CS & IT ENGINEERING

DISCRETE MATHS
SET THEORY

Lecture No. 14

By- SATISH YADAV SIR

TOPICS TO BE COVERED

01 Algebraic structures

02 Semi Group

03 Monoid

04 Group

GROUP THEORY

Group.

$(G, *)$

1) closed $a \in G$. $b \in G$. $a * b \in G$.

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

3) Identity: $a * e = a$ 4) Inverse: $a * a^{-1} = e$.

GROUP THEORY

$(Z, +)$ ✓

1) closed.
2) Associative
3) identity: $a+0=a$ $(e=0)$ (unique)
4) Inverse: $a * a^{-1} = e$.

$2+(-2)=0$

$(Z, \times)$ → not Group.

1) closed.
2) Associative.
3) Identity:

$a \times I = a$.

4) Inverse:

$a \times \frac{1}{a} = 1$.

GROUP THEORY

$(Q, \times)$ $\quad$ $(Q \neq 0, \times) \to$ Group.

1) closed.

2) Associative.

3) $a \times 1 = a$ ($\overset{1}{\text{identity}}$)

4) $a \times \frac{1}{a} = 1$ $(a = 0)$

GROUP THEORY

Group

Infinite Groups:

$(\mathbb{Z}, +)$

$(\mathbb{Q} \neq 0, \times)$

finite Group:

$(\{1, \omega, \omega^2\}, \times)$

$(\{1, i, -i, -1\}, \times)$

GROUP THEORY

Cayley table

$*$	e_1	e_2	$\dots$
e_1			
e_2			
$\vdots$			

$$\omega^3 = 1.$$

$$(\{1, \omega, \omega^2\}, \times)$$

$\times$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$$\omega^2 \times 1 = \omega^2$$

1) closed.
2) Associative.
3) identity
4) Inverse.

$$1' = 1$$
$$\omega' = \omega^2$$
$$\omega^{2'} = \omega$$

GROUP THEORY

f_1	f_2	f_3	f_4	f_5	f_6
$1 \to 1$	$1 \to 1$	$1 \to 2$	$1 \to 2$	$1 \to 3$	$1 \to 3$
$2 \to 2$	$2 \to 3$	$2 \to 1$	$2 \to 3$	$2 \to 1$	$2 \to 2$
$3 \to 3$	$3 \to 2$	$3 \to 3$	$3 \to 1$	$3 \to 2$	$3 \to 1$

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1						
f_2						
f_3						
$\vdots$						

$f_4 \circ f_5 = f_1$

$2 - \quad 1 - 2$
$3 - \quad 2 - 3$
$1 - \quad 3 - 1$

$\underbrace{}_{f_4}$

$= 1 - 1$
$2 - 2$
$3 - 3$

$(3, 1, 2)$

GROUP THEORY

$$\left(\{0, 1, 2, 3, 4, 5\} \ \oplus_6 \right)$$

$\oplus_6$	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	[illegible]	[illegible]

1) closed ✓
2) Associative ✓
3) identity ✓
4) Inverse.

$0' = 0$ $\quad$ $4' = 2$

$1' = 5$ $\quad$ $5' = 1$

$2' = 4$

$3' = 3$

GROUP THEORY

$\oplus_6$	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		

$(G, *)$ Group

Subgroup:

H is called subgroup of G.

1) $H \subseteq G$.

2) H should also satisfy.

   A) Closed.

   B) Associative.

   C) identity.

   D) Inverse.

GROUP THEORY

$\{\{0,1,2,3,4,5\}, \oplus_6\}$

$H = \{1, 3, 5\}$

$\oplus_6$	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		

1) $H \subseteq G$ ✓

not subgroup. coz, identity element is absent

2)

GROUP THEORY

$\{\{0, 1, 2, 3, 4, 5\}, \oplus_6\}$

$\oplus_6$	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	[illegible]	[illegible]

$H = \{0, 3, 5\}$.

1) $H \subseteq G$ ✓

2) closed.

not closed.

not Group.

not subgroup.

GROUP THEORY

$\{\{0, 1, 2, 3, 4, 5\}, \oplus_6\}$

$\oplus_6$	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	[illegible]	[illegible]

$H = \{0, 2, 4\}$

1) $H \subseteq G$

2) H is also Group

	0	2	4
0	0	2	4
2	2	0	4
4	4	0	2

GROUP THEORY

Thm : if H is subgroup of G, then $\frac{|G|}{|H|}$. (viceversa is not True).

$H = \{0, 2, 4\}$ $|G| = 6$

H is subgroup of G. $\longrightarrow \frac{|G|}{|H|} \rightarrow \frac{6}{3}$

$|H| = 3$

$H_1 = \{1, 3, 5\}$

GROUP THEORY

Every Group contain 2 Trivial ~~Sub~~group.

