DISCRETE MATHEMATICAL STRUCTURES

→ purpose of logic is to construct valid arguments.

→ once we prove a mathematical statement true → we call it Theore

Proposition: declarative sentence.

which can be either True (or) False [but not both]

Ex: Delhi is capital of India — True (T)

1 + 1 = 2 — True (T)

Banglore is in Gujrat — False (F)

What time it is ? (Not a proposition)

Go to bed. (Not a proposition)

$\frac{0}{0} = 0$ - False (F)

Also known as sentential logic / Statement logic.

Logical Operators:

1) AND - conjunction ($P \wedge Q$)
2) OR - disjunction ($P \vee Q$)
3) NOT - negation ($\sim P$)
4) Conditional ($P \rightarrow Q$) — Implication
5) Bi Condititional ($P \leftrightarrow Q$)

Conjunction:

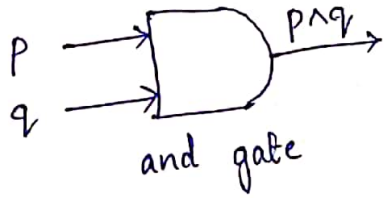
Multiplication ↑

P	Q	$P \wedge Q$
F	F	F
F	T	F
T	F	F
T	T	T

P AND Q

$P \wedge Q$

→ and
→ but



No. of cases = $2^{(\text{no. of propositions})}$

- 0 - False
  1 - True

propositions — P, q ....

conjuction — X or intersection (∩)

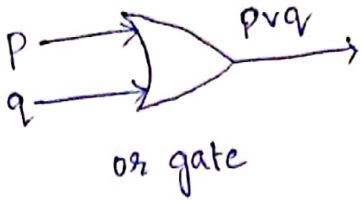
Disjunction:

P	Q	P∨Q
F	F	F
F	T	T
T	F	T
T	T	T

addition

P OR Q
P∨Q

~~→ and~~
~~→ but~~

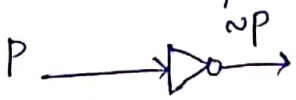


or gate

Negation:

P	~P
F	T
T	F

NOT P
~P / ¬P



→ 'It is not the case that...'
→ 'It is false that...'
→ doesn't.

Examples:

P: Pavana speaks English.
Q: Pavana speaks Hindi.
P∧Q – Pavana speaks English and Hindi.
P∨Q – Pavana speaks English or Hindi.
~P – It is false that Pavana speaks English.
~Q – It is not the case that Pavana speaks Hindi.

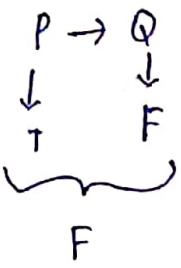
- P: The function is differentiable → antecedent (hypothesis) / premise
  Q: The function is continuous. → consequent (conclusion) / consequence
  P → Q: If the function is differentiable then it is continuous.

Conditional Statement:

P → Q

- P only if Q
- P implies Q
- P is sufficient for Q
- Q if P
- If P, the Q
- If P, Q.

P	Q	P → Q
F	F	T
F	T	T
T	F	F
T	T	T



Bi conditional:

P if and only if Q

$P \longleftrightarrow Q$

P, Q → identical truth values → T

else → Truth value is F

P	Q	$P \longleftrightarrow Q$
F	F	T
F	T	F
T	F	F
T	T	T

Ex: Two lines are parallel if and only if they have same slope.

Truth Table for:

$P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R)$

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
F	F	F	F	F	F	F	F
F	F	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	T	T	T	F	F	F	F
T	F	F	F	F	F	F	F
T	F	T	T	T	F	T	T
T	T	F	T	T	T	F	T
T	T	T	T	T	T	T	T

$\therefore P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R)$

→

P	Q	$P \vee Q$	$\sim(P \vee Q)$	$\sim P$	$\sim Q$	$\sim P \wedge \sim Q$
F	F	F	T	T	T	T
F	T	T	F	T	F	F
T	F	T	F	F	T	F
T	T	T	F	F	F	F

$\therefore \sim(P \vee Q) \iff (\sim P) \wedge (\sim Q)$

Tautology:

A compound statement that is always true, irrespective of truth values of proposition that occur in it, is called tautology.

$[P \wedge (P \to Q)] \to Q$ is a tautology.

P	Q	$P \to Q$	$P \wedge (P \to Q)$	$[P \wedge (P \to Q)] \to Q$
F	F	T	F	T
F	T	T	F	T
T	F	F	F	T
T	T	T	T	T

→ $(P \to Q) \iff (\sim P \vee Q)$

P	Q	$P \to Q$	$\sim P$	$\sim P \vee Q$	$(P \to Q) \longleftrightarrow (\sim P \vee Q)$
F	F	T	T	T	T
F	T	T	T	T	T
T	F	F	F	F	T
T	T	T	F	T	T

→ $(P \to Q) \wedge (Q \to R) \to (P \to R)$

P	Q	R	$P \to Q$	$Q \to R$	$P \to R$	$(P \to Q) \wedge (Q \to R)$	$(P \to Q) \wedge (Q \to R) \to (P \to R)$
F	F	F	T	T	T	T	T
F	F	T	T	T	T	T	T
F	T	F	T	F	T	F	T
F	T	T	T	T	T	T	T
T	F	F	F	T	F	F	T
T	F	T	F	T	T	F	T
T	T	F	T	F	F	F	T
T	T	T	T	T	T	T	T

1) $\{P \to (Q \to R)\} \to \{(P \to Q) \to (P \to R)\}$

P	Q	R	P→Q	Q→R	P→R	P→(Q→R)	(P→Q)→(P→R)	P→(Q→R) (P→Q)→(P→
F	F	F	T	T	T	T	T	T
F	F	T	T	T	T	T	T	T
F	T	F	T	F	T	T	T	T
F	T	T	T	T	T	T	T	T
T	F	F	F	T	F	T	T	T
T	F	T	F	T	T	T	T	T
T	T	F	T	F	F	F	F	T
T	T	T	T	T	T	T	T	T

2) (i) $\sim(P \vee \sim Q) \to \sim P$

P	Q	~Q	P∨~Q	~(P∨~Q)	~P	~(P∨~Q)	~(P∨~Q)→~P
F	F	T	T	F	T	F	T
F	T	F	F	T	T	T	T
T	F	T	T	F	F	F	T
T	T	F	T	F	F	F	T

(ii) $\sim P \to (P \to Q)$

P	Q	~P	P→Q	~P→(P→Q)
F	F	T	T	T
F	T	T	T	T
T	F	F	F	T
T	T	F	T	T

Contradiction:

A compound statement that is always false, irrespective of the truth ~~table~~ value of proposition occurs in it, is called contradiction.

Ex: $P \wedge \sim P$ is a contradiction

But $P \vee \sim P$ is a tautology

P	~P	P∧~P
F	T	F
T	F	F

Contingency:

A statement that is neither tautology nor a contradiction is called a contingency.

~~Converse~~:

→ $P \wedge (\sim P \wedge Q)$ is a contradiction.

P	Q	$\sim P$	$\sim P \wedge Q$	$P \wedge (\sim P \wedge Q)$
F	F	T	F	F
F	T	T	T	F
T	F	F	F	F
T	T	F	F	F

converse:

The proposition $Q \to P$ is called converse of $P \to Q$

contrapositive:

The proposition $\sim Q \to \sim P$ is called contrapositive of $P \to Q$

Inverse:

The proposition $\sim P \to \sim Q$ is called inverse of $P \to Q$

Ex: P: Today is a holiday.
Q: I will go for a movie.

converse: If I will go for a movie then today is a holiday.

contrapositive: If I will not go for a movie the it is not a holiday.

inverse: If I ~~will~~ is not a holiday then I will not go for a movie.

Equivalence (Bi-conditional)

$P \leftrightarrow Q$ is tautology and is denoted as $P \Leftrightarrow Q$

P	$\sim P$	$\sim(\sim P)$	$\sim(\sim P) \leftrightarrow P$
F	T	F	T
T	F	T	T

$\therefore \sim(\sim P) \Leftrightarrow P$

$P \wedge P \Leftrightarrow P$

P	P	$P \wedge P$	$P \wedge P \leftrightarrow P$
F	F	F	T
T	T	T	T

→ $(P \rightarrow Q) \Leftrightarrow (\sim P) \vee Q$

P	Q	$P \rightarrow Q$	$\sim P$	$\sim P \vee Q$	$(P \rightarrow Q) \leftrightarrow (\sim P \vee Q)$
F	F	T	T	T	T
F	T	T	T	T	T
T	F	F	F	F	T
T	T	T	F	T	T

→ $[(P \wedge (\sim P)) \vee Q] \Leftrightarrow Q$

P	Q	$\sim P$	$P \wedge \sim P$	$(P \wedge (\sim P)) \vee Q$	$(P \wedge (\sim P)) \vee Q \leftrightarrow Q$
F	F	T	F	F	T
F	T	T	F	T	T
T	F	F	F	F	T
T	T	F	F	T	T

→ $P \vee (\sim P) \Leftrightarrow Q \vee (\sim Q)$

P	Q	$\sim P$	$\sim Q$	$P \vee (\sim P)$	$Q \vee (\sim Q)$	$P \vee (\sim P) \leftrightarrow Q \vee (\sim Q)$
F	F	T	T	~~F~~ T	T	T
F	T	T	F	~~F~~ T	T	T
T	F	F	T	~~F~~ T	T	T
T	T	F	F	~~F~~ T	T	T

→

P	Q	R	PVQ	$(PVQ) \rightarrow R$	$P \rightarrow R$	$Q \rightarrow R$	$(P \rightarrow R) \wedge (Q \rightarrow R)$	$(PVQ) \rightarrow R \Leftrightarrow (P \rightarrow R) \wedge (Q \rightarrow R)$
F	F	F	F	T	T	T	T	T
F	F	T	F	T	T	T	T	T
F	T	F	T	F	T	F	F	T
F	T	T	T	T	T	T	T	T
T	F	F	T	F	F	~~F~~	F	T
T	F	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F	T
T	T	T	T	T	T	T	T	T

→ $P \vee (Q \wedge R) \iff [(P \vee Q) \wedge (P \vee R)]$

P	Q	R	$Q \wedge R$	$P \vee (Q \wedge R)$	$P \vee Q$	$P \vee R$	$(P \vee Q) \wedge (P \vee R)$	$P \vee (Q \wedge R) \leftrightarrow (P \vee Q) \wedge (P \vee R)$
F	F	F	F	F	F	F	F	T
F	F	T	F	F	F	T	F	T
F	T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T	T
T	F	F	F	T	T	T	T	T
T	F	T	F	T	T	T	T	T
T	T	F	F	T	T	T	T	T
T	T	T	T	T	T	T	T	T

The Laws of Logic

1) Law of double negation:

$$\sim(\sim P) \iff P$$

2) Idempotent Laws:

$P \vee P \iff P$

$P \wedge P \iff P$

3) Identity laws:

$P \vee F \iff P$

$P \wedge T \iff P$

4) Inverse laws:

$P \vee \sim P \iff T$

$P \wedge \sim P \iff F$

5) Domination Laws:

$P \vee T \iff T$

$P \wedge F \iff F$

6) Commutative laws:

$P \vee Q \iff Q \vee P$

$P \wedge Q \iff Q \wedge P$

7) Absorption laws:

$P \vee (P \wedge Q) \iff P$

$P \wedge (P \vee Q) \iff P$

P	Q	$P \wedge Q$	$P \vee (P \wedge Q)$	$P \vee Q$	$P \wedge (P \vee Q)$
F	F	F	F	F	F
F	T	F	F	T	F
T	F	F	T	T	T
T	T	T	T	T	T

8) De Morgan laws $\quad \wedge \to \vee$

(i) $\sim(P \vee Q) \Leftrightarrow \sim P \wedge \sim Q \quad \vee \to \wedge$

(ii) $\sim(P \wedge Q) \Leftrightarrow \sim P \vee \sim Q$

9) Associative laws

(i) $P \vee (Q \vee R) \Leftrightarrow (P \vee Q) \vee R$

(ii) $P \wedge (Q \wedge R) \Leftrightarrow (P \wedge Q) \wedge R$

10) Distributive laws

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

(ii) $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$

11) Law of negation of a condition.

(i) $\sim(P \to Q) \Leftrightarrow P \wedge (\sim Q)$

P	Q	$P \to Q$	$\sim(P \to Q)$	$\sim Q$	$P \wedge (\sim Q)$
F	F	T	F	T	F
F	T	T	F	F	F
T	F	F	T	T	T
T	T	T	F	F	F

(ii) $\sim(P \vee Q) \Leftrightarrow \sim P \wedge \sim Q$

(iii) $\sim(P \wedge Q) \Leftrightarrow \sim P \vee \sim Q$

(iv) $(P \to Q) \Leftrightarrow (\sim P) \vee Q$

Example: Prove logical equivalence

$$(P \to Q) \wedge [\sim Q \wedge (R \vee \sim Q)] \Leftrightarrow \sim(Q \vee P)$$

Sol: LHS: $(P \to Q) \wedge [\sim Q \wedge (R \vee \sim Q)]$ By commutative law

$(P \to Q) \wedge [\sim Q \wedge (\sim Q \vee R)]$ By Absorption law

$(P \to Q) \wedge (\sim Q) \quad P \to Q \Rightarrow P \wedge \sim Q$

~~$(\sim P) \vee Q) \wedge (\sim Q)$~~ By commutative law

$\sim ((P \to Q) \to Q)$

$\sim \sim (P \to Q) \vee Q$

$\sim (P \wedge \sim Q) \vee Q$ By distribution law

$\sim (Q \vee P) \wedge (Q \vee \sim Q)$

$\sim (Q \vee P) \wedge T$

$\sim (Q \vee P)$

→ $[(P \vee Q) \wedge \sim(\sim P \wedge (\sim Q \vee \sim R))] \vee (\sim P \wedge \sim Q) \vee (\sim P \wedge \sim R)$

Sol: $[(P \vee Q) \wedge P \vee (Q \wedge R)] \vee \sim(P \vee Q) \vee \sim(P \vee R)$ By double negation law and de morgan's law

$[(P \vee Q) \wedge (P \vee Q) \wedge (P \vee R)] \vee \sim(P \vee Q) \vee \sim(P \vee R)$

By Distribution Law and Idempotent law

$(P \vee Q) \wedge (P \vee R) \vee \sim((P \vee Q) \wedge (P \vee R))$ By Inverse law $P \vee \sim P = T$

Associative law.

~~$(P \vee Q)$~~ $= T$

Tautology

Satisfiable:

A compound proposition is satisfiable if there is an assignment of truth values to its variables that makes it true. when no such assignments exists, that is, when compound preposition is false for all assignments of truth ~~tables~~ values to its variables, the compound proposition is unsatisfiable.

Duality Law:

$S, S^* \longrightarrow$ $\wedge \rightarrow \vee$

$T \rightarrow F$ (or)

$F \rightarrow T$

(4th)

→ $[(\sim P \vee Q) \wedge (P \wedge (P \wedge Q))] \Leftrightarrow P \wedge Q$ deduce to

$[(\sim P \vee Q) \vee (P \wedge (P \wedge Q))] \Leftrightarrow P \vee Q$

Sol: $[(\sim P \vee Q) \wedge (P \wedge (P \wedge Q))] \Leftrightarrow P \wedge Q$

$[\sim(\sim P \vee Q) \vee \sim(P \wedge (P \wedge Q))] \Leftrightarrow \sim P \vee \sim Q$

By

LHS : (Given)

$(\sim P \vee Q) \wedge (P \wedge (P \wedge Q))$

$\Leftrightarrow (\sim P \vee Q) \wedge ((P \wedge P) \wedge Q)$ Associative laws

$\Leftrightarrow (\sim P \vee Q) \wedge (P \wedge Q)$

$\Leftrightarrow (\sim P \vee Q) \wedge (Q \wedge P)$ Distributive law

$\Leftrightarrow [(\sim P \vee Q) \wedge Q] \wedge P$ re arranging to solve

$\Leftrightarrow [Q \wedge (\sim P \vee Q)] \wedge P$ Distributive laws

$\Leftrightarrow$ By Absorption Law,

$P \wedge (P \vee Q) \Leftrightarrow P$

So, $Q \wedge (Q \vee \sim P) \Leftrightarrow Q$

* HINT & idea is here

RHS : (Proved)

$\Leftrightarrow Q \wedge P \Leftrightarrow P \wedge Q$ (Distributive)

Deducing by replacing 'V' with '$\wedge$' $\Longrightarrow$

$[(\sim P \vee Q) \wedge (P \wedge (P \wedge Q))] \Leftrightarrow P \wedge Q$.

So, is

$[(\sim P \wedge Q) \vee (P \vee (P \vee Q))] \Leftrightarrow P \vee Q$.

Rules of Inference

$P_1, P_2, P_3, \ldots P_n$ & C → propositions

A compound proposition of form $(P_1 \wedge P_2 \wedge P_3 \wedge \cdots P_n) \rightarrow C$ is called argument

$P_1, P_2, P_3, \ldots P_n$ → premises C → conclusion

$C = P_1 \cap P_2 \cap P_3 \ldots \cap P_n$

P_1
P_2
P_3
$\vdots$
P_n
$\therefore C$

If the conjunction of the premises $(P_1 \wedge P_2 \wedge P_3 \wedge \cdots P_n)$ is true in atleast one possible situations, then the premises $P_1, P_2, P_3 \ldots P_n$ of an argument is said to be consistent.

Ex: $(P \vee Q)$ and $\sim P$ in an argument are consistence.

Sol: Expression $\Rightarrow (P \vee Q) \wedge \sim P$

P	Q	P∨Q	~P	(P∨Q) ∧ ~P
F	F	F	T	F
F	T	T	T	T
T	F	T	F	F
T	T	T	F	F

$(P \vee Q) \wedge \sim P$ is true when P is F and Q is T

Hence, consistent.

If the conjunction of the premises $(P_1 \wedge P_2 \wedge P_3 \wedge \cdots P_n)$ is False in every possible situation, then premises $P_1, P_2, P_3 \ldots P_n$ of an argument is said to be inconsistent.

Ex: P and $(\sim P \wedge Q)$ in an argument is inconsistent.

Sol: Expression $\Rightarrow P \wedge (\sim P \wedge Q)$

P	Q	~P	~P∧Q	P∧(~P∧Q)
F	F	T	F	F
F	T	T	T	F
T	F	F	F	F
T	T	F	F	F

∴ All possible situations are False in $P \wedge (\sim P \wedge Q)$

Hence, inconsistent.

Ex: Validity of the following argument

"If I try and I have a talent, then I will become scientist
If I become scientist, then I will be happy.
Therefore, If I will not be happy then I didnot try hard or
I do not have talent".

Sol: Propositions: 1) I try — P
2) I have a talent — Q
3) I will become scientist — R
4) I will be happy. — S

$\Rightarrow (P \wedge Q) \rightarrow R$

$\Rightarrow R \rightarrow S$

$\Rightarrow (\sim S) \rightarrow (\sim P) \vee (\sim Q)$

$P \wedge Q \rightarrow R$

$R \rightarrow S$

$\therefore (\sim S) \rightarrow (\sim P) \vee (\sim Q)$

Validity of the Argument:

An argument with premises $P_1, P_2, P_3 \ldots P_n$ and conclusion C is said to be valid. if each of premises $P_1, P_2, P_3 \ldots P_n$ is true, then conclusion C is likewise true. The conclusion is true only in the case of valid argument.

conjunction of premises $\rightarrow$ conclution.

$(P_1 \wedge P_2 \wedge P_3 \wedge \ldots P_n) \rightarrow C$ is a tautology.

Method:

→ Truth table construction
→ Identify the rows called critical rows in which all premises are T.
In case no such row is found, the argument is invalid.
→ In each critical row, find whether conclusion is true.
In such case the argument is valid, otherwise invalid.
→ If atleast one critical row contains false conclusion, then argument is invalid.

Ex: If the morning is fine, I go for a walk
I do not go for a walk

∴ The morning is not fine

Sol: Propositions:

$P \rightarrow$ The Morning is fine
$Q \rightarrow$ I go for a walk

$\sim P \rightarrow$ The morning is not fine
$\sim Q \rightarrow$ I donot go for a walk.

$$\begin{array}{l} P \rightarrow Q \\ \sim Q \\ \hline \therefore \sim P \end{array}$$

Valid

P	Q	$P \rightarrow Q$ Premises	$\sim Q$ Premises	$\sim P$ Conclusion
F	F	T	T	T ✓
F	T	T	F	T
T	F	F	T	F
T	T	T	F	F

The critical row here row 1 contains true conclusions and hence the argument is valid.

Critical row decide nature of the row.
Critical row is considered for premises only. (T, T) case only.

Ex: If two sides of a triangle are equal, then the opposite angels are equal
P Q
(Two sides of a triangle are not equal) $\sim P$
$\therefore$ (The opposite angles are not equal) $\sim Q$

Sol:

$$\begin{array}{l} P \rightarrow Q \\ \sim P \\ \hline \therefore \sim Q \end{array}$$

P	Q	PREMISES $P \rightarrow Q$	$\sim P$	CONCLUSION $\sim Q$	$(P \rightarrow Q) \wedge \sim P$	$(P \rightarrow Q) \wedge \sim P \rightarrow \sim Q$
F	F	(T	T)	T ✓	T	T
F	T	(T	T)	F X	T	F
T	F	F	F	T	F	T
T	T	T	F	F	F	T

$(P \rightarrow Q) \wedge \sim P \rightarrow \sim Q$ is not a tautology.
critical row 1 $\rightarrow$ T
critical row 2 $\rightarrow$ F

Hence, the argument is invalid.

Rules of Interference:

1) $\begin{array}{l} P \\ P \rightarrow q \\ \hline \therefore q \end{array}$ $\quad p \wedge (p \rightarrow q) \rightarrow q$ — Modus ponens

2) $\begin{array}{l} \sim q \\ p \rightarrow q \\ \hline \therefore \sim p \end{array}$ $\quad (\sim q) \wedge (p \rightarrow q) \rightarrow \sim p$ — Modus tollens

3) $\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$ $\quad (p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$ — Hypothetical Syllogism

4) $p \vee q$, $\sim p$ $\therefore q$ — $(p \vee q) \wedge (\sim p) \rightarrow q$ — Disjunctive Syllogism

5) p $\therefore p \vee q$ — $p \rightarrow (p \vee q)$ — Addition

6) $p \wedge q$ $\therefore p$ — $(p \wedge q) \rightarrow p$ — Simplification

7) p, q $\therefore p \wedge q$ — $p \wedge q \rightarrow (p \wedge q)$ — Conjunction

8) $p \vee q$, $\sim p \vee r$ $\therefore q \vee r$ — $(p \vee q) \wedge (\sim p \vee r) \rightarrow (q \vee r)$ — Resolution

Ex: If (I study), I will not fail in the examination
If I do not watch TV in the evenings, I will study
q (I failed in the examination)
Therefore, (I must have watched TV in the evenings)
r

Sol: $p \rightarrow \sim q$, $\sim r \rightarrow p$, q $\therefore r$

Logical expression:

$(p \rightarrow \sim q) \wedge (\sim r \rightarrow p) \wedge q \Longleftrightarrow r$

		(C)		(P)		(P)
p	q	r	$\sim q$	$p \rightarrow \sim q$	$\sim r$	$\sim r \rightarrow p$
F	F	f	T	T	T	F
F	F	T ✓	T	(T)	F	(T)
F	T	F	F	T	T	F
F	T	T ✓	F	(T)	F	(T)
T	F	F ✗	T	(T)	T	(T)
T	F	T ✓	T	(T)	F	(T)
T	T	F	F	F	T	T
T	T	T	F	F	F	T

4 Critical rows
3 → True 1 → False

Invalid

→ Without using Truth tables

$(p \to \sim q) \wedge (\sim r \to p) \wedge q$

Sol: By contrapositive

$(\sim\sim q \to \sim p) \wedge (\sim p \to \sim\sim r) \wedge q \qquad (\sim\sim u \Leftrightarrow u)$

$(q \to \sim p) \wedge (\sim p \to r) \wedge q$ By Hypothetical syllogism

$(q \to r) \wedge q$ By Modus ponens

r

∴ The argument is valid.

Ex: (I will get grade A in this course) or (I will not graduate)

If I do not graduate, (I will join the army)

I got grade A

Therefore, I will not join the army

Sol: $P \vee \sim Q$

$\sim Q \to R$

P

$\therefore \sim R$

(P) P	Q	R	$\sim Q$	$P \vee \sim Q$ (P)	$\sim Q \to R$ (P)	$\sim R$ (C)
F	F	F	T	T	F	T
F	F	T	T	T	T	F
F	T	F	F	F	T	T
F	T	T	F	F	T	F
T	F	F	T	T	F	T
(T)	F	T	T	(T	T)	F X
(T)	T	F	F	(T	T)	T ✓
(T)	T	T	F	(T	T)	F X

3 critical Rows

2 – False

1 – True

Invalid

$(P \vee \sim Q) \wedge (\sim Q \to R) \wedge P \Leftrightarrow \sim R$

$(p \vee \sim q) \wedge (\sim q \rightarrow r) \wedge p \iff \sim R$

LHS: $(p \vee \sim q) \wedge (\sim(\sim q) \vee r)) \wedge p$

$(p \vee \sim q) \wedge (q \vee r) \wedge p$

$(\sim q \vee p) \wedge (q \vee r) \wedge p$

$(p \vee r) \wedge p$

$(p \wedge p) \vee (p \wedge r)$

$p \vee p \wedge R \neq \sim R$ Invalid

Ex:
$p \rightarrow q$
$r \rightarrow s$
$\sim q \vee \sim s$
$\therefore \sim(p \wedge r)$

Sol: $(p \rightarrow q) \wedge (r \rightarrow s) \wedge (\sim q \vee \sim s)$

$(\sim p \vee q) \wedge (\sim r \vee s) \wedge \sim(q \wedge s)$

$(\sim p \vee q) \wedge (\sim q \vee \sim s) \wedge (\sim r \vee s)$

$(q \vee \sim p) \wedge (\sim q \vee \sim s) \wedge (\sim r \vee s)$

$(\sim p \vee \sim s) \wedge (\sim r \vee s)$

$((\sim p) \vee (\sim s)) \wedge (s \vee (\sim r))$

$((\sim s) \vee (\sim p)) \wedge (s \vee (\sim r))$

$(\sim p \vee \sim r)$

$\sim(p \wedge r)$ Valid

Ex:
$p \rightarrow q$
$r \rightarrow s$
$p \vee r$
$\therefore (q \vee s)$

Sol: $(p \rightarrow q) \wedge (r \rightarrow s) \wedge (p \vee r) \iff (q \vee s)$

LHS: $(p \rightarrow q) \wedge (r \rightarrow s) \wedge (p \vee r)$

$(\neg p \vee q) \wedge (\neg r \vee s) \wedge (p \vee r)$

$(p \vee r) \wedge (\neg p \vee q) \wedge (\neg r \vee s)$

$(r \vee q) \wedge (\neg r \vee s)$

$(q \vee s)$ Valid

Ex: Show that $p \to q, p \to r, q \to \neg r, r$ are consistent whereas $p \to q, p \to r, q \to \neg r, p$ are inconsistent.

Sol: $(p \to q) \wedge (p \to r) \wedge (q \to \neg r) \wedge r$ ⟶ consistent

p	q	r	$p \to q$	$p \to r$	$\neg r$	$q \to \neg r$	$(p \to q) \wedge (p \to r) \wedge (q \to \neg r) \wedge r$
F	F	F	T	T	T	T	F
F	F	T	T	T	F	T	T ✓
F	T	F	T	T	T	T	F
F	T	T	T	T	F	F	F
T	F	F	F	F	T	T	F
T	F	T	F	T	F	T	F
T	T	F	T	F	T	T	F
T	T	T	T	T	F	F	F

$(p \to q) \wedge (p \to r) \wedge (q \to \neg r) \wedge p$ ⟶ inconsistent.

p	q	r	$p \to q$	$p \to r$	$\neg r$	$q \to \neg r$	$(p \to q) \wedge (p \to r) \wedge (q \to \neg r) \wedge p$
F	F	F	T	T	T	T	F
F	F	T	T	T	F	T	F
F	T	F	T	T	T	T	F
F	T	T	T	T	F	F	F
T	F	F	F	F	T	T	F
T	F	T	F	T	F	T	F
T	T	F	T	F	T	T	F
T	T	T	T	T	F	F	F

All False conclusions

∴ inconsistent.

Predicate Calculus: — Predicates, — Quantifiers

Logic + predicate + quantifi

"x is greater than 5"

x ↓ variable, greater than 5 ↓ predicate

Statement is denoted by P(x)

when particular value is substituted for x, then statement is called proposition. (P(x))

when given x = 3 P(3) — F

x = 9 P(9) — T

"x = y+2" denoted as Q(x,y)

for x = 1, y = 2 Q(x,y) — F

for x = 2, y = 0 Q(x,y) — T

Ex: "x + y = z"

Quantifiers:

Quantification expresses the extent to which a predicate is true over a range of elements.

P(x): x + 5 > 2

for all x in N i.e, ∀ x ∈ N (set of all Natural nos)

P(x) is true

→ for every integer x, x^2 is a non-negative integer

→ There exists a real number whose square is equal to itself

The words all, every, some, there exists are associated with the idea of a quantity Such words are called quantifiers.

Types: — Universal quantifier, — Existential quantifier

Universal Quantifier: "P(x) for all values of x in the domain"

(∀) x P(x) → universal quantification of P(x)

↳ universal quantifier. ∀x P(x) → P(x) is true for every x

for all, for every.

An element for which P(x) is false is called counter example of ∀x P(x).

- For every
- For all
- All of
- For each
- Given any
- For arbitary
- For any.

All x elements → $x_1, x_2, x_3 \ldots x_n$ $\Rightarrow \forall x\, P(x)$ is same as conjunction $P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n)$ are all true. $T \wedge T \Leftrightarrow T$ (only)

Existential Quantifier: The existential quantification of $P(x)$ is the proposition "There exists an element x in the domain such that $P(x)$."

$\exists x\, P(x)$ ⟶ existential quantification of $P(x)$

↳ existential quantifier

$\exists x\, P(x)$. There is an x for which $P(x)$ is true.

- For some
- For at least one
- there is one.

All elements, $x_1, x_2, x_3 \ldots x_n$

$\exists x\, P(x)$ is same as the disjunction $P(x_1) \vee P(x_2) \vee P(x_3) \ldots \vee P(x_n)$ true if and only if atleast one of $P(x_1), P(x_2) \ldots P(x_n)$ is true.

Example: For the universe of all integers.

$p(x)$: $x > 0$

$q(x)$: x is even

$r(x)$: x is a perfect square

$s(x)$: x is divisible by 3

$t(x)$: x is divisible by 7

(i) At least one integer is even. $\exists x, q(x)$

(ii) There exist a positive integer that is even. $\exists x, [p(x) \wedge q(x)]$

(iii) Some even integers are divisible by 3. $\exists x, [q(x) \wedge s(x)]$

(iv) If x is even and a perfect square, then x is not divisible by 3.

(v) If x is odd or is not divisible by 7, then x is divisible by 3.

(iv) $\forall x, [[q(x) \wedge r(x)] \longrightarrow \sim s(x)]$

(v) $\forall x, [[\sim q(x) \vee \sim t(x)] \longrightarrow s(x)]$

Example 1: Express each of these statements using predicates and quantifiers.

1) A passenger on an airline qualifies as an elite flyer if the passenger flies more than 25,000 miles in a year or takes more than 25 flights during that year.

Sol: Let $E(x)$: person x qualifies as an elite flyer in a given year.

$F(x,y)$: person x flies more than y miles in a given year.

$S(x,y)$: person x takes more than y flights in a given year.

Symbolic form: $\forall x, ((F(x,25000) \vee S(x,25)) \rightarrow E(x)$

elite → best trained

2) A man qualifies for the marathon if his best pervious time is less than 3 hours and a woman qualifies for the marthon if her best previous time is less than 3.5 hours.

Sol: $Q(x)$: Person x qualifies the marathon

$M(x)$: Person x is a man

$T(x,y)$: Person x has run a marathon in less than y hours.

$\forall x, [(M(x) \wedge T(x,3)) \wedge (\sim M(x) \wedge T(x,3.5))] \rightarrow Q(x)$

3) A student must take at least 60 course hours, or atleast 45 course hours and waite a master's thesis, and recieve a grade not lower than an B in all required courses, to recieve a master's degree.

Sol: Let M: The student recieved a master degree

$H(x)$: The student took at least x course hours.

T : The student wrote a thesis.

$G(B,y)$: The person got grade B or higher in a course y.

The symbolic form is,

$[(H(60) \vee (H(45) \wedge T)) \wedge \forall y\ G(B,y)] \rightarrow M$

4) There is a student who has taken more than 21 credit hours in a semester and receieved all A's.

Sol: $T(x,y)$: person x took more than y credit hours.

$G(x,P)$: Person x earned grade point average P

The Symbolic form is, $[\exists x, [T(x,21) \wedge G(x,4.0)]$

Example: Express each of these systems specifications using predicates and logical connectives.

1) At least one mail message can be saved if there is a disk with more than 10 kilobytes of free space

Sol: $F(x,y)$: Disc x has more than y kilobytes of free space.

$S(x)$: Mail message x can be saved.

$(\exists x, F(x,10)) \rightarrow \exists, S(x)$

2) Whenever there is an active alert, all queued messages are transmitted.

Sol: $A(x)$: Alert x is active.

$Q(x)$: Message x is queued.

$T(x)$: Message x is transmitted

$(\exists x, A(x) \rightarrow \forall x, (Q(x) \rightarrow T(x)))$

3) The diagnostic monitor tracks the status of all systems except the main console.

Sol: $T(x)$: diagnostic monitor tracks the status of system x.

$\forall x, (x \neq \text{main console}) \rightarrow T(x)$

4) Each participant on the conference call whom the host of the call did not put on special list was billed.

Sol: $L(x)$: host put x participants on list

$B(x)$: participant x was billed

$\forall x, (\sim L(x) \rightarrow B(x))$

Logical Equivalence involving quantifiers.

1) $\forall x, (P(x) \wedge Q(x)) \Leftrightarrow (\forall x, P(x)) \wedge (\forall x, Q(x))$

2) $\exists x, (P(x) \vee Q(x)) \Leftrightarrow (\exists x, P(x)) \vee (\exists x, Q(x))$

3) $\exists x, (P(x) \rightarrow Q(x)) \Leftrightarrow \exists x, (\sim P(x) \vee Q(x))$

4) $\sim [\forall x, P(x)] \equiv \exists x, [\sim P(x)]$

5) $\sim [\exists x, Q(x)] \equiv \forall x, [\sim Q(x)]$

6) $\sim \forall x (P(x) \rightarrow Q(x)) \equiv \exists x (P(x) \wedge \sim Q(x))$

Two rules of Interference

1) Rule of universal instantation: If an open statement $P(x)$ is known to be true for all x in a universe S and if $c \in S$, the $P(c)$ is true

2) Rule of universal generalization: If an open statement $P(x)$ is proved to be true for any (arbitary) x choosen from a set S, then the quantified statement $\forall x \in S, P(x)$ is true.

Rules of Interference for Quantified Statements:

→ $\dfrac{\forall x\ P(x)}{P(c)}$ universal instantiation.

→ $\dfrac{P(c) \text{ for an arbitary } c}{\forall x\ P(x)}$ universal generalization.

→ $\dfrac{\exists x\ P(x)}{P(c) \text{ for some element } c}$ Existential instantiation

→ $\dfrac{P(c) \text{ for some element } c}{\exists x\ P(x)}$ existential generalization.

Ex: 1) Test Validity of the argument

All men are mortal
Scrotes is a man
$\therefore$ Scrotes is mortal

Sol: $P(x)$: x is mortal (living things. Ex: people)

$S \Rightarrow$ set of all men $a \Rightarrow$ Scrotes

$$\frac{\begin{array}{c}\forall x \in S, P(x) \\ a \in S\end{array}}{P(a)}$$

$\forall x \in S, P(x)$ and $a \in S$ ⟶ universal instantiation rule

$P(a)$ is true.

Hence, the argument is valid.

2) No engineering student of First or second Semester studies logic
Anil is an engineering student who studies logic

$\therefore$ Anil is not in the second semester

Sol: $P(x)$: Engineering student x of First Semester

$Q(x)$: " " x " Second "

$R(x)$: Engg student x studies logic

a : Anil

$\forall x, (P(x) \vee Q(x) \longrightarrow \sim R(x))$

$R(a)$

$\sim Q(a)$

$\forall x, [P(x) \vee Q(x) \rightarrow (\sim R(x))] \wedge (R(a))$

$[P(a) \vee Q(a) \rightarrow \sim R(a)] \wedge R(a)$ Rule of universal instantiation.

Contitutative law and contrapositive law

$R(a) \wedge [R(a) \rightarrow \sim(P(a) \vee Q(a))]$ modus ponens.

$\sim(P(a) \vee Q(a))$ de Morgan law

$\sim P(a) \wedge \sim Q(a)$

$\sim Q(a) \wedge \sim P(a)$ Commutative law

$\sim Q(a)$ Simplification.

$\therefore$ Valid

→ When a hypothetical statement $p \rightarrow q$ is such that q is true whenever p is true, we say that p implies q i.e $p \Rightarrow q$.

Ex: $p \wedge (p \rightarrow q) \Rightarrow q$

p	q	$p \rightarrow q$	$p \wedge (p \rightarrow q)$	q	$(p \wedge (p \rightarrow q)) \rightarrow q$
F	F	T	F	F	T
F	T	T	F	T	T
T	F	F	F	F	T
T	T	T	T	T	T

3) Prove the following argument is valid.

$\forall x, [P(x) \vee Q(x)]$

$\exists x, \sim P(x)$

$\forall x, [\sim Q(x) \vee R(x)]$

$\forall x, [S(x) \rightarrow \sim R(x)]$

$\therefore \exists x, \sim S(x)$

Solution: $\forall x, [P(x) \vee Q(x)] \wedge [\exists x, \sim P(x)]$ for some a in universe

$[P(a) \vee Q(a)] \wedge (\sim P(a))$ Disjunctive Syllagism.

$\Rightarrow Q(a)$

Now, $\{\forall x, [P(x) \vee Q(x)] \wedge [\exists x, \sim P(x)] \wedge \forall x [\sim Q(x) \vee R(x)]$

$Q(a) \wedge (\sim Q(a) \vee R(a))$ commutative law

$(\sim Q(a) \vee R(a)) \wedge Q(a)$ Disjunctive Syllagism.

$\Rightarrow R(a)$

Now, $\{\forall x, [P(x) \vee Q(x)] \wedge [\exists x, \sim P(x)] \wedge \forall x [\sim Q(x) \vee R(x)] \wedge \forall x [S(x) \rightarrow \sim R(x)]$

$R(a) \wedge (S(a) \rightarrow \sim R(a))$ Modus tollens.

$\sim S(a)$ existential generalization.

$\exists x, \sim S(x)$

Proofs

→ A theorem may be the universal quantification of a conditional statement.

→ A proof is a valid argument that establishes the truth of a theorem

→ A corollary is a theorem that can be established directly from a theorem that has been proved.

→ A conjecture is a statement that is being proposed to be true statement, with some partial evidence, a heuristic argument, or the intuition of an expert.

Principle of Mathematical Induction:

Let $P(n)$ be a statement defined for all integers $n \geq n_0$

The given statement is true, if we can prove that

1) if $P(n_0)$ is true

2) if $P(k)$ is true for some $k > n_0$, the $P(k+1)$ must be true.

Ex: $P(n) = 11^{n+2} + 12^{2n+1}$ is divisible by 133.

when $n = 1$

$P(1) = 11^3 + 12^3 = 3059$

which is divisible by 133 $P(1)$ is true

now, $n = k$, $k \geq 1$

$p(k) = 11^{k+2} + 12^{2k+1} = 133(m)$ (Assume)

$p(k+1) = 11^{k+3} + 12^{2k+3}$

$= 11 \cdot 11^{k+2} + 144\,(12^{2k+1})$

$= 11 \cdot 11^{k+2} + (11 + 133)\ 12^{2k+1}$

$= 11\,(11^{k+2} + 12^{2k+1}) + 133 \cdot 12^{2k+1}$

$= 11 \cdot 133m + 13 \cdot 12^{2k+1}$

$p(k+1) = 133\,(11m + 12^{k+1})$

$p(n) = 133\,(11m + 12^n)$ is divisible by 133.

By principle of mathematical induction the statement is true for $n \geq 1$.

Methods of Proof:

- Direct Proof
- Indirect Proof

1) Direct Proof:

$P_1, P_2, P_3 \ldots P_n$ lead to conclusion c

$(P_1 \wedge P_2 \wedge P_3 \ldots P_n) \rightarrow c$ is a tautology

Such proof is called direct proof.

The direct method of proving a conditional $p \rightarrow q$ has the following lines of argument:

(i) Hypothesis: First assume p is true

(ii) Analysis: Employ rules / laws to prove q is true

(iii) Proof: $p \rightarrow q$ is true

Ex: P : healthy person

Q : Fruit juice in breakfast

a : Anil.

$\forall x, \; P(x) \rightarrow Q(x)$

$\sim Q(a)$

$\therefore \sim P(a)$

$P(a) \rightarrow Q(a)$

$\sim Q(a)$

$\therefore \sim P(a)$

By Modus tollens

The argument is true.

Ex: Prove that product of 2 odd integers is an odd integer.

Sol: $m = 2p+1$

$n = 2q+1$

$m.n \Rightarrow (2p+1)(2q+1)$

$\Rightarrow 4pq + 2(p+q) + 1$

$\Rightarrow 2(2pq + p+q) + 1$

$\Rightarrow 2(m)+1$ is odd integer

Indirect Proof: not direct

(i) proof by contraposition $p \rightarrow q \Leftrightarrow \sim q \rightarrow \sim p$

(ii) proof by contradiction

(i)

Ex: Prove that n^2 is even, then n is even, where n be an integer.

Sol: Let p : n^2 is even

q : n is even.

to prove $p \rightarrow q$ by proof of contraposition to show that $\sim q \rightarrow \sim p$

Let n is not even $\Rightarrow$ n is odd

$n = 2m+1$

$n^2 = (2m+1)^2 = 4m^2+4m+1$

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

$= 2(M)+1$ is odd

n^2 = odd which is contrapositive of given statement.

$\therefore n^2$ is even, n is even.

Ex: Prove that $m+n \geq 73$, then $m \geq 37$ or $n \geq 37$ where m, n are +ve integ

Sol: p: $m+n \geq 73$

q: ($m \geq 37$ or $n \geq 37$)

$p \rightarrow q$ by contraposition to prove $\sim q \rightarrow \sim p$

i.e, (not $m \geq 37$ and not $n \geq 37$) $\rightarrow$ not ($m+n \geq 73$)

$m \leq 36$ and $n \leq 36$

$m+n \leq (36+36)$

$m+n \leq 72$

not $(m+n) \geq 73$

Hence proved

(ii) Proof by contradiction.

1) Hypothesis: Assume $p \rightarrow q$ is false, p - true, q - false

2) Analysis: starting from q is false, $\therefore$ p is false

This contradicts the assumption is true.

3) Conclusion: $p \rightarrow q$ is true.

Ex: Prove that there is no rational number P/q whose square is 2, i.e show that $\sqrt{2}$ is an irrational number.

Sol: $(P/q)^2 = 2$ P, q - integers and have no common factor, $q \neq 0$

$p^2 = 2q^2$ i.e p^2 is even $\Rightarrow$ p is even

Let $p = 2m$

$p^2 = 4m^2 = 2q^2$

$q^2 = 2m^2$

q^2 is even and q is even

P, q are even and have common factor 2, which is a contradict to the Assumption p, q have no common factors.

Hence our assumption $\sqrt{2}$ is a rational no. is wrong

$\sqrt{2}$ is irrational no.

Ex: Prove that if $3n+2$ is even, then n is even, where n is an integer using
- proof by contraposition
- proof by contradiction.

Sol: $n \Rightarrow$ integer

if $3n+2$ is even, then n is even

(i) $\sim q \rightarrow \sim p$

n is not even then $(3n+2)$ is not even

or

n is odd the $(3n+2)$ is odd

Let n is odd i.e $n = 2k+1$

$$3n+2 = 3(2k+1)+2 = 6k+5 = 2(3k+2)+1$$

$(3n+2)$ is odd.

Hence, if $(3n+2)$ is even, then n is even.

(ii) $n = 2k+1$ (odd)

$$3n+2 = 3(2k+1)+2 = 6k+5 = 2(3k+2)+1$$

$3n+2$ is odd.

Contradiction that $(3n+2)k$ is even.

By Contradiction, if $3n+2$ is even, then n is even.

Q. Give (i) a direct proof (ii) an indirect proof and (iii) proof by contradiction for the statement:
"If n is an odd integer, the $n+11$ is an even integer".

Sol: $n = 2k+1$

(i) $n+11 = (2k+1)+11$

$= 2k+12$

$= 2(k+6)$

$\therefore n+11$ is even integer.

(ii) n is even $\Rightarrow 2k$. $\quad p \rightarrow q \iff \sim q \rightarrow \sim p$

$n+11 = 2k+11 \Rightarrow$ odd

$\therefore$ By contraposition. if n is odd $n+11$ is even.

4) P: Nixon is re-elected.
Q: Tulsa keeps air base
R: Tulsi votes

$\neg P \rightarrow \neg Q$
$P \leftrightarrow R$
$Q \rightarrow P$

P

$(\neg P \rightarrow \neg Q) \wedge (P \leftrightarrow R) \wedge (Q \rightarrow P)$ Contrapositive

$(Q \rightarrow P) \wedge (Q \rightarrow P) \wedge (P \leftrightarrow R)$

$(Q \rightarrow P) \wedge (P \leftrightarrow R)$

$(\neg Q \vee P) \wedge (P \leftrightarrow R)$ demorgan

$(\neg p \wedge q) \wedge (P \leftrightarrow R)$

~~$(P \rightarrow q) \wedge (P \leftrightarrow R)$ $\neg p \wedge (p \leftrightarrow R)$~~

~~$(\neg P \wedge p) \leftrightarrow (\neg p \wedge R)$~~ Inverse

~~$F \leftrightarrow (\neg p \wedge R)$~~

$F \wedge Q = F$

Invalid

5) For each of these arguments determine ~~the~~ whether the argument is correct or incorrect and explain why.

(a) $\forall x, P(x)$: x student in the class understand logic.

a = Xavier.

P(a) Universal instantiation.

Correct statement.

(b) $\forall x$, P(x): x Computer science student takes discrete.

a = Natasha.

P(a). Universal instantiation.

Correct statement.

(c) $\exists x$, P(x): x parrot like fruit

$\exists a$ = pet bird $a \neq$ parrot. Existential instantiation.

P(a) = F

Correct statement.

(d) $\forall x$, P(x): x eats granole everyday is healthy.

$\exists a$ = Linda. Existential instantiation.

P(a) = F

Linda does not eat granole every day

Correct statement

(iii) n is even $\Rightarrow 2k$

$n+11 = 2k+11 \rightarrow$ odd

By contradiction

n is odd then $n+11$ is even.

Practice Problems:

1) Test validity of an argument.

P: I will be physicist

Q: I will be a mathematician.

$P \vee Q$

$\sim Q$

P

$(P \vee Q) \wedge \sim Q \Leftrightarrow P$ Commutative law.

$(Q \vee P) \wedge \sim Q$ Disjunctive Syllogism

P Valid

2) P: Income tax rates ~~are lowered~~ increases

Q: Income tax collections increases.

$\sim p \rightarrow Q$

Q

$\sim p$

~~$(\sim p \rightarrow Q) \wedge Q \Leftrightarrow \sim p$~~ ~~Modus tollens.~~

~~$(p \vee Q) \wedge Q \quad \sim p$~~ .

$(\sim p \rightarrow Q) \wedge Q \Leftrightarrow \sim p$

$(P \vee Q) \wedge Q$ conjunction.

$(P \wedge Q) \wedge Q$ Simplification

P Invalid

3) P: I study

Q: I fail in the examination

R: my father gifts a two wheeler to me..

$(P \rightarrow \sim Q)$

$(\sim Q \rightarrow R)$

$(P \rightarrow R)$

$(P \rightarrow \sim Q) \wedge (\sim Q \rightarrow R)$

$(P \rightarrow R)$ Hypothetical syllogism

Valid

Nested Quantifiers:

Ex: $\forall x \exists y (x+y=0)$

everything within the scope of a quantifier can be thought of as a propositional function.

$\forall x \exists y (x+y=0) \Longrightarrow \forall x Qx$, $Q(x)$ is $\exists y P(x,y)$, $P(x,y) \Rightarrow x+y=0$

Ex: "The sum of two positive integers is always positive."

Ex: Assume that the domain for the variables x and y consists of all real numbers.

Sol: $\forall x \forall y (x+y = y+x)$ Says that

$x+y = y+x$ for all real numbers x and y.

* Commutative law for addition of real numbers *

Ex: The statement $\forall x \exists y((x+y)=0)$ say that for every real number x there is a real no. y such that $x+y=0$.

* Every real number has an additive inverse *

Ex: $\forall x \forall y \forall z (x + (y+z) = (x+y) + z)$

* Associative law for addition of real numbers *

Ex: Translate the compound propositions into English statement.

$\forall x \forall y ((x>0) \wedge (y<0) \rightarrow (xy<0))$, where the domain for both variables consists of all real numbers.

Sol: for every real no. x and y.

if $x>0$ (i.e x is positive) and $y<0$ (i.e y is negative), then $xy<0$ (i.e negative)

* The product of a positive real number and a negative real number is always a negative real number.".

Quantification as loops $\forall x \exists y$

- $\forall x \exists y = P(x,y)$, we loop through all values of x

For each x, we loop throw the values of y, untill we find y for which $P(x,y)$ is true.

If Some x we hit such a y, then $\forall x \exists y P(x,y)$ is true;

If Some x we never hit such a y, then $\forall x \exists y P(x,y)$ is False.

- $\exists x \forall y P(x,y)$, we loop through values of x until we find an x for which $P(x,y)$ is always true when we loop through all values for y.
  Once we find such an x, we know $\exists x \forall y P(x,y)$ is true.
  If we never hit such an x, then we know that $\exists x \forall y P(x,y)$ is False.
- $\exists x \exists y P(x,y)$, we loop through values of x, where each ~~loop~~ x we loop through the values of y until we hit an x for which we hit a y for which $P(x,y)$ is true.
  $\exists x \exists y P(x,y)$ is False only if we never hit an x for which we hit a y such that $P(x,y)$ is true.

The Order of Quantifiers:

Ex: Let $P(x,y)$ be the statement "$x+y = y+x$". What are the truth values of the quantifications $\forall x \forall y P(x,y)$ and $\forall y \forall x P(x,y)$ where the domain for all variables consists of all real numbers?

Sol: The quantification $\forall x \forall y P(x,y)$ denotes the proposition "For all real nos x, for all real nos y, $x+y = y+x$".
Because $P(x,y)$ is true for all real nos. x and y. (it is the commutative law for addition), the proposition $\forall x \forall y P(x,y)$ is true.
$\forall x \forall y P(x,y)$ and $\forall y \forall x P(x,y)$ have the same meaning, ~~the~~ and both are true.

Note: This illustrates the principle that the order of nested universal quantifier in a statement without the quantifiers can be changed without changing the meaning of the quantified statement.

Ex: Let $Q(x,y)$ denote "$x+y = 0$". What are the truth values of the quantifications $\exists y \exists x Q(x,y)$ and $\forall x \exists y Q(x,y)$, where the domain for all variables consists of all real numbers?

Sol: $\exists y \forall x Q(x,y)$
"There is a real number y such that for every real number x, $Q(x,y)$."
No matter what value of y is chosen, there is only one value of x for which $x+y = 0$.
Because there is no real no y such that $x+y=0$ for all real nos x

$\exists y \forall x\ Q(x,y)$ is False.

$\forall x \exists y\ Q(x,y)$

"For every real no. x there is a real no. y such that $Q(x,y)$".

$x \to y \Rightarrow x+y=0. \Rightarrow y=-x.$

$\forall x \exists y\ Q(x,y)$ is true.

→ $\exists y \forall x\ P(x,y)$ and $\forall x \exists y\ P(x,y)$ are not logically equivalent.

→ If $\exists y \forall x\ P(x,y)$ is True then $\forall x \exists y\ P(x,y)$ is true but if $\forall x \exists y\ P(x,y)$ is True it is not necessary that $\exists y \forall x P(x,y)$ to be true.

Ex: $Q(x,y,z) \Rightarrow$ "$x+y=z$". What are the truth values of the statements $\forall x \forall y \forall z\ Q(x,y,z)$ and $\exists z \forall x \forall y\ Q(x,y,z)$. where the domain of all variables consists of all real numbers?

Sol: Suppose $x, y \to$ Assigned value. $z \to$ real

$x+y=z$

$\forall x \forall y \exists z\ Q(x,y,z)$

For all real nos x, y, there is z such that $x+y=z$ is true".

$\exists x \forall x \forall y\ Q(x,y,z)$ is false because there is no value of z that satisfies the eqn $x+y=z$ for all values of x and y.

For two variables

Statement	When True?	When False?
$\forall x \forall y\ P(x,y)$ $\forall y \forall x\ P(x,y)$	$P(x,y)$ is true for every x, y pair.	There is a pair x, y for which $P(x,y)$ is False.
$\forall x \exists y\ P(x,y)$	For every x there is y for which $P(x,y)$ is true.	There is an x such that $P(x,y)$ is False for every y.
$\exists x \forall y\ P(x,y)$	There is an x for which $P(x,y)$ is true for every y.	For every x there is a y for which $P(x,y)$ is false.
$\exists x \exists y\ P(x,y)$ $\exists y \exists x\ P(x,y)$	There is a pair x, y for which $P(x,y)$ is true.	$P(x,y)$ is false for every pair x, y.

Ex: "The sum of two positive integers is always positive". Translate into a logical expression.

Sol: "For every two integers, if these integers are both positive, then the sum of these integers is positive."

variables x and y:

"For all positive integers x and y, $x+y$ is positive."

$\forall x \forall y ((x>0) \wedge (y>0) \rightarrow (x+y>0))$,

"The sum of two positive integers is always positive"

$\forall x \forall y (x+y>0)$

$x, y \rightarrow$ positive integers.

Ex: "Every real number except zero has a multiplicative inverse". (A multiplicative inverse of a real number x is a real number y such that $xy=1$).

Sol: "For every real number x except zero, x has a multiplicative inverse."

"For every real number x, if $x \neq 0$, then there exists a real number y such that $xy=1$."

$\forall x ((x \neq 0) \rightarrow \exists y (xy=1))$.

Mathematical Statements into Statements

Ex: (Requires Calculus) Use quantifiers to express the defination of the "limit of a real-valued function $f(x)$ of a real variable x at a point a in its domain!"

Sol: $\lim_{x \to a} f(x) = L$. For every real no. $\epsilon > 0$ there exists a real no. $\delta > 0$ such that $|f(x) - L| < \epsilon$ whenever $0 < |x-a| < \delta$.

$\forall \epsilon \exists \delta \forall x (0 < |x-a| < \delta \rightarrow |f(x) - L| < \epsilon)$, where the domain for the variables δ and ϵ consists of all real numbers, rather than just the positive real numbers.

$\forall x > 0 P(x)$ means that for all x with $x > 0$, $P(x)$ is true.

Ex: Translate the statement $\forall x (C(x) \vee \exists y (C(y) \wedge F(x,y)))$ into English where $C(x)$ is "x has a computer", $F(x,y)$ is "x and y are friends," and the domain for both x and y consists of all students in your school.

Sol: every student x in your school., x has a computer or there is a student y such that y has a computer and x and y are friends.

every student in your school has a computer or has a friend who has a computer.

Ex: $\exists x \forall y \forall z ((F(x,y) \wedge F(x,z) \wedge (y \neq z)) \rightarrow \neg F(y,z))$

into English, which F(a,b) means a and b are friends and the domain for x, y and z consists of all students in your school.

Sol: student x such that for all students y and all students z other than y, if x and y are friends and x and z are friends, then y and z are not friends.

Ex: Express statement "If a person is female and is a parent then this person is someone's mother". as logical expression involving predicates, quantifiers with a domain consisting of all people and logical connectivity.

Sol: "For every x person, if person x is female and person x is a parent, then there exists a person y such that person x is mother of person y.

F(x) → x is Female

P(x) → x is parent.

M(x,y) → x is the mother of y

$\forall x (F(x) \wedge P(x)) \longrightarrow \exists y\ M(x,y))$

→ Since y doesnot appear in $F(x) \wedge P(x)$, we can get the logically equivalent expression $\forall x \exists y ((F(x) \wedge P(x)) \rightarrow M(x,y))$.

Ex: Express the statement "Everyone has exactly one best friend" as a logical expression involving predicates, quantifiers with a domain consisting of all people and logical connectives.

Sol: "For every person x, person x has exactly one best friend":

y is best friend of x

z is not the best friend of x

$\exists y (B(x,y) \wedge \forall z ((z \neq y) \longrightarrow \neg B(x,z)))$

$\forall x \exists y ((B(x,y) \wedge \forall z ((z \neq y \longrightarrow \neg B(x,z))) \Rightarrow \forall x \exists! y B(x,y)$

Ex: Use quantifiers to express the statement. "There is a woman who has taken a flight on every airline in the world.".

Sol: $P(w,f)$: "w has taken f"

$Q(f,a)$: "f is a flight on a"

$\exists w \forall a \exists f (P(w,f) \wedge Q(f,a))$. → preferable.

(or)

$\exists w \forall a \exists f \; R(w,f,a)$ → "w has taken f on a".

Ex: Express the negation of the statement $\forall x \exists y (xy = 1)$ so that no negation preceeds a quantifiers.

Sol: $\forall x \exists y (xy = 1)$

$\sim (\forall x \exists y (xy = 1))$

$\exists x \sim [\exists y (xy = 1))$

$\exists x . \forall y (\sim (xy = 1))$

$\exists x . \forall y (xy \neq 1)$

Ex: Use quantifiers to express the statement that "There doesnot exist a woman who has taken a flight on every airline in the world".

Sol: $\sim [\exists w \forall a \exists f (P(w,f) \wedge Q(f,a))]$

Ex: Usee quantifiers and predicates to express the fact that $\lim_{x \to a} f(x)$ doesn't exist where $f(x)$ is a real-valued function of a real variable x and a belong to domain of f.

Sol: $\lim_{x \to a} f(x)$ doesn't exist, means for all real nos. L.

$\lim_{x \to a} f(x) = L$. (definition of limit)

$\sim \forall \epsilon > 0 \; \exists \delta > 0 \; \forall x (0 < |x-a| < \delta \rightarrow |f(x) - L| < \epsilon)$

Rules: (construct this sequence)

$\sim \forall \epsilon > 0, \exists \delta > 0 \; \forall x (0 < |x-a| < \delta \rightarrow |f(x) - L| < \epsilon)$.

$\equiv \exists \epsilon > 0 \; \sim \exists \delta > 0 \; \forall x (0 < |x-a| < \delta \rightarrow |f(x) - L| < \epsilon)$

$\equiv \exists \epsilon > 0 \; \forall \delta > 0 \; \sim \forall x (0 < |x-a| < \delta \rightarrow |f(x) - L| < \epsilon)$

$\equiv \exists \epsilon > 0 \; \forall \delta > 0 \; \exists x \sim (0 < |x-a| < \delta \rightarrow |f(x) - L| < \epsilon)$

DISCRETE MATH

*→ MODULE - 2 :

- When a divides b we say a is factor or divisor of b, and that b is a multiple of a.
- The notation $a|b$ denotes that a divides b
- We write $a \nmid b$ when a doesn't divide b
- floor function (P) → $\lfloor 2.53 \rfloor = 2$, $\lfloor -1.33 \rfloor = -1$ $\{P+1=Q\}$
- Ceiling function (Q) → $(2.53) = 3$, $(-1.33) = 0$

Theorem - 1 : $a|b$ & $a|c$ then $a|(b+c)$

Theorem - 2 : $a|b$ & $a|bc$ then for all integers c-

Theorem -3 : $a|b$ & $b|c$ then $a|c$

*. Let a be an integer & d a positive integer. Then there are unique integers q and r, with IMP $0 \leq r < d$ such that $a = dq + r$

IMP * dividend = divisor * quotient + rem

IMP * a mod d = a-d

dividend mod divisor = remainder

* If a & b are integer & m is positive integer then a is congruent to b module m if m divides a - b

⇒ $a \equiv b \pmod{m}$ to indicate that a is congruent to b module m.

⇒ Example : $1 \equiv 7 \pmod{2}$

* MODULAR ARITHMETIC :

a mod m ⇒ a % m (mod is remainder)

e.g., $-16 \% 3 = 2$, $16 \% 3 = 1$

$a \equiv b \pmod{m} \Rightarrow m \mid (a-b)$

$a \% m = b \% m$

* Theorem - 4 : Let a and b be integers, and let m be positive integer.

Then $a \equiv b \pmod{m}$ if and only if

a mod b = b mod m

* IMP

Example : Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution : $17 \equiv 5 \pmod 6$ TRUE

$24 \not\equiv 14 \pmod 6$ False

*. Theorem - 4 : Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is integer K such that

$a = b + Km$.

Proof : If $a \equiv b \pmod m \iff m \mid (a-b)$

i.e. there is integer K such that $a - b = Km$

so that, $\boxed{a = b + Km}$

Conversely, If integer K such that $a = b + Km$

$a - b = Km \implies m \mid a-b \implies \boxed{a \equiv b \pmod m}$

NOTE : All Congruent $\Rightarrow$ Congruence class of a mod m

16 mod 3 $\quad 3K+1,\ K \in Z$

24 mod 5 $\quad 5K \mp 1,\ K \in Z$

$3K+1$

$3(-1)+1$

$3(-2)+1$

-2 ✓

-5 ✓

-8 ✓

$24 \% 5 = 4$

$5(0)-1$

$5K-1$

Theorem - 5 : $a \equiv b \pmod m$, $c \equiv d \pmod m$ $\Rightarrow$ $a+c = b+d \pmod m$, $ac = bd \pmod m$

Proof : Since $a \equiv b \pmod m$, $c \equiv d \pmod m$

$b = a + sm$, $d = c + tm$ $\Rightarrow$ $b+d = (a+sm) + (c+tm)$

$= (a+c) + m(s+t)$

Example :

If $7 \equiv 2 \pmod 5$

$11 \equiv 1 \pmod 5$

$18 = 7+11 \equiv 2+1 = 3 \pmod 5$

$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod 5$

Theorem : $(a+b) \bmod m = [(a \bmod m) + (b \bmod m)] \bmod m$

Theorem : $(ab) \bmod m = [(a \bmod m)(b \bmod m)] \bmod m$

*IMP

Question : $5 \equiv 16 \pmod 3$

$5 \% 3 = 2$

$16 \% 3 = 1$

$m \mid (a-b)$

$3 \mid (5-16)$

$3 \mid (-11)$

↓ remainder $\neq 0$

Question : $-16 \equiv -5 \pmod 7$

$-16 \% 7 = 5$

$-5 \% 7 = 2$

$-16 \equiv -5 \pmod 7$

$7 \mid (-16+5)$

$7 \mid (-11) \Rightarrow$ remainder $= 3 \neq 0$

Example: Use defination of addition & multiplication in Z_m to find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

$-10 \bmod 26 = 26 - 10 = 16$

$$\left.\begin{aligned} a +_m b &= (a+b) \bmod m \\ a \cdot_m b &= (a \cdot b) \bmod m \end{aligned}\right\} \text{Arthemetic Modulo m} \quad * \text{IMP}$$

$7 +_{11} 9 \Rightarrow (7+9) \bmod 11 = 5$

$7 \cdot_{11} 9 \Rightarrow (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8$

Properties:

1. Closure : $a +_m b$ & $a \cdot_m b \in Z_m$
2. Associative : $(a +_m b) +_m c = a +_m (b +_m c)$ & multi
3. Commutative : $a +_m b = b +_m a$ & multiplication
4. Identity : $a +_m 0 = 0 +_m a = a$ & $a \cdot_m 1 = 1 \cdot_m a = a$
5. Additive inverse : If $a = 0 \in Z_m$ then $m - a$ is an additive inverse of a modulo m & 0 is its own. $a +_m (m-a) = 0$ and $0 +_m 0 = 0$
6. Distributive : $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$

$(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$

* Multiplicative inverse of $3 \bmod 4 \equiv 9 \bmod 4$

$\equiv 3$ is multiplicative inverse

* PRIMES & GREATEST COMMON DIVISORS :

Theorem : Fundamental Theorem of Arithmetic

Any prime number can be factorized unique product of primes.

$100 = 2 \times 2 \times 5 \times 5$

$641 = 641$ prime

$999 = 3 \times 3 \times 3 \times 37$

$1024 = 2^{10}$

Theorem : Consider n is divisible by a, b times

$\Rightarrow n = ab$

$\Rightarrow$ either $a \leq \sqrt{n}$ (or) $b \leq \sqrt{n}$ (To be proved)

but $a > \sqrt{n}$ & $b > \sqrt{n}$

then $ab > \sqrt{n} \cdot \sqrt{n} = n$, which is contradiction

Consequently $a \leq \sqrt{n}$ & $b \leq \sqrt{n}$.

$\therefore$ n is prime number.

* MERSENNE PRIMES:

Which can be written as $2^p - 1$ where p is also prime

example: $2^{2} - 1 = 3$ (2 prime) $\quad 2^{10} - 1 = 1023$ ✗ (10 not prime)

$2^{3} - 1 = 7$ (3 prime) $\quad 2^{5} - 1 = 31$ ✓ (5)

* Theorem: The prime number theorem:

The ratio of no. of primes not exceeding x and x

* Twin Prime Conjecture – pair of primes that differ by 2.

* Greatest Common Divisor:

→ 24, 36

$24 = 2 \times 2 \times 2 \times 3$

$36 = 2 \times 2 \times 3 \times 3$

No common pair ✗ don't consider

Common pairs $2 \times 2 \times 3 = 12$

* When $GCD(a,b) = 1 \Rightarrow$ a & b are relatively prime.

* $gcd(a_i, a_j) = 1$ when $1 \le i < j \le n$ → pair wise relatively prime

$a = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$

$gcd(a,b) = p_1^{\min(a_1 b_1)} \times p_2^{\min(a_2 b_2)} \times p_3^{\min(a_3 b_3)} \cdots$

$120 = 2^3 \times 3^1 \times 5^1$

$500 = 2^2 \times 5^3$

$2^2 \times 3^0 \times 5^1 = \underline{20}$ GCD

$$LCM = P_1^{\max(a_1, b_1)} \times P_2^{\max(a_2, b_2)} \times P_3^{\max(a_3, b_3)} \cdots \times P_n^{\max(a_n, b_n)} \quad *$$

$2^4 \times 3^5 \times 7^2$

$49 \times$

$$a \times b = gcd(a, b) \times Lcm(a, b) \quad *IMP$$

Consider, $24 = 2^3 \times 3^1$

$40 = 2^3 \times 5^1$

$\rightarrow$ $LCM = 2^3 \times 3 \times 5 = 120$

$GCD = 2^3 = 8$

$24 \times 40 = 120 \times 8 \Rightarrow 960 = 960$ (True)

$\therefore$ [product of two numbers = GCD x LCM] *IMP

*. EUCLIDEAN ALGORITHM :

If $a = bq + r$ then $GCD(a, b) = GCD(b, r)$

Here, $a \geq b$ (remember)

$r_{n-1} = r_n q_n$ *. $0 \leq r_n < r_{n-1}$

$GCD(a, b) = r_n$

GCD is last non-zero greatest remainder before last step.

*. Find $GCD(414, 662)$

$a = 662$

$b = 414$ $a > b$

~~GCD~~ In this problem → * divisor = dividend x quotient + remainder

$662 = 414 \cdot 1 + 248$

$414 = 248 \cdot 1 + 166$

$248 = 166 + 82$

$166 = 82 \cdot 2 + (2)$ → this is the GCD.

$82 = 2 \cdot 41 + 0$

remainder < dividend

remember

previous step non-zero remainder.

GCD(115, 250)

~~250 = 115 + + 135~~

~~135 =~~

$250 = 115 \cdot 2 + 20$

$115 = 20 \cdot 5 + 15$

$20 = 15 \cdot 1 + (5)$ → GCD

$15 = 5 \cdot 3 + 0$

GCD = 5 * Answer.

If a, b are integers ⇒ GCD = sa + tb

Bezout's theorem

Ex: (252, 198)

$252 = 198 \cdot 1 + 54$

$198 = 3 \cdot 54 + 36$

$54 = 1 \cdot 36 + (18)$ → GCD

$36 = 2 \cdot 18$

GCD(252, 198) = 18

$18 = 54 - 1 \cdot 36$

$36 = 198 - 3 \cdot 54$

$54 = 252 - 198$

$18 = 54 - 198 + 3 \cdot 54$

$18 = 4(252 - 198) - 198$

$18 = 4(252) - 5(198)$ ⇒

GCD = sa + tb

⇓

Bezout's theorem

GCD (220, 115)

~~220 = 115 · 2 + 0~~

~~115 = 5 · 23~~

$220 = 115 \cdot 1 + 105$

$115 = 105 \cdot 1 + 10$

$105 = 10 \cdot 10 + (5)$ → GCD

$10 = 5 \cdot 2$

→ EUCLUDIAN ALGORITHM

$5 = 105 - 10 \cdot 10$

$= 105 - 10(115 - 105)$

$= 11(105) - 10(115)$

$= 11(220 - 115) - 10(115)$

$5 = 11(220) - 21(115)$

→ BEZOUT'S THEOREM

*. let m be positive integer and let a, b, c integers $\boxed{ac \equiv bc \pmod m}$ $GCD(c, m) = 1$

then $\boxed{a \equiv b \pmod m}$ * IMP

*. CONGRUENCY RELATIONS :

The relation of form $ax \equiv b \pmod m$, So, values of x which solves this equation.

$$ax \equiv b \pmod m$$

$x = ?$ (all possible values)

$a \equiv b \pmod m$

$\boxed{a \cdot \bar{a} \equiv 1 \pmod m}$ $\Rightarrow$ $\bar{a}$ is inverse of a.

$d = gcd(a, m)$ in $ax \equiv b \pmod m$

- If $d \mid b$ (d divides b) then solution exists
- Solve by $\frac{a}{d} x \equiv \frac{b}{d} \pmod m$
- a & m are relatively prime.

observation (if m is small)

By inspection method :

$3 * j$ for $j = \{0, 1, 2, 3, 4, 5, 6\}$

choose j value upto last value of m

$j < m \quad (j \in Z)$

Find inverse of 3 mod 7

$6x \equiv 3 \bmod 9$

IMPORTANT

*. Find solution of $6x \equiv 3 \pmod 9$.

i. $a = 6$, $b = 3$, $m = 9$, $d = 3$

$d = GCD(a, m)$

$= GCD(6, 9) = 3$

$d \mid b \Rightarrow 3 \mid 3 \Rightarrow$ Solution exists

ii. $\frac{a}{d} x \equiv \frac{b}{d} \pmod m$

$\frac{6}{3} x \equiv \frac{3}{3} \pmod 9$

$2x \equiv 1 \pmod 9$

So, $2x \equiv 1 \pmod 9$

Now, choose value of $2 * j$, $j \in Z$, $j < 9$

$2 * j = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$4x \equiv 3 \pmod 2$

$a = 4$

$b = 3$

$m = 2$

$d = GCD(a, m)$

$= GCD(4, 2) = 2$

$d \mid b \Rightarrow 3 \mid 2$ X not possible

no solution

---

*. INVERSE MODULO :

1. GCD must be 1.

Example :

Find inverse of 101 modulo 4620

Sol :

First, we use the Euclidean algorithm,

GCD (101, 4620)

$4620 = 45 \cdot 101 + 75$

$101 = 1 \cdot 75 + 26$

$75 = 2 \cdot 26 + 23$

$26 = 1 \cdot 23 + 3$

$23 = 7 \cdot 3 + 2$

$3 = 1 \cdot 2 + (1) \longrightarrow$ GCD

$2 = 1 \cdot 2$

$\therefore$ GCD (101, 4620) = 1

Then we will reverse the steps to find Bezout' Coefficients a and b such that,

$101a + 4620b = 1$

$4620 = 45 \cdot 101 + 75$ ← From GCD step back tracing

$\Rightarrow 1 = 3 - 1 \cdot 2$

$= 3 - 1(23 - 7 \cdot 3)$

$= 3 - 23 + 7 \cdot (3) = 8(3) - 23$

$= 8(26 - 23) - 23 = 8(26) - 9(23)$

$= 8(26) - 9(75 - 2 \cdot 26)$

$= 8(26) - 9(75) + 18(26) = 26(26) - 9(75)$

$= 26(101 - 75) - 9(75) = 26(101) - 35(75)$

$= 26(101) - 35(4620 - 45 \cdot 101)$

$= 26(101) - 35(4620) + 1575(101)$

$= 101(1601) + 4620(-35)$

~~1 = 1601 x 4620 + (-35)(101)~~

We obtained

$$1 = 1601\,(101) + (-35)(4620)$$

This tells us that -35 and 1601 are Bezout coefficients of 4620 and 101, and 1601 is inverse of 101 module 4620

Suppose Consider a case,

$$1601 \times 4620 - 35 \times 101 = 1$$

$$\frac{1601 \times 4620}{4620} - \frac{35 \times 101}{4620} = \frac{1}{4620} \quad \text{(remainder)}$$

Hypothetical Situation

$$0 - (4620 - 35) = 1$$

↓

answer inverse of 101

4585 is inverse of 101.

5/11

4620 TO

35

4585

---

*. Given $3x \equiv 4 \pmod 7$

$a = 3$

$b = 4$

$m = 7$

$d = 1$

$d = GCD(a, m)$

$= GCD(3, 7) = 1$

$$\boxed{a\,x \equiv b \pmod m}$$

Since GCD = 1 $\Rightarrow$ $\bar{3}^1 . 3 . x \equiv \bar{3}^1 . 4 \pmod 7$

We got

$$1 = 1601\,(101) + (-35)\,(4620)$$

Applying modulo 4620 both sides,

$$1 \,\%\, 4620 = [1601\,(101)] \,\%\, 4620 + [(-35)(4620)] \,\%\, 4620$$

$1 \,\%\, 4620$: remainder = 1

$[1601\,(101)] \,\%\, 4620$: remainder = ?

$[(-35)(4620)] \,\%\, 4620$: remainder = 0, exactly divisible

$$(1601 \times 101) \,\%\, 4620 = 1$$

When you are dividing by 4620 & you are getting remainder = 1 $\Rightarrow$ both the numbers are multiplicative inverse of each other

$\therefore$ inverse of 101 mod 4620 = 1601

For hypothetical example

$$1 = 1601\,(4620) + (-35)\,(101)$$

Applying modulo 4620,

$$1 \,\%\, 4620 = [1601\,(4620)] \,\%\, 4620 + (-35)\,(101) \,\%\, 4620$$

$$\Rightarrow 1 = (101)\,(-35) \,\%\, 4620$$

$\Rightarrow$ remainder = 1 $\Rightarrow$ 101 & 4620 % (-35) are multiplicative inverse of each other

For hypothetical example,

$$1 = 1601\,(4620) + (-35)(101)$$

$$1 \,\%\, 4620 = 0 + [101\,(-35)] \,\%\, 4620$$

$1 \,\%\, 4620$ → remainder = 1

0 → remainder = 0, exactly divisible

$[101\,(-35)] \,\%\, 4620$ → remainder = ?

$$1 = 101\,(-35) \,\%\, 4620$$

Here, since -35 is negative number, 101 and $(-35) \,\%\, 4620$ are multiplicative inverse of each other under 4620 modulo world.

So, multiplicative inverse of $101 \,\%\, 4620$

$$= (-35) \,\%\, 4620$$

$$= 4620 - 35$$

$$= 4585$$

↓

multiplicative inverse of 101 under modulo 4620

Example : inverse of 3 mod 7

$7 = 3 \cdot 2 + 1$ → GCD

$2 = 1 \cdot 2$

$1 = 7 - 3(2)$

$1 = 7(1) + (-2)(3)$

$1 = 7a + 3b$ $\quad a, b \rightarrow$ Bezout' coefficients

$1 = 7(1) + (-2)(3)$

$1 \% 7 = 7 \% 7 + 3(-2) \% 7$

$1 = 0 + 3(-2) \% 7$

$3(-2) \% 7 = 1$

⇒ 3, -2 are multiplicative inverse of each other in modular 7 world

So, multiplicative inverse of 3 mod 7 = $-2 \% 7$

$-2 \% 7 = (7-2) \% 7 = 5 \% 7 = \underline{5}$

∴ Multiplicative inverse of 3 mod 7 = 5

$$\boxed{-a \bmod m = (m-a) \bmod m}$$ * IMP

Example: What are solutions of linear Congruence

$$3x \equiv 4 \pmod 7 \quad ?$$

5 is inverse of 3 modulo 7.

Multiplying both sides of Congruency by 5 shows that

$$5 \times 3x \equiv 5 \cdot 4 \pmod 7$$

$$15 \equiv 1 \pmod 7$$

$$20 \equiv 6 \pmod 7$$

} from this equation

We need to determine whether every x with

$x \equiv 6 \pmod 7$ is solution.

So, general solution, $\boxed{x = 6 + 7m}$, $m \in \mathbb{Z}$

~~(inverse × b) mod m~~

$$3x \equiv 4 \pmod 7$$

$$5 \cdot 3x = 5 \cdot 4 \pmod 7$$

$$15x = 20 \pmod 7$$

$$15x \,\%\, 7 = (20 \,\%\, 7) \pmod 7$$

remainder ↓ remainder

$$1x = 6 \pmod 7$$

$$x \equiv 6 \pmod 7$$

(Ans) $\boxed{x = 6 + 7m, \; m \in \mathbb{Z}}$ * imp

*. THE CHINESE REMAINDER THEOREM :

Example :

When divided by 3, the remainder is 2, when divided by 5, the remainder is 3, and when divided by 7, the remainder is 2. What will be the no. of things ?

let the no. divided is x,

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 5$$

$$x \equiv 2 \pmod 7$$

→ Pair wise relatively prime, unique solution

Method to solve System of linear Congruencies :

Theorem 2 :

Let $m_1, m_2, m_3, \ldots m_n$ be pairwise relatively prime greater than one and $a_1, a_2, \ldots a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_n \pmod{m_n}$$

has unique solution module $m = m_1 \cdot m_2 \cdots m_n$

i.e. (There is solution x with $0 \leq x < m$, and all other solutions are congruent module m to solution.)

① $M_K = \frac{m}{m_K}$ for $\forall\ K = 1, 2, \ldots n$

& $m = m_1 \cdot m_2 \cdot m_3 \ldots m_n$

$GCD(m_K, M_K) = 1$

② Find y_K such that $M_K y_K \equiv 1 \pmod{m_K}$

i.e. y_K is inverse of module m_K such that

③ Find inverse of M_K under module m_K $\forall\ K \in I$

④ solution, $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n$

$a_K \rightarrow$ from given relations, $K \in \{1, 2, 3, \ldots n\}$

$M_K \rightarrow \frac{m}{m_K} = \frac{m_1 \cdot m_2 \cdot m_3 \cdot m_4 \ldots m_n}{m_K}$, $K \in N$

$y_K \rightarrow$ inverse of M_K under module m_K, $K \in N$

⑤ Final result, $\boxed{x \equiv a_K \pmod{m_K}}$ $\forall\ K \in N$

$\boxed{x = \left(\sum_{K=1}^{n} a_K M_K y_K\right) \bmod m}$ ∴ * IMP

Example : (previous)

$x \equiv 2 \pmod 3$, $m_1 = 3$

$x \equiv 3 \pmod 5$, $m_2 = 5$

$x \equiv 2 \pmod 7$, $m_3 = 2$

check 3, 5, 7 pair wise relatively prime. ✓

$m = 3 \times 5 \times 7 = 105$

$a_1 = 2$, $a_2 = 3$, $a_3 = 2$

$M_1 = \frac{m}{m_1}$ $\quad M_2 = \frac{m}{m_2}$ $\quad M_3 = \frac{m}{m_3}$

$M_1 = \frac{105}{3} = 35$ $\quad a_1 = 2$

$M_2 = \frac{105}{5} = 21$ $\quad a_2 = 3$

$M_3 = \frac{105}{7} = 15$ $\quad a_3 = 2$

$y_1 = ? \Rightarrow \quad M_1 y_1 \equiv 1 \pmod{m_1}$

$35 \times y_1 \equiv 1 \pmod 3$

$35 y_1 \equiv 1 \pmod 3$

So, $\boxed{x = \left(\sum_{k=1}^{n} a_k M_k y_k \right) \pmod m}$

$m = 105$	a_k	M_k	y_k	$a_k M_k y_k$
$k=1$	2	35	2	140
$k=2$	3	21	1	63
$k=3$	2	15	1	30

$35 y_1 \equiv 1 \pmod 3$

$\boxed{y_1 = 2}$

$M_2 y_2 \equiv 1 \pmod{m_2}$

$21 y_2 \equiv 1 \pmod 5$

$\boxed{y_2 = 1}$

$M_3 y_3 \equiv 1 \pmod{m_3}$

$15 y_3 \equiv 1 \pmod 7$

$\boxed{y_3 = 1}$

$y_1 = 2$
$y_2 = 1$
$y_3 = 1$

$$x = \left(\sum_{k=1}^{3} a_k M_k y_k \right) \pmod{m}$$

$$= (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3) \pmod{m}$$

$$= (140 + 63 + 30) \pmod{105}$$

$$= 233 \bmod 105$$

~~$x = 20$~~ $\quad\quad$ $\boxed{x = 23}$

∴ The no. of things = 23

---

* $x \equiv 1 \pmod 2$

$x \equiv 2 \pmod 5$

$x \equiv 5 \pmod 7$

$M_1 = \frac{2 \times 5 \times 7}{2} = 35$

$M_2 = \frac{2 \times 5 \times 7}{5} = 14$

$M_3 = \frac{2 \times 5 \times 7}{7} = 10$

$10\, y_2 \equiv 1 \pmod 7$

$\boxed{y_2 = 5}$

10

$35\, y_1 \equiv 1 \pmod 2$

$\boxed{y_1 = 1}$

$14\, y_2 \equiv 1 \pmod 5$

$\boxed{y_2 = 4}$

$= \overset{a_1\ M_1\ y_1}{(1 \times 35 \times 1)} + \overset{a_2\ M_2\ y_2}{(2 \times 14 \times 4)} + \overset{a_3\ M_3\ y_3}{(5 \times 10 \times 5)}$

$= 35 + 112 + 250$

$= 397 \bmod 70 = \underline{47}$

*. BACK SUBSTITUTION METHOD : (CRT)

$x \equiv 1 \pmod 5$ — (1) $\Rightarrow$ $5t + 1 = x$

$x \equiv 2 \pmod 6$ — (2)

$x \equiv 3 \pmod 7$ — (3)

Put $5t+1 = x$ in (2)

$x \equiv b \pmod m$

$\boxed{mq + b = x}$

$5t + 1 \equiv 2 \pmod 6$

~~$5t \equiv 1 \pmod 6$~~ $\Rightarrow$ $\boxed{t = 5}$

~~$x = 5(5) + 1 = 26$~~ $\Rightarrow$ $\boxed{x = 26}$

---

*. FERMAT'S LITTLE THEOREM :

If p is prime and a is integer not divisible by p, then

$$\boxed{a^{p-1} \equiv 1 \pmod p}$$

$\gcd(a, p) = 1$

Example : What is remainder when 2^{237} is divided by 5.

Since 5 is prime, 5 doesn't divide 2,

$GCD(2, 5) = 1$

From fermat's $2^{5-1} \equiv 1 \pmod 5$

$7^{222} \bmod 11 = ?$

From fermat's theorem,

$$7^{11-1} \equiv 1 \pmod{11}$$

$$7^{10} \equiv 1 \pmod{11}$$

$$7^{22 \times 10 + 2} \bmod 11$$

$$(7^{10})^{22} \cdot 49 \bmod 11$$

$7^2 \bmod 11 \Rightarrow 49 \bmod 11 = 5$

CRYPTOGRAPHY

- Number theory plays key role in Cryptography.

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9

K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z
20	21	22	23	24	25

In the set of Z_{26} elements — alphabets A to Z from 0 to 25

↓

Z_{26} mod 26

Example : CAESAR CIPHER

M E E T	YOU	IN	THE	PARK
12 4 4 19	24 14 20	8 13	19 7 4	15 0 17 10

Add +3 mod 26 → convert back to digits ...

(12+3) mod 26 = 15 → P

(4+3) mod 26 = 7 → H, H

(19+3) mod 26 = 22 → W

(24+3) mod 26 = 27 mod 26 = 1 → B

(14+3) mod 26 = 17 → R

(20+3) mod 26 = 23 → X

(8+3) mod 26 = 11 → L

(13+3) mod 26 = 16 → Q

(19+3) mod 26 = 19 → W

(7+3) mod 26 = 10 → K

(4+3) mod 26 = 7 → H

(15+3) mod 26 = 18 → S

(0+3) mod 26 = 3 → D

(17+3) mod 26 = 20 → U

(10+3) mod 26 = 13 → N

$$f(p) = (p+3) \bmod 26$$ → ENCRYPTION

$$f^{-1}(p) = (p-3) \bmod 26$$ → DECRYPTION

MEET YOU IN THE PARK is encrypted as

PHHW BRX LQ WKH SDUN

*. GENERALIZATION :

$f(p) = (p+k) \bmod 26$ → ENCRYPTION

K is shifted.

K is key

$f^{-1}(p) = (p-k) \bmod 26$ → DECRYPTION

*. Example :

STOP GLOBAL WARMING

Shift = K

$18 \rightarrow 29 \bmod 26 = 3 \sim D$

$19 \rightarrow 30 \bmod 26 = 4 \sim E$

$14 \rightarrow 25 \bmod 26 = 25 \sim Z$

$15 \rightarrow 26 \bmod 26 = 0 \sim A$

$6 \rightarrow 17 \bmod 26 = 17 \sim R$

$22 \rightarrow 22 \bmod 26 = 22 \sim W$

$f(p) = (p+k) \bmod 26$

↓

For encrypting

$6 \rightarrow 17 \bmod 26 = 17 \sim R$

Decrypt : L E W L Y P L U J L P Z H N Y

L H A A L H J O L Y

Shift = k = 7

*- AFFINE CIPHER :

$$f(p) = (ap + b) \bmod 26$$

where a, b are integers, choosen so that f is bijection.

Note: The function $f(p) = (ap + b) \bmod 26$ is bijection if and only if $\gcd(a, 26) = 1$

Such a mapping is called Affine Transformation.

Ex: What letter replaces the letter K when the function $f(p) = (7p + 3) \bmod 26$ is used for encryp

Sol: Note that 10 represents K.

$$f(10) = (7 * 10 + 3) \bmod 26 = 21$$

Because 21 represents V, K is replaced by V in encrypted message.

$f = (7p+3)$

Message : M E E T Y O U I N T H E P A R K

M = 12	U = 20	P = 15
E = 4	I = 8	A = 0
E = 4	N = 13	R = 17
T = 19	T = 19	K = 10
Y = 24	H = 7	
O = 14	E = 4	

M → $7 \times 12 + 3 = 87 \bmod 26 = 9 = J$

E → $7 \times 4 + 3 = 31 \bmod 26 = 5 = F$

E → $7 \times 4 + 3 = 31 \bmod 26 = 5 = F$

T → $7 \times 19 + 3 = 136 \bmod 26 = 6 = G$

Y → $7 \times 24 + 3 = 171 \bmod 26 = 15 = P$

O → $7 \times 14 + 3 = 101 \bmod 26 = 23 = X$

U → $7 \times 20 + 3 = 143 \bmod 26 = 13 = N$

I → $7 \times 8 + 3 = 59 \bmod 26 = 7 = H$

N → $7 \times 13 + 3 = 94 \bmod 26 = 16 = Q$

T → $19 \times 7 + 3 = 136 \bmod 26 = 6 = G$

H → $7 \times 7 + 3 = 52 \bmod 26 = 0 = A$

E → $7 \times 4 + 3 = 31 \bmod 26 = 5 = F$

P → $7 \times 15 + 3 = 108 \bmod 26 = 4 = E$

A → $7 \times 0 + 3 = 3 \bmod 26 = 3 = D$

R → $7 \times 17 + 3 = 122 \bmod 26 = 18 = S$

K → $7 \times 10 + 3 = 73 \bmod 26 = 21 = V$

*. BLOCK CIPHERS :

Text : MEET YOU IN THE PARK

Make according to block value

block value : $\{1, 2, 3, 4\} \sim 4(\text{block})$

MEET YOUI NTHE PARK

4 (block) 4 (block) 4 4 (block)

*. TRANSPOSITION CIPHER :

1. Split it into block of size m
2. We encrypt block $P_1 P_2 \ldots P_m$

Example :

Permutation set $\sigma = \{1, 2, 3, 4\}$

a. Encrypt plaintext message PIRATE ATTACK.

PIRA | TEAT | TACK (make block of 4 letters)

- Split it into block of size $m = 4$
- To encrypt each block, we send the first letter to the third position, the second letter to the first position. third position to fourth position.

1st → 3rd
2nd → 1st
3rd → 4th
4th → 2nd

letters (2, 4, 1, 3) Encrypted
this will look in this order after

(3, 1, 4, 2) Decrypted
looks like this order after

PIRA | TEAT | TACK
IAPR | ETTA | AKTC → Encrypted

b. Decrypt - SWUE TRAE OEHS

SWUE | TRAE | OEHS
USEW | ATER | HOSE → Decrypted

USE WATER HOSE (analyse randomly)

* INTRODUCTION TO COUNTING :

→ Used in password security

→ Telephone Number, Internal protocal

→ Sequencing of DNA.

→ Permutations, Combinations, Probability.

* PRODUCT RULE :

n_1 → ways to do first task (AND)

n_2 → ways to do Second task ⟹ DEPENDENT

$n_1 \times n_2$ → ways to complete task

* Binary Strings :

$B = \{0, 1\}$

$|B|^n = 2^n$ (possibility cases)

* SUM RULE :

n_1 → ways to first task (OR)

n_2 → ways to Second task ⟹ INDEPENDENT

$n_1 + n_2$ → ways to complete

* $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3|$

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

* $|A - B| = A \cap \overline{B}$

* $|A - B| = A - (A \cap B) = (A \cup B) - B$

*. $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

*. Subtraction Rule : (Inclusion – Exclusion for Two Sets)

→ Count the total no. of distinct element in Cardinality of set.

→ Used when two sets are not distinct.

Ex : How many bit strings of length eight either start with 1 bit or end with two bits 00 ?

1 _ _ _ _ _ _ _ → total possible 2^7

_ _ _ _ _ _ 0 0 → total possible = 2^6

1 _ _ _ _ _ 0 0 → total possible = 2^5

(1 bit start) or (two bit 00 end) =

= (1 bit start) + (two bit 00 end) – (1 bit start & 00 end)

= $2^7 + 2^6 - 2^5$

= $2^7 + 2^6 - 2^5 = 2^5(4 + 2 - 1) = 5 \cdot 2^5$

*. PIGEONHOLE PRINCIPLE : (Think for worst case)

- If n pigeons are placed in (n-1) pigeon holes than there exists atleast one 1 pigeon hole with at least two pigeons in it. (more than 1 pigeon)

- Conclusion : 1. No. of pigeons > No. holes

2. Atleast one hole with more than 1 pigeon.

In terms of Mathematics,

→ If K is positive integer and K+1 or more objects then apply PIGEON HOLE PRINCIPLE.

Corollary: A function f from a set with K+1 or more elements to a set with K elements is not one-to-one.

Applications:

① Total persons = 366. (Given)

Atleast 2 persons will share same birth day.

Total days in year = 365

② Total characters in string = 27 (Given)

Atleast one letter repeats twice.

No. of alphabets = 26.

n pigeon holes = (n+1) pigeon

$n > m$

n-objects ⇒ $n, m \in N$ (finite & arbitrary)

m-containers

Atleast one of the m containders will contain K+1 or more of the n objects (at least as many)

$$\boxed{K+1 = \left\lceil \frac{n}{m} \right\rceil}$$

$$\lceil x \rceil = \min_{n \in Z} \{ n \geq x \}$$

* COUNTING :

$$nP_r = \frac{n!}{(n-r)!} \qquad nC_r = \frac{n!}{(n-r)!\, r!}$$

$$C(n+r-1, r) = C(n+r-1, n-r) = \frac{(n+r-1)!}{r!\,(n-1)!}$$

r - combinations from set with n elements when repetition of elements is allowed.

$$\frac{(6+4-1)!}{4!\,(5!)} = \frac{9 \times \overset{2}{8} \times 7 \times \cancel{6}}{4 \times \cancel{3} \times 2}$$

$$\begin{array}{r} 18 \\ \times 7 \\ \hline 126 \end{array}$$

* SOLVING LINEAR HOMOGENEOUS RECURRENCE RELATION :

Theorem : Suppose $r^2 - c_1 r - c_2 = 0$ has two distinct roots r_1, r_2. Then sequence of solution

$a_n = c_1 a_{n-1} + c_2 a_{n-2}$ if and only if

$$\boxed{a_n = \alpha_1 r_1^n + \alpha_2 r_2^n} \qquad \forall \; n = 0, 1, 2 \ldots$$

α is constant

Example : What is the solution of

$a_n = a_{n-1} + 2a_{n-2}$ with $a_0 = 2$, $a_1 = 7$

The characteristic equation is $r^2 - r - 2 = 0$

If roots are, $r = 2$, $r = -1$

$$a_n = \alpha_1 2^n + \alpha_2 (-1)^n$$

To find α_1, α_2 $\quad a_0 = 2, \; a_1 = 7$

$$a_n = \alpha_1 2^n + \alpha_2 (-1)^n$$

$$a_0 = \alpha_1 (1) + \alpha_2 (1) = 2$$

$$\alpha_1 + \alpha_2 = 2 \quad \text{--(1)}$$

$$a_1 = \alpha_1 (2)^1 + \alpha_2 (-1)^1 = 7$$

$$7 = 2\alpha_1 - \alpha_2 \quad \text{--(2)}$$

$\Rightarrow$ $\boxed{\alpha_1 = 3}$ $\quad$ $\boxed{\alpha_2 = -1}$

with $a_n = 3 \cdot 2^n - (-1)^n$ is solution.

---

* Fibonacci Recurrence Relation :

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2}$$

$r^2 - r - 1 = 0 \longrightarrow$ characteristic eq

$$r = \frac{+1 \pm \sqrt{1 - 4(-1)}}{2} = \frac{+1 \pm \sqrt{5}}{2} = \cancel{1 \pm (0.1) \; 2}$$

~~$a_n = \alpha_1 (1)^n + \alpha_2 (-2)^n$~~

~~$a_n = \alpha_1 + \alpha_2 (-2)^n$~~

~~$a_0 = \alpha_1 + \alpha_2 = 0 \Rightarrow \alpha_1 = -\alpha_2$~~

~~$a_1 = \alpha_1 - 2\alpha_2 = 1 \Rightarrow -\alpha_2 - 2\alpha_2 = 1$~~

~~$-3\alpha_2 = 1$~~

$\alpha_1 = \frac{1}{3}$ $\quad$ $\alpha_2 = -\frac{1}{3}$

$a_n = \frac{1}{3}(1)^n + \left(-\frac{1}{3}\right)(-3)^n$

$$\boxed{f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n}$$ * Solution of recurrence relation

---

*. Theorem 2 :

$$a_n = \alpha r_0^n + \alpha_2 n r_0^n = (\alpha_1 + n\alpha_2) r_0^n$$

Case for repeated roots of recursive relation.

Ex : $a_n = 6a_{n-1} - 9a_{n-2}$, $a_0 = 1$ $a_1 = 6$

$$r^2 - 6r + 9 = 0$$

$$r^2 - 3r - 3r + 9 = 0$$

$$(r-3)(r-3) = 0 \Rightarrow r = 3, 3$$

$$a_n = (\alpha_1 + n\alpha_2) 3^n \quad , \quad a_0 = 1 \quad a_1 = 6$$

$$a_0 = \alpha_1 3^0 = \boxed{\alpha_1 = 1}$$

$$a_1 = (\alpha_1 + n\alpha_2) 3 = 6$$

$$6 = 3 + 3n\alpha_2$$

$$3 = 3n\alpha_2 \Rightarrow 3(1)\alpha_2 = 3 \Rightarrow \boxed{\alpha_2 = 1}$$

$$a_n = \alpha_1 r_0^n + \alpha_2 n \cdot r_0^n$$

$$= 1 \cdot 3^n + 1 \cdot n \cdot 3^n = \underline{(n+1)3^n}$$

* GENERATING FUNCTION :

Generating function is sequence $a_0, a_1, \ldots a_k$ upto infinity

$$G(x) = a_0 + a_1 x + \ldots + a_k x^k$$

$$= \sum_{k=0}^{\infty} a_k x^k$$

Example : The sequence $\{a_k\}$ with $a_k = 3$ has generating function,

$$G(x) = 3 + 3x + 3x^2 + \ldots + 3x^k$$

$$= \sum_{k=0}^{\infty} 3 \cdot x^k$$

(IMP)

Example : let m be positive integer. let $a_k = C(m, k)$ for $k = 0, 1, 2 \ldots m$ what is the generating function of sequence $a_0, a_1 \ldots a_m$?

Solution

$$G(x) = C(m,0) + C(m,1)x + C(m,2)x^2 + \ldots + C(m,m)x^m$$

The binomial theorem shows =

$$mC_0 + mC_1 x + mC_2 x^2 + \ldots + mC_m x^m$$

$$= (1+x)^m$$

*. Questions about the convergens of these series are ignored.

Example : $f(x) = \frac{1}{1-x}$ is generating function of sequence $1, 1, 1, \ldots$ because

$$\frac{1}{1-x} = 1 + x + x^2 + \ldots \quad \text{for } |x| < 1$$

Example : $f(x) = \frac{1}{1-ax}$ is generating function of sequence $1, a, a^2, a^3 \ldots a^n \ldots \quad |ax| < 1$

Because $\frac{1}{1-ax} = 1 + ax + a^2x^2 + a^3x^3 + \ldots \quad |ax| < 1$

*. PROPERTIES :

Let $f(x) = \sum_{k=0}^{\infty} a_k x^k$ and $g(x) = \sum_{k=0}^{\infty} b_k x^k$ then

- $f(x) + g(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k$ and
- $f(x) - g(x) = \sum_{k=0}^{\infty} \left[\sum_{j=0}^{k} a_j b_{k-j} \right] x^k$

Example : Let $f(x) = \frac{1}{(1-x)^2}$. Find coefficient $a_0, a_1, a_2 \ldots$ in expansion $f(x) = \sum_{k=0}^{\infty} a_k x^k$

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \ldots .$$

Hence, $\frac{1}{(1-x)^2} = \frac{1}{(1-x)} \cdot \frac{1}{(1-x)} =$ product of $f(x)\, g(x)$

$$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} 1 \right) x^k = \sum_{k=0}^{\infty} (k+1)\, x^k$$

*. $$\binom{u}{k} = \begin{cases} \dfrac{u(u-1)\ldots(u-(k-1))}{k!} & \text{if } k > 0 \\ 1 & \text{if } k = 0 \end{cases}$$

(take upto $(u-k+1)$ only)

↑ Extended binomial Coefficient,

IMP

*. Find $-2C_3$ and $\frac{1}{2}C_3$

Sol: Taking $u = -2$ & $k = 3$

$$\binom{-2}{3} = \frac{(-2)(-3)(-4)}{3!} = -4$$

(take upto $(u-k+1)$ only)

Similarly taking $u = 1/2$ $k = 3$ gives us,

$$\binom{\frac{1}{2}}{3} = \frac{\left(\frac{1}{2}\right)\left(\frac{1}{2}-1\right)\left(\frac{1}{2}-2\right)}{3!} = \frac{1}{16}$$

$$\binom{-n}{r} = (-1)^r \, C(n+r-1, r)$$

$$-nC_r = (-1)^r \, {}^{(n+r-1)}C_r$$

n = negative integer

r = positive

$$(1+x)^u = \sum_{k=0}^{\infty} \binom{u}{k} x^k$$ *IMP

Extended Binomial theorem, for all $u \in R$

$$(1+x)^{-n} = \sum_{k=0}^{\infty} \binom{-n}{k} x^k$$

Generating function of $(1+x)^{-n}$

$$(1+x)^{-n} = \sum_{k=0}^{\infty} (-1)^k C(n+k-1, k) x^k$$ *IMP

GF of $1-x$

$$(1-x)^{-n} = \sum_{k=0}^{\infty} C(n+k-1, k) x^k$$ *IMP

→ Generating Functions formulaes are saved in laptop.

*IMP
Find the no. of solutions $e_1 + e_2 + e_3 = 17$

for $2 \le e_1 \le 5$, $3 \le e_2 \le 6$ & $4 \le e_3 \le 7$

Sol:

$2 \le e_1 \le 5 \rightarrow (x^2 + x^3 + x^4 + x^5)$

$3 \le e_2 \le 6 \rightarrow (x^3 + x^4 + x^5 + x^6)$

$4 \le e_3 \le 7 \rightarrow (x^4 + x^5 + x^6 + x^7)$

$x^{17} \rightarrow (x^2 + x^3 + x^4)(x^3 + x^4 + x^5 + x^6)(x^4 + x^5 + x^6 + x^7)$

This follows because we obtain term equal to x^{17} in product by picking a term in first sum x^{e_1}

second sum x^{e_2}

third sum x^{e_3}

where, e_1, e_2, e_3 are exponents satisfy

$e_1 + e_2 + e_3 = 17$.

$$(x^2 + x^3 + x^4 + x^5)(x^3 + x^4 + x^5 + x^6)(x^4 + x^5 + x^6 + x^7)$$

	x^4	x^6	x^7
	x^5	x^5	x^7
	x^5	x^6	x^6

---

*- Some useful Identities :

$G(x)$	a_k
$(1+x)^n = \sum_{k=0}^{n} C(n,k)\, x^k$ $= 1 + C(n,1)x + C(n,2)x^2 + \dots + x^n$	${}^nC_k$
$(1+ax)^n = \sum_{k=0}^{n} C(n,k)\, a^k x^k$	$C(n,k)\, a^k$
$(1+x^r)^n = \sum_{k=0}^{n} C(n,k)\, x^{rk}$	$C(n, k/r)$ if $r \mid k$ 0 otherwise
$\frac{1-x^{n+1}}{1-x} = \sum_{k=0}^{n} x^k$	1 if $k \le n$ 0 otherwise
$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k$	1
$\frac{1}{1-ax} = \sum_{k=0}^{\infty} a^k x^k$	a^k

$\frac{1}{1-x^r} = \sum_{k=0}^{\infty} x^{rk}$	$1 \begin{cases} \text{if } r \mid k \\ 0 \end{cases}$ otherwise
$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1)\, x^k$	$k+1$
$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} C(n+k-1, k)\, x^k$	$= C(n+k-1, k)$ $= C(n+k-1, n-1)$
$\frac{1}{(1+x)^n} = \sum_{k=0}^{\infty} C(n+k-1, k)(-1)^k x^k$	$= (-1)^k C(n+k-1, k)$ $= (-1)^k C(n+k-1, n-1)$
$\frac{1}{(1-ax)^n} = \sum_{k=0}^{\infty} C(n+k-1, k)\, a^k x^k$	$= C(n+k-1, k)\, a^k$ = $= C(n+k-1, n-1)\, a^k$
$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$	$\frac{1}{k!}$
$\ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k$	$(-1)^{k+1} / k$

Note : The series the last two generating functions can be found in most books when power series are discus

*. COUNTING PROBLEMS & GENERATING FUNCTIONS :

$$e_1 + e_2 + \cdots + e_n = C$$

where C is constant & each e_i a non negative integer that may be subject to a specified constraint.

Ex : Determine the coefficient of x^{15} in

$$f(x) = (x^2 + x^3 + x^4 + \dots)^4$$

$$f(x) = (x^2 + x^3 + x^4 + \dots)^4 = [x^2(1 + x + x^2 + \dots)]^4$$

$$= \left[\frac{x^2}{1-x}\right]^4 = \frac{x^8}{(1-x)^4}$$

Hence the solution is coefficient of x^7 in $(1-x)^{-4}$

which is $x^7 \rightarrow k = 7$

$$\frac{1}{(1-x)^n} \rightarrow a_k = C(n+k-1, k)$$

$$\frac{1}{(1-x)^4} \rightarrow a_k = C(4+7-1, 7) = C(10,7)$$

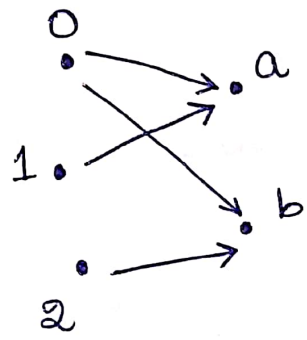
* - Find the no. of ways to select R balls from a pile of 2 red, 2 green, 2 blue balls.

$$x^{e_1} x^{e_2} x^{e_3} \qquad e_1 + e_2 + e_3 = R$$

RELATIONS

Let $A = \{0,1,2\}$ and $B = \{a,b\}$. Then $\{(0,a), (0,b), (1,a), (2,b)\}$ is relation from A to B.

This means that $0 R A$, but $1 \not R B$. Relations can be represented graphically, as shown in Figure, using arrows to represent ordered pairs.

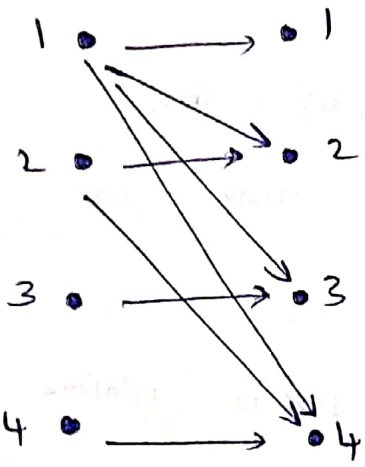


R	a	b
0	X	X
1	X	
2		X

* Example: Let $A = \{1,2,3,4\}$. Which ordered pair are in relation $R = \{(a,b) \mid a \text{ divides } b\}$?

Solution: Because R is relation of a divides b where (a,b) in R & $a,b \in \mathbb{Z}^+$ not exceeding 4 such that a divides b,

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



R	1	2	3	4
1	X	X	X	X
2		X		X
3				X
4			X	X

* - How many relations are there on set with n elements

A has n elements, A X A has n^2 elements

Set with n elements has 2^n subsets

There are 2^{n^2} subsets of A X A. Thus, there are 2^{n^2} relations on set with n elements. For example, there are $2^{3^2} = 2^9 = 512$ relations on $\{a, b, c\}$

Transitive → If (a,b) and (b,c) then (a,c) must

Reflexive → (a,a) or (b,b) or (c,c) must

Symmetric → If (a,b) then (b,a) must

Anti Symmetric → If (a,b) & (b,a) then a = b

No. of Reflexive relations = $2^{n(n-1)}$, n is no. of el in a set

Equivalence → Reflexive, Symmetric, Transitive

Partial order set POSET → Reflexive Anti Symmetric, Transitive

* Let $A = \{1, 2, 3\}$ and $B = \{1, 2, 3, 4\}$. The relations

$R_1 = \{(1,1), (2,2), (3,3)\}$ and

$R_2 = \{(1,1), (1,2), (1,3), (1,4)\}$ then

$R_1 \cup R_2 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (3,3)\}$

$R_1 \cap R_2 = \{(1,1)\}$

$R_1 - R_2 = \{(2,2), (3,3)\}$

$R_2 - R_1 = \{(1,2), (1,3), (1,4)\}$

divisibility → Reflexive, Transitive, anti-symmetric

lessthan → Transitive, anti-symmetric

Greater than → Transitive, anti symmetric

Congruence → Equivalence

Power set : $(R)^n \subseteq R$, R is a set

*. PARTIAL ORDER RELATION :

- POR → reflexive, antisymmetric, transitive.
- POSET → A set S with POR.
- Greater than or equal to & less than or equal to are best examples of "POSET".

IMP ⊙ When two elements in set are called "TOTAL ORDERING" (TOR) – TOR is also called LOR (linearly ordered set)

Ex ⊙ The partial order relation of theorem is called Lexicographic order of S.

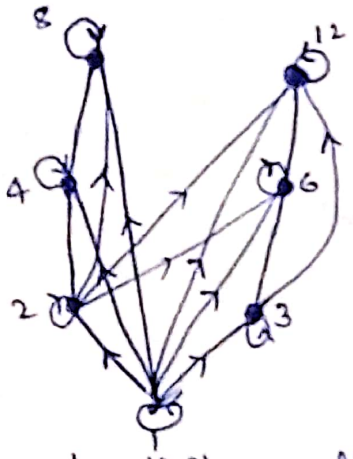
(DICTIONARY ORDER)

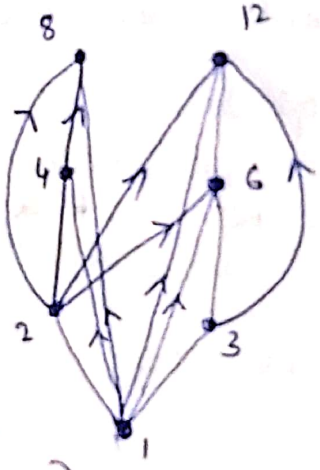
- discreet ≤ discrete (e<t)
- discrete ≤ discrete (c<r)
- discreti ≤ discrete (e<t)

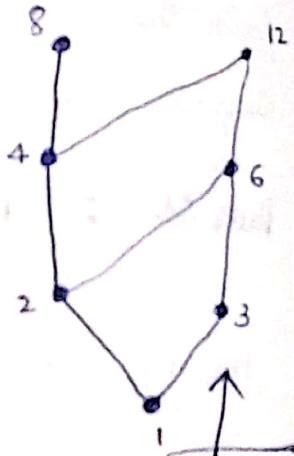
*. HASSE DIAGRAM :

- Each dot represents node or vertex indicating element
- If x is immediate predecessor of y, then the node for y is placed above node for x, these are connected by a straight line segment.

Ex: Draw Hasse diagram representing PO $\{(a,b) \mid a \text{ divide } b\}$ on $\{1,2,3,4,6,8,12\}$







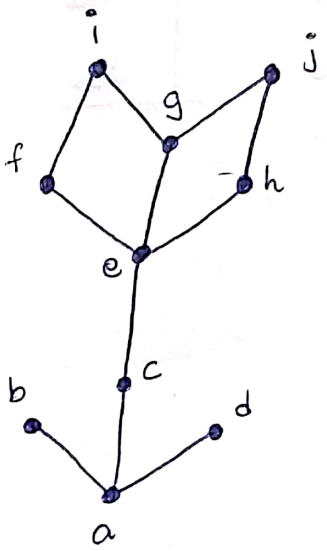
1 divides all
2 divides 2, 4, 6, 8, 12
3 divides 3, 6, 12
4 divides 4, 8, 12
6 divides 6, 12
8 divides 8
12 divides 12

1. Draw all these
2. Remove loops
3. Remove repeated
4. Simplify a|b b|c a|c
5. Simplify transitive by single line
6. Hasse diagram obtained.
7. Note: Remove ↑ directions

HASSE DIAGRAM

- lower bound – least common element in Hasse Diagram
- upper bound – greatest common element in Hasse Diagram
- least lower bound – The least element in all lower bound elem
- least upper bound – The least element in all elements of Upper bo
- Greatest lower bound – The greatest element in all lower bound element
- Greatest upper bound – The greatest element in all upper bound elements

*. LATTICES : LUB + GLB = least upper bound + Greatest lower Bound



Minimal & Minimum element = a

Maximal & Maximum element = b, d, i, j

GLB of {c, e} = LB of {c, e} is
out of a, c ← {a, c}
greater is c
∴ GLB of {c, e} = c

LUB of {c, e} = LB of {c, e} is
out of a, c ← {a, c}
least is a
∴ LUB of {c, e} = a

Upper bound of {c, e} → {e, f, g, h, i, j} (least … greatest)

least upper bound of {c, e} = e

greatest upper bound of {c, e} = j

---

*. REPRESENTING RELATIONS :

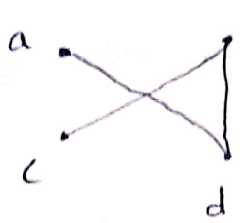
$$m_{ij} = \begin{cases} 1 & \text{if } (a_i, b_j) \in R \\ 0 & \text{if } (a_i, b_j) \notin R \end{cases} \qquad M_R = [m_{ij}]$$

(check laptop)

*. GRAPHS :

Type	Edges	Multiple Edges	Loops Allowed?
Simple Graph	Undirected	No	No
Multi Graph	Undirected	Yes	No
Pseudo Graph	Undirected	Yes	Yes
Simple directed Graph	Directed	No	No
Directed multi Graph	Directed	Yes	Yes
Mixed Graph	Directed and Undirected	Yes	Yes

* BASIC TERMINOLOGY:



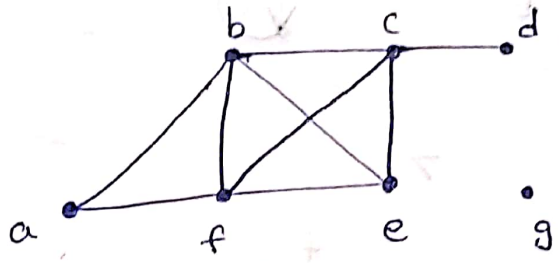
only { a, d / b, c / b, d } are adjacent since they are connected to the line

- Adjacent — Neighbourhood.
- degree zero — isolated

degree

- loop at vertex — twice
- degree one — pendant

Example:



degree

a = 2 d = 1

b = 4 e = 3

c = 4 f = 4

g = 0

neighbourhood

a = b, f

b = a, f, e, c = 4

d = c

g = ∅ = empty set

* HAND SHAKING THEOREM:

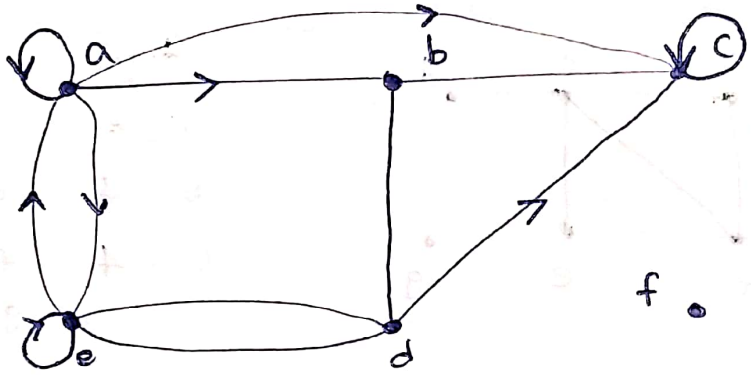
$$2m = \sum \deg(\text{vertices}) = \text{Sum of all degree of vertices}$$

m - edges of graph for undirected graph.

$$\boxed{\text{Sum of degree of vertices} = 2\left[\text{no. of edges}\right]}$$ * IMP

- $2m = \sum \text{degree}(\text{vertices}) = \sum \text{degree}(\text{vertices}_1) + \sum \text{deg}(\text{v}_2)$
- An undirected graph has an even number of vertices of odd degree
- in degree = $\deg^-(v)$
- out degree = $\deg^+(v)$
- Loop at vertex contributes 1 to both in in degree and out degree

Example :

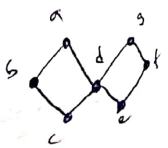


indegree – point towards that vertex (come towards)
Out degree – point away that vertex (leave away)

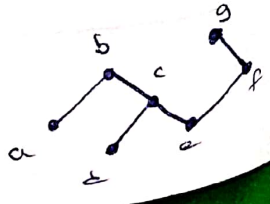
* . $|E|$ – Cardinality of E .

COMPLETE GRAPH

* . Cyclic Graphs – degree of each vertex = 2
– atleast one cycle.



* . Acyclic Graphs – degree of each vertex = 1
– ~~atleast~~ no cycles .

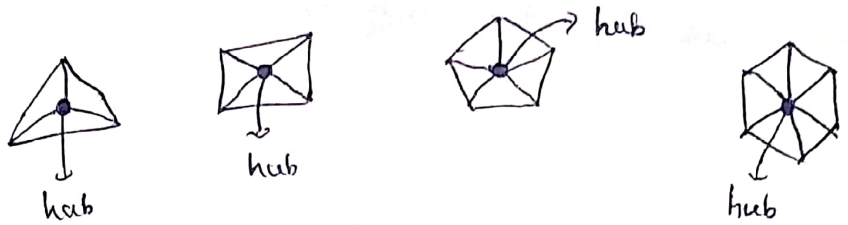


*. HUB – wheel graph $W(n)$

cycle + new vertex (center) is connected to each & every vertex.

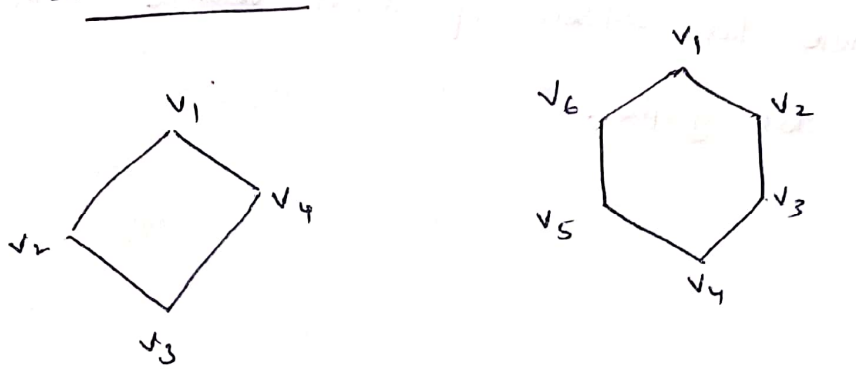
n - no. of vertices

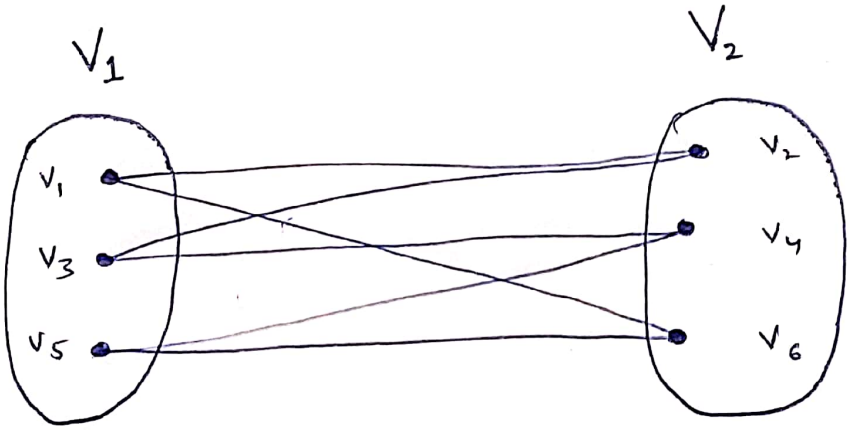
$n \geq 3$

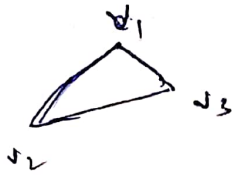


No. of vertices for n positions = 2^n

*. BIPARTITE GRAPHS :







*. GRAPH COLORING :

A simple, graph is Bipartite if and only if it is possible to assign one of two different

*. Complete Bipartite Graph :

$K_{m,n}$ is graph that has its vertex set partitioned into two subsets of m, n vertices with edge between two graphs.

TREE

- A tree is connected undirected graph with no simple circuits.
- An undirected graph is tree if and only if there is unique simple path between any two of its vertices.

Theorem : A tree with n-vertices → (n-1) edges

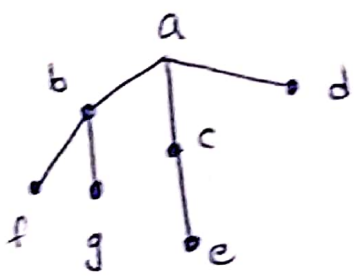
- Rooted tree :

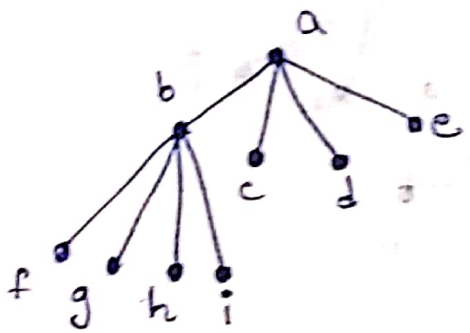
  which one vertex has been designated as root and every edge is directed away from root.

* Properties :

*. M-ary Tree :

- A rooted tree is called m-ary tree if every vertex has no more than m children.
- The tree is called full m-ary tree if every internal vertex has exactly m children.
- A rooted m-ary tree is balanced if all leaves are at levels h or h-1.





- Theorem-1 : Full m-array tree with i internal vertices contains $n = mi + 1$ vertices.
- Theorem-2 : A full m-array tree with

i. n-vertices has $i = \frac{n-1}{m}$ internal vertices

$l = \frac{(m-1)n+1}{m}$ leaves.

ii. i internal vertices has $n = mi + 1$ vertices.

$$l = \frac{(m-1)n + 1}{m} \text{ leaves.}$$

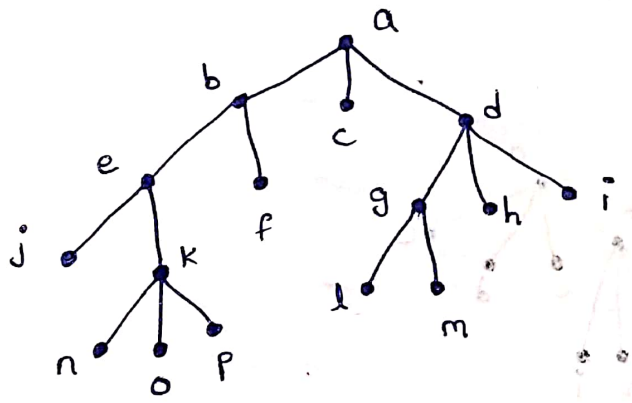
iii. l leaves has $n = \frac{ml - 1}{m-1}$ vertices and

$$i = \frac{l-1}{m-1} \text{ internal vertices.}$$

- Theorem -3 : There are most (m^h) leaves in an m-ary tree of height h.

* . TREE TRAVERSALS :

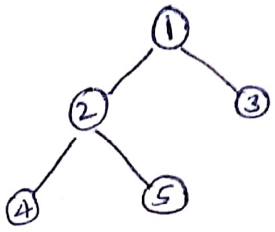
1. Inorder – Left, root, Right
2. Preorder – Root, Left, right
3. Post order – Left, Right, root



1. Inorder : j e n k o p b f a c l g m d h i

2. Preorder : a b e j k n o p f c d g l m h i

3. Post order : j n o p k e f b c l m g h i d a



1. Inorder : 4 2 5 1 3
2. Preorder : 1 2 4 5 3
3. Post order : 4 5 2 3 1

- Breadth First or level order Traversal : 1 2 3 4 5

- Inorder traversal gives nodes in non-decreasing order. To get nodes of BST in non-increasing order, a variation of inorder traversal where inorder traversals reversed can be used.

- Preorder traversal is used to create a copy of tree. Preorder traversal is also used to get prefix expression on of an expression tree.

- Postorder : Postorder travel is used to delete the tree. It is also useful to get the postfix expression.

GRAPHS :

- A Graph $G = (V, E)$ consists of V, a non empty set of vertices (or nodes) and E, a set of edges. Each edge has either one or two vertices associated with it, called its endpoints. An edge is said to connect its endpoint.

- Infinite Graph - Infinite vertex set or Infinite no. of edges of graph.

- Finite Graph - Finite vertex set or Finite no. of edges of graph.

- No edge connects a vertex to itself.
- No two different edges connect the same pair of vertices.

- Simple Graph - A Graph in which each edge connects two different vertices and where no two edges connect same pair of vertices.

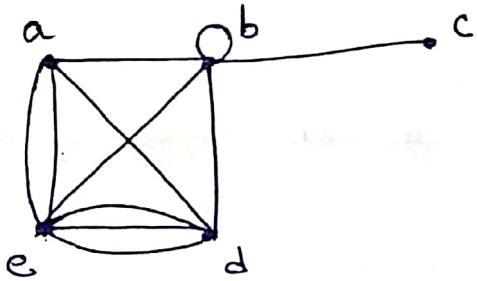
- Digraph - A Directed graph (V, E) consists of non empty set of vertices V and a set of directed edges E.

- The directed edge associated with ordered pair (u, v) is said to start at u & end at v.

* Graph Terminology :

Type	Edges	Multiple Edges allowed	Loops Allowed?
Simple Graph	Undirected	✗	✗
Multi Graph	Undirected	✓	✗
Pseudo Graph	Undirected	✓	✓
Simple Directed Graph	Directed	✗	✗
Directed Multi Graph	Directed	✓	✓
Mixed Graph	Directed & Undirected	✓	✓

- **Degree** - The degree of vertex in an undirected Graph is the no. of edges incident with it, except the loop at a vertex contributes twice to the degree of that vertex. $\{ \deg(v) \}$



$\deg(a) = 2$

$\deg(b) = 6$ (loop 2 times)

$\deg(c) = 1$

$\deg(d) = 5$

$\deg(e) = 6$

Vertices = $\{a, b, c, d, e\}$

This in undirected Graph

* . Hand Shaking Theorem :

Let $G = (V, E)$ be an undirected graph with m edges then,

$$2m = \sum_{v \in V} \deg(v)$$

imp • How many edges are there in graph with 10 vertices each of degree six.

edge, $m = ?$

$$\text{edges} = \frac{\text{Sum of all vertices degree}}{2}$$

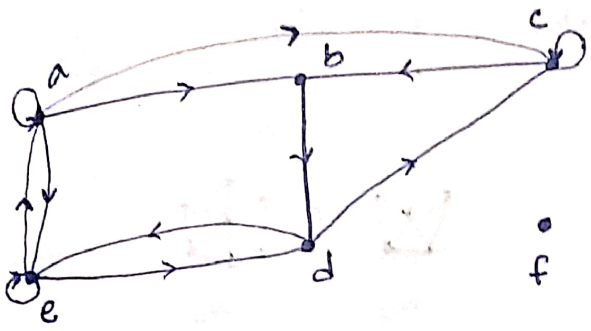
no. of vertices = 10
degree of each vertex = 6
} total Sum of degree of all vertices = $6 \times 10 = 60$

$$\text{edges} = \frac{60}{2} = 30$$

∴ No. of edges = 30

- An undirected graph has an even number of vertices of odd degree.

- in-degree : $\deg^-(v)$ - terminal vertex
- out-degree : $\deg^+(v)$ - initial vertex
- Loop at vertex contributes 1 to both the in-degree and the out-degree of this vertex.



$\deg^-(a) = 2$
$\deg^-(b) = 2$
$\deg^-(c) = 3$
$\deg^-(d) = 2$
$\deg^-(e) = 3$
$\deg^-(f) = 0$

} coming towards the vertex

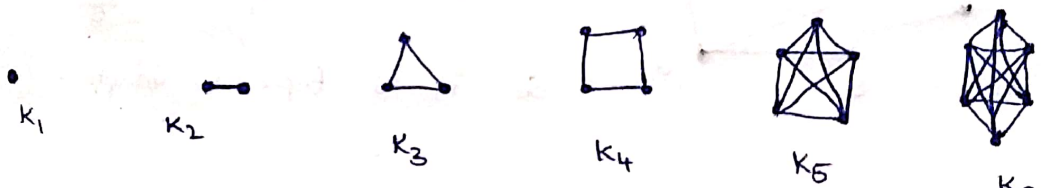
$\deg^+(a) = 4$
$\deg^+(b) = 1$
$\deg^+(c) = 2$
$\deg^+(d) = 2$
$\deg^+(e) = 3$
$\deg^+(f) = 0$

} going away from vertex

- $\sum_{v \in V} \deg^-(v) = \sum_{v \in V} \deg^+(v) = |E|$

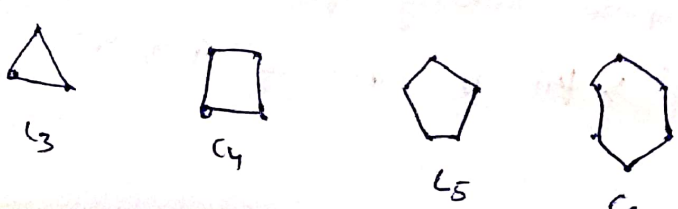
*. SPECIAL SIMPLE GRAPHS :

① Complete Graph : with n vertices = K_n

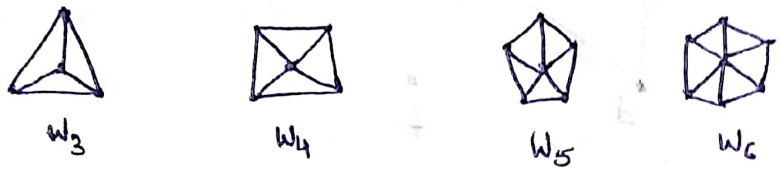


each vertex is connected to each & every other vertex

② Cycles : n vertices , $n \geq 3$: C_n

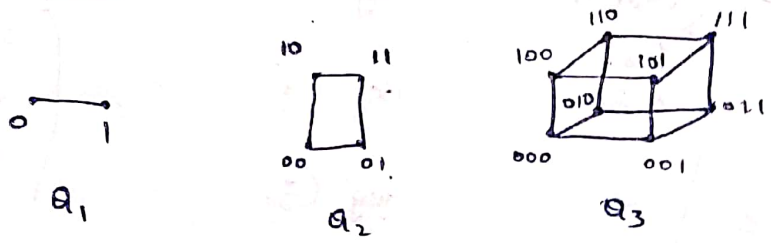


③ Wheels : n vertices, $n \geq 3(+1)$



extra vertex at centre for a cycle graph. All the vertices are connected to that centre vertex.

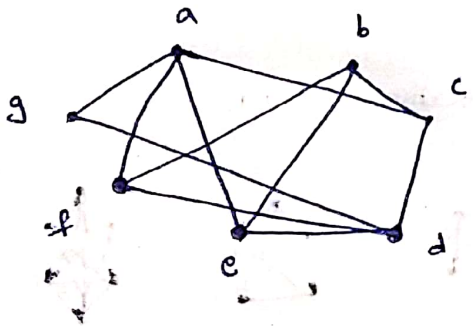
④ n-cube :



⑤ Bipartite Graph :

No common edge for two categorized set of vertices

$\{v_1, v_2, v_3 \dots\}$ & $\{u_1, u_2, u_3, \dots\}$



$\{a, b, d\}$ → no common edge

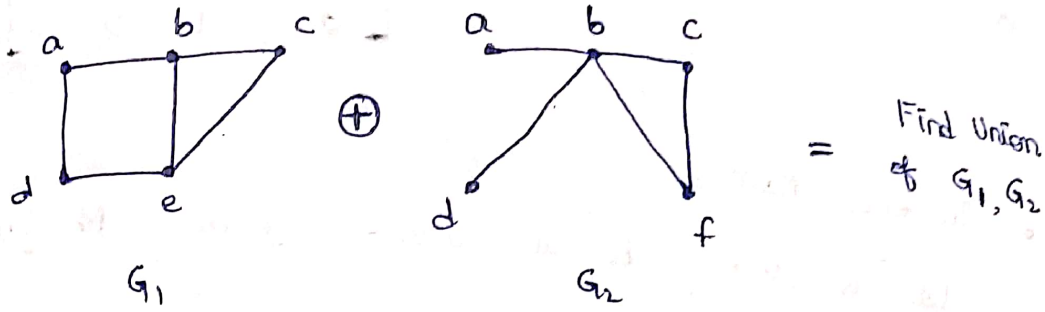
$\{c, e, f, g\}$ → no common edge

So, it is Bipartite Graph.

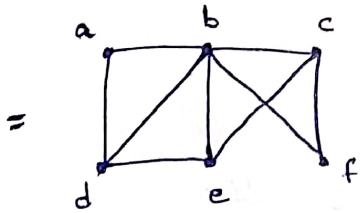
* HALL'S MARRIAGE THEOREM :

The bipartite graph $G = (V, E)$ with bipartition (V_1, V_2) has a complete matching from V_1 to V_2 if and only if $|N(A)| \geq |A|$ ∀ subsets of A of V_1.

- A subgraph of $G = (V, E)$ is a graph $H = (W, F)$, where $W \subseteq V$ and $F \subseteq E$. A subgraph H of G is a proper subgraph of G if $H \neq G$.



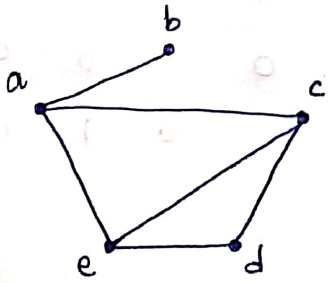
G_1 G_2



= → The Union of $G_1 \cup G_2$

*. REPRESENTING GRAPHS :

- Use Adjacency list to describe the figure.



vertex	Adj. Vertices
a	b, c, e
b	a
c	a, d, e
d	c, e
e	a, c, d

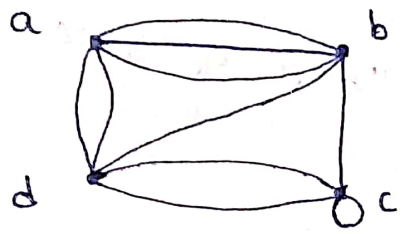
- Adjacency Matrices :

Suppose $G = (V, E)$ is simple Graph, $|V| = n$

$A = [a_{ij}]$, than

$$a_{ij} = \begin{cases} 1 & \text{if } \{v_i, v_j\} \text{ is edge of } G \\ 0 & \text{otherwise} \end{cases}$$

- Use Adjacency Matrix to represent :



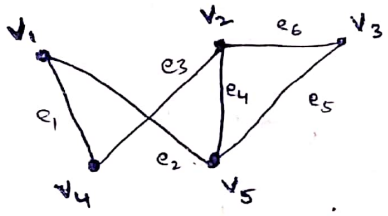
	a	b	c	d
a	0	3	0	2
b	3	0	1	1
c	0	1	1	2
d	2	1	2	0

- Incidence Matrices :

Let $G = (V, E)$ be an undirected graph, $M = [m_{ij}]$

$$m_{ij} = \begin{cases} 1 & \text{when edge } e_j \text{ is incident with } v_i \\ 0 & \text{otherwise} \end{cases}$$

Ex: Represent below graph with Incidence Matrix.



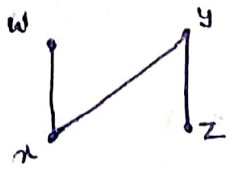
	e_1	e_2	e_3	e_4	e_5	e_6
v_1	1	1	0	0	0	0
v_2	0	0	1	1	0	1
v_3	0	0	0	0	1	1
v_4	1	0	1	0	0	0
v_5	0	1	0	1	1	0

- The Definition of Isomorphism is,

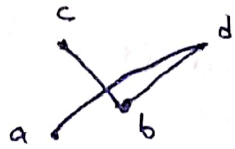
Let graphs $G1 = \{V1, E1\}$ and $G2 = \{V2, E2\}$ are isomorphic if :

i. There is bijection f from V1 to V2 and

ii. There is bijection g from E1 to E2 that maps each edge (v, u) to $\{f(v), f(u)\}$.



G

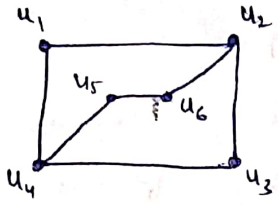


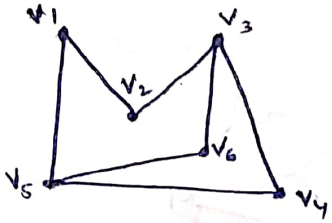
H

$f(w) = a$, $f(x) = d$, $f(y) = b$, $f(z) = c$

$f : V(G) \longrightarrow V(H)$

- Determine below graphs are isomorphic or not :





$f(u_1) = v_4$ or v_6

Assume $f(u_1) = v_6 \Rightarrow f(u_2) = v_3$ or v_5

Assume $f(u_2) = v_3 \Rightarrow f(u_3) = v_4$

&, $f(u_4) = v_5$ & $f(u_5) = v_1$ & $f(u_6) = v_2$

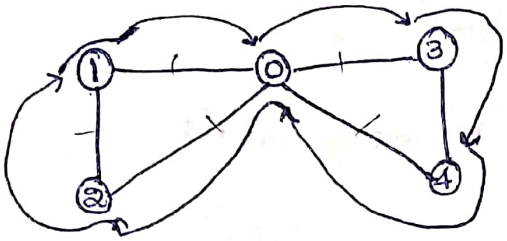
$A_G =$

	u_1	u_2	u_3	u_4	u_5	u_6
u_1	0	1	0	1	0	0
u_2	1	0	1	0	0	1
u_3	0	1	0	1	0	0
u_4	1	0	1	0	0	0
u_5	0	0	0	1	0	1
u_6	0	1	0	0	1	0

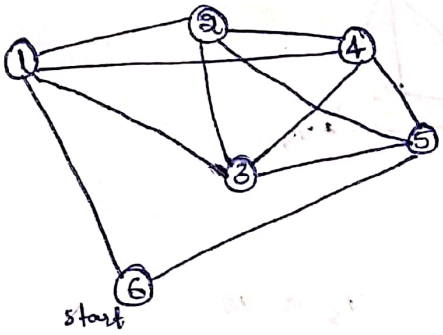
We will get similar for $\cong A_H$

*. EULER GRAPH :-

Any random traversal in graph in which no edge is repeated (a vertex can) which starts & ends at same vertex.



→ Example of Euler Graph



6 → 1
1 → 2
2 → 3
3 → 1
1 → 4
4 → 2
2 → 5
5 → 3
3 → 4
4 → 5
5 → 6

Traversal from 6 & end at 6 ↓ EULER GRAPH

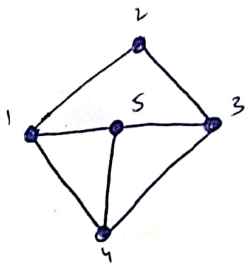
- Condition to identify Euler :

1. Every vertex has even degree
2. If there is any vertex with odd degree, then Euler Circuit is not possible.
3. There can exist a vertex with degree 0 (even degree = 0) So, Euler Circuit is possible
4. Semi-Eulerian Graph : Couldn't start & end at same vertex but complete edges are traversed.
   - ↳ All vertices have even degree except the starting & ending vertex. (only 2)

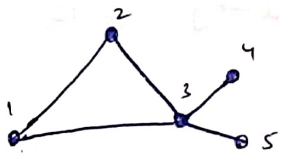
DIRAC's Theorem : If G is simple Graph with n vertices ($n \geq 3$) such that degree of every vertex in G is at least $n/2$. Then G is Hamilton Circuit.

* HAMILTONIAN GRAPH :

- A simple circuit in G that passes through every vertex exactly once.



$1 \to 2$ $2 \to 3$ $3 \to 4$ $4 \to 5$
$5 \to 1$ is Hamiltonian Circuit



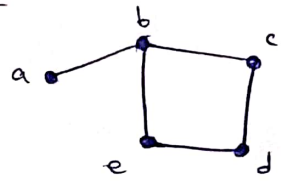
$1 \to 2$ $2 \to 3$ $3 \to 4$ ✗ Not possible
$3 \to 5$

- edge can be visited n no. of times
- vertex only to be once visited.

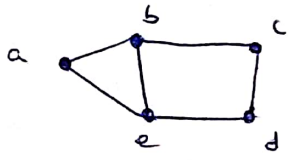
Examples : → Cycle Graphs
→ Complete Graph
→ Wheel Graphs

- Hamiltonian Path : Couldn't reach to the starting vertex but traversed every vertex it is Hamiltonian path

ex :



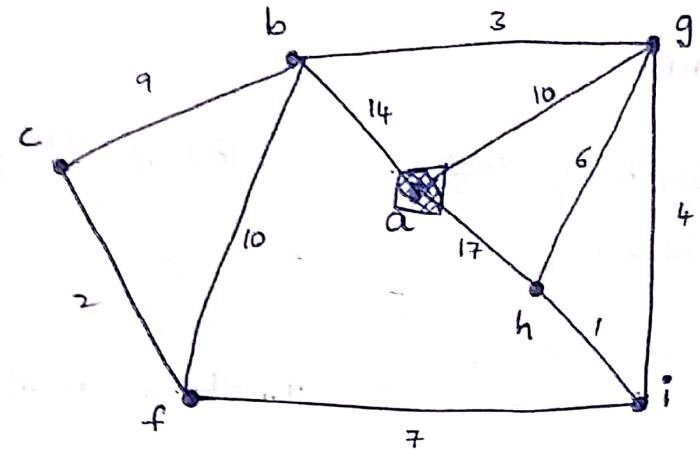
$a \to b$ $d \to e$
$b \to c$ $e \to$ ✗ → all vertices are traversed but didn't reach "a" again
$c \to d$



$a \to b$
$b \to c$
$c \to d$
$d \to e$
$e \to a$
} reached & started at "a"
So, Hamiltonian Circuit.

* Shortest Path Problems :

i. Dijkstra's Algorithm :



Starting at a

Case - i

$a \to b$: $(a, 14)$ ✗

$a \to g$: $(a, 10)$ ✓ ⟶ $a \to g : (a, 10)$

$a \to h$: $(a, 17)$ ✗

Case - ii :

$g \to b$: $(g, 13)$ ✓ ⟶ $g \to b : (g, 13)$

$g \to h$: $(g, 16)$

$g \to i$: $(g, 14)$

Case - iii :

$b \to c$: $(b, 22)$ ✓

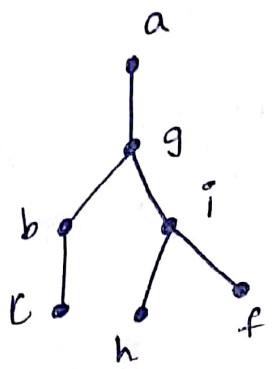
$b \to f$: $(b, 23)$ ✗

Case - ii : $g \to i$: $(g, 14)$ ✓

Case - iv : $i \to h$: $(i, 15)$ ✓

$i \to f$: $(i, 21)$ ✓

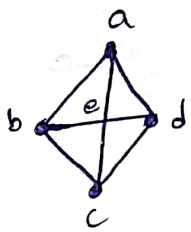
$f \to b$: $(f, 23)$ ✗



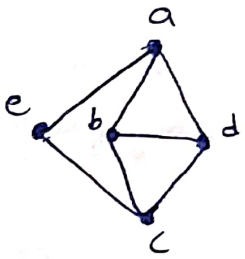
→ Minium Spanning Tree.

* Planar Graphs :

- A Graph G is planar iff it can be drawn without any crossing edges.



⟹ can be redrawn as



All complete Graphs are not planar Graphs :

K_1 ⟹

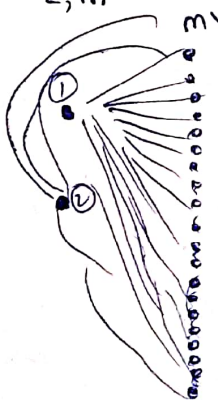
K_2 ⟹

K_3 ⟹

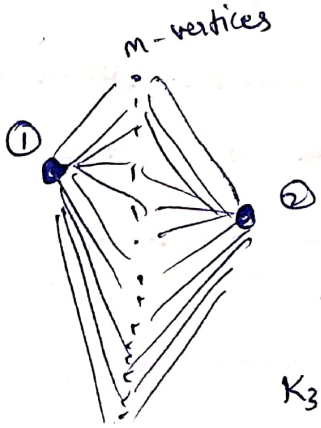
K_4 ⟹

For a Complete bipartite graph ?

$K_{2,m}$



⟹ Can be redrawed as



✓

$K_{3,2} \cong K_{2,3}$

- **Euler's Formula :**

Let G be a connected planar simple graph with e edges and v vertices. Let r be no. of regions in planar representation of G. Then

$$\boxed{r = e - v + 2}$$

Ex : Suppose a planar simple graph has 20 vertices, each of degree 3. Into how many regions does it represent of graph spliting the plane ?

$v = 20$, deg of each $= 3$ ⟩ total degree of vertices $= 20 \times 3 = 60$

$2 \times$ edges $= 60 \Rightarrow$ edges $= 30$

regions, $\boxed{r = \text{edges} - \text{vertices} + 2}$

$r = 30 - 20 + 2 = 12$ regions.

- If G is connected planar simple graph, then G has a vertex of degree not exceeding 5.

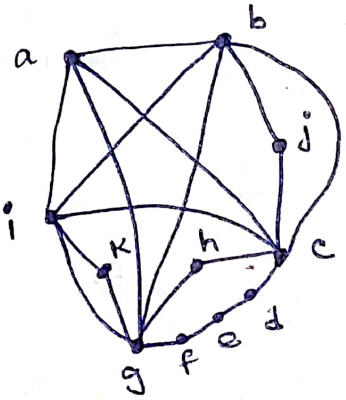
- If G is connected planar simple graph with edges (e) & vertices (v), where $v \geq 3$ then :

IMP * $\boxed{e \leq 3v - 6}$

- If a connected planar simple graph has e edges and v vertices with $v \geq 3$ and no circuits of length 3, then $e \leq 2v - 4$.

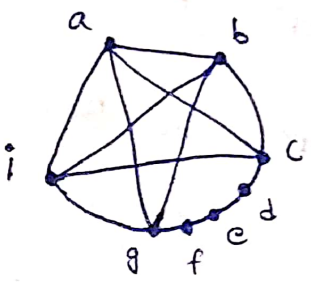
- A Graph is non-planar iff it contains a sub graph homeomorphic to $K_{3,3}$ or K_5.

Ex: Determine if the Graph(G) is planar or not?



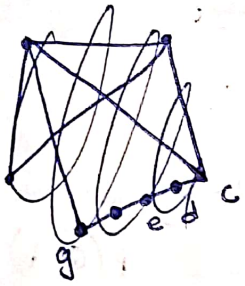
Graph G

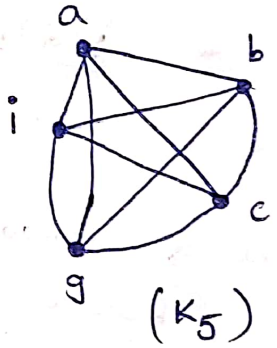
Undirected Graph
(Given)



Graph H

Subgraph homeomorphic to K_5





(K_5)

→ Graph G has subgraph H homeomorphic to K_5

→ Graph H is obtained by deleting all edges incident with those vertices H is homeomorphic to K_5

→ Because it can be obtained from K_5 (a, b, c, g, i) adding d, e, f. So, G is non planar.

Graph Coloring:

A Graph Coloring is giving color to each vertex of graph so that no two adjacent vertices are assigned the same color.

graph, G $= \gamma(G)$

Complete graph, K_n $= n$

cycle graph C_n, $n>1$ $= \begin{cases} 3 & \text{for } n \text{ odd} \\ 2 & \text{for } n \text{ even} \end{cases}$

Star graph, S_n, $n>1$ $= 2$

wheel graph, W_n, $n>2$ $= \begin{cases} 3 & \text{for } n \text{ odd} \\ 4 & \text{for } n \text{ even} \end{cases}$

- The chromatic number of graph is least number of colors needed for coloring of this graph. The chromatic number of graph G is $\boxed{\gamma(G) = \text{colors}}$

  n - number of vertices.

- Let d be the no. of available colors for G. We want to find a chromatic polynomial $P(G,d)$ that tells us how many ways we can color a graph with atmost d colors.

① $|V| = n$ & $E = \phi$, then $P(G,d) = d^n$

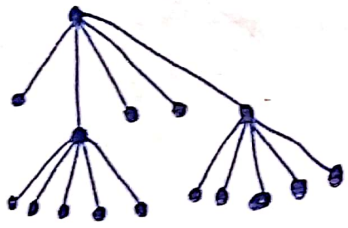
② $G = K_n$ then $P(G,d) = \dfrac{d!}{(d-n)!}$

TREES :

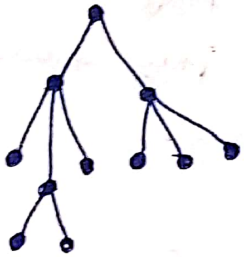
- A tree is a connected undirected graph with no simple circuits.

- A rooted tree is a tree which one vertex has been designated as the root and every edge is directed away from the root.

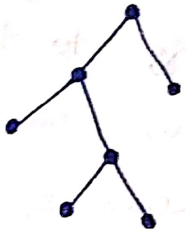
- m-array Tree : A rooted tree is called m-array tree, if every internal vertex has more than m children.
- The tree is called full m-ary tree, if every internal vertex has exactly m children.
- A m-ary tree with $m=2$ is called Binary Tree.



Full 5-ary Tree



not full m-array Tree. Just m-array

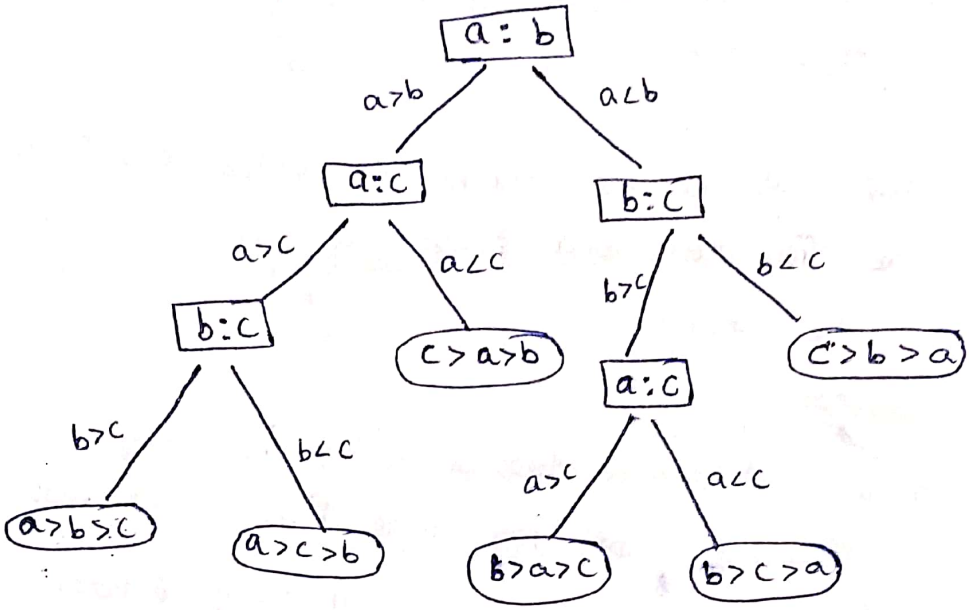


Binary Tree ($m=2$)

*. Properties :

- A tree has $\boxed{\text{edges} = n-1}$ with $\boxed{\text{vertices} = n}$.
- A full m-array tree with i internal vertices contains $n = mi + 1$ vertices.
- There are at most m^h leaves in an m-ary tree of height h.

- List a, b, c comparing them as Decision Tree.

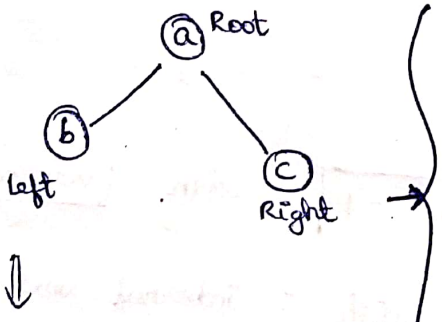


A Decision Tree for sorting three distinct elements.

- The value of a vertex of a game tree tells us the pay off to the first player if both players follow the min-max strategy and play starts from position represented by this vertex.

*. TREE TRAVERSAL : (Binary Tree)

Tree :



Pre order : a b c

Post order : b c a

In order : b a c

① Pre-order :

Root - Left - Right

② Post-order :

Left - right - root

③ In-order :

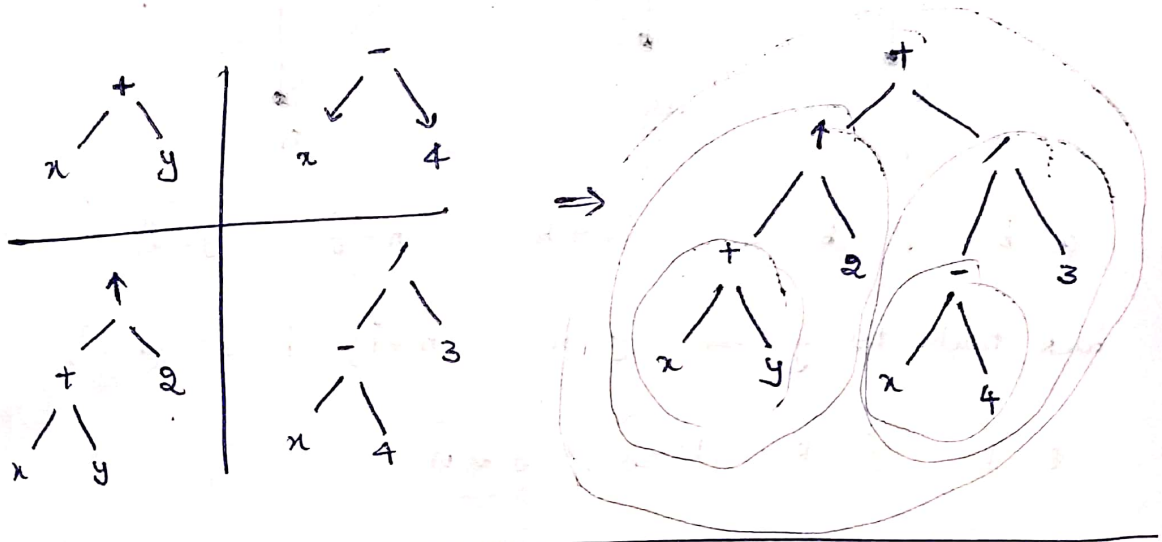
Left - Root - Right

*. Infix, Prefix, Postfix :

+ : addition − : subtraction

* : multiplication / : division ↑ : exponentiation

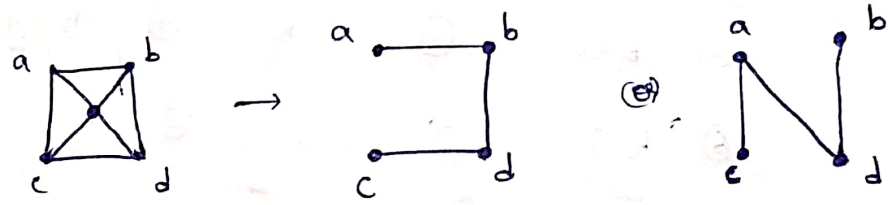
Expression : $[(x+y)\uparrow 2] + [(x-4)/3]$?



---

*. Spanning Tree :

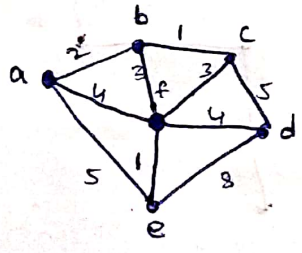
- A graph which contains all vertices with minimum number of edges.

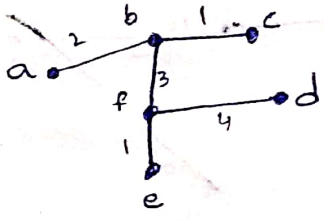


Graph Spanning tree (or) Spanning Tree

number of vertices = n ⇒ no. of edges, $\boxed{e = n-1}$

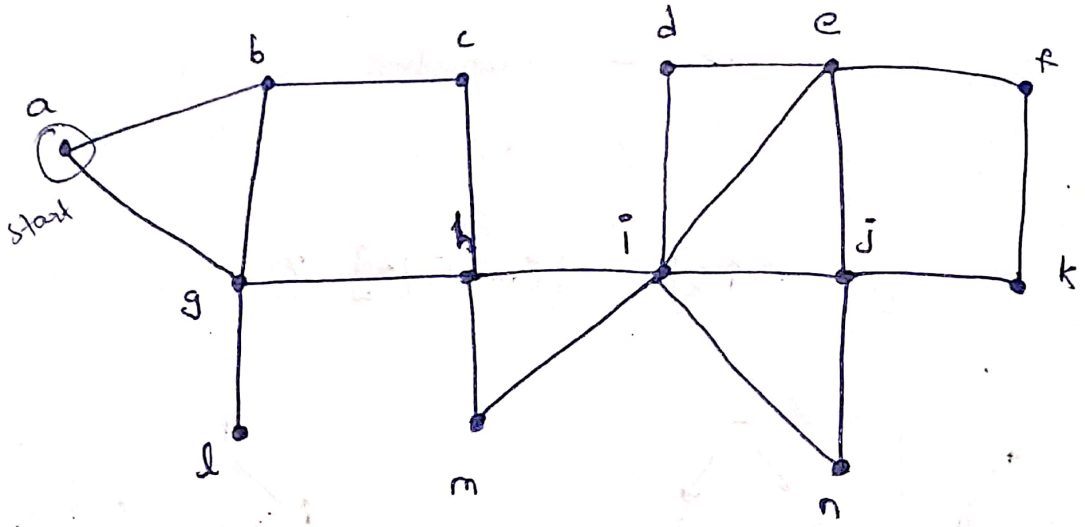
- Minimum Spanning Tree : Total sum of edges = minimum





cycle should n't be formed

Depth First Search :



a - b , b - c , c - h , h - g , g - l

back track to g ⇒ g - h , h - i , i - d , d - e ,

e - f , f - k , k - j , j - n

back track to j , ⇒ j - K , K - f , f - e ,

e - d , d - i , i - m

What path we took,

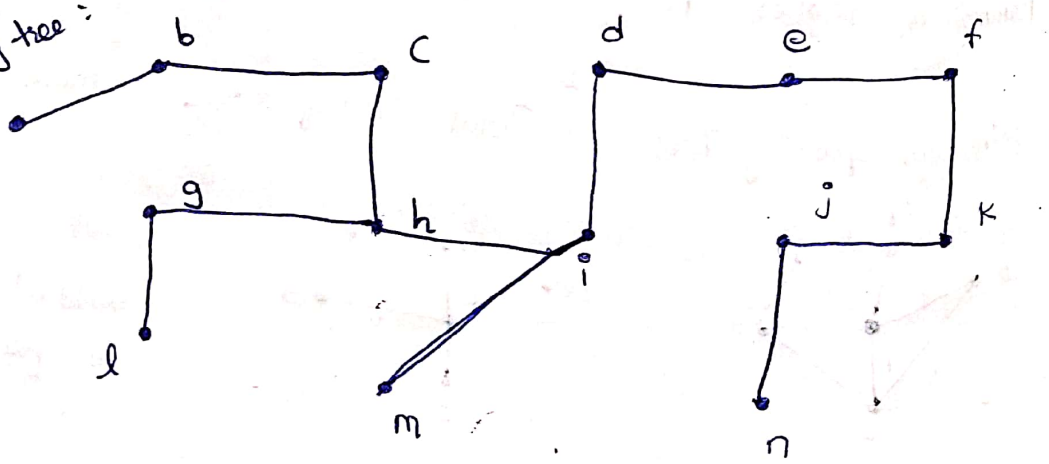
① a - b ② b - c ③ c - h ④ h - g

⑤ g - l ⑥ h - i ⑦ i - d ⑧ d - e

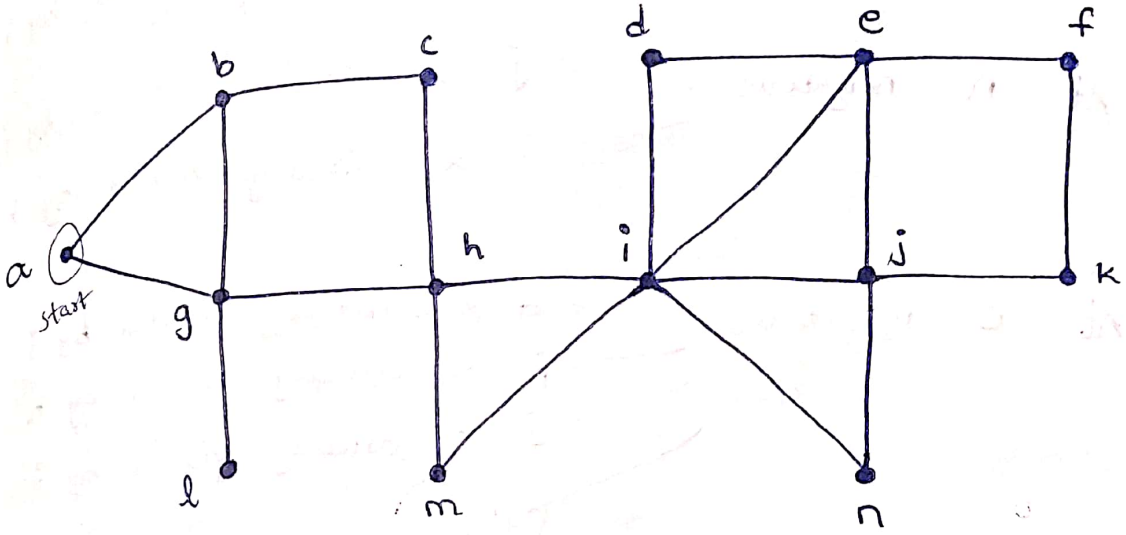
⑨ e - f ⑩ f - k ⑪ K - j ⑫ j - n

⑬ i - m

minimum spanning tree :



Breadth First Search :



Start a neighbours — b ✓, g ✓

At b neighbours — c ✓

g ✗ already visited by a

At g neighbours — b ✗ already visited by a

h ✓, l ✓

At c neighbours — h ✗ already visited by g

At h neighbours — g ✗ already visited by a

c ✗ already visited by b

m ✓, i ✓

At l neighbours — g ✗ already visited by a

At i neighbours — h ✗ already visited by g

d ✓, n ✓, e ✓

m ✗ already visited by h

j ✓

At d neighbours — e ✗ already visited by i
i ✗ already visited by h

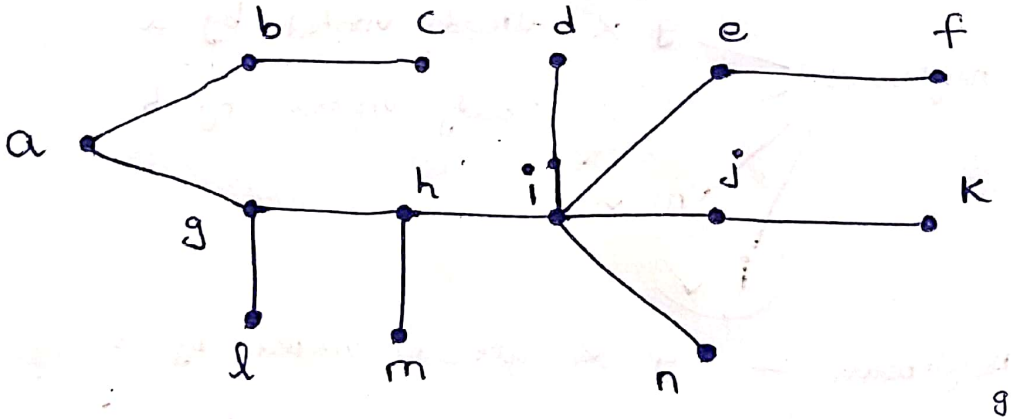
At n neighbours — j ✗ already visited by i
i ✗ already visited by h

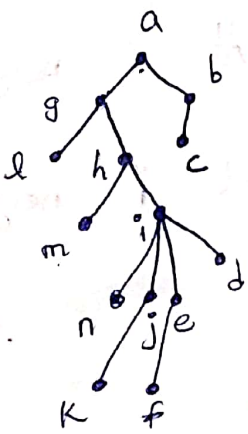
At e neighbours — d ✗ already visited by i
i ✗ already visited by h
j ✗ already visited by i
f ✓

At j neighbours — i ✗ already visited by h
n ✗ already visited by i
e ✗ already visited by i
K ✓

At f neighbours — e ✗ already visited by i
K ✗ already visited by k

At K neighbours — j ✗ already visited by i
f ✗ already visited by e





Spanning Tree
by BFS Algorithm.

- A minimum spanning tree in a connected weighted graph is that has the smallest possible sum of weights of its edges.

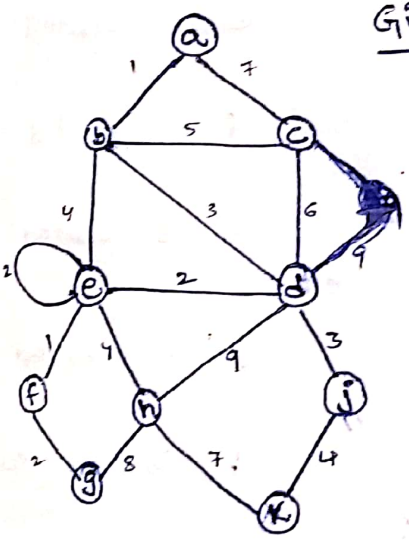
* PRIM'S ALGORITHM :

① Remove loops and parallel edges (keep min weights)

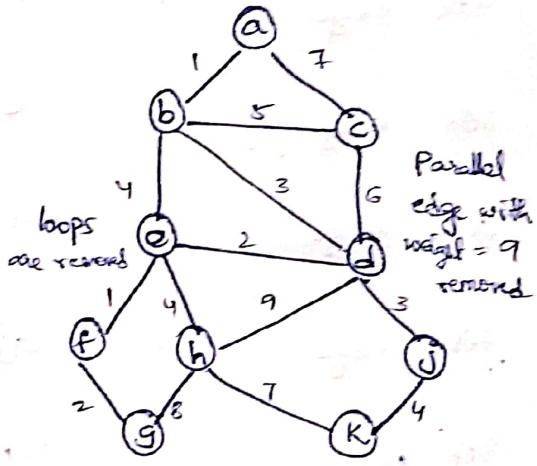
② While adding new edge, select edge with minimum weight out of the edges from already visited vertices. (No cycle allowed)

③ Stop at exactly edges $= n-1$ where vertices $= n$ until then repeat step 2

Given



After step ①

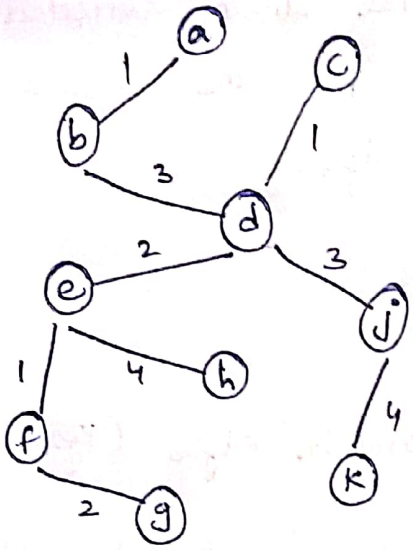


Visited vertices = a, b, d, c, e, f, g, j, h, K

Vertices = 10, so, edges = 9 (10-1)

Edges to choosed from = ~~ab~~ (1), ac (7), bc (5), ~~bd~~ (3), be (4), ~~dc~~ (6), ~~de~~ (2), dh (9), ~~dj~~ (3), ~~ef~~ (1), ~~eh~~ (4), ~~fg~~ (2), gh (8), ~~jK~~ (4), hK (7)

Answer :



As we are starting at a 'a' is already added to visited vertex set & edge will be

ab, ac

⋮

start	edge	weight	remark
1st edge :	ab	→ 1	b is added as visited
2nd edge :	bd	→ 3	d is visited
3rd edge :	dc	→ 1	c is visited
4th edge :	de	→ 2	e is visited
5th edge :	ef	→ 1	f is visited
6th edge :	fg	→ 2	g is visited
7th edge :	dj	→ 3	j is visited
8th edge :	eh	→ 4	h is visited
9th edge :	jk	→ 4	k is visited

stop since 10 edges > (n-1) edges = 9 All done

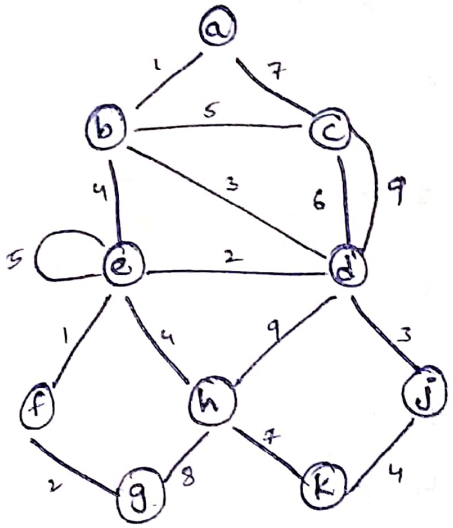
---

*. KRUSKAL'S ALGORITHM :

① Remove loops and parallel edges (keep minimum weight)

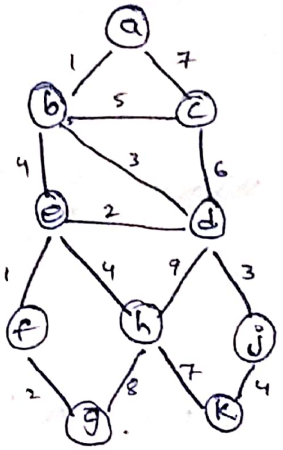
② List all edges & sort them according to weights (Asc)

③ Take n-1 edges from sorted list (skip cycle)



Given graph

After step 1



After step 2

vertex a :
- ab = 1
- ac = 7

vertex b :
- ba = 1 ×
- bc = 5
- bd = 3
- be = 4

vertex c :
- cb = 5 ×
- cd = 6
- ca = 7 ×

vertex d :
- db = 3 ×
- dc = 6 ×
- de = 2
- dh = 9
- dj = 3

vertex e :
- ed = 2 ×
- eb = 4 ×
- ef = 1
- eh = 4

sorting

ab = 1	ab = 1 ✓
ac = 7	ef = 1 ✓
bc = 5	de = 2 ✓
bd = 3	fg = 2 ✓
be = 4	bd = 3 ✓
cd = 6	dj = 3 ✓
de = 2	be = 4 ✗ → makes cycle
dh = 9	eh = 4 ✓
dj = 3	kj = 4 ✓
ef = 1	bc = 5 ✓
eh = 4	— complete
fg = 2	cd = 6
gh = 8	ac = 7
hk = 7	hk = 7
kj = 4	gh = 8
	dh = 9

not needed since (n-1) edges finished

vertex f : $fe = 1$ ×

$fg = 2$

vertex g : $gf = 2$ ×

$gh = 8$

vertex h : $hd = 9$ ×

$he = 4$ ×

$hg = 8$ ×

$hk = 7$

vertex j : $jd = 3$ ×

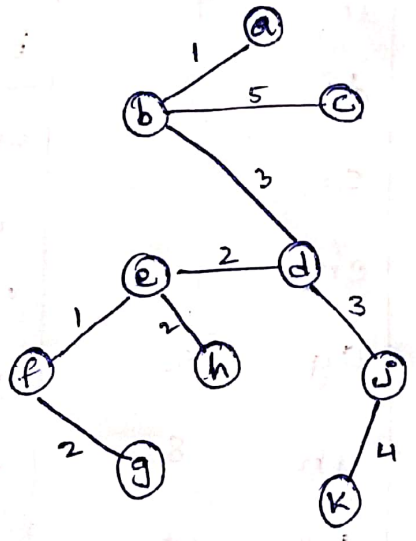
$jk = 4$

vertex K : $kh = 7$ ×

$kj = 4$ ×

no. of vertices = 10 = n

no. of edges = $n-1 = 10-1 = 9$



1
1
2
2
3
3
4
4
5

total weight = 25

MODULE - 4 : GROUP THEORY

*. Groupoid or Binary Algebra : Defination

- A non-empty set G equipped with one binary operation is called Groupoid. i.e.
  - → G is a groupoid if G is closed for *.
  - → It is denoted by (G, *).

Ex: (N, +) , (Z, −) , (Q. ×) etc...

Note: Groupoid is also called Quasi Group.

*. Semi - Group :

- An algebraic structure (G) is called semi-group if the binary operation * satisfies (G, *) Associative property i.e.

$$(a * b) * c = a * (b * c) \quad \forall\ a \in G$$

- Ex: The Algebraic structures (N,+) , (Z,+) , (Z,*) are semi Groups but the structure (Z, −) is not so because subtraction (−) is not associative.

*. Monoid :

- A semi Group is called Monoid , if there exists an identity element 'e' in G such that :

$$e * a = a * e = a \quad \forall\ a \in G$$

- Ex: The semi Group (N, *) is monoid because 1 is the identity for the multiplication. But semi Group (N, +) is not , because 0 is the identity for addition is not in N.

* Group :

- An algebraic structure set of G and a binary operation * defined in G i.e. $(G, *)$ is called a group if * satisfies the following :

→ Closure : $a \in G$, $b \in G \Rightarrow a * b \in G$, $\forall a, b \in G$

→ Associative : The composition * is associative in G i.e.

$$(a * b) * c = a * (b * c) \quad \forall a, b, c \in G$$

→ Existence of Identity : There exists an identity element e in G such that

$$e * a = a * e = a \quad \forall a \in G$$

→ Existence of Inverse : Each element of G is invertible i.e. $\forall a \in G$, there exists $\bar{a}^{-1}$

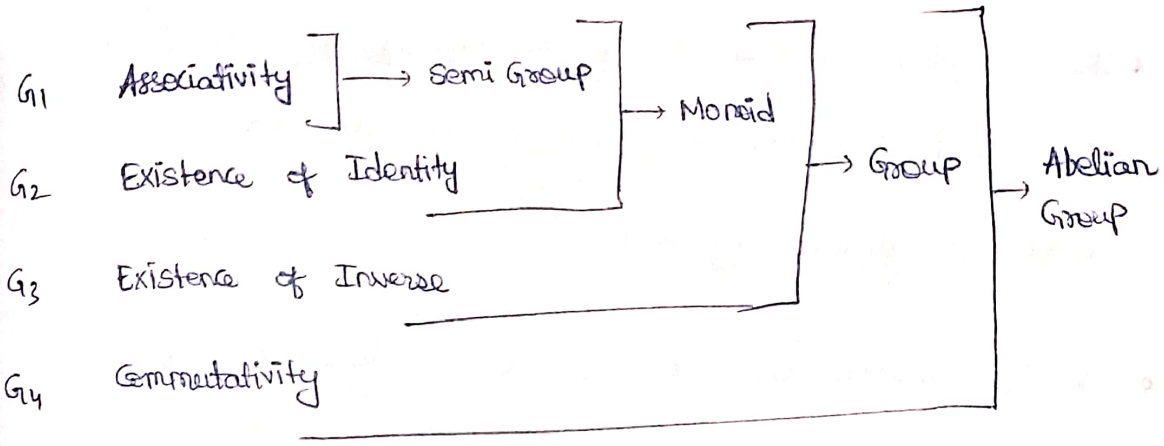
$$a * \bar{a}^{-1} = \bar{a}^{-1} * a = e \text{ (Identity)}$$

- Thus Group $(G, *)$ is a monoid in which each of its element is invertible.

* Abelian Group or Commutative Group :

- A group $(G, *)$ is said to be abelian or commutative if * is commutative also A group $(G, *)$ is an abelian group, if $[G_4]$ Commutative :

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



*. Finite & Infinite Groups:

- A group $(G, *)$ is said to be finite if its underlying set G is a finite set and a group which is not finite is called an infinite Group.

*. Order of Group:

- The Number of elements in a finite Group is called the order of the Group.
- It is denoted by $O(G)$.
- If $(G, *)$ is infinite Group, then it is said to be of infinite order.

Examples:

*. Addition & Multiplication module m:

- There are two special types of operations addition module m, written as $+ \bmod m$ or $\oplus_m$ or $+_m$ and multiplication module m, written as $\times \bmod m$ or $\otimes \bmod m$ or $\times_m$ on the set of integers Z.
- Let a & b be two integers and m be +ve integer greater than 1

- The addition modulo m of a and b is defined as the least non-negative remainder r obtained when $a+b$ is divided by m.
- It is written as $a +_m b = r$, where $0 \leq r < m$.

Ex: $5 +_4 5 = 2$ ($\because$ $5+5 = 10$ when 10 is divided by 4, remainder = 2)

$23 \times_7 10 = 6$ ($\because$ $23 \times 10 = 230$ mod $7 = 6$)

Example - 1 :

Prove that $Z_4 = \{0,1,2,3\}$ is an abelian group w.r.t addition modulo 4

Solution:

$$Z_4 = \{0,1,2,3,4\}$$

Cayley's table or composition table :

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

closure : output table also belongs to Z_4.

Associative : $(a +_m b) +_m c = a +_m (b +_m c)$

Identity : 0 is the identity element

Inverse : $\bar{0}^{-1} = 0$ $\quad \bar{2}^{-1} = 2$

$\bar{1}^{-1} = 3$ $\quad \bar{3}^{-1} = 1$

Commutative : Symmetric

*. GROUP AND PROPERTIES :

1. Theorem : Uniqueness of identity

2. Theorem : Uniqueness of inverse

3. Theorem : If G is a group for $a, b \in G$

$$(a^{-1})^{-1} = a$$

$$(ab)^{-1} = b^{-1} \cdot a^{-1} \quad \text{(Reversal law)}$$

4. Theorem : If a, b are elements of group G, then the equations $ax = b$ and $ya = b$ have unique solution in G.

*. Sub Group :

- A non empty subset H of a group G is called a subgroup of G if:
  - i. H is closed for composition defined in G i.e.

$$a \in H, \; b \in H \Rightarrow ab \in H$$

  - ii. and H itself is a group for composition induced by G.

*. Proper & Improper (Trivial) subgroup :

- Every group G of order greater than 1 has atleast two subgroups which are :
  - i. G (itself)
  - ii. $\{e\}$ – the group of identity alone.

  > improper or trivial subgroups

- A subgroup other than above is proper subgroup.

Important Remark:

- If any subset of the group G is a group of any operation other than the composition of G, then it is not called a sub group of G.

Ex: The group $\{1, -1\}$ is a part of $(C, +)$ which is group for the multiplication but not for the composition $(+)$ of the basic group. So, this is not the subgroup of $(C, +)$

Examples of Sub Group:

i. Additive Groups:

Ex: $(Z, +)$ is subgroup of $(Q, +)$

Ex: $(Q, +)$ is subgroup of $(R, +)$

Ex: The set of E even integers is proper subgroup of additive group $(E, +)$ whereas the set O of odd integers is not a subgroup of additive groups $(Q, +)$, $(Z, +)$.

ii. Multiplicative Groups:

Ex: $(Q^+, *)$ is a sub group of $(R^+, *)$

Ex: $\{1, -1\}$, $\{1, \omega, \omega^2\}$, $\{1, -1, i, -i\}$ are sub groups of $(C_0, *)$, the group of non-zero complex numbe

Ex: For multiplication operation $(\{1, -1\}, *)$ is a subgroup of $\{1, -1, i, -i\}$

Theorem : If H is a subgroup of a G, then :

i. The identity of H is the same as that of G,

ii. The inverse of any element a of H is the same as the inverse of the same regarded as an element of G.

iii. The order of any element a of H is the same as the order of a in G.

Theorem : A non-void subset H of a group G is a subgroup iff $a \in H, b \in H \Rightarrow ab^{-1} \in H$.

Remark : If the operation of the group is addition (+), then the condition is, $a \in H, b \in H \Rightarrow (a-b) \in H$.

Theorem : A non-void subset H of a group G is a subgroup iff $a \in H, b \in H \Rightarrow ab \in H$.

Theorem : The intersection of any two subgroups of a group G is again a subgroup of G.

Remark : The union of two subgroups is not necessarily a subgroup.

Ex : The Group $G = (Z, +)$ has two subgroups.

$$H = \{2n : n \in Z\} \quad \text{and} \quad K = \{3n : n \in Z\}$$

Then their union $H \cup K = \{\ldots, -6, -4, -3, -2, 0, 2, 3, 4, 6 \ldots\}$ is not a subgroup of G because this is not closed for +.

$2 \in H \cup K$
$3 \in H \cup K$
$\Rightarrow 2 + 3 = 5 \notin (H \cup K)$ which shows that $H \cup K$ is not closed for addition.

Theorem : If H and K are two sub groups of a group G, then HK is a subgroup of G iff ($\Leftrightarrow$) $HK = KH$.

*. COSETS & LANGRANGE'S THEOREM :

- Subgroup = Subset + Group
- H is subgroup of G : $H \leq G$
- Two standard subgroups of G :
  - → G - itself
  - → Trivial Group = $\{e\}$

*. LAGRANGE'S THEOREM :

- If $H \leq G$, then the order of H divides the order of G.
- order of G = # of elements in G = $|G|$
- $\boxed{H \leq G \Rightarrow |H| \text{ divides } |G|}$ *

Example: Let G be group with $|G| = 323 = 17 \times 19$

Divisors of 323 = 1, 17, 19, 323

Possible subgroups orders : 1 or 17 or 19 or 323

Standard subgroup : $G, \{e\}$

$|G| = 323 \qquad |\{e\}| = 1$

Any other subgroup has order 17 or 19

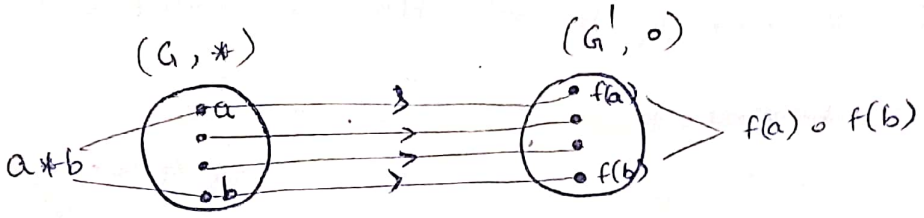
*. HOMOMORPHISM :

A mapping from group $(G, *)$ to a group (G', o) is called homomorphism from G to G' if

$$f(a * b) = f(a) \circ f(b),$$

Thus, if f is morphism from G to G', then it preserves the composition in both the groups G and G' i.e.,

image of composite = composite of images.



Example :

→ Let $(R, +)$ be the additive group of real numbers and $(R_0, *)$ be the multiplicative group of non-zero real numbers

→ The mapping $f : (R, +) \longrightarrow (R_0, *)$;

$f(x) = 2^x \quad \forall\, x \in R$ is a homomorphism of R into R_0 because of any $x_1, x_2 \in R$.

$$f(x_1 + x_2) = 2^{x_1 + x_2} = 2^{x_1} \cdot 2^{x_2} = f(x_1) \cdot f(x_2)$$

- Monomorphism, if f is injection (one - one)
- Epimorphism, if f is surjection (onto)
- Isomorphism, if f is bijection (one-one & onto)
- Endomorphism, if $G' = G$ (itself)
- Automorphism, if $G' = G$ and f is bijection.

Theorem : If f is a homomorphism from a group G to G' and if e and e' be their respective identities then,

a. $f(e) = e'$

b. $f(a^{-1}) = [f(a)]^{-1}$, $a \in G$

Theorem : If f is homomorphism of a group G to a group G', then :

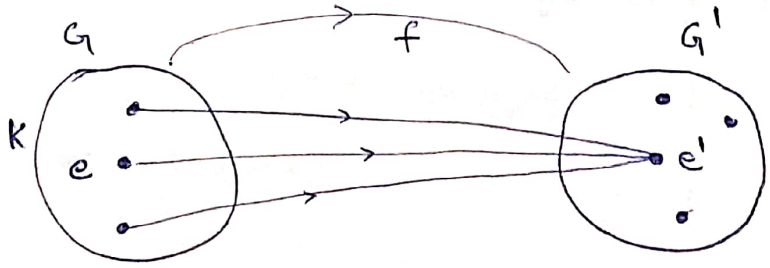
a. H is subgroup of G $\Rightarrow$ $f(H)$ is subgroup of G'.

b. H' is subgroup of G' $\Rightarrow$ $f^{-1}(H') = \{ x \in G \mid f(x) \in H \}$ is subgroup of G.

* . KERNAL OF HOMOMORPHISM :

- Let f be a homomorphism of group G into G', then the set of K of all those elements of G which are mapped to the identity e' of G' is called the kernal of homomorphism f.
- It is denoted by Ker f or Ker(f).

IMP • $\text{Ker}(f) = \{ x \in G \mid f(x) = e' \}$



Example 1 :

The mapping $f : (C_0, \times) \longrightarrow (R_0, \times)$ $f(z) = |z|$, $\forall z \in C_0$ is a homomorphism of C_0 onto R_0 because for $z_1, z_2 \in C_0$.

$$f(z_1 z_2) = |z_1 z_2| = |z_1|\,|z_2| = f(z_1) \cdot f(z_2)$$

Again $\ker(f) = \{ z \in C_0 \mid f(z) = 1 \}$

$$= \{ z \in C_0 \mid |z| = 1 \}$$

Example 2 :

$f : R_0 \to R_0$, $f(x) = x^4$; $x \in R_0$ is a homomorphism on R_0, because for any $x_1, x_2 \in R_0$

$$f(x_1 x_2) = (x_1 x_2)^4 = x_1^4 \cdot x_2^4 = f(x_1) \cdot f(x_2)$$

$$\ker(f) = \{ x \in R_0 \mid f(x) = 1 \}$$

$x^4 = 1 \Rightarrow \ker(f) = \{ x \in R_0 \mid x^4 = 1 \} = \{1, -1\}$

$x^4 - 1 = 0$

$(x^2 - 1)(x^2 + 1) = 0$

$x = \pm 1, (x \neq \pm i)$ ✓ Real R_0 only

Example 3 :

The mapping $f : (R, +) \longrightarrow (C_0, *)$, $f(x) = e^{ix}$, $\forall x \in R$ is homomorphism from R to C_0 because $\forall x_1, x_2 \in R$.

$$f(x_1 + x_2) = e^{i(x_1 + x_2)} = e^{ix_1 + ix_2} = e^{ix_1} \cdot e^{ix_2} = f(x_1) \cdot f(x_2)$$

$$\Rightarrow f(x_1 + x_2) = f(x_1) \cdot f(x_2) \longrightarrow \text{homomorphism}$$

$$\text{Ker}(f) = \{x \in R \mid f(x) = 1\}$$

$$e^{ix} = 1$$

$$ix = 0$$

$$\cos x + i\sin x = 1$$

$$2m\pi, \quad m \in Z$$

$$\Rightarrow m = \{0, \pm 2\pi, \pm 4\pi \cdots\}$$

$$\Rightarrow = \{x \in R \mid e^{ix} = 1\}$$

$$= \{2m\pi \mid m \in Z\}$$

$$= \{0, \pm 2\pi, \pm 4\pi, \pm 6\pi, \ldots\}$$

Example 4 :

If $f : (C, +) \to (R, +)$; $f(x+iy) = x$ then f is homomorphism from C to R, because for any $(x_1 + iy_1)$, $(x_2 + iy_2) \in C$.

$$f\left[(x_1 + iy_1) + (x_2 + iy_2)\right] = f\left[(x_1 + x_2) + i(y_1 + y_2)\right]$$

$$= x_1 + x_2$$

$$= f(x_1 + iy_1) + f(x_2 + iy_2)$$

Again, $\text{Ker}(f) = \{(x+iy) \in C \mid f(x+iy) = 0\}$

$\{(x+iy) \in C \mid x = 0\}$ = the set of imaginary numbers.

Theorem : If f is a homomorphism from a group G to G' with kernal K, then K ◁ G (K normal sub group)

Theorem : Every Homomorphism image of a cyclic group is cyclic but not conversely.

Theorem : Every group is homomorphic to its quotient group

Theorem : Every homomorphic image of a group G is isomorphic to some quotient group of G.

*. ISOMORPHISM :

Homomorphism + one one + onto = Isomorphism

- $f(a * b) = f(a) \circ f(b)$ → Homomorphism
- If $f(a) = f(b) \Rightarrow a = b$ → one one
- $f(G) = G'$ → onto

} bijection

- Represented by $G \cong G'$.

*. CYCLIC GROUP :

- A group G is a cyclic Group if there exists an element $a \in G$, such that $G = [a]$ i.e. every element of G

EXTRA TOPIC :

- A UPC has 12 decimal digits
- the First digit identifies the product category
- The next five digits identifies manufacturer
- The following five digits identify particular product
- And last digit has check digit.

* The check digit is determined by sequence / congruence :

$$\Rightarrow 3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + 3x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}$$

IMP

$$\Rightarrow 3(\text{sum of digits in odd position}) + (\text{sum of digits in even position}) \equiv 0 \bmod 10$$

Example :

Suppose that the first 11 digits of UPC are 93764323341 What is the check digit.

Solution :

$$3(9) + 3 + 3(7) + 6 + 3(4) + 3 + 3(2) + 3 + 3(3) + 4 + 3(1) + x_{12} + x_2 \equiv 0 \pmod{10}$$

$$(27 + 3 + 21 + 6 + 12 + 3 + 6 + 3 + 9 + 4 + 3) + x_{12} \equiv 0 \bmod 10$$

$$107 + x_{12} \equiv 0 \pmod{10} \Rightarrow \boxed{x_{12} = 3}$$

- The USPS sells money order identified by an 11-digit $x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}$.

$$x_{11} = (x_1 + x_2 + \dots + x_{10}) \bmod 9$$

Example :

Determine the given 7405148962**3** is a valid USPS money order identification number ?

$= (7+4+0+5+1+4+8+9+6+2) \bmod 9$

$= 49 \bmod 9 = 4$

But Given last digit $x_{11} = 3 \Rightarrow 3 \neq 4$. So not a valid USPS number.

* . ISBN (International Standard Book Number) :

- All books are identified by an International Standard Book Number (ISBN-10), a 10 digit code with x_1, x_2, x_3, x_4, x_5 $x_6, x_7, x_8, x_9, x_{10}$, assigned by publisher.

Example : ISBN-10 : 0 - 19 - 94527 9 - 8 → check digit

(0 → language, 19 → publisher, 94527 → publishing company)

- This check digit is selected so that;

$$x_{10} = \sum_{i=1}^{9} i\, x_i \pmod{11}$$

[OR]

$$\sum_{i=1}^{10} i \cdot x_i = 0 \pmod{11}$$

Solved Example :

(a). The first 9 digits of ISBN-10 of the sixth edition book are 007288008. What is check digit.

Sol :

The check digit is determined by congruence

$$\sum_{i=1}^{10} i x_i = 0 \pmod{11}$$

$$x_{10} = [1(0) + 2(0) + 3(7) + 4(2) + 5(8) + 6(8) + 7(0) + 8(0) + 9(8)] \mod 11$$

$$x_{10} = 189 \pmod{11} = \underline{2}$$

(b) Is 0849301 49X a valid ISBN-10 ?

Sol:

$$\sum_{i=1}^{10} i \cdot x_i = 0 \pmod{11}$$

$$X = 1(0) + 2(8) + 3(4) + 4(9) + 5(3) + 6(0) + 7(1) + 8(4) + 9(9)$$

$$= 16 + 12 + 36 + 15 + 7 + 32 + 81 = 199 \mod 11$$

$$x_{10} = X = 199 \mod 11 = 1$$

But given $x_{10} = 10 \Rightarrow$ Not a valid ISBN