- Modules

(1) Introduction → To understand basic concepts & notation.

(2) Finite Automata & Regular Languages → To understand FA

(3) Context Free Language & Push Down Automata

(4) Turing Machines

(5) Computability & Decidability

- Pre-requisites

(1) Set, sequence, & Tuples
(2) Relation & Function
(3) Boolean Logic
(4) Graphs
(5) Strings & Languages.

Automata Theory

→ Also known as ToC. is a theoretical branch of computer science & mathematics, which deals with the logic of computation with respect to a simple machine, referred to as Automata.

→ Automata enables the scientists to understand how machines compute the functions and solves the problems.

* Set-Theory

→ Mathematics is the language of ToC. So we need to know set.

→ It was founded in 1874 by Georg Cantor (German Mathematician)

→ A set is a collection of well-defined distinct objects. (Unordered Pair).

→ The term well-defined signifies that all the elements of the set can be defined by a single definition and this definition decides weather an element is a member of set or not.

For Ex:- $A = \{a, b, c, d, e\}$

are called members / elements of set A.

∴ belonging.

→ b is an element of set L.

∴ $b \in L$. (b is in L, or L contains b).

→ 2 is not an element of L.

$2 \notin L$.

Note:- Capital letters A, B, C, ... are used to denote set and a, b, c, ... to denote elements of set.

Notations :-

① $\mathbb{N}$: The set of all natural numbers. $\mathbb{N} = \{1, 2, 3, \ldots\}$

② $\mathbb{Z}$: The set of all integers, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

③ $\mathbb{Z}^*$: The set of all non-zero integer.

④ $\mathbb{Z}^+$: The set of all positive integer.

⑤ $\mathbb{E}$: The set of all Even integers.

⑥ $\mathbb{Q}$: The set of all rational Number. $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$

⑦ $\mathbb{I}$: The set of all irrational Numbers.

⑧ $\mathbb{Q}^*$: The set of all non-zero rational number.

⑨ $\mathbb{Q}^+$: The set of all positive rational number.

⑩ $\mathbb{R}$: The set of all real number.

⑪ $\mathbb{R}^*$: The set of all non-zero real number.

⑫ $\mathbb{R}^+$: The set of all positive real number.

⑬ $\mathbb{C}$: The set of all coplex number. $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$

⑭ $\mathbb{C}^*$: The set of all non-zero complex number.

Representation of Set

① **Roster Notation** :— List all the elements of the set.

- $A = \{a, e, i, o, u\}$
- $B = \{1, 2, 3, \ldots, 20\}$

② **Set-builder Notation** :-

- $B = \{x : 2 \leq x \leq 20$ and x is an even number$\}$
- $A = \{x \mid R(x)$, where $R(x)$ is a rule$\}$
- $C = \{x : x$ is an odd integer and $x > 0\}$

: or | ← "Such that"

* Null Set- :—

- A set is empty (null) if it contains no elements.
- The empty set is written as ϕ.
- The empty set is sub-set of every set.

Ex: $A = \{x : x \in R^2$ and $x^2 + 1 = 0\}$

$B = \{x : x \in Z$ and $4 < x < 5\}$

* Cardinality of set- :-

- Number of distinct elements of the set.
- We denote it as $|A|$ or $n(A)$ for set A.

$\therefore A = \{1, 2, 3, 4\}$, then $|A| = 4$, $n(A) = 4$.

$|\phi| = 0$.

* Sub-set :-

→ A set A is a subset of a set B, if each element of A is also an element of B.

$A \subseteq B$.

→ $O = \{x : x \in N$ and x is not divisible by $2\}$

$\therefore O \subseteq N$.

→ Any set A is a subset of itself. $A \subseteq A$

→ A is a not a subset of B $\Rightarrow A \not\subseteq B$

* Proper Subset :- If a set A is a subset of B but not equal to B.

→ A is a proper subset of B, then all elements of A are also in B, but B contains at-least one element that is not in A.

$A \subset B$.

Ex:- $B = \{1, 2, 3, 4, 5\}$
$A = \{1, 3, 5\}$
$\therefore A \subset B$.

$Z^+ \subset Z$ ← int set.
$Z^* \subset Z$.

→ The empty set ϕ is a subset of every set.
If B is a set, then $\phi \subset B$.

* Superset- :-

→ If $X \subseteq Y$, then "X is contained in Y" or "Y contains X" or Y is a superset of X.

i.e. $Y \supseteq X$.

* Equality of set-

→ Two set- A and B are equal if $A \subseteq B$ and $B \subseteq A$.

→ Every element- of A must be an element of B and vice versa.

Ex: ① $|A| = 5$ and $|B| = 5$ A and B may not- same.

② $|A| = 4$ and $|B| = 3$. A nor B are not- same.

③ $X = \{$ red, blue, green $\}$. therefore $X = Y$

$Y = \{ c : c$ is a primary color $\}$

* Power-set- :-

→ For any set- X, the power set- of X is written as. $P(X)$. that- is all subset- of X.

Ex:- If $X = \{$ red, green, black $\}$

$\therefore P(X) = \{ \phi, \{red\}, \{green\}, \{black\}, \{red, green\}, \{red, black\}, \{green, black\}, \{red, green, black\} \}$

$\therefore$ If $|X| = n$ then $|P(X)| = 2^n$.

* Union of Sets

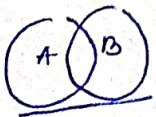
→ The union of two sets A and B is the set of elements which are in A and in B. or in both.

→ $A \cup B = \{x : x \in A \text{ and } x \in B\}$.

$A = \{1, 3, 5, 7\}$ and $B = \{2, 4, 6, 7\}$

or

$A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$



$A \cup B$.

* Intersection of Sets

→ $A \cap B$. ⇒ $A \cap B = \{x : x \in A \text{ and } x \in B\}$ i.e. $x \in (A \cap B)$

Ex:- $A = \{1, 2, 3\}$ $B = \{2, 3\}$ $A \cap B = \{2, 3\}$

$A \cap B$.

* Universal Set :- The universal set is the collection of all objects in a particular context or theory.

→ it is denoted by U.

→ The complement of U is ϕ

Ex:- If we are talking about people of India, China, & Japan. then the universal set will be the set of all people of these three countries.

