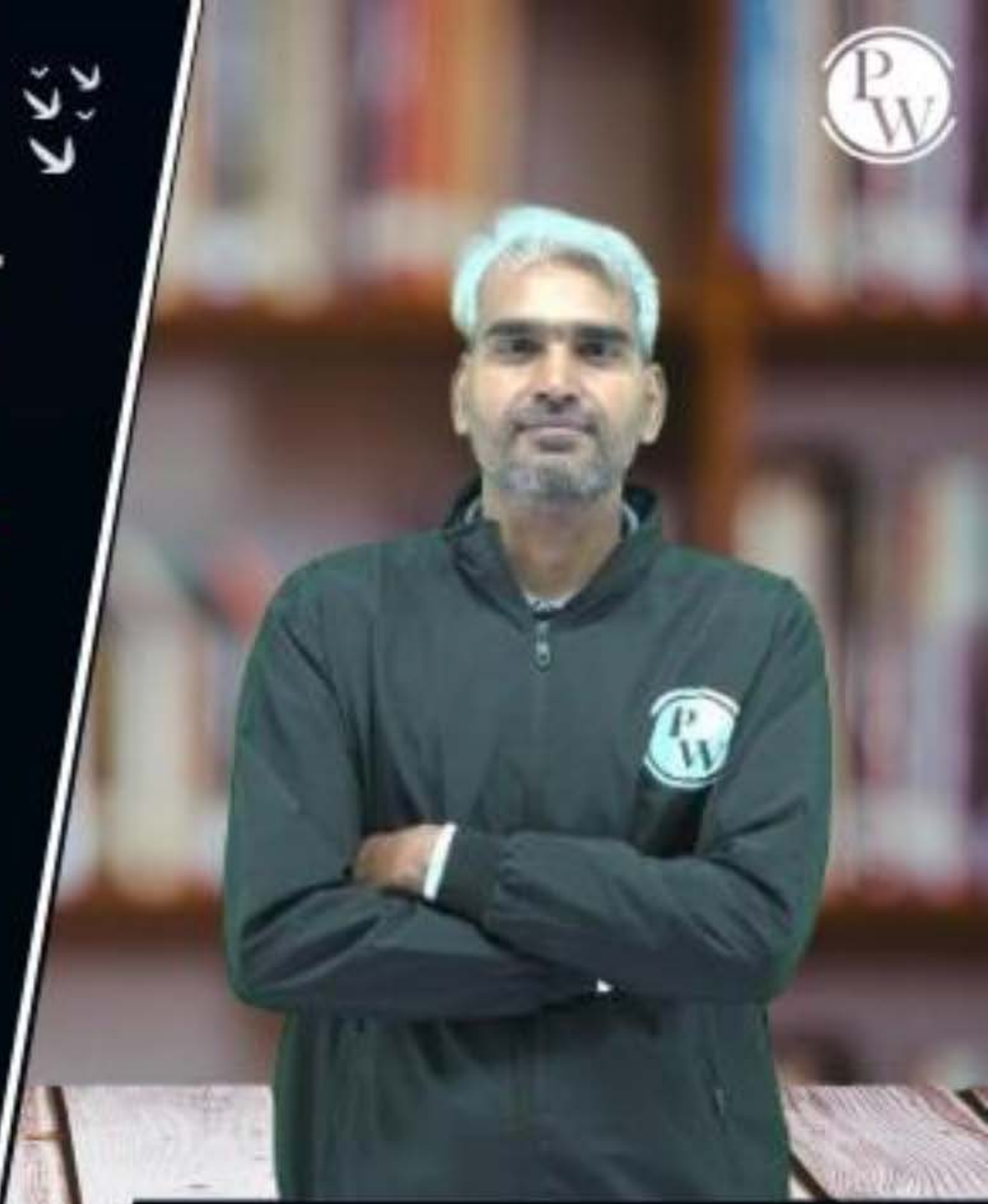
Computer Science & IT

Discrete Mathematics

Set Theory & Algebra

Lecture No. 20



By- Vishal Sir

Recap of Previous Lecture

- **Topic** Algebraic structure ✓
- **Topic** Semi-group ✓
- **Topic** Monoid ✓
- **Topic** Group ✓
- **Topic** Abelian group / Commutative group ✓

Slide

Topics to be Covered

Topic Finite Group

Topic Addition modulo ‘m’ $\oplus_m$

Topic Multiplication modulo ‘m’ $\otimes_m$

Topic Order of an element in a group (G,*)

