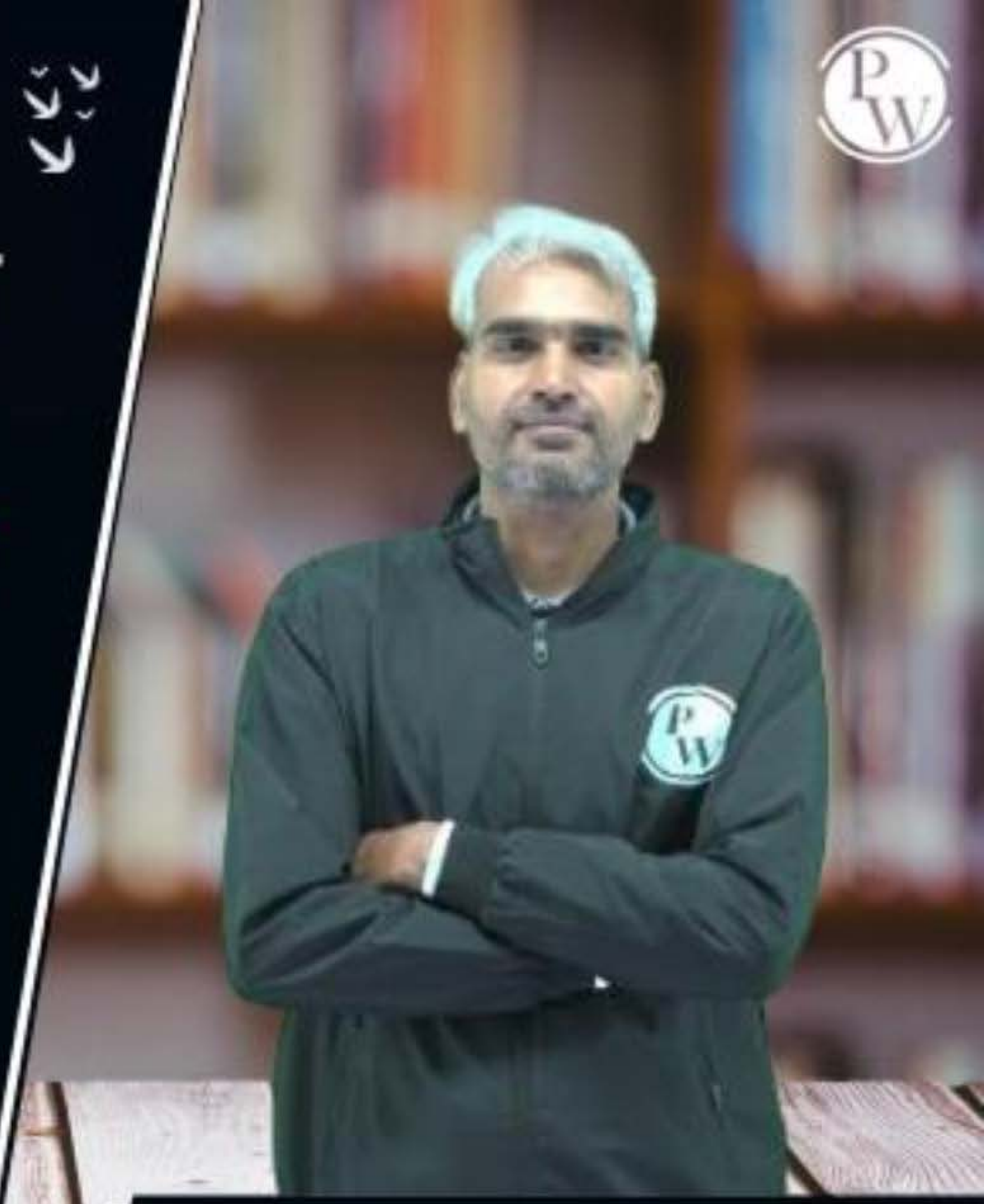
Computer Science & IT

Discrete Mathematics

Set Theory & Algebra

Lecture No. 22



By- Vishal Sir

Recap of Previous Lecture

Topic Addition modulo 'm' $\oplus_m$

Topic Multiplication modulo 'm' $\otimes_m$

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

Slide

Topics to be Covered

Topic Subgroup ✓

Topic Cyclic group ✓

Topic Some important properties ✓

Slide

$\{e\}$

Topic : Subgroup

Let $(G, *)$ be a group. A subset H of set G is called a subgroup of group $(G, *)$ if $(H, *)$ is a group.

- Let $(G, *)$ be a group with 'e' as the identity element; then $(G, *)$ and $(\{e\}, *)$ are the trivial subgroup of group $(G, *)$, any other subgroup of group $(G, *)$ will be called a proper subgroup of $(G, *)$

* let $(G, *)$ is a group of order $= |G|$, then

$(G, *)$ is a subgroup of order $= |G|$,

and $(\{e\}, *)$ is a sub-group of order $= 1$

eg: Let $\underbrace{\{1, -1, i, -i\}}$ is a group w.r.t. multiplication.

