Group theory

Algebric structures :-

1) Carrier of Algebra : on which underlying set we are going to work.

2) Operations defined on carrier.

3) Distinguished element / special elements : e

Z → set

* → generic operator

→ Identity element : to perform unity identity element we get the same element back.

0 → addition's identity element.

$\forall a \in Z, e \in Z$

let $a * e = a$

$e * a = a$

→ Inverse element : to perform unity & inverse element we get are identity element.

$\forall a \in Z, \exists a' \in Z$

$a * a' = e$

$a' * a = e$

Z → integers

Semi-group :- It should satisfy the following axioms.

$< S, * >$ (non-empty set, * → binary operation)

(1) closed under the operation *. [closure property]

eg. $S = \{ x \mid 1 \le x \le 20 \}$.

$\forall a, b \in S$, $a * b \in S$

if $* = +$ 20, 2 $20 + 2 = 22$ ✗ (not closed).

if $S = Z$.

if $* = +$ $+$ ✓ (closed)

(2) Binary operation should have associative property

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

$(a * b) * c = a * (b * c)$.

$[Z, + >$, $< Z, *>$ → multiplication.

Monoid :- It satisfy axioms of semi-group and one more axiom :

(3) Existence of Identity ele. $e \in S$.

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

$e * a = a$.

eg. $< Z, + >$

0 → identity element.

$< Z, * >$ $e = 1$.

Group :- It satisfies axioms of monoid. with one more axiom

(4) Existence of inverse element.

$\forall a \in S, \exists a' \in S, \quad a * a' = e$
$a' * a = e$

eg:- $\langle Z, + \rangle$ $\forall a, \exists (-a)$

$\langle Z, * \rangle$ Not a group but a semi-group & monoid.

as $1/a$ is a real number.

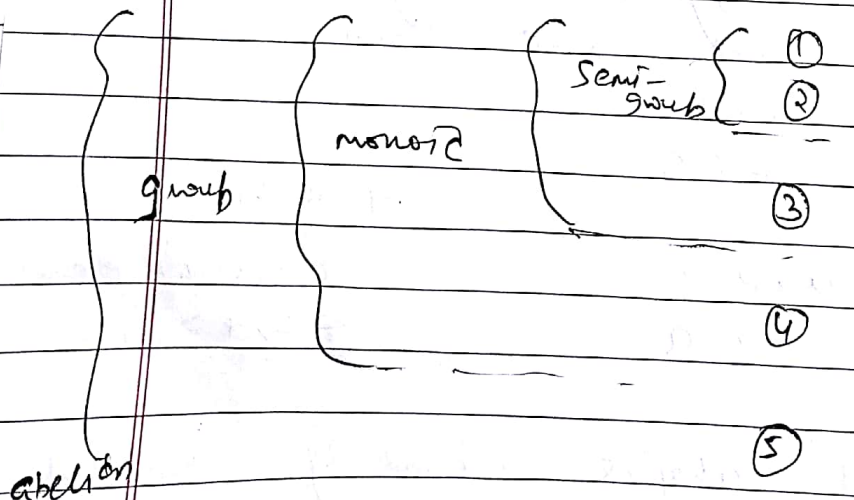
Abelian group :- It satisfy axioms of group with one more axiom

(5) Commutative property

$\forall a, b \in S$
$a * b = b * a$

Finite group :- finite no. of elements

Infinite group :- Infinite no. of elements



Q. Let a group G be a set of all non-zero real no., let $a * b = \frac{ab}{2}$

$\langle G, * \rangle$

show it's a abelian group.

$G = R^+$

(1) $\forall\ a, b \in G \quad a * b = \frac{1}{2}ab \in G$. closure property.

(2) $(a * b) * c = a * (b * c)$

$\left(\frac{1}{2}ab\right) * c = a * \left(\frac{1}{2}bc\right)$ associative property.

$\frac{1}{4}abc = \frac{1}{4}abc$.

(3) $a, e \in R$.

$a * e = \frac{ae}{2} = \frac{1}{2}a(2) = a$.

$e = 2$ identity element

(4) $a * a' = e$

$\frac{1}{2}aa' = 2$

$\frac{1}{2}a\left(\frac{4}{a}\right) = 2$ $\quad a' = 4/a$ inverse element

(5) $a * b = b * a$

$\frac{1}{2}ab = \frac{1}{2}ba$ Commutative property.

