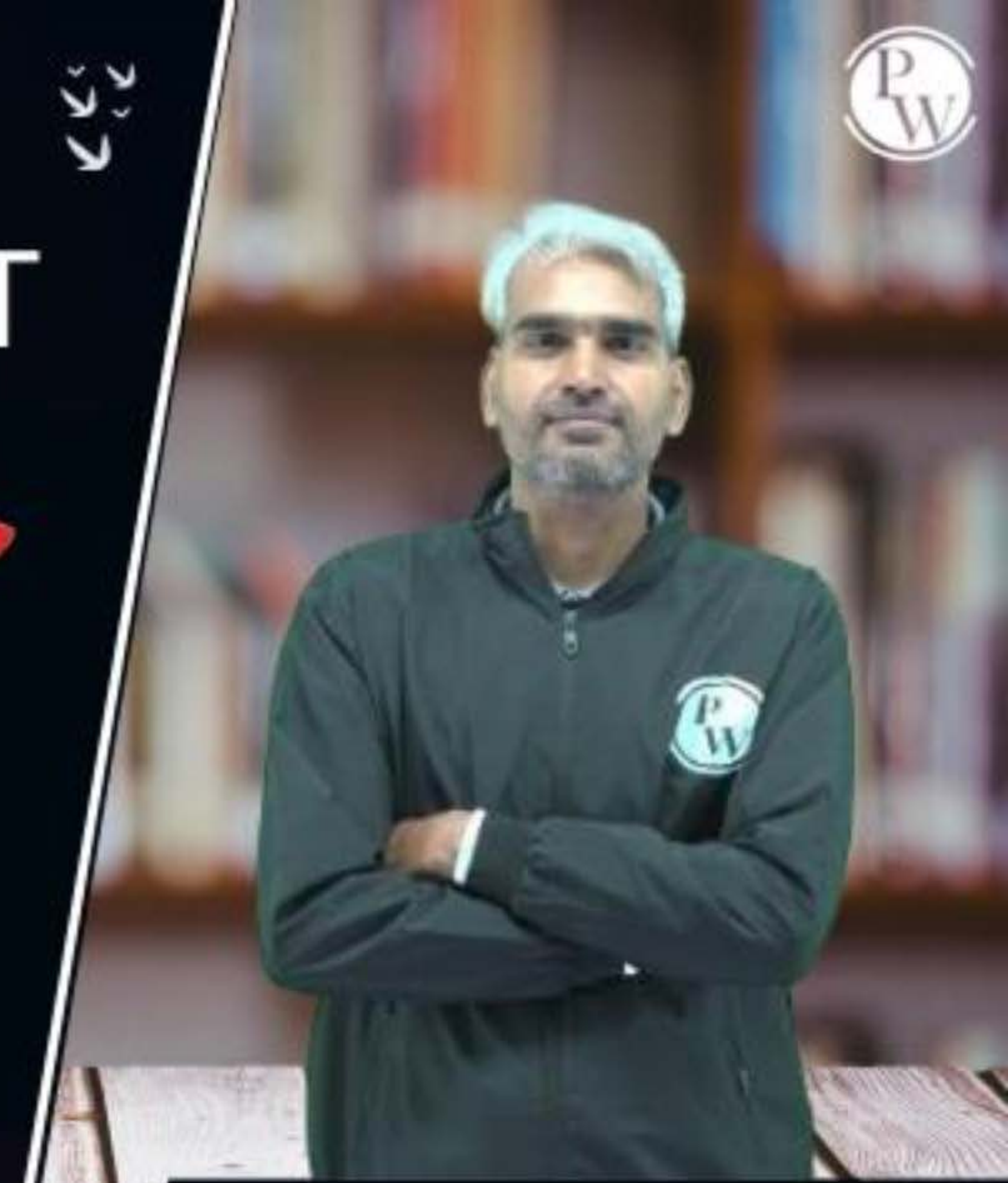
Computer Science & IT

Discrete Mathematics

Set Theory & Algebra

Lecture No. 21



By- Vishal Sir

Recap of Previous Lecture

Topic Example of groups w.r.t. $\oplus_m$ & $\otimes_m$

Topic Order of an element of the group (G,*)