→ $(\{1, -1, i, -i\}, \cdot)$ and $(\{1\}, \cdot)$ are trivial subgroups of the given group.

→ $(\{1, -1\}, \cdot)$ is a proper subgroup of given group eg: $\{1, 3, 5, 7\}$ is a group w.r.t. $\otimes_8$.

$\Rightarrow$ $(\{1,3,5,7\}, \otimes_8)$ and $(\{1\}, \otimes_8)$ are trivial sub-groups

$\Rightarrow$ $(\{1,3\}, \otimes_8)$, $(\{1,5\}, \otimes_8)$, $(\{1,7\}, \otimes_8)$ are proper sub-groups of given group.

Topic : Properties w.r.t. Subgroup

(1) Let $(G, *)$ be a group, and H is a non-empty subset of G,

$(H, *)$ is a subgroup of G if and only if

$(a * b^{-1}) \in H, \forall a, b \in H$

Let $(a*b^{-1}) \in H, \ \forall a,b \in H$

identity

let $a \in H$,

$\therefore a, a \in H$

$(a*b^{-1}) \in H, \ \forall a,b \in H$

and $a, a \in H$

$\therefore (a*a^{-1}) \in H$

i.e. $\boxed{\underset{\text{identity}}{e} \in H}$

Associative :-

We know $(G,*)$ is a group

$\therefore$ "$*$" is associative w.r.t. elements of set H as well

inverse :

let $a \in H$,

and we know $e \in H$

for $e, a \in H$

We know $(e*a^{-1}) \in H$

i.e. $\boxed{a^{-1} \in H}$

Closure :-

let $a, b \in H$

we know, $a^{-1}, b^{-1} \in H$

for element, $a, b^{-1} \in H$

We know $(a*(b^{-1})^{-1}) \in H$

i.e. $\boxed{(a*b) \in H}$

Note: $(G, *)$ is a group if and only if

① $a * b^{-1} \in G, \ \forall a, b \in G$

and ② '$*$' is associative

Topic : Properties w.r.t. Subgroup

(2) Let $(G,*)$ be a group, and H is any non-empty subset of G.

$(H,*)$ is a subgroup of group $(G,*)$. if and only if

(1) $(a*b) \in H$, $\forall a,b \in H$

and (2) $a^{-1} \in H$, $\forall a \in H$

Topic : Properties w.r.t. Subgroup

(3) Let $(G, *)$ is a group and $(H, *)$ is a subgroup of group G, then $O(H)$ divides $O(G)$

very very very Imp

Lagrange's Theorem

Order of subgroup divides the order of the original group.

Topic : Properties w.r.t. Subgroup

(4) Let $(G, *)$ is a group, and H_1 and H_2 are two subgroups of group G, then

$H_1 \cup H_2$ is a subgroup of group $(G, *)$

if and only if

$$\begin{cases} H_1 \subseteq H_2 & \{\text{i.e. } H_1 \cup H_2 = H_2\} \\ \text{or} & \\ H_2 \subseteq H_1 & \{\text{i.e. } H_1 \cup H_2 = H_1\} \end{cases}$$

otherwise Union of H_1 & H_2 will not be closed w.r.t. '$*$'

Q: let $(G,*)$ is a group, and H_1 & H_2 are two subgroups of $(G,*)$

$\Rightarrow$ We know $G = (Z, +)$ is a group

let $H_1 = \{0, \pm 2, \pm 4, \pm 6, \pm 8 \ldots\}$, and we know $(H_1, +)$ is a subgroup of $(Z,+)$

let $H_2 = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$ and we know $(H_2,+)$ is a subgroup of $(Z,+)$

$H_1 \cup H_2 = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 9, \ldots\}$

$2+3=5 \notin H_1 \cup H_2$

$H_1 \cup H_2$ is not closed w.r.t Addition

Topic : Properties w.r.t. Subgroup

(5) Let $(G, *)$ is a group, and H_1 and H_2 are two subgroups of group G, then $H_1 \cap H_2$ is always a subgroup of group $(G, *)$

Proof

Let $a, b \in H_1 \cap H_2$, then $a, b \in H_1$ and $a, b \in H_2$

H_1 is a subgroup $\qquad$ H_2 is a subgroup

$\therefore a * b^{-1} \in H_1 \cap H_2 \Longleftarrow \therefore a * b^{-1} \in H_1$ (and) $a * b^{-1} \in H_2$

$\therefore H_1 \cap H_2$ is a group w.r.t. '$*$'

Q: Let $(G, *)$ is a group of prime order, then find the number of subgroups of group G.

* $O(G)$ = Prime number,
  and order of any subgroup of group $(G, *)$ must divide $O(G)$

* $O(G)$ = Prime no (p) $\therefore$ only divisors of prime no. 'p'
  are 1 & p.

