Cyclic Groups

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

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

For example:-

i) $(Z, +)$ is a cyclic group generated by (-1) and $+1$

ii) $(Z_4, +)$ is a cyclic group generated by $\bar{1}$ and $\bar{3}$.

iii) $S = \{1, i, -1, -i\}$ is a cyclic group generated by $i, -i$.

Note:- Klein's 4 group V is not a cyclic group since no element of V can generate the whole group V.

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

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 since $-r$ is an

integer, $b \in H$

thus $b \in G \Rightarrow b \in H$ and therefore $G \subset H$ — (i)

let $q \in H$ then $q = (\bar{a}^1)^s$ for some integer s.

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

thus $q \in H \Rightarrow q \in G$ and therefore $H \subset G$ — (ii)

from (i) and (ii) $G = H$; that is $G = \{(\bar{a}^1)^n : n \in Z\}$

this proves that $\bar{a}^1$ is a generator of G.

(2) Every cyclic group is abelian

proof:- Let (G, o) be a cyclic group generated by a

Let $p, q \in G$, then $p = a^r$ and $q = a^s$ for some integer r and s.

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

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

since $(r+s) = (s+r)$ so $p \circ q = q \circ p$ for all $p, q \in G$

$\therefore$ the group is abelian.

Note:- 1) An abelian group is not necessarily a cyclic group. For example, Klein's 4 group V is abelian but it is not cyclic.

2) The symmetric group S_3 is not cyclic since it is not abelian.

(3) The dihedral group D_4 is not cyclic. Since it is not abelian.

Some remarks

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

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

(3) Let (G,o) be a cyclic group generated by a. Then G is infinite iff $o(a)$ is infinite.

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

(5) 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.

(6) The total number of generators of a finite cyclic group of order n is $\phi(n)$ where $\phi(1) = 1$ and for $n > 2$; $\phi(n)$ = the number of positive integers less than n and prime to n.