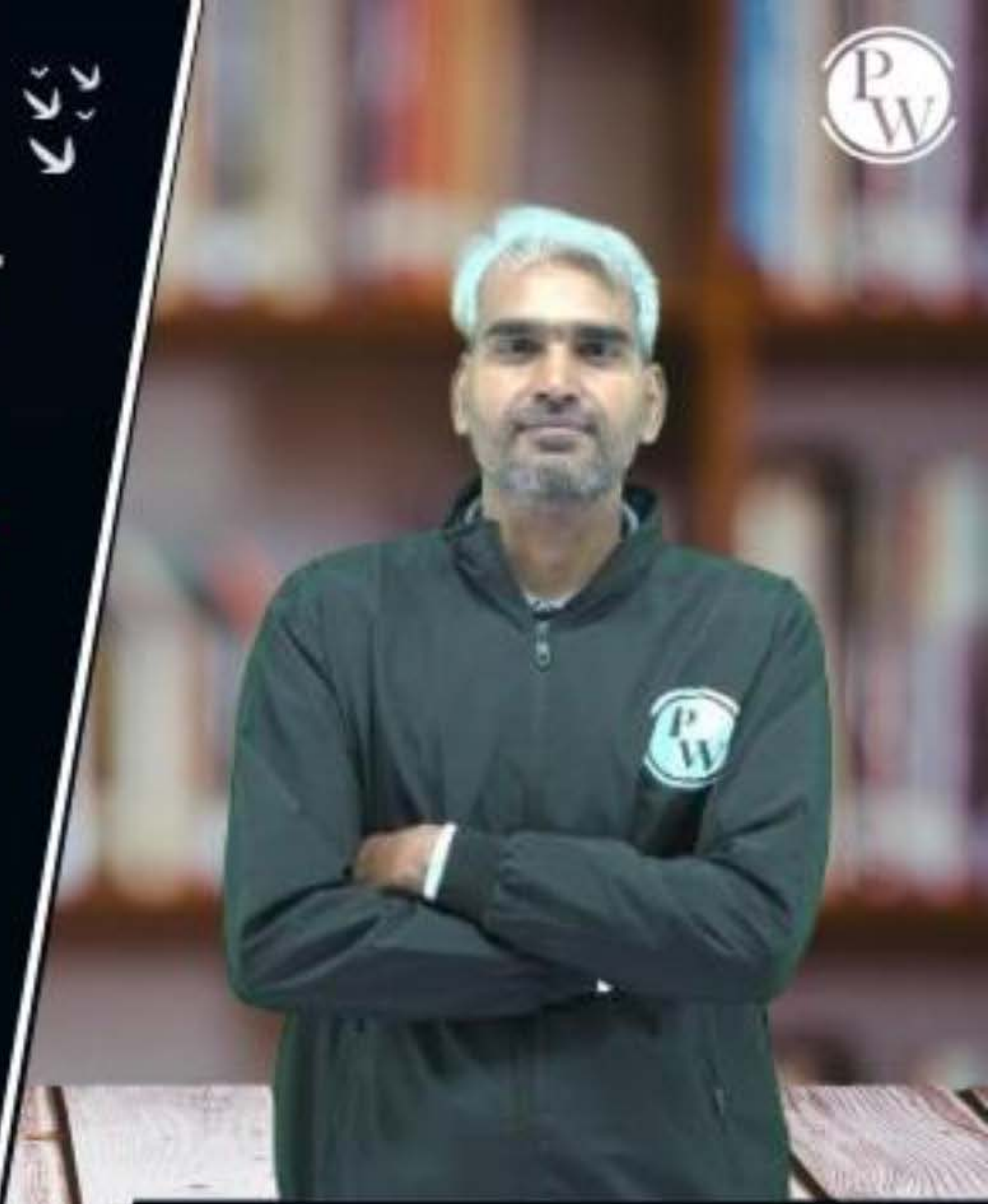
Computer Science & IT

Discrete Mathematics

Set Theory & Algebra

Lecture No. 21



By- Vishal Sir

Recap of Previous Lecture

Topic Finite Group

Slide

Topics to be Covered

gives remainder

Topic Addition modulo ‘m’ $\oplus_m$

Topic Multiplication modulo ‘m’ $\otimes_m$

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

Topic Subgroup

Slide

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 opn 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.
- $(-1)\cdot(-1) = 1 = e$, $\therefore inv(-1) = -1$

Multiply

- 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

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

(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 = ?

