Dr. O. P. Raman
Dept of Mathematics

For T.D.C. Part II
Paper - 3

Abstract (Modern) Algebra

21. *Define with examples*
(i) order of a group, (ii) order of an element of a group.

Definition

(i) *Order of a group*

A group with n elements, where n is finite, is said to have the order n.

Examples

1. $G = \{1, -1, i, -i\}$ where $i^2 = -1$, is a group of four elements under multiplication of complex numbers. So this is a group of order 4.

2. if w be one of the imaginary cube roots of unity then $\{1, w, w^2\}$ is a group under multiplication. So this group is of order 3.

If the number of elements in a group is infinite, the group is said to be of infinite order.

Examples

1. The set R of real numbers is a group of infinite order under ordinary addition.

2. The set C of all complex numbers is a group of infinite order with respect to addition.

(ii) *Order of an element of a group.*

The order of an element a of a group (G, o) is the least positive integer n such that $a^n = e$, the identity element of group where $a \circ a \circ a \circ a \circ \ldots$ up to n times is denoted by a^n.

The order of an element a is denoted by $O(a)$.

If no such positive integer n exists such that $a^n = e$, we say the order of the element a is zero (or infinite).

Clearly order of the identity element e is 1.

8. **The order of an element a of a group is the same as that of its inverse a i.e., $o(a) = o(a^{-1})$.**

Proof : Let n and m be the orders of a and a^{-1} respectively so that

$$a^n = e \text{ and } (a^{-1})^m = e.$$

Now, $a^n = e \Rightarrow (a^n)^{-1} = e^{-1} \Rightarrow (a^{-1})^n = e$

$$\Rightarrow o(a^{-1}) \leq n \Rightarrow m \leq n$$

Again, $(a^{-1})^m = e \Rightarrow (a^m)^{-1} = e$

$$\Rightarrow a^m = e \Rightarrow o(a) \leq m$$

$$\Rightarrow n \leq m$$

Thus (1) and (2), $m \leq n, n \leq m \Rightarrow m = n$.

Hence proved.

Cyclic Group: *If a group G contains an element a such that every element of G is of the form a^k for some integer k, we say that G is a cyclic group and that G is generated by a or that a is a generator of G.*

Taking additive composition, each element of the cyclic group is some positive or negative multiples of the generator i.e., of the form $na = a + a + \ldots + a$ (n times), where a is the generator.

The fact that G is a cyclic group generated by a is denoted by the symbol $G = \langle a \rangle$.

▸ **Ex.1.** *Prove that the set G consisting of four fourth roots of unity i.e., $G = \{1, -1, i, -i\}$ is a cyclic group.*

Soln. We know that G is a group and now it can be shown that G forms a cyclic group with generators i and $-i$ since.

$i = i$	$-i = -i$
$(i)^2 = -1$	$(-i)^2 = -1$
$(i)^3 = -i$	$(-i)^3 = i$
$(i)^4 = 1$	$(-i)^4 = 1$

It can be readily seen that 1 or -1 cannot be used as generators for G.

Every subgroup H of a cyclic group G is also a cyclic group.

Proof : Suppose that the cyclic group G is generated by a and let H be a subgroup of G.

Then every member of H will be evidently some integral powers of a, positive or negative.

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

We shall show that H is a cyclic subgroup generated by a^m.

Let a^k be any element of H.

Obviously $k > m$.

By the division algorithm, we may write, $k = qm + r$, where $0 \leq r < m$.

Hence $a^k = a^{qm+r} = (a^m)^q \cdot a^r$

$\Rightarrow \quad a^r = a^k \cdot (a^m)^{-q}$.

Since $a^m \in H$ and $a^k \in H$, this equation implies that $a^r \in H$.

But m is the smallest positive integer such that $a^m \in H$. Since $r < m$, we must have $r = 0$.

Therefore $k = qm$ and hence every element a^k of H is of the form $(a^m)^q$ for some integer k.

This shows that H is a cyclic group generated by a^m, i.e., a^m is a generator of H.

Q. *prove that every group of prime order is a cyclic group.* (5)

Proof. Let G be a group of order p, p being a prime number. Let $e \neq a \in G$. By closure law, $a^m \in G$ for all m.

But G has only finite number of elements.

So we get $H = \{a, a^2, a^3, \ldots, a^k = e\}$, a finite subgroup of G.

No two elements of H are equal for otherwise

$$a^i = a^j \Rightarrow a^{i-j} = e = a^k$$

which is impossible because $i - j < k$, each of i, j being less then k.

Thus the order of the subgroup $H = k$. By Lagrange's theorem p is a multiple of k say $p = kt$. But p is prime.

It is only possible when $t = 1$ i.e. $p = k$.

$\therefore$ $G = H$. But H is a cyclic group with the generator a. Hence G is a cyclic group.

For this, we will have to show that the cyclic group G has exactly n distinct elements

$$a, a^2, a^3, \ldots, a^n = e = a^0 \qquad \ldots(2)$$

Now let us verify whether any two elements of (2) are equal or not.

If possible, let $a^r = a^s$, where $0 < s < r < n$.

Then $a^r \cdot a^{-s} = a^s \cdot a^{-s} \Rightarrow a^{r-s} = a^0 = e$,

where $r - s$ is positive integer less than n.

But this is not possible because n is the order of a. Hence there cannot be any other integer $r - s < n$ such that $a^{r-s} = e$. That is,

$$a^{r-s} \neq e \Rightarrow a^r \neq a^s.$$

Hence all the elements in (2) are distinct.

Now we shall show that the set (2) shall not contain more than n elements.

Let a^p be any element of G, where p be any integer greater than n.

Then there exist integers q and r such that

$$p = nq + r, \text{ where } 0 \leq r < n.$$

$$\therefore a^p = a^{nq+r} = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = e \cdot a^r.$$

Since $0 \leq r < n$, therefore a^r is one of the n elements of (2). This shows that the set (2) shall not contain more than n elements. At the same time these elements are distinct. Hence G has exactly n elements given in (2).

That is, $O(G) = O(a)$.