CS- 302 Discrete Structures

Unit-I

Set Theory, Relation, Function, Theorem Proving Techniques : Set Theory: Definition of sets, countable and uncountable sets, Venn Diagrams, proofs of some general identities on sets Relation: Definition, types of relation, composition of relations, Pictorial representation of relation, Equivalence relation, Partial ordering relation, Job-Scheduling problem Function: Definition, type of functions, one to one, into and onto function, inverse function, composition of functions, recursively defined functions, pigeonhole principle. Theorem proving Techniques: Mathematical induction, Proof by contradiction.

Unit-II

Algebraic Structures: Definition, Properties, types: Semi Groups, Monoid, Groups, Abelian group, properties of groups, Subgroup, cyclic groups, Cosets, factor group, Permutation groups, Normal subgroup, Homomorphism and isomorphism of Groups, example and standard results, Rings and Fields: definition and standard results.

Unit-III

Propositional Logic: Proposition, First order logic, Basic logical operation, truth tables, tautologies, Contradictions, Algebra of Proposition, logical implications, logical equivalence, predicates, Normal Forms, Universal and existential quantifiers. Introduction to finite state machine Finite state machines as models of physical system equivalence machines, Finite state machines as language recognizers

Unit-IV

Graph Theory: Introduction and basic terminology of graphs, Planer graphs, Multigraphs and weighted graphs, Isomorphic graphs, Paths, Cycles and connectivity, Shortest path in weighted graph, Introduction to Eulerian paths and circuits, Hamiltonian paths and circuits, Graph coloring, chromatic number, Isomorphism and Homomorphism of graphs.

Unit V

Posets, Hasse Diagram and Lattices: Introduction, ordered set, Hasse diagram of partially, ordered set, isomorphic ordered set, well ordered set, properties of Lattices, bounded and complemented lattices. Combinatorics: Introduction, Permutation and combination, Binomial Theorem, Multimonial Coefficients Recurrence Relation and Generating Function: Introduction to Recurrence Relation and Recursive algorithms , Linear recurrence relations with constant coefficients, Homogeneous solutions, Particular solutions, Total solutions , Generating functions , Solution by method of generating functions,

Refereences:

1. C.L.Liu, “Elements of Discrete Mathematics” Tata Mc Graw-Hill Edition.
2. Trembley, J.P & Manohar; “Discrete Mathematical Structure with Application CS”, MH.
3. Kenneth H. Rosen, “Discrete Mathematics and its applications”, McGraw Hill.
4. Lipschutz; Discrete mathematics (Schaum); TMH
5. Deo, Narsingh, “Graph Theory With application to Engineering and Computer.Science.”, PHI.
6. Krishnamurthy V; “Combinatorics Theory & Application”, East-West Pre.Pvt. Ltd., New Delhi.
7. S k Sarkar “ Discrete Mathematics”, S. Chand Pub

Subject Notes
CS301 - Discrete Structures

Introduction

Mathematics can be broadly classified into two categories −

1. **Continuous Mathematics** − It is based upon continuous number line or the real numbers. It is characterized by the fact that between any two numbers, there are almost always an infinite set of numbers. For example, a function in continuous mathematics can be plotted in a smooth curve without breaks.
2. **Discrete Mathematics** − It involves distinct values; i.e. between any two points, there are a countable number of points. For example, if we have a finite set of objects, the function can be defined as a list of ordered pairs having these objects, and can be presented as a complete list of those pairs.

UNIT-1

Discrete Mathematics - Sets

German mathematician **G. Cantor** introduced the concept of sets. He had defined a set as a collection of definite and distinguishable objects selected by the means of certain rules or description.

Set theory forms the basis of several other fields of study like counting theory, relations, graph theory and finite state machines. In this chapter, we will cover the different aspects of **Set Theory**.

Set - Definition

A set is an unordered collection of different elements. A set can be written explicitly by listing its elements using set bracket. If the order of the elements is changed or any element of a set is repeated, it does not make any changes in the set.

Some Example of Sets

1. A set of all positive integers
2. A set of all the planets in the solar system
3. A set of all the states in India
4. A set of all the lowercase letters of the alphabet

Representation of a Set

Sets can be represented in two ways −

1. Roster or Tabular Form
2. Set Builder Notation

1. Roster or Tabular Form

The set is represented by listing all the elements comprising it. The elements are enclosed within braces and separated by commas.

Example 1 − Set of vowels in English alphabet, $A=\{a,e,i,o,u\}$

Example 2 − Set of odd numbers less than 10, $B=\{1,3,5,7,9\}$

2. Set Builder Notation

The set is defined by specifying a property that elements of the set have in common. The set is described as $A=\{x:p(x)\}$

Example 1 − The set {a,e,i,o,u}

is written as −

A={x:x is a vowel in English alphabet}

Example 2 − The set {1,3,5,7,9}

is written as −

$B=\{x:1\le x<10 \text{ and } (x\%2)\neq 0\}$

If an element x is a member of any set S, it is denoted by $x\in S$

and if an element y is not a member of set S, it is denoted by $y \notin S$.

Example 3− If $S=\{1,1.2,1.7,2\}, 1\in S$

but $1.5 \notin S$

Some Important Sets

N − the set of all natural numbers = {1,2,3,4,..... }

Z − the set of all integers = {.....,−3,−2,−1,0,1,2,3,..... }

Z$^+$ − the set of all positive integers

Q − the set of all rational numbers

R − the set of all real numbers

W − the set of all whole numbers

Types of Sets

Sets can be classified into many types. Some of which are finite, infinite, subset, universal, proper, singleton set, etc.

1. **Finite Set-** A set which contains a definite number of elements is called a finite set.

Example − $S=\{x|x\in N \text{ and } 70>x>50\}$

2. **Infinite Set-** A set which contains infinite number of elements is called an infinite set.

Example − $S=\{x|x\in N \text{ and } x>10\}$

3. **Subset-** A set X is a subset of set Y (Written as $X\subseteq Y$) if every element of X is an element of set Y.

Example 1 − Let, $X=\{1,2,3,4,5,6\}$ and $Y=\{1,2\}$. Here set Y is a subset of set X as all the elements of set Y is in set X. Hence, we can write $Y\subseteq X$

Example 2 − Let, $X=\{1,2,3\}$ and $Y=\{1,2,3\}$. Here set Y is a subset (Not a proper subset) of set X as all the elements of set Y is in set X. Hence, we can write $Y\subseteq X$

4. **Proper Subset-** The term “proper subset” can be defined as “subset of but not equal to”. A Set X is a proper subset of set Y (Written as $X\subset Y$) if every element of X is an element of set Y and $|X|<|Y|$

Example − Let, $X=\{1,2,3,4,5,6\}$ and $Y=\{1,2\}$. Here set $Y\subset X$ since all elements in Y are contained in X too and X has at least one element is more than set Y

5. **Universal Set-**It is a collection of all elements in a particular context or application. All the sets in that context or application are essentially subsets of this universal set. Universal sets are represented as U

Example − We may define U as the set of all animals on earth. In this case, set of all mammals is a subset of U, set of all fishes is a subset of U, set of all insects is a subset of U , and so on.

6. **Empty Set or Null Set-** An empty set contains no elements. It is denoted by $\emptyset$. As the number of elements in an empty set is finite, empty set is a finite set. The cardinality of empty set or null set is zero.

Example − $S=\{x|x\in N \text{ and } 7<x<8\}=\emptyset$

7. **Singleton Set or Unit Set-** Singleton set or unit set contains only one element. A singleton set is denoted by $\{s\}$

Example − $S=\{x|x\in N,\ 7<x<9\} = \{8\}$

8. **Equal Set-** If two sets contain the same elements they are said to be equal.

Example − If $A=\{1,2,6\}$ and $B=\{6,1,2\}$ they are equal as every element of set A is an element of set B and every element of set B is an element of set A.

9. **Equivalent Set-** If the cardinalities of two sets are same, they are called equivalent sets.

Example − If $A=\{1,2,6\ \}$ and $B=\{16,17,22\}$, they are equivalent as cardinality of A is equal to the cardinality of B. i.e. $|A|=|B|=3$

10. **Overlapping Set -** Two sets that have at least one common element are called overlapping sets.

In case of overlapping sets −

i. $n(A\cup B)=n(A)+n(B)-n(A\cap B)$
ii. $n(A\cup B)=n(A-B)+n(B-A)+n(A\cap B)$
iii. $n(A)=n(A-B)+n(A\cap B)$
iv. $n(B)=n(B-A)+n(A\cap B)$

Example − Let, $A=\{1,2,6\}$ and $B=\{6,12,42\}$

There is a common element ‘6’, hence these sets are overlapping sets.

11. **Disjoint Set -** Two sets A and B are called disjoint sets if they do not have even one element in common. Therefore, disjoint sets have the following properties −

$n(A\cap B)=\emptyset$

$n(A\cup B)=n(A)+n(B)$

Example − Let, $A=\{1,2,6\}$ and $B=\{7,9,14\}$ there is not a single common element, hence these sets are overlapping sets.

Cardinality of a Set

Cardinality of a set S, denoted by $|S|$, is the number of elements of the set. The number is also referred as the cardinal number. If a set has an infinite number of elements, its cardinality is ∞.

Example − $|\{1,4,3,5\}|=4, |\{1,2,3,4,5,\ldots\}|=\infty$

If there are two sets X and Y,

i. $|X|=|Y|$ denotes two sets X and Y having same cardinality. It occurs when the number of elements in X is exactly equal to the number of elements in Y. In this case, there exists a bijective function 'f' from X to Y.
ii. $X|\leq|Y$ denotes that set X's cardinality is less than or equal to set Y's cardinality. It occurs when number of elements in X is less than or equal to that of Y. Here, there exists an injective function 'f' from X to Y.
iii. $|X|<|Y|$ denotes that set X's cardinality is less than set Y's cardinality. It occurs when number of elements in X is less than that of Y. Here, the function 'f' from X to Y is injective function but not bijective.
iv. *If* $|X|\leq|Y|$ and $|X|\leq|Y|$ then $|X|=|Y|$ The sets X and Y are commonly referred as equivalent sets.

Venn Diagrams

Venn diagram, invented in 1880 by John Venn, is a schematic diagram that shows all possible logical relations between different mathematical sets.

Set Operations

Set Operations include Set Union, Set Intersection, Set Difference, Complement of Set, and Cartesian Product.

1. **Set Union -** The union of sets A and B (denoted by $A\cup B$) is the set of elements which are in A, in B, or in both A and B. Hence, $A\cup B=\{x|x\in A \text{ } OR \text{ } x\in B\}$

Example − If $A=\{10,11,12,13\}$
and B = {13,14,15}, then $A\cup B=\{10,11,12,13,14,15\}$
(The common element occurs only once)

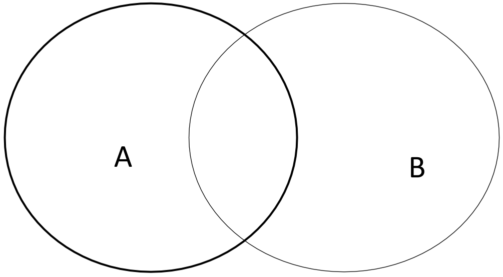


Figure 1.1 Union of two set

2. **Set Intersection -** The intersection of sets A and B (denoted by $A\cap B$) is the set of elements which are in both A and B. Hence, $A\cap B=\{x|x\in A \text{ } AND \text{ } x\in B\}$

Example − If $A=\{11,12,13\}$ and $B=\{13,14,15\}$, then $A\cap B=\{13\}$

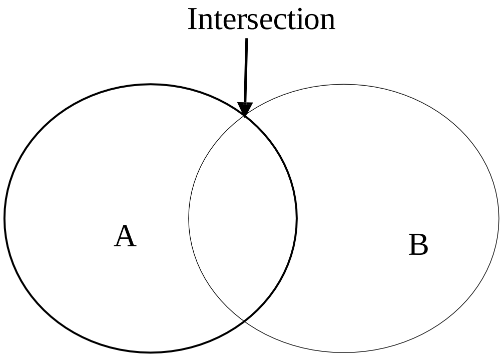


Figure 1.2 Intersection of two set

3. **Set Difference/ Relative Complement -** The set difference of sets A and B (denoted by $A-B$) is the set of elements which are only in A but not in B. Hence, $A-B=\{x|x\in A\ AND\ x ø B\}$

Example − If $A=\{10,11,12,13\}$
and $B=\{13,14,15\}$, then $(A-B)=\{10,11,12\}$ and $(B-A)=\{14,15\}$. Here, we can see $(A-B)\neq(B-A)$

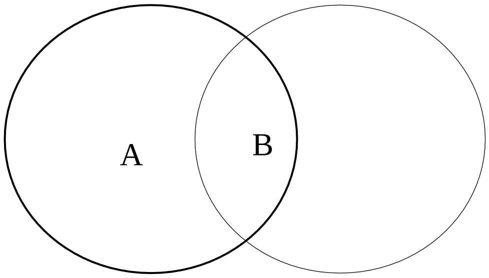


Figure 1.3 Set Difference of two set

4. **Complement of a Set -** The complement of a set A (denoted by A') is the set of elements which are not in set A. Hence, $A'=\{x|x ø A\}$

More specifically, $A'=(U-A)$ where U is a universal set which contains all objects.
Example − If A={x|x belongs to set of odd integers} then A′={y|y does not belong to set of odd integers}

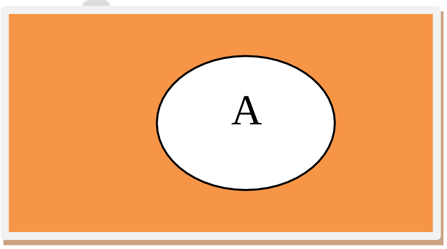


Figure 1.4 Complement of set

5. **Cartesian Product / Cross Product -** The Cartesian product of n number of sets $A1,A2,\ldots An$ denoted as $A1\times A2\cdots\times An$ can be defined as all possible ordered pairs $(x1,x2,\ldots xn)$ where $x1\in A1,x2\in A2,\ldots xn\in An$

Example − If we take two sets $A=\{a,b\}$ and $B=\{1,2\}$
The Cartesian product of A and B is written as − $A\times B=\{(a,1),(a,2),(b,1),(b,2)\}$
The Cartesian product of B and A is written as − $B\times A=\{(1,a),(1,b),(2,a),(2,b)\}$

6. **Power Set -** Power set of a set S is the set of all subsets of S including the empty set. The cardinality of a power set of a set S of cardinality n is $2n$. Power set is denoted as $P(S)$

Example –
For a set $S=\{a,b,c,d\}$
let us calculate the subsets −

i. Subsets with 0 elements − $\{\emptyset\}$ (the empty set)
ii. Subsets with 1 element − $\{a\},\{b\},\{c\},\{d\}$
iii. Subsets with 2 elements − $\{a,b\},\{a,c\},\{a,d\},\{b,c\},\{b,d\},\{c,d\}$
iv. Subsets with 3 elements − $\{a,b,c\},\{a,b,d\},\{a,c,d\},\{b,c,d\}$
v. Subsets with 4 elements − $\{a,b,c,d\}$

Hence, $P(S)=\{\{\emptyset\},\{a\},\{b\},\{c\},\{d\},\{a,b\},\{a,c\},\{a,d\},\{b,c\},\{b,d\},\{c,d\},\{a,b,c\},\{a,b,d\},\{a,c,d\},\{b,c,d\},\{a,b,c,d\}\}$

|*P*(*S*)|=24=16

Note − The power set of an empty set is also an empty set. |*P*({∅})|=20=1

Solved problems on union of sets:

1. Let A = {x : x is a natural number and a factor of 18} and B = {x : x is a natural number and less than 6}. Find A ∪ B.

Solution:

A = {1, 2, 3, 6, 9, 18}

B = {1, 2, 3, 4, 5}

Therefore, A ∪ B = {1, 2, 3, 4, 5, 6, 9, 18}

2. Let A = {0, 1, 2, 3, 4, 5}, B = {2, 4, 6, 8} and C = {1, 3, 5, 7} Verify (A ∪ B) ∪ C = A ∪ (B ∪ C)

Solution:

(A ∪ B) ∪ C = A ∪ (B ∪ C)

L.H.S. = (A ∪ B) ∪ C

A ∪ B = {0, 1, 2, 3, 4, 5, 6, 8}

(A ∪ B) ∪ C = {0, 1, 2, 3, 4, 5, 6, 7, 8} ....(1)

R.H.S. = A ∪ (B ∪ C)

B ∪ C = {1, 2, 3, 4, 5, 6, 7, 8}

A ∪ (B ∪ C) = {0, 1, 2, 3, 4, 5, 6, 7, 8} .... (2)

Therefore, from (1) and (2), we conclude that;

(A ∪ B) ∪ C = A ∪ (B ∪ C) [*verified*]

3. Let X = {1, 2, 3, 4}, Y = {2, 3, 5} and Z = {4, 5, 6}.

(i) Verify X ∪ Y = Y ∪ X **(ii) Verify (X ∪ Y) ∪ Z = X ∪ (Y ∪ Z)**

Solution:

(i) X ∪ Y = Y ∪ X

L.H.S = X ∪ Y

= {1, 2, 3, 4} ∪ {2, 3, 4} = {1, 2, 3, 4, 5}

R.H.S. = Y ∪ X

= {2, 3, 5} U {1, 2, 3, 4} = {2, 3, 5, 1, 4}

Therefore, X ∪ Y = Y ∪ X [*verified*]

(ii) (X ∪ Y) ∪ Z = X ∪ (Y ∪ Z)

L.H.S. = (X ∪ Y) ∪ Z

X ∪ Y = {1, 2, 3, 4} U {2, 3, 5}

= {1, 2, 3, 4, 5}

Now (X ∪ Y) ∪ Z

= {1, 2, 3, 4, 5, 6} {4, 5, 6}

= {1, 2, 3, 4, 5, 6}

R.H.S. = X U (Y ∪ Z)

Y ∪ Z = {2, 3, 5} ∪ {4, 5, 6}

= {2, 3, 4, 5, 6}

X ∪ (Y ∪ Z) = {1, 2, 3, 4} ∪ {2, 3, 4, 5, 6}

Therefore, (X ∪ Y) ∪ Z = X ∪ (Y ∪ Z) [*verified*]

Solved problems on intersection of sets:

1. Let A = {x : x is a natural number and a factor of 18} B = {x : x is a natural number and less than 6}

Find A ∪ B and A ∩ B.

Solution:

$A = \{1, 2, 3, 6, 9, 18\}$ $B = \{1, 2, 3, 4, 5\}$

Therefore, $A \cap B = \{1, 2, 3\}$

2. If P = {multiples of 3 between 1 and 20} and Q = {even natural numbers upto 15}. Find the intersection of the two given set P and set Q.

Solution:

P = {multiples of 3 between 1 and 20} So, $P = \{3, 6, 9, 12, 15, 18\}$

Q = {even natural numbers upto 15} So, $Q = \{2, 4, 6, 8, 10, 12, 14\}$

Therefore, intersection of P and Q is the largest set containing only those elements which are common to both the given sets P and Q

Hence, $P \cap Q = \{6, 12\}$.

3. Let $A = \{0, 1, 2, 3, 4, 5\}$, $B = \{2, 4, 6, 8\}$ and $C = \{1, 3, 5, 7\}$ Verify $(A \cap B) \cap C = A \cap (B \cap C)$

Solution:

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

L.H.S. = $(A \cap B) \cap C$

$A \cap B = \{2, 4\}$

$(A \cap B) \cap C = \{\emptyset\}$.................... (1)

R.H.S. = $A \cap (B \cap C)$

$B \cap C = \{\emptyset\}$

$A \cap \{B \cap C\} = \{\emptyset\}$.................... (2)

Therefore, from (1) and (2), we conclude that;

$(A \cap B) \cap C = A \cap (B \cap C)$ [*verified*]

4. Given three sets P, Q and R such that:

P = {x : x is a natural number between 10 and 16},

Q = {y : y is a even number between 8 and 20} and

$R = \{7, 9, 11, 14, 18, 20\}$

(i) Find the difference of two sets P and Q

(ii) Find Q - R

(iii) Find R - P

(iv) Find Q – P

Solution:

According to the given statements:

$P = \{11, 12, 13, 14, 15\}$

$Q = \{10, 12, 14, 16, 18\}$

$R = \{7, 9, 11, 14, 18, 20\}$

(i) P – Q = {Those elements of set P which are not in set Q}

$= \{11, 13, 15\}$

(ii) Q – R = {Those elements of set Q not belonging to set R}

$= \{10, 12, 16\}$

(iii) R – P = {Those elements of set R which are not in set P}

$= \{7, 9, 18, 20\}$

(iv) Q – P = {Those elements of set Q not belonging to set P}

$= \{10, 16, 18\}$

Proofs of Some General Identities on Sets-

Identities

1. **Commutative Laws:** $A \cap B = A \cap B$ and $A \cup B = B \cup A$
2. **Associative Laws:** $(A \cap B) \cap C = A \cap (B \cap C)$
   $(A \cup B) \cup C = A \cup (B \cup C)$
3. **Distributive Laws:** $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4. **Intersection and Union with universal set:** $A \cap U = A$ and $A \cup U = U$
5. **Double Complement Law:** $(A^c)^c = A$
6. **Idempotent Laws:** $A \cap A = A$ and $A \cup A = A$
7. **De Morgan's Laws:** $(A \cap B)^c = A^c \cup B^c$ and $(A \cup B)^c = A^c \cap B^c$
8. **Absorption Laws:** $A \cup (A \cap B) = A$ and $A \cap (A \cup B) = A$
9. **Alternate Representation for Difference:** $A - B = A \cap B^c$
10. **Intersection and Union with a subset:** if $A \subseteq B$, then $A \cap B = A$ and $A \cup B = B$

Some Proofs of Identities:

1. **$A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$**

Sol. $x\in A\cup(B\cap C)$

$\Leftrightarrow$ $x\in A \vee x\in(B\cap C)$

$\Leftrightarrow$ $x\in A \vee (x\in B \wedge x\in C)$

$\Leftrightarrow$ $(x\in A \vee x\in B) \wedge (x\in A \vee x\in C)$

(distributive law for logical expressions)

$\Leftrightarrow$ $x\in(A\cup B) \wedge x\in(A\cup C)$

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

2. **$A \oplus B = (A - B)$ U $(B - A)$**

Sol. $A \oplus B = \{ x : (x \in A \wedge x \notin B)$ v $(x \in B \wedge x \notin A)\}$

$= \{ x : (x \in A - B)$ v $(x \in B - A)\}$

$= \{ x : x \in ((A - B)$ U $(B - A))\}$

$= (A - B)$ U $(B - A)$

3. **Show $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.**

Sol. Assume $x\in A\cap(B\cup C)$, & show $x\in(A\cap B)\cup(A\cap C)$.

We know that $x\in A$, and either $x\in B$ or $x\in C$.

- Case 1: $x\in B$. Then $x\in A\cap B$, so $x\in(A\cap B)\cup(A\cap C)$.
- Case 2: $x\in C$. Then $x\in A\cap C$, so $x\in(A\cap B)\cup(A\cap C)$.

Therefore, $x\in(A\cap B)\cup(A\cap C)$.

Therefore, $A\cap(B\cup C)\subseteq(A\cap B)\cup(A\cap C)$.

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

Sol. $(x \in \overline{A\cup B})$

$\Rightarrow (x \notin (A$ U $B))$

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

$\Rightarrow (x \in \overline{A}\cap\overline{B})$

$(x \in(\overline{A}\cap\overline{B}))$

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

$\Rightarrow (x \notin A$ U $B)$

$\Rightarrow (x \in \overline{A \cup B})$

Problems on Operation on Sets

1. If A = {1, 3, 5}, B = {3, 5, 6} and C = {1, 3, 7}

(i) Verify that A ∪ (B ∩ C) = (A ∪ B) ∩ (A ∪ C)

(ii) Verify A ∩ (B ∪ C) = (A ∩ B) ∪ (A ∩ C)

Solution:

(i) A ∪ (B ∩ C) = (A ∪ B) ∩ (A ∪ C)

L.H.S. = A ∪ (B ∩ C)

B ∩ C = {3}

A ∪ (B ∩ C) = {1, 3, 5} ∪ {3} = {1, 3, 5}....................(1)

R.H.S. = (A ∪ B) ∩ (A ∪ C)

A ∪ B = {1, 3, 5, 6}

A ∪ C = {1, 3, 5, 7}

(A ∪ B) ∩ (A ∪ C) = {1, 3, 5, 6} ∩ {1, 3, 5, 7} = {1, 3, 5}........................(2)

From (1) and (2), we conclude that;

A ∪ (B ∩ C) = A ∪ B ∩ (A ∪ C) [*verified*]

(ii) A ∩ (B ∪ C) = (A ∩ B) ∪ (A ∩ C)

L.H.S. = A ∩ (B ∪ C)

B ∪ C = {1, 3, 5, 6, 7}

A ∩ (B ∪ C) = {1, 3, 5} ∩ {1, 3, 5, 6, 7} = {1, 3, 5} .... (1)

R.H.S. = (A ∩ B) ∪ (A ∩ C)

A ∩ B = {3, 5}

A ∩ C = {1, 3}

(A ∩ B) ∪ (A ∩ C) = {3, 5} ∪ {1, 3} = {1, 3, 5}.......................(2)

From (1) and (2), we conclude that;

A ∩ (B ∪ C) = (A ∩ B) ∪ (A ∩ C) [*verified*]

2. Let A = {a, b, d, e}, B = {b, c, e, f} and C = {d, e, f, g}

(i) Verify A ∩ (B ∪ C) = (A ∩ B) ∪ (A ∩ C)

(ii) Verify A ∪ (B ∩ C) = (A ∪ B) ∩ (A ∪ C)

Solution:

(i) A ∩ (B ∪ C) = (A ∩ B) ∪ (A ∩ C)

L.H.S. = A ∩ (B ∪ C)

B ∪ C = {b, c, d, e, f, g}

A ∩ (B ∪ C) = {b, d, e} .... (1)

R.H.S. = (A ∩ B) ∪ (A ∩ C)

A ∩ B = {b, e}

A ∩ C = {d, e}

(A ∩ B) ∪ (A ∩ C) = {b, d, e}........................(2)

From (1) and (2), we conclude that;

A ∩ (B ∪ C) = (A ∩ B) ∪ (A ∩ C) [*verified*]

(ii) A ∪ (B ∩ C) = (A ∪ B) ∩ (A ∪ C)

L.H.S. = A ∪ (B ∩ C)

B ∩ C = {e, f}

A ∪ (B ∩ C) = {a, b, d, e, f} .... (1)

R.H.S. = (A ∪ B) ∩ (A ∪ C)

A∪B = {a, b, c, d, e, f}
A∪C = {a, b, d, e, f, g}
(A ∪ B) ∩ (A ∪ C) = {a, b, d, e, f}....................... (2)
From (1) and (2), we conclude that;
A ∪ (B ∩ C) = A ∪ B ∩ (A ∪ C) [*verified*]

The Inclusion-Exclusion principle

The **Inclusion-exclusion principle** computes the cardinal number of the union of multiple non-disjoint sets. For two sets A and B, the principle states −

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

For three sets A, B and C, the principle states −

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

The generalized formula –

$$|\bigcup_{i=1}^{n} A_i|=\sum_{1\le i<j<k\le n}|A_i\cap A_j|+\sum_{1\le i<j<k\le n}|A_i\cap A_j\cap A_k|-\cdots+(-1)^{\pi-1}|A_1\cap\cdots\cap A_2|$$

Numerical on Sets:-

1. **Let A and B be two finite sets such that n(A) = 20, n(B) = 28 and n(A ∪ B) = 36, find n(A ∩ B).**

Solution:

Using the formula n(A ∪ B) = n(A) + n(B) - n(A ∩ B).
then n(A ∩ B) = n(A) + n(B) - n(A ∪ B)
= 20 + 28 - 36
= 48 - 36
= 12

2. If n(A - B) = 18, n(A ∪ B) = 70 and n(A ∩ B) = 25, then find n(B).

Solution:

Using the formula n(A∪B) = n(A - B) + n(A ∩ B) + n(B - A)
70 = 18 + 25 + n(B - A)
70 = 43 + n(B - A)
n(B - A) = 70 - 43
n(B - A) = 27
Now n(B) = n(A ∩ B) + n(B - A)
= 25 + 27
= 52

3. In a group of 60 people, 27 like cold drinks and 42 like hot drinks and each person likes at least one of the two drinks. How many like both coffee and tea?

