PROOF TECHNIQUES

* Terminology

- Definition: Something already given, and doesn't require proof.
- Theorem (or Result): Something which has been proven to be true.
- Axiom: Something which is considered to be true, (without any proof).

Ex: Probability of an event, $P(E)$ is, $0 \leq P(E) \leq 1$.

Ex: Euclid's Axiom: If there are two points in a plane then there is a unique line passing through them.

* Direct Proof:

In a direct proof, we assume the antecedent to be true, and then use rules of inference, axioms, definitions, and/or previously proven theorems to show that the consequent is true.

Ex. Show that every Int. n divisible by 6, is divisible by 3

Assume n is divisible by 6, i.e., $n = 6K = 2 \times 3 \times K$

Say, $2K = l$, then, $n = 3 \times l$, therefore n is divisible by 3

Ex. If a, b are consecutive integers then, sum a+b is odd.

Proof:

Given: a & b are consecutive integers, i.e. $b = a+1$

p: $a = 2n$, then $b = a+1 = 2n+1$

or $a = 2n+1$, then $b = a+1 = 2n+1+1 = 2(n+1)$

then q: $a+b = 2n+2n+1 = 4n+1 = 2(2n)+1$

or $a+b = 2m+1+2m+2 = 4m+2+1$

$\Rightarrow 2(2m+1)+1$

$\therefore$ $a+b$ is odd.

Ex. If n is an odd integer, then n^2 is odd integer.

Proof: Given: n is odd.

p: $n = 2k+1$

then, $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$

$\Rightarrow 2(2k^2+2k)+1$

$\Rightarrow 2l+1$

is odd.

Ex. If m & n are perfect square, then $m+n+2\sqrt{mn}$ is also perfect square.

Perfect Square: An integer 'a' is perfect square, if $\sqrt{a} = b$, & b is an integer.

$\exists a\,([a \in Z] \wedge [\sqrt{a} \in Z]) \rightarrow a$ is perfect square.

Proof:

Given: m & n are perfect sq.

p: $m = k^2$, $n = l^2$, $k, l \in Z$

then,

$$m+n+2\sqrt{mn} = k^2 + l^2 + 2lk = (k+l)^2$$

$\therefore$ $m+n+2\sqrt{mn}$ is a perfect square.

Note: $a|b$: a divides b.

$a|b \not\equiv a \div b$.

Ex.

$8 \div 4 = 2 = 8/4$ {$a|b$ acts as boolean operator}

$4|8 =$ True {4 divides 8}

$8|4 =$ False {8 divides 4}

$\therefore$ $a|b \Rightarrow b = ax(x)$

Ex. If $5|2a$, for $a \in Z$, then $5|a$.

Proof: If $5|2a$, $2a = 5 \times K$

then, K has to be even for $2a$ is even.

$\Rightarrow a = 5 \times \frac{K}{2} = 5 \times l$

* Proof by Contraposition

A type of indirect proof that makes use of the fact that $p \to q$ is equivalent to its contrapositive, $\neg q \to \neg p$. So we assume $\neg q$ is true. then work to prove. $\neg p$ is true.

Ex. If n^2 is even, then n is even.

Say. we try by Direct Proof.

$n^2 = 2K$

$\sqrt{n^2} = n = \sqrt{2k}$

There is no good way to show $\sqrt{2k}$ is even.

Statement $(p \to q)$: If n^2 is even, then n is even.

$(\neg q \to \neg p)$: If n is odd, then n^2 is odd.

$n = 2K+1$

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

$\Rightarrow 2l+1$

$\therefore \neg q \to \neg p$

$\therefore p \to q$.

Ex. If n is integer, & $3n+2$ is odd then n is odd.

$\neg q \to \neg p$: If n is even, then $(3n+2)$ is even

$n = 2K$, $\quad 3n+2 = 3 \times 2K + 2$

$\Rightarrow 2(3K+2) = 2l$

$\therefore \neg q \to \neg p$

Ex. If $n = ab$, where a, b are +ve, then, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

$\neg q \rightarrow \neg p$: If $a > \sqrt{n}$ & $b > \sqrt{n}$, then $n \neq a \times b$

Let $a = \sqrt{n} + K$ $\quad b = \sqrt{n} + l$

$$a \times b = (\sqrt{n} + K)(\sqrt{n} + l)$$
$$\Rightarrow n + \sqrt{n}(K + l) + Kl$$
$$\therefore a \times b \Rightarrow n + S$$
$$\therefore a \times b \neq n$$

Ex. Prove using Direct Proof & Proof by Contraposition: Suppose $x \in Z$. If $7x + 9$ is even then x is odd.

Proof: Direct Proof

p: $7x + 9$ is even.

i.e. $\underbrace{7x}_{\text{odd}} + \underbrace{9}_{\text{odd}} = 2K$

then $7x$ must be odd for $7x+9$ to be even

$\underbrace{7x}_{\text{odd}}$

then x must be odd for $7x$ to be odd.

Proof by Contraposition

$\neg q \rightarrow \neg p$: If x is even, then $7x + 9$ is odd.

$x = 2K$, then

$$7x + 9 = 14K + 9 = \underbrace{2(7K)}_{\text{even}} + \underbrace{9}_{\text{odd}}$$

even + odd is odd.

* Rational Number: Any number that can be represented as p/q, where $p, q \in \mathbb{Z}$ & $q \neq 0$.

Ex. If m, n are non-zero +ve integers, then prove that $\frac{m+n}{mn}$ is rational.

$(m+n)$ is integer & mn is integer & $\neq 0$.

$\therefore \frac{m+n}{mn}$ is rational.

• Summation of Rational No.: Rational # + Rational # = Rational #

* Irrational Numbers: Any number that can't be represented as p/q, where $p, q \in \mathbb{Z}$ & $q \neq 0$.

Ex. $\sqrt{2}$, $\sqrt{3}$, π, e, $\sqrt{\text{irrational \#}}$

Ex. If r is irrational, then $\sqrt{r}$ is irrational.

$\neg q \rightarrow \neg p$: If $\sqrt{r}$ is rational, then r is rational

let $\sqrt{r} = \frac{p}{q}$, $p, q \in \mathbb{Z}$ & $q \neq 0$.

$r = \frac{p \times p}{q \times q}$ → integer, → integer & $q^2 \neq 0$.

$\therefore$ r is rational.

* Proof by Contradiction

To prove P, you prove that not P would lead to ridiculous result, and so P must be true.

Ex. Prove: There is no largest integer.

Note: ∞ is not a number. Its just an idea of something really large.

Lets assume 'n' is the largest integer.

But, $(n+1)$ is also an integer & $(n+1) > n$.

Hence must not be the largest integer.

* . Natural No.: 1, 2, 3, 4, ... {Positive Integers}
  . Whole No.: 0, 1, 2, 3, 4, ... {Non-negative Integers}

Ex. Prove: If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.

Assume: $a^2 - 4b = 2$

$a^2 = \underbrace{2 + 4b}_{\text{even}}$

then a must be even

$\therefore a = 2k$

$\Rightarrow (2k)^2 - 4b = 2$

$\Rightarrow \underbrace{2(k^2 - b)}_{\text{even}} = \underbrace{1}_{\text{odd}}$ $\therefore$ Contradiction.

Ex: Prove $\sqrt{2}$ is irrational

W.K.T: a rational no. of form where both num. & denom. are even is not in lowest form

Assume: $\sqrt{2}$ is rational.

$\therefore \sqrt{2} = \frac{p}{q}$ in lowest form.

then (p, q) can be
$(e, o), (o, o), (o, e)$

$\Rightarrow 2q^2 = p^2$
(2q² is even)

then $p^2 \& p \Rightarrow$ even
$p = 2k$.

$\Rightarrow 2q^2 = (2k)^2$

$\Rightarrow q^2 = 2k^2$

then $q^2, q \Rightarrow$ even.

then $\frac{p}{q}$ is not in lowest form.

$\therefore$ Contradiction.
& Assumption was wrong.

$\therefore \sqrt{2}$ is irrational.

* Mathematical Induction

Ex. Suppose there is a ladder with steps 1, 2, 3, 4, ...
For a person, there are two rules:
(1) They can climb the 1st step.
(2) If they are on p^{th} step, they can go to $(p+1)^{th}$ step.

- Can the person go to 1000^{th} step? Yes.
- Can the person go to $(999999)^{999...9+n}$ step? Yes.
- Can the person go to "∞^{th}" step? ∞ is not a no., so there is no step no. ∞.

So a person can go to any step where the step no. is a natural no.

* The principle of Mathematical Induction states that for some property P(n) if

P(0) is true } Base Case

&

For any natural no. 'n', $P(n) \rightarrow P(n+1)$

then,
P(n) is true for any natural no. 'n'.

Ex. Show that : $1+2+\dots+n = \frac{n(n+1)}{2}$

$P(n)$: $1+2+3+\cdots+n = \frac{n(n+1)}{2}$

Base Case: $(n=1)$

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

Assuming: $P(K)$ is true, i.e.

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

Now, $P(K+1)$:

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

$$\Rightarrow \frac{K(K+1)+2(K+1)}{2}$$

$$\Rightarrow \frac{(K+2)(K+1)}{2}$$

$\therefore$ LHS = RHS

$\therefore$ $P(K) \rightarrow P(K+1)$

Ex. Show that for all non-negative integers, 'n',

$1+2+2^2+\cdots+2^n = 2^{n+1}-1$

Base Case: $n=0$

$$2^0 = 1 = 2^{0+1}-1 = 1.$$

Assuming: $P(K)$ is true.

$$1+2+2^2+\cdots+2^K = 2^{K+1}-1.$$

Then, $P(K+1)$:

$$1+2+2^2+\dots+2^K+2^{K+1} = 2^{K+1}-1+2^{K+1}$$

$$\Rightarrow 2\times 2^{K+1}-1$$

$$\Rightarrow 2^{K+2}-1$$

$\therefore$ LHS = RHS.

$\therefore P(K) \rightarrow P(K+1)$

Ex. Show, n^3-n is divisible by 3, where 'n' is +ve integer.

Base Case: $n=1$

$1^3-1=0$ is divisible by 3.

Assumption: $P(K)$ is true, i.e.,

K^3-K is divisible by 3.

Then $P(K+1)$:

$$(K+1)^3-(K+1)$$

$$\Rightarrow K^3+3K^2+3K+1-K-1$$

$$\Rightarrow K^3+3K^2+2K$$

$$\Rightarrow K^3-K+3K^2+3K$$

$$\Rightarrow \underbrace{(K^3-K)}_{\text{div by 3}} + \underbrace{3(K^2+K)}_{\text{div by 3.}}$$

$\therefore P(K+1)$ is true.

$\therefore P(K) \rightarrow P(K+1)$

NUMBER THEORY (BASICS)

* Summation Notation:

$$\sum_{i=1}^{n} x_i$$

last value of i → n

starting value of i → $i=1$

- Shifting indices of summation

Ex. $\sum_{j=0}^{3} 2j$ Shift summation with 1 as start.

$$\sum_{i=1}^{4} 2(i-1)$$

Ex. $\sum_{i=2}^{19} i(i-2)$ Shift summation with 1 as start

$$\sum_{i=1}^{18} (i+1)(i-2+1) = \sum_{i=1}^{18} (i^2-1)$$

Ex. $\sum_{i=1}^{n} \frac{i-1}{n}$ Start from 0.

$$\sum_{i=0}^{n-1} \frac{(i+1)-1}{n} = \sum_{i=0}^{n-1} \frac{i}{n}$$

• Summation Identities

1. $\sum_i a x_i = a \sum_i x_i$

2. $\sum_i (x_i + y_i) = \sum_i x_i + \sum_i y_i$

3. $\sum_{i=a}^{b} f(x) = \sum_{i=0}^{b} f(x) - \sum_{i=0}^{a-1} f(x)$

* AP & GP

• Arithmetic Progression:

first term = a common diff. = d

$$a_n = a + (n-1)d$$

$$S_n = \frac{n}{2}(2a + (n-1)d)$$

↳ Sum of first n terms of AP

• Summation Formulas:

* $1 + 2 + \dots + n = \frac{n(n+1)}{2}$

* $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$

* $1^3 + 2^3 + \dots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$

• Geometric Progression

first term = a common ratio = r

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

$$S_n = \frac{a(1-r^n)}{(1-r)}, \quad n \text{ is finite}, \; r \neq 1$$

$$S_n = \frac{a}{1-r}, \quad \text{Infinite series}$$

$$S_n = na, \quad r = 1$$

• Arithmetic-Geometric Progression

Ex. $1, 2, 3, \ldots n$ (AP)

$x, x^2, x^3, \ldots x^n$ (GP)

$$x + 2x^2 + 3x^3 + \ldots + nx^n \quad \text{(AGP)}$$

Ex. $a_n = \begin{cases} n+1, & n \text{ is odd} \\ 1, & \text{otherwise} \end{cases}$ Find $\sum_{n=0}^{\infty} a_n x^n$

$$S = a_0x^0 + a_1x^1 + a_2x^2 + a_3x^3 \ldots$$

$$\Rightarrow 1 + 2x + x^2 + 4x^3 + x^4 \ldots$$

$$\Rightarrow 1 + x^2 + x^4 + \ldots + 2(x + 2x^3 + 3x^5 + 4x^7 + \ldots)$$

$$\Rightarrow \frac{1}{1-x^2} + 2(S')$$

$$S' = x + 2x^3 + 3x^5 + 4x^7 + \ldots$$
$$-x^2S' = -x^3 + 2x^5 + 3x^7 + \ldots$$
$$S'(1-x^2) = x + x^3 + x^5 + x^7 + \ldots$$

$$S' = \frac{x}{(1-x^2)^2}$$

$$\therefore S = \frac{1}{1-x^2} + \frac{2x}{(1-x^2)^2}$$

* Division Algorithm

Let a be an integer & d a positive integer, then there are unique integers q & r, with $0 \le r < d$ such that

$$a = dq + r$$

& $r = a \bmod d$

Q0. if $r \neq 0$ then $d \nmid a$ {d doesn't divide a}

Ex. Q & R when 101 is divided by 11?

$101 = 11 \times 9 + 2$
↳Q ↳R

Ex. Q & R when −11 div. by 3.

$-11 = 3 \times (-4) + 1$

{ $-11 = 3 \times (-3) + (-2)$ is incorrect.
r cant be less than 0 }

* Modular Arithmetic

$r = a \bmod m$
{ r is remainder when a is divided by m }

* Congruency: 'a' is said to be congruent to b mod n, if $n \mid (a-b)$ & is denoted by

$a \equiv b \pmod{m}$ or $a \equiv_m b$

Ex. $23 \equiv 7 \pmod{8}$
Ex. $23 \equiv 3 \pmod{10}$

- If $n \mid (a-b)$ then it's not necessary that $n \mid a$ & $n \mid b$

* Theorem: Let 'a' & 'b' be integers & let 'm' be a positive integer, then $a \equiv b \pmod m$ if & only if $a \bmod m = b \bmod m$

Proof: $p \to q$: If $a \bmod m = b \bmod m$ then, $a \equiv b \pmod m$.

Say, $r = a \bmod m = b \bmod m$.

Also, $a = m \times k_1 + r$ $\quad b = m \times k_2 + r$

$a \equiv b \pmod m$ is then,

$$m \mid (a-b) \Rightarrow (a-b) = (m \times k_1 + r) - (m \times k_2 + r)$$
$$= m(k_1 - k_2)$$
$$\therefore m \mid (a-b) \quad \because \text{remainder} = 0.$$

Ex. For 5, which are the values which give different remainders.

0: 0, 5, 10, 15, 20, ...
1: 1, 6, 11, 16, 21, ...
2: 2, 7, 12, 17, 22, ...
3: 3, 8, 13, 18, 23, ...
4: 4, 9, 14, 19, 24, ...

} all these values are congurent to each other, i.e $a \bmod 5 \equiv b \bmod 5$

Each of the series consist of values congursent with value from the same series.

- Therefore these all mean the same thing:
$a \equiv b \bmod m$, $m \mid (a-b)$, $a \bmod m = b \bmod m$.

classmate
Date
Page

- If $a \bmod m = n$, then, $(a \pm m) \bmod m = n$
  and also,

$$(a \pm km) \bmod m = n$$
$$k \in \mathbb{Z}$$

- $a \equiv b \bmod m$ is same as $b \equiv a \bmod m$.

Ex. If $a \equiv b \bmod n$, is $a+m \equiv b+n \bmod n$ as well?

$a \equiv b \bmod n : n \mid (k_1 n + r) - (k_2 n + r)$
$\Rightarrow n \mid [(k_1 - k_2)n]$.

$a+m \equiv b+n \bmod n : n \mid (k_1 n + r + m) - (k_2 n + r + n)$
$\Rightarrow n \mid [(k_1 - k_2)n]$.

Hence True.

Ex If $a \equiv b \bmod n$, then is $a+k \equiv b+k \bmod n$

$a \equiv b \bmod n : a \bmod n = b \bmod n$
$\Rightarrow r = r$.

$a+k \equiv b+k \bmod n : (a+k) \bmod n = (b+k) \bmod n$
$\Rightarrow (a \bmod n + k \bmod n) \bmod n = (b \bmod n + k \bmod n) \bmod n$
$\Rightarrow (r + k\%n)\%n = (r + k\%n)\%n$

$\therefore$ LHS = RHS

- If $a \equiv b \bmod n$ & $b \equiv c \bmod n$, then $a \equiv c \bmod n$

* If we have,

$a = b$

$c = d$

then we can,

$a \pm c = b \pm d$

$a \times c = b \times d$.

Similarly, if,

$a \equiv b \pmod n$

$c \equiv d \pmod n$

then

$a + c \equiv b + d \pmod n$

$a - c \equiv b - d \pmod n$

$a \times c \equiv b \times d \pmod n$

- Can you cancel abritrary number?

$8 \times 2 \equiv 3 \times 2 \pmod{10}$

$\Rightarrow 8 \equiv 3 \pmod{10}$

Not true. ∴ Cancelling doesn't always give right answer.

Ex. Reduce $100^5 \pmod 7$.

$\Rightarrow 100^5 \pmod 7 = (100 \% 7)^5 \% 7 = (2^5) \% 7$

$\Rightarrow 4$

classmate
Date
Page

* . $(a+b) \% n = (a\%n + b\%n) \% n$

. $(a \times b) \% n = (a\%n \times b\%n) \% n$

. $a^k \% n = (a\%n)^k \% n$

Ex. Simplify $(17)^{753}$ mod 9.

$(17)^{753} \% 9$

$\Rightarrow (17\%9)^{753} \% 9$

$\Rightarrow (-1\%9)^{753} \% 9$

$\Rightarrow (-1)^{753} \% 9$

$\Rightarrow (-1) \% 9$

$\Rightarrow 8$

Ex. Simplify $13^{99} \% 17$

$\Rightarrow (13)^{99} \% 17$

$\Rightarrow (-4)^{99} \% 17$

$\Rightarrow -4 \times (4)^{98} \% 17$

$\Rightarrow -4 \times (16)^{49} \% 17$

$\Rightarrow (-1 \times 4 \times (16)^{49}) \% 17$

$\Rightarrow [(-1)\%17 \times 4\%17 \times (-1)\%17] \% 17$

$\Rightarrow (16^2 \times 4) \% 17$

$\Rightarrow 1 \times 4 \% 17$

$\Rightarrow 4$

Ex. Simplify $3^{51} \% 5$

$\Rightarrow 3^{51} \% 5$

$\Rightarrow (-2)^{51} \% 5$

$\Rightarrow (-2 \times (-2)^{50}) \% 5$

$\Rightarrow (-2\%5 \times (4)^{\frac{25}{\%5}}) \% 5$

$\Rightarrow (3 \times 4) \% 5$

$\Rightarrow 2$

Ex. Simplify $(17 \times 18) \% 19$.

$[(-2) \times (-1)] \% 19$

$\Rightarrow 2$

Ex. Simplify $7^{2015} \% 48$.

$\Rightarrow 7^{2015} \% 48$

$\Rightarrow (7 \times 7^{2014}) \% 48$

$\Rightarrow (7 \times 49^{1007}) \% 48$

$\Rightarrow (7 \times 1) \% 48$

$\Rightarrow 7$

* Primes & Greatest Common Divisor

* Prime: An integer p, greater than 1, is prime if & only if the only +ve factors of p are 1 & p.

Statement: If 'a' is composite one of its divisors has to be less than equal to $\sqrt{n}$.

* GCD: For 'a' & 'b' their GCD is the largest integer that divides both of them.

Statement: 'a' & 'b' are relatively prime, if their GCD is 1.

Euclidean Algorithm:

$$\gcd(a, b) = \gcd(b \% a, a) \text{ if } b \% a \neq 0$$
$$= a, \text{ if } b \% a = 0$$

Ex. gcd (91, 287)

$287 \% 91 = 14$

$\Rightarrow$ gcd (14, 91)

$91 \% 14 = 7$

$\Rightarrow$ gcd (7, 14)

$14 \% 7 = 0$

$\therefore$ gcd (91, 287) = 7

PROPOSITIONAL LOGIC

* Mathematical Logic: The rules of logic specify the meaning of mathematical statements.

Natural language is ambiguous & hence it is difficult to represent different Mathematical reasonings in it.

- Mathematical Logic are of different types, the two of our interest are: Propositional Logic & First Order Logic.

* Propositional Logic:

- The world of Propositional Logic has only two types: True or False. Either something is True or it is False.

- Proposition: A declarative statement that can either be true or false & not both.

Ex.
- Drilling for oil caused dinosours to be extinct.
- All cows are brown.
- $2 \times 2 = 5$

Ex. Not Propositions:
- Sit down.
- Are you going? {Although a T or F question, but still question, the value of the "question stmt" isn't itself T or F}
- $x + 2 = 2x$ {x is a variable. Truth value depends on x}

Ex. Is the following proposition:

(1) Today is Friday
(2) He is a good boy.
(3) John is a good boy.

Depends on the author. There is an ambiguity between the exact definition of a statement being proposition.
{Won't be asked anywhere}

* Standard Conclusion:

Question, Command, Exclamation statements are never proposition.

Ex. "This statement is false".

Not a proposition, since self-contradiction.

* Propositional Variable: A variable representing a proposition.

* Compound Propositions: Propositions created with atomic propositions using connectives like, "and", "or", etc.

Ex: p: A is good. q: B is good. } atomic proposition

$p \wedge q$: A and B are good.

* Standard Logical Connectives:

① Negation	⑤ Implication
② And	⑥ Bi-Implication
③ Or	⑦ NAND
④ Ex-Or	⑧ NOR

* Negation ($\neg$)

If p is any proposition, then negation of p denoted by, $\neg p$ is the statement:

"It is not the case that p".

Ex. P: This book is interesting.

$\neg p$ can be stated as:

(1) This book is not interesting.

(2) This book is uninteresting.

(3) It is not the case that this book is interesting.

p	$\neg p$
T	F
F	T

* Conjunction ($\wedge$)

If p & q are two propositions then their conjunction, $p \wedge q$ is the statement

"p and q"

p	q	$p \wedge q$
F	F	F
F	T	F
T	F	F
T	T	T

Ex. c: Joe is a good president.
d: Joe is a boomer.

Stmt: Joe is a good president even though Joe is a boomer.

$c \wedge d$.

- Similary, 'but', 'however', 'yet', etc. in English are used to mean conjunction only.
- "," also means conjunction in logic.

* Disjunction ($\vee$)

If p & q are propositions, then their disjunction, $p \vee q$ is the statement: "p or q".

Ex. p: He will come on Monday.
q: He will come on Sunday.

$p \vee q$: He will come on Monday or Sunday.

p	q	p ∨ q
F	F	F
F	T	T
T	F	T
T	T	T

(Also called Inclusive OR)

* Exclusive Or (⊕):

If p & q are propositions, then their exclusive or, p ⊕ q, is the statement: "p or q but not both"

p	q	p ⊕ q
F	F	F
F	T	T
T	F	T
T	T	F

(Also called XOR)

* Some ambiguities:

① "p or q" given in exam. like, "She is a singer or poet" would mean p ∨ q & not p ⊕ q.

② "either p or q" is ambiguous & hence not generally given in exam.

Ex. p: This book is interesting.
q: I'm staying at home.

$p \oplus q$: Either this book is interesting or I'm staying at home.

* NAND and NOR

NAND: Negation of AND $(\uparrow) = \neg(p \wedge q)$
NOR: Negation of OR $(\downarrow) = \neg(p \vee q)$

p	q	$p \uparrow q$	$p \downarrow q$
F	F	T	T
F	T	T	F
T	F	T	F
T	T	F	F

* Conditional / Implication ($\rightarrow$)

If p & q are propositions, then $p \rightarrow q$ is the statement:

"if p then q"

$p \rightarrow q$

p: hypothesis / antecedant
q: conclusion / consequent

* $p \to q$ can be interpreted as: the conclusion q must be true as long as the hypothesis p is true.

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

Ex: p: You take Rajdhani.
q: You reach Delhi

$p \to q$: If you take Rajdhani, then you reach Delhi.

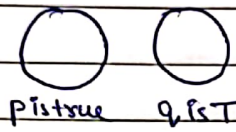
This statement will be true when one takes Rajdhani & reaches Delhi. It is still true if one doesn't take Rajdhani, & reaches Delhi. The claim is still not false when Rajhani is not taken & one doesn't reach Delhi.

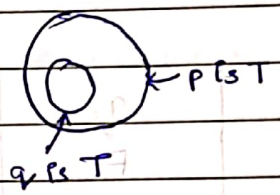
The claim only becomes false when Rajdhani is taken but one doesn't reach Delhi.

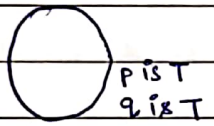
* $p \to q$ can be written as:

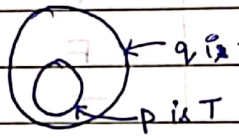
① if p then q.
② p is sufficient for q
③ q is necessary for p
④ p only if q
⑤ q unless not p
⑥ q whenever p
⑦ q follows from p

Ex. If it is known that $p \to q$ is false which of the following diagrams is possible?

(A) 

(B) 

(C) 

(D) 

A & B are possible, since at least one case where p is true & q is false.

Examples for above diagrams:

A: If x is greater than 0, x is -ve integer.
B: If p is prime, then p is odd
C: If x is divisible by 2, x is even.
D: If x is Natural no., x is integer

* . Implication is not commutative.

$$p \to q \neq q \to p$$

. Implication is right associative.

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

* If ≡ When ≡ Whenever ≡ Provided that ≡ Given that

* Biconditional ($\leftrightarrow$)

If p & q are propositions, then $p \leftrightarrow q$ is the statement:

"p if and only if q"

- $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

(if p true, q true) and (if q is true, p true)

Ex. p: x is even q: x+2 is even.

