Cyclic Group :

Semester: II (UG)

Paper : C201

Course - Mathematics(H)

Prepared by Dr. A. K. Maiti

Cyclic Group:

Defn: A group $(G, \circ)$ is said to be a cyclic group if there exists an element a in G such that $G = \{a^n : n \in \mathbb{Z}\}$ i.e $G = \langle a \rangle$. a is said to be a generator of the cyclic group.

In additive notation, $G = \{na : n \in \mathbb{Z}\} = \langle a \rangle$.

Examples:

(i) $(\mathbb{Z}, +)$ is a cyclic group generated by 1. -1 is also a generator.

(ii) Let $S = \{1, -1, i, -i\}$. Then $(S, \cdot)$ is a cyclic group generated by i. $-i$ is also a generator.

(iii) $(\mathbb{Z}_4, +)$ is a cyclic group generated by $\bar{1}$. $\bar{3}$ is also a generator.

(iv) Let $S = \{1, -1\}$. Then $(S, \cdot)$ is a cyclic group generated by -1. -1 is the only generator of the group.

(v) Klein's 4-group V is not a cyclic group. The elements of V are e, a, b, c and none element of V can generate the whole group V. But the group V is abelian.

Theorem: Prove that every cyclic group is abelian.

Proof: Let $(G, \circ)$ be a cyclic group generated by a. Let $p, q \in G$. Then $p = a^r$, $q = a^s$ for some integers r and s.

$\therefore p \circ q = a^r \circ a^s = a^{r+s} = a^{s+r} = a^s \cdot a^r = q \circ p$ $\left[\because r+s = s+r\right]$

$\therefore p \circ q = q \circ p \quad \forall\, p, q \in G$.

Therefore, the group is abelian.

Note: An abelian group is not necessarily a cyclic group.

For example: Klein's 4-group V is abelian group but it is not cyclic group.

Ex: Give an example of the group which is neither cyclic nor abelian.

Ans : (i) The symmetric group S_3 is not cyclic and is not abelian.

(ii) The dihedral group D_4 is not cyclic and not abelian.

(Ex) : Give an example of an abelian group which is not cyclic.

Ans : $(Q, +)$ is an abelian group but it is not cyclic.

Theorem : Let (G, o) be a cyclic group generated by a. Then $\bar{a}^1$ is also a generator. V.H - C.H-bb.

Proof : Since a is a generator, $G = \{a^n : n \in Z\}$.

Let $H = \{(\bar{a}^1)^n : n \in Z\}$.

Let $p \in G$. Then $p = a^r$ for some integer r.

p can be expressed as $(\bar{a}^1)^{-r}$ and $-r$ is an integer, $p \in H$.

Thus, $p \in G \Rightarrow p \in H$

$\therefore G \subseteq H$ (i)

Let $q \in H \Rightarrow q \in G$ and therefore $H \subseteq G$ (ii).

From (i) and (ii), $G = H$.

ie $G = \{(\bar{a}^1)^n : n \in Z\}$.

This shows that $\bar{a}^1$'s also a generator of G.

Theorem : Let (G, o) be a finite cyclic group generated by a. Then $o(G) = n$ iff $o(a) = n$.

Proof : Let $o(a) = n$.

Then $a, a^2, a^3, \ldots, a^n = e$ are distinct elements of G.

Therefore, $\{a, a^2, a^3 \ldots a^n\} \subseteq G$ (i)

Again, G is cyclic group generated by a. Then

$G = \{a^m : m \in Z\}$.

Let p be an arbitrary element of G. Then $p = a^m$ for some integer m.

By division algorithm, there exist integers q and r such that

$m = nq + r$, $0 \le r < n$.

Therefore, $p = a^m = a^{nq+n} = (a^n)^q \cdot a^r = e \cdot a^r = a^r$ [$\because a^n = e$]

ie $p \in \{a, a^2, \ldots a^{n-1}, a^n (=e)\}$.

Therefore, $G \subseteq \{a, a^2, a^3, \ldots, a^n\}$ — (ii).