Ex:- $N = \{1, 2, 3, \ldots\}$, $A = \{1, 3, 5, 7, \ldots\}$, $B = \{2, 4, 6, \ldots\}$

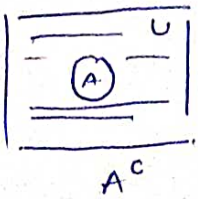
∴ N will be the universal set of A and B.

* Absolute Complement :-

→ The absolute complement of a set A is the set contains all the elements that are in the universe set U, but not in A.

→ The complement of A is $\overline{A}$ or A^c or A'

$\therefore \overline{A} = \{ x : x \in U \text{ and } x \notin A \}$ or $A^c = \{ x : x \in (U - A) \}$



* Relative compliment :- If A and B are sets, then the relative compliment of A and B is denoted by B − A or B/A.

→ Formally $B - A = \{ x : x \in B \text{ and } x \notin A \}$

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

$B - A = \{ 4 \}$

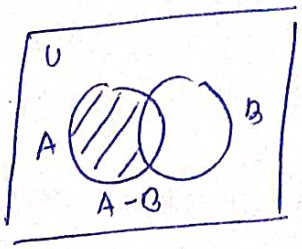
$A - B = \{ 1 \}$.

$\therefore \mathbb{R} = \{$ set of all real Numbers $\}$.

$\mathbb{Q} = \{$ set of all rational Numbers $\}$.

$\therefore \mathbb{R} - \mathbb{Q} = \mathbb{I}$

$\mathbb{I} = \{$ set of all irrational numbers $\}$.



* Symmetric difference of two sets

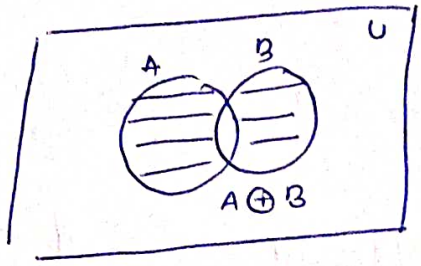
→ The symmetric difference of A and B is a set that contains those elements that are in A, or in B, but not in both.

→ $A \oplus B = (A-B) \cup (B-A) = (A \cup B) - (A \cap B)$ or

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

Ex:- $A = \{1, 2, 3, 4\}$ $B = \{3, 4, 5\}$

$A \oplus B = A \Delta B = \{1, 2, 5\}$

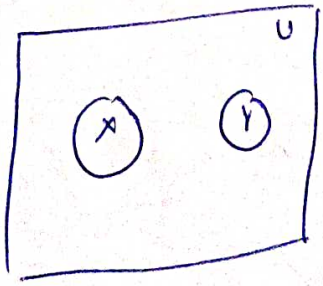


* Disjoint Sets :-

→ Two sets X and Y are said to be disjoint if

$X \cap Y = \phi$

Ex:- $X = \{2, 4, 6\}$ $Y = \{3, 5, 7\}$ $\therefore X \cap Y = \phi$



* Cartesian Product of Set

→ Let A and B be sets, the cartesian product of A and B, denoted by $A \times B$, is the all ordered pairs (a, b) where $a \in A$ and $b \in B$.

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

→ But $A \times B \neq B \times A$ unless $A = \phi$ and $B = \phi$

→ Ex: $A = \{1, 2\}$

$B = \{3, 4\}$

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

→ Note :- $A \times \phi = \phi \times A = \phi$ because there is no element in ϕ to form a ordered pair.

* Algebra of sets :-

① Idempotent Law :-

- $A \cup A = A$
- $A \cap A = A$

② Associative Law :-

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

③ Distributive Law :-

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

④ Properties of Empty set :-

- $A \cup \phi = A$
- $A \cap \phi = \phi$

⑤ Properties of universal set :-

- $A \cup U = U$
- $A \cap U = A$.

⑥ Properties of the complement :-

- $\overline{(\bar{A})} = A$
- $(A \cap \bar{A}) = \phi$
- $(A \cup \bar{A}) = U$
- $(\bar{U}) = \phi$
- $(\bar{\phi}) = U$

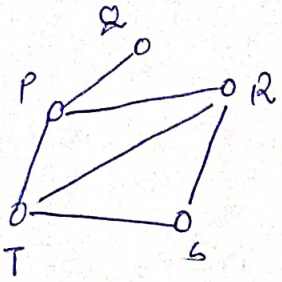
⑦ De Morgan's Law :-

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

- A graph is a pictorial representation of a set of objects where some pairs of objects are connected by links.
- An undirected graph, or simple graph $G(V, E)$ is a set of points with lines connecting some points.

→ The points are called nodes or vertices. (V).

→ The lines are called edges (E)



– Edges
- vertex

∴ $V = \{P, Q, R, S, T\}$
$E = \{PQ, PR, PT, RS, IT, RT\}$

* Applications :-
1. Can be used in circuit designing
2. Used in Kruskal's Algorithm
3. Used in Prim's Algorithm
4. Used to represent molecular structure and chemical structure of substance.
5. DNA structure of organism.

* Degree of Vertex :-

→ It is the number of vertices adjacent to a vertex v.

→ Notation : $\deg(v)$.

→ In a simple graph with n number of vertices, the degree of any vertex is. $\deg(v) \leq n-1$ for $\forall v \in G$.

* Degree of vertex can be considered under two cases of graph :-

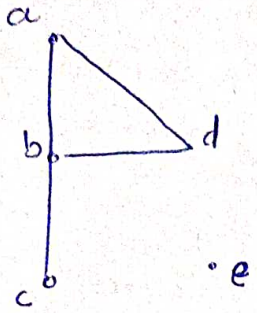
① Undirected Graph

② Directed Graph.

* Degree of vertex in undirected Graph :-

→ An undirected graph has no directed edges.

Ex:- ①



$\therefore \deg(a) = 2$

$\deg(b) = 3$

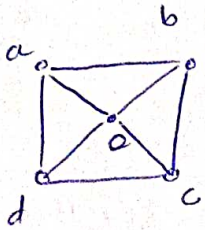
$\deg(d) = 2$

$\deg(c) = 1$

$\deg(e) = 0$

$\therefore$ e is an isolated vertex.

Ex:- ②



$\deg(a) = 3$ $\quad \deg(c) = 3$ $\quad \deg(e) = 4$

$\deg(b) = 3$ $\quad \deg(d) = 3$

$n-1$

* Degree of vertices in a directed graphs -

→ In directed graph, each vertex has an indegree and an outdegree.