↳ least positive integer 'n' s.t. $a^n = e$ (identity)

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

- $\{0, 1, 2, \ldots (n-1)\}$ is a group w.r.t. $\oplus_n$
- Set of all natural no.s less than 'n' & coprime to 'n' form a group w.r.t. $\otimes_n$
- $\{1, 2, 3, \ldots (P-1)\}$ form a group w.r.t. $\otimes_P$, where 'P' is a prime no.

Slide

Topics to be Covered

Topic Subgroup

Topic Cyclic group

Slide

Topic : Subgroup

* Let $(G, *)$ is a group, a subset H of set G is called a sub-group of group $(G, *)$ if and only if $(H, *)$ is a group.

* Let $(G, *)$ be a group and 'e' is the identity element w.r.t. binary opⁿ '$*$' then $(G, *)$ and $(\{e\}, *)$ are called trivial sub-group of group $(G, *)$ and any other sub-group of group $(G, *)$ will be called Proper subgroup of group $(G, *)$

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

then $(G, *)$ is a sub-group of group $(G, *)$ and its order is $|G|$

& $(\{e\}, *)$ is a subgroup of group $(G, *)$ and its order is '1'.

- We know $\{1, -1, i, -i\}$ is a group of order $= 4$ w.r.t. multiplication

- $\{1\}$ will be a trivial subgroup of order $= 1$,
$\{1, -1, i, -i\}$ will be a trivial sub-group of order $= 4$

$\{1, -1\}$ is a proper subgroup of above group.
and its order is '2'.

$\boxed{\text{$\{1, i\}$ is a sub-set of set $\{1, -1, i, -i\}$, but it is not a sub-group of given group.}}$

<u>because</u> $\{1, i\}$ is not a group w.r.t. binary opn multiplication

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

* $\{1\}$ w.r.t $\otimes_8$ is a group,
$\{1, 3, 5, 7\}$ w.r.t $\otimes_8$ is a group.

$\{1\}$ & $\{1, 3, 5, 7\}$ are trivial sub groups of above group.

* $\{1, 3\}$, $\{1, 5\}$ & $\{1, 7\}$ are proper sub-groups of above group

Topic : Properties w.r.t. Subgroup

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

then

$(H,*)$ is a sub-group of group $(G,*)$

if and only if,

$$\boxed{a*b^{-1}\in H, \quad \forall a,b\in H}$$

i.e. H is (1) Closed

(2) identity exist

& (3) Inverse exist for every element

Topic : Properties w.r.t. Subgroup

(2) Let $(G, *)$ be a finite group of order $= |G|$, and $(H, *)$ is a sub-group of group $(G, *)$ and order of sub-group $(H, *)$ is $|H|$,

then $|H|$ divides $|G|$.

Lagrange's theorem

i.e., order of sub-group divides the order of original group

Topic : Properties w.r.t. Subgroup

③ Let $(G, *)$ be a group, and $(H_1, *)$ & $(H_2, *)$ are any two sub-groups of group $(G, *)$

then $(H_1 \cap H, *)$ is also a sub-group of group $(G, *)$

* Let $a, b \in H_1 \cap H_2$,

$\therefore a, b \in H_1$ and $a, b \in H_2$

we know $(H_1, *)$ is a group

we know H_2 is also a group

$\therefore a * b^{-1} \in H_1$

$\therefore a * b^{-1} \in H_2$

$\therefore a * b^{-1} \in H_1 \cap H_2$

i.e. if $a, b \in H_1 \cap H_2$ then $a * b^{-1} \in H_1 \cap H_2$

$\therefore (H_1 \cap H_2, *)$ is also a group. $\therefore$ it is also a subgroup of $(G, *)$

