CS & IT ENGINEERING

Discrete mathematics
Set theory

Lecture No.9

By- SATISH YADAV SIR

TOPICS TO BE COVERED

01 Group

02 Semigroup

03 monoid

04 Abelian Group

05 Practice

$(G, *)$ is called group. (algebric structure)

$(G, *)$ Semigroup

1) $a \in G,\ b \in G\quad a * b \in G$. (closed)

2) $a * (b * c) = (a * b) * c$ [associative]

$(G, *)$ monoid.

3) $a * e = a = e * a$. [Identity]

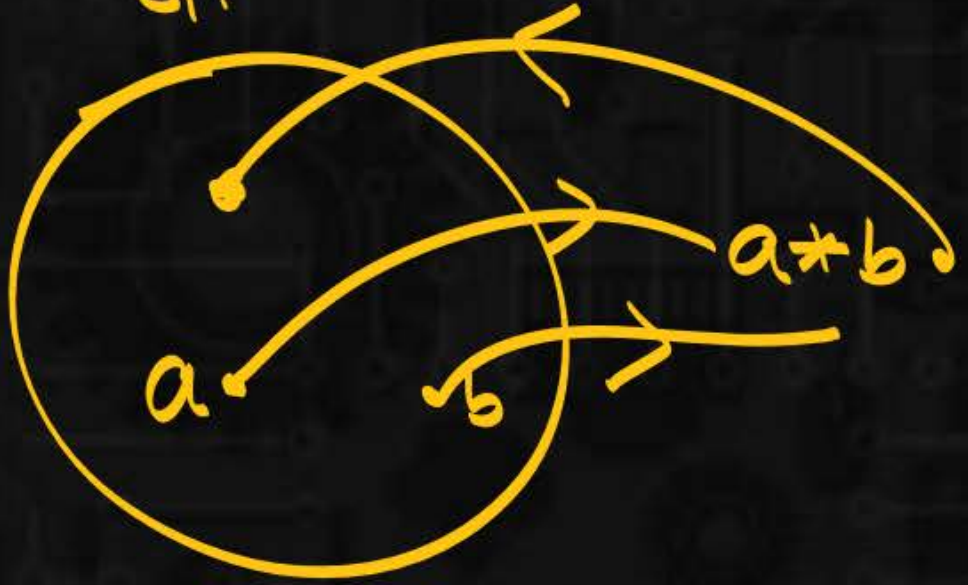
$\hookrightarrow$ identity element.

4) $a * a^{-1} = e = a^{-1} * a$.

$\hookrightarrow$ Inverse

Closed :

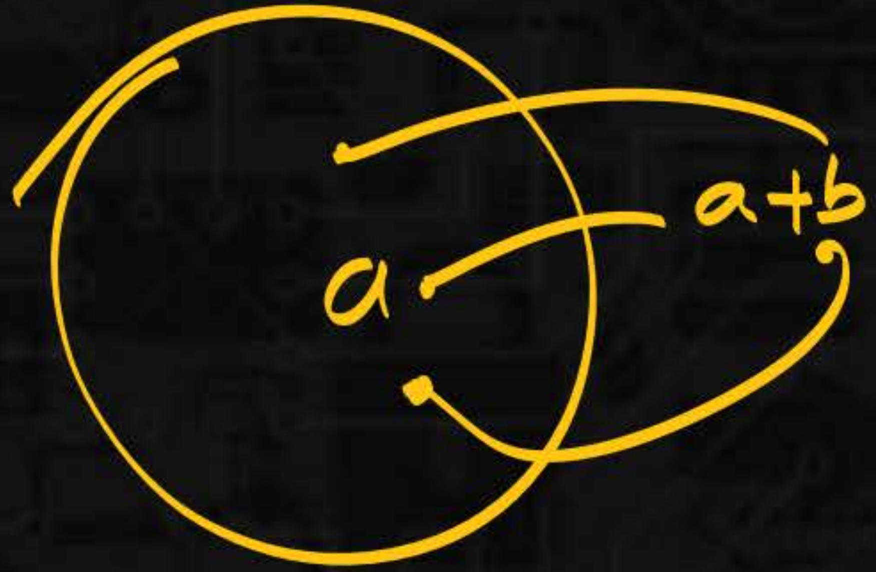
G :