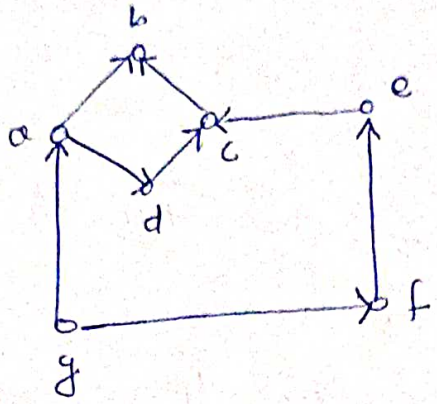
① Indegree :- The no of edges that are coming into v.

notation ⇒ $\deg^-(v)$

② outdegree :- The no of edges that are going out from v.

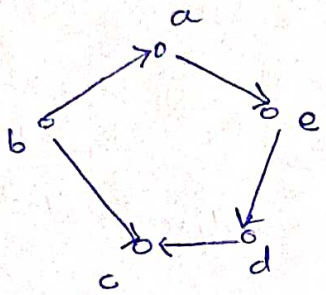
notation ⇒ $\deg^+(v)$

Ex:- ①



V	in	out
a	1	2
b	2	0
c	2	1
d	1	1
e	1	1
f	1	1
g	0	2

Ex:- ②

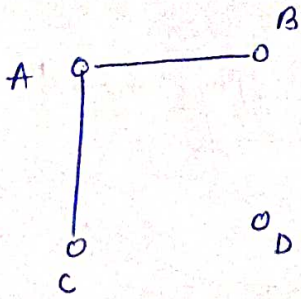


V	In	out
a	1	1
b	0	2
c	2	0
d	1	1
e	1	1

o Pendent Vertex :- A vertex with degree one(1) is called pendent- vertex.

o Isolated vertex :- A vertex with degree zero (0) is isolated vertex.

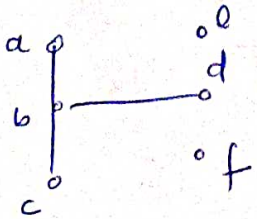
Ex:-



pendant V = {B, C}

Isolated v = {D}

Ex:-



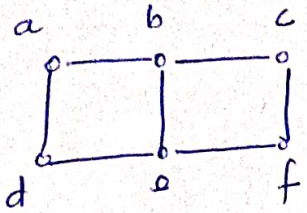
pendent v = {d}

Isolated v = {e, f}.

○ Adjacency :- ① In a graph, two vertices are said to be adjacent, if there is an edge between the two vertices.

② In a graph, two edges are said to be adjacent, if there is a common vertex between the two edges.

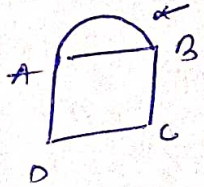
Ex:-



* adjacent vertices pair :-
ab, bc, ad, be, cf, de, ef.

* adjacent edges :-
① ab and ad ② ab and bc
③ bc and cf ④ ab and be etc.

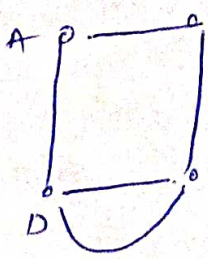
○ Parallel Edges :- In a graph, if the pair of vertices is connected by more than one edge, then those edges are called parallel edges.

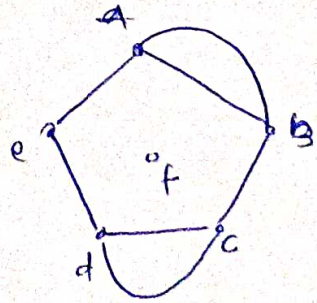


← Pralel edges.

○ Multi Graph :- A graph having pralleel edges is known as multigraph.

Ex:

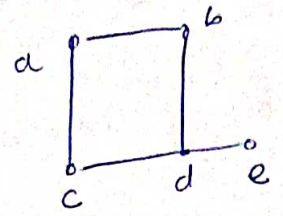




o **Degree sequence of Graph :-**

– If the degrees of all vertices in a graph are arranged in descending or ascending order, then the sequence obtained is known as degree sequence of the Graph.

Ex :-

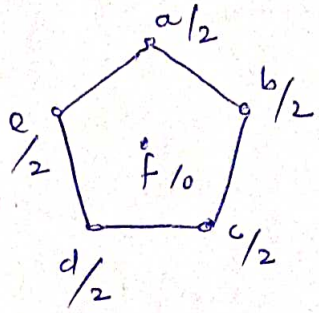


Vertices	a	b	c	d	e
degree	2	2	2	3	1

$\therefore$ {3, 2, 2, 2, 1} ⇒ Seq.

{d, a, b, c, a} vertices

Ex



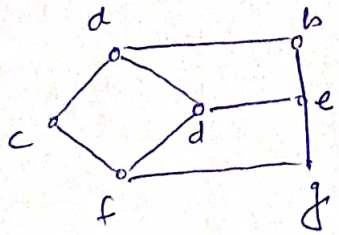
{a, b, c, d, e, f} degree seq. is {2, 2, 2, 2, 2, 0}

o **Distance between two vertices :-**

– it is the number of edges between tow vertices u and v via shortest path.

– Notation d(u, v)

Ex:-



d(d, e) = 1.

Paths :- for (d, e).

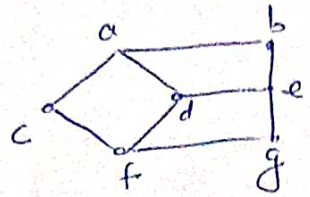
(i) d → e = 1
(ii) d → a → b → e = 3
(iii) d → a → c → f → g = 4
(iv) d → f → g → e = 3
(v) d → f → c → d → b → e = 5

o **Eccentricity of a vertex :-**

· The maximum distance between a vertex to all the other vertex is considered as the eccentricity of the vertex.

→ Notation: $e(v)$

Ex:-



$e(a) = 3$

$d(a,b) = 1$ $\quad d(a,f) = 2$

$d(a,c) = 1$ $\quad d(a,e) = 2$

$d(a,d) = 1$ $\quad d(a,g) = 3$.

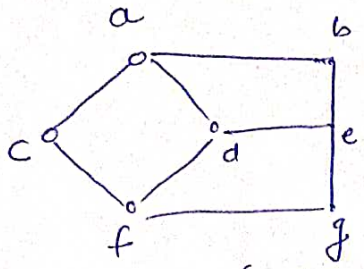
○ Radius of a Connected Graph :-

→ The minimum eccentricity from all the vertices is considered as the radius of the graph.