From (i) and (ii), $G = \{a, a^2, a^3, \ldots, a^n\}$.

$\therefore O(G) = n$.

Conversely, Let $O(G) = n$.

Since G is a finite group, every element of G is of finite order.

Let $O(a) = k$. Then $a, a^2, \ldots, a^k (=e)$ are distinct elements of G.

Since G contains n elements, $\therefore k \le n$.

But k is not less than n, because $O(a) = k$ implies that $O(G) = k$, a contradiction.

Therefore, $O(a) = n$.

Hence the theorem.

Theorem: Prove that every subgroup of a cyclic group is cyclic.

V.H-'06 C.H-'06

Proof: Let (G, o) be a cyclic group generated by a and let (H, o) be a subgroup of G.

Case-I: If $G = H$ ie H is improper subgroup of G. Then H is cyclic group.

Case-II: If $H = \{e\}$ ie H is trivial subgroup G then $H = \{e^n : n \in \mathbb{Z}\}$. Therefore, H is a cyclic group.

Case-III: H is a proper subgroup of G other than trivial subgroup $\{e\}$. Then there is an element x in H such that $x \ne e$. Since $x \in G$, $x = a^s$ for some integer

$\cdot s \neq 0$.

Since H is a subgroup, $\bar{x}' \in H$ i.e. $\bar{a}^s \in H$.

Therefore, H contains elements which are positive as well as negative integral powers of a.

Let m be the least positive integer such that $a^m \in H$.

Then we shall prove that $H = \langle a^m \rangle$ i.e. H is a cyclic and is generated by a^m.

Let at be any arbitrary element of H.

By division algorithm, there exist integers q and r such that

$$t = mq + r, \quad 0 \leq r < m.$$

Now, $a^m \in H \Rightarrow (a^m)^q \in H$ [By closure prop].

$\Rightarrow a^{mq} \in H$

$\Rightarrow \bar{a}^{mq} \in H$ [$\because H$ is a subgroup]

Also, $a^t \cdot \bar{a}^{mq} \in H \Rightarrow a^t \cdot \bar{a}^{mq} \in H$

$\Rightarrow a^{t-mq} \in H$

$\Rightarrow a^r \in H$ [$\because r = t - mq$]

Since $0 \leq r < m$ and m is the least positive integer and $a^m \in H$.

Therefore, r must be equal to 0.

$\therefore t = mq$.

$\therefore a^t = a^{mq} = (a^m)^q$, q is an integer.

$\therefore$ Hence $H = \langle a^m \rangle$.

Hence the theorem.

Cyclic Subgroup:

Defn: Let $(G, \circ)$ be a group and a be an element of G. Let H be the subset of G defined by $H = \{a^n : n \in \mathbb{Z}\}$ i.e. $H = \langle a \rangle$

a is the generator of the cyclic subgroup H of G.

(Ex): Prove that (H, o) is subgroup of (G, o) where $H = \{a^n : n \in Z\}$.

Ans: Since H is a non-empty subset of G, since $a \in H$.

Let $p \in H$, $q \in H$. Then $p = a^r$, $q = a^s$ for some integers r, s.

Now, $p o q = a^{r+s} \in H$, since $r+s$ is an integer.

Also, $\bar{p}' = \bar{a}^r \in H$, since $-r$ is an integer.

Therefore, $p \in H, q \in H \Rightarrow p o q \in H$.

and $p \in H \Rightarrow \bar{p}' \in H$.

Thus, (H, o) is a subgroup of (G, o).

(Ex) If $a = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}$ then show that the set $\{a, a^2, a^3, a^4\}$ forms a cyclic group.

Ans: We have $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$.

$$\therefore a^2 = a \cdot a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$a^3 = a^2 \cdot a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

$$a^4 = a^3 \cdot a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = I.$$

Hence, $a^5 = a^4 \cdot a = I \cdot a = a$

Similarly, $a^6 = a^5 \cdot a = a \cdot a = a^2$

$a^7 = a^6 \cdot a = a^2 \cdot a = a^3$

$a^8 = a^7 \cdot a = a^3 \cdot a = a^4 = I$ and so on.