$inv(1) = 1$

$inv(-1) = -1$

$inv(i) = -i$

$inv(-i) = i$

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

Topic : Addition modulo 'm' $\oplus_m$

Let 'm' is any fixed positive integer.

for two non-negative integers a & b

$$a \oplus_m b = (a+b) \text{ Mod } m = \begin{cases} (a+b) & \text{if } (a+b) < m \\ r, & \text{if } (a+b) \geq m \end{cases}$$

Where r is the remainder obtained from $\frac{(a+b)}{m}$

eg: $2 \oplus_6 3 = 5$

eg: $3 \oplus_6 4 = 1$

Topic : Multiplication modulo 'm' $\otimes_m$

let 'm' be any fixed positive integer,
For any two non-negative integers a & b,

$$a \otimes_m b = (a \cdot b) \bmod m = \begin{cases} ab & \text{if } ab < m \\ r & \text{if } ab \geq m \end{cases}$$

where r is remainder of $\left(\frac{ab}{m}\right)$

eg: $2 \otimes_7 3 = 6$

eg: $2 \otimes_7 4 = 1$

Topic : NOTE

(1) The set $\{0, 1, 2, 3, \ldots (n-1)\}$ form a group of order $= n$ w.r.t. binary operation $\oplus_n$

eg. $\{0, 1, 2, 3, 4\}$ is a group w.r.t. $\oplus_5$

$inv(0) = 0$

$inv(1) = 5-1 = 4$

$inv(2) = 5-2 = 3$

$inv(3) = 5-3 = 2$

$inv(4) = 5-4 = 1$

Topic : NOTE

let $A = \{x \mid 1 \le x < n, \text{ and } \underbrace{GCD(x,n) = 1}\}$

Set of all +ve integers Which are less than 'n' and Co-prime to 'n'.

IMP

Note:- Set of all +ve integers which are coprime to 'n' and less than 'n' form a group w.r.t. $\otimes_n$

eg: $\{1,3,5,7\}$ form a group w.r.t. $\otimes_8$

$\{1,5\}$

$\{1,3\}$

$\{1,7\}$

$\{1\}$

$\otimes_8$	1	3	5	7
1	1=e	3	5	7
3	3	1=e	7	5
5	5	7	1=e	3
7	7	5	3	1=e

$inv(1) = 1$

$inv(3) = 3$

$inv(5) = 5$

$inv(7) = 7$

In this case every element is inverse of itself, but it is not necessary in all such groups

- Identity w.r.t. $\oplus_n$ will be $= 0$
- Identity w.r.t $\otimes_n$ will be $= 1$

eg: = $\{1, 2, 4, 7, 8, 11, 13, 14\}$ form a group w.r.t $\otimes_{15}$

+ find inverse of every element of the group.

identity = 1

$1 \otimes_{15} 1 = 1 = e \Rightarrow \therefore inv(1) = 1$

$2 \otimes_{15} 8 = 1 = e \Rightarrow \therefore inv(2) = 8$

$4 \otimes_{15} 4 = 1 = e \Rightarrow \therefore inv(4) = 4$

$7 \otimes_{15} 13 = 1 = e \Rightarrow \therefore inv(7) = 13$

$inv(8) = 2$

$11 \otimes_{15} 11 = 1 = e \Rightarrow \therefore inv(11) = 11$

$inv(13) = 7$

$14 \otimes_{15} 14 = 1 = e \Rightarrow inv(14) = 14$

If 'P' is any prime number, then

$\underbrace{\{1, 2, 3, 4, \ldots (P-1)\}}$ will form a group w.r.t $\times_P$.

e.g. $\{1, 2, 3, 4, 5, 6\}$ form a group w.r.t. $\times_7$

- identity = 1

$inv(1) = 1$

$inv(2) = 4$ & $inv(4) = 2$

$inv(3) = 5$ & $inv(5) = 3$

$inv(6) = 6$

Q: Which of the following is/are false.

*false (a) $\{1,2,3,4,5\}$ form a group w.r.t. $\otimes_6$

$2 \otimes_6 3 = 0$ $\therefore$ not closed, hence can not be a group.

false (b) $\{1,2,3,4,5\}$ form a group w.r.t. $\oplus_6$

$1 \oplus_6 5 = 0$ $\therefore$ not closed, hence can not be a group

(True) (c) $\{1,5\}$ form a group w.r.t. $\otimes_8$ ✓

Closed ✓ $\otimes_8$ is associative ✓ identity = 1 is present ✓ inv(1) = 1 & inv(5) = 5 ✓

(False) (d) $\{1,3,5\}$ form a group w.r.t. $\otimes_8$ ✓

$3 \otimes_8 5 = 7$ $\therefore$ not closed hence not a group.

(false) (e) $\{0,1,2,3,4\}$ form a group w.r.t. $\otimes_5$

inv(0) does not exist w.r.t. $\otimes_5$ $\{$ inv(0) does not exist w.r.t. $\otimes_n$ for any n $\}$

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

* Let $(G, *)$ is a group.
* For an element $a \in G$ the order of element 'a' is the least positive integer 'n' such that $(a)^n = e$ (identity)

$$(a)^n = \underbrace{a * a * a * \cdots * a}_{n \text{ times}}$$

* Order of element 'a' is denoted by $O(a)$.

eg: Find order of every element of group $\{1, -1\}$ w.r.t multiplication $\{O(G) = 2\}$

Can not be zero. Because in $(a)^n$, n must be +ve integer

$(1)^1 = 1 = e \quad \therefore \boxed{O(1) = 1}$

$(-1)^1 = -1 \neq e$

$(-1)^2 = 1 = e \Rightarrow \therefore \boxed{O(-1) = 2}$

$\underbrace{-1 \cdot -1}_{} = 1 = e$

$Inv(-1) = -1$

eg: Find order of every element of group.

