Lecturered By Dr. H.K. Yadav
Deptt. of Mathematics, Marwari College, D1310.
B.Sc - part-I (H). paper-I. 11-05-2020

Q.1: Define Cyclic groups and give an example?

Soln: Cyclic Groups: → If a group G contains an element a such that every element $x \in G$ is of the form a^m, where $m \in Z$, then G is said to be cyclic group and G is generated by a i.e. a is the generator of G, and we write $G = (a)$.

For example:

The multiplicative group $G = \{1, -1, i, -i\}$ is a cyclic group with generator i,

$(i)^1 = i, (i)^2 = -1, (i)^3 = -i$ and $(i)^4 = 1$

⇒ each element of G can be expressed as some integral power of i.

⇒ G is cyclic, generated by i.

Q.2: Every cyclic group is necessarily abelian but the converse is not necessarily true.

Proof: Let $G = \{a\}$ is a cyclic group generated by an element $a \in G$.

Let x and y be any two elements of G.

Then $x = a^m$ and $y = a^n$, for some integer m and n.

Now, $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n . a^m = yx$

⇒ $xy = yx \;\; \forall x, y \in G$.

⇒ G is abelian.

Conversely: An abelian group is not always a cyclic groups. It is illustrated by the following example.

The set R_0 of all non-zero real numbers is an abelian group with respect to multiplication.

If $a \in R_0$, then $H = \{a^n : n \in Z\}$ is a countable subset of R_0 and so it can not be equal to the uncountable set R_0.

⇒ All the elements of R_0 cannot be expressed as some integral power of a single element of R_0.

⇒ $(R_0, *)$ is not cyclic group.

B.Sc-part-I(H), paper-I Date- 11-05-2020.

Q.3. The order of a cyclic group is equal to the order of any generator of the group.

Proof: Let a be the generator of a group $G = \{a\}$.

Let $o(a) =$ finite $= n$.

$\Rightarrow a^n = e, a^r \neq e$ for $0 < r < n$.

We have to prove that $o(a) = o(G) = n$

Step-I First of all, we show G contains n elements

The elements of the cyclic group G is given below:

$a, a^2, a^3, \ldots a^n = e = a^0$.

Let if possible, G contains an element a^m besides these elements where $m > n$. Then by division algorithm.

$m = nq + r, \; 0 \leq r < n$ and $q, r \in N$.

$a^m = a^{nq+r} = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = e \cdot a^r = a^r$.

$\therefore a^m = a^r, \; 0 \leq r < n$

$\because a^r$ is already contained in the set of n elements and so a^m is also contained

$\Rightarrow G$ contains n elements.

Step-II. Now we have to show that any two elements of G are not equal. For this, we have to show that $a^r \neq a^s$, where $r \neq s, 0 < r < n, 0 < s < n$.

Let $r < s < n$

then $s - r > 0$

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

$\Rightarrow o(a) \leq s - r$ and $s - r < n$

$\Rightarrow o(a) < n$.

Which is a contradiction. Hence, $a^r \neq a^s$ where $r \neq s$.

Thus, we have shown that G contains n distinct elements and hence $o(G) = n$.

Hence, the order of a cyclic group is equal to the order of any generator of the group.

Proved.