Solution:

Let A = Set of people who like cold drinks.
B = Set of people who like hot drinks.
Given
(A ∪ B) = 60   n(A) = 27   n(B) = 42 then;
n(A ∩ B) = n(A) + n(B) - n(A ∪ B)
= 27 + 42 - 60
= 69 - 60 = 9
Therefore, 9 people like both tea and coffee.

4. There are 35 students in art class and 57 students in dance class. Find the number of students who are either in art class or in dance class.

(i) When two classes meet at different hours and 12 students are enrolled in both activities.

(ii) When two classes meet at the same hour.

Solution:

n(A) = 35,   n(B) = 57,   n(A ∩ B) = 12

(Let A be the set of students in art class.
B be the set of students in dance class.)

(i) When 2 classes meet at different hours $n(A \cup B) = n(A) + n(B) - n(A \cap B)$
$= 35 + 57 - 12$
$= 92 - 12$
$= 80$

(ii) When two classes meet at the same hour, $A \cap B = \emptyset$ $n(A \cup B) = n(A) + n(B) - n(A \cap B)$
$= n(A) + n(B)$
$= 35 + 57$
$= 92$

5. In a group of 100 persons, 72 people can speak English and 43 can speak French. How many can speak English only? How many can speak French only and how many can speak both English and French?

Solution:

Let A be the set of people who speak English.
B be the set of people who speak French.
A - B be the set of people who speak English and not French.
B - A be the set of people who speak French and not English.
$A \cap B$ be the set of people who speak both French and English.

Given,

$n(A) = 72$ $n(B) = 43$ $n(A \cup B) = 100$

Now, $n(A \cap B) = n(A) + n(B) - n(A \cup B)$
$= 72 + 43 - 100$
$= 115 - 100$
$= 15$

Therefore, Number of persons who speak both French and English = 15

$n(A) = n(A - B) + n(A \cap B)$
$\Rightarrow n(A - B) = n(A) - n(A \cap B)$
$= 72 - 15$
$= 57$

and $n(B - A) = n(B) - n(A \cap B)$
$= 43 - 15$
$= 28$

Therefore, Number of people speaking English only = 57
Number of people speaking French only = 28

6. In a competition, a school awarded medals in different categories. 36 medals in dance, 12 medals in dramatics and 18 medals in music. If these medals went to a total of 45 persons and only 4 persons got medals in all the three categories, how many received medals in exactly two of these categories?

Solution:

Let A = set of persons who got medals in dance.

B = set of persons who got medals in dramatics.
C = set of persons who got medals in music.

Given,

$n(A) = 36$ $n(B) = 12$ $n(C) = 18$
$n(A \cup B \cup C) = 45$ $n(A \cap B \cap C) = 4$

We know that number of elements belonging to exactly two of the three sets A, B, C
$= n(A \cap B) + n(B \cap C) + n(A \cap C) - 3n(A \cap B \cap C)$
$= n(A \cap B) + n(B \cap C) + n(A \cap C) - 3 \times 4$..............(i)

$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(B \cap C) - n(A \cap C) + n(A \cap B \cap C)$

Therefore, $n(A \cap B) + n(B \cap C) + n(A \cap C) = n(A) + n(B) + n(C) + n(A \cap B \cap C) - n(A \cup B \cup C)$

From (i) required number

$= n(A) + n(B) + n(C) + n(A \cap B \cap C) - n(A \cup B \cup C) - 12$

$= 36 + 12 + 18 + 4 - 45 - 12$

$= 70 - 67$

$= 3$

7. Each student in a class of 40 plays at least one indoor game chess, carrom and scrabble. 18 play chess, 20 play scrabble and 27 play carrom. 7 play chess and scrabble, 12 play scrabble and carrom and 4 play chess, carrom and scrabble. Find the number of students who play (i) chess and carrom. (ii) chess, carrom but not scrabble.

Solution:

Let A be the set of students who play chess

B be the set of students who play scrabble

C be the set of students who play carrom

Therefore, We are given $n(A \cup B \cup C) = 40$,

$n(A) = 18$, $n(B) = 20$ $n(C) = 27$,

$n(A \cap B) = 7$, $n(C \cap B) = 12$ $n(A \cap B \cap C) = 4$

We have

$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(B \cap C) - n(C \cap A) + n(A \cap B \cap C)$

Therefore, $40 = 18 + 20 + 27 - 7 - 12 - n(C \cap A) + 4$

$40 = 69 – 19 - n(C \cap A)$

$40 = 50 - n(C \cap A)$ $n(C \cap A) = 50 - 40$

$n(C \cap A) = 10$

Therefore, Number of students who play chess and carrom are 10.

Also, number of students who play chess, carrom and not scrabble

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

$= 10 – 4$

$= 6$

Relations

Whenever sets are being discussed, the relationship between the elements of the sets is the next thing that comes up. **Relations** may exist between objects of the same set or between objects of two or more sets.

Definition and Properties

A binary relation R from set x to y (written as xRy or $R(x,y)$) is a subset of the Cartesian product $x \times y$. If the ordered pair of G is reversed, the relation also changes. Generally an n-ary relation R between sets $A1, \ldots,$ *and* An is a subset of the n-ary product $A1 \times \cdots \times An$. The minimum cardinality of a relation R is Zero and maximum is $n2$ in this case. A binary relation R on a single set A is a subset of $A \times A$

For two distinct sets, A and B, having cardinalities m and n respectively, the maximum cardinality of a relation R from A to B is mn.

Domain and Range

If there are two sets A and B, and relation R have order pair (x, y), then −

i. The **domain** of R, Dom(R), is the set {x|(x,y) ∈ Rfor some y in B}

ii. The **range** of R, Ran(R), is the set {y|(x,y) ∈ R for some x inA}

Examples Let, $A=\{1,2,9\}$ and $B=\{1,3,7\}$

Case 1 − If relation R is 'equal to' then $R=\{(1,1),(3,3)\}$

Dom(R) = {1,3},$Ran(R)=\{1,3\}$

Case 2 − If relation R is 'less than' then $R=\{(1,3),(1,7),(2,3),(2,7)\}$
Dom(R) = {1,2},$Ran(R)=\{3,7\}$
Case 3 − If relation R is 'greater than' then $R=\{(2,1),(9,1),(9,3),(9,7)\}$
Dom(R) = {2,9},$Ran(R)=\{1,3,7\}$

Properties of Relation

1. **Reflexive :** A relation R on a set A is called **reflexive** if (a, a)∈R for every element a∈A. **Example :** Are the following relations on {1, 2, 3, 4} reflexive?
   1. R = {(1, 1), (1, 2), (2, 3), (3, 3), (4, 4)} No
   2. R = {(1, 1), (2, 2), (2, 3), (3, 3), (4, 4)} Yes
   3. R = {(1, 1), (2, 2), (3, 3)} No
2. **Irreflexive :** A relation on a set A is called **irreflexive** if (a, a)∉R for every element a∈A.
3. **Symmetric :** A relation R on a set A is called **symmetric** if (b, a)∈R whenever (a, b)∈R for all a, b∈A.
4. **Asymmetric :** A relation R on a set A is called **asymmetric** if (a, b)∈R implies that (b, a)∉R for all a, b∈A.
5. **Antisymmetric :** A relation R on a set A is called **antisymmetric** if a = b whenever (a, b)∈R and (b, a)∈R.

Types of Relations

1. The **Empty Relation** between sets X and Y, or on E, is the empty set ∅
2. The **Full Relation** between sets X and Y is the set $X\times Y$
3. The **Identity Relation** on set X is the set $\{(x,x)|x\in X\}$
4. The Inverse Relation R' of a relation R is defined as − $R'=\{(b,a)|(a,b)\in R\}$

Example − If $R=\{(1,2),(2,3)\}$ then R' will be $\{(2,1),(3,2)\}$

Composition of Relation

Definition: Let R be a relation from the set A to B and S be a relation from B to C, i.e. R ⊆ A×B and S ⊆B×C the composite of *R* and S is the relation consisting of ordered pairs (a,c) where a∈A, c∈C and for which there exists an element b∈B such that (a,b)∈R and (b,c)∈S. We denote the composite of R and S by R ᵒ S

$(a,b)\in S\circ R \leftrightarrow \exists x:(a,x)\in R\wedge (x,b)\in S$

Note $(a,b)\in R\wedge (b,c)\in S\rightarrow (a,c)\in S\circ R$

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

$S=\{(1,0),(2,0),(3,1),(3,2),(4,1)\}$

$S\circ R=\{(1,0),(1,1),(2,1),(2,2),(3,0),(3,1)\}$

Representation of Relations using Graph

A relation can be represented using a directed graph. The number of vertices in the graph is equal to the number of elements in the set from which the relation has been defined. For each ordered pair (x, y) in the relation R, there will be a directed edge from the vertex ‘x’ to vertex ‘y’. If there is an ordered pair (x, x), there will be self- loop on vertex ‘x’.

Suppose, there is a relation $R=\{(1,1),(1,2),(3,2)\}$ on set $S=\{1,2,3\}$, it can be represented by the following graph –

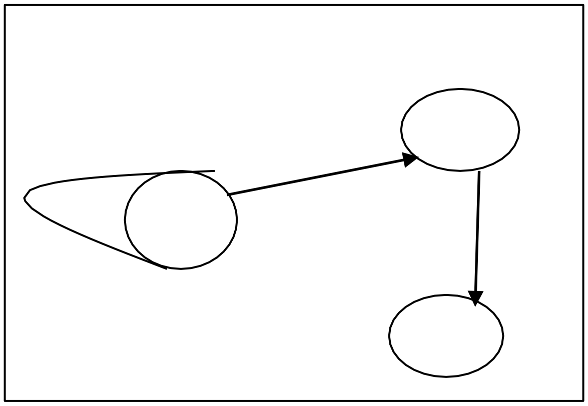


Figure 1.5 Relation as a graph

Equivalance Relation

Equivalence relation on set is a relation which is reflexive, symmetric and transitive.

A relation R, defined in a set A, is said to be an equivalence relation if and only if

(i) R is reflexive, that is, aRa for all a ∈ A.

(ii) R is symmetric, that is, aRb ⇒ bRa for all a, b ∈ A.

(iii) R is transitive, that is aRb and bRc ⇒ aRc for all a, b, c ∈ A.

Partial Order Relation

Partial order relation on set is a relation which is reflexive, antisymmetric and transitive.

A relation R, defined in a set A, is said to be an equivalence relation if and only if

(i) R is reflexive, that is, aRa for all a ∈ A.

(ii) R isantisymmetric if a = b whenever (a, b)∈R and (b, a)∈R

(iii) R is transitive, that is aRb and bRc ⇒ aRc for all a, b, c ∈ A.

A Job Scheduling Problem

We consider the problem of scheduling the execution of a set of a tasks on a multiprocessor computing system which has a set of identical processors.

Job Scheduling Problem means to make a schedule for a finite no. of workers to complete a given set of task.

Let T={T1 , T2 , T3 ---------------Tn } denote a set of tasks to be executed on the computing system. Suppose that the execution of a task occupies one and only one processor. Moreover since the processors are identical, a task can be executed on any one of the processors. Let P(Ti) denoted the execution time of task Ti , the amount of time it takes to execute Ti on a processor. Ti ≠ Tj , Ti ≤ Tj if and only if the execution of task Tj cannot begin until the execution of task Ti has been completed.

Functions

A **Function** assigns to each element of a set, exactly one element of a related set. Functions find their application in various fields like representation of the computational complexity of algorithms, counting objects, study of sequences and strings, to name a few. The third and final chapter of this part highlights the important aspects of functions.

Function - Definition

A function or mapping (Defined as $f:X\rightarrow Y$) is a relationship from elements of one set X to elements of another set Y (X and Y are non-empty sets). X is called Domain and Y is called Codomain of function 'f'. Function 'f' is a relation on X and Y such that for each $x\in X$, there exists a unique $y\in Y$ such that $(x,y)\in R$. 'x' is called pre-image and 'y' is called image of function f. A function can be one to one or many to one but not one to many.

1. **Injective / One-to-one function-** A function $f:A \rightarrow B$ is injective or one-to-one function if for every $b \in B$, there exists at most one $a \in A$ such that $f(s)=t$. This means a function **f** is injective if $a1 \neq a2$ implies $f(a1) \neq f(a2)$

Example

a) $f:N \rightarrow N, f(x)=5x$ is injective.

b) $f:N \rightarrow N, f(x)=x2$ is injective.

c) $f:R \rightarrow R, f(x)=x2$ is not injective as $(-x)2=x2$

2. **Surjective / Onto function -** A function $f:A \rightarrow B$ is surjective (onto) if the image of f equals its range. Equivalently, for every $b \in B$, there exists some $a \in A$ such that $f(a)=b$. This means that for any y in B, there exists some x in A such that $y=f(x)$

Example

a) $f:N \rightarrow N, f(x)=x+2$ is surjective.

b) $f:R \rightarrow R, f(x)=x2$ is not surjective since we cannot find a real number whose square is negative.

3. **Bijective / One-to-one Correspondent** - A function $f:A \rightarrow B$ is bijective or one-to-one correspondent if and only if **f** is both injective and surjective.

Problem - Prove that a function $f:R \rightarrow R$ defined by $f(x)=2x-3$ is a bijective function.

Explanation − We have to prove this function is both injective and surjective.

If $f(x1)=f(x2)$, then $2x1-3=2x2-3$ and it implies that $x1=x2$. Hence, f is **injective**.

Here, $2x-3=y$

So, $x=(y+5)/3$ which belongs to R and $f(x)=y$. Hence, f is **surjective**.

Since **f** is both **surjective** and **injective**, we can say **f** is **bijective**.

4. **Inverse of a Function -** The **inverse** of a one-to-one corresponding function $f:A \rightarrow B$, is the function $g:B \rightarrow A$, holding the following property − $f(x)=y \Leftrightarrow g(y)=x$ The function f is called **invertible**, if its inverse function g exists.

Example

A Function $f:Z \rightarrow Z, f(x)=x+5$, is invertible since it has the inverse function $g:Z \rightarrow Z, g(x)=x-5$.

A Function $f:Z \rightarrow Z, f(x)=x2$ is not invertiable since this is not one-to-one as $(-x)2=x2$

Composition of Functions

Two functions $f:A \rightarrow B$ and $g:B \rightarrow C$ can be composed to give a composition *gof*. This is a function from A to C defined by $(gof)(x)=g(f(x))$

Example

Let $f(x)=x+2$

and $g(x)=2x$, find $(fog)(x)$ and $(gof)(x)$

.

Solution

$(fog)(x)=f(g(x))=f(2x+1)=2x+1+2=2x+3$

$(gof)(x)=g(f(x))=g(x+2)=2(x+2)+1=2x+5$

Hence, $(fog)(x) \neq (gof)(x)$

Some Facts about Composition

a) If f and g are one-to-one then the function (*gof*) is also one-to-one.

b) If f and g are onto then the function (*gof*) is also onto.

c) Composition always holds associative property but does not hold commutative property.

Example : Let f:R->R be defined by f(x)= 2x+1, x<=0; x^2+1 ,x>0

Let g:R->R be defined by g(x)=3x-7 , x<=0; x^3, x>0

Then find the composition gof. :

Solution:

Let x = -2,-1,0,1,2,3…….

For x =-2,-1,0	for x= 1,2,3….
$F(x)=2x+1$	$f(x)= x^2+1$
$F(-2)= -3$	$f(1)=2$
$F(-1)= 0$	$f(2)=5$
$F(0)= 1$	$f(3)= 10$

Let x = -2,-1,0,1,2,3…….

For x =-2,-1,0	for x= 1,2,3….
$G(x)=3x-7$	$g(x)=x^3$
$G(-1)=-10$	$g(1)=1$
$G(-2)=-13$	$g(2)=8$
$G(0)=-7$	$g(3)=27$

Gof=g[f(x)]

G[f(-2)]=g(-3)=-16

G[f(-1)] =g(0)=-7

G[f(0)] =g(1)=1

G[f(1)] =g(2)=8

G[f(2)] =g(5)=125

G[f(3)] =g(10)=1000…………

Pigeonhole principle

If the number of pigeon is more than the number of pigeonholes, then some pigeonhole must be occupied by two or more than two pigeons. This statement is called the Pigeon hole principle, it is also called Dirchlet Drawer Principle. This statement is also written as "**If n pigeonholes are occupied by n + 1 or more pigeons, then at least one pigeonhole is occupied by more than one pigeon**".

Example 1 Among 13 people there are two who have their birthdays in the same month.

Example 2 A basket of fruit is being arranged out of apples, bananas, and oranges. What is the smallest number of pieces of fruit that should be put in the basket in order to guarantee that either there are at least 8 apples or at least 6 bananas or at least 9 oranges? Answer: $8 + 6 + 9 - 3 + 1 = 21$.

Mathematical Induction

Mathematical induction, is a technique for proving results or establishing statements for natural numbers. This part illustrates the method through a variety of examples.

Definition Let P(n) be a mathematical statement about nonnegative integers n and n be a fixed nonnegative integer.

(1) Suppose **P(no)** is true i.e.. P(n) is true for n = **no**.

2) Whenever **k** is an integer such that **k ≥ no and P(k)** is **true**, then **P(k + 1)** is true.

Then **P(n)** is true for all integers n ≥ no.

We note that a proof by mathematical induction consists of three steps.

Step 1. (Basis) Show that P(no) is true.

Step 2. (Inductive hypothesis). Write the inductive hypothesis: Let k be an integer such that k ≥ no and P(k) be true.

Step 3. (Inductive step). Show that P(k + 1) is true.

Numericals on Mathematical Induction

1. Using the principle of mathematical induction, prove that

$$1^2 + 2^2 + 3^2 + ... + n^2 = (1/6)\{n(n + 1)(2n + 1\} \text{ for all } n \in N.$$

Solution : Let the given statement be P(n). Then,

P(n): $1^2 + 2^2 + 3^2 + ...+n^2 = (1/6)\{n(n + 1)(2n + 1)\}$.

Putting n =1 in the given statement, we get

LHS = $1^2 = 1$ and RHS = $(1/6) \times 1 \times 2 \times (2 \times 1 + 1) = 1$.

Therefore LHS = RHS.

Thus, P(1) is true.
Let P(k) be true. Then,

P(k): $1^2 + 2^2 + 3^2 + ... + k^2 = (1/6)\{k(k + 1)(2k + 1)\}$.

Now, $1^2 + 2^2 + 3^2 + ... + k^2 + (k + 1)^2$

$= (1/6) \{k(k + 1)(2k + 1) + (k + 1)^2$

$= (1/6)\{(k + 1).(k(2k + 1)+6(k + 1))\}$

$= (1/6)\{(k + 1)(2k^2 + 7k + 6\})$

$= (1/6)\{(k + 1)(k + 2)(2k + 3)\}$

$= 1/6\{(k + 1)(k + 1 + 1)[2(k + 1) + 1]\}$

$\Rightarrow$ P(k + 1): $1^2 + 2^2 + 3^2 +...... + k^2 + (k+1)^2$

$= (1/6)\{(k + 1)(k + 1 + 1)[2(k + 1) + 1]\}$

$\Rightarrow$ P(k + 1) is true, whenever P(k) is true.

Thus, P(1) is true and P(k + 1) is true, whenever P(k) is true.

Hence, by the principle of mathematical induction, P(n) is true for all n ∈ N.

2. Using the principle of mathematical induction, prove that

$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 +....... + n(n + 1) = (1/3)\{n(n + 1)(n + 2)\}$.

Solution : Let the given statement be P(n). Then,

P(n): $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + ... + n(n + 1) = (1/3)\{n(n + 1)(n + 2)\}$.

Thus, the given statement is true for n = 1, i.e., P(1) is true.

Let P(k) be true. Then,

$P(k): 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots\ldots + k(k + 1) = (1/3)\{k(k + 1)(k + 2)\}.$

Now, $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 +. \ + k(k + 1) + (k + 1)(k + 2)$

$= (1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 +\ldots\ldots\ldots+ k(k + 1)) + (k + 1)(k + 2)$

$= (1/3)\ k(k + 1)(k + 2) + (k + 1)(k + 2)$ [using (i)]

$= (1/3)\ [k(k + 1)(k + 2) + 3(k + 1)(k + 2)$

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

$\Rightarrow P(k + 1): 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 +. \ldots. + (k + 1)(k + 2)$

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

$\Rightarrow P(k + 1)$ is true, whenever $P(k)$ is true.

Thus, $P(1)$ is true and $P(k + 1)$is true, whenever $P(k)$ is true.

Hence, by the principle of mathematical induction, $P(n)$ is true for all values of $\in N$.

3. Using the principle of mathematical induction, prove that

$1 \cdot 3 + 3 \cdot 5 + 5 \cdot 7 +\ldots.. + (2n - 1)(2n + 1) = (1/3)\{n(4n^2 + 6n - 1).$

Solution : Let the given statement be $P(n)$. Then,

$P(n): 1 \cdot 3 + 3 \cdot 5 + 5 \cdot 7 +. \ldots.. + (2n - 1)(2n + 1)= (1/3)n(4n^2 + 6n - 1).$

When $n = 1$, LHS $= 1 \cdot 3 = 3$ and RHS $= (1/3) \times 1 \times (4 \times 1^2 + 6 \times 1 - 1)$

$= \{(1/3) \times 1 \times 9\} = 3.$

LHS = RHS.

Thus, $P(1)$ is true.

Let $P(k)$ be true. Then,

$P(k): 1 \cdot 3 + 3 \cdot 5 + 5 \cdot 7 + \ldots.. + (2k - 1)(2k + 1) = (1/3)\{k(4k^2 + 6k - 1)\ldots\ldots.$ (i)

Now,

$1 \cdot 3 + 3 \cdot 5 + 5 \cdot 7 +\ldots\ldots\ldots+ (2k - 1)(2k + 1) + \{2k(k + 1) - 1\}\{2(k + 1) + 1\}$

$= \{1 \cdot 3 + 3 \cdot 5 + 5 \cdot 7 + \ldots\ldots\ldots\ldots+ (2k - 1)(2k + 1)\} + (2k + 1)(2k + 3)$

$= (1/3)\ k(4k^2 + 6k - 1) + (2k + 1)(2k + 3)$ [using (i)]

$= (1/3)\ [(4k^3 + 6k^2 - k) + 3(4k^2 + 8k + 3)]$

$= (1/3)(4k^3 + 18k^2 + 23k + 9)$

$= (1/3)\{(k + 1)(4k^2 + 14k + 9)\}$

$= (1/3)[k + 1)\{4k(k + 1)^2 + 6(k + 1) - 1\}]$

$\Rightarrow$ $P(k + 1){:}\ 1 \cdot 3 + 3 \cdot 5 + 5 \cdot 7 + \ldots\ldots + (2k + 1)(2k + 3)$

$= (1/3)[(k + 1)\{4(k + 1)^2 + 6(k + 1) - 1)\}]$

$\Rightarrow$ P(k + 1) is true, whenever P(k) is true.

Thus, P(1) is true and P(k + 1) is true, whenever P(k) is true.

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

4. Using the principle of mathematical induction, prove that

$1/(1 \cdot 2) + 1/(2 \cdot 3) + 1/(3 \cdot 4) + \ldots\ldots + 1/\{n(n + 1)\} = n/(n + 1)$

Solution : Let the given statement be P(n). Then,

$P(n){:}\ 1/(1 \cdot 2) + 1/(2 \cdot 3) + 1/(3 \cdot 4) + \ldots\ldots + 1/\{n(n + 1)\} = n/(n + 1).$

Putting n = 1 in the given statement, we get

LHS= $1/(1 \cdot 2) =$ and RHS = $1/(1 + 1) = 1/2$.

LHS = RHS.

Thus, P(1) is true.

Let P(k) be true. Then,

$P(k){:}\ 1/(1 \cdot 2) + 1/(2 \cdot 3) + 1/(3 \cdot 4) + \ldots.. + 1/\{k(k + 1)\} = k/(k + 1)$ ..... (i)

Now $1/(1 \cdot 2) + 1/(2 \cdot 3) + 1/(3 \cdot 4) + \ldots\ldots + 1/\{k(k + 1)\} + 1/\{(k + 1)(k + 2)\}$

$[1/(1 \cdot 2) + 1/(2 \cdot 3) + 1/(3 \cdot 4) + \ldots\ldots + 1/\{k(k + 1)\}] + 1/\{(k + 1)(k + 2)\}$

$= k/(k + 1)+1/\{\ (k + 1)(k + 2)\}.$

$\{k(k + 2) + 1\}/\{(k + 1)^2/[(k + 1)k + 2)]$ using …(ii)

$= \{k(k + 2) + 1\}/\{(k + 1)(k + 2\}$

$= \{(k + 1)^2 \}/\{(k + 1)(k + 2)\}$

$= (k + 1)/(k + 2) = (k + 1)/(k + 1 + 1)$

⇒ $P(k + 1): 1/(1 \cdot 2) + 1/(2 \cdot 3) + 1/(3 \cdot 4) + \ldots\ldots\ldots + 1/\{ k(k + 1)\} + 1/\{(k + 1)(k + 2)\}$

$= (k + 1)/(k + 1 + 1)$

⇒ $P(k + 1)$ is true, whenever $P(k)$ is true.

