Lecturered By Dr. H.K. Yadav.
Deptt. of Mathematics.
Marwari College, Darbhanga.
B.Sc. part-I(H), paper-I, Date-30-04-2020

Algebra:

Q.1. Define order of an element in a group G, prove that: (I) $o(a)=o(a^{-1})$ (II) $o(ab)=o(ba)$ (III) $o(a)=o(x^{-1}ax)$, for all $x\in G$, where $a,b\in G$ and $o(a)$ stands for order of a in G.

Soln: Order of an element in a group:—

Let $(G,\circ)$ be any group. Then the least positive integer n, if it exists such that $a^n=e$ (identity) is called the order of $a\in G$.

If, however, there does not exist n for which $a^n=e$, then, the order of a is infinite.

The identity of every group has order 1.

The order of an element $a\in G$ is denoted by $o(a)$.

Proof: (I) $o(a)=o(a^{-1})$, $\forall\, a\in G$.

Let G be a group and $a\in G$.
Let a^{-1} be the inverse of a.
Then $a^{-1}\in G$. Let $o(a)=m$ and $o(a^{-1})=n$
Then, by definition of order of an element in a group, we have

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

We know that the order of any power of an element of a group cannot exceed the order of the element.
Since, a^{-1} is a power of a, therefore

$$o(a^{-1})\le o(a)$$
$$\Rightarrow n\le m \quad \text{——— (I)}$$
$$\Rightarrow (a^{-1})^n=e$$
$$\Rightarrow a^{-n}=e$$
$$\Rightarrow a^{-n}a=ea$$
$$\Rightarrow a^{-(n-1)}=a \quad [\because \text{by identity axiom}]$$
$$\Rightarrow (a^{-1})^{n-1}=a$$

this shows that a is equal to some power of a^{-1}.

$$\therefore\ o(a)\le o(a^{-1})$$
$$\Rightarrow m\le n \quad \text{——— II}$$

From I and II, we infer that $m=n$. Proved.

B.Sc - part-I (H), paper-I, Algebra, Date - 30-04-2020

Q.1 (ii) proof: $o(ab) = o(ba)$, $\forall\ a, b \in G$.

We have, $a^{-1}(ab)a = (a^{-1}a)(ba)$ [$\because$ by associative axiom]

$= e(ba)$ [$\because$ by inverse axiom]

$= ba$ [$\because$ by identity axiom]

We know that the order of ab = the order of $a^{-1}(ab)a$.

Hence, $o(ab) = o(ba)$

(iii) $o(a) = o(x^{-1}ax)$

$\Rightarrow o(a) = o(x^{-1}ax)$

Let $o(a) = m$, hence m is the least positive integer, such that $a^m = e$

Now, $(x^{-1}ax)^2 = (x^{-1}ax)(x^{-1}ax) = x^{-1}a(xx^{-1})ab$ [$\because$ by associativity]

$\Rightarrow (x^{-1}ax)^2 = x^{-1}aeax$ [$\because xx^{-1} = e$]

$= x^{-1}a^2x$ [$\because ae = a$]

Similarly, $(x^{-1}ax)^3 = x^{-1}a^3x$

$\Rightarrow (x^{-1}ax)^3 = (x^{-1}ax)(x^{-1}ax) \ldots$ to m factors.

$= x^{-1}axx^{-1}ax \ldots x^{-1}ax$ [$\because$ By associativity]

$= x^{-1}a(xx^{-1})a(xx^{-1}) \ldots (xx^{-1})ax$ [$\because$ By associativity]

$= x^{-1}a^mx = x^{-1}ex = x^{-1}x = e$ [$\because a^m = e$]

Thus, we have $(x^{-1}ax)^m = x^{-1}a^mx = e$

Now, since, m is the least positive integer such that $a^m = e$, it follows that m is the least positive integer such that

$(x^{-1}ax)^m = e$

Hence, $o(x^{-1}ax) = m$

proved.

Q.2. The order of any integral power of an element a cannot exceed the order of a.

Proof: Let a^r by any integral power of a and let $o(a) = n$

Now, $o(a) = n \Rightarrow a^n = e$

$\Rightarrow (a^n)^r = e^r \Rightarrow a^{nr} = e$

$\Rightarrow (a^r)^n = e \Rightarrow o(a^r) \le n$.

$\Rightarrow o(a^r)$ cannot exceed the $o(a)$.

Proved.