B.Sc Part II (Hons)

Order of an element

Definition(1) Let e be the identity in a group G. An element $a \in G$ is said to be order (or period) n if n is the least positive integer such that

$$a^n = e.$$

Definition (2) - An element $a \in G$ is of order n if n is a positive integer s.t. $a^n = e$ and $a^r \neq e$ $\forall r \in N$ such that $r < n$.

The order of a is denoted by $o(a)$.

If $a^n \neq e$ for any $n \in N$

then a is said to be of zero order or infinite order.

Additive Composition:- An element a of a group $(G, +)$ is said to be of order n if n is the least positive integer such that

$na = e$ = identity of G.

i.e. if $na = e$ and $ra \neq e$ for $0 < r < n$.

If $na \neq e$ for any positive integer n then a is said to be of zero order or infinite order

Example:- Let $G = \{1, -1, i, -i\}$ be a multiplicative group. Find the order of every element.

Solution:- 1 is the identity element in G.

(i) $1^1 = 1 \Rightarrow o(1) = 1$.

(ii) $(-1)^2 = 1$, $(-1)^n \neq 1$ for any positive integer $n < 2$.

This $\Rightarrow o(-1) = 2$.

(iii) $\Rightarrow (i)^4 = 1$ and $(i)^n \neq 1$ for any positive integer $n < 4$. This $\Rightarrow o(i) = 4$.

(iv) $(-i)^4 = 1$ and $(-i)^n \neq 1$ for any positive integer $n < 4$ This $\Rightarrow o(-i) = 4$.

Lagrange's Theorem :— The order of each subgroup of a finite group is a divisor (factor) of the order of the group.

Proof:— Let H be a subgroup of a finite group G and let $O(G) = n$, $O(H) = m$.

To prove m is a divisor of n.

For this we have to prove that $n = mp$ for some $p \in N$.

Let Ha be any right coset of H in G.

$O(H) = m \Rightarrow \exists$ m distinct elements $h_1, h_2, \dots h_m \in H$

$\Rightarrow \exists$ m distinct elements $h_1a, h_2a, \dots h_ma \in Ha$.

For any map from H into Ha is one-one onto.

$\Rightarrow O(Ha) = m = O(H)$ $\forall$ $a \in G$.

This means that every right coset of H in G has m distinct elements. Since G is finite and hence number of distinct right cosets of H in G will be finite. Say P. We also know that any two right cosets of H will be either identical or disjoint. Hence P distinct right cosets of H in G will contain mp distinct elements.

$\therefore G = H \cup Ha \cup Hb \cup Hc, \dots$ Where $a, b, c, \dots \in G$.

$O(G) = O(H) + O(Ha) + O(Hb) + \dots = m + m + \dots$ p times.

Consequently G will contain exactly mp distinct elements, so that $O(G) = mp$.

$O(G) = mp \Rightarrow n = mp$

For $O(G) = n$.

Hence the theorem.