CYCLIC GROUP - 2

Theorem - 6 Let $(G, \circ)$ be a finite cyclic group of order $n > 1$, generated by a. Then for any positive integer r, a^r is also a generator of the group if and only if r is less than n and prime to n.

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

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

Since a^r is a generator and $a \in G$,

$$a = (a^r)^k \text{ for some integer } k.$$

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

We know theorem that,

"If a be an element of a group $(G, \circ)$, where $o(a) = n$ and $a^m = e$, then n is a divisor of m."

Here $o(a) = n$ and $a^{rk-1} = e$.

So by the above theorem n is a divisor of $(rk-1)$.

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

ie $kr + sn = 1$ where k and s are integers and this implies $\gcd(r, n) = 1$.

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

Conversely, let r be less than and prime to n.

We know the theorem that,

"If a be an element of a group $(G, \circ)$ where $o(a) = n$, then $o(a^p) = n$ if and only if p is prime to n."

So by the above theorem, $o(a^r) = n$, and therefore a^r is a generator of G.

This completes the proof.

2

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

Examples –

1. The number of generators of the cyclic group $(S, \cdot)$ where $S = \{1, i, -1, -i\}$ is 2, since $\phi(4) = 2$.

2. The number of generators of the cyclic group of a prime order p is $p-1$ since $\phi(p) = p-1$. Therefore each non-identity element of the group is a generator.

3. The number of generators of the cyclic group $(\mathbb{Z}_2, +)$ is 1, since $\phi(2) = 1$

Theorem 7. Every subgroup of a cyclic group is cyclic.

Proof Let $(G, \cdot)$ be a cyclic group generated by a and let $(H, \cdot)$ be a subgroup of G.

If $H = G$ there is nothing to prove. We consider two cases.

Case I. $H = \{e\}$. Since $e^n = e$ for all $n \in \mathbb{Z}$, $H = \{e^n : n \in \mathbb{Z}\}$.
Therefore H is the cyclic group $\langle e \rangle$.

Case II   H is a proper subgroup of G other than the trivial subgroup $\{e\}$.

Then there is an element x in H such that $x \neq e$

Since $x \in G$, $x = a^k$ for some integer $k \neq 0$

Since H is a subgroup, $x \in H \Rightarrow x^{-1} \in H$

and $x^{-1} = a^{-k}$.

So a^k and a^{-k} both belong to H for some integer $k \neq 0$.

Therefore there are some positive integral powers of a in H.

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

Such an m exists by the well ordering property of the set $\mathbb{N}$.

We propose to prove that a^m is a generator of H.

Let h be an element of H.

Then $h = a^p$ for some integer p.

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

$p = qm + r$

Since H is a subgroup, $a^m \in H \Rightarrow a^{-qm} \in H$.

Also $a^p \in H$ and $a^{-qm} \in H \Rightarrow a^{p-qm} \in H$ ie $a^r \in H$.

But $0 \leq r < m$ and $a^r \in H$ are both satisfied only if $r = 0$, because otherwise m fails to be the smallest positive integral power of a in H.

Consequently, $p = qm$ and therefore $h = (a^m)^q$ where q is an integer.

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

This completes the proof.

Note 1. If a subgroup H of a finite cyclic group $G (= \langle a \rangle)$ of order n is generated by a^m, then m is a divisor of n.

Note 2 For a cyclic group G, the cyclic subgroups generated by different elements of G are the only subgroups of G.

Theorem 8

A cyclic group of prime order has no proper non-trivial subgroup.

Proof Let $(G, \circ)$ be a cyclic group of prime order p and let $G = \langle a \rangle$.

Let $(H, \circ)$ be a cyclic subgroup generated by a^m where m is the least positive integer such that $a^m \in H$.

Since $o(G) = p$, $a^p = e$

Since $H = \langle a^m \rangle$ and $a^p \in H$, $p = mk$ for some positive integer k.

Therefore m is a divisor of p.

Since p is a prime, m is either 1 or p.

But $m = 1$ implies that $H = G$, $m = p$ implies that $H = \{e\}$.

Therefore $(H, \circ)$ is either the trivial subgroup $\{e\}$, or the improper subgroup G.

This completes the proof.