→ SETS: 1. Discrete
2. Continuous.

Discrete set :- A set of no:s that is bijective with the set of ~~real~~ natural numbers.

- Logic & Proofs:

- Declaration Statements: Statements that can be assigned true or false value.

Eg: 1> $2+2=4$

2> It is raining now in Hyd.

Non Eg :- 1>. $2+x=-1$. (Ambiguous).

$P(x)$: $2+x=-1$; $x \in \mathbb{R}$

$\exists x\ P(x)$ True. (quantifier).

$\forall x\ P(x)$. False. (for all not true)

2>. Will you eat ?

3>. Read the book.

} questions / orders.

- Compound Statements:

Statements that combine two or more declaration statements.

Eg: It will rain today & $2+2=4$.

Connectives

→ AND ∧.

p	q	p ∧ q
T	T	T
T	F	F
F	T	F
F	F	F.

→ OR . V (inclusive).

p	q	p V q
T	T	T
T	F	T
F	T	T
F	F	F

Exclusive OR $\bar{V}$

[only either one conditions must be true].

p	q	$p \bar{V} q$
T	T	F
T	F	T
F	T	T
F	F	F

Conditional $p \rightarrow q$.

1. If p, then q.
2. If p, q
3. p is "sufficient for q.
4. q is necessary for p
5. q. whenever p
6. p implies q.

$p \to q$

classmate
Date
Page

p	q	$p \to q$.	
T	T	T	
T	F	F	← (cheat).
F	T	T	
F	F	T.	

- **Biconditional:** $(p \rightleftharpoons q)$

$\approx (p \to q) \wedge (q \to p)$

p implies q & q implies p.

→ Converse, Inverse, Counterpositive.

$p \to q$.

1. $q \to p$
2. $\neg p \to \neg q$
3. $\neg q \to \neg p$.

Converse	$Q \to P$
Inverse	$\neg P \to \neg Q$
Counter +ve	$\neg Q \to \neg P$

To prove :-

- $p \to q$ & $\neg q \to \neg p$ same.
- converse & Inverse

converse (=) inverse

p	q	$p \to q$.
T	T	T
T	F	F
F	T	T
F	F	T

p	q	$\neg q \to \neg p$
T	T	T
T	F	F
F	T	T
F	F	T

- Equivalent Statements :-

~~P ∧ Q (=)~~

1. $P \wedge P \;(=)\; P$ } Idempotent law.
2. $P \vee P \;(=)\; P$ }

3. $P \vee Q \;(=)\; Q \vee P$ } commutative.

4. $(P \vee Q) \vee R \;(=)\; P \vee (Q \vee R)$ } Associative.
5. $(P \wedge Q) \wedge R \;(=)\; P \wedge (Q \wedge R)$ }

6. $P \wedge (Q \vee R) \;(=)\; (P \wedge Q) \vee (P \wedge R)$
7. $P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$

8. $\neg(P \wedge Q) \;(=)\; \neg P \vee \neg Q$ } De Morgan's laws
9. $\neg(P \vee Q) \;(=)\; \neg P \wedge \neg Q$ }

- Well Formed Formulae (WFF)
  Paranthesis placed correctly

1) A statement by itself is a WFF
2) Negation of a statement is a WFF
3) $(P \wedge Q)$, $(P \vee Q)$, $(P \rightarrow Q)$, $(P \rightleftharpoons Q)$
4) Any formulae using the above are WFF

Examples

1. $((P \vee Q) \rightarrow R)$ YES.

Should have paranthesis.

2. $P \wedge \neg Q \vee R \rightarrow Q \vee P$ NO.

$((P \wedge \neg Q) \vee ((R \rightarrow Q) \vee P))$ YES.

- **Substitution instance:**

A statement formula is a substitution instance of another formula if a statement is replaced by some formula throughout.

Eg:

1. $(P \rightarrow Q) \vee R$ is a substitution instance of $S \vee R$.
∴, S is replaced by $(P \rightarrow Q)$.

2. $(P \wedge \neg Q) \vee (Q \vee R)$ is a sub. instance of $(P \wedge \neg Q) \vee (S \vee R)$.

$P \vee \neg P \iff T$ (Tautology)

something $\vee$ (not something) $= T$.

P by $(\neg Q \vee R) \wedge (R \vee F) \wedge T$.

Examples:

① Show that :-

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

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

$(\neg P \wedge (\neg Q \wedge R)) \vee ((Q \vee P) \wedge R)$. Distributive

$((\neg P \wedge \neg Q) \wedge R) \vee ((Q \vee P) \wedge R)$.

$((\neg P \wedge \neg Q) \vee (Q \vee P)) \wedge R$.

Associative.

$((\neg P \wedge \neg Q) \wedge R) \vee ((Q \vee P) \wedge R)$.

$((\neg P \wedge \neg Q) \vee (Q \vee P)) \wedge R$.

Tautology.

$T \wedge R = R$!

② $((P \vee Q) \wedge \neg(\neg P \wedge (\neg Q \vee \neg R))) \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R)$ is a tautology.

$((P \vee Q) \wedge \neg(\neg P \wedge (\neg Q \vee \neg R))) \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R)$.

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

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

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

$(P \vee (Q \wedge \neg(\neg Q \vee \neg R))) \vee \neg P \wedge (\neg Q \vee \neg R)$.

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

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

$P \vee (Q \wedge R) \vee \neg P \wedge \neg(Q \wedge R)$.

~~$P \vee \neg P \vee R \wedge \neg(Q \wedge R)$~~

$P \vee (Q \wedge R) \vee \neg P \wedge \neg(Q \wedge R)$.

$P \vee (Q \wedge R) \vee \neg P \wedge (Q \vee R)$.

$(P \vee \neg P) (Q \wedge R) \wedge \neg(Q \vee R)$.

$= T$.

- **Duality law:**
Statement formula A and A^* are said to be dual of each other if

$\wedge \leftrightarrow \vee$

$T \leftrightarrow F$.

Eg: $A = (P \wedge (Q \vee R)) \wedge F$.

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

→ In General:

If:

$A(P_1, P_2, P_3, \ldots P_n)$

To get dual :-

1. Do $\neg A(P_1, P_2, P_3 \ldots)$
2. Do $\neg A(\neg P_1, \neg P_2, \ldots, \neg P_n)$.

- **Implication Laws:**

$P \rightarrow Q$ has a truth table.

$P \Rightarrow Q$ No truth table.

Definite T

sufficient to prove :-

$(P \wedge Q) \rightarrow P$ is tautology.

1 → for eg: $P \wedge Q \Rightarrow P$

To prove this.

$P \wedge Q \rightarrow P$ is a Tautology.

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

$(\neg P \vee \neg Q) \vee P$.

$\neg P \vee P \vee \neg Q$.

$T \vee \neg Q = T$.

2 → $P \wedge Q \Rightarrow Q$.

3 → $P \Rightarrow P \vee Q$.

$P \rightarrow P \vee Q$

$P \vee \neg(P \vee Q)$ $\neg P \vee (P \vee Q)$

$P \vee \neg P \wedge \neg Q$.

$T \wedge \neg Q = T$.

4 → $Q \Rightarrow P \rightarrow Q$.

$Q \rightarrow (P \rightarrow Q)$. $\neg Q \vee (P \rightarrow Q)$

$Q \vee \neg(P \rightarrow Q)$ $\neg Q \vee (\neg P \vee Q)$

$\neg Q \vee (\neg P \vee Q)$.

$\neg Q \vee Q \vee \neg P$.

$T \vee \neg P$ Tautology.

5 → $\neg(P \rightarrow Q) \Rightarrow P$.

$\neg(P \rightarrow Q) \rightarrow P$. $\neg(\neg(P \rightarrow Q)) \vee P$

$\neg(P \vee \neg Q) \vee \neg P$ $\neg(\neg(\neg P \vee Q)) \vee P$

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

$\neg P \vee Q \vee P = T$.

7. → $\neg(P \to Q) \Rightarrow \neg Q$.

$\neg(P \to Q) \to \neg Q$.

$\neg(P \vee \neg Q) \vee Q$.

$\neg P \wedge Q \vee Q$.

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

$\neg(\neg(\neg P \vee Q)) \vee \neg Q$

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

$\neg P \vee Q \vee \neg Q = T$.

8. → $P \wedge (P \to Q) \Rightarrow Q$

9. → $\neg Q \wedge (P \to Q) \Rightarrow \neg P$

10 → $\neg P \wedge (P \vee Q) \Rightarrow Q$.

11 → $(P \to Q) \wedge (Q \to R) \Rightarrow P \to R$.

12 → $(P \vee Q) \wedge (P \to R) \wedge (Q \to R) \Rightarrow R$.

* Theorem:

If $(H_1 \wedge H_2 \ldots \wedge H_m \wedge P) \Rightarrow Q$

then $(H_1 \wedge H_2 \wedge \ldots \wedge H_m) \Rightarrow P \to Q$

Proof: let $H_1 \wedge H_2 \ldots \wedge H_m$ be S.

If;

$(S \wedge P) \Rightarrow Q$ then $S \Rightarrow P \to Q$.

Ex: For the following.

1). If I work hard, I will get good grades.

i) Inverse

ii) Converse

iii) Contrapositive

i) ~~Inverse~~: P: I work hard
Q: I get good grades.

i) Inverse $\neg P \rightarrow \neg Q$

If I don't work hard I wont get good grades.

ii) Converse.

$Q \rightarrow P$

If I get good grades, I work hard.

iii) $\neg Q \rightarrow \neg P$.

If I will not get good grades I don't work hard.

- **Functionally complete set of connectives:**

1) $\wedge$ 2) $\vee$ 3) $\neg$ 4) $\rightarrow$, 5) $\rightleftarrows$

a) $\{\neg, \vee\}$ b) $\{\neg, \wedge\}$.

More connectives:

- NAND : NOT (AND (P, Q))
Denoted by $\uparrow$
$P \uparrow Q = \neg(P \wedge Q)$.

▲ NOR : NOT (OR (P, Q))

Denoted by ↓.

$P \downarrow Q = \neg(P \vee Q)$.

Eg: ① $\neg P = P \uparrow P$

$= \neg(P \wedge P)$

$= \neg P$.

② $P \wedge Q = (P \uparrow Q) \uparrow (P \uparrow Q)$

$= \neg(P \uparrow Q)$

$= \neg(\neg(P \wedge Q) = P \wedge Q$.

③ $P \vee Q = (P \uparrow P) \uparrow (Q \uparrow Q)$

$= \neg P \uparrow \neg Q$

$= \neg(\neg P \wedge \neg Q)$.

$= P \vee Q$.

→ Nand is :-

commutative but not associative.

$P \uparrow (Q \uparrow R) \not\equiv (P \uparrow Q) \uparrow R$

$P \uparrow (\neg Q \wedge R))$ $\quad$ $\neg(P \wedge Q) \uparrow R$

$\neg(P \wedge (\neg Q \wedge R))$ $\quad$ $\neg(\neg(P \wedge Q) \wedge R)$

$\neg P \vee \neg(\neg Q \wedge R)$. $\quad$ $(P \wedge Q) \vee \neg R$.

$\neg P \vee (Q \vee \neg R)$ $\quad$ $\neg R$

Q: Express $P \rightarrow (\neg P \rightarrow Q)$ in terms of

$P \rightarrow (\neg P \rightarrow Q)$.

P

$((P \uparrow Q) \uparrow (P \uparrow Q)) \uparrow (P \uparrow Q)$

Q: Express $P \uparrow Q$ in terms of $\downarrow$

$P \uparrow Q : \neg(P \wedge Q)$

$= \neg P \vee \neg Q$

$(P \downarrow P) \downarrow (Q \downarrow Q)) \downarrow ((P \downarrow P) \downarrow (Q \downarrow Q))$

$((P \downarrow P) \downarrow (Q \downarrow Q)) \downarrow ((P \downarrow P) \downarrow (Q \downarrow Q))$.

NORMAL FORMS:

Product ≡ conjunction

Sum ≡ Disjunction.

→ Let $A(P_1, P_2, \ldots P_n)$ be a statement formula then A is defined to be identically true if A is true regardless of truth values of $P_1, P_2 \ldots P_n$.

→ Let $A(P_1 P_2 \ldots P_n)$ be a statement formula. then A is defined to be identically false if A is false regardless of truth values of $P_1, P_2 \ldots P_n$.

→ Let $A(P_1, P_2 \dots P_n)$ be a statement formula then A is said to be satisfiable if A takes value true atleast for one combination of truth values of $P_1 P_2 \dots P_n$.

→ **Elementary Product:**
A product of the variables and their negations in a formula is called elementary product.

Eg:
- $\neg P \wedge Q$ → Yes.
- $\neg P \wedge Q \vee R$ → NO!
- $\neg P \wedge \neg(Q \vee R) = \neg P \wedge \neg Q \wedge \neg R$ → Yes.

→ **Elementary Sum:**
A sum of the variables & their negations in a formula is called elementary sum.

→ **Factor:**
Any part of an elementary sum or product which is itself an el. sum/product is called a factor.

Eg: Find factors of :-

Q: $\neg Q \wedge P \wedge \neg P$

A: $\neg Q$, $\neg Q \wedge P$, $P \wedge \neg Q$,

★ A necessary condition for an elementary product to be identically false is that it contains at least one pair of factors in which one is the negation of the other.

Eg: $P \wedge \neg Q \wedge R \wedge \neg P \wedge Q \wedge R \wedge \neg R \wedge \forall x, Y \wedge \neg X$.
We have $P \wedge \neg P$, a factor which is F.

★ A necessary condition for an elementary sum to be identically true is that it contains at least one pair of factors in which one is a negation of the other.

→ Disjunctive normal forms (DNF).
A formula which is equivalent to a given formula & which consists of sums of elementary products is called disjunctive normal form.

→ Conjunctive Normal forms (CNF).
A formula which is equivalent to a given formula & which consists of product of elementary sums.

Ex: Obtain DNFs :-

a) $P \wedge (P \rightarrow Q)$ $\neg(\neg P \vee Q)$

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

b) $\neg(P \vee Q) \rightleftarrows (P \wedge Q)$

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

Step 1: If the negation to the formula or a part of a formula and not to the variables appearing in it, then by using De Morgan's law law an equivalent formula can be obtained where negation applies only to the variable.

Eg: Obtain DNF

$\neg(P \rightarrow Q) \vee R$

$\neg(\neg P \vee Q) \vee R$

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

Step 2: There may be some parts that are still POS, by repeated application of distributive law, we can obtain the desired form.

Eg: $P \wedge (P \rightarrow Q)$

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

Eg: $\neg(P \vee Q) \rightleftarrows (P \wedge Q)$

~~$(\neg P \wedge \neg Q) \vee (P \wedge P)$~~.

$(\neg P \vee Q) \rightarrow (P \wedge Q)) \wedge ((P \wedge Q) \rightarrow \neg(P \vee Q))$.

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

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

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

$(P \vee Q) \wedge (\bar{P} \vee \bar{Q})$

$(P \vee Q \vee (P \wedge Q)) \wedge ((\bar{P} \wedge \bar{Q}) \vee (\bar{P} \vee \bar{Q}))$

$(P \vee ((Q \vee P) \wedge (Q \vee Q))) \wedge (((\bar{P} \vee \bar{P}) \wedge (\bar{Q} \vee \bar{P})) \vee \bar{Q})$

$(P \vee ((Q \vee P) \wedge Q)) \wedge ((\bar{P} \wedge (\bar{Q} \vee \bar{P})) \vee \bar{Q})$

$[(P \vee Q \vee P) \wedge (P \vee Q)] \wedge [((\bar{P} \vee \bar{Q}) \wedge (\bar{Q} \vee \bar{P} \vee \bar{Q})]$

$[(P \vee Q) \wedge (P \vee Q)] \wedge [(\bar{P} \vee \bar{Q}) \wedge ($

• PRINCIPAL DNF :

→ Minterms :

$P \wedge Q$, $P \wedge \neg Q$, $\neg P \wedge Q$, $\neg P \wedge \neg Q$.

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

$\therefore \neg(P \to Q) \vee P = (P \wedge Q) \vee (P \wedge \neg Q)$.

Q: $\neg(P \rightleftarrows Q) \wedge Q$.

$\neg((P \to Q) \wedge (Q \to P))$

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

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

P	Q	$P \to Q$	$Q \to P$	$\neg(P \rightleftarrows Q) \wedge Q$
T	T	T	T	F
T	F	F	F	F
F	T	F	F	T
F	F	T	T	F

∴ Ans :- $\neg P \wedge Q$

▲ To obtain PDNF (without truth table).

1). Replace conditionals & biconditionals by $\neg$, $\wedge$ or $\vee$.

2). Apply negations to variables by De Morgans Laws.

3). Apply distributive law.

4). Any element product which is F is dropped.

5). Minterms are obtained in disjunction by introducing the missing factors.

6). Identical minterms in disjunction are deleted.

Eg: a) $\neg P \vee Q$.

$(\neg P \ldots) \vee (Q \ldots)$

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

$= [\neg P \wedge (Q \vee \bar{Q})] \vee [Q \wedge (P \vee \bar{P})]$

$= (\bar{P} \wedge Q) \vee (\bar{P} \wedge \bar{Q}) \vee (Q \wedge P) \vee (Q \wedge \bar{P})$ ↳ redundant

$= (Q \wedge P) \vee (\bar{P} \wedge \bar{Q}) \vee (Q \wedge \bar{P})$.

Eg: Obtain PDNF of :-

$(\neg P \rightarrow R) \wedge (Q \rightleftarrows P)$. without Truth table.

$(\neg(\neg P) \vee R) \wedge ((Q \rightarrow P) \vee (P \rightarrow Q))$

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

$(P \vee R) \wedge (Q \vee \neg Q \vee P \vee \neg P)$.

$(P \vee R) \wedge (T)$.

$(P \vee R) \wedge T$

$(P \wedge T) \vee (R \wedge T)$.

$(P \wedge (Q \vee \neg Q)) \vee (R \wedge (Q \vee \neg Q))$.

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

$(P \wedge Q \wedge (R \vee \bar{R})) \vee (P \wedge \neg Q \wedge (R \vee \bar{R})) \vee (R \wedge Q \wedge (P \vee \bar{P})) \vee (R \wedge \bar{Q} \wedge (P \vee \bar{P}))$

$(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \bar{R}) \vee (P \wedge \bar{Q} \wedge R) \vee (P \wedge \bar{Q} \wedge \bar{R}) \vee (R \wedge Q \wedge P) \vee (R \wedge Q \wedge \bar{P}) \vee (R \wedge \bar{Q} \wedge P) \vee (R \wedge \bar{Q} \wedge \bar{P})$

$(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \bar{R}) \vee (P \wedge \bar{Q} \wedge R) \vee ($

→ $(\neg P \wedge \neg Q \wedge R) \vee (P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R)$

TUTORIAL - 1.

1). Valid Statements :-

1. Invalid - Order.
2. Invalid - Point of view.
3. Valid.
4. Invalid - Question.
5. Invalid - Opinion.
★ 6. Valid.
7. Invalid - Contradiction.
8. Invalid - Opinion.
9. Invalid - contradiction.
10. Invalid - Order
11. Invalid order.
12. Invalid - Question
13. Invalid - Ambiguity.
14. Invalid - "
15. " Question.
16. " Request.
17. " Question.
18. Valid.
19. Invalid. Ambiguity.
20. "
"
"
"
"

Find PDNF of :- $\neg S$.

$\neg S = (\neg P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R)$

for 3 inputs P, Q, R.

Minterms :- $P \wedge Q \wedge R$, $P \wedge Q \wedge \neg R$, $\neg P \wedge Q \wedge R$, $P \wedge \neg Q \wedge R$
$P \wedge \neg Q \wedge \neg R$, $\neg P \wedge \neg Q, R$, $\neg P \wedge Q, \neg R$, $\neg P \wedge \neg Q, \neg R$.

Maxterms: → duals of minterms.

- Theory of Inference :-

Deduction / formal proof :-
when a conclusion is derived from a set of premises (given set of statements) by using accepted set of reasoning

~ In a formal proof, every rule of inference that is used at any stage in the derivation is acknowledged.

Q: When is conclusion admitted to be true?

A: When the premises are accepted to be true and the reasoning used in deriving the conclusion from the premised follows certain accepted ~~to~~ rule of logical inference. We say that from a set of premises: $H_1, H_2, H_3 \ldots H_m$ a conclusion C follows logically H

$$H_1 \wedge H_2 \wedge H \ldots\ldots H_n \Rightarrow C$$

Rules of Inference:

Rule P: A premise may be ~~use~~ introduced at any point in the derivation.

Rule T: A formula S may be introduced in the derivation if S is tautologically implied by any or more of preceeding formulae in the derivation.

Implication Table:

1. $P \wedge Q \Rightarrow P$ } simplification
2. $P \wedge Q \Rightarrow Q$ }
3. $P \Rightarrow P \vee Q$ } addition
4. $Q \Rightarrow P \vee Q$ }
5. $\neg P \Rightarrow P \vee Q$
6. $Q \Rightarrow P \rightarrow Q$

7. $\neg(P \to Q) \Rightarrow P$

8. $\neg(P \to Q) \Rightarrow \neg Q$

9. $P, Q \Rightarrow P \wedge Q$.

10. $\neg P, P \vee Q \Rightarrow Q$.

11. $P, P \to Q \Rightarrow Q$.

12. $\neg Q, P \to Q \Rightarrow \neg P$.

13. $P \to Q, Q \to R \Rightarrow P \to R$. (hypothetical)

14. $P \vee Q, P \to R, Q \to R \Rightarrow R$

Eg 1: Show that R is a valid inference from the premise

$P \to Q$, $Q \to R$, and P.

(1)	P	Rule P
(2)	$P \to Q$	Rule P.
(3)	Q	Rule T, I_{11} (1), (2).
(4)	$Q \to R$	Rule P,
(5)	R	Rule T, I_{11}, (3),

Eg 2: Show that RVS follows from CVD, $(CVD) \to \neg H$, $\neg H \to (A \wedge \neg B)$ and $(A \wedge \neg B) \to (RVS)$.

(1)	CVD	Rule P.
(2)	$(CVD) \to \neg H$	Rule P.
(3)	$\neg H$	Rule T, I_{11}, (1), (2)
(4)	$\neg H \to (A \wedge \neg B)$	Rule P.

(5) $A \wedge \neg B$ Rule T I_{11}, (3), (4).

(6) $(A \wedge \neg B) \rightarrow (R \vee S)$ Rule P

(7) $R \vee S$ Rule T, I_{11}, (6), (5).

∴, RVS is valid!
(I13 can also be used)

Eg 3: Show that SVR is tautologically implied by $(P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow S)$.

Ⓐ: ⚠ Convert the one that's not → to →.

∴, $(\neg P \rightarrow Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow S)$.

$(\neg P \rightarrow Q) \wedge (Q \rightarrow S) \wedge (P \rightarrow R)$.

→ [$P \vee Q$ (∈) step 1]

(1) $(\neg P \rightarrow Q) \wedge (Q \rightarrow S) \wedge (P \rightarrow R)$ Rule P.

(2) $(\neg P \rightarrow Q) \wedge (Q \rightarrow S)$ Rule T, I_1, (1).

(3) $(\neg P \rightarrow S)$ Rule T I_{13} (2).

(4) $(\neg P \rightarrow S) \wedge (P \rightarrow R)$ Rule P.

(5) $(\neg S \rightarrow P) \wedge (P \rightarrow R)$ Equivalence rel.

(6) $(\neg S \rightarrow R)$ Rule T I_{13} (5).

(7) $(S \vee R)$.

Eg 4: Show that $R \wedge (P \vee Q)$ is a valid conclusion from $P \vee Q$, $Q \rightarrow R$, $P \rightarrow M$ & $\neg M$.

(1) $\neg M$ Rule P

(2) $P \rightarrow M$ Rule P

(3) ~~$P \vee Q$~~ ~~Rule P~~.

(3)	$\neg P$	Rule T. I_{12} (1), (2)
(4)	$P \vee Q$	Rule P.
(5)	Q	Rule T I_{10} (3), (4)
(6)	$Q \rightarrow R$.	Rule P.
(7)	R	Rule T I_{11}, (6), (5)
(8)	$P \vee Q$	Rule P.
(9)	$R \wedge (P \vee Q)$	Rule T, I_9 (7), (8)

★ **Rule CP :-**

If we can derive S from R and a set of premise, then we can derive $R \rightarrow S$ from the set of premise alone.

$(P \wedge R) \rightarrow S \iff P \rightarrow (R \rightarrow S)$.

Rule CP is also called deduction.

Rule CP is used when the conclusion is of the form $\boxed{R \rightarrow S}$ (conditional)

ie: if we want to prove $R \rightarrow S$ then add R as an additional premise & prove S.

Eg: Show that $R \rightarrow S$ can be derived from

$P \rightarrow (Q \rightarrow S)$, $\neg R \vee P$, Q

(1)	$\neg R \vee P$	Rule P
(2)	$R \rightarrow P$	($\in$)
(3)	R	Rule CP.
4)	P	Rule T, I_{11}, (2), (3)

5)	$P \rightarrow (Q \rightarrow S)$	Rule P.
6).	$(Q \rightarrow S)$	Rule T, I_{II} (4), (5).
7).	Q	Rule P.
8) .	S	Rule T I_{II}, (6), (7).

Eg: If A works hard, then either B or C will enjoy themselves. If B enjoys himself, then A will not work hard. If D enjoys himself, C will not.
[Therefore If A works hard then D will not enjoy himself].

A : A works hard

B/C/D : B/C/D enjoys.

$A \rightarrow (B \vee C)$, $B \rightarrow (\neg A)$, $D \rightarrow \neg C$

Validate $A \rightarrow \neg D$.

1)	A	CP Rule.
2).	$A \rightarrow (B \vee C)$	Rule P.
3)	$(B \vee C)$	Rule T, I_{II}, (1), (2).
(4)	$(\neg B \rightarrow C)$	(E).
(5)	$B \rightarrow \neg A$.	Rule P.
(6)	$\neg B \rightarrow A$	(E).
(7)	.	

1)	A	Rule CP.
2)	$A \rightarrow (B \vee C)$	Rule P.
3)	$B \vee C$	Rule T I_{11} (1) (2)
4)	$A \rightarrow \neg B$	Rule P (3)
5)	$\neg B$	Rule T I_{11}
6)	C	I_{10}
	$C \rightarrow \neg D$	
	$\neg D$	

- Consistency Of Premise and indirect method of proof :-

A set of families $H_1, H_2 \ldots H_n$ is said to be consistent if their conjunction has truth value T for some assignment of truth value of $H_1, H_2 \ldots H_n$.

A set of formulae $H, H_2 \ldots H_D$ is said to be inconsistent if for any assignment of truth values $H_1, H_2 \ldots H_n$ $H_1 \wedge H_2 \wedge H_3 \ldots H_n$ is false.

→ Method of Contradiction :-

To prove : $H_1 \wedge H_2 \wedge \ldots \wedge H_m \Rightarrow C$

By contradiction prove

$H_1 \wedge H_2 \wedge \ldots \wedge \neg C \Rightarrow F$

Eg: Show that $\neg(P \wedge Q)$ follows from $\neg P \wedge \neg Q$.

Sol: $H_1 = \neg(P \wedge Q)$ $\quad \neg P \wedge \neg Q$.

$C = \neg P \wedge \neg Q$ $\quad \neg(P \wedge Q)$

∴, we need to prove.

$H_1 \Rightarrow C$.

We wish to prove this by method of contradiction. We assume that $\neg C$ as an additional premise ie :-

$H_2 = \neg C = P \wedge Q$.

∴, Claim $H_1, H_2 \Rightarrow F$ a contradiction.

1)	$\neg P \wedge \neg Q$.	P
2)	$P \wedge Q$	P
3)	P	T I_1, (2)
4)	$\neg P$	T, I_1 (1).
5)	$P \wedge \neg P$	T I_9 (3) (4).

which is a contradiction Hence C proved.

★ $H_1 \wedge H_2 \wedge H_3 \ldots \Rightarrow C$.

$\underbrace{H_1 \wedge H_2 \wedge H_3 \ldots}_{\text{Hypothesis considered T}} \wedge (\neg C) \Rightarrow F$.

$\neg C$ → F

∴, $\neg C = F$

$\Rightarrow C = T$.

Eg: Show that the following are inconsistent.

1) If Jack misses classes through illness, then he fails high school. (P) → Q.

P: Jack misses class through illness.
Q: He fails high school.

2) If Jack fails high school he is uneducated ← R. Q

3) If Jack reads a lot of books, then he is not uneducated. ← ¬R. S.

4) Jack misses many classes through illness & reads a lot of books. P, S.

P → Q , Q → R , ~~P ∧ S~~ , S → ¬R

~~P ∧ Q~~ P ∧ S.

1) P → Q
2) Q → R
3) P → R
4) S → ¬R
5) P ∧ S
6) S
7) ~~Q~~ R

Rule P
Rule P
Rule T I 1, 2.
Rule P
Rule P
Rule T I 3, 6.

1).	$P \rightarrow Q$	Rule P
2)	$Q \rightarrow R$	Rule P.
3).	$P \rightarrow R$	Rule T I_{13} (1), (2).
4).	$P \wedge S$	Rule P.
5)	P	Rule T I_2 (4).
6).	R	Rule T, I_{11} (3) (5).
7).	$S \rightarrow \neg R$.	Rule P.
8)	S	Rule I_1, (4).
9).	$\neg R$	Rule T.
10).	$R \wedge \neg R$	Rule T.

$\therefore$ A contradiction.

PREDICATE CALCULUS :-

If x is even, $x+1$ is odd.

John is a bachelor

Smith is a bachelor.

"is a bachelor is a predicate".

$B(x)$: x is a bachelor.

$B(x)$ is a statement, x is object variable.

A : all humans are mortal.

B : John is a human.

C : John is mortal.

Symbolize statement A :-

For all x, if x is a human being then x is mortal

Define :

$H(x)$: x is a human

$M(x)$: x is mortal.

$$\forall(x)\ (H(x) \rightarrow M(x)).$$

Eg: Every non-zero integer is either a positive integer or negative integer

$I(x)$: x is a non zero int.

$P(x)$: x is a positive integer

$N(x)$: x is a negative integer

$$\forall(x)\ (I(x) \rightarrow P(x)\ \bar{V}\ (N(x))).$$

- Well formed formulae for Predicate calculus.

(1) An atomic formula is a well formed formula.

(2) If A is a WFF, then $\neg A$ is a WFF

③ If A & B are WFF then $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $(A \rightleftarrows B)$ are WFF.

④ If A is a WFF & x is any variable then $\forall x\, A(x)$ & $\exists x\, (A(x))$ WFF.

⑤ Only those formulae obtained using ① to ④ are WFF.

Eg:

① There exist a man.
② Some men are clever
③ Some real no:s are rational.

1. There exists an x such that x is man
2. There is atleast one x such that x is a man & x is clever.
3. There exits at least one x such that x is real & x is rational.

→ 1 $(\exists x)(M(x))$.
→ 2 $(\exists x)(M(x) \wedge C(x))$.
→ 3 $(\exists x)(R(x) \wedge Q(x))$.

FREE & BOUND VARIABLE :-

Given a formula containing

$(\forall x) P(x)$ or $(\exists x) P(x, y)$.

[x is bound, y is free]

Any occurance of x in an x-bound part of a formula is called a bound occurance of x. While any occurance of x or of any variable that is not a bound occurance, is called a free occurance

Eg 1: $\forall(x)\,(P(x,y))$.

Here x is a bound occurance & y is a free occurance.

Eg 2: $(P(x) \rightarrow Q(x))$.

x is a free occurance.

Eg 3: $\forall(x)\,(P(x) \rightarrow R(x)) \vee \forall(x)\,(P(x) \rightarrow Q(x))$.

x is bound.

Eg 4: $P(x) \rightarrow (\exists y)\,R(x,y)$.

x is free, y is bound.

Eg 5: $(\exists x)(P(x) \wedge Q(x))$

x is bound.

Eg 6: $(\exists(x))\,P(x) \wedge Q(x)$.

x is bound; x is free.

TUTORIAL - 2.

Q: Well formed ?

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

Yes.

b). $((P \rightarrow (\sim P)) \longrightarrow \sim P)$.

No.

c). $((\sim Q \wedge P) \wedge Q$

No.

d). $((\sim P \rightarrow Q) \rightarrow (Q \rightarrow P)))$

No.

Q: Show the following :-

1). $P \rightarrow Q \Rightarrow P \rightarrow (P \wedge Q)$.

T.P.

$(P \rightarrow Q) \rightarrow (P \rightarrow (P \wedge Q))$ is a tautology.

$(\neg P \vee Q) \rightarrow (\neg P \vee (P \wedge Q))$.

$(\neg P \vee Q) \rightarrow (\neg P \vee P) \wedge (\neg P \vee Q)$.

$(\neg P \vee Q) \rightarrow (\neg P \vee Q)$.

$\neg(\neg P \vee Q) \vee (\neg P \vee Q)$.

T.

a). $(P \to Q) \to Q \Rightarrow P \vee Q$.

To prove.

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

$[(\neg P \vee Q) \to Q] \to [P \vee Q]$.

$[\neg(\neg P \vee Q) \vee Q] \to [P \vee Q]$.

$[(P \wedge Q) \vee Q] \to P \vee Q$.

~~$[P \wedge Q]$~~ $[(P \vee Q) \wedge (Q \vee Q)] \to P \vee Q$.

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

T.

Q: Prove :-

① $P \to (Q \to P) \iff \sim P \to (P \to Q)$.

$\neg P \vee (Q \to P)$.	$\propto P \vee (P \to Q)$
$\neg P \vee (\neg Q \vee P)$.	$P \vee (\neg P \vee Q)$
$\neg P \vee \neg Q \vee P$	$P \vee \neg P \vee Q$
$\neg P \vee P \vee \neg Q$	$T \vee Q$
$T \vee \neg Q$	$T \vee Q$
$T \vee \neg Q$.	
T	T.

$\neg Q \to$

② $P \to (Q \vee R) \iff (P \to Q) \vee (P \to R)$.

$\neg P \vee (Q \vee R)$	$(\neg P \vee Q) \vee (\neg P \vee R)$.
$\neg P \vee Q \vee R$	$\neg P \vee \neg P \vee Q \vee R$
$\neg P \vee Q \vee R$	$\neg P \vee Q \vee R$

③. $\sim(P \leftrightarrow Q) \iff (P \wedge \sim Q) \vee (\sim P \wedge Q)$.

$\sim((P \to Q) \wedge (Q \to P))$ ⇔ $(P \wedge \sim Q) \vee (\sim P \wedge Q)$.

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

~~$\sim\sim P \vee \sim P$~~ ~~$P \vee \sim P$~~

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

Proved.

Q: Reduce.

① contains only $\wedge$ $\sim$.

$\sim(P \leftrightarrow (Q \to (R \vee P)))$.

$\sim(P \leftrightarrow (\neg Q \vee R \vee P))$.

$\sim((P \to (\neg Q \vee R \vee P)) \wedge ((\neg Q \vee R \vee P) \to P))$.

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

~~$\sim(T \wedge (Q \wedge \neg R \wedge \neg P) \vee P)$~~

$\sim(P \to (Q \vee R \vee P) \wedge (Q \wedge \neg R \wedge \neg P)$.

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

② $((P \vee Q) \wedge R) \to (P \vee R)$.

$\neg((P \vee Q) \wedge R) \vee (P \vee R)$.

$(\neg(P \vee Q) \wedge \neg R) \vee (P \vee R)$.

$(\neg P \wedge \neg Q \wedge \neg R) \vee (P \vee R)$.

~~$\neg\neg(\neg P$~~ $(\neg P \wedge \neg Q \wedge \neg R) \vee P \vee R$.

$\neg(\neg(\neg P \wedge \neg Q \wedge \neg R) \wedge (\neg P \wedge \neg R))$.

Q: Show that $\{\wedge, \vee\}$ is not functionally complete.

Let A be any statement :-

$A \Rightarrow A_1 \wedge \ldots \vee \ldots A_K \ldots A_n$.

Can be represented as minterms

ie: $(\wedge) \vee (\wedge) \vee (\wedge)$

lets take $A_1, A_2 \ldots A_n$.

If $\{\wedge, \vee\}$ is functionally complete then I can get 'F' for some statement formula 'G'.

Assume all $A_1, A_2 \ldots A_n$ are true.

We know that any statement formula can be reduced to SOP or POS, so we will get

~~ie: $(A_1 \wedge A_2) \vee (A_i \wedge A_{i+1})$~~

ie: $G = (A_i \wedge A_{i+1}) \vee (A_4 \wedge A_5)$.

Since all A terms are true, we will always get T & F will not be obtained.

→ If there is any part of formula with $\forall(x)(A(x))$ and $\exists(x)\, A(x)$, then it is called x-bound part. We say that x is bounded. If x is not bounded its

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

bounded.

b) $\forall(x)\ (P(x) \rightarrow Q(x)) \vee R(x)$

bounded. free.

$\forall(x)\ (P(x) \rightarrow Q(x)) \vee (\exists(x)\ R(x))$

bounded. bounded

- **Statements to Predicate:**

1. Someone from your school visited Agra.

S(x) : "someone from your school".

A(x) : "someone visited Agra

$\exists(x)\ (S(x) \wedge (A(x))$.

(If all) :-

$\forall(x)\ (S(x) \rightarrow A(x))$.

2. Everyone has exactly one fav language.

P(x, y) : x has a favourite language y.

z : z is a language.

$(\forall(x))(\exists y)\ P(x,y) \wedge ((\forall z)(z \neq y) \rightarrow \neg P(x,z))$.

→ Universe Of Discourse.
(Domain of the variables).

&

eg: $S(a,b)$ a is divisible by b

Universe of a, b :-

(1) $\{3, 5, 10, 11\}$. Here we can also set the (universe)

$\forall(x)\ S(a,b)$ False.

$\exists(x)\ S(a,b)$ True.

(2) $\{0\}$.

$\forall(x)\ S(a,b)$ False.

★ Using De Morgans :

1). $\neg \forall(x)\ P(x) = \exists(x)\ \neg P(x)$

$\neg \exists(x)\ P(x) = \forall(x)\ \neg P(x)$.

Eg: Not all drivers obey the speed limit

Negation ⊙ All drivers obey the speed limit

● Theory Of Inference for Predicate :-

① Rule VS (Universal specification).

It is used to conclude $P(a)$ is true when a is any particular number of universe of discourse given that $\forall(x)\ P(x)$ is true.

② Rule UG (Universal Generalization)

It states that $\forall(x)\, P(x)$ is true when the given premise $P(a)$ is true. Here a must be arbitrary.

Caution: If $P(a)$ is true only for some a then $\forall(x) P(x)$ may not be true.

ie: $P(a)$ must be true for any a in universe.

③ Rule ES [Existantial Specification]

It permits us to conclude that there exists an element a in the universe for which $P(a)$ is true. Here selected a cannot be arbitrary. But it should be an element such that $P(a)$ is true.

$\exists(x) P(x)$

$\therefore P(a)$.

④ Rule EG (Existantial General)

It is used to conclude that $(\exists x) P(x)$ is true when a particular element a exists in the universe for which $P(a)$ is true.

$P(a)$

$\therefore \exists(x) P(x)$

Eg: $S(a, b)$: a is divisible by b

$U = \{3, 5, 9, 13\}$.

$\exists(x) S(9, 3)$ is true.

Deriving :-

1) $\exists(x)\ S(9, 3)$ Start with this premise.

(2) $S(y, 3)$ ES

(3) $\forall(x)\ S(y, 3)$ UG (FALSE)

incorrect !

Here y is not arbitrary.

Q: Prove that

$$\forall(x)(P(x) \to Q(x)) \wedge \forall(x)(Q(x) \to R(x)) \Rightarrow \forall(x)(P(x) \to R(x))$$

Sol.

1)	$(\forall x)(P(x) \to Q(x))$	P
2)	$(\forall x)(Q(x) \to R(x))$	P
3)	$P(a) \to Q(a)$	US (1)
4)	$Q(a) \to R(a)$	US (2)
(5)	$P(a) \to R(a)$	T, I_{13} (3), (4)
(6)	$(\forall x)(P(x) \to R(x))$	UG

Q: $(\exists x)(P(x) \wedge Q(x)) \Rightarrow (\exists x)P(x) \wedge (\exists x)Q(x)$.

(1)	$(\exists x)(P(x) \wedge Q(x))$	P
(2)	$P(a) \wedge Q(a)$	ES (1)
(3)	$P(a)$	I_1, T (2).
4)	$Q(a)$	I_2, T (3).
5)	$(\exists x)P(x)$	EG
6)	$(\exists x)Q(x)$	EG
7)	$(\exists x)P(x) \wedge (\exists x)Q(x)$	T, I_9, (5), (6).

Q: $(\exists x)(P(x)) \wedge (\exists x)(Q(x)) \Rightarrow (\exists x)(P(x) \wedge Q(x))$

1)	$(\exists x)(P(x)) \wedge (\exists x) Q(x)$	P.
2)	$(\exists x) P(x)$	I_1 (1)
3)	$(\exists x) Q(x)$.	I_2 (1).
4).	$P(a)$	ES (2)
5)	$Q(b)$	ES (3).

∴, this cannot be concluded.

Q: Show that :-

a) $(\exists x)(P(x) \wedge S(x)) \rightarrow (\forall y)(M(y) \rightarrow W(y))$

b) $(\exists y)(M(y) \wedge \neg W(y))$.

1) $(\exists x)(P(x) \wedge S(x))$ P

2) $P(a) \wedge S(a)$ ES.

3) $P(a)$

4) $S(a)$

implies :- $(\forall x)(P(x) \rightarrow \neg S(x))$

1). $(\exists x)(P(x) \wedge S(x)) \rightarrow (\forall y)(M(y) \rightarrow W(y))$.

2) $(\exists y)(M(y) \wedge \neg W(y))$ P.

3) $M(a) \wedge \neg W(a)$ ES.

4). $M(a)$ T, I_1 (3).

5) $\neg W(a)$ $T\ I_2$ (3).

6) $M(a) \rightarrow \neg W(a)$ T, I_6 (4), (5).

7). $(\forall x)(M(x) \rightarrow \neg W(x))$

Proof Techniques :-

(1) **Direct Proof**

$P \Rightarrow P_1 \Rightarrow P_2 \Rightarrow \dots \Rightarrow Q.$ $\left(\begin{matrix} x>0 \\ \Rightarrow x^2>0 \end{matrix}\right)$.

(2). **Contradiction:-**

If to prove :- $P \Rightarrow Q$.

Proving $P \wedge \neg Q \Rightarrow F$ is sufficient.

(3) **Countrapositive :-**

Prove : $\neg Q \Rightarrow \neg P$ $\left(\begin{matrix} n^2 \text{ is odd} \\ \Rightarrow n \text{ is odd} \end{matrix}\right)$

(4) **Induction :-**

Applied mostly to natural nos:

- Base case $Q(b)$ is true ; $b \in \mathbb{N}$
- Induction hypothesis.
  ↓
  Assume $Q(k)$ is true for some $k \in \mathbb{N}$.
  To prove $Q(k+1)$ is also true.

Parity Proofs.

Eg: Prove that there are infinitely many primes.

Proof: $T \Rightarrow Q$.

Contradiction

$\neg Q$: There are finitely many primes.
Let those finitely many primes be
$p_1, p_2, p_3 \dots p_n$.

Consider : $N = p_1 p_2 p_3 \dots p_n + 1$. — (*)

$m \mid a$, $m \mid b$

$m \mid ax + by$; $x, y \in Z$.

(i) $N > P_i$; $i = 1, 2, 3, \ldots, n$.

$\Rightarrow$ N is composite

$\Rightarrow$ P_i divides N for some i.

from $\circledast$,

$$1 = N - P_1 P_2 P_3 \ldots P_n .$$

If P_i divides $N - P_1 P_2 P_3 \ldots P_n$

$\Rightarrow$ P_i divides 1.

$\therefore$, $P_i = \pm 1$.

But P_i is a prime and ± 1 is not a prime.

Eg: Prove that $\sqrt{2} + \sqrt{5}$ is irrational.

Assume $\sqrt{2} + \sqrt{5}$ is rational.

ie: $\sqrt{2} + \sqrt{5} = \frac{p}{q}$ $q \neq 0$ p, q co-primes

Squaring ; $2 + 5 + 2\sqrt{10} = \frac{p}{q}$.

$$2\sqrt{10} = \frac{p}{q} - 7$$

$$\sqrt{10} = \frac{\frac{p}{q} - 7}{2}$$

$\sqrt{10} = p/q$.

$q^2 10 = p^2$.

$10 \mid p^2$ $2 \mid p^2$, $5 \mid p^2$

$2 \mid p$, $5 \mid p$.

$\therefore$, $10 \mid p$

$\therefore$, $10 \mid q$.

RHS is rational but LHS is irrational.

$\therefore$, This is a contradiction.

$\therefore$, $\sqrt{2} + \sqrt{5}$ is irrational.

Q: Prove $1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$ by PMI

Step 1: P(1) is true ... to prove

$P(1) = 1^2 = 1$

$\frac{1(1+1)(1+1)}{6} = 1$

LHS = RHS
Hence true.

Step 2: Assume P(K) is true for some $K \in N$

ie: $1^2 + 2^2 + \dots + K^2 = \frac{K(K+1)(2K+1)}{6}$ —①

To prove P(K+1) is also true.

ie: $\underbrace{1^2 + 2^2 + \dots + K^2} + (K+1)^2 = \frac{(K+1)(2K+3)(K+2)}{6}$

Sub from ①; $\frac{K(K+1)(2K+1)}{6} + (K+1)^2$

$= \frac{K(K+1)(2K+1) + 6(K+1)^2}{6}$

$= \frac{(K+1)}{6}[2K^2 + K + 6K + 6]$

$= \frac{(K+1)}{6}[2K^2 + 7K + 6]$

$= \frac{K+1}{6}[2K^2 + 4K + 3K + 6]$

$= \frac{K+1}{6}[2K(K+2) + 3(K+2)]$

$= \frac{(K+1)(K+2)(2K+3)}{6} = RHS$

∴, P(K+1) is also true.

Q: Prove that $\bigcup_{i=1}^{\infty} A_n$ is countable if $A_1, A_2, \ldots$ are countable.

Step 1: A_1 is countable.

And $A_1 \cup A_2$ $n=2$ is a countable union of 2 countable sets.

Step 2: let ~~$A_n = A_{n+1}$~~ the statement be true for some $K \in N$.

ie: $\bigcup_{i=1}^{K} A_i$ is ~~true~~ countable.

To prove $\bigcup_{i=1}^{K+1} A_i$ is countable.

We have:-

$$\bigcup_{i=1}^{K+1} A_i = \left(\bigcup_{i=1}^{K} A_i\right) \cup A_{K+1}$$

countable by induction hypothesis.

Also from base case, union of two countable sets is countable.

$$\Rightarrow \bigcup_{i=1}^{\infty} A_i \text{ is countable.}$$

Q: Prove: If n^2 is odd, n is odd.

P : n^2 is odd Q : n is odd.

We prove this by contrapositive method

ie: $\neg Q \Rightarrow \neg P$.

That is if n is not odd $\Rightarrow n^2$ is not odd.

Since n is even :- $n = 2k \quad k \in \mathbb{Z}$

& $n^2 = (2k)^2 = 2(2k^2) = 2\ell$

$\ell = 2k^2 \quad k \in \mathbb{Z}$.

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

Hence proved.

TUTORIAL - 3

Q: 8: Every nail has exactly one picture hanging on it. Express using 2 variables.

~~P:~~ ~~x~~ x is a nail.

y is a painting z : is a

$P(x,y)$: y is a painting on x.

$(\forall x)(\exists y)\,(P(x,y)) \wedge (\forall x)(\exists z)(z \neq y)(P(x,$

11

$G(x,y)$ = x gets y.

$W(x,y)$ = x wants y.

$P(x)$: x is a person.

1). $(\forall x)(\exists y)$ ~~$(\forall x)$~~ $[(P(x) \wedge W(x,y)) \longrightarrow \neg(G(x,y))]$

$(\exists x)(\exists y)$ ($W(x,y) \rightarrow \neg(G(x,y)$

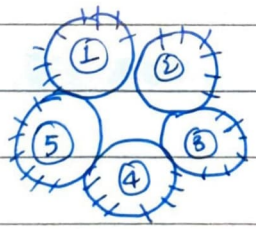
3. $(\forall x)(\exists y)\left[P(x) \wedge \neg(W(x \to y))\right]$

Consider 5 gears, interlocked.
Prove rotation isn't possible.

Observations :-

1) There are odd no: of gears.
2) In any gear system the neighbouring gear rotates in the direction opposite to its direction.
3) Odd no: gears rotate in same direction (vice-versa even).

Proof: Assume that we can rotate one gear which is ①.
Assume we rotate in clockwise direction.



∴ ① ⇒ ② & ⑤ rotate anticlockwise → *

⑤ We know that all odds rotate in one direction while all evens rotate in the other direction

But * contradicts statement ⑤.
Hence our initial assumption that we can rotate ① is false. And since ① was arbitrary, we cannot rotate any.

Q: Make 25 Rupees by using exactly 10 notes with denominations of 1₹, 3₹, 5

Sol: Consider :-

$$m \times 1 + n \times 3 + l \times 5 = 25$$

And, $$m + n + l = 10.$$

Subtracting : $$2n + 4l = 15.$$

LHS is even but RHS is odd.

∴, Summing odd numbers even no: of times is even.

∴, This is not possible.

Q: Product of 22 integers is +1. Then can the sum of the integers be 0?

Sol:

(I) $\prod_{i=1}^{22} x_i = 1 \Rightarrow x_i$ are (+1) or (-1)

$\Rightarrow$ even no: of (-1)s

further $\Rightarrow$ even no: of (+1)s.

let $2m$ be even no: of (-1)s. $m \in Z$

$2n$ be even no. of (+1)s. $n \in Z$.

And, $2m + 2n = 22$

$\Rightarrow m + n = 11.$ — (I).

Assume that sum : $\sum_{i=1}^{22} x_i = 0$

ie: $(x_1^{+1} + x_2^{+1} + \dots) + (x_1^{-1} + x_2^{-1} + x_3^{-1} \dots) = 0$

$2m(+1) + 2n(-1) = 0$.

$\Rightarrow \quad m = n. \quad — (2)$.

From (1) & (2).

$2m = 11 \quad m = 11/2 \notin z$

∴, Statement (2) contradicts (1).

Hence our initial assumption is false.

And $\sum_{i=1}^{22} x_i$ is ~~fals~~ $\neq 0$.

8: Can you form a 6×6 magic square Given first 36 prime no:s.

Proof: If 2 is placed in any column/row, the sum becomes odd.

While in the remaining columns/rows the sum of odd no:s even no: of times makes it even.

Therefore this is not possible.

Invariant Proofs :-

1 0 1 0 0 1 0 0 0 1 1.

① There are 11 nos.
Repeat this algorithm 10 times

② a) If 2 nos are not equal put 1
b) else put 0.

Which no: remains in the end.

Sol: Consider the invariant :
S_i = sum of no:s in the list in step 1.
$S_1 = 5$.

Any step ② a) or ② b) can change the sum by 0 / or 2.

∴ Only one no: will be left in the end. And we must have 1 left.

Q: Consider a two letter language AO - AO which contains only letters A or O

→ If we delete 2 neighbouring letters AO in the word then the meaning of the word doesn't change.

→ Meaning of the word doesn't change

if we insert OA & AOO

??? Does AOO & OAA have same meaning?

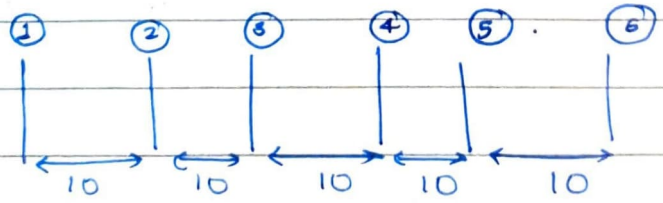
Sol Invariant: Difference of ~~no: of~~ no: of A's & Os.

In AOO Difference is +1.

In OAA Difference is -1

According to ① × ② the different should remain the same.

Q: There are 6 sparrows sitting on 6 trees, one sparrow on each tree. The trees stand in a row with 10 mtrs between neighbouring trees. If a sparrow flies from some tree to another then at the same tree another sparrow flies another tree to another tree same distance away in opp. direction.



??? Is it possible for all sparrows to gather on on tree?

TRY:

PIGEON HOLE PRINCIPLE:

If we put $n+1$ pigeons into n pigeon holes then some pigeon hole must contain 2 or more pigeons.

Q: A bag contains marbles of 2 colours black & white. What is the small no: of marbles you pick so that have 2 marbles of the same colo

TUTORIAL- 3

4) 2> $\sum b_k^2 < n$. $\Rightarrow$ one of the b_i must be 0.

$b_i^2 \geq 1$.

$1+1+1+1+\ldots n$

∴, This inequality doesn't hold unl at least one of the $b_k = 0$

3) 1> Prove that set $A = \left\{ \frac{n-1}{n} \quad n \in Z^+ \right\}$ does not have a greatest elemen

Proof: Assume $K \in A$ S.T. K_1 is the larges no:

∴, $K_1 = \frac{n-1}{n}$ $\quad n \in Z^+$

Consider $K_2 = \frac{(n+1)-1}{n+1} = \frac{n}{n+1}$

Now, $k_2 > k_1$

$\because \quad \frac{n}{n+1} > \frac{n-1}{n}$.

$n^2 > n^2 - 1$ True.

$\therefore$, we see $k_2 > k_1$ but our assumption was k_1 is greatest.

$\therefore$, false.

2) Consider $n_1, n_2, n_3, n_4 \in Z$

Mean $= n$.

T.P at least one no: $> n+1$.

let $(n+1)$ be the largest no:

$\therefore$, Other no:s are: $n, n-1, n-2$.

$$\text{Mean} = \frac{(n+1) + n + (n-1) + (n-2)}{4} = \frac{4n-2}{4} = n - \frac{1}{2} \neq n$$

$\therefore$, there must be at least one no: $> n+1$

3) T.P there is no rational number r such that $2^r = 3$.

T.P no $r = \frac{p}{q}$.

Assume $2^r = 3$ $\quad r = p/q$.

ie: $(2)^{p/q} = 3$.

$2^p = 3^q$.

LHS will always be even while RHS will be odd. $\therefore$, equality false.

1) a) $P \to Q$ & $\neg Q \to \neg P$

Prove n is divisible by 7

$\Rightarrow$ n^2 is divisible by 7.

b) $m > 10$ & $n \geq 0$

$\Rightarrow$ $mn \neq 100$.

ie: m n

ie: $(10+x)(10+y)$ $x, y > 0$

$= 100 + 10(x+y) + xy > 100$

$\therefore$ proved.

c). If $x^2 \geq x$

$x \in (-\infty, 0] \cup [1, \infty)$.

$x^2 - x \geq 0$

$x(x-1) \geq 0$.

2). T.P $|x+y| = |x| + |y|$ iff $xy \geq 0$

If $xy \geq 0$.

either $x \geq 0$, $y \geq 0$.

$\Rightarrow$ $x+y = |x| + |y|$.

Or $x < 0$, $y < 0$.

$\Rightarrow$ $|-(x+y)| = x + y$.

Also $xy = |x||y|$.

$xy \geq 0$.

~~$m|n \nRightarrow n|m$ iff~~

$m|n$ & $n|m$ iff $m = n$.

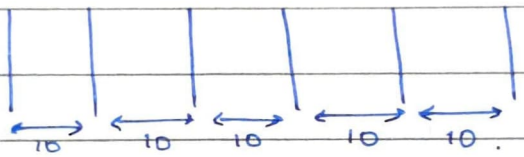
ie: $n = k_1 m$ — ①

$m = k_2 n$. — ②

From ① & ② $k_1, k_2 \in N$.

For this to hold true $m = n$

- **Sparrow Problem:**



Can all sparrows gather on same tree?

Invariant : Sum of distance is constant.

$\therefore$, $S = 10+20+30+40+50+60 = 210$ [from origin]

If all sparrows gather on a tree number K, the total distance of sparrows is

ie: $60K = 210$.

$K = \frac{210}{60} = \frac{7}{2} \notin Z$.

$\therefore$, This scenario isn't possible.

→ **Pigeon Hole Principle:**

If we put $n+1$ pigeons into ~~$n+1$~~ n pigeon holes then atleast one hole will

contain at least 2 pigeons.

P:- There are n+1 pigeons in n holes.
Q:- At least one hole contain 2 pigeons.

TQ:- ~~No hole will contain more~~
All holes contain 1 or less pigeons.
⇒ N holes will contain at most n pigeons

∴ TP:- will be contradiction.

Q: Given 12 integers show that 2 of them can be chosen whose diff. is divisible by 11

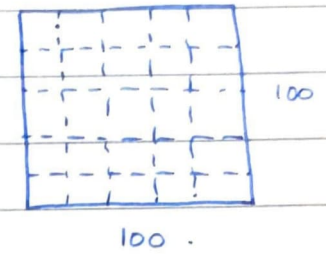
Pigeons : Numbers.
Holes : Remainders.

Atmost 11 remainders are possible.
2 of these numbers have the same remainder

General principle :
If we put nk+1 pigeons into N holes then at least one hole contains k+1 pigeons.

Q: Given a square of side length 1m consider 51 pts inside the square show that ∃ a square of side 20cm that contains at least 3 pts.

Max. no: of squares of size 20 x 20 cm = 25 squares.



Assign 2 pts. to each square (50 pts).

But we have 51 points in total

∴, At least one square has 3 pts.

Pigeons = 51 = (25) × 2 + 1. NK + 1.

Holes = (25) N

Q: Given eq. triangle show that all the three vertices cannot be covered by 2 smaller eq. triangles.

If there are n numbers whose sum is S

then there must be at least one no. less than $\frac{S}{n}$ & at least one no $> \frac{S}{n}$.

→ STRONG INDUCTION :-

1) Base case $P(b)$ is true.
2) Induction $P(k)$ is true $\forall k$ from b.
3) Prove $P(k+1)$ is true.

Q. Prove that every natural no: can be written as a sum of distinct powers of 2.

base: $1 = 2^0$ $\quad 2 = 2^1$

Assume true upto $n-1$.

$\therefore$, $n = 2q + r \quad q < n$

$0 \leq r \leq 1$

since q is less than n

$q = \sum_{i=1}^{n} 2^{ij} \quad ij \neq ik$ if $j \neq k$

$\therefore$, $n = 2\left(\sum_{i=1}^{n} 2^{ij}\right) + r$

$= \sum_{i=1}^{n} 2^{ij+1} + r$

Here ~~$r=0$ & $r=1$~~ $r = 0$ & $r = 1$

then $n = \sum_{i=1}^{n} 2^{ij+1} + 0$ for $r = 0$

$n = \sum_{i=1}^{n} 2^{ij+1} + 1$ for $r = 1$

$= 2^0$

SETS, RELATIONS, FUNCTIONS :-

Set: Unordered collection of distinct objects.

Equal sets: $A = B$

if $a \in A \Rightarrow a \in B$

& $b \in A \Rightarrow b \in B$.

Eg: $\{1, 3, 3, 5\}$, $\{1, 3, 5\}$.

Subset: A set A is a subset of set B if every element in A is also an element in B.

If $A = B$.

$(A \subseteq B) \wedge (B \subseteq A)$.

Power set: Set of all subsets.

Eg :- $\{\{\phi\}\} \longrightarrow \{\phi, \{\{\phi\}\}\}$

$\{\phi\} \longrightarrow \{\phi, \{\phi\}\}$.

Cardinality: No: of elements in a set.

Denoted by $|A|$

eg: $|\phi| = 0$.

$|\{\phi\}| = 1$

$|P(A)| = ?$ where $|A| = n$.

$= 2^n$.

Q: Does $\phi \in \{\phi\}$?

Yes.

Q: Find power set of

$\{a, b, \{a, b\}\}$

$\{ a, b, \{a,b\}, \{a, \{a,b\}\}, \{b, \{a,b\}\}, \{a,b\}$
$\{a, b, \{a,b\}\}, \phi \}$.

→ Cartesian Product:

$A \times B$.

$A \times B = \{ (a,b) \}$ S.T. $a \in A$ & $b \in B$

$A \times B \neq B \times A$.

$|A \times B| = ?$ if $|A| = m$ $|B| = n$.

$= mn$.

Q: $S = \{ x \mid x \notin x \}$

a) $S \in S$.

b) $S \notin S$.

] Russels Paradox. ∴, Neither of these case tru

→ Set Op:

$A \cap B = \{ x \mid x \in A \wedge x \in B \}$.

$A \cup B = \{ x \mid x \in A \vee x \in B \}$.

Q: $|A \cup B| = ?$

given $|A|$, $|B|$, $|A \cap B|$

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

→ **Complement**

$\overline{A} = \{ x \mid x \notin A \}$.

→ **De Morgans Laws:**

$\overline{A \cup B} = A' \cap B'$

$\overline{A \cup B} = \{ x \mid x \notin (A \cup B) \}$.

$= \{ x \mid \neg (x \in (A \cup B)) \}$.

$= \{ x \mid \neg ((x \in A) \vee (x \in B)) \}$.

$= \{ x \mid (x \notin A) \wedge (x \notin B) \}$.

$= A' \wedge B'$.

→ **Distributive Laws:**

$A \cup (B \wedge C) = (A \cup B) \wedge (A \vee C)$.

$= \{ x \mid (x \in A) \vee (x \in (B \wedge C)) \}$

$= \{ x \mid (x \in A) \vee ((x \in B) \wedge (x \in C)) \}$.

$= \{ x \mid (x \in A) \vee (x \in B) \wedge (x \in A) \vee (x \in C) \}$.

→ **Symmetric Diff: & Diff:**

DIFF: $A - B = \{ x \mid (x \in A) \wedge (x \notin B) \}$.

Eg: $A = \{1, 2, 5\}$ $\quad B = \{3, 2, 1, 5\}$

$A - B = 1$.

SYM: $A \oplus B$

$= (A - B) \cup (B - A)$ — Remove common elements

$= \{1, 3\}$

Show:

$(A - B) - C = (A - C) - (B - C)$

LHS: $(A - B) - C$.

$= \{ x \mid x \in (A - B) \wedge (x \notin C) \}$

$= \{ x \mid (x \in A) \wedge (x \notin B) \wedge (x \notin C) \}$.

$(P \wedge \neg Q) \wedge \neg R$

RHS: $(A - C) - (B - C)$

$= \{ x \mid x \in (A - C) \wedge x \notin (B - C) \}$

$= \{ x \mid ((x \in A) \wedge (x \notin C)) \wedge \neg (x \in (B - C)) \}$

$= \{ x \mid ((x \in A) \wedge (x \notin C)) \wedge \neg ((x \in B) \wedge (x \notin C)) \}$

$(P \wedge \neg R) \wedge \neg (Q \wedge \neg R)$

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

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

→ Is $A \times B = B \times A$?

NO

Relation:

A relation R between 2 sets A & B is a subset of $A \times B$

Q: Find some relation b/w A & B.

1). $A \in Z$ $B \in Z$.

2) $A \in R$ $B \in Z$.

3) $A \in R$ $B \in R$.

(1) $A: \{1, 2, 3\}$ $B: \{2, 6\}$.

$A \times B$ $\{(1,2), (1,6), (2,2), (2,6), (3,2), (3,6)\}$.

(1) aRb $a = b$.

aRb $a < b$.

aRb $a > b$.

(2) aRb $[a] = b$

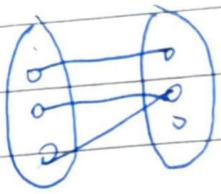
Functions:

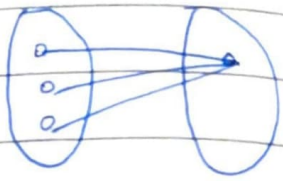
A function from set A to B is a relation such that:

1. Every el. of A is related to some el. of set B.

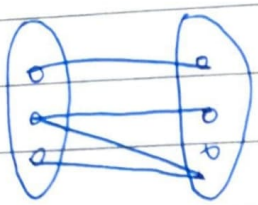
2. Every el. of A is related to exactly one el. of B.

Functions:





Not a function:



Given a function :- $A \to B$.

A: Domain B: Codomain

For $a \in A$ $f(a) \in b$ is called the image under f

For $b \in B$, st. $\exists\, a \in A$ such that $f(a) = b$, $a \to$ preimage.

Eg: $f: \mathbb{R} \to \mathbb{R}$. $f(x) = x^2$.

Codomain & Dom $= \mathbb{R}$

Image of $\sqrt{2} \to 2$

Premage of $1 \to \pm 1$.

→ **Injective Func:**

A func. from $A \to B$ is injective if every el. of A is related to one unique el. of B.

ie: if $f(a) = f(b) \Rightarrow a = b$.

Q: If $f: \mathbb{R} \to \mathbb{R}$
for x^2 injective.
Consider $f(-1) = f(1)$.
$-1 \neq 1$ ∴, Not injective.

But if domain modified. $\mathbb{R}^+ \to \mathbb{R}$
then yes, injective.

→ Surjective func:

A func. f is surjective if each el. in B has a pre-image in A.
$b \in B \quad \exists\ a \in A$.

Q: $f: \mathbb{R} \to \mathbb{R}$.
Is $f(x) = e^x$ surjective?
Consider $b = -1 \in \mathbb{R}$ there does not exist any $a \in A$ such that $e^a = f(a) = -1$

∴, Modifying :→ $f: \mathbb{R} \to \mathbb{R}^+$

→ Equal func:
$f: A \to B \qquad g: C \to D$
These are equal if.
$(A = C) \wedge (B = D)$
& $f(a), a \in A = g(a)$.

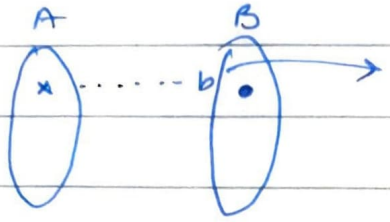
★ If $f: A \to A$ & A is finite then f is injective iff f is surjective

f is inj $\Rightarrow$ f is surjective.

contrapositive: f is not sur $\Rightarrow$ f is not injective.

$\downarrow$

$\exists\ b \in A$ s.t. $\nexists\ a \in A$ s.t. $A(a) = (b)$.



Proof:- Let cardinality of A is n
Since f is a func. $f: A \to A$
each of the n el. of A are mapped but since b in A does not have a preimage, n el. of A must map to (n-1) el. of A (dom)
*

∴ by PHP :- Pegions are n & holes are n-1 ∴ $\Rightarrow$ at least ~~1 el. in~~ 2 el. of A mapped to 1 el. of A
$\Rightarrow$ f is not injective.

→ BIJECTIVE FUNC:

A func. $f: A \to B$ is called bijective if it is both injective & surjective

★ If $f: A \to B$ is bijective & A & B are finite

$$|A| = |B|$$

Q: Write a bijection map :-

$f : A \to B$

S.T. $A \subseteq B$

A: Consider $f: \mathbb{E} \to \mathbb{Z}$

$$\boxed{f(n) = \frac{n}{2}}$$

Claim f is 1-1.

$$f(a) = f(b)$$

$$\frac{a}{2} = \frac{b}{2} \quad = \quad a = b \quad \therefore \text{ 1-1.}$$

Claim f is onto.

Let $m \in \mathbb{Z}$

Take $2m \in \mathbb{E}$

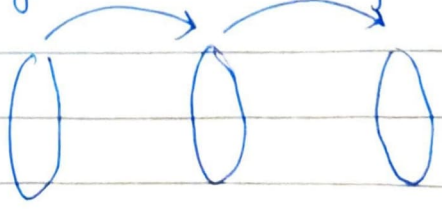
$$f(2m) = \frac{2m}{2} = m \in \mathbb{Z}.$$

f is onto.

→ COMPOSITE FUNCTIONS.

Composition of 2 functions :-

f & g. ~~to~~ f o g.



Eg: $f(x) = e^x$

$g(x) = x^2 - 2$

$fog(x) = f(g(x))$

$= f(x^2 - 2)$

$= e^{x^2-2}$.

→ **IDENTITY:**

A fn. $f: A \to A$ denoted by I_A is identity fn if

$I(x) = x$.

→ **INVERSE**

A. fn. f: $f^1: B \to A$ is called inverse of $f: A \to B$ if

$f \circ f^{-1} = I_x$.

Eg. $f(x) = x + 2$.

$f^{-1} = x - 2$.

★ Inverse of a func. is unique

let us assume f_1^{-1} & f_2^{-1} are two inverses of f

$f_1^{-1} = f_1^{-1} \circ I$

$= f_1^{-1} \circ (f_2^{-1} \circ f)$.

$= f_1^{-1} \circ (f \circ f_2^{-1})$ [associativity of composition].

$= (f_1^{-1} \circ f) \circ f_2^{-1}$

$= I \circ f_2^{-1}$.

$\therefore \quad f_1^{-1} = f_2^{-1}$.

→ Which of these are onto :-

$f(m,n) = 2m - n$

$f : \mathbb{Z} \times \mathbb{Z} \to Y$.

let $l \in \mathbb{Z}$.

$f(m, n) = l$.

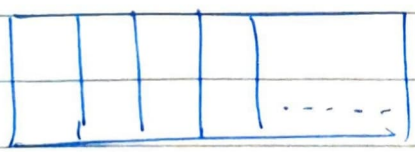
Claim $m = 0, \quad n = -l$.

$f(0, -l) = l$. $\therefore$ ONTO.

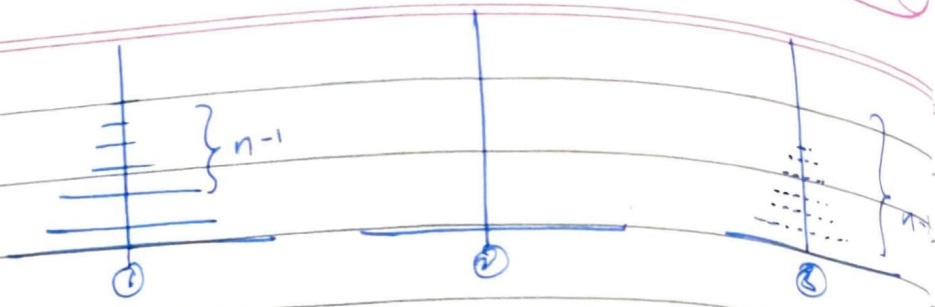
→ Inverse of composition

$(fog)^{-1} = g^{-1} \circ f^{-1}$

RECURSIVE RELATIONS



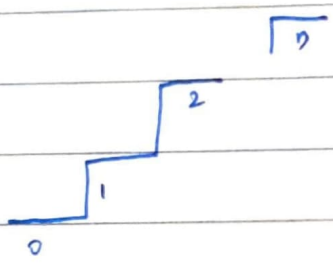
In how many ways can the $2 \times n$ board be filled with 1×2 dominos.



$T_n = 2T_{n-1} + 1.$

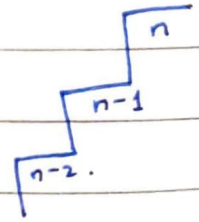
Since after the $(n-1)$ plates move to form a tower at (2)
Again T_{n-1} steps are required to place it above plate n

→



Consider n steps: you can jump either 1 or 2 steps at a time.
Define recursive function.

$T(n) = T(n-1) + T(n-2).$



$T(1) = 1$ one way
$T(2) = 2$ 2 ways.

Q: Find no. of ways to triangulate an n-gon.

→ Linear Homogenous Recursive Relations:-

Let $a_1, a_2, a_3 \ldots, a_n$ be a seq. of nos. A linear hom. recursive relation of order k with const. co-efficient is a recurrance relation.

$$a_n + c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k} = 0$$

$c_k \neq 0$, $c_1, c_2, c_3 \ldots$ are const. The c_i's are found using (base case) initial co-efficient.

Eg: $T_n = T_{n-1} + T_{n-2}$.
is a LHR. with order 2.

Q: which are linear?

i) $a_n = 3a_{n-1} + a_{n-2}$.

ii) $a_n = 3a_{n-1} + \boxed{5}$ (not homogenous)

iii) $a_n = 3a_{n-1} + a_{n-2}a_{n-3}$ (not linear).

(iv) $a_n = 3a_{n-1} + n\,a_{n-2}$ not linear.
↙ not const.

→ Solution of a Recurrance Relation:-

A seq. $S_1, S_2, S_3 \ldots S_n$ is said to satisfy a linear homogenous recurrance relation set

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots c_k a_{n-k}$$

$k \neq 0$

if $S_n = C_1 S_{n-1} + C_2 S_{n-2} + C_3 S_{n-3} \ldots$

Eg: Consider :

$$a_n = 7a_{n-1} - 12a_{n-2}$$ [Base case :- $a_0 = 3$, $a_1 = 11$]

Substitute $a_n = t^n \quad t \neq 0.$

$$\Rightarrow \quad t^n = 7t^{n-1} - 12t^{n-2}.$$

$$t^2 = 7t - 12.$$

$$t^2 - 7t + 12 = 0$$

$$(t-3)(t-4) = 0$$

$$t = 3 \quad \text{or} \quad t = 4.$$

Claim : $S_n = C_1 3^n + C_2 4^n$

For $n = 0$;

$$C_1 + C_2 = 3.$$

For $n = 1.$

$$11 = 3C_1 + 4C_2.$$

$$11 = 3C_1 + 4(3 - C_1).$$

$$11 = 12 - C_1.$$

$$C_1 = 1$$

$$C_2 = 2.$$

$$\therefore S_n = 3^n + 2 \cdot 4^n$$

THEOREM: Let $a_n = C_1 a_{n-1} + C_2 a_{n-2}$ where $C_2 \neq 0$ be a linear homo. recurrance rel with const. co-efficients. Let t be a non-zero real no:

$t^2 - c_1 t - c_2 = 0$ → characteristic eq.

then the seq. $\{t^n\}$ satisfies the recurrance iff

$$t^2 - c_1 t - c_2 = 0.$$

Eg Consider $\{\$ t^n\}$ is a solution of the recurrance.

$$t^n = c_1 t^{n-1} + c_2 t^{n-2}$$

$\Rightarrow$ ~~$t^2 - c_1$~~

Given :-

$$t^2 - c_1 t - c_2 = 0 \cdot \quad \text{multiply by } t^{n-2}$$

$$t^n - c_1 t^{n-1} - c_2 t^{n-2} = 0.$$

$\Rightarrow$ $\{t^n\}$ is the sol. of the given rec.

- Th: Suppose $\{t^n\}$ is a solution of the recurrance

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

→ If r_1, r_2 are distinct roots of the eqn.

~~$t^2 - ct - c_2 t^{n-2}$~~

$$t^2 - c_1 t - t_2 = 0$$

then there exist constants b & d such that

$$a_n = b r_1^n + d r_2^n.$$

→ If $r_1 = r_2$

$$s_n = b r^n + d n \ell^n$$

Eg:

$a_n = 4a_{n-1} + 4a_{n-2}$.

$a_0 = 4 \quad a_1 = 12$.

Let $a_n = t^n$

$t^n = 4t^{n-1} + 4t^{n-2}$

$t^2 - 4t + 4 = 0$

$(t-2)^2 = 0$

$t = 2$.

~~$S_n = 2t$~~ $S_n = b(2)^n + dn(2)^n$.

Using initial conditions

$n = 0, \quad b = 4$

$n = 1, \quad 2b + 2d = 12.$

$b + d = 6.$

$d = 2.$

$\therefore, \quad S_n = 4(2)^n + 2n(2)^n$ solution

→ In general form:

$Q_n = C_1 a_{n-1} + C_2 a_{n-2} + \ldots + C_k a_{n-k} \quad C_k \neq 0$

let ~~$\{t^n\}$~~ t be a non-zero real no then

$\{t^n\}$ is a solution of the given ~~relation~~ recurrence iff

$t^k - C_1 t^{k-1} - C_2 t^{k-2} - \ldots - C_k = 0.$

characteristic eqn.

→ **Th.** Let $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots c_k a_{n-k}$

$c_k \neq 0$

be a linear homogenous ~~eqn~~. recurrance relation of order k, $c_1, c_2 \dots c_k$ are constants

Let $t^n - c_1 t^{n-1} - c_2 t^{n-2} \dots - c_k = 0$. — (*)

be the characteristic eqn.

~ If the sequence $\{s_n\}_{n=0}^{\infty}$ & $\{p_n\}_{n=0}^{\infty}$ are solutions then

$\{s_n + p_n\}_{n=0}^{\infty}$ is also a solution.

~ If $r_1, r_2, \dots r_k$ are distinct then

$a_n = b_1 r_1^n + b_2 r_2^n + \dots b_k r_k^n$

where $b_1, b_2, \dots b_k$ are constants which are determined using initial conditions

~ If r is a root of multiplicity m of the characteristic eqn then

$a_n = r^n$, $a_n = n r^n$, $a_n = n^{n-1} r^n$

are solutions of (*)

Suppose that

$a_0 = d_0$, $a_1 = d_1$, $\dots$ $a_{n-1} = d_{n-1}$

are initial conditions of recurrance where $d_0, d_1, \dots d_{n-1}$ are constants

If $s_1, s_2 \ldots s_t$ are t distinct roots of char. eqn with multiplicities $m_1, m_2, \ldots m_t$

$m_1 + m_2 + \ldots m_t = k$ then

$$a_n = \left(c_{00} + c_{01} n + \ldots + c_{0(m_1-1)} n^{m_1-1}\right) s_1^n +$$

$$\left(c_{10} + c_{11} n + \ldots + c_{1(m_2-1)} n^{m_2-1}\right) s_2^n +$$

$$\ldots \quad +$$

$$\left(c_{(t-1)0} + c_{(t-1)1} n + \ldots + c_{(t-1)(t-1)} n^{m_t-1}\right) s_t^n$$

→ Solve the following recurrences :-

$$a_n = 5a_{n-1} - 8a_{n-2} + 4a_{n-3}.$$

~ $a_0 = 0 \quad a_1 = 2 \quad a_2 = 10$

Let $a_n = t^n$.

$$\Rightarrow \quad t^n = 5t^{n-1} - 8t^{n-2} + 4t^{n-3}.$$

$$t^3 = 5t^2 - 8t + 4$$

$$\text{i.e.: } t^3 - 5t^2 + 8t - 4 = 0.$$

$$(t-1)(t-2)^2 = 0$$

$t = 1, 2, 2$ are roots

$$S_n = c_1 1^n + c_2 2^n + c_3 n 2^n$$

$a_0 = 0 \;\Rightarrow\; 0 = c_1 + c_2.$

$a_1 = 2$; $2 = C_1 + 2C_2 + 2C_3$.

$a_2 = 10$; $10 = C_1 + 4C_2 + 8C_3$.

$C_1 = -C_2$.

$\therefore$, $2C_3 + C_2 = 2$.

$8C_3 - 3C_2 = 10$.

$6C_3 - 3C_2 = 6$

$5C_3 = 4$ $\quad 2C_3 = 4$ $\quad \boxed{C_3 = 2}$

$C_3 = 4/5$

$C_2 = C_3 - 2 = \frac{4}{5} - 2 = \frac{-6}{5}$.

$C_1 \neq -6/5$. $\quad C_2 = 2 - 2C_3$

$= 2 - 2 \cdot 2 = -2$

$\therefore$, $C_1 = 2$.

$\therefore$, $a_n = 2 \cdot 1^n - 2 \cdot 2^n + 2n \cdot 2^n$.

Qn: SOLVE :-

$a_n = 6a_{n-1} - 9a_{n-2}$ if $n \geq 2$.

Let $a_0 = 1$, $a_1 = 9$.

$a_n = t^n$.

$\therefore$, $t^n = 6t^{n-1} - 9t^{n-2}$.

$t^2 = 6t - 9$.

$t^2 - 6t + 9 = 0$.

$(t-3)^2 = 0$ $\quad t = 3$

$\therefore$, $S_n = C_1 \cdot 3^n + C_2 \cdot n \cdot 3^n$.

$$S_n = C_1 3^n + C_2 \cdot n 3^n$$

$a_0 = 4$

$$4 = C_1$$

$a_1 = 9$,

$$9 = 3C_1 + 3C_2$$

$$C_1 + C_2 = 3$$

$$C_2 = -1$$

$$\therefore S_n = \underline{4 \cdot 3^n + (-1) n \cdot 3^n}$$

- **Linear Non-Homogenous Recurrance Rel**

It is of the form

$$a_n + C_1 a_{n-1} + \ldots + C_k a_{n-k} = f(n)$$

— For general $f(n)$, there are no known general methods.

— Consider $f(n) = b^n p(n)$

b^n = constant

$p(n)$ = polynomial in n.

Eg: ① $a_n + 5a_{n-1} + 6a_{n-2} = 3^n$

② $a_n + 5a_{n-1} + 6a_{n-2} = 3^n (n^2 + 6n + 5)$

Eg: Solve :-

$a_n - 5a_{n-1} = 3^n$, $n \geq 1$

$a_0 = 1$

let t_n be any solution.

$\therefore$, $t_n - 5t_{n-1} = 3^n$ — ①.

let p_n be some particular solution.

$$p_n - 5p_{n-1} = 3^n \text{ —— ②}.$$

① - ② :- $(t_n - p_n) - 5(t_{n-1} - p_{n-1}) = 0$

let $u_n = t_n - p_n$ which is the homogenous sol.

$\Rightarrow t_n = u_n + p_n$ → sol will be of this form.

Try $p_n = d3^n$ $\because f(n) = 3^n$.

$p_n - 5p_{n-1} = 3^n$ [from ①]

$d3^n - 5d3^{n-1} = 3^n$.

$d3 - 5d = 3$

$-2d = 3$. $d = -3/2$.

Now, $p_n = \frac{-3}{2} \cdot 3^n$.

Consider hom. eq :-

$a_n - 5a_{n-1} = 0$

char eqn :-

$t - 5 = 0$ $t = 5$.

$u_n = c_1 5^n$ $t_n = u_n + p_n$.

$$t_n = C 5^n - \frac{3}{2} 3^n$$

For $n = 0$, $a_0 = 1$.

$$C_1 \, 5^0 - \frac{3}{2} 3^0 = 1$$

$$C_1 = 5/2.$$

$\therefore$, $t_n = \frac{5}{2} \cdot 5^n - \frac{3}{2} \cdot 3^n$ sol. with initial conditions

Eg: solve :-

$$a_n - 4a_{n-1} = 8^n \quad \text{①} \qquad n \geq 1 \quad a_0 = 1.$$

let $t_n - 4t_{n-1} = 8^n$ any sol

And, $p_n - 4p_{n-1} = 8^n$. particular sol

$$(t_n - p_n) - 4(t_{n-1} - p_{n-1}) = 0.$$

let $u_n = t_n - p_n$ $\quad t_n = u_n + p_n$

let $p_n = d \cdot 8^n$

ie.

$$d\,8^n - 4d\,8^{n-1} = 8^n.$$

$$d \cdot 8 - 4d = 8.$$

$$8d - 4d = 8 \quad d = 2.$$

$$p_n = 2 \cdot 8^n.$$

Homogeneous : $t_n - 4t_{n-1} = 0$

char eqn :- $t - 4 = 0 \quad t = 4.$

$$u_n = C_1 4^n.$$

$(t_n - p_n) = 4(t_{n-1} - p_{n-1}) = 8^n$

$u_n = 4u_n$ $\quad d \cdot 8^n - 4d8^{n-1} = 8^n$

$\therefore, \quad t_n = u_n + p_n.$

$= C_1 4^n + 2 \cdot 8^n$

for $n = 0, \quad a_0 = 1.$

$\therefore, \quad C_1 \cdot 4^0 + 2 \cdot 8^0 = 1.$

$C_1 + 2 = 1$

$C_1 = -1.$

$\therefore, \quad t_n = \underline{-4^n + 2 \cdot 8^n.}$

Converting to nonogeneous.

① Change n to $n-1$.

$\Rightarrow a_{n-1} - 4a_{n-2} = 8^{n-1}.$

②. Multiply 8

$8a_{n-1} - 32a_{n-2} = 8^n. \quad -(2).$

① - ② :-

$a_n - 12a_{n-1} + 32a_{n-2} = 0$

$a_0 = 1 \qquad a_1 = 12.$

$t^n - 12t^{n-1} + 32t^{n-2} = 0.$

$t^2 - 12t + 32 = 0.$

$(t-8)(t-4) = 0$

$t = 8, 4.$

$\therefore S_n = C_1 8^n + C_2 4^n$.

$a_0 = 1$ $\qquad a_1 = 12$.

$1 = C_1 + C_2$.

$12 = 8C_1 + 4C_2$.

$12 = 8C_1 + 4(1 - C_1)$.

$12 = 8C_1 + 4 - 4C_1$.

$8 = 4C_1$

$C_1 = 2$

$C_2 = -1$.

$$S_n = 2 \cdot 8^n - 4^n$$

Theorem:

Let

$$a_n - d a_{n-1} = b^n (u_n + v) \qquad n \geq 0.$$

$$a_0 = e_0 \qquad \text{---(1)}$$

where d, b, v, u, e_0 are constants
b, u are non-zero.

→ Change to linear.

1) $n \to n-1$.

$$a_{n-1} - d a_{n-2} = b^{n-1} (u(n-1) + v)$$

2) $\times b$:-

$$b a_{n-1} - bd a_{n-2} = b^n (u(n-1) + bv) \qquad \text{---(2)}$$

① - ②.

$$a_n - (b+d)\,a_{n-1} + bd\,a_{n-2} = ub^n \quad -③$$

Change n to $n-1$.

$$a_{n-1} - (b+d)\,a_{n-2} + bd\,a_{n-3} = ub^{n-1} \quad -④.$$

× by b.

$$ba_{n-1} - b(b+d)a_{n-2} + b^2d\,a_{n-3} = ub^n \quad -④.$$

③ - ④ :-

$$a_n + (-2b+d)\,a_{n-1} + (2bd+b^2)\,a_{n-2} - b^2d\,a_{n-3} = 0$$

$a_0 = 0$ -

$a_1 = d\,a_0 + b^n(un+v)$.

$a_1 = b(u+v)$.

$a_2 = da_1 + b^2(2u+v)$

$t^3 + (-2b+d)\,t^2 + (2bd+b^2)\,t - b^2d = 0$.

~~$t_n = c_1 b^n + c_2 n b^n + c_3 d^n$~~

$t_1 + t_2 + t_3 = 2b + d$.

$t_1 t_2 t_3 = b^2 d$.

Eg: $a_n - 3a_{n-1} = 2^n(4n+3)$ — ① $\quad n \geq 1, \; a_0 = 0$

Let $n \to n-1$.

$\therefore$, $a_{n-1} - 3a_{n-2} = 2^{n-1}(4(n-1)+3)$

$\times 2$:-

$2a_{n-1} - 6a_{n-2} = 2^n(4(n-1)+3)$ — ②

① - ② :-

$a_n - 5a_{n-1} + 6a_{n-2} = 2^n \cdot 4$ — ③

change $n \to n-1$:-

$a_{n-1} - 5a_{n-2} + 6a_{n-3} = 2^{n-1} \cdot 4$

$\times 2$:-

$2a_{n-1} - 10a_{n-2} + 12a_{n-3} = 2^n \cdot 4$ — ④

③ - ④ :-

$a_n - 7a_{n-1} + 16a_{n-2} - 12a_{n-3} = 0.$

$t^3 - 7t^2 + 16t - 12 = 0.$

$t = 2, \; 2, \; 3.$

$\therefore \; a_n = C_1 2^n + C_2 n \cdot 2^n + C_3 3^n.$

Sub initial conditions

Eg: Solve :-

$$a_n + 2a_{n-1} - 3a_{n-2} = 2^n(n^2 + n + 1) \quad \text{— (1)}$$

- $n \to n-1$:-

$$a_{n-1} + 2a_{n-2} - 3a_{n-3} = 2^{n-1}((n-1)^2 + (n-1) + 1)$$

$\times 2$:-

$$2a_{n-1} + 4a_{n-2} - 6a_{n-3} = 2^n((n-1)^2 + (n-1) + 1) \quad \text{— (2)}$$

(1) − (2) :-

$$a_n - 7a_{n-2} + 6a_{n-3} = 2^n \cdot 2n \quad \text{— (3)}$$

- $n \to n-1$:-

$$a_{n-1} - 7a_{n-3} + 6a_{n-4} = 2^{n-1} \cdot 2(n-1)$$

$\times 2$:-

$$2a_{n-1} - 14a_{n-3} + 12a_{n-4} = 2^n(2(n-1)) \quad \text{— (4)}$$

(3) − (4)

$$a_n - 2a_{n-1} - 7a_{n-2} + 20a_{n-3} - 12a_{n-4} = 2^n \cdot 2 \quad \text{— (5)}$$

- $n \to n-1$:-

$$a_{n-1} - 2a_{n-2} - 7a_{n-3} + 20a_{n-4} - 12a_{n-5} = 2^{n-1} \cdot 2$$

$\times 2$:-

$$2a_{n-1} - 4a_{n-2} - 14a_{n-3} + 40a_{n-4} - 24a_{n-5} = 2 \cdot 2^n \quad \text{— (6)}$$

(5) − (6) :-

$$a_n - 4a_{n-1} - 3a_{n-2} + 34a_{n-3} - 52a_{n-4} + 24a_{n-5} = 0$$

$$t^5 - 4t^4 - 3t^3 + 34t^2 - 52t + 24 = 0.$$

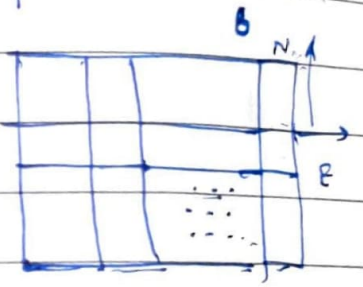
Q: Find the no: of solutions of

$x_1 + x_2 + \dots + x_n = n$

where x's are either 1 ~~&~~ or 2.

Q: Taxi cab: Find the no: of ways to go from A - B in a $m \times n$ grid.

1) can only go E or N.
2) Can go only one step at a time



In initial step:-

2 possibilities:- can move either N or E.

$T(m, n) = (m+1) \times (n+1)$ grid

$\therefore, T(m, n) = T(m, n-1) + T(m-1, n)$

$T(1, 2) = 1$, $T(2, 1)$

~~$T(1,1) = 2$~~

$T(1, n) = n + 1$

$T(1, m) = m + 1$.

$T(3, 4) = T(2, 4) + T(3, 3)$

$= T(1,4) + T(2,3) + T(2,3) + T(3,2)$

$= 5 + T(1,3) + T(2,2) + T(1,3) + T(3,2)$

$+ T(2,2) + T(3,1)$

$5 + 4 + 4 + 4 + 3 \cdot T(1,2) + 3(T(1,3))$

$17 + 6 \cdot 3 = 35$

11/10/18.

PERMUTATIONS & COMBINATIONS:

→ **Product Rule:**

Suppose that a procedure ...

Q: A company has 2 employees A, B, There are 11 offices How many ways can they be assigned.

Total ways = $11 \times 10 = 110$

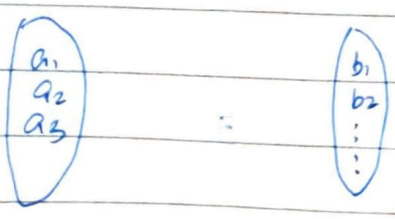
Q: How many ~~bits~~ strings of 7 bits can be formed

$= 2 \cdot 2 \cdot 2 \cdots 2 = 2^7$

Q: How many ~~elements~~ fns. can be mapped from A to B

(i) where $|A| = m$ $|B| = n$

∴,



∴, $a_1 \to n$ $a_2 \to n$ ... = $n \cdot n \cdot n \cdots$ (m times)

$= n^m$

(ii) How many one-one functions.

For $a_1 \longrightarrow n$ choices

$a_2 \longrightarrow (n-1)$ choices

$\therefore$ $a_n \longrightarrow n-(m-1)$ choices.

By product rule:-

$$n(n-1)\ldots\ldots\ (n-m+1) =$$

iii) Bijections from $A \to B$.

$\Rightarrow$ $n!$ $[n = |A| = |B|.]$

→ **Sum Rule:**

If a task can be done in one of n_1 ways or in one of n_2 ways where none of n_1 ways is the same as any of the set of n_2 ways, then there are $n_1 + n_2$ ways to do that task.

Eg: No: of ways to pick either of 5 apples or 4 oranges is $4+5 = 9$.

Q: How many possible passwords are there if:-

i) passwords are of length 6/7/8

ii) Upper case letters & digits are allowed

iii) There is at least one digit

Q1: Passwords with Upper case only

6 digits = 26^6

7 digits 26^7

8 digits = 26^8.

with upper cases & digits.

6 digits :-

6 → 36^6

7 → 36^7

8 → 36^8

with at least one digit :-

$(36^6 - 26^6) + (36^7 - 26^7) + (36^8 - 26^8)$

- **Permutations** : selecting ordered objects

Q: In how many ways can we select 3 students from a group of five stand in a line for a picture.

Ordered selection :-

$${}^5P_3 = \frac{5!}{2!}$$

$= 5 \cdot 4 \cdot 3$

$= 60$ ways

classmate
Date
Page

If n is a positive integer and r is an int $1 \le r \le n$ then there are $P(n, r)$ r-permutations of a set with distinct elements.

then

$$^nP_r = \frac{n!}{(n-r)!} = n(n-1)\dots(n-(r-1))$$

Q: How many permutations of letters

ABCDEFGHIJ :-

Consider ABC as one block.

$\therefore$ 8! ways.

Combinations:

Q: How many diff committees of 3 students can be formed from a group of 4 students :-

$$^4C_3 = 4.$$

The no. of r-combinations of a set with n-distinct elements is denoted by

$$^nC_r = \frac{n!}{r!(n-r)!}.$$

Proof: $^nC_r \times r!$ $=$ ^nP_r.

(^nC_r: pick n unordered obj; $r!$: permute)

NUMBER THEORY:

Nos: greater than 1 can be prime or composite.

Fact 1 → Infinitely many primes.

Fact → 2 every int greater than 1 has a prime divisor.

→ To find all primes b/w 1 & n
Sieve algorithm.
To optimise more, $p \leq \frac{n}{2}$.
Further optimising, $p \leq \sqrt{n}$

Fact 3: → If n is a composite integer then there exists a prime divisor p st $p \leq$

Proof: Let $n = ab$ $\quad 1 < a \leq b < n$
By contradiction.
Assume $a > \sqrt{n}$, $\therefore b > \sqrt{n}$
$\therefore ab > n$
ie: a contradiction.

→ $a \leq \sqrt{n}$.
a is a factor of n.
a has a prime divisor p.
⇒ p is a prime divisor of n
$\therefore$ since a exist exceed $\sqrt{n}$, $\therefore$

p can't exceed $\sqrt{n}$.

If n doesn't have a prime divisor $p \leq n$, then is prime.

→ Given $x \in \mathbb{R}$, How many prime no.s are there which are $\leq x$.

$\pi(x)$ = # primes $\leq x$

Obs 1: $\pi(x) \Big/ \left(x/(\log x - 1.08)\right) \approx 1$.

Obs 2: $\bar{\pi}(x) \Big/ \left(x/(\log x)\right) \approx 1$

conjecture :-

$R(x) = \bar{\pi}(x) \Big/ \left(\frac{x}{\log x}\right) \to 1$ as $x \to \infty$

$$C_1 \frac{x}{\log x} \leq \pi(x) \leq C_2 \frac{x}{\log x}$$

$C_1 \approx C_2 \approx 1$

If $R(x)$ converges it converges to 1

Riemann :-

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod \left(1 - \frac{1}{p^{-s}}\right)$$

→ Gaps in Primes:

consider $n > 2$

then the composite nos are :-

$n! + 2$, $n! + 3$, $n! + n$

∴ We cannot find a prime for next n numbers

∴ There are arbitrarily large gaps between primes.

→ Conjecture in Primes:

- Twin Prime conj:-
  There infinitely many twin primes
  ie: primes of the form p, $p+2$ where p is prime

- Goldbach conj:-
  Every positive even int > 2 is a sum of 2 primes

- $n^2 + 1$ conjecture :-
  There are infinitely many primes of the form $n^2 + 1$.

→ GCD (Greatest Common Divisor)
The GCD of 2 nos: a, b $a \neq 0$, $b \neq 0$ is the largest int. that divides both.

By convention
$$\gcd(a, 0) = 0.$$

→ RELATIVELY PRIME:

a, b are called relatively prime if $(a, b) = 1$.

Fact 5: $a, b \in \mathbb{Z}$ & $(a, b) = d$
then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$

Fact 6: $a, b, c \in \mathbb{Z}$.
then $(a + cb, b) = (a, b)$

Any common divisor of $a + cb$ & b is also a common divisor of a & b.

Assume d is a common divisor of a & b

Start: $\Rightarrow d \mid a \quad d \mid b \Rightarrow d \mid cb$

$\Rightarrow d \mid (a + cb)$.

$\therefore$, d is a common divisor of $a + cb$ & b.

End:

Let f be a common divisor of $a + cb$, b

$\Rightarrow f \mid a + cb \quad f \mid (b) \Rightarrow f \mid [cb]$.

$f \mid (a + cb - cb) \quad f \mid a$.

→ Computing GCD.

120, 325.

↳ 5.

→ Linear combination of 2 integers

$ma + nb$, $m, n \in \mathbb{Z}$

$(120, 325) = m(120) + 325(n)$.

$5 = m(120) + n(325)$.

$352 = 120 \cdot 2 +$

$120 = 85 +$

$85 = 35 \cdot 2$

$35 = 15 \cdot 2$

$15 = 5 \cdot$

$5 = 35 - 15 \cdot 2$

$= 35 - (85 - 35 \cdot 2) \cdot 2$

⋮

$5 = 19(120) + (-7)(325)$

* gcd of a, b is $\min \{ma + nb > 0, m, n \in \mathbb{Z}\}$

GCD: The gcd of 2 positive nos a, b is the least positive no:

$ma + nb$ $m, n \in \mathbb{Z}$

i.e.: $\gcd(a, b) = \min \{ma + nb > 0 \mid m, n \in \mathbb{Z}\}$

→ Euclidean Algo:

Let $r_0 = a$, $r_1 = b$ be integers such that $a \geq b > 0$. if div algo is successively applied

$$r_j = r_{j+1} q_{j+1} + r_{j+2}$$

$j = 0, 1, 2 \ldots n-2$ & $r_{n+1} = 0$

then $(a, b) = r_n$, last non-zero rem.

Euclidean algo can be used to find m & n ST $\gcd(a, b) = ma + nb$

→ Fundamental th. of arithmetic :-

Every positive integer > 1 can be written uniquely as a product of primes

$$12 = 4 \times 3 = 2^2 \times 3.$$

Well ordering : every non-empty set of integers has a least element.

Proof: Let n be the least integer that cannot be written as a product of primes

Case 1: If n is prime itself then n is a product of primes ie: n. This is not possible. Hence n must be composite

$$n = ab \qquad 1 < a < n \qquad 1 < b < n$$

Since $a < n$ & $b < n$

a & b can be written as product of primes.

Since $n = ab$ = product of primes.

$\therefore$, Our initial assumption is incorrect.

Uniqueness:

let $n = p_1^{i_1} \cdot p_2^{i_2} \cdots = q_1^{j_1} \cdot q_2^{j_2} \cdots$

cancelling common factors

$$p_1^{i_1'} \cdot p_{i_2}^{i_2'} \cdots p_{i_m}^{i_m'} = q_{j_1}^{j_1'} \cdot q_{j_2}^{j_2'} \cdots q_{j_N}^{j_N'}$$

Since $p_{ik} \mid p_{i_{j_1}}^{i_1'} \cdots p_{i_{j_1}}^{i_m'}$

and $\Rightarrow p_{ik} \mid q_{ji}^{} \cdots q_{ji}^{}$

contradiction

Prove: If $(a,b) = 1$ $\quad a \mid bc$ $\quad$ then $a \mid c$

$$ma + nb = 1$$

$\times c :-$ $\quad mac + nbc = c$

$\div a :-$ $\quad mc + \frac{nbc}{a} = \frac{c}{a}.$

$a \mid bc \quad \therefore, \quad a \mid mac + nbc$

$\Rightarrow a \mid c.$

- **CONGRUENCES:**

We say that $a \equiv b \pmod m$ if $m \mid a-b$ ie: a is 'congruent' to b (mod m)

classmate
Date
Page

→ Properties :-

If a, b, c, d, m are integers $m > 0$

$a \equiv b \pmod m$ $\quad c \equiv d \pmod m$ then

a) $(a+c) \equiv (b+d) \pmod m$

b) $(a-c) \equiv (b-d) \pmod m$

c) $ac \equiv bd \pmod m$.

ie: a> $m \mid (a-b)$ $\quad m \mid c-d$

$m \mid (a-b) + (c-d)$

$m \mid (a+c) - (b+d)$.

$\therefore (a+c) \equiv (b+d) \pmod m$.

c>. $a-b = mk$ & $c-d = ms$

$ac = mkd + m^2ks + bd + bms$.

$ac - bd = m(\underline{\text{int}})$

$\therefore m \mid ac-bd) \mid$.

Prove: A no: is divisible by 3 if the sum of its digits is divisible by 3.

Let the no: be :-

$n = d_n d_{n-1} d_{n-2} \cdots d_0$

$m = d_0 + 10d_1 + 10^2 d_2 + \cdots + 10^n d_n$

$10 \equiv 1 \pmod 3$ $\quad \times \quad a_0 \equiv d_0 \pmod 3$

$10^2 \equiv 1 \pmod 3$ $\quad \times \quad 10d_1 \equiv d_1 \pmod 3$.

$10^3 \equiv 1 \pmod 3$ $\quad \times$

Add:

$(d_0 + 10d_1 + \cdots 10^n d_n) \equiv (d_0 + d_1 + d_2 + \cdots d_n) \pmod 3$.

• Chinese Remainder Theorem :-

(1) $ax \equiv ay \pmod{m}$ iff
$x \equiv y \pmod{\left(\frac{m}{a, m}\right)}$

(2) If $ax \equiv ay \pmod{m}$ & $(a, m) = 1$
$\Rightarrow x \equiv y \pmod{m}$

(3) If $(x \equiv y) \pmod{n_i}$ for $i = 1, 2, 3 \ldots$ iff
$x \equiv y \pmod{\text{LCM}(m_1, m_2 m_3 \ldots m_r)}$

→ (1) $m \mid ax - ay$

$ax - ay = mz$.

$$\frac{ax}{(a,m)} - \frac{ay}{(a,m)} = \frac{mz}{(a,m)}$$

Also $\left(\frac{a}{a,m}, \frac{m}{a,m}\right) = 1$.

$$\Rightarrow \frac{a}{(a,m)}(x-y) = \left(\frac{mz}{a,m}\right)$$

$$\therefore \left(\frac{m}{a,m}\right) \mid (x-y) \qquad (x \equiv y) \pmod{\left(\frac{m}{a,m}\right)}.$$

THEOREM: Find x such that :-

$$\left.\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}\right\} \text{CRT.}$$

Let $m_1, m_2 \dots m_r$ denote a positive int that are relatively prime in pairs & let $a_1, a_2 \dots a_r$ denote r integeress. Then CRT has common sol. If x_0 denotes one sol. then an int x satisfies CRT iff x is in the form

$$x = x_0 + km \qquad k \in \mathbb{Z}.$$

$$\downarrow$$

$$m = m_1 m_2 m_3 \dots$$

Proof: Write $m = m_1 m_2 \dots m_r$. We see that m/m_j is an int such that.

$$\left(\frac{m}{m_j}, m_j\right) = 1$$

$$\exists\ x, y \in \mathbb{Z}\ ; \quad \frac{m}{m_j} x + m_j y = 1 \qquad (2)$$

Taking (mod m_j) of CRT (2):

$$\Rightarrow \frac{m}{m_j} x \equiv 1 \pmod{m_j}$$

Let $b_j = x$

$$\frac{m}{m_j} b_j \equiv 1 \pmod{m_j} \quad - \text{CRT } (3)$$

$$\frac{m}{m_i} b_j \equiv 0 \pmod{m_i} \quad \text{iff } i \neq j \quad \text{CRT } (4)$$

Put: $x_0 = \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j$

$$x_0 = \frac{m}{m_1} b_1 a_1 + \frac{m}{m_2} a_2 b_2 + \dots + \frac{m}{m_{i-1}} b_{i-1} a_{i-1} + \frac{m}{m_i} b_i a_i + \dots + \frac{m}{m_j} a_j b_j + \dots + \frac{m}{m_r} b_r a_r$$

$$\equiv \frac{m}{m_i} b_i a_i$$

Because from CRT (4): all other terms $i \neq j$ vanish we recall that

$$\frac{m}{m_i} b_i \equiv 1 \pmod{m_i}$$

$$\therefore\ x_0 \equiv a_i \pmod{m_i}.$$

Modern Algorithm / Abstract algorithm.

Eg CRT:-

Find least positive int x such that

$x \equiv 5 \pmod 7$

$x \equiv 7 \pmod{11}$

$x \equiv 3 \pmod{13}$.

$a_1 = 5 \quad a_2 = 7 \quad a_3 = 3$

$m_1 = 7 \quad m_2 = 11 \quad m_3 = 13$

m_i's are relatively prime

$$m = m_1 m_2 m_3$$
$$= 7 \times 11 \times 13. \quad = 1001$$

$$\therefore \left(\frac{m}{m_1}, m_1\right) = (11, 13, 7) = 1$$

$$\therefore \quad 11.13x + 7y = 1$$

$(143, 7) = 1.$

$143 = 7(20) + 3.$

$7 = 3(2) + 1.$

$3 = 1 \times 3 + 0.$

$1 = 7 - 3.2.$

$= 7 - (143 - 7.20).2$

$= 7 + 7.40 - 143.2$

$= -143.2 + 7.41$

$\therefore \quad x = (-2) \qquad y = (41)$

∴, Sol: $x_0 = \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j$

$\frac{m}{m_1} = 145 \qquad b_1 = (-2)$

Again :- $\left(\frac{m}{m_2}, m_2\right)$

$(7.13, 11) = 1.$

$7.13x + 11y = 1.$

$91 = 11 \times 8 + 3$

$11 = 3 \cdot 3 + 2$

$3 = 2 \cdot 1 + 1.$

$2 = 1 \cdot 2 + 0.$

∴, $1 = 3 - 2 \cdot 1$

$1 = 3 - (11 - 3 \cdot 3)$

$1 = 3 - (11 - 3 \cdot (91 - 88))$

$1 = 3 - 11 + 3 \cdot 91 - 3 \cdot 88$

$= 7.13(4) + (-33)(11)$

∴, $b_2 = 4.$

✗ $7.11(-1) + 6 \cdot (13) = 1.$

$b_3 = (-1)$

∴, $x_0 = 11.13 \cdot (-2)(5) + 7.13 \cdot 4 \cdot 7 + 7.11(-1) \cdot 3$

$= -1430 + 2548 - 231$

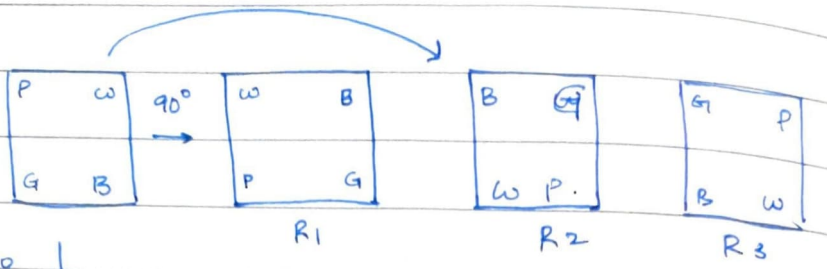
$= \underline{887}$

use transformation matrix

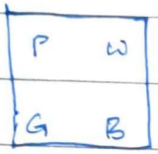
$$\begin{bmatrix} \cos & \sin \\ -\sin & \cos \end{bmatrix}$$

→ Modern Algebra / Abstract Algorithm

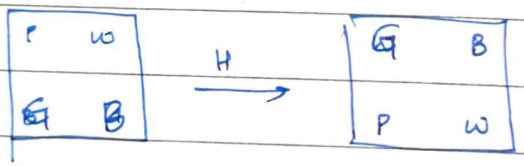
- Symmetry patterns of a square



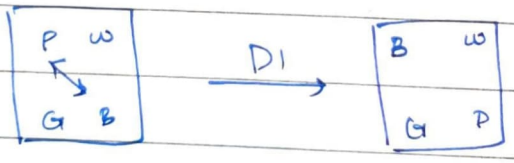
R0 ↓



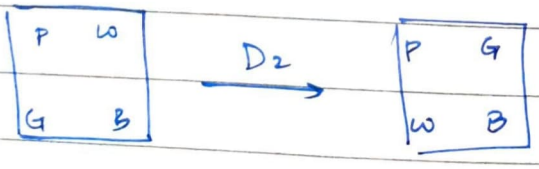
R0



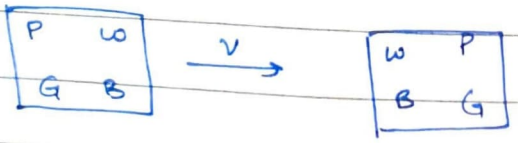
R1



R2



R3



Group:

$D_4 = \{ R_0, R_{90}, R_{180}, R_{270}, H, V, D_1, D' \}$

Dihedral group with 4 vertices.

$|D_n| = 2n$

(1) Closure Property :-
composition of any two from D_4 is a motion in D_4

(2) Identity :
R_0 is an identity

(3) $R_0 \cdot R_0 = R_0$
$R_{90} \cdot R_{270} = R_0$
$R_{180} \cdot R_{180} = R_0$
$H \cdot H = R_0$.
$V \cdot V = R_0$.
Inverses ↑

$R_{270} \cdot R_{90} = R_0$
$D \cdot D = R_0$
$D' \cdot D' = R_0$.

(4) D_4 is not commutative
$\because HD \neq DH$.

• Binary Operations :-
Let G, be a set. A binary operation on G is a function that assigns each ordered pair & elements in G an element of G.

$o : (G \times G) \longrightarrow G$

o : binary Op.

Group :

A set G together with a binary operation is a group if

i) Associativity ie:

$(a\,b)\,c = a(b\,c) \quad \forall \quad a, b, c \in G.$

ii) Identity :

There is an element e in G s.t

$ae = ea = a.$

iii) Inverse :

For each element $a \in G$, there is an element $b \in G$ s.t.-

$ab = ba = e$

b is called the inverse of a.

eg: $\langle \mathbb{Z}, + \rangle$ (Notation for groups : $\langle \text{Nos}, \text{op} \rangle$.

1) Associative
2) Identity : 0.
3) For any m, inverse $-m \in \mathbb{Z}$

eg: $\langle \mathbb{Z}, \times \rangle$

1) Associative
2) Identity : 1.
3) 0 does not have inverse

ie: $\nexists\ m \in \mathbb{Z}$

In fact only 1, -1 have inverses

Eg: $G \{1, -1, i, -i\}$.

$\langle G, \times \rangle$.

1) Associativity satisfies.

2) Identity 1

3) inverse exists for all

Eg: $\langle Z_4, +_4 \rangle$ $+$ modulo 4.

$Z_4 = \{0, 1, 2, 3\}$.

$1 +_4 3 = (3+1) \pmod 4 = 0$.

1) Associative.

2) Identity is trial.

3) Inverse. for any m in Z_4.
inverse is $4 - m$
For $m = 0$, inverse is 0.

Eg: $\langle Z_4, *_4 \rangle$.

1) Identity = 1

2) for $m = 0$ doesn't have an inverse. ∴ NOT a group.

Eg: $\langle Z_6, \times_6 \rangle$

$Z_6 = \{1, 5\}$.

- Remove all entries that aren't co-prime with 6.

$\{1, 5\}$. ∵ their inverses don't exist.

Only $\langle Z^*, *_n \rangle$ are groups.

→ $\langle Z_n^* , \times_n \rangle$ is a group

$Z_n^* = \{ m \in Z_n \mid (m, n) = 1 \}$.

Q: $\langle Q^+ , \times \rangle$

1) Associative
2) Identity → 1
3) Inverse exists.

∴ Yes this is a group.

Q: $\langle M_2 , + \rangle$

$M_2 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in Z \right\}$

1) Associative
2) Identity $= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$
3) Inverse $= \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$

→ Identity is Unique:

By contradiction.
Let there be 2 identities e & e'

$ee' = e'e = e$

But $ee' = e'e = e'$

$\Rightarrow e'$ should be $= e$

∴ There exists only 1 identity.

Cancellation Property:

If $ba = ca \Rightarrow b = c$ | $ab = ac \Rightarrow b = c$.

Since $a \in G$, $a^{-1} \in G$

multiplying by a^{-1} from right:

$ba \cdot a^{-1} = ca a^{-1}$

Associativity: $b(a \cdot a^{-1}) = c(aa^{-1})$

$be = ce$

$b = c$. $\square$

→ Fact: Inverse is unique :-

Pf: Let $a \in G$, Let there be two inverses b, c.

Since b is inverse of a: $ab = ba = e$

Since c is inverse of a $ac = ca = e$.

$ab = ac \Rightarrow b = c$

Order of Group:

Order of a group is the no: of el' in the group. Denoted by $|G|$.

$\langle \mathbb{Z}, + \rangle$ $\quad$ $\langle Z_4, +_4 \rangle$

$|\mathbb{Z}| = \infty$ $\quad$ $|Z| = 4$

$\langle Z_4^*, \times_4 \rangle$

$|Z_4^*| = 2$.

$\langle \mathbb{Z}, +_n \rangle$

$|\mathbb{Z}| = n.$

$\langle \mathbb{Z}_n^*, \times_n \rangle$

$|\mathbb{Z}_n^*| = \phi(n)$ (Euler's ϕ-fn)

$\phi(p) = p - 1$; p is prime

$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$ $\alpha > 1$

$\phi(n) = \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m})$ Eulers.

$\phi(mn) = \phi(m) \cdot \phi(n)$.

$\Rightarrow \phi(n) = \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k})$

$= \phi(p_1^{\alpha_1}) \phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k})$

$= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots$

Eg: $\phi(36) = \phi(4 \cdot 9)$

$= \phi(2^2 \cdot 3^2)$

$= \phi(2^2) \cdot \phi(3^2)$

$= (2^2 - 2^1)(3^2 - 3^1) = 2 \cdot 6 = 12$

$|\mathbb{Z}_{36}^*| = 12.$

Fact. $(ab)^{-1} = b^{-1} a^{-1}$

Pf: We have

$ab(b^{-1} a^{-1})$

$= a(b b^{-1}) a^{-1}$

$= a \cdot e \cdot a^{-1}$

$= e \cdot aa^{-1}$

$= e$.

→ Repeatations of the same el are allowed in groups.

classmate
Date
Page

• Definition of Group:- Subgroup:

G. group, $H \leq G$

Then if H is a group under the operation of G then H is a subgroup of G.

Eg: $G = \{1, -1, i, -i\}$.

$H = \{1, -1\}$.

$\{1\}$ is a trivial sub-group

→ Subgroup to set: One Step Test.

G: group. $H \leq G$ $H \neq \phi$

If whenever $a, b \in H$ then $ab^{-1} \in H$ then H is subgroup G.

i) Pf: $e \in H$. → Claim.

since $H \neq \phi$ $\exists\ a \in H$

$\Rightarrow aa^{-1} \in H$

$\Rightarrow e \in H$.

ii) whenever $b \in H \Rightarrow b^{-1} \in H$ ... claim

Choose ~~a = e~~ $a = e$, $b = b$

$\Rightarrow ab^{-1} = eb^{-1} = b^{-1} \in H$.

iii) Associativity → trivial

iv) Closure: $a, b \in H$

Since $b \in H \Rightarrow b^{-1} \in H$

Since $a, b^{-1} \in H$

$\Rightarrow a(b^{-1})^{-1} \in H \Rightarrow ab \in H$.

Def: **ABELIAN grp:**

G is called Abelian if $\forall\ a, b \in G$

$ab = ba$

Eg: G : Abelian gp

$H = \{ x \in G \mid x^2 = e \}$

A: Let $a, b \in H$

then $a^2 = e$, $b^2 = e$.

Claim $ab^{-1} \in H$ $(ab^{-1})^2 = e$

we have: $(ab^{-1})(ab^{-1}) = e$.

$= a(b^{-1}a)b^{-1}$

$= a a b^{-1} b^{-1}$ (G is abelian)

$= a^2 \cdot (b^{-1})^2$

$= e \cdot e^{-1}$

$= e \cdot e = e$.

- **2ND STEP TEST:**

G, group $H \neq \phi$ $H \leq G$

then H is a sub group if

One Step test :-

ab^{-1}

$a, b \in H$.

i) $ab \in H$ whenever $a, b \in H$.

ii) $a^{-1} \in H$ whenever $a \in H$.

Pf: $H \neq \phi \Rightarrow \exists\, a \in H$.

$a^{-1} \in H$

$a \cdot a^{-1} = e \in H$.

Eg: Let G: Abelian.

$H = \{ x \mid |x| \text{ is finite} \}$

Defn (Order of an el):

Order of an el. $a \in G$ is the least +ve int n such that $a^n = e$.

$a^n = a * a * \cdots * a$ (n op.)

Eg: $\langle \mathbb{Z}_4, +_4 \rangle$

$|2| = 2$. $\quad 2^2 = 0$.

If no such n exists, then order is ∞.

Eg: $\langle \mathbb{Z}, + \rangle$

$|1| = \infty$.

Pf:- $e^{a \cdot 1} = e$

$\Rightarrow |e| = 1 \Rightarrow e \in H$

ii) Let $a, b \in H$.

$|a| = m \Rightarrow a^m = e$

$|b| = n \Rightarrow b^n = e$

$(ab)^{mn} = \underbrace{ab \cdot ab \cdot ab \cdots ab}_{mn}$

$\Rightarrow \quad (ab)^{mn} = (a^m)^n \cdot (b^n)^m$

$= e^n \cdot e^m = e \cdot e = e$

$\therefore \quad |ab| \leq mn$. (finite)

$\Rightarrow ab \in H$.

(iii) Let $a \in H$ $\quad |a|$ finite

$a^{m} = e^{-1} \Rightarrow a^{-m} = e \Rightarrow (a^{-1})^m = e$

$|a^{-1}| = m$. finite

$a^{-1} \in H$.

- **Definition**: Centre of a group :-

$Z(G) = \{ g \in G \mid gx = xg \quad \forall x \in G \}$.

is a subgroup of G

i) Since $xe = ex \quad \forall x$.

$e \in Z(G)$.

ii) let $a \in Z(G) \Rightarrow ax = xa \quad \forall x \in G$

$x = a^{-1} x a$

$xa^{-1} = a^{-1} x. \qquad a^{-1} \in Z(G)$.

iii) $a, b \in H$

$ax = xa \qquad \forall x \in G$

$bx = xb \qquad \forall x \in G$

$bax = bxa$

$(ab)x \; (= axb)$.

$= x(ab)$.

all generators are co-prime with n.

CYCLIC GROUPS :

A group G is cyclic if $\exists\ a \in G$ such that any $g \in G$ is $g = a^i$ for some $i \in \mathbb{Z}$

eg: $\langle \mathbb{Z}_4, +_4 \rangle$ $\exists$ an el. $1 \in \mathbb{Z}_4$ s.t. $m \in \mathbb{Z}_4$.

$1^i = m$.

Now, $\langle \mathbb{Z}_n, +_n \rangle$

$\langle m \rangle = \mathbb{Z}_4$

$(m, n) = 1$ ⟶ co primes.

⟶ $\langle \mathbb{Z}, + \rangle$.

$1^0 = 0$

$1^2 = 1+1 = 2.$

$1^1 = 1.$

$1^{-1} = -1.$

$1^{-2} = -2.$

Fact: Let G be a group. a be an element of order n then $a^k = e$ ⇒ n divides k

Fact: Let $a \neq b \in G$, $|G|$ is finite $*$ $ab = ba$ then $|ab|$ divides $|a|\,|b|$.

Pf: $|ab| = m$ $(ab)^m = e$

⇒ $(ab)(ab)\ldots$ $a^m b^m = e$

$a^s = e$ $\quad a^{st} = e$ — ①

$b^t = e$ $\quad b^{st} = e$ — ②

$m \mid st$

$a^{st}\ b^{st} = e \cdot e = e$

$\underbrace{(a \ldots a)}_{st}\underbrace{(b \ldots b)}_{st} = e$

$(ab)^{st} = e$

Fact: Let $|a| = n$; k is a +ve integer then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

& $|a^k| = \dfrac{n}{\gcd(n,k)}$

Pf: Let $d = \gcd(n, k)$

$\Rightarrow d \mid k$

$\Rightarrow (a^d)^s = a^k \quad s \in \mathbb{Z}$

$\therefore, \quad \langle a^k \rangle \subseteq \langle a^{\gcd(n,k)} \rangle$

Since $d = \gcd(n, k)$.

$\exists\ x, y \in \mathbb{Z}$

s.t. $d = nx + ky$

$a^d = a^{nx+ky} = a^{nx} \cdot a^{ky}$.

$= (a^n)^x \cdot (a^k)^y$

$e^x \cdot a^{ky} = a^{ky} = (a^k)^y$

let $x \in \langle a^d \rangle$

$\Rightarrow x = (a^d)^p \qquad p \in \mathbb{Z}$

From ① :-

$\Rightarrow x = \left((a^k)^q\right)^p = (a^k)^{qp} \in \langle a^k \rangle$

$\langle a^d \rangle \subseteq \langle a^k \rangle$.

Eg: $\langle \mathbb{Z}_6, +_6 \rangle$

$\langle 2 \rangle = \langle 2^0, 2^1, 2^2 \ldots \rangle$

$= \{0, 2, 4\}$.

Choose $a = 1 \quad |a| = 6$

$\langle 1^k \rangle = \langle 1^{(\gcd\langle n,k\rangle)} \rangle$.

Eg: Find all the subgroups of this $\langle \mathbb{Z}_{30}, +_{30} \rangle$.

$\langle 2 \rangle = \langle 1^2 \rangle = \langle 0, 2, 4 \ldots, 28 \rangle$.

$\langle 1^4 \rangle = \langle 1^8 \rangle = \langle 1^{16} \rangle = \langle 1^{26} \rangle$

$\langle 1^{22} \rangle = \langle 1^{28} \rangle$

GCD = 2

$\langle 3 \rangle = \langle 1^3 \rangle = \{0, 3, 6, 9, 12 \ldots 27\}$

$= \langle 1^9 \rangle = \langle 1^{21} \rangle = \langle 1^{27} \rangle$

ϕ maps from $G \to \bar{G}$
then ϕ^{-1} maps from $\bar{G}$ to G.

isomorphic groups have the same order.

Isomorphism:

An isomorphism ϕ from group G to a group $\bar{G}$ is a 1-1 & onto map $a \neq \bar{G}$ such that

$$\phi(ab) = \phi(a) \cdot \phi(b).$$

In this case we say that G is isomorphic to $\bar{G}$ denoted as

$$G \approx \bar{G}.$$

eg: Show that

$$\langle \mathbb{R}, + \rangle \approx \langle \mathbb{R}^+, \times \rangle$$

Define $\phi(x) = e^x$. $x \in \mathbb{R}$

This func. is 1-1 & onto.

let $a, b \in \mathbb{R}$

then $\phi(a+b) = e^{a+b} = e^a \cdot e^b$

$= \phi(a) \cdot \phi(b)$

$\therefore$ It is an isomorphism.

eg: Any cyclic group of order k is isomorphic to $\langle \mathbb{Z}_k, +_k \rangle$

Let $G = \langle a \rangle \quad |G| = k.$

$= \{ a^0, a^1, a^2 \ldots a^{k-1} \} \approx \{ 0, 1, 2 \ldots k-1 \}$

$$\phi(a^i) = i \pmod k.$$

Let $x, y \in \langle a \rangle$

$\Rightarrow x = a^s, \quad y = a^t$

$$\phi(xy) = \phi(a^s \cdot a^t)$$
$$= \phi\, a^{s+t}$$
$$= (s+t) \bmod k.$$
$$= [s \pmod k + t \pmod k] \bmod k.$$
$$= \phi(a^s) + \phi(a^t)$$
$$\text{ie: } \phi(x) \cdot \phi(y)$$

Eg: $G = \{1, -1, i, -i\}$

$\langle i \rangle = \langle -i \rangle$

Any cyclic gp of order k is isomorphic to Z_k

- Properties of isomorphism :-

$\phi: G \to \bar{G}$ is an isomorphism.

a) Let e & $\bar{e}$ be identities of G & $\bar{G}$ resp. then $\phi(e) = \bar{e}$

Pf: $\phi(e) = \phi(e \cdot e)$

$= \phi(e) \cdot \phi(e)$.

Multiply by $\phi(e^{-1})^{-1}$ on both sides

$\phi(e)^{-1} \cdot \phi(e) = \phi(e)^{-1} \cdot \phi(e) \cdot \phi(e)$

$\bar{e} = \bar{e}\, \phi(e)$.

$\Rightarrow \phi(e) = \bar{e}$

b) For every integer n & for every group element a in G

$$\phi(a^n) = [\phi(a)]^n$$

Pf: $\phi(\underbrace{a \cdot a \cdot a \cdots a}_{n}) = \phi(a) \cdot \phi(a) \cdots \phi(a)$

$= [\phi(a)]^n$

c) For any element $a, b \in G$, a & b commute if and only if $\phi(a)$ & $\phi(b)$ commute.

Pf: $\phi(ab) = \phi(a)\phi(b)$

$\phi(ba) = \phi(b)\phi(a)$.

If $ab = ba$ then RHS should also be equal.

$\rightarrow \quad \phi(a)\phi(b) = \phi(b)\phi(a)$

d) $G = \langle a \rangle$ if & only if $\bar{G} = \langle \phi(a) \rangle$

Let $G = \langle a \rangle$

Claim $\bar{G} = \langle \phi(a) \rangle$.

$\bar{g} \in \bar{G}$ is of the form $\bar{g} = (\phi(a))^m$

Since ϕ is onto :- $\exists\ g \in G$

s.t. $\phi(g) = \bar{g}$

Here $g = a^k$, $k \in \mathbb{Z}$

$\bar{g} = \phi(g) = \phi(a^k) = [\phi(a)]^k$

$\Rightarrow \bar{G} = \langle \phi(a) \rangle$

Fact: If ϕ $G \to \bar{G}$ is isomorphism then ϕ^{-1} $\bar{G} \to G$ is isomorphic.

Since ϕ is isomorphic $\Rightarrow$ ϕ is one-one & onto
$\Rightarrow$ ϕ^{-1} is also 1-1 & onto.

$$\phi^{-1}(\bar{a}\bar{b}) = \phi^{-1}(\bar{a}) \cdot \phi^{-1}(\bar{b}) \quad — (1)$$

$\exists$ a in G s.t. $\phi(a) = \bar{a}$
b in G s.t. $\phi(b) = \bar{b}$. — (2)

WKT: $\phi(ab) = \phi(a) \cdot \phi(b)$.

From (1): $\bar{a}\bar{b} = \phi(\phi^{-1}(\bar{a}) \cdot \phi^{-1}(\bar{b}))$.

From (2):

$$\phi(a) \cdot \phi(b) = \phi(\phi^{-1}(\phi(a)) \cdot \phi^{-1}(\phi(b)))$$
$$\phi(a) \cdot \phi(b) = \phi(ab)$$

Fact: If G is Abelian then $\bar{G}$ must be Abelian if $G = \bar{G}$.

COSETS & LAGRANGE TH.

G, a group. $H \subseteq G$ $H \neq \phi$
For $a \in G$

$$aH = \{ah \mid h \in H\}.$$

If H is a subgroup of G then
aH is called left co-set. Right coset Ha

Eg: $H = \{0, 3, 6\}$ in Z_9 under $+_9$

Consider

$$2H = \{ 2 +_9 h \mid h \in H \}$$
$$= \{2, 5, 8\}.$$

$$3H = \{ 3 +_9 h \mid h \in H \} = H$$

$$4H = \{ 4 +_9 h \mid h \in H \}.$$
$$\{4, 7, 1\}.$$

$G = H \cup 2H \cup 4H$

cardinality of the sets is the same

$|H| = |2H| = |4H| = r$

$|G| = 3r$

$3r \Rightarrow r \mid |G| \Rightarrow |H| \mid |G|$

× ——— ×

TUTORIAL

Q: Certain things whose no: is unknown.
when div by 3 rem is 2
when div by 5 rem is 3
when div by 7 rem is 2
No: of things = ?

$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

classmate

Date

Page

$m_1 = 3 \qquad m_2 = 5 \qquad m_3 = 7.$

$a_1 = 2 \qquad a_2 = 3 \qquad a_3 = 2.$

$\frac{m}{m_1} = \frac{3 \times 5 \times 7}{3} = 5 \times 7. = 35.$

Now, $35x + 3y = 1.$

$x = (-1) \qquad y = 12$

$\therefore, \quad b_1 = (-1). \qquad \text{—— (1)}$

$\frac{m}{m_2} = 21$

$21x + 5y = 1.$

$x = 1 \qquad y = -4$

$b_2 = 1 \qquad \text{—— (2)}$

$\frac{m}{m_3} = 15.$

$15x + 7y = 1.$

$x = 1 \qquad y = -2.$

$b_3 = 1.$

Now, $sol = \sum_{j=1}^{n} \frac{m}{m_j} b_j a_j$

$= 35 \times (-1)(2) + 21(1)(3) + 15(1)(2)$

$= -70 + 63 + 30$

$= -70 + 93$

$= 23.$

Q: $ax + by = c$.

a & b are given integers.

Are there possible values for x, y.

Condition if $\gcd(a, b) \mid c$ then

⇒ Yes, there are solutions for x, y.

GCD (888, 54).

$888 = 54 \times 16 + 24$

$54 = 24 \times 2 + 6$

$24 = 6 \times 4 + 0$

$6 = 54 - 24 \cdot 2$

$= 54 - (888 - 54 \cdot 16) \cdot 2$

$= 54 - 2(888) + 54 \times 32$

$= 888(-2) + 33(54)$

COSETS & LAGRANGES TH.

Properties of co-sets.

a) $a \in aH$

b) $aH = H$ iff $a \in H$

c) $aH = bH$ iff $a \in bH$

d) $aH = bH$ or $aH \cap bH = \phi$

Normal subgroup H

if $aH = Ha$ for all a in G

e). $aH = bH$ iff

$a^{-1}b \in H$.

f) $|aH| = |bH|$.

14.

a). $a = ae \in aH$ since $e \in H$.

b). Claim $aH = H \Rightarrow a \in H$

Since $aH = H \Rightarrow ah_1 = h_2$; $h_1, h_2 \in H$.

$ah_1h_1^{-1} = h_2h_1^{-1}$

$a = h_2h_1^{-1} \in H$

Claim: $a \in H \Rightarrow aH = H$ ie: $(aH \subseteq H) \wedge (H \subseteq aH)$

Let $x \in aH$ ie: $x = ah \in H$.

$\therefore aH \subseteq H$.

Let $y \in H$

$\Rightarrow y = a(a^{-1}y) \in aH$

$H \subseteq aH$.

c). $aH = bH \Rightarrow a \in bH$.

$ah_1 = bh_2$ $h_1h_2 \in H$

$a = bh_2h_1^{-1}$ but $h_2h_1^{-1} \in H$

$\therefore a = bH$ $a \in bH$

Also,

Since $a \in bH$

$a = bh$

Let $x \in aH \Rightarrow x = ah_1$, $h_1 \in H$.

$\therefore x = b(hh_1)$ but $hh_1 \in H$

$\therefore x \in bH \Rightarrow aH \subseteq bH$

let $z \in bH \Rightarrow z = bh_2$

$z = a(h^{-1}h_2) \in aH$

$\Rightarrow bH \subseteq aH$

$\therefore$

$aH = bH.$

d) $aH = bH$ or $aH \cap bH = \phi$

let $aH \cap bH \neq \phi$

$\Rightarrow \exists\ c \in aH \cap bH.$

$\Rightarrow c \in aH$ and $c \in bH$

$\Rightarrow cH = aH \wedge cH = bH.$

$\Rightarrow aH = bH$

e) $aH = bH$ iff $a^{-1}b \in H$

since $aH = bH \Rightarrow ah_1 = bh_2$; $h_1, h_2 \in H.$

$h_1 = a^{-1}bh_2$

$\underbrace{h_1h_2^{-1}}_{\in H} = a^{-1}b \in H.$ $\quad a^{-1}b \in H$

$a^{-1}b = h_1$

for ~~[illegible]~~ $b = ah_1$

~~[illegible]~~ let $x \in aH \Rightarrow y = ah_3$

$= bh_1^{-1}h_3.$

$= \in bH.$

$\therefore aH \subseteq bH$

classmate
Date
Page

Q. $|aH| = |bH|$

$f : aH \to bH$ $\quad$ f is 1-1 & onto.

$f(ah) = bh.$

→ f is 1-1.

$f(ah_1) = f(ah_2)$

$\Rightarrow bh_1 = bh_2 \Rightarrow h_1 = h_2.$

$\Rightarrow ah_1 = ah_2 \Rightarrow f$ is 1-1.

→ Onto:

Let $y \in bH \Rightarrow y = bh$ $h \in H$

Take $x = ah$

$f(x) = f(ah) = bh = y.$

N Proof for Lagrange's th.

Th. Let G be a finite group & H is a subgroup of G

$\Rightarrow |H| \mid |G|$

Pf: $G = a_1H \cup a_2H \cup \cdots \cup a_rH.$

& $a_iH \cap a_jH = \phi$ if $i \neq j$

& $|a_iH| = |a_jH|$ for $i \to j$ ★

Now, $|G| = |a_1H| + |a_2H| + \cdots + |a_rH|.$

$= r|H|$

$\Rightarrow |H| \mid |G|.$

Eg. For $|G| = 36$

Possibilities for order of subgroups :-

1, 2, 3, 4, 6, 9, 12, 18, 36.

• RINGS:

A ring R is a set with 2 binary operations addition & multiplication such that for all, $a, b, c \in R$:-

1) $a+b = b+a$.
2) $(a+b)+c = a+(b+c)$
3) There is an additive identity $0 \in R$ s.t. $a+0 = a$.
4) There is an element $-a \in R$ s.t. $a+(-a) = 0$
5) $a(bc) = (ab)c$
6) $a(b+c) = ab + ac$.

Remarks: If every non-zero el. has an inverse then it is a field.

Eg: $\langle \mathbb{Z}, +, \times \rangle$ is a ring :

All 6 properties are satisfied.

Eg: $\langle Z_n, +_n, \times_n \rangle$.

$\langle Z_n, +_n \rangle$ is a group.
& also, commutativity is true.

Now, for associativity under multiplication
$a \times_n (b \times_n c) = (a \times_n b) \times_n c$.
$a \times_n (b +_n c) = a \times_n b + a \times_n c$.

Eg: $\langle M_{m \times n}, +, \times \rangle$.

• Properties of Rings :-

a) $aO = Oa = O$

b) $a(-b) = (-a)(b) = -(ab)$.

c) $(-a)(-b) = ab$

d) $a(b-c) = ab - ac$.

Pf. a) $O = a + (-a)$.
$aO = a[a + (-a)]$

$ab = a(b + O)$
$ab = ab + aO$.

$ab + (-ab) = ab + (-ab) + aO$
$O = aO$.

$\because aO = O$.

b). Claim : $a(-b) + (ab) = O$

$a(-b + b) = O$ $\quad a(O) = O$

from (1)

$\Rightarrow \quad a(-b) = -(ab)$

Similarly $\quad (-a)(b) + ab = 0.$

$(-a+a)\,b = 0$

$0b = 0$

$\Rightarrow \quad \underline{(-a)(b) = -(ab).}$

INTEGRAL DOMAIN :

Def. (zero divisor) :

A zero divisor is a non-zero el. a of a commutative ring R such that $\exists$ a non zero el. $b \in R$ with $ab = 0$

[commutative ring : Multiplication is comm] $ab = ba.$

Eg: (1) In $\langle \mathbb{Z}, +, \times \rangle$ there are no zero divisors.

(2) In $\langle Z_n, +_n, \times_n \rangle$.

Let $n = 4$.

$Z_4 = \{0, 1, 2, 3\}$.

$a = 2$, $b = 2$ are zero divisors because $a \neq 0$, $b \neq 0$ in $\langle Z_4, +_4 \rangle$.

But $a \times_4 b = 2 \times_4 2 = 0$.

★ Int. Dom: It is a commutative ring without zero divisors

Eg → $\langle Z_p, +_p, \times_p \rangle$ p ... prime

Eg → $\langle Z, +, \times \rangle$

(3) $\langle Q^+, \times, + \rangle$

$\langle Q^+, \times \rangle$ ... is a group.

Let $p, q, r \in Q^+$

$(p+q)+r = p+(q+r)$

$p+qr = (p+q)\cdot(p+r)$ ✗ FAIL] ✗

(4) $\langle D_{m\times n}, +, \times \rangle$.

$$\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}_a \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}_b = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$a \neq 0$, $b \neq 0$ but $ab = 0$.

● FIELD:

A field is a commutative ring in which every non-zero el. is invertible wrt to multiplication. (second op.)

Eg: $\langle R, +, \times \rangle$

$\langle Q, +, \times \rangle$

$\langle Z_p, +_p, \times_p \rangle$. p → prime.

TUTORIAL - 4:

5) c) $(n-1)$ in Z^*_n $n > 2$.

16) 

GRAPH TH.

Proof: Prove there are even no. of odd deg. vertices

$$\sum_{i=1}^{n} d(v_i) = 2|E|.$$

$$\sum_{i=1}^{p} d^o(v_i) + \sum_{i=1}^{s} d^e(v_i).$$

even.

$$\sum_{i=1}^{p} (2k+1) = \text{even} - \text{even}.$$

$\Rightarrow$ p $\rightarrow$ even.

In an simple graph, with $|V| = n$ then ~~strict degree~~ $|v_i| \leq n-1$ for all $i = 1 \rightarrow n$.

Proof: In a simple graph, with at least 2 vertices, then G has 2 vertices with the same degree.

Case 1: G is ~~considered~~ connected then $d(v_i) = 0 \quad \forall i = 1 \dots n$.

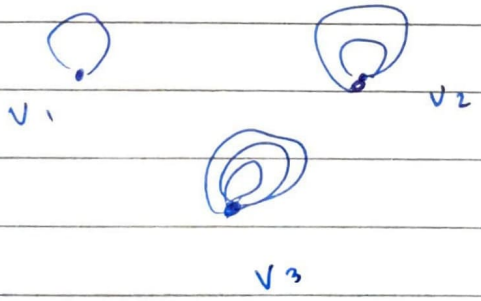
Choose pigeons → vertices.
pigeon holes → degrees.

∴, By PHP, n vertices n−1 degrees.
∴ at least 2 have same degree.

Case 2: G is not connected, then we have a graph with $(n-1)$

Again utilize PHP:-
$n-1$ vertices $n-2$ edges:

Q: Construct a non-simple graph whose vertices have different degrees.



→ Bouquet graph → only 1 vertex.

→ complete graph → every ~~edge~~ vertex has an edge with every other vertex.

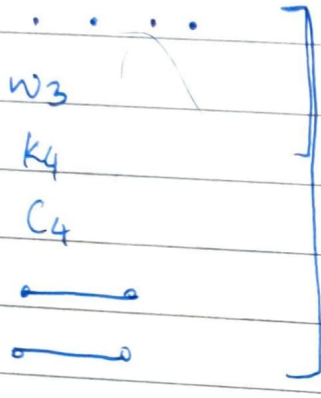
Only wheel graph that is regular is W_3

→ Regular → all vertices have same degree.

Q: Construct all regular simple n vertex for $n = 2, 3, 4, 5$

$n = 2$:  2.

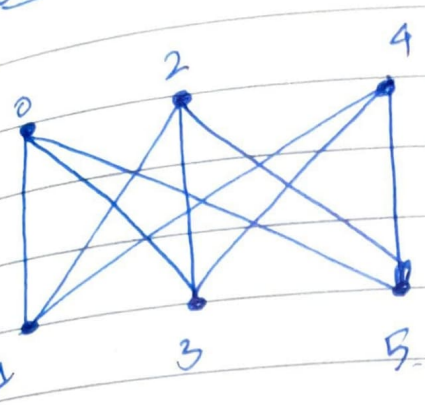
$n = 3$  2.

$n = 4$ 
W_3
K_4
C_4

$= 6.$

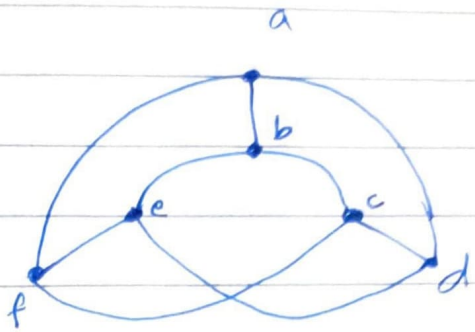
→ Bipartite Set: vertex set can be partitioned s.t every edge joins a vertex in one cell to a vertex in another cell.

- A path graph is bipartite
- Even cycle graph " "



$K_{3,3}$.

is bipartite.



$\begin{pmatrix} a \\ c \\ e \end{pmatrix} \begin{pmatrix} b \\ d \\ f \end{pmatrix}$

bipartite.

∴ Mapping :-

$0 \longrightarrow a$

$2 \longrightarrow c$

$4 \longrightarrow e$

$1 \longrightarrow b$

$3 \longrightarrow d$

$5 \longrightarrow f$

To check for isomorphism :-

→ check if bipartite

→ check for cycles.

Bipartite graphs cannot have odd cycles

Spanning cycle is a cycle in a graph that contains all the vertices of a graph.