A group (multiplicative) G is said to be cyclic if its all element can be generated by single element.

IV B - (5)

Page No.
Date

Q(10) Define cyclic group.

Soln:- A group G is said to be cyclic if there exists $a \in G$ such that the subgroup generated by a is the group itself.

In other words, $G = \{a, a^2, a^3, \dots, a^n = e\}$

If a group G contains an element a such that every element of G is of the form a^k for some integer K, we say that G is a cyclic group and that G is generated by a or a is a generator of G. denoted by symbol $G = \langle a \rangle$

Note (i) The identity element can not be generator of group.
(ii) The generator of group can be more than one.

Ex- Prove that the set G consisting of four fourth roots of unity i.e. $G = \{1, -1, i, -i\}$ is a cyclic group.

Soln:-

We know that G is a group.

Now, it can be shown that G forms a cyclic group with generators i and $-i$ since.

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

It can be readily seen that 1 and -1 cannot be used as generators of G.

Ex- The group $G = \{0, 1, 2, 3, 4\}$ addition modulo 5 is a cyclic group. Prove it:

~~$0+0=0$~~ $\quad 1+_5 1 = 2 \quad 3+_5 3 = 1$

$0+0+0=0 \quad 2+_5 2 = 4$

V.V.I

Theo (15) Prove that every cyclic group is abelian.

Proof:- Let G be a cyclic group generated by a. Let x, y be any two elements $\in G$.

Then, there exist integers r and s such that

$$x = a^r \text{ and } y = a^s$$

Now,

$$x \cdot y = a^r \cdot a^s = a^{r+s}$$

and $$yx = a^s \cdot a^r = a^{s+r} = a^{r+s}$$

$$\therefore xy = yx, \quad \forall x, y \in G$$

Hence, G is an abelian group.

Theo (16) Prove that If a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Proof:- Let G be a cyclic group generated by a.

Let a^r be any element of G, where r is some integer.

We write,

$$a^r = (a^{-1})^{-r}$$ since $-r$ is also some integer.

Therefore,

G is also generated by a^{-1}

Hence, a^{-1} is also generator of G.

~~Theo~~ # Number of generators of a finite ~~group~~ cyclic group:-

Theorem (18) Number of generators of a finite cyclic group of order n is $\phi(n)$, where $\phi(n)$ is the Euler's ϕ function.

Proof:- Let

Page No.
Date

Ex(1) Find all the generators of the cyclic group $G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$

Soln:- Here, 1, 5 are primes to 6
$\therefore$ Generators are a^1 and a^5

Ex(2) Find all generators of the cyclic group
$G = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$

Here 1, 3, 5, 7 are primes to 8
$\therefore$ The generators are a^1, a^3, a^5, a^7.

Ex(3) How many generators can a cyclic group of order 12 have?

Ans:- The order of $a = 12$
$\therefore G = \{a, a^2, a^3, \ldots, a^{12}\}$

Here, 1, 5, 7, 11 are primes to 12
$\therefore$ The generators are a, a^5, a^7, a^{11}.

$\boxed{\text{Subgroup of a cyclic group}}$

Theorem (17) Every subgroup H of a cyclic group G is also cyclic. Prove it.

Proof:-
Let G is a cyclic group generated by a.
Let H be a subgroup of G.
Every element of H will be evidently some integral powers of a, positive or negative.

Let m be the smallest positive integer such that $a^m \in H$
we shall show that H is a cyclic group generated by a^m.

Let $a^k \in H$, Obviously $k > m$.

By division alogorithm, we may write

$k = qm + r$, where $0 \le r < m$

Hence, $a^k = a^{qm+r} = (a^m)^q . a^r$

$\Rightarrow a^r = a^k . (a^m)^{-q}$

Since, $a^m \in H$ and $a^k \in H$, this equation implies that $a^r \in H$.

But m is the smallest positive integer such that $a^m \in H$.

Since, $r < m$, we must have $r = 0$

Therefore, $k = qm$ and

Hence, every element a^k of H is of the form $(a^m)^q$ for some integer k.

This shows that H is a cyclic group generated by a^m

i.e. a^m is a generater of H.

Theo(8) If H is a subgroup of the cyclic group G, then the order of G is a multiple of the order of H.

Theo(9) Every proper subgroup of an infinite cyclic group is infinite.

Theo(10) EX- Find the proper subgroups of the cyclic group $G = \{w, w^2, w^3, w^4, w^5, w^6 = e\}$

Soln:- The order of cyclic group is 6.

The divisors of 6 are 2 and 3.

$\therefore$ The proper subgroups are $H_1 = \langle w^2 \rangle$ and $H_2 = \langle w^3 \rangle$

i.e. $H_1 = \{w^2, w^4, w^6 = e\}$, $H_2 = \{w^3, w^6 = e\}$

EX - Given an example of finite, abelian group which is not cyclic

Ans: Let G be the set of four real number.

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ is an abelian group w.r.to multiplication but not cyclic.

Scanned with OKEN Scanner