$p \leftrightarrow q$: x is even if and only if x+2 is even.

p	q	$p \rightarrow q$	$q \rightarrow p$	$p \leftrightarrow q$
F	F	T	T	T
F	T	T	F	F
T	F	F	T	F
T	T	T	T	T

(By this, $p \leftrightarrow q$ is logically equivalent to $p \odot q$, {p XNOR q})

* $p \leftrightarrow q$ can be read as:

① p if and only if q
② p is sufficient and necessary for q
③ p double implies q.

* In general in English, "if and only if" is not explicit, rather, "if" is used & "if and only if" is implied.

* Implication tells property. Biimplication tells definition.

Ex. If I'm PM of India, then I am Indian.

Being Indian is a property of PM of India.

Ex. x is even if and only if x is multiple of 2.

Being multiple of 2 is definition of even.

Ex. Let p represent true statement while q & r represent false statements. Find truth value of:

(1) $\sim [(\neg p \wedge \neg q) \vee \neg q] = F$
(2) $\neg (p \wedge q) \wedge (r \vee \neg q) = T$
(3) $\neg (\neg p \wedge \neg q) \vee (\neg r \vee \neg p) = T$

** Precedence of Connectives:

1. $\neg$
2. $\wedge$
3. $\vee$
4. $\rightarrow$
5. $\leftrightarrow$

Ex. $\neg p \wedge q \equiv (\neg p) \wedge q$
$\not\equiv \neg(p \wedge q)$

Ex. $\neg a \wedge b \rightarrow q \leftrightarrow r$
$\equiv \{[(\neg a) \wedge b] \rightarrow q\} \leftrightarrow r$

Ex. $p \vee q \wedge r$
$\equiv p \vee (q \wedge r)$

- Implication is right associative.

Ex. $p \rightarrow q \rightarrow r$
$\equiv p \rightarrow (q \rightarrow r)$

Note: For other connectives paranthesis would be specified.

Ex. Suppose that the stmt $[(p \wedge q) \vee r] \rightarrow (r \vee s)$ is false. Find the values of p, q, r and s.

$(p \wedge q) \vee r = T$
$\Rightarrow r = F$
$\therefore p \wedge q = T$
$\therefore p = T$
$\therefore q = T$

$r \vee s = F$
$\therefore r = F$
$\therefore s = F$

* Truth Table for Statements

Ex. $p \vee (p \to q)$

p	q	$p \to q$	$p \vee (p \to q)$
F	F	T	T
F	T	T	T
T	F	F	T
F	F	T	T

Ex. $(p \vee q) \wedge \neg(p \wedge q)$

p	q	$p \vee q$	$\neg(p \wedge q)$	$(p \vee q) \wedge \neg(p \wedge q)$
F	F	F	T	F
F	T	T	T	T
T	F	T	T	T
T	T	T	F	F

Ex. $Y : (p \vee \neg q) \longrightarrow (p \wedge q)$

p	q	$p \vee \neg q$	$p \wedge q$	$(p \vee \neg q) \longrightarrow (p \wedge q)$
F	F	T	F	F
F	T	F	F	T
T	F	T	F	F
T	T	T	T	T

$\therefore Y \equiv q.$

* **Tautology:** A statement is called Tautology if its truth value is always True for all combinations of the atomic propositions. (a.k.a. Valid)

Contradiction: A statement is called Contradiction if its truth value is always False, for all combinations of the atomic propositions.

Contingency: A statement, neither Tautology nor Contradiction is called Contingency.

Satisfiable: A statement is satisfiable if at least one combination of its atomic proposition yields the truth value True.

Falsifiable: A statement is falsifiable if for at least one combination of its atomic proposition yields the truth value False.

Ex. $p \vee \neg(p \wedge q)$

$\Rightarrow p \vee \neg p \vee \neg q$ {Demorgan's Rule}

$\Rightarrow T \vee \neg q$

$\Rightarrow T$ ∴ Tautology.

Ex. $(p \leftrightarrow q) \wedge (\neg p \wedge q)$

$\Rightarrow (\neg p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \wedge q)$

$\Rightarrow (\neg p \vee q) \wedge (F \neg p \neg q) \wedge q$

$\Rightarrow (\neg p \vee q) \wedge F$

$\Rightarrow F$ ∴ Contradictions.

* Logical Equivalence: Two compound propositions, p and q are called logically equivalent if $p \leftrightarrow q$ is a tautology, i.e. for all combinations of atomic propositions truth value of p & q are same, denoted by $p \equiv q$, or $p \Leftrightarrow q$.

* $p \to q \equiv \neg p \vee q$
  $p \to q \equiv \neg q \to \neg p$

* $(p \leftrightarrow q) \equiv (p \to q) \wedge (q \to p)$

* $T \oplus p \equiv \neg p$
  $F \oplus p \equiv p$

* $p \wedge T \equiv p$
  $p \vee F \equiv p$

* $p \vee T \equiv T$
  $p \wedge F \equiv F$

* $p \vee p \equiv p$
  $p \wedge p \equiv p$

* $p \leftrightarrow T \equiv p$
  $p \leftrightarrow F \equiv p'$

• Any operation # is idempotent iff $\forall p$,

$$p \# p = p$$

Ex. Which of the following operators is/are idempotent?

(A) $\wedge$ (B) $\vee$ (C) $\oplus$ (D) $\rightarrow$ (E) $\leftrightarrow$ (F) $\uparrow$ (G) $\downarrow$

* $\neg(\neg p) \equiv p$

* $p \vee q \equiv q \vee p$
  $p \wedge q \equiv q \wedge p$

* $(p \vee q) \vee r \equiv p \vee (q \vee r)$
  $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

* $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
  $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

• Operation # is distributive over operation * iff:

$$a \# (b * c) = (a \# b) * (a \# c)$$

Ex. Prove or disprove:

1. $\rightarrow$ is distributive over $\wedge$

$$p \rightarrow (q \wedge r) \equiv (p \wedge q) \rightarrow (p \wedge r)$$

Case 1: $p = T$

LHS: $(q \wedge r)$

RHS: $q \rightarrow r$

$\therefore$ Not equivalent

2. $\wedge$ over $\rightarrow$

$$p \wedge (q \rightarrow r) \equiv (p \wedge q) \rightarrow (p \wedge r)$$

C1: $p = T$
LHS = $q \rightarrow r$
RHS = $q \rightarrow r$

C2: $p = F$
LHS = F
RHS = T

$\therefore$ Not eq.

3. $\rightarrow$ over $\vee$

$$p \rightarrow (q \vee r) \equiv (p \rightarrow q) \vee (p \rightarrow r)$$

C1: $p = T$
LHS = $q \vee r$
RHS = $q \vee r$

C2: $p = F$
LHS = T
RHS = T

$\therefore$ Equivalent

4. $\vee$ over $\rightarrow$

$$p \vee (q \rightarrow r) \equiv (p \vee q) \rightarrow (p \vee r)$$

C1: $p = T$
LHS: T
RHS: T

C2: $p = F$
LHS = $q \rightarrow r$
RHS = $q \rightarrow r$

$\therefore$ Equivalent

5. $\oplus$ over $\rightarrow$

$$p \oplus (q \rightarrow r) \equiv (p \rightarrow q) \oplus (p \rightarrow r)$$

C1: $p = T$

LHS $= \neg(q \rightarrow r)$

RHS $= q \oplus r$

$\therefore$ Not equivalent

6. $\rightarrow$ over $\oplus$

$$p \rightarrow (q \oplus r) \equiv (p \rightarrow q) \oplus (p \rightarrow r)$$

C1: $p = T$

LHS $= q \oplus r$

RHS $= q \oplus r$

C2: $p = F$

LHS $= T$

RHS $= F$

$\therefore$ Not eq.

* $\neg(p \wedge q) \equiv \neg p \vee \neg q$
  $\neg(p \vee q) \equiv \neg p \wedge \neg q$

* $p \vee (p \wedge q) \equiv p$
  $p \wedge (p \vee q) \equiv p$

* $p \vee (\neg p \wedge q) \equiv p \vee q$
  $p \wedge (\neg p \vee q) \equiv p \wedge q$

Ex. Assume G is falsifiable, then $\bar{G}$ is:

(A) Tautology (c) Not Valid (e) Satisfiable ✓
(B) Contingency (d) Contradiction

p q r	G	$\bar{G}$	
	–	–	
	–	–	
	⋮	⋮	
	F	T	∴ Atleast once $\bar{G}$ is true.
	⋮	⋮	
	=	=	

Ex. $\overline{\text{Tautology}}$ = Contradiction
$\overline{\text{Contradiction}}$ = Tautology
$\overline{\text{Contingency}}$ = Contingency

Ex. $(p \oplus q) \rightarrow (p \vee q)$. Check if tautology.

Making RHS false, i.e.
$p \vee q = F$
$\therefore p = F, q = F.$

Checking if LHS is true.

$p \oplus q = F \oplus F = F.$

$\therefore F \rightarrow F = T$
$\therefore$ Can't show $T \rightarrow F$. $\therefore$ Tautology.

Ex. $(p \wedge q) \longrightarrow (p \uparrow q)$. Check for tautology.

Making LHS True.

$p \wedge q = T$

$\therefore p = T \quad q = T$

Now, checking if RHS is false.

$p \uparrow q = T \uparrow T = F.$

$\therefore T \rightarrow F = F$

$\therefore$ Not tautology.

Ex. $(p \leftrightarrow q) \longrightarrow (p \downarrow q)$. Check if tautology.

Making LHS True.

$p \leftrightarrow q = T$

$\therefore p \equiv q.$

Cheking if RHS is false.

$p \downarrow q = \neg(p \vee q) = \neg(p \vee p) = \neg p.$

$\therefore$ Not false. Not true either.

& For $p = T$

$T \rightarrow F = F$

$\therefore$ Not tautology

Ex. $[(p \to q) \wedge (\neg r \to s) \wedge (p \vee r)] \to (q \vee s)$

$\Rightarrow [(\neg p \vee q) \wedge (\neg r \vee s) \wedge (p \vee r)] \to (q \vee s)$

$\Rightarrow [(\neg p \neg r \vee q, p \vee q, r) \wedge (\neg r \vee s)] \to (q \vee s)$

$\Rightarrow [\neg p \neg r s \vee p q, \neg r \vee p q, s \vee q, r s] \to (q \vee s)$

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

$\Rightarrow \neg [(\neg p \vee q) \wedge (r \vee s) \wedge (p \vee r)] \vee (q \vee s)$

$\Rightarrow p\bar{q} \vee r\bar{s} \vee \bar{p}\bar{r} \vee q \vee s$

$\Rightarrow p \vee r \vee \bar{p}\bar{r} \vee q \vee s$

$\Rightarrow \underline{p} \vee r \vee \underline{\bar{p}} \vee q \vee s$

$\Rightarrow T$

Method 2:

Making RHS false.

$q \vee s = F$

$\Rightarrow q = F$ & $s = F$.

Checking LHS

$[(p \to F) \wedge (r \to F) \wedge (p \vee r)]$

$\Rightarrow [\neg p \wedge \neg r \wedge (p \vee s)]$

$\Rightarrow [\neg(p \vee r) \wedge (p \vee r)]$

$\Rightarrow F.$

$\therefore F \rightarrow F = T$

$\therefore$ Can't make $T \rightarrow F$

$\therefore$ Tautology.

- Making LHS of implication T & checking RHS for False, or Making RHS F & checking LHS for T, is a fast way to check if implication is Tautology.

- Similary to check if $p \rightarrow q$ is contradiction or not, we can apply simple tests.

(1) If p is F, then $p \rightarrow q$ is not contradiction.
(2) If p is T & q is T then $p \rightarrow q$ is not contradiction.

Ex. Check if contradiction. $p \rightarrow (p \vee q)$.

Making LHS T, $p = T$

RHS: $p \vee q = T \vee q = T$

$\therefore T \rightarrow T = T$ $\therefore$ Not contradiction.

Ex. Check if contradiction. $[p \leftrightarrow (Q \wedge R)] \longrightarrow (P \oplus Q)$

Not contradiction for

$P = T$ $Q = F$

Ex. Check if contradiction. $(P \vee \bar{P}) \rightarrow (Q \wedge \bar{Q})$

Yes. LHS is always True. RHS is always False.

Ex: Check if $(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$

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

Ex. Check if contingency. $(p \rightarrow q)(\neg p \vee q)$
$(p \rightarrow q)(p \rightarrow q)$
$\Rightarrow p \rightarrow q$

$\therefore$ Contingency.

Ex. Check if tautology, contradiction or conting.

(1) $(p \vee q) \wedge (\neg p \wedge \neg q)$
$\Rightarrow (p \vee q) \wedge \neg (p \vee q)$
$\Rightarrow F$ $\therefore$ Contrad.

(2) $(p \leftrightarrow q) \wedge (\neg p \leftrightarrow \neg q)$
$\Rightarrow T$ if $p = q$
$\Rightarrow F$ if $p \neq q$. $\therefore$ Conting.

(3) $(p \vee q) \wedge (\neg p \vee r) \rightarrow (p \vee r)$

Checking if tautology:

Making RHS false: $p \vee r = F \Rightarrow p = F$
$r = F$.

LHS: $(F \vee q) \wedge (T \vee F)$
$\Rightarrow q \wedge T$
$\Rightarrow q$.

∴ Not tautology.

Checking Contradiction.

① $(p \vee q) \wedge (\neg p \vee r)$
$\Rightarrow pr \vee \neg pq \vee qr$
$\neq F$

② Making LHS True. RHS
$p = T \; q = T \; r = T$
$(T \vee T) \wedge (T \vee F)$ $(T \vee T)$
$\Rightarrow T$ $\Rightarrow T$

∴ Not contradiction

∴ Contingency

(4) $((p \to q) \to r) \leftrightarrow (p \to (q \to r))$

For Tautology :

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

Making RHS F :

$p \to (q \to r)$

T F

$q \to r$

T F

Checking LHS :

$((T \to T) \to F)$

$\Rightarrow T \to F$

$\Rightarrow F$

∴ Tautology

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

Making RHS F :

$(p \to q) \to r$

T F

Checking LHS

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

F

$\Rightarrow p \to \bar{q}$

∴ Contingency

∴ Contingency

* If $S : p \to q$ is a conditional statement, then,

- $\neg p \to \neg q$ is called Inverse of S.
- $q \to p$ is called converse of S.
- $\neg q \to \neg p$ is called contrapositive of S.

* $(p \to q) \equiv (\neg q \to \neg p)$

i.e. a conditional is logically equivalent to its contrapositive.

Ex. Assume p & q are propositional variables, then:

(A) $p \to q$ is never equivalent to $q \to p$.

(B) $p \to q$ is always equivalent to $\neg q \to \neg p$

Both true, since p & q are atomic propositions & hence consist of all the combinations.

Ex. Assume α & β are propositional formula, then:

(A) $\alpha \to \beta$ is never equivalent to $\beta \to \alpha$

(B) $\alpha \to \beta$ is always equivalent to $\neg\beta \to \neg\alpha$

Only B is true, since a conditional is always equivalent to its contrapositive.

A is n't true since α, β are propositional formulas & may or may not consist of all possibilities.

Ex. $\alpha: p \wedge \neg p$ $\beta: p \oplus p$

p	α	β	$\alpha \to \beta$	$\beta \to \alpha$
F	F	F	T	T
T	F	F	T	T

Here (α, β) has only one combination (F, F).

* Propositional Variable: Atomic proposition. Value of which doesn't depend on other propositions.

Propositional Formula / Expression: Made up of one or more atomic propositions.

* If $\alpha \to \beta \equiv \beta \to \alpha$ then $\alpha \equiv \beta$.

* Translating English to Logic:

* Negation

Negation of p is:

① It is not the case that p.
② It is not true that p.
③ p is false.

* Conjunction.

① p is true, and q is true : $p \wedge q$
② p is true, but q is false : $p \wedge \neg q$
③ p and q : $p \wedge q$
④ p is false and q is false : $\neg p \wedge \neg q$.

* Implication

① If p is true, then q is true : $p \rightarrow q$.
(If p then q)

② If p is false, then q is true : $\neg p \rightarrow q$.

③ p is false or q is true : $p \rightarrow q \equiv \neg p \vee q$.
④ q is true, unless p is false : $p \rightarrow q \equiv q \vee \neg p$

* Exclusive OR

$P \oplus Q =$ (P is T and Q is False)
or
(P is F and Q is T)

$\equiv P\bar{Q} + \bar{P}Q$

* Biconditional

$P \leftrightarrow Q =$ (P is T and Q is T)
or
(P is F and Q is F)

$\equiv PQ + \bar{P}\bar{Q}$

* If p then q unless r : $(p \rightarrow q) \vee r$

$\equiv \neg r \rightarrow (p \rightarrow q)$

* Logical Inference

The idea is to, given some proposition, derive logical conclusion.

Symbol: $\models$

Ex. If it is raining, he'll take umbrella.
It is raining. → p → q

Knowledge Base:
① $p \rightarrow q$
② p is True.

Conclusion: q is True.

$p \rightarrow q, p \models q$

- Knowledge Base is a set of premises/hypothesis.

$KB \models Q$ means:
Q is logically infered from KB.
OR
There is no condition in which Q is false while all premises in KB are true.
OR
$KB \rightarrow Q$ is tautology

Ex. Which is correct:

(1) $P \rightarrow Q, Q \models P$

(2) $P \oplus Q, Q \models \neg P$

(3) $P \leftrightarrow Q, \neg Q \models \neg P$

(4) $P \leftrightarrow Q \models P$

(5) $P \wedge Q \models P$

(6) $P \rightarrow \bar{Q}, \bar{P} \models \bar{Q}$

* $X \rightarrow Y$: Means $X \rightarrow Y$ is tautology

$X \not\rightarrow Y$: Means $X \rightarrow Y$ is either contradiction or contingency.
(X doesn't imply Y)

- "$X \rightarrow Y$ is false" means "$X \rightarrow Y$ is falsifiable".

"$X \rightarrow Y$ is equivalent to False" means "$X \rightarrow Y$ is contradiction".

* Logical Inference ≡ Logical Entailment ≡ Logical Consequence ≡ Logical Implication.

* Argument: Set of premises, along with the conclusion is known as argument. It may be valid or invalid.

Ex. If you have password, you can login.
You have password. .. Valid.
Conclusion: You can login.

Ex. If it rains, he'll take umbrella.
It isn't raining.

Conclusion: He doesn't take umbrella.

Invalid.

- An argument is valid iff,

  if all premises are true, then conclusion must be true.

  i.e.

  $(P_1 \wedge P_2 \wedge P_3 \ldots) \rightarrow C$.

- To check validity of argument, make the conclusion False, then try to make all the premises true.
  If it is possible, argument is invalid.
  Else argument is valid.

Ex.
$$\begin{array}{l} P \vee Q \\ R \vee S \\ \neg P \vee \neg R \\ \hline Q \oplus S \end{array}$$

$Q \oplus S \equiv$ False $\rightarrow (Q \wedge S) \vee (\neg Q \wedge \neg S)$

① $\neg P \vee \neg R$

② If $\neg P$ then Q.

If Case: $\neg Q \wedge \neg S$

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

$(\neg S)$, $(R \vee S) \rightarrow R$.

But then,

$\neg P \vee \neg R$ = False.

∴ Invalid.

Case: $Q \wedge S$

$P \vee T$

$T \vee R$

$\neg P \vee \neg R$.

P & R both can be false.

∴ $\neg P \vee \neg R$ = True.

Method 2:

$P \vee Q \equiv \neg P \rightarrow Q$ —(1)

$R \vee S \equiv \neg R \rightarrow S$ —(2)

$\neg P \vee \neg R \equiv P \rightarrow \neg R$. —(3)

from (2) & (3)

$P \rightarrow S$ — (4)

from (1)

$\neg Q \rightarrow P$. —(5)

from (4) & (5)

$\neg Q \rightarrow S$

$\equiv Q \vee S$

∴ (Q, S) can be (T, T) combination.

∴ $Q \oplus S$ is not followed from (1), (2) & (3).

Ex. $p \to q$ —(1)

$r \to s$ —(2)

$\neg p \vee \neg r$ —(3)

$\neg q \vee \neg s$

Method 2:

from (3)

$p \to \neg r$

$r \to s$

No conclusion

$p \to \neg r$

$p \to q \equiv \neg q \to \neg p$

No conclusion.

∴ Conclusion doesn't follow from premises.

* Rules of Inference.

1. $p \to q$, p ∴ q — Modus ponens

2. $p \to q$, $\neg q$ ∴ $\neg p$ — Modus Tollens

3. $p \to q$, $q \to r$ ∴ $p \to r$ — Hypothetical syllogism.

4. $p \vee q$, $\neg p$ ∴ q — Disjunctive syllogism

5. $p \wedge q$ Conjunctive Simplification.
$\therefore p$
$\therefore q$

6. p Addition
$\therefore p \vee q$

7. $p \vee q$ Resolution
$\neg p \vee r$
$\therefore q \vee r$

FIRST ORDER LOGIC

Logic is the formal language which allows us to unambiguously express statements

Ex.
"If you have access to n/w, you can change your grade"
"You have access to n/w".
∴ "You can change your grade"

Logically this argument is valid.

By propositional logic:

$P \rightarrow Q$

P

$\therefore P$.

So by Prop. logic also, argument is valid.

∴ Prop. logic helps express this argument unambiguously

Ex. "All men are mortal"
"Socrates is a man"
∴ Socrates is mortal.

This is logically valid.

By Propositional Logic:

P

S

$\therefore R$

So, by Prop. logic argument becomes seems invalid.

So, propositional logic is inefficient / unable to express such arguments correctly.

Similary statements like:

① Some natural nos. are prime.
② All Indians are Asians.
!
etc.

can't be properly expressed using propositional logic.

The problem with Propositional Logic is that it treats everything as either true or false. It can't quantify the extent of a proposition.

* A better Logic:

(1) The variables should be able to take value from some domain.

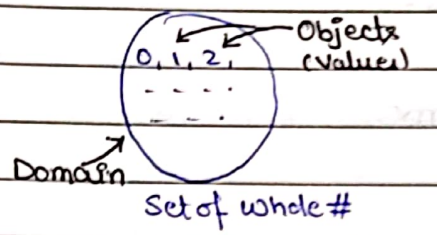
(2) Should be able to express objects (humans, mobile, etc) and their properties.

(3) Should be able to express relationship b/w objects.
Ex. friend $(x, y) \equiv x$ is friends with y

(4) Transformation / function of objects.
Ex.
$f(x) = x^2$ father_of (x)
father_of (India) = Gandhi

Ex.

Relationship → sum (x, y, z) : $x + y = z$



So, sum(1,2,3) is true.
sum(3,4,8) is false

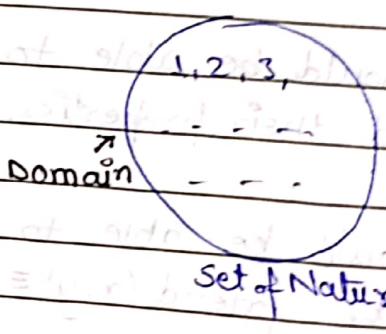
(5) Should be able to quantify objects.
Ex: Some humans.
All planets.

* First Order Logic

FOL is the logic with a world of objects, their properties, relationships (predicate), quantification & transformation.

Ex. P(x): x is prime
↑ property

P(1) : 1 is prime = F
P(2) = T
P(3) = T
P(4) = F
⋮



P(0) = Invalid
(∵ 0 is not in the domain)

Ex. $P(x,y): x < y$ Domain : Set of Natural #

↑ Relationship / Predicate

$P(1,2) = T$

$P(2,3) = T$

$P(3,1) = F$

$P(1,1) = F$

Both x & y can take any value from the domain N.

So, domain of $P(x,y)$ would be N^2.

* Predicate over a single variable is also called Property / Unary predicate. Ex: $F(x)$, $L(y)$, etc.

- $P(x_1, x_2, x_3, \ldots, x_n)$ is n-ary predicate

  ↓ ↓ ↓ ↓

  { D_1 D_2 D_3 D_n } Domains

- Once all the variables in the predicate are replaced by values from their domain, then it becomes a proposition (and hence has value either True or False).

- Predicate with no variable, 0-ary predicate, is automatically proposition.

Ex. $Sum(x,y): x+y$ Domain : Set of all Natural #

↑ Function

$Sum(1,2) = 3$

$Sum(5,5) = 10$

Ex. For ~~operation~~ $N \times N \to N$

Sum (x, y): $x + y$ is valid

Mul (x, y): $x * y$ is valid.

sub (x, y): $x - y$ is invalid

* Quantification

The ability to express the extent or quantity of objects.

Ex. All humans.
Some mice.

Ex. P: All elements in the domain of x are vovel.

$\forall \; x \in D(x) \;\; Vovel(x)$

OR

$\forall x \; Vovel(x)$ is False.

$\equiv Vovel(a) \wedge Vovel(b) \ldots \wedge Vovel(z)$

$\equiv$ False

Eg. Alphabet: a, b, c, d, - - -

Q: Some elements in domain of x are vovels

$\exists x \in D(x) \;\; Vovel(x)$

OR

$\exists x \; Vovel(x)$

$\equiv Vovel(a) \vee Vovel(b) \vee Vovel(c) \ldots \vee Vovel(z)$

$\equiv$ True.

* $\exists$: There exists
  $\forall$: For all

* $\forall x\ P(x) = P(x_1) \wedge P(x_2) \wedge \ldots P(x_n)$ } All
  $\exists x\ P(x) = P(x_1) \vee P(x_2) \vee \ldots P(x_n)$ } At least one

* Predicate maps objects to True or False.
  Function maps objects to objects.

* Objects are just the elements from the domain.

* Note: Domain in FOL is always non-empty, unless explicity stated.

  By default, if nothing is mentioned about domain of different variables, then domain of different variables is same.

* Making Proposition from Predicate:

1. Say, $E(x)$: x is even. Domain: $\mathbb{N}$
   Then, by substituting values of x, we can get proposition.

2. Another way is quantification.
   Ex. Say, $E(x)$: x is even, Domain: $\mathbb{N}$
   then,
   "for all x, $E(x)$ is true"
   "there exist some x, for which $E(x)$ is true"

are proposition.

- Standard quantifiers

(1) Universal Quantifier
(2) Existential Quantifier

* Universal Quantifier

The statement of the form:

$\forall x$ some-formula

is true, if for every choice of x, the statement some-formula is true when x is plugged into it.

Ex. Domain: All animals.

$\forall x$ Human(x) $\longrightarrow$ $\forall x$ Needs-Oxygen(x)

is True, since LHS is false, RHS is true.