[ ] → equivalence class.

$[13]_6 = [1]_6$

Additive group mod n :- [Addition modulo n operation]

$\langle Z_n, + \rangle$

$a = a' \bmod n$

$b = b' \bmod n$

$a + b = a' + b' \pmod n$

$[a_n] + [b_n] = [a+b]_n$

eg. $\langle Z_6, + \rangle$

$[0]_6 = \{\ldots -12, -6, 0, 6, 12, \ldots\}$

$[1]_6 = \{\ldots -11, -5, 1, 7, 13 \ldots\}$

$[2]_6 = \{\ldots -10, -4, 2, 8, 14 \ldots\}$

$[3]_6 = \{\ldots -9, -3, 3, 9, 15 \ldots\}$

$[4]_6 = \{\ldots -8, -2, 4, 10, 16, \ldots\}$

$[5]_6 = \{\ldots -7, -1, 5, 11, 17 \ldots\}$

$[13]_6 + [-4]_6 = [13-4]_6$

$[0]_6$

$1 + 2 = [9]_6$

$3 = 3.$

Cayley table :

Cayley table for $<Z_6, +>$

Z_6	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Identity element = 0.

inverse elem of 5 : 1
1 : 5

multiplicative group model n $<Z_n^*, \cdot)$
or
$\in Z_n^*, \times)$
multiplicative.

$<Z_5^*, \cdot)$

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

0 not taken as multiplicative inverse as 0 doesn't exist

$ax = 1 \bmod n$.
↳ multiplicative inverse.

$3x = 1 \bmod 5$
$x = 2$ is a multiplicative inverse of 3.

If n = prime no, it is a multiplicative group.

$x = -3$ also etc,
(multiple multiplicative inverse exists)

$\langle Z_{12}^{*}, a \rangle$ → can be a group,
only when then the elements are co-prime to 12.

$= \{1, 5, 7, 11\}$ (for each group table or not?)

$\langle Z_6^{*}, \cdot \rangle \rightarrow \{1, 5\}$ Coprime to 6.

Sub-group :→

Let G be a group, H is subset of G ($H \subseteq G$) we say that (H) is a group under binary operation ($*$), then we call it as a sub-group of G.

Just enough to checks closure & inverse property

$\langle G, * \rangle$ be a group under binary operation '$*$' with 'e' as its identity element.

$H \subseteq G$ if $\exists a \in G$, the group can be generated using the integral powers of an ele 'a'. then that group is called as cyclic group, and a is called as generator of the group.

$a^n = a \cdot a \cdot a \ldots a$ (n times) → operation n times.

after doing this if we get whole group G back then it's a cyclic group.

$G = \langle Z_6, + \rangle = \{0, 1, 2, 3, 4, 5\}$

$0^0 = 0 \bmod 6 = 0$ | $1^0 = 0 \bmod 6 = 0$

$0^1 = 0 \bmod 6 = 0$ | $1^1 = 1 \bmod 6 = 1$

$0^2 = 0 \bmod 6 = 0$ | $1^2 = (1+1) \bmod 6 = 2$

⋮ | $1^3 = (1+1+1) \bmod 6 = 3$

$0^5 = 0 \bmod 6 = 0.$ | $1^4 = (1+1+1+1) \bmod 6 = 4$

| $1^5 = (1+1+1+1+1) \bmod 6 = 5$

{0} subgroup

G is a cyclic group, and 1 is generator

$2^0 = 0$
$2^1 = 2$
$2^2 = 4$
$2^3 = 6 \bmod 6 = 0$
$2^4 = 8 \bmod 6 = 2$
$2^5 = 4$

0 2 4 repeats.

$4^0 = 0$
$4^1 = 4$
$4^2 = 2$ } repeat here 1 0 2 0 try subset to check
$4^3 = 0$
$4^4 = 4$
$4^5 = 2$

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

{0, 2, 4} subgroup ↗ as closure & inverse exists.

$3^0 = 0$ $3^1 = 3$
$3^2 = 0$ $3^3 = 3$
$3^4 = 0$ $3^5 = 3$

$+_6$	0	3
0	0	3
3	3	0

{0, 3} subgroup.