Topic : Properties w.r.t. Subgroup

(4) Let $(G, *)$ be a group and $(H_1, *)$ & $(H_2, *)$ are any two sub-groups of $(G, *)$, then

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

if and only if (1) $H_1 \subseteq H_2$ $\{$i.e. $H_1 \cup H_2 = H_2\}$

or (2) $H_2 \subseteq H_1$ $\{$i.e. $H_1 \cup H_2 = H_1\}$

eg We know $\{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \ldots\}$ is a group w.r.t. binary opn addition

Let $H_1 = \{0, \pm 2, \pm 4, \pm 6, \pm 8, \ldots\}$ is a subset of above set and it is a group w.r.t addition, $\therefore (H_1, +)$ is a sub group of above group

& $H_2 = \{0, \pm 3, \pm 6, \pm 9, \pm 12, \ldots\}$ is also a subset of above set, and it is also a group w.r.t. addition, $\therefore (H_2, +)$ is also a sub group of above group

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

$2 + 3 = 5 \notin H_1 \cup H_2$, it is not closed w.r.t. addition

$\therefore H_1 \cup H_2$ is not a group w.r.t. addition

Hence, $(H_1 \cup H_2, *)$ is not a subgroup of given group.

Q:- Let $(G, *)$ be a group of order $= |G|$, if $|G|$ is a prime number, then find the total number of subgroups of group $(G, *)$

$\because$ Order of subgroup of group $(G, *)$ must divide order of group i.e. $|G|$

let $|G| = p$ (Prime no.)

$\because$ Because 'p' is a prime number,

$\therefore$ order of subgroup can be 1 or p only.

1 → it is w.r.t. trivial sub-group $(\{e\}, *)$

p → it is w.r.t. trivial sub-group $(G, *)$

$\therefore$ Only two sub-groups are possible, and both of them are trivial

Q: Let $(G, *)$ be a group of order $= 8$; then How many sub-groups are possible for group $(G, *)$

Can not be answered,
until we know the elements of the group
and binary op^n '$*$'!

Topic : Cyclic group

Let $(G, *)$ be a group, If there exist any element $a \in G$, such that every element of set G can be written in the form $(a)^n$ for some positive integer 'n', then group $(G, *)$ is called a cyclic group, and element 'a' is called generator w.r.t. cyclic group $(G, *)$.

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

$\boxed{\text{A cyclic group may have more than one generator}}$

eg. We know $\{1, -1\}$ is a group of order $= 2$. wrt multiplication

$\rightarrow O(G) = 2$

1 = identity

$(1)^1 = 1$ = identity

$(1)^2 = 1$ = identity

$\vdots$

$(e)^1 = e$

$(e)^2 = e$

$\vdots$

$(e)^n = e$

identity element can not generate any other element except itself.

$\left.\begin{array}{l}(-1)^1 = -1 \\ (-1)^2 = 1 = e\end{array}\right\}$ ← '-1' can generate all elements of the set for different powers of '-1'

$\therefore \{1, -1\}$ is a cyclic group w.r.t. multiplication, with '-1' as its generator

$$\boxed{O(-1) = 2 = O(G)}$$

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

- 1 = identity $\therefore$ '1' can not generate any other element except itself
- $(\omega)^1 = \omega$
  $(\omega)^2 = \omega^2$
  $(\omega)^3 = \omega^3 = 1 = e$

'ω' can generate all the elements

$\boxed{O(\omega) = 3 = O(G)}$

$\therefore \{1, \omega, \omega^2\}$ is a cyclic group & 'ω' is one of its generator

$(\omega^2)^1 = \omega^2$
$(\omega^2)^2 = \omega$
$(\omega^2)^3 = 1 = e$

ω^2 can also generate all elements.