"If every animal is human, then every animal needs oxygen."

Ex. Domain: All animals.

$\forall x$ (Human(x) $\longrightarrow$ Needs-Oxygen(x))

is true, since, if x is human, then it needs oxygen.

"For all animals, if the animal is human, then it needs oxygen."

* Existential Quantifier

The statement of the form:

$$\exists x \text{ some-formula}$$

is true, if there exist at least one x, for which some-formula is true.

Ex. Domain: $\mathbb{N}$

$$\exists x \, (\text{Even}(x) \wedge \text{Prime}(x))$$

is true for $x = 2$.

↳ witness

Ex. Domain: $\{1, 2, 3\}$ $\quad P(x): x + 2 = 2x$.

(1) $\forall x \, P(x)$ is false
(2) $\exists x \, P(x)$ is true for 2.
(3) $\forall x \, \neg P(x)$ is false, since $P(x)$ is true for 2
(4) $\exists x \, \neg P(x)$ is true for 1 & 3.
(5) $\neg \exists x \, P(x)$ is false, $\because P(x)$ is true for 2
(6) $\neg \forall x \, P(x)$ is true, $\because P(x)$ is false for 1 & 3.

Ex. Drinker's Paradox

"There is someone in this meeting such that if he/she is drinker then everyone is drinker"

Is this true?

$\exists x \, (D(x) \rightarrow \forall y \, D(y))$

This is true.

C1: Everyone is drinker.
C2: At least 1 person is not drinker.
Say x_K.

$D(x_K)$: False
$D(x_K) \rightarrow \forall y \, D(y)$: True

$\therefore \exists x \, (D(x) \rightarrow \forall y \, D(y))$: True.

	True	False
$\forall x \, P(x)$	when for all x $P(x)$ true.	when for some x, $P(x)$ is false.
$\exists x \, P(x)$	For some x, $P(x)$ is true.	For all x, $P(x)$ is false.

* • Universal quantifier is true unless there is a counter example.

q unless not p.

i.e. If there is no counterexample, then universal quantification is true.

• Existential quantification is false, unless there is a witness.

i.e.
If no witness, then existential quantification is false.

• So, when domain is empty, there are no counterexamples & there are no witnesses.

∴ Universal quantification on empty domain : True

∴ Existential quantification on empty domain : False.

* Bounded & Free Variables

A predicate (propositional formula) is converted to proposition when all the variables are either
- replaced by a value from their domain or
- bound by a quantifier

Ex. $P(x)$: $x > 8$. is predicate.

- $P(2)$: $2 > 8$ is a proposition.
- $\forall x\, P(x)$ is a proposition.

so, in

$P(x)$: $x > 8$

x is free to take any value from the domain.

∴ Since there is a free variable, $P(x)$ is not a proposition.

Ex. $P(x, y, z)$: $x + y = z$

- $P(-4, 6, 2)$: $-4 + 6 = 2$ is proposition.
- $P(2, y, 3)$: $2 + y = 3$ is not proposition.

free variable

Ex. For $P(x)$, a propositional formula,

$\forall x\, P(x) = P(x_1) \wedge P(x_2) \wedge \ldots P(x_n)$

There are no variables here. x takes values because of quantification. x is bounded by the quantifier.

Ex. $P(x, y)$: $x + y = 10$

$\forall x P(x, y)$: $\forall x (x + y = 10) = [x_1 + y = 10] \wedge [x_2 + y = 10] \ldots\ldots$

bounded variable — free variable

$\forall x P(x, 2)$: $\forall x (x + 2 = 10) = [x_1 + 2 = 10] \wedge [x_2 + 2 = 10] \ldots\ldots$

Proposition. bounded variable. values

∵ There are no free variables. $\forall x P(x, 2)$ is a proposition.

∴ Free variables can be replaced by values from their domain.
∴ Bounded variables are just dummy variables.

Ex. $P(m, n)$: $mn > 0$.

So, is $\forall m P(1, n)$ a proposition?

$\forall m P(1, n)$: $\forall m (n > 0)$

bounded — free.

∴ Not proposition

* Quantifiers can quantify only free variable. It can't quantify a bounded / already quantified variable.

Ex. $P(x)$: x is prime.

$\forall x$ • can affect ~~$\exists x$~~ x.

Ex. $P(x, y)$: $x + y > 0$.

For $P(0, y)$: $y > 0$

$\forall x$ doesn't affect
$\exists x$ doesn't affect.

$\forall y$ & $\exists y$ can affect.

Ex. $P(x)$: x is prime.

say,

Q : $\exists x P(x)$ i.e. x is bound.

In,

$\forall x \exists x P(x) \equiv \forall x (\exists x P(x))$, $\forall x$ doesn't have any effect.

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

Ex. If in α, there are no free variables, "x", then which is/are necessarily true?

(A) $\forall x \alpha \equiv \alpha$ ✓

(B) $\forall y \alpha \equiv \alpha$

(C) $\exists x \alpha \equiv \alpha$ ✓

(D) $\exists y \alpha \equiv \alpha$

{ $\because \forall x$ & $\exists x$ won't affect α, $\because$ no free "x". }

* Scope of a Quantifier:

The part of the logical expression to which a quantifier is applied is called it's scope.

Ex. $\forall x P(x)$
↳ scope of $\forall x$.

Ex. $\forall x\ E(x) \rightarrow P(x)$
$\equiv \forall x\ E(x) \rightarrow P(y)$
$\equiv \forall z\ E(z) \rightarrow P(y)$
↓ scope of $\forall x$ or $\forall y$ or $\forall z$
↳ not in scope of $\forall x$

$\forall x\ [E(x) \rightarrow P(x)]$
$\equiv \forall y\ [E(y) \rightarrow P(y)]$
$\equiv \forall z\ [E(z) \rightarrow P(z)]$
↓ in scope of $\forall x$

Ex. $\forall x\ P(x) \rightarrow \forall x\ Q(x)$ (not same)
$\equiv \forall x\ P(x) \rightarrow \forall y\ Q(y)$
↓ scope of $\forall x$ ↓ scope of $\forall y$

Ex. $\exists x\ [xPy \wedge \forall z\ [zPy \rightarrow z = x]]$

y is free variable.

Ex. $\phi = \forall y\ [(P(y) \wedge Q(x)) \vee \forall x\ (P(x) \vee Q(y) \wedge P(z))]$
↑ free ↑ free.

No. of free variables?
2.

* Revised Precedence

1. $\exists, \forall$
2. $\neg$ or $\sim$
3. $\wedge$
4. $\vee$
5. $\rightarrow$
6. $\leftrightarrow$

* Quantifier with restricted domain

Ex. Domain = $\mathbb{R}$

$\forall x<0 \ (x^2>0)$

Read: For every real no. $x<0$, $x^2>0$.

Ex. $\forall y \neq 0 \ (y^3 \neq 0)$

Reads: For every $y \neq 0$, $y^3 \neq 0$.

Ex. Domain: Set of all animals

S: Every rabbit is small.

G: $\forall x$ Small (x)

The logical expression G doesn't express the

english statement 8:

Note: A logical expression G expresses an English statement S, iff. ~~whereas~~ S is true, G is true & vice versa.

iff

So, S is correctly expressed by:

$$\forall x \in \text{Rabbit}\ \text{Small}(x)$$
$$\equiv \forall x\ \text{Rabbit}(x) \rightarrow \text{Small}(x)$$

Every Rabbit is small.
≡ For all animals x, if x is a rabbit, then x is small.

•Some rabbits are small.

~~$\exists x$ Rabbit Small~~

(1) $\exists x$ Small (x)
This is wrong, since the 'x' may or may not be rabbit & the statement ~~would~~ still be true.

(2) $\exists x \in$ Rabbit Small (x)
This is correct.

(3) Is (2) same as $\exists x$ Rabbit$(x) \rightarrow$ Small (x)?
No. Since, the English statement, and (2) require 1 or more rabbit to be small, ~~whereas~~ whereas,

$$R(x) \rightarrow S(x)$$

means if x is rabbit, it must be small, meaning it requires all rabbits to be cute.

Also, if x is not Rabbit, $R(x)$ is false, & $R(x) \rightarrow S(x)$ is true, even for non-Rabbit.

So, irrelevent x is witness here.

i.e.

$$(R(x=R_1) \rightarrow S(x=R_1)) \vee (R(x=R_2) \rightarrow S(x=R_2)) \vee (R(x=T_1) \rightarrow S(x=T_1))$$

↑ irrelevent witness.

$\Rightarrow F \vee F \vee T$

$\Rightarrow T$

↑ wrongly True.

(4) Is (2) same as $\underline{\exists x\,[R(x) \wedge S(x)]}$

Yes. "There exist an animal x, such that x is a Rabbit & x is small".

$$[R(x=R_1) \wedge S(x=R_1)] \vee [R(x=R_2) \wedge S(x=R_2)] \vee [R(x=T_1) \wedge S(x=T_1)]$$

$\Rightarrow [T \wedge F] \vee [T \wedge F] \vee [F \wedge T]$

$\Rightarrow F$

∴ No false witness, since we check if x is witness (in this case a Rabbit).

* • Conjunction & Existential quantifier are associated with each other.

• Implication & Universal quantifier are associated.

Ex. "All animals are cute." Domain: All animals.

(A) $\forall x\, C(x)$ ✓
(B) $\forall x\, [\neg A(x) \rightarrow C(x)]$ ✓
(C) $\forall x\, [A(x) \vee C(x)]$

B is $\forall x\, [T \rightarrow C(x)]$
$\equiv \forall x\, C(x)$

C is True even when all animals are not cute.
$\forall x\, [T \vee C(x)]$
$\equiv \forall x\, T$ ↳ doesn't matter here.
$\equiv T$
∴ C is wrong.

Ex. "Some rabbits are small" Domain: All rabbits.

(A) $\exists x\, S(x)$ ✓
(B) $\exists x\, (R(x) \rightarrow S(x))$ ✓
(C) $\exists x\, (R(x) \wedge S(x))$ ✓
(D) $\exists x\, (R(x) \leftrightarrow S(x))$ ✓
(E) $\exists x\, (S(x) \rightarrow R(x))$
(F) $\exists x\, (S(x) \oplus R(x))$
(G) $\exists x\, (R(x) \vee S(x))$

Ex. "Some p are q"
$\exists x\, [p(x) \wedge q(x)]$

Ex. "All p are q"
$\forall x\, [p(x) \rightarrow q(x)]$

Ex. "No p are q"

$\equiv \neg \exists x [P(x) \wedge Q(x)]$

$\equiv \forall x \neg [P(x) \wedge Q(x)]$

$\equiv \forall x [P(x) \rightarrow \neg Q(x)]$

Ex. "Some p aren't q"

$\equiv \neg \forall x [P(x) \rightarrow Q(x)]$

$\equiv \exists x \neg [P(x) \rightarrow Q(x)]$

$\equiv \exists x [P(x) \wedge \neg Q(x)]$

Ex. Which of the following is correct?

(A) If $\alpha \models \gamma$ or $\beta \models \gamma$ then $(\alpha \wedge \beta) \models \gamma$

(B) If $(\alpha \wedge \beta) \models \gamma$ then $\alpha \models \gamma$ or $\beta \models \gamma$

A can be translated to, "if $\alpha \rightarrow \gamma$ is tautology, and $\beta \rightarrow \gamma$ is a tautology, then $(\alpha \wedge \beta) \rightarrow \gamma$ is tautology

$\alpha \rightarrow \gamma$	$\beta \rightarrow \gamma$	$(\alpha \wedge \beta) \rightarrow \gamma$
T	T	
T	⋮	
⋮	⋮	
⋮	⋮	
T	T	

If $(\alpha \wedge \beta)$ were to be false then,

$(\alpha \wedge \beta) \equiv T$ & $\gamma \equiv F$

i.e. $\alpha \equiv T$ & $\beta \equiv T$ $\gamma \equiv F$

then,

$\alpha \rightarrow \gamma = F$ & $\beta \rightarrow \gamma = F$

which is contradiction.

∴ A is true

B can be interpred as, "if $(\alpha \wedge \beta) \rightarrow \gamma$ is tautology then either $\alpha \rightarrow \gamma$ or $\beta \rightarrow \gamma$ (or both) are tautology.

α	β	γ	$(\alpha \wedge \beta) \rightarrow \gamma$	$\alpha \rightarrow \gamma$	$\beta \rightarrow \gamma$
			T	⋮	⋮
			⋮	⋮	⋮
T	F	F	T	F	⋮
F	T	T	T	⋮	F
			⋮	⋮	⋮
			T		
			Tautology	Invalid	Invalid.

To check, make RHS, i.e.

$$(\alpha \models \gamma) \vee (\beta \models \gamma)$$

false.

So,

$\alpha \rightarrow \gamma$ is not tautology

& $\beta \rightarrow \gamma$ is not tautology.

meaning $\alpha \rightarrow \gamma \equiv F$; $\beta \rightarrow \gamma \equiv F$

α: T, γ: F ; β: T, γ: F

$\therefore \alpha = T \quad \gamma = F \quad \beta$ can be anything.

Say $\beta = F$

$\therefore (\alpha \wedge \beta) \rightarrow \gamma \equiv T$

$\therefore$ LHS is still tautology.

$\therefore \beta = T \quad \gamma = F \quad \alpha$ can be anything.

Say $\alpha = F$

$\therefore (\alpha \wedge \beta) \rightarrow \gamma \equiv T$

$\therefore$ LHS still tautology

$\therefore$ LHS is tautology, but $(\alpha \models \gamma)$ is not & $(\beta \models \gamma)$ is not tautology.

$\therefore$ B is false.

* Note: When domain in FOL is not specified then domain consists of everything.

* English to FOL

Ex. "All crows are black".

$\forall x [Crow(x) \rightarrow Black(x)]$

Ex. "Some crows are black"

$\exists x [Crow(x) \wedge Black(x)]$

Ex. "No crows are black".

$\equiv$

"There doesn't exist any crow which is black".

$\equiv$

"For all elements, if the element is crow, then it is not black."

$\equiv \neg \exists x [Crow(x) \wedge Black(x)]$

$\equiv \forall x \neg [Crow(x) \wedge Black(x)]$

$\equiv \forall x \; Crow(x) \rightarrow \neg Black(x)$

Ex. "Some crows are not black".

$\equiv$ "Not all crows are black"

$\equiv$ "There exist some element which is crow

but not black":

$\equiv \neg \forall x \; [C(x) \rightarrow B(x)]$
$\equiv \exists x \; \neg [C(x) \rightarrow B(x)]$
$\equiv \exists x \; C(x) \wedge \neg B(x)$

* Negation of Quantifiers:

(1) $\neg \forall x \; P(x) \equiv \exists x \; \neg P(x)$

"Not all x $P(x)$" "Some x not $P(x)$"

(2) $\neg \exists x \; P(x) \equiv \forall x \; \neg P(x)$

"Not some x, $P(x)$" "All x, not $P(x)$"

Ex. "All and only crows are black"

$\forall x \; [C(x) \leftrightarrow B(x)]$

Ex. "Only crows are black"
$\equiv$ "If not crow, not black"

$\forall x \; [\neg C(x) \rightarrow \neg B(x)]$
$\equiv \forall x \; [B(x) \rightarrow C(x)]$

Ex. "Every student takes some course"

$\forall x \; [S(x) \rightarrow \exists y \; [C(y) \wedge T(x,y)]]$

Ex. "Every student loves some other student"

$\forall x [S(x) \rightarrow \exists y \; [S(y) \wedge [x \neq y] \wedge L(x,y)]]$

Ex. "There is a student who is loved by every other student"

$\exists x \; [S(x) \wedge \forall y \; [[S(y) \wedge (x \neq y)] \rightarrow L(y,x)]]$

Ex. "Bill takes Analysis or Geometry (not both)"

$Takes(Bill, Analysis) \oplus Takes(Bill, Geometry)$

Ex. "Bill has no sister"

$\neg \exists x \; Sister(x, Bill)$

Ex. "Bill has at least one sister"

$\exists x \; Sister(x, Bill)$

Ex. "Only students walk or talk".

≡ "If an element walks or talks, then they must be student"

≡ $\forall x\ [(W(x) \vee T(x)) \rightarrow S(x)]$

* Numerical Quantification

Ex. "There is atleast one cube"

$\exists x\ C(x)$

Ex. "There are at least two cube"

$\forall x \forall y\ [C(x) \wedge C(y)]$ Is this correct?

No. Say there's only one cube C_1 & x & y both take value C_1, then the above wrongly becomes true.

So,

$\forall x \forall y\ [C(x) \wedge C(y) \wedge (x \neq y)]$

Ex. "There are at least two elements in domain"

$\forall x \forall y\ (x \neq y)$.

Ex. "There is exactly one cube"

$\exists x\ [C(x) \wedge \forall y\ [x \neq y \rightarrow \neg C(y)]]$

OR

$\exists x \forall y\ [C(y) \leftrightarrow y = x]$

Ex. "There is at most one cube"

$$\forall x \forall y \, [C(x) \wedge C(y) \rightarrow x = y]$$

OR

There is no cube $\vee$ There is exactly one cube.

$$[\forall x \neg C(x)] \vee [\exists x [C(x) \wedge \forall y (C(y) \rightarrow x = y)]]$$

Ex. "There are at most two cube"

$$\forall x \forall y \forall z \, [C(x) \wedge C(y) \wedge C(z) \rightarrow [(x=y) \vee (y=z) \vee (z=x)]]$$

Ex. "There are exactly two cubes"

$$\exists x \exists y \, [(x \neq y) \wedge C(x) \wedge C(x) \wedge \forall z \, [C(z) \rightarrow (z=x) \vee (z=y)]]$$

* Nested Quantifier

Two quantifiers are nested if one is within the scope of another.

Ex. $\forall x \{\exists y \{(x+y)=0\}\}$

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

$\Rightarrow \forall x \; P(x)$

$P(x)$ ↑ only x is free

$Q(x,y)$ ↑ both x & y are free

Many statements in FOL require a combination of quantifier.

Ex. For every natural no. there exist another greater natural no.

Domain: Natural no.

$\forall x \exists y \bullet x < y$.

Quantifiers can be nested as:

1. $\forall x \forall y \; P(x,y)$
2. $\forall x \exists y \; P(x,y)$
3. $\exists x \forall y \; P(x,y)$
4. $\exists x \exists y \; P(x,y)$

* $\forall x \forall y\ P(x,y)$

Ex. $\forall x \forall y\ [\text{ASCII}(x) < \text{ASCII}(y)]$

$x \in \{a, b, c\}$
$y \in \{p, q, r\}$

is True.

Ex. $\forall x \forall y\ (x+y = y+x)$
$x, y \in \mathbb{N}$. Is True

* $\forall x \exists y\ P(x,y)$

Ex. $\forall x \exists y$ Ascii(x) < Ascii(y)

$x \in \{m, n, o\}$
$y \in \{a, b, z\}$

is True.

For every x, there exist at least one y, such that Ascii(x) < Ascii(y).

* $\exists x \forall y\ P(x,y)$

Ex. $\exists x \forall y$ Ascii(x) < Ascii(y)

$x \in \{a, m, z\}$
$y \in \{b, n, y\}$

is True with witness for x : a.

There exists some x, such that, its ascii value is lesser than all ys.

* $\exists x \exists y\ P(x,y)$

Ex. $\exists x\ \exists y$ Ascii(x) < Asaii(y)

$x \in \{'y', 'z'\}$ $y \in \{'a', 'b', 'z'\}$.

True for witness $x = 'y'$, $y = 'z'$

* (1) $\forall x \forall y\ P(x,y) \equiv \forall y \forall x\ P(x,y)$

(2) $\exists x \exists y\ P(x,y) \equiv \exists y \exists x\ P(x,y)$

Ex. "For any natural no. n, n is even if and only if, n^2 is even".

$$\forall x \, [\text{Natural}(x) \longrightarrow (\text{Even}(x) \longleftrightarrow \text{Even}(x^2))]$$

$$\equiv \forall x \, [\text{Natural}(x) \longrightarrow \{\exists y \, (x = 2y) \longleftrightarrow \exists y \, (x^2 = 2y)\}]$$

Ex. "Everyone loves someone"

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

Negation:

$$\neg \forall x \, \exists y \, L(x, y) \equiv \exists x \, \neg \exists y \, L(x, y)$$
$$\equiv \exists x \, \forall y \, \neg L(x, y)$$

i.e. "There exists someone, who doesn't love anyone".

Ex. Negation of

"$\exists S \, [\text{set}(S) \wedge \forall x \, \neg (x \in S)]$"

is

$$\forall S \, [\neg \text{Set}(S) \vee \exists x \, (x \in S)]$$

* Interpretation, Model in Propositional Logic.

Ex. Say we have a Prop. Logic formula:

$G: a \vee (b \rightarrow c)$

Then the only info required to know truth value of G is the truth value of a, b & c.

Ex. $a = T, b = F, c = T$

Then, $G = T$.

This is called Interpretation of G.

- The assignment of boolean values to variables of a sentence is called as the interpretation of the sentence in propositional logic.

So, for 2 variables : $2^2 = 4$ interpretations.
for 3 variables : $2^3 = 8$ interpretations.

- In Propositional logic, a Model is an interpretation for which the sentence is true.

Ex. Consider a vocabulary with only four propositional variables, A, B, C, D. How many models for the formula: $B \vee C$?

$$\underbrace{(B \times C)}_{3} \quad \underbrace{A}_{2} \quad \underbrace{D}_{2} = 3 \times 2 \times 2 = 12$$

• Comodel in propositional logic is an interpretation for which the formula/sentence is false.

Ex. KB = {P → Q, Q, R} Vars: P, Q, R

#Interpretations = $2^3 = 8$.

Models.

Q R P
↓ ↓ ↓
T T T/F

1 x 1 x 2 = 2.

∴ 2 models.

Comodels = 8 - 2 = 6.

* In propositional logic.
(1) Tautology: Every interpretation is model. (Valid)
(2) Contradiction: Every interpretation is comodel.
(3) Satisfiable: Some interpretation is model.
(4) Falsifiable: Some interpretation is comodel.

* Interpretation, Model in FOL:

Ex. G: $\forall x P(x)$
What do we need to interpret G?

(1) P(x)
(2) Domain.

Interpretation 1	Interpretation 2
Domain: N	Domain: N
P(x): x is even.	P(x) = x > 0.
G = False.	G = True.
So, this interpretation is a Comodel.	So, this interpretation is model.

- Finite Model: Model with finite domain.
- Finite Comodel: Comodel with finite domain.

Ex. S: $\forall x\, P(x)$
Is the following a Model?
domain: $\emptyset$
P(x): x is even

No. Domain is empty.

* Notes:
(1) Domain is never empty, unless stated in question.
(2) Domain for all vars. is same unless explicity stated.

Ex. $S: \forall x \exists y P(x,y)$

(1) Give a finite model

Domain: $\{2, 4, 8, 16\}$
$P(x,y)$: $y|x$.

(2) Finite comodel.

Domain: $\{2, 4, 6, 8\}$
$P(x,y)$: $y < x$

* $\forall x P(x) \longrightarrow \exists x P(x)$ is always true. {we don't consider empty domain}

∴ Is valid

* In First Order Logic:

(1) Valid: All interpretations are model.
(2) Satisfiable: Some interpretation is model.
(3) Contradiction: No interpretation is model
(4) Falsifiable: Some interpretation is comodel.

Tautolog ≠ Valid in FOL

Ex. $\exists x\, P(x)$

(1) Is it satisfiable?

Yes. Ex. Domain: $\mathbb{N}$

$P(x)$: $x \mid x$

(2) Is it Valid?

No. There exist comodel. Ex. Domain: $\mathbb{N}$

$P(x)$: $x < 0$

Ex. $\forall x\, [P(x) \vee \neg P(x)]$

(1) Is it satisfiable?

Yes. Ex: Domain: $\mathbb{N}$

$P(x)$: $x > 0$.

(2) Is it valid?

Yes. Every interpretation is model.

Ex. $\forall x\, P(x) \vee \forall x \neg P(x)$

Give finite model.

Ex: Domain: $\{2, 4, 8\}$

$P(x)$: x is even.

* Functions in Predicate Logic.

Ex. Domain: $\mathbb{N}$

function: $S(x) = x^2$ → function symbol.

predicate: $f(x)$: x is prime.
↳ predicate symbol

Which is true?

(1) $\forall x \; (S(x) \rightarrow \neg P(x))$
(2) $\exists x \; (S(x) \rightarrow P(x))$

1 says, $\forall x$ (x^2 → x is not prime)

So, false. Counterexamples

(1) $\forall x \; [f(S(x))]$
(2) $\exists x \; [f(S(x))]$

1 is saying $\forall x$ [x^2 is prime].
1 is false.

2 is saying $\exists x$ [x^2 is prime]
2 is false.

Ex. Working with a unary predicate symbol P, binary predicate symbol Q, & a unary func. symbol f, which of the following formulas are satisfied in the interpretation M,

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

$P^M = \{a, b\}$

$Q^M = \{(a,b), (b,b), (c,b)\}$

$f^M(a) = b,\ f^M(b) = b,\ f^M(c) = a$ & $f^M(d) = c$.

{ $P^M = \{a, b\}$ means $P(a) = T$ & $P(b) = T$ }

{ $Q^M = \{(a,b), (b,b) \ldots\}$ means $Q(a,b) = T,\ Q(b,b) = T \ldots$ }

{ Note: Unary predicate is also called property.
Binary predicate is also called relation }

1. $\forall x\ [P(x) \rightarrow \exists y\ Q(y, x)]$

$x = a$: $P(a) \rightarrow \exists y\ Q(y, a)$

is false.

∴ 1 is false. Hence, not satisfied.

∴ For 1, interpretation M is comodel.

2. $\forall x\ Q(f(x), x)$

$x = a$: $Q(f(a), a) = Q(b, a) = F$.

∴ 2 is not satisfied.

∴ For formula 2, M is comodel.

3. $\forall x\ (Q(f(x), x) \rightarrow Q(x, x))$

$x = a$: $Q(f(a), a) \rightarrow Q(a, a)$
$\equiv F \rightarrow Q(a, a)$
$\equiv T.$

$x = b$: $Q(f(b), b) \rightarrow Q(b, b)$
$\equiv Q(b, b) \rightarrow Q(b, b)$
$\equiv T$

$x = c$: $Q(f(c), c) \rightarrow Q(c, c)$
$\equiv Q(a, c) \rightarrow Q(c, c)$
$\equiv F \rightarrow Q(c, c)$
$\equiv T$

$x = d$: $Q(f(d), d) \rightarrow Q(d, d)$
$\equiv Q(c, d) \rightarrow Q(d, d)$
$\equiv F \rightarrow Q(d, d)$
$\equiv T.$

$\therefore$ formula 3 $\equiv T \wedge T \wedge T \wedge T$
$\equiv T$
$\therefore$ 3 is satisfied & M is a model for formula 3.

