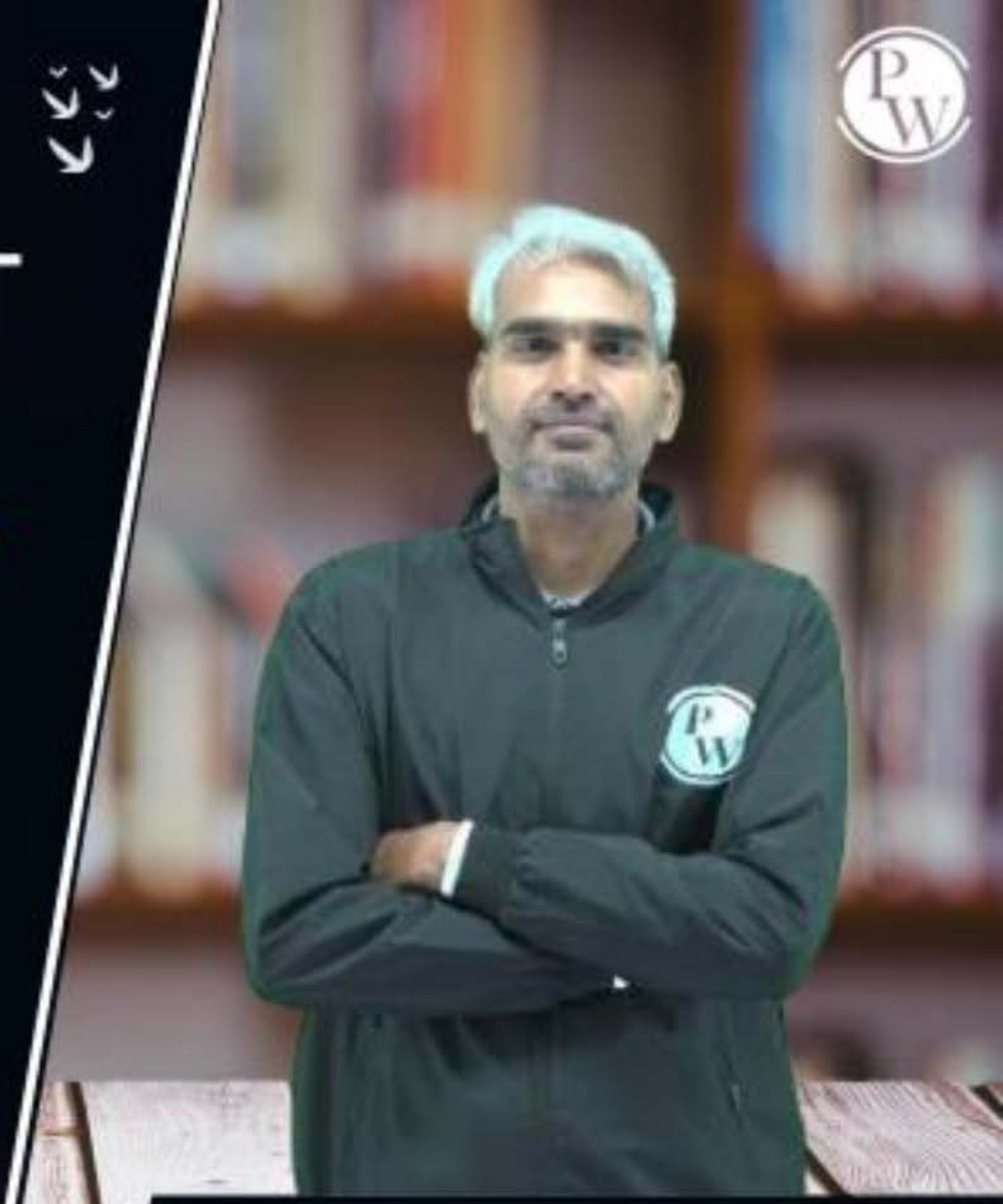
Computer Science & IT

Discrete Mathematics

Set Theory & Algebra

Lecture No. 19



By- Vishal Sir

Recap of Previous Lecture

Topic — Introduction to group theory

Topic — Algebraic structure (groupoid) (Closed)

Topic — Semi-group (Closed + Associative)

Topic — Monoid (Closed + associative + identity)

Topic — Group (——, —— + inverse)

Topic — Abelian group / Commutative group (——, ——, —— + Commutative)