Thus, $P(1)$ is true and $P(k + 1)$is true, whenever $P(k)$ is true.

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

5. Using the principle of mathematical induction, prove that

$\{1/(3 \cdot 5)\} + \{1/(5 \cdot 7)\} + \{1/(7 \cdot 9)\} + \ldots\ldots\ldots + 1/\{(2n + 1)(2n + 3)\} = n/\{3(2n + 3)\}$.

Solution : Let the given statement be $P(n)$. Then,

$P(n): \{1/(3 \cdot 5) + 1/(5 \cdot 7) + 1/(7 \cdot 9) + \ldots\ldots\ldots + 1/\{(2n + 1)(2n + 3)\} = n/\{3(2n + 3)$.

Putting $n = 1$ in the given statement, we get

and LHS $= 1/(3 \cdot 5) = 1/15$ and RHS $= 1/\{3(2 \times 1 + 3)\} = 1/15$.

LHS = RHS

Thus , $P(1)$ is true.

Let $P(k)$ be true. Then,

$P(k): \{1/(3 \cdot 5) + 1/(5 \cdot 7) + 1/(7 \cdot 9) + \ldots\ldots\ldots + 1/\{(2k + 1)(2k + 3)\} = k/\{3(2k + 3)\}$.......(i)

Now, $1/(3 \cdot 5) + 1/(5 \cdot 7) + \ldots\ldots\ldots + 1/[(2k + 1)(2k + 3)] + 1/[\{2(k + 1) + 1\}2(k + 1) + 3$

$= \{1/(3 \cdot 5) + 1/(5 \cdot 7) + \ldots\ldots + [1/(2k + 1)(2k + 3)]\} + 1/\{(2k + 3)(2k + 5)\}$

$= k/[3(2k + 3)] + 1/[2k + 3)(2k + 5)]$ [using (i)]

$= \{k(2k + 5) + 3\}/\{3(2k + 3)(2k + 5)\}$

$= (2k^2 + 5k + 3)/[3(2k + 3)(2k + 5)]$

$= \{(k + 1)(2k + 3)\}/\{3(2k + 3)(2k + 5)\}$

$= (k + 1)/\{3(2k + 5)\}$

$= (k + 1)/[3\{2(k + 1) + 3\}]$

$= P(k + 1): 1/(3 \cdot 5) + 1/(5 \cdot 7) + \dots\dots\dots + 1/[2k + 1)(2k + 3)] + 1/[\{2(k + 1) + 1\}\{2(k + 1) + 3\}]$

$= (k + 1)/\{3\{2(k + 1) + 3\}]$

$\Rightarrow P(k + 1)$ is true, whenever $P(k)$ is true.

Thus, $P(1)$ is true and $P(k + 1)$ is true, whenever $P(k)$ is true.

Hence, by the principle of mathematical induction, $P(n)$ is true for $n \in N$.

6. Using the principle of mathematical induction, prove that

$1/(1 \cdot 2 \cdot 3) + 1/(2 \cdot 3 \cdot 4) + \dots\dots\dots + 1/\{n(n + 1)(n + 2)\} = \{n(n + 3)\}/\{4(n + 1)(n + 2)\}$ for all $n \in N$.

Solution : Let $P(n): 1/(1 \cdot 2 \cdot 3) + 1/(2 \cdot 3 \cdot 4) + \dots\dots\dots + 1/\{n(n + 1)(n + 2)\} = \{n(n + 3)\}/\{4(n + 1)(n + 2)\}$. Putting $n = 1$ in the given statement, we get

LHS $= 1/(1 \cdot 2 \cdot 3) = 1/6$ and RHS $= \{1 \times (1 + 3)\}/[4 \times (1 + 1)(1 + 2)] = (1 \times 4)/(4 \times 2 \times 3) = 1/6$.

Therefore LHS = RHS.

Thus, the given statement is true for $n = 1$, i.e., $P(1)$ is true.

Let $P(k)$ be true. Then,

$P(k): 1/(1 \cdot 2 \cdot 3) + 1/(2 \cdot 3 \cdot 4) + \dots\dots\dots + 1/\{k(k + 1)(k + 2)\} = \{k(k + 3)\}/\{4(k + 1)(k + 2)\} \dots\dots\dots$ (i)

Now, $1/(1 \cdot 2 \cdot 3) + 1/(2 \cdot 3 \cdot 4) + \dots\dots\dots\dots\dots + 1/\{k(k + 1)(k + 2)\} + 1/\{(k + 1)(k + 2)(k + 3)\}$

$= [1/(1 \cdot 2 \cdot 3) + 1/(2 \cdot 3 \cdot 4) + \dots\dots\dots\dots\dots + 1/\{ k(k + 1)(k + 2\}] + 1/\{(k + 1)(k + 2)(k + 3)\}$

$= [\{k(k + 3)\}/\{4(k + 1)(k + 2)\} + 1/\{(k + 1)(k + 2)(k + 3)\}]$
[using(i)]

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

$= (k^3 + 6k^2 + 9k + 4)/\{4(k + 1)(k + 2)(k + 3)\}$

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

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

$\Rightarrow P(k + 1): 1/(1 \cdot 2 \cdot 3) + 1/(2 \cdot 3 \cdot 4) + \dots\dots\dots\dots\dots + 1/\{(k + 1)(k + 2)(k + 3)\}$

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

$\Rightarrow P(k + 1)$ is true, whenever $P(k)$ is true.

Thus, P(1) is true and P(k + 1) is true, whenever P(k) is true.

Hence, by the principle of mathematical induction, P(n) is true for all n ∈ N.

7. Using the Principle of mathematical induction, prove that

{1 - (1/2)}{1 - (1/3)}{1 - (1/4)}........ **{1 - 1/(n + 1)} = 1/(n + 1) for all n ∈ N.**

Solution : Let the given statement be P(n). Then,

P(n): {1 - (1/2)}{1 - (1/3)}{1 - (1/4)} .... {1 - 1/(n + 1)} = 1/(n + 1).

When n = 1, LHS = {1 – (1/2)} = ½ and RHS = 1/(1 + 1) = ½.

Therefore LHS = RHS.

Thus, P(1) is true.

Let P(k) be true. Then,

P(k): {1 - (1/2)}{1 - (1/3)}{1 - (1/4)} .... [1 - {1/(k + 1)}] = 1/(k + 1)

Now, [{1 - (1/2)}{1 - (1/3)}{1 - (1/4)} .... [1 - {1/(k + 1)}] · [1 – {1/(k + 2)}]

= [1/(k + 1)] · [{(k + 2) - 1}/(k + 2)}]

= [1/(k + 1)] · [(k + 1)/(k + 2)]

= 1/(k + 2)

Therefore p(k + 1): [{1 - (1/2)}{1 - (1/3)}{1 - (1/4)} .... [1 - {1/(k + 1)}] = 1/(k + 2)

⇒ P(k + 1) is true, whenever P(k) is true.

Thus, P(1) is true and P(k + 1) is true, whenever P(k) is true.

Hence, by the principle of mathematical induction, P(n) is true for all n ∈ N.

8. Using the principle of mathematical induction, prove that
a + ar + ar^2 +........ + ar^{n-1} = (ar^{n-1})/(r - 1) for r > 1 and all n ∈ N.
Solution : Let the given statement be P(n). Then,

P(n): a + ar + ar^2 +....... +ar^{n-1} = {a(r^n -1)}/(r - 1).

When n = 1, LHS = a and RHS = {a(r^1 - 1)}/(r - 1) = a

Therefore LHS = RHS.

Thus, P(1) is true.

Let P(k) be true. Then,

P(k): $a + ar + ar^2 + \ldots\ldots + ar^{k-1} = \{a(r^k - 1)\}/(r - 1)$

Now, $(a + ar + ar^2 + \ldots\ldots + ar^{k-1}) + ar^k = \{a(r^k - 1)\}/(r - 1) + ar^2$ .... [using(i)]

$= a(r^{k+1} - 1)/(r - 1)$.

Therefore,
P(k + 1): $a + ar + ar^2 + \ldots\ldots + ar^{k-1} + ar^k = \{a(r^{k+1} - 1)\}/(r - 1)$

⇒ P(k + 1)is true, whenever P(k) is true.

Thus, P(1) is true and P(k + 1) is true, whenever P(k) is true.
Hence, by the principle of mathematical induction, P(n) is true for all n ∈ N.

9. Let a and b be arbitrary real numbers. Using the principle of mathematical induction, prove that $(ab)^n = a^n b^n$ for all n ∈ N.
Solution : Let the given statement be P(n). Then,

P(n): $(ab)^n = a^n b^n$.
When = 1, LHS = $(ab)^1$ = ab and RHS = $a^1 b^1$ = ab
Therefore LHS = RHS.
Thus, the given statement is true for n = 1, i.e., P(1) is true.

Let P(k) be true. Then,

P(k): $(ab)^k = a^k b^k$.

Now, $(ab)^{k+1} = (ab)^k (ab)$

$= (a^k b^k)(ab)$ [using (i)]

$= (a^k \cdot a)(b^k \cdot b)$ [by commutativity and associativity of multiplication on real numbers]

$= (a^{k+1} \cdot b^{k+1})$.

Therefore P(k+1): $(ab)^{k+1} = ((a^{k+1} \cdot b^{k+1})$

⇒ P(k + 1) is true, whenever P(k) is true.

Thus, P(1) is true and P(k + 1) is true, whenever P(k) is true.

Hence, by the principle of mathematical induction, P(n) is true for all n ∈ N.

10. Using the principle of mathematical induction, prove that $(x^n - y^n)$ is divisible by (x - y)for all n ∈ N.
Solution : Let the given statement be P(n). Then,

P(n): $(x^n - y^n)$ is divisible by $(x - y)$.

When n = 1, the given statement becomes: $(x^1 - y^1)$ is divisible by $(x - y)$, which is clearly true.

Therefore P(1) is true.

Let p(k) be true. Then,

P(k): $x^k - y^k$ is divisible by $(x-y)$.

Now, $x^{k+1} - y^{k+1} = x^{k+1} - x^k y - y^{k+1}$

[on adding and subtracting x)^{k}y]

$= x^k(x - y) + y(x^k - y^k)$, which is divisible by $(x - y)$ [using (i)]

⇒ P(k + 1): $x^{k+1} - y^{k+1}$is divisible by $(x - y)$

⇒ P(k + 1) is true, whenever P(k) is true.

Thus, P(1) is true and P(k + 1) is true, whenever P(k) is true.

Hence, by the Principal of Mathematical Induction, P(n) is true for all n ∈ N.

11. Using the principle of mathematical induction, prove that $(10^{2n-1} + 1)$ is divisible by 11 for all n ∈ N.

Solution : Let P (n): $(10^{2n-1} + 1)$ is divisible by 11.

For n=1, the given expression becomes $\{10^{(2 \times 1 - 1)} + 1\} = 11$, which is divisible by 11.

So, the given statement is true for n = 1, i.e., P (1) is true.

Let P(k) be true. Then,

P(k): $(10^{2k-1} + 1)$ is divisible by 11

⇒ $(10^{2k-1} + 1) = 11$ m for some natural number m.

Now, $\{10^{2(k-1)-1} + 1\} = (10^{2k+1} + 1) = \{10^2 \cdot 10^{(2k-1)} + 1\}$

$= 100 \times \{10^{2k-1} + 1\} - 99$

$= (100 \times 11m) - 99$

$= 11 \times (100m - 9)$, which is divisible by 11

⇒ P (k + 1): $\{10^{2(k+1)} - 1 + 1\}$ is divisible by 11

⇒ P (k + 1) is true, whenever P(k) is true.

Thus, P (1) is true and P(k + 1) is true , whenever P(k) is true.

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

12. Using the principle if mathematical induction, prove that (7n – 3n) is divisible by 4 for all $n \in N$.

Solution : Let P(n) : $(7^n – 3^n)$ is divisible by 4.

For n = 1, the given expression becomes $(7^1 - 3^1) = 4$, which is divisible by 4.

So, the given statement is true for n = 1, i.e., P(1) is true.

Let P(k) be true. Then,

P(k): $(7^k - 3^k)$ is divisible by 4.

$\Rightarrow (7^k - 3^k) = 4m$ for some natural number m.

Now, $\{7^{(k+1)} - 3\ (k + 1)\} = 7^{(k+1)} – 7 \cdot 3^k + 7 \cdot 3^k - 3^{(k+1)}$

(on subtracting and adding 7 · 3k)

$= 7(7^k - 3^k) + 3^k\ (7 - 3)$

$= (7 \times 4m) + 4 \cdot 3k$

$= 4(7m + 3^k)$, which is clearly divisible by 4.

$\therefore$ P(k + 1): $\{7^{(k+1)} - 3\ (k + 1)\}$ is divisible by 4.

$\Rightarrow$ P(k + 1) is true, whenever P(k) is true.

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

13. Using the principle if mathematical induction, prove that
$(2 \cdot 7^n + 3 \cdot 5^n - 5)$ is divisible by 24 for all $n \in N$.

Solution : Let P(n): $(2 \cdot 7^n + 3 \cdot 5^n - 5)$ is divisible by 24.

For n = 1, the given expression becomes $(2 \cdot 7^1 + 3 \cdot 5^1 - 5) = 24$, which is clearly divisible by 24.

So, the given statement is true for n = 1, i.e., P(1) is true.

Let P(k) be true. Then,

P(k): $(2 \cdot 7^n + 3 \cdot 5^n - 5)$ is divisible by 24.

$\Rightarrow (2 \cdot 7^n + 3 \cdot 5^n - 5) = 24m$, for m = N

Now, $(2 \cdot 7^n + 3 \cdot 5^n - 5)$

$= (2 \cdot 7^k \cdot 7 + 3 \cdot 5^k \cdot 5 - 5)$

$= 7(2 \cdot 7^k + 3 \cdot 5^k - 5) = 6 \cdot 5^k + 30$

= (7 × 24m) - 6(5^k - 5)

= (24 × 7m) - 6 × 4p, where (5^k - 5) = 5(5^{k-1} - 1) = 4p
[Since (5^{k-1} - 1) is divisible by (5 - 1)]

= 24 × (7m - p)

= 24r, where r = (7m - p) ∈ N

⇒ P (k + 1): (2 · 7^k + 13 · 5^k + 1 - 5) is divisible by 24.

⇒ P(k + 1) is true, whenever P(k) is true.

Thus, P(1) is true and P(k + 1) is true, whenever P(k) is true.

Hence, by the principle of mathematical induction, P(n) is true for all n ∈ N.

14. Using the principle of mathematical induction, prove that n(n + 1)(n + 5) is a multiple of 3 for all n ∈ N.
Solution : Let P(n): n(n + 1)(n + 5) is a multiple of 3.

For n = 1, the given expression becomes (1 × 2 × 6) = 12, which is a multiple of 3.

So, the given statement is true for n = 1, i.e. P(1) is true.

Let P(k) be true. Then,

P(k): k(k + 1)(k + 5) is a multiple of 3

⇒ K(k + 1)(k + 5) = 3m for some natural number m, ... (i)

Now, (k + 1l)(k + 2)(k + 6) = (k + 1)(k + 2)k + 6(k + 1)(k + 2)

= k(k + 1)(k + 2) + 6(k + 1)(k + 2)

= k(k + 1)(k + 5 – 3) + 6(k + 1)(k + 2)

= k(k + 1)(k + 5) – 3k(k + 1) + 6(k + 1)(k + 2)

= k(k + 1)(k + 5) + 3(k + 1)(k +4) [on simplification]

= 3m + 3(k + 1)(k + 4) [using (i)]

= 3[m + (k + 1)(k + 4)], which is a multiple of 3

⇒ P(k + 1): (k + 1)(k + 2)(k + 6) is a multiple of 3

⇒ P(k + 1) is true, whenever P(k) is true.

Thus, P(1) is true and P(k + 1) is true, whenever P(k) is true.

Hence, by the principle of mathematical induction, P(n) is true for all n ∈ N.

15. Using the principle of mathematical induction, prove that $(n^2 + n)$ is even for all n ∈ N.
Solution : Let P(n): $(n^2 + n)$ is even.

For n = 1, the given expression becomes $(1^2 + 1) = 2$, which is even.

So, the given statement is true for n = 1, i.e., P(1)is true.

Let P(k) be true. Then,

P(k): $(k^2 + k)$ is even

⇒ $(k^2 + k) = 2m$ for some natural number m......(i)

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

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

$= 2m + 2(k + 1)$ [using (i)]

$= 2[m + (k + 1)]$, which is clearly even.

Therefore, P(k + 1): $(k + 1)^2 + (k + 1)$ is even

⇒ P(k + 1) is true, whenever P(k) is true.

Thus, P(1) is true and P(k + 1) is true, whenever P(k) is true.

Hence, by the principle of mathematical induction, P(n)is true for all n ∈ N.

Subject Notes
CS301 - Discrete Structures

UNIT-2

Group Theory is a branch of mathematics and abstract algebra that defines an algebraic structure named as **Group**. Generally, a group comprises of a set of elements and an operation over any two elements on that set to form a third element also in that set. In 1854, Arthur Cayley, the British Mathematician, gave the modern definition of group for the first time −

"**A set of symbols all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a group. These symbols are not in general convertible [commutative], but are associative.**"

Any set of elements in a mathematical system may be defined with a set of operators and a number of postulates.

Algebric Structure

an algebraic structure is a set (called carrier set or underlying set) with one or more finitary operations defined on it that satisfies a list of axioms.

A binary operator defined on a set of elements is a rule that assigns to each pair of elements a unique element from that set. For example, given the set A={1,2,3,4,5}

, we can say o is a binary operator for the operation c=aob, if it specifies a rule for finding c for the pair of (a,b), such that a,b,c∈A.

Properties of Algebric Structure

The **postulates** of a mathematical system form the basic assumptions from which rules can be deduced. The postulates are −

1. **Closure-** A set is closed with respect to a binary operator if for every pair of elements in the set, the operator finds a unique element from that set.

Example

Let $A=\{0,1,2,3,4,5,\ldots\}$

This set is closed under binary operator into (∗) , because for the operation $c=a*b$, for any $a,b\in A$, the product $c\in A$.

The set is not closed under binary operator divide (÷) , because, for the operation $c=a\div b$, for any $a,b\in A$, the product c may not be in the set A. If $a=7,b=2$, then $c=3.5$. Here $a,b\in A$ but *cøA*

2. **Associative Laws -** A binary operator ⊗ on a set A is associative when it holds the following property −

$$(x\otimes y)\otimes z=x\otimes(y\otimes z) \text{ , where } x,y,z\in A$$

Example

Let $A=\{1,2,3,4\}$ The operator plus (+) is associative because for any three elements, $x,y,z\in A$, the property $(x+y)+z=x+(y+z)$ holds.

The operator minus (−) is not associative since

$$(x-y)-z\neq x-(y-z)$$

3. **Commutative Laws -** A binary operator ⊗ on a set A is commutative when it holds the following property −

$$x\otimes y=y\otimes x \text{ , where } x,y\in A$$

Example

Let $A=\{1,2,3,4\}$ The operator plus (+) is commutative because for any two elements, $x,y\in A$, the property $x+y=y+x$ holds.

The operator minus (−) is not associative since

$$x-y\neq y-x$$

4. **Distributive Laws -** Two binary operators ⊗ and ⊛ on a set A, are distributive over operator ⊛

when the following property holds −

$$\boldsymbol{x\otimes(y\circledast z)=(x\otimes y)\circledast(x\otimes z)}\text{ , where } x,y,z\in A$$

Example

Let $A=\{1,2,3,4\}$ The operators into ($*$) and plus (+) are distributive over operator + because for any three elements, $x,y,z\in A$, the property $x*(y+z)=(x*y)+(x*z)$ holds.

However, these operators are not distributive over $*$ since

$x+(y*z)\neq(x+y)*(x+z)$

5. **Identity Element -** A set A has an identity element with respect to a binary operation $\otimes$ on A, if there exists an element $e\in A$, such that the following property holds −

$$\boldsymbol{e\otimes x=x\otimes e}\text{ , where } x\in A$$

Example

Let $Z=\{0,1,2,3,4,5,\ldots\}$ The element 1 is an identity element with respect to operation $*$

since for any element $x\in Z$,

$1*x=x*1$

On the other hand, there is no identity element for the operation minus (−)

6. **Inverse -** If a set A has an identity element e with respect to a binary operator $\otimes$, it is said to have an inverse whenever for every element $x\in A$, there exists another element $y\in A$, such that the following property holds −

$$\boldsymbol{x\otimes y=e}$$

Example

Let $A=\{\cdots-4,-3,-2,-1,0,1,2,3,4,5,\ldots\}$ Given the operation plus (+) and $e=0$, the inverse of any element x is $(-x)$ since $x+(x)=0$

Semigroup

A finite or infinite set 'S' with a binary operation 'o' (Composition) is called semigroup if it holds following two conditions simultaneously −

i. **Closure** − For every pair $(a,b)\in S,(aob)$ has to be present in the set S
ii. **Associative** − For every element $a,b,c\in S,(aob)oc=ao(boc)$ must hold.

Example

The set of positive integers (excluding zero) with addition operation is a semigroup. For example, $\boldsymbol{S=\{1,2,3,\ldots\}}$

Here closure property holds as for every pair $(a,b)\in S,(a+b)$ is present in the set S. For example, $1+2=3\in S$]

Associative property also holds for every element $a,b,c\in S,(a+b)+c=a+(b+c)$. For example, $(1+2)+3=1+(2+3)=5$

Monoid

A monoid is a semigroup with an identity element. The identity element (denoted by e or E) of a set S is an element such that $(aoe)=a$, for every element $a\in S$. An identity element is also called a **unit element**. So, a monoid holds three properties simultaneously − **Closure, Associative, Identity element**.

Example

The set of positive integers (excluding zero) with multiplication operation is a monoid. $\boldsymbol{S=\{1,2,3,\ldots\}}$

1. Here closure property holds as for every pair $(a,b)\in S,(a\times b)$ is present in the set S. [For example, $1\times2=2\in S$ and so on]
2. Associative property also holds for every element $a,b,c\in S,(a\times b)\times c=a\times(b\times c)$ [For example, $(1\times2)\times3=1\times(2\times3)=6$ and so on]
3. Identity property also holds for every element $a\in S,(a\times e)=a$ [For example, $(2\times1)=2,(3\times1)=3$

and so on]. Here identity element is 1.

Group

A group is a monoid with an inverse element. The inverse element (denoted by I) of a set S is an element such that $(aoI)=(Ioa)=a$, for each element $a\in S$. So, a group holds four properties simultaneously −

i) Closure, ii) Associative, iii) Identity element, iv) Inverse element.

The order of a group G is the number of elements in G and the order of an element in a group is the least positive integer n such that an is the identity element of that group G.

Examples

The set of *N*×*N* non-singular matrices form a group under matrix multiplication operation.

1. The product of two *N*×*N* non-singular matrices is also an *N*×*N*
2. non-singular matrix which holds closure property.
3. Matrix multiplication itself is associative. Hence, associative property holds.
4. The set of *N*×*N* non-singular matrices contains the identity matrix holding the identity element property.

As all the matrices are non-singular they all have inverse elements which are also nonsingular matrices. Hence, inverse property also holds.

Abelian Group

An abelian group G is a group for which the element pair $(a,b)\in G$ always holds commutative law. So, a group holds five properties simultaneously –

i) Closure, ii) Associative, iii) Identity element, iv) Inverse element, v) Commutative.

Example

The set of positive integers (including zero) with addition operation is an abelian group. $G=\{0,1,2,3,\ldots\}$

1. Here closure property holds as for every pair $(a,b)\in S,(a+b)$ is present in the set S. [For example, $1+2=2\in S$ and so on]
2. Associative property also holds for every element $a,b,c\in S,(a+b)+c=a+(b+c)$ [For example, (1+2)+3=1+(2+3)=6 and so on]
3. Identity property also holds for every element $a\in S,(a\times e)=a$ [For example, (2×1)=2,(3×1)=3 and so on]. Here, identity element is 1.
4. Commutative property also holds for every element $a\in S,(a\times b)=(b\times a)$ [For example, (2×3)=(3×2)=3
5. Inverse Property also holds for every element a • b = b • a = e [For example 0+1 = 1+0 =1]

Properties of Groups

1. If G is a group with binary operation ∗, then the left and right cancellation laws hold in G. that is, a ∗b=a ∗c implies b=c, and b ∗a=c ∗a implies b=c for all a, b, c ∈G.

Proof - Suppose a * b = a * c. Then there exists an inverse of a’ to a. Apply this inverse on the left,

a’ * (a * b) = a’ *(a * c)

By the associatively law,

(a’ * a) * b = (a’ * a) * c

Since a’ is the inverse of a, a’ * a =e, we have

e * b = e * c

By the definition of e,

b = c

Similarly for the right cancellation

2. If G is a group with binary operation ∗, and if a and b are any elements of G, then the linear equations a ∗ x=b and y ∗ a=b have unique solutions x and y in G.

Proof: First we show the existence of at least one solution by just computing that a’ ∗ b is a solution of a ∗ x=b. Note that

a * (a’ * b) = (a *a’) * b, associative law,

=e * b, definition of a’,

=b, property of e.

Thus x= a′ ∗ b is a solution a ∗ x=b. In a similar fashion, y=b ∗ a′ is a solution of y ∗ a=b.
To show uniqueness of y, we assume that we have two solutions, y_1 and y_2, so that $y_1 * a=b$ and $y_2 * a=b$. Then $y_1 * a=y_2 * a$, and by Theorem 4.15, $y_1=y_2$. The uniqueness of x follows similarly.