4. $\forall x \forall y\ [Q(x, y) \rightarrow P(x)]$

~~Counter~~
Counterexample: $Q(c, b) \rightarrow P(c)$
$\equiv T \rightarrow F$
$\equiv F$

5. $\forall x \exists y [Q(x,y) \vee Q(y,x)]$

Counterexample: $x = d$:

$\exists y [Q(d,y) \vee Q(y,d)]$

$\equiv F$

∴ 5 is not satisfied.

* Uniqueness Quantifier ($\exists!$)

"There is exactly one".

Ex. $\exists! x P(x)$ $P(x)$: x is Prime Domain: $\mathbb{N}$.

is saying "There is exactly one prime no."

$\equiv \exists x [P(x) \wedge \forall y (P(y) \rightarrow x = y)]$

is false.

Ex. $\exists! x (P(x) \wedge E(x))$ $P(x)$: x is prime

$E(x)$: x is even.

$\equiv \exists x [E(x) \wedge P(x) \wedge \forall y \{(E(y) \wedge P(y)) \rightarrow x = y\}]$

is True.

* Negation of $\exists!$

"Either No x. $P(x)$ or At least two x, $P(x)$ is true".

$\equiv \neg \exists! x P(x)$

- $S = \exists! x P(x) \equiv$ Unique $x, P(x)$.

$\neg S = \neg \exists x P(x) \vee \exists x \exists y (P(x) \wedge P(y) \wedge x \neq y)$

$\neg \exists x P(x)$ → No $x, P(x)$

$\exists x \exists y (P(x) \wedge P(y) \wedge x \neq y)$ → Two or more $x, P(x)$

$\neg S \equiv$ For every x, either $\neg P(x)$ or there is some y, $P(y)$.

$\equiv \forall x [\neg P(x) \vee \exists y (x \neq y \wedge P(y))]$

* Validity in FOL

- Procedure.

α, β are FOL Expression

$\alpha \longrightarrow \beta$: Valid ??

S1: Assume domain $D = \{a, b, c, d, \ldots\}$

S2: Try to make $\alpha \rightarrow \beta$ false:

(1) Assume $\alpha = T$, make $\beta = F$

(2) Assume $\beta = F$, make $\alpha = T$

Ex $\forall x P(x) \longrightarrow \exists x P(x)$

Approach 1:

Making $\forall x P(x) \equiv T$
then, $\exists x P(x)$ can't be made false.

$\therefore \forall x P(x) \longrightarrow \exists x P(x)$ is Valid.

Ex. S: $\forall x [P(x) \wedge Q(x)] \longrightarrow \forall x P(x) \wedge \forall x Q(x)$

Approach 1: Say domain = {a, b, c, ...}

Making $\forall x [P(x) \wedge Q(x)] \equiv T$.
So,

$(P(a) \wedge Q(a))$
$\wedge (P(b) \wedge Q(b))$
$\wedge$ ...

So, $P(a), P(b)$ .... are all T
& $Q(a), Q(b)$ .... are all T.

$\therefore \forall x P(x) \wedge \forall x Q(x)$ is T.

$\therefore$ S is valid.

Also R: $\forall x P(x) \wedge \forall x P(x) \longrightarrow \forall x [P(x) \wedge Q(x)]$ is also valid.

$\therefore S \equiv R$

Ex. $\forall y\, P(y) \longrightarrow \forall y\, (P(y) \wedge Q(y))$

Approach 1:

Say. $D = \{a\}$ $\quad P(a) = T$ & $Q(a) = F$.

$LHS = \forall y\, P(y) = P(a) = T$

$RHS = \forall y\, (P(y) \wedge Q(y)) = [P(a) \wedge Q(a)]$

$\equiv T \wedge F$

$\equiv F$

$\therefore T \rightarrow F$

$\equiv F$

* Logical Equivalence in FOL.

If α, β are FOL expressions, and

iff $\alpha \rightarrow \beta$ is valid &
iff $\beta \rightarrow \alpha$ is valid,

then

$\alpha \equiv \beta$.

* Distributive Property of Quantifiers:

The distribution of a quantifier Π {$\exists, \forall, \exists!$} over connective # {$\wedge, \vee, \oplus$, etc} can be given as:

$$\underbrace{\Pi x\ [P(x)\ \#\ Q(x)]}_{\text{compact form}} \rightleftarrows \underbrace{\Pi x\, P(x)\ \#\ \Pi x\, Q(x)}_{\text{expanded form}}$$

if both $\rightarrow$ & $\leftarrow$ are valid, then

$\alpha \equiv \beta$.

(or compact form $\equiv$ expanded form)

Ex. $\exists x\,[P(x) \wedge Q(x)]$ & $\{\exists x P(x) \wedge \exists x Q(x)\}$

1. Compact $\rightarrow$ Expanded. ∴ valid?

Assuming LHS is true.

$\therefore \exists x\,[P(x) \wedge Q(x)]$

$\equiv [P(a) \wedge Q(b)] \vee [P(b) \wedge Q(b)] \ldots$

$\equiv T$

{say for 'b'}

On RHS:

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

$\Rightarrow \underset{\{\text{for b}\}}{T} \wedge \underset{\{\text{for b}\}}{T}$

$\Rightarrow T$

$\therefore$ 1 is valid.

Q. $E \rightarrow C$. Valid?

Assuming LHS True.
i.e.

$\exists x P(x) \wedge \exists x Q(x)$
$\equiv T \wedge T$
$\equiv T$

Say $\exists x P(x)$ is T for 'a'
$\exists x Q(x)$ is T for 'b'.

RHS:

$\exists x [P(x) \wedge Q(x)]$
$\Rightarrow [P(a) \wedge Q(a)] \vee [P(b) \wedge Q(b)]$
$\Rightarrow F \vee F$
$\Rightarrow F$

$\therefore$ Q is invalid.

Ex. $\exists x [P(x) \vee Q(x)]$ & $\exists x P(x) \vee \exists x Q(x)$

$\exists x [P(x) \vee Q(x)]$
$\equiv [P(a) \vee Q(a)] \vee [P(b) \vee Q(b)] \vee \ldots$
$\equiv [P(a) \vee P(b) \vee P(c) \ldots] \vee [Q(a) \vee Q(b) \vee Q(c) \ldots]$
$\equiv \exists x P(x) \vee \exists x Q(x)$

$\therefore \exists x [P(x) \vee Q(x)] \equiv \exists x P(x) \vee \exists x Q(x)$

Ex. $\exists x [P(x) \oplus Q(x)]$ & $\exists x P(x) \oplus \exists x Q(x)$

① Compact → Expanded. Valid?

Making LHS True.

$\equiv \exists x [P(x) \oplus Q(x)]$

$\equiv [P(a) \oplus Q(a)] \vee [P(b) \oplus Q(b)] \ldots$

T F F T

RHS:

$\equiv \exists x P(x) \oplus \exists x Q(x)$

$\equiv [P(a) \vee P(b)] \oplus [Q(a) \vee Q(b)]$

$\equiv T \oplus T$

$\equiv F$

∴ Not Valid.

② Expanded → Compact. Valid?

Making LHS True.

$\equiv \exists x P(x) \oplus \exists x Q(x)$

$\equiv T \oplus F$

$\equiv T$ {Say $P(a) = T$}

RHS

$\equiv \exists x (P(x) \oplus Q(x))$

$\equiv [P(a) \oplus F] \vee [P(b) \oplus F] \ldots$

$\equiv T \vee F \vee \ldots$

$\equiv T$

∴ $\exists x P(x) \oplus \exists x Q(x) \longrightarrow \exists x [P(x) \oplus Q(x)]$

*	$\forall$	$\exists$
$\wedge$	$\equiv$	$C \to E$
$\vee$	$E \to C$	$\equiv$
$\to$	$C \to E$	$E \to C$
$\leftrightarrow$	$C \to E$	X
$\oplus$	X	$E \to C$
$\uparrow$	$C \to E$	$E \to C$
$\downarrow$	$C \to E$	$E \to C$

$\equiv$: Equivalent
$C \to E$: Compact $\to$ Expanded
$E \to C$: Expanded $\to$ Compact

* Null Quantification Rules

Note: If a statement "S" doesn't have free variable "x", then,

$$\forall x\, S \equiv S$$
$$\exists x\, S \equiv S$$

* Null Quantification Rule: For some formula "S", when quantified for x, if there is some part of S, A, such that A has no free variable x, then, null quantification rules are applied.

Ex. $\forall x [P(x) \wedge A]$ =

affects

doesn't affect

Ex. $\forall x [(x>0) \wedge (2+2=5)]$

Ex. $\forall x (P(x) \vee A) \equiv \forall x P(x) \vee A$

Is it valid?

{ Here A has no free variable x
$\therefore \forall x A \equiv A$ }

Case 1: A = T.
LHS = T
RHS = T

Case 2: A = F
LHS = $\forall x P(x)$
RHS = $\forall x P(x)$

$\therefore$ Valid.

Ex. $\forall x [P(x) \vee A(x)] \equiv \forall x [P(x)] \vee \forall x A(x)$

Not valid.

Ex. $\exists x [P(x) \vee A] \equiv \exists x P(x) \vee A$

C1: A = T
LHS = T
RHS = T

C2: A = F
LHS = $\exists x P(x)$
RHS = $\exists x P(x)$

$\therefore$ Valid.

Ex. $\forall x [P(x) \to A] \equiv \forall x P(x) \to A$

C1: $A = T$
LHS = T
RHS = T

C2: $A = F$
LHS = $\forall x \neg P(x)$
RHS = $\neg \forall x P(x)$

∴ Not valid.

Ex. $\forall x [A \to P(x)] \equiv A \to \forall x P(x)$

C1: $A = F$
LHS = T
RHS = T

C2: $A = T$
LHS = $\forall x P(x)$
RHS = $\forall x P(x)$

∴ Valid.

* So, for $\# \in \{\wedge, \vee\}$.

$\forall x [P(x) \# A] \equiv \forall x P(x) \# A$
$\exists x [P(x) \# A] \equiv \exists x P(x) \# A$

- For $\to$,

$\forall x [A \to P(x)] \equiv A \to \forall x P(x)$
$\exists x [A \to P(x)] \equiv A \to \exists x P(x)$

- $\forall x [P(x) \to A] \equiv \exists x P(x) \to A$
$\exists x [P(x) \to A] \equiv \forall x P(x) \to A$

Ex. $\exists x\,(P(x) \to A) \equiv \forall x\, P(x) \to A$.

C1: A = F
LHS = $\exists x \neg P(x)$
RHS = $\neg \forall x\, P(x) \equiv \exists x \neg P(x)$

C2: A = T
LHS = T
RHS = T

Ex. "If anyone makes noise, then everyone will suffer."

$\exists x\, \underbrace{N(x)}_{P(x)} \to \underbrace{\forall x\, S(x)}_{A}$

$\equiv \forall x\, [\underbrace{N(x)}_{P(x)} \to \underbrace{\forall x\, S(x)}_{A}]$

Ex. $\exists x\, [P(x) \leftrightarrow A] \equiv \exists x P(x) \leftrightarrow A$.

C1: A = T
LHS = $\exists x\, P(x)$
RHS = $\exists x\, P(x)$

C2: A = F
LHS = $\exists x \neg P(x)$
RHS = $\neg \exists x P(x)$

$\therefore$ ~~Valid~~. Not Valid.

* Arguments in FOL

Argument { A(x), B(x) } → Premises
{ $\therefore$ C(x) } → conclusion.

* Procedure:

(1) Make conclusion false.
(2) Try to make all premises true.

If sucessful, then argument is invalid.
Else, valid argument.

Ex. Every man is mortal.
Aristotle is a man.
∴ Aristotle is mortal.

$\forall x\ [Man(x) \rightarrow Mortal(x)]$
$Man(Aristotle)$
$\therefore Mortal(Aristotle)$

or $\forall x\ [P(x) \rightarrow Q(x)]$
$P(a)$
$\therefore Q(a)$

Making $Q(a) = F$

$P(a) = T$.

But, $\forall x\ [P(x) \rightarrow Q(x)] = [P(a) \rightarrow Q(a)] \wedge [P(b) \rightarrow Q(b)] \ldots$
$= F \wedge \ldots$
$= F$.

∴ All Premises can't be made false.

∴ Valid argument.

* Rules of Inference.

1. $\forall x\ P(x)$ — Universal Instantiation.
   $\therefore$ for "specific" a, $P(a)$

2. for "arbitrary" a, $P(a)$ — Universal Generalization.
   $\therefore \forall x\ P(x)$

3. $\exists x\ P(x)$ — Existential Instantiation.
   $\therefore$ for "some" a, $P(a)$

4. for "some" a, $P(a)$ — Existential Generalization.
   $\therefore \exists x\ P(x)$

Ex. $\forall x\ [P(x) \vee Q(x)]$

$\forall x\ [\neg P(x) \wedge Q(x) \longrightarrow R(x)]$

$\therefore \forall x\ [\neg R(x) \longrightarrow P(x)]$

Making Conclusion false:
say for a.

$\neg R(a) \rightarrow P(a) \equiv F$

$\therefore R(a) = F$

$P(a) = F$

Premise (1) could still hold if $Q(a) = T$

$P(2)$ for a.

$T \wedge T \rightarrow F$

$T \rightarrow F \equiv F$

$\therefore P(2)$ is false $\forall x$.

$\therefore$ All premises can't be made false.

$\therefore$ Valid argument.

Ex. $\forall x [P(x) \vee Q(x)]$ —(1)

$\forall x [\neg Q(x) \vee S(x)]$ —(2)

$\forall x [R(x) \rightarrow \neg S(x)]$ —(3)

$\exists x \neg P(x)$ —(4)

$\therefore \exists x \neg R(x)$

Say, $\neg P(a) = T$ in (4).

from (1) $\forall x [\neg P(x) \rightarrow Q(x)]$

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

(1) & (4) : $Q(a)$ —(5)

from (2): $\forall x [Q(x) \rightarrow S(x)]$

$\therefore Q(a) \rightarrow S(a)$

(5) & (2) : $S(a)$ —(6)

from (3): $\forall x [S(x) \rightarrow \neg R(x)]$

$\therefore S(a) \rightarrow \neg R(a)$

from (6) & (3) : $\neg R(a)$

$\therefore \exists x \neg R(x)$

* Tautology in FOL

- In propositional logic, a tautology is a formula which is always true.

- In P.L. Tautology is same as Valid.

Ex. "2+2=4" is not tautology. It's just a statement.
Say, P. P can be T or F. P is contingency.

"2+2=4" or "2+2≠4" is a tautology.
P ∨ ¬P

Tautology is something trivially true. It's only a concept of Propositional Logic.

Ex. $[\forall x\, P(x)] \rightarrow [\forall x\, P(x)]$ is tautology.

$S \rightarrow S$

Uniformly replaced the formula with propositional variable makes the statement tautology in P.L.

Ex. $\forall x\, P(x) \rightarrow \exists x\, P(x)$

$S \rightarrow T$

This is not tautology in P.L.
∴ $\forall x P(x) \rightarrow \exists x P(x)$ is not tautology in FOL.
Although it is valid in FOL.

Ex. $\underbrace{\forall x\,(x=x)}_{S}$

S is not P.L. Tautology.

∴ $\forall x\,(x=x)$ is not tautology in FOL, although valid.

Ex. $[\underbrace{\forall x \neg P(x)}_{A} \rightarrow \underbrace{\neg P(x)}_{\neg B}] \rightarrow [\underbrace{P(x)}_{B} \rightarrow \underbrace{\neg \forall x \neg P(x)}_{\neg A}]$

$(A \rightarrow \neg B) \rightarrow (B \rightarrow \neg A)$

is PL Tautology.

∴ FOL Tautology.

SET THEORY

A set is an unordered collection of distinct elements.

Two sets are equal if they have same content ignoring the order.

Ex. No. of elements in set {1,1, a, a, a, 2, 3} = 4.

* Belongs To / Element of: (∈)

Used to indicate that something is an element of the set.

Ex apple ∈ {apple, ball, cat}.
Ex. 2 ∈ Set of prime nos.

* Finite Set: Set in which no. of elements is equal to some whole nos.

Infinite Set: Set with ∞ no. of membess.
Ex. N = {1, 2, 3, ...}
Z = {..., -3, -2, -1, 0, 1, 2, 3, ...}
Q = Set of rational nos. = {p/q | p, q ∈ Z, q ≠ 0}
R = Set of real nos. = {0, 1, 2.2, π, e, ...}

{∞ is not a no., its just a placeholder for a very large value}

* Cardinality {Finite set}

Cardinality of a set S is the no. of elements in the set. Denoted by |S|.

Ex. $S = \{1, 2\}$ $\quad |S| = 2$.

* Empty Set

A set with cardinality 0. Denoted by, $\{\}$ or $\emptyset$.

- $\emptyset \neq \{\emptyset\}$.
- $|\emptyset| = 0$
- $|\{\emptyset\}| = 1$.

* Set Builder Notation

Ex. Set of all even nos.

$$\{x \mid x \in \mathbb{N} \wedge 2 \mid x\}$$

or

$$\{2n \mid n \in \mathbb{N}\}$$

* $\{ x \mid \text{some property of } x \}$

↑

Set Builder Notation

* Subsets

A set 'x' is called a subset of set 'S', and is formed by removing 0 or more elements from 'S'. Denoted by,

$$X \subseteq S.$$

- Every element of X is in S.
- Every element of S may/maynot be in X.

- ϕ is subset of every set.
- A set S is always its own subset.

* Proper Subset

A set P is proper subset of S if P is a subset of S, and $P \neq S$. Denoted by,

$$P \subset S.$$

- A set S, $S \subseteq S$ ✓
  $S \subset S$ ✗

* Power Set

The Power set of a set S, denoted by P(S), is the set of all the subsets of S.

Ex. $S = \{a, b, c\}$

$P(S) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

• Cardinality of P(S) = # of subsets of $S = 2^n$ or $2^{|S|}$

{where n = no. of elements in S}

Ex. $S = \{\}$

$P(S) = \{\emptyset\}$

Ex. $S = \{\emptyset\}$

$P(S) = \{\emptyset, \{\emptyset\}\}$

$P(P(S)) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$

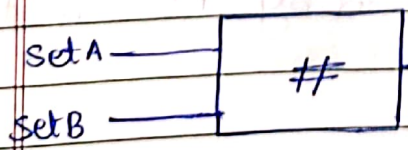
* Universal Set

A set containing everything under consideration.
• content depend on context.

* Set Operations

• We have +, −, /, * for numbers.
• We have ∧, ∨, ⊕, etc. for propositions.

• For sets we have Union, Intersection, Difference, complement, etc.



{or can be unary operator like complement.}

Input is/are set & Output is set.

{ $x \in$ Universal Set }

* Intersection

$A \cap B$ = All elements which belong to both A & B.

$\Rightarrow \forall x [x \in A \wedge x \in B \rightarrow x \in A \cap B]$

$\Rightarrow \{x \mid x \in A \wedge x \in B\}$

* Union

$A \cup B$ = All elements which either belong to A or B or both.

$\Rightarrow \forall x [x \in A \vee x \in B \rightarrow x \in A \cup B]$

$\Rightarrow \{x \mid x \in A \vee x \in B\}$.

* Symmetric Difference

$A \Delta B$ = All elements which either belong to A or B, but not both.

$\Rightarrow \forall x [x \in A \oplus x \in B \rightarrow x \in A \Delta B]$

$\Rightarrow \{x \mid x \in A \oplus x \in B\}$

* Complement

$\bar{A}$ = All elements which don't belong to A

$\Rightarrow \forall x [\neg(x \in A) \rightarrow x \in \bar{A}]$

$\Rightarrow \{x \mid x \notin A\}$

* Set Difference (- or \)

A - B = All elements which belong to A, but not B.

$\{A \setminus B\} \Rightarrow \forall x [x \in A \wedge \neg(x \in B) \longrightarrow x \in A - B]$

$\Rightarrow \{x \mid x \in A \wedge x \notin B\}$

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

$\{B \setminus A\}$

$\{A - B \neq B - A\}$

- If for sets A & B, $A \cap B = \emptyset$, then A & B are disjoint sets.

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

  Ex. $A = \emptyset$ $B = \emptyset$

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

  $\Rightarrow (A - B) \cup (B - A)$

- $A - B = A \cap \bar{B}$
- $\bar{A} = U - A$

* Set Equality

Two sets are equal if

$\forall x [x \in A \longleftrightarrow x \in B]$

or

$A = B$ iff $A \subseteq B$ and $B \subseteq A$

* Proving $A \subseteq B$:

(1) Assume arbitrary $x \in A$.
(2) Prove $x \in B$.

Ex. Prove $A - B = A \cap \bar{B}$

Check 1: $(A-B) \subseteq (A \cap \bar{B})$

Assuming $x \in (A-B)$
So, $x \in A$ & $x \notin B$.
$\Rightarrow x \in \bar{B}$
$\therefore x \in A$ and $x \in \bar{B}$
$\therefore x \in A \cap \bar{B}$

Hence,
$(A-B) \subseteq (A \cap \bar{B})$

Check 2: $(A \cap \bar{B}) \subseteq (A-B)$

Assuming $x \in (A \cap \bar{B})$
So, $x \in A$ & $x \in \bar{B}$
$x \in A$ & $x \notin B$.
$\therefore x \in A - B$

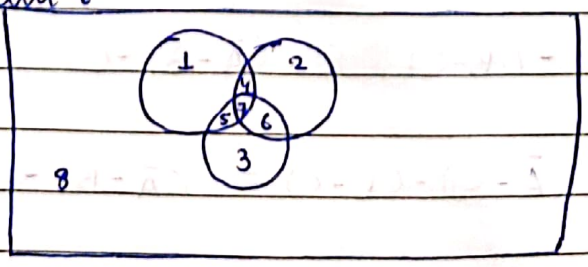
Hence,
$(A \cap \bar{B}) \subseteq (A-B)$

&

$\therefore A - B = A \cap \bar{B}$

Ex. Prove $(\bar{A} - B) - C = (\bar{A} - C) - (B - C)$

LHS Venn Diagram:



$\bar{A} = 2, 3, 6, 8$

$\bar{A} - B = 3, 8$

$(\bar{A} - B) - C = 8.$

RHS

$\bar{A} - C = 2, 8$

$B - C = (2,4,7,6) - (5,7,6,3)$
$= (2,4)$

$(\bar{A} - C) - (B - C) = (2,8) - (2,4)$
$= 8$

Analytical:

Check 1:

$(\bar{A} - B) - C \subseteq (\bar{A} - C) - (B - C)$

Assuming $x \in (\bar{A} - B) - C$.

So,

$x \in (\bar{A} - B)$ & $x \notin C$.

$\Rightarrow x \in \bar{A}$ & $x \notin B$ & $x \notin C$.

$\Rightarrow x \in \bar{A}$ & $x \notin B \subseteq C$ & $x \notin B$ & $x \notin C$.

$\Rightarrow x \in (\bar{A} - C)$ & $x \notin B$ & $x \notin C$

$\Rightarrow x \in (\bar{A} - C)$ & $x \notin (B - C)$

$\Rightarrow x \in [(\bar{A} - C) - (B - C)]$.

$\therefore (\bar{A} - B) - C \subseteq (\bar{A} - C) - (B - C)$

Check 2:

$(\bar{A} - C) - (B - C) \subseteq (\bar{A} - B) - C$.

Assuming $x \in (\bar{A} - C) - (B - C)$

So, $x \in (\bar{A} - C)$ & $x \notin (B - C)$

$\Rightarrow x \in \bar{A}$ & $x \notin C$ & $x \notin (B - C)$

$\Rightarrow x \in \bar{A}$ & $x \notin C$ & $x \notin B$

$\Rightarrow x \in (\bar{A} - B)$ & $x \notin C$

$\Rightarrow x \in [(\bar{A} - B) - C]$

$\therefore (\bar{A} - C) - (B - C) \subseteq (\bar{A} - B) - C$.

$\therefore (\bar{A} - C) - (B - C) = (\bar{A} - B) - C$.

Ex. Prove $A - (A-B) \subseteq B$

Assuming arbitrary $x \in A-(A-B)$

So,

$x \in A \quad \& \quad x \notin (A-B)$

$x \in A \quad \& \quad \boxed{x \in A \ \& \ x \in B}$ ($\because x \in A$ it must $\in B$ for it to $\notin (A-B)$)

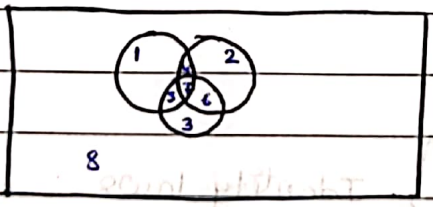
$\therefore x \in A \ \& \ x \in B$

$\therefore x \in B.$

$\therefore A - (A-B) \subseteq B.$

Ex. Prove $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$

Method 1: Venn Diagram



LHS:

$A = 1,4,5,7$

$B = 2,4,6,7$

$C = 3,5,6,7$

$B \cap C = 6,7$

$A \cup (B \cap C) = 1,4,5,6,7.$

RHS:

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

$A \cup C = 1,3,4,5,6,7$

$(A \cup B) \cap (A \cup C) = 1,4,5,6,7.$

$\therefore$ LHS $\subseteq$ RHS

Method 2: Analytical.

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

$\therefore x \in A$ or $x \in B \cap C$

$\Rightarrow x \in A$ or $[x \in B$ and $x \in C]$

C1: $x \in A$.

$\Rightarrow x \in A \cup B$ & $x \in A \cup C$.

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

C2: $x \in B$ and $x \in C$.

$\Rightarrow x \in A \cup B$ and $x \in A \cup C$.

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

* Set Identities

{ universal set: ω }

1. $S \cup \phi = S$
2. $S \cap \omega = S$.

} Identity laws

. ~~Identity~~ Identity Element: 'e' should satisfy the following properties to be the identity element of the operation #:

$S \# e = S$

$e \# S = S$.

3. $S \Delta \phi = \phi \Delta S = S$.

4. $S - \phi = S$ ∴ $-$ has no identity element.
$\phi - S = \phi$

- Cross Product: $A \times B = \{(a,b) \mid a \in A, b \in B\}$.
(x)

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

$A \times B = A$ iff, $A = \phi$.
$\phi \times B = \phi$.

5. $A \cup \omega = \omega$ } Domination Laws.
6. $A \cap \phi = \phi$ }

7. $A \cup A = A$ } Idempotent Laws.
8. $A \cap A = A$ } $\{A \# A = A\}$.

9. $\overline{\overline{A}} = A$.