$a \in G \mid b \in G.$

$(\mathbb{Z}, +)$

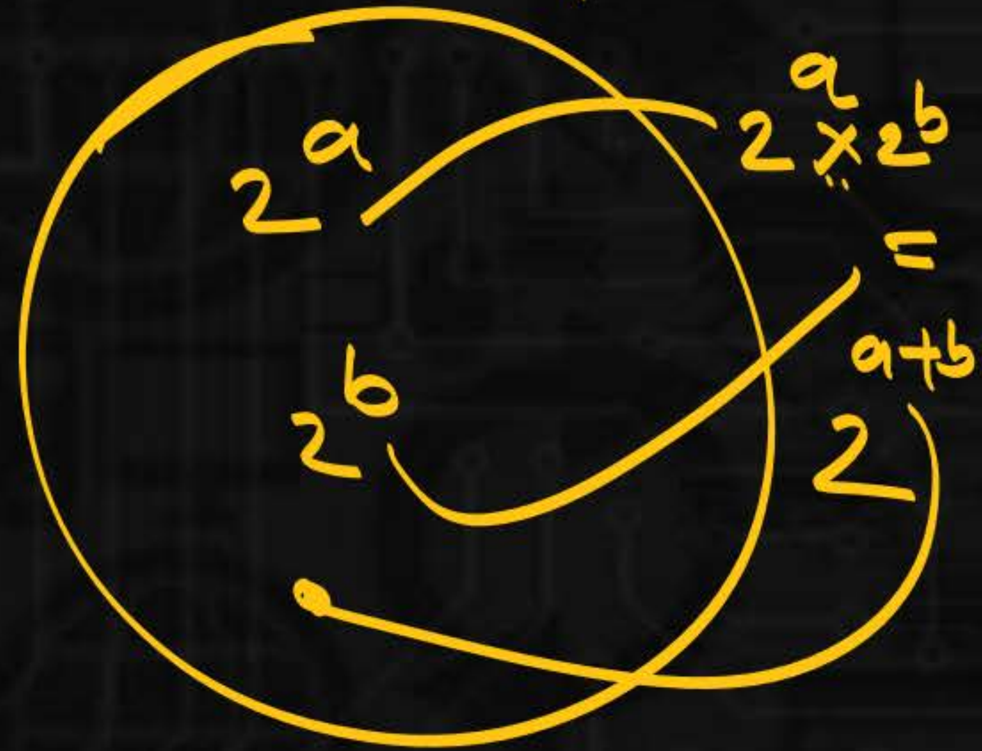
$a \in \mathbb{Z},\ b \in \mathbb{Z}.\ a+b \in \mathbb{Z}.$



$(A, \underline{\times})$ closed

$A = \{ 2^n \mid n \in \mathbb{Z} \}.$

$2^a \mid a \in \mathbb{Z}.\quad 2^b \mid b \in \mathbb{Z}$



$(\mathbb{Z}, +)$ <u>Group.</u>

1) $a \in \mathbb{Z}, b \in \mathbb{Z} \quad a+b \in \mathbb{Z}$.

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

3) $a+0 = a$ [0 is identity element] ($e = 0$) unique

$a + \_ = a$

4) $a * a^{-1} = e$

$a + (-a) = 0$

$2 + (-2) = 0$

$-3 + (-(-3)) = 0$

$(\mathbb{Z}, \times)$

1) $a \in \mathbb{Z}, b \in \mathbb{Z} \quad a \times b \in \mathbb{Z}$.

2) $a \times (b \times c) = (a \times b) \times c$.

3) $a \times 1 = a$

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

$\left(\frac{1}{a} \notin \mathbb{Z}\right)$

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

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

$(A, \times)$ $A = \{2^n \mid n \in Z\}$.

1) $2^a \in A,\ 2^b \in A$ $2^a \times 2^b \in A$.

2) $2^a \times (2^b \times 2^c) = (2^a \times 2^b) \times 2^c$.

$2^{a+b+c} = 2^{a+b+c}$

3) $2^a \times 2^0 = 2^a$.

4) $2^a \times 2^{-a} = 2^0$

$(R_{\neq 0}, *)$ $a * b = \frac{ab}{2}$.

1) $a \in R,\ b \in R$ $a * b \in R$.

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

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

$\frac{\frac{ab}{2} \times c}{2}$ $\frac{a \times \frac{bc}{2}}{2}$

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

$$a * b = \frac{ab}{2}$$

3) $a * e = a$

$$\frac{\cancel{a} \cdot e}{2} = \cancel{a}$$

$$e = 2$$

4) $a * a^{-1} = e$

$$\frac{a \cdot a^{-1}}{2} = e$$

$$\frac{a \cdot a^{-1}}{2} = 2$$

$$a^{-1} = \frac{4}{a} \quad (a \neq 0)$$

$a = 1$ $\quad a^{-1} = \frac{4}{a}$

$1^{-1} = \frac{4}{1}$

$a = 0$

$$a^{-1} = \frac{4}{0}$$

$A = \{10n \mid n \in z\}$

$(set, +)$

$(A, +)$

$\{10(-4), 10(-1), 10(0)\ 10(1), 10(2), 10(3), 10(4) \ldots\ldots\}$

$(z, *)$

$x * y = x + y + 1$

1) $10(a)\ ,\ 10(b) \qquad 10(a) + 10(b)$

$10(a+b) \mid a+b \in z$

2) $10(a) + (10(b) + 10(c)) = (10(a) + 10(b)) + 10(c)$

$10(a+b+c) = 10(a+b+c)$

3) $10(a) + 10(0) = 10(a)$

4) $10(a) + 10(-a) = 0$

Group

Infinite Group

eg:

$(Z, +)$

$(Q \neq 0, \times)$

finite group:

(set, operation)

(Cayley table)

$\odot$	a	b	c	d
a				
b				
c				
d				

Set $A: \{1, -1, i, -i\}$. $\quad i^2 = -1$.

3) identity :

$(A, \times)$

1) closed.

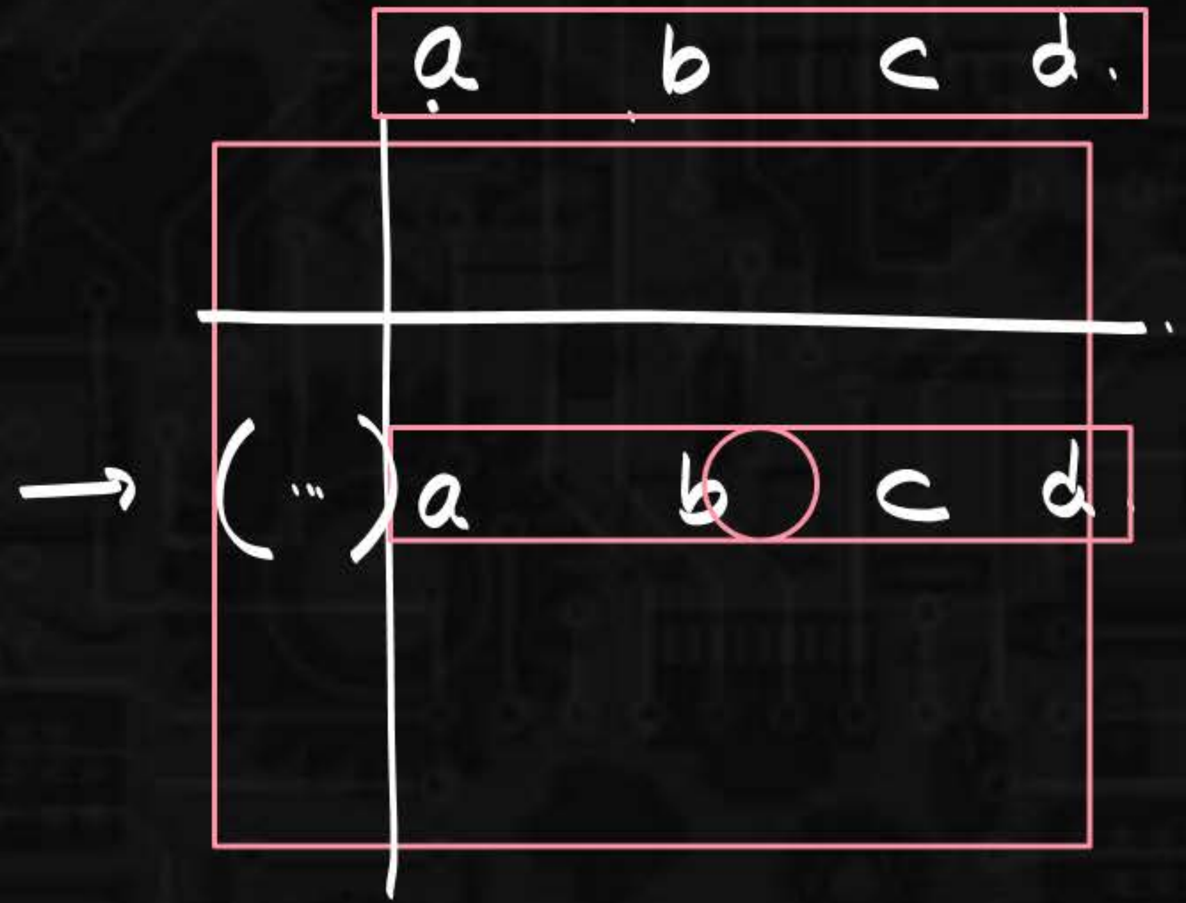
2) $i \times (-i \times 1) = (i \times -i) \times 1$.

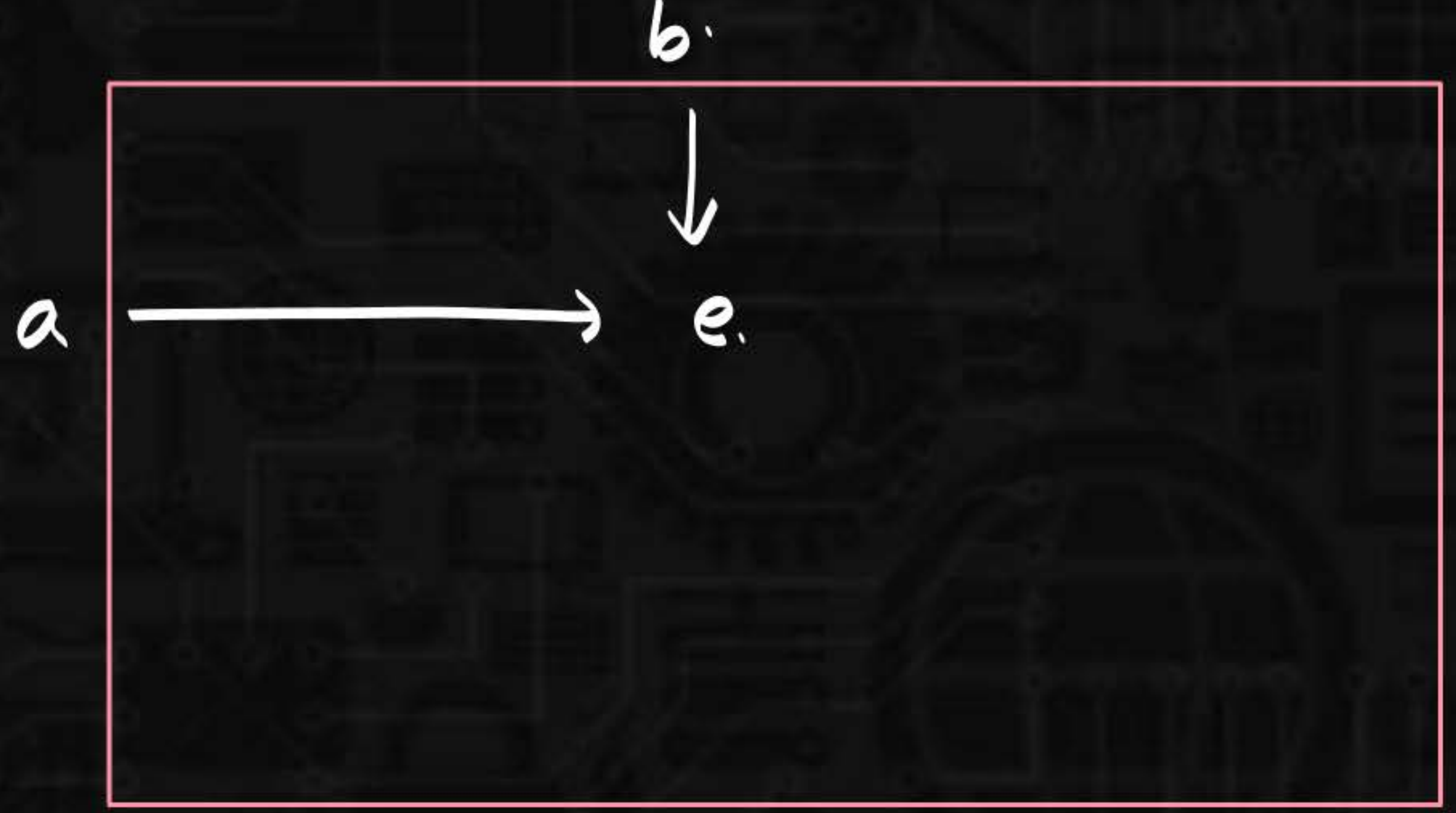
$i \times -i = -i^2 \times 1$

$-i^2$

$1. = 1$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1





$a * b = e$

$a * e = a$

Try to find identity in ans.

$A = \{1, \omega, \omega^2\}$

$(A, \times)$ $\omega^3 = 1.$

$(\{0, 1, 2, 3, 4, 5\}, *)$ $a * b = (a+b) \bmod 6.$

$\oplus_6$	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	3	4.

1) closed.

2) Associative

$(3 \oplus_6 5) \oplus_6 2 = 3 \oplus_6 (5 \oplus_6 2)$

$2 \oplus_6 2.$ $= 3 \oplus_6 ($

$4.$ $= 3 \oplus_6 1$

$= 4.$

3) $3 \oplus_6 0 = 3$

4)

$\oplus_6$	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.

$(G, *)$ Group.

$(H, *)$

① Sub/group ②

1) $H \subseteq G$.

2) H should also be a group.

A) closed.

B) Associative.

C) identity.

d) Inverse

$\oplus_6$	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.

$H = \{0, 1, 2\}$. $|H| = 3$

$|G| = 6$.

1) $H \subseteq G$. ✓

2)

	0	1	2
0	0	1	2.
1	1	2	3
2			

$(1+2) \bmod 6$

$3 \bmod 6$.

$= 3$.

$1 \in H$, $2 \in H$, $1 \oplus_6 2 \notin H$.

it is not closed.

not Group.

not subgroup.

$\oplus_6$	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.

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

1) $H \subseteq G$ ✓

2)

	0	2	4
→ 0	0	2	4
2	2	4	0
4	4	0	2

$(0 \oplus_6 2) \oplus_6 4$
$= 0 \oplus_6 (2 \oplus_6 4)$

Closed ✓

Associative

identity.

Inverse

H is subgroup of G.

Every Group contains 2 Trivial subgroup.

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

I) $e \subseteq G$

2)

2) G is subgroup of itself.

$\begin{cases} 1) \; G \subseteq G. \\ 2) \; G \text{ should be Group.} \end{cases}$

Lagrange's Thm.

if H is subgroup of G then $|H|$ will divide $|G|$. (but vice versa is not True)

$H = \{0, 2, 4\}$ $G = \{0, 1, 2, 3, 4, 5\}$.

$|H| = 3$ $|G| = 6$.

$\frac{6}{3} \in Z$.

(Ans: 84)

1) $|G| = 84$, what will be maximum size of its subgroup.

2) $|G| = 84$, what will be maximum size of its proper subgroup. (GATE)

Ans: 42.

Exponential :

$a^1 = a.$

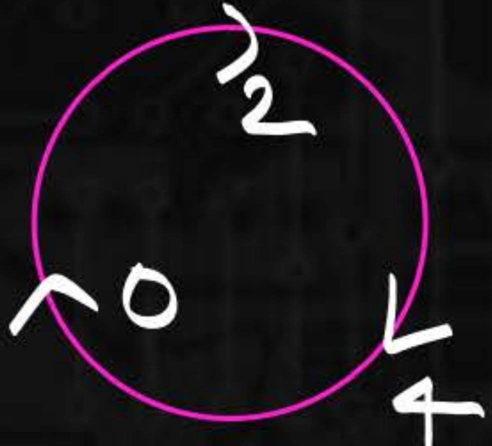
$a^2 = a * a.$

$a^3 = \underbrace{a * a}_{a^2} * a.$

$= a^2 * a.$

Subgroup of cyclic Group is also cyclic Group.

$\oplus_6$	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



$2^1 = 2$

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

$2^3 = \boxed{2 * 2} * 2$

$= 4 * 2$

$= 0$

$2^4 = \boxed{2 * 2 * 2} * 2$

$= 0 * 2$

$= 2$

by taking exponentiation 2 has generated 0, 2, 4.

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

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

$\langle a \rangle$

$\oplus_6$	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.

$1^1 = \underline{1}$

$1^2 = 1 * 1 = 2$

$1^3 = \underline{1 * 1} \times 1$
$= 2 * 1 = 3$

$1^4 = 1^3 * 1$
$= 3 * 1$
$= 4$

$1^5 = 1^4 * 1$
$= 4 * 1 = 5$

$1^6 = 1^5 * 1$
$= 5 * 1 = 0$

$1^7 = 1^6 * 1$
$= 0 * 1 = \underline{\underline{1}}$.

1 has generated.
1, 2, 3, 4, 5, 0
In fact
1 has generated.
all elements in
Group.

hence 1 is
called Generator
of the Group.

Group contains Generator.
↓
Cyclic Group.

$\oplus_6$	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

$$1^1 = \underline{1}$$

$$1^2 = 1 * 1 = 2$$

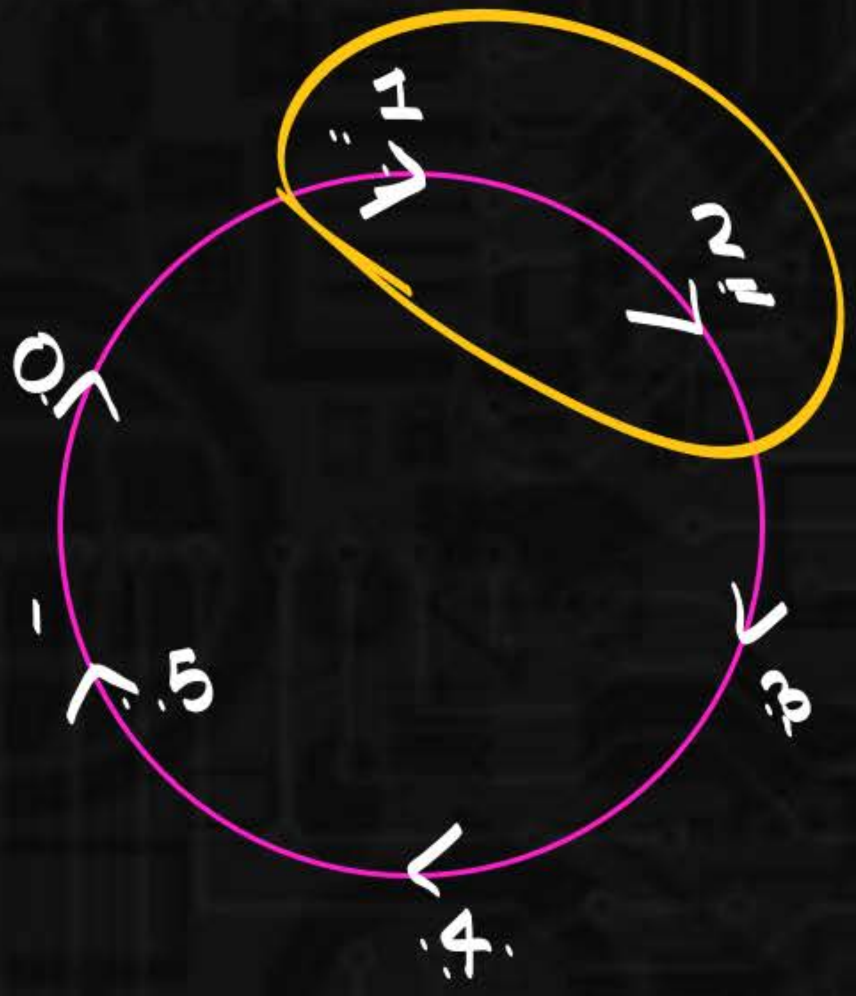
$$1^3 = \underline{1 * 1} \times 1 = 2 * 1 = 3$$

$$1^4 = 1^3 * 1 = 3 * 1 = 4$$

$$1^5 = 1^4 * 1 = 4 * 1 = 5$$

$$1^6 = 1^5 * 1 = 5 * 1 = 0$$

$$1^7 = 1^6 * 1 = 0 * 1 = 1$$



5 is also Generater.

$\oplus_6$	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

$5^1 = 5$

$5^2 = 5 * 5$
$= 4$

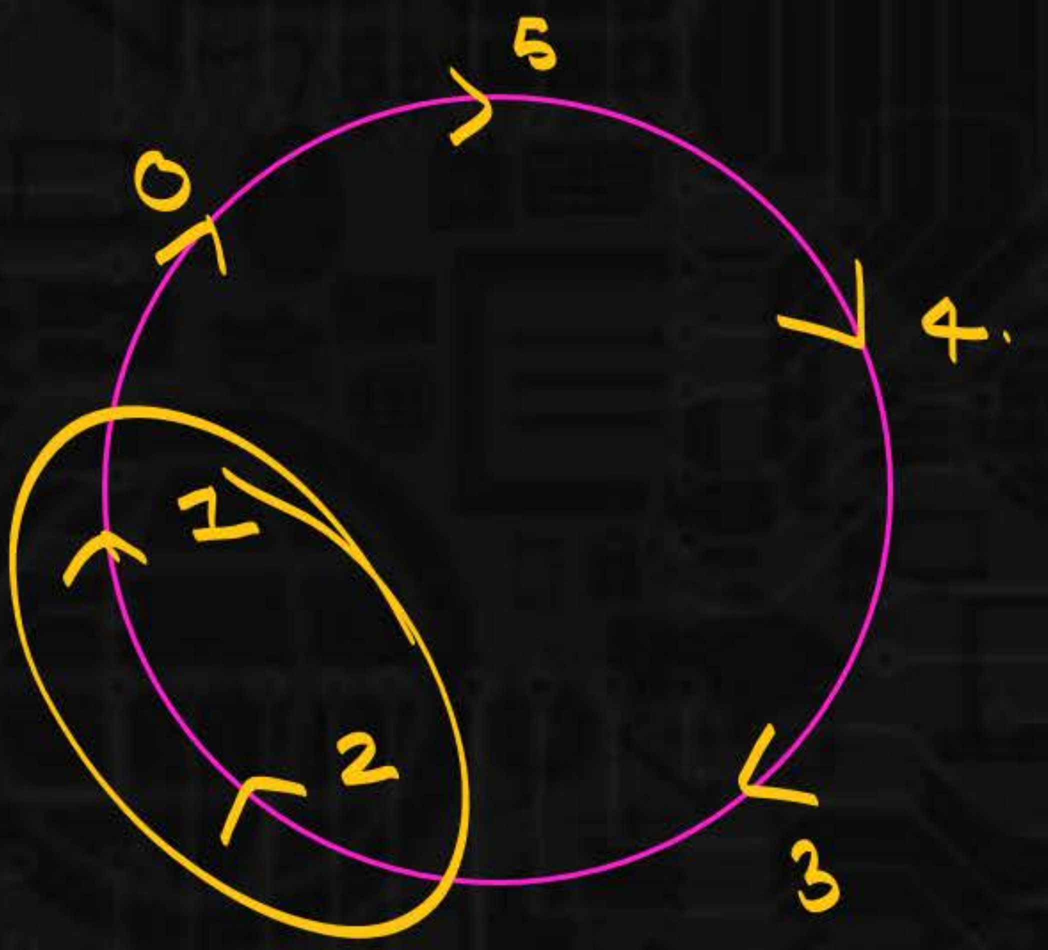
$5^3 = 5^2 * 5$
$= 4 * 5$
$= 3$

$5^4 = 3 * 5$
$= 2$

$5^5 = 2 * 5$
$= 1$

$5^6 = 1 * 5$
$= 0$

$5^7 = 0 * 5$
$= 5$



$\oplus_6$	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	3	4.


THANK YOU GW
SOLDIERS !