Slide

det $\neq 0$ of order $n \times n$

#Q. Let A be the set of all non-singular matrices over real number and let * be the matrix multiple operation. Then

false :→ Matrix Multiplication is associative

A. A is closed under * but ⟨A ,*⟩ is not a semigroup

B. ⟨A ,*⟩ is a semigroup but not a monoid.

C. ⟨A ,*⟩ is a monoid but not a group.

D. ⟨A ,*⟩ is a group but not an abelian group.

Commutative Matrix Multiplication is not

(A, *) AS (i) Closed

SG (ii) * is associative

Monoid (iii) Identity Matrix ∈ A

Group (iv) for every matrix of set A inverse exists in set A

$I_S \in F(s)$ s.t. $f_1 \circ I_S = I_S \circ f_1 = f_1 \;, \forall f_1 \in F(s)$

#Q. Let S be any finite set, and F(s) is defined as set of all function on set S. Then F(s) with respect to function composition operation (ie., o) is.

$F(s)$ = Set of all functions on set S

$(F(s), \circ) = ?$

A Not a semigroup

B Semi group but not a monoid

C Monoid but not a group.

D A group

$\therefore$ F(s) is closed w.r.t. 'o'

let $f_1, f_2 \in F(s)$

$f_1 : S \to S$

$f_2 : S \to S$

$f_1 \circ f_2 : S \to S$

$f_2 \circ f_1 : S \to S$

$\therefore f_1 \circ f_2 \in F(s)$, $f_2 \circ f_1 \in F(s)$

$(F(s), \circ)$ → Closed ✓, Associative ✓, Identity ✓, ~~inverse~~

$F(S)$ is a set of all functions on set S, but all functions on set S need not be bijective, $\therefore$ inverse does not exist for the functions that are not bijective.

$\therefore (F(S), \circ)$ is a Monoid, but not a group

$\boxed{Max(e, a) = a \ \forall a \in Z}$ Identity w.r.t max = ?

#Q. Let Z is the set of all integers. The binary operation * is defined as a*b = max (a, b) then the structure (Z,*) is

e will be the smallest integer
and smallest integer is unknown
∴ Identity does not exist.

A. Not a semigroup

B. Semi group but not a monoid ✓

C. Monoid but not a group.

D. A group

① if $a, b \in Z$ then $\max(a,b) \in Z$ ∴ Closed

② $\underbrace{Max(a, Max(b,c)) = Max(Max(a,b), c)}$ it will result max of three elements

∴ Associative

$Z = \{\ldots -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots\}$

#Q. Let Q^* be the set of all positive rational numbers. The binary operation * is defined as $a * b = \frac{ab}{3}$ $\forall a, b, \in Q^*$ If $(Q^*, *)$ is a group then find

(i) identity element of the group

(ii) inverse of any element a, $\forall a \in$ Group

(i) $a * b = \frac{ab}{3}$

let e = identity

$\therefore\ a * e = a$

$\frac{\cancel{a}e}{3} = \cancel{a} \Rightarrow \boxed{e = 3}$

(ii) let $inv(a) = a^{-1}$

We know $a * a^{-1} = e$

$\frac{a \cdot a^{-1}}{3} = 3$

$\boxed{a^{-1} = 9/a}$

inv(0) = 0 inv(4k) = -4k,
inv(2k) = -2k, inv(6k) = -6k ... etc

#Q. Which of the following statement is/are not true.

all elements which are multiple of "2k"

A $\{0, \pm 2k, \pm 4k,, \pm 6k, ...\}$ is a group with respect to addition where any fixed positive integer (True)

closed ✓ Addition is associative ✓ identity w.r.t addⁿ = 0 ✓

B $A = \{x \mid x$ is real number and $0 < x \leq 1\}$ is a group with respect to multiplication

(False) $(A, \cdot) \Rightarrow$ Closed ✓ | Associative ✓ | identity: $1 \in A$, and identity w.r.t Multiplication = 1 ✓ | inverse: inverse does not exist for any element except 1

$\therefore$ not a group.

C $\{2^n \mid n$ is an integer$\}$ is a group with respect to multiplication

D None of these

#Q. Which of the following statement is/are not true.

A $\{0, \pm 2k, \pm 4k,, \pm 6k, ...\}$ is a group with respect to addition where any fixed positive integer (True)

ity

B $\{x \mid x \text{ is real number and } 0 < x \leq 1\}$ is a group with respect to multiplication (False)

C $B = \{2^n \mid n \text{ is an integer}\}$ is a group with respect to multiplication (True)

D None of these

$B = \{ 2^n \mid n \text{ is an integer} \}$

$B = \{ \ldots 2^{-5}, 2^{-4}, 2^{-3}, 2^{-2}, 2^{-1}, 2^{0}, 2^{1}, 2^{2}, 2^{3}, 2^{4}, \ldots \}$

③ Identity $= 1$, and $2^0 = 1$

$\therefore$ Identity exists.