→ i.e., the minimum among all the maximum distances between one vertex to other.

→ Notation ~~$r(G)$~~ $\Rightarrow$ $r(G)$

Ex:-



$e(a) = 3$.

$e(b) = \max(1,1,2,2,2,3) = 3$.

$e(e) = \max(1,1,1,2,2,3) = 3$.

$e(g) = \max(1,1,2,2,2,3) = 3$.

$e(f) = \max(1,1,1,2,2,3) = 3$

$e(c) = \max(1,1,2,2,2,3) = 3$

$e(d) = \max(1,1,1,2,2,2) = 2$

$\therefore r(G) = \min(3,3,3,3,3,2)$

$= 2$

○ Diameter of the Graph :-

→ The maximum eccentricity from all the vertices is considered as diameter of the graph.

→ Notation: $d(G)$

Ex:- Above graph. $d(G) = \max(3,3,3,3,3,2) = 3$

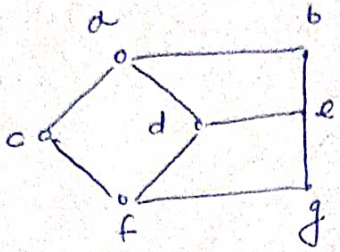
○ Central points :-

→ If the eccentricity of any vertex is equal to the radius of the graph. i.e. considered as central point.

→ $e(v) = r(G)$ Ex:- $e(d) = 2$, $r(G) = 2$ So, d is the central point.

- **Circumference :-**
  → The number of edges in the longest cycle in the graph is the circumference of the graph.

Ex:-

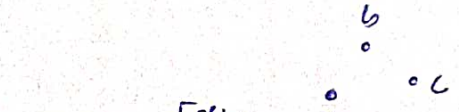


cycles :-
(i) a-c-f-a = 4
(ii) a-b-e-d-a = 4
(iii) a-c-f-g-e-b-a = 6
(iv) a-c-f-d-e-b-a = 6

- **Girth :-**
  → The number of edges in the shortest cycle of Graph is the girth.

Ex:- (i) a-c-f-d-a = 4
(ii) a-d-e-b-a = 4
(iii) d-e-g-f-d = 4

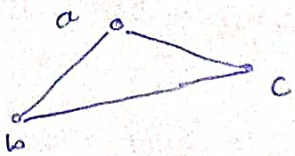
- **Null graph :-** Graph with no edges. Ex:-



- **Trivia Graph :-** A graph with only one vertex Ex:-

- **Simple Graph :-** Graph with no loops and parallel edges.
  → Max edges possible = $^{n}C_2 = \frac{n(n-1)}{2}$.
  → The no of Simple Graph possible with 'n' vertices = $2^{^{n}C_2} = 2^{n(n-1)/2}$

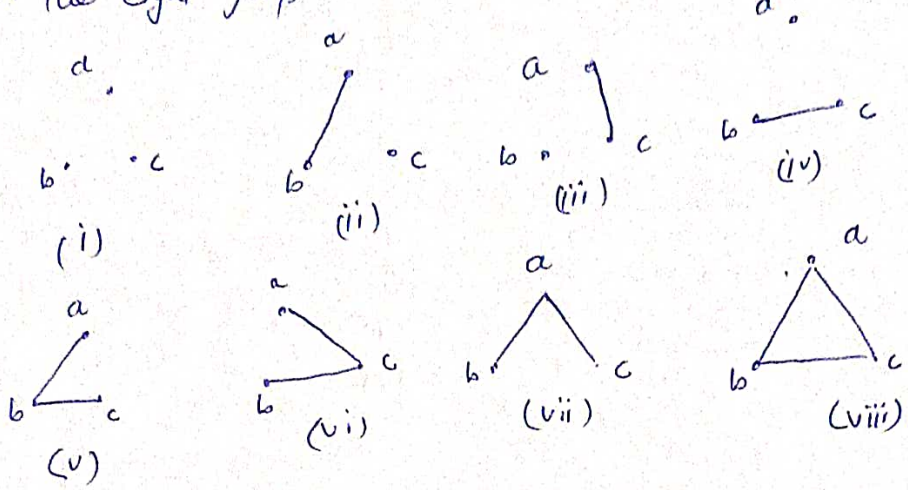
Let ⇒ edges = 3 and vertices = 3.



(1) Max edges ⇒ $^{3}C_2 = \frac{3(3-1)}{2} = 3$.

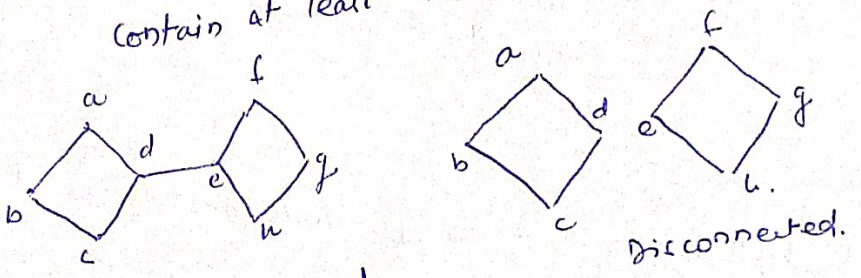
(2) Max no of Simple Graph ⇒ $2^{^{3}C_2} = 2^{3} = 8$.

→ The eight graphs are:



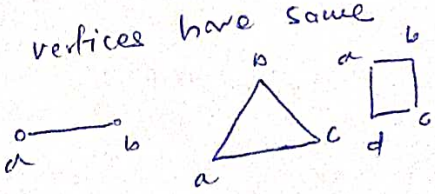
- **Connected Graph:-** A graph is said to be connected if there exist a path between every pair of vertices.
- **Disconnected Graph:-** A graph is disconnected if it does not contain at least two connected vertices.

Ex:-

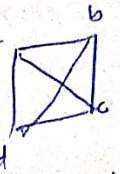


- **Regular Graph:-** Graph in which all vertices have same degree.

