

① Prove that a non-commutative group of order  $2n$  where  $n$  is odd prime, must have subgroup of order  $n$ . (8)

Proof

$G$  is non-abelian group

Suppose  $\forall a \in G$

$$o(a) = 2$$

$$\Rightarrow (ab)^2 = e$$

$$\Rightarrow ab = (ab)^{-1}$$

$$= b^{-1}a^{-1}$$

$$\Rightarrow ab = b^{-1}a^{-1} \Rightarrow a^{-1} = a \text{ and } b^{-1} = b$$

$\Rightarrow G$  is abelian

hence contradiction

$\Rightarrow \exists$  a element  $a$  of  $G$  of order other than 2

$\therefore$  possible order are  $n$  and  $2n$

if  $a \in G \Rightarrow o(a) = 2n$

$$\Rightarrow G = \langle a \rangle$$

hence cyclic  $\Rightarrow$  abelian

$\therefore$  contradiction

Using Lagrange's theorem

$\exists$  an element  $b \in G$

$$o(b) = n$$

$\therefore \langle b \rangle$  is of order  $n$



79) Find all the homomorphism from the Group  $(\mathbb{Z}, +)$  to  $(\mathbb{Z}_4, +)$  --- (10)

Soln:-

$$\phi: \mathbb{Z} \rightarrow \mathbb{Z}_4$$

$$\phi(x) = 0 \pmod{4} \quad \forall x \in \mathbb{Z}$$

A homomorphism  $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_4$  is determined by  $\phi(1)$  since

$$\phi(n) = \phi(\underbrace{1+1+\dots+1}_{n \text{ times}}) = \underbrace{\phi(1) + \phi(1) + \dots + \phi(1)}_{n \text{ times}}$$

$$\phi(n) = n\phi(1) \quad \forall n \in \mathbb{Z}$$

Also, for any  $a \in \mathbb{Z}_4$  we can get a homomorphism  $\mathbb{Z} \rightarrow \mathbb{Z}_4$  taking 1 to  $a$  by sending  $n$  to the reduction mod 4 of  $an$ . So, there are 4 homomorphisms

$\phi: \mathbb{Z} \rightarrow \mathbb{Z}_4$ , one for each value in  $\mathbb{Z}_4$ .  
if  $\phi(1) = 0$  we get trivial map.  
 $\ker \phi = \mathbb{Z}$  and  $\text{img } \phi$  is  $\{0\}$

$$\text{if } \phi(1) = 1 \pmod{4}$$

$\phi$  is onto.  $\text{image of } \phi = \mathbb{Z}_4$ .

$$\ker \phi = 4\mathbb{Z}$$

$$\text{if } \phi(1) = 2 \pmod{4}$$

$$\text{image } \phi = \{0, 2\}$$

$$\ker \phi = 2\mathbb{Z}$$

$$\text{if } \phi(1) = 3 \pmod{4}$$

$$\text{img } \phi = \mathbb{Z}_4$$

$$\ker \phi = 4\mathbb{Z}$$



21d) Let  $R$  be a commutative ring with unity.  
prove that an ideal  $P$  of  $R$  is prime  
iff  $\frac{R}{P}$  is an integral domain.  
(10)

Sol<sup>n</sup>:- Defn:- prime ideal:-

A prime ideal  $A$  of a commutative  
Ring  $R$  is a proper ideal of  $R$   
 $\exists a, b \in R$  and  $a \cdot b \in A$  imply  
 $a \in A$  or  $b \in A$ .

Sol<sup>n</sup>:- let  $R$  be an integral domain

and  $a \cdot b \in P$

$$\therefore (a+P) \cdot (b+P) = ab+P = P$$

where  $P$  is zero element

$$\text{of } \frac{R}{P}$$

$\therefore$  either  $a+P = P$  or  $b+P = P$

$$\Rightarrow a \in P \text{ or } b \in P$$

$\therefore P$  is prime ideal.

conversely,

let  $P$  is prime ideal.

$\frac{R}{P}$  is commutative ring with

unity where  $1+P$  is unity element.

we just have to show that

$\frac{R}{P}$  has no-zero divisors.

$\therefore P$  is prime ideal.

consider,



$$(a+p) \cdot (b+p) = 0+p = p$$

$$\therefore ab+p = p$$

$$\Rightarrow ab \in p$$

$$\Rightarrow a \in p \text{ or } b \in p$$

$$\Rightarrow \text{either } a+p = p \text{ or } b+p = p$$

$\therefore \frac{R}{p}$  is integral domain.

b) show by an eg that in a finite commutative Ring, every maximal ideal need not be prime. (10)

Let  $R = \{0, 2, 4, 6\}$  under binary operation  $+$  and  $\times$ .

then  $R$  is commutative ring.

$I = \{0, 4\}$  is maximal ideal in  $R$ .

$$\text{but } \overline{2} \times \overline{6} = \overline{4} \in I$$

$$\text{but both } \overline{2} \text{ and } \overline{6} \notin I.$$

hence  $I$  is not prime ideal.



4] c] let  $H$  be a cyclic subgroup of a group  $G$ . if  $H$  be a normal subgroup of  $G$  prove that every subgroup of  $H$  is a normal subgroup of  $G$ . (10)

Sol<sup>n</sup>: let  $H = \langle a \rangle$   
 $H$  is normal subgroup of  $G$

$\therefore \forall g \in G$

$$g^{-1}Hg = H$$

let  $K$  is subgroup of  $H$ .

any subgroup of cyclic group is cyclic.  
 $\therefore$  let  $K = \langle a^m \rangle$

we have to show that  $K$  is normal subgroup of  $G$ .

$\therefore$  let  $g \in G$  be arbitrary and  $k \in K$   
 $\therefore k = (a^m)^n$  for some  $n \in \mathbb{Z}$

$$\therefore g^{-1}kg = g^{-1}(a^m)^ng$$

$$= g^{-1}(a^n)^mg$$

$$= (g^{-1}a^n g)^m$$

$$\therefore H = \langle a \rangle$$

$$\therefore a^n \in H$$

$$\therefore H \trianglelefteq G$$

$$g^{-1}a^n g \in H$$

$$\therefore g^{-1}a^n g = a^t \text{ for } t \in \mathbb{Z}$$

$$\therefore g^{-1}kg = (a^t)^m = (a^m)^t \in K$$

$$\therefore K \trianglelefteq G.$$