CYCLIC GROUP

A group (G, o) is said to be a cyclic group if there exists an element 'a' in G such that $G = \{a^n : n \in Z\}$

ie $G = \langle a \rangle$

'a' is said to be a generator of the cyclic group. This is in multiplicative notation.

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

There may be more than one generator of a cyclic group.

Examples

1. $(Z, +)$ is a cyclic group generated by 1.

Because, the set of Integers, with the operation of addition, form a group.

All integers can be written by repeatedly adding the single number 1.

Therefore 1 is the generator of this group.

Again -1 is also another generator of this group.

2. $(S, \cdot)$ is a group, where $S = \{1, w, w^2\}$ where w is the cube root of unity.

Here $(S, \cdot)$ is a cyclic group, because

$S = \{w^3, w^1, w^2\} = \langle w \rangle$

$\therefore$ w is a generator of the group.

Again $S = \{(w^2)^3, (w^2)^2, (w^2)^1\} = \langle w^2 \rangle$

$\therefore$ w^2 is another generator of the group.

3. Let $S = \{1, i, -1, -i\}$, where $i = \sqrt{-1}$

Then $(S, \cdot)$ is a cyclic group generated by i and $-i$.

Because $S = \{i^4, i, i^2, i^3\} = \langle i \rangle$

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

4. $(\mathbb{Z}_4, +)$ is a cyclic group.

We know $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

The composition table is

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

ere $\langle \bar{0} \rangle = \{\bar{0}\}$.

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

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

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

ere $\bar{1}$ and $\bar{3}$ are the generators.

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

Illustration $(-1)^1 = -1$, $(-1)^2 = 1$

ie $S = \langle -1 \rangle$

Theorem: Let $(G, \circ)$ be a cyclic group generated by a. Then a^{-1} is also a generator.

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

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

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

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

Thus $b \in G \Rightarrow b \in H$ and therefore $G \subset H$. $\leftarrow$ (i)

Let $q \in H$, then $q = (a^{-1})^s$ for some integer s.

q can be expressed as a^{-s} and since $-s$ is an integer, $q \in G$.

Thus $q \in H \Rightarrow q \in G$ and therefore $H \subset G$ $\leftarrow$ (ii)

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

That is, $G = \{(a^{-1})^n : n \in \mathbb{Z}\}$.

This proves that a^{-1} is a generator of G.

(4) Theorem 2 — 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 integer r and s.

$p \circ q = a^r \circ a^s = a^{r+s}$

$q \circ p = a^s \cdot a^r = a^{s+r}$

Since $r + s = s + r$, $\therefore p \circ q = q \circ p$ for all $p, q \in G$

Therefore the group is abelian.

Note. An abelian group is not necessarily a cyclic gr
for example Klein's 4-group is abelian
but it is not cyclic.

(5)

Klein's 4-group

Let $S = \{e, a, b, c\}$ and let $\circ$ be the binary composition defined on S by

$e \circ a = a \circ e = a.$

$e \circ b = b \circ e = b,$

$e \circ c = c \circ e = c,$

$e \circ e = a \circ a = b \circ b = c \circ c = e.$

$a \circ b = b \circ a = c$

$a \circ c = c \circ a = b$

$b \circ c = c \circ b = a$

The composition table is given below:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$(S, \circ)$ is an abelian group of order 4.

It is called Klein's 4-group and is denoted by V.

Klein was a German mathematician and V comes from the German word Vierergruppe.

An important property of the Klein-4 group is that every element of the group is its own inverse.

Note Klein's 4-group V is not a cyclic group. (but a

The elements of V are e, a, b, c and none of $\langle e \rangle, \langle a \rangle, \langle b \rangle$ and $\langle c \rangle$ equals V.

Therefore no element of V can generate the whole group V.

(6) **Theorem 3** Let $(G, \circ)$ be a finite cyclic group generated by a. Then $O(G) = n$ if and only if $o(a) = n$

order of a group = No. of elements in G

order of an element (a) of a group if $a^n = e$ then order of the element a is n.

Proof Let $o(a) = n$

then $a, a^2, a^3 \cdots a^n (= e)$ are distinct elements of G.

Therefore $\{a, a^2, a^3 \cdots a^n\} \subset G$ ---- (i)

Again $G = \{a^n : n \in \mathbb{Z}\}$.

Let b be an arbitrary element of G. Then

$b = a^m$ for some integer m.

By division algorithm, there exist integers q and r such that $m = qn + r$ where $0 \leq r < n$.

Therefore, $b = a^m = a^{qn+r} = (a^n)^q \circ a^r = (e)^q \circ a^r$

$= e \circ a^r = a^r \quad [\because a^n = e]$

As $b = a^r$ for some r satisfying

$0 < r \leq n$, $b \in \{a^0, a, a^2 \cdots a^{n-1}\}$

that is $b \in \{a, a^2, \cdots a^{n-1}, a^n (= e)\}$

Therefore $G \subset \{a, a^2, \cdots, a^{n-1}, a^n\}$ --- (ii)

from (i) & (ii), $G = \{a, a^2, \cdots a^{n-1}, a^n\}$

and therefore $O(G) = n$.

Conversely,

Let $O(G) = n$

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

(7) Let $o(a) = k$
Then $a, a^2, a^{k-1}, a^k = (e)$ are distinct elements of G.
Since G contains n elements, $k \leq n$.
But k is not less than n, because by the foregoing argument, $o(a) = k$ implies that $o(G) = k$, a contradiction.
Therefore $o(a) = n$ and this completes the proof.

Corollary If $G = \langle a \rangle$ and $o(a) = n$, then
$G = \{a, a^2, \cdots a^n (= e)\}$.

(8)

Th 4 Let $(G, \circ)$ be a cyclic group generated by a. Then G is infinite if and only if $o(a)$ is infinite.

Proof Let $o(a)$ be infinite. Then the set $\{a, a^2, a^3, \dots\}$ is an infinite set of distinct elements.

If not, let $a^r = a^s$ for some positive integer r, s where $r > s$.

Therefore $a^{r-s} = e$ and this implies that $o(a)$ is finite, a contradiction.

But $\{a, a^2, a^3, \dots\} \subset G$

Hence $o(G)$ is infinite.

Conversely,

Let $o(G)$ be infinite.

If possible, let $o(a)$ be finite.

Then $o(G)$ is finite by Th. 3

and this is a contradiction.

Hence $o(a)$ is infinite.

(9) Th 5 . A finite group $(G, \circ)$ of order n is cyclic if and only if there exists an element b in G such that $o(b) = n$.

Proof Let $(G, \circ)$ be a cyclic group and let $G = \langle a \rangle$

Since $o(G) = n$, $o(a) = n$.

Therefore b exists and $b = a$

Conversely,

Let $o(G) = n$ and there exists one element b in G such that $o(b) = n$.

Since $o(b) = n$, then elements $b, b^2, b^3, \ldots b^{n-1}, b^n (= e)$ are distinct element of G

Since $o(G) = n$, $G = \{ b, b^2, \ldots b^n \}$.

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

Since $b \in G$, $b^0, b, b^{-1}, b^2, b^{-2}$ ... all belongs to G

Therefore $\{ b^n : n \in \mathbb{Z} \} \subset G$ ---(ii)

from (i) and (ii), $G = \{ b^n : n \in \mathbb{Z} \}$

Therefore G is a cyclic group generated by b.