Property of set represented 10|02|2023

as $\langle S, \cdot \rangle$

$\cdot \rightarrow$ property / relation

① closure → Algebric structure / Grupoid

② Associativity → Semi Group

③ Identity element → monoid

④ Inverse → Group

⑤ Commutative → Abelian Group

N = Set of Natural numbers

W = Set of whole numbers

R = Set of real numbers

Q = Set of rational numbers

C = Complex numbers

Cyclic Algebric Structure

a^n

Cyclic group

A group $\langle G, \cdot \rangle$ is called a cyclic group if for some $a \in G$ every element in G is of the form a^n where n is same integer

The element 'a' is called generated element of G.

①

Q: Prove that $S = \{1, -1, i, -i\}$ form a multiplicative cyclic group!

Composition table

$*$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

i) Closure – all elements in the table belongs to S

↳ Closed

ii) Associative –

$1 \times (i \times -1) = (1 \times i) \times -1$

$-i = -i$

iii) Identity :

$e \times a = a \times e = a \quad \forall a \in S$

$\therefore e = 1$

iv) Inverse :

Inverse of 1 is 1

" -1 is -1

" i is $-i$

" $-i$ is i

$\therefore \langle S = \{1, -1, i, -i\}, * \rangle$ is a cyclic group.

Generator element

$(-i)^1 = -i$

$(-i)^2 = -1$

$(-i)^3 = +i$

$(-i)^4 = 1$

As $-i$ is a generator element.

$\therefore$ The given set 'S' forms a multiplicative cyclic group.

H/W

Q: $S = \{1, \omega, \omega^2\}$

$\omega = \sqrt[3]{1}$

② Prove that the group $\langle Z, +_5 \rangle$ is a cyclic group. ↳ Addition modulo 5

Sol: $a \equiv b \pmod{n}$

$\mathbb{Z} = \{0, 1, 2, 3, 4\}$

ⓐ Closure ↳ reminder modulo 5.

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(b) Associativity :

$a+(b+c) = (a+b)+c$

$\forall\, a,b,c \in Z$

(c) Identity : $0+a = a$

(d) Inverse : (mod 5)

$0+0=0$

$1+4=0$

$2+3=0$

$3+2=0$

$4+1=0$

$\therefore$ Inverse exists for all $a \in S$.

(e) Generator element

$1 = 1 \pmod 5$

$1+1 = 2 \pmod 5$

$1+1+1 = 3 \pmod 5$

$1+1+1+1 = 4 \pmod 5$

$1+1+1+1+1 = 0 \pmod 5$ ↳ remainder

(3) $\langle S = \{1, 2, 3, 4\}, *_5 \rangle$

Composition table

$*_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Generator element :

$2 = 2 \pmod 5$

$2\times2 = 4$

$2\times2\times2 = 3$

$2\times2\times2\times2 = 1$

$3 = 3 \pmod 5$

$3\times3 = 4$

$3\times3\times3 = 2$

$3\times3\times3\times3 = 1$

$\therefore$ 2 & 3 are generator elements

Note : We can have more than one generator elements in a cyclic group.

Theorem :

i) Every cyclic group is abelian group

ii) If 'a' is a generator element in G then 'a^{-1}' also a generator of G.

Eg: $<\{1,2,3,4\}, \times_5>$

Inverse of 2 is 3

$2 \times 3 \pmod 5 = 1$

2 is generator

$\therefore$ 3 is also generator

Lagrange's Theorem

Order of a group = O(G)

= no. of element in set G.

→ The order of each sub-group of a finite group is a divisor of the order of the group.

Eg: $G = <\{1,-1,i,-i\}, *>$

G - is a group

$S = <\{1,-1\}, *>$

S - is a subgroup

$|G| = 4$

$|S| = 2$

Lagrange Theorem

$|G| / |S|$

$4/2$

Ring:

- An Algebric System $<R,+,\cdot>$ is called a ring if:

i) $<R,+>$ is an abelian group

ii) $<R,\cdot>$ is a semigroup

iii) The '$\cdot$' operation is distributive over '+' operation.

$a\cdot(b+c) = (a\cdot b)+(a\cdot c)$

$\forall a,b,c \in R$

Eg: $<\mathbb{Z},+,\cdot>$

$<\mathbb{Z},+>$ → abelian group

$<\mathbb{Z},\cdot>$ → Semi group

$4*(5+6) = (4*5)+(4*6)$

↳ distribution over addition

$\therefore <\mathbb{Z},+,\cdot>$ is a Ring

Commutative Ring

if Commutative Property is satisfied by both '+' and '.' on the elements then it is a Commutative Ring.

Ring with zero divisor

Let R be a ring and $0 \neq a, b \in R$. R is called ring with zero divisor if $a.b=0$ is true for some nonzero a and b

Eg: $R = \{0,1,2,3,4,5\}$

$\langle R, +_6, \cdot_6 \rangle$

$2 \cdot_6 3 = 0$

Ring without zero divisor

A ring R is called ring without zero divisor if whenever $a.b=0$

$\Rightarrow$ either $a=0$ (or) $b=0$

Integral Domain

R is a Commutative Ring

R has no zero division

then R is a Integral Domain

Field:

$\langle F, +, \cdot \rangle$ is called a field if the following conditions are satisfied:

1. $\langle F, + \rangle$ — abelian group
2. $\langle F', \cdot \rangle$ — is an abelian group

where $F' = \{x \in F \mid x \neq 0\}$

3. $a.(b+c) = (a.b)+(a.c)$ $\forall a, b, c \in F$

$F' \rightarrow$ set without zero.

Question: Check wheather the following is group / field / ring.

$\langle Q, +, \cdot \rangle$

Sol: i) $\langle Q, + \rangle$ = abelian group

ii) $\langle Q', \cdot \rangle$ = abelian group

$Q' = Q - \{0\}$

iii) $a \cdot (b+c) = (a.b)+(a.c)$

$\forall a, b, c \in F$

$\therefore$ 3 Conditions are satisfied it is field