

Topic: - Concept of subgroup and cyclic group with Example

Subgroup :- Def Let  $G$  be a group and  $H$  a subset of  $G$ . Then it is called to be subgroup of  $G$  if  $H$  is group under group operation of  $G$ .

Example :- The set  $E$  of even integer is a subgroup of group  $Z$  of integer under ordinary addition.

Soln: - Clearly the set  $Z$  of integers is a group under ordinary addition,  $0$  being the identity element and  $-a \in Z$  being the inverse element of  $a \in Z$ .

Now  $b \in E$  means  $b = 2a$  where  $a \in Z$ . Clearly  $E \subset Z$

Also, it can easily be verified that  $E$  is a group under ordinary addition,  $0$  being the identity element and  $-b \in E$  being the inverse element of  $b \in E$ .

Thus  $E \subset Z$  and  $E$  is a group under

the same operation as that on  $\mathbb{Z}$ .

Cyclic group :- def: - A group  $(G, \cdot)$  is called cyclic group if there exists an element  $a \in G$  such that every element  $b$  of  $G$  can be expressed as an integral (positive or negative) power  $a^n$  of  $a$ . The element  $a$  whose power exhaust the set  $G$  is called a generator of the cyclic group.

Thus a cyclic group consists only of integral powers of a particular element of the group.

Example: - The set of fourth roots of unity form a cyclic group under multiplication of complex number.

The set of fourth roots of unity is  $G = \{1, -1, i, -i\}$  we know  $G$  is a group under the multiplication of complex numbers.  $1$  being the identity



element and its inverse element  
being  $1, -1, -i, i$  respectively

$$\text{Now } (1)^1 = 1, (1)^2 = 1 \text{ etc}$$

$$(-1)^1 = -1, (-1)^2 = 1, (-1)^3 = -1 \text{ etc}$$

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

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

Thus we find the integral  
power of  $i$  exhaust all the elements  
of  $G$ . So  $(G, \cdot)$  is a cyclic

group with  $i$  as generator.

Theorem: - To prove that a non empty  
subset  $H$  of the group  $G$  under the  
operation  $\circ$  forms a subgroup if  
and only if

$$a, b \in H \Rightarrow a \circ b^{-1} \in H$$

Proof: - Let  $H$  be a subgroup of the  
group  $G$  under the operation  $\circ$ .  
Then  $H \subseteq G$  and  $H$  is group under  $\circ$ .

$$\therefore b \in H \Rightarrow b^{-1} \in H \quad (\because \text{inverse element exists in a group})$$

$$\therefore a, b \in H \Rightarrow a \in H, b^{-1} \in H$$

$$\Rightarrow a \circ b^{-1} \in H \quad (\text{closure law holds in group})$$

$\therefore$  The condition is necessary

Next let  $H \subseteq G$  and  $a, b \in H \Rightarrow a \circ b \in H$  (1)  
we have to prove that  $H$  is a group under the operation  $\circ$ .

Now  $a \in H, a^{-1} \in H \Rightarrow a \circ a^{-1} \in H$  by (1)  
 $\Rightarrow e \in H$

$\therefore$  The identity element exists in  $H$ .

Again  $e \in H, a \in H \Rightarrow e \circ a^{-1} \in H$  by (1)  
 $\Rightarrow a^{-1} \in H$

$\therefore$  Inverse elements of the elements of  $H$  exists in  $H$ . (2)

Now  $a \in H, b \in H \Rightarrow a \circ b \in H, b^{-1} \in H$  by (2)  
 $\Rightarrow a \circ (b^{-1})^{-1} \in H$  by (1)  
 $\Rightarrow a \circ b \in H$

$\therefore$  The closure law holds in  $H$ .

Also the associative law holds in  $H$  because  $H \subseteq G$  and the associative law holds in  $G$  because it is a group. Hence  $\circ$  satisfies  $H$  itself under operation  $\circ$ .

Thus  $H$  is a subgroup of  $G$  under the operation  $\circ$ .

$\therefore$  The condition is also sufficient.