1) $e \subseteq G$.

2) $G \subseteq G$.

$$\begin{array}{c|c} * & e \\ \hline e & e \end{array}$$

closed.
Asso
identity $e * e = e$
inverse $e * e = e$.

GROUP THEORY

if $|G| = 84$, then what will be manimime size of $\boxed{\text{sub}}$group. → 84.

— ,, — size of $\boxed{\text{proper sub}}$group. → 42.

GROUP THEORY

G be group with subgroup H & K. $|G| = 660$

$|K| = 66$

what are the possible values of H.

$K \subset H \subset G$

$\downarrow \quad \downarrow \quad \downarrow$

$66 \qquad\qquad 660$

$66. \quad \begin{cases} 66\times 2 \\ \text{OR} \\ 66\times 5 \end{cases} \quad 66\times 10.$

$K \subseteq H \subseteq G.$

$\downarrow \quad \downarrow \quad \downarrow$

$66 \quad \begin{cases} 66 \\ 66\times 2 \\ 66\times 5 \\ 66\times 10. \end{cases} \quad 660.$

GROUP THEORY

$\oplus_6$	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	[illegible]	[illegible]

$a^1 = a$

$a^2 = a * a$

$a^3 = \underline{a * a} * a$

$a^2 * a$

$= a^3$

$a^4 = \underline{a * a * a} * a$

$a^3 * a$

$= a^4$

GROUP THEORY

$\oplus_6$	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	[illegible]	[illegible]

Subgroup of cyclic Group is also cyclic Group.

$2^1 = 2$

$2^2 = 2 \oplus_6 2 = 4$

$2^3 = \underline{2 \oplus_6 2} \oplus_6 2 = 0$

$4 \oplus_6 2$

$= 0$

$\{0, 2, 4\}$

subgroup

$2^4 = 0 \oplus_6 2 = 2$

2 has generated $\{0, 2, 4\}$

$\langle 2 \rangle = \{0, 2, 4\}$

GROUP THEORY

$\oplus_6$	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	[illegible]	[illegible]