Thus, the set $G = \{a, a^2, a^3, a^4\}$ is closed with respect to permutation multiplication.

The Permutation multiplication is associative

The identity element in G is $a^4 = I$.

The inverse of a, a^2, a^3, a^4 are respectively a^3, a^2, a, a^4.

Also, all elements of G are integral powers of a.

Hence, it forms a cyclic group.

(Ex): Show that the set $\{1,-1,i,-i\}$ forms a cyclic group under multiplication. Find its generators.

Ans: We have previously proved that the set $\{1,-1,i,-i\}$ forms a group under multiplication.

Again, we see that $i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.

Thus, we see that it is a cyclic group with generator i.

Also, $(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1$.

Thus, the group is cyclic whose generator is $-i$.

(Ex): Find all cyclic subgroups of the group $(S, \cdot)$ where $S = \{-i, i, -1, 1\}$.

Ans: $\langle 1 \rangle = \{1\}$

$\langle i \rangle = \{i, i^2, i^3, i^4\} = \{1, -1, i, -i\} = S$.

$\langle -1 \rangle = \{1, -1\}$

$\langle -i \rangle = \{1, -1, i, -i\} = S$.

Therefore, the cyclic subgroups are $(\{1\}, \cdot)$, $(\{-1,1\}, \cdot)$, and $(S, \cdot)$.

(Ex): Find all cyclic subgroups of the symmetric group S_3.

Ans: The elements of S_3 are $\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5$

where $\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

$\rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\rho_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\rho_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

Here ρ_0 is the identity element.

Now, $\langle \rho_0 \rangle = \{\rho_0\}$

$\langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\}$ since $\rho_1^2 = \rho_2$, $\rho_1^3 = \rho_0$

$\langle \rho_2 \rangle = \{\rho_0, \rho_1, \rho_2\}$ since $\rho_2^2 = \rho_1$, $\rho_2^3 = \rho_0$

$\langle \rho_3 \rangle = \{\rho_0, \rho_3\}$, since $\rho_3^2 = \rho_0$

$\langle \rho_4 \rangle = \{\rho_0, \rho_4\}$, since $\rho_4^2 = \rho_0$

$\langle \rho_5 \rangle = \{\rho_0, \rho_5\}$, since $\rho_5^2 = \rho_0$

Therefore the cyclic subgroups are $(\{\rho_0\}, \cdot)$, $(\{\rho_0, \rho_1, \rho_2\}, \cdot)$, $(\{\rho_0, \rho_3\}, \cdot)$, $(\{\rho_0, \rho_4\}, \cdot)$ and $(\{\rho_0, \rho_5\}, \cdot)$.

(Ex): Find all cyclic subgroups of $(Z_5, +)$

Ans: The elements of Z_5 are $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$.

Here $\bar{0}$ is the identity element in Z_5.

Now, $\langle \bar{0} \rangle = \{\bar{0}\}$.

$\langle \bar{1} \rangle = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ since $2\cdot\bar{1} = \bar{2}$, $3\cdot\bar{1} = \bar{3}$, $4\cdot\bar{1} = \bar{4}$, $5\cdot\bar{1} = \bar{0}$.

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

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

$\langle \bar{4} \rangle = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$, since $2\cdot\bar{4} = \bar{3}$, $3\cdot\bar{4} = \bar{2}$, $4\cdot\bar{4} = \bar{1}$, $5\cdot\bar{4} = \bar{0}$.

Thus, the cyclic subgroup generated by each non-identity element is the group itself.

(Ex) Find all subgroups of the group $(Z, +)$.

Ans: $(Z, +)$ is cyclic group with 1 as a generator.

Therefore, every subgroup of the group $(Z, +)$ is cyclic.