Slide

Topics to be Covered

Topic Practice questions

Topic Finite group

Topic Addition modulo ‘m’ $\oplus_m$

Topic Multiplication modulo ‘m’ $\otimes_m$

Slide

Topic : Group Theory

- Algebraic Structure (Groupoid)
- Semi-group
- Monoid
- Group
- Abelian group / Commutative group

Slide

Topic : Special Sets

N = Set of all natural numbers

Z = Set of all integers

Q = Set of all rational numbers

Q^* = Set of all non-zero rational numbers

Slide

Topic : Algebraic Structure / Groupoid

A non-empty set 'S' w.r.t. binary opⁿ '$*$'
is called an algebraic structure / groupoid
if $\boxed{a * b \in S \quad \forall a, b \in S}$ → i.e. set 'S' is closed w.r.t binary opⁿ '$*$'

it is called Closure Property

Slide

	Algebraic Structure	Semi-Group	Monoid	Group	Abelian Group
(N,+)	✓				
(N, .)	✓				
(N,−)	$2-5=-3 \quad -3 \notin N$ ✗				
(N,÷)	$1 \div 2 = 0.5 \notin N$, ✗				
(Z,+)	✓				
(Z, .)	✓				
(Z,-) −	✓				
(Z ,÷) ÷	$1 \div 2 = 0.5 \notin Z$, ✗				
(Q,+)	✓				
(Q, .) .	✓				
(Q, -) −	✓				
(Q, ÷) ÷	✗ $0 \in Q$, & $\frac{p}{0}$ = Not defined				
(Q^*, +)	$\frac{p}{q}+\left(-\frac{p}{q}\right)=0 \notin Q^*$ ✗				
(Q^*, .) .	✓				
(Q^*, -) −	$\frac{p}{q}-\frac{p}{q}=0 \notin Q^*$ ✗				
(Q^*,÷) ÷	✓				

Set N

w.r.t binary opⁿ '+'

Q^* set of all non-zero rational No.

Slide

Topic : Semi-group

i.e., it must be closed.

An $\underbrace{\text{algebraic structure}}$ (groupoid) $(S, *)$ is called a semi group

if $\boxed{(a*b)*c = a*(b*c), \ \forall a, b, c \in S}$

Associativity Property

i.e. binary opⁿ '$*$' must be associative

{Associativity property depends only on binary opⁿ}

Slide

Set N
w.r.t binary op^n '+'

	Algebraic Structure	Semi-Group	Monoid	Group	Abelian Group
(N,+)	✓	✓			
(N, .)	✓	✓			
(N,−)	$2-5=-3$ $-3\notin N$ X	X			
(N,÷)	$1\div 2=0.5\notin N$, X	X			
(Z,+)	✓	✓			
(Z, .)	✓	✓			
(Z,-)	✓	X			
(Z ,÷)	$1\div 2=0.5\notin Z$, X	X			
(Q,+)	✓	✓			
(Q, .)	✓	✓			
(Q, -)	✓	X			
(Q, ÷)	X $0\in Q$, & $\frac{p}{0}$ = Not defined	X			
(Q*, +)	$\frac{p}{q}+\left(\frac{-p}{q}\right)=0\notin Q^*$ X	X			
(Q*, .)	✓	✓			
(Q*, -)	$\frac{p}{q}-\frac{p}{q}=0\notin Q^*$ X	X			
(Q*,÷)	✓	X			

Q^* Set of all non-zero rational No.

Slide

Topic : Monoid

(i) closed
(ii) Associative

A semi group $(S, *)$ is called monoid

if there exist an element $e \in S$,

such that, $a * e = a$, $\forall a \in S$

and $e * a = a$

where 'e' is called identity element w.r.t. binary opⁿ '$*$'

i.e., identity element w.r.t. binary opⁿ '$*$' must be present in a Monoid

Slide

Set N

w.r.t binary opⁿ '+'

	Algebraic Structure	Semi-Group	Monoid	Group	Abelian Group
(N,+)	✓	✓	$0 \notin N$ ✗	← identity w.r.t. addition will be 0	
(N, .)	✓	✓	$1 \in N$ ✓	← identity w.r.t. multiplication will be '1'	
(N,−)	$2-5=-3$, $-3 \notin N$ ✗	✗	✗		
(N,÷)	$1 \div 2 = 0.5 \notin N$, ✗	✗	✗		
(Z,+)	✓	✓	$0 \in Z$, ✓		
(Z, .)	✓	✓	$1 \in Z$, ✓		
(Z,-) −	✓	✗	✗		
(Z, ÷) ÷	$1 \div 2 = 0.5 \notin Z$, ✗	✗	✗		
(Q,+)	✓	✓	$0 \in Q$, ✓		
(Q, .) .	✓	✓	$1 \in Q$, ✓		
(Q, -) −	✓	✗	✗		
(Q, ÷) ÷	✗ $0 \in Q$, & $\frac{p}{0}$ = Not defined	✗	✗		
(Q*, +)	$\frac{p}{q} + \left(-\frac{p}{q}\right) = 0 \notin Q^*$ ✗	✗	✗		
(Q*, .) .	✓	✓	$1 \in Q^*$, ✓		
(Q*, -) −	$\frac{p}{q} - \frac{p}{q} = 0 \notin Q^*$ ✗	✗	✗		
(Q*, ÷) ÷	✓	✗	✗		