3. In a group G with binary operation ∗, there is only one element e in G such that

$$e * x = x * e = x$$

for all x ∈G. Likewise for each a ∈G, there is only one element a′ in G such that

$$a' * a = a * a' = e$$

<u>**Cyclic Group and Subgroup**</u>

A **cyclic group** is a group that can be generated by a single element. Every element of a cyclic group is a power of some specific element which is called a generator. A cyclic group can be generated by a generator 'g', such that every other element of the group can be written as a power of the generator 'g'.

Example

The set of complex numbers {1,-1,*i*,-*i*} under multiplication operation is a cyclic group.

Solution- There are two generators – *I* and –*i* as *i*1=*i*,*i*2=−1,*i*3=−*i*,*i*4=1 and also (–*i*)1=–*i*,(–*i*)2=−1,(–*i*)3=*i*,(–*i*)4=1 which covers all the elements of the group. Hence, it is a cyclic group.

Note − A **cyclic group** is always an abelian group but not every abelian group is a cyclic group. The rational numbers under addition is not cyclic but is abelian.

A **subgroup** H is a subset of a group G (denoted by *H*≤*G*) if it satisfies the four properties simultaneously − **Closure, Associative, Identity element**, and **Inverse**.

A subgroup H of a group G that does not include the whole group G is called a proper subgroup (Denoted by *H*<*G*). A subgroup of a cyclic group is cyclic and a abelian subgroup is also abelian.

Example

Let a group *G*={1,*i*,−1,−*i*}

Then some subgroups are *H*1={1},*H*2={1,−1}, This is not a subgroup − *H*3={1,*i*} because that (*i*)−1=−*i* is not in *H*3

<u>**Coset**</u>

Given H ≤ G, a left coset of H in G is a subset of G of the form gH = {gh|h∈ H} for some g ∈ G. Similarly a right coset of H in G is a subset of G of the form Hg = {hg|h∈ H} for some g ∈ G. Notice since g = eg = ge that g ∈ Hg and g ∈gH.

Example Suppose G = Σ_3, H =< (1, 2) >= {e,(1, 2)} and g = (1, 3). Then a simple computation shows that gH = {(1, 3),(1, 2, 3)} while Hg = {(1, 3),(1, 3, 2)} and sogH 6= Hg. Thus we see that for a fixed element g, the left cosetgH may be different from the right coset Hg in general.

Multiplying elements and sets Of course, the expression gH does not make immediate sense from the group axioms. What it means, by definition, is gH = {gh | h ∈ H} .

To put this another way, the golden rule is this: if you know that f ∈gH, then you can conclude that there is some h ∈ H so that f = gh.

Applying the golden rule Consider G = S4 and H = {id,(1, 2)}. If g = (2, 3, 4), thengH = {(2, 3, 4),(2, 3, 4)(1, 2)} = {(2, 3, 4),(1, 3, 4, 2)}. Now let f = (3, 4, 2, 1)—this is an element of gH. Which h ∈ H satisfies f = gh?

Or

if g = (1, 3)(2, 4), then gH = {(1, 3)(2, 4),(1, 4, 2, 3)}. If you let f = (1, 4, 2, 3), which h ∈ H satisfies f = gh this time?

compute the two cosets g1H ⊂ S4 and g2H ⊂ S4 for H = {id,(1, 2, 3, 4),(1, 3)(2, 4),(1, 4, 3, 2)} and g1 = (1, 3, 2), g2 = (1, 2, 3, 4).

Factor Group

If N is a normal subgroup of G, then the group of left cosets of N in G is called the factor group of G determined by N. It will be denoted by G/N.

Example Let N be a normal subgroup of G. If a ∈G, then the order of aN in G/N is the smallest positive integer n such that a^n ∈N.

Permutations Group

A permutation of a set X is a function σ : X → X that is one-to-one and onto, i.e., a bijective map.

Example

A = {1,2,3}

There are six permutations for this set, namely

$$\begin{pmatrix}1 & 2 & 3\\1 & 2 & 3\end{pmatrix}\quad\begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix}\quad\begin{pmatrix}1 & 2 & 3\\2 & 1 & 3\end{pmatrix}\quad\begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix}\quad\begin{pmatrix}1 & 2 & 3\\3 & 1 & 2\end{pmatrix}\quad\begin{pmatrix}1 & 2 & 3\\3 & 2 & 1\end{pmatrix}$$

Normal Subgroup

A normal subgroup is a subgroup which is invariant under conjugation by members of the group of which it is a part. In other words, a subgroup H of a group G is normal in G if and only if gH = Hg for all g in G; i.e., the sets of left and right cosets coincide.

gH = Hg

Homomorphism

Definition: A group homomorphism ϕ : G → G0 is an isomorphism if ϕ is a bijection. If there is an isomorphism between G and G0 we say G and G0 are isomorphic. This is denoted by G ∼= G0 .

Given a homomorphism ϕ : G → G0 there are subgroups of each that can indicate to us whether ϕ is injective or surjective. Definition. Let ϕ : G → G0 be a homomorphism. Define ker(ϕ) = {g ∈ G : ϕ(g) = eG0}. This is called the kernel of ϕ. Define im(ϕ) = {ϕ(g) : g ∈ G}. This is called the image of ϕ. We usually use the notation ϕ(G) for im(G).

Example If ϕ : GL2(R) → R\{0} is given by ϕ(A) = det(A) then ker(ϕ(A)) = SL2(R) and im(ϕ) = R\{0}.

Theorem Letϕ : G → G0 be a homomorphism. Then 1.ker(ϕ) is a subgroup of G, and ϕ is injective if and only if ker(ϕ) = eG. 2. im(ϕ) is a subgroup of G0 , and ϕ is surjective if and only if im(ϕ) = G0 (or equivalently, ϕ(G) = G0).

Proof. If a, b ∈ker(ϕ), then ϕ(ab−1) = ϕ(a)ϕ(b) −1 = eG0(eG0) −1 = eG0 so by the Subgroup Test, ker(ϕ) is a subgroup.

Now if ker(ϕ) = {e} then ϕ(a) = ϕ(b) =⇒ϕ(ab−1) = e =⇒ ab−1 = e =⇒ a = b.

Moreover, if ϕ is injective, then

ϕ(a) = e =⇒ϕ(a) = ϕ(e) =⇒ a = e, so ker(ϕ) = {e}.

Isomorphism

The homomorphism ϕ : G → G0 is an isomorphism if and only if there exists a homomorphism ψ : G0 → G such that ϕ ◦ ψ = ψ ◦ ϕ are identity maps on their respective groups.

Proof : Define ψ(a) to be the unique pre-image of a under ϕ. Since ϕ is a bijection, this is well defined and ϕ ◦ ψ = ψ ◦ ϕ are identity maps between their respective groups. One needs to check ψ is indeed a homomorphism, but this effectively comes for free since ϕ is one.

Example and standard result on Group

Integers Z with addition

(G1) a, b ∈ Z =⇒ a + b ∈ Z

(G2) (a + b) + c = a + (b + c)
(G3) the identity element is 0 as a + 0 = 0 + a = a and 0 ∈ Z
(G4) the inverse of a ∈ Z is −a as a + (−a) = (−a) + a = 0 and −a ∈ Z (G5) a + b = b + a

The set Zn of congruence classes modulo n with addition
(G1) [a], [b] ∈ Zn =⇒ [a] + [b] = [a + b] ∈ Zn
(G2) ([a] + [b]) + [c] = [a + b + c] = [a] + ([b] + [c])
(G3) the identity element is [0] as [a] + [0] = [0] + [a] = [a]
(G4) the inverse of [a] is [−a] as [a] + [−a] = [−a] + [a] = [0]
(G5) [a] + [b] = [a + b] = [b] + [a]

The set Gn of invertible congruence classes modulo n with multiplication
A congruence class [a]n ∈ Zn belongs to Gn if gcd(a, n) = 1.
(G1) [a]n, [b]n ∈Gn =⇒gcd(a, n) = gcd(b, n) = 1 =⇒gcd(ab, n) = 1 =⇒ [a]n[b]n = [ab]n ∈Gn
(G2) ([a][b])[c] = [abc] = [a]([b][c])
(G3) the identity element is [1] as [a][1] = [1][a] = [a]
(G4) the inverse of [a] is [a] −1 by definition of [a] −1
(G5) [a][b] = [ab] = [b][a]

Permutations S(n) with composition (= multiplication)
(G1) u and σ are bijective functions from the set {1, 2, . . . , n} to itself =⇒ so is uσ
(G2) (u σ)τ and u(σ τ) applied to k, 1 ≤ k ≤ n, both yield u(σ(τ (k))).
(G3) the identity element is id as u id = id u = u
(G4) the inverse of u is u −1 by definition of the inverse function (G5) fails for n ≥ 3 as (as (1 2)(2 3) = (1 2 3) while (2 3)(1 2) = (1 3 2).

Ring
The definition of a ring: A structure (R, +, ·) is a ring if R is a non-empty set and + and · are binary operations:
+: R × R → R, (a, b) 7→ a + b · : R × R → R, (a, b) 7→ a · b
such that
Addition: (R, +) is an abeliangroup, that is,
(A1) associativity: for all a, b, c ∈ R we have a + (b + c) = (a + b) + c
(A2) zero element: there exists 0 ∈ R such that for all a ∈ R we have a + 0 = 0 + a = a
(A3) inverses: for any a ∈ R there exists −a ∈ R such that a + (−a) = (−a) + a = 0
(A4) commutativity: for all a, b ∈ R we have a + b = b + a

Multiplication:
(M1) associativity: for all a, b, c ∈ R we have a · (b · c) = (a · b) · c

Addition and multiplication together (D) for all a, b, c ∈ R,
a · (b + c) = a · b + a · c and (a + b) · c = a · b + b · c.
We sometimes say 'R is a ring', taken it as given that the ring operations are denoted + and ·. As in ordinary arithmetic we shall frequently suppress · and write ab instead of a · b

Special types of rings: definitions. Assume (R; +, ·) is a ring. We say R is a commutative ring if its multiplication · is commutative, that is,
(M4) Commutativity: a · b = b · a for all a, b ∈ R. We say R is a ring with 1 (or ring with identity) if there exists an identity for multiplication, that is,
(M2) identity element: there exists 1 ∈ R such that for all a ∈ R we have a · 1 = 1 · a = a.

Examples of rings

Number systems

(1) All of Z, Q, R and C are commutative rings with identity (with the number 1 as the identity).

(2) N is NOT a ring for the usual addition and multiplication. These are binary operations and we do have a zero element, namely 0, so axiom (A2) holds. However (A3) (existence of additive inverses) fails: there is no n ∈ N for which 1 + n = 0, for example.

(3) Consider the set of even integers, denoted 2Z, with the usual addition and multiplication. This is a commutative ring without an identity. To verify that (M2) fails it is not sufficient just to say that the integer 1 does not belong to 2Z. Instead we argue as follows. Suppose for contradiction that there were an element e ∈ 2Z such that n·e = n for all n ∈ 2Z. In particular 2e = 2, from which we deduce that e would have to be 1. Since 1 ∈/ 2Z we have a contradiction.

Matrix rings Under the usual matrix addition and multiplication Mn(R) and Mn(C), are rings with 1, but are not commutative (unless n = 1). If we restrict to invertible matrices we no longer have a ring, because there is then no zero for addition.

PolynomialsPolynomials, with real coefficients, form a commutative ring with identity under the usual addition and multiplication; we denote this by R[x].

Modular arithmetic Binary arithmetic on {0, 1} (see 1.2(4)) gives us a 2-element commutative ring with identity. More generally we get a commutative ring with identity if we consider addition and multiplication mod n on {0, 1, . . . , n − 1}.

Calculational rules for rings.

Assume that (R; +, ·) is a commutative ring.

Let a, b, c ∈ R.

(i) If a + b = a + c then b = c.

(ii) If a + a = a then a = 0.

(iii) −(−a) = a.

(iv) 0a = 0.

(v) −(ab) = (−a)b = a(−b). Assume in addition that R has an identity 1 Then

(vi) (−1)a = −a.

(vii) If a ∈ R has a multiplicative identity a −1 then ab = 0 implies b = 0.

Field

A field is a ring in which the elements, other than the identity element for addition, and the multiplication operator, also form a group.

- There are only two kinds of finite fields. One kind is the field formed by addition and multiplication modulo a prime number.
- The other kind of finite field has a number of elements that is a power of a prime number.
- The addition operator consists of multiple independent additions modulo that prime. The elements of the field can be thought of as polynomials whose coefficients are numbers modulo that prime. In that case, multiplication is polynomial multiplication, where not only the coefficients modulo that prime, but the polynomials are modulo a special kind of polynomial, known as a primitive polynomial. All finite fields, but particularly those of this second kind, are known as Galois fields.
- A commutative ring which has more than one element such that every non-zero element of S has a multiplicative inverse in S is called a field.

The ring of even integers is a subring of the ring of integers. Let •> and Å , ¤ > be rings. A mapping of g : R® S is called a ring homomorphism from and Å ,¤ > if for any a, b, Î R g(a + b) = g(a) Å g(b) and g(a • b) = g(a) ¤ g(b).

Standard results

If R is a ring and a, b, c, d ∈ R, evaluate (a + b)(c + d).

Solution: (a + b)(c + d) = a(c + d) + b(c + d)
by distributive law
= (ac + ad) + (bc + bd)
= ac + ad + bc + bd

Prove that if a, b ∈ R, then $(a + b)^2 = a^2 + ab + ba + b^2$ where by x^2 we mean xx.

Solution: $(a + b)^2 = (a + b)(a + b) = a(a + b) + b(a + b) = a^2 + ab + ba + b^2$ Note that if R is not a commutative ring ab 6= ba.

If in a ring R every x ∈ R satisfies $x^2 = x$,prove that R must be commutative (A ring in which $x^2 = x$ for all elements is called a Boolean ring).

Solution: Let x, y ∈ R. Then $(x + y)^2 = (x + y)(x + y) = x^2 + xy + yx + y^2$ Since $x^2 = x$ and $y^2 = y$ we have x + y = x + xy + yx + y. Hence xy = −yx. But for every x ∈ R $(−x) = (−x)^2 = (−x)(−x) = x^2 = x$. Hence −yx = yx i.e. we obtain xy = yx.

Prove that any field is an integral domain.

Solution: Let a 6= 0 and b be two elements in the field F and ab = 0. Since F is a field and a 6= 0. we have a −1 ∈ F. Hence a −1ab = a −10 = 0. So we obtain b = 0. Hence there exists no zero divisor in F.

If U is an ideal of R and 1 ∈ U, prove that U = R.

Solution: Since for any r ∈ R and u ∈ U, ru∈ U we have for any r ∈ R, r1 = r ∈ U. Hence R = U.

UNIT-3

Propositional Logic

The rules of mathematical logic specify methods of reasoning mathematical statements. Greek philosopher, Aristotle, was the pioneer of logical reasoning. Logical reasoning provides the theoretical base for many areas of mathematics and consequently computer science. It has many practical applications in computer science like design of computing machines, artificial intelligence, definition of data structures for programming languages etc.

Propositional Logic is concerned with statements to which the truth values, “true” and “false”, can be assigned. The purpose is to analyze these statements either individually or in a composite manner.

Prepositional Logic – Definition

A proposition is a collection of declarative statements that has either a truth value "true” or a truth value "false". A propositional consists of propositional variables and connectives. We denote the propositional variables by capital letters (A, B, etc). The connectives connect the propositional variables.

Some examples of Propositions are given below −

i. "Man is Mortal", it returns truth value “TRUE”
ii. "12 + 9 = 3 – 2", it returns truth value “FALSE”

The following is not a Proposition −

"A is less than 2". It is because unless we give a specific value of A, we cannot say whether the statement is true or false.

First Order Logic

First-order logic (FOL) models the world in terms of

i. **Objects,** which are things with individual identities
ii. **Properties** of objects that distinguish them from other objects
iii. **Relations** that hold among sets of objects
iv. **Functions,** which are a subset of relations where there is only one “value” for any given “input”

Examples:

a. Objects: Students, lectures, companies, cars .
b. Relations: Brother-of, bigger-than, outside, part-of, has-color, occurs-after, owns, visits.
c. Properties: blue, oval, even, large.
d. Functions: father-of, best-friend, second-half, one-more-than .
e. Variable symbols E.g., x, y, foo
f. Connectives :Same as in PL: not ($\neg$), and ($\wedge$), or ($\vee$), implies ($\rightarrow$), if and only if (biconditional $\leftrightarrow$)

g. Quantifiers: Universal ∀**x** or **(Ax)** , Existential ∃**x** or **(Ex)**

Basic Logic Operation

In propositional logic generally we use five connectives which are −

i. OR (v)
ii. AND (A)
iii. Negation/ NOT (¬)
iv. Implication / if-then (→)
v. If and only if (⇔).

OR (v**)** − The OR operation of two propositions A and B (written as *A*v*B*) is true if at least any of the propositional variable A or B is true. The truth table is as follows –

A	**B**	**A** ∨ **B**
True	True	True
True	False	True
False	True	True
False	False	False

Table 3.1 Operation of OR

AND (A**)** − The AND operation of two propositions A and B (written as *AAB*) is true if both the propositional variable A and B is true. The truth table is as follows −

A	**B**	**A** A **B**
True	True	True
True	False	False
False	True	False
False	False	False

3.2 Operation of AND

Negation (¬) – The negation of a proposition A (written as ¬*A*) is false when A is true and is true when A is false. The truth table is as follows –

A	**¬ A**
True	False
False	True

Table 3.3 Operation of Negation

If and only if (⇔) – *A*⇔*B*- is bi-conditional logical connective which is true when p and q are same, i.e. both are false or both are true. The truth table is as follows –

A	**B**	**A ⇔ B**
True	True	True
True	False	False
False	True	False
False	False	True

Table 3.4 Operation of bi conditional

Truth Tables

A truth table lists all possible combinations of truth values. In a two-valued logic system, a single statement *p* has two possible truth values: truth (T) and falsehood (F). Given two statements *p* and *q*, there are four possible truth value combinations, that is, TT, TF, FT, FF. As a result, there are four rows in the truth table. With three statements, there are eight truth value combinations, ranging from TTT to FFF. In general, given *n* statements, there are 2*n* rows (or cases) in the truth table.

Example

A	**B**	**A ⇔ B**
True	True	True
True	False	False

False	True	False
False	False	True

Table 3.5 Truth Table

Tautologies - A Tautology is a formula which is always true for every value of its propositional variables.

Example − Prove [(*A*→*B*)A*A*]→*B* is a tautology

The truth table is as follows –

A	**B**	**A & B**	**(A & B)** A **A**	**[(A & B)** A **A] & B**
True	True	True	True	True
True	False	False	False	True
False	True	True	False	True
False	False	True	False	True

Table 3.6 Tautology

As we can see every value of [(*A*→*B*)A*A*]→*B*

is "True", it is a tautology.

Contradictions - A Contradiction is a formula which is always false for every value of its propositional variables.

Example − **Prove (*A*∨*B*)**A**[(¬*A*)**A**(¬*B*)] is a contradiction**

The truth table is as follows –

A	**B**	**A ∨ B**	**¬ A**	**¬ B**	**(¬ A)** A **(¬ B)**	**(A ∨ B)** A **[(¬ A)** A **(¬ B)]**
True	True	True	False	False	False	False
True	False	True	False	True	False	False

False	True	True	True	False	False	False
False	False	False	True	True	True	False

Table 3.7 Contradiction

As we can see every value of (*A*v*B*)A[(¬*A*)A(¬*B*)] is “False”, it is a contradiction.

<u>Contingency</u> - A Contingency is a formula which has both some true and some false values for every value of its propositional variables.

Example - Prove (*A*v*B*)A(¬*A*) a contingency

The truth table is as follows –

A	**B**	**A ∨ B**	**¬ A**	**(A ∨ B) A (¬ A)**
True	True	True	False	False
True	False	True	False	False
False	True	True	True	True
False	False	False	True	False

Table 3.8 Contingency

As we can see every value of (*A*v*B*)A(¬*A*) has both “True” and “False”, it is a contingency.

Algebra of Proposition

1. Identity:

p V p ≡ p	p Λ p ≡ p	p → p ≡ T	p ⨯ p ≡ T
p V T ≡ T	p Λ T ≡ p	p → T ≡ T	p ⨯ T ≡ p
p V F ≡ p	p Λ F ≡ F	p → F ≡ ~p	p ⨯ F ≡ ~p
		T → p ≡ p	
		F → p ≡ T	

2. Commutative:

p V q ≡ q V p	p Λ q ≡ q Λ p	p → q ≠ q → p	p ⨯ q ≡ q ⨯ p

3. Complement:

p V ~p ≡ T	p Λ ~p ≡ F	p → ~p ≡ ~p	p ⨯ ~p ≡ F
		~p → p ≡ p	

4. Double Negation:

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

5. Associative:

$p \lor (q \lor r) \equiv (p \lor q) \lor r$

$p \land (q \land r) \equiv (p \land q) \land r$

6. Distributive:

$p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$

$p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$

7. Absorbtion:

$p \lor (p \land q) \equiv p$

$p \land (p \lor q) \equiv p$

8. De Morgan's:

$\sim(p \lor q) \equiv \sim p \land \sim q$

$\sim(p \land q) \equiv \sim p \lor \sim q$

9. Equivalence of Contrapositive:

$p \to q \equiv \sim q \to \sim p$

10. Others:

$p \to q \equiv \sim p \lor q$

$p \times q \equiv (p \to q) \land (q \to p)$

<u>Logical Implication</u>

An implication *A→B* is the proposition "if A, then B". It is false if A is true and B is false. The rest cases are true. The truth table is as follows −

A	**B**	**A & B**
True	True	True
True	False	False
False	True	True
False	False	True

Table 3.9 Logical Implication

<u>Logical Equivalences</u>

Two statements X and Y are logically equivalent if any of the following two conditions hold –

i. The truth tables of each statement have the same truth values.
ii. The bi-conditional statement $X \Leftrightarrow Y$
iii. is a tautology.

Example – Prove $\neg(A \vee B) and [(\neg A) \mathrm{A} (\neg B)]$ are equivalent

Testing by 1st method (Matching truth table)

A	**B**	**A ∨ B**	**¬ (A ∨ B)**	**¬ A**	**¬ B**	**[(¬ A)** A **(¬ B)]**
True	True	True	False	False	False	False
True	False	True	False	False	True	False
False	True	True	False	True	False	False
False	False	False	True	True	True	True

Table 3.10 Truth Table

Here, we can see the truth values of $\neg(A \vee B) and [(\neg A) \mathrm{A} (\neg B)]$

are same, hence the statements are equivalent.

Testing by 2nd method (Bi-conditionality)

A	**B**	**¬ (A ∨ B)**	**[(¬ A)** A **(¬ B)]**	**[¬ (A ∨ B)] ⇔ [(¬ A)** A **(¬ B)]**
True	True	False	False	True
True	False	False	False	True
False	True	False	False	True
False	False	True	True	True

Table 3.11 Truth Table

As $[\neg(A \vee B)] \Leftrightarrow [(\neg A) \mathrm{A} (\neg B)]$

is a tautology, the statements are equivalent.

Inverse, Converse, and Contra-positive

1. Implication / if-then ($\rightarrow$) is also called a conditional statement. It has two parts −
   i. Hypothesis, p
   ii. Conclusion, q

As mentioned earlier, it is denoted as $p \rightarrow q$

Example of Conditional Statement − "If you do your homework, you will not be punished." Here, "you do your homework" is the hypothesis, p, and "you will not be punished" is the conclusion, q.

1. **Inverse** − An inverse of the conditional statement is the negation of both the hypothesis and the conclusion. If the statement is "If p, then q", the inverse will be "If not p, then not q". Thus the inverse of $p \rightarrow q$ is $\neg p \rightarrow \neg q$

Example − The inverse of "If you do your homework, you will not be punished" is "If you do not do your homework, you will be punished."

2. **Converse** − The converse of the conditional statement is computed by interchanging the hypothesis and the conclusion. If the statement is "If p, then q", the converse will be "If q, then p". The converse of $p \rightarrow q$ is $q \rightarrow p$

Example − The converse of "If you do your homework, you will not be punished" is "If you will not be punished, you do not do your homework".

3. **Contra-positive** − The contra-positive of the conditional is computed by interchanging the hypothesis and the conclusion of the inverse statement. If the statement is "If p, then q", the contra-positive will be "If not q, then not p". The contra-positive of $p \rightarrow q$ is $\neg q \rightarrow \neg p$

Example − The Contra-positive of " If you do your homework, you will not be punished" is "If you are not punished, then you do not do your homework".

Duality Principle

Duality principle states that for any true statement, the dual statement obtained by interchanging unions into intersections (and vice versa) and interchanging Universal set into Null set (and vice versa) is also true. If dual of any statement is the statement itself, it is said **self-dual** statement.

Example − The dual of $(A \cap B) \cup C$ is $(A \cup B) \cap C$

Predicate Logic - It deals with predicates, which are propositions containing variables.

Definition - A predicate is an expression of one or more variables defined on some specific domain. A predicate with variables can be made a proposition by either assigning a value to the variable or by quantifying the variable.

The following are some examples of predicates –

i. Let E(x, y) denote "x = y"
ii. Let X(a, b, c) denote "a + b + c = 0"
iii. Let M(x, y) denote "x is married to y"

<u>**Well Formed Formula**</u> **-** Well Formed Formula (wff) is a predicate holding any of the following −

i. All propositional constants and propositional variables are wffs
ii. If x is a variable and Y is a wff, $\forall xY$and $\exists xY$ are also wff
iii. Truth value and false values are wffs Each atomic formula is a wff
iv. All connectives connecting wffs are wffs

<u>Normal Forms</u>

We can convert any proposition in two normal forms −

i. Conjunctive normal form
ii. Disjunctive normal form

i. Conjunctive Normal Form - A compound statement is in conjunctive normal form if it is obtained by operating AND among variables (negation of variables included) connected with ORs. In terms of set operations, it is a compound statement obtained by Intersection among variables connected with Unions.

Example - $(AvB)A(AvC)A(BvCvD)$

ii. Disjunctive Normal Form- A compound statement is in conjunctive normal form if it is obtained by operating OR among variables (negation of variables included) connected with ANDs. In terms of set operations, it is a compound statement obtained by Union among variables connected with Intersections.

Example - $(AAB)v(AAC)v(BACAD)$

<u>**Quantifiers**</u> **-** The variable of predicates is quantified by quantifiers. There are two types of quantifier in predicate logic − Universal Quantifier and Existential Quantifier.

1. **Universal Quantifier -** Universal quantifier states that the statements within its scope are true for every value of the specific variable. It is denoted by the symbol ∀.