Ex:-



- **Complete Graph:-** If every vertex is connected to all the other vertices of a

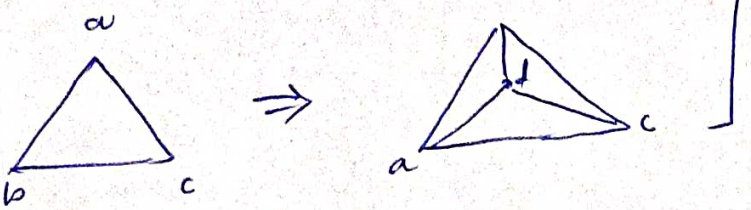


- **cycle Graph:-** A simple graph with 'n' vertices ($n \geq 3$) and 'n' edges is called cycle graph if all its edges form a cycle of length n.

Notation:- C_n

- **cyclic Graph:-** Contains at least one cycle.
- **Acyclic Graph:-** Contain no cycle.

- **Wheel Graph :-** A wheel graph is obtained from a cyclic graph by adding a new vertex at the center. That new vertex is called 'Hub' and it is connected to all the other vertices.



No of edges =
No of edges from Hub +
No of edges from all the other nodes.

$= (n-1) + (n-1)$

$= 2(n-1)$

Lecture-3 :-

* **Sub-graph** :- Let $G(V, E)$ is a graph and $H(V', E')$ is another graph.

if. $\forall\ V'(H) \subseteq V(G)$ and

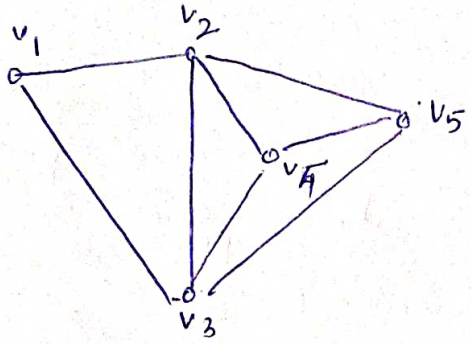
$E'(H) \subseteq E(G)$

$\therefore$ we can call H is a sub-graph of G.

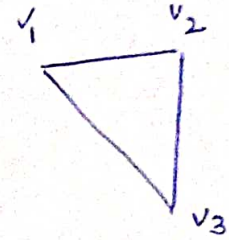
→ A graph is called sub graph of G, if all the vertices and all the edges of H are in G, and each edge of H has the same end vertices as in G.

Ex:-

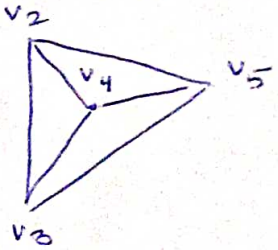
G ⇒



(i)



(ii)

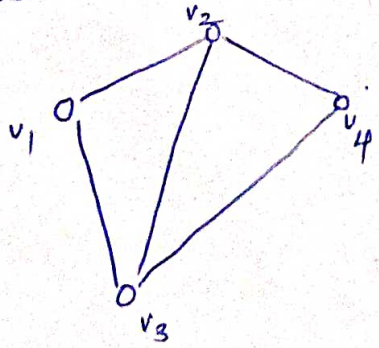


* **Walk** :-

→ A walk is a sequence of vertices and edges in the graph i.e. if we traverse a graph then we get a walk.

→ Vertices and edges can be repeated.

Ex:-



Walk:- $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_2 \rightarrow v_1$

→ Walk can be open or closed.

Walk → open :- A walk is said to be open, if starting & ending vertices are different.

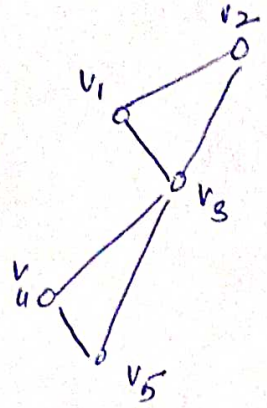
→ closed :- A walk is said to be closed walk if the starting and ending vertices are identical.

open walk :- $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow$

Closed walk :- $v_1 \rightarrow v_2 \rightarrow v_5 \rightarrow v_4 \rightarrow v_3 \rightarrow v_1$

* Trail :-

Trail is an open walk in which no edges are repeated. However, vertices can be repeated.



$v_1 \rightarrow v_3 \rightarrow v_4 \rightarrow v_5 \rightarrow v_3 \rightarrow v_2$

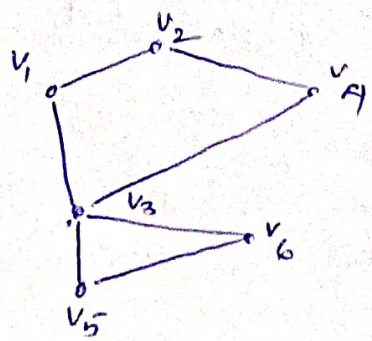
↑ open trail

$v_1 \rightarrow v_3 \rightarrow v_4 \rightarrow v_5 \rightarrow v_3 \rightarrow v_2 \rightarrow v_1$

↑ closed trail

* Circuit :- it is closed trail.

→ Traversing a graph such that- not an edge is repeated but vertex can be repeated, and it is closed.



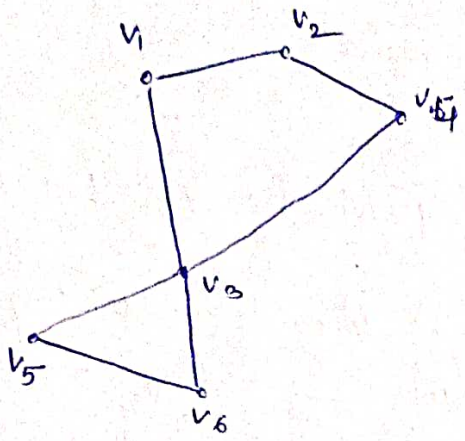
$v_1 \rightarrow v_2 \rightarrow v_4 \rightarrow v_3 \rightarrow v_6 \rightarrow v_5 \rightarrow v_3 \rightarrow v_1$

i.e. closed trail or circuit.

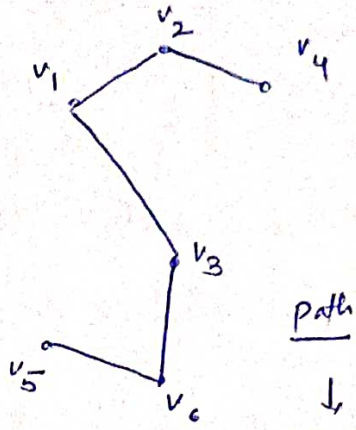
* **Path :-** A trail in which neither vertices nor edges are repeated.