Q^* Set of all non-zero rational No.

Slide

Topic : Group

i.e., (i) Closed
(ii) Associative
(iii) Identity element must be Present

A monoid $(S, *)$ is called group,

if, for each element $a \in S$
there exists an element $b \in S$
such that

$a * b = e$ (identity)

and

$b * a = e$

element a & b are called inverse of each other

In a group inverse of each element must exist

Slide

Set N

w.r.t binary opⁿ '+'

Q^* set of all non-zero rational No.

	Algebraic Structure	Semi-Group	Monoid	Group	Abelian Group
(N,+)	✓	✓	$0 \notin N$ ✗	✗	
(N, .)	✓	✓	$1 \in N$ ✓	✗ ← inverse does not exist for any element of the set (except for element '1')	
(N, −)	$2-5=-3$, $-3 \notin N$ ✗	✗	✗	✗	
(N, ÷)	$1 \div 2 = 0.5 \notin N$, ✗	✗	✗	✗	
(Z,+)	✓	✓	$0 \in Z$, ✓	✓ $x+(-x)=0$ (identity)	
(Z, .)	✓	✓	$1 \in Z$, ✓	✗ ← inverse does not exist for any other element of the set except for '1' & '−1'	
(Z, -)	✓	✗	✗	✗	
(Z , ÷)	$1 \div 2 = 0.5 \notin Z$, ✗	✗	✗	✗	
(Q,+)	✓	✓	$0 \in Q$, ✓	✓ $\left(\frac{p}{q}\right)+\left(-\frac{p}{q}\right)=0$ (identity)	
(Q, .)	✓	✓	$1 \in Q$, ✓	$0 \in Q$, ∴ Not a group ← inverse of '0' can never exist w.r.t binary opⁿ 'multiplication'	
(Q, -)	✓	✗	✗	✗	
(Q, ÷)	✗ $0 \in Q$, & $\frac{p}{0}$ = Not defined	✗	✗	✗	
(Q*, +)	$\frac{p}{q}+\left(-\frac{p}{q}\right)=0 \notin Q^*$ ✗	✗	✗	✗	
(Q*, .)	✓	✓	$1 \in Q^*$, ✓	$\frac{p}{q} \times \frac{q}{p} = 1$ (identity) ✓	
(Q*, -)	$\frac{p}{q} - \frac{p}{q} = 0 \notin Q^*$ ✗	✗	✗	✗	
(Q*, ÷)	✓	✗	✗	✗	

Slide

Topic : Abelian group / Commutative group

(i) closed, (ii) Associative, (iii) identity, (iv) inverse

A group $(S, *)$ is called an abelian group

if $\boxed{a * b = b * a \quad \forall a, b \in S}$

Commutative Property

$\downarrow$

Binary operation '$*$' must follow Commutative Property on elements of set.

Commutative Property depends on binary opⁿ as well as on type of elements on which opⁿ will be Performed

Slide

Set N

w.r.t binary opⁿ +

	Algebraic Structure	Semi-Group	Monoid	Group	Abelian Group
(N,+)	✓	✓	$0 \notin N$ ✗	✗	✗
(N, .)	✓	✓	$1 \in N$ ✓	✗	✗
(N,−)	$2-5=-3$ $-3 \notin N$ ✗	✗	✗	✗	✗
(N,÷)	$1 \div 2 = 0.5 \notin N$, ✗	✗	✗	✗	✗
(Z,+)	✓	✓	$0 \in Z$, ✓	✓	✓
(Z, .)	✓	✓	$1 \in Z$, ✓	✗	✗
(Z,-) −	✓	✗	✗	✗	✗
(Z , ÷) ÷	$1 \div 2 = 0.5 \notin Z$, ✗	✗	✗	✗	✗
(Q,+)	✓	✓	$0 \in Q$, ✓	✓	✓
(Q, .) .	✓	✓	$1 \in Q$, ✓	✗	✗
(Q, -) −	✓	✗	✗	✗	✗
(Q, ÷) ÷	✗ $0 \in Q$, & $\frac{p}{0}$ Not defined	✗	✗	✗	✗
(Q*, +)	$\frac{p}{q} + \left(-\frac{p}{q}\right) = 0 \notin Q^*$ ✗	✗	✗	✗	✗
(Q*, .) .	✓	✓	$1 \in Q^*$, ✓	✓ $\left(\frac{p}{q} \times \frac{q}{p} = 1 \in Q\right)$	✓
(Q*, -) −	$\frac{p}{q} - \frac{p}{q} = 0 \notin Q^*$ ✗	✗	✗	✗	✗
(Q*, ÷) ÷	✓	✗	✗	✗	✗

