Group Theory

2. Order of a group:

A group is said to be finite if it has a finite number of elements. Otherwise, it is said to be infinite. The number of elements of a finite group is called the order of the group.

Example: The finite group $S=\{1,-1,i,-i\}$ is group of order 4 under ordinary multiplication.

The group of all integers $G=\{....,-2,-1,0,1,2...\}$ is an infinite group under addition.

Cyclic group: Consider a group $G=\{a,b,c....\}$, which may not be finite. Suppose that all the elements of G can be created by taking the powers of an appropriately chosen element, say a of G. Then G is called a cyclic group, and a is called a generator of the group.

Example: Consider a finite group

$S=\{1,-1,i,-i\}$ $\odot =$ ordinary multiplication

$(i)^1=i,\quad (i)^2=-1$

$$(i)^3 = i, \quad (i)^4 = 1$$

Thus, whole group is generated by taking only the positive powers of element i. The element i is a generator of the group. We may also generate the same group by taking only negative power of i. We may also generate this group by taking positive power of $-i$. The generator of a cyclic group is therefore not necessarily unique.

Consider an infinite group of even integer,

$$\{....,-6,-4,-2,0,2,4,6,....\}$$

in which law of composition is ordinary addition.

The group can be generated by taking integral (positive and negative) multiple of its element, which is thus a generator of the group. The element $-i$ is another generator of this group.

We observe that if 'a' is generator of a cyclic group, then each element of the group has the form a^p (multiplicative notation) or pa (additive notation) where p is an integer.

Order of Cyclic Group: A finite cyclic $G(q_1,q_2,....q_n)$ group whose generator is 'a' can be represented (multiplication notation)

$$G = \{a, a^2, a^3, ...a^n\}$$

If p is the smallest positive integer for which $g^p = e$, where e is the identity element, then p is called the order. Period or cycle of the element 'g'. If p is the order of generator of a cyclic group, i.e. $a^p = 1$ then it is also an order of the cyclic group.

Thus, $G = \{1, a, a^2, a^3, ...a^{n-1}\}$

In the example $\{1,-1,i,-i\}$, order of element $1=1 \quad \because (1)^1 = 1$

Order of element $(-1)^2 = 1 = 2$

Order of element $i=4 \qquad \because (i)^4 = 1$

Order of element $-i=4 \qquad (-i)^4 = 1$

Since i in generator and $(i)^4 = 1$, therefore the order of group is 4.

Example: Show that $z_n = \{0,1,2,3,4,5,6\} \odot$ mod is cyclic group.

$$1+1=2 \qquad\qquad 3+3=6$$

$1+1+1=3$	$3+3+3=2$
$1+1+1+1=4$	$3+3+3+3=5$
$1+1+1+1+1=5$	$3+3+3+3+3=1$
$1+1+1+1+1+1=6$	$3+3+3+3+3+3=4$
$1+1+1+1+1+1+1=0$	$3+3+3+3+3+3+3=0$

It turns out that $z_n=\{0,1,2,3,4,5,6\}$, every non zero element generates the group.

Example: $z_6=\{0,1,2,3,4,5\}\odot$ mod 6 only 1 and 5 are generators.

Cyclic group are abelian.

A result

It can be shown that order p of an element of group is divisor of order of group.

If m is order of an element 'a' of group of order n then m is divisor of n.

Example: Set $G\{a,b,c\}$

(a) What are the possible order of each element of G other than the identity?

Solution: G is group of order four, hence the possible order of a,b,c are 2 or 4.

(b) If each of the elements a,b,c have the same order, what can it be?

Solution: If $a^4=e$, then group $G=\{e,a,b,c\}$ can be written as $G=\{e,a,a^2,a^3\}$

Then order of b and c must be a^2

Now $\left(a^2\right)^2=a^4=e$

order of b or $c=2$

Then all of (a,b,c) can not have order 4 on the other hand each (a,b,c) can have order of two.

$$a^2=e$$

$$b^2=\left(a^2\right)^2=e$$

$$c^2=\left(a^2\right)^2=e$$