Hence all subgroups of $(\mathbb{Z}, +)$ are given by the cyclic subgroups generated by different elements of $\mathbb{Z}$.

The cyclic subgroup generated by the integer m is $(m\mathbb{Z}, +)$. Therefore, all subgroups of $(\mathbb{Z}, +)$ are precisely $(m\mathbb{Z}, +)$, where m is an integer.

Since the subgroups $(m\mathbb{Z}, +)$ and $(-m\mathbb{Z}, +)$ are identical, the totality of the subgroups of the group $(\mathbb{Z}, +)$ are given by $(m\mathbb{Z}, +)$, where m is a non-negative integer.

(Ex): Prove that $(\mathbb{Q}, +)$ is a non-cyclic group. Deduce that the group $(\mathbb{R}, +)$ is non-cyclic.

Ans: If possible let, $(\mathbb{Q}, +)$ be a cyclic group generated by an element a. Then a is a non-zero element of $\mathbb{Q}$.

Since a is a generator of the additive group $(\mathbb{Q}, +)$, every element of $\mathbb{Q}$ must be expressed as ma for some integer m.

But $\frac{1}{2}a \in \mathbb{Q}$ and $\frac{1}{2}a$ can not be expressed as ma for some integer m. Therefore, a is not a generator of $(\mathbb{Q}, +)$.

This proves that $(\mathbb{Q}, +)$ is not a cyclic group.

2nd Part:

$(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$. If $(\mathbb{R}, +)$ be cyclic, then $(\mathbb{Q}, +)$ being a subgroup of the cyclic group $(\mathbb{R}, +)$ must be cyclic.

But $(\mathbb{Q}, +)$ is non-cyclic and therefore $(\mathbb{R}, +)$ is a non-cyclic group.

(Ex) Give an example of a non-cyclic group having all proper subgroups as cyclic subgroups. Justify your answer. C.H'03, 05.

Ans: (i) The non-cyclic group is Klein's 4-group whose elements are e, a, b, c. Thus the set $G = \{e, a, b, c\}$

We form a composition with respect to multiplication [See previous]

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

From the composition table it is easy to verify that $(G, \cdot)$ is a commutative group.

Again G is not acyclic group. Since none of $\langle e\rangle, \langle a\rangle, \langle b\rangle$ and $\langle c\rangle$ is equal to G.

Again we see that

$\langle e\rangle = \{e\}$

$\langle a\rangle = \{e, a\}$

$\langle b\rangle = \{e, b\}$

$\langle e\rangle = \{e, e\}$.

These are the subgroups of the group G.

All of them are cyclic group.

Since $\langle e\rangle = \{e^n : n \in Z\}$

$\langle a\rangle = \{a^n : n \in Z\}$

$\langle b\rangle = \{b^n : n \in Z\}$

$\langle c\rangle = \{c^n : n \in Z\}$.

Hence G is not cyclic but all its proper subgroups $(\{e, a\}, \cdot)$, $(\{e, b\}, \cdot)$, $(\{e, c\}, \cdot)$ are cyclic.

~~Another example~~.

(iii) ~~Let us consider the symmetric group S_3 of degree 3 which is not~~ cyclic and non-abelian.

Ex: Give an example of a non-cyclic and non-abelian group having all proper subgroups as cyclic subgroups. Justify your answer. C-H-05.

Ans: Let us consider the symmetric group S_3 of degree 3 which is non-cyclic and non-abelian.

The elements of S_3 are $\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5$ where

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\rho_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \rho_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

We form a composition table with respect to permutation multiplication.

$\cdot$	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_1	ρ_1	ρ_2	ρ_0	ρ_5	ρ_3	ρ_4
ρ_2	ρ_2	ρ_0	ρ_1	ρ_4	ρ_5	ρ_3
ρ_3	ρ_3	ρ_4	ρ_5	ρ_0	ρ_1	ρ_2
ρ_4	ρ_4	ρ_5	ρ_3	ρ_2	ρ_0	ρ_1
ρ_5	ρ_5	ρ_3	ρ_4	ρ_1	ρ_2	ρ_0

All subgroups of S_3 is obtained by its cyclic subgroups.
Here ρ_0 is the identity element.

