Cyclic-Group

Def^{n}. (Cyclic Group):- A group G_1 is called cyclic if, for some $a \in G_1$, every element $x \in G_1$ is of the form a^n, where n is some integer. The element a is then called a generator of G_1.

(Theorem 1.) Every cyclic group is an abelian group.

Proof:- Let $G_1 = \{a\}$ be a cyclic group generated by a.

Let x, y be any two elements of G_1.

Then $\exists$ integers r and s such that, $x = a^r, y = a^s$.

Now $xy = a^r, a^s = a^{r+s} = a^{s+r}$

$= a^s a^r = yx$.

Thus, we have $xy = yx \; \forall \; x, y \in G_1$.

Therefore G_1 is abelian.

(Theorem 2):- A cyclic group G_1 with generator of finite order n, is isomorphic to the multiplicative group of n nth roots of unity.

Proof:- Let a be a generator of the cyclic group G_1. Since the order of a is n, therefore n is the least +ve integer such that,

$$a^n = e.$$

We shall show that the group G_1 has exactly n distinct elements,

$$a, a^2, a^3, \text{----} a^n = e = a^0 \text{ ---- } (1)$$

No two elements of (1) can be equal. For if Possible, let

$a^r = a^s$, $1 \leq s < r \leq n$. Then $a^{r-s} = a^0 = e$.

Since $0 < r - s < n$, therefore $a^{r-s} = e$ implies that the order

of a is less than n.

Hence, $a^r \neq a^s$.

Therefore all the n elements in ① are distinct. Again, let a^t be any element of G_1. By division algorithm, there exist two integers p & q such that,

$t = np + q$, $0 \leq q < n$. [We can write $t/n = p + q/n$]

$\therefore a^t = a^{np+q}$

$= a^{np} a^q = (a^n)^p a^q = e^p a^q = e a^q = a^q$.

Since $0 \leq q < n$, therefore a^q is one of the n elements in ①. Thus each element of G_1 is equal to some member of ①. Therefore G_1 has exactly n elements given in ①. Thus $O(a) = o(G_1)$.

We shall now show that G_1 is isomorphic to the multiplicative group G_1' of the n nth roots of unity, namely,

$1 = e^{2\pi i 0/n}, e^{2\pi i/n}, e^{4\pi i/n}, \cdots, e^{2\pi r i/n}, \cdots e^{2\pi(n-1)i/n}$

Consider the mapping $f: G_1 \to G_1'$ defined by

$f(a^r) = e^{2\pi i r/n}$, where $0 \leq r \leq n-1$.

The mapping f is one-one. Since

$f(a^r) = f(a^s)$, where $0 \leq r \leq n-1$, $0 \leq s \leq n-1$.

$\Rightarrow e^{2\pi i r/n} = e^{2\pi i s/n} \Rightarrow r = s \Rightarrow a^r = a^s$.

Again, the number of elements in G_1 is equal to the number of elements in G_1'. Therefore f is one-one implies f must be onto G_1'.

Finally, $f(a^r a^s) = f(a^{r+s}) = f(a^{nu+k})$, where u is some integer & $0 \leq k < n$

$= f(a^{nu} a^k) = f[(a^n)^u a^k]$

$= f(a^k)$ $[\because a^n = e]$

$= e^{2\pi ki/n}$ [by defⁿ of f]

$= e^{2\pi nui/n} e^{2\pi ki/n}$ $[\because e^{2\pi ui} = 1]$

$= e^{2\pi i(nu+k)/n}$

$= e^{2\pi i(r+\beta)/n} = e^{2\pi ir/n} e^{2\pi i\beta n} = f(a^r) f(a^\beta)$.

Therefore f Preserves Combositions in G_1 and G_1'. Hence G_1 is isomorphic to G_1'.

Since every finite cyclic group of order n is isomorphic to the multiplicative group of n nth roots of unity.

(Theorem 3):- Every group of Prime order is cyclic.

Proof:- Suppose G_1 is a finite group whose order is a Prime number p, then to prove that G_1 is a cyclic group, and its only divisors of p are $\pm 1, \pm p$.

Since G_1 is a group of Prime order, therefore G_1 must Contain at least 2 elements. Therefore, there must exist an element $a \in G_1$ such that $a \neq$ the identity element e.

Since a is not the identity element, therefore $o(a)$ is definitely ≥ 2. Let $o(a) = m$. If H is the cyclic subgroup of G_1, generated by a, then $o(H) = o(a) = m$ [By Lagrang's theorem m must be a divisor of p.]

But p is Prime and $m \geq 2$. Hence $m = p$.

$\therefore H = G_1$. Since H is cyclic therefore G_1 is cyclic and a is a generator of G_1.