④ for element $2^{n_1} \in B$, there exists $2^{-n_1} \in B$ s.t. $2^{n_1} \cdot 2^{-n_1} = 2^0 = 1 = e$ } inverse exists for every element

* let $2^{n_1}, 2^{n_2} \in B$, w.r.t. n_1 & n_2 are integers

① Closed: Now $2^{n_1} \cdot 2^{n_2} = 2^{n_1+n_2}$, if n_1 & n_2 are integers then n_1+n_2 is also an integer

$\therefore 2^{n_1+n_2} \in B$, hence closed

② Multiplication is associative

Topic : Finite Group

* A group $(G, *)$ is called a finite group, if underlying set 'G' is a finite set.

* If $(G, *)$ is a finite group, then number of elements in set G defines the order of group G, order of group G can be denoted by $O(G)$ or $|G|$.

Topic : Finite Group

Note:-

(1) $\{0\}$ form a group of order $= 1$, w.r.t. binary operation addition.

(2) $\{1\}$ form a group of order $= 1$, w.r.t. binary op^n multiplication

Note: In a finite group of order $= 1$, the only element of the set will be identity element w.r.t. binary operation

Topic : Finite Group

③ $\{1, -1\}$ form a finite group of order $= 2$ w.r.t. binary operation multiplication

- $inv(1) = 1$, because inverse of identity element is identity element itself.
- $\underbrace{(-1) \cdot (-1)}_{\text{Multiply}} = 1 = e$, $\therefore$ $inv(-1) = -1$

- Note: In a finite group of order $= 2$, every element is inverse of itself.

Topic : NOTE

(1) $\{0\}$ is the only finite group of real numbers w.r.t. operation addition.

(2) $\{1\}$ and $\{-1, 1\}$ are the only two finite groups of real numbers w.r.t. operation multiplication

Topic : Finite Group

- cube roots of unity are $1, \omega, \omega^2$

Note: $\{1, \omega, \omega^2\}$ form a finite group of order $= 3$ w.r.t. multiplication

$$\left\{\begin{array}{l} \omega^3 = 1 \\ 1 + \omega + \omega^2 = 0 \end{array}\right\}$$

(i) $\{1, \omega, \omega^2\}$ will be closed w.r.t. multiplication

(ii) Multiplication is associative

(iii) identity $= 1 \in \{1, \omega, \omega^2\}$

(iv) inverse = ?

$inv(1) = 1$

$inv(\omega) = \omega^2$

$inv(\omega^2) = \omega$

Binary op^n

$\cdot$	1	ω	ω^2
1	$1 = e$	ω	ω^2
ω	ω	ω^2	$\omega^3 = 1 = e$
ω^2	ω^2	$\omega^3 = 1 = e$	$\omega^4 = \omega^3 \cdot \omega = 1 \cdot \omega = \omega$

Composition table

Topic : Finite Group

Four roots of unity are $1, -1, i, -i$

$$\begin{cases} i = \sqrt{-1} \\ i^2 = -1 \\ 1 + (-1) + (i) + (-i) = 0 \end{cases}$$

Note: four roots of unity i.e., $\{1, -1, i, -i\}$ form a finite group of order $= 4$ w.r.t. multiplication

(i) $\{1, -1, i, -i\}$ is closed w.r.t. multiplication

(ii) Multiplication is associative

(iii) $1 \in \{1, -1, i, -i\}$ $\therefore$ identity exists

(iv) inverse = ?

$inv(1) = 1$

$inv(-1) = -1$

$inv(i) = -i$

$inv(-i) = i$

$\cdot$	1	-1	i	$-i$
1	$1 = e$	-1	i	$-i$
-1	-1	$1 = e$	$-i$	$+i$
i	i	$-i$	$i^2 = -1$	$-i^2 = -(-1) = 1 = e$
$-i$	$-i$	$+i$	$-i^2 = -(-1) = 1 = e$	$+i^2 = -1$

* **Note:-** Any set of n^{th} root of unity will form a group of "order = n" w.r.t. multiplication

2 mins Summary

Topic Finite group

Topic Addition modulo 'm' $\oplus_m$

Topic Multiplication modulo 'm' $\otimes_m$

Topic Order of an element in a group $(G,*)$

Slide

THANK - YOU

Slide