$\{1, \omega, \omega^2\}$ w.r.t Multiplication $\{O(G) = 3\}$

$1 = e \Rightarrow \therefore \boxed{O(1) = 1}$

$(\omega)^1 = \omega \neq e$

$(\omega)^2 = \omega^2 \neq e$

$(\omega)^3 = \omega^3 = 1 = e \Rightarrow \therefore \boxed{O(\omega) = 3}$ $\boxed{inv(\omega) = \omega^2}$

$(\omega^2)^1 = \omega^2 \neq e$

$(\omega^2)^2 = \omega^4 = \omega \neq e$

$(\omega^2)^3 = \omega^6 = 1 = e \Rightarrow \therefore \boxed{O(\omega^2) = 3}$

eg: Find order of every element of group $\{1, -1, i, -i\}$ w.r.t. Multiplication $\{O(G) = 4\}$

$1 = e \Rightarrow \therefore \boxed{O(1) = 1}$

$(-1)^1 = -1 \neq e$

$(-1)^2 = 1 = e \Rightarrow \therefore \boxed{O(-1) = 2}$

$(i)^1 = i$

$(i)^2 = i^2 = -1$

$(i)^3 = i^2 \cdot i$

$= -1 \cdot i = -i$

$(i)^4 = i^2 \cdot i^2$

$= -1 \cdot -1$

$= 1 = e$

$\boxed{inv(i) = -i}$ $\therefore \boxed{O(i) = 4}$

$(-i)^1 = -i$

$(-i)^2 = i^2 = -1$

$(-i)^3 = -(i)^3 = -i^2 \cdot i$

$= -(-1 \cdot i)$

$= +i$

$(-i)^4 = +i^4 = i^2 \cdot i^2$

$= -1 \cdot -1 = 1 = e$

$\therefore \boxed{O(-i) = 4}$

eg: Find order of every element of group.

$\{0, 1, 2, 3\}$ w.r.t. $\oplus_4$ $\{O(G) = 4\}$

$\Rightarrow$ identity $= 0$

* $0 = e \Rightarrow \therefore \boxed{O(0) = 1}$

* $(1)^1 = 1$

$(1)^2 = 1 \oplus_4 1 = 2$ $\{inv(1) = 3\}$

$(1)^3 = 1 \oplus_4 1 \oplus_4 1 = (1 \oplus_4 1) \oplus_4 1 = (1)^2 \oplus_4 1 = 2 \oplus_4 1 = 3$

$(1)^4 = (1)^3 \oplus_4 1 = 3 \oplus_4 1 = 0 = e \quad \therefore \boxed{O(1) = 4}$

$(2)^1 = 2$

$(2)^2 = 2 \oplus_4 2 = 0 = e$

$\boxed{inv(2) = 2}$ $\quad \therefore \boxed{O(2) = 2}$

$(3)^1 = 3$

$(3)^2 = 3 \oplus_4 3 = 2$

$(3)^3 = (3)^2 \oplus_4 3 = 2 \oplus_4 3 = 1$

$(3)^4 = (3)^3 \oplus_4 3 = 1 \oplus_4 3 = 0 = e$

$\therefore \boxed{O(3) = 4}$

Q: Find order of every element of the group $\{1, 2, 3, 4\}$ w.r.t $\otimes_5$

* $\boxed{\text{identity} = 1 \quad \therefore O(1) = 1}$

*

$(2)^1 = 2$

$(2)^2 = 4$

$(2)^3 = 3$

$(2)^4 = 1 = e \quad \therefore \boxed{O(2) = 4}$

$\text{inv}(2) = 3$

$\therefore \boxed{O(3) = O(2) = 4}$

$(4)^1 = 4$

$(4)^2 = 1 = e$

$\therefore \boxed{O(4) = 2}$

H.W. Find order of every element of the group $\underbrace{\{0, 1, 2, 3, 4\}}$ w.r.t $\oplus_5$

$\boxed{\begin{array}{l} \text{identity} = 0, \quad \therefore\ O(0) = 1 \\ \text{and} \quad O(1) = O(2) = O(3) = O(4) = O(\text{n}) = \underset{\text{Prime No.}}{5} \end{array}}$

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

(1) order of identity element of the group is always '1'.

(2) Order of an element of the group is less than or equal to the order of the group.

(3) For an element 'a' $O(a) = O(a^{-1})$ {order of an element is same as order of its inverse}

Topic : Properties w.r.t. Finite Group

IMP

Note: ① Order of any element of the group divides the order of the group.

Note: ② for an element $a \in$ Group if $O(a) = 2$, then 'a' is inverse of itself.

i.e. if $O(a) = 2$, then $a^{-1} = a$

③ If Order of the group G is a prime number, then,

$O(\text{identity}) = 1$

and $O(a) = O(G)$, $\forall a \in G$, except identity element

2 mins Summary

Topic Addition modulo 'm' $\oplus_m$

Topic Multiplication modulo 'm' $\otimes_m$

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

Topic Subgroup

Slide

THANK - YOU

Slide