Q^* set of all non-zero rational No.

Slide

Topic : Note

In a group,

1. Identity element in the set is always unique.
2. Inverse of each element of the group exist and it is unique for each element

2 (a) if $inv(a) = b$, then $inv(b) = a$

2 (b) $(a^{-1})^{-1} = a$

3. $\underbrace{(a * b)^{-1} = b^{-1} * a^{-1}}$ $\forall a, b \in$ Group

It will always hold true irrespective of Commutative Property.

4. Inverse of identity element is always identity element itself.

Slide

Note :- A non-empty set S w.r.t. binary opⁿ '$*$' is a group if and only if, ① '$*$' is associative

and ② $\underbrace{a * b^{-1} \in S, \quad \forall a, b \in S}$

↳ This statement is enough for
(i) identity
(ii) inverse
(iii) Closure

Note :- A non-empty set S w.r.t. binary opn '$*$' is a group if and only if, (1) '$*$' is associative and (2) $a*b^{-1} \in S \quad \forall a,b \in S$.

(1) Identity

let $a \in S$

for $a, a \in S$ we know

$$\underbrace{a*a^{-1}}_{\downarrow} \in S$$

i.e., $e \in S$
(identity)

(2) Inverse :

If identity element is the only element of the set, then $inv(e) = e$ always holds

let $e, a \in S$ { i.e. set contains at least two element }

$$\therefore \underbrace{e*(a)^{-1}}_{\downarrow} \in S$$

$$\underbrace{a^{-1} \in S}_{\text{inverse exist for every element}}$$

(3) Closure Property :

we know if, $a, b \in S$ then $a^{-1}, b^{-1} \in S$

$\therefore$ if $a, b \in S$, then $a, b^{-1} \in S$

$\therefore$ we know $a*(b^{-1})^{-1} \in S$

i.e. $\underbrace{a*b \in S}$

$\therefore$ closed

#Q. Let $A = \{0, \pm 2, \pm 4, \pm 6, ...\}$

$B = \{0 \pm 1, \pm 3, \pm 5 .....\}$

Which of the following is not a semi- group

odd + odd = even {∴ Set B is not closed w.r.t. opⁿ addition}

A (A, +) → Closed ✓; + is associative ✓

B (A, •) → Closed ✓; Multiplication is associative ✓

C (B, +) → Closed ✗

D (B, •) → closed ✓; Associative ✓

Empty string is also included
ε or λ

#Q. Consider the set Σ^* of all strings over the alphabet $\Sigma = \{0, 1\}$. Σ^* with the concatenation operator for strings

A. Not a semigroup

B. Semi group but not a monoid

C. Monoid but not a group.

D. A group

Monoid

① Closed

② Associative

(0111 + 1011) + 011   0111 + (1011 + 011)

0111 1011 + 011   0111 + 1011 011

0111 1011 011 = 0111 1011 011

③ Identity (ε or λ)

0111 + ε = 0111

but not a group.

④ Inverse does not exist for any string
Except for empty string

determinant value is not zero

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

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.

Group
1. Closed ✓
2. Associative ✓
3. Identity (Identity Matrix)
4. Inverse ($\det(\text{Matrix}) \neq 0$ ∴ inverse will exist for every Matrix, it will also be a matrix of order $n \times n$)

5. Matrix Multiplication is not Commutative → Not Abelian

all functions on set S need not be bijective

#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.

A Not a semigroup

B Semi group but not a monoid

C Monoid but not a group.

D A group

Monoid

① closed $f_1 : S \to S$ & $f_2 : S \to S$ then $f_1 o f_2 : S \to S$ ∴ Closed

② Function Composition is associative

③ Identity function on set S will also belong to F(s) ∴ $f_1 : S \to S$, $f_1 \circ I_S = f_1$

but not a group

④ Every function on set S need not be bijective. ∴ Inverse need not exist for every element of set F(s).