∴ path is also a trail

∴ path is also an open walk.



⇒



Path.

↓

Closed path

i.e. starting vertex & end vertex are same

↓

cycle.

* **Strongly connected Graph :-**

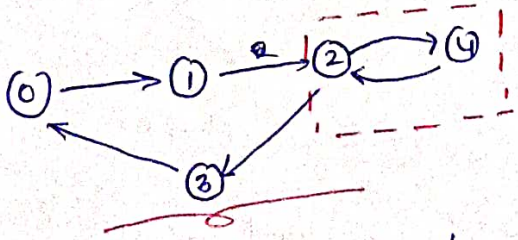
∘ A directed graph is strongly connected if a directed path connects every two nodes.

* Every vertex is reachable from every other vertex.

⇓

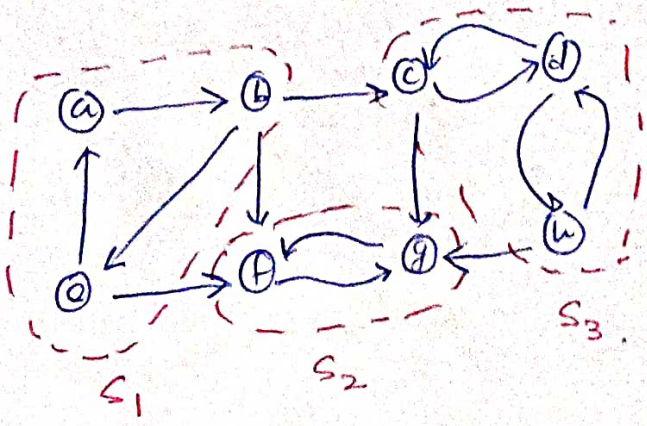
Strongly connected.

Ex :-



∘ A directed graph is called strongly connected, if their is a path between each pair of vertices in each direction.

Ex :-



* **Sequence :-** A sequence is an ordered list of elements, which can also be infinite (E.g. → the sequence composed of real numbers).

↳ order of element matters.

Ex:- Sequence $(1,2,3) \neq$ Sequence $(3,2,1) \neq$ Sequence $(1,3,2)$

↳ Empty sequence $()$.

↳ Sequence may have repeated element E.g. $(1,1,1)$

- **Subsequence :-** A subsequence is formed by deleting some elements of the sequence, while keeping the order of the other.

* **Tuples :-** A tuple is also an ordered list of elements, and it may also include repeated elements. The only difference between sequence & tuple is that the tuples has finite list of elements.

∴ Tuple with n elements are called → n-tuple.

→ Strings and Languages :-

* **Alphabet :-** (Σ) is a finite set of symbols.
(Γ)

$\Sigma_1 = \{0,1\}$

$\Sigma_2 = \{a,b,c\}$

* String or word :-

→ A string over an alphabet is a finite sequence of symbols drawn from the alphabet.

→ Empty string ⇒ ϵ

→ Σ^* is the set of all possible string over the alphabet Σ.

Alphabet-Name.	Symbol	Example.
English alphabet	$\{a, b, c, \ldots, z\}$	ϵ, aab, abc, abz, etc.
Binary alphabet	$\{0, 1\}$	ϵ, 0, 1, 011, 010, 00100, etc.

* string operation s :-

① Length → $|s|$ is the no of symbols in the string s.

$|\epsilon| = 0 \quad |00100100| = 8$

② Concatenation → xy is the concatenation of string x and y.

if $x = 001$ and $y = 100$

i.e. $xy = 001100$

$yx = 100001$

③ Replication :- For each string w and each natural number i, the string w^i is defined as follows:

$w^0 = \epsilon$

for $i > 0$

w^i = i copies of w concatinated together

Let $w = 10$ ∴ $w^i = 1010$

$i = 2$

④ Reverse :- For each string w, w^R is the reverse of w.

Ex:- $w = 001$
$w^R = 100$

⑤ Concatination of reverse :- if w and x are string then

$$(wx)^R = x^R w^R$$

Ex:- $w = ab$, $w^R = ba$
$x = 10$, $x^R = 01$

$wx = ab10$

$\therefore (wx)^R = \underline{\underline{01ba}}$

$x^R w^R = \underline{\underline{01ba}}$

Important :- → string → prefix
→ post-fix
→ proper prefix
→ proper post-fix

* Substring :- The string x is a substring of w if it is a contiguous sequence of character in w.

if $|w| > |x|$, it is a proper substring
$|w| \geq |x|$, it is a substring

(i) Every string is a substring of itself
(ii) The empty string is a substring of all string.

* Language :- A Language is a (finite or infinite) set of strings over an alphabet Σ.

Let $\Sigma = \{0, 1\}$

Some Languages over Σ.
(i) $\emptyset$, (the L. with no string).
(ii) $\{\epsilon\}$, (the L. containing just empty string)
(iii) $\{a, b\}$ (iv) $\{\epsilon, a, aa, aaa, aaaa, \ldots\}$

Ex:- $L = \{ x \in \{a,b\}^* :$ all a's precede all b's $\}$.

Then:

abbb, aabb, and aaaabbbb are in L.

and

aba, bbaa, and baba are not in L.

Q:- what about:- ϵ, a, aa, and bb ?

Boolean Logic

* Boolean Logic :- it is a mathematical system built around the two values i.e. TRUE & FALSE.

→ These two values are called as Boolean values and are often represented as '1' and '0'.

→ Boolean values can be manipulated using Boolean operations.

(i) Negation or NOT ($\neg$) i.e. $\neg 0 = 1$ and $\neg 1 = 0$.

(ii) Conjunction or AND ($\wedge$)

(iii) Disjunction or OR ($\vee$)

$0 \wedge 0 = 0$
$0 \wedge 1 = 0$
$1 \wedge 0 = 0$
$1 \wedge 1 = 1$

$\}$ $\wedge$

$0 \vee 0 = 0$
$0 \vee 1 = 1$
$1 \vee 0 = 1$
$1 \vee 1 = 1$

$\}$ $\vee$.

→ The Boolean operations are used for combining simpler statements into more complex Boolean expressions.

E.g.:- P is a boolean value representing → "the sun is shining"

Q is a boolean value representing → "today is Monday"

∴ P ∧ Q ⇒ "the sun is shining and today is monday".