10. $A \cup \bar{A} = \omega$
11. $A \cap \bar{A} = \phi$

- Commutative Laws: An operation # is commutative iff:
$A \# B = B \# A$.

12. $A \cup B = B \cup A$ {$-$, $\times$ are not commutative}
13. $A \cap B = B \cap A$
14. $A \Delta B = B \Delta A$

• Associative Law: An operation # is associative iff:

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

15. $A \cup (B \cup C) = (A \cup B) \cup C$
16. $A \cap (B \cap C) = (A \cap B) \cap C$.
17. $A \Delta (B \Delta C) = (A \Delta B) \Delta C$

• Distributive Property: An operation # is distributive over operation * iff

$$A \# (B * C) = (A \# B) * (A \# C)$$

18. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
19. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

• Absorption Laws:

20. $A \cup (A \cap B) = A$
21. $A \cap (A \cup B) = A$

• Demorgan Laws:

22. $\overline{(A \cup B)} = \bar{A} \cap \bar{B}$
23. $\overline{(A \cap B)} = \bar{A} \cup \bar{B}$

24. $A - B = A \cap \bar{B} = \bar{B} - \bar{A}$
25. $A \oplus B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$

• Precedence of Operations:

1. $\bar{A}$ Complement
2. $A \cap B$ Intersection
3. $A \cup B$ Union.

Ex. $E = A \cup B \cap C$.

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

$\Rightarrow \bar{A} \cap \overline{[B \cap C]}$

$\Rightarrow \bar{A} \cap [\bar{B} \cup \bar{C}]$

* Proofs Related to Power Set.

- $P(A) = \{S \mid S \subseteq A\}$.
- $|P(A)| = 2^{|A|}$
- $X \subseteq A$ iff $X \in P(A)$
- For any set A, $\emptyset \in P(A)$
- For any set A, $A \in P(A)$
- If $X \in P(A)$, then X is a set.

Ex. Show that, $A \cap B = A$ iff $A \in P(B)$.

Check: $(A \cap B = A) \longrightarrow (A \in P(B))$

i.e. $(A \cap B = A) \rightarrow (A \subseteq B)$

$\because A \cap B = A$, all elements of A are in B.

$\therefore A \subseteq B$.

Check 2: $(A \subseteq B) \longrightarrow (A \cap B = A)$

$\because A \subseteq B$, every element of A is in B.

$\therefore A \cap B = A$.

Ex. Show that $P(A) \cap P(B) = P(A \cap B)$

Check 1:
Assuming $X \in [P(A) \cap P(B)]$.

$\therefore X \in P(A)$ & $X \in P(B)$
$\Rightarrow X \subseteq A$ & $X \subseteq B$.
$\Rightarrow \forall x\,(x \in X \rightarrow x \in A)$ & $\forall x\,(x \in X \rightarrow x \in B)$
$\Rightarrow \forall x\,(x \in X \rightarrow x \in (A \cap B))$
$\Rightarrow X \subseteq A \cap B$.
$\Rightarrow X \in P(A \cap B)$.

Check 2:
Assuming $X \in [P(A \cap B)]$.
$\Rightarrow X \subseteq A \cap B$
$\Rightarrow X \subseteq A$ & $X \subseteq B$.
$\Rightarrow X \in P(A)$ & $X \in P(B)$
$\Rightarrow X \in [P(A) \cap P(B)]$.

Ex. Show that, $[P(A) \subseteq P(B)] \rightarrow (A \subseteq B)$

~~Assuming, $X \in P(A)$.~~

$\Rightarrow P(A) \subseteq P(B)$

$\Rightarrow \forall x [x \in P(A) \rightarrow X \in P(B)]$

$\Rightarrow \forall x [X \subseteq A \rightarrow X \subseteq B]$

$\Rightarrow$ every subset of A is subset of B.
A is subset of A.

$\therefore A \subseteq B$.

RELATIONS

* Cartesian Product / Cross Product

The cartesian product $A \times B$ b/w the sets A & B, is a set of ordered pairs (a,b) where $a \in A$ & $b \in B$.

$$A \times B = \{(a,b) \mid a \in A \ \& \ b \in B\}$$

: Ordered pair: $(a_1, a_2, \ldots, a_n)$ n-tuple. (a,b) is an ordered pair, since order of a & b matters, i.e.

$$(a,b) \neq (b,a).$$

- n-tuple: A tuple with n elements in order.
- $|A \times B| = |A| \cdot |B|$
- $A \times (B \times C) \neq (A \times B) \times C$

  Ex. $A = \{1,2\}$ $B = \{a,b\}$ $C = \{\alpha, \beta\}$

  $A \times (B \times C) = \{(1,(a,\alpha)), (1,(a,\beta)), (1,(b,\alpha)), \ldots\}$

  $(A \times B) \times C = \{((1,a),\alpha), ((1,b),\alpha), ((2,a),\alpha), \ldots\}$

- $A \times B = B \times A$ iff

  (1) $A = B$ or

  (2) $A = \phi$ or

  (3) $B = \phi$

- $A \times B \times C = \{(a,b,c) \mid a \in A, b \in B, c \in C\}$.

$A \times B \times C \neq A \times (B \times C) \neq (A \times B) \times C$

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

- $A_1 \times A_2 \times A_3 \times \dots \times A_n = \{(a_1, a_2, a_3 \dots, a_n) \mid a_i \in A_i\}$

* Relations

A relation R b/w set A & B is a subset of $A \times B$ based on certain property of (a,b), where $(a,b) \in A \times B$.

Ex.

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

$A \times B = \{(1,4), (2,4), (3,4), (1,0), (2,0), (3,0)\}$

Say, $R = \{(a,b) \mid (a,b) \in R,\ a < b\}$
$= \{(1,4), (2,4), (3,4)\}$.

$R: A \to B$ is subset of $A \times B$.
xRy iff $x < y$, $x \in A$, $y \in B$.

- $(a,b) \in R \equiv aRb$
- Relation from A to B is one way, i.e.
  $aRb \neq bRa$.

Ex. $T: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
$(a,b)\,T\,y$ iff $(a+b) = y$.

$T = \{((1,1),2), ((1,2),3), ((2,5),7) \dots\}$
So, $T \subseteq (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$
$T \not\subseteq \mathbb{N} \times \mathbb{N} \times \mathbb{N}$.

- No. of relations that can be created from set A to set B:

each relation $R \subseteq A \times B$

∴ No. of possible relations = No. of subsets of $A \times B$ = $|P(A \times B)|$

$= 2^{|A \times B|}$

$= 2^{|A| \times |B|}$

∴ No. of relations = $2^{|A| \times |B|}$

- a is related to b ≠ b is related to a.
  {order matters}

- Relation of type "from A to A", i.e.

$R: A \to A$

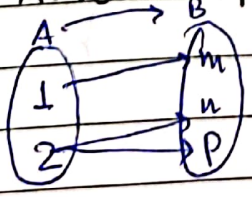
is read as "relation is on set A".

* Representations of Relations:

Eg. $R: A \to B$ $\quad A = \{1, 2\}$ $\quad B = \{m, n, p\}$.

$1Rm, 2Rn, 2Rp$.

(1) Arrow Repr. (2) Set Repr.



$R = \{(1, m), (2, n), (2, p)\}$

. For relations on A ($R: A \to A$) there are two additional representations :

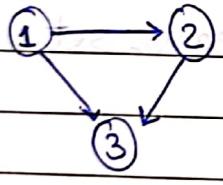
(1) Matrix Repr. (2) Graph Repr.

Ex. $A = \{1, 2, 3\}$ R is on A.

$x R y$ iff $x < y$.

$R = \{(1,2), (1,3), (2,3)\}$ // Set Repr.

Graph Repr.

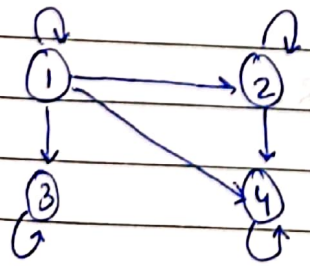


Matrix Repr.

R	1	2	3
1	x	✓	✓
2	x	x	✓
3	x	x	x

Ex. $A = \{1, 2, 3, 4\}$ R is on A.

$x R y$ iff $x | y$.



R	1	2	3	4
1	✓	✓	✓	✓
2	x	✓	x	✓
3	x	x	✓	x
4	x	x	x	✓

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

Ex. $R = \{((a,b),(c,d)) \mid a,c \in Z, b,d \in N, a+c=b+d\}$

$R : (Z \times N) \to (Z \times N)$

Base set: $(Z \times N)$

Which of the following is/are correct?

(A) $(1,2)\ R\ (-3,-4)$ ✗ $(-3,-4) \notin (Z \times N)$

(B) $(-2,1)\ R\ (3,x),\ x \in N$ ✗ No such $x \in N$.

(C) $(-2,2)\ R\ (5,x),\ x \in N$ ✓ $x = 1$

(D) $(1,2)\ R\ (3,2)$ ✓

★ Note: Always take care of base set.

Ex $R : Z \to Z$ Relation R on Z {Z is base set}

xRy iff $n \mid (x-y)$ where $n \in Z^+$

or

$x \equiv y \pmod{n}$

for $n = 7$, which of the following $\in R$:

(A) $9\ R\ 2$ ✓ $7 \mid (9-2) = 7 \mid 7$

(B) $-3\ R\ 11$ ✓ $7 \mid -14$

(C) $(14, 0)$ ✓ $7 \mid 14$

(D) $3\ R\ 7$ $7 \nmid -4$

for $7Rx$, $n=3$, $x=?$

(A) $3x+2$; $x \in Z$

(B) $3x+1$; $x \in Z$ ✓

(C) $3x+1$; $x \in Z^+$ ✓

Ex. For the Universe $U = \{1,2,3,4,5,6,7\}$, consider the set $C = \{1,2,3,6\}$. Define a rel. R on $P(U)$, by ARB when $A \cap C = B \cap C$.

R is on $P(U)$, i.e., $R: P(U) \to P(U)$.

$R = \{(\phi, \phi), (\{1\},\{1\}), (\{2\},\{2\}), \ldots (\{1,2,5,7\},\{1,2\}), \ldots\}$

- A & B are subsets of U.
- For $\forall A \in P(U)$, ARA

* Properties of Relations:

* Reflexivity

- A pair (a,a) is called Reflexive pair.
- Reflexive Relation: A relation R on set A is reflexive iff:

$$\forall x\, [x \in A \to (xRx)]$$

i.e. all the elements of A should be related to themselves.

- The relation R will be not reflexive if

$$\exists x\,[x \in A \wedge x \not R x]$$

i.e. at least one element should be not related to itself.

- Irreflexive Relation : A relation R on base set A is irreflexive iff:

$$\forall x\,[x \in A \rightarrow x \not R x]$$

i.e. no element at all should be related to itself.

- Diagonal / Equality / Identity Relation:
A Diagonal relation R on base set A is defined as:

$$R = \{(x,x) \mid x \in A\}$$

i.e. only self related ordered pairs.

Ex. What is the type of following relations:

(1) $R = \phi$ on $A = \phi$
Reflexive

(2) $R = \phi$ on $A = \{a, b\}$
Irreflexive.

* Symmetry:

- **Symmetric Pairs:** (a, b) & (b, a) are symmetric pairs.
- **Symmetric Relation:** A relation R on base set A is symmetric iff:

$$\forall x \forall y \, [[x \in A \wedge y \in A \wedge xRy] \rightarrow yRx]$$

or

$$\forall x \in A \, \forall y \in A \, [xRy \rightarrow yRx]$$

- **Anti-Symmetric Relation:** A relation R on base set A is anti-symmetric iff:

$$\forall x \in A \, \forall y \in A \, [(xRy) \wedge (yRx) \rightarrow (a = b)]$$

i.e. for any two distinct elements x & y, both (x, y) and (y, x) shouldn't belong to R.

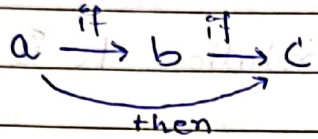
- **Asymmetric Relation:** A relation R on base set A is asymmetric iff:

$$\forall x \in A \, \forall y \in A \, [xRy \rightarrow yRx]$$

i.e. Anti-Symmetric + Irreflexive.

* Transitivity

- Transitive Property: if (aRb), (bRc) then (aRc)

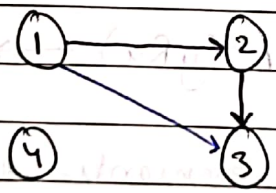


- Transitive Relation: A relation R on base set A, is transitive relation, iff:

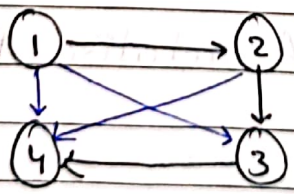
$$\forall x \forall y \forall z \; [(xRy) \wedge (yRz) \longrightarrow xRz]$$

Ex. Make the following transitive:

(1)

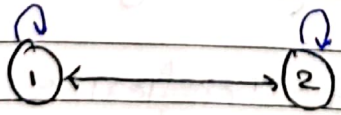


(2)



{(1,2), (2,3), (3,4), (1,3), (3,4), (1,4)}

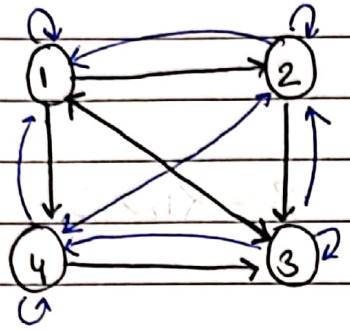
(3)



{(1,2), (2,1), (1,1), (2,2)}

★ Transitive Closure procedure

(4)



{(1,2), (1,3), (1,4), (2,3), (3,1), (4,3), (1,1), (2,1), (3,2), (3,3), (3,4), (4,1), (4,2), (4,4), (2,2), (2,4)}.

* Equivalence Relation:

A relation R on base set A is Equivalence iff:

(1) R is Reflexive.
(2) R is Symmetric.
(3) R is Transitive.

* Partition of Set

A partition of a set S (non-empty set) into parts $P_1, P_2, P_3 \dots P_n$ is division of elements of S into the parts such that:

(1) $\forall i \forall j \; P_i \cap P_j = \emptyset, \; i \neq j$
(2) $\bigcup_{i=1} P_i = S$
(3) $\forall i \; P_i \neq \emptyset$

Ex. $S = \{1, 2, 3, 4\}$. Which of the following is/are partitions of S:

(A) $\{\{1\}, \{2,3\}, \{4\}\}$ ✓
(B) $\{\{1,2\}, \{2,3\}, \{4\}\}$ ✗
(C) $\{\{1,2\}, \{3,4\}, \{\}\}$ ✗

(D) $\{\{1,2,3,4\}\}$ ✓

Ex. No. of partitions of set $S = \{1,2,3\}$

$P_1 = \{\{1,2,3\}\}$
$P_2 = \{\{1\},\{2,3\}\}$
$P_3 = \{\{2\},\{1,3\}\}$
$P_4 = \{\{3\},\{1,2\}\}$
$P_5 = \{\{1\},\{2\},\{3\}\}$

∴ 5 partition.

Ex. Which of the following are valid partitions on set $\mathbb{Z}$?

(A) {even, odd} ✓
(B) {+ve, -ve} ✗ 0 is neither.
(C) {prime, composite} ✗ 1 is neither
(D) $\{\%10=0, \%10=1, \ldots, \%10=9\}$ ✓

Ex. Π is a partition of $S = \{a,b,c,d,e,f\}$ with 3 parts. a,b are in same part. c,d are in same part. No. of all such partitions.

$P_1 = \{\{a,b,c,d\},\{e\},\{f\}\}$
$P_2 = \{\{a,b\},\{c,d\},\{e,f\}\}$
$P_3 = \{\{a,b,e\},\{c,d\},\{f\}\}$
$P_4 = \{\{a,b\},\{c,d,e\},\{f\}\}$
$P_5 = \{\{a,b,f\},\{c,d\},\{e\}\}$
$P_6 = \{\{a,b\},\{c,d,f\},\{e\}\}$

∴ 6.

* Equivalence Relation (contd.)

Ex. $S = \{2,3,4,5,6,7,8\}$. R is a relation over S. xRy iff $x-y = 3n$ for some $n \in Z$. Check if R is equivalence relation

$x-y = 3n$
$\Rightarrow 3 \mid (x-y)$
$= x \bmod 3 = y \bmod 3$.

(1) for all x, $x-x = 0 = 3n \Rightarrow n = 0$.
$\therefore$ R is reflective.

(2) If $x-y = 3n$ then $(y-x) = -3n$.

$\therefore$ R is reflexive.

(3) If xRy & yRz, then

$x \bmod 3 = y \bmod 3 = r$.

$y \bmod 3 = z \bmod 3 = r$.

$\therefore x \bmod 3 = z \bmod 3 = r$.
$\therefore (x-z) = 3n$.

$\therefore$ R is transitive.
$\therefore$ R is equivalence relation.

- $[a]_R = \{ b \mid aRb \}$. {class of 'a'}
{where R is an equivalence relation}

- $[2]_R = \{2, 5, 8\}$
- $[3]_R = \{3, 6\}$
- $[4]_R = \{4, 7\}$
- $[5]_R = \{5, 2, 8\}$
- $[6]_R = \{6, 3\}$
- $[7]_R = \{4, 7\}$
- $[8]_R = \{2, 5, 8\}$
- So, class of 2 = class of 5 = class of 8.
  class of 3 = class of 6.
  class of 4 = class of 7.

- All the unique classes form a partition of the base set S.

  Ex.

  $\{[2]_R, [3]_R, [4]_R\}$.

Each part in R is called Equivalence Class.

* Equivalence Class $[a]_R$ where R is an equivalence relation is the set of all b, such that aRb.

$$[a]_R = \{b \mid aRb\}.$$

Ex. $A = \{0, 1, 2\}$. $R = \{(0,0), (1,1), (2,2), (0,1), (0,2), (1,0), (1,2), (2,0), (2,1)\}$. R is equivalence rel. Analyze.

R is the full (universal) relation. i.e.

$$R = A \times A$$

- R is symmetric.
- R is reflexive.
- R is not anti-symmetic.
- R is transitive.

- $[0]_R = \{0, 1, 2\}$.
- $[1]_R = \{0, 1, 2\}$
- $[2]_R = \{0, 1, 2\}$.

$\therefore [0]_R = [1]_R = [2]_R$

$\therefore$ Relation R has one equivalence class & hence 1 partition.

Ex. $A = \{1, 2, \ldots 20\}$. R on A, xRy, iff. $x \equiv y \pmod 4$. No. of partition of A by R?

R is equivalance relation.

$[1]_R = \{1, 5, 9, 13, 17\}$

$[2]_R = \{2, 6, 10, 14, 18\}$

$[3]_R = \{3, 7, 11, 15, 19\}$

$[4]_R = \{4, 8, 12, 16, 20\}$.

$\therefore$ R divides A into 4 partitions. Each equivalance class represents 1 part.

- In an equivalence class, every element is related to every other element.

- If, for an equivalence relation R, we have information about the equivalence classes, what is the value of |R|?

∵ For every $[a]_R$ every element is related to every other element.

So,

$$|R| = |[a_1]_R|^2 + |[a_2]_R|^2 + \dots + |[a_n]_R|^2$$
$$\text{or } |E_1|^2 + |E_2|^2 + \dots |E_n|^2$$

Ex. $A = \{2, 3, 5, 6, 11, 12\}$. R on A. $x \, R \, y$ iff $x \equiv y \pmod 3$.

R is equivalence Relation.

$[2]_R = \{2, 5, 11\}$
$[3]_R = \{3, 6, 12\}$

∴ $|R| = |[2]_R|^2 + |[3]_R|^2$
$\Rightarrow (3)^2 + (3)^2$
$\Rightarrow 18.$

- So every unique Equivalence relation R on A gives unique partition of A.

Also, for every partition of A, we have unique ER R corresponding to that partition.
∴ No. of possible ER on A is same as no. of partition of A.

Ex. $A = \{a,b,c\}$ $P = \{\{a\}, \{b,c\}\}$

If we assume each part as equivalence class of some ER, R, then,

$$R = (E_1 \times E_1) \cup (E_2 \times E_2) \cup \ldots (E_n \times E_n)$$

$$\Rightarrow (\{a\} \times \{a\}) \cup (\{b,c\} \times \{b,c\})$$
$$\Rightarrow \{(a,a)\} \cup \{(b,b), (b,c), (c,b), (c,c)\}.$$
$$\Rightarrow \{(a,a), (b,b), (c,c), (b,c), (c,b)\}.$$

$$|R| = |E_1|^2 + |E_2|^2$$
$$\Rightarrow 1^2 + 2^2$$
$$\Rightarrow 5.$$

- For the base set A:
  1. Largest Eq. Relation will be $A \times A$.
     Cardinality of largest ER = $|A \times A|$
     No. of equivalence classes = 1.

  2. Smallest ER = Identity Relation.
     Cardinality = $|A|$
     No. of Equivalence Classes = $|A|$

* Number of Relations

{ Consider the base set A. $|A| = n$ }

- No. of possible reflexive relations:

Every element in A, must have (a,a) pair in R for R to be reflexive. Other ordered pairs in A x A may or may not be in R.

$$1^n \times 2^{n^2-n}$$
$$\Rightarrow 2^{n^2-n}$$

- No. of irreflexive relations:

Every diagonal ordered pair (a,a) must be absent from R.

$$1^n \times 2^{n^2-n}$$
$$\Rightarrow 2^{n^2-n}$$

- No. of Symmetric Relations:

Every pair of ordered pairs (a,b) & (b,a) has two choices, either both pairs are absent, or both pairs are present.

$$\Rightarrow 2^n \times 2^{\frac{n^2-n}{2}}$$

• No. of Anti-Symmetric Relations

Every pair of ordered pair (a,b) & (b,a) $\{a \neq b\}$ has three choice. Either both are absent, or pair 1 present pair 2 absent or pair 1 absent, pair 2 present.

$$\Rightarrow 2^n \times 3^{\frac{n^2-n}{2}}$$

• No. of Asymmetric Relations

Along with the non-diagonal pairs of AxA having 3 choices, diagonal pairs have one choice. To be absent.

$$1^n \times 3^{\frac{n^2-n}{2}}$$
$$\Rightarrow 3^{\frac{n^2-n}{2}}$$

• No. of Equivalence Relations

Since there is one-to-one mapping b/w no. of partitions of a set A & no. of equivalence relations.

$$\#\text{ of ER} = \#\text{ of Partitions of A.}$$

This can be calculated using Bell Triangle:

1				
1	2			
2	3	5		
5	7	10	15	
15	20	27	37	52

$n=1 \quad B_1 = 1$

$n=2 \quad B_2 = 2$

$n=3 \quad B_3 = 5$

$n=4 \quad B_4 = 15$

$n=5 \quad B_5 = 52.$

For a set A, $|A| = n$, B_n gives the no. of possible Equivalence relations (and no. of possible Partitionings of A).

$B_0 = 1$

* Partial Order Relations (POR)

Ex. Say we have a set of subjects

$S = \{DM, TOC, DL, CD, CO\}$

and we want to figure out the order in which we study the study.

We can define a relation R on S, xRy iff x is prerequesite of y.

So,

DM R TOC
TOC R CD
DM R CD
DL R CO.

Now we have a ordering.

$DM \longrightarrow TOC \longrightarrow CD$

$DL \longrightarrow CO$

} Partial Order

But this ordering isn't Total; since there is

no order b/w say, DM & DL, or CO and TOC, etc.

A possible Total Order could be:

DL → CO → DM → TOC → CD

or

DL → DM → CO → TOC → CD

etc.

- So to get an order on elements of a set A, we define a Relation R on the elements of A.

Which properties should this relation satisfy?

(1) Symmetric: Says (a, b) → (b, a). Ex if a is pre-requesite of b, then b should be prereq. of a.
This doesn't make sense.

No.

(2) Anti-Symmetric: Says either (a, b) or (b, a) ∈ R or none do.
This is useful.

YES

(3) Transitive: Says if (a, b) & (b, c), then (a, c).
Ex. DM → TOC → CD

YES

(4) Reflexive: Says $(a,a) \in R$.

Ex. In case say a subject is not ~~subject~~ prerequesite of any subject, or doesn't have one, still it should be studied. This can be signified by adding (a,a) to the relation.

∴ YES.

* Partial Order Relation is a relation which satisfies the following properties: (RAnT)

(1) Reflexivity
(2) Anti-Symmetry
(3) Transitivity.

If R is a POR on the base set A, then, (A,R) is called Poset.

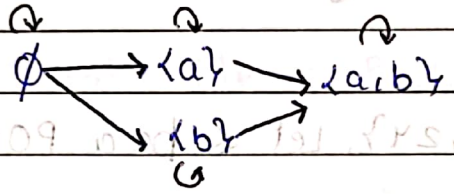
* Some standard POR:

1. $\leq$ on $\mathbb{N}$.
$(\mathbb{N}, \leq)$ is a Poset.
$(\mathbb{Z}, \leq)$ is a Poset
$(\mathbb{R}, \leq)$ is a Poset.

2. $(\mathbb{N}, \geq)$
$(\mathbb{Z}, \geq)$
$(\mathbb{R}, \geq)$ are Posets

3. $\subseteq$ on $P(A)$
$(P(A), \subseteq)$ is a Poset.

Ex. $A = \{a, b\}$ $P(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$



$R = \{ (\phi, \phi), (\{a\}, \{a\}), (\{b\}, \{b\}), (\{a,b\}, \{a,b\}),$
$(\phi, \{a\}), (\{a\}, \{a,b\})$
$(\phi, \{b\}), (\{b\}, \{a,b\})$
$(\phi, \{a,b\})$
$\}$

4. $\supseteq$ on $P(A)$
{superset}

5. $|$ on $\mathbb{N}$
{divides}
i.e. R on $\mathbb{N}$ such that $x R y$ iff $x | y$.

So, $(\mathbb{N}, |)$ is a Poset.

- Generally as a placeholder for R in Poset (A, R), "$\leq$" or "$\sim$" is used.

Ex.

$(\{1,2,3,4\}, R) \equiv (\{1,2,3,4\}, \leq) \equiv (\{1,2,3,4\}, \sim)$

$x R y$ iff $x|y$ $\quad$ $x \leq y$ iff $x|y$ $\quad$ $x \sim y$ iff $x|y$

→ x is related to y ←

Ex. Let $X = \{1, 2, 3, 6, 12, 24\}$, Let $\leq$ be a POR defined by: $x \leq y$ iff $x|y$.

(A) $2 \leq 3$
(B) $2 \leq 6$ ✓
(C) $3 \leq 12$ ✓
(D) $12 \leq 6$

- Total Order: A relation R on set A is total order iff for every $x, y \in A$, there is an order b/w x & y.