$\underbrace{1}_{\text{w.r.t } (\{e\}, *)}$ & $\underbrace{p}_{\text{w.r.t } (G, *)}$

Topic : Cyclic group

Let $(G, *)$ be a group, if there exists any element $a \in G$, such that every element of group $(G, *)$ can be written in the form a^n for some +ve integer 'n', then $(G, *)$ is called a cyclic group and element 'a' is called generator of cyclic group $(G, *)$ {because every element can be generated from element 'a'}

$$\underbrace{a * a * a * \cdots * a}_{n \text{ times}}$$

eg: $\{1, -1\}$ is a cyclic group of order $= 2$ w.r.t. multiplication., where '-1' is the generator of the cyclic group.

Solu^n

$$\left.\begin{aligned} (-1)^1 &= -1 \\ (-1)^2 &= 1 \end{aligned}\right\}$$

we can generate all the elements of set using '-1'.

$\therefore$ '-1' is a generator & group is a cyclic group.

Note: let e = identity element

$$(e)^1 = e$$
$$(e)^2 = e * e = e$$
$$(e)^3 = e^2 * e = e * e = e$$
$$(e)^4 = e^3 * e = e * e = e$$

identity element can not generate any other element except itself.

Identity element can not be the generator of a set containing any other element except itself.

* eg. We know $\{1, \omega, \omega^2\}$ is a group w.r.t. multiplication

1 = identity ∴ can not be the generator

$\Rightarrow (\omega)^1 = \omega$
$(\omega)^2 = \omega^2$
$(\omega)^3 = \omega^3 = 1 = e$
all elements of the set

$\Rightarrow (\omega^2)^1 = \omega^2$
$(\omega^2)^2 = \omega^4 = \omega$
$(\omega^2)^3 = \omega^6 = 1 = e$
all elements of the set

ω & ω^2 are generator

& $\{1, \omega, \omega^2\}$ is a cyclic group of order = 3 w.r.t. multiplication eg: $\{1, -1, i, -i\}$ is a group w.r.t. multiplication

$\boxed{1 = \text{identity}}$

$(-1)^1 = -1$

$(-1)^2 = 1 = e$ $\therefore O(-1) = 2 \neq O(G)$

Repeating the elements

$(-1)^3 = -1$

$(-1)^4 = 1 = e$

Repeating the elements

$(-1)^5 = -1$

$(-1)^6 = +1 = e$

$(i)^1 = i$

$(i)^2 = -1$

$(i)^3 = -i$

$(i)^4 = 1 = e$ $O(i) = 4 = O(G)$

generated all elements

$(-i)^1 = -i$

$(-i)^2 = -1$

$(-i)^3 = +i$

$(-i)^4 = 1 = e \Rightarrow O(-i) = 4 = O(G)$

generated all elements

$\therefore \{1, -1, -i, i\}$ is a cyclic group, where i & $-i$ are the generators

Topic : Cyclic group

(1) For any cyclic group $(G, *)$, if 'a' is the generator of cyclic group G, then $O(a) = |G|$ {order of generator is same as order of group}

(2) If element 'a' is the generator of cyclic group $(G, *)$, then a^{-1} is also a generator of the same cyclic group.

Topic : Cyclic group

(3) In a group $(G, *)$ if these exists any element whose order is same as the order of the group, then group is called a cyclic group and that element will become generator of the cyclic group.

Topic : Cyclic group

(4) In a finite group $(G, *)$ if there exists no element whose order is same as the order of finite group $(G, *)$, then group $(G, *)$ is not a cyclic group.

eg: $\{1, 3, 5, 7\}$ w.r.t $\otimes_8$ is a group of order $= 4$

$1 =$ identity, $\therefore \boxed{O(1) = 1}$

$(3)^1 = 3$

$(3)^2 = 3 \otimes_8 3 = 1 = e. \quad \therefore \boxed{O(3) = 2}$

$(5)^1 = 5$

$(5)^2 = 5 \otimes_8 5 = 1 = e \quad \therefore \boxed{O(5) = 2}$

$(7)^1 = 7$

$(7)^2 = 7 \otimes_8 7 = 1 = e \quad \therefore \boxed{O(7) = 2}$

No element whose order is same as order of the given group.

$\therefore \{1,3,5,7\}$ w.r.t $\otimes_8$ is not a cyclic group.

Q: $\{0, 1, 2, 3, 4\}$ is a group w.r.t. $\oplus_5$, Check whether group is a cyclic group or not? If cyclic then find all the generators of the cyclic group

0 = identity $\therefore \boxed{O(0) = 1}$

$(1)^1 = 1$
$(1)^2 = 2$
$(1)^3 = 3$
$(1)^4 = 4$
$(1)^5 = 0 = e$

all elements
$\therefore$ '1' is a generator
$inv(1) = 4$
$\therefore$ 4 is also a generator
$\therefore \boxed{O(1) = 5}$

$(2)^1 = 2$
$(2)^2 = 4$
$(2)^3 = 1$
$(2)^4 = 3$
$(2)^5 = 0 = e$

all elements
$\therefore$ '2' is a generator
$inv(2) = 3$
$\therefore$ 3 is also a generator
$\therefore \boxed{O(2) = 5}$

Group is a cyclic group, and 1, 2, 3 & 4 are the generators of the cyclic group.

2 mins Summary

Topic Subgroup

Topic Cyclic group

Topic Important properties of group

Slide

THANK - YOU

Slide