$\forall xP(x)$ is read as for every value of x, P(x) is true.

Example − "Man is mortal" can be transformed into the propositional form $\forall xP(x)$

where P(x) is the predicate which denotes x is mortal and the universe of discourse is all men.

2. **Existential Quantifier -** Existential quantifier states that the statements within its scope are true for some values of the specific variable. It is denoted by the symbol ∃.

$\exists x P(x)$ is read as for some values of x, P(x) is true.

Example − "Some people are dishonest" can be transformed into the propositional form $\exists x P(x)$

where P(x) is the predicate which denotes x is dishonest and the universe of discourse is some people.

3. **Nested Quantifiers -** If we use a quantifier that appears within the scope of another quantifier, it is called nested quantifier.

Example

i. $\forall\, a \exists b P(x,y)$ where $P(a,b)$ denotes $a+b=0$
ii. $\forall\, a \forall b \forall c P(a,b,c)$ where $P(a,b)$ denotes $a+(b+c)=(a+b)+c$

Note – $\forall a \exists b P(x,y) \neq \exists a \forall b P(x,y)$

<u>Rules of Inference</u> - To deduce new statements from the statements whose truth that we already know, **Rules of Inference** are used.

- Mathematical logic is often used for logical proofs. Proofs are valid arguments that determine the truth values of mathematical statements.
- An argument is a sequence of statements. The last statement is the conclusion and all its preceding statements are called premises (or hypothesis). The symbol "∴ ", (read therefore) is placed before the conclusion. A valid argument is one where the conclusion follows from the truth values of the premises.
- Rules of Inference provide the templates or guidelines for constructing valid arguments from the statements that we already have.

Table of Rules of Inference

Rule of Inference Name Rule of Inference Name

1. **Addition**

If P is a premise, we can use Addiction rule to derive $P \lor Q$

$\boldsymbol{P \therefore P \lor Q}$

Example

Let P be the proposition, "He studies very hard" is true

Therefore − "Either he studies very hard Or he is a very bad student." Here Q is the proposition "he is a very bad student".

2. **Conjunction**

If P and Q are two premises, we can use Conjunction rule to derive $P \land Q$

$\boldsymbol{PQ \therefore P \land Q}$

Example

Let P – “He studies very hard”

Let Q – “He is the best boy in the class”

Therefore – "He studies very hard and he is the best boy in the class"

3. Simplification

If *P*Λ*Q* is a premise, we can use Simplification rule to derive P.

P*Λ*Q*∴*P

Example

"He studies very hard and he is the best boy in the class", *P*Λ*Q*

Therefore – "He studies very hard"

4. Modus Ponens

If P and *P*→*Q* are two premises, we can use Modus Ponens to derive Q.

P*&*QP*∴*Q

Example

"If you have a password, then you can log on to facebook", *P*→*Q*

"You have a password", P Therefore – "You can log on to facebook"

5. Modus Tollens

If *P*→*Q*and ¬*Q* are two premises, we can use Modus Tollens to derive ¬*P*

P*&*Q*¬*Q*∴¬*P

Example

"If you have a password, then you can log on to facebook", *P*→*Q*

"You cannot log on to facebook", ¬*Q*

Therefore – "You do not have a password "

6. Disjunctive Syllogism

If ¬*P* and *P*v*Q* are two premises, we can use Disjunctive Syllogism to derive Q.

¬*PP*v*Q*∴*Q*

Example

"The ice cream is not vanilla flavored", ¬*P*

"The ice cream is either vanilla flavored or chocolate flavored", *P*v*Q*

Therefore − "The ice cream is chocolate flavored"

7. Hypothetical Syllogism

If *P*→*Q* and *Q*→*R* are two premises, we can use Hypothetical Syllogism to derive *P*→*R*

P&QQ&R∴P&R

Example

"If it rains, I shall not go to school", *P*→*Q*

"If I don't go to school, I won't need to do homework", *Q*→*R*

Therefore − "If it rains, I won't need to do homework"

8. Constructive Dilemma

If (*P*→*Q*)A(*R*→*S*) and *P*v*R* are two premises, we can use constructive dilemma to derive *Q*v*S*

(*P&Q*)A**(*R&S*)*P*v*R∴Q*v*S***

Example

"If it rains, I will take a leave", (*P*→*Q*)

"If it is hot outside, I will go for a shower", (*R*→*S*)

"Either it will rain or it is hot outside", *P*v*R*

Therefore − "I will take a leave or I will go for a shower"

9. Destructive Dilemma

If (*P*→*Q*)A(*R*→*S*) and ¬*Q*v¬*S* are two premises, we can use destructive dilemma to derive *P*v*R*

(*P&Q*)A**(*R&S*)¬*Q*v¬*S∴P*v*R***

Numerical

1. Prove by truth table that the following is tautology.

$$(p \leftrightarrow q \wedge r) \Rightarrow (\sim r \rightarrow \sim p)$$

Solution: Given statement can be written as

$[p \leftrightarrow (q \wedge r)\ ] \Rightarrow [(\sim r) \rightarrow (\sim p)]$

Suppose $A \equiv p \leftrightarrow (q \wedge r)$ and $B \equiv$ **$(\sim r \rightarrow \sim p)$**then A $\Rightarrow B$ is a tautology.

Truth table:

p	q	r	$q \wedge r$	$A \equiv p \leftrightarrow (q \wedge r)$	$\sim r$	$\sim p$	$B \equiv (\sim r) \rightarrow (\sim p)$	$A \Rightarrow B$
T	T	T	T	**T**	F	F	**T**	**T**
T	T	F	F	**F**	T	F	**F**	**T**
T	F	T	F	**F**	F	F	**T**	**T**
T	F	F	F	**F**	T	F	**F**	**T**
F	T	T	T	**F**	F	T	**T**	**T**
F	T	F	F	**T**	T	T	**T**	**T**
F	F	T	F	**T**	F	T	**T**	**T**
F	F	F	F	**T**	T	T	**T**	**T**

Table 3.12 Truth Table

Thus the given statement is a tautology.

2. Obtain the principal disjunctive normal form of the following formula;-

$\boldsymbol{\sim (p \vee q) \leftrightarrow (p \wedge q)}$

Solution: Given: $\sim (p \vee q) \Leftrightarrow (p \wedge q)$

$$\Leftrightarrow \quad \lceil\lfloor \sim (p \vee q) \Rightarrow (p \wedge q) \rceil\rfloor \wedge \lceil\lfloor (p \wedge q) \Rightarrow \sim (p \vee q) \rceil\rfloor$$

$$\Leftrightarrow \quad \lceil\lfloor \sim (p \vee q) \wedge (p \wedge q) \rceil\rfloor \vee \lceil\lfloor (p \vee q) \wedge \sim (p \wedge q) \rceil\rfloor \wedge \lceil\lfloor (p \wedge q) \wedge \sim (p \vee q) \rceil\rfloor \vee \lceil\lfloor (p \vee q) \wedge \sim (p \wedge q) \rceil\rfloor$$

$$\Leftrightarrow [\sim p \wedge \sim q \wedge p \wedge q] \vee \lfloor\lceil (p \vee q) \wedge (\sim p \vee \sim q) \rceil\rfloor \wedge \lceil\lfloor (p \wedge q) \wedge (\sim p \wedge \sim q) \rceil\rfloor \vee \lceil\lfloor (p \vee q) \wedge (\sim p \vee \sim q) \rceil\rfloor$$

$$\Leftrightarrow \quad [\sim p \wedge \sim q \wedge p \wedge q] \vee \lfloor\lceil (p \vee q) \wedge (\sim p \vee \sim q) \rceil\rfloor \qquad \text{[By De-Margon]}$$

$$\Leftrightarrow \quad [\sim p \wedge \sim q \wedge p \wedge q] \vee \lfloor\lceil \{(p \vee q) \wedge \sim p\} \vee \{(p \vee q) \wedge \sim q\} \rceil\rfloor \qquad \text{[By Distributive Law]}$$

$$\Leftrightarrow \quad [\sim p \wedge \sim q \wedge p \wedge q] \vee \lfloor\lceil (p \wedge \sim p) \vee (q \wedge \sim p) \vee (p \wedge \sim q) \vee (q \wedge \sim q) \rceil\rfloor \text{[By Distributive Law]}$$

This is required principle disjunctive normal form.

3. Investigate the validity of the following argument

$p \rightarrow r$

$\sim p \rightarrow q$

$q \rightarrow s$

$\therefore$ **$\sim r \rightarrow s$**

Solution- “If it rains, I will take a leave”, (*P*→*Q*)

“If it is hot outside, I will go for a shower”, (*R*→*S*)

“Either I will not take a leave or I will not go for a shower”, ¬*Q*v¬*S*

Therefore − "Either it rains or it is hot outside"

p	q	r	s	$p \rightarrow r$	$\sim p$	$\sim p \rightarrow q$	$q \rightarrow s$	$(p \rightarrow r) \wedge (\sim p \rightarrow q)$	A	$\sim r$	$B = \sim r \rightarrow s$	$A \Rightarrow B$
T	*T*	*T*	*T*	*T*	*F*	*T*	*T*	*T*	*T*	*F*	*T*	*T*
T	*T*	*T*	*F*	*T*	*F*	*T*	*F*	*T*	*F*	*F*	*T*	*T*
T	*T*	*F*	*T*	*F*	*F*	*T*	*T*	*F*	*F*	*T*	*T*	*T*
T	*T*	*F*	*F*	*F*	*F*	*T*	*F*	*F*	*F*	*T*	*F*	*T*
T	*F*	*T*	*T*	*T*	*F*	*T*	*T*	*T*	*T*	*F*	*T*	*T*
T	*F*	*T*	*F*	*T*	*F*	*T*	*T*	*T*	*T*	*F*	*T*	*T*
T	*F*	*F*	*T*	*F*	*F*	*T*	*T*	*F*	*F*	*T*	*T*	*T*
T	*F*	*F*	*F*	*F*	*F*	*T*	*T*	*F*	*F*	*T*	*F*	*T*
F	*T*	*T*	*T*	*T*	*T*	*T*	*T*	*T*	*T*	*F*	*T*	*T*
F	*T*	*T*	*F*	*T*	*T*	*T*	*F*	*T*	*F*	*F*	*T*	*T*
F	*T*	*F*	*T*	*T*	*T*	*T*	*T*	*T*	*T*	*T*	*T*	*T*
F	*T*	*F*	*F*	*T*	*T*	*T*	*F*	*T*	*F*	*T*	*F*	*T*
F	*F*	*T*	*T*	*T*	*T*	*F*	*T*	*F*	*F*	*F*	*T*	*T*
F	*F*	*T*	*F*	*T*	*T*	*F*	*T*	*F*	*F*	*F*	*T*	*T*
F	*F*	*F*	*T*	*T*	*T*	*F*	*T*	*F*	*F*	*T*	*T*	*T*
F	*F*	*F*	*F*	*T*	*T*	*F*	*T*	*F*	*F*	*T*	*F*	*T*

Table 3.13 Truth Table

Since all entries in the last column are of “*T*” only, therefore *A* *B* is a tautology. Hence the given argument.

4. Prove that the validity of the following argument:

“If Ram is selected in IAS examination, then he will not be able to go to London. Since Ram is going to London, he will not be selected in IAS examination. Solution: Suppose $p \equiv$ Ram is selected in IAS examination

$q \equiv$ Ram is going to London

The given argument, in symbolic form, may be written as

$p \rightarrow {\sim}q$ (Premises)

q (Premises)

$\therefore$ ${\sim}p$ (Conclusion)

Here two premises are $p \rightarrow {\sim}q$, q and conclusion is ${\sim}p$. The given argument will be valid if

$[(p \rightarrow {\sim}q) \wedge (q)] \Rightarrow ({\sim}p)$ is a tautology.

Suppose A $\equiv (p \rightarrow {\sim}q) \wedge (q)$ and B $\equiv {\sim}p$, then A $\Rightarrow$ B is a tautology. Truth table:

p	q	${\sim}q$	$p \rightarrow {\sim}q$	$A \equiv (p \rightarrow {\sim} q) \wedge q$	$B \equiv {\sim} p$	$A \Rightarrow B$
T	T	F	F	F	F	T
T	F	T	T	F	F	T
F	T	F	T	T	T	T
F	T	T	T	F	T	T

Table 3.14 Truth Table

Since all entries in the last column are of “*T*” only, therefore *A* ->*B* is a tautology. Hence the given argument is Valid.

<u>Introduction to Finite State Machine</u>

Finite state machine :a finite state machine (sometimes called a finite state automaton) is a computation model that can be implemented with hardware or software and can be used to simulate sequential logic and some computer programs. Finite state automata generate regular languages. Finite state machines can be used to model problems in many fields including mathematics, artificial intelligence, games, and linguistics.

A Finite state machine has 6 tuples (Q, Σ , $\delta : Q \times \Sigma \rightarrow Q$, g, q_0, q_f)

1. Finite set of states Q
2. Finite input alphabet Σ
3. Transition function $\delta : Q \times \Sigma \rightarrow Q$
4. Various possibilities for output g
5. Initial state q_0
6. Final state q_f

Finite state machines as models of physical system equivalence machines:

Deterministic Finite-State Automata

A DFSA can be formally defined as A = (Q, Σ, 6, q_0, F):

- Q, a finite set of states
- Σ, a finite alphabet of input symbols
- q0 ∈ Q, an initial start state
- F ⊆ Q, a set of final states
- 6 (delta): Q x Σ → Q, a transition function

We can define 6 on words, 6_w, by using a recursive definition:

- 6_w : Q x Σ* → Q a function of (state, word) to a state
- 6_w(q,ε) = q in state q, output state q if word is ε
- 6_w(q,xa) = 6(6_w(q,x),a) otherwise, use 6 for one step and recurse

For an automaton A, we can define the language of A:

- L(A) = {w∈Σ* : 6_w(q_0,w) ∈ F }
- L (A) is a subset of all words w of finite length over Σ, such that the transition function 6_w(q_0,w) produces a state in the set of final states (F).
- Intuitively, if we think of the automaton as a graph structure, then the words in L(A) represent the "paths" which end in a final state. If we concatenate the labels from the edges in each such path, we derive a string w ∈L(A).

1. States are shown as circles;
2. the start state is indicated by the bold incoming arrow.
3. The next state function and output functions are shown using directed arrows from one state to

another. Each arrow is labeled with one element of I and one element of O.

4. If the machine is in some state s and the current input symbol is x, then we follow the arc labeled x/y from s to a new state and produce output y.

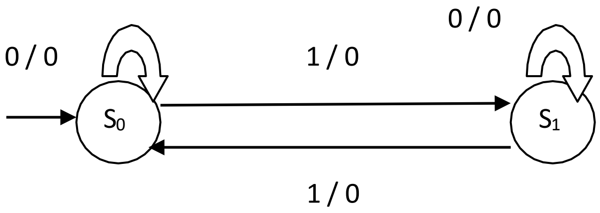


Figure 3.1

Finite State Machines as Language Recognizers

Input = {0,1}

acceptingstate : A state is said to be an accepting state if its output is 1.

rejectingstate : A state is said to be an rejecting state if its output is 0.

An input sequence is said to be accepted by the finite state machine if it leads the machine from the initial state to an accepting state. On the other hand, an input sequence is said to be rejected by the finite state machine if it leads the machine from the initial state to an rejecting state.

finite state language

A language is said to be a finite state language if there is a finite state machine that accepts exactly all sentences in the language.

Theorem Let L be a finite state language accepted by a finite state machine with N states. For any sequence α whose length is N or larger in the language, α can be written as uvw such that v is nonempty and uv^iw is also in the language for $i \geqq 0$, where vi denotes the concatenation of i copies of the sequence v. (In other words, uw, uvw, uvvw, uvvvw, … are all in the language.)

Proof :

Letα= a1a2a3…aN, without loss of generality.

Let s_{j0}, s_{j1}, s_{j2}, …,s_{jN} denote the states the machine visits, where s_{j0} is the initial state and s_{jN} is an accepting state.

Among the N+1 states s_{j0}, s_{j1}, s_{j2}, …,s_{jN} there are two of them that are the same. Suppose that is state s_k, we realize that the sequences uw, uvw, uvvw, uvvvw, …, uv^lw, … will all lead the machine from the initial state s_{j0} to the accepting state s_{jN}.

Subject Notes
CS301 - Discrete Structures
UNIT-4

Graph

Definition − A graph (denoted as $G=(V,E)$) consists of a non-empty set of vertices or nodes V and a set of edges E.

Example − Let us consider, a Graph is $G=(V,E)$where $V=\{a,b,c,d\}$ and $E=\{\{a,b\},\{a,c\},\{b,c\},\{c,d\}\}$

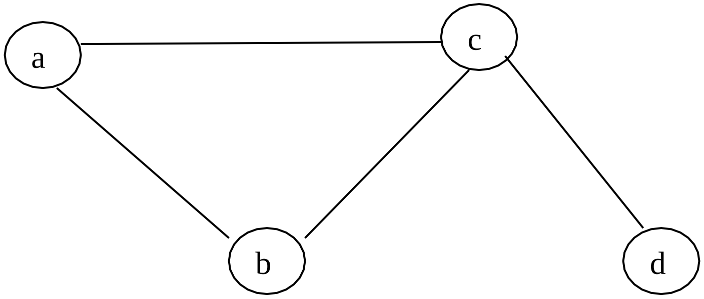


Figure 4.1 Example of Graph

Degree of a Vertex − The degree of a vertex V of a graph G (denoted by deg (V)) is the number of edges incident with the vertex V.

Example Consider the figure no. 4.1

Vertex	Degree	Even / Odd
a	2	even
b	2	even
c	3	odd
d	1	odd

Table 4.1 Degree of Vertex

Even and Odd Vertex − If the degree of a vertex is even, the vertex is called an even vertex and if the degree of a vertex is odd, the vertex is called an odd vertex.

Degree of a Vertex − The degree of a graph is the largest vertex degree of that graph. For the above graph the degree of the graph is 3.

The Handshaking Lemma − In a graph, the sum of all the degrees of all the vertices is equal to twice the number of edges.

Types of Graphs

There are different types of graphs, which we will learn in the following section.

1. **Null Graph -** A null graph has no edges. The null graph of n vertices is denoted by Nn

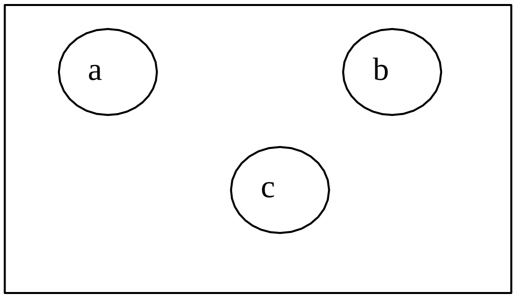


Figure 4.2 Null Graph

2. **Simple Graph** -A graph is called simple graph/strict graph if the graph is undirected and does not contain any loops or multiple edges.

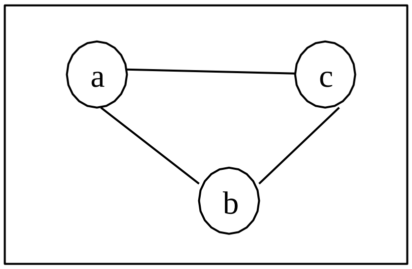


Figure 4.3 Simple Graph

3. **Directed and Undirected Graph -** A graph *G*=(*V*,*E*) is called a directed graph if the edge set is made of ordered vertex pair and a graph is called undirected if the edge set is made of unordered vertex pair.

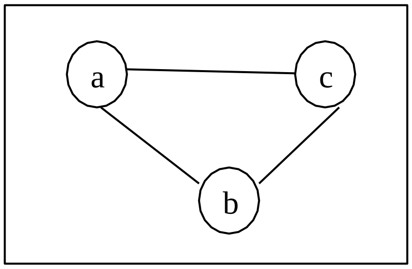


Figure 4.4 Undirected Graph

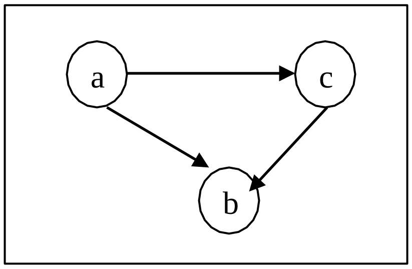


Figure 5.5 Directed Graph

4. **Connected and Disconnected Graph -** A graph is connected if any two vertices of the graph are connected by a path; while a graph is disconnected if at least two vertices of the graph are not connected by a path. If a graph G is disconnected, then every maximal connected subgraph of *G* is called a connected component of the graph *G*

.

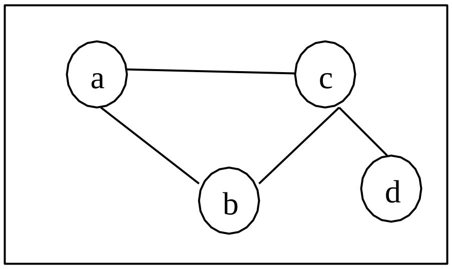


Figure 4.6 Connected Graph

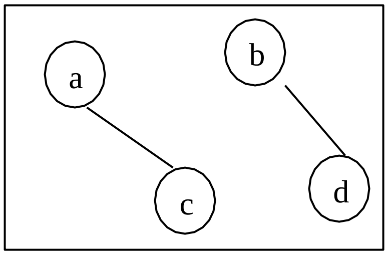


Figure 4.7 Disconnected Graph

5. **Regular Graph -** A graph is regular if all the vertices of the graph have the same degree. In a regular graph G of degree *r*, the degree of each vertex of *G* is r.

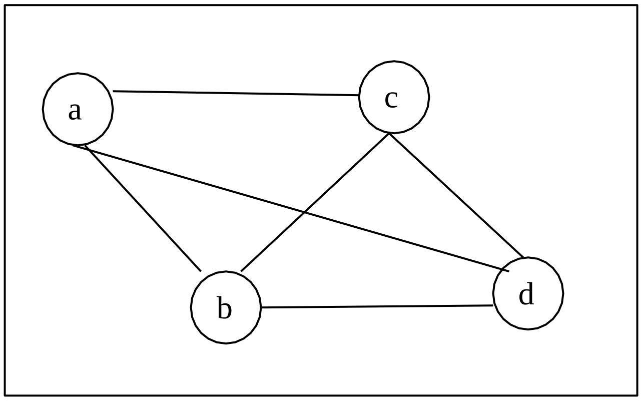


Figure 4.8 Regular Graph

6. **Complete Graph-** A graph is called complete graph if every two vertices pair are joined by exactly one edge. The complete graph with n vertices is denoted by *Kn*

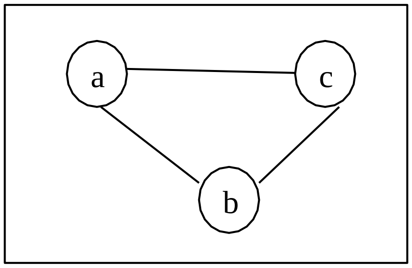


Figure 4.9 Complete Graph

7. **Cycle Graph**- If a graph consists of a single cycle, it is called cycle graph. The cycle graph with n vertices is denoted by *Cn*

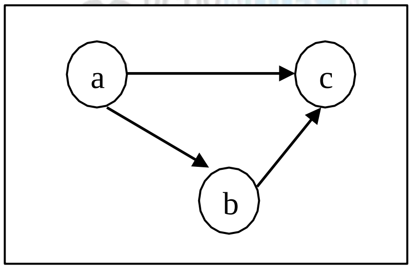


Figure 4.10 Cycle Graph

8. **Bipartite Graph** - If the vertex-set of a graph G can be split into two disjoint sets, *V*1 and *V*2, in such a way that each edge in the graph joins a vertex in *V*1 to a vertex in *V*2, and there are no edges in G that connect two vertices in *V*1 or two vertices in *V*2, then the graph *G* is called a bipartite graph.

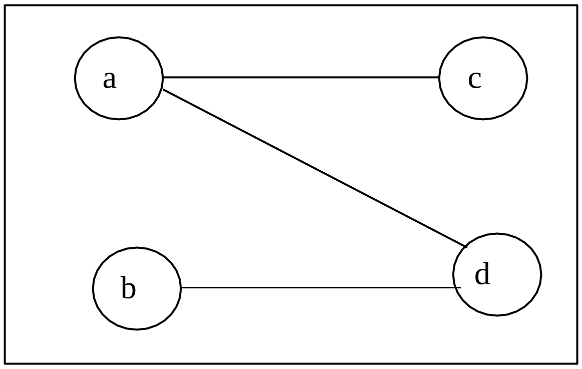


Figure 4.11 Bipartite Graph

9. **Complete Bipartite Graph-** A complete bipartite graph is a bipartite graph in which each vertex in the first set is joined to every single vertex in the second set. The complete bipartite graph is denoted by *Kx*,*y* where the graph *G* contains *x* vertices in the first set and *y* vertices in the second set.

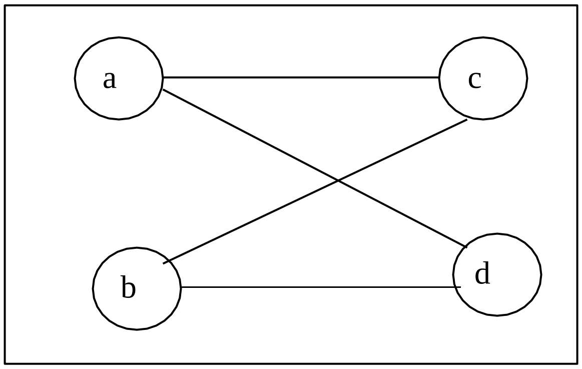


Figure 4.12 Complete Bipartite Graph

Representation of Graphs

There are mainly two ways to represent a graph –

1. Adjacency Matrix
2. Adjacency List

1. **Adjacency Matrix -** An Adjacency Matrix *A*[*V*][*V*] is a 2D array of size *V*×*V* where *V* is the number of vertices in a undirected graph. If there is an edge between *Vx* to *Vy* then the value of *A*[*Vx*][*Vy*]=1 and *A*[*Vy*][*Vx*]=1, otherwise the value will be zero. And for a directed graph, if there is an edge between *Vx* to *Vy*, then the value of *A*[*Vx*][*Vy*]=1 , otherwise the value will be zero.