$3^1 = 3$

$3^2 = 3 \oplus_6 3 = 0$

$3^3 = 0 \oplus_6 3 = 3$

$\langle 3 \rangle = \{0, 3\}$

GROUP THEORY

$\oplus_6$	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		

$1^1 = 1$

$1^2 = 1 \oplus_6 1 = 2$

$1^3 = 2 \oplus_6 1 = 3$

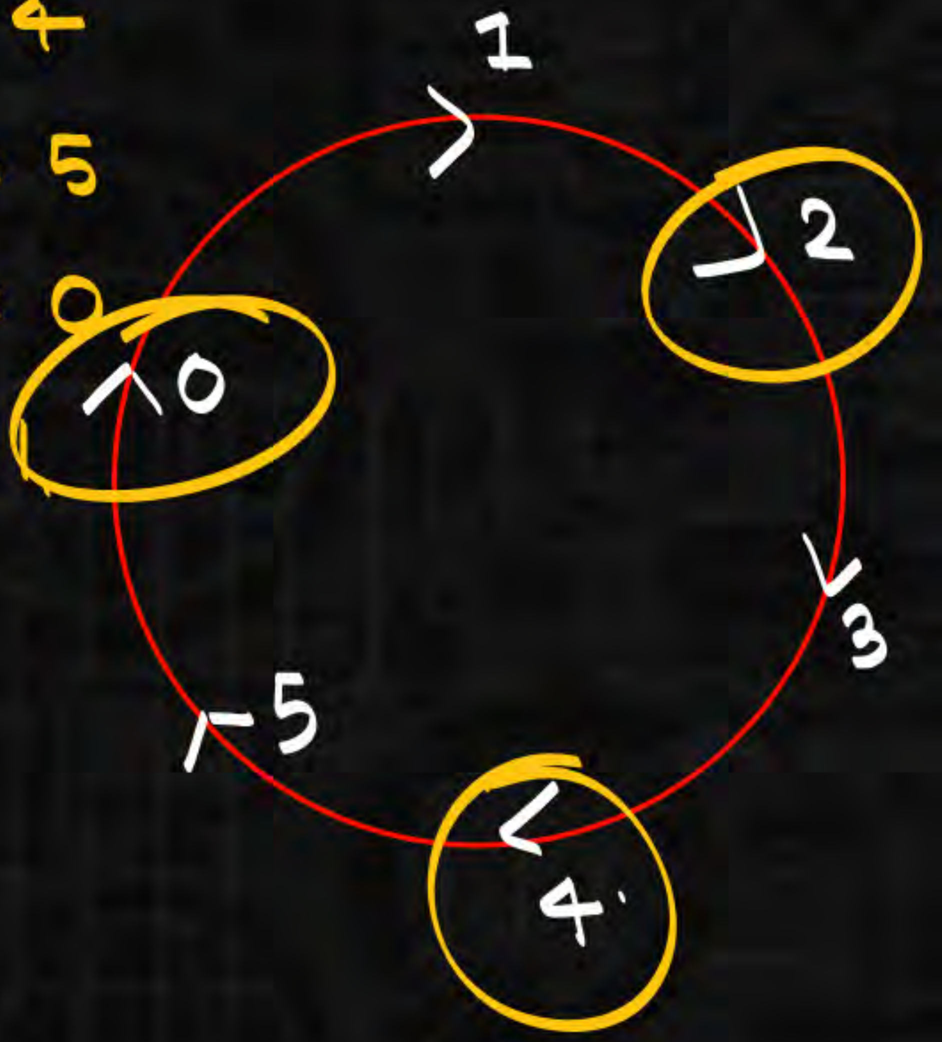
$1^4 = 3 \oplus_6 1 = 4$

$1^5 = 4 \oplus_6 1 = 5$

$1^6 = 5 \oplus_6 1 = 0$

$1^7 = 0 \oplus_6 1 =$

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



GROUP THEORY

$\oplus_6$	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

$5^1 = 5$

$5^2 = 5 \oplus_6 5 = 4$

$5^3 = 4 \oplus_6 5 = 3$

$5^4 = 3 \oplus_6 5 = 2$

$5^5 = 2 \oplus_6 5 = 1$

$5^6 = 1 \oplus_6 5 = 0$

$5^7 = 0 \oplus_6 5 = 5$

$1^1 = 5$

1 has generated every element in the Group.

1 is called Generator.

Group → Generator → cyclic Group.

GROUP THEORY

Group + commutative = Abelian Group.

Closed	Associative	identity	Inverse.

Closed → Algebric structure

semigroup

monoid

Group.

a) $\{-1, 1\}$ under multiplication

b) $\{-1, 1\}$ under addition

c) $\{-1, 0, 1\}$ under addition

d) $\{10n \mid n \in \mathbf{Z}\}$ under addition

e) The set of all one-to-one functions $g: A \to A$, where $A = \{1, 2, 3, 4\}$, under function composition

f) $\{a/2^n \mid a, n \in \mathbf{Z}, n \geq 0\}$ under addition

(a) Yes. The identity is 1 and each element is its own inverse.
(b) No. The set is not closed under addition and there is no identity.
(c) No. The set is not closed under addition.
(d) Yes. The identity is 0; the inverse of $10n$ is $10(-n)$ or $-10n$.
(e) Yes. The identity is 1_A and the inverse of $g: A \to A$ is $g^{-1}: A \to A$.
(f) Yes. The identity is 0; the inverse of $a/(2^n)$ is $(-a)/(2^n)$.

4. Let $G = \{q \in \mathbf{Q} \mid q \neq -1\}$. Define the binary operation $\circ$ on G by $x \circ y = x + y + xy$. Prove that $(G, \circ)$ is an abelian group.

5. Define the binary operation $\circ$ on $\mathbf{Z}$ by $x \circ y = x + y + 1$. Verify that $(\mathbf{Z}, \circ)$ is an abelian group.

(i) For all $a, b, c \in G$,
$(a \circ b) \circ c = (a + b + ab) \circ c = a + b + ab + c + (a + b + ab)c = a + b + ab + c + ac + bc + abc$
$a \circ (b \circ c) = a \circ (b + c + bc) = a + b + c + bc + a(b + c + bc) = a + b + c + bc + ab + ac + abc.$
Since $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$ it follows that the (closed) binary operation is associative.
(ii) If $x, y \in G$, then $x \circ y = x + y + xy = y + x + yx = y \circ x$, so the (closed) binary operation is also commutative.
(iii) Can we find $a \in G$ so that $x = x \circ a$ for all $x \in G$?
$x = x \circ a \Longrightarrow x = x + a + xa \Longrightarrow 0 = a(1 + x) \Longrightarrow a = 0$, because x is arbitrary, so 0 is the identity for this (closed) binary operation.
(iv) For $x \in G$, can we find $y \in G$ with $x \circ y = 0$? Here $0 = x \circ y = x + y + xy \Longrightarrow -x = y(1 + x) \Longrightarrow y = -x(1 + x)^{-1}$, so the inverse of x is $-x(1 + x)^{-1}$.
It follows from (i) - (iv) that $(G, \circ)$ is an abelian group.