$\langle \rho_0 \rangle = \{\rho_0\}$.

$\langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\}$ since $\rho_1^2 = \rho_2$, $\rho_1^3 = \rho_0$

$\langle \rho_2 \rangle = \{\rho_0, \rho_1, \rho_2\}$, since $\rho_2^2 = \rho_1$, $\rho_2^3 = \rho_0$

$\langle \rho_3 \rangle = \{\rho_0, \rho_3\}$, since $\rho_3^2 = \rho_0$.

$\langle \rho_4 \rangle = \{\rho_0, \rho_4\}$, since $\rho_4^2 = \rho_0$

$\langle \rho_5 \rangle = \{\rho_0, \rho_5\}$, since $\rho_5^2 = \rho_0$.

The cyclic subgroups are $(\{\rho_0\}, \cdot)$, $(\{\rho_0, \rho_1, \rho_2\}, \cdot)$, $(\{\rho_0, \rho_3\}, \cdot)$, $(\{\rho_0, \rho_4\}, \cdot)$ and $(\{\rho_0, \rho_5\}, \cdot)$.

Therefore, all proper cyclic subgroups of S_3 are $(\{\rho_0, \rho_1, \rho_2\}, \cdot)$, $(\{\rho_0, \rho_3\}, \cdot)$ $(\{\rho_0, \rho_4\}, \cdot)$ and $(\{\rho_0, \rho_5\}, \cdot)$, $(\{\rho_0\}, \cdot)$

Hence the result.

(Ex) In a cyclic group G, if g_1, g_2 be its two generators then $g_1 g_2$ is also a generator of G. Justify.

Ans: Try yourself

~~In a cyclic group G, g_1, g_2 be its generator then $g_1 g_2$ is not a generator of G.~~ Let G be an infinite cyclic group generated by a. Prove a and $\bar{a}^1$ are also the only generators of G.

Proof: We consider this case when G is an infinite cyclic group.

We 1st prove that if (G, o) be an infinite cyclic group generated by a, then a and $\bar{a}^1$ are the only generators of the group.

Let b be a generator of the group.

Since $b \in G$ and a is a generator, $b = a^m$ for some integer m.

Since $a \in G$ and b is a generator, $a = b^p$ for some integer p.

So, $a = b^p = (a^m)^p = a^{mp}$

$\Rightarrow a^{mp-1} = e$, e being the identity element.

Since $G = \langle a \rangle$ and $O(G)$ is infinite, $o(a)$ is infinite.

Since $o(a)$ is infinite and $a^{mp-1} = e$, we have $mp - 1 = 0$

i.e. $mp = 1$.

So, either $m = 1$ and $p = 1$ or $m = -1$ and $p = -1$.

Therefore either $b = a$ or $b = a^{-1}$.

Thus a and a^{-1} are the only generators of an infinite cyclic group G. Therefore $a \cdot a^{-1} = e$ is not a generator of the group G.

Examples (a) Let us consider an infinite cyclic group $(\mathbb{Z}, +)$.

1 and -1 are the generators of this group.

Now $1 + (-1) = 0$ which can not generates G.

(b) Again we consider the finite cyclic group.

Let $S = \{1, -1, i, -i\}$ is a finite cyclic group

with i and $-i$ as generators.

But $i(-i) = -i^2 = 1$ is not a generator of S.

Hence the justification.

Theorem: A cyclic group of finite order n has one and only one subgroup of order d for every positive divisor d of n.

Proof: Let $G = \langle a \rangle$ be a finite group of order n. Then $o(a) = n$ and

$G = \{a, a^2, \ldots a^n (= e)\}$.

The trivial subgroup $\{e\}$ is the only subgroup of G of order 1.

The improper subgroup G is the only subgroup of order n.

Therefore $d = 1$ and $d = n$ then the theorem is obvious.