$5^0 = 0$
$5^1 = 5$
$5^2 = 4$
$5^3 = 3$
$5^4 = 2$
$5^5 = 1$

$5^6 = 0$
$5^7 = 5$

5 is also a generator.

sub-groups = {0}, {0, 3}, {0, 2, 4}, {0, 1, 2, 3, 4, 5}

if it is an abelian group ⇒ left co-set = right co-set

Left coset & Right cosets: For a group G, Let $\langle G, * \rangle$ be a group & $(H, *)$ be a sub-group.

For any $a \in G$, the set aH is called left co-set & the set Ha is called Right coset.

$$aH = \{ a * h \mid \forall h \in H \}$$

$$Ha = \{ h * a \mid \forall h \in H \}.$$

$$\langle G, * \rangle = a_1H \cup a_2H \cdots \cup a_kH.$$

$$a_1H \cap a_2H \cap \cdots \cap a_kH = \phi.$$

Co-set decomposition are the elements whose coset union gives G.

Q) $G = \langle Z_{12}, + \rangle$

$H = \{ [0], [4], [8] \}$ of G.

And all left-cosets of H & G & also obtain corresponding co-set decomposition.

Ans $\langle Z_{12}, + \rangle = \{ [0], [1], [2], \ldots [11] \}$

	H		
	0	4	8
0	0	4	8
4	4	8	0
8	8	0	4

0 4 8

left coset

$[0]+H = \{[0]+[0], [0]+[4], [0]+[8]\}$

$= \{[0], [4], [8]\}$ 0H

coset decomposition

$[1]+H = \{[1]+[0], [1]+[4], [1]+[8]\}$

$= [[1], [5], [9]]$ 1H

$[2]+H = \{[2], [6], [10]\}$ 2H

$[3]+H = [[3], [7], [11]]$ 3H

$[4]+H = [[4], [8], [0]]$ 4H

$[5]+H = \{[5], [9], [1]\}$ 5H

$[6]+H = \{[6], [10], [2]\}$ 6H

coset decomposition

$[7]+H = \{[7], [11], [3]\}$ 7H

$[8]+H = \{[8], [0], [4]\}$ 8H

$[9]+H = \{[9], [1], [5]\}$ 9H

$[10]+H = \{[10], [2], [6]\}$ 10H

$[11]+H = \{[11], [3], [7]\}$ 11H

coset decomposition

$0H \cup 1H \cup 2H \cup 3H = G$ $0H \cap 1H \cap 2H \cap 3H = \phi$

Illy $4H \cup 5H \cup 6H \cup 7H = G$ $4H \cap 5H \cap 6H \cap 7H = \phi$

Illy $8H \cup 9H \cup 10H \cup 11H = G$ $8H \cap 9H \cap 10H \cap 11H = \phi$

$|H| = |aH| = |Ha|$ → same cardinality

One to one correspondence from element of subgroup to element of left coset.

Scanned by CamScanner

Lagrange's theorem :-

if $\langle G, * \rangle$ is a finite group & let $\langle H, * \rangle$ be the sub-group of G then the order of H divides the order of G (Cardinality)

Let $Ha_1, Ha_2, \ldots Ha_r$ be distinct right cosets of H in G. (r cosets)

Rule of right coset decomposition,

$$G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_r$$

$$O(G) = O(Ha_1) + O(Ha_2) + \cdots + O(Ha_r)$$

Cardinality or order

we know that

$$O(Ha_1) = O(Ha_2) = \cdots = O(H_{a_r})$$

$$O(G) = r * O(H)$$

$$r = O(G) / O(H).$$

Q. Let G be a group with sub-group H & K, if cardinality of G is 660, cardinality of K is 66. What are possible value of cardinality of H.

$K \leq H \leq G$

Proof

$$|G| = r_1 |H|$$

$$|H| = r_2 |K|$$

classmate
Date
Page

$660 = r_1 |H|$

$|H| = r_2\ 66$

$r_1 r_2 = 10$

$660 = r_1 r_2\ 66$

$r_1 r_2 = 10$

$r_1, r_2 : \{(1, 10)$

$= (10, 1)$

$= (2, 5)$

$= (5, 2)$

$660 = r_1 (11)$

$|H| = \frac{660}{r_1}$

$|H| = \{660, 66, 330, 132\}$