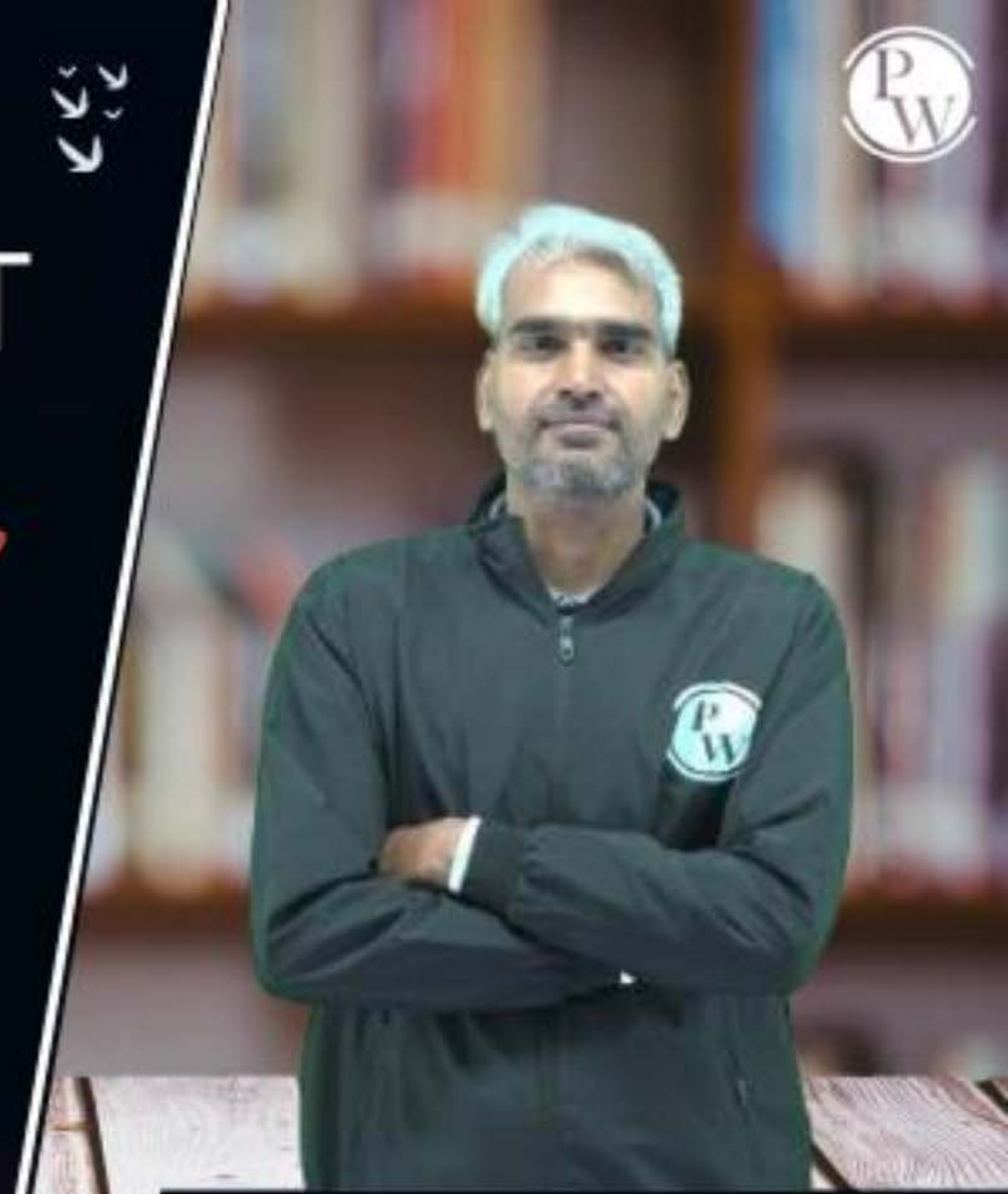
Computer Science & IT

Discrete Mathematics

Set Theory & Algebra

Lecture No. 18



By- Vishal Sir

Recap of Previous Lecture

- Topic: Inverse of a function
- Topic: Identity function
- Topic: Constant function
- Topic: Identical function
- Topic: Function composition

Slide

Topics to be Covered

Group Theory

- **Topic** Introduction to group theory
- **Topic** Algebraic structure
- **Topic** Semi-group
- **Topic** Monoid
- **Topic** Group
- **Topic** Abelian group / Commutative group

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

 / 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

	Algebraic Structure	Semi-Group	Monoid	Group	Abelian Group
(N,+)	✓				
(N, .)	✓				
(N,−)	$2-5=-3$ $-3\notin N$ ✗				
(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 opⁿ '+'

	Algebraic Structure	Semi-Group	Monoid	Group	Abelian Group
(N,+)	✓	✓			
(N, .)	✓	✓			
(N,−)	$2-5=-3$ $-3\notin N$ ✗	✗			
(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*, ÷) ÷	✓	✗			

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

Slide

Topic : Monoid

(i) closed
(ii) Associative

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

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

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

and $e * a = a$

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

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

Slide

	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*,÷) ÷	✓	✗	✗		

Set N

w.r.t binary op" + "

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

$$a * b = e \text{ (identity)}$$

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 '+'

	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*,÷) ÷	✓	✗	✗	✗	

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

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

↓

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

Commutative Property depends on binary op^n as well as on type of elements on which op^n will be Performed

Slide

Set N

w.r.t binary op^n +

	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*, .)	✓	✓	$1 \in Q^*$, ✓	✓	✓
(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) $a * b^{-1} \in S, \ \forall a, b \in S$

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

$\underbrace{a*a^{-1}}_{\text{i.e., } e \in S} \in S$

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 }

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

$a^{-1} \in S$

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. $\underbrace{a*b \in S}_{\therefore \text{ closed}}$

$\therefore$ closed

H.W.

#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

A $(A, +)$

B $(A, \bullet)$

C $(B, +)$

D $(B, \bullet)$

H.W.

#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

H/W.

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 $\langle A, * \rangle$ is not a semigroup

B) $\langle A, * \rangle$ is a semigroup but not a monoid.

C) $\langle A, * \rangle$ is a monoid but not a group.

D) $\langle A, * \rangle$ is a group but not an abelian group.

H.W.

#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

H.W.

#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. Not a semigroup

B. Semi group but not a monoid

C. Monoid but not a group.

D. A group

H.W.

#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

H.W.

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

K is

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

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

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

D None of these

2 mins Summary

- **Topic** Introduction to group theory
- **Topic** Algebraic structure
- **Topic** Semi-group
- **Topic** Monoid
- **Topic** Group
- **Topic** Abelian group / Commutative group

Slide

THANK - YOU

Slide