P ∨ Q ⇒ "the sun is shining or today is monday".

(iv) NAND :⇒ $X = \sim(P \wedge Q)$.

(v) NOR :⇒ $X = \sim(P \vee Q)$

(v) XOR ⇒ Exclusive OR ⇒ $\oplus$

P	Q	P ⊕ Q.
0	0	0
0	1	1
1	0	1
1	1	0

(vi) Equality :⇒ $\leftrightarrow$. if operands both have same value then 1.

$0 \leftrightarrow 0 = 1$

$0 \leftrightarrow 1 = 0$

$1 \leftrightarrow 0 = 0$

$1 \leftrightarrow 1 = 1$

(vii) Implication :⇒ symbol : $\rightarrow$, if first operand is 1 and second operand is 0. ⇒ 0 else all are 1.

$0 \rightarrow 0 = 1$

$0 \rightarrow 1 = 1$

$1 \rightarrow 0 = 0$

$1 \rightarrow 1 = 1$

* Boolean operations in terms of- AND, OR, NOT.

(i) $P \vee Q \Rightarrow \neg(\neg P \wedge \neg Q)$

(ii) $P \rightarrow Q \Rightarrow \neg\{P \vee Q\} \Rightarrow \neg P \vee Q$

(iii) $P \longleftrightarrow Q \Rightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$

(iv) $P \oplus Q \Rightarrow \neg(P \longleftrightarrow Q)$

* Distributive Law :- on AND and OR.

(i) $P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$

(ii) $P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$.

* De-Morgans Law :-

(i) $\sim(P \wedge Q) = (\sim P) \vee (\neg Q)$

(ii) $\neg(P \vee Q) = (\neg P) \wedge (\neg Q)$

Lecture ④ :- Fundmental Technique of Proof

① Direct Proof (Proof by construction)
② Proof by contradiction
③ Proof by induction.

① Direct Proof :-

In a constructive proof one attempts to demonstrate $P \Rightarrow Q$ directly.

1. Assumes P is true
2. Use P to show Q is true.

i.e., it is used to prove implications, statements which have 2 parts, an "if-part" known as Premises and a "then Part" known as conclusion.

→ In this one starts with a perwises and proceed directly to conclusion with a chain of implications that use known facts, laws, and functions.

E.g.① Prove that- " If n is an odd integer then n^2 is odd".

Proof :- Let assume n is an odd integer.
∴ there must be a k such that.

$$n = 2k+1.$$

$$\therefore n^2 = (2k+1)^2$$

$$n^2 = 4k^2 + 4k + 1$$

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

∴ any no is multiplied by 2 is an even number and even+1 = odd

∴ n^2 is an odd number.

Eg. ② If a and b are both consicutive numbers then show that- a+b is odd number.

proof :- Let us assume a and b are consicutive.

So, $b = a+1$

$\therefore a+b = a+(a+1)$

$= 2a+1$

$\Rightarrow$ even +1 $\neq$ odd

$\therefore$ As any no is multiplied by 2 it is even number.

$\therefore$ And even+1 is odd number.

Eg. ③ Show that- if m and n are both square numbers then m.n is also a square number.

proof :- Let us assume. m and n both are square no.

$\therefore$ there must u and v, such that

$m = u^2$

$n = v^2$

$\therefore m.n = u^2 v^2$

$= (u.v)^2$

As. m.n is square of u.v so m.n is also a square number.

(2) Proof by contradiction :-

"A common form of proving theorems is assuming that theorem is false, and then show that the assumption is false itself, and is therefore a contradiction."

Technique :- If p then q. [$p \wedge q$ is true]

- Assume the negation of q.
- In other words, assume that $p \wedge \neg q$ is true.
- Then arrived at a contradiction $p \wedge \neg q$
- Since $p \wedge \neg q$ can not happen, our assumption must be wrong
- Thus $\neg q$ is wrong so q is true

In short :-
1. Assume p is true
2. Assume $\neg q$ is true
3. Use p and $\neg q$ to show contradiction.

E.g. (1) If a and b are consecutive integers, then the sum $a+b$ is odd.

Proof :- Let us assume- a and b are consequtive integers.
Let us assume that- $a+b$ is even.
∴ there must not be any k such that-
$a+b \neq 2k+1$

but as. a and b are consecutive so
$a \pm b = 2a+1$

i.e. $a+b \neq 2k+1$ and
$a+b = 2a+1$ this is contradiction

∴ $a+b$ is odd number.

E.g. ② If 'a' is a real number and $a > 0$ then $\frac{1}{a}$ is also > 0.

Proof :- $\frac{1}{a} > 0$ To prove.

Let use assume that- $a > 0$ and $\frac{1}{a} \leq 0$

Since $\frac{1}{a} \leq 0$ so there exist some real number $b > 0$

Such that- $\frac{1}{a} + b = 0$

$\therefore$ multiply both side by a.

$$\therefore \quad a\left(\frac{1}{a}\right) + ab = 0$$

$$1 + ab = 0$$

So as per assumption, either both $a > 0$ and $b > 0$

So $a.b > 0$

$\therefore$ To hold $1 + ab = 0$

$1 < 0$ as $ab > 0$

this contradict the fact that $1 > 0$. therefore the assumption $\frac{1}{a} \leq 0$ is false.

$\therefore \frac{1}{a} > 0$ is true.

E.g. ③ :- If $(3n+2)$ is odd, then n is also odd number.

Proof :- Let $(3n+2)$ is odd.

now, assume that n is not odd, that is n is even.

∴ If n is even, there is some integer k

∴ $n = 2k$.

∴ $(3n+2) \Rightarrow (3 \times 2k + 2) \Rightarrow 2(3k+1)$

i.e. 2 times of a number.

Thus, $(3n+2)$ turned out to be even, but we know is odd.

∴ This is contradiction and the assumption is wrong.

∴ n must be odd.

E.g. (4) Prove that $\sqrt{2}$ is irrational number.

proof:- (1) Let us assume $\sqrt{2}$ is rational.

∴ we can say that $\sqrt{2} = \frac{a}{b}$ and $b \neq 0$

Additionally, we assume that a and b are two lowest terms. ∴ either of a and b one must be even and one must be odd. If both are even that we can further simplify a/b. — (1)

or. $\sqrt{2} = \frac{a}{b}$

$(\sqrt{2})^2 = \left(\frac{a}{b}\right)^2$

$2 = \frac{a^2}{b^2}$

or $a^2 = 2b^2$

So the square of a is even number ∴ a is even

now, as a is even, so there must be k such that-

$a = 2k$.

now, substitute $a = 2k$. in eq^n (1)

$2 = \frac{(2k)^2}{b^2}$

$$2 = (2k)^2 / b^2$$

$$2 = \frac{4k^2}{b^2}$$

$$2 \cdot b^2 = 4k^2$$

$$b^2 = 2k^2$$

This mean that b^2 is even, $\therefore$ b is even. and it- is contradiction. that- a is even and b is even

$\therefore$ $\sqrt{2} \neq$ rational

so $\sqrt{2}$ is irrational.

Proof:- ② Let us assume that- $\sqrt{2}$ is rational. with p and q as co-prime and $q \neq 0$.

$\therefore \sqrt{2} = \frac{p}{q}$ and HCF(p, q) = 1

$$(\sqrt{2})^2 = \frac{p^2}{q^2}$$

$$2 = \frac{p^2}{q^2}$$

$p^2 = 2q^2$ $\therefore$ p^2 is even number so, p is even.

$\therefore$ as p is even so, $p = 2k$ for some k.

Now, we can write

$$(\sqrt{2})^2 = \frac{(2k)^2}{q^2}$$

$$2^2 = \frac{4k^2}{q^2}$$

$$2q^2 = 4k^2$$

$q^2 = 2k^2$ $\therefore$ q^2 is even so, q is also even.

∴ as p and q both are even

So, they have 2 as common factor.

i.e. HCF(p, q) = 2

∴ p and q are not co-prime.

that is the contradiction ∴ $\sqrt{2}$ is irrational no.

Proof :- (3) Euclid Proof

Let us assume $\sqrt{2}$ is rational

$\therefore \sqrt{2} = \frac{p}{q}$ for some p and q where, $q \neq 0$.

$(\sqrt{2})^2 = \frac{p^2}{q^2}$

$\therefore 2 = \frac{p^2}{q^2}$

$p^2 = 2q^2$ ⇒ as p^2 is even so p is even

$\therefore p = 2m$ for some m.

$\therefore 2 = \frac{p^2}{q^2}$

$2 = \frac{(2m)^2}{q^2}$

$2q^2 = 4m^2$

$q^2 = 2m^2$ ⇒ as q^2 is even so q is even

$\therefore q = 2n$. for some n.

$\therefore \sqrt{2} = \frac{p}{q} = \frac{2m}{2n} = \frac{m}{n}$ → simplified version.

→ Now repeat the same process for $\frac{m}{n}$ and go on.

But, we know that any rational number can not be simplified indefinitely. ∴ Contradiction.

$\sqrt{2}$ is irrational.

(3) Proof by Induction :-

→ It is a technique used to prove statements about objects that can be defined using recursive function.

→ It is a very powerful method, that uses recursion.

1. Show that propositional form $P(x)$ is true for some basic case.
2. Assume that $P(n)$ is true for some n, and show that $P(n+1)$ is true.
3. Then from $P(n)$ is true for all n greater than or equal to the basis case.

E.g. ① :- If a and b are consicutive integers, then the sum a+b is odd.

Proof :- Let a and b are two consecutive numbers.

So, let $a = x$
$b = x+1$

$\therefore F(x) = a+b$
$= x + x+1$

Step ① :- Conside $F(x)$ for $x=1$.

$F(1) = 1+1+1 = 3$.

$\therefore F(x)$ is true for $x=1$.

Step ② :- assume that $F(x)$ is true for some x.

we will say that $x+(x+1)$ is odd.

$\therefore F(x) = x+x+1$
$= \underline{2x+1}$.

Step ③ :- proof for $F(x+1)$

$F(x+1) = \cancel{(x+1)(x+1)}\ x+1+(x+1)+1$

$F(x+1) = 2x+1+2$

$F(x+1) = \underbrace{2x+1}_{odd} + 2$

$= \underbrace{odd+2}_{odd}$.

$\therefore F(x+1)$ is odd.

Thus, we can claim that by principle of mathematic Induction $F(x)$ is odd for all x.

E.g.(2) :- proof that- $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$ for $\forall\, n \in Z_+$.

proof :- To prove.

$$f(n) = \sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}, \quad \forall\, n \in Z_+.$$

Base case:- for $n=1$.

$$\therefore \frac{1}{1\cdot(1+1)} = \frac{1}{1+1}$$

$\frac{1}{2} = \frac{1}{2}$, so $F(n)$ is true for $n=1$.

Induction step:- Let $k \in Z_+$ and we assume that- $F(k)$ is true. Then.

$$F(k) = \sum_{i=1}^{k} \frac{1}{i(i+1)} = \frac{k}{k+1} \quad \text{is true.}$$

Let use proof for $F(k+1)$

$$F(k+1) = \sum_{i=1}^{k+1} \frac{1}{i(i+1)} = \sum_{i=1}^{k} \frac{1}{(i+1)} + \frac{1}{(k+1)(k+2)}$$

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

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

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

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

$$= \frac{k+1}{k+2}$$

$$= \frac{k+1}{(k+1)+1} \quad \text{for } n=k+1$$

Thus $F(n)$ holds for $n=k+1$.

$\therefore$ By principle of mathematical induction $F(n)$ is true for $\forall\, n \in Z_+$

E.g. (3) prove that $\sum_{i=1}^{n} (2i-1) = n^2$ for all $n \in Z+$

proof Let $F(n) \Rightarrow \sum_{i=1}^{n} (2i-1) = n^2 \quad \forall n \in Z+$

Base Case :- When $n=1$.

$F(1) \Rightarrow (2 \times 1 - 1) = 1^2$

$2-1 = 1^2$

$1 = 1$ proved. $F(n)$ is true for $n=1$.

Induction :- Let $k \in Z+$ and $F(k)$ is true

$\therefore$ for $k+1$

$$\therefore F(k+1) = \sum_{i=1}^{k+1} (2i-1)$$

$$= \sum_{i=1}^{k} (2i-1) + \sum_{i=k+1}^{k+1} (2i-1)$$

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

$$= k^2 + 2k + 2 - 1$$

$$= k^2 + 2k + 1$$

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

$\therefore$ True. for $F(k+1) = (k+1)^2$

$\therefore$ By principle of mathematical induction we can say that $F(n)$ is true for $\forall n \in Z+$.