Since $x, y \in \mathbf{Z} \Longrightarrow x + y + 1 \in \mathbf{Z}$, the operation is a (closed) binary operation (or $\mathbf{Z}$ is closed under $\circ$). For all $w, x, y \in \mathbf{Z}$, $w \circ (x \circ y) = w \circ (x + y + 1) = w + (x + y + 1) + 1 = (w + x + 1) + y + 1 = (w \circ x) \circ y$, so the (closed) binary operation is associative. Furthermore, $x \circ y = x + y + 1 = y + x + 1 = y \circ x$, for all $x, y \in \mathbf{Z}$, so $\circ$ is also commutative. If $x \in \mathbf{Z}$ then $x \circ (-1) = x + (-1) + 1 = x [= (-1) \circ x]$, so -1 is the identity element for $\circ$. And finally, for each $x \in \mathbf{Z}$, we have $-x-2 \in \mathbf{Z}$ and $x \circ (-x-2) = x + (-x-2) + 1 = -1 [= (-x-2) + x]$, so $-x-2$ is the inverse for x under $\circ$. Consequently, $(\mathbf{Z}, \circ)$ is an abelian group.

8. For any group G prove that G is abelian if and only if $(ab)^2 = a^2b^2$ for all $a, b \in G$.

9. If G is a group, prove that for all $a, b \in G$,

a) $(a^{-1})^{-1} = a$ **b)** $(ab)^{-1} = b^{-1}a^{-1}$

10. Prove that a group G is abelian if and only if for all $a, b \in G$, $(ab)^{-1} = a^{-1}b^{-1}$.

8. Proof: Suppose that G is abelian and that $a, b \in G$. Then $(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2b^2$, by using the associative property for a group and the fact that this group is abelian.
Conversely, suppose that G is a group where $(ab)^2 = a^2b^2$ for all $a, b \in G$. If $x, y \in G$, then $(xy)^2 = x^2y^2 \Rightarrow (xy)(xy) = x^2y^2 \Rightarrow x(yx)y = x(xy^2) \Rightarrow (yx)y = xy^2$ (by Theorem 16.1 (c)) $\Rightarrow (yx)y = (xy)y \Rightarrow yx = xy$ (by Theorem 16.1 (d)). Therefore, the group G is abelian.

9. (a) The result follows from Theorem 16.1(b) since both $(a^{-1})^{-1}$ and a are inverses of a^{-1}.
(b) $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}(e)b = b^{-1}b = e$ and $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(e)a^{-1} = aa^{-1} = e$. So $b^{-1}a^{-1}$ is an inverse of ab, and by Theorem 16.1(b), $(ab)^{-1} = b^{-1}a^{-1}$.

10. G abelian $\Longrightarrow a^{-1}b^{-1} = b^{-1}a^{-1}$. By Exercise 9(b), $b^{-1}a^{-1} = (ab)^{-1}$, so G abelian $\Longrightarrow a^{-1}b^{-1} = (ab)^{-1}$. Conversely, if $a, b \in G$, then $a^{-1}b^{-1} = (ab)^{-1} \Longrightarrow a^{-1}b^{-1} = b^{-1}a^{-1} \Longrightarrow ba^{-1}b^{-1} = a^{-1} \Longrightarrow ba^{-1} = a^{-1}b \Longrightarrow b = a^{-1}ba \Longrightarrow ab = ba \Longrightarrow G$ is abelian.

5. Let G be a group with subgroups H and K. If $|G| = 660$, $|K| = 66$, and $K \subset H \subset G$, what are the possible values for $|H|$?

From Lagrange's Theorem we know that $|K| = 66 (= 2 \cdot 3 \cdot 11)$ divides $|H|$ and that $|H|$ divides $|G| = 660 (= 2^2 \cdot 3 \cdot 5 \cdot 11)$. Consequently, since $K \neq H$ and $H \neq G$, it follows that $|H|$ is $2(2 \cdot 3 \cdot 11) = 132$ or $5(2 \cdot 3 \cdot 11) = 330$.

11. Let H and K be subgroups of a group G, where e is the identity of G.

a) Prove that if $|H| = 10$ and $|K| = 21$, then $H \cap K = \{e\}$.

(a) Let $x \in H \cap K$. $x \in H \Longrightarrow o(x) | 10 \Longrightarrow o(x) = 1, 2, 5$, or 10. $x \in K \Longrightarrow o(x) | 21 \Longrightarrow o(x) = 1, 3, 7$, or 21. Hence $o(x) = 1$ and $x = e$.


THANK YOU GW
SOLDIERS !