Let $1 < d < n$. Then $dm = n$ for some integer m.

$$a^m \in G \text{ and } o(a^m) = \frac{n}{\gcd(m, n)} = \frac{n}{m} = d$$

Therefore the cyclic subgroup $\langle a^m \rangle$ is of order d.

Let $H = \langle a^m \rangle$. The order of the subgroup H is d

Let K be the another subgroup of G such that $o(K) = d$.

Since G is cyclic, K must be cyclic. Let p be the least

Positive integer such that $a^p \in K$. Then $K = \langle a^p \rangle$.

As $O(K) = d$, $(a^p)^d = e$.

By division algorithm, there exists integers q and r such that $p = mq + r$, $0 \le r < m$.

Now $pd = mdq + rd$.

Therefore $a^{pd} = a^{mdq+rd} = a^{mdq} a^{rd} = a^{pd}$

$\Rightarrow a^{rd} = e$.

But $rd < md = n$ and $a^{rd} = e$ together imply $r = 0$.

Thus $p = mq$.

Therefore $\langle a^p \rangle \subseteq \langle a^m \rangle$

i.e. $K \subseteq H$.

Since $O(H) = O(K)$, $K = H$ and this proves that H is unique.

Hence the theorem

(Ex): If $G = \{x : x^{15} = 1\}$, then find all the proper subgroups of $(G, \cdot)$ are cyclic.

Ans: We know that a cyclic group finite order n has a subgroup of order d for every positive divisor d of n.

By the above theorem, G has subgroups of order 3 and 5 because 3 and 5 divides 15. (Order 1 and 15 are not possible).

Again we know that every group of prime order is cyclic.

Hence the subgroups of order 3 and 5 are cyclic.

Hence the result.

(Ex): Let G be an abelian group of order 6 containing an element of order 3. Prove that G is cyclic group.

Ans: Let $a \in G$ and $O(a) = 3$.

Since G is a finite group of even order, it contains at least one element, say b, of order 2. ie $O(b) = 2$.

Since $O(a)$ and $O(b)$ are prime to each other and $ab = ba$ the order of ab is 6.

Since $O(G) = 6$ and there exists an element of order 6 in G, so, G is cyclic.

(Ex): Let n be a positive Integer and let S be the set of n nth roots of unity. Show that $(S, \cdot)$ is a cyclic group. Find all possible generators. V.H.

Ans: The elements of S are $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ where

$$\alpha = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

S is a finite group with respect to multiplication and $O(S) = n$.

n is the least positive integer n such that $\alpha^n = 1$

$\therefore O(\alpha) = n$.

Since S is a finite group containing n elements and $\alpha \in S$ with $O(\alpha) = n$, So, $(S, \cdot)$ is a cyclic group generated by α.

2nd Part: If r be a positive integer, then α^r is a generator of the group if and only if r is less than and prime to n.

The possible generators ~~are the st~~ of the cyclic group $(S, \cdot)$ are the special roots of $x^n - 1 = 0$.

(Ex): How many generators are there of the cyclic group of order 8.

Ans: Let a be a generator of G. Then $O(a) = 8$.

We can write $G = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 (= e)\}$

7 is prime to 8. Therefore a^7 is also a generator of G. Again 5 and 3 are prime to 8. Therefore, a^5, a^3 are also generators of G.

Thus, a, a^3, a^5, a^7 are the generators of the group of order 8.

Theorem: Let (G, o) be a finite cyclic group of order $n > 1$, generated by a. Then for a positive integer r, a^r is also a generator of the group iff r is less than n and prime to n.

Proof: Since $o(G) = n$, $a^n = e$ and $G = \{a, a^2, \ldots, a^n (= e)\}$.

Let a^r be a generator of the group. Then $1 \leq r < n$.

Since a^r is a generator and $a \in G$, $a = (a^r)^k$ for some integer k.

Hence $a^{rk-1} = e$.

Since $o(a) = n$, n is a divisor of $rk-1$.

