Study Material

UG. Sem III (Mathematics)

Paper - CC6

(Group Theory)

Date: 9/5/20
Dr. M. A. Khan
Associate Prof.
Dept. of Mathematics
Tata College,
Chaibasa

Order of a group:- A group which has a finite number of elements is called a finite group and number of its elements is called the order of the group.

For example, a group G has n elements where n is a positive integer, G is said to be a group of order n. We denote this by writing $O(G) = n$.

If there exists no such positive integer, G is said to have infinite order.

Ex:- (i) The additive group of integers has infinite order

(ii) The multiplicative group $\{1, -1, i, -i\}$ is of finite order 4.

Order of an element of a group:-

An element of a group G is said to be of order n if n is the least positive integer such that $a^n = e$, where e is the identity element of G. Thus $a^k = e$ and $k \neq n \Rightarrow k > n$.

Ex:- find the order of the elements of the multiplicative group $G = \{1, -1, i, -i\}$

The order of $1 = 1$ i.e $o(1) = 1$ as $1^1 = 1$

order of $-1 = o(-1) = 2$ as $(-1)^2 = 1$

order of $1 = o(i) = 4$ as $i^4 = 1$

or of of $-i = o(-i) = 4$ as $(-i)^4 = 1$

Theorem:- The order of every element of a finite group is finite and is less than or equal to the order of the group.

Proof:- Let G be a finite group. Let $a \in G$. Consider all positive integral powers of a i.e $a, a^2, a^3, a^4, \ldots$

By closure law, these are all elements of G.

Since G has a finite number of elements, therefore all these integral powers of a cannot be distinct elements of G.

Let us suppose that $a^r = a^s$ $(r > s)$

Now $a^r = a^s \Rightarrow a^r a^{-s} = a^s a^{-s}$

$\Rightarrow a^{r-s} = a^{s-s}$

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

Let $r - s = m$ So that $a^m = e$

$\because r > s$, m is a positive integer.

Thus there exist a positive number m such that $a^m = e$.

Now by well ordering principle, we know that every set of positive integer has a least member.

Therefore the set of all those positive integer m such that $a^m = e$ has a least member, say n. Thus there exits a least positive integer n such that $a^n = e$. Therefore order of a i.e. $O(a)$ is finite.

Now we need to prove that $o(a) \leq o(G)$

i.e $o(a) \leq n$ where $n = o(G)$

On Contrary, let $o(a) = p$, say where $p > n$

$\because a \in G$, therefore by closure property,

$a, a^2, a^3, \ldots a^n$ are elements of G.

No two of these elements are equal.

For if possible,

Let $a^r = a^s$ where $1 \leq s < r \leq n$.

Then $a^{r-s} = e$

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

$\Rightarrow$ the order of a is less than n.

But we have assumed that $o(a) > n$.

This is a contradiction.

Hence $a, a^2, a^3, \ldots a^n$ are distinct elements of G.

Since $p > o(G)$, this is not possible

Hence we must have $o(a) \leq n$

i.e. $o(a) \leq o(G)$.

2020.05.9