

## PART-II (PAPER-III) Abstract Algebra

### CHAPTER:- Rings, Integral Domains and Field.

Theorem:- Prove that intersection of two subrings is a subring

Proof:- Let  $S_1$  and  $S_2$  be two subrings of a ring  $R$ .

$$\text{Let } S = S_1 \cap S_2$$

Since  $0 \in S_1$  and  $0 \in S_2 \therefore 0 \in S_1 \cap S_2$  i.e.  $0 \in S$ .

$$\text{Let } a, b \in S = S_1 \cap S_2$$

$$\text{Now, } a \in S_1 \cap S_2 \Rightarrow a \in S_1 \text{ and } a \in S_2$$

$$b \in S_1 \cap S_2 \Rightarrow b \in S_1 \text{ and } b \in S_2$$

Since  $S_1$  and  $S_2$  are both subrings, we have

$$a \in S_1, b \in S_1 \Rightarrow a+b \in S_1 \text{ and } ab \in S_1,$$

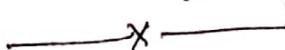
$$\text{and } a \in S_2, b \in S_2 \Rightarrow a+b \in S_2 \text{ and } ab \in S_2$$

$$\text{Now } a+b \in S_1, a+b \in S_2 \Rightarrow a+b \in S_1 \cap S_2 \text{ i.e. } a+b \in S$$

$$\text{and } ab \in S_1, ab \in S_2 \Rightarrow ab \in S_1 \cap S_2 \text{ i.e. } ab \in S$$

$$\text{Thus } a \in S, b \in S \Rightarrow a+b \in S \text{ and } ab \in S$$

Hence  $S$  is a subring of  $R$  i.e.  $S_1 \cap S_2$  is a subring of  $R$



Theorem:- For each element  $a \in R$  (Ring) Prove that  $a \cdot 0 = 0 \cdot a = 0$

Proof:- Since  $a+0=a$ , it follows that

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

But by the distributive law,  $a(a+0) = a \cdot a + a \cdot 0$

$$\text{Hence } a \cdot a + a \cdot 0 = a \cdot a$$

$$\text{But } a \cdot a + 0 = a \cdot a.$$

$$\text{Hence } a \cdot a + a \cdot 0 = a \cdot a + 0$$

$$\Rightarrow a \cdot 0 = 0 \quad (\text{By left cancellation law})$$

Similarly we can prove that

$$0 \cdot a = 0$$



Theorem:- If  $a, b, c$  are any three elements of a ring  $R$  (1)  
 then prove that (i)  $a \cdot (b-c) = a \cdot b - (a \cdot c)$   
 (ii)  $(b-c) \cdot a = ba - (c \cdot a)$

Proof:- (i) We have

$$\begin{aligned} a(b-c) + (a \cdot c) &= a(b-c+c), \text{ by distributive law.} \\ &= a \cdot (b+0) \\ &= a \cdot b \end{aligned}$$

Adding  $-(a \cdot c)$  on both sides we get

$$a(b-c) = ab - ac$$

(ii) Similarly we prove that

$$(b-c) \cdot a = ba - ca.$$

Theorem:- If  $a$  and  $b$  are any two elements of a ring  $R$ ,

then (i)  $a(-b) = -(a \cdot b) = (-a) \cdot b$ .

(ii)  $(-a)(-b) = ab$

Proof:- (i) We have

$$a \{b + (-b)\} = a \cdot 0 = 0$$

But by distributive law.

$$a \{b + (-b)\} = ab + a(-b)$$

Hence  $ab + a(-b) = 0$ , But since  $ab$  has an unique additive inverse  $-(ab)$ , it follows that

$$a(-b) = -(ab)$$

Similarly we can prove that

$$(-a)b = -(ab)$$

(ii) We have

$$(-a)(-b) = -\{(-a)b\} \text{ by (1)}$$

$$= -\{-a(ab)\} \text{ again by (1)}$$

$$= ab$$

Theorem:- Prove that the additive inverse of an element of a ring is unique. (3)

Proof:- Let, if possible  $b$  and  $b'$  are two additive inverses of  $a \in R$ .

$$\text{Then } a+b = 0$$

$$a+b' = 0$$

$$\Rightarrow a+b = a+b'$$

$$\Rightarrow (-a)+(a+b) = (-a)+(a+b')$$

$$\Rightarrow \{(-a)+a\}+b = \{(-a)+a\}+b', \text{ by associative law}$$

$$\Rightarrow 0+b = 0+b'$$

$$\Rightarrow b = b'$$

This proves that, in a ring  $R$ , the inverse of all elements is unique.

————— X —————

Theorem :- Prove that every field is necessarily an integral domain.

Proof :- Let  $(F, +, \cdot)$  be a field. So  $(F, +, \cdot)$  is a commutative ring with unity.

If we can prove that the divisor of zero are absent in  $F$ .

i.e.  $ab=0 \rightarrow a=0 \text{ or } b=0$  then  $(F, +, \cdot)$  will be an integral domain.

Let  $a, b \in F$  and  $a \cdot b=0$ , if possible let  $a \neq 0$

As  $F$  is a field and  $a(\neq 0) \in F$  we get  $a^{-1} \in F$

(by existence of multiplicative inverse)

$$\therefore a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b. \quad (\text{by associative law})$$

$$-1 \cdot b = b$$

(4)

and  $a^{\dagger}(ab) = a^{\dagger}(0)$ 

$$= 0.$$

 $\therefore a^{\dagger}(ab) = b = 0$  i.e.  $b = 0$  $\therefore$  If  $a \neq 0$  then  $a \cdot b = 0 \Rightarrow b = 0$ Similarly, if  $b \neq 0$  then  $a \cdot b = 0 \Rightarrow a = 0$  $\therefore a \cdot b = 0 \Rightarrow a = 0$  or  $b = 0$  $\therefore F$  is an integral domain.

Hence every field is necessarily an integral domain.

Theorem: Prove that every finite integral domain is necessarily a field.Proof: Let  $D$  denotes the finite integral domain having  $a_1, a_2, \dots, a_n$  all the distinct elements where  $a_{n+1}$  is the unity element of  $D$ . If  $b(\neq 0) \in D$  then $a_i b \in D$  and all  $a_i b$  are distinct for  $i = 1, 2, \dots, n$   
for if they are not all distinct, let

$$a_i