So, $rk - 1 = sn$ for some integer s.

$\Rightarrow$ $kr + sn = 1$ where k and s are integers.

$\Rightarrow$ $\gcd(r, n) = 1$.

It follows that r is less than n and prime to n.

Conversely, let r be less than n and prime to n. Then $o(a^r) = n$ and therefore a^r is a generator of G.

Hence the theorem.

Theorem: Any two left cosets of H in G have the same cardinality.

Proof: Let aH, bH be two left cosets of H in G. Let us define a mapping $f: aH \to bH$ by $f(ah) = bh$ for every $h \in H$.

To prove that f is injective.

Let us take two distinct elements ah_1, ah_2 in aH.

$\therefore f(ah_1) = bh_1$

and $f(ah_2) = bh_2$

$\therefore f(ah_1) = f(ah_2)$

$\Rightarrow bh_1 = bh_2$

$\Rightarrow h_1 = h_2$ [by cancellation law]

$\Rightarrow ah_1 = ah_2$

Therefore, $ah_1 \neq ah_2 \Rightarrow f(ah_1) \neq f(ah_2)$ and this proves that f is injective.

To prove that f is surjective. Let us take an element bh in bH such that $f(ah) = bh$.

Thus, ah is the pre-image of bh.

Therefore, f is surjective.

Consequently, f is a bijection and therefore aH and bH have the same cardinality.

Theorem: A finite group (G, o) of order n is cyclic iff there exists an element b in G such that $O(b) = n$.

Proof: Let (G, o) be a cyclic group and $G = \langle a \rangle$.

Since $O(G) = n$, $O(a) = n$. There exists element b such that $b = a$.

$\therefore O(b) = n$.

Conversely, Since $O(b) = n$, the elements $b, b^2, \ldots, b^{n-1}, b^n (= e)$ are distinct elements of G. Since $O(G) = n$, $G = \{b, b^2, \ldots, b^n (= e)\}$

Therefore, $G \subseteq \{b^n : n \in Z\}$ ---(i)

Since, $b \in G$, $b^0, b, b^{-1}, b^2, b^{-2}, \ldots \in G$.

$\therefore \{b^n : n \in Z\} \subseteq G$ ---(ii)

From (i) and (ii), $G = \{b^n : n \in Z\}$ Therefore, G is a cyclic group generated by b.

Ex-1 Let $S = \{1, \alpha, \alpha^2, \ldots \alpha^5\}$ where $\alpha = \cos\pi/3 + i\sin\pi/3$. Prove that S is a cyclic group under multiplication.

Ans: We form a composition table as follows.

	1	α	α^2	α^3	α^4	α^5
1	1	α	α^2	α^3	α^4	α^5
α	α	α^2	α^3	α^4	α^5	1
α^2	α^2	α^3	α^4	α^5	1	α
α^3	α^3	α^4	α^5	1	α	α^2
α^4	α^4	α^5	1	α	α^2	α^3
α^5	α^5	1	α	α^2	α^3	α^4

Since $\alpha^6 = (\cos\pi/3 + i\sin\pi/3)^6$

$= \cos 2\pi + i\sin 2\pi$

$= 1$ [De-Moivre's theorem]

$\therefore \alpha^6 = 1$

(i) It clear from the table that S is closed w.r.to multiplication.

(ii) Multiplication is associative.

(iii) 1 is the identity element in S.

(iv) The inverses of $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$ are $1, \alpha^5, \alpha^4, \alpha^3, \alpha^2, \alpha$ respectively.

So, $(S, \cdot)$ is a group w.r.to multiplication.

Since $O(S) = 6$, $O(\alpha) = 6$, 6 is the least positive integer.

Since S is a finite group containing 6 elements and $\alpha \in S$ with $O(\alpha) = 6$, $(S, \cdot)$ is a cyclic group generated by α.

Ex Let $S = \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$ where $\omega = \cos 2\pi/3 + i\sin\frac{2\pi}{3}$. Prove that S is a cyclic group under multiplication.