#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

$a*b = \max(a,b)$

Semi-group { ① Closed ② Associative

③ Identity {does not exist}

$\therefore$ Not a Monoid

$\max(?, x) = x$

it must be the smallest integer → & it does not exist

A. Not a semigroup

B. Semi group but not a monoid

C. Monoid but not a group.

D. A group

#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, ∀, ∈ Group

(1) $a * e = a$

$$\frac{\cancel{a} \cdot e}{3} = \cancel{a}$$

$$\boxed{e = 3}$$

(2) $a * a^{-1} = e$

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

$$\boxed{(a)^{-1} = \frac{9}{a}}$$

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

True

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

K is

① Closed ✓ ③ Identity w.r.t addition $0 \in$ set

② Associative ④ Inverse $inv(+2k) = -2k$ . . and so on

False

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

① closed ✓

② Associative ✓

③ identity w.r.t multiplication '1' $\in$ set ✓

④ inverse does not exist for any element except for '1'

$inv(0.5) = 2 \notin$ set

True

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

$\{... 2^{-3}, 2^{-2}, 2^{-1}, 2^{0}, 2^{1}, 2^{2}, 2^{3}, ...\}$

① $2^p \times 2^q = 2^{p+q}$ if $p, q \in Z$ then $p+q \in Z$ ∴ closed

② Multiplication is associative ✓

③ $2^0 = 1 \in$ set ∴ identity is present

④ $2^p \times 2^{-p} = 2^0 = 1 =$ (identity) ∴ inverse exist for every element

D None of these

Topic : Finite Group

- A group with finite number of elements in the underlying set is called a finite group

- Let G is finite set and $(G, *)$ is a group.

Order of group $(G, *)$ is denoted by $O(G)$.
and it is defined as

$O(G) = |G| =$ No. of elements in set G

Topic : Finite Group

eg. $\{0\}$ is a finite group of order = '1' w.r.t. binary opⁿ addition.

eg. $\{1\}$ is a finite group of order = '1' w.r.t. binary opⁿ multiplication

eg. $\{1, -1\}$ is a finite group of order = '2' w.r.t. binary opⁿ multiplication

Above three groups are the only finite groups of real numbers w.r.t. addition and/or Multiplication

Note: If 'e' is the identity element w.r.t. any binary operation '$*$', then

$\{e\}$ is always a finite group of order = 1, w.r.t binary opⁿ '$*$'.

Note: In any finite group of order = '2'

every element is inverse of itself.

Topic : Finite Group

Cube root of unity are.
$1, \omega, \omega^2$

The set of Cube roots of unity i.e., $\{1, \omega, \omega^2\}$ form a finite group of order = 3 w.r.t. multiplication

we know, $\boxed{\omega^3 = 1}$

1. Closed ✓
2. Associative ✓
3. Identity $1 \in$ Set ✓
4. Inverse ✓

Inverse :- inverse exist for every elemen

$inv(1) = 1$

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

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

Multiplication Composition table

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

Topic : Finite Group

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

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

We know, $\boxed{i^2 = -1}$

1. Closed ✓
2. Associative ✓
3. Identity '1' ∈ Set ✓
4. Inverse: $\text{inv}(1) = 1$, $\text{inv}(-1) = -1$, $\text{inv}(i) = -i$, $\text{inv}(-i) = i$

inverse exist for every element

Multiplication →

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

Note: The set of n^{th} roots of unity will form a finite group of order $= n$, w.r.t. multiplication

Topic : Addition modulo 'm' $\oplus_m$

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

$$a \oplus_m b = \begin{cases} a+b, & \text{if } (a+b) < m \\ r, & \text{otherwise, where 'r' is remainder obtained on dividing } (a+b) \text{ by } m. \end{cases}$$

$\equiv (a+b) \% m$

$$\boxed{\begin{aligned} 2 \oplus_7 3 &= 5 \\ 4 \oplus_7 5 &= 2 \end{aligned}}$$

Topic : Multiplication modulo 'm' $\otimes_m$

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

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

Where r is the remainder obtained on dividing $(a \cdot b)$ by m

$\equiv (a \cdot b) \% m$

$2 \otimes_7 3 = 6$

$4 \otimes_7 5 = 6$

2 mins Summary

Topic — Practice questions

Topic — Finite group

Topic — Addition modulo 'm' $\oplus_m$

Topic — Multiplication modulo 'm' $\otimes_m$

Slide

THANK - YOU

Slide