$\boxed{O(\omega^2) = 3 = O(G)}$

$\therefore \omega^2$ is also the generator of cyclic group $\{1, \omega, \omega^2\}$ w.r.t. multiplication

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

$\therefore \omega^2$ will also be a generator eg: We know $\{1, -1, i, -i\}$ is a group of Order = 4 wrt multiplication

$O(G) = 4$

* 1 = identity, ∴ can not generate any other element except itself

* $(-1)^1 = -1$
$(-1)^2 = 1 = e$
$(-1)^3 = -1$
$(-1)^4 = 1 = e$
$(-1)^5 = -1$
$(-1)^6 = 1 = e$

elements are repeated

Once we have obtained the identity element, if we increase the power then already generated elements will be repeated

$(i)^1 = i$
$(i)^2 = -1$
$(i)^3 = -i$
$(i)^4 = 1 = e$

$\boxed{O(i) = 4 = O(G)}$ ∴ 'i' is a generator

all elements

inv(i) = $-i$ ∴ '$-i$' will also be a generator

$(-i)^1 = -i$
$(-i)^2 = -1$
$(-i)^3 = +i$
$(-i)^4 = 1 = e$

all elements ∴ '$-i$' is also a generator

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

$(1, -1, i, -i)$ is a cyclic group

i.e., generator needs to generate all other elements of the set before it generates identity element

Q: $\{1,3,5,7\}$ w.r.t. $\otimes_8$ is a group of order $= 4$ → $O(G) = 4$

+ $1 =$ identity, $\therefore$ '1' can not generate any other element except itself.

+ $(3)^1 = 3$

$(3)^2 = 3 \otimes_8 3 = 1 = e$

← does not generate all elements of the group.

$\boxed{O(3) = 2 \neq O(G)}$

+ $(5)^1 = 5$

$(5)^2 = 5 \otimes_8 5 = 1 = e$

← does not generate all elements of the group.

$\boxed{O(5) = 2 \neq O(G)}$

$(7)^1 = 7$

$(7)^2 = 7 \otimes_8 7 = 1 = e$

← does not generate all elements

$\boxed{O(7) = 2 \neq O(G)}$

No element of the group $\{1,3,5,7\}$ w.r.t $\otimes_8$ can generate all elements of the group.

$\therefore$ generator of the elements of the group does not exist.

Hence, group is not a cyclic group.

Topic : Cyclic group

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

Topic : Cyclic group

(2) Let $(G,*)$ be a finite group of order $= |G|$.
if there exist any element $a \in G$, such that

$O(a) = O(G)$, then $(G,*)$ is a cyclic group and element 'a' is one of the generator of cyclic group $(G,*)$

Topic : Cyclic group

(3) Let $(G,*)$ be a finite group of order $= |G|$.
if there exist no element $a \in G$, such that $O(a) = O(G)$, then $(G,*)$ is not a cyclic group.

i.e

$$\boxed{O(a) \neq O(G), \ \forall a \in G}$$

Topic : Cyclic group

(4) Let $(G, *)$ be a finite group of order $= |G|$.
if there exist any element $a \in G$, such that
$O(a) = O(G)$, then $(G, *)$ is a cyclic group
and element 'a' is one of
the generator of cyclic group $(G, *)$

We know $O(a) = O(a^{-1})$

$\therefore$ if $O(a) = O(G)$, then $O(a^{-1}) = O(G)$

Hence if element $a \in G$ is a generator, then a^{-1} is also a generator of that cyclic group

Q: We know $\{0, 1, 2, 3, 4\}$ is a group of order = 5 (Prime No.) w.r.t. binary opⁿ $\oplus_5$,

find all generators of above group

Solⁿ Order of group is = 5 = prime no.

$\therefore$ order of elements will divide order of group.

i.e., order of elements will be 1 or 5

1 → for identity element → it can never be the generator containing any other element except itself.

5 → for every other non-identity element

$\therefore O(1) = 5 = O(G)$ $\therefore$ generator

$O(2) = 5 = O(G)$ $\therefore$ generator

$O(3) = 5 = O(G)$ $\therefore$ generator

$O(4) = 5 = O(G)$ $\therefore$ generator

2 mins Summary

- **Topic** Subgroup
- **Topic** Cyclic group

Slide

THANK - YOU

Slide