4/8/22

lecture-4

Cyclic Group:- A group $(G, *)$ is said to be cyclic group if $\exists$ atleast one element 'a' in G such that — $\boxed{O(a) = O(G)}$

Ex→ $(Z_n, +_n)$ is abelian as well as cyclic group.

$Z_n = \{0, 1, 2, \dots\dots, (n-1)\}$

Show that→ $(Z_3, +_3)$ is an abelian group.

$Z_3 = \{0, 1, 2\}$

$+_3$	0	1	2
0	$\boxed{0}$	1	2 ✓
1	1	2	$\boxed{0}$
2	2	$\boxed{0}$	1

Since all the elements under caley table belongs to the set Z_3, it satisfies closure as well as associative property.

Here $e = 0 \in Z_3$

Hence, existence of identity is satisfied.

$(0)^{-1} = 0$

$(1)^{-1} = 2$

$(2)^{-1} = 1$

Since, inverse of all the elements exists Hence, existence of inverse is satisfied.

Since the matrix under caley table is symmetric in nature, hence commutative property holds.

(#) $(U(n), \cdot)$ is an abelian group but need not be cyclic.

☆ $U(n) = \{m \in Z^+, 1 \leq m < n, \gcd(m,n) = 1\}$

$U(2) = \{1\}$
$U(3) = \{1, 2\}$
$U(4) = \{1, 3\}$
$U(5) = \{1, 2, 3, 4\}$
$U(6) = \{1, 5\}$

$|U(n)| = \phi(n)$

<u>Euler ϕ functions:-</u>

$\phi(1) = 1$
$\phi(2) = 1$
$\phi(3) = 2$
$\phi(4) = 2$
$\phi(5) = 4$
$\phi(6) = 2$

① If P is Prime

$$\boxed{\phi(P) = P - 1}$$

② If $n = P_1 \cdot P_2$

$\phi(n) = \phi(P_1 P_2)$

$$\boxed{\phi(n) = \phi(P_1) \cdot \phi(P_2)}$$

(3) If $n = P_1 P_2 \cdots\cdots P_n$

$$\phi(n) = \phi(P_1 P_2 \cdots P_n)$$

$$\boxed{\phi(n) = \phi(P_1)\cdot\phi(P_2)\cdots\phi(P_n)}$$

(4) If $n = P^K$

$$\boxed{\phi(n) = \phi(P^K) = P^K - P^{K-1}}$$ where P is prime
$K \to$ +ve integer

(5) If $n = P_1^{K_1} \cdot P_2^{K_2} \cdots\cdots P_r^{K_r}$

$$\phi(n) = \phi(P_1^{K_1} \cdot P_2^{K_2} \cdots\cdots P_r^{K_r})$$
$$= \phi(P_1^{K_1}) \cdot \phi(P_2^{K_2}) \cdots\cdots \phi(P_r^{K_r})$$
$$= (P_1^{K_1} - P_1^{K_1 - 1})(P_2^{K_2} - P_2^{K_2 - 1}) \cdots\cdots (P_r^{K_r} - P_r^{K_r - 1})$$
$$= P_1^{K_1}\left(1 - \frac{1}{P_1}\right) P_2^{K_2}\left(1 - \frac{1}{P_2}\right) \cdots\cdots P_r^{K_r}\left(1 - \frac{1}{P_r}\right)$$
$$= (P_1^{K_1} \cdot P_2^{K_2} \cdots\cdots P_r^{K_r})\left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right)\cdots\cdots\left(1 - \frac{1}{P_r}\right)$$

$$\boxed{\phi(n) = n\left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right)\cdots\cdots\left(1 - \frac{1}{P_r}\right)}$$

Ex $n = 150$

$150 = 2^1 \times 3^1 \times 5^2$

2	150
3	75
5	25
5	5
	1

$$\phi(150) = 150\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$
$$= \cancel{150}^{10} \times \frac{1}{\cancel{2}} \times \frac{\cancel{2}}{\cancel{3}} \times \frac{4}{\cancel{5}}$$
$$= 40 \quad \underline{\text{Ans}}$$