Adjacency Matrix of an Undirected Graph

Let us consider the following undirected graph and construct the adjacency matrix –

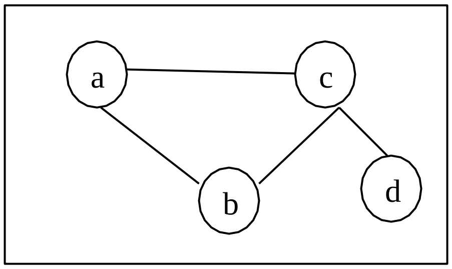


Figure 4.13 Undirected Graph

Adjacency matrix of the above undirected graph will be –

	a	b	c	d
a	0	1	1	0
b	1	0	1	0
c	1	1	0	1
d	0	0	1	0

Table 4.2 Representation of Adjacency matrix of an Undirected Graph

Adjacency Matrix of a Directed Graph

Let us consider the following directed graph and construct its adjacency matrix –

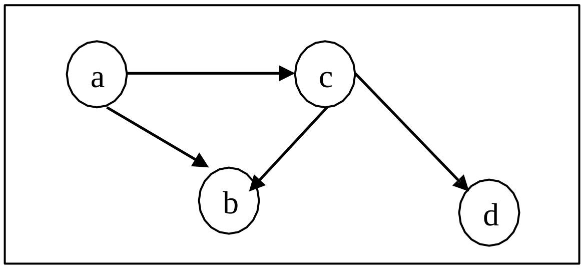


Figure 4.14 Directed Graph

Adjacency matrix of the above directed graph will be –

	a	**b**	**c**	**d**
a	0	1	1	0
b	0	0	1	0
c	0	0	0	1
d	0	0	0	0

Table 4.3 Representation of Adjacency matrix of an Directed Graph

2. **Adjacency List -** In adjacency list, an array (*A*[*V*]) of linked lists is used to represent the graph G with *V* number of vertices. An entry *A*[*Vx*] represents the linked list of vertices adjacent to the *Vx*−*th* vertex. The adjacency list of the undirected graph is as shown in the figure below −

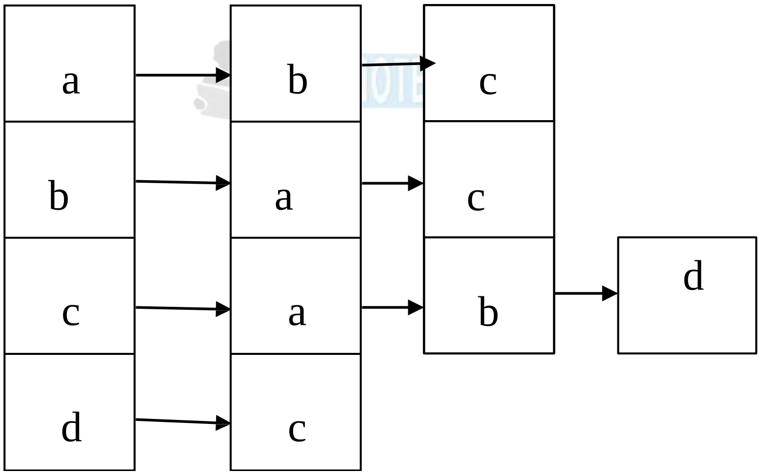


Figure 4.15 Adjacency List

Planar graph − A graph *G* is called a planar graph if it can be drawn in a plane without any edges crossed. If we draw graph in the plane without edge crossing, it is called embedding the graph in the plane.

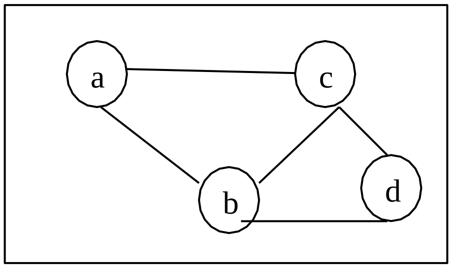


Figure 4.15 Planar Graph

Non-planar graph − A graph is non-planar if it cannot be drawn in a plane without graph edges crossing.

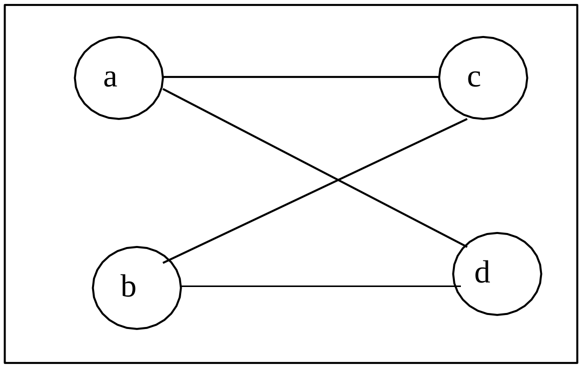


Figure 4.16 Non Planar Graph

Multi-Graph- If in a graph multiple edges between the same set of vertices are allowed, it is called Multigraph. In other words, it is a graph having at least one loop or multiple edges.

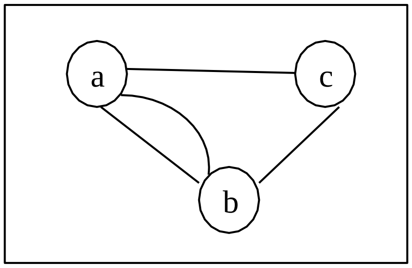


Figure 4.17 Multi Graph

Weighted Graph- In a weighted graph, each edge is assigned a weight or cost.

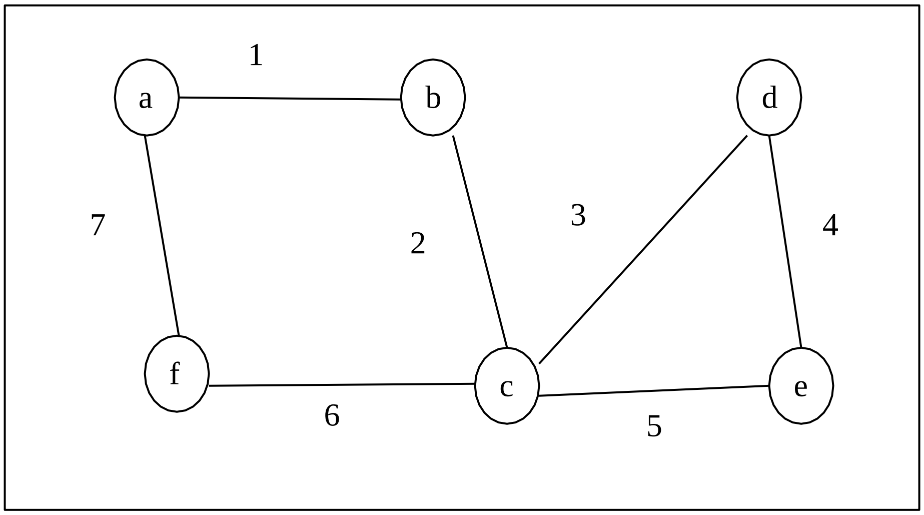


Figure 4.18 Weighted Graph

Isomorphic Graphs- If two graphs G and H contain the same number of vertices connected in the same way, they are called isomorphic graphs (denoted by *G*≅*H*).

It is easier to check non-isomorphism than isomorphism. If any of these following conditions occurs, then two graphs are non-isomorphic −

i. The number of connected components are different
ii. Vertex-set cardinalities are different
iii. Edge-set cardinalities are different
iv. Degree sequences are different

Example

The following graphs are isomorphic –

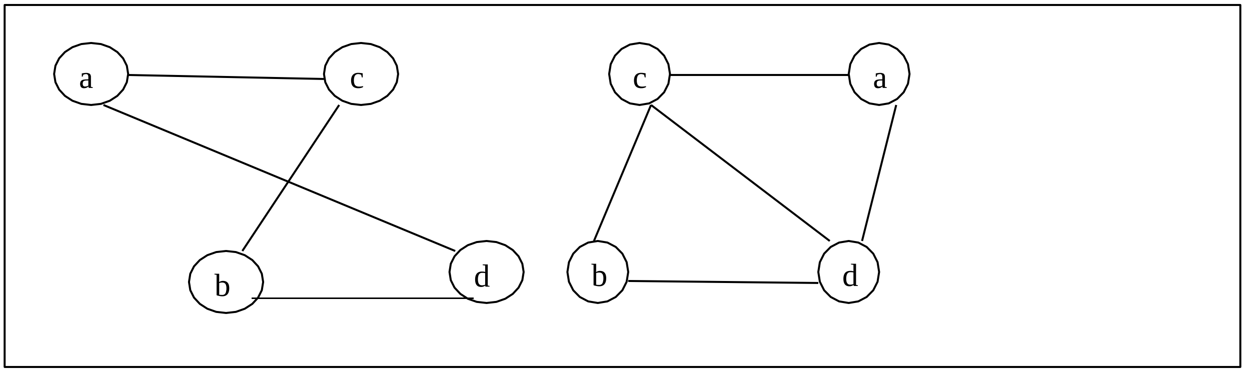


Figure 4.19 Isomorphic Graphs

Path - A path is a sequence of vertices such that each vertex is adjacent to the next. In a path, each edge can be traveled **only once**. The length of a path is the number of edges in that path.

Cycle - A path that starts and ends at the same vertex is called a circuit or Cycle.

Connectivity - A graph is *connected* if any two vertices can be joined by a path. If this is not possible then the graph is disconnected.

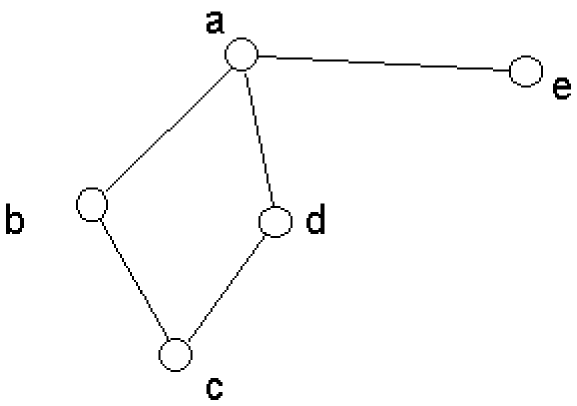


Figure 4.20 Path, Cycle, Connectivity

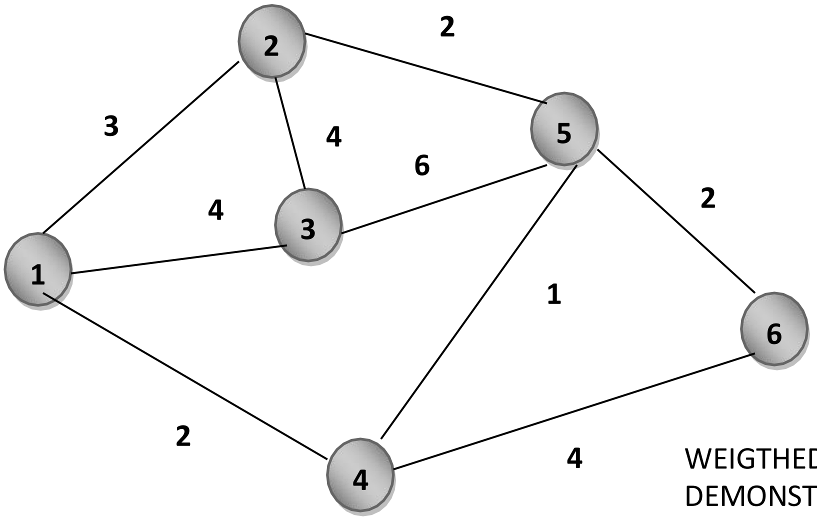
Shortest Path in Weighted Graph

Dijkstra algorithm-

1. It maintains a list of unvisited vertices.
2. It chooses a vertex (the source) and assigns a maximum possible cost (i.e. infinity) to every other vertex.
3. The cost of the source remains zero as it actually takes nothing to reach from the source vertex to itself.
4. In every subsequent step of the algorithm it tries to improve(minimize) the cost for each vertex. Here the cost can be distance, money or time taken to reach that vertex from the source vertex. The minimization of cost is a multi-step process.
    a. For each unvisited neighbor (vertex 2, vertex 3, vertex 4) of the current vertex (vertex 1) calculate the new cost from the vertex (vertex 1).
    b. For e.g. the new cost of vertex 2 is calculated as the minimum of the two ((existing cost of vertex 2) or (sum of cost of vertex 1 + the cost of edge from vertex 1 to vertex 2))
5. When all the neighbors of the current node are considered, it marks the current node as visited and is removed from the unvisited list.

6. Select a vertex from the list of unvisited nodes (which has the smallest cost) and repeat step 4.
7. At the end there will be no possibilities to improve it further and then the algorithm ends

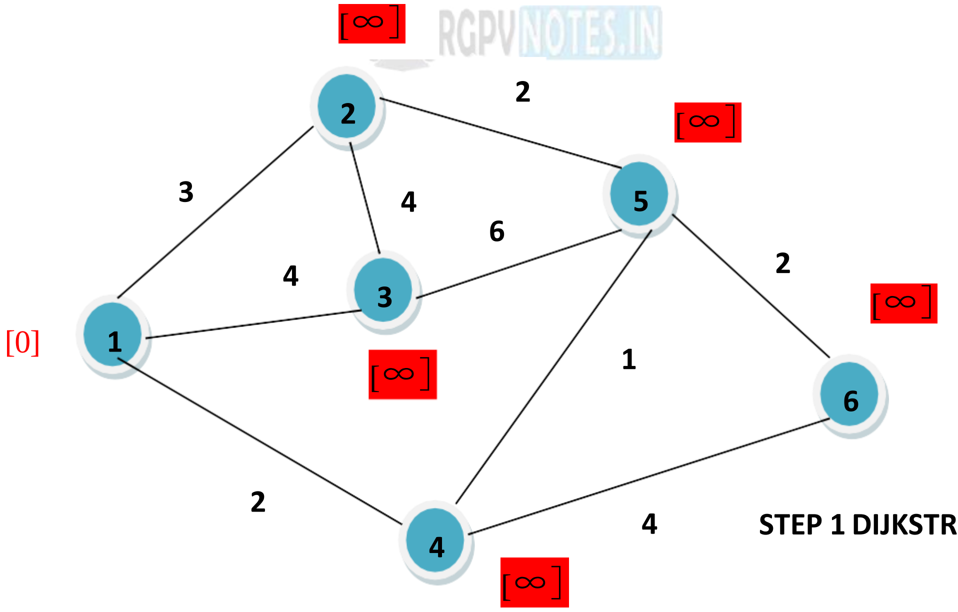
For demonstration we will consider the below graph:



WEIGTHED GRAPH FOR
DEMONSTRATING DIJKSTRA'S

Figure 4.21 Weighted Graph

Step 1:Mark Vertex 1 as the source vertex. Assign a cost zero to Vertex 1 and (infinite to all other vertices). The state is as follows:



STEP 1 DIJKSTRA'S ALGORITHMS

Figure 4.21(a) Step 1

Step 2: For each of the unvisited neighbors (Vertex 2, Vertex 3 and Vertex 4) calculate the minimum cost as min(current cost of vertex under consideration, sum of cost of vertex 1 and connecting edge). Mark Vertex 1 as visited , in the diagram we border it black. The new state would be as follows:

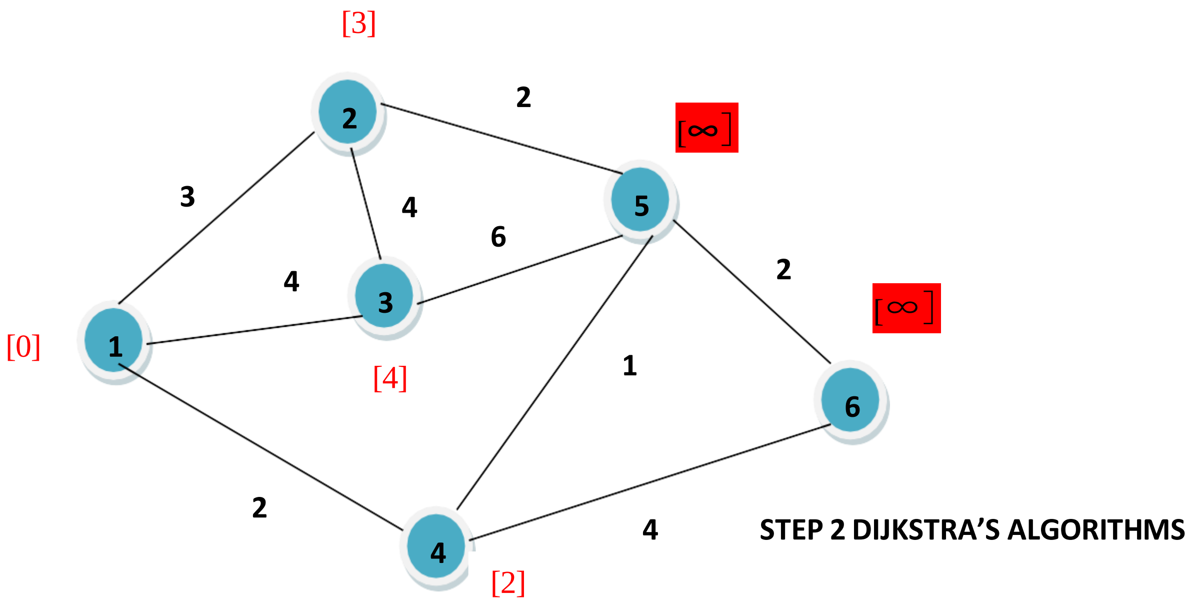


Figure 4.21(b) Step 2

Step 3: Choose the unvisited vertex with minimum cost (vertex 4) and consider all its unvisited neighbors (Vertex 5 and Vertex 6) and calculate the minimum cost for both of them. The state is as follows:

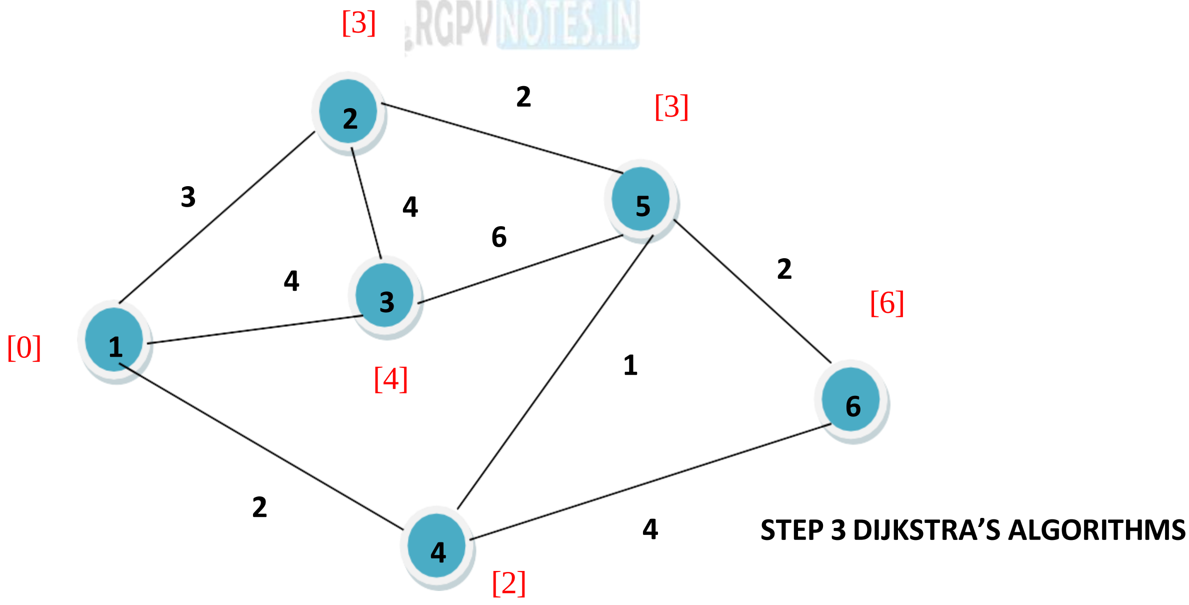


Figure 4.21(c) Step 3

Step 4: Choose the unvisited vertex with minimum cost (vertex 2 or vertex 5, here we choose vertex 2) and consider all its unvisited neighbors (Vertex 3 and Vertex 5) and calculate the minimum cost for both of them. Now, the current cost of Vertex 3 is [4] and the sum of (cost of Vertex 2 + cost of edge (2,3)) is 3 + 4 = [7]. Minimum of 4, 7 is 4. Hence the cost of vertex 3 won't change. By the same argument the cost of vertex 5 will not change. We just mark the vertex 2 as visited, all the costs remain same. The state is as follows:

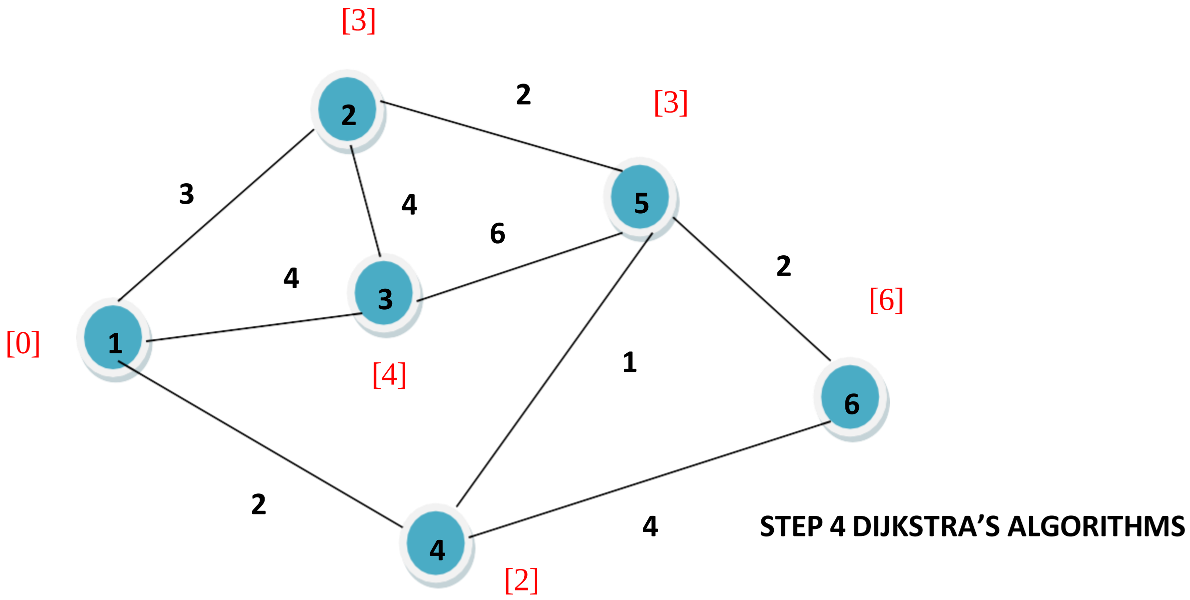


Figure 4.21(d) Step 4

Step 5: Choose the unvisited vertex with minimum cost (vertex 5) and consider all its unvisited neighbors (Vertex 3 and Vertex 6) and calculate the minimum cost for both of them. Now, the current cost of Vertex 3 is [4] and the sum of (cost of Vertex 5 + cost of edge (5,3)) is 3 + 6 = [9]. Minimum of 4, 9 is 4. Hence the cost of vertex 3 won't change. Now, the current cost of Vertex 6 is [6] and the sum of (cost of Vertex 5 + cost of edge (3,6)) is 3 + 2 = [5]. Minimum of 6, 5 is 45. Hence the cost of vertex 6 changes to 5. The state is as follows:

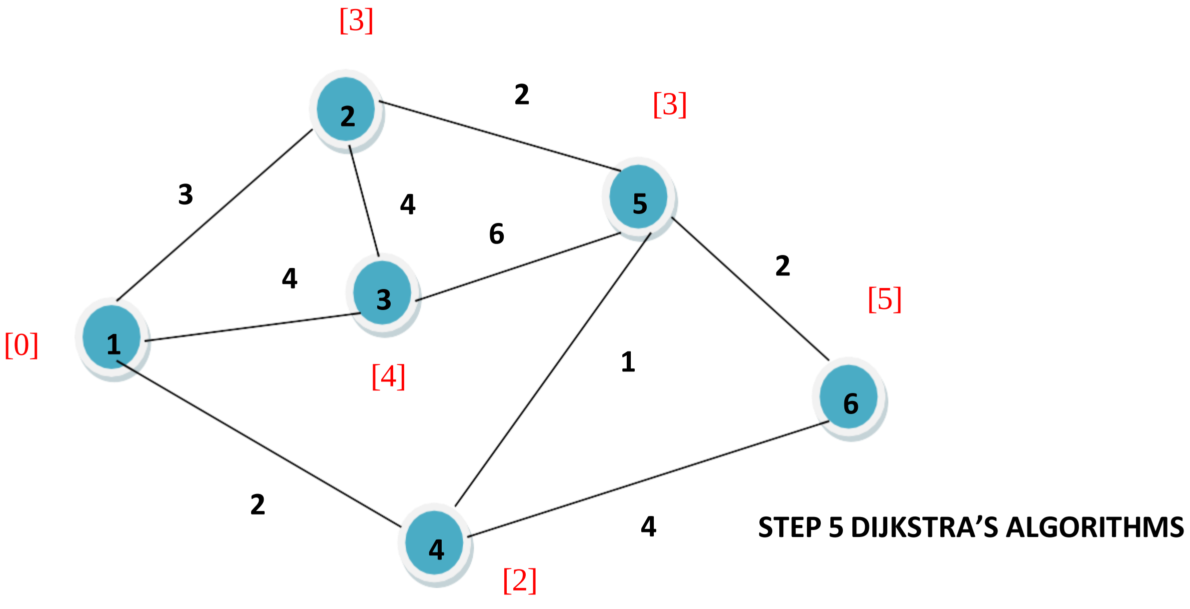


Figure 4.21(e) Step 5

Step 6: Choose the unvisited vertex with minimum cost (vertex 3) and consider all its unvisited neighbors (none). So mark it visited. The state is as follows:

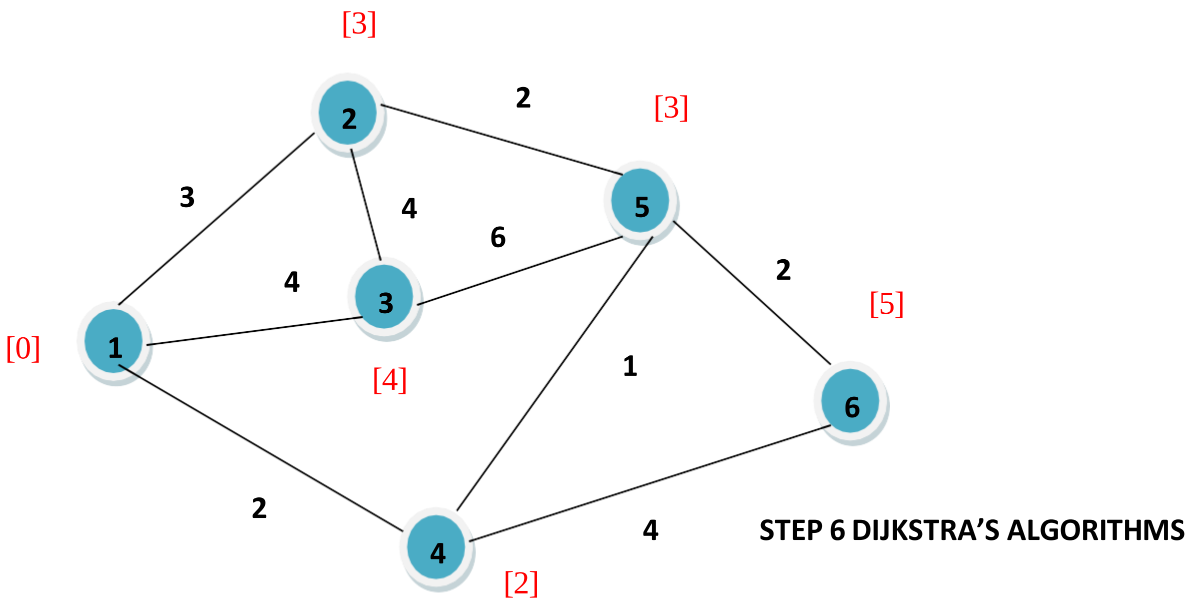


Figure 4.21(f) Step 6

Step 7: Choose the unvisited vertex with minimum cost (vertex 6) and consider all its unvisited neighbors (none). So mark it visited. The state is as follows:

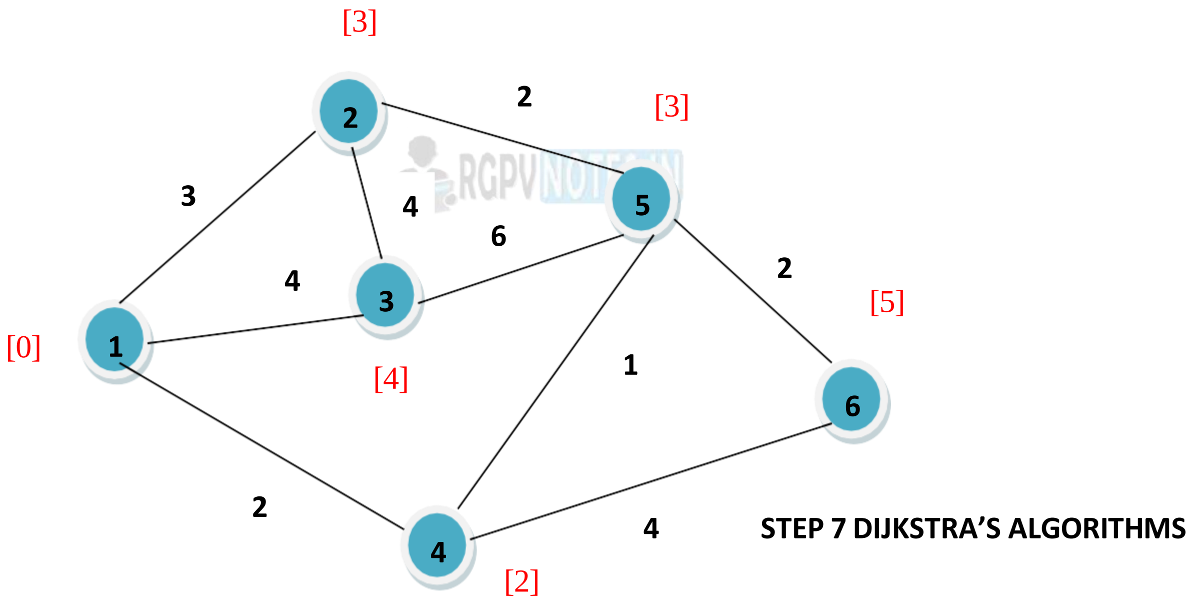


Figure 4.21(g) Step 7

Now there is no unvisited vertex left and the execution ends. At the end we know the shortest paths for all the vertices from the source vertex 1. Even if we know the shortest path length, we do not know the exact list of vertices which contributes to the shortest path until we maintain them separately or the data structure supports it.

Numerical

Find the shortest path between a to z using Dijkstra's algorithm.

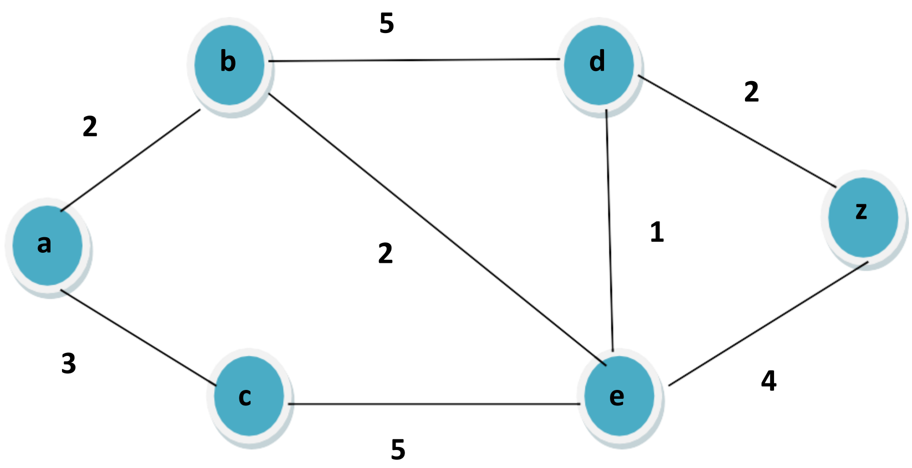


Figure 4.22 Example to find shortest path

Solution

Consider the graph G=(V,E), Where V is the set of Vertices and E is the set of Edges.

V= {a,b,c,d,e,z}

Step -1 P1 ={a} **T1= V-P1**

T1 = {b,c,d,e,z}

l(b) =2, l(c)=3, l(d)= ∞ , l(e)= ∞, l(z)= ∞

b has the minimum index 2.

Step-2 P2 ={a,b} **T2= V-P2**

T2= {c,d,e,z}

l(c)= min(3, 2+∞) =3
l(d)= min(∞, 2+5)=7
l(e)= min(∞, 2+2)=4
l(z)= min (∞, 2+∞)=∞

c has the minimum index 3.

Step-3 P3 ={a,b,c} **T3= V-P3**

T3={d,e,z}

l(d)=min{7, 3+5} = 7
l(e)=min(4, 4+1} = 4
l(z)=min(∞, 3+∞}=∞

e has the minimum index 4.

Step-4 P4 ={a,b,c,e} **T4= V-P4**

T4={d,z}

l(d)=min{7, 4+1} = 5
l(z)=min(∞, 4+4}=8

d has the minimum index 5.

Step-5 P5 ={a,b,c,e,d} **T5= V-P5**

T5={z}

l(z)=min(8, 5+2}=7

Hence the minimum distance from the source a to destination z is 7.

The Shortest path is **a -> b -> e -> d ->z**

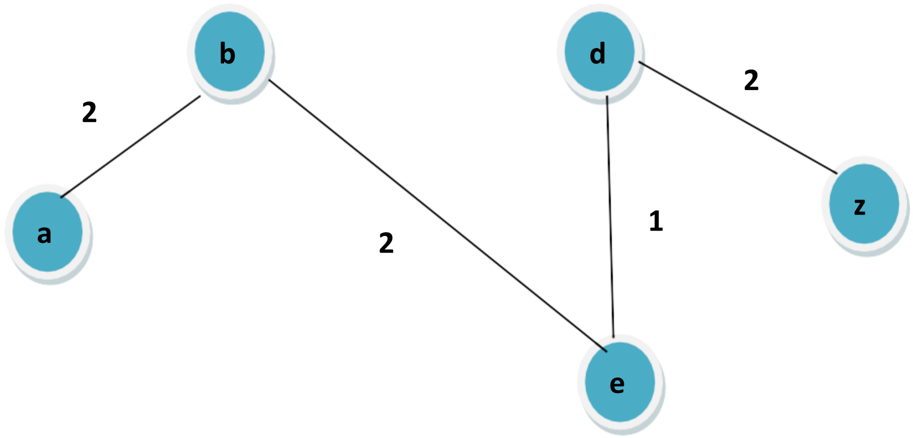


Figure 4.22 (a) Solution of shortest path

Eulerian Path and Circuits - A connected graph ***G*** is called an Euler graph, if there is a closed trail which includes every edge of the graph ***G*** . An Euler path is a path that uses every edge of a graph exactly once. An Euler path starts and ends at different vertices. An Euler circuit is a circuit that uses every edge of a graph exactly once. An Euler circuit always starts and ends at the same vertex. A connected graph ***G*** is an Euler graph if and only if all vertices of ***G*** are of even degree, and a connected graph ***G*** is Eulerian if and only if its edge set can be decomposed into cycles.

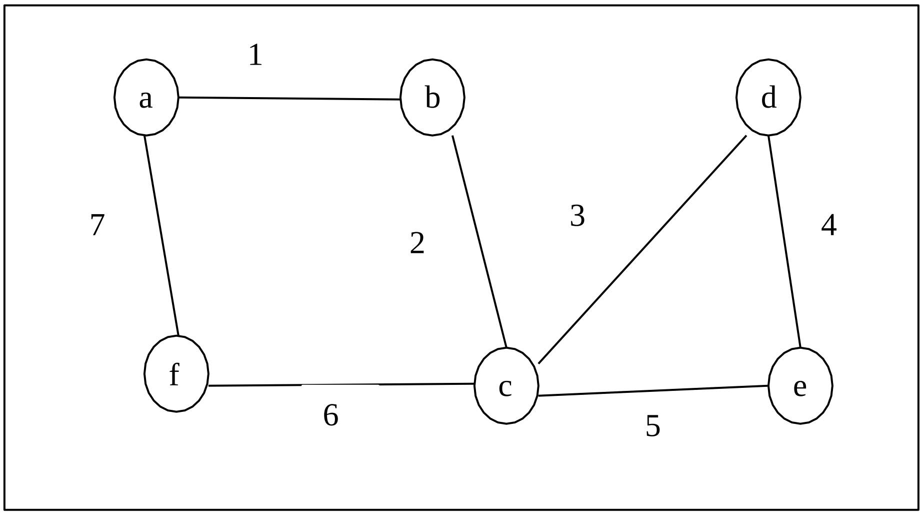


Figure 4.23 Eulerian Path and Circuits

The above graph is an Euler graph as "*a*1*b*2*c*3*d*4*e*5*c*6*f*7*g*"covers all the edges of the graph.

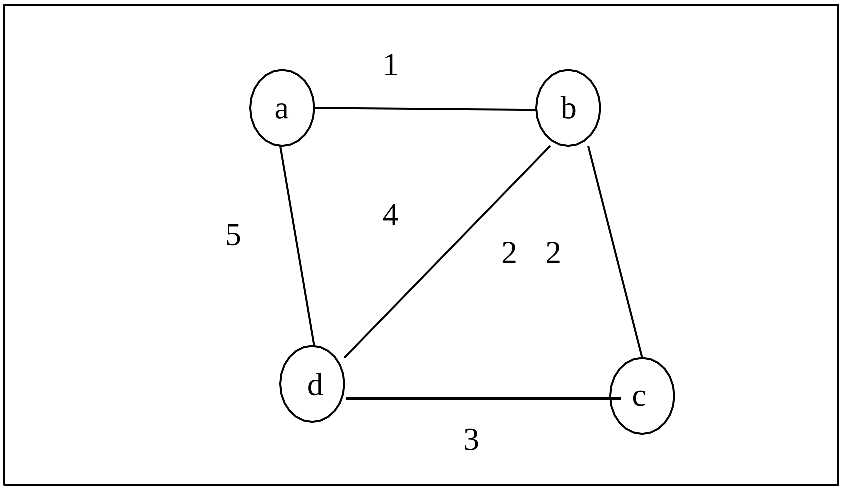


Figure 4.24 Eular Graph

__Hamiltonian Paths and circuits__ **-** A connected graph ***G*** is called Hamiltonian graph if there is a cycle which includes every vertex of ***G*** and the cycle is called Hamiltonian cycle. Hamiltonian walk in graph ***G*** is a walk that passes through each vertex exactly once. If ***G*** is a simple graph with n vertices, where ***n***≥3 If ***deg*(*v*)≥*n***2 for each vertex ***v***, then the graph ***G*** is Hamiltonian graph. This is called Dirac's Theorem. If ***G*** is a simple graph with ***n*** vertices, where ***n***≥2 if ***deg*(*x*)+*deg*(*y*)≥*n*** for each pair of non-adjacent vertices x and y, then the graph ***G*** is Hamiltonian graph. This is called Ore's theorem.

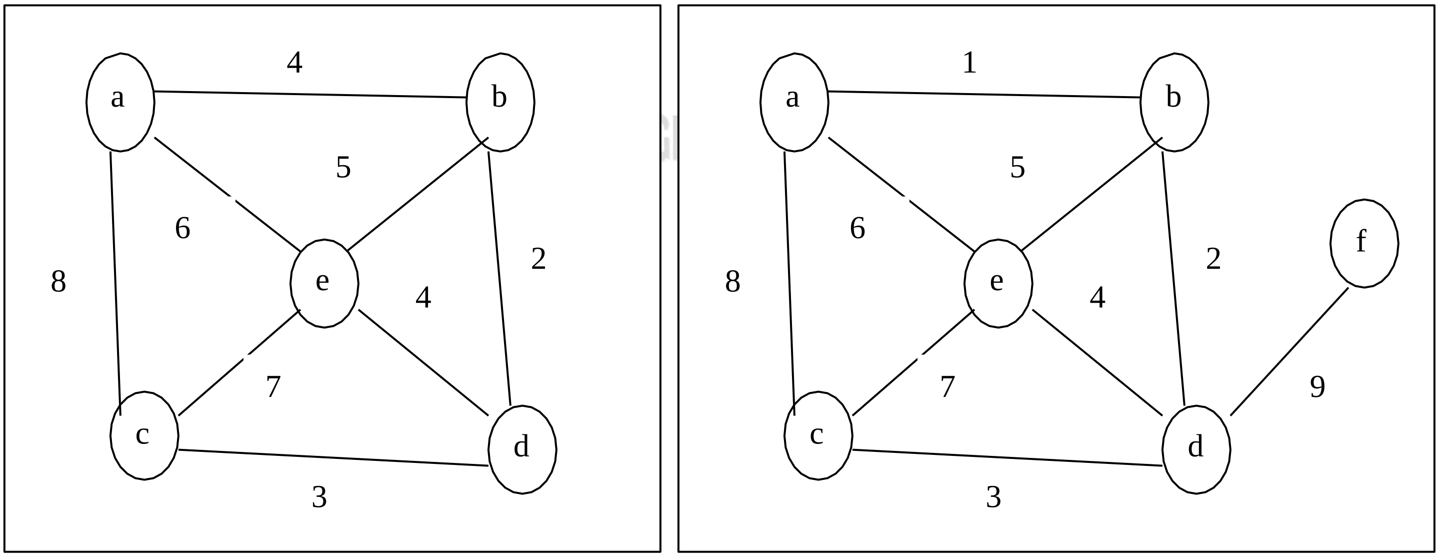


Figure 4.25 Hamiltonian Paths and circuits

__Graph Coloring__ **-** Graph coloring is the procedure of assignment of colors to each vertex of a graph G such that no adjacent vertices get same color. The objective is to minimize the number of colors while coloring a graph. The smallest number of colors required to color a graph G is called its chromatic number of that graph. Graph coloring problem is a NP Complete problem.

Method to Color a Graph

The steps required to color a graph G with n number of vertices are as follows −

Step 1 − Arrange the vertices of the graph in some order.

Step 2 − Choose the first vertex and color it with the first color.

Step 3 − Choose the next vertex and color it with the lowest numbered color that has not been colored on any vertices adjacent to it. If all the adjacent vertices are colored with this color, assign a new color to it. Repeat this step until all the vertices are colored.

Example

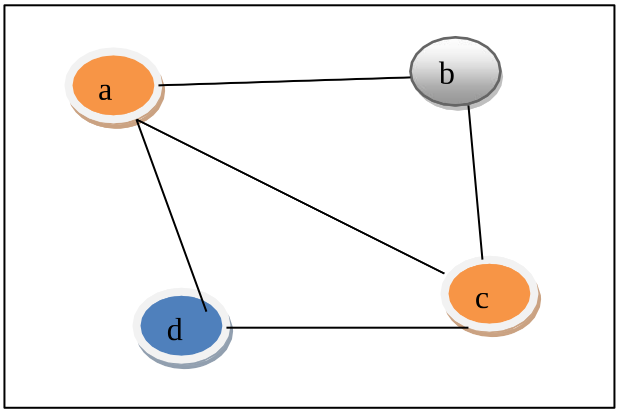


Figure 4.26 Graph Coloring

In the above figure, at first vertex *a* is colored red. As the adjacent vertices of vertex a are again adjacent, vertex *b* and vertex *d* are colored with different color, green and blue respectively. Then vertex *c* is colored as red as no adjacent vertex of *c* is colored red. Hence, we could color the graph by 3 colors. Hence, the chromatic number of the graph is 3.

Chromatic Number- The chromatic number of a graph $G$is the smallest number of colors needed to color the vertices of G so that no two adjacent vertices share the same color, i.e., the smallest value of $k$possible to obtain a k-coloring.

Isomorphism - If two graphs G and H contain the same number of vertices connected in the same way, they are called isomorphic graphs (denoted by ***G***≅***H***).

It is easier to check non-isomorphism than isomorphism. If any of these following conditions occurs, then two graphs are non-isomorphic −

v. The number of connected components are different

vi. Vertex-set cardinalities are different

vii. Edge-set cardinalities are different

viii. Degree sequences are different

Example

The following graphs are isomorphic −

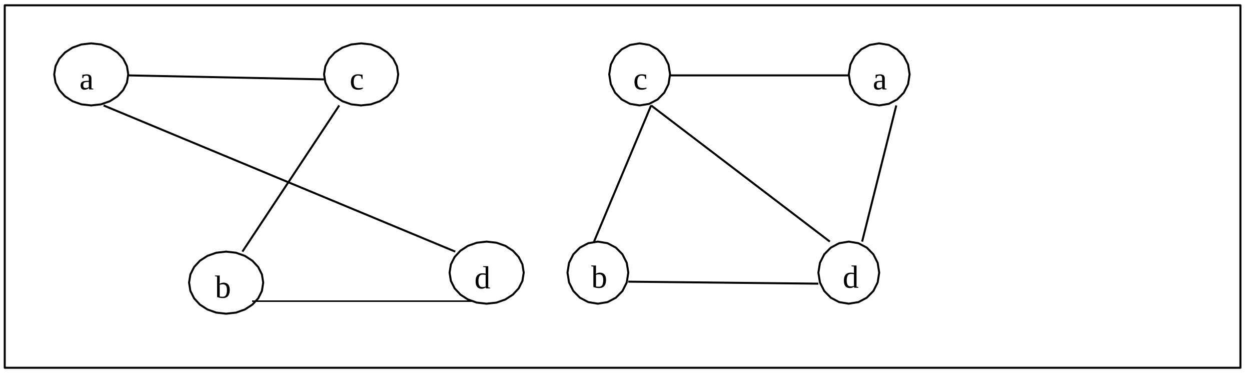


Figure 4.27 Isomorphism

Homomorphism - A homomorphism from a graph ***G*** to a graph ***H*** is a mapping (May not be a bijective mapping)***h***:***G***&***H*** such that − **(*x*,*y*)∈*E*(*G*)&(*h*(*x*),*h*(*y*))∈*E*(*H*)**. It maps adjacent vertices of graph ***G*** to the adjacent vertices of the graph ***H.***

Properties of Homomorphisms

i. A homomorphism is an isomorphism if it is a bijective mapping.

ii. Homomorphism always preserves edges and connectedness of a graph.

iii. The compositions of homomorphisms are also homomorphisms.

UNIT-5

Partially Ordered Set (POSET) - A partially ordered set consists of a set with a binary relation which is reflexive, antisymmetric and transitive. "Partially ordered set" is abbreviated as POSET.

Examples

1. **The set of real numbers under binary operation less than or equal to (≤) is a poset.**

Solution - Let the set S={1,2,3} and the operation is ≤

The relations will be {(1,1),(2,2),(3,3),(1,2),(1,3),(2,3)}

This relation R is reflexive as {(1,1),(2,2),(3,3)}$\in R$

This relation R is anti-symmetric, as

{(1,2),(1,3),(2,3)}$\in R$ *and* {(1,2),(1,3),(2,3)}$ø R$

This relation R is also transitive as {(1,2),(2,3),(1,3)}$\in R$

Hence, it is a **poset**.

The vertex set of a directed acyclic graph under the operation ‘reachability’ is a poset.

Hasse Diagram - The Hasse diagram of a poset is the directed graph whose vertices are the element of that poset and the arcs covers the pairs (x, y) in the poset. If in the poset $x<y$, then the point x appears lower than the point y in the Hasse diagram. If $x<y<z$ in the poset, then the arrow is not shown between x and z as it is implicit.

Example

The poset of subsets of {1,2,3}={∅,{1},{2},{3},{1,2},{1,3},{2,3},{1,2,3}} is shown by the following Hasse diagram –

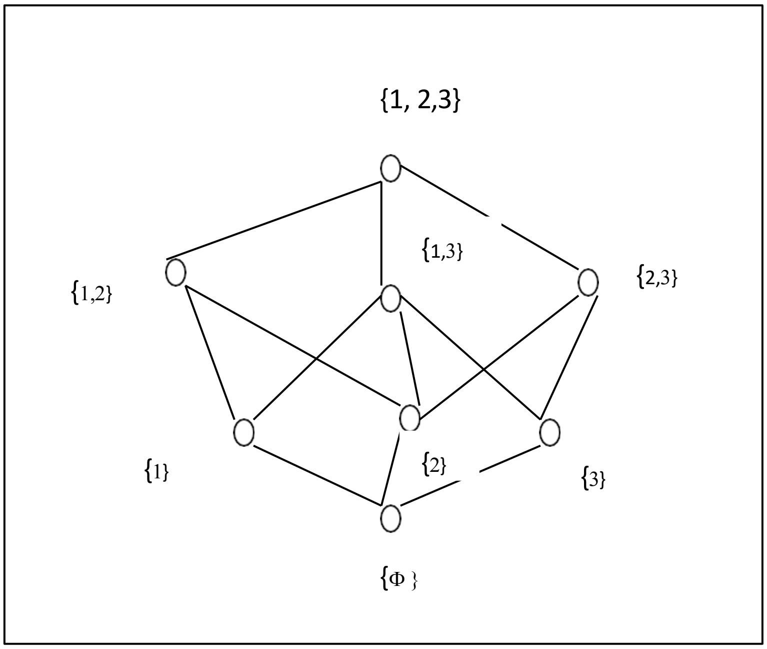


Figure 5.1 Hasse Diagram

Linearly Ordered Set - A Linearly ordered set or Total ordered set is a partial order set in which every pair of element is comparable. The elements $a,b \in S$ are said to be comparable if either $a \le b$ or $b \le a$ holds. Trichotomy law defines this total ordered set. A totally ordered set can be defined as a distributive lattice having the property {*a*v*b*,*a*A*b*}={*a*,*b*} for all values of a and b in set S.

Example

The powerset of {*a*,*b*} ordered by \subseteq is a totally ordered set as all the elements of the power set *P*={∅,{*a*},{*b*},{*a*,*b*}} are comparable.

Example of non-total order set

A set *S*={1,2,3,4,5,6} under operation x divides y is not a total ordered set.

Here, for all $(x,y) \in S, x|y$ have to hold but it is not true that 2 | 3, as 2 does not divide 3 or 3 does not divide 2. Hence, it is not a total ordered set.

Isomorphic Ordered Set - Two partially ordered sets are said to be isomorphic if their "structures" are entirely analogous. Formally, partially ordered sets $P=(X, \le)$and $Q=(X', \le')$are isomorphic if there is a bijection $f$from $X$to X'such that $x_1 \le x_2$precisely when $f(x_1) \le' f(x_2)$.

Well Ordered Set - A well-ordered set is a totally ordered set in which every nonempty subset has a least member.

Lattice - A lattice is a poset (*L*,≤) for which every pair {*a*,*b*}∈*L* has a least upper bound (denoted by *a*v*b*) and a greatest lower bound (denoted by *a*Λ*b*). LUB ({*a*,*b*}) is called the join of a and b. GLB ({*a*,*b*}) is called the meet of a and b.

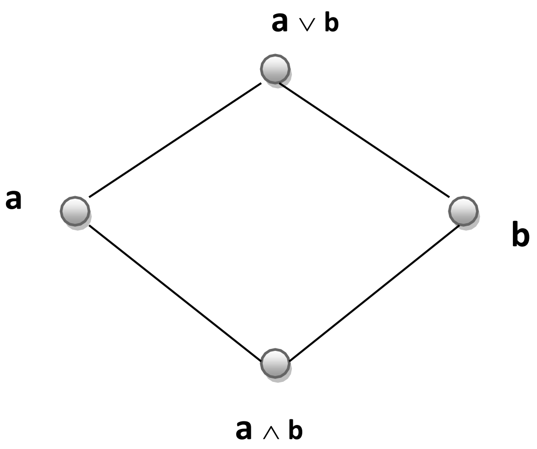


Figure 5.2 Lattice

Example

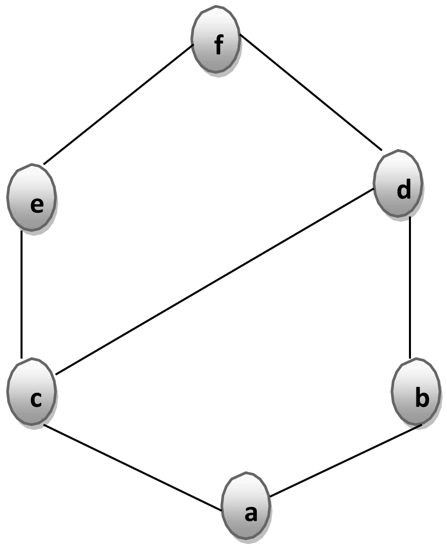


Figure 5.2.1 Example of Lattice

This above figure is a lattice because for every pair {*a*,*b*}∈*L* , a GLB and a LUB exists.

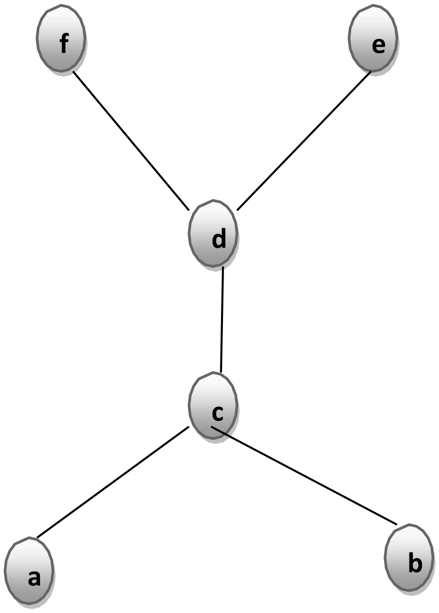


Figure 5.2.2 Lattice

This above figure is a not a lattice because $GLB(a,b)$ and $LUB(e,f)$ does not exist.

Some other lattices are discussed below −

1. **Bounded Lattice -** A lattice L becomes a bounded lattice if it has a greatest element 1 and a least element 0.
2. **Complemented Lattice -** A lattice L becomes a complemented lattice if it is a bounded lattice and if every element in the lattice has a complement. An element x has a complement x' if $\exists x(x\mathrm{A}x'=0andx\mathrm{v}x'=1)$
3. **Distributive Lattice -** If a lattice satisfies the following two distribute properties, it is called a distributive lattice.

a) $a\mathrm{v}(b\mathrm{A}c)=(a\mathrm{v}b)\mathrm{A}(a\mathrm{v}c)$

b) $a\mathrm{A}(b\mathrm{v}c)=(a\mathrm{A}b)\mathrm{v}(a\mathrm{A}c)$

4. **Modular Lattice -** If a lattice satisfies the following property, it is called modular lattice.

$a\mathrm{A}(b\mathrm{v}(a\mathrm{A}d))=(a\mathrm{A}b)\mathrm{v}(a\mathrm{A}d)$

Properties of Lattices

1. **Idempotent Properties**
   a) $a\mathrm{v}a=a$
   b) $a\mathrm{A}a=a$
2. **Absorption Properties**
   a) $a\mathrm{v}(a\mathrm{A}b)=a$
   b) $a\mathrm{A}(a\mathrm{v}b)=a$
3. **Commutative Properties**
   a) $a\mathrm{v}b=b\mathrm{v}a$
   b) $a\mathrm{A}b=b\mathrm{A}a$
4. **Associative Properties**
   a) $a\mathrm{v}(b\mathrm{v}c)=(a\mathrm{v}b)\mathrm{v}c$
   b) $a\mathrm{A}(b\mathrm{A}c)=(a\mathrm{A}b)\mathrm{A}c$

Dual of a Lattice - The dual of a lattice is obtained by interchanging the 'v ' and 'A ' operations.

Example

The dual of [*a*v(*b*A*c*)] *is* [*a*A(*b*v*c*)]

Counting Theory - In daily lives, many a times one needs to find out the number of all possible outcomes for a series of events. For instance, in how many ways can a panel of judges comprising of 6 men and 4 women be chosen from among 50 men and 38 women? How many different 10 lettered PAN numbers can be generated such that the first five letters are capital alphabets, the next four are digits and the last is again a capital letter. For solving these problems, mathematical theory of counting are used. **Counting** mainly encompasses fundamental counting rule, the permutation rule, and the combination rule.

The Rules of Sum and Product

The **Rule of Sum** and **Rule of Product** are used to decompose difficult counting problems into simple problems.

1. **The Rule of Sum** − If a sequence of tasks $T1,T2,\dots,Tm$ can be done in $w1,w2,\dots wm$ ways respectively (the condition is that no tasks can be performed simultaneously), then the number of ways to do one of these tasks is $w1+w2+\cdots+wm$. If we consider two tasks A and B which are disjoint (i.e. $A\cap B=\emptyset$), then mathematically $|A\cup B|=|A|+|B|$
2. **The Rule of Product** − If a sequence of tasks $T1,T2,\dots,Tm$ can be done in $w1,w2,\dots wm$ ways respectively and every task arrives after the occurrence of the previous task, then there are $w1\times w2\times\cdots\times wm$ ways to perform the tasks. Mathematically, if a task B arrives after a task A, then $|A\times B|=|A|\times|B|$

Example

Question − **A boy lives at X and wants to go to School at Z. From his home X he has to first reach Y and then Y to Z. He may go X to Y by either 3 bus routes or 2 train routes. From there, he can either choose 4 bus routes or 5 train routes to reach Z. How many ways are there to go from X to Z?**

Solution − From X to Y, he can go in 3+2=5 ways (Rule of Sum). Thereafter, he can go Y to Z in 4+5=9 ways (Rule of Sum). Hence from X to Z he can go in 5×9=45ways (Rule of Product).

Permutations - A **permutation** is an arrangement of some elements in which order matters. In other words a Permutation is an ordered Combination of elements.

Examples

1. From a set S ={x, y, z} by taking two at a time, all permutations are − *xy*,*yx*,*xz*,*zx*,*yz*,*zy*
2. We have to form a permutation of three digit numbers from a set of numbers $S=\{1,2,3\}$

Different three digit numbers will be formed when we arrange the digits. The permutation will be = 123, 132, 213, 231, 312, 321

Number of Permutations

The number of permutations of ‘n’ different things taken ‘r’ at a time is denoted by nPr

$nPr=n!(n\text{-}r)!$

where $n!=1.2.3....(n-1).n$

Proof − Let there be ‘n’ different elements.

There are n number of ways to fill up the first place. After filling the first place (n-1) number of elements is left. Hence, there are (n-1) ways to fill up the second place. After filling the first and second place, (n-2) number of elements is left. Hence, there are (n-2) ways to fill up the third place. We can now generalize the number of ways to fill up r-th place as [n – (r–1)] = n–r+1

So, the total no. of ways to fill up from first place up to r-th-place −

$nPr=n(n-1)(n-2).\ ...\ (n-r+1)$

$=[n(n-1)(n-2)...(n-r+1)][(n-r)(n-r-1)...3.2.1]/[(n-r)(n-r-1)...3.2.1]$

Hence,

$nPr=n!/(n-r)!$

Some important formulas of permutation

1. If there are n elements of which $a1$ are alike of some kind, $a2$ are alike of another kind; $a3$ are alike of third kind and so on and ar are of rth kind, where $(a1+a2+...ar)=n$ Then, number of permutations of these n objects is = $n!/[(a1!(a2!)...(ar!)]$
2. Number of permutations of n distinct elements taking n elements at a time = $nPn=n!$
3. The number of permutations of n dissimilar elements taking r elements at a time, when x particular things always occupy definite places = $n-xpr-x$
4. The number of permutations of n dissimilar elements when r specified things always come together is − $r!(n-r+1)!$
5. The number of permutations of n dissimilar elements when r specified things never come together is − $n!-[r!(n-r+1)!]$
6. The number of circular permutations of n different elements taken x elements at time = npx/x
7. The number of circular permutations of n different things = npn/n

Some Problems

Problem 1 − From a bunch of 6 different cards, how many ways we can permute it?

Solution − As we are taking 6 cards at a time from a deck of 6 cards, the permutation will be $6P6=6!=720$

Problem 2 − In how many ways can the letters of the word 'READER' be arranged?

Solution − There are 6 letters word (2 E, 1 A, 1D and 2R.) in the word 'READER'.

The permutation will be $=6!/[(2!)(1!)(1!)(2!)]=180$.

Problem 3 − In how ways can the letters of the word 'ORANGE' be arranged so that the consonants occupy only the even positions?

Solution − There are 3 vowels and 3 consonants in the word 'ORANGE'. Number of ways of arranging the consonants among themselves $=3P3=3!=6$.

The remaining 3 vacant places will be filled up by 3 vowels in $3P3=3!=6$ ways. Hence, the total number of permutation is $6×6=36$

<u>Combinations</u> - A **combination** is selection of some given elements in which order does not matter. The number of all combinations of n things, taken r at a time is −

$\boldsymbol{nCr=n!r!(n-r)!}$

Problem 1 - Find the number of subsets of the set {1,2,3,4,5,6} having 3 elements.

Solution - The cardinality of the set is 6 and we have to choose 3 elements from the set. Here, the ordering does not matter. Hence, the number of subsets will be $6C3=20$

Problem 2 - There are 6 men and 5 women in a room. In how many ways we can choose 3 men and 2 women from the room?

Solution - The number of ways to choose 3 men from 6 men is $6C3$ and the number of ways to choose 2 women from 5 women is $5C2$

Hence, the total number of ways is − $6C3×5C2=20×10=200$

Problem 3 - How many ways can you choose 3 distinct groups of 3 students from total 9 students?

Solution - Let us number the groups as 1, 2 and 3

For choosing 3 students for 1st group, the number of ways − $9C3$

The number of ways for choosing 3 students for 2nd group after choosing 1st group − $6C3$

The number of ways for choosing 3 students for 3rd group after choosing 1st and 2nd group − $3C3$

Hence, the total number of ways $=9C3\times 6C3\times 3C3=84\times 20\times 1=1680$

Pascal's Identity

Pascal's identity, first derived by Blaise Pascal in 19th century, states that the number of ways to choose k elements from n elements is equal to the summation of number of ways to choose (k-1) elements from (n-1) elements and the number of ways to choose elements from n-1 elements.

Mathematically, for any positive integers k and n: $nCk=n-1Ck-1+n-1Ck$

Proof −

$n-1Ck-1+n-1Ck$

$=(n-1)!(k-1)!(n-k)!+(n-1)!k!(n-k-1)!$

$=(n-1)!(kk!(n-k)!+n-kk!(n-k)!)$

$=(n-1)!nk!(n-k)!$

$=n!k!(n-k)!$

$=nCk$

Probability - Closely related to the concepts of counting is Probability. We often try to guess the results of games of chance, like card games, slot machines, and lotteries; i.e. we try to find the likelihood or probability that a particular result with be obtained.

Probability can be conceptualized as finding the chance of occurrence of an event. Mathematically, it is the study of random processes and their outcomes. The laws of probability have a wide applicability in a variety of fields like genetics, weather forecasting, opinion polls, stock markets etc.

Basic Concepts

Probability theory was invented in the 17th century by two French mathematicians, Blaise Pascal and Pierre de Fermat, who were dealing with mathematical problems regarding of chance.

Before proceeding to details of probability, let us get the concept of some definitions.

Random Experiment − An experiment in which all possible outcomes are known and the exact output cannot be predicted in advance is called a random experiment. Tossing a fair coin is an example of random experiment.

Sample Space − When we perform an experiment, then the set S of all possible outcomes is called the sample space. If we toss a coin, the sample space *S*={*H*,*T*}

Event − Any subset of a sample space is called an event. After tossing a coin, getting Head on the top is an event.

The word "probability" means the chance of occurrence of a particular event. The best we can say is how likely they are to happen, using the idea of probability.

Probabilityofoccurenceofanevent=TotalnumberoffavourableoutcomeTotalnumberofOutcomes

As the occurrence of any event varies between 0% and 100%, the probability varies between 0 and 1.

Steps to find the probability

Step 1 − Calculate all possible outcomes of the experiment.

Step 2 − Calculate the number of favorable outcomes of the experiment.

Step 3 − Apply the corresponding probability formula.

Tossing a Coin

If a coin is tossed, there are two possible outcomes − Heads (*H*) or Tails (*T*)

So, Total number of outcomes = 2

Hence, the probability of getting a Head (*H*)

on top is 1/2 and the probability of getting a Tails (*T*)

on top is 1/2

Throwing a Dice

When a dice is thrown, six possible outcomes can be on the top − 1,2,3,4,5,6.

The probability of any one of the numbers is 1/6

The probability of getting even numbers is 3/6 = 1/3

The probability of getting odd numbers is 3/6 = 1/3

Taking Cards From a Deck

From a deck of 52 cards, if one card is picked find the probability of an ace being drawn and also find the probability of a diamond being drawn.

Total number of possible outcomes − 52

Outcomes of being an ace – 4

Probability of being an ace = 4/52 = 1/13

Probability of being a diamond = 4/52 = 1/13

Probability Axioms

1. The probability of an event always varies from 0 to 1. $[0 \leq P(x) \leq 1]$
2. For an impossible event the probability is 0 and for a certain event the probability is 1.
3. If the occurrence of one event is not influenced by another event, they are called mutually exclusive or disjoint.
4. If $A1, A2....An$ are mutually exclusive/disjoint events, then $P(Ai \cap Aj) = \emptyset$ for $i \neq j$ and $P(A1 \cup A2 \cup ... An) = P(A1) + P(A2) + ... P(An)$

Properties of Probability

1. If there are two events x and $\overline{x}$ which are complementary, then the probability of the complementary event is –

   $$p(\overline{x}) = 1 - p(x)$$

2. For two non-disjoint events A and B, the probability of the union of two events –

   $$P(A \cup B) = P(A) + P(B)$$

3. If an event A is a subset of another event B (i.e. $A \subset B$), then the probability of A is less than or equal to the probability of B. Hence, $A \subset B$ implies $P(A) \leq p(B)$

Conditional Probability

The conditional probability of an event B is the probability that the event will occur given an event A has already occurred. This is written as $P(B|A)$.

Mathematically – $P(B|A) = P(A \cap B)/P(A)$

If event A and B are mutually exclusive, then the conditional probability of event B after the event A will be the probability of event B that is $P(B)$

Problem 1 - In a country 50% of all teenagers own a cycle and 30% of all teenagers own a bike and cycle. What is the probability that a teenager owns bike given that the teenager owns a cycle?

Solution - Let us assume A is the event of teenagers owning only a cycle and B is the event of teenagers owning only a bike.

So, $P(A) = 50/100 = 0.5$

and $P(A \cap B) = 30/100 = 0.3$

from the given problem.

$P(B|A)=P(A\cap B)/P(A)=0.3/0.5=0.6$

Hence, the probability that a teenager owns bike given that the teenager owns a cycle is 60%.

Problem 2 - In a class, 50% of all students play cricket and 25% of all students play cricket and volleyball. What is the probability that a student plays volleyball given that the student plays cricket?

Solution - Let us assume A is the event of students playing only cricket and B is the event of students playing only volleyball.

So, $P(A)=50/100=0.5$

and $P(A\cap B)=25/100=0.25$

from the given problem.

$0.25/0.5=0.5$

Hence, the probability that a student plays volleyball given that the student plays cricket is 50%.

Problem 3 - Six good laptops and three defective laptops are mixed up. To find the defective laptops all of them are tested one-by-one at random. What is the probability to find both of the defective laptops in the first two pick?

Solution- Let A be the event that we find a defective laptop in the first test and B be the event that we find a defective laptop in the second test.

Hence, $P(A\cap B)=P(A)P(B|A)=3/9\times 2/8=1/21$

Bayes' Theorem

Theorem − If A and B are two mutually exclusive events, where $P(A)$ is the probability of A and $P(B)$ is the probability of B, $P(A|B)$ is the probability of A given that B is true. $P(B|A)$ is the probability of B given that A is true, then Bayes' Theorem states −

$P(A|B)=P(B|A)P(A)\sum ni=1P(B|Ai)P(Ai)$

Application of Bayes' Theorem

1. In situations where all the events of sample space are mutually exclusive events.

2. In situations where either $P(Ai\cap B)$ for each Ai or $P(Ai)$ and $P(B|Ai)$ for each Ai is known.

Problem - Consider three pen-stands. The first pen-stand contains 2 red pens and 3 blue pens; the second one has 3 red pens and 2 blue pens; and the third one has 4 red pens and 1 blue pen. There is equal probability of each pen-stand to be selected. If one pen is drawn at random, what is the probability that it is a red pen?

Solution - Let *Ai* be the event that i^{th} pen-stand is selected. Here, i = 1,2,3.

Since probability for choosing a pen-stand is equal, *P*(*Ai*)=1/3

Let B be the event that a red pen is drawn.

The probability that a red pen is chosen among the five pens of the first pen-stand,

P(*B*|*A*1)=2/5

The probability that a red pen is chosen among the five pens of the second pen-stand,

P(*B*|*A*2)=3/5

The probability that a red pen is chosen among the five pens of the third pen-stand,

P(*B*|*A*3)=4/5

According to Bayes' Theorem,

P(*B*)=*P*(*A*1).*P*(*B*|*A*1)+*P*(*A*2).*P*(*B*|*A*2)+*P*(*A*3).*P*(*B*|*A*3)

=1/3.2/5+1/3.3/5+1/3.4/5

=3/5

Binomial Theorem - The binomial theorem states a formula for expressing the powers of sums.

The formal expression of the Binomial Theorem is as follows:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Recurrence Relation - It Show how recursive techniques can derive sequences and be used for solving counting problems. The procedure for finding the terms of a sequence in a recursive manner is called **recurrence relation**. We study the theory of linear recurrence relations and their solutions. Finally, we introduce generating functions for solving recurrence relations.

Definition

A recurrence relation is an equation that recursively defines a sequence where the next term is a function of the previous terms (Expressing Fn as some combination of Fi with $i<n$).

Example − Fibonacci series − $Fn=Fn-1+Fn-2$, Tower of Hanoi − $Fn=2Fn-1+1$

Linear Recurrence Relations

A linear recurrence equation of degree k or order k is a recurrence equation which is in the format$xn=A1xn-1+A2xn-1+A3xn-1+\ldots Akxn-k$ (An is a constant and $Ak\neq 0$) on a sequence of numbers as a first-degree polynomial.

These are some examples of linear recurrence equations −

Recurrence relations	**Initial values**	**Solutions**
$F_n = F_{n-1} + F_{n-2}$	$a_1 = a_2 = 1$	Fibonacci number
$F_n = F_{n-1} + F_{n-2}$	$a_1 = 1, a_2 = 3$	Lucas Number
$F_n = F_{n-2} + F_{n-3}$	$a_1 = a_2 = a_3 = 1$	Padovan sequence
$F_n = 2F_{n-1} + F_{n-2}$	$a_1 = 0, a_2 = 1$	Pell number

How to solve linear recurrence relation

Suppose, a two ordered linear recurrence relation is − $Fn=AFn-1+BFn-2$

where A and B are real numbers.

The characteristic equation for the above recurrence relation is −

$x2-Ax-B=0$

Three cases may occur while finding the roots −

Case 1 − If this equation factors as $(x-x1)(x-x1)=0$

and it produces two distinct real roots $x1$ and $x2$, then $Fn=axn1+bxn2$

is the solution. [Here, a and b are constants]

Case 2 − If this equation factors as $(x-x1)2=0$

and it produces single real root $x1$, then $Fn=axn1+bnxn1$

is the solution.

Case 3 − If the equation produces two distinct complex roots, $x1$

and $x2$ in polar form $x1=r\angle\vartheta$ and $x2=r\angle(-\vartheta)$, then $Fn=rn(acos(n\vartheta)+bsin(n\vartheta))$

is the solution.

Problem 1 - Solve the recurrence relation $Fn=5Fn\text{-}1\text{-}6Fn\text{-}2$ where $F0=1$ and $F1=4$

Solution - The characteristic equation of the recurrence relation is −

$x2-5x+6=0$,

So, $(x-3)(x-2)=0$

Hence, the roots are −

$x1=3$ and $x2=2$

The roots are real and distinct. So, this is in the form of case 1

Hence, the solution is −

$Fn=axn1+bxn2$

Here, $Fn=a3n+b2n$ (As $x1=3$ and $x2=2$)

Therefore,

$1=F0=a30+b20=a+b$

$4=F1=a31+b21=3a+2b$

Solving these two equations, we get $a=2$

and $b=-1$

Hence, the final solution is −

$Fn=2.3n+(\text{-}1).2n=2.3n\text{-}2n$

Problem 2 Solve the recurrence relation - $Fn=10Fn\text{-}1\text{-}25Fn\text{-}2$ where $F0=3$ and $F1=17$

Solution The characteristic equation of the recurrence relation is −

$x2-10x-25=0$

So $(x-5)2=0$

Hence, there is single real root $x1=5$

As there is single real valued root, this is in the form of case 2

Hence, the solution is −

$Fn=axn1+bnxn1$

$3=F0=a.50+b.0.50=a$

$17=F1=a.51+b.1.51=5a+5b$

Solving these two equations, we get $a=3$

and $b=2/5$

Hence, the final solution is − $Fn=3.5n+(2/5).n.2n$

Problem 3 Solve the recurrence relation $Fn=2Fn$-1-2Fn-2 where $F0=1$ and $F1=3$

Solution The characteristic equation of the recurrence relation is −

$$x2-2x-2=0$$

Hence, the roots are −

$x1=1+i$

and $x2=1-i$

In polar form,

$x1=r\angle\vartheta$

and $x2=r\angle(-\vartheta)$, where $r=2\text{–}\surd$ and $\vartheta=\pi4$

The roots are imaginary. So, this is in the form of case 3.

Hence, the solution is −

$Fn=(2\text{–}\surd)n(acos(n.\Pi/4)+bsin(n.\Pi/4))$ $1=F0=(2\text{–}$

$\surd)0(acos(0.\Pi/4)+bsin(0.\Pi/4))=a$

$3=F1=(2\text{–}\surd)1(acos(1.\Pi/4)+bsin(1.\Pi/4))=2\text{–}\surd(a/2\text{–}\surd+b/2\text{–}\surd)$

Solving these two equations we get $a=1$

and $b=2$

Hence, the final solution is −

$Fn=(2–\sqrt{})n(cos(n.\pi/4)+2sin(n.\pi/4))$

Non-Homogeneous Recurrence Relation and Particular Solutions

A recurrence relation is called non-homogeneous if it is in the form

$Fn=AFn-1+BFn-2+f(n)$

where $f(n)\neq 0$

Its associated homogeneous recurrence relation is $Fn=AFn–1+BFn-2$

The solution (an) of a non-homogeneous recurrence relation has two parts.

First part is the solution (ah) of the associated homogeneous recurrence relation and the second part is the particular solution (at)

.

$an=ah+at$

Solution to the first part is done using the procedures discussed in the previous section.

To find the particular solution, we find an appropriate trial solution.

Let $f(n)=cxn$; let $x2=Ax+B$ be the characteristic equation of the associated homogeneous recurrence relation and let $x1$ and $x2$ be its roots.

a) If $x\neq x1$ and $x\neq x2$, then $at=Axn$
b) If $x=x1$, $x\neq x2$, then $at=Anxn$
c) If $x=x1=x2$, then $at=An2xn$

Example

Let a non-homogeneous recurrence relation be $Fn=AFn–1+BFn-2+f(n)$

with characteristic roots $x1=2$ and $x2=5$. Trial solutions for different possible values of $f(n)$

are as follows −

f(n)	**Trial solutions**
4	A

5.2^{n}	$An2^{n}$
8.5^{n}	$An5^{n}$
4^{n}	$A4^{n}$
$2n^{2}+3n+1$	$An^{2}+Bn+C$

Problem

Solve the recurrence relation $Fn=3Fn\text{-}1+10Fn\text{-}2+7.5n$ where $F0=4$ and $F1=3$

Solution

This is a linear non-homogeneous relation, where the associated homogeneous equation is $Fn=3Fn-1+10Fn-2$

and $f(n)=7.5n$

The characteristic equation of its associated homogeneous relation is −

$x2-3x-10=0$

Or, $(x-5)(x+2)=0$

Or, $x1=5$

and $x2=-2$

Hence $ah=a.5n+b.(-2)n$, where a and b are constants.

Since $f(n)=7.5n$, i.e. of the form $c.xn$, a reasonable trial solution of at will be $Anxn$

$at=Anxn=An5n$

After putting the solution in the recurrence relation, we get −

$An5n=3A(n–1)5n-1+10A(n–2)5n-2+7.5n$

Dividing both sides by $5n-2$, we get

$An52=3A(n-1)5+10A(n-2)50+7.52$

Or, $25An=15An-15A+10An-20A+175$

Or, $35A=175$

Or, $A=5$

So, $Fn=An5n=5n5n=n5n+1$

The solution of the recurrence relation can be written as −

$Fn=ah+at =a.5n+b.(−2)n+n5n+1$

Putting values of $F0=4$

and $F1=3$, in the above equation, we get $a=−2$ and $b=6$

Hence, the solution is −

$Fn=n5n+1+6.(−2)n−2.5n$

Generating Functions - Generating Functions represents sequences where each term of a sequence is expressed as a coefficient of a variable x in a formal power series.

Mathematically, for an infinite sequence, say $a0,a1,a2,…,ak,…$, the generating function will be −

$Gx=a0+a1x+a2x2+\cdots+akxk+\cdots=\sum k=0\infty akxk$

Some Areas of Application

Generating functions can be used for the following purposes –

a) For solving a variety of counting problems. For example, the number of ways to make change for a Rs. 100 note with the notes of denominations Rs.1, Rs.2, Rs.5, Rs.10, Rs.20 and Rs.50

b) For solving recurrence relations

c) For proving some of the combinatorial identities

d) For finding asymptotic formulae for terms of sequences

Problem 1 - What are the generating functions for the sequences {ak} with $ak=2$ and $ak=3k$?

Solution When $ak=2$, generating function, $G(x)=\sum\infty k=02xk=2+2x+2x2+2x3+…$

When $ak=3k,G(x)=\sum\infty k=03kxk=0+3x+6x2+9x3+……$

Problem 2 - What is the generating function of the infinite series; 1,1,1,1,…?

Solution Here, $ak=1$, for $0\le k\le\infty$

Hence, $G(x)=1+x+x2+x3+…\cdots=1(1−x)$

Some Useful Generating Functions

a) For $ak=ak,G(x)=\sum\infty k=0akxk=1+ax+a2x2+\ldots\ldots\cdots=1/(1-ax)$
b) For $ak=(k+1),G(x)=\sum\infty k=0(k+1)xk=1+2x+3x2\ldots\ldots\cdots=1(1-x)2$
c) For $ak=cnk,G(x)=\sum\infty k=0cnkxk=1+cn1x+cn2x2+\ldots\ldots\cdots+x2=(1+x)n$
d) For $ak=1k!,G(x)=\sum\infty k=0xkk!=1+x+x22!+x33!\ldots\ldots\cdots=ex$