

Question 11] Define order of an element of a group. Prove that the order of every element of a finite group is finite and is less than or equal to the order of the group.

Answer. Definition:- Suppose G is a group and the composition has been denoted multiplicatively. By the order of an element $a \in G$ is meant the positive integer n , if one exists, such that

$$a^n = e \quad [\text{the identity of } G].$$

If there exists no positive integer n such that $a^n = e$, then we say that a is of infinite order or of zero order.

The order of a is denoted by $o(a)$. In additive notation we use the words $na = e$ in place of $a^n = e$.

Proof of the theorem: Let us suppose G be a finite group, the composition being denoted multiplicatively. Let $a \in G$. Consider all the ~~integers~~ integral powers of a i.e. a, a^2, a^3, a^4, \dots . All those are elements of G , by closure axiom. Since G has a finite number of elements, therefore all these integral powers of a cannot be distinct element of G .

Suppose $a^r = a^s$ ($r > s$)

$$\text{Now } a^r = a^s \Rightarrow a^r a^{-s} = a^s a^{-s} \quad [\because a^{-s} \in G]$$

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

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

$$\Rightarrow a^m = e \text{ where } m = r-s$$

Since $r > s$, therefore m is a negative integer. Thus there exists a positive integer m such that $a^m = e$. Since every set of integers has a least number. Therefore the set of all those positive integers m such that $a^m = e$ has least number say n . Thus there exists a least positive integer n such that $a^n = e$.

Therefore $o(a)$ is finite.

Now we shall try to prove that $o(a) \leq o(G)$.

Let $o(a) = n$ where $n > o(G)$. Since $a \in G$, therefore by closure property a, a^2, a^3, \dots, a^n are elements of G . Now two of these are equal. For if possible, let $a^r = a^s$, $1 \leq s < n$. Then $a^{r-s} = e$. Since $0 < r-s < n$, therefore $a^{r-s} = e$ implies that the order of a is less than n . This is a contradiction. Hence a, a^2, a^3, \dots, a^n are not distinct elements of G . Since $n > o(G)$, therefore this is not possible. Hence we must have $o(a) \leq o(G)$.

Nence the theorem

C.S.
 Deptt. of maths
 Sherukhan College, Srinagar