# Chapter-4
# cyclic groups

**Def$^n$**:- A group $G$ is called a cyclic group if $\exists$ an element $a \in G$, such that every element of $G$ can be expressed as a power of $a$.

i.e $G = \{a^n / n \in Z\}$ (in addition $G = \{na / n \in Z\}$)

such an element is called generator of $G$

i.e $G = \langle a \rangle$

**Ex** $Z_n = \{0, 1, \cdots (n-1)\}$

is a cyclic group under addition modulo $n$ with 1 is a generator

**Remark**:- Any ~~this~~ cyclic group can have more than one generator

**Ex**:- $Z_8 = \{0, 1, 2 \cdots 7\}$

generator of $Z_8$ are $\langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = Z_8$

$\langle 3 \rangle = \{3, 3+3 \pmod 8, 3\times 3 \pmod 8, 3\times 4 \pmod 8, \cdots 3\times 8 \pmod 8\}$

Now

$\langle 2 \rangle = \{0, 2, 4, 6, 8\} \neq Z_8$

$\Rightarrow \langle 2 \rangle$ is not a generator of $Z_8$

Ex $U(10) = \{1, 3, 7, 9\} = \{3^0, 3^1, 3^2, 3^3\} = \langle 3 \rangle$

also $U_{10} = \{7^0, 7^1, 7^2, 7^3\}$

as

$7^0 \pmod{10} = 1$

$7^1 \pmod{10} = 7$

$7^2 \pmod{10} = 49 \pmod{10} = 9$

$7^3 \pmod{10} = 243 \pmod{10} = 3$

$\Rightarrow U(10) = \{1, 3, 7, 9\} = \langle 7 \rangle$

$\Rightarrow U(10)$ is cyclic group

**Theorem 4.1 :- Criterion for $a^i = a^j$**

Let G be a group, and let 'a' $\in$ G. If 'a' has infinite order, then $a^i = a^j$ if and only if $i = j$. If 'a' has finite order, say n, then $\langle a \rangle = \{e, a, a^2, \ldots a^{n-1}\}$ & $a^i = a^j$ if and only if n divides $i-j$

**Corollary 1 :-** For any group element 'a'

$o(a) = o(\langle a \rangle)$

**Corollary (2)** $a^k = e$ implies that $o(a)$ divides $k$

Let $G$ be a group and let '$a$' be an element of order $n$ in $G$. If $a^k = e$ then $n$ divides $k$.

**Theorem 4.2** :- $\langle a^k \rangle = \langle a^{gcd(n,k)} \rangle$ and $o(a^k) = \frac{n}{gcd(n,k)}$

Let '$a$' be an element of order $n$ in a group and let $k$ be a positive integer. Then $\langle a^k \rangle = \langle a^{gcd(n,k)} \rangle$ and $o(a^k) = \frac{n}{gcd(n,k)}$.

**Corollary (1)** In a finite cyclic group, the order of ~~the~~ an element divides the order of the group.

**Cor (2)** Let $o(a) = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ if and only if $gcd(n,i) = gcd(n,j)$ and $o(a^i) = o(a^j)$ if and only if $gcd(n,j) = gcd(n,i)$

**Cor (3)** Let $o(a) = n$. Then $\langle a \rangle = \langle a^i \rangle$ if and only if $gcd(n,j) = 1$ and $o(a) = o(\langle a^i \rangle)$ if and only if $gcd(n,i) = 1$

**Cor (4)** An integer $k$ in $Z_n$ is a generator of $Z_n$ if only if $gcd(n,k) = 1$.

Ex Show that cyclic group is abelian

Sol$^{n}$ Let $G$ be any cyclic group

$\Rightarrow G = \langle a \rangle$ for some $a \in G$

Let $x, y \in G = \langle a \rangle$

$\Rightarrow x = a^n$

$y = a^m$ for some integers $n, m$

Now $xy = a^n \cdot a^m = a^{n+m}$

$= a^{m+n}$

$= a^m \cdot a^n$

$= yx$

Hence $G$ is abelian group.

Remark:- order of a subgroup divides order of a group.

Ex Prove that a group $G$ of prime order must be cyclic and every element of $G$ other than identity can be taken as its generator.

Sol$^{n}$ Let $o(G) = p$, a prime

Let $a \in G$ and $a \neq e$

Assume $H = \{a^n \mid n \text{ is integer}\}$

$\Rightarrow H$ is cyclic subgroup of $G$.

ie $H = \langle a \rangle$

also $\because o(H) \mid o(G)$

$\Rightarrow o(H) = 1$ or $p$

but $o(H) \neq 1$ as $a \neq e$

$\Rightarrow o(H) = p$

$\Rightarrow H = G$

$\because H$ is cyclic

$\Rightarrow G$ is cyclic group generated by $a$ and $a \neq e$.

Note :- Group of prime order is cyclic.

Theorem 4.3 :- Fundamental Theorem of cyclic groups

Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of $n$; and for each positive divisor $k$ of $n$, the group $\langle a \rangle$ has exactly one subgroup of order $k$, namely $\langle a^{n/k} \rangle$.

Corollary :- Subgroup of $Z_n$

For each positive divisor $k$ of $n$, the set $\langle n/k \rangle$ is the unique subgroup of $Z_n$ of order $k$, moreover, these are the only subgroups of $Z_n$.

Ex :- Subgroup of $Z_{30}$

$\langle 1 \rangle = \{0, 1, 2, \ldots 29\}$ with order 30

$\langle 2 \rangle = \{0, 2, 4, \ldots 28\}$ with order 15

$\langle 3 \rangle = \{0, 3, 6, \ldots 27\}$ with order 10

$\langle 5 \rangle = \{0, 5, 10, 15, 20, 25\}$ with order 6

$\langle 6 \rangle = \{0, 6, 12, 18, 24\}$ with order 5

$\langle 10 \rangle = \{0, 10, 20\}$ with order 3

$\langle 15 \rangle = \{0, 15\}$ with order 2

$\langle 30 \rangle = \{0\}$ with order 1

# Euler's $\phi$ function

Let $n$ be any positive integer and let $n = p_1^{n_1} \times p_2^{n_2} \times \cdots \times p_k^{n_k}$ where $p_1, p_2, \cdots p_k$ are distinct prime factors of $n$ $(n > 1)$ then

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

(1) If $n$ is prime i.e $p$ then $\phi(p) = p-1$

(2) $\phi(1) = 1$

(3) If $m, n$ are coprime then

$$\phi(mn) = \phi(m)\,\phi(n)$$

Ex $n = 20 = 2^2 \times 5^1$

$$\phi(n) = 20 \times \left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$$

$$\phi(20) = 20 \times \frac{1}{2} \times \frac{4}{5}$$

$$= 8$$

**Theorem :-** The number of generators of a finite cyclic group of order $n$ is $\phi(n)$

Ex : $Z_8$

$n = 8 = 2^3$

No. of generator $= \phi(8)$

$$= 8\left(1-\frac{1}{2}\right)$$

$$= 8 \times \frac{1}{2} = 4$$

generators of $Z_8$ is $\langle 1\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle$

**Theorem :-** If $d$ is a positive divisor of $n$, the number of elements of order $d$ in a cyclic group of order $n$ is $\phi(d)$.

**Corollary :-** In a finite group, the number of elements of order $d$ is a multiple of $\phi(d)$.

**Qu** Find all the generators of $Z_6$, $Z_8$ & $Z_{20}$.

**Sol$^n$ :-** $Z_6 = \{0, 1, 2, 3, 4, 5\}$

Using the theorem that 'k' is generator of $Z_n$ iff $\gcd(n, k) = 1$

$\Rightarrow$ generators are $\langle 1 \rangle = \langle 5 \rangle$

(2) $Z_8 = \{0, 1, 2, \dots 7\}$

using Euler's $\phi$ function

No. of generators are $\phi(8) = 8\left(1 - \frac{1}{2}\right) = 4$

$\Rightarrow$ generators are $= \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$

$20 = 2^2 \times 5$

(3) $Z_{20} = \{0, 1, 2 \dots 19\}$

No. of generators $= \phi(20) = 20 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right)$

$= 20 \times \frac{1}{2} \times \frac{4}{5}$

$= 8$

generators are $= \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle = \langle 11 \rangle = \langle 13 \rangle$
$\langle 17 \rangle = \langle 19 \rangle$

Ques List the elements of the subgroups $\langle 3 \rangle$ and $\langle 7 \rangle$ in $U(20)$.

Sol$^n$ $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$

$\langle 3 \rangle$ = subgroup generated by 3

$3^0 \bmod 20 = 1$

$3^1 \bmod 20 = 3$

$3^2 \bmod 20 = 9$

$3^3 \bmod 20 = 7$

$3^4 \bmod 20 = 1$

$\Rightarrow \langle 3 \rangle = \{1, 3, 7, 9\}$

subgroup generated by 7

$7^0 \bmod 20 = 1$

$7^1 \bmod 20 = 7$

$7^2 \bmod 20 = 9$

$7^3 \bmod 20 = 3$

$7^4 \bmod 20 = 1$

$\Rightarrow \langle 7 \rangle = \{1, 3, 7, 9\}$

Ques Find an example of a non cyclic group, all of whose proper subgroups are cyclic

Sol$^n$ $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ which is not cyclic group

subgroups are

$A = \{\pm 1, \pm i\}$

$B = \{\pm 1, \pm j\}$

$B = \{\pm 1, \pm k\}$

all A, B, C are cyclic ∴ subgroups of $Q_8$

as $o(i) = 4$ and $o(A) = 4$

$\because$ $o(j) = 4$ and $o(B) = 4$

and $o(k) = 4$ and $o(C) = 4$

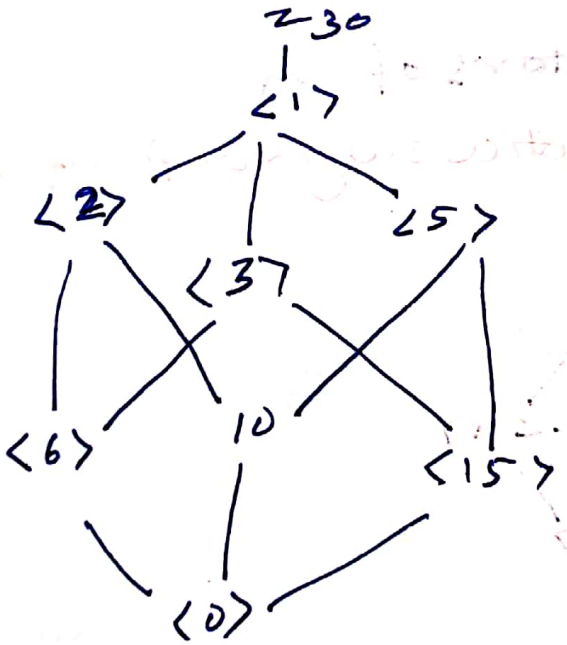
**Qn** Prove that a group order 3 must be cyclic

**Sol$^n$**: ① Using the theorem that group of prime order is cyclic

$\Rightarrow$ $o(G) = 3$ is cyclic

## * Subgroup lattice

**Ex** $Z_{30}$




**Qn (21)** Let G be a group and let a be an elements of G.

① If $a^2 = e$, what can we say about the order of a?

(b) If $a^m = e$, what can you say about order of a group

Sol$^n$ (a) If $a^{12} = e$

then using theorem that if $a^k = e$ that order of a divides k

$\Rightarrow o(a)$ = factor of 12

$= 1, 2, 3, 4, 6, 12$

(b) $a^m = e$

if m is Prime

then $o(a) = 1$ or $m$

if m is composite

Then $o(a) =$ ~~for~~ factors of $m$

Qu Determine the lattice subgroup of $Z_8$

Sol$^n$