

① a) IF  $G$  is a Group in which  $(ab)^4 = a^4 \cdot b^4$   
 $(ab)^5 = a^5 \cdot b^5$  and  $(ab)^6 = a^6 \cdot b^6$   
 for all  $a, b \in G$ , then prove that  $G$  is  
 abelian. (8)

Sol<sup>n</sup>

Given that

$$(ab)^4 = a^4 \cdot b^4 \quad \text{--- ①}$$

$$(ab)^5 = a^5 \cdot b^5 \quad \text{--- ②}$$

$$(ab)^6 = a^6 \cdot b^6 \quad \text{--- ③}$$

consider,

$$(ab)^6 = a^6 \cdot b^6$$

$$(ab)(ab)^5 = a^6 \cdot b^6$$

$$(ab)(a^5 \cdot b^5) = a^6 \cdot b^6 \quad \text{--- using ②}$$

$$ba^5 = a^5 \cdot b \quad \text{--- ④ using cancellation}$$

$$\text{Similarly, } (ab)^5 = a^5 \cdot b^5$$

$$(ab)(ab)^4 = a^5 \cdot b^5$$

$$(ab)(a^4 b^4) = a^5 b^5 \quad \text{--- using ①}$$

$$ba^4 = a^4 \cdot b \quad \text{--- using cancell<sup>n</sup>}$$

post multiplying by  $a$  we get

$$ba^5 = a^4 \cdot ba$$

$$\Rightarrow a^5 b = a^4 \cdot ba \quad \text{--- using ④}$$

$$\therefore ab = ba \quad \text{--- using cancell<sup>n</sup>}. \quad \text{--- using ④}$$

$G$  is abelian.



2] a) let  $\mathbb{Z}_n$  be the set of integers mod  $n$ . then prove that  $\mathbb{Z}_n$  is ring under the operation of addition and multiplication mod  $n$ . under what condition of  $n$ ,  $\mathbb{Z}_n$  is a field. Justify your ans. (10)

Sol<sup>n</sup> let  $\mathbb{Z}_n$  be the set of integers mod  $n$ . then  $\mathbb{Z}_n$  has  $n$  distinct elements. Thus  $\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$

let  $[a], [b] \in \mathbb{Z}_n$

then we define addition and multiplication of modulo  $n$  as follows.

$$[a] + [b] = [a+b]$$

$$[a] \cdot [b] = [a \cdot b]$$

$\therefore [a+b]$  and  $[a \cdot b]$  are both modulo  $n$

$\therefore \mathbb{Z}_n$  is closed with respect to addition and multiplication.

now let  $[a], [b], [c]$  be any elements of  $\mathbb{Z}_n$ . then we observe

commutativity of addition:-

$$\begin{aligned} [a+b] &= [a+b] \quad \text{--- by def of residue} \\ &= [b+a] \quad \text{--- integers are commutative} \\ &= [b] + [a] \end{aligned}$$

Associativity of addition:-

$$\begin{aligned} ([a] + [b]) + [c] &= [a+b] + [c] \\ &= [(a+b) + c] = [(a) + (b+c)] \\ &= [a] + ([b+c]) \end{aligned}$$



Additive identity: we have  $[0] \in \mathbb{J}_n$  if  $[a] \in \mathbb{J}_n$   
then  $[a] + [0] = [a+0]$   
 $= [a]$

Additive inverse: let  $[a] \in \mathbb{J}_n$  then  $[-a] \in \mathbb{J}_n$   
where  $[-a] = [n-a]$   
 $\therefore [a] + [-a] = [a-a] = [0]$   
 $\therefore [-a] = [n-a]$  is additive inverse.

Associative of multiplication:-

$$\begin{aligned} ([a][b])[c] &= [ab][c] \\ &= [ab]c \\ &= [a(bc)] \\ &= [a][bc] \\ &= [a]([b][c]) \end{aligned}$$

Commutative:-

$$[a][b] = [ab] = [ba] = [b][a]$$

Distributive:-

$$\begin{aligned} [a]([b] + [c]) &= [a][b+c] \\ &= [a(b+c)] \\ &= [ab+ac] \\ &= [ab] + [ac] \\ &= [a][b] + [a][c] \end{aligned}$$

Thus  $\mathbb{J}_n$  is a commutative Ring.

If  $\mathbb{J}_n$  is finite ring having  $n$  elements. it is prime. then  
to prove that  $\mathbb{J}_n$  is field.

let  $[a], [b] \in \mathbb{J}_n$

$$\begin{aligned} \therefore [a] \cdot [b] &= [0] \\ &= [a \cdot b] = [0] \end{aligned}$$

$\Rightarrow n$  is divisor of  $ab$ :  $n|ab$



but  $n$  is prime

$\therefore n|a$  or  $n|b$

$= [a] = 0$  or  $[b] = 0$

$\therefore \mathbb{Z}_n$  is integral domain.

but we know that finite integral domains are field.

$\therefore \mathbb{Z}_n$  is field.

3] a) let  $R$  be an integral domain with unity. prove that the units of  $R$  and  $R[x]$  are same. (10) (as 2018)

sol<sup>n</sup>: Given  $R$  is an integral domain with unity.

$\therefore 1 \in R$

$\therefore 1 + 0x + 0x^2 + \dots + 0x^n + \dots$  is unity in  $R[x]$ .

let  $P(x) = a_0 + a_1x + a_2x^2 + \dots$  is unit in  $R[x]$

$\therefore \exists Q(x) = b_0 + b_1x + b_2x^2 + \dots$  s.t.  
 $P(x) \cdot Q(x) = 1 + 0x + 0x^2 + \dots$

$\therefore (a_0 \cdot b_0) + (a_0b_1 + b_0a_1)x + \dots = 1 + 0x + \dots$   
but two polynomials are equal iff  $a_i = b_i \quad \forall i \in \mathbb{Z}$

$\therefore a_0b_0 = 1$  &  $a_1 = a_2 = \dots = a_n = b_1 = b_2 = b_n = 0$

$\therefore$  either  $a_0 \neq 0$  and  $b_0 \neq 0$

$\rightarrow \therefore R$  is I.D.

$\therefore P(x) = a_0$  is unit in  $R[x]$   
iff  $a_0$  is unit in  $R$ .