Ex:

$A = \{1^{st}\text{Sem}, 2^{nd}\text{Sem}, 3^{rd}\text{Sem}, 4^{th}\text{Sem}\}$
$B = \{\text{BTech}, \text{MTech}, \text{MBA}, \text{UPSC}\}$

R is such that xRy iff x must be done before y.

(1) R is total order on A. (and also Partial Order)

$1^{st}\text{Sem} \leq 2^{nd}\text{Sem} \leq 3^{rd}\text{Sem} \leq 4^{th}\text{Sem}$.

(Q) R on B is partial order since not all the elements are comparable.

Btech → MTech
MBA
UPSC.

- In a POR R, a & b are comparable iff either aRb or bRa.

- So, Total Order = Partial Order + Every two element comparable.

Ex. A relation R is defined on ordered pairs of integers:

$(x, y)\ R\ (u, v)$ iff $x \leq u$ and $y \geq v$

R is on $Z \times Z$.

Then R is:
(1) Equivalence
(2) POR
(3) TOR

Reflexivity: $(x, y)\ R\ (x, y) \Rightarrow x < y$ & $y > y$ is false.

∴ Not Reflexive.

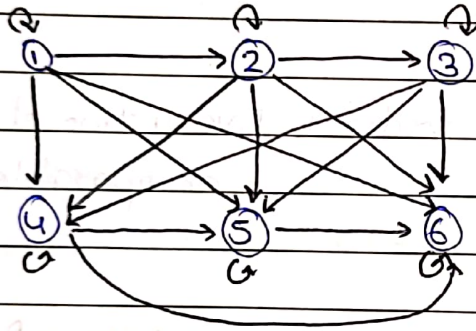
∴ None of the above.

* Hasse Diagram:

We can create a Hasse Diagram for a relation R iff R is POR.

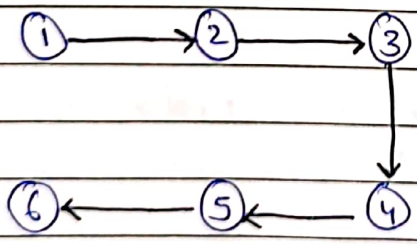
Ex. $(\{1,2,3,4,5,6\}, \leq)$

↳ less than equal to



This graph repr. or arrow diagram gets very uncomprehendable.

We already know, $\leq$ is a POR. We can avoid showing reflexive & transitive arrows.



Hasse Diagram. {Partial}

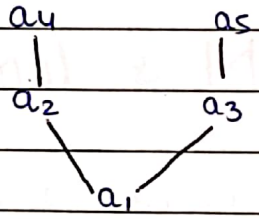
- In Hasse Diagram :
  (1) We don't show self loops.
  (2) Don't show transitive edges.
  (3) Don't show arrow, just edges. The direction is from bottom towards top.

So,

Hasse Diagram

{Implicitly, direction is upward. ↑}

Ex.



which of the following are true?

(A) $a_4 R a_5$ ✓

(B) $a_2 R a_5$ ×

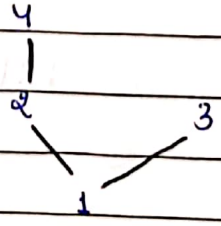
(C) $a_3 R a_1$ ×

(D) $a_3 R a_2$ ×

(E) $a_2 R a_4$ ✓

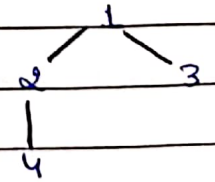
Ex. ({1,2,3,4}, |)

1R2R4; 1R3



Ex. ({1,2,3,4}, Multiple of)

4R2R1; 3R1



Ex. $(\{3,4,5\}, |)$

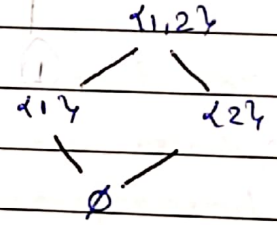
3 4 5 or

4 5 or

5 4 3

All are same since there are no upward path.

Ex. $(P(\{1,2\}), \subseteq)$



$\emptyset R \{1\}$ $R \{1,2\}$

$\emptyset R \{2\}$ $R \{1,2\}$

Ex. $(\{a,b,c\}, R)$

Possible HDs:

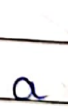
(1)

a b c

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

$|R| = 3$

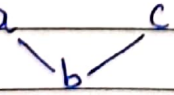
(2)



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

$|R| = 4$.

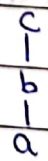
(3)



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

$|R| = 5$

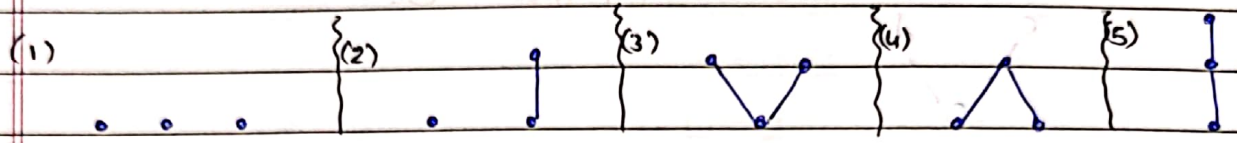
(4)



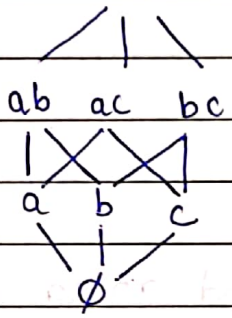
$R = \{(a,a), (b,b), (c,c), (a,b), (a,c), (b,c)\}$

$|R| = 6$.

So the following configurations are possible :



Ex. $(P(\{a,b,c\}), \subseteq)$



* Maximal & Minimal Elements

For a Poset (A, R) an element a is called :

1. Maximal iff,

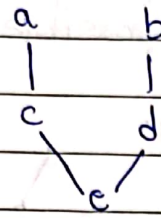
$$\forall x \in A \, [\, x \neq a \rightarrow a \not R x \,]$$

i.e. 'a' is not related to any element other than itself.

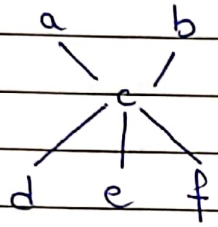
2. Minimal iff,

$$\forall x \in A \, [\, x \neq a \rightarrow x \not R a \,]$$

i.e. no element is related to 'a' other than itself.

Ex. 

Maximal : a, b
Minimal : e.

Ex. 

Maximal : a, b
Minimal : d, e, f.

- There is no upward going edge from Maximal elements.
- There is no incoming upward going edge to Minimal elements.

* Greatest / Maximum, Least / Minimum Element :

For a Poset (A, R) an element 'a' is called :

1. Maximum / Greatest iff

$$\forall x \in A \; [x R a]$$

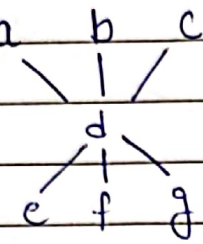
i.e. every element is related to 'a'.

2. Minimal / Least iff

$$\forall x \; [a R x]$$

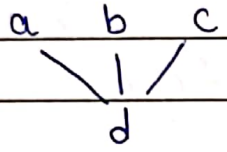
i.e. 'a' is related to every element.

Ex.



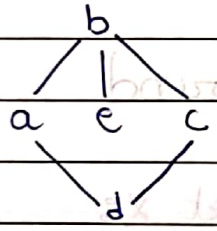
Maximal : a, b, c
Minimal : e, f, g
Greatest : –
Least : –

Ex.



Maximal : a, b, c
Minimal : d
Greatest : –
Least : d

Ex.

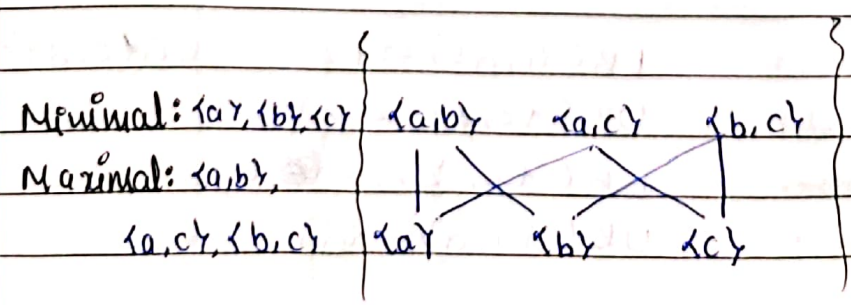


Maximal : b
Minimal : d, e
Greatest : b
Least : –

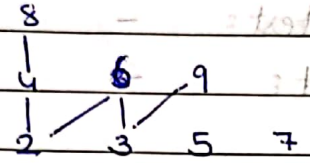
- There can be more than one maximal as well as minimal element possible.

There can be at most one greatest as well as least element possible.

Ex. $A = \{a, b, c\}$ $S = P(A) - \{\phi, \{a, b, c\}\}$. Hasse Diagram for S.



Ex. $(\{2,3,4,5,6,7,8,9\}, |)$



Maximal: 8, 6, 9, 5, 7
Minimal: 2, 3, 5, 7
Greatest: –
Least: –

* Upper Bound, Lower Bound.

In a Poset (A, R) for a subset X:

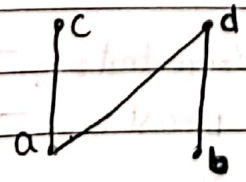
- Upper Bound of X is the elements a, $a \in A$, ($\{UB(x)\}$ ← set of all) such that

$$\forall x \in X \quad x R a.$$

- Lower Bound of X is the elements a, $a \in A$, ($\{LB(x)\}$ ← set of all) such that

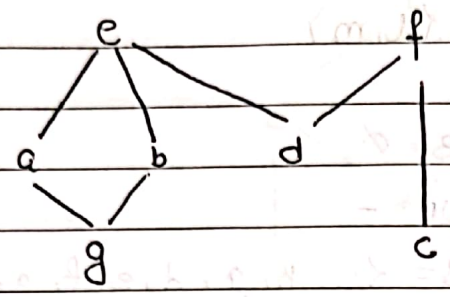
$$\forall x \in X \quad a R x.$$

Ex.



$LB(\{c,d\}) = \{a\}$ $\quad UB(\{c,d\}) = \{-\}$
$UB(\{c,a\}) = \{c\}$
$LB(\{c,b\}) = \emptyset$
$UB(\{a,d\}) = \{d\}$

Ex.



Maximal = {e, f}
Minimal = {c, d, g}

Greatest = ∅
Lowest = –

UB({a, g, b}) = {e}
LB({a, g}) = {g}
UB({a, g}) = {a, g, e}
LB({e, f}) = {d}
UB({e, f}) = ∅
UB({a}) = {a, e}
UB({g}) = {g, a, b, e}

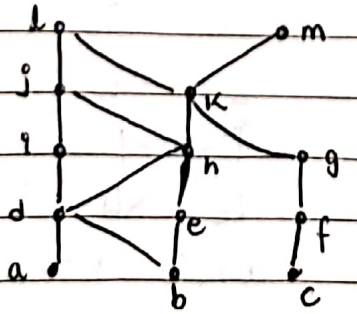
- Least Upper Bound of subset X, $X \subseteq A$, is the element 'a', $a \in UB(X)$. {∨}

$$\forall x \in UB(X) \quad a \, R \, x$$

- Greatest Lower Bound of subset X, $X \subseteq A$, is the element 'a', $a \in LB(X)$. {∧}

$$\forall x \in LB(X) \quad x \, R \, a$$

Ex.



Minimal: l, m
Maximal: a, b, c
Greatest: –
Least: –

(i) {d, K, f}

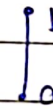
UB = {K, l, m}
LUB = K
LB = ∅
GLB = -

(ii) {l, m}

UB = ∅
LUB = -
LB = {K, h, g, d, e, f, a, b, c}
GLB = K.

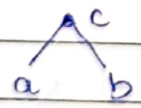
- Some useful information on finding GLB & LUB for two elements quickly:

1. $a \vee a = a$
2. $a \wedge a = a$
3. if $a R b$ then
   - $a \vee b = b$
   - $a \wedge b = a$.

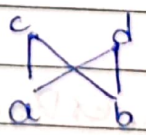


4. if $a \not R b$ and $b \not R a$, then
   - $a \vee b$ is the unique first joining point upwards of a & b.

Ex

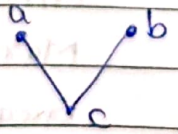


$a \vee b = c$

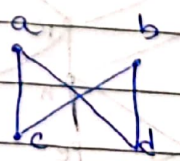


$a \vee b$ = Doesn't exist.

- $a \wedge b$ is the unique first joining point downwards of a & b.

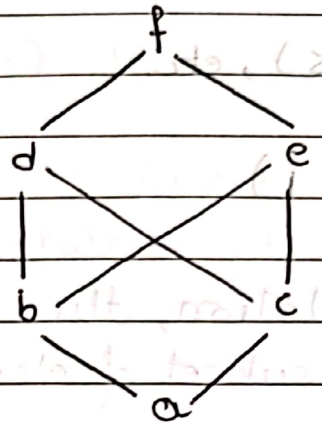


$a \wedge b = c$



$a \wedge b$ = Doesn't exist

Ex.

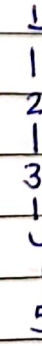


- $b \wedge c = a$
- $b \vee c$ = Doesn't exist {not unique}
- $b \wedge a = a$.
- $b \vee a = b$
- $d \wedge e$ = DNE
- $d \vee e = f$

*• GLB is also called meet.
• LUB is also called join.

* Hasse Diagram of Total Order Relation

Ex. $(\{1,2,3,4,5\}, >=)$



(a.k.a. Chain / Linear line / Total Order)

Ex. $(\mathbb{Z}, \leq)$, $(\mathbb{N}, \leq)$, etc.

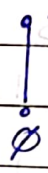
Ex. $(\{1, 2, 4, 8, 16\}, |)$

* In | {divides} relation, the LUB is LCM, & GLB is HCF, of subset of elements.

* (POA), $\subseteq$) is a TOR iff $|A| \leq 1$.

Ex. $A = \emptyset$

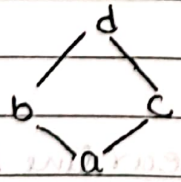
Ex. $A = \{a\}$



* Therefore, a POR is TO iff, its Hasse Diagram is chain.

* • Chain: Every element is comparable.
• Antichain: No two element are comparable.

Ex.



longest chain = abd, acd.
longest anti-chain = bc

Ex. $(\{1, 2, 3, 4, 5\}, |)$

largest chain = $(\{1, 2, 4\}, |)$ size = 3
largest antichain = $(\{2, 3, 5\}, |)$ size = 3.

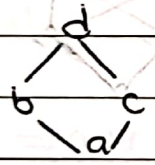
Ex. $(\{1,2,4,8,16\}, 1)$

Largest chain = $(\{1,2,4,8,16\}, 1)$
Largest Antichain = $(\{1\}, 1)$ or $(\{2\}, 1)$, etc.

* Lattice

A Lattice is a poset (P, R) in which every two elements, a & b have a LUB & a GLB.

Ex.



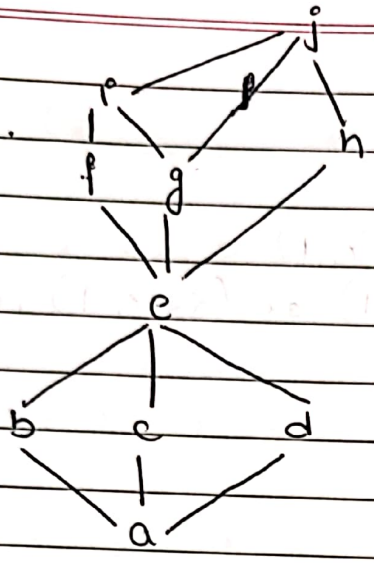
~~$a \vee b$~~ = $a \vee a = a$, $a \wedge a = a$ } $a \vee c = c$, $a \wedge c = a$ }
~~$a \vee c$~~ =
~~$a \vee d$~~ =
~~$b \vee c$~~ $a \vee b = b$, $a \wedge b = a$ } $a \vee d = d$, $a \wedge d = a$ }
~~$b \vee d$~~
~~$c \vee d$~~
⋮ ⋮

Checking like this takes a lot of time. Some points:

(1) $a \vee a$, $a \wedge a$ is unnecessary to check.
(2) $a \vee b$, $a \wedge b$, when a & b are comparable, then its unnecessory to check.

Therefore only check for uncomparable elements.

Ex.

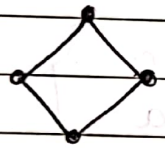


(b,c) has both LUB, GUB.
(b,d) ✓
(c,d) ✓
(f,g) ✓
(f,h) ✓
(g,h) ✓
(i,h) ✓

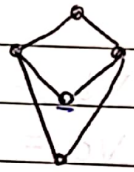
∴ Lattice.

Ex. Which is lattice?

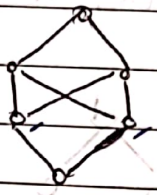
(A) ✓



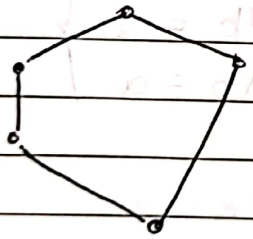
(B) ✗



(C) ✗



(D) ✓



Ex. (ℕ, /) is Lattice.

LUB = LCM GLB = HCF

Ex. (P(A), ⊆) is Lattice

LUB = ∪

GLB = ∩

* For every lattice:

1. • $a \vee a = a$
   • $a \wedge a = a$
   } Idempotent law.

2. • $a \vee b = b \vee a$
   • $a \wedge b = b \wedge a$.
   } Commutative law.

3. • $(a \vee b) \vee c = a \vee (b \vee c)$
   • $(a \wedge b) \wedge c = a \wedge (b \wedge c)$
   } Associative law.

4. • $a \vee (a \wedge b) = a$.
   } Absorption Law

Proof:

C1: a & b comparable. aRb

$\Rightarrow a \vee (a \wedge b)$

$\Rightarrow a \vee a$

$\Rightarrow a$.

C2: a & b comparable. bRa.

$\Rightarrow a \vee (a \wedge b)$

$\Rightarrow a \vee b$

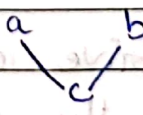
$\Rightarrow a$.

C3: a & b not comparable.

$\Rightarrow a \vee (a \wedge b)$

$\Rightarrow a \vee c$ {∵ lattice}

$\Rightarrow a$.

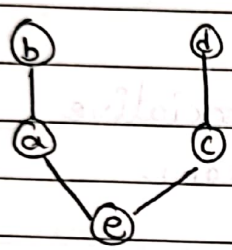


• $a \wedge (a \vee b) = a$
} Absorption Law.

* Finding Cardinality of POR from Hasse Diagram:

- For every element x, create all the possible (x,y) ordered pair possible from the Hasse diagram.

Ex.



No. of elements in base set = 5.

$A = \{a, b, c, d, e\}$

(A, R)

(e, α): $(e,e), (e,a), (e,b), (e,c), (e,d)$

(a, α): $(a,a), (a,b)$

(b, α): (b,b)

(c, α): $(c,c), (c,d)$

(d, α): (d,d)

$\therefore |R| = 5 + 2 + 1 + 2 + 1$

$= 11.$

- e is least element, minimal element.
- b & d are maximal element.

Ex. Give a Hasse diagram with 3 elements, what is the maximum possible cardinality of R?

So, $|R| = |(a, \alpha)| + |(b, \alpha)| + |(c, \alpha)|$

$\downarrow$

$3 + 2 + 1$

$= 6.$

* On 'n' elements the largest possible POR is a chain.

* The smallest possible POR is an antichain.

* Iff for set A, $|A| \geq 2$, then $A \times A$ is never POR.

Ex. If for a set A, the relation $R = A \times A$ is POR. What are the possible cardinalities of A?

0 & 1.

Say, $|A| = 1$
$A = \{a\}$
$R = \{(a,a)\}$
R is reflexive, symmetric, anti-symmetric, transitive.
∴ R is POR.

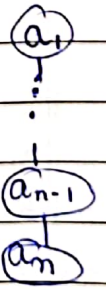
Say, $|A| = 0$.
$A = \{\}$
$R = \{\}$
R is Reflexive, Irreflexive, Symm., Antisymm., Asymm. & Transitive.
∴ R is POR.

Ex. An empty relation R on non-empty set A is:

✓ Symm. ✓ AntiSymm. ✓ Asymm. ✓ Reflexive. ✓ Irreflexive ✓ Transitive

Ex. Cardinality of a relation R on a set A, $|A| = n$, such that R is a chain.

$|R| = n + (n-1) + \dots + 2 + 1$
$= \frac{n(n+1)}{2}$



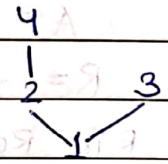
* Sublattice.

* Deletion of an element from Base set in any POSET, does it remain POSET?

Yes. Ex. $(\mathbb{N}, \geq) \rightarrow (\{1,2,4,8\}, \geq)$, etc.

* Deletion of an element from R, where R is POSET, does R remain POSET?

No. Ex. $(\{1,2,3,4\}, |)$

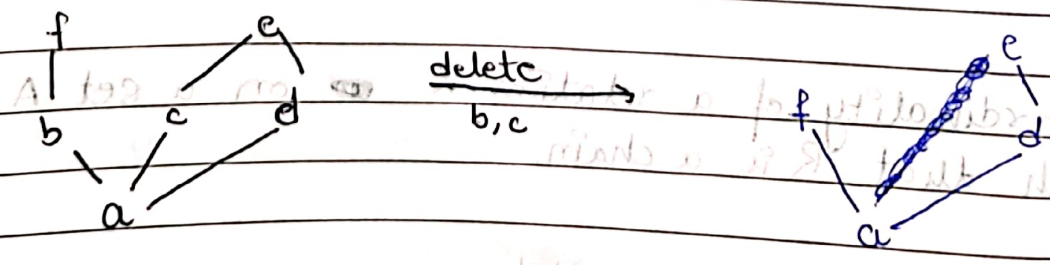


$R = \{(1,1), (1,2), (1,3), (1,4), (2,2), (3,3), (3,4), (4,4)\}$

Deleting (2,4). R is not POR.

∴ ~~Can't~~ Deleting element from POR doesn't always result in POR.

Ex.



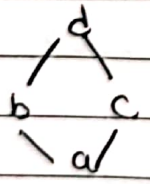
* Therefore, For all POSET (A, R), then, (B, R) is also POSET, if $B \subseteq A$.

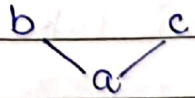
- If (A, R) is equivalent relation, then (B, R) is also equivalence relation, if $B \subseteq A$.

* Sublattice of a lattice L, is a subset of L, that is a lattice with the same meet and join operations as L.

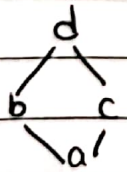
Therefore, for S to be a sublattice of L:

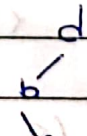
1. S should be subset of L.
2. S should be a lattice.
3. For every $a, b \in S$, GLB & LUB must be same in S & L.

Ex. 

Deleting 'd'. 

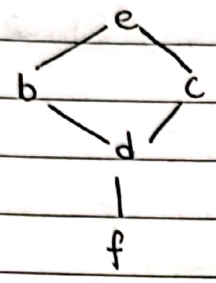
∴ Is not Lattice.
∴ Is not Sublattice

Ex. 

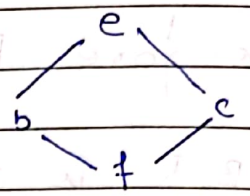
Deleting 'c'. 

Subset. ✓
Lattice. ✓
GLB, LUB same, ✓ in L & S.

Ex.



Deleting 'd'.



Subset. ✓

Lattice. ✓

	L	S
$b \vee c$	e	e
$b \wedge c$	d	f

~~GLB & LUB~~

∴ GLB $b \wedge c$ is not same in L & S.

∴ Not sublattice.

- Therefore, the intuition behind sublattice is:
  If you are taking subset $S = \{a, b, \ldots\}$,
  then take GUB & LUB for values.

Ex. $(P(A), \subseteq)$, $A = \{1, 2, 3\}$

Is Lattice.

$S = \{\phi, \{1,2\}, \{2,3\}, \{1,2,3\}\}$

Comment on $(\phi, \subseteq)$.

Note: Base set is by default non-empty, unless mentioned in question.

① $S \subseteq P(A)$.

② S is lattice.

③

	P(A)	S
$\{1,2\} \wedge \{2,3\}$	$\{2\}$	ϕ

∴ $(S, \subseteq)$ is lattice, but not a sublattice.

(In such ques, remember to consider infinite sets A)

Ex. R is POR on some set A. Which of the following statement is true?

(A) (A,R) has at least one minimal element & one maximal element.

(B) If (A,R) has a smallest & largest element, then every two element of A are comparable.

(C) If (A,R) has no maximal, then A is infinite set.

(D) If (A,R) has a single minimal element, then it is a smallest element.

(E) If every two elements are comparable, then there is a smallest & largest element.

A: False. $(\mathbb{N}, \leq)$, etc.

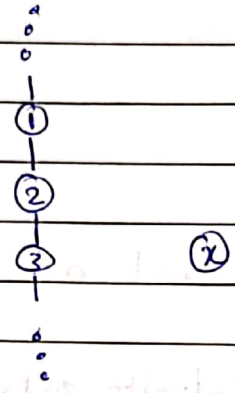
B: False. $(P(A), \subseteq)$

~~C: False. $(\phi, \{\phi\})$~~

C: True } we don't consider ϕ }

D: False

Ex:



Minimal: x

least: DNE.

So, infinite Poset is counterexample.

True for finite Poset.

E: False. Ex. $(\mathbb{N}, \leq)$

For finite poset, it is true.

* Types of Lattices

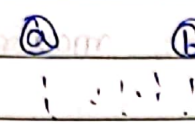
1. Bounded Lattice: A lattice L is bounded if it has both a greatest and least element denoted by 1 & 0 respectively.

Could be finite & infinite.

Ex. $([0,1], \leq)$ is infinite.

Ex. Can we have more than one maximal in finite lattice?

No. Suppose a & b both are maximal in lattice L.



But then $a \vee b$ doesn't exist.

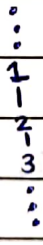
∴ By contradiction, every finite lattice has exactly one maximal element.
Similarly, finite lattice has exactly one minimal element.

∴ Every finite lattice has a greatest & least element.

∴ If Finite lattice then bounded lattice.

Ex. "If (A,R) has no maximal element, then R is infinite".

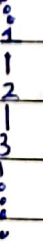
True. Ex.



If R would be finite, then there would be maximal & minimal element.

Ex. "If R is infinite, (A,R) has no maximal element".

False. Ex.



x

x is both maximal & minimal.

Ex. $(\mathbb{N}, \geq)$ etc.

1 is maximal.

Ex. (1) A Lattice can have more than one maximal element. F

(2) A Lattice can have more than one minimal element. F

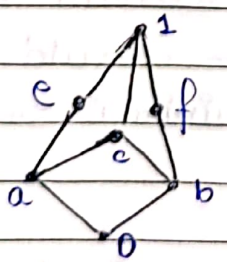
Ex. (1) Every lattice must have at least one maximal element. F. Ex. $(N, \leq)$

(2) Every lattice must have at least one minimal element. F. Ex. $(N, \geq)$

* Therefore every lattice has at most one maximal and at most one minimal element.

Every finite lattice has exactly one maximal & exactly one minimal element, which are greatest and lowest elements respectively.

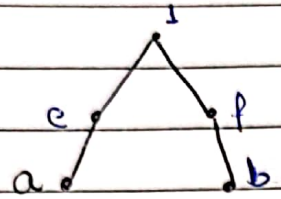
Ex.



Is this Lattice?

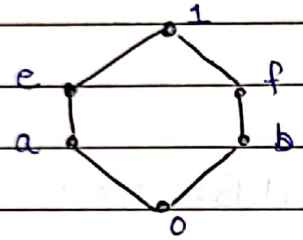
Checking all non-comparable pairs.

1. $a \vee b = c$ $a \wedge b = c$.
2. $a \vee f = 1$ $a \wedge f = 0$
3. $b \vee c = 1$ $b \wedge c = 0$
4. $e \vee f = 1$ $e \wedge f = 0$
5. $e \vee c = 1$ $e \wedge c = a$
6. $f \vee c = 1$ $f \wedge c = b$



Is this sublattice of L?

Nb. Not even a lattice. $a \wedge b$ DNE.



Is this sublattice of L?

(1) Checking non-comparable pairs:

1. $a \vee b = 1$ $a \wedge b = 0$
2. $a \vee f = 1$ $a \wedge f = 0$
3. $b \vee e = 1$ $b \wedge e = 0$
4. $e \vee f = 1$ $e \wedge f = 0$.

∴ Lattice.

(2) LUB of a, b in L: c, in S: 1.

∴ Not sublattice.

* Identity Element: For a binary operation, *, an identity element is such that for all x,

(1) $x * e = x$

(2) $e * x = x$.

Ex. $(\mathbb{N}, \leq)$

Id. Element for GLB: DNE!
Id. element for LUB: 1.

i.e. $\forall x \in \mathbb{N} \quad x \vee 1 = x$
$1 \vee x = 1$

- For a finite lattice:
  - Identity element for GLB: Maximum element
  - Idententy element for LUB: Least element.

* Bounded Lattice

- A lattice is Bounded if it has both greatest & least element.

OR

A Lattice is bounded if it has identity element for both GLB & LUB.

- Greatest Element: 1
  Least Element: 0.

- For a bounded lattice, L,
  (1) $1 \vee x = 1, \quad \forall x \in L$
  (2) $0 \wedge x = 0, \quad \forall x \in L$

} Dominator Law

* Complemented Lattice.

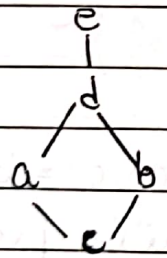
- Complement of an element: We say an element 'b' is complement of element 'a' iff

$$a \vee b = 1$$
$$a \wedge b = 0.$$

{ For complement to exist lattice must be bounded since greatest & least element must exist }

complement of a is denoted as a^{-1}.

Ex.

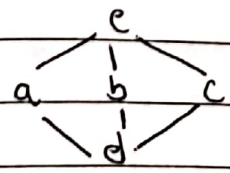


a^{-1} = DNE d^{-1} = DNE.
b^{-1} = DNE
$c^{-1} = e$
$e^{-1} = c$.

- Complement of least element is the greatest element.
- If $a^{-1} = b$, then $b^{-1} = a$.

- A lattice in which every element has at least one complement is called Complemented Lattice

Ex.



$a^{-1} = b, c$ $e^{-1} = d$
$b^{-1} = a, c$ $d^{-1} = e$.
$c^{-1} = a, b$

∴ Complemented lattice.

* Distributive Lattice

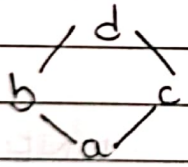
- Distributive Property

(1) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

(2) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

- Distributive Lattice: A lattice L is distributive if $\forall a, b, c \in L$, they satisfy distributive property.

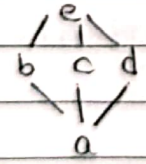
Ex.



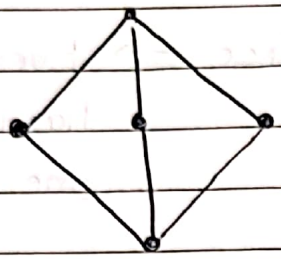
$a \vee (b \wedge c) = a \vee a = a$. $(a \vee b) \wedge (a \vee c) = b \wedge c = a$.

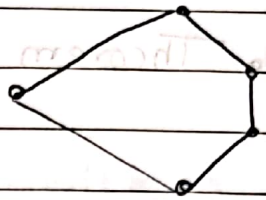
Similary all triplets satisfy distributive property.

Ex



$b \vee (c \wedge d) = b \vee 0 = b$ $(b \vee c) \wedge (b \vee d) = e \wedge e = e$





Kite Lattice / Diamond Lattice.

Pentagon Lattice.

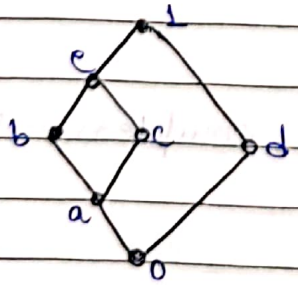
These are popular non-distributive lattice.

Theorem: Lattice L is distributive iff none of its sublattice is Kite Lattice and Pentagon Lattice

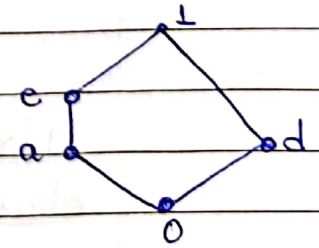
or

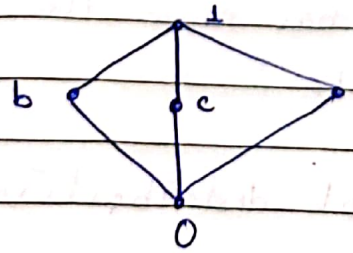
Iff for lattice L, some sublattice is Kite or Pentagon lattice, then L is ~~not~~ not ~~distributive~~ distributive lattice.

Ex. Is this distributive?



No. Sublattice with $\{0, a, e, d, 1\}$





This is not a sublattice.
$b \vee c = 1$ here.

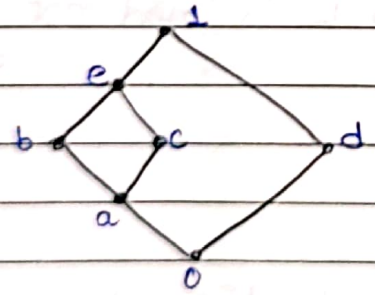
• Theorem : Distributive Lattice → Every element has at most one complement

Ex. Choose correct option.

(A) If every element of lattice has at most one complement it is distributive.

✓ (B) If some element of a lattice has more than one complement then it is not distributive.

Ex. Is the following Distributive Lattice?



Firstly we can check for complement of elements.

$a^{-1} = d$

$b^{-1} = d$

$c^{-1} = d$

$d^{-1} = a, b, c$

∵ d has more than 1 complement.

∴ Not distributive.

- Steps to check Distributive.

1. Check if $|L| \leq 4$ then distributive.
2. If $|L| = 5$ and not Kite nor pentagon then distributive.
3. If L is total order then L is distributive.
4. If any element has more than one complement, then not distributive.
5. ~~The~~ If Kite or Pentagon sublattice then not distributive.

* In Distributive Lattice every element has at most one complement.

In Complemented Lattice every element has at least one element.

∴ Distributive Complemented lattice → every element has exactly one complement.

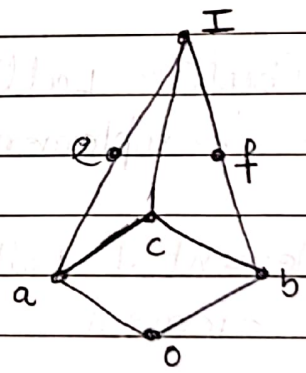
- A distributive lattice isn't necessarily bounded.
- Definition: A lattice is distributive iff it satisfies either one of the two distributive property.

* Boolean Lattice or Boolean Algebra.

- A lattice L is called Boolean Lattice iff it is:
  (1) Bounded
  (2) Complemented
  (3) Distributive

- A Boolean Lattice is Complemented Distributive lattice.

Ex. Analyze:



- Minimal: 0, c Minimum: 0
  Maximal: I Maximum: I

- Checking for lattice:
  $a \vee b = c$ $a \vee f = I$ $b \vee e = I$ $e \vee f = I$
  $a \wedge b = 0$ $a \wedge f = 0$ $b \wedge e = 0$ $e \wedge f = 0$

∴ Lattice.

- Since, I & 0 exist, so Bounded.

- Checking Complements:

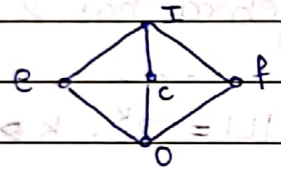
$0^{-1} = I$ $\quad c^{-1} = DNE$ $\quad I^{-1} = 0$

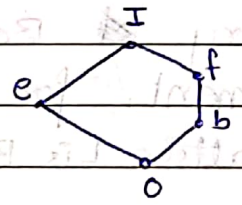
$a^{-1} = f$ $\quad e^{-1} = b$

$b^{-1} = e.$ $\quad f^{-1} = a.$

∴ Not Complemented Lattice.

- Checking for Distributive:





Not sublattice. $\quad$ Sublattice.

$(e \wedge c)$

∴ Pentagon sublattice.

∴ Not distributive.

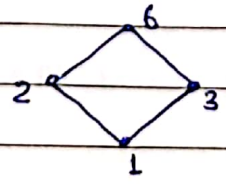
- Since lattice isn't Complemented & isn't Distributive

∴ Not Boolean.

- Since Boolean Lattice is Complemented & Distributive, every element has exactly one complement.

Ex. Check if Boolean Algebra: $(\{1, 2, 3, 6\}, 1)$

$|A| < 5$, ∴ Distributive.

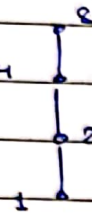


$1^{-1} = 6$ $\quad 3^{-1} = 2$

$2^{-1} = 3$ $\quad 6^{-1} = 1$

∴ Complemented.

Ex. Check if Boolean Algebra: $(\{1,2,4,8\}, |)$



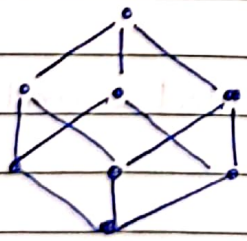
Distributive since chain.
Not complemented.
2^{-1} = DNE.

∴ Not Boolean Algebra.

- Theorem: Every Boolean Algebra has 2^K element, for $K = 0, 1, 2, 3, \ldots$.
  i.e. If lattice L is BA, then $|L| = 2^K$, $K = 0, 1, 2 \ldots$

- If Boolean Algebra always has 2^K elements, then its structure would be similar to $(P(A), \subseteq)$ where $|A| = K$.

Ex. Say, $|A| = 3$ $\quad |P(A)| = 2^3 = 8$.



Then Boolean Algebra with $2^3 = 8$ element will have this structure only.

- Boolean Lattice satisfies: Identity, Commutative, Distributive, Idempotent, Complement, DeMorgan, etc.

* Analysis of TOR

- A TOR is always a Lattice, since every two elements are comparable.

- A finite chain is :
  (1) Lattice
  (2) Bounded
  (3) Complemented iff ≤ 2
  (4) Distributive
  (5) Boolean Lattice iff ≤ 2.

- An infinite chain is :
  (1) Lattice
  (2) May/May not be Bounded. Ex. $([0,1], 1)$, $(\mathbb{N}, 1)$
  (3) Never Complemented
  (4) Distributive
  (5) Never Boolean Algebra.

* Analysis of "Subset" Relation

Say, for a set S, there exist a set A such that

$$A \subseteq P(S).$$

- $(A, \subseteq)$ is :
  (1) Reflexive
  (2) Anti-symmetric
  (3) Transitive
  (4) Maybe Symmetric. Ex. $(\{\{a\}\}, \subseteq)$. $R = \{(\{a\}, \{a\})\}$

- $(P(S), \subseteq)$ is:
  (1) Reflexive
  (2) Antisymmetric
  (3) Transitive
  (4) Symmetric, iff $S = \phi$, i.e. $P(S) = \{\phi\}$

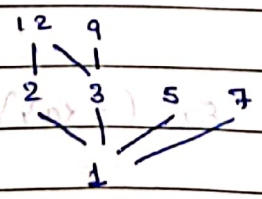
- $(P(S), \subseteq)$ is:
  (1) Lattice.
  (2) Complemented
  (3) Distributive
  (4) Boolean Algebra.

- In the Lattice $(P(S), \vee, \wedge)$
  - LUB: Union
  - GLB: Intersection
  - Greatest: S
  - Least: ϕ

* Analysis of Divisibility Relation

- Divisibility relation is always a POSET.

Ex. $(\{1, 2, 3, 5, 7, 9, 12\}, |)$



Greatest: DNE Maximal: 5, 7, 9, 12
Least: 1 Minimal: 1

- Not a lattice; 12 ∨ 9 DNE.

Ex. $(\mathbb{N}, |)$

- Is a POSET.
- Minimal: 1 Minimum: 1
  Maximal: DNE Maximum: DNE
- GLB = Greatest Common Divisor.
  LUB = Least Common Multiple.
- Lattice since every pair a, b has GCD & LCM.
- Not Bounded.
- Not Complemented.

Ex. $(\mathbb{Z}, |)$

- Is not Poset, since not Anti-symmetric.
  Ex. $2|-2$ & $-2|2$.

Ex. $(W, |)$, $W = \{0, 1, 2, \ldots\}$

- Is Poset.
- Minimum: 1
  Maximum: 0.

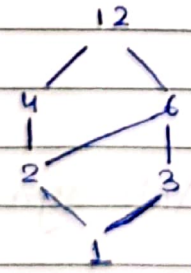
* For, $n \in N$,
D_n = Set of all divisors of n.

Ex.
$D_{20} = \{1, 2, 4, 5, 10, 20\}$

$(D_n, |)$ is a Lattice.

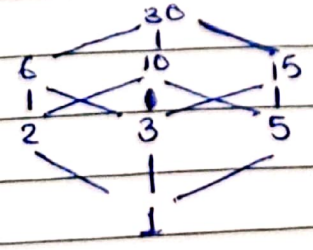
- $(D_n, |)$ is :
  (1) Lattice.
  (2) Bounded. Greatest: n, Least: 1
  (3) May or may not be complemented.
  (4) Distributive, since GCD & LCM distribute over each other.

Ex. $(D_{12}, |)$



(1) Lattice.
(2) Greatest: 12 Least: 1.
(3) $1^{-1} = 12$
$2^{-1} =$ DNE
∴ Not complemented.
(4) Distributive.

Ex. $(D_{30}, |)$ $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$



(1) Lattice
(2) Greatest: 30 Least: 1
(3) 1^{-1}: 30 3^{-1}: 10 6^{-1}: 5 15^{-1}: 2
2^{-1}: 15 5^{-1}: 6 10: 3 30^{-1}: 1

∴ Complemented.

(4) Distributive.

(5) Boolean Lattice.

- $(D_n, |)$ would form a Boolean Lattice for a 'n' which is squarefree

'n' is square free if there exists no prime no. p such that $p^2 | n$.

i.e.,

$n = p_1^1 \times p_2^1 \times p_3^1 \times \ldots$

FUNCTIONS

* A function is a special type of relation.

* A func., $f: A \to B$ is such that, every element of set A is related to exactly one element of set B.

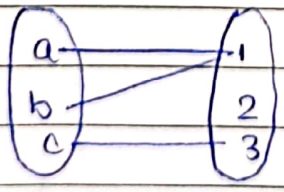
* In a function, $f: A \to B$,

(1) 'A' is known as the domain.
(2) 'B' is known as the co-domain.
(3) $f(a) = b$ is read as "image of a under f is b"
(4) $f(a) = b$ is also read as "pre-image of b under f is a".

* For an element in the domain, there exists exactly one image in co-domain.

• For an element in the co-domain, there can exist zero or more preimage.

Ex.



image(a) = 1
img(b) = 1
img(c) = 3.

preimg(1) = {a, b}
preimg(2) = { }
preimg(3) = {c}.

* Range of a func. $f: A \to B$, is a subset X of B, such that,

$\forall x \in A \; f(x) \in X$

i.e. Range of a func. is set of all values of codomain reachable by domain.

Ex. Which of the following is not a func.?

(A) $f: N \to N$ $\quad f(x) = x^2$
(B) $f: N \to N$ $\quad f(x) = \sqrt{x}$ ✓
(C) $f: Z \to Z$ $\quad f(x) = x^2$
(D) $f: Z \to Z$ $\quad f(x) = \sqrt{x}$ ✓
~~(E) $f: \{1, 4, 9\} \to \{1, 2, 3\}$~~

B. since, $\sqrt{5} \notin N$.
D. since, $\sqrt{4} = \pm 2$. Not unique mapping to codomain

* For 2 sets A & B, $|A| = m$, $|B| = n$, the no. of possible functions $f: A \to B$ possible is

n^m

{∵ Each element of A has n choices}

* • Real-Valued func: Codomain must be real value.
• Integer-Valued func: Codomain must be integer.
• Boolean func: Codomain must be boolean.

* For two real-valued / integer-valued func. with same domain, $f(x)$ & $g(x)$:
• $(f+g)(x) = f(x) + g(x)$
• $(f \times g)(x) = f(x) \times g(x)$

Ex. $f: \{1,2,3\} \to R$ $\quad f(x) = x^2$

$g: \{1,2,3\} \to R$ $\quad g(x) = x+1$

$\therefore (f+g)(x) = f(x) + g(x)$

$= x^2 + x + 1$

$(f+g)(1) = 1^2 + 1 + 1 = 3$

$(f+g)(2) = 2^2 + 2 + 1 = 7$

$(f+g)(3) = 3^2 + 3 + 1 = 13.$

* One - One function (Injective)

A func. in which every element in domain has a unique image, in the codomain.

i.e. No two elements in the domain have the same image.

No. of one-one func. from set A to B, $|A|=m$, $|B|=n$,

$n \times (n-1) \times (n-2) \times \dots (n-m+1)$

$\Rightarrow {}^nP_m \quad (n \geq m)$

* Onto function (Surjective)

A func. in which every element in the codomain has at least one preimage.

i.e. Range = Codomain.

No. of surjective func. from A to B, $|A| = m$, $|B| = n$

$m \geq n$

$$n^m - {}^nC_1(n-1)^m - {}^nC_2(n-2)^m - \dots - {}^nC_{n-1}(1)^m$$

↑ all func.

↑ funcs. where only one element in codomain has pre-img

↑ funcs. where only $(n-1)$ elements in codomain have preimg.

* Bijective function

A func. which is both one-one & onto.

i.e.

Every element of domain has a unique img & every element of codomain has exactly one pre-img.

No. of bijective func. from A to B, $|A| = m$, $|B| = n$,

$m = n$

$n!$

* For a func. $f: A \to B$, to prove:

(1) Injection: Assume $f(a) = f(b)$, then show that $a = b$.

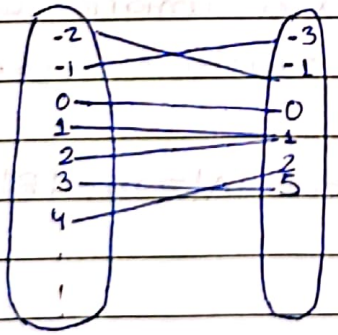
(2) Not Injective: Find two elements x, y in domain such that $x \neq y$ but $f(x) = f(y)$.

(3) Surjective: Consider an arbitrary element $y \in B$, and show that there exist an $x \in A$, such that $f(x) = y$.

(4) Not Surjective: Find a $y \in B$, such that $\forall x \in A$, $f(x) \neq y$.

Ex. $f: Z \to Z$ $\quad f(x) = \begin{cases} 2x-1, & x \text{ odd} \\ x/2, & x \text{ even} \end{cases}$

* One-One:



$f(1) = 1 \quad f(2) = 1$

$\therefore$ Not one-one func.

* Onto:

$f(x) = 2x - 1 \quad (x \text{ odd})$

$x = \frac{f(x)+1}{2} \quad (f(x)+1 \text{ is even})$

$\therefore x \in Z$

$f(x) = \frac{x}{2} \Rightarrow x = 2f(x)$

$\therefore x \in Z$

$\therefore$ Surjective.

* Combining Relations:

- Every relation $R: A \to B$ is a set & a subset of $A \times B$.
- Since relations are also sets, set operations can be applied on them.

Ex. A = Set of all students B = Set of all courses.

$R_1: A \to B$ $R_1 = \{(a,b) \mid$ student a has taken course b$\}$

$R_2: A \to B$ $R_2 = \{(a,b) \mid$ student a needs to take course b$\}$

$R_1 \cup R_2 = \{(a,b) \mid$ Student a has taken course b, or needs to or both$\}$

$R_1 - R_2 = \{(a,b) \mid$ student a has taken course b, but doesn't need to$\}$.

$R_1 \cap R_2 = \{(a,b) \mid$ a has taken the required course b$\}$.

$R_1 \times R_2 = \{((a,b),(c,d)) \mid$ a has taken b, c needs d$\}$

- There are two operations specially for relations:
  (1) Composition
  (2) Inverse.

- Composition: For two relations, $R: A \to B$ and $S: B \to C$, their composition is the relation,

$$S \circ R = \{(a,c) \mid \exists b, (a,b) \in R \wedge (b,c) \in S\}$$

i.e for some 'b', $(a,b) \in R$ & $(b,c) \in S$, then $(a,c) \in S \circ R$. $\{b \in B\}$

Composition is denoted by '$\circ$'.

Composition is associative.

$$T \circ (S \circ R) = (T \circ S) \circ R$$

* Function Composition

- For functions $f: A \to B$ & $g: B \to C$

$g \circ f : A \to C$.

& $g \circ f = g(f(x))$

- Composition of f & $g = g(f(x))$
  Composition of g & $f = f(g(x))$

Ex. $f(x) = 2x$ $\quad g(x) = x + 1$

$f: A \to A$ $\quad g: A \to A$.

$g \circ f = g(f(x)) = g(2x) = 2x + 1$

$f \circ g = f(g(x)) = f(x+1) = 2(x+1)$.

{Here both fog & $g \circ f$ are defined}.

Ex. $f: N \to Z \quad f(x) = x^2$

$g: N \to N \quad g(x) = x + 1$

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

$g \circ f$ = Not defined since codomain of $gf \neq$ domain of fg

Ex. $f: A \to A \quad g: A \to A$. (1) Both f & g are one-one. Then fog & $g \circ f$ are ...?

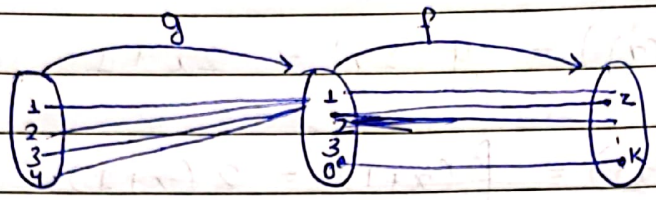
Both are one-one.

(2) Both are onto. Then fog & $g \circ f$ are?

For every $x \in$ Range(fg) has a preimg. Similarly, all $y \in$ Range(f) has preimg. Therefore fog & $g \circ f$ are onto.

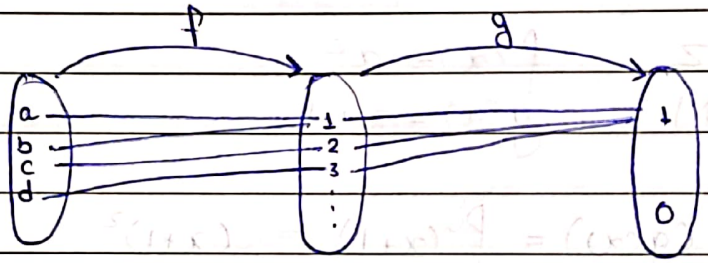
(3) f is onto. Then fog & $g \circ f$ are ...?

fog:



∴ fog isn't onto.

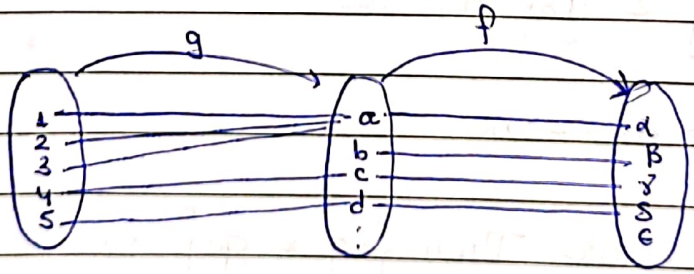
gof:



∴ gof isn't onto.

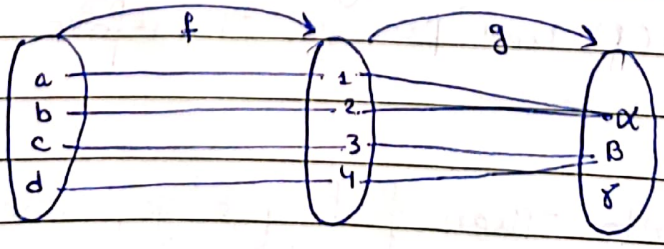
(4) f is one-one. fog & gof are...?

fog:



∴ Not one-one.

gof:



∴ Not one-one.

Ex. If fog is one-one then:

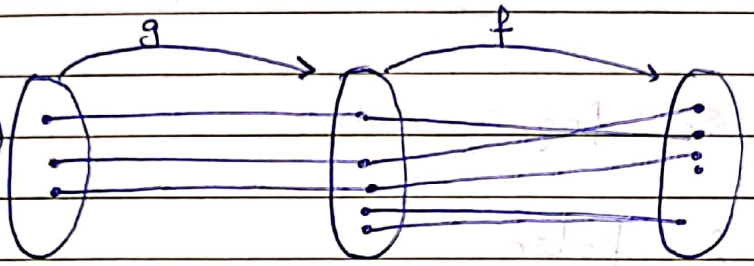
(1) f must be one-one

(2) g must be one-one ✓

(3) NOTA.

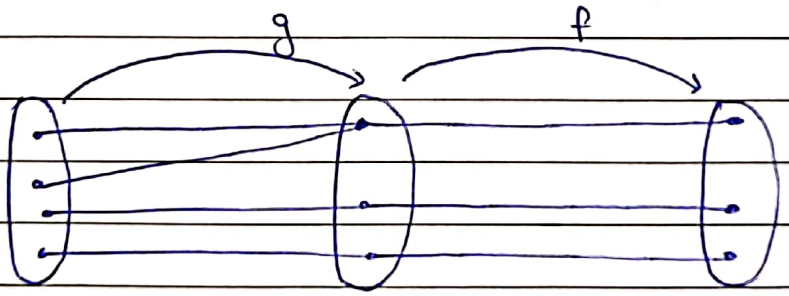
Opt 1:

¬(f o-o) → ¬(fog one-one)



false.

Opt 2: ¬(g one-one) → ¬(fog one-one)



So, true.

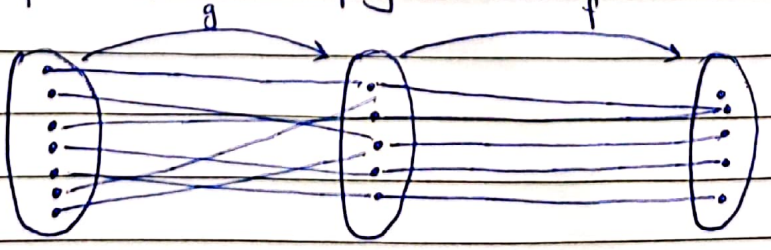
Ex. If fog is surjective then.

(1) f must be surjective ✓

(2) g must be surjective

(3) NOTA.

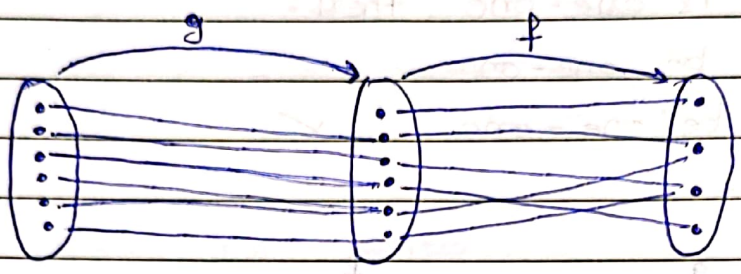
Opt1: ¬(f onto) → ¬(fog onto)



So, fog is not onto.

∴ True.

opt 2: $\neg(g \text{ onto}) \rightarrow \neg(fog \text{ onto})$

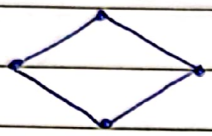


So, fog is onto.

∴ false.

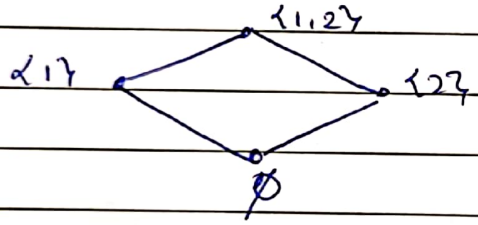
GROUP THEORY

* Abstract Algebra

Eg. 

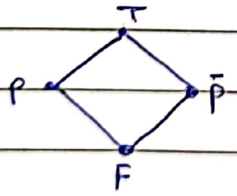
we know this is a Boolean algebra, and satisfies properties like: Commutative, Distributive, Demorgan, etc.

Now. $(P(\{1,2\}), \subseteq)$ is



Now, since the structure is same as the abstract structure, we know this satisfies all the above properties.

Similarly ($\{T, F, P, \bar{P}\}$, $\rightarrow$ is tautology) is also a B.A. & hence satisfies above properties.



So, rather than studying every such structure we only study the abstract structure & its operations.

- Abstract Algebra is the study of abstract structures.

* Algebraic Structure: A base set along with operations is known as an Algebraic Structure.

(Base Set, +, −, *, /, ...)

In syllabus we only have A.S. with single binary operations.

Ex. $(\mathbb{Z}, *)$ or $(\mathbb{N}, +)$, etc.

* Binary Operation & Closure Property

- Closure Property: For a A.S. $(S, *)$, if $\forall a, b \in S \; a * b \in S$ then $(S, *)$ satisfies the closure property.

Ex. $(\{1, 0\}, \wedge)$

$1 \wedge 1 = 1$

$1 \wedge 0 = 0$

$0 \wedge 0 = 0$

$0 \wedge 1 = 0$

$\therefore$ This satisfies closure property.

Ex. $(\{1, 2, 3\}, +)$

Not closed under +, since, $2 + 2 = 4$.

Ex. $(\{1, 2\}, *)$

*	1	2
1	1	2
2	2	4

$4 \notin \{1, 2\}$ $\therefore$ Not closed.

- Binary Operation: A operation # is called binary operation on a set S, iff (S,#) satisfies closure property.

$$\#: S \times S \rightarrow S$$

* Associative Property

An A.S. (S, #) is associative iff,

$$\forall a,b,c \in S \quad a \# (b \# c) = (a \# b) \# c.$$

Ex. Check if (N, #) $a \# b = a^2 + b$ satisfies assoc. property.

$a \# b = a^2 + b$, $\because a^2 \in N$, if $a \in N$ & N is closed under +
$\therefore$ ~~a#b ∈ S~~ (N, #) satisfies closure property.

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

$(a \# b) \# c = (a^2 + b)^2 + c$
$\Rightarrow a^4 + b^2 + 2a^2b + c.$

$\therefore$ Not associative.

* Identity Property

An A.S. (S, #) satisfies Identity property iff

$$\exists a \in S, \forall x \in S, \quad a \# x = x \# a = x$$

and the element 'a' is called Identity Element of $(S, \#)$.

Ex. $(\mathbb{N}, *)$

Id. element = 1,
$\because 1 * x = x * 1 = x$.

Ex. $(\mathbb{N}, +)$

No Id. element.

Ex. $(W, +)$

Id. element = 0
$\because 0 + x = x + 0 = x$.

Ex. $(\mathbb{Z}, -)$

No Id. element.
$\because 0 - x \neq x - 0$.

Ex. $(\mathbb{N}, \#)$ $a \# b = \max(a, b)$

- It is closed.
- It is associative.
- Id. element = 1.

Ex. $(\mathbb{Z}, \#)$ $a \# b = \max(a, b)$

- No Identity element.

Ex. $(S, *)$, Which one of the following is associative for $S = \{T, F\}$

(1) $\wedge$ ✓
(2) $\vee$ ✓
(3) $\rightarrow$ ✗ $F \rightarrow (F \rightarrow F) \neq (F \rightarrow F) \rightarrow F$
(4) $\oplus$ ✓
(5) $\leftrightarrow$ ✓
(6) $\uparrow$ ✗
(7) $\downarrow$ ✗

Ex. $(S, *)$. Which of the following satisfies Identity property? $S = \{T, F\}$

(1) $\wedge$	✓	$e = T$	(5) $\oplus$	✓	$e = T$
(2) $\vee$	✓	$e = F$	(6) $\uparrow$	x	
(3) $\rightarrow$	x		(7) $\downarrow$	x	
(4) $\leftrightarrow$	✓	$e = T$			

- We can never have more than one identity element.

Proof: Assume two identity elements : e, f of $(S, *)$

So,

$\forall x \in S \quad e * x = x * e = x$

$e * f = f$

$\forall x \in S \quad f * x = x * f = x.$

$f * e = e.$

$\therefore$ e must be equal to f.

* Inverse Property

For an A.S. $(S, *)$, which has an identity element 'e', it satisfies Inverse Property, iff

$$\forall a \in S, \exists b \in S, \quad a * b = b * a = e.$$

then, b is called as inverse of a.

$a^{-1} = b$. &

$b^{-1} = a$.

Ex. $(\mathbb{N}, *)$

Identity elem. $= 1$

Checking inverse for 2.

$2 * b = b * 2 = 1$

$b = \frac{1}{2} \notin \mathbb{N}$

∴ Doesn't satisfy Inverse property.

Ex. $(\mathbb{Z}, +)$

$e = 0$.

$a^{-1} = -a$.

Ex. $(\mathbb{R}, \times)$

$e = 1$

$0^{-1} = \text{DNE}$

∴ Doesn't satisfy Inverse Property.

Ex. $(\mathbb{N}, +)$

No e. ∴ Doesn't satisfy Inv. property.

- The inverse of identity element is itself.

$$e^{-1} = e.$$

- In an A.S. $(S, *)$ an element 'a' can have more than one inverse.

* Commutative Property

An A.S. $(S, *)$ satisfies commutative property iff

$$\forall a, b \in S \quad a * b = b * a.$$

* Classification of Algebraic Structure

Name of Structure	Satisfied Properties
(1) Algebraic Structure / Magma / Groupoid	Closure Property
(2) Semi-group	Magma + Associative Property
(3) Monoid	Semi-group + Identity Property
(4) Group	Monoid + Inverse Property
(5) Abellian Group	Group + Commutative Property.

Ex. Classify $(\mathbb{Z}, *)$ $a*b = a+b-3$

Closure: $\because a, b \in \mathbb{Z}$, $a*b \in \mathbb{Z}$.

Assoc:

$(a*b)*c$ | $a*(b*c)$

$\Rightarrow (a+b-3)*c$ | $\Rightarrow a*(b+c-3)$

$\Rightarrow a+b-3+c-3$ | $\Rightarrow a+b+c-3-3$.

$\therefore$ Assoc.

Identity: $a*e = e*a = a$.

$\Rightarrow a+e-3 = e+a-3 = a$.

$\Rightarrow e = 3. \in \mathbb{Z}$

$\therefore e = 3$.

Inv:

$a^{-1} = b \Rightarrow a * b = b * a = e.$

$\Rightarrow a + b - 3 = 3$

$\Rightarrow b = 6 - a.$

$6 - a \in \mathbb{Z}$

∴ Inverse exists.

Comm.:

$a * b$ $\qquad$ $b * a.$

$\Rightarrow a + b - 3$ $\qquad$ $\Rightarrow b + a - 3.$

∴ Commutative.

∴ $(\mathbb{Z}, *)$ is Abelian Group.

Ex. $(Q, *)$, $a * b = \frac{ab}{4}$ $\qquad$ ~~Commutative Group~~

Closure: $a, b \in Q \rightarrow a \times b \in Q \rightarrow ab/4 \in Q.$

Assoc.: $(a * b) * c$ $\qquad$ $a * (b * c)$

$\Rightarrow \frac{\frac{ab}{4} \times c}{4} \Rightarrow \frac{abc}{16}$ $\qquad$ $\Rightarrow \frac{a \times \frac{bc}{4}}{4} = \frac{abc}{16}$

Identity: $a * e = a$ $\qquad$ Inv.: $a * a^{-1} = 4$

$\Rightarrow \frac{ae}{4} = a$ $\qquad$ $a \times a^{-1} = 16$

$a^{-1} = \frac{16}{a}.$

$\Rightarrow e = 4.$

$\forall\, a \in Q \rightarrow \frac{16}{a} \in Q.$

but if $a = 0$ then $a^{-1} = \frac{1}{0} \notin \mathbb{Q}$.

∴ Commutative Monoid.

* Order of a structure : Cardinality of base set
Finite structure : Base set is finite.

* Given A.S. $(S, *)$, $|S| = n$, the total no. of binary operations $*$ possible is:

$$n^{n \times n}$$

$(\because * : S \times S \to S)$

No. of possible commutative operations :
every pair (a,b) & (b,a) maps to same value.

$$\therefore n^{\frac{n^2-n}{2}} \times n^{n}$$

$\frac{n^2-n}{2}$ ↑ : no. of (a,b) (b,a) pairs

n ↑ : no. of (a,a) (b,b) ⋮

* • In any structure, there is only one identity element.
• In a monoid, we don't have left & right cancellation property.

Eg. If $(S, *)$ is a group, but not Abelian, then:

(A) $\forall a, b \in S \quad a*b \neq b*a$.

(B) $\exists a, b \in S \quad a*b \neq b*a$. ✓

A is false, since for identity element,

$$e*e = e*e.$$

&

$$a*e = e*a = a.$$

and for any element a,

$$a * a^{-1} = a^{-1} * a = e.$$

∴ In a group ($\forall a, b \in S \quad a*b \neq b*a$) is never true.

* Roots of Unity

- for $x = 1 \Rightarrow S = \{1\}$ $(S, \times)$ is a group. $e = 1$
- for $x^2 = 1 \Rightarrow S = \{-1, 1\}$ $(S, \times)$ is a group. $e = 1$.
- for $x^3 = 1 \Rightarrow S = \left\{1, \frac{-1+\sqrt{3}i}{2}, \frac{-1-\sqrt{3}i}{2}\right\}$

ω $\quad$ ω^2

$\Rightarrow S = \{1, \omega, \omega^2\}$ are called cube roots of unity.

& $1 + \omega + \omega^2 = 0$

& $(S, \times)$ is a group.

(1) Closure:

$1 \times \omega = \omega$ $\quad$ $1 \times 1 = 1$

$1 \times \omega^2 = \omega^2$ $\quad$ $\omega \times \omega = \omega^2$

$\omega \times \omega^2 = \omega^3 = 1$ $\quad$ $\omega^2 \times \omega^2 = \omega^4 = \omega \times \omega^3 = \omega$

(2) Assoc:

$(1 \times \omega) \times \omega^2$ $\quad$ $1 \times (\omega \times \omega^2)$

$\Rightarrow \omega \times \omega^2$ $\quad$ $\Rightarrow 1 \times \omega^3$

$\Rightarrow \omega^3 = 1$ $\quad$ $\Rightarrow 1 \times 1 = 1$

(3) Identity: 1

(4) Inverse:

$1^{-1} = 1$

$\omega^{-1} = \omega^2$

$(\omega^2)^{-1} = \omega$

- for $x^4 = 1 \Rightarrow S = \{-1, 1, -i, i\}$ & $(S, \times)$ is a group.

Closure:

$-1 \times 1 = -1$ $\quad$ $1 \times -i = -i$ $\quad$ $-1 \times -1 = 1$ $\quad$ $i \times i = -1$.

$-1 \times -i = i$ $\quad$ $1 \times i = i$ $\quad$ $1 \times 1 = 1$

$-1 \times i = -i$ $\quad$ $-i \times i = 1$ $\quad$ $-i \times -i = -1$

Assoc: $(1 \times i) \times -i$ $\Rightarrow -1$

$-1 \times (i \times -i)$ $\Rightarrow -1 \times -(-1)$ $\Rightarrow -1$

Identity: $e = 1$.

Inverse:

$1^{-1} = 1$ $\quad i^{-1} = -i$

$-1^{-1} = -1$ $\quad -i^{-1} = i$

4^{th} roots of unity.

So, for $n \geq 1$, $x^n = 1$,

$$x = \{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$$

forms an abelian group under multiplication & is called n^{th} roots of unity.

* Addition Mod n

Z_n : Set of all integers $\{0, 1, 2, \ldots, n-1\}$

$*$: $a * b = (a + b) \bmod n$ $\quad (* \text{ is } \oplus_n)$

Then, $(Z_n, *)$ is an Abelian group for $n \in \mathbb{Z}^+$

Ex. $(Z_5, \oplus_5)$ $\quad Z_5 = \{0,1,2,3,4\}$

① Closed. ✓

② Ass.

$(a \oplus_5 b) \oplus_5 c$

$\Rightarrow (2 \oplus_5 3) \oplus_5 4$

$\Rightarrow 0 \oplus_5 4$

$\Rightarrow 4$

$a \oplus_5 (b \oplus_5 c)$

$\Rightarrow 2 \oplus_5 (3 \oplus_5 4)$

$\Rightarrow 2 \oplus_5 2$

$\Rightarrow 4.$

③ Identity : $e = 0$

④ Inverse :

$0^{-1} = 0$

$1^{-1} = 4$

$2^{-1} = 3$

$3^{-1} = 2$

$4^{-1} = 1.$

Ex. When will $(Z_n, \otimes_n)$ a group?

Let's take, $Z_4 = \{0,1,2,3\}$.

Closed ✓

Ass. ✓

Identity $e = 1$

Inverse:

$0^{-1} = DNE.$

$\therefore (Z_n, \otimes_n)$ is never a group. $\because$ $0^{-1} = DNE.$

Ex. Let $U_n = \{1, 2, \ldots n-1\}$, then is $(U_n, \otimes_n)$ a group?

Lets take $(U_5, \otimes_5)$.

① Closed ✓
② Assoc ✓
③ $e = 1$
④ $1^{-1} = 1$
$2^{-1} = 3$
$3^{-1} = 2$.
$4^{-1} = 4$.
⑤ Commutative ✓

$\therefore$ $(U_5, \otimes_5)$ is a commutative group.

Lets take $(U_6, \otimes_6)$

① Closed ✗ $(2 \times 3) = 6 \% 6 = 0 \notin U_6$.
② Assoc. ✓
③ $e = 1$
④ $1^{-1} = 1$
$2^{-1} = DNE$.

$\therefore$ Not Group.

Similarly $(U_9, \otimes_9)$ isn't group since, $(3 \times 3) \% 9 = 0 \notin U_9$.

- For a value 'a', a^{-1} doesn't exist under $\otimes_n$, if a & n aren't relatively prime.

- For $(S, \otimes_n)$ to be an Abelian group, S should contain co-primes of n.

  Ex. $\{1, 3, 5, 7\}, 8)$

- Therefore $(U_p, \otimes_p)$ would be Abelian group iff p is prime.

Ex. Prove that in a group every element has a unique inverse.

Suppose a^{-1} is both b & c.

$a * b = e$ $\qquad$ $a * c = e$.

$\Rightarrow \quad a * b = a * c$

$\Rightarrow \quad a^{-1} * (a * b) = a^{-1} * (a * c)$

$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c$

$\Rightarrow \quad e * b = e * c$

$\Rightarrow \quad b = c$.

Ex. Prove that group has left cancellation property.

LCP: if $a * b = a * c$ then $b = c$.

Assuming: $a * b = a * c$.

then,

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$
$$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c.$$
$$\Rightarrow e * b = e * c.$$
$$\Rightarrow b = c.$$

Ex. For a group, prove that $(a*b)^{-1} = b^{-1} * a^{-1}$

$$\Rightarrow (a*b) * (a*b)^{-1} = e.$$
$$\Rightarrow a^{-1} * [(a*b) * (a*b)^{-1}] = a^{-1} * e.$$
$$\Rightarrow [(a^{-1} * a) * b] * (a*b)^{-1} = a^{-1}$$
$$\Rightarrow b^{-1} * [b * (a*b)^{-1}] = b^{-1} * a^{-1}$$
$$\Rightarrow (b^{-1} * b) * (a*b)^{-1} = b^{-1} * a^{-1}$$
$$\Rightarrow e * (a*b)^{-1} = b^{-1} * a^{-1}$$
$$\Rightarrow (a*b)^{-1} = b^{-1} * a^{-1}$$

Ex. $(\{1, 5, 7, 11\}, \otimes_{12})$. Create Cayley Table.

$\otimes_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Ex. If $(G, *)$ is a group & $a, b \in G$ commute then a^2 & b^2 also commute?

$$a * b = b * a.$$
$$\Rightarrow a * a * b = a * (b * a).$$
$$\Rightarrow a^2 * b * b = [a * (b * a)] * b$$
$$\Rightarrow a^2 * b^2 = ab\,ab.$$
$$\Rightarrow baab.$$
$$\Rightarrow baba$$
$$\Rightarrow bbaa.$$
$$\Rightarrow b^2 * a^2$$

$\therefore$ True.

Ex. For a group $(G, \circ)$, prove that $ax = b$ has unique sol. for x.

$$\Rightarrow ax = b$$
$$\Rightarrow a^{-1}ax = a^{-1}b$$
$$\Rightarrow x = a^{-1}b$$

Assume there are two sol. y, z, then

$$\Rightarrow ay = b \qquad \Rightarrow az = b$$
$$\Rightarrow ay = az$$
$$\Rightarrow a^{-1}ay = a^{-1}az$$
$$\Rightarrow \boxed{y = z.}$$

• Ex. In a group $(G, \cdot)$,

① if $b * a = e$, then $a * b = e$?
② $a * e = a \quad \forall a \in G$.

① $b * a = e \Rightarrow a^{-1} = b$.
$\Rightarrow a * a^{-1} = e$.
$\Rightarrow a * b = e$.

② True, by definition of identity element.

Ex. For a group, prove: $(a^{-1}ba)^3 = a^{-1}b^3a$.

$(a^{-1}ba)^3 = (a^{-1}ba) * (a^{-1}ba)(a^{-1}ba)$
$\Rightarrow a^{-1}bbba$
$\Rightarrow a^{-1}b^3a$.

* Caylay Table & Properties of Group.
{ Group: $(G, *)$

• Each element $g \in G$, appears exactly once in each row & column of the Caylay table.

So, every row or column is simply a permutation of the group G.

Ex.

•	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Check properties of Caylay Table.

① Closure ✓
② Assoc. :
③ Identity ✓
④ Inverse ✓
⑤ Commutative

: (a.b).c a.(b.c)
⇒ c.c ⇒ a.a
⇒ e ⇒ e.

• a(cb) (ac)b
⇒ aa ⇒ bb
⇒ e ⇒ e.

• b(ac) (b(a)e)
⇒ c ⇒ e.
• b(ca) (bc)a
⇒ e ⇒ e.
• c(ab) = (ca)b
⇒ e ⇒ e
• c(ba) (cb)a
⇒ e ⇒ e.

• (aa)b a(ab)
• eb ac
⇒ b ⇒ b.

* • Nb. of non-isomorphic Groups of order 1 is 1.

•	x
x	x

$(\{x\}, \cdot)$

Ex. $(\{T\}, \wedge)$, $(\{\perp\}, \times)$, etc. all have same Caylay table.
So only one unique Caylay table structure

- Order 2:

·	e	a
e	e	a
a	a	e.

Again only 1 CT structure.
identity element : e.

- Order 3:

	e	a	b
e	e	a	b
a	a	$X_{2\times2}$	
b	b		

$X_{2\times2}$ can't have b in col. 3 & a in col. 2.

$\therefore X_{22} = \begin{bmatrix} b & e \\ e & a \end{bmatrix}$

$\therefore$ 1 CT structure.

- Order 4:

·	e	a	b	c
e	e	a	b	c
a	a			
b	b		$X_{3\times3}$	
c	c			

$X_{33} = \begin{bmatrix} e & c & b \\ c & e & a \\ b & a & e \end{bmatrix}$ ① , $\begin{bmatrix} e & c & b \\ c & a & e \\ b & e & a \end{bmatrix}$ ② , $\begin{bmatrix} b & c & e \\ c & e & a \\ e & a & b \end{bmatrix}$ ③

(c)	e	b
e	c	a
b	a	e

(4)

These satisfy permutation property, aswell as Identity.
All four satisfy closure & Inverse property

~~2 isn't assoc: ex: (a a) b.~~ ~~a (a b)~~

~~⇒ e b~~ ~~⇒ a c.~~

~~⇒ b~~ ~~⇒ b.~~

~~⇒ (c c) d~~ ~~⇒ d (c a)~~

~~⇒ a a~~ ~~⇒ c b~~

~~⇒ e.~~ ~~⇒ e~~

2, 3 & 4 are isomorphic: e, 1 element is inverse of itself,
2 remaining elems are inverse of each other.

∴ Only two unique structures. Structure 1 & structure (2, 3 & 4)

For Order 4, there are two ~~ee~~ unique Caylay Table, both of which are Abellian.

*	Monoid	Group
	• Unique identity	• Unique Identity
	• Inverse may not exist.	• Inverse is unique for each element.
	• Left & right cancellation is wrong.	• Left & right cancellation is valid.

Ex. In a Groupoid can we say that:

① $a*(b*c) = (a*b)*c$.

Nb. A Groupoid may/maynot satisfy Assoc. property.

② $a*(a*a) = (a*a)*a$.

No. Counter example $(P(\{1,2,3\}), -)$

$\{1\} - (\{1\} - \{1\})$ $\quad$ $(\{1\} - \{1\}) - \{1\}$

$\Rightarrow \{1\}$ $\quad$ $\Rightarrow \emptyset$

* Power of element of Group $\{(G, *)\}$

$a^0 = e$.

$a^n = a^{n-1} * a, \quad n \geq 1$

$a^{-n} = (a^{-1})^n, \quad n \geq 1$.

Ex. $(\{0,1,2\}, \oplus_3)$

$2^2 = (2+2) \bmod 3 = 1$

$2^3 = 2^2 * 2 = (1+2) \bmod 3 = 0$

$2^4 = 2^3 * 2 = (0+2) \bmod 3 = 2$

- For $\forall a \in G$,
  (1) $a^n * \bar{a}^n = e$
  (2) $a^m * a^n = a^{m+n}$
  (3) $(a^m)^n = a^{mn}$

- For $\forall a \in S$, where S is a semi-group :
  $a^1 = a$
  $a^n = a^{n-1} * a, \quad n \geq 2$

Ex. $(\{1, -1, i, -i\}, \times)$

$i^{-3} = (i^{-1})^3 = (-i)^3 = (-i * -i) * -i = i$

$(-i)^{-5} = ((-i)^{-1})^5 = (i)^5 = i^5$

* Subgroup

For a group $(G, *)$, a group $(S, *)$ is called its subgroup iff $S \subseteq G$ & operation is same
Represented as: $S \leq G$

Ex. $(\{1, -1, i, -i\}, \times)$ then which is a subgroup:

(A) $(\{-1, 1\}, \times)$

Closure ✓

Assoc ✓

Identity (1) ✓

Inverse ✓

$\{-1, 1\} \subseteq \{1, -1, i, -i\}$

∴ Subgroup

(B) $(\{1, i\}, \times)$

Closure ✗

Not Group. ∴ Not Subgroup

(C) $(\{1, 0, i\}, \times)$

Not subset. ∴ Not Subgroup

(D) $(\{1, -1\}, +)$

Diff operation. ∴ Not subgroup.

- To create subgroup from group $(G, *)$:
  (1) Take identity element.
  (2) If you take a, then take $a^{-1}, a^2, a^3, a^4, \ldots$ as well.
  {Because of closure property}

* Subgroups generated by element

- For an element $a \in G$, $(G, *)$,
  $\langle a \rangle$ = Smallest subgroup generated by a
  $\Rightarrow \{a^n \mid n \in \mathbb{Z}\}$