of Ha, i.e $a \in Ha$.
- Similarily, a is an element of the left coset aH.
- Thus, no left coset and no right coset can be empty
- If the group G is abelian, then we have $ah = ha \; \forall h \in H$ therefore the right coset Ha will be equal to the corresponding left coset aH.
- If H is a subgroup of group G, the number of distinct left or right cosets of H in G is called the index of H in G and is denoted by $\boxed{[G:H] \text{ or } i_G(H)}$.

- Properties of Cosets

1. $a \in aH$
2. $aH = H$ iff $a \in H$
3. $aH = bH$ or $aH \cap bH = \phi$
4. $aH = bH$ iff $a^{-1}b \in H$

Normal Subgroup [R1]

- A subgroup H of a group G is normal subgroup if $a^{-1} H a \subseteq H$ for every $a \in G$.
- Equivalently, H is normal if $aH = Ha \; \forall a \in G$, i.e. if the right and left cosets coincide.
- Clearly every subgroup of an abelian group is a normal subgroup.
- To verify that a subgroup is normal one can use the following theorem.

THEOREM 01

A subgroup H of a group G is normal iff $g^{-1} h g \in H$ for every $h \in H, g \in G$.

THEOREM 02

Let H be a normal subgroup of a group G. Then the cosets of H form a group under coset multiplication.

$$\boxed{(aH)(bH) = abH}$$

References:

1. Jean Paul Trembley, R Manohar, "Discrete Mathematical Structures with Applications to Computer Science," McGraw Hill

Q] If G is an additive group of all integers and H is additive subgroup of all even integers of G, then find all the cosets of H in G

Sol^n: Let $G = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$

and $H = \{0, \pm 2, \pm 4, \cdots\}$

Then Right cosets of H in G are

$$Ha = \{ha : h \in H\}$$

$$H+0 = \{0, \pm 2 \pm 4, \pm 6 \cdots\}$$

$$H+1 = \{0+1, \pm 2+1, \pm 4+1 \cdots\}$$

$$= \{1, 3, -1, 5, -3 \ldots\}$$

$$H+2 = \{0+2, \pm 2+2, \pm 4+2 \cdots\}$$

$$= \{2, 4, 0, 6, -2, \cdots\}$$

Also, Left cosets of H in G are

$$aH = \{ah : h \in H\}$$

$$0+H = \{0, \pm 2 \pm 4 \pm 6 \pm \ldots\}$$

$$1+H = \{1+0, 1\pm 2, 1\pm 4 \ldots\} = \{1, 3, -1, 5, -3 \ldots\}$$

$$2+H = \{2+0, 2\pm 2, 2\pm 4 \ldots\} = \{2, 4, 0, 6, -2 \ldots\}$$

Q] Consider the group Z of integers under addition & the subgroup $H = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$ considering the multiple of 5. Find cosets of H in Z.

Sol^n: Let $G = \{0, \pm 1, \pm 2, \pm 3, \dots\}$

and $H = \{\dots, -10, -5, 0, 5, 10 \dots\}$ (given)

Then Right cosets of H in G are

$$Ha = \{ha : h \in H\}$$

$$H+0 = \{\dots -10, -5, 0, 5, 10 \dots\}$$

$$H+1 = \{\dots, -10+1, -5+1, 0+1, 5+1, 10+1, \dots\}$$

$$= \{\dots, -9, -4, 1, 6, 11 \dots\}$$

$$H+2 = \{\dots, -10+2, -5+2, 0+2, 5+2, 10+2, \dots\}$$

$$= \{\dots, -8, -3, 2, 7, 12, \dots\}$$

Also, Left Cosets of H in G are

$$aH = \{ah : h \in G\}$$

$$0+H = \{\dots, -10, -5, 0, 5, 10, \dots\}$$

$$1+H = \{\dots, 1+(-10), 1+(-5), 1+0, 1+5, 1+10, \dots\}$$

$$= \{\dots, -9, -4, 1, 6, 11, \dots\}$$

$$2+H = \{\dots, 2+(-10), 2+(-5), 2+0, 2+5, 2+10, \dots\}$$

$$= \{\dots -8, -3, 2, 7, 12, \dots\}$$

Theorem: The union of all left or right cosets of H in G is equal to G ie. $\boxed{G = Ha_1 \cup Ha_2 \cup Ha_3 \cup Ha_4 \dots \cup Ha_k}$ — (A)

Order of a Group

- The number of elements in a group is called the order of the group.
- It is denoted by $O(G)$.
- A group of finite order is called finite group.

Lagrange's Theorem

STATEMENT 1

The $\underbrace{\text{order}}_{\text{no. of elements of a Subgroup}}$ of each sub-group of a finite group G is a divisor of the $\underbrace{\text{order of the group G}}_{\text{no. of elements of a group}}$.

STATEMENT 2

The order of a sub-group H of group G divides the order of G.

PROOF

- Let G be finite group of order n

  ie. $\boxed{O(G) = n}$

  ie. $\boxed{G = \{a_1, a_2, a_3, \dots, a_n\}}$

- Let H be subgroup of G of order m

  ie. $\boxed{O(H) = m}$

  ie. $\boxed{H = \{h_1, h_2, h_3, \dots, h_m\}}$

- Let $a_1 \in G$, then

$Ha_1 = \{h_1a_1, h_2a_1, h_3a_1, \ldots, h_ma_1\}$ be right coset of H in G generated by a_1 having all distinct elements.

- Suppose if possible,

$$h_ia = h_ja$$

$$\therefore \boxed{h_i = h_j} \text{ (By left cancellation law)} \quad \text{— I}$$

$\therefore$ by equ^n I, each right coset of H in G has m distinct elements

- w.k.t, the union of all left or right coset of H in G is equal to group. (from Theorem A)

ie. $\boxed{G = Ha_1 \cup Ha_2 \cup Ha_3 \cup Ha_4 \cup \ldots \cup Ha_K}$

where

$Ha_1 = \{h_1a_1, h_2a_1, h_3a_1, h_4a_1, \ldots, h_ma_1\}$

$Ha_2 = \{h_1a_2, h_2a_2, h_3a_2, h_4a_2, \ldots, h_ma_2\}$

$Ha_3 = \{h_1a_3, h_2a_3, h_3a_3, h_4a_3, \ldots h_ma_3\}$

$\vdots$

$Ha_K = \{h_1a_K, h_2a_K, h_3a_K, h_4a_K, \ldots h_ma_K\}$

- now, number of elements in G = number of elements in Ha_1 + number of elements in Ha_2 + number of elements in Ha_3 + … + number of elements in Ha_K

$\Longrightarrow \quad n = m + m + m + \cdots + K\text{times}$

$\Longrightarrow \quad n = mk$

$\Rightarrow k = \frac{n}{m}$

$\Rightarrow \boxed{k = \frac{O(G)}{O(H)}}$ ——— II

from II, we can observe that "O(H) is the divisor of O(G)"

Hence proved

Quotient Group

- Also called as Factor Group.
- The set of all cosets of H in G is known as Quotient or Factor Group.
- Denoted as $\boxed{G/H}$

$$\boxed{G/H = \{Ha : a \in G\}}$$

THEOREM 1

The product of two right (left) cosets in G is also right (left) coset in G.

THEOREM 2

The set of all cosets of a normal subgroup is a group w.r.t multiplication.

THEOREM 3

There exists an one-to-one correspondance between the elements of subgroup H and those of any cosets of H in G.

UNIT 02

LECTURE NO. 05

KEYWORDS:
Permutation,
Permutation Group,
Cyclic Permutation,
Transposition

Permutation [R1]

- Suppose S be a finite set having 'n' distinct elements, then a one-to-one mapping of S onto itself is called a Permutation of degree 'n'.
- That is a function $f: S \rightarrow S$ is said to be permutation of S if
  - (i) f is one-one
  - (ii) f is onto
- The number of distinct elements in the finite set S is known as the Degree of permutation.

Symbol of Permutation [R1]

- If $S = \{1, 2, 3, 4\}$ is a finite set having 4 elements then $f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{bmatrix}$ etc. are called permutation; where $f(1) = 2$, $f(2) = 4$, $f(3) = 1$ and $f(4) = 3$. i.e. each element in the second row is the f-image of the element of the first row lying directly above it.
- In general, it is written as

$$f = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{bmatrix}$$

Equality of Two Permutations [R1, R2, R3]

- Let f and g are two permutations on a set S, then $f = g$ iff $f(x) = g(x)$ $\forall$ $x \in S$.

- Example:

If $f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$, $g = \begin{bmatrix} 2 & 4 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{bmatrix}$

are two permutations of degree 4.

then we have $f = g$, because

$$f(1) = 2 = g(1)$$
$$f(2) = 3 = g(2)$$
$$f(3) = 4 = g(3)$$
$$f(4) = 1 = g(4)$$

Identity Permutation [R3]

- If each element of a permutation be replaced by itself, then it is called the Identity Permutation and is denoted by symbol I.
- Example:

$$I = \begin{bmatrix} a & b & c \\ a & b & c \end{bmatrix}$$

Product of Permutations / Composition of Permutation [R3]

- The product of two permutations f and g of same degree is denoted by $f \circ g$ or fg, meaning first perform f and then perform g.
- $f = \begin{bmatrix} a_1 & a_2 & a_3 \dots & a_n \\ b_1 & b_2 & b_3 \dots & b_n \end{bmatrix}$, $g = \begin{bmatrix} b_1 & b_2 & b_3 \dots & b_n \\ c_1 & c_2 & c_3 \dots & c_n \end{bmatrix}$

then $f \circ g = \begin{bmatrix} a_1 & a_2 & a_3 \dots & a_n \\ c_1 & c_2 & c_3 \dots & c_n \end{bmatrix}$

- It should be observed that the permutation g has been written in such a manner that the second row of f coincides with the first row of g.

Inverse Permutation [R3]

- Since a permutation is one-one, onto map and hence it is invertible, i.e., every permutation f on a set.

$$P = \{a_1, a_2, \ldots, a_n\}$$

has a unique inverse permutation denoted by f^{-1}

Thus if $f = \begin{bmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{bmatrix}$

then $f^{-1} = \begin{bmatrix} b_1 & b_2 & \ldots & b_n \\ a_1 & a_2 & \ldots & a_n \end{bmatrix}$

Total number of Permutations [R3]

- Let X be a set consisting of n distinct elements.
- Then the elements of X can be permuted in $n!$ distinct ways.
- If S_n be the set consisting of all permutations of degree n, then the set S_n will have $n!$ distinct permutations of degree n.
- This set S_n is called the symmetric set of permutations of degree n.
- Example: if $A = \{1, 2, 3\}$, then $n = 3$

$\therefore S_3 = \{p_0, p_1, p_2, p_3, p_4, p_5\}$, where

$p_0 = I_A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$ $\quad p_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$

$p_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$ $\quad p_3 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$

$p_4 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$ $\quad p_5 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$

Permutation Group [R1, R2]

- Let A be a set of degree n.
- Let P_n be the set of all permutations of degree n on A. Then $(P_n, *)$ is a group, called a Permutation Group and the operation $*$ is the composition of permutations.
- Also called as Symmetric Group.

THEOREM

The set P_n of all permutations on n symbols is finite group of order $n!$ w.r.t the binary composition of permutations.

For $n \leq 2$, P_n is abelian group and for $n > 2$ it is always non-abelian.

- Permutation group follows the following properties:

1. Closure Property
2. Associativity
3. Existence of Identity
4. Existence of Inverse

Cyclic Permutations [R1, R2]

- Let f be a permutation of degree 'n' on a set S having 'n' distinct elements.
- Suppose it is possible to arrange 'm' elements of the set 'S' in a row in such a way that the f-image of each element of the set S in a row is the element follows it, the f-image of the last element is the first element and the remaining $(n-m)$ elements of the set S are left unchanged by f.
- Then f is called a Cyclic Permutation.

- Example:

$$f = (1, 3, 4, 5) = \begin{bmatrix} 1 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 \end{bmatrix}$$

Length of a Cycle [R3]

- By the length of a cycle, we mean the number of elements permuted by a cycle.
- A cycle of length one means that the image of an element is the element itself and represents Identity Permutation. cycle of length one are generally omitted.
- Disjoint Cycles* Refer Pg 11 are those which have no common elements. Every permutation of a finite set can be expressed as a cycle or as a product of disjoint cycles.
- Example: $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}$

  this is written as (1, 2), (3, 4, 6), (5)

  Cycle (1, 2) has length 2.
  Cycle (3, 4, 6) has length 3.
  Cycle (5) has length 1.

Transposition (Refer Pg10). [R3]

- A cyclic permutation such as (a, b) which interchange the symbols leaving all other unchanged is called a transposition.
- In other words, transposition is a cycle of length 2.

Even and Odd Permutations (Refer Pg10) [R3]

- A permutation is said to be an even permutation if it can be expressed as a product of an even number of transpositions otherwise it is said to be an odd permutation.

Alternating Group [R3]

- The set A_n of all even permutations of degree 'n' forms a finite group of order $\frac{n!}{2}$ w.r.t the composition of permutation and is called Alternative Group and is denoted by A_n.

Symmetric Group (Cont. from Pg 08) [R1, R2]

- Refer example from pg 08
  here $A = \{1, 2, 3\}$ and $S_3 = \{\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5\}$

- Now multiplication table for S_3

$\circ$	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_1	ρ_1	ρ_2	ρ_0	ρ_5	ρ_3	ρ_4
ρ_2	ρ_2	ρ_0	ρ_1	ρ_4	ρ_5	ρ_3
ρ_3	ρ_3	ρ_4	ρ_5	ρ_0	ρ_2	ρ_2
ρ_4	ρ_4	ρ_5	ρ_3	ρ_1	ρ_0	ρ_1
ρ_5	ρ_5	ρ_3	ρ_4	ρ_2	ρ_1	ρ_0

- The table shows that:

  i) The multiplication of any two permutations of S_3 gives a permutation of S_3. So S_3 is closed w.r.t multiplication.

  ii) Associativity holds for $(\rho_1 \rho_3)\rho_4 = \rho_5 \rho_4 = \rho_0$ &
  $\rho_1(\rho_3 \rho_4) = \rho_1 \rho_1 = \rho_0$

  iii) Identity element exists, ρ_0 when composed with any permutation gives that permutation.

  iv) Every permutation has its own inverse.

Hence S_3 is a group. Not an abelian group since $\rho_1\rho_2 \neq \rho_2\rho_1$, $\rho_3\rho_2 \neq \rho_2\rho_3$ and so on.

Example for Transposition (Cont. from Pg 09) [R3]

- A transposition is a cycle of length 2.
- $\therefore$ In $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}$, (1,2) is a cycle of length 2
  $\therefore$ (1,2) is a transposition.

Example of Even and Odd Permutation [R1, R2, R3]

- When a permutation can be expressed as a product of even no. of transposition it is called Even Permutation
- Example: $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{bmatrix}$

$$= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{bmatrix} = (1\ 6)(2\ 3\ 4\ 5)$$

$$= (1\ 6)(2\ 3)(2\ 4)(2\ 5)$$

= product of Even no of Transpositions.

- When a permutation can be expressed as a product of odd no. of transposition it is called Odd Permutation
- Example: $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{bmatrix}$

$$= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{bmatrix} = (1\ 5)(2\ 6\ 3)$$

$$= (1\ 5)(2\ 6)(2\ 3)$$

= product of odd no. of Transpositions

Q] Show that $f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 1 & 8 & 5 & 6 & 2 & 4 \end{bmatrix}$ is even

Solⁿ: We have

$$f = \begin{bmatrix} 1 & 7 & 2 & 3 \\ 7 & 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 4 & 8 \\ 8 & 4 \end{bmatrix} \begin{bmatrix} 5 \\ 5 \end{bmatrix} \begin{bmatrix} 6 \\ 6 \end{bmatrix}$$

$$= \underbrace{(1\ 7\ 2\ 3)}_{\text{Break this cycle into transposition}} \underbrace{(4\ 8)}_{\text{Transposition}} \underbrace{(5)(6)}_{\text{ignore cycles with length 1}}$$

$= (1\,7)(1\,2)(1\,3)(4\,8)$

= product of even transpositions

$\therefore f$ is even.

Q] Show that $f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 3 & 6 & 5 & 8 & 7 & 2 \end{bmatrix}$ is odd.

Solⁿ: We have

$$f = \begin{bmatrix} 2 & 4 & 6 & 8 \\ 4 & 6 & 8 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \begin{bmatrix} 5 \\ 5 \end{bmatrix} \begin{bmatrix} 7 \\ 7 \end{bmatrix} \begin{bmatrix} 3 \\ 3 \end{bmatrix}$$

$$= \underbrace{(2\ 4\ 6\ 8)}_{\text{Break this cycle into transposition}} \underbrace{(1)(5)(7)(3)}_{\text{ignore cycles with length 1}}$$

$= (2\,4)(2\,6)(2\,8)$

= product of odd transposition.

$\therefore f$ is odd.

Disjoint Cycle [R1]

- Let $S_n = \{a_1, a_2, a_3, \ldots, a_n\}$. If f and g are two cycles on S such that they have no element in common, then f and g are said to be disjoint cycle.

* NOTE :

1. The product of two disjoint cycles is commutative.
2. Even & Odd permutations can be written as a product of Disjoint cycles & Transpositions.

- Example of Disjoint cycle:

$S = \{1, 2, 3, 4, 5, 6\}$

then $f = (1, 4, 5)$ and $g = (2, 3, 6)$ are disjoint cycles because they have no elements in common & are cyclic in nature.

- Example on Note 1

Let $f = (1, 2, 3)$ and $g = (4, 5)$ be two permutations of S_5

Then

$$fg = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{bmatrix}$$

$$gf = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{bmatrix}$$

$\therefore \boxed{fg = gh}$ ie. Disjoint cycles are commutative.

KEYWORDS:
Homomorphism, Isomorphism

LECTURE NO 06

Homomorphism * Refer Pg 13 [R1, R2]

- Homomorphism is also termed as Homomorphic Mapping.
- Suppose G and G' are two groups. A mapping f from G into G' is said to be homomorphic mapping or homomorphism of G into G' if

$$f(a.b) = f(a).f(b) \quad \forall \; a, b \in G$$

- If f is a homomorphic mapping of a group G onto the group G' so that $f(G) = G'$ then the group G' is called a homomorphic image of the group G.
- In general, a mapping $f: G \to G'$ where $(G, *)$ and (G', o) are groups, is called a homomorphism if for each $a, b \in G$.
- We have $\boxed{f(a*b) = f(a) \circ f(b)}$

* Note: If $(A, *)$ & (A', o) are two semigroups, then $f: A \to A'$ is called a semigroup Homomorphism if $\boxed{f(a*b) = f(a) \circ f(b)}$ where $a, b \in A$, where $f(a)$ & $f(b)$ shall be images of a & b in A'

* Note ① If f is surjective it is said to be a semigroup Epimorphism
② If f is injective it is said to be a semigroup monomorphism
③ If f is Bijective it is said to be a semigroup Isomorphism

Isomorphism [R1, R2]

- A mapping $f: G \to G'$ where $(G, *)$ and (G', o) are groups, is an isomorphism if
  i) f is one-to-one i.e., distinct elements in G have distinct f-image in G'
  ii) f is onto and
  iii) f is homomorphism

Isomorphic Groups [R1, R2]

- Suppose G and G' are two groups.
- Further suppose that the compositions in both G and G' have been denoted multiplicatively.

- Then we say that the group G is isomorphic to the group G' if there exists a one-to-one mapping f of G onto G' such that $\boxed{f(ab) = f(a)f(b) \ \forall\, a,b \in G}$ i.e. mapping f preserves the compositions in G and G'.

- If the group G is isomorphic to the group G', symbolically we write $G \cong G'$. Another notation for isomorphism $\cong$.

Endomorphism [R1, R2]

- A homomorphism of a group into itself is called an endomorphism

$$f : G \to G$$

1. f is onto 2. $f(a,b) = f(a) \cdot f(b)$

Kernel of Homomorphism [R2]

If f be homomorphism of group G into G' then a subset k is said to be kernel if it consists of all those elements of G whose image is the identity of G'

$$\boxed{\ker f = k = \{\alpha : f(\alpha) = e' \ \forall\, a \in G\}}$$

Automorphism [R2]

By automorphism, we mean isomorphism of G onto itself.

$$\boxed{f : G \xrightarrow[\text{onto}]{\text{one-one}} G \text{ is an automorphism of } G \text{ if } f(ab) = f(a)f(b) \ \forall\, a,b \in G}$$

Examples on Homomorphism [R3]

1. Let $f:\langle R,+\rangle \to \langle R^+, *\rangle$ be the function such that $f(x)=e^x$. Show that f is a homomorphism.

Sol^n: $f(x+y) = f(x)\cdot f(y)$

i.e. $e^{x+y} = e^x \cdot e^y$ (by properties of Exponents)

$\therefore f$ is a homomorphic function

2. Let $f: \langle Z,+\rangle \to \langle R,\cdot\rangle$ where $f(x)=x+1$. Show that whether f is a homomorphic function

Sol^n: For f to be homomorphic it should satisfy the following condition.

$$\boxed{f(x+y) = f(x)\cdot f(y)}$$

now, for $f(1+2) = f(3) = 3+1 = 4$

and $f(1)\cdot f(2) = (1+1)\cdot(2+1) = 6$

$\therefore f(1+2) \neq f(1)\cdot f(2)$

$\therefore f$ is not homomorphic.

Examples on Isomorphism [R3]

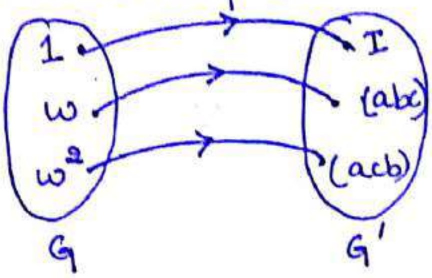
1. Show that the multiplicative group $G = \{1, \omega, \omega^2\}$ is isomorphic to permutation group of $G' = \{I, (abc), (acb)\}$ on three symbols.

Sol^n: We can see that

for G: $o(1)=1$, $o(\omega)=3$, $o(\omega^2)=3$

for $G' = o(I)=1$, $o(abc)=3$, $o(acb)=3$

Let us define the mapping $f: G \to G'$ such that same order elements map each other



Then, we can say f is one-to-one and onto.
now for f to be homomorphic it should satisfy

$\boxed{f(x \cdot y) = f(x) \cdot f(y)}$ (because G1 is multiplicative Group & G2 a Permutation Group)

for $f(\omega \cdot \omega^2) = f(\omega^3)$
$= f(1)$
$= I = \begin{bmatrix} a & b & c \\ a & b & c \end{bmatrix}$ (identity Permutation)

now $f(\omega) \cdot f(\omega^2) = (abc)(acb)$
$= \begin{bmatrix} a & b & c \\ b & c & a \end{bmatrix} \begin{bmatrix} a & c & b \\ c & b & a \end{bmatrix}$

$= \begin{bmatrix} a & b & c \\ a & b & c \end{bmatrix} = I$

$\therefore f(\omega \cdot \omega^2) = f(\omega) \cdot f(\omega^2)$

$\therefore$ f is isomorphic.

2. If G is a multiplicative group of three cube roots of unity i.e. $G = \{1, \omega, \omega^2\}$ where $\omega^3 = 1$ and G' be the additive group of integers modulus 3 i.e. $G' = \{0, 1, 2\} +_3$. Find if f is isomorphic.

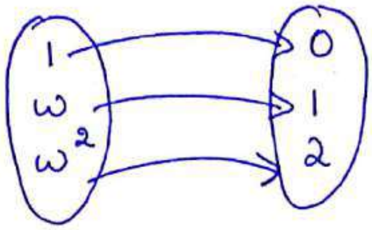
Solⁿ: Composition Table for G & G' is as follows.

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Let the mapping of f be defined as

$$f : G \rightarrow G'$$



$\therefore f$ is one-to-one & onto.

now for f to be homomorphic it should satisfy

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

so, $f(1 \cdot \omega) = f(\omega)$

$= 1$

$f(1) + f(\omega) = 0 + 1$

$= 1$

$\therefore f(1 \cdot \omega) = f(1) + f(\omega)$

$\therefore f$ is isomorphic

References:

1. PDF: Homomorphisms 1. Introduction to Group Theory, " www. math. uconn. edu".
2. PDF: Group Homomorphism," facstaff. cbu. edu"

Q. Let A be a set of all even integers. Show that function $f: (Z,+) \rightarrow (A,+)$ defined by $f(x) = 2x \ \forall x \in Z$ is a semigroup isomorphism.

Solⁿ: To show that f is one-one

assume that $a_1, a_2 \in Z$ and $f(a_1) = f(a_2)$

$\Rightarrow 2a_1 = 2a_2$ (given)

$\therefore a_1 = a_2$

$\therefore$ f is one-one

To show that f is onto

assume that $b \in A \Rightarrow b$ is even.

It means that $\boxed{b = 2a}$ for some $a \in Z$

ie b or 2a is the image in set A.

as $\boxed{b = 2a = f(a)}$

$\therefore$ f is onto

To prove that f is homomorphism

assume $a_1, a_2 \in Z$, then

$$f(a_1 + a_2) = 2(a_1 + a_2)$$
$$= 2a_1 + 2a_2$$
$$= f(a_1) + f(a_2)$$

$\therefore$ f is homomorphism.

since all three conditions are satisfied, $\therefore$ f is is a semigroup Isomorphism.

Congruence Relation

An equivalence relation R on a semigroup $(A, *)$ is called a congruence relation if

$$\boxed{aRa' \text{ and } bRb' \Rightarrow (a*b) \, R \, (a'*b')}$$

Q. let $(Z, +)$ be a semigroup and $f(x) = x^2 - x - 2$. Let R be a relation on Z defined as aRb iff $f(a) = f(b)$ then show that R is not a congruence relation.

Solⁿ: for a relation R be a congruence relation, the following condition must be satisfied

if $\boxed{aRa' \text{ and } bRb' \Rightarrow (a*b)\, R\, (a'*b')}$

for a semigroup $(A, *)$ where $a, a', b, b' \in A$

now let $a = -1$, $b = -2$, $a' = 2$ and $b' = 3 \in A$.

then according to definition

L.H.S.

if aRa' and bRb'

ie $-1 R 2 \Rightarrow f(-1) = f(2)$

$f(-1) \Rightarrow (-1)^2 - (-1) - 2 \Rightarrow 1 + 1 - 2 = 0$

$f(2) \Rightarrow (2)^2 - (2) - 2 = 4 - 4 = 0$

$\therefore aRa'$

and $-2 R 3 \Rightarrow f(-2) = f(3)$

$f(-2) \Rightarrow (-2)^2 - (-2) - 2 = 4$

$f(3) \Rightarrow (3)^2 - (3) - 2 = 4$

$\therefore bRb'$

and since aRa' and bRb'

RHS $\Rightarrow (a*b)\, R\, (a'*b')$ ie $f(a*b) = f(a'*b')$

now $(a*b) \Rightarrow -1 + -2 = -3 \quad \therefore f(-3) = (-3)^2 - (-3) - 2 = 10$

$(a'*b') \Rightarrow 2 + 3 = 5 \quad \therefore f(5) = (5)^2 - (5) - 2 = 18$

since $f(-3) \neq f(5)$

$\therefore$ LHS $\not\Rightarrow$ RHS

and hence f is not a congruence relation.

Q. Show that if $(Z,+)$ is a semigroup and R is an equivalence relation on Z defined by aRb iff $a \equiv b \pmod 2$ [ie a and b give the same remainder when divided by 2] then R is a congruence relation.

Sol^n: let $a,b,c,d \in Z$

$$\left.\begin{aligned} a \equiv b \pmod 2 &\Rightarrow (a-b)/2 \\ \text{and } c \equiv d \pmod 2 &\Rightarrow (c-d)/2 \end{aligned}\right] — (A)$$

which means

$a-b = 2m$ — (I)   from (I) & (II), aRb and cRd

and $c-d = 2n$ — (II)   where $m,n \in Z$

adding (I) & (II), we get

$$(a-b)+(c-d) = 2m+2n$$

$$(a-b)+(c-d) = 2(m+n)$$

ie $(a-b)+(c-d) = 2(m+n)$

ie $(a+c)-(b+d) = 2(m+n)$ — (B)

ie from (A) & (B) we get

$$\boxed{(a+c) \equiv (b+d) \pmod 2}$$

$\therefore$ aRb and cRd $\Rightarrow (a+c) R (b+d)$

$\therefore$ R is a congruence relation.

Scanned by CamScanner

LECTURE NO. 07

Rings

- A ring $(R, *, \circ)$ is a set R together with two binary operations $*$ and $\circ$ defined on R such that the following axioms are satisfied.

R1. The first operation is associative ie $(a*b)*c = a*(b*c)$ $\forall a, b, c \in R$

R2. The first operation is commutative ie $a*b = b*a$ $\forall a, b \in R$

R3. There exists an element 0 in R such that $a*0 = a = 0*a$ $\forall a \in R$

Note: Here 0 is any element $\in R$ and it does not mean the number zero. It is called zero element or Identity element for the operation $*$.

R4. To each element $a \in R$ there exists an element $(-a) \in R$ such that $a*(-a) = 0 = (-a)*a$

Note: Here $(-a)$ is not the negative of a. It denotes an element in R such that if we apply the operation $*$ between $(-a)$ and a, the resulting element is the zero element.

R5. The second operation is associative ie. $a \circ (b \circ c) = (a \circ b) \circ c$ $\forall a, b, c \in R$

R6. The second operation is distributive over first operation

ie. $a \circ (b*c) = (a \circ b)*(a \circ c)$ [Left Distributive Law]

and $(b*c) \circ a = (b \circ a) * (c \circ a)$ [Right Distributive Law]

- That is, an algebraic structure $(R, *, \circ)$ is called a Ring if

i) $(R, *)$ is an abelian group.

ii) $(R, \circ)$ is a semigroup

iii) $\circ$ is distributive over $*$

Commutative Ring

- It is a ring R in which the second operation $\circ$ is commutative ie. $a \circ b = b \circ a \ \forall a, b \in R$.

Ring with Unity

- It is a ring R which contains an identity element $e \in R$ for the second operation. OR
- If in a ring R there exists an element denoted by e such that $e \circ a = a \circ e = a \ \forall a \in R$, then R is called a Ring with unity.

<u>Note</u>: In a ring R, an element $e \in R$ is called an Unit (Identity) element.

<u>Note</u>: An unit element of a ring R (if it exists) is an element of the semigroup $(R, \circ)$.

Null Ring or Zero Ring

- The set R consisting of a single element e (unit element) and equipped with two binary operation defined as $e * e = e$ and $e \circ e = e$ is called a null ring.

Properties of a Ring

<u>THEOREM 1</u>: In a ring R, $\forall a, b, c \in R$

a) $a \circ 0 = 0 \circ a = 0$

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

c) $(-a) \circ (-b) = a \circ b$

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

e) $(b - c) \circ a = b \circ a - c \circ a$

<u>PROOF</u>:

a) $a \circ 0 = a \circ (0 * 0)$ [since $0 * 0 = 0$, 0 being identity in R for $*$]

$= a \circ 0 * a \circ 0$ [distributive law]

$0 = a \circ 0$ [by Right cancellation law] —— (I)

Similarily, $0 \circ a = (0 * 0) \circ a$

$= 0 \circ a * 0 \circ a$

$0 = 0 \circ a$ —— (II)

Scanned by CamScanner

From (I) & (II), we get

$a \circ 0 = 0 \circ a = 0$

Hence Proved.

b) w.k.t $a \circ [(-b) * b] = a \circ 0$ [since 0 is identity in R for *]

or $a \circ (-b) * a \circ b = 0$ [since $a \circ 0 = 0$ by result (a)]

Similarily $(-a * a) \circ b = 0 \circ b$

or $(-a) \circ b * a \circ b = 0$

$\Rightarrow (-a) \circ b = -(a \circ b)$ [since in a Ring, $a * b \Rightarrow a = -b$]

Hence Proved

c) w.k.t $(-a) \circ (-b) = -[(-a) \circ b]$

$= -[-(a \circ b)]$ [since $(-a) \circ b = -(a \circ b)$]

$= a \circ b$ (since R is a group w.r.t * in which $-(-a) = a$)

Hence Proved

d) $a \circ (b - c) = a \circ [b * (-c)]$

$= a \circ b * a \circ (-c)$

$= a \circ b * [-(a \circ c)]$ [By distributive Law]

$= a \circ b - a \circ c$

Hence Proved

e) $(b - c) \circ a = [b * (-c)] \circ a$

$= b \circ a * (-c) \circ a$

$= b \circ a * [-(c \circ a)]$

$= b \circ a - c \circ a$

Hence Proved.

How to Prove an Algebraic Structure (R, *, o) to be a Ring

The following steps are to followed:

1. First prove that the two operations * and o are binary operations. If it is given that two operations are binary operations, then proceed to step 2.

2. Prove that R is an abelian group w.r.t one of the two operations say *. It is achieved by proving R1 - R4.

3. Then prove the satisfaction of R5 & R6 w.r.t operation o.
4. Prove it to be commutative Ring. (Commutative Ring)
5. Prove it to be a Ring with unity. (Ring with Unity)

Q. If $(R, *, o)$ is a ring such that $a^2 = a$, $a \in R$ then prove that

i) $a * a = 0$, $a \in R$ ie each element of R is it's own inverse

ii) $a * b = 0 \Rightarrow a = b$

iii) R is commutative ring.

Sol^n: i) $a \in R \Rightarrow a * a \in R$

w.k.t $a^2 = a$ (given)

$\therefore (a * a)^2 = (a * a)$

$\Rightarrow (a*a) \circ (a*a) = a * a$

$\Rightarrow ((a*a)\circ a) * ((a*a)\circ a) = a * a$ [Distributive Law]

$\Rightarrow ((a\circ a) * (a\circ a)) * ((a\circ a) * (a\circ a)) = a * a$

$\Rightarrow (a*a) * (a*a) = a * a$ [as $a^2 = a\circ a = a$ is given]

$\Rightarrow (a*a) * (a*a) = (a*a) * 0$ [since, $a * 0 = a$]

$\Rightarrow (a*a) = 0$ [By left cancellation law]

Hence Proved.

ii) $a * b = 0 \Rightarrow a * b$

$= a * a$ [Proved in (i)]

$\Rightarrow b = a$ [By Left Cancellation Law]

iii) Given that $(a*b)^2 = a * b$

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

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

$\Rightarrow [(a\circ a) * (b\circ a)] * [(a\circ b) * (b\circ b)] = a * b$

$\Rightarrow [a * (b\circ a)] * [a\circ b * b] = a * b$ [as $a\circ a = a$, $b\circ b = b$]

$\Rightarrow (b\circ a) * (a\circ b) = 0$ [By left Cancellation law)

$\Rightarrow a\circ b = b\circ a$ [By (ii)]

$\therefore$ R is commutative.

Q. Prove that the set $R = \{0, 1, 2, 3, 4\}$ is a commutative ring w.r.t $+_5$ and $\times_5$ as the two ring compositions.

Solⁿ:

1. We can prove that $(R, +_5)$ is an abelian group which proves the first four postulates.
2. The zero element or identity element is zero.
3. Now, we construct the composition table for R for second operation $\times_5$ as given below:

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

It is evident from this composition table that the operation $\times_5$ is a binary operation on R is closed w.r.t this operation.

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

4. $\times_5$ is an associative composition in R

ie $a \times_5 (b \times_5 c) = (a \times_5 b) \times_5 c \quad \forall a, b, c \in R$

5. $\times_5$ is distributive over the first operation $+_5$

ie $a \times_5 (b +_5 c) = (a \times_5 b) +_5 (a \times_5 c)$

similarily $(b +_5 c) \times_5 a = (b \times_5 a) +_5 (c \times_5 a)$

6. It is clear from composition table that operation $\times_5$ is commutative, ∴ ring is commutative.

Hence $(R, +_5, \times_6)$ is a commutative Ring.

Q. If $(R, +, \cdot)$ is a ring with unity, show that, for all $a \in R$,

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

ii) $(-1) \cdot (-1) = 1$

Solⁿ: i) Given that $(R, +, \cdot)$ is a ring with unity

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

because R is ring with unity ie. $1 \in R$ such that

$1 \cdot x = x = x \cdot 1 \quad \forall x \in R$

ii) $(-1)\cdot(-1) = -[(-1)\cdot 1]$

Given that $(R, +, \cdot)$ is a ring with unity

$$(-1)\cdot(-1) = -[(-1)\cdot 1]$$
$$= -[-(1\cdot 1)]$$
$$= 1\cdot 1 = 1$$

Hence Proved

Zero Divisors

- Let R be a Ring.
- An element $a \in R$ is said to be a left zero divisor if there exists an element $b \neq 0$ (zero element) $\in R$ such that $a \circ b = 0$ (zero or identity element for operation $*$)
- Similarly if an element $b \neq 0 \in R$ exists such that $b \circ a = 0$, then element a is said to be the right zero divisor.
- Or, we can say that if corresponding to a non-zero element $a \in R$, there exists a non-zero element $b \in R$ such that either $a \circ b = 0$ or $b \circ a = 0$ (zero element or identity element), then the element is said to be a ring with zero divisors.

Q. Show that if $M = \{0, 1, 2, 3, 4, 5\}$, then the ring $(M, +_6, \times_6)$ is a ring with zero divisors.

Solⁿ: W.k.t for a Ring $(R, *, \circ)$, there exists an element $e \in R$ for the first operation such that

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

$\therefore$ for $+_6$, $\boxed{e = 0}$ identity element

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	[illegible]	2	4
3	0	3	1	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

now, a ring $(R, *, \circ)$ is a ring with zero divisors, if $a \circ b = 0(e)$ or $b \cdot a = 0(e)$

let $a = 2$, $b = 3$.
$\therefore 2 \times_6 3 = 0 = 3 \times_6 2$

$\therefore (M, +_6, \times_6)$ is Ring with zero divisors.

Q. Identify if $M = \{0,1,2,3,4\}$ then the ring $(M, +_5, \times_6)$ is a ring with zero divisor or not.

Cancellation Laws in a Ring

THEOREM 2

A ring is without zero divisors iff the cancellation laws hold in R.

PROOF: Let R be a ring without zero divisor, ie. the product of no two non zero elements in the ring is zero ie. $a, b \in R$, then $a \circ b = 0 \Rightarrow$ either $a = 0$ or $b = 0$.

now let $a, b, c \in R$ such that $a \neq 0$ and $a \circ b = a \circ c$

Then $a \circ b = a \circ c \Rightarrow (a \circ b - a \circ c) = 0$

$\Rightarrow a \circ (b - c) = 0$

as $a \neq 0$ and R is without zero divisors,

$\therefore \boxed{b - c = 0 \text{ or } b = c}$

Thus $a \circ b = a \circ c \Rightarrow b = c$ which means that left cancellation law holds.

Similarily, it can be shown that right cancellation law also holds.

Integral Domain

- A ring which is
  i) Commutative
  ii) has unit element
  iii) is without zero divisors

is called an Integral Domain.

- Examples: $(Q, +, \times)$, $(R, +, \times)$, $(C, +, \times)$

Q. Show that the ring $(\{0,1,2,3,4\}, +_5, \times_5)$ is an integral domain.

(* Refer to THEOREM 03 on next page)

Field

- A ring $(R, *, \circ)$ with atleast two elements is called a field if
  i) it is commutative
  ii) it possesses a unit element
  iii) it is such that each non-zero element possesses an inverse w.r.t the operation $\circ$.

THEOREM 3

A commutative ring R is an integral domain, iff, for any non zero element $x \in R$, $x \circ a = x \circ b \Rightarrow a = b$ where $a, b \in R$

PROOF

Suppose that R is a commutative ring and

$$\boxed{x \circ a = x \circ b \Rightarrow a = b} \text{ — (I) where } x_1, x, a, b \in R$$

putting $a = x_1$ and $b = 0$ in (I), we get

for $x \neq 0$; $\boxed{x \circ x_1 = x \circ 0 \Rightarrow x_1 = 0}$, which means that R is without zero divisor. Thus R is an integral domain.

THEOREM 4

Every field is an integral domain.

PROOF:

As a field F is a commutative ring with unity, therefore for a field to be integral domain the field should ~~be~~ have no zero divisors.

let $a, b \in F$, $a \neq 0$ such that $a \circ b = 0$

as $a \neq 0$; a^{-1} must exist

now $a \circ b = 0 \Rightarrow a^{-1} \circ (a \circ b) = a^{-1} \circ b$

$\Rightarrow (a^{-1} \circ a) \circ b = 0 \Rightarrow 1 \circ b = 0$

$\Rightarrow b = 0$

Similarily for $a \circ b = 0$, where $b \neq 0$, we have $(a \circ b) \circ b^{-1} = a \circ b^{-1}$

$\Rightarrow a \circ (b \circ b^{-1}) = 0$

$\Rightarrow a \circ 1 = 0$

$\Rightarrow a = 0$

Therefore F is a field with no zero divisors and hence is a integral domain.

Divison Ring or Skew Field

- A ring with at least two elements is called a division ring or skew field if it
  i) has unity
  ii) is such that each non zero element possesses inverse under the second operation $\circ$.
- A commutative divison ring is a field.
- Every field is a divison ring.

THEOREM 05

A ring R is a divion ring iff the equation $a \circ x = b$ and $y \circ a = b$ have unique solutions in R where $a \neq 0$, $a, b \in R$

PROOF - Let R be a division ring.
- As non zero elements of R are invertible (possesses inverse), R is a group w.r.t the operation $\circ$.
- $\therefore$, the equations $a \circ x = b$ and $y \circ b = b$ have unique solutions provided $b \neq 0$.
- In case $b = 0$, then $a \neq 0$, $a \circ x = b$ and $y \circ a \Rightarrow x = 0$ and $y = 0$ (since R has no zero divisor)

THEOREM 06

A divison ring has no divisor of zero.

PROOF :- Let R be a divison ring and $x_1, x_2 \in R$ such that $x_1 \circ x_2 = 0$ and $x_1 \neq 0$.
- Therefore by definition of ring, x_1^{-1} exists and $x_1^{-1} \in R$ where

$$x_1 \circ x_1^{-1} = x_1^{-1} \circ x_1 = 1$$

$$\begin{aligned} x_2 &= 1 \circ x_2 \\ &= (x_1^{-1} \circ x_1) \circ x_2 \\ &= x_1^{-1} \circ (x_1 \circ x_2) \\ &= x_1^{-1} \circ 0 = 0 \end{aligned}$$

- It means that for $x_1 \neq 0$, $x_1 \circ x_2 = 0 \Rightarrow x_2 = 0$.
  Hence R is without zero divisors.

Subring

- let the algebraic structure $(R, *, \circ)$ be a ring.
- If $S \subseteq R$ such that $(S, *, \circ)$ is also a ring w.r.t the operations on R, then S is called subring of R

Sub-Field

- let the algebraic structure $(F, *, \circ)$ be a field.
- If $S \subseteq F$ such that $(S, *, \circ)$ is also a field w.r.t the operations on F then it is called sub-field of F.

UNIT 02

KEYWORDS:
Integer Addition Modulo, Multiplication Modulo

LECTURE NO. 08

Integer Modulo m [R1, R2]

1. ADDITION MODULO m

- If a and b are any two integers then the operation of addition modulo m is defined as the least non-negative remainder when the ordinary sum of a and b divided by m.
- This operation when applied over the integers a and b is written as $\boxed{a +_m b}$ and is defined as

$$\boxed{a +_m b = r, \quad 0 \leq r < m}$$

where r is left non-negative remainder when (a+b) is divided by m.

2. MULTIPLICATION MODULO m

- Now we define a similar composition known as multiplication modulo m and it is written as $\boxed{a \cdot_m b \text{ or } a \times_m b}$
where a and b are any integers and m is fixed positive integers.
- If a and b are any two integers then the operation of multiplication modulo m is defined as the least non-negative remainder when the ordinary product of a and b i.e (ab) is divided by m.

• Thus $\boxed{a \times_m b = r, \quad 0 \leq r < p}$

where r is the least non-negative remainder when $(a \cdot b)$ is divided by m.

References:

1. Liu and Mohapatra, "Elements of Discrete Mathematics", McGraw Hill
2. Jean Paul Tremblay, R Manohar, "Discrete Mathematical Structures with Applications of Computer Science", McGraw Hill

Q] Prove that the set $\{0,1,2,3,4\}$ is a finite abelian group of order 5 under addition modulo 5 as composition!

Sol^n: Here $G = \{0,1,2,3,4\}$

The Composition table is as following

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

From the above table we get,

i) G1: Closure Property

All the elements of composition table belong to set G

$\boxed{\therefore (G, +_5) \text{ satisfied closure property.}}$

ii) G2: Associative Property $(a +_5 b) +_5 c = a +_5 (b +_5 c)$

let $a = 0, b = 1, c = 2$

then, $(a +_5 b) +_5 c = (0 +_5 1) +_5 2$
$= 1 +_5 2$
$= \underline{\underline{3}}$

now, $a +_5 (b +_5 c) = 0 +_5 (1 +_5 2)$
$= 0 +_5 3$
$= \underline{\underline{3}}$

since $(a +_5 b) +_5 c = a +_5 (b +_5 c)$

$\boxed{\therefore (G, +_5) \text{ satisfies Associative Property}}$

iii) G3: Existence of Identity $(a +_5 e = a)$

Here, in the composition table, 0 is the identity element for $+_5$ for every element.

ie.

$+_5$	0	1	2	3	4
0	$\boxed{0}$	1	2	3	4
1	1	2	3	4	$\boxed{0}$
2	2	3	4	$\boxed{0}$	1
3	3	4	$\boxed{0}$	1	2
4	4	$\boxed{0}$	1	2	3

* $a +_5 e = a$

$0 +_5 0 = 0$
$1 +_5 0 = 1$
$2 +_5 0 = 2$
$3 +_5 0 = 3$
$4 +_5 0 = 4$

There exists identity element '0' for every element of G in the composition table

∴ $(G, +_5)$ satisfies Existence of Identity property

iv) G4: Existence of Inverse $(a +_5 b = e)$

from G3, w.k.t $\boxed{e = 0}$

Here, in the composition table, the inverse of every element of G exists.

* $a +_5 b = e$

$0 +_5 0 = 0$
$1 +_5 4 = 0$
$2 +_5 3 = 0$
$3 +_5 2 = 0$
$4 +_5 1 = 0$

ie.

$+_5$	0	1	2	3	4
0	$\boxed{0}$	1	2	3	4
1	1	2	3	4	$\boxed{0}$
2	2	3	4	$\boxed{0}$	1
3	3	4	$\boxed{0}$	1	2
4	4	$\boxed{0}$	1	2	3

There exists inverse element for every element of G in the composition table.

∴ $(G, +_5)$ satisfies Existence of Inverse Property

v) G5: Commutative Property $(a +_5 b) = (b +_5 a)$

let $a = 1$, $b = 2$

then $a +_5 b = 1 +_5 2$
$= \underline{\underline{3}}$

$b +_5 a = 2 +_5 1$
$= \underline{\underline{3}}$

since $(a +_5 b) = (b +_5 a)$

$\boxed{\therefore (G, +_5) \text{ satisfies Commutative Property}}$

$\therefore (G, +_5)$ is an Abelian Group.

Q] Let $G = \{0, 1, 2, 3, 4, 5\}$, prove that G is an abelian group under operation $+_6$.

Q] Show that the set $\{1, 2, 3, 4, 5\}$ is not a group under multiplication modulo 6.

Soln] Here, $G = \{1, 2, 3, 4, 5\}$

The Composition Table is as follows —

$\times_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

From the above table,

i) G1: Closure Property

Since $0 \notin G$, $\boxed{\therefore (G, \times_6) \text{ does not satisfy Closure Property}}$

Hence $(G, \times_6)$ is not a Group

UNIT 03

KEYWORDS:
POSET, Total Ordered Set, Successor, Predecessor

LECTURE NO. 01

Partially Ordered Sets (POSET) [R1]

- A non empty set A, together with a binary relation R is said to be a partially ordered set or a POSET if following conditions are satisfied:

1. REFLEXIVITY: $aRa \quad \forall a \in A$
2. ANTISYMMETRIC: If $a, b \in A$ then $aRb,\ bRa \Rightarrow a=b$
3. TRANSITIVITY: If $a, b, c \in A$ then $aRb,\ bRc \Rightarrow aRc$

- The relation R on this set A is called "Partially Ordered Relation"

- POSET is denoted by (A, R) or $(A, \leq)$ → It may have nothing to do with the usual less than equal to relation.

- Example 1:
The set S on any collection of sets. The relation $\subseteq$ read as "is subset of" is partial ordering of S. Prove.

Sol^n: The set S is poset if it satisfies the following conditions:

P1: REFLEXIVE: since $A \subseteq A$ for any subset A of S
$\therefore \subseteq$ is reflexive.

P2: ANTISYMMETRIC: If $A \subseteq B$ and $B \subseteq A \ \forall A, B \in S$ then $A = B$ $\therefore \subseteq$ is Antisymmetric

P3: TRANSITIVE: If $A \subseteq B$ and $B \subseteq C$ for any sets $A, B, C \in S$, then $A \subseteq C$ $\therefore \subseteq$ is Transitive

$\therefore (S, \leq)$ is a Poset.

- Example 2 :

A set $S = \{a, b, c\}$ together with the relation of set inclusion $\subseteq$ is a partial order on $P(S)$ where $P(S)$ is power set of S. Prove.

Sol^n: The power set of S is $P(S) = \{\phi, \{a\}, \{b\}, \{c\}, \{a,b\}, \{b,c\}, \{a,c\}, \{a,b,c\}\}$.

Then $P(S)$ is partial order relation if it satisfies the following conditions:

P1: REFLEXIVE : Since every $A \subseteq A$ $\forall A \in P(S)$. Hence, it is reflexive.

P2: ANTISYMMETRIC : If $A \subseteq B$ and $B \subseteq A \Rightarrow A = B$. Hence, it is antisymmetric.

P3: TRANSITIVE : If $A \subseteq B$, $B \subseteq C \Rightarrow A \subseteq C$. Hence, it is transitive.

$\therefore$ $(P(S), \subseteq)$ is a Poset.

- Example 3 :

Let $A = \{2, 3, 6, 12, 24, 36\}$ and R be the relation in A which is defined by a divides b then R is partial order in A. Prove.

Sol^n: $R = \{(2,2), (2,6), (2,12), (2,24), (2,36), (3,3), (3,6), (3,12), (3,24), (3,36), (6,6), (6,12), (6,24), (6,36), (12,12), (12,24), (12,36), (24,24), (36,36)\}$

Now A is a Poset if it satisfies the following conditions:

P1: REFLEXIVE : since $a|a$ $\forall a \in A$ $\therefore$ '|' is reflexive

P2: ANTISYMMETRIC : If $a|b$ & $b|a$ $\forall a, b \in A$ then $a = b$
$\therefore$ '|' is antisymmetric

P3: TRANSITIVE : If $a|b$ & $b|c$ $\forall a, b, c \in A$ then $a|c$
$\therefore$ '|' is transitive

ILLUSTRATION: If $2|2$ & $2|6$ then $2|6$
or If $2|6$ & $6|12$ then $2|12$

$\therefore$ (A, |) is a Poset.

- Example 4

The set of integers $\mathbb{Z}$ with usual ordering $\leq$ read as "Less than or equal to" is a poset. Prove.

Solⁿ: The set of integer $\mathbb{Z}$ is a poset if it satisfies the following conditions:

P1: REFLEXIVE : since $a \leq a$ for every integer a, $\therefore \leq$ is reflexive

P2: ANTISYMMETRIC : If $a \leq b$ and $b \leq a$ then $a = b$ $\forall a, b \in \mathbb{Z}$.
Hence $\leq$ is antisymmetric.

P3: TRANSITIVE : If $a \leq b$ and $b \leq c$, where $a, b, c \in \mathbb{Z}$
then $a \leq c$ $\therefore \leq$ is a transitive relation

$\therefore (\mathbb{Z}, \leq)$ is a Poset.

- Example 5

If R is partially ordered relation on a subset X and $A \subseteq X$, show that $R \cap (A \times A)$ is a partial ordering relation on A.

Solⁿ: Denote $R \cap (A \times A)$ by R' then R' will be partial order relation or poset if it satisfies the following conditions:

P1: REFLEXIVE : Let $x \in A$, then $(x, x) \in A \times A$.
since R is reflexive, ie. $(x, x) \in R \Rightarrow xRx$
$(x, x) \in R \cap (A \times A) = R'$

P2: ANTISYMMETRIC : Suppose $(x, y) \in R'$ and $(y, x) \in R'$
Then $(x, y) \in R \cap (A \times A)$ and $(y, x) \in R \cap (A \times A)$
since R is antisymmetric, $(x, y) \in R$ and $(y, x) \in R$
Then $x = y$ $\therefore R'$ is antisymmetric.

P3: TRANSITIVITY : Suppose $(x, y) \in R' = R \cap (A \times A)$ and
$(y, z) \in R' = R \cap (A \times A)$

Then $(x, y), (y, z) \in R$ and $(A \times A)$ is R transitive
$(x, y) \in R, (y, z) \in R \Rightarrow (x, z) \in R$ since $R \subset A \times A$
$\therefore (x, z) \in A \times A$ and hence $(x, z) \in R \cap (A \times A) = R'$

$\therefore R' = R \cap (A \times A)$ is a Poset.

*NOTE

- Two elements 'a' & 'b' in a POSET $(S, \leq)$ are said to be comparable if either $a \leq b$ or $b \leq a$

- Example:

  $2|6$, $6|12$, $12|36$

- 'a' & 'b' are called Incomparable if neither $a \leq b$ nor $b \leq a$.

Total Ordered Relation/Total Ordered Set [R2, R3]

- A relation R on a set A is said to be total ordered relation if the relation R is

  1. REFLEXIVE
  2. ANTISYMMETRIC
  3. TRANSITIVE
  4. Satisfies the following relation called "Law of Dichotom

  ie. for each $a, b \in A$, either $a \leq b$ or $b \leq a$ ie. any two elements of A are comparable.

- Example

  Give an example of a set X such that $(P(X), \subseteq)$ is totally ordered set.

Solⁿ: Let $X = \{a, b, c\}$, then

$P(X) = \{\phi, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$. Then $P(X)$ is total ordered set if it satisfies following conditions:

P1: REFLEXIVE: Since each set is subset to itself, ie. $\{a\} \subseteq \{a\}$ $\forall$ $\{a\} \in P(X)$. Hence, it is reflexive.

P2: ANTISYMMETRIC: If $A \subseteq B$ and $B \subseteq A \Rightarrow A = B$

Hence, it is antisymmetric

P3: TRANSITIVE: If $A \subseteq B$ and $B \subseteq C \Rightarrow A \subseteq C$.

Hence, it is transitive.

$\therefore (P(X), \subseteq)$ is a POSET

P4: <u>LAW OF DICHOTOMY</u>: For each $\{a\} \in P(X)$ and $\{a,b\} \in P(X) \Rightarrow \{a\} \subseteq \{a,b\}$

ie. any two elements in P(X) are comparable.

. Then . $(P(X), \subseteq)$ is Total Ordered Set.

Immediate Predecessor and Immediate Successor [R2,R3]

- Let $(A, \leq)$ be a poset and $a, b \in A$. 'a' is said to be Immediate Predecessor of b or b is immmediate successor of a, written as

$$a << b$$

- If $a < b$, and no elements of A lies between a and b ie $\nexists c \in A$ such that $a < c < b$

References

1. Y. N. Singh, "Discrete Mathematics", Wiley India.
2. PDF: Partially Ordered Sets," https://www.math.cmu.edu"
3. PDF: Partially Ordered Sets - IIT Kharagpur," cse.iitkgp.ac.in"

UNIT 03

LECTURE NO. 02

Graphs of Relations [R1]

⇒ GRAPH:

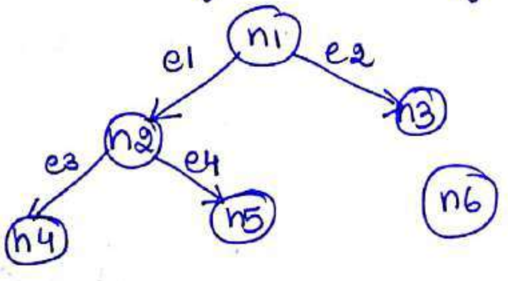
- A graph has a set of nodes and a set of edges that connects these nodes.
- A graph $G=(V,E)$ consists of a non-empty finite set V of nodes and a set E of edges containing ordered or unordered pairs of nodes.

⇒ TYPES OF GRAPH

1. DIRECTED GRAPH/DIGRAPH

- If in a graph $G=(V,E)$, each edge $e \in E$ is associated with an ordered pair of nodes, then graph G is called a Directed graph or Digraph

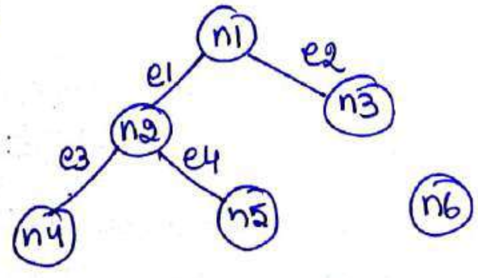
- Example:



2. UNDIRECTED GRAPH

- If each edge is associated with an unordered pair of nodes, then graph G is called an Undirected graph.

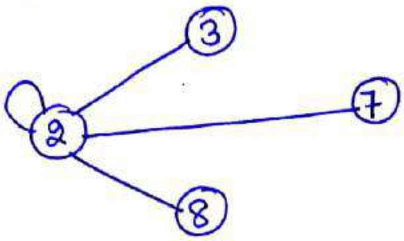
- Example:



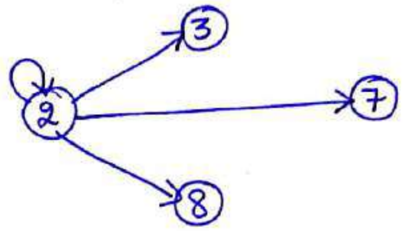
* NOTE: In a graph, nodes are represented by Circles & Edges by Lines.

Q] For the given $R = \{(2,2), (2,3), (2,7), (2,8)\}$, draw the
i) Directed graph
ii) Undirected graph

<u>Sol^n</u>: i) DIRECTED GRAPH



(ii) UNDIRECTED GRAPH

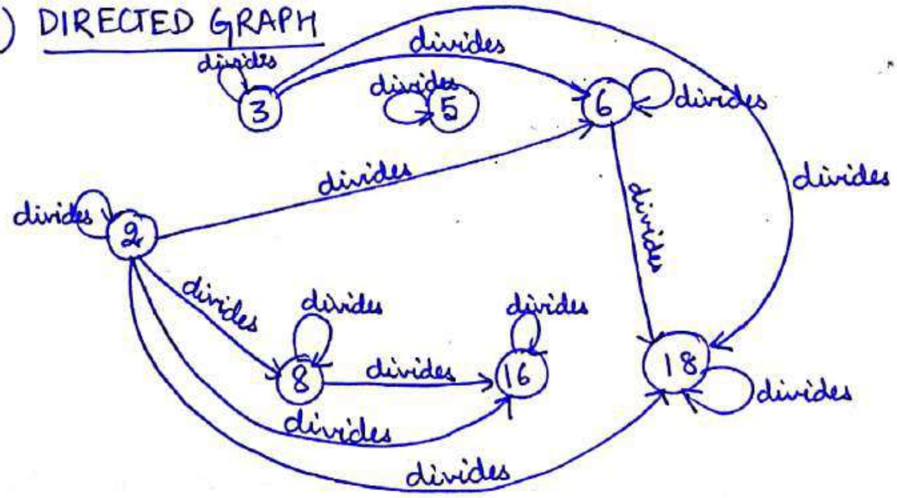


Q] Let $X = \{2, 3, 5, 6, 8, 16, 18\}$. The relation on X is defined by 'x divides y'.
i) Find R
ii) Find R^{-1}
iii) Draw the Digraph to represent R.

<u>Sol^n</u>: i) $R = \{(2,2), (2,6), (2,8), (2,16), (2,18), (3,3), (3,6), (3,18), (5,5), (6,6), (6,18), (8,8), (8,16), (16,16), (18,18)\}$

ii) $R^{-1} = \{(2,2), (6,2), (8,2), (16,2), (18,2), (3,3), (6,3), (18,3), (5,5), (6,6), (18,6), (8,8), (16,8), (16,16), (18,18)\}$

iii) <u>DIRECTED GRAPH</u>



Hasse Diagram: [R2]

- A graphical representation of a POSET in which all arrow heads are understood to be pointing upwards.
- Since the Hasse Diagrams are drawn for POSETS, hence they follow the following three properties:

1. REFLEXIVE : $aRa \ \forall a \in A$

2. ANTISYMMETRIC : aRb & bRa then $a=b \ \forall a,b \in A$

3. TRANSITIVE : aRb & $bRc \Rightarrow aRc \ \forall a,b,c \in A$

Procedure of Drawing Hasse Diagram [R2]

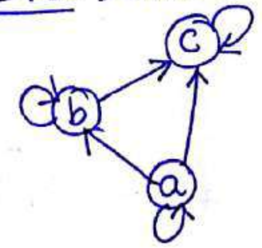
1.** Draw the digraph of given relation.
2. Delete all cycles from digraph.
3. Eliminate all edges that are implied by Transitive relation.
4. Draw the digraph of a partial order with edges pointing upwards so that arrows may be omitted from edges.
5. Replace the circle representing the vertices by dots.

** Procedure of Drawing the Digraph of given relation

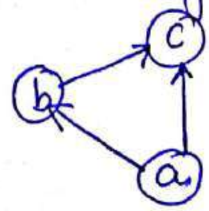
1. Nodes having arrows ONLY from itself goes on level 0.
2. Nodes having arrows from nodes of level 0, goto level 1.
3. Nodes having arrows from nodes of level 1, goto level 2.

Q] Draw the Hasse Diagram for the given relation
$R = \{(a,a), (a,b), (a,c), (b,b), (b,c), (c,c)\}$

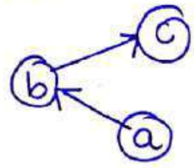
Sol^n: STEP1: Draw the Digraph



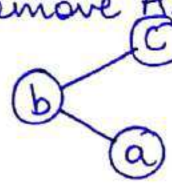
STEP2 : Delete cycles from Digraph



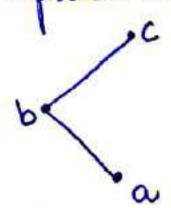
STEP3: Eliminate Transitive Edges



STEP4 : Remove Arrowheads



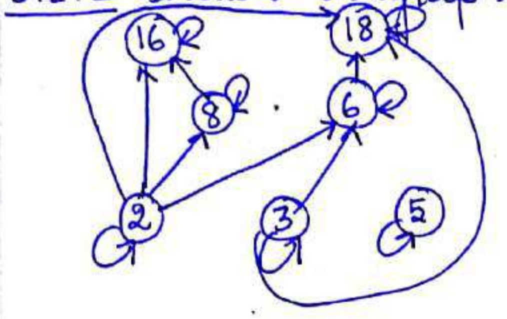
STEP5 : Replace circles by dots



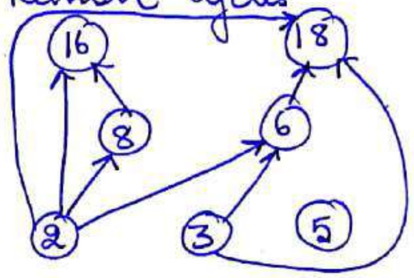
Q] Let $X = \{2,3,5,6,8,16,18\}$. The relation on X is defined by 'x divides y'. Draw the Hasse Diagram to represent R.

Sol^n: $R = \{(2,2),(2,6),(2,8),(2,16),(2,18),(3,3),(3,6),(3,18),(5,5),(6,6),(6,18),$
$(8,8),(8,16),(16,16),(18,18)\}$

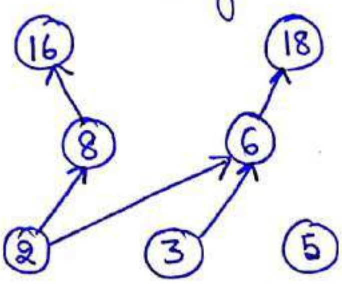
STEP1: Draw the Digraph



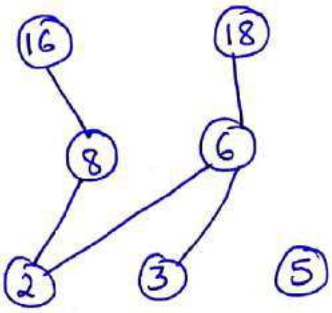
STEP2: Remove Cycles



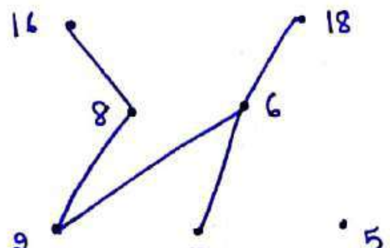
STEP3: Remove Transitive Edges



STEP 4: Remove Arrowheads



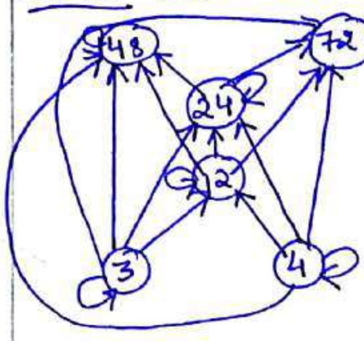
STEP5: Replace Circles by Dots



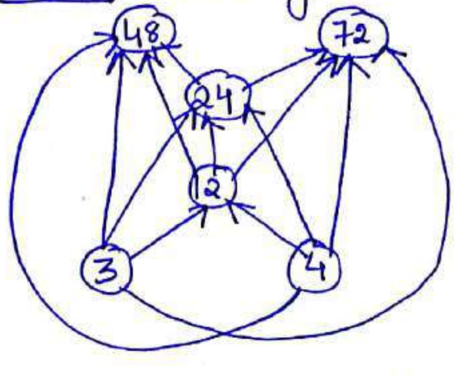
Q] Draw the Hasse Diagram of $(A, \leq)$ where $A = \{3,4,12,24,48,72\}$ and relation $\leq$ be such that $a|b$.

Sol^n: $R = \{(3,3),(3,12),(3,24),(3,48),(3,72),(4,4),(4,12),(4,24),(4,48),$
$(4,72),(12,12),(12,24),(12,48),(12,72),(24,24),(24,48),(24,72),$
$(48,48),(72,72)\}$

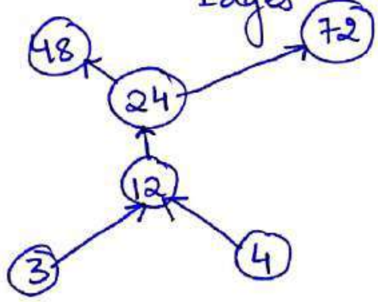
Solⁿ: STEP1: Draw the Digraph



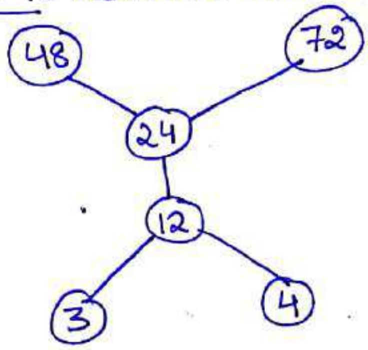
STEP2: Remove Cycle



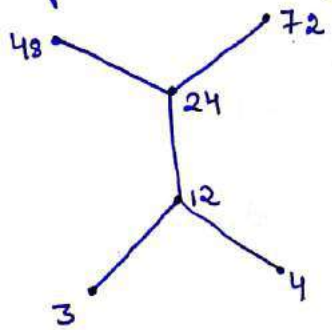
STEP3: Remove Transitive Edges



STEP4: Remove Arrowheads



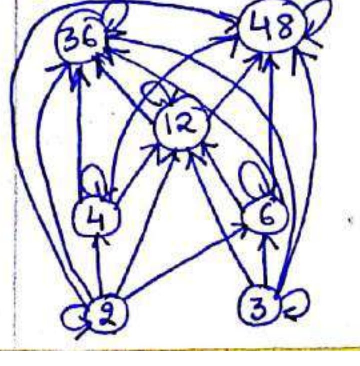
STEP5: Replace Circles by Dots



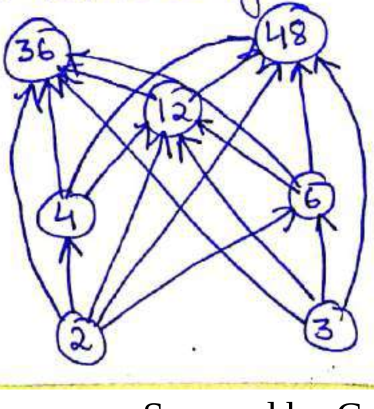
Q] Draw the Hasse Diagram of $(A, \leq)$ where $A = \{2, 3, 4, 6, 12, 36, 48\}$ and relation $\leq$ be such that $a|b$

Solⁿ: $R = \{(2,2), (2,4), (2,6), (2,12), (2,36), (2,48), (3,3), (3,6), (3,12), (3,36), (3,48), (4,4), (4,12), (4,36), (4,48), (6,6), (6,12), (6,36), (6,48), (12,12), (12,36), (12,48), (36,36), (48,48)\}$

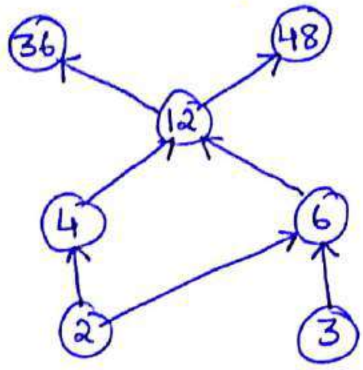
STEP1: Draw the Digraph



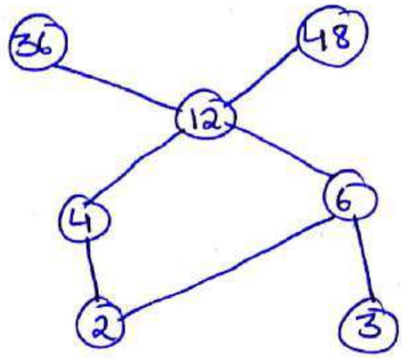
STEP2: Remove Cycles



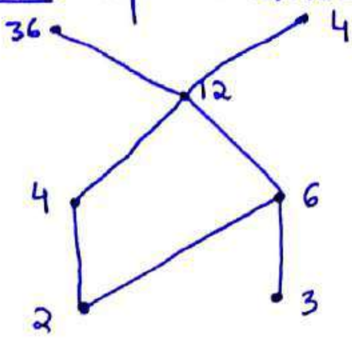
STEP3: Remove Transitive Edges



STEP4 : Remove Arrowheads

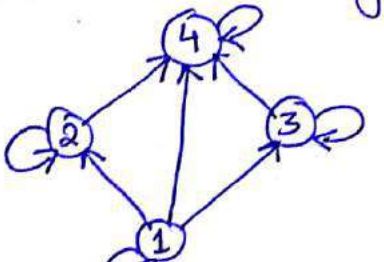


STEP5: Replace Circles by Dots

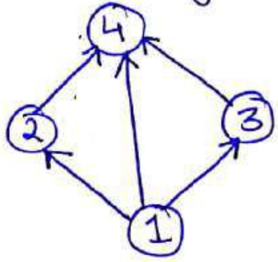


Q] Determine the Hasse Diagram of R, where $A = \{1, 2, 3, 4\}$ and $R = \{(1,1), (1,2), (2,2), (2,4), (1,3), (3,3), (3,4), (1,4), (4,4)\}$

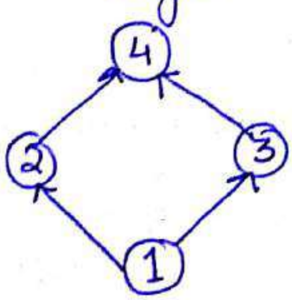
Sol^n: **STEP1:** Draw the Digraph



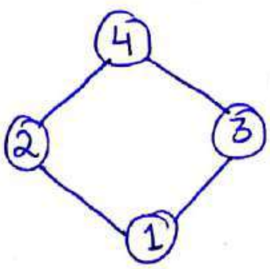
STEP2: Remove Cycles



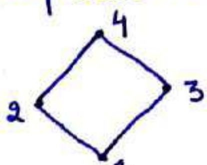
STEP3: Remove Transitive Edges



STEP4 : Remove Arrowheads



STEP5: Replace Circle by Dots



Q] Draw the Hasse Diagram of the relation on A, where $A = \{1, 2, 3, 4, 5\}$ whose matrix is shown.

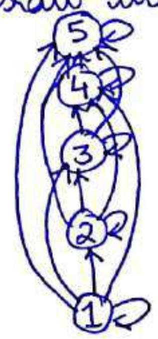
$$M_R = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Sol^n: Here

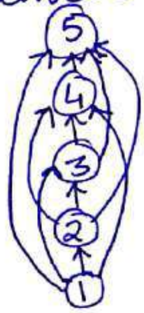
$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

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

STEP 1: Draw the Digraph



STEP 2: Remove the Cycles



STEP 3: Remove Transitive Edges

STEP 4: Remove Arrowheads

STEP 5: Replace circles with dots

Scanned by CamScanner

Q. Draw the Hasse Diagram for the partial ordering $\{(A,B) / A \subseteq B\}$ on the power set $P(S)$ where $S = \{a,b,c\}$

Solⁿ: Given that $S = \{a,b,c\}$

$\therefore$ Powerset of S is $P(S) = \{\phi, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$

$\therefore$ - $\phi \leq$ All elements of Poset $\quad \therefore \phi$ lies at Level 0

- $\{a\} \leq \{a\}$
  $\{a\} \leq \{a,b\}$
  $\{a\} \leq \{a,c\}$
  $\{a\} \leq \{a,b,c\}$
- $\{b\} \leq \{b\}$
  $\{b\} \leq \{a,b\}$
  $\{b\} \leq \{b,c\}$
  $\{b\} \leq \{a,b,c\}$
- $\{c\} \leq \{c\}$
- $\{c\} \leq \{a,c\}$
- $\{c\} \leq \{b,c\}$
- $\{c\} \leq \{a,b,c\}$

$\therefore \{a\}, \{b\}, \{c\}$ lie at level 1

- $\{a,b\} \leq \{a,b\}$
  $\{a,b\} \leq \{a,b,c\}$
- $\{a,c\} \leq \{a,c\}$
  $\{a,c\} \leq \{a,b,c\}$
- $\{b,c\} \leq \{b,c\}$
- $\{b,c\} \leq \{a,b,c\}$

$\therefore \{a,b\}, \{a,c\}, \{b,c\}$ lie at level 2

- $\{a,b,c\} \leq \{a,b,c\}$

$\therefore \{a,b,c\}$ lies at level 3.

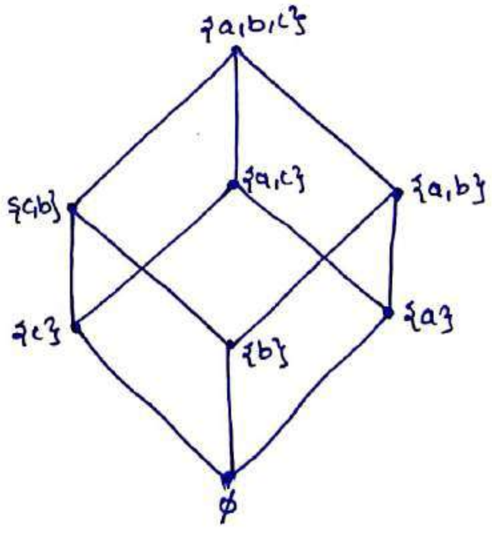
$\therefore$ The Hasse Diagram of $(P(S), \subseteq)$ is as shown below:

LEVEL3

LEVEL2

LEVEL 1

LEVEL0



UNIT 03

LECTURE NO. 03

Combination of Partial Ordered Sets or Components of Posets [RI]

⇒ MAXIMAL ELEMENT

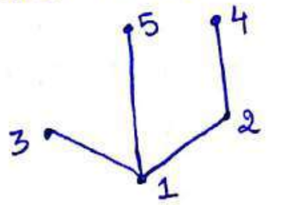
An element belonging to a POSET $(a, \leq)$ is said to be Maximal Element of A if there is no element c in A such that $a \leq c$.

⇒ MINIMAL ELEMENT

An element $b \in A$ is said to be minimal element of A if there is no element c in A such that $c \leq b$.

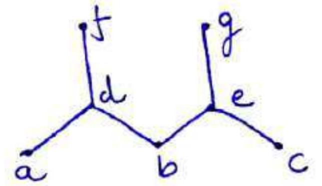
Q] Find all the maximal and minimal elements of posets whose Hasse Diagram is given below

i)



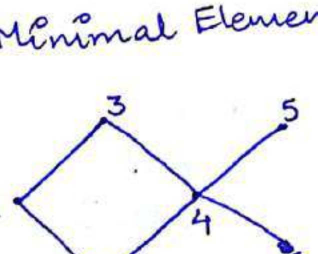
Sol^n: Maximal Elements = 3, 4, 5
Minimal Element = 1

(iii)



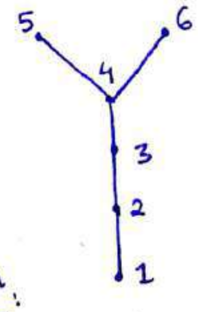
Sol^n: Maximal Elements = f, g
Minimal Elements = a, b, c

ii)



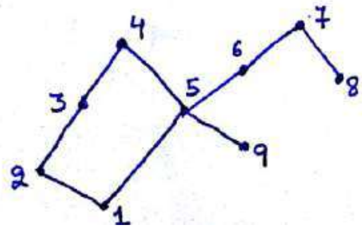
Sol^n:
Maximal Elements = 3, 5
Minimal Elements = 1, 6

(iv)



Sol^n:
Maximal Elements = 5, 6
Minimal Elements = 1

(v)



Sol^n:
Maximal Elements = 4, 7
Minimal Elements = 1, 9, 8

⇒ GREATEST ELEMENT / MAXIMUM ELEMENT

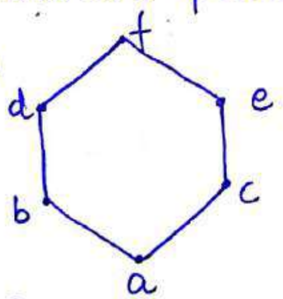
- An element $a \in A$ is said to be a Greatest Element of A if $x \leq a$ for all $x \in A$.
- The greatest element is also called Last Element or Unit Element of A.
- The greatest element if exists is unique. It may happen that the greatest element does not exist.
- The greatest element is generally denoted by 1.

⇒ LEAST ELEMENT / MINIMUM ELEMENT

- An element $a \in A$ is called a Least Element of A if $a \leq x$ for all $x \in A$.
- The least element is also called First Element or Zero Element of A.
- The least element if exists is unique. It may happen that the least element does not exist.
- The least element is generally denoted by 0.

Q] Find the Greatest and Least elements of Hasse Diagram.

i)

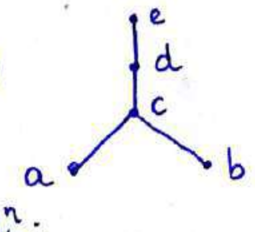


Solⁿ:

Greatest Element = f

Least Element = a

ii)

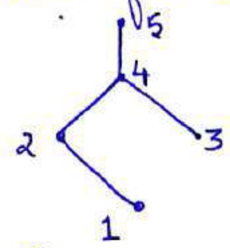


Solⁿ:

Greatest Element = e

Least Element = NIL

iii)

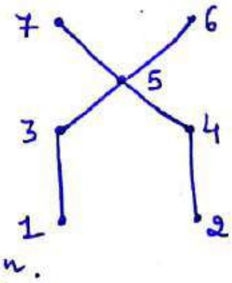


Solⁿ:

Greatest Element = 5

Least Element = NIL

iv)



Solⁿ:

Greatest Element = NIL

Least Element = NIL

⇒ UPPER BOUND

- Let B be a subset of a POSET $(A, \leq)$. An element $a \in A$ is called an "Upper Bound" of B if a succeeds every element of B

  i.e. $x R a \ \forall x \in B, a \in A$

  or $x \leq a \ \forall x \in B, a \in A$

⇒ LOWER BOUND

- Let B be a subset of a POSET $(A, \leq)$. An element $a \in A$ is called a "Lower Bound" of B if a preceeds every element of B

  ie $a R x \ \forall x \in B, a \in A$

  or $a \leq x \ \forall x \in B, a \in A$

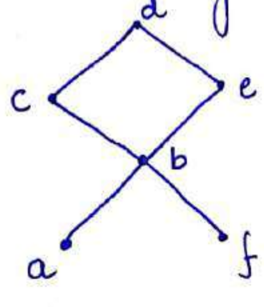
⇒ LEAST UPPER BOUND

- Also called as Supremum of A or Sup(A).
- An element $a \in A$ is called a Least Upper Bound of A if a is an upper bound of B and $a R a'$ or $a \leq a'$ whenever a is the upper bound of B.

⇒ GREATEST LOWER BOUND

- Also called as Infimum of A or Inf(A).
- An element $a \in A$ is called the Greatest Lower Bound of A if a is the lower bound of B and $a' R a$ or $a' \leq a$ whenever a is the lower bound of B.

Q] Consider the Poset whose diagram is given by

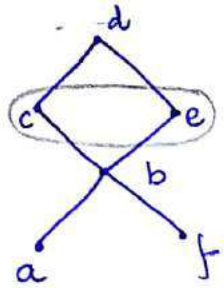


$A = \{a, b, c, d, e, f\}$

Find out the upper bound, lower bound, least upper bound and greatest lower bound of set $\{c, e\}$ and $\{a, f\}$

Scanned by CamScanner

Sol^n:



For $B = \{c, e\}$

I] UPPER BOUND (UB)

here, xRa, where $x \in B$ & $a \in A$

For $a = d$, cRd, eRd $\therefore$ d is an upper bound

$\therefore$ $\boxed{UB \text{ of } B = \{d\}}$

II] LOWER BOUND (LB)

here aRx, where $x \in B$ & $a \in A$

For $a = a$, aRc, aRe $\therefore$ a is a lower bound

For $a = f$, fRc, fRe $\therefore$ f is a lower bound

For $a = b$, bRc, bRe $\therefore$ b is a lower bound

$\therefore$ $\boxed{LB \text{ of } B = \{a, f, b\}}$

III] LEAST UPPER BOUND (LUB)

here a is an LUB if (i) $a, a' \in \{UB\}$
(ii) aRa'

now $UB = \{d\}$

and dRd (reflexive relation)

$\therefore$ $\boxed{LUB = \{d\}}$

IV] GREATEST LOWER BOUND (GLB)

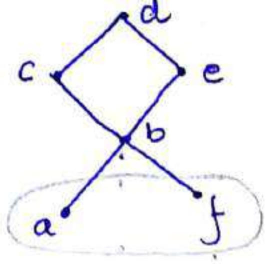
here a is a GLB if (i) $a, a' \in \{LB\}$
(ii) $a'Ra$

now $LB = \{a, f, b\}$

now			
	aRa	$a \not R f$	aRb
	$f \not R a$	fRf	fRb
	$b \not R a$	$b \not R f$	bRb
	$\therefore$ a is not GLB	$\therefore$ f is not GLB	$\therefore$ b is a GLB

$\therefore$ $\boxed{GLB = \{b\}}$

For $B = \{a, f\}$



I] UPPER BOUND (UB)

here, xRa, where $x \in B$, $a \in A$

For $a = b$, aRb, fRb $\therefore$ b is an upperbound

For $a = c$, aRc, fRc $\therefore$ c is an upperbound

For $a = e$, aRe, fRe $\therefore$ e is an upper bound

For $a = d$, aRd, fRd $\therefore$ d is an upper bound

$\therefore \boxed{\text{UB of } B = \{b, c, d, e\}}$

II] LOWER BOUND (LB)

here aRx, where $x \in B$, $a \in A$

since $a \not R f$ and $f \not R a$

$\therefore \boxed{\text{LB of } B = \text{NIL}}$

III] LEAST UPPER BOUND (LUB)

here a is an LUB if (i) $a \in \{UB\}$
(ii) aRa'

now $UB = \{b, c, d, e\}$

now

bRb	$c \not R b$	$d \not R b$	$e \not R b$
bRc	cRc	$d \not R c$	$e \not R c$
bRd	cRd	dRd	eRd
bRe	$c \not R e$	$d \not R e$	eRe
$\therefore$ b is a LUB	$\therefore$ c is not LUB	$\therefore$ d is not LUB	$\therefore$ e is not LUB

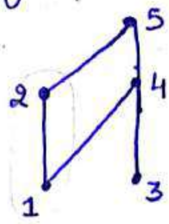
$\therefore \boxed{LUB = \{b\}}$

IV] GREATEST LOWER BOUND GLB

since there is no LB of B

$\therefore \boxed{GLB = \text{NIL}}$

Q]. Consider the Hasse Diagram and find the UB, LB, LUB & GLB



$B = \{1, 2\}$

Solⁿ: I] UPPER BOUND (UB)

$\boxed{UB \text{ of } B = \{2, 5\}}$

II] LOWER BOUND (LB)

LB of $B = \{1\}$

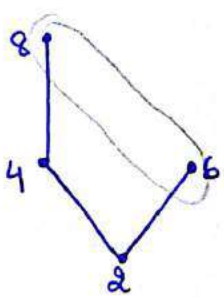
III] LEAST UPPER BOUND (LUB)

$\boxed{LUB = \{2\}}$

IV] GREASTEST LOWER BOUND (GLB)

$\boxed{GLB = \{1\}}$

Q] Consider the Hasse Diagram and find the UB, LB, LUB & GLB of $\{6, 8\}$



I] UPPER BOUND (UB)

$\boxed{UB \text{ of } B = NIL}$

II] LOWER BOUND (LB)

$\boxed{LB \text{ of } B = \{2\}}$

III] LEAST UPPER BOUND (LUB)

$\boxed{LUB = NIL}$

IV] GREATEST LOWER BOUND (GLB)

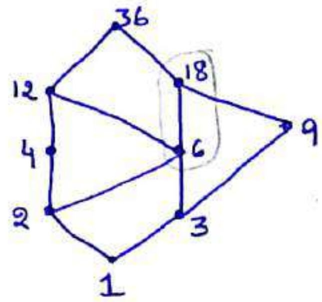
$\boxed{GLB = \{2\}}$

Scanned by CamScanner

Q] Consider the poset A = {1, 2, 3, 4, 6, 9, 12, 18, 36}, '|'}. Find the greatest lower bound and least upper bound of the set {6, 18} and {4, 6, 9}.

Solⁿ: Hasse diagram under relation of divisibility.

for B = {6, 18}



An integer is an upperbound of {6, 18} iff it is divisible by 6 and 18.

∴ $\boxed{\text{UB of } B = \{18, 36\}}$

now

$\boxed{\text{LUB} = \{18\}}$

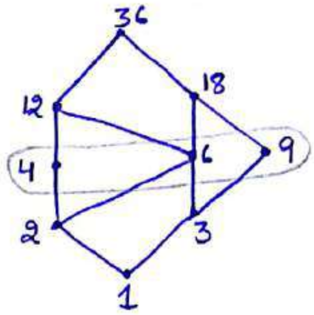
An integer is a lowerbound of {6, 18} iff 6 & 18 are divisible by this integer.

∴ $\boxed{\text{LB} = \{1, 2, 3, 6\}}$

now

$\boxed{\text{GLB} = \{6\}}$

For B = {4, 6, 9}



An integer is an upper bound of {4, 6, 9} iff it is divisible by 4, 6 & 9.

∴ $\boxed{\text{UB} = \{36\}}$

now

$\boxed{\text{LUB} = \{36\}}$

An integer is a lower bound of {4, 6, 9} iff 4, 6, 9 are divisible by this integer

∴ $\boxed{\text{LB} = \{1\}}$

now

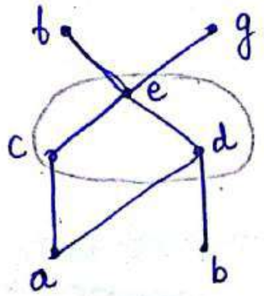
$\boxed{\text{GLB} = \{1\}}$

Q] Let S = {a, b, c, d, e, f, g} and B = {c, d, e}

a) Find UB & LB of B

b) Identify LUB & GLB if exists

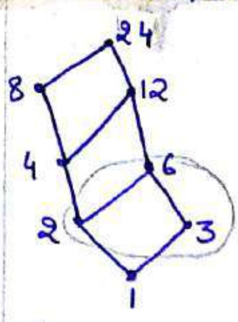
Solⁿ:



UB = {e, f, g}
LB = {a}
LUB = {e}
GLB = {a}

... UB, LB, LUB, GLB of following Hasse Diagram.

1.



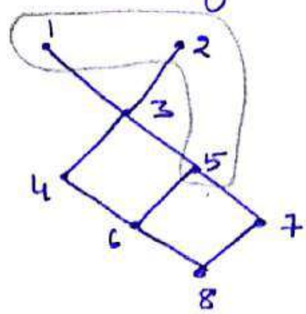
UB = {6, 12, 24}

LB = {1}

LUB = {6}

GLB = {1}

4.



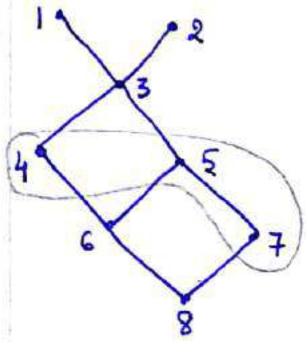
UB = NIL

LB = {5, 6, 7, 8}

LUB = NIL

GLB = {5}

2.



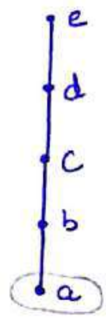
UB = {1, 2, 3}

LB = {8}

LUB = {3}

GLB = {8}

5.



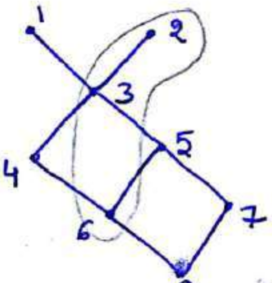
UB = {a, b, c, d, e}

LB = {a}

LUB = {a}

GLB = {a}

3.



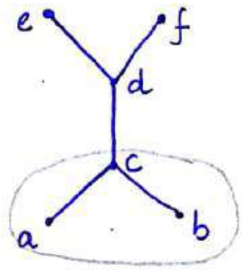
UB = {2}

LB = {6, 8}

LUB = {2}

GLB = {6}

6.



UB = {c, d, e, f}

LB = NIL

LUB = {c}

GLB = NIL

References:

1. Liu and Mohapatra, "Elements of Discrete Mathematics," McGraw Hill

UNIT 03

LECTURE NO. 04

Well Ordered Set

- A partially ordered set $(A, \leq)$ is said to be well ordered if every non-empty subset of S has a least element.

Complete Order

- A linear order $\leq$ on a set X is called complete if every non-empty subset of X has a Supremum in X.
- Every well order is complete.

Dual of a Poset [R2]

- Let R be a relation on a set X.
- Then converse of R, denoted by $\bar{R}$ is a relation on X defined by setting $a \bar{R} b \Leftrightarrow bRa \ \forall a, b \in X$.
- If R is a partial order relation, denoted by $\leq$ on X, then $\bar{R}$ is the converse of R denoted by $\geq$.
- ie. Let $(A, \leq)$ be a poset, then $(A, \geq)$ is also a poset; where $(A, \geq)$ is called the Dual of $(A, \leq)$.
- The dual of a poset is also a poset because $\bar{R}$ satisfies all the three properties, which are

  a) Reflexive
  b) Antisymmetric
  c) Transitive

- The least element of poset $(A, \leq)$ is equal to the greatest element of $(A, \geq)$ and vice versa.

  ie. $glb(A, \leq) = lub(A, \geq)$

Product of Two Posets [R2]

- Let A and B be two posets. Then product of two posets is defined as $A \times B = \{(a, b) : a \in A, b \in B\}$, under the relation

$$(a1, b1) \leq (a2, b2) \text{ if } a1 \leq a2 \text{ on } A \text{ and } b1 \leq b2 \text{ on } B.$$

- If A & B are two posets then $A \times B$ will also be a poset, where $(a, b) \leq (c, d)$ iff $a \leq c$ and $b \leq d$; because $A \times B$ satisfies all the three properties of a Poset.

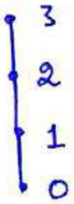
Isomorphic Posets [R2]

- Two posets A and B are said to be isomorphic if there is a function $f: A \to B$ such that f is one-one and onto function

Q] Let $A = \{1, 2, 4, 8\}$ and let $\leq$ be the partial order of divisibility on A. Let $A' = \{0, 1, 2, 3\}$ and let $\leq$ be the usual relation "less than or equal to" on integers. Show that $(A, \leq)$ and $(A', \leq)$ are isomorphic.

Solⁿ: The Hasse Diagram of $(A, |)$ is

The Hasse Diagram of $(A', \leq)$ is



The mapping of $f: A \to A'$

$f(8) = 3$

$f(4) = 2$

$f(2) = 1$

$f(1) = 0$

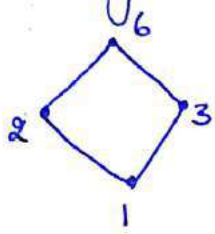
$\therefore (A, |)$ and $(A, \leq)$ are isomorphic to each other.

Q] Let $A = \{1, 2, 3, 6\}$ and let $\leq$ the divisibility relation on A. Let $B = \{\phi, \{a\}, \{b\}, \{a, b\}\}$ and let $\leq$ be the relation $\subseteq$. Then $(A, \leq)$ and $(B, \subseteq)$ are isomorphic. Prove.

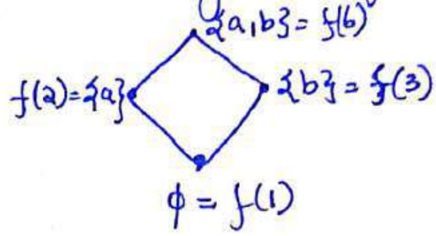
Sol^n: Let $f : A \to B$ be defined as

$$f(1) = \phi,\ f(2) = \{a\},\ f(3) = \{b\},\ f\{6\} = \{a, b\}$$

Hasse Diagram of $(A, \leq)$



Hasse Diagram of $(B, \subseteq)$



$\therefore$ $(A, \leq)$ and $(B, \subseteq)$ are isomorphic to each other.

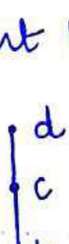
* Refer Pg 13.1 for more questions on Isomorphic Posets.

Lattice [R1, R2]

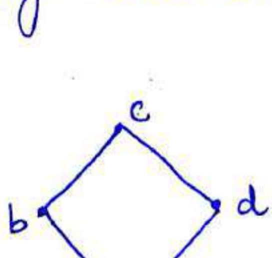
- A Poset $(P, \leq)$ is said to be a lattice if every two elements in set P has unique LUB (sup) and a unique GLB (inf)
- i.e. A poset $(P, \leq)$ is a lattice if for every $a, b \in P$ $\sup\{a, b\}$ and $\inf\{a, b\}$ exists in P
- i.e. $\boxed{\begin{array}{l} \sup\{a,b\} = a \vee b = a \text{ joint } b \\ \inf\{a,b\} = a \wedge b = a \text{ meet } b \end{array}}$

Q] Determine whether the following Hasse Diagram represent Lattice or not.

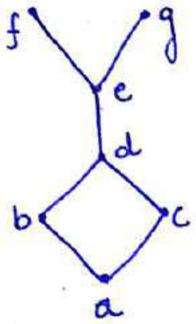
i)



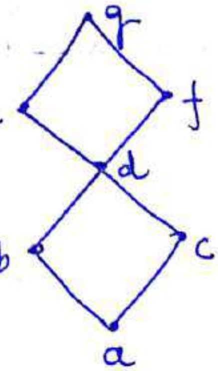
ii)



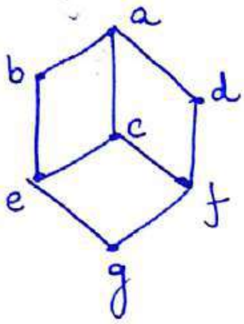
iii)



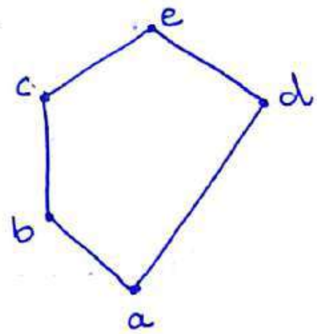
(iv)



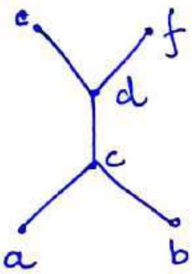
v)



(vi)



vii)



<u>Solⁿ</u>: i) Construct the closure tables for lub (∨) and glb (∧)

∨	a	b	c	d
a	a	b	c	d
b	b	b	c	d
c	c	c	c	d
d	d	d	d	d

∧	a	b	c	d
a	a	a	a	a
b	a	b	b	b
c	a	b	c	c
d	a	b	c	d

since each subset of two elements has lub and glb
∴ This is a Lattice.

ii) Construct the closure tables for lub(∨) and glb(∧)

∨	a	b	c	d
a	a	b	c	d
b	b	b	c	c
c	c	c	c	c
d	d	c	c	d

∧	a	b	c	d
a	a	a	a	a
b	a	b	b	a
c	a	b	c	d
d	a	a	d	d

Since each subset of two elements has lub & glb
∴ This is a Lattice.

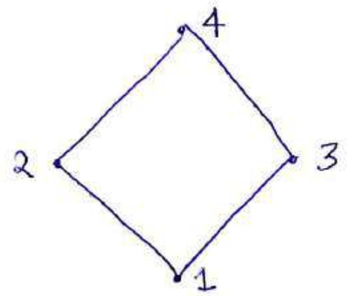
Scanned by CamScanner

Q. Let $A = \{1, 2, 3, 4\}$ and $\leq$ (relation) be partial order of divisibility on A. Let $B = \{0, 1, 2, 3, 4\}$ and $\leq$ (relation) be usual less than or equal to on set B. Show that $(A, \leq)$ and $(B, \leq)$ are isomorphic posets.

Sol^n: $A = \{1, 2, 3, 4\}$

& $(R_1) \leq = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)\}$

∴ Hasse Diagram of $(A, \leq)$

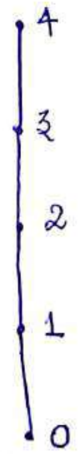


now

$B = \{0, 1, 2, 3, 4\}$

and $(R_2) \leq = \{(0,0), (0,1), (0,2), (0,3), (0,4), (1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$

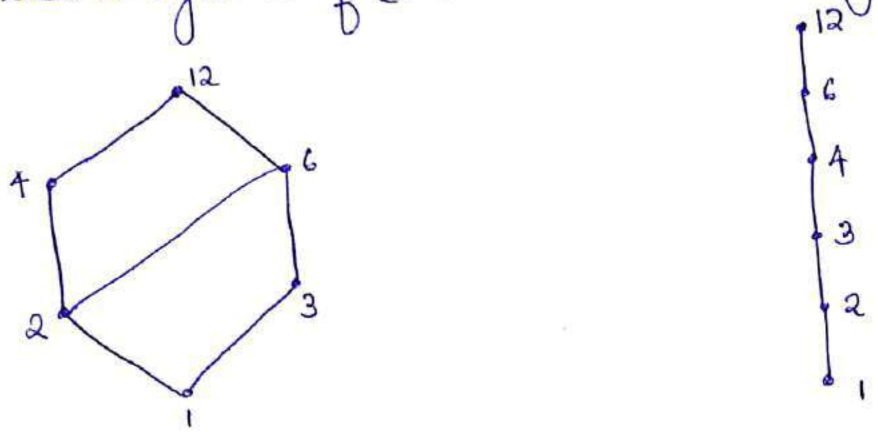
∴ Hasse Diagram of $(B, \leq)$



$(A, \leq)$ and $(B, \leq)$ are not isomorphic since $\leq$ is not one-one & onto.

Q. Let $A = \{1, 2, 3, 4, 6, 12\}$. Let R be the partial order relation on A given by xRy iff $x|y$. Then (A, R) is a poset. Consider another poset $(A, \leq)$ in which $\leq$ denotes the usual "less than or equal to" relation on A. Then prove that (A, R) and $(A, \leq)$ are not isomorphic.

Sol^n: Hasse Diagram of (A, R) and $(A, \leq)$ are given below



Now, let 4 and 6 be two distinct elements in (A, R) and $f(4)$ and $f(6)$ be two distinct elements in $(A, \leq)$.
Now $f(4)$ and $f(6)$ are comparable in $(A, \leq)$, while 4 and 6 are not comparable.

$\therefore (A, R)$ and $(A, \leq)$ are not isomorphic posets.

Scanned by CamScanner

iii) Construct the closure tables for lub ($\vee$) and glb ($\wedge$)

$\vee$	a	b	c	d	e	f	g
a	a	b	c	d	e	f	g
b	b	b	d	d	e	f	g
c	c	d	c	d	e	f	g
d	d	d	d	d	e	f	g
e	e	e	e	e	e	f	g
f	f	f	f	f	f	f	-
g	g	g	g	g	g	-	g

$\wedge$	a	b	c	d	e	f	g
a	a	a	a	a	a	a	a
b	a	b	a	b	b	b	b
c	a	a	c	c	c	c	c
d	a	b	c	d	d	d	d
e	a	b	c	d	e	e	e
f	a	b	c	d	e	f	e
g	a	b	c	d	e	e	g

Since (f,g) and (g,f) do not have lub

$\therefore$ This is not a lattice.

Similarily, other questions can be solved.

Q] For any positive integer m, Dm denote the set of divisors of m ordered of divisibility, then (Dm; |) is a lattice, where

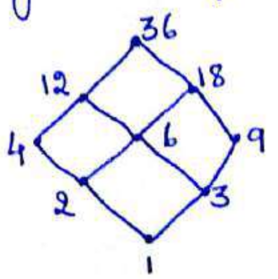
$$\sup(a,b) = \mathrm{lcm}(a,b)$$
$$\inf(a,b) = \mathrm{gcm}(a,b)$$

for any pair a, b in Dm. Prove Dm is a lattice.

Soln: Let m = 36

$\therefore D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$

The Hasse diagram of (D_{36}; |) is



Since each subset of two elements has Lub & glb
$\therefore$ It is a lattice.

Dual Lattice [R1]

- Let $(L, \leq)$ be a lattice, for any $a, b \in L$, the converse of relation $\leq$, denoted by $\geq$ is defined as

$$a \geq b \iff b \leq a$$

Then $(L, \geq)$ is also a lattice called Dual lattice of $(L, \leq)$.

Properties of Lattice [R1]

1. IDEMPOTENT LAW

for each $a \in L$

i) $a \wedge a = a$ ii) $a \vee a = a$

2. COMMUTATIVE LAW

for any $a, b \in L$

i) $a \wedge b = b \wedge a$ (ii) $a \vee b = b \vee a$

3. ASSOCIATIVE LAW

for any $a, b, c \in L$

i) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

ii) $(a \vee b) \vee c = a \vee (b \vee c)$

4. ABSORPTION LAW

for any $a, b \in L$

i) $a \wedge (a \vee b) = a$ (ii) $a \vee (a \wedge b) = a$

Q] Show that the dual of a lattice is a lattice.

Sol^n: Let $(L, \leq)$ be a lattice and let $(L, \geq)$ be its dual, where the relation $\geq$ is defined as

$$x \geq y \text{ iff } y \leq x$$

we now show that $\geq$ is reflexive, antisymmetric and transitive

1. $\geq$ is Reflexive

Let $a \in L$. Since $\leq$ is reflexive, we have

$$a \leq a \ \forall a \in L \Rightarrow a \geq a \ \forall a \in L$$

$\therefore \geq$ is reflexive

2. $\geq$ is Anti-Symmetric

Let $a, b \in L$ be such that $a \geq b$ and $b \geq a$. Then

$$a \geq b \text{ and } b \geq a \Rightarrow b \leq a \text{ and } a \leq b$$
$$\Rightarrow a = b \quad (\because \leq \text{ is antisymmetric})$$

Thus $a \geq b$ and $b \geq a \Rightarrow a = b$.

Hence $\geq$ is antisymmetric.

3. $\geq$ is Transitive

Let $a, b, c \in L$ such that $a \geq b$ and $b \geq c$. Then

$$a \geq b \text{ and } b \geq c \Rightarrow b \leq a \text{ and } c \leq b$$
$$\Rightarrow c \leq b \text{ and } b \leq a$$
$$\Rightarrow c \leq a \quad (\because \leq \text{ is transitive})$$
$$\Rightarrow a \geq c$$

Thus $a \geq b$ and $b \geq c \Rightarrow a \geq c$

Hence, $\geq$ is transitive

$\therefore (L, \geq)$ is a Poset.

Let, $a, b \in L$. Then since $(L, \leq)$ is a lattice, $\sup\{a, b\}$ exists in $(L, \leq)$.

Let $a \vee b = \sup\{a, b\}$ in $(L, \leq)$. Then

$$a \leq a \vee b \text{ and } b \leq a \vee b$$

now $a \leq a \vee b$ and $b \leq a \vee b$

$\Rightarrow a \vee b \geq a$ and $a \vee b \geq b$

$\Rightarrow a \vee b$ is a lowerbound of $\{a, b\}$ in $(L, \geq)$.

now,

Let 'l' be any lower bound of $\{a, b\}$ in $(L, \geq)$. Then

$l \geq a$ and $l \geq b \Rightarrow a \leq l$ and $b \leq l$

$\Rightarrow l$ is an upper bound of $\{a, b\}$ in $(L, \leq)$

$\Rightarrow$ lub $\{a, b\} \leq l$ in $(L, \leq)$

$\Rightarrow a \vee b \leq l$ in $(L, \leq)$

$\Rightarrow l \geq a \vee b$.

$\Rightarrow a \vee b$ is glb of $\{a, b\}$ in $(L, \geq)$.

Similarly, we can show that $a \wedge b$ is the lub of $\{a, b\}$ in $(L, \geq)$. Hence $(L, \geq)$ is a lattice.

References:

1. Liu and Mohpatra, "Elements of Discrete Mathematics", McGraw Hill.

2. Jean Paul Trembly, R. Manohar, "Discrete Mathematical Structures with applications to Computer Science," McGrawHill

Sub Lattice

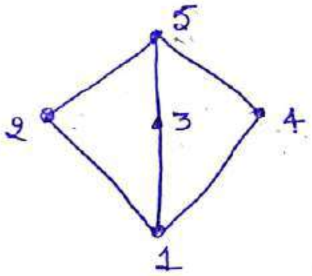
- A non-empty subset of M of lattice $(L, \leq)$ is said to be a sub-lattice of L if M is closed w.r.t meet $(\wedge)$ and joint $(\vee)$ ie.

$$x, y \in M \Rightarrow x \vee y \in M \text{ and } x \wedge y \in M$$

or

- A non empty subset of M of lattice $(L, \leq)$ is said to be sub-lattice of L if M itself formed lattice w.r.t $\vee$ and $\wedge$ operation.

Q. Consider the lattice $L = \{1, 2, 3, 4, 5\}$ as shown in figure below. Determine all sublattices with three or more elements.



sol^n: All the sublattice with three or more elements are those whose LUB and GLB exists for every pair of elements which are as follows:

i) $\{1, 2, 5\}$ (ii) $\{1, 3, 5\}$ iii) $\{1, 4, 5\}$

iv) $\{1, 2, 3, 5\}$ v) $\{1, 3, 4, 5\}$ vi) $\{1, 2, 3, 4, 5\}$

vii) $\{1, 2, 4, 5\}$

Q. Consider the lattice of all integer 'I' under the operation of divisibility. The Lattice D_n of all divisors of $n > 1$ is a sub-lattice of 'I'. Determine all the sublattice of D_{30} that contain atleast four elements.

$\underline{Sol^n}$: $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$

The sublattice of D_{50} that solution at least four elements are as follows:

i) $\{1, 2, 6, 30\}$ (ii) $\{1, 2, 3, 30\}$ (iii) $\{1, 5, 15, 30\}$

iv) $\{1, 3, 6, 30\}$ v) $\{1, 5, 10, 30\}$ vi) $\{1, 3, 15, 30\}$

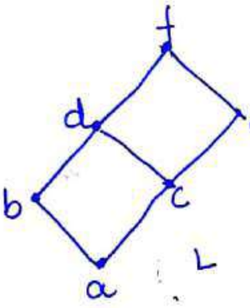
UNIT 03

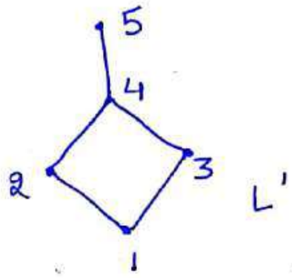
LECTURE NO. 05

Isomorphic Lattice [R1]

- Two lattice L_1 and L_2 are isomorphic if there exists a one-to-one correspondance $f: L_1 \to L_2$ such that $f(a \wedge b) = f(a) \wedge f(b)$
and $f(a \vee b) = f(a) \vee f(b)$

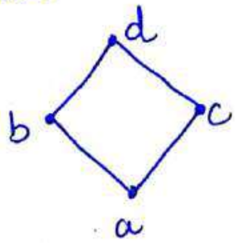
Q] Show that the lattice L and L' given below are not isomorphic?

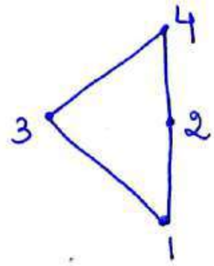




Sol: Consider the mapping
$f = \{(a,1), (b,2), (c,3), (d,4)$ (e, not defined)$\}$
Since there is no one to one correspondance between L and L'
$\therefore$ They are not isomorphic

Q] Determine whether the lattice shown are isomorphic or not





Sol^n: Consider the mapping

$f = \{(a,1),(b,2),(c,3),(d,4)\}$

$\therefore$ there is one-to-one correspondance

now T.P $f(a \wedge b) = f(a) \wedge f(b)$

& $f(a \vee b) = f(a) \vee f(b)$

So; $f(b \wedge c) = f(a) = 1$

$f(b) \wedge f(c) = 2 \wedge 3 = 1$

and $f(b \vee c) = f(d) = 4$

$f(b) \vee f(c) = 2 \vee 3 = 4$

$\therefore$ L1 and L2 are isomorphic.

* Refer to Question on Isomorphic lattice on Pg 17.

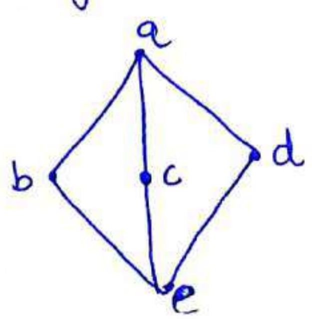
Distributive Lattice [R1]

- A lattice L is called distributive lattice if for any element a, b & c, it satisfies the following properties

i) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

ii) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

Q] Show that the given lattice is not a distributive lattice.



where $L = \{a,b,c,d,e\}$ and $\leq$ is a partial ordering relation.

Solⁿ: The joint and meet operations are defined by:

$$a \vee b = \text{lub}\{a, b\}$$
$$a \wedge b = \text{glb}\{a, b\}$$

$\vee$	a	b	c	d	e
a	a	a	a	a	a
b	a	b	a	a	b
c	a	a	c	a	c
d	a	a	a	d	d
e	a	b	c	d	e

$\wedge$	a	b	c	d	e
a	a	b	c	d	e
b	b	b	e	e	e
c	c	e	c	e	e
d	d	e	e	d	e
e	e	e	e	e	e

for a, b, c

$$a \vee (b \wedge c) = a \vee e = a$$

$$a \wedge (b \vee c) = a \wedge a = a$$

$$(a \vee b) \wedge (a \vee c) = a \wedge a = a$$

$$(a \wedge b) \vee (a \wedge c) = b \vee c = a$$

satisfies the condition for a, b, c.

for b, c, d

$$b \vee (c \wedge d) = b \vee e = b$$

$$b \wedge (c \vee d) = b \wedge a = b$$

$$(b \vee c) \wedge (b \vee d) = a \wedge a = a$$

$$(b \wedge c) \vee (b \wedge d) = e \vee e = e$$

condition fails for b, c, d.

$\therefore$ It is not a distributed Lattice.

Q] Explain in detail

a) Sub-lattice

b) Complete Lattice

c) Complemented Lattice

d) Bounded Lattice

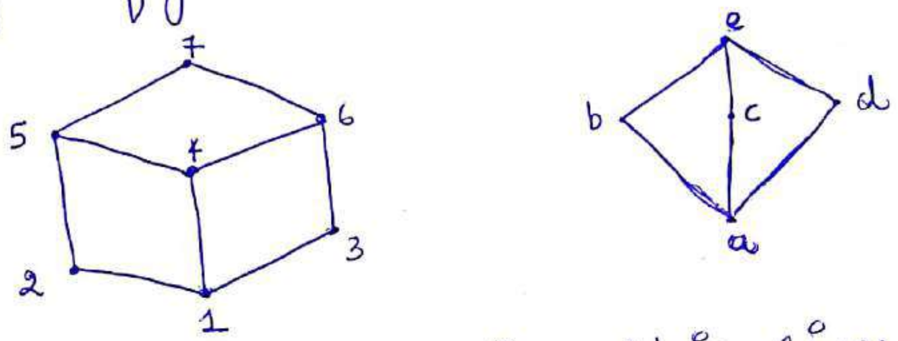
e) Modular Lattice.

References:

1. Liu and Mohpatra, "Elements of Discrete Mathematics," McGraw Hill.

*Question on Isomorphic lattice (from pg 16)

Q. Determine whether the lattice shown in the given figure are isomorphic.

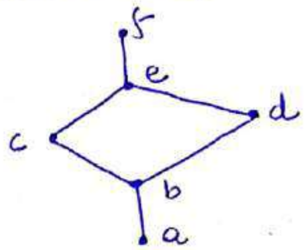


Solⁿ: L1 and L2 lattices are isomorphic. Since one-one corresponding is not possible as the element of two lattices are not same.

Bounded Lattice

- A lattice L is said to be a bounded lattice if it has a greatest element 1 and a least element 0.

- If L is a bounded lattice, then for any element $a \in L$, we have the following identities



   i) $0 \leq a \leq 1$
   ii) $a \vee 0 = a$, $a \wedge 0 = 0$
   iii) $a \vee 1 = 1$, $a \wedge 1 = a$

- The Bounded lattice is represented as $\boxed{(L, \wedge, \vee, 0, 1)}$

Complete Lattice

- A lattice is called complete if each of its non-empty subsets has a LUB and GLB.

Complemented Lattice

- A lattice L is called a complemented lattice if it is
   i) Bounded
   ii) Every element in it has a complement.

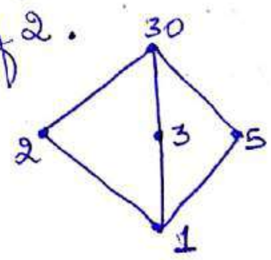
Procedure to find the complement of an element of L

- In a bounded lattice $(L, \wedge, \vee, 0, 1)$ an element $b \in L$ is called a complement of an element $a \in L$ if

$$\boxed{a \wedge b = 0 \text{ and } a \vee b = 1}$$

where 0 and 1 are the Lower and upper bound of L.

Q. Let $A = \{1, 2, 3, 5, 30\}$ and $a \leq b$ iff a divides b. The Hasse diagram is shown below. Find complement of 2.



Sol^n: Here $\wedge$ or $0 = 1$
and $\vee$ or $1 = 30$

now, let $a = 2$ and $b = 3$

$2 \wedge 3 = 1$ and $2 \vee 3 = 30$

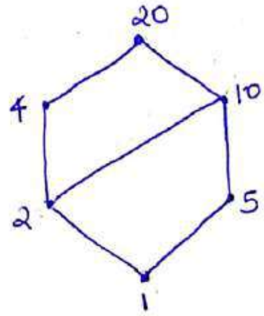
$\therefore$ 3 is the complement of 2.

now, let $a = 2$ and $b = 5$

$2 \wedge 5 = 1$ and $2 \vee 5 = 30$

$\therefore$ 5 is also the complement of 2

Q. Consider the lattice D_{20} under the partial order of divisibility whose Hasse Diagram is as follows; Prove that it is not a complemented lattice



Sol^n: Here $\wedge$ or $0 = 1$

and $\vee$ or $1 = 20$

we observe that

if $a = 2$ and $b = 5$

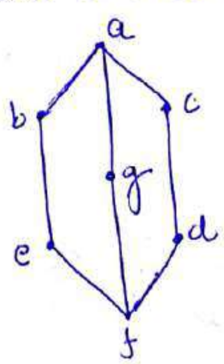
we have $2 \wedge 5 = 1$ and $2 \vee 5 = \underset{\text{not } \vee \text{ element}}{10}$

also if $a = 10$ and $b = 4$

we have $10 \wedge 4 = \underset{\text{not } \wedge \text{ element}}{2}$ and $10 \vee 4 = 20$

we observe that elements 4 and 10 in D_{20} have no complements. $\therefore$ It is not a complemented lattice.

Q. In the lattice defined by Hasse Diagram given by foll. figures How many complements does the element 'e' have?



Sol^n: here $\wedge$ or $0 = f$

and $\vee$ or $1 = a$

now

let $a = e$ & $b = g$

$e \wedge g = f$

$e \vee g = a$

let $a = e$ & $b = c$

$e \wedge c = f$

$e \vee c = a$

let $a = e$ & $b = d$

$e \wedge d = f$

$e \vee d = a$

let $a = e$ & $b = b$

$e \wedge b$

$e \vee b$

$\therefore$ d, c, g are complements of e.

Modular Lattice

- The Lattice $(L, \leq)$ is said to be Modular Lattice if

$$\boxed{a \vee (b \wedge c) = (a \vee b) \wedge c}$$

whenever $a \leq c$, $\forall a, b, c \in L$

- Every distributive lattice is modular.

UNIT 03

LECTURE NO. 06

Boolean Algebra

- Boolean Algebra is used to analyse and simplify the digital (logic) circuits.
- It uses only the binary numbers ie 0 and 1.
- It is also called as Binary Algebra or Logical Algebra.
- Boolean Algebra was invented by George Boole in 1854.

Logical Statements

- These are the sentences which can be determined to be true or false.
- Logical statements are also called as Truth Function.
- Example: Today is Monday (T or F)
  Sit down (cannot be represented as T or F)
- Results 'True' or 'False' are called Truth Values, ie. result of logical statement is called Truth Values.
- True is denoted by '1' and False is denoted by '0'.

Binary Valued/ Logical Variables

- These are the variables which can store the Truth Values.
- These variable can store any one of the two value at a time, ie it can either store T(1) or F(0) at particular time.

Logical Operations

- These are the specific operations that can be applied on Truth Functions or Logical statements.

Truth Table

- It is a table which represents all possible values of logical variable/statements along with all the possible results of the given combinations of values.

- **Example:**

X	Y	R
0	0	0
0	1	0
1	0	0
1	1	1

i/p combinations; o/p

⟹ Truth Table for logical variables X and Y.

Logical operators

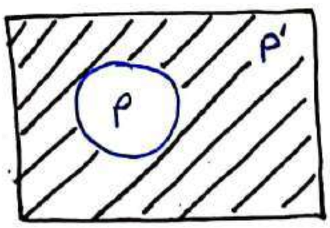
- Logical operators are applied on Logical variables.
- Basic logical operators are: NOT, OR and AND Operator
- Other logical operators are: XOR, NOR etc.

1. NOT OPERATOR
   - It operates on single variable and the operation is called Complementation
   - Denoted by ¯ (Bar), '.
   - NOT operator is also called as Inverter.
   - Truth Table of NOT

P	$\bar{P}$/P'
T	F
F	T

P	$\bar{P}$/P'
1	0
0	1

- Venn Diagram

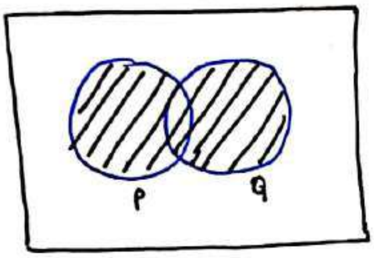


2. OR OPERATOR

- It denotes logical addition.
- Denoted by '+' ; 'v'
- Truth Table of OR

P	Q	P + Q
0	0	0
0	1	1
1	0	1
1	1	1

- Venn Diagram of OR

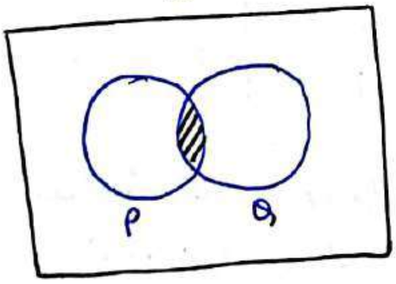


3. AND OPERATOR

- It is called logical multiplication.
- Denoted by '·' ; '∧'
- Truth Table of AND

P	Q	P · Q
0	0	0
0	1	0
1	0	0
1	1	1

- Venn Diagram of AND



Evaluation of Boolean Expressions using Truth Table

* no. of combⁿ 2^n

Q. Construct truth table for $X + \overline{YZ}$

Solⁿ:

X	Y	Z	Y.Z	$\overline{YZ}$	$X + \overline{YZ}$
0	0	0	0	1	1
0	0	1	0	1	1
0	1	0	0	1	1
0	1	1	1	0	0
1	0	0	0	1	1
1	0	1	0	1	1
1	1	0	0	1	1
1	1	1	1	0	1

Q. In the Boolean Algebra, verify using truth table that $X + XY = X$, for each X, Y in $\{0, 1\}$

Sol^n:

X	Y	XY	X + XY
0	0	0	0
0	1	0	0
1	0	0	1
1	1	1	1

X and X+XY are same

$\therefore X + XY = X$

Hence Proved.

Q. In the Boolean Algebra, verify using truth table that $(X+Y)' = X'Y'$ for each X, Y in $\{0, 1\}$

Sol^n:

X	Y	X+Y	(X+Y)'	X'	Y'	X'.Y'
0	0	0	1	1	1	1
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	1	0	0	0	0

$(X+Y)'$ and $X'.Y'$ are same

$\therefore (X+Y)' = X'.Y'$

Hence Proved

Q. Prepare table of combinations for the following Boolean Algebra Expressions: $\bar{X}\bar{Y} + \bar{X}Y$

Sol^n:

X	Y	$\bar{X}$	$\bar{Y}$	$\bar{X}.\bar{Y}$	$\bar{X}.Y$	$\bar{X}\bar{Y} + \bar{X}Y$
0	0	1	1	1	0	1
0	1	1	0	0	1	1
1	0	0	1	0	0	0
1	1	0	0	0	0	0

UNIT 03

LECTURE NO. 07

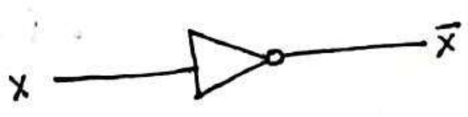
Basic Logic Gate

- A gate is a basic electronic circuit, which operates on one or more signals to produce an output signal.
- Gates are 2-state circuits, and hence digital.
- 2 states can be
  - (i) LOW VOLTAGE (0)
  - (ii) HIGH VOLTAGE (1)
- Hence input of Logic Gates will be either 0 or 1.

Types of Logic Gates : BASIC

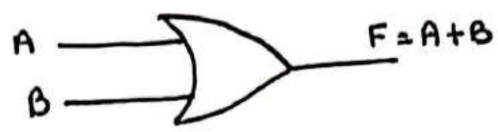
i) Inverter (NOT GATE)
ii) OR GATE
iii) AND GATE

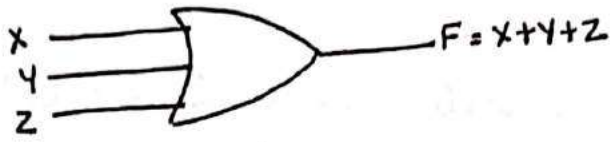
1. INVERTOR/ NOT GATE
   - It is the gate with only one i/p signal and one o/p signal.
   - o/p state is always opposite of i/p state
   - Symbol:



2. OR GATE
   - It has two or more i/p signals but only one o/p signal.
   - If any one of the i/p is 1 (high), the o/p is 1, else 0.

• Symbol :



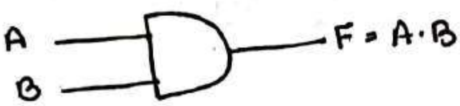


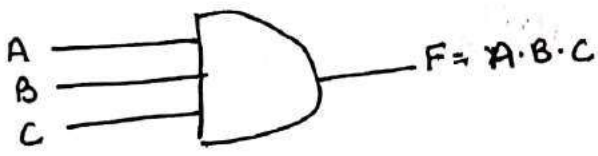
3. AND GATE

• It has two or more i/p signals and produces an o/p signal.

• When all i/p are 1 (high), then o/p is 1, else 0.

• Symbol





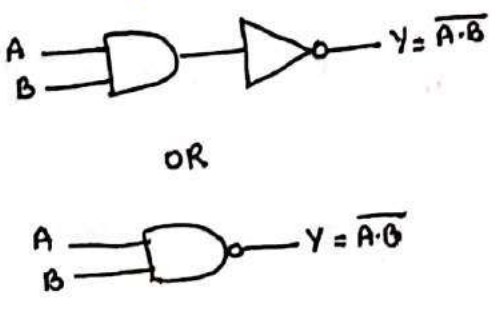
Other Types of Logic Gates

1. NAND GATE

• A NOT - AND operation is known as NAND operation.

• It has two or more i/p signals and produces 1 o/p signal.

• Symbol



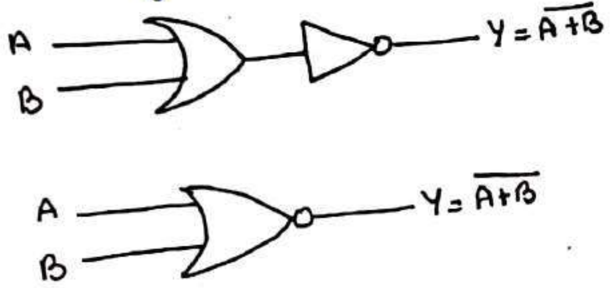
• Truth Table

A	B	$\overline{A \cdot B}$
0	0	1
0	1	1
1	0	1
1	1	0

Scanned by CamScanner

2. NOR GATE

- A NOT-OR operation is known as NOR operation
- It has two or more i/p signals and produces 1 o/p signal.
- Symbol

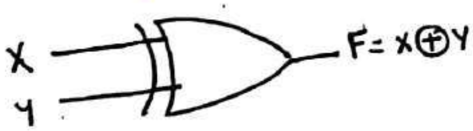


- Truth Table

A	B	$\overline{A+B}$
0	0	1
0	1	0
1	0	0
1	1	0

3. XOR GATE

- XOR or Ex-OR Gate is a special type of gate.
- It can be used in the half adder, full adder or subtractor.
- The EXCLUSIVE OR GATE is abbreviated as EX-OR GATE or sometimes as X-OR GATE.
- It has two or more i/p signals and produces 1 o/p signal.
- Symbol

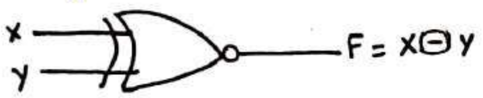


- Truth Table

A	B	A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

4. XNOR GATE

- XNOR gate is a special type of gate.
- It can be used in half adder, full adder and subtractor.
- The EXCLUSIVE-NOR GATE is abbreviated as EX-NOR gate or some time as X-NOR gate.
- It has two or more i/p signals and produces 1 o/p signal.
- Symbol



- Truth Table

X	Y	X⊙Y
0	0	1
0	1	0
1	0	0
1	1	1

UNIT 03

LECTURE NO. 08

Basic Postulates of Boolean Algebra

- These are the fundamental laws of Boolean Algebra.

1. If $X \neq 0$, then $X = 1$
   and if $X \neq 1$, then $X = 0$
2. OR Relations (Logical Addition)

$$\left.\begin{array}{l} 0+0=0 \\ 0+1=1 \\ 1+0=1 \\ 1+1=1 \end{array}\right\} \text{*Truth Table of OR OPN}^{n}$$

3. AND Relations (Logical Multiplication)

$$\left.\begin{array}{l} 0\cdot 0=0 \\ 0\cdot 1=0 \\ 1\cdot 0=0 \\ 1\cdot 1=1 \end{array}\right\} \text{*Truth Table of AND OPN}^{n}$$

4. Complement Rules (NOT/INVERSION)

$$\left.\begin{array}{l} \bar{0}=1 \\ \bar{1}=0 \end{array}\right\} \text{*Truth Table of NOT OPN}^{n}$$

Principle of Duality

- It states that starting with a boolean relation, another boolean relation can be derived by,
  1. Changing each OR sign (+) to AND sign (·) and vice versa.
  2. Replacing each 0 by 1 and vice versa
- Derived relation/expression using duality principle is called as <u>Dual</u> of original expression.

• Example

SR. NO.	Expression	Dual Expression
1.	0 + 0 = 0	1 · 1 = 1
2.	0 + 1 = 1	1 · 0 = 0
3.	1 + 0 = 1	0 · 1 = 0
4.	1 + 1 = 1	0 · 0 = 0
	OR oprⁿ	AND oprⁿ

Basic Theorems of Boolean Algebra

1. Properties of 0 and 1

a) $0 + X = X$

Proof: using Truth Table

0	X	0 + X
0	0	0
0	1	1

here $0 + X = X$
hence proved

c) $0 \cdot X = 0$

Proof: using Truth Table

0	X	0 · X
0	0	0
0	1	0

here $0 \cdot X = 0$
hence proved

b) $1 + X = 1$

Proof: using Truth Table

1	X	1 + X
1	0	1
1	1	1

here $1 + X = 1$
hence proved

d) $1 \cdot X = X$

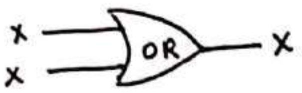
Proof: using Truth Table

1	X	1 · X
1	0	0
1	1	1

here $1 \cdot X = X$
hence proved

2. Idempotence Law

a) $X + X = X$

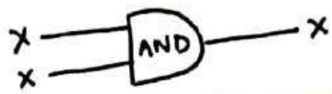


Proof: using Truth Table

X	X	$X+X$
0	0	0
1	1	1

here $X+X = X$
hence proved

b) $X \cdot X = X$



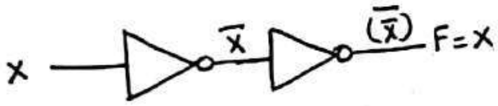
Proof: using Truth Table

X	X	$X \cdot X$
0	0	0
1	1	1

here $X \cdot X = X$
hence proved

3. Involution Law

$(\overline{\overline{X}}) = X$



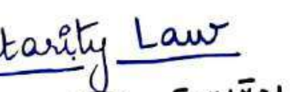
Proof: using Truth Table

X	$\overline{X}$	$(\overline{\overline{X}})$
0	1	0
1	0	1

here $(\overline{\overline{X}}) = X$
hence proved

4. Complementarity Law

a) $X + \overline{X} = 1$



Proof: using Truth Table

X	$\overline{X}$	$X+\overline{X}$
0	1	1
1	0	1

here $X + \overline{X} = 1$
hence proved

b) $X \cdot \overline{X} = 0$

Proof: using Truth Table

X	$\overline{X}$	$X \cdot \overline{X}$
0	1	0
1	0	0

here $X \cdot \overline{X} = 0$
hence proved

5. Commutative Law

a) $x + y = y + x$

Proof: using Truth Table

x	y	x + y	y + x
0	0	0	0
0	1	1	1
1	0	1	1
1	1	1	1

here $x+y = y+x$
hence proved

b) $x \cdot y = y \cdot x$

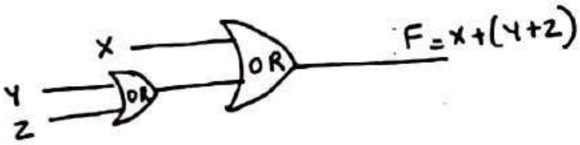
Proof: using Truth Table

x	y	x · y	y · x
0	0	0	0
0	1	0	0
1	0	0	0
1	1	1	1

here $x \cdot y = y \cdot x$
hence proved

6. Associative Law

a) $x + (y+z) = (x+y) + z$

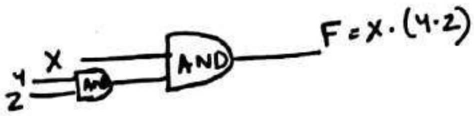


Proof: using Truth Table

x	y	z	(y+z)	x+(y+z)	(x+y)	(x+y)+z
0	0	0	0	0	0	0
0	0	1	1	1	0	1
0	1	0	1	1	1	1
0	1	1	1	1	1	1
1	0	0	0	1	1	1
1	0	1	1	1	1	1
1	1	0	1	1	1	1
1	1	1	1	1		1

here
$x+(y+z) = (x+y)+z$
hence proved

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



here
$x \cdot (y \cdot z) = (x \cdot y) z$
hence proved

Proof: using Truth Table

x	y	z	(y·z)	x·(y·z)	(x·y)	(x·y)·z
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	1	0	0	0
1	0	0	0	0	0	0
1	0	1	0	0	0	0
1	1	0	0	0	1	0
1	1	1	1	1	1	1

7. Distributive Law

a) $x(y+z) = xy + xz$

Proof: using Truth Table

x	y	z	y+z	x·(y+z)	xy	xz	xy+xz
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

here $x \cdot (y+z) = xy \cdot xz$
hence proved

b) $x + (y \cdot z) = (x+y) \cdot (x+z)$

Proof: using Laws

R.H.S: $(x+y) \cdot (x+z)$

$\Rightarrow xx + xz + yx + yz$ (xx = x by idempotent law) (xy = yx, xz = zx commutative law)

$\Rightarrow x + xy + xz + yz$

$\Rightarrow x(1+y) + xz + yz$ (1+y = 1 prop of 0&1)

$\Rightarrow (x \cdot 1) + xz + yz$ (x·1 = x prop of 0&1)

$\Rightarrow x + xz + yz$

$\Rightarrow x(1+z) + yz$ (1+z = 1 prop of 0&1)

$\Rightarrow (x \cdot 1) + yz$ (x·1 = x prop of 0&1)

$\Rightarrow x + yz$

$\Rightarrow$ L.H.S

here L.H.S = R.H.S
hence proved

Scanned by CamScanner

8. Absorption Law

a) $X + XY = X$

Proof: using Laws

$L.H.S = X + XY$

$\Rightarrow X \cdot (1+Y)$

$\Rightarrow X \cdot 1$ $\quad (1+Y = 1$, prop. of 0&1)

$\Rightarrow X$ $\quad (X \cdot 1 = X$, prop. of 0&1)

$\Rightarrow R.H.S$

here $L.H.S = R.H.S$
hence proved

b) $X(X+Y) = X$

Proof: using Laws

$L.H.S = X(X+Y)$

$= X \cdot X + X \cdot Y$

$= X + X \cdot Y$ $\quad (X \cdot X = X$, Idempotence law)

$= X \cdot (1+Y)$

$= X \cdot 1$ $\quad (1+Y = 1$, prop. of 0&1)

$= X$

$= R.H.S$

here $L.H.S = R.H.S$
hence proved

9. Other Rules of Boolean Algebra

a) $X + \overline{X}Y = X + Y$ (Third Distributive Law)

Proof: using Laws

$L.H.S = X + \overline{X}Y$

$= X \cdot 1 + \overline{X} \cdot Y$

$= X \cdot (1+Y) + \overline{X} \cdot Y$

$= X + X \cdot Y + \overline{X} \cdot Y$

$= X + Y(X + \overline{X})$

$= X + Y \cdot 1$ $\quad (X + \overline{X} = 1$ Complementarity law)

$= X + Y$ $\quad (Y \cdot 1 = Y$, OR rel^n law)

$= R.H.S$ $\quad$ here $L.H.S = R.H.S$
hence Proved

UNIT 03

LECTURE NO. 09

DeMorgan's Theorem

1. FIRST THEOREM: $\overline{X+Y} = \overline{X}\cdot\overline{Y}$

Proof: using Laws

let us assume, $\boxed{P = X+Y}$ — (A)

now, according to Complementarity law,

$\boxed{P+\overline{P}=1 \text{ and } P\cdot\overline{P}=0}$ — (B)

now if, $\overline{P} = \overline{X+Y} = \overline{X}\cdot\overline{Y}$ (assuming it to be true)

$\therefore \boxed{\overline{P} = \overline{X}\cdot\overline{Y}}$ — (C)

ie if X+Y's compliment is $\overline{X}\,\overline{Y}$, then the following must be true;

substituting (C) in (B), we get

$P+\overline{P} = 1$

$\Rightarrow \underbrace{(X+Y)+(\overline{X}\cdot\overline{Y})=1}_{\text{must be true}}$ (from (A) & (C))

$\Rightarrow ((X+Y)+\overline{X})\cdot((X+Y)+\overline{Y})$ (Distribⁿ Law)

$\Rightarrow (X+\overline{X}+Y)\cdot(X+Y+\overline{Y})$

$\Rightarrow (1+Y)\cdot(1+X)$ $(X+\overline{X}=1 \;\&\; Y+\overline{Y}=1)$

$\Rightarrow (1)\cdot(1)$ (1+X=1; prop of 0&1) (OR opⁿ)

$\Rightarrow 1$

$\therefore \boxed{P+\overline{P}=1}$ hence proved

hence our assumption is correct.

$P\cdot\overline{P}=0$

$\Rightarrow \underbrace{(X+Y)\cdot(\overline{X}\cdot\overline{Y})=0}_{\text{must be true}}$ (from (A) & (C))

$\Rightarrow (\overline{X}\cdot\overline{Y}\cdot X)+(\overline{X}\cdot\overline{Y}\cdot Y)$

$\Rightarrow (\overline{X}\cdot X\cdot\overline{Y})+(\overline{X}\cdot\overline{Y}\cdot Y)$

$\Rightarrow (0\cdot\overline{Y})+(0\cdot Y)$

$\Rightarrow 0+0$ $(0\cdot\overline{Y}=0$; prop of 0&1)

$\Rightarrow 0$ (And opⁿ)

$\therefore \boxed{P\cdot\overline{P}=0}$ hence proved

hence our assumption is correct.

hence $\overline{X+Y} = \overline{X}\cdot\overline{Y}$

2. SECOND THEOREM : $\overline{X \cdot Y} = \overline{X} + \overline{Y}$

Proof: using Laws, let $P = X \cdot Y$, then let $\overline{P} = \overline{X} + \overline{Y}$ and $P + \overline{P} = 1$ & $P \cdot \overline{P} = 0$ (complementarity)

If XY's complement is $\overline{X} + \overline{Y}$, then the following must be true,

$P + \overline{P} = 1$

ie $XY + (\overline{X} + \overline{Y}) = 1$

$\Rightarrow XY + (\overline{X} + \overline{Y})$

$\Rightarrow (\overline{X} + \overline{Y}) + XY$

$\Rightarrow (\overline{X} + \overline{Y} + X) \cdot (\overline{X} + \overline{Y} + Y)$

$\Rightarrow (\overline{X} + X + \overline{Y}) \cdot (\overline{X} + \overline{Y} + Y)$

$\Rightarrow (1 + \overline{Y}) \cdot (1 + \overline{X})$

$\Rightarrow (1) \cdot (1)$

$\Rightarrow 1$ hence proved

$P \cdot \overline{P} = 0$

ie $XY \cdot (\overline{X} + \overline{Y}) = 0$

$\Rightarrow XY \cdot (\overline{X} + \overline{Y})$

$\Rightarrow (XY\overline{X}) + (XY\overline{Y})$

$\Rightarrow (X\overline{X}Y) + (XY\overline{Y})$

$\Rightarrow (0 \cdot Y) + 0 \cdot X)$

$\Rightarrow 0 + 0$

$\Rightarrow 0$ hence prove

hence our assumption is correct

hence $\overline{X \cdot Y} = \overline{X} + \overline{Y}$

Demorganization

- The process follows given below steps:
  1. Complement entire function.
  2. Change all the ANDs ($\cdot$) to ORs ($+$) and vice versa.
  3. Complement each of the individual variables.

Q. Evaluate $\overline{\overline{AB} + \overline{A} + AB}$

Sol^n: $\overline{\overline{AB} + \overline{A} + AB}$

$\Rightarrow \overline{\overline{A} + \overline{B} + \overline{A} + AB}$

$\Rightarrow \overline{(\overline{A} + \overline{B}) + (\overline{A} + AB)}$

$\Rightarrow (\overline{\overline{A} + \overline{B}}) \cdot (\overline{\overline{A} + AB})$ (DeMogran's Law : $\overline{X+Y} = \overline{X} \cdot \overline{Y}$)

$\Rightarrow \overline{\overline{A}} \cdot \overline{\overline{B}} \cdot \overline{\overline{A}} \cdot \overline{AB}$ (DeMorgan's law : $\overline{X+Y} = \overline{X} \cdot \overline{Y}$)

$\Rightarrow A \cdot B \cdot A \cdot \overline{AB}$

$\Rightarrow A \cdot B \cdot A \cdot \overline{A} + \overline{B}$ (DeMorgan's law : $\overline{XY} = \overline{X} + \overline{Y}$)

$\Rightarrow AB \cdot (A(\overline{A} + \overline{B}))$

$\Rightarrow AB(A\bar{A} + A\bar{B})$

$\Rightarrow AB(0 + A\bar{B})$ $(0 + x = x$: 0 & 1's prop.)

$\Rightarrow AB\cdot 0 + AB\cdot A\bar{B}$

$\Rightarrow 0 + AB\cdot A\bar{B}$

$\Rightarrow 0 + AA\cdot B\bar{B}$

$\Rightarrow 0 + AA\cdot 0$

$\Rightarrow 0 + 0$

$\Rightarrow 0$ final answer

Boolean Expression Minimization

- Boolean Expression Minimization refers to less no. of gates resulting into simplified circuitary
- It can be done by two methods :
  1) Algebraic Method
  2) K-Maps

$\Rightarrow$ ALGEBRAIC METHOD

- This method uses boolean postulates , rules and theorems to simplify expressions.

Q1. Simplify $A\bar{B}C\bar{D} + A\bar{B}CD + ABC\bar{D} + ABCD$.

Sol^n: $A\bar{B}C\bar{D} + A\bar{B}CD + ABC\bar{D} + ABCD$

$\Rightarrow A\bar{B}C[\bar{D} + D) + ABC(\bar{D} + D)$ $(\because x + \bar{x} = 1$, complementarity law)

$\Rightarrow A\bar{B}C\cdot 1 + ABC\cdot 1$ $(\because 1\cdot x = x$, prop. of 0 & 1)

$\Rightarrow A\bar{B}C + ABC$

$\Rightarrow AC[\bar{B} + B]$ $(\because x + \bar{x} = 1$, complementarity law)

$\Rightarrow AC\cdot 1$ $(\because 1\cdot x = x$, prop of 0 & 1)

$\Rightarrow AC$

Q2. Simplify $\overline{XY} + \overline{X} + XY$

Solⁿ: $\overline{XY} + \overline{X} + XY$

$\Rightarrow \overline{X} + \overline{Y} + \overline{X} + XY \quad$ ($\because \overline{XY} = \overline{X} + \overline{Y}$; DeMorgan's law)

$\Rightarrow \overline{X} + \overline{X} + \overline{Y} + XY$

$\Rightarrow \overline{X} + \overline{Y} + XY \quad$ ($\because X + X = X$; Idempotence Law)

$\Rightarrow \overline{X} + \overline{\overline{X}}Y + \overline{Y} \quad$ ($\because (\overline{\overline{X}}) = X$; Involution Law)

$\Rightarrow \overline{X} + Y + \overline{Y} \quad$ ($\because X + \overline{X}Y = X + Y$; Third Distributive Law)

$\Rightarrow \overline{X} + 1 \quad$ ($\because X + \overline{X} = 1$; Complementarity law)

$\Rightarrow 1 \quad$ ($\because X + 1 = 1$; Propertity of 0 & 1)

Q3. Simplify $\overline{X}\,\overline{Y}\,\overline{Z} + \overline{X}Y\overline{Z} + X\overline{Y}\,\overline{Z} + XY\overline{Z}$

Solⁿ: $\overline{X}\,\overline{Y}\,\overline{Z} + \overline{X}Y\overline{Z} + X\overline{Y}\,\overline{Z} + XY\overline{Z}$

$\Rightarrow \overline{X}(\overline{Y}\,\overline{Z} + Y\overline{Z}) + X(\overline{Y}\,\overline{Z} + Y\overline{Z})$

$\Rightarrow \overline{X}(\overline{Z}(\overline{Y} + Y)) + X(\overline{Z}(\overline{Y} + Y))$

$\Rightarrow \overline{X}(\overline{Z} \cdot 1) + X(\overline{Z} \cdot 1) \quad$ ($\because X + \overline{X} = 1$; Complementarity law)

$\Rightarrow \overline{X}\,\overline{Z} + X\overline{Z} \quad$ ($\because X \cdot 1 = X$; prop. of 1 & 0)

$\Rightarrow \overline{Z}(\overline{X} + X) \quad$ ($\because X + \overline{X} = 1$; Complementarity law)

$\Rightarrow \overline{Z} \cdot 1 \quad$ ($\because X \cdot 1 = X$; prop. of 1 & 0)

$\Rightarrow \overline{Z}$

⇒ K-MAP METHOD

- Karnaugh (K-Map) is a graphical display of the fundamental products in a truth table.
- It contains squares, each representing maxterm | minterm.

Sum of Products (SOP) Reduction using K-Maps.

- In SOP, each square of K-Map represents minterm.
- We fill each minterm of square with '1'.
- for 'n' no. of variables ; 2^n cells are required in K-Map.

Scanned by CamScanner

- Filling of K-MAP: Procedure

2-Variable K-Map

X \ Y	0 ($\bar{Y}$)	1 (Y)
($\bar{X}$) 0	0 00	1 01
(X) 1	2 10	3 11

3-Variable K-Map

X \ YZ	00	01	11	10
0	0 000	1 001	3 011	2 010
1	4 100	5 101	7 111	6 110

(OR)

XY \ Z	0	1
00	0	1
01	2	3
11	6	7
10	4	5

4-Variable K-Map

WX \ YZ	00	01	11	10
00	0	1	3	2
01	4	5	7	6
11	12	13	15	14
10	8	9	11	10

*Note: The binary code 00, 01, 11, 10, is called Gray code. It is the code in which each successive number differs only in 'one' place.

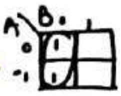
- Rules of SOP reduction using K-MAP

i) Prepare truth table for given function.
ii) Draw an empty K-Map for the given function (2var, 3var..)
iii) Map the given func^n be entering 1's for the o/p as 1 in corresponding squares.
iv) Enter 0's in all left out empty squares.
v) Make group of cells (octet, Quad, Pair etc) * 2^n adjacent cells
  * Make the largest possible groups.
vi) Remove redundant groups (if any).
vii) Write the reduced expression for all the groups and OR(+) them.

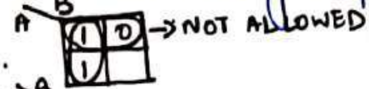
Scanned by CamScanner

- Rules for Grouping/Filling of Cells $\begin{bmatrix} *SOP \rightarrow 1 \\ POS \rightarrow 0 \end{bmatrix}$

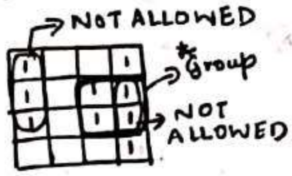
i) Adjacent cells which have 1's can be grouped together.



ii) Groups can't contain a 0.

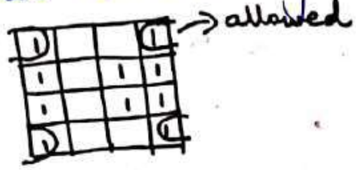


iii) Groups can't be diagonal.



iv) Groups must contain 2^n cells.

v) Each group should be as large as possible.



Q1. Reduce $F(a,b,c,d) = \sum(0,2,7,8,10,15)$ ↳ (Σ: min)

Sol^n: here $n=4$

$\therefore$ no. of cells $= 2^n = 16$

AB \ CD	$\bar{C}\bar{D}$ 00	$\bar{C}D$ 01	CD 11	$C\bar{D}$ 10
$\bar{A}\bar{B}$ 00	1 (0)	(1)	(3)	1 (2)
$\bar{A}B$ 01	(4)	(5)	1 (7)	(6)
AB 11	(12)	(13)	1 (15)	(14)
$A\bar{B}$ 10	1 (8)	(9)	(11)	1 (10)

→ Group1: Quad $\Rightarrow m_0 + m_2 + m_8 + m_{10} \Rightarrow \bar{B}\bar{D}$

→ Group2: Pair $\Rightarrow m_7 + m_{15} \Rightarrow BCD$

$\therefore$ $\boxed{Ans = \bar{B}\bar{D} + BCD}$

Q2. Find simplified boolean equation for the given func^n:

Sol^n: $F(A,B,C,D) = \sum(7,9,10,11,12,13,14,15)$

here $n=4$ $\therefore$ no. of cells $= 2^n = 16$

AB \ CD	$\bar{C}\bar{D}$ 00	$\bar{C}D$ 01	CD 11	$C\bar{D}$ 10
$\bar{A}\bar{B}$ 00	(0)	(1)	(3)	(2)
$\bar{A}B$ 01	(4)	(5)	1 (7)	(6)
AB 11	1 (12)	1 (13)	1 (15)	1 (14)
$A\bar{B}$ 10	(8)	1 (9)	1 (11)	1 (10)

→ Group1: Pair $\Rightarrow m_7 + m_{15} \Rightarrow BCD$

→ Group 2: Quad $\Rightarrow m_{12} + m_{13} + m_{15} + m_{14} \Rightarrow AB$

→ Group3: Quad: $m_9 + m_{11} + m_{13} + m_{15} \Rightarrow AD$

→ Group4: Quad $\Rightarrow m_{10} + m_{11} + m_{14} + m_{15} \Rightarrow AC$

$\therefore$ $\boxed{Ans = BCD + AB + AD + AC}$

Q3. Minimize following function using K-Map.

Solⁿ: $F(W,X,Y,Z) = \Sigma(0,4,8,12)$

WX \ YZ	$\bar{Y}\bar{Z}$ 00	$\bar{Y}Z$ 01	YZ 11	$Y\bar{Z}$ 10
$\bar{W}\bar{X}$ 00	1 (0)	(1)	(3)	(2)
$\bar{W}X$ 01	1 (4)	(5)	(7)	(6)
WX 11	1 (12)	(13)	(15)	(14)
$W\bar{X}$ 10	1 (8)	(9)	(11)	(10)

$\therefore$ $\boxed{\text{Ans} = \bar{Y}\bar{Z}}$

↳ Group 1: Quad: m_0 : $\bar{Y}\bar{Z}$

Q4. Obtain simplified form of following Boolean Expression:

$F(A,B,C,D) = \Sigma(0,1,2,4,5,7,8,9,10,11,14)$

Solⁿ:

AB \ CD	$\bar{C}\bar{D}$ 00	$\bar{C}D$ 01	CD 11	$C\bar{D}$ 10
$\bar{A}\bar{B}$ 00	1 (0)	1 (1)	(3)	1 (2)
$\bar{A}B$ 01	1 (4)	1 (5)	1 (7)	(6)
AB 11	(12)	(13)	(15)	1 (14)
$A\bar{B}$ 10	1 (8)	1 (9)	1 (11)	1 (10)

→ Group 1: Quad: $m_0 + m_2 + m_8 + m_{10} \Rightarrow \bar{B}\bar{D}$

→ Group 3: Pair : $m_5 + m_7 \Rightarrow \bar{A}BD$

→ Group 4: Pair: $m_{10} + m_{14} \Rightarrow AC\bar{D}$

→ Group 5: Quad: $m_8 + m_9 + m_{10} + m_{11} \Rightarrow A\bar{B}$

→ Group 2: Quad: $m_0 + m_1 + m_4 + m_5 \Rightarrow \bar{A}\bar{C}$

$\therefore$ $\boxed{\text{Ans} = \bar{B}\bar{D} + \bar{A}\bar{C} + \bar{A}BD + AC\bar{D} + A\bar{B}}$

Product of Sum (POS) Reduction using K-Map

- In POS, each square of K-Map represents a maxterm.
- In POS, map is filled by placing 0's.
- Rules for deriving POS boolean expression are exactly same as that of SOP except that adjacent 0's are encircled in groups.
- One major difference is that in POS K Maps, complemented letters represent 1's whereas uncomplemented letters represent 0's.

Q1: Find minimum POS expression of $Y(A,B,C,D) = \Pi(0,1,3,5,6,7,10,14,15)$

$\hookrightarrow (\Pi : \text{Max})$

Sol^n:

$AB \backslash CD$	$C+D$ 00	$C+\bar{D}$ 01	$\bar{C}+\bar{D}$ 11	$\bar{C}+D$ 10
$A+B$ 00	0 (0)	0 (1)	0 (3)	(2)
$A+\bar{B}$ 01	(4)	0 (5)	0 (7)	0 (6)
$\bar{A}+\bar{B}$ 11	(12)	(13)	0 (15)	0 (14)
$\bar{A}+B$ 10	(8)	(9)	(11)	0 (10)

Group 1: Quad: $M_1+M_3+M_5+M_7 \Rightarrow A+\bar{D}$

Group 2: Quad: $M_6+M_7+M_{14}+M_{15} \Rightarrow \bar{B}+\bar{C}$

group 4: Pair: $M_{10}+M_{14} \Rightarrow \bar{A}+\bar{C}+D$

Group 3: Pair: $M_0+M_1 \Rightarrow A+B+C$

$\therefore \boxed{Ans = (A+\bar{D})(\bar{B}+\bar{C})(A+B+C)(\bar{A}+\bar{C}+D)}$

Q2. Simplify $F(ABC) = \bar{A}BC + B\bar{C} + AB\bar{C} + A\bar{B}C$ in POS form

Sol^n:

$A \backslash BC$	$B+C$ 00	$B+\bar{C}$ 01	$\bar{B}+\bar{C}$ 11	$\bar{B}+C$ 10
A 00	0 (0)	0 (1)	1 (3)	1 (2)
$\bar{A}$ 01	0 (4)	1 (5)	0 (7)	1 (6)

* For POS, fill the empty cells by 0.

Group 3: $\overset{M_7}{\bar{A}+\bar{B}+\bar{C}}$

group 2: $B+C$ $\quad M_0+M_4$

Group 1: $A+B$ $\quad M_0+M_1$

$\therefore \boxed{Ans = (A+B)(B+C)(\bar{A}+\bar{B}+\bar{C})}$

Q3: Solve using K-Map:

$f = (A+B+C)(A+B+\bar{C})(A+\bar{B}+\bar{C})(\bar{A}+B+C)(\bar{A}+\bar{B}+C)(\bar{A}+\bar{B}+\bar{C})$

Sol^n:

$A \backslash BC$	$B+C$ 00	$B+\bar{C}$ 01	$\bar{B}+\bar{C}$ 11	$\bar{B}+C$ 10
A 00	0 (0)	0 (1)	0 (3)	(2)
$\bar{A}$ 01	0 (4)	(5)	0 (7)	0 (6)

Q4: Solve using K-Map: $f(A,B,C) = \Pi(0,3,6,7)$

Sol^n:

$A \backslash BC$	$B+C$ 00	$B+\bar{C}$ 01	$\bar{B}+\bar{C}$ 11	$\bar{B}+C$ 10
A 00	0 (0)	(1)	0 (3)	(2)
$\bar{A}$ 01	(4)	(5)	0 (7)	0 (6)

group 1: pair: $\overset{M_3+M_7}{\bar{B}+\bar{C}}$

group 2: pair: $M_6+M_7 \quad \bar{A}+\bar{B}$

group 3: single: $A+B+C$

$\therefore \boxed{Ans: (\bar{B}+\bar{C})(\bar{A}+\bar{B})(A+B+C)}$

Practice Questions on K-Map

Q1. Solve using K-Map: $f(A,B,C,D) = \Sigma(0,7,9,12,15)$.

Q2. Solve using K-Map: $f(A,B,C,D) = \Sigma m(0,2,3,7,11,13,14,15)$

Q3. Solve using K-Map: $f(A,B,C,D) = \Sigma m(0,2,3,5,7,8,10,11,14,15)$

Q4. Simplify following expression using K-Map:

$$F(A,B,C,D) = \Sigma m(4,5,6,7,8,9,10,11,12,13,14,15)$$

Q5. Simplify using K-Map: $F(A,B,C) = \bar{A}BC + B\bar{C} + AB\bar{C} + A\bar{B}C$

UNIT 03

LECTURE NO. 10

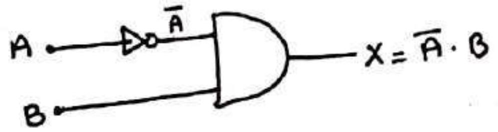
Logic Circuit Design

- Basic procedures are used to design a logic circuit, when the desired circuit requirements are given.
- Circuit requirements are given in the form of:
  1) Truth Table
  2) Word statement / Expression
- Logic Design Methods: Two general forms of Logic Expressions are used in the methods:
  1) SOP method
  2) POS method

Q. Design a logic circuit for the given truth table

A	B	X
0	0	0
0	1	1
1	0	0
1	1	0

Sol^n:



Q. Design a logic circuit for the given truth table

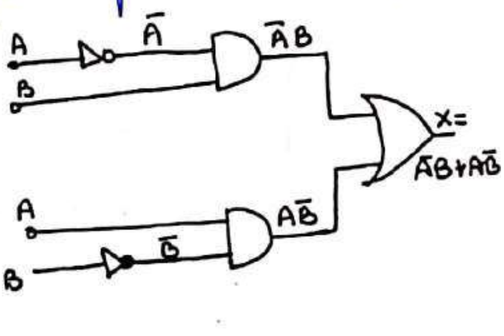
A	B	X
0	0	0
0	1	1
1	0	1
1	1	1

Sol^n: using SOP: w.k.t, in SOP, we represent the expressions using 1's.

- We convert the 1's in the output (x) to expression as shown below

$$X = \bar{A}B + A\bar{B}$$

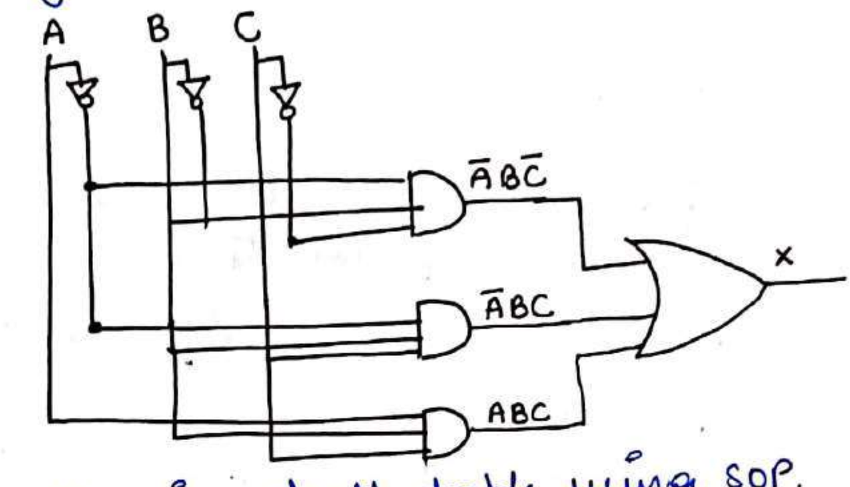
- now we construct the logic circuit



Q. Design the circuit for the given truth table

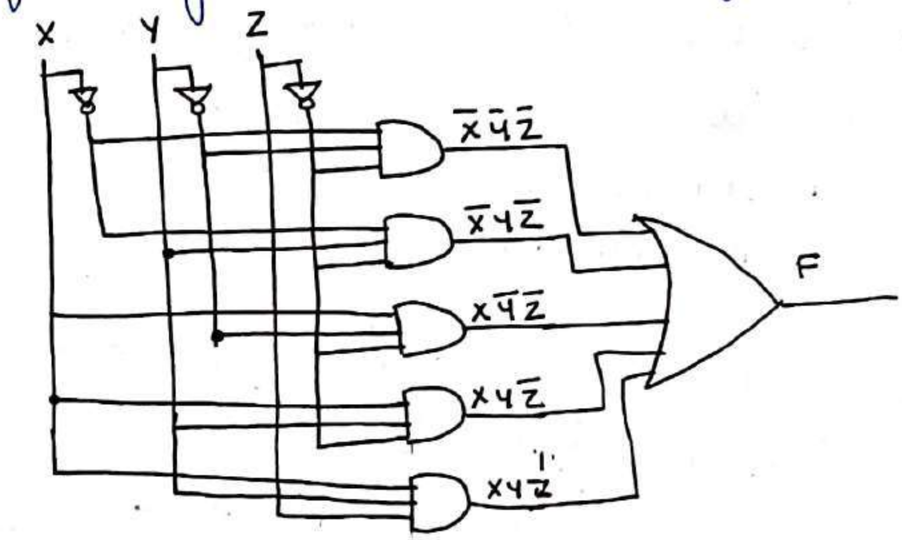
A	B	C	X
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

Solⁿ: using SOP, $X = \bar{A}B\bar{C} + \bar{A}BC + ABC$



Q. Design the circuit for the given truth table using SOP.

X	Y	Z	F
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1



using SOP

$F = \bar{X}\bar{Y}\bar{Z} + \bar{X}Y\bar{Z} + X\bar{Y}\bar{Z}$
$+ XY\bar{Z} + XYZ$

Q. $Y = ABC + B\bar{C}D + \bar{A}BC$

i) simplyfy this equation and realize using basic gates.

ii) Realize the simplified equation using only NOR gates.

Solⁿ: i) Simplification of expression

$Y = ABC + B\bar{C}D + \bar{A}BC$

$Y = ABC + \bar{A}BC + B\bar{C}D$

$Y = BC(A + \bar{A}) + B\bar{C}D$

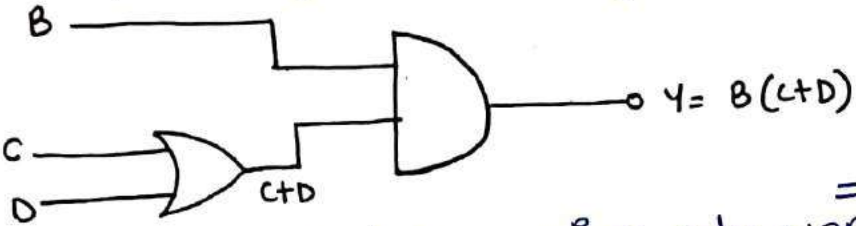
$Y = BC \cdot 1 + B\bar{C}D$ ($A + \bar{A} = 1$, ∵ complementarity law)

$Y = BC + B\bar{C}D$ ($BC \cdot 1 = 1$; properties of 0 & 1)

$Y = B(C+\bar{C}D)$

$\boxed{Y = B(C+D)}$ $(X+\bar{X}Y = X+Y$; Third Dist. Law)

i) Realization of simplified term using gates



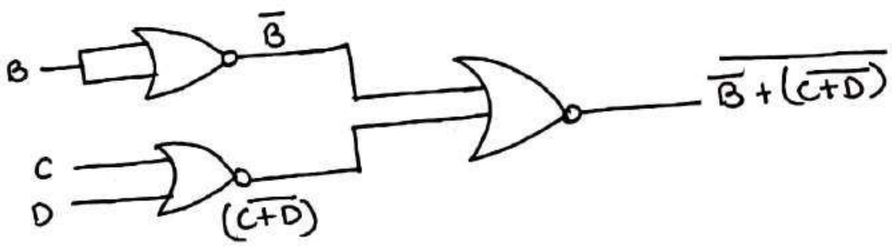
ii) Realization of simplified term using only NOR Gates

w.k.t $Y = B(C+D)$

taking double inversion of expression, we get

$Y = \overline{\overline{B(C+D)}}$

$Y = \overline{\bar{B} + \overline{(C+D)}}$ (DeMorgan's Law)



Laws of Algebra of Proposition [R1, R2]

1. Idempotent Law
   a) $p \vee p = p$
   b) $q \wedge q = q$

2. Commutative Law
   a) $p \vee q = q \vee p$
   b) $p \wedge q = p \vee q$

3. Associative Law
   a) $p \vee (q \vee r) = (p \vee q) \vee r$
   b) $p \wedge (q \wedge r) = (p \wedge q) \wedge r$

4. Distributive Law
   a) $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$
   b) $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$

5. Identity Law
   a) $p \vee T = T$
   b) $p \vee F = p$
   c) $p \wedge T = p$
   d $p \wedge F = F$

6. Complement Law
   a) $p \vee \neg p = T$
   b) $p \wedge \neg p = F$

7. Involution Law
   a) $\neg\neg p = p$

8. De Morgan's Law
   a) $\neg(p \vee q) = \neg p \wedge \neg q$
   b) $\neg(p \wedge q) = \neg p \vee \neg q$

9. Absorption Law
   a) $p \vee (p \wedge q) = p$
   b) $p \vee (p \vee q) = p$

10. Contrapositive Law
    a) $p \rightarrow q = \neg q \rightarrow \neg p$
    b) $p \Rightarrow q = \neg p \vee q$
    c) $(p \rightarrow q) \wedge (p \rightarrow \neg q) \rightarrow p$

11. $P \leftrightarrow Q = (P \wedge Q) \vee (\neg P \wedge \neg Q)$ and $P \leftrightarrow Q = (P \rightarrow Q) \wedge (Q \rightarrow P)$

Q] Use the laws to show

$\neg(p \vee q) \vee (\neg p \wedge q) = \neg p$

Solⁿ: LHS $\neg(p \vee q) \vee (\neg p \wedge q)$

$= (\neg p \wedge \neg q) \vee (\neg p \wedge q)$ (De Morgan's law)

(Distributive law)

$= \neg p \wedge (\neg q \vee q)$

$= \neg p \wedge T$ (Complement law)

$= \neg p$ (Identity law)

$=$ R.H.S

L.H.S = R.H.S , Hence Proved.

Q] Show that $\{[(p \vee q) \rightarrow r] \wedge (\neg p)\} \Rightarrow (q \rightarrow r)$ is a Tautology (i) without using Truth Table
(ii) using Truth Table

Q] Is the statement a Tautology? Use Laws.

$((p \rightarrow q) \wedge (q \rightarrow r)) \Rightarrow (p \rightarrow r)$

References:

1. Lipschutz, "Discrete Mathematics," McGraw Hill
2. B. Kolman, R.C. Busby and S.C. Ross, "Discrete Mathematical Structures", PHI

UNIT 04

LECTURE NO. 07

Literal [R1]

- In propositional logic, a literal is an atomic formula or its negation, which can't be further divided.
- Example: $p, q, \neg p, r$ etc.
- Literals are of two types:
  a) Positive literal : p
  b) Negative literal: $\neg r$
- $(p, \neg p)$ is called as the pair of literals.

Clause [R1]

- A clause is an expression formed from a finite collection of literals.
- Also called as Propositional Formula.

Elementary Product [R2]

- A product or conjunction of the variables and their negations in a formula is called an Elementary Product.
- Example: $p \wedge q \wedge \neg r$

Elementary Sum [R2]

- A sum or disjunction of the variables and their negations is called Elementary sum.
- Example: $p \vee \neg p \vee q \vee \neg r$

Normal Form [R2]

- By comparing Truth Table, one can determine whether two logical expression P and Q are equivalent but the process is very difficult when the number of variables increase.
- A better option is to transform the expression to the standard form also called as the normal form.
- Some basic Normal Forms are

1. Disjunctive Normal Form (DNF)

- A formula which is equivalent to a given formula and which consists of a sum of elementary products is called a DNF of the given formula.
- Example: $\underbrace{(p \wedge q)}_{\text{Elementary Product}} \underset{\text{Sum}}{\vee} \underbrace{(\neg p \wedge \neg q)}_{\text{Elementary Product}}$

Q] Convert the WFF to DNF

$(\neg p \vee \neg q) \Rightarrow (p \Leftrightarrow \neg q)$

$= \neg(\neg p \vee \neg q) \vee (p \Leftrightarrow \neg q)$ $\quad (p \to q = \neg p \vee q)$

$= \neg(\neg p \vee \neg q) \vee ((p \wedge \neg q) \vee (\neg p \wedge \neg(\neg q)))$ $\quad (p \Leftrightarrow q = (p \wedge q) \vee (\neg p \wedge \neg q))$

$= (\neg\neg p \wedge \neg\neg q) \vee ((p \wedge \neg q) \vee (\neg p \wedge q))$ $\quad$ (De Morgan's Law & Involution Law)

$= (p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge q)$

$=$ DNF

Q] Convert the WFF into DNF

$(P \Rightarrow (Q \wedge R)) \wedge (\neg P \Rightarrow (\neg Q \wedge \neg R))$

$= (\neg P \vee (Q \wedge R)) \wedge (\neg(\neg P) \vee (\neg Q \wedge \neg R))$ $\quad (P \to q = \neg P \vee q)$

$= (\neg P \vee (Q \wedge R)) \wedge (P \vee (\neg Q \wedge \neg R))$

$= [(\neg P \vee (Q \wedge R)) \wedge P] \vee [(\neg P \vee (Q \wedge R)) \wedge (\neg Q \wedge \neg R)]$ (Distrib Law)

$= [(\neg P \wedge P) \vee ((Q \wedge R) \wedge P)] \vee [(\neg P \wedge (\neg Q \wedge \neg R)) \vee$
$\quad ((Q \wedge R) \wedge (\neg Q \wedge \neg R))]$

$= (\neg P \wedge P) \vee ((Q \wedge R) \wedge P) \vee (\neg P \wedge (\neg Q \wedge \neg R)) \vee ((Q \wedge R) \wedge (\neg Q \wedge \neg R))$

= DNF

2. Conjuctive Normal Form (CNF)

- A formula which is equivalent to a given formula and which consists of a product of elementary sums is called CNF of the given formula.

- Example: $\underbrace{(P \vee q)}_{\text{Elementary Sum}} \underset{\text{product}}{\wedge} \underbrace{(q \vee r)}_{\text{Elementary Sum}} \underset{\text{product}}{\wedge} \underbrace{(P \vee S)}_{\text{Elementary Sum}}$

Q] Convert the WFF to CNF

$(\neg P \vee \neg Q) \Rightarrow (P \Leftrightarrow \neg Q)$

$= \neg(\neg P \vee \neg Q) \vee (P \Leftrightarrow \neg Q)$ $\quad (P \to q = \neg P \vee q)$

$= \neg(\neg P \vee \neg Q) \vee (P \to \neg Q) \wedge (\neg Q \to P)$ $\quad (P \leftrightarrow Q = (P \to Q) \wedge (Q \to P))$

$= \neg(\neg P \vee \neg Q) \vee (\neg P \vee \neg Q) \wedge (\neg\neg Q \vee P)$ $\quad (P \to Q = \neg P \vee Q)$

$= (\neg\neg P \wedge \neg\neg Q) \vee (\neg P \vee \neg Q) \wedge (Q \vee P)$ (DeMorgan's Law)

$= (P \wedge Q) \vee [(\neg P \vee \neg Q) \wedge (Q \quad P)]$ (Distributive Law)

$= P \vee [(\neg P \vee \neg Q) \wedge (Q \vee P)] \wedge q \vee [(\neg P \vee \neg Q) \wedge (Q \vee P)]$

$$= (p \vee (\neg p \vee \neg q)) \wedge (p \vee (q \vee p)) \wedge (q \vee (\neg p \vee \neg q)) \wedge (q \vee (q \vee p))$$

$=$ CNF

References:

1. Lipschutz, "Discrete Mathematics", McGraw Hill.
2. B. Kolman, R.C. Busby and S.C. Ross, "Discrete Mathematical Structures", PHI.

UNIT 04

LECTURE NO. 01

PROPOSITIONAL LOGIC

Statement [R1]

- A statement is a declarative sentence which is TRUE or FALSE, but not both.
- ie. a statement is a declarative sentence which has a definitive truth value.
- Truth value of a statement is TRUE or FALSE.
- Statement is termed as proposition if it has some truth value associated with it.
- EXAMPLES

SR.NO.	EXAMPLE	TRUTH VALUE	STATEMENT
1.	$\{x : x^2 = 36\} = \{-6, -6\}$	True	✓
2.	$3 > 9$	False	✓
3.	The capital of UP is Lucknow	True	✓
4.	Blood is Red	True	✓
5.	$5 + 4 = 10$	False	✓
6.	How are You?	Interrogative	×
7.	Please go from here	Request	×
8.	May God help you	Wish	×

Statement Letters [R1]

- We know that symbols have great importance in Mathematics and therefore symbols can be used to represent statements.
- These symbols are called statement letters or sentence variables.
- To represent statements usually letters are used P, Q, R ... p, q, r ...
- EXAMPLE

If statement 'Lucknow is the capital of UP' is denoted by letter 'p', then in mathematics it is written as follows:

$\boxed{\text{p: Lucknow is the capital of UP}}$

Logical Connectives or Sentence Connectives [R1, R2]

- logical connectives or sentence connectives are the words or symbols used to combine two statements to form a compound statement.

Connective Word	Name of Connective Symbol	Connective Symbol	Rank
NOT	Denial or Negation	$\sim$ or $\neg$	1
AND	Conjunction	$\wedge$	2
OR	Disjunction	$\vee$	3
IF... THEN	Condition	$\rightarrow$ or $\Rightarrow$	4
IF AND ONLY IF (IFF)	Bi-Conditional	$\leftrightarrow$ or $\Leftrightarrow$	5

increasing order

- EXAMPLE

1. π is greater than 3 and π is less than 3.2

Solⁿ: p = π is greater than 3
q = π is less than 3.2

$\therefore \boxed{p \wedge q}$

2. a is equal to 4 or b is equal to 4

Solⁿ: p = a is equal to 4
q = b is equal to 4

$\therefore \boxed{p \vee q}$

3. If two lines are parallel, then they do not intersect.

Solⁿ: p = Two lines are parallel
q = Two lines do not intersect

$\therefore \boxed{p \Rightarrow q}$

4. A is right angled triangle if the sum of squares of its two sides is equal to the square of the third side.

Solⁿ: p = A is right angled triangle
q = square of two sides of a triangle is equal to the square of the third side

$\therefore \boxed{p \Leftrightarrow q}$

5. It is cold. Find the negation of this statement.

Solⁿ: p = It is cold.
$\sim p$ = It is not cold.

Use of Brackets [R1, R2]

- The use of brackets in statement or proposition is very important.
- The meaning of statement is included in brackets.
- Ex: $(p \wedge q) \Rightarrow r$ & $p \wedge (q \Rightarrow r)$ are different.
- Therefore, following rules are followed for brackets in statement.

RULE 1: If connective 'NOT ($\sim$)' is repeated, then bracket is not required

i.e $\sim\sim p$ is same as $\sim(\sim p)$

RULE 2: If in a statement, the connectives of the same rank appears, then brackets are applied from the left.

ie. $p \wedge q \wedge r \wedge s \wedge t = \{(p \wedge q) \wedge r\} \wedge t$

RULE 3: If the connective of different rank appears, then first of all the brackets of that connective is removed which is of lower rank.

ie. $[(p \vee q) \Rightarrow r]$

Types of Sentences [R1, R2]

1. SIMPLE SENTENCE

- A simple sentence has no connectives.
- Also called as Atomic Sentence.

2. COMPOUND SENTENCE

- A compound sentence is composed of various connectives.
- Also called as Molecular Sentence.

Connective	Compound Sentence
$\wedge$	Conjunction Sentence
$\vee$	Disconjunction Sentence
$\rightarrow$ or $\Rightarrow$	Conditional Sentence
$\leftrightarrow$ or $\Leftrightarrow$	Biconditional Sentence
$\sim$ or $\neg$	Negative Sentence

Open statement
- A sentence, which contains one or more variables such that when certain value are substituted for variables becomes a statement is called an Open Stmt.

ex: $x+3=9$.

Proposition
- If p, q, r are simple statement then the compound statement P is called a Proposition

ex: $\sim p \wedge q$.
- The Truth Table is a simple way to show this relationship.

*** NOTE 1:**

In a conditional sentence $p \Rightarrow q$

p is called	q is called
• antecedent	• consequent
• hypothesis	• conclusion
• premise	

*** NOTE 2:**

- The sentences used to form a compound sentence are called its Components.
- Components of $p \wedge q$ are p, q

\# Principal Connective: The logical connective, which is used in the end of a Compound Sentence, is called a Principal Connective.

ex: $(p \wedge q) \Rightarrow r$; PC : $\Rightarrow$

$(r \Rightarrow p) \vee (p \Leftrightarrow q)$; PC : $\vee$

Well Formed Formula [R2]

- A statement is called WFF if

a) A statement variable p standing alone is WFF.

b) If p is WFF, then $(\sim p)$ is a WFF.

c) If p and q are WFFs, then $(p \wedge q)$, $(p \vee q)$, $(p \Rightarrow q)$, $(p \Leftrightarrow q)$ are WFF.

d) A string of symbols is a WFF iff it is obtained by finitely many applications of rule (a),(b) & (c).

Q] Which of the following sentences are statements? Also state their truth value.

i) Is 3 a prime number?

ii) $x^2 - 5x + 6 = 0$

iii) There will be snow in December.

iv) Give me ten rupees.

v) Ramesh is poor but honest.

Sol^n: i) It is not a statement (Interrogative)

ii) It is not a statement. It's truth value depends upon the value of x, and we donot know what is x

iii) It is a statement because it has a truth value.

iv) It is not a statement (wish)

v) It is a statement because it can have a truth value.

Q] Which of the following sentences are proposition? What are the truth values of those that are propositions?

i) Kolkata is the capital of India.

ii) Answer this question.

iii) What time is it?

iv) $x+y = y+x$ for every pair of real number x & y

v) $5+6=10$

vi) $x+3=3$

vii) $x+2=5$ if $x=1$

viii) Do not go

Sol^n: i) It is a statement (Truth Value = False)

ii) Not a statement (Interrogation)

iii) Not a statement (Interrogation)

iv) It is a statement (Truth Value = True)

v) It is a statement (Truth Value = False)

vi) Not a statement (Value depends on x, x is unknown)

vii) It is a statement (Truth Value = False)

viii) Not a statement (Wish)

9] Find out which of the following are statements and which are not.

i) Where are you going?

ii) Gitanjali is sick or old.

iii) It is raining and the sun is shinning.

iv) Intersection of two non-empty sets is always a non empty set.

v) Two individuals are always related

vi) The real number x is less than 3

vii) Do not pluck the flowers.

viii) $5x+8y=17$

Sol^n: i) Not a statement (Interrogation)

ii) It is a statement (Truth Value can be judged)

iii) It is a statement (Truth Value can be judged)

iv) It is a statement (Truth Value can be judged)

v) It is a statement (Truth Value can be judged)

vi) Not a statement (Open Sentence, value depends on x)

vii) Not a statement (Order)

viii) Not a statement (Open Sentence, value depends on x & y)

Q] If p = he is poor, q = he is laborious, then write down the following statements in symbols.

i) He is poor and laborious

ii) He is poor but is not laborious

iii) It is false that he is poor or laborious.

iv) It is false that he is not poor or laborious.

v) Neither he is poor nor he is laborious.

vi) He is poor or is not poor and is laborious.

vii) It is not true that he is not poor or is not laborious.

Sol^n: i) $p \wedge q$ (ii) $p \wedge \sim q$ (iii) $\sim(p \vee q)$

iv) $\sim(\sim p \vee q)$ (v) $\sim p \wedge \sim q$ (vi) $p \vee (\sim p \wedge q)$

(vii) $\sim(\sim p \vee \sim q)$

Q] Let p = Ravi is Rich and q = Ram is happy.
Write the following statements in symbolic form:

i) Ram is poor but happy

ii) Ravi is neither rich nor happy

Sol^n: Here, p = Ravi is Rich

$\sim p$ = Ravi is not Rich

q = Ram is happy

$\sim q$ = Ram is not happy

Let r = Ravi is happy

$\sim r$ = Ravi is not happy

s = Ram is Rich

$\sim s$ = Ram is not Rich/Ram is Poor

i) $\sim s \wedge q$ (ii) $\sim p \wedge \sim r$

Q] Write the following sentences in symbol

i) When sheela will come then I shall go to college.

ii) Until Sheela will not come I shall not go to college.

Solⁿ: Let p = Sheela will come

q = I shall go to college.

i) $p \Rightarrow q$ (ii) $\sim p \Rightarrow \sim q$

Q] If p: It is 4 o'clock, q: The train is late, then state in words the following results.

i) $p \vee q$ (ii) $p \wedge q$ (iii) $p \wedge (\sim q)$

iv) $q \vee \sim p$ (v) $(\sim p) \wedge q$ (vi) $(\sim p) \wedge (\sim q)$

(vii) $(\sim p) \vee (\sim q)$ (viii) $\sim (p \wedge q)$ (ix) $\sim p \Rightarrow q$

Solⁿ: i) It is 4 o'clock, or the train is late.

ii) It is 4 o'clock, and the train is late.

iii) It is 4 o'clock, and the train is not late / It is 4 o'clock but the train is not late.

iv) The train is late or it is not 4 o'clock.

v) It is not 4 o'clock, and the train is late.

vi) It is not 4 o'clock, and the train is not late / Neither it is 4 o'clock, nor the train is late.

vii) It is not 4 o'clock, or the train is not late / Either it is not 4 o'clock, or the train is not late.

viii) It is not true that it is 4 o'clock and the train is late.

ix) If it is not 4 o'clock, then the train is late.

9] Let p = It is cold, q = It is raining. Give a simple verbal sentence which describes each of the following statements

i) $\sim p$ (ii) $p \wedge q$ (iii) $p \vee q$

iv) $q \Leftrightarrow p$ (v) $p \Rightarrow \sim q$ (vi) $q \vee \sim p$

vii) $\sim p \wedge \sim q$ (viii) $p \Leftrightarrow \sim q$ (ix) $\sim \sim q$

(x) $(p \wedge \sim q) \Rightarrow p$ (xi) $\sim \sim p$ (xii) $(q \wedge \sim p) \Rightarrow q$

Solⁿ: i) It is not cold.

ii) It is cold and raining.

iii) It is cold or it is raining.

iv) It is raining if and only if it is cold.

v) If it is cold, then it is not raining.

vi) It is raining or it is not cold.

vii) It is neither cold, nor it is raining.

viii) It is cold if and only if it is not raining.

ix) It is raining

x) If it is cold and not raining, then it is cold.

xi) It is cold.

xii) If it is raining and not cold, then it is raining.

References:

1. Lipschutz, "Discrete Mathematics," McGraw Hill.
2. B. Kolman, R.C. Busby and S.C. Ross", Discrete Mathematical Structures", PHI

UNIT 04

LECTURE NO 02

Truth Tables of Basic Logical Operations [R1, R2]

1. CONJUNCTION

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

2. DISJUNCTION

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

3. NEGATION

p	$\sim p$
T	F
F	T

4. CONDITIONAL

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

5. BI- CONDITIONAL

p	q	$p \Leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Q] Find the negation of the propositions

i) It is cold

ii) Today is Sunday

iii) Tim is poor.

Soln:

i) It is not cold.

ii) Today is not Sunday

iii) Tim is not poor.

Q] Write the negation of each of the following

i) $2+7 \leq 13$

ii) 3 is an odd integer and 8 is an even integer

iii) Nice people are dangerous.

iv) The weather is bad and I will not go to work.

v) I grow fat only if I eat too much.

Solⁿ: i) $2+3$ is not less than or equal to 13.

ii) 3 is not an odd integer and 8 is not an even integer.

iii) Nice people are not dangerous.

iv) The weather is not bad and I will go to work

v) I do not grow if I do not eat too much

Types of Conditional Statements [R1, R2]

SR.NO.	CONDITIONAL	NAME OF TYPE
1.	$p \Rightarrow q$	Direct Implication
2.	$q \Rightarrow p$	Converse Implication
3.	$\sim p \Rightarrow \sim q$	Inverse/Opposite Implication
4.	$\sim q \Rightarrow \sim p$	Contrapositive Implication

Tautology [R1, R2]

- A tautology is a proposition which is true for all truth values of its sub propositions or components.
- A tautology is also called Logically Valid or Logically True.

Scanned by CamScanner

Q] Show that the truth values of the following formula are Tautology.

i) $(p \wedge (p \to q)) \to q$

ii) $(p \to q) \Leftrightarrow (\sim p \vee q)$

iii) $((p \to q) \wedge (q \to r)) \to (p \to r)$

Solⁿ: i) $(p \wedge (p \to q)) \to q$

p	q	$p \to q$	$A = p \wedge (p \to q)$	$A \to q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

⇒ All True ∴ Tautology.

ii) $(p \to q) \Leftrightarrow (\sim p \vee q)$

p	q	$p \to q$	$\sim p$	$\sim p \vee q$	$(p \to q) \Leftrightarrow (\sim p \vee q)$
T	T	T	F	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

⇒ All True ∴ Tautology

iii) $((p \to q) \wedge (q \to r)) \to (p \to r)$

p	q	r	$(p \to q)$	$(q \to r)$	$(p \to r)$	$((p \to q) \wedge (q \to r)) = A$	$A \to (p \to r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	T	F	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

All Tru

Contradiction [R1, R2]

- A contradiction is a proposition which is false for all truth values of of its sub propositions or components.
- A contradiction is also called Logically Invalid or Logically False.

Q] Prove that $(p \vee q) \wedge (\sim p) \wedge (\sim q)$ is a contradiction.

Solⁿ:

p	q	$(p \vee q)$	$\sim p$	$\sim q$	$(p \vee q) \wedge \sim p$	$(p \vee q) \wedge (\sim p) \wedge (\sim q)$
T	T	T	F	F	F	F
T	F	T	F	T	F	F
F	T	T	T	F	T	F
F	F	F	T	T	F	F

All False
∴ Contradiction

Q] Prove that $P = (p \vee q) \wedge (p \vee \sim q) \wedge (\sim p \vee q) \wedge (\sim p \vee \sim q)$ is a contradiction.

Solⁿ:

p	q	$\sim p$	$\sim q$	$R = (p \vee q)$	$S = (p \vee \sim q)$	$U = (\sim p \vee q)$	$V = (\sim p \vee \sim q)$	$P = R \wedge S \wedge U \wedge V$
T	T	F	F	T	T	T	F	F
T	F	F	T	T	T	F	T	F
F	T	T	F	T	F	T	T	F
F	F	T	T	F	T	T	T	F

All False
∴ Contradiction

References:

1. Lipschutz, "Discrete Mathematics", McGrawHill.
2. B. Kolman, R.C. Busby and S.C. Ross, "Discrete Mathematical Structures", PHI

UNIT 04

LECTURE NO. 03

Q] Consider the conditional statement p. If the floods destroy my house or fire destroys my house, then my insurance company will pay me. Write converse, inverse and contrapositive of statement.

Solⁿ: Let the atomic statements be:

p: The floods destroy my house
q: The fire destroys my house
r: My insurance company will pay me

i) Converse: $r \rightarrow (p \vee q)$

"If my insurance company will pay me, then the floods will destroy my house or fire will destroy my house".

ii) Inverse: $\sim(p \vee q) \rightarrow \sim r$

"If the floods will not destroy my house or the fire will not destroy my house; then my insurance company will not pay me."

iii) Contrapositive: $\sim r \rightarrow \sim(p \vee q)$

"If my insurance company will not pay me, then the floods will not destroy house or the fire will not destroy my house".

Q] Find the inverse and contrapositive of the given statement: "If I come early, then I can get car."

Solⁿ: Let
p: I come early.
q: I can get car.

i) Inverse : $\sim p \Rightarrow \sim q$

"If I cannot come early, then I can not get car"

ii) Contrapositive : $\sim q \Rightarrow \sim p$

"If I cannot get car, then I shall not come early."

Q] The inverse of statement is given. Write the converse and contrapositive of the statement.

'If a man is not fisherman, then he is not swimmer"

Solⁿ: Inverse of statement is given ie. $\sim p \Rightarrow \sim q$ is given

ie $\sim p$ = If a man is not fisherman

$\sim q$ = He is not swimmer

$\therefore$ p = If a man is a fisherman

q = He is a swimmer

i) Converse : $q \Rightarrow p$

"If he is swimmer, then the man is a fisherman"

ii) Contrapositive : $\sim q \Rightarrow \sim p$

"If he is not a swimmer, then the man is not a fisherman".

Q] The contrapositive of statement is given

"If $x<2$ then $x+4<6$ "

Write the converse and inverse.

Solⁿ: Contrapositive of statement is given. ie $\sim q \Rightarrow \sim p$ is given

i.e $\sim q = x<2$

$\sim p = x+4<6$

$\therefore$ p = $x+4$ is not less than 6

q = x is not less than 2.

Scanned by CamScanner

ii) Inverse : $\sim p \Rightarrow \sim q$

"If $x+4<6$ then $x<2$."

i) Converse: $q \Rightarrow p$

"If x is not less than 2 then, $x+4$ is not less than 6".

Q] Given that the value of $p \to q$ is false, determine the value of $(\sim p \vee \sim q) \to q$.

Solⁿ: We shall construct the truth table for $p \to q$ & $(\sim p \vee \sim q) \to q$

p	q	$\sim p$	$\sim q$	$p \to q$	$\sim p \vee \sim q$	$(\sim p \vee \sim q) \to q$
T	T	F	F	T	F	T
T	F	F	T	F	T	F
F	T	T	F	T	T	T
F	F	T	T	T	T	F

From the table, we observe that for $(p \to q)$ to be false, the corresponding value of $(\sim p \vee \sim q) \to q$ is False.

Logical Equivalence [R1]

- Two statements or propositions are called logically Equivalent if the truth values of both the statements or propositions are always identical.

- i.e. two statements are called logically equivalent if when either is true the other is true and when either is false the other is false.

- If two statements P and Q are logically equivalent then these are represented by $P \equiv Q$.

- If $P \equiv Q$, then $P \Leftrightarrow Q$ is a tautology.

* **NOTE:**

The necessary and sufficient condition for two statements P and Q to be logically equivalent is that $P \Leftrightarrow Q$ is a tautology.

Q] If p and q are two statements, show that the implication $p \Rightarrow q$ and its contra positive $\sim q \Rightarrow \sim p$ are logically equivalent.

Solⁿ:

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

$p \Rightarrow q$ and $\sim q \Rightarrow \sim p$ are identical hence logically equivalent.

Q] Show that $\sim(p \Rightarrow q) \equiv \{p \wedge (\sim q)\}$ are logically equivalent.

Solⁿ: If $\sim(p \Rightarrow q) \equiv \{p \wedge (\sim q)\}$, then $\sim(p \Rightarrow q) \Leftrightarrow \{p \wedge (\sim q)\}$ is a tautology.

p	q	$\sim q$	$(p \Rightarrow q)$	$\sim(p \Rightarrow q)$	$p \wedge \sim q$	$\sim(p \Rightarrow q) \Leftrightarrow \{p \wedge (\sim q)\}$
T	T	F	T	F	F	T
T	F	T	F	T	T	T
F	T	F	T	F	F	T
F	F	T	T	F	F	T

All True ∴ Tautology

since $\sim(p \Rightarrow q) \Leftrightarrow \{p \wedge (\sim q)\}$ is a Tautology

$$\therefore \sim(p \Rightarrow q) \equiv \{p \wedge (\sim q)\}$$

References:
1. Lipschutz, "Discrete Mathematics," McGraw Hill

UNIT 04

LECTURE NO. 04

Argument [R1]

- In logical mathematics, we require the process of reasoning.
- Given a certain set of propositions, we are required to derive other propositions by logical reasoning.
- The given set of propositions is called Premises or Hypothesis and the propositions derived from this set is called Conclusion.
- An argument is a process which yields a conclusion (i.e. another proposition) from a given set of propositions, called premises.
- Let premises be $p_1, p_2, \cdots, p_n$ and let argument yield the conclusion q, then such an argument is denoted by

$$\boxed{p_1, p_2, \cdots, p_n \vdash q}$$

or

$$\boxed{\begin{array}{c} p_1 \\ p_2 \\ \vdots \\ p_n \\ \hline q \end{array}}$$

Valid Argument [R1]

- An argument $p_1, p_2, \ldots, p_n \vdash q$ is called Valid if q is true whenever all its premises $p_1, p_2, \ldots, p_n$ are true.
- An argument is valid iff the premises implies the conclusion.
- Thus, the argument $p_1, p_2, \ldots, p_n \vdash q$ is said to be valid iff the statement $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$ is Tautology.

Falacy Argument [R1]

- An argument which is not valid is said to be a fallacy or an Invalid Argument.

Representation of an Argument [R1]

- An argument $p_1, p_2, \ldots, p_n \vdash q$ is written as

$$\begin{array}{l} \left.\begin{array}{c} p_1 \\ p_2 \\ \vdots \\ p_n \end{array}\right\} \text{premises} \\ \hline q \text{ (Conclusion)} \end{array}$$

- Premises are listed above the horizontal line and the conclusion below the horizontal line.

Q] Show that the following argument is valid:

$$\begin{array}{c} p \vee q \\ \sim p \\ \hline q \end{array}$$

Soln: Here the two premises are $p \vee q$ and $\sim p$, and the conclusion is q.

The given argument will be Valid if $[(p \vee q) \wedge \sim p] \Rightarrow q$ is a Tautology.

p	q	$\sim p$	$p \vee q$	$(p \vee q) \wedge \sim p$	$[(p \vee q) \wedge \sim p] \Rightarrow q$
T	T	F	T	F	T
T	F	F	T	F	T
F	T	T	T	T	T
F	F	T	F	F	T

All True $\therefore$ Tautology

Since $[(p \vee q) \wedge \sim p] \Rightarrow q$ is a Tautology

$\therefore$ The argument is valid.

Law of Syllogism (or Transitive Rule)

$$\left.\begin{array}{l} p \rightarrow q \\ q \rightarrow r \end{array}\right\} \text{Premises}$$

$$p \Rightarrow r \quad \text{Conclusion}$$

Rule of Detachment (Modus Ponens)

$$\left.\begin{array}{l} p \\ p \Rightarrow q \end{array}\right\} \text{Premises}$$

$$q \quad \text{Conclusion}$$

* NOTE:

The validity of a given argument can be checked by the help of a Truth Table and also without it.

8] Show that the argument $p, p \to q, q \to r \vdash r$ is valid by both the methods.

Solⁿ: METHOD 1: WITHOUT USING TRUTH TABLE

p (Premise)

$p \to q$ (Premise)

---

q (Conclusion by Rule of Detachment)

$q \to r$ (Premise)

---

r (Conclusion by Rule of Detachment)

Hence the given argument is Valid.

METHOD 2: USING TRUTH TABLE

The given argument will be valid iff $[p \wedge (p \to q) \wedge (q \to r)] \to$ is a Tautology.

p	q	r	$p \to q$	$q \to r$	$p \wedge (p \to q)$	$p \wedge (p \to q) \wedge (q \to r) = A$	$A \to r$
T	T	T	T	T	T	T	T
T	T	F	T	F	T	F	T
T	F	T	F	T	F	F	T
T	F	F	F	T	F	F	T
F	T	T	T	T	F	F	T
F	T	F	T	F	F	F	T
F	F	T	T	T	F	F	T
F	F	F	T	T	F	F	T

All Tr… ∴ Tautology

Since $[p \wedge (p \to q) \wedge (q \to r)] \to r$ is a Tautology

∴ argument is Valid.

Scanned by CamScanner

Q] Test the validity of the argument $p, p \to q \vdash q$ by using Truth Table only.

Solⁿ: The given argument will be valid iff $[p \wedge (p \to q)] \to q$ is a Tautology.

p	q	$p \to q$	$p \wedge (p \to q)$	$[p \wedge (p \to q)] \to q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

All True ∴ Tautology

Since $[p \wedge (p \to q)] \to q$ is a Tautology

∴ argument is valid.

Q] Test the validity of the following argument

If a man is a bachelor, he is worried (premise)

If a man is worried, he dies young (premise)

Bachelors die young (Conclusion)

Solⁿ: Let p: A man (he) is a bachelor

q: He is worried

r: He dies young

Writting the given argument in symbolic form:

$p \to q$ (premise)

$q \to r$ (premise)

$p \to r$ (Conclusion)

METHOD 1: WITHOUT USING TRUTH TABLE

$$\begin{array}{ll} p \to q & \text{(premise)} \\ \underline{q \to r} & \text{(premise)} \\ p \to r & \text{(conclusion)} \end{array}$$

The given argument is Valid by Law of Syllogism.

METHOD 2: USING TRUTH TABLE

The given argument will be Valid iff $[(p \to q) \wedge (q \to r)] \to (p \to r)$ is a Tautology.

p	q	r	$p \to q$	$q \to r$	$(p\to q)\wedge(q\to r) = A$	$(p \to r)$	$A \to (p \to r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

All True

Since $[(p \to q) \wedge (q \to r)] \to (p \to r)$ is a Tautology

$\therefore$ argument is Valid.

8] Test the validity of the following arguments "If I study, then I will not fail in Mathematics. If I do not play basketball, then I will study. I failed in Mathematics. Therefore, I must play basketball."

Solⁿ: Let p: I study

q: I will not fail in Mathematics

r: I do not play basketball

Scanned by CamScanner

writing the given argument in symbolic form:

$$\begin{array}{l} p \to q \\ r \to p \\ \underline{\sim q} \\ \sim r \end{array}$$

<u>Using truth table</u>

The given argument will be valid iff $[(p\to q)\wedge(r\to p)\wedge \sim q] \Rightarrow \sim r$ is a Tautology

p	q	r	$\sim q$	$\sim r$	$(p\to q)$	$(r\to p)$	A = $(p\to q)\wedge(r\to p)$	A $\wedge \sim q$	A $\Rightarrow \sim r$
T	T	T	F	F	T	T	T	F	T
T	T	F	F	T	T	F	F	F	T
T	F	T	T	F	F	T	F	F	T
T	F	F	T	T	F	T	F	F	T
F	T	T	F	F	T	F	F	F	T
F	T	F	F	T	T	T	T	F	T
F	F	T	T	F	T	F	F	F	T
F	F	F	T	T	T	T	T	T	T

All True

$\therefore$ Tautolo

since $[(p\to q)\wedge(r\to p)\wedge\sim q] \to \sim r$ is a Tautology

$\therefore$ argument is valid.

Q] Test the validity of the following statements: "If it rains then it will be cold. If it is cold then I shall stay at home. Since it rains therefore I shall stay at home"

sol^n: let;
p: It rains
q: It will be cold
r: I shall stay at home

Scanned by CamScanner

The given argument in symbollic form can be written as:

$$\begin{array}{c} p \rightarrow q \\ q \rightarrow r \\ p \\ \hline r \end{array}$$

<u>Using Truth Table</u>

The given argument is valid iff $[(p \rightarrow q) \wedge (q \rightarrow r) \wedge p] \rightarrow r$ is a Tautology.

p	q	r	$p \rightarrow q$	$q \rightarrow r$	A = $(p \rightarrow q) \wedge (q \rightarrow r)$	B = $A \wedge p$	$B \rightarrow r$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	F	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	F	T
F	T	F	T	F	F	F	T
F	F	T	T	T	T	F	T
F	F	F	T	T	T	F	T

All True ∴ Tautology

since $[(p \rightarrow q) \wedge (q \rightarrow r) \wedge p] \rightarrow r$ is a Tautology
∴ it is valid argument.

9] Test the validity of the argument: If 8 is even then 2 does not divide 9. Either 7 is not prime or 2 divides 9. But 7 is prime, therefore, 8 is odd.

<u>Soln</u>:
Let p: 8 is even
q: 2 divides 9
r: 7 is prime

The given argument in symbolic form can be written as:

$$\begin{array}{c} p \rightarrow \sim q \\ \sim r \vee q \\ r \\ \hline \sim p \end{array}$$

Using Truth Table

The given argument is valid iff $[\{(p \to \sim q) \wedge (\sim r \vee q) \wedge r\} \to \sim p]$ is a Tautology.

p	q	r	$\sim p$	$\sim q$	$\sim r$	$A = (p \to \sim q)$	$B = (\sim r \vee q)$	$C = A \wedge B$	$D = C \wedge r$	$D \to r$
T	T	T	F	F	F	F	T	F	F	T
T	T	F	F	F	T	F	T	F	F	T
T	F	T	F	T	F	T	F	F	F	T
T	F	F	F	T	T	T	T	T	F	T
F	T	T	T	F	F	T	T	T	T	T
F	T	F	T	F	T	T	T	T	F	T
F	F	T	T	T	F	T	F	F	F	T
F	F	F	T	T	T	T	T	T	F	T

since $[(p \to \sim q) \wedge (\sim r \vee q) \wedge r] \to \sim p$ is a Tautology

$\therefore$ it is a valid argument

Q. Test the validity of the statement

If two sides of the triangle are equal, then the opposide angles are equal.

Two sides of a triangle are not equal

$\therefore$ The opposite angles are not equal

Sol^n: let p: Two sides of a triangle are equal.

q: The opposite angles of a triangle are equal

The given argument in symbolic form can be written as

$$\left.\begin{array}{c} p \to q \\ \sim p \end{array}\right\} \text{premise}$$

$\sim q$ conclusion

Using Truth Table

The given argument is valid iff $[(p \Rightarrow q) \wedge \sim p] \Rightarrow \sim q$ is a Tautology.

p	q	$p \Rightarrow q$	$\sim p$	$\sim q$	$(p \Rightarrow q) \wedge \sim p$	$[(p \Rightarrow q) \wedge \sim p] \Rightarrow \sim q$
T	T	T	F	F	F	T
T	F	F	F	T	F	T
F	T	T	T	F	T	F
F	F	T	T	T	T	T

since $[(p \Rightarrow q) \wedge \sim p] \Rightarrow \sim q$ is not a Tautology, hence it is not a Valid argument.

Q. State whether the argument given below is valid. (without using Truth Table)

If I drive to work then I will arrive tired.

I drive to work

$\therefore$ I will arrive tired.

sol^n: let p: I drive to work

q: I will arrive tired

The give argument in symbolic form can be written as

$$\left.\begin{array}{l} p \rightarrow q \\ p \end{array}\right\} \text{premise}$$
$$\overline{\quad q \quad} \text{ conclusion}$$

after rearangement, we get

$$\left.\begin{array}{l} p \\ p \rightarrow q \end{array}\right\} P$$
$$\overline{\quad q \quad} \} C$$

apply law of Detachment, we get q.

Hence it is a valid argument

Q. State whether the argument given below is valid or not valid.

I will become famous or I will be writer

I will not be a writer

∴ I will become famous.

sol^n: let p: I will become famous
q: I will be writer

The given argument in symbolic form can be written as

$$\left.\begin{array}{c} p \vee q \\ \sim q \end{array}\right\} \text{premise}$$

$$\overline{\quad p \quad} \quad \text{conclusion}$$

The given argument is valid iff $[(p \vee q) \wedge \sim q] \to p$ is a Tautology

p	q	$\sim q$	$p \vee q$	$(p \vee q) \wedge \sim q$	$[(p \wedge q) \wedge (\sim q)] \to p$
T	T	F	T	F	T
T	F	T	T	T	T
F	T	F	T	F	T
F	F	T	F	F	T

since $[(p \wedge q) \wedge (\sim q)] \to p$ is a Tautology ∴ It is a valid argument.

UNIT 04

LECTURE NO. 05

Rules of Inference for Propositional Calculus [R1]

RULE OF INFERENCE	TAUTOLOGICAL FORM	NAME
p / $\therefore p \vee q$	$p \Rightarrow (p \vee q)$	Addition
$p \wedge q$ / $\therefore p$	$(p \wedge q) \Rightarrow p$	Simplification
p, q / $\therefore p \wedge q$	$((p) \wedge (q)) \Rightarrow (p \wedge q)$	Conjunction
$p \Rightarrow q$, p / $\therefore q$	$[(p \Rightarrow q) \wedge p] \Rightarrow q$	Modus Ponen
$p \Rightarrow q$, $\sim q$ / $\therefore \sim p$	$[(p \Rightarrow q) \wedge \sim q] \Rightarrow \sim p$	Modus Tollen
$p \Rightarrow q$, $q \Rightarrow r$ / $\therefore p \Rightarrow q$	$[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$	Hypothetical Syllogism
$p \vee q$, $\sim p$ / $\therefore q$	$[(p \vee q) \wedge \sim p] \Rightarrow q$	Disjunction Syllogism

Q] Prove the validity of the following argument
"If I get the job and work hard, then I will get promoted. If I get promoted, then I will be happy. I will not be happy. Therefore either I will not get the job or I will not work hard".

Solⁿ: Let p : I get the job
q : I work hard
r : I get promoted
s : I will be happy

Given argument can be written in symbolic form

$$(p \wedge q) \Rightarrow r$$
$$r \Rightarrow s$$
$$\sim s$$

now
$$\begin{array}{l} (p \wedge q) \Rightarrow r \\ r \Rightarrow s \\ \hline (p \wedge q) \Rightarrow s \end{array}$$
(By Hypothetical Syllogism)

now
$$\begin{array}{l} (p \wedge q) \Rightarrow s \\ \sim s \\ \hline \sim(p \wedge q) \end{array}$$
(By Modus Tollens)

$$\sim(p \wedge q) = \sim p \vee \sim q$$

i.e. either I will not get the job or I will not work hard.

Hence the argument is Valid.

References:
1. Lipschutz, "Discrete Mathematics", McGraw Hill

UNIT 04

LECTURE NO. 06

Law of Duality [R1]

- Here, we consider only those statements which contain the connectives $\wedge$, $\vee$ and $\sim$ only.
- Two statements p & q are said to be dual of each other if either one can be obtained from the other by replacing $\wedge$ by $\vee$, $\wedge$ by $\vee$, T by F and F by T.

Principle of Duality [R1]

- It states that if any two statements are equal then their dual are also equal.

Q Find the dual of the following

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

Sol^n: $(p\wedge q)\vee r$

(b) $(p\wedge q)\vee T$

Sol^n: $(p\vee q)\wedge F$

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

Sol^n: $(p\vee q)\vee(p\wedge\sim(p\vee s))$

(d) $(p\wedge T)\wedge(F\vee p')=F$

Sol^n: $(p\vee F)\ (T\wedge p')=T$

(e) $(p\vee q)\wedge r = p\wedge q'$

Sol^n: $(p\wedge q)\vee r = p\vee q'$

(f) $p\vee(q\wedge r)=(p\vee q)\wedge(p\vee r)$

Sol^n: $p\wedge(q\vee r)=(p\wedge q)\vee(p\wedge r)$

Types of Propositions [R2]

1. SATISFIABLE PROPOSITION

- A proposition is satisfiable if its Truth table contains True atleast once.
- Example: $p \wedge q$

2. TAUTOLOGY

- A proposition is a Tautology if its truth table contains all True.
- Example: $p \vee \neg p$

3. CONTRADICTION

- A proposition is a Contradiction if its Truth table contains all False.
- Example: $p \wedge \neg p$

4. CONTINGENCY

- A proposition is Contigency if it is neither a Tautology nor a Contradiction.
- Example: p

Q]. Check whether $[p \rightarrow (q \rightarrow r)] \rightarrow [(p \rightarrow q) \rightarrow (p \rightarrow r)]$ is a Tautology or Contradiction or Contingency.

UNIT 04

LECTURE NO. 08

Predicate Calculus [R1]

- The propositional calculus does not allow us to represent many of the statements that we use in mathematics and in every day life.
- Proposition logic is a logic that includes propositions and connectives but not quantifiers and variables.
- Predicate logic is propositional logic on predicates instead of atomic propositions.
- Example: If two propositions P1 and P2 are

  P1: Rohit is an Engineer
  P2: Mohit is an Engineer

as propositions, there is no relation between P1 and P2, but they have some common part.

- We can replace the two propositions by a single statement "x is an Engineer" and we can get P1 & P2 by replacing x by Rohit and Mohit respectively.
- Common Feature or the part of the statement that follows the subject/object "is an engineer" is a Predicate.

ie. $x \underbrace{\text{is an Engineer}}_{\text{Predicate}}$

- Thus a declarative sentence describing the properties of an object or relation among object is known as a Predicate.

- We can express this as $P(x)$ where P denotes the predicate and x is the variable or predicate variable.

Universe of Discourse [R1]

- The universe of discourse or domain or universe of a predicate variable is the set of all possible values that may be substituted in place of variables.

- Example: $P(x)$: x is a student

  'x' can be taken as the set of all human names.

Quantifier [R1]

- Quantifiers are words that refer to quantities such as 'some' or 'all' and indicate how frequently a certain statement is true.

- Quantifiers are classified into two types:

1. UNIVERSAL QUANTIFIER

- denoted as $\forall x$; which means "for all", "for every".
- Here predicate $P(x)$ is the statement "for all values $x \in A$ $P(x)$ is true".

  ie $\boxed{\forall x \in A : P(x)}$

2. EXISTENTIAL QUANTIFIER

- denoted by $\exists x$; which means "There exists", "For Some", "For Atleast One".
- Predicate $P(x)$ is the statement, "there exists atleast one value x in A such that $P(x)$ is True".

ie. $\boxed{\exists x \in A : P(x)}$

Q] Let $M(x)$: x is a man
$N(x)$: x is a mortal
$A(x)$: x is integer
$B(x)$: x is either positive or negative

Express the following using quantifiers

a) All men are mortal.

Solⁿ: $\forall x\ (M(x) \Rightarrow N(x))$

b) Any integer is either a positive or negative integer

Solⁿ: $\forall x\ (A(x) \Rightarrow B(x))$

Q] Let $A(x)$: x is student
$B(x)$: x is clever
$C(x)$: x is successful

Express the following using quantifier

a) There exists a student

Solⁿ: $\exists x\ A(x)$

b) Some students are clever

Solⁿ: $\exists x\ (A(x) \rightarrow B(x))$

c) Some students are not successful

Sol^n: $\exists x\ (A(x) \wedge \neg C(x))$

Negation of Quantifiers [RI]

Negation	Equivalent Statement	when Negation is TRUE	when Negation is FALSE
$\neg \exists x\, P(x)$	$\forall x\, \neg P(x)$	$P(x)$ is false for every x	There is an x for which $P(x)$ is True.
$\neg \forall x\, P(x)$	$\exists x\, \neg P(x)$	There is an x for which $P(x)$ is False	$P(x)$ is True for every x

	STATEMENT	NEGATION
All True	$\forall x\, P(x)$	$\exists x \neg P(x)$
Atleast one False	$\exists x\, [\neg P(x)]$	$\forall x\, P(x)$
All False	$\forall x [\neg P(x)]$	$\exists x\, P(x)$
Atleast one True	$\exists x\, P(x)$	$\forall x \neg P(x)$

Q] Negate the statement

'For all real numbers x if $x > 5$ then $x^2 > 25$.'

Sol^n: Let $P(x) : x > 5$

$Q(x) : x^2 > 25$

Scanned by CamScanner

Given statement can be written as

$$\forall x \, (P(x) \rightarrow Q(x))$$

$$\equiv \forall x \, (\neg P(x) \vee Q(x)) \qquad (\because P \rightarrow Q = \neg P \vee Q)$$

Negation of the statement is

$$\neg \forall x \, (\neg P(x) \vee Q(x))$$

$$= \exists x \, \neg (\neg P(x) \vee Q(x))$$

$$= \exists x \, (\neg\neg P(x) \wedge \neg Q(x))$$

$$= \exists x \, (P(x) \wedge \neg Q(x))$$

i.e. There exists a real number x such that $x > 5$ and not $x^2 > 25$.

De Morgan's Law [R1]

- If $P(x)$ is a propositional function defined on the domain D, then negation is

$$\neg (\forall x \in D) \, P(x) = (\exists x \in D) \, \neg P(x)$$

$$\neg (\exists x \in D) \, P(x) = (\forall x \in D) \, \neg P(x)$$

Q] Let $M(x)$ be "x is mammal". Let $A(x)$ be "x is an animal". Let $W(x)$ be "x is warm blooded".

a) Translate into a formula: "Every mammal is warm blooded"

Sol^n: $\forall x \, (M(x) \rightarrow W(x))$

b) Translate into English: $\exists x \, (A(x) \wedge (\neg (M(x)))$

Sol^n: There exist some animals which are not mammals.

Q] Translate the following statements into predicate calculus.

i) Some pet dogs are dangerous

Solⁿ: Let $P(x)$: x is a pet dog

$D(x)$: x is dangerous

$$\therefore \exists x\, [P(x) \rightarrow D(x)]$$

ii) Some cats are Black but all buffaloes are black.

Solⁿ: Let $C(x)$: x is a cat

$B(x)$: x is Black

$BF(x)$: x is Buffalo

$$\therefore \exists x\, [C(x) \rightarrow B(x)] \wedge \forall x\, [BF(x) \rightarrow B(x)]$$

iii) Some mathematicians are not good in Computer Science

Solⁿ: Let $M(x)$: x is a Mathematician

$C(x)$: x is good in Computer Science

$$\therefore \exists x\, [M(x) \rightarrow \sim C(x)]$$

iv) All integers are either odd integers or even integers

Solⁿ: Let $I(x)$: x is integer, $O(x)$: x is Odd

$E(x)$: x is Even

$$\therefore \forall x\, [I(x) \rightarrow O(x) \vee E(x)]$$

v) All fish except shark are kind to children.

Sol^n: Let $F(x)$: x is Fish

$S(x)$: x is Shark

$K(x)$: x is Kind to children

$$\therefore \forall x[F(x) \neq S(x)] \Rightarrow K(x)$$

References:

1. Lipschutz, "Discrete Mathematics," McGraw Hill.

Q. Use quantifiers to say that $\sqrt{3}$ is not a rational number.

Sol^n: let $A(x) : \sqrt{x}$

$R(x)$: x is a rational no.

$P(x)$: x is a prime no.

now, $\boxed{\forall x, x \in A, B(x) \rightarrow \sim C(x)}$

ie square root of every prime no. is not rational.

Q. Negate the proposition "All integers are greater than 8".

Sol^n: let $I(x)$: x is an integer

$G(x)$: x is greater than 8

So, $\boxed{\forall x [I(x) \rightarrow G(x)]}$

now, negation is

$$\sim \forall x [I(x) \rightarrow G(x)]$$

$$\exists x \sim [I(x) \rightarrow G(x)]$$

(Contrapositive law $p \to q = \sim p \vee q$)

$$\exists x \sim [\sim I(x) \vee G(x)]$$

$$\boxed{\exists x [I(x) \wedge \sim G(x)]}$$

ie. There exists some integers which are not greater than 8.

OR

Not all Integers are greater than 8.

Q. Translate the following statements given in English into equivalent statements of Propositional/Predicate calculus.

a) Some physicists are not good in chemistry.

Sol^n: let $P(x)$: x is physicist

$C(x)$: x is good in chemistry

$\therefore \boxed{\exists x [P(x) \rightarrow \sim C(x)]}$

b) Americans will stop driving big cars only if they are comfortable with small cars

Sol^n: Let $A(x)$. American will stop driving big cars

$S(x)$ x is comfortable with small cars

$\therefore$ $\boxed{\forall x\, [A(x) \rightarrow S(x)]}$

c) Not all birds can fly.

Sol^n: Let $B(x)$: x is bird

$F(x)$: x can fly

$\sim [\forall x\, [B(x) \rightarrow F(x)]]$

d) Himadari, who is a doctor, is a good sports person also.

Sol^n: Let x be Himadari

$D(x)$: x is doctor

$S(x)$: x is sports person

$\exists x\, [D(x) \wedge S(x)]$

UNIT 05

LECTURE NO. 07

Recurrence Relation and Generating Functions

Generating Functions [R1]

- Generating Functions are one of the most useful inventions in Discrete Maths.
- Roughly speaking, generating functions transform problems about sequences into problem about functions.
- The ordinary Generating Function for the infinite sequence $\langle a_0, a_1, a_2, \dots \rangle$ is the power series:

$$\boxed{A(z) = \sum_{n=0}^{\infty} a_n z^n = a_0 + a_1 z + a_2 z^2 + \dots + a_r z^r + a_n z^n + \dots}$$

where z is a variable.

- Generating functions are important for solving counting problem.
- Examples:

1. The generating function of sequence $\langle 0, 0, 0 \dots \rangle$ is $A(z) = 0 + 0.z + 0.z^2 + \dots = \underline{\underline{0}}$

2. The generating function of sequence $\langle 1, 0, 0, 0 \dots \rangle$ is $A(z) = 1 + 0.z + 0.z^2 + \dots = \underline{\underline{1}}$

3. The generating function of sequence $\langle 2, 3, 1, 0 \dots \rangle$ is $A(z) = 2 + 3z + 1z^2 + 0.z^3 + \dots = 2 + 3z + 1z^2$
$= \underline{\underline{2 + 3z + z^2}}$

4. The generating function of sequence $\langle 1, 1, 1, \ldots, 1, 1, \ldots 1 \ldots \rangle$ is $A(z) = 1 + 1.z + 1.z^2 + \ldots + 1.z^k + \ldots$

$$= \frac{1}{1-z}$$

- In general, the sequence $\langle a^n \rangle$ has the generating function,

$$A(z) = 1 + az + a^2z^2 + \ldots$$

$$\therefore \boxed{A(z) = \sum_{k=0}^{\infty} a_k z^k = \frac{1}{1-az}}$$

- The above generating function, in which coefficients of z^n are sequence terms of the sequence a, is called Binomial Generating Function of the sequence a.

- Another type of generating function is Exponential Generating Function, which is defined as

$$A(z) = a_0 + a_1 z + a_2 \frac{z^2}{2!} + a_3 \frac{z^3}{3!} + \ldots$$

$$\therefore \boxed{A(z) = \sum_{n=0}^{\infty} a_n \frac{z^n}{n!}}$$

Q] Find the generating function for the sequence $b = 1, 3, 9, \ldots 3^n \ldots$

Scanned by CamScanner

Solⁿ: The given sequence, $b = 1, 3, 9, \dots, 3^n, \dots$

Here the general term $b_n = 3^n$

Let $A(z)$ be Binomial Generating function for the given sequence, then

$$A(z) = \sum_{n=0}^{\infty} b_n z^n$$

$$= \sum_{n=0}^{\infty} 3^n \cdot z^n$$

$$\boxed{A(z) = \frac{1}{1-3z}}$$

now let $A(z)$ be Exponential Generating function for the given sequence, then

$$A(z) = \sum_{n=0}^{\infty} b_n \frac{z^n}{n!}$$

$$= \sum_{n=0}^{\infty} 3^n \frac{z^n}{n!}$$

$$= 1 + 3z + \frac{(3z)^2}{2!} + \frac{(3z)^3}{3!} + \dots$$

$$\boxed{A(z) = e^{3z}}$$

Q] Determine the generating function of a numeric function a_r where

$$a_r = \begin{cases} 2^r & \text{if } r \text{ is even} \\ -2^r & \text{if } r \text{ is odd} \end{cases}$$

Sol^n: We know that for a sequence, the general generating function is

$$A(z) = \sum_{n=0}^{\infty} a_n z^n = a_0 + a_1 z + a_2 z^2 + \dots + a_n z^n$$

here in the given data

$$A(z) = \sum_{r=0}^{\infty} a_r z^n = a_0 + a_1 z + a_2 z^2 + \dots + a_r z^r \quad \text{—— (I)}$$

now substitute in (I)

$$a_r = \begin{cases} 2^r & \text{if } r \text{ is even} \\ -2^r & \text{if } r \text{ is odd} \end{cases}$$

equ^n (I) becomes,

$$A(z) = 2^0 + (-2)^1 \cdot z + (2)^2 \cdot z^2 + (-2)^3 \cdot z^3 + \dots$$

$$\boxed{A(z) = 1 - 2z + 2^2 z^2 - 2^3 z^3 + \dots}$$

Q] If the generating function of a sequence $a_0, a_1, a_2 \dots$ is given by $A(z) = \dfrac{2}{(1-4z^2)}$, find an the $(n+1)^{th}$ term of the sequence.

Sol^n: The given generating function is

$$A(z) = \frac{2}{1-4z^2}$$

$$= \frac{2}{(1-2z)(1+2z)}$$

$$= \frac{1}{(1-2z)} + \frac{1}{(1+2z)} \qquad \text{(By Partial Fractions)}$$

$$= 2^n + (-2^n)$$

$= \cancel{2^n}$ $(n+1)^{th}$ term of the sequence.

Scanned by CamScanner

Table of Generating Functions [R1]

	Sequence	Generating Function $A(z)$
1.	$C(K,n)$	$(1+z)^K$
2.	1	$\frac{1}{1-z}$
3.	a^n	$\frac{1}{1-az}$
4.	$(-1)^n$	$\frac{1}{1+z}$
5.	$(-1)^n a^n$	$\frac{1}{1+az}$
6.	$n+1$	$\frac{1}{(1-z)^2}$
7.	n	$\frac{z}{(1-z)^2}$
8.	$(n+2)(n+1)$	$\frac{2}{(1-z)^3}$
9.	$(n+1)n$	$\frac{2z}{(1-z)^3}$
10.	n^2	$\frac{z(1+z)}{(1-z)^3}$
11.	n^3	$\frac{z(1+4z+z^2)}{(1-z)^2}$
12.	$(n+3)(n+2)(n+1)$	$\frac{6}{(1-z)^4}$
13.	$(n+2)(n+1)(n)$	$\frac{6z}{(1-z)^4}$

References:

1. Lipschutz, "Discrete Mathematics," McGraw Hill

UNIT 05

LECTURE NO. 08

Recurrence Relations [R1]

- Also called as Difference Equation.
- Recurrence Relations define the terms of a sequence.
- A sequence is a function whose domain is some infinite set of integers and whose range is a set of real numbers.
- Consider a sequence $\langle a_n \rangle = \langle 2^0, 2^1, 2^2, 2^3, \ldots 2^r, \ldots \rangle$, then the general term of this sequence can be specified by the expression

$$\boxed{a_r = 2^r, \ r \geq 0}$$

- A recurrence relation is a formula that relates for any integer $n \geq 1$, the n^{th} term of a sequence $A = \langle a_n \rangle_{n=0}^{\infty}$ to one or more of the terms $a_0, a_1, a_2, \ldots, a_{n-1}$

Solution of Linear Recurrence Relation with Constant Coefficients. [R1, R2]

1. HOMOGENEOUS SOLUTIONS, which satisfy the recurrence relations when the right hand side of the equation is set to zero.
2. PARTICULAR SOLUTIONS, which satisfy the recurrence relations with $f(r)$ on the right hand side.

- Suppose $c_0 a_r + c_1 a_{r-1} + c_2 a_{r-2} + \dots + c_k a_{r-k} = 0$ is a linear homogeneous recurrence relation of order k with constant coefficients.

- The solution of this equation is supposed to be of the form $\boxed{a_r = A\alpha_1^r}$

- Substituting this into the relation, we get

$$c_0(A\alpha_1^r) + c_1(A\alpha_1^{r-1}) + c_2(A\alpha_1^{r-2}) + \dots + c_k(A\alpha_1^{r-k}) = 0$$

or $A\alpha_1^{r-k}[c_0\alpha_1^k + c_1\alpha_1^{k-1} + \dots + c_k] = 0$

or $\boxed{c_0\alpha_1^k + c_1\alpha_1^{k-1} + \dots + c_k = 0}$

which is called the characteristic equation of the Recurrence Relation; α_1 is called the characteristic root and $A\alpha_1^r$ is a homogeneous solution to the recurrence relation.

- A characteristic equation of k^{th} degree has k characteristic roots.

Q] Solve the recurrence relation $a_r - 6a_{r-1} + 9a_{r-2} = 0$

Solⁿ: The characteristic equation corresponding to the given recurrence relation is

$$\alpha^2 - 6\alpha + 9 = 0 \quad \text{or} \quad x^2 - 6x + 9 = 0$$

$$(x-3)^2 = 0$$

$$\therefore x = 3, 3$$

Since the roots are repeated, the homogeneous solution is $\boxed{a_r = (A_1 + A_2 r)3^r}$

Q] Solve the recurrence relation $a_r - 6a_{r-1} + 8a_{r-2} = 0$

Solⁿ: The characteristic equation is given by

$$x^2 - 6x + 8 = 0$$

$$\therefore (x-2)(x-4) = 0$$

$$\therefore \boxed{x = 2, 4}$$

∴ The homogeneous solution is

$$\boxed{a_r = A_1 2^r + A_2 4^r}$$

Q] Solve $a_r - 5a_{r-1} + 6a_{r-2} = 0$ where $a_0 = 2$ and $a_1 = 5$

Solⁿ: Characteristic equation is $x^2 - 5x + 6 = 0$

$$(x-3)(x-2) = 0$$

$$\therefore x = 3, 2$$

The homogeneous solution is

$$\boxed{a_r = A_1 2^r + A_2 3^r}$$

we have $a_0 = 2$, $a_1 = 5$

$$\therefore a_0 = A_1 2^0 + A_2 3^0 = 2$$

$$\therefore \boxed{A_1 + A_2 = 2} \quad \text{——— (I)}$$

$$a_1 = A_1 2^1 + A_2 3^1 = 5$$

$$\therefore \boxed{2A_1 + 3A_2 = 5} \quad \text{——— (II)}$$

solving (I) & (II), we get $A_1 = 1$ & $A_2 = 1$

∴ Final solution is

$$\boxed{a_r = 2^r + 3^r}$$

Q] Solve the recurrence relation

$$a_{r+4} + 2a_{r+3} + 3a_{r+2} + 2a_{r+1} + a_r = 0$$

Sol^n: Characteristic Equation is $x^4 + 2x^3 + 3x^2 + 2x + 1 = 0$

After solving this equation, we get

$$x = \frac{-1 \pm i\sqrt{3}}{2}, \frac{-1 \pm i\sqrt{3}}{2}$$

Therefore, the homogeneous solution is

$$\boxed{a_r = (A_1 + A_2 r)\left(\frac{-1+i\sqrt{3}}{2}\right)^r + (A_3 + A_4 r)\left(\frac{-1-i\sqrt{3}}{2}\right)^r}$$

- The procedure for obtaining the particular solution of a recurrence relation depends on the form of $f(r)$ i.e. the right hand side of the given relation.

CASE 1: If $f(r)$ is a polynomial of degree t in r

i.e. $f(r) = f_1 r^t + f_2 r^{t-1} + \dots + f_t r + f_{t+1}$

Then the solution to be assumed as

$$\boxed{a_r^{(P)} = P_1 r^t + P_2 r^{t-1} + \dots + P_t r + P_{t+1}}$$

Q] Find the particular solution of the recurrence relation $a_r + 5a_{r-1} + 6a_{r-2} = 3r^2$

Sol^n: Here $f(r)$ is a polynomial of degree 2 in r

We assume that the general form of the particular solution is $a_r^{(P)} = P_1 r^2 + P_2 r + P_3$

Putting this into LHS of the given recurrence relation, we get

$$(P_1 r^2 + P_2 r + P_3) + 5(P_1(r-1)^2 + P_2(r-1) + P_3) + 6(P_1(r-1)^2 + P_2(r-2) + P_3) = 3r^2$$

$$= 12P_1 r^2 + (12P_2 - 34P_1)r + (29P_1 - 17P_2 + 12P_3) = 3r^2$$

Comparing the coeffients of r^2, r and constants we get,

$$12P_1 = 3 \quad \text{——— (I)}$$

$$12P_2 - 34P_1 = 0 \quad \text{——— (II)}$$

$$29P_1 - 17P_2 + 12P_3 = 0 \quad \text{——— (III)}$$

solving (I), (II) & (III), we get

$$P_1 = 1/4, \quad P_2 = 17/24, \quad P_3 = 115/288$$

$\therefore$ The particular solution is

$$\boxed{a_r^{(P)} = \frac{1}{4}r^2 + \frac{17}{24}r + \frac{115}{288}}$$

<u>CASE 2:</u> If $f(r)$ is in the form of β^r, where β is not a characteristic root, then the particular solution to be assumed as

$$\boxed{a_n^{(P)} = P\beta^r}$$

9] Find the particular solution of the recurrence relation $a_n = 5a_{n-1} - 6a_{n-2} + 7^n$

<u>Solⁿ:</u> The given recurrence relation is

$$a_n = 5a_{n-1} - 6a_{n-2} + 7^n \quad \text{or} \quad a_n - 5a_{n-1} + 6a_{n-2} = 7^n$$

The characteristic equation corresponding to this is

$$\alpha^2 - 5\alpha + 6 = 0$$

$$(\alpha - 3)(\alpha - 2) = 0$$

$$\alpha = 3, 2$$

$$\therefore \boxed{a_n = A_1 3^n + A_2 2^n}$$

where A1 & A2 are constants

Here $f(n) = 7^n$

The particular solution is

$$a_n^{(P)} = P \cdot 7^n$$

substituting the terms in recurrence relation

$$P \cdot 7^n = 5P \cdot 7^{n-1} - 6P \cdot 7^{n-2} + 7^n$$

$$49P = 35P - 6P + 49 \qquad (n=2)$$

$$20P = 49$$

$$\therefore \boxed{P = \frac{49}{20}}$$

Hence the particular solution is

$$a_n^{(P)} = P \cdot 7^n$$

$$\boxed{a_n^{(P)} = \frac{49}{20} \cdot 7^n}$$

CASE3: If $f(r)$ is in the form of $f(r) = C$ (constant) and if 1 is not a root of characteristic equation, then the particular solution is

$$\boxed{a_n^{(P)} = P}$$

8] Find the particular solution of the recurrence relation $a_r - 5a_{r-1} + 6a_{r-2} = 1$

Sol^n: The $f(r)$ is a constant. So, the particular solution is $a_r^{(P)} = P$

Put the value in given recurrence relation, we get

$$P - 5P + 6P = 1$$

$$2P = 1$$

$$P = 1/2$$

$$\therefore \boxed{a_r^{(P)} = \frac{1}{2}}$$

References:

1. Liu and Mohpatra, "Elements of Discrete Mathematics", McGraw Hill

2. Lipschutz, "Discrete Mathematics", McGraw Hill

UNIT 05

LECTURE NO. 09

Solution of Recurrence Relation by the method of Generating Functions [R1, R2]

- Generating function can also be used solve a recurrence relation.
- Before using this method, ensure that the given recurrence equation is in linear form.
- A non linear recurrence equation can not be solved by the generating method.
- We use substitution of variable technique to convert a non-linear recurrence relation into linear equation.

Q] Solve the recurrence relation $a_r - 3a_{r-1} + 2a_{r-2} = 0$ $r \geq 2$ by generating function method with the initial conditions $a_0 = 2$ and $a_1 = 3$.

Sol^n: Let $A(z)$ be the generalting function of the sequence $\langle a_n \rangle$

i.e. $A(Z) = \sum_{r=0}^{\infty} a_r Z^r$

multiply the given recurrence relation by z^r, we get

$$a_r z^r - 3a_{r-1} z^r + 2a_{r-2} z^2 = 0 \quad \text{——— (I)}$$

summing (I) from $r=2$ to ∞, we obtain

$$\sum_{r=2}^{\infty} a_r z^r - 3\sum_{r=2}^{\infty} a_{r-1} z^r + 2\sum_{r=2}^{\infty} a_{r-2} z^2 = 0 \quad \text{——— (II)}$$

$$(A(z) - a_0 - a_1 z) - 3z(A(z) - a_0) + 2z^2 A(z) = 0$$

$$(2z^2 - 3z + 1)A(z) - a_0 - a_1 z + 3a_0 z = 0 \quad \text{——— (III)}$$

now substituting $a_0 = 2$ and $a_1 = 3$ in (III), we get

$$(2z^2 - 3z + 1)A(z) - 2 - 3z + 6z = 0$$

$$A(z) = \frac{2 - 3z}{2z^2 - 3z + 1}$$

$$A(z) = \frac{1}{(1-z)} + \frac{1}{(1-2z)} \quad \text{(By Partial Fractions)}$$

$$\therefore \boxed{a_r = 1 + 2^r} \qquad \left(\because \frac{1}{1-az} = a^n\right)$$

Q] Solve the recurrence relation $a_r - 5a_{r-1} + 6a_{r-2} = 2$, $r \geq 2$ by the generating function method with boundary conditions $a_0 = 1$ and $a_1 = 1$.

Solⁿ: Let $A(z) = \sum_{r=0}^{\infty} a_r z^r$ be the generating function of the sequence $\langle a_n \rangle$, $n \geq 0$.

Multiplying the recurrence relation by z^r and summing for all $r \geq 2$, we obtain

$$\sum_{r=2}^{\infty} a_r z^r - 5\sum_{r=2}^{\infty} a_{r-1} z^r + 6\sum_{r=2}^{\infty} a_{r-2} z^r = \sum_{r=2}^{\infty} 2z^r$$

$$(A(z) - a_0 - a_1 z) - 5z(A(z) - a_0) + 6z^2 A(z) = 2[z^2 + z^3 + \dots] \quad \text{(I)}$$

substituting the boundary conditions $a_0 = 1$ & $a_1 = 1$, we get

$$A(z)[1 - 5z + 6z^2] - 1 + 4z = \frac{2z^2}{1-z}$$

$$A(z)[6z^2 - 5z + 1] = \frac{2z^2}{1-z} + 1 - 4z$$

$$A(z) = \frac{2z^2}{(1-z)(1-2z)(1-3z)} + \frac{1-4z}{(1-2z)(1-3z)} = \frac{1}{1-z}$$

$$\therefore \quad a_r = 1^r$$

$$\boxed{a_r = 1}$$

References:

1. Liu and Mohpatra, "Elements of Discrete Mathematics", McGraw Hill
2. Lipschutz, "Discrete Mathematics," McGraw Hill

UNIT 05

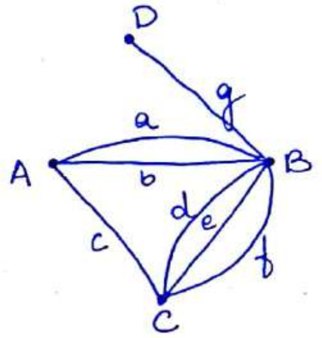
LECTURE NO. 03

Graph [R1]

A simple graph G is a pair $\boxed{G = (V,E)}$ where V is a finite set of vertices and E is a finite set of Edges.

- Example

Routes between Cities



• Here, there are

3 routes between cities B&C

2 routes between cities A&B

Single route between cities A&C and B&D.

Basic Terminologies of Graph [R1]

1. LOOP

• An edge having the same vertex as both its end vertices is called a Self-Loop or simply a loop.

• In fig 01, e1 is a loop.

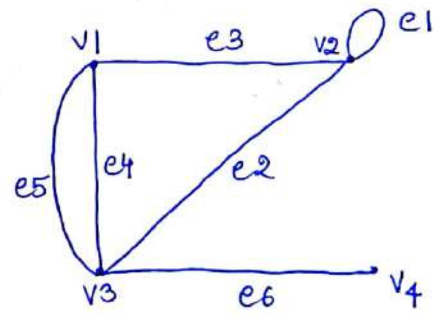


FIG 01.

2. PARALLEL EDGES

• Edges having the same starting vertex and same end vertex are called as Parallel Edges.

• In fig 01, e5 & e4 are parallel edges.

3. INCIDENCE

- When a vertex v_i is an end vertex of some edge e_j, v_i and e_j are said to be incident with each other.
- In fig 01, e2, e4, e5 and e6 are incident with vertex V_4.

4. ADJACENT EDGES

- Two non-parallel edges are said to be adjacent if they are incident on a common vertex.
- In fig 01, e2 & e6 are adjacent edges.

5. ADJACENT VERTICES

- Two vertices are said to be adjacent if they are the end vertices of the same edges.
- In fig 01, V3 & V4 are adjacent vertices.

6. DEGREE OF A VERTEX

- The number of edges incident on a vertex v_i, with self loop counted twice, is called the degree of vertex v_i.
- It is also called as Valency of vertex.
- In fig 01,

deg(v1) = 3
deg(v2) = 4
deg(v3) = 4
deg(v4) = 1.

now,

deg(v1) + deg(v2) + deg(v3) + deg(v4)
= 3+4+4+1 = 12 = Twice the no. of edges

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

Scanned by CamScanner

7. ISOLATED VERTEX

- A vertex having no incident edge is called an Isolated Vertex.
- The degree of an isolated vertex is Zero.

8. PENDANT VERTEX

- A vertex of degree one is called as pendent Vertex.

9. SIMPLE GRAPH

- The graph with neither self loops nor parallel edges is called a Simple Graph.

10. MULTIGRAPH

- A graph in which no loops are allowed but parallel edges are allowed is called a multigraph.

11. PSEUDO GRAPH

- A graph in which both self loops and parallel edges are allowed is called a Pseudo graph.

12. FINITE GRAPH

- A graph with finite number of vertices as well as a finite number of edges is called a Finite Graph.

13. INFINITE GRAPH

- A graph which is not finite is called Infinite Graph

14. UNDIRECTED GRAPH

- An undirected graph G consists of set V of vertices and a set E of edges such that each edge $e \in E$ is associated with unordered pair of vertices.

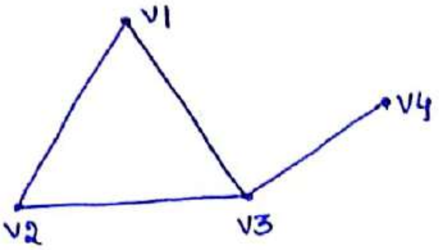


Fig 02 : Undirected Graph

15. DIRECTED GRAPH

- A directed graph is also known as Digraph.
- A digraph G consists of a set V of vertices and a set E of edges such that e∈E is associated with an ordered pair of vertices.
- In digraph each edge of a graph has a direction.

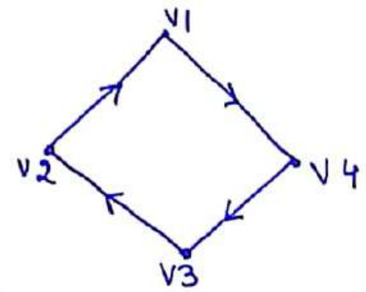


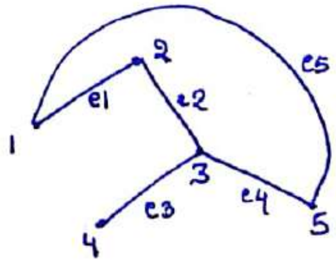
Fig 03: Directed Graph

16. TRIVIAL GRAPH

- A finite graph with one vertex and no edge is called the Trivial graph.

17. LABELLED GRAPH

- A graph $G = (V, E)$ is known as labelled graph if its edges are labelled with name or data.
- We write label in place of an ordered pair.



$G = (V, E)$

$G = (\{1, 2, 3, 4, 5\}, \{e1, e2, e3, e4, e5\})$

18. IN DEGREE AND OUT DEGREE

- In a directed graph G, the out degree of a vertex v_i is denoted by $\boxed{\text{out deg}(v_i) \text{ or } \deg^{+}(v_i)}$
- It is the number of edges beginning at V.
- Indegree of a vertex v_i is denoted by $\boxed{\text{indeg}(v_i) \text{ or } \deg^{-}(v_i)}$
- The sum of the indegree and outdegree of a vertex is called the Total Degree of the vertex.
- A vertex with zero indegree is called a 'Source' and a vertex with zero outdegree is called a 'sink'.

19. WALKS, PATHS & CIRCUIT

- A walk of a graph G is an alternating sequence (finite) of vertices and edges, beginning and ending with vertices, such that each edge is incident with the vertices preceding and following it.

$$\boxed{\text{Walk}(w) = v_0 e_1 v_1 e_2 v_2 e_3 \dots v_K \; e_K \; v_K}$$

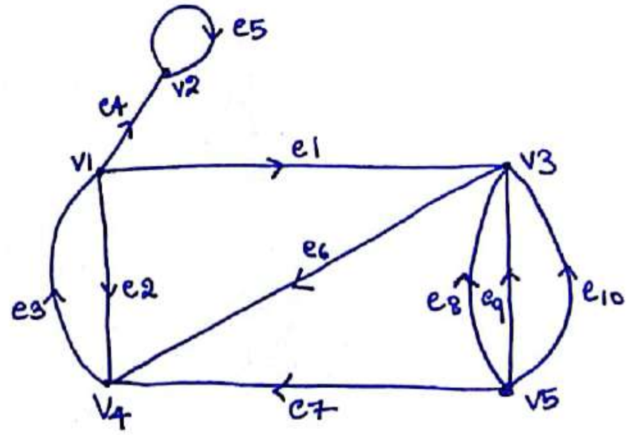
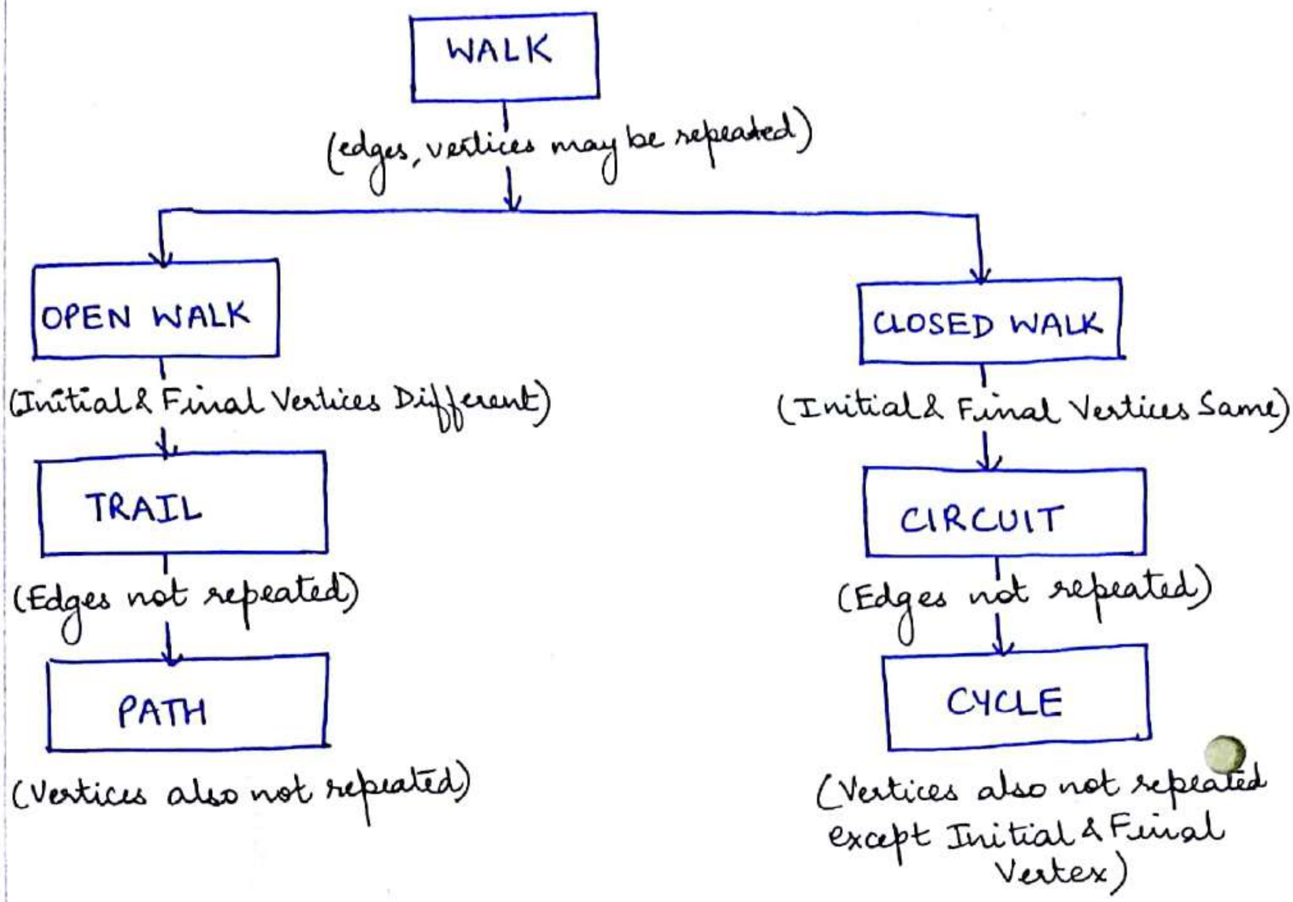


Fig 04



20. REGULAR GRAPH

- A graph G is called a regular graph if its all vertices are of same degree.
- If the degree of each vertex is k then the graph is called k-regular graph or regular graph of degree k.

21. COMPLETE GRAPH

- A simple graph G is said to be complete if every vertex in G is connected with every other vertex.
- A complete graph contains exactly one edge between each pair of distinct vertices.
- A complete graph is denoted by K_n, where n = no. of nodes.
- K_n has exactly $\frac{K(n-1)}{2}$ edges.

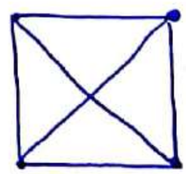


Fig 05

Scanned by CamScanner

22. NULL GRAPH

- A graph with n vertices and zero edges is called a Null Graph.
- i.e. the Edge set of graph is empty.
- A null graph is totally disconnected graph.
- Every vertex of null graph is an isolated vertex.
- Denoted by N_n, where n is the no. of nodes.

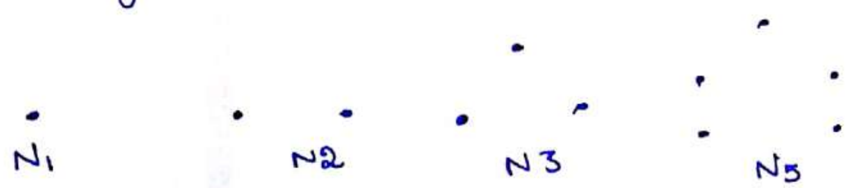


Fig 06: Null Graphs

23. BIPARTITE GRAPH

- A graph G is said to be bipartite if its vertices V can be partitioned into two subsets M & N such that each edge of G connects a vertex of M to a vertex of N.
- By a complete bipartite graph, we mean that each vertex of M is connected to each vertex of N and this graph is denoted by $K_{m,n}$ where m is the no. of vertices in M and n is the no. of vertices in N.
- We assume that $m \leq n$ for standardization

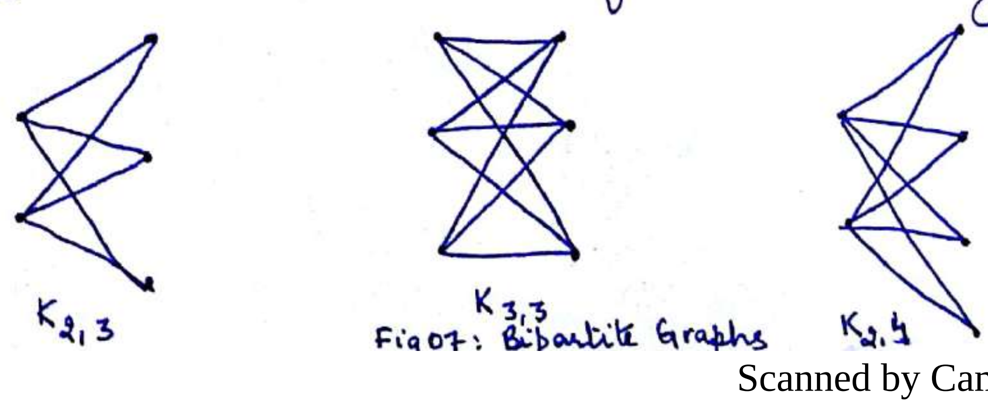


Fig 07: Bipartite Graphs

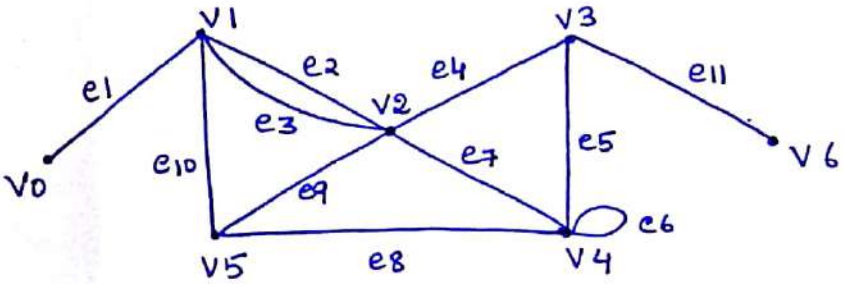
24. EULER GRAPH

- If some closed walk in a graph contains all the edges of the graph, then the walk is called an Euler line and the graph an Euler Graph.

25. UNICURSAL GRAPH

- If some open walk in a graph contains all the edges of the graph, then the walk is called an Unicursal line or Open Euler line and the graph an Unicursal Graph.

Q. In the graph, determine whether the following are path, simple path, trails or circuits



i) $V_0\, e_1\, V_1\, e_{10}\, V_5\, e_9\, V_2\, e_2\, V_1$

Sol^n: • Since the initial & final vertex is not same ∴ it is an Open Walk, hence it can not be a Circuit.

- Since edge V1 is repeated ∴ it can not be a Path.
- Since edge V1 is repeated but no edge is repeated ∴ it is a Trail.

ii) $V_5\ V_2\ V_3\ V_4\ V_4\ V_4\ V_5$

Solⁿ: • The above sequence can be written as

$V_5\ e_9\ V_2\ e_4\ V_3\ e_5\ V_4\ e_6\ V_4\ e_6\ V_4\ e_8\ V_5$

• Since the initial and end vertex are same
∴ it is a Closed Walk.

• Since edge e_6 and vertex V_4 are repeated
∴ it is not a Cycle.

It is neither a Path, Trail or a Circuit.

iii) $V_4\ e_7\ V_2\ e_9\ V_5\ e_{10}\ V_1\ e_3\ V_2\ e_9\ V_5$

Solⁿ: The sequence has different initial and end vertex. Therefore it is open Walk.

Since both edges and vertices are repeated (e_9 & V_2, V_5) ∴ it is neither a path, Trail or circuit.

26. HAMILTONIAN GRAPH

• A Hamiltonian Trail is a path in a graph that passes every vertex exactly once.

• A Hamiltonian Circuit is a circuit in a graph that contains each vertex exactly once except the initial and the end vertex.

• A graph consisting of a Hamiltonian Circuit is called as Hamiltonian Graph.

27. PLANAR GRAPH

- If a graph can be drawn in the plane without any of its edge crossing or intersecting, it is said to be planar.
- A planar graph is a graph which can be embedded in the plane i.e. it can be drawn on the plane in such a way that its edges may intersect only at their end points.
- A graph which is not planar is called a <u>Non Planar Graph</u>.
- Drawing of geometric representation of a graph on any surface such that no edges intersect is called <u>Embedding</u>.

Fig 08: Planar Graph

28. EULER'S FORMULA

- If G is a planar graph, then any plane drawing of G divides the plane into regions.
- The Euler's formula relates the number of vertices, edges and regions of the planar graph.
- Euler's Formula is $\boxed{n-e+f=2}$

where n = no. of nodes (vertices)
e = no. of edges
f = no. of regions

References:
1. Narsingh Deo, "Graph Theory with Applications to Engineering & CS" EE

UNIT 05

LECTURE NO. 04

Graph Isomorphism [R1, R2]

- Suppose $G=(V,E)$ and $G'=(V',E')$ are two graphs. A function $f: V \to V'$ is called Graph isomorphism if
  i) f is one-to-one
  ii) f is onto
  iii) for all, $a, b \in V$, $\{a,b\} \in E$ iff $\{f(a), f(b)\} \in E'$ when such a function exists, G and G' are called Isomorphic Graphs and written as $\boxed{G \cong G'}$

- Conditions for Graph Isomorphism
  1. Both graph G and G' must have the same number of vertices.
  2. Both must have the same number of edges.
  3. *Degree sequence of both graphs are same.

* DEGREE SEQUENCE

- If $v_1, v_2, \dots, v_n$ are the vertices of G, then the sequence $(d_1, d_2, \dots d_n)$ where $d_i =$ degree(v_i) is the degree sequence of G.
- Usually, we order the vertices so that the degree sequence is monotonically increasing

  ie $\boxed{d_1 \leq d_2 \leq \dots \leq d_n}$

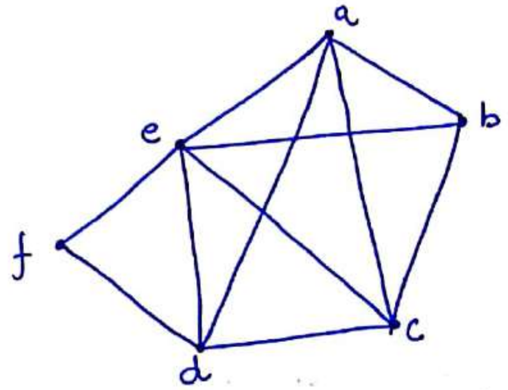


Fig 09 : Graph G

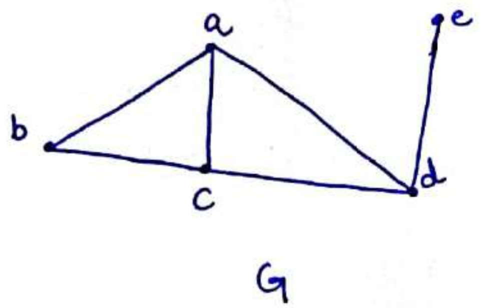
here

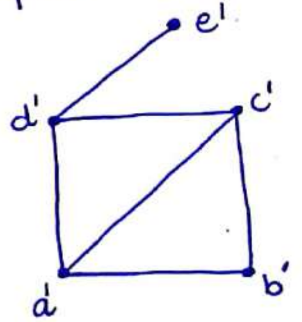
deg(a) = 4 deg(d) = 4
deg (b)=3 deg (e) = 5
deg (c) = 4 deg (f) = 2

since the degree sequence is monotonically increasing.

$\therefore$ $\boxed{\text{deg seq.} = (2, 3, 4, 4, 4, 5)}$

Q] Show that the following graphs are isomorphic.





Sol^n: 1. Both the graphs G and G' have the same no. of vertices ie. <u>5 vertices</u>.

2. Both the graphs G and G' have the same no. of edges. ie. <u>6 edges</u>.

3. Degree of both G & G'

deg (G)

deg (a) = 3
deg (b) = 2
deg (c) = 3
deg (d) = 3
deg (e) = 1

deg seq = (1, 2, 3, 3, 3)

deg (G')

deg (a') = 3
deg (b') = 2
deg (c') = 3
deg (d') = 3
deg (e') = 1.

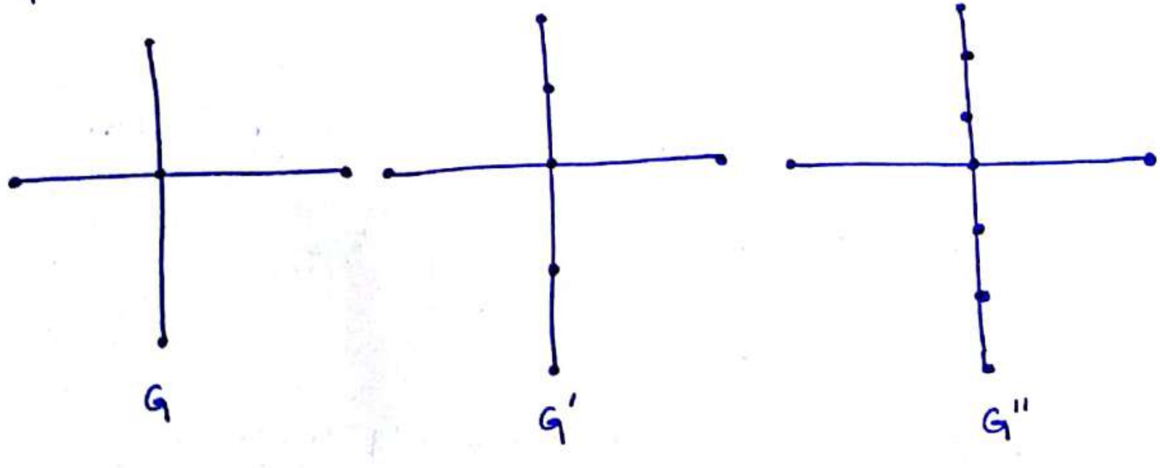
deg seq = (1, 2, 3, 3, 3)

∴ Degree Sequences of Both graph G and G' are same.

∴ G and G' are Isomorphic Graphs.

Homeomorphic Graphs [R2]

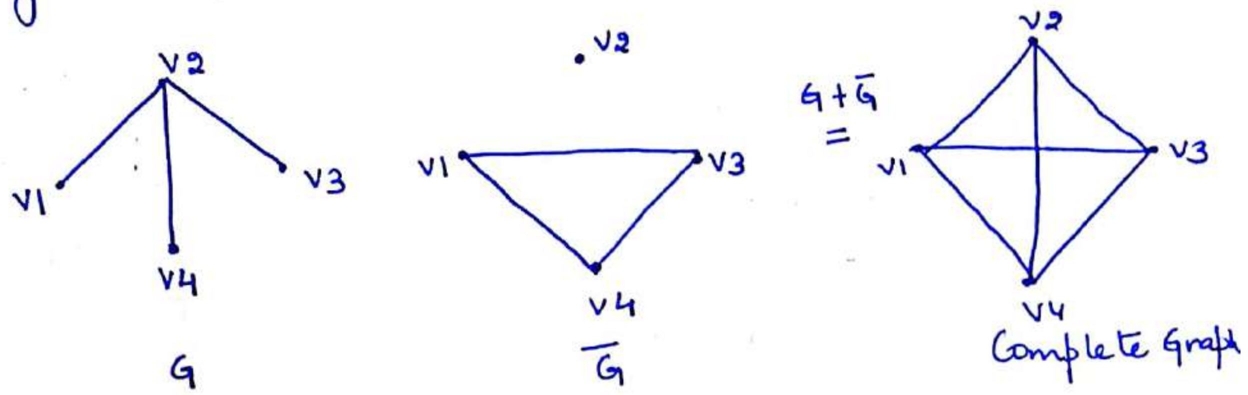
- Given any graph G, we can obtain a new graph by dividing an edge of G with additional vertices.
- Two graphs G and G' are said to be homeomorphic if they can be obtained from the same graph.

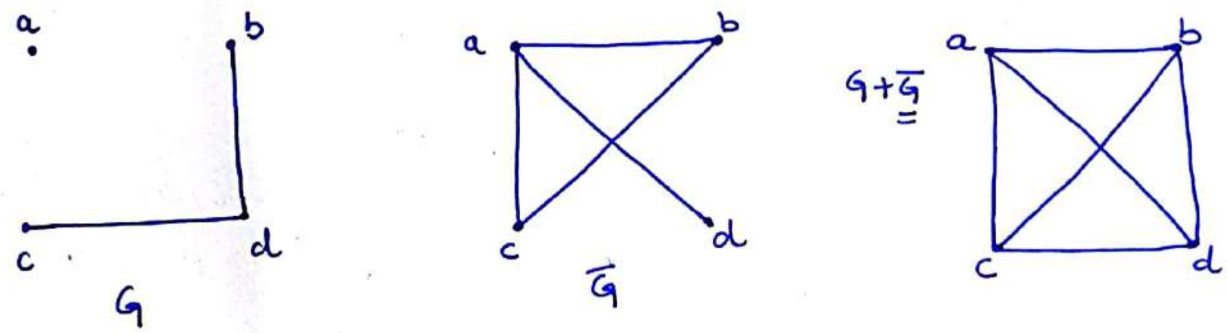


The graphs G' and G'' are homeomorphic since they can be obtained from graph G.

Complement of a Simple Graph [R1]

- If a Graph G is on n-vertices then the complement $\overline{G}$ is the complete graph K_n with all of the edges in G deleted.





Self Complementary Graphs [R1]

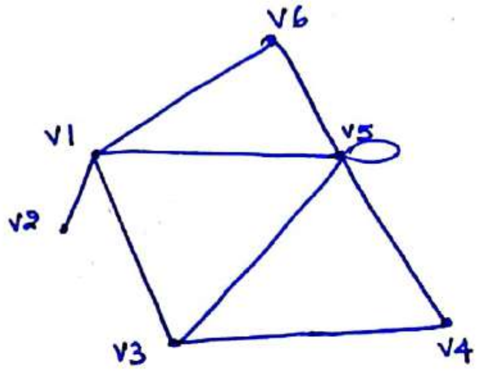
A graph G is said to be self complementary graph if it is isomorphic to its complements.

Connected & Disconnected Graphs [R1]

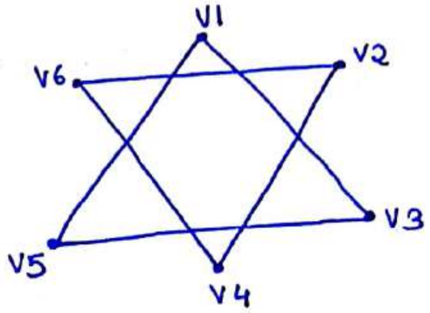
- A graph G is connected if we can reach any vertex from any other vertex by traveling along the edges.
- Two Vertices in graph G are said to be connected if there exists atleast one path from one vertex to the other.

Scanned by CamScanner

- A graph G is said to be <u>Disconnected</u> if G has atleast one pair of vertices between which there is no path.



CONNECTED GRAPH



DISCONNECTED GRAPH

- A complete graph is always connected and a null graph of more than one vertex is disconnected.

- Every graph G consists of one or more connected graphs, each such connected graph is a subgraph of G and is called a <u>Component</u> of G

<u>Rank of Graph G</u> [R1,R2]

$$\boxed{\rho(G) = n-k}$$

where
n = no. of nodes
m = no. of edges
k = no. of components

<u>Nullity of Graph G</u> [R1,R2]

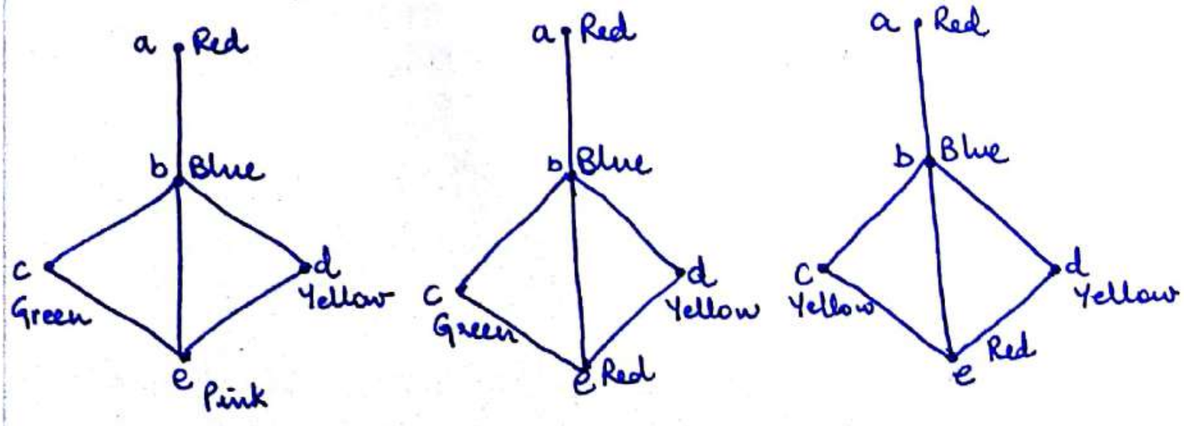
$$\boxed{\mu(G) = m - \rho(G) = m-n+k}$$

Colouring of Graphs [R1]

- Suppose that we are given a graph G with n vertices and are asked to paint its vertex such that no two adjacent vertices have the same color.
- Painting / Coloring all the vertices of a graph with colors such that no two adjacent vertices have the same colour is called Proper Coloring or coloring of a Graph, and the graph is called Properly Colored Graph.
- Here $C = \{c_1, c_2, c_3, \ldots, c_n\}$ is the set of n colors used for proper coloring of graph.
- Also called as Vertex Coloring.
- Any function $f : V \rightarrow C$ is called a coloring of the graph G using n colors.
- For each vertex u, f(u) is the color of u.

Chromatic Number [R1]

- The smallest number of colors to produce a proper coloring of a Graph G is called the chromatic number of graph G
- Denoted by $\chi(G)$ or 'K'



- Therefore, chromatic number denotes the minimum numbers of colors 'K', required for proper coloring of the graph.
- Such a graph is called a <u>K- Vertex chromatic Graph</u> or <u>K- vertex colorable graph</u>.

<u>Properties of K- chromatic Graph</u> [RI]

1. The chromatic number of a graph consisting of isolated vertices is one i.e. it is a <u>1- chromatic graph</u>.

2. The chromatic number of a complete graph with n vertices ie. K_n is n because each vertex of this graph is adjacent to its every other vertex.
   i.e. K_n is <u>n- chromatic graph</u>.

3. A graph with at least one edge is at-least 2- chromatic or bichromatic.

4. A graph having one cycle with at least 3-vertices is 2- chromatic if the number of vertices n is even and 3- chromatic if n is odd.

5. Chromatic number of bipartite graph with non empty edge set is 2.

6. Chromatic number of a tree with at least two vertices is 2 as these are connected acyclic graph.

UNIT 05

LECTURE NO. 05

Elementary Combinatories

Basic Counting Principles [R1]

1. SUM RULE

- Also called as Principle of Disjunctive Counting.
- If one action can be performed independently in n_1 different ways and another disjoint action can be performed independtly in n_2 different ways, and yet another disjoint action can be performed independently in n_3 different ways, and so on (the number of actions being finite) then the total number of ways in which either of these actions can be performed is

$$\boxed{n_1 + n_2 + n_3 + \cdots}$$

Q. How many ways can we get a sum of 8 when two indistinguishable dice are rolled?

Sol^n: We can obtain a sum of 8 by the outcomes (2,6), (3,5), (4,4), (5,3) and (6,2); but the dice are similar so the outcomes {(2,6) and (6,2) and {(3,5) and (5,3)} can not be differentiated.

$\therefore$ $\boxed{\text{ways in which we can obtain } 8 = 3}$

Q] If there are 36 boys and 24 girls in a class, find the number of ways of selecting one student as class representation, using Sum Rule.

Sol^n Using sum rule; $36+24=$ 60 ways are there of selecting one student as CR.

Q] In how many ways can we draw a heart or a spade from an ordinary deck of cards?

Sol^n: In a deck of cards, there are 13 spades and 13 hearts. Thus, by sum rule, a spade or a heart may be drawn in $13+13=$ 24 ways

Q] In how many ways can we choose a prime number or an even number between 10 and 20 (excluding both numbers)

Sol^n: A prime number between 10 and 20 can be chosen in 4 ways ie. 11, 13, 17 and 19.

An even number between 10 and 20 can be chosen in 4 ways ie. 12, 14, 16, and 18.

Thus, by sum rule, a prime or an even number between 10 and 20 can be chosen in $4+4=$ 8 ways

2. PRODUCT RULE

- Also called as The Principle of Sequential Counting.
- If one action can be performed independently in n1 different ways, and after it has been done, if second action be performed independently in n2 different ways, and after both have been done, if a third action can be performed independently in n3 different ways and so on

Q] How many 4-digits nos. can be formed using the digits 1, 3, 4, 6, 7 and 8? How many 4-digit nos. can be formed it no digit can be repeated?

<u>Sol^n</u>: It is given 6 digits can be used to form a 4-digit number. So each of the four digits can be chosen in 6 ways.

Therefore, by product rule, $6 \times 6 \times 6 \times 6 = 6^4 = \underline{1296}$ four digit numbers can be formed

If the repetition of digits is not allowed, then thousands place can be filled in 6 ways, hundreds place can be filled in 5 ways, ten's place can be filled in 4 ways and units place in 3 ways.

Thus, by product rule, $6 \times 5 \times 4 \times 3 = \underline{360}$ different four digit numbers can be formed.

Q] How many 2-digit or 3-digit numbers can be formed using digits 1, 2, 3, 5, 7, 9 if no repetition is allowed.

<u>Sol^n</u>: It is given 6 digits can be used to form a 2-digit number with no repetitions.

Therefore, $6 \times 5 = \underline{30}$ different 2 digits numbers can be formed.

Also 6 digits can be used to form a 3-digit numbers with no repetitions.

Therefore, $6 \times 5 \times 4 = \underline{120}$ different 3 digits numbers can be formed.

(the no. of action being finite) then the total number of ways in which all the actions can be performed together is

$$\boxed{n_1 \times n_2 \times n_3 \times \dots}$$

Q] A coin is tossed four times and the result of each toss is recorded. How many different sequences of heads and tails are possible?

Solⁿ: Each tossing of a coin results in either head or tail i.e. there are two possible outcomes for each toss.

Thus, by product rule, there are $2 \times 2 \times 2 \times 2 = \underline{2^4 \text{ ways}}$ or 2^4 different sequences of heads & tails are possible.

Q] An office building contains 27 floors and has 40 offices on each floor. How many offices are there in building?

Solⁿ: There are 27 ways to choose a floor and 27 ways to choose an office for each floor.

Thus, by product rule, there are $27 \times 40 = \underline{1080 \text{ offices}}$

Q] How many different bit strings are there of length 7?

Solⁿ: Since there are 2 bits 0 and 1

Therefore, the product rule shows there are total of $2^7 = 128$ different bit strings of length 7.

References:

1. Lipschutz, "Discrete Mathematics," McGraw-Hill

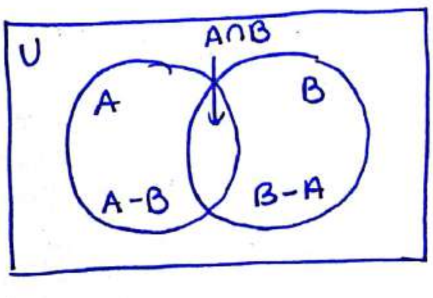
UNIT 05

LECTURE NO. 06

The Inclusion-Exclusion Principle [R1, R2]

- The counting methods Sum Rule and Product Rule can only be used if the sets are disjoint.
- However, if the sets are not disjoint, we must refine the statement of the Sum Rule to a Rule commonly called as the Principle of Inclusion-Exclusion.
- When two tasks can be done at the same time (i.e. the tasks are not disjoint), to find the number of ways to do one of the tasks, we add numbers of ways in which each task can be done and subtract the number of ways in which both tasks can be done.
- In terms of sets, this principle can be stated as

Let A and B be finite sets. Let T_1 be the task of choosing an element from A and T_2 be the task of choosing an element from B.
There are $|A|$ or $n(A)$ ways to do T1, $|B|$ or $n(B)$ ways to do B. $|A \cup B|$ ways to do T_1 or T_2 and $|A \cap B|$ ways to do to T_1 and T_2,



Then

$$\boxed{|A \cup B| = |A| + |B| - |A \cap B|}$$

is the Inclusion-Exclusion Principle.

From Venn Diagram, we can observe

$$|A \cup B| = |A-B| + |B-A| + |A \cap B| \quad \text{—— (I)}$$

where $|A| = |A-B| + |A \cap B|$ —— (II)

$|B| = |A \cap B| + |B-A|$ —— (III)

Adding (I) & (III), we get

$$|A| + |B| = |A-B| + 2|A \cap B| + |B-A|$$

i.e. $|A| + |B| = \underbrace{|A-B| + |A \cap B| + |\quad|}_{= |A \cup B| \text{ (from (I))}} + |\quad|$ —— (IV)

$\therefore$ equ^n (IV) becomes

$$|A| + |B| = |A \cup B| + |A \cap B|$$

i.e. $\boxed{|A \cup B| = |A| + |B| - |A \cap B|}$ Inclusion-Exclusion Principle

- For three sets, this principle can be stated as

For A, B & C

$$\boxed{|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap}$$

Q] How many positive integers not exceeding 100 are divisible either by 4 or by 6?

Sol^n: Integers which are divisible by 4 : 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100.

ie. 25 integers not exceeding 100 which are divisible by 4.

Similarly, Integers which are divisible by 6: 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96 ie. 16 integers i.e. $n(A) = 25$

$n(B) = 16$

Applying the Inclusion-Exclusion Principle, we get

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

$$= 25 + 16 - 8$$

$$\therefore \boxed{|A \cup B| = 33}$$

Pigeonhole Principle [R2]

- Also called as Dirichlet Drawer Principle or Shoe Box Principle.
- Pigeonhole Principle is sometimes useful in counting methods.
- The pigeon-hole principle states that if there are more pigeons than pigeonholes, then there must be atleast one pigeonhole having at least two pigeons in it.
- In the set theoretic notation, the pigeonhole principle can be stated as follows:

"If X and Y are any two finite sets such that $|X| < |Y|$ then a function $f: X \to Y$ cannot be one-one i.e there exists at least two elements x_1, x_2 in X such that $f(x_1) = f(x_2)$".

- PROOF

Let m pigeonholes be numbered with the numbers 1 to m.

Beginning with the pigeon 1, each pigeon is assigned in order to the pigeonholes with the same number.

Since $m<n$ ie. no. of pigeonholes is less than the pigeons, $n-m$ pigeons are left without having assigned a pigeonhole.

Thus, at least one pigeonhole will be assigned to a second pigeon.

- Pigeonhole Principle tells us nothing about how to locate the pigeonhole that contains two or more pigeons. It only asserts the existence of a pigeonhole containing two or more pigeons.
- This principle is also applicable to other objects besides pigeons and pigeonholes.

References:

1. Liu and Mohpatra, "Elements of Discrete Mathematics" McGraw Hill

2. Lipschutz, "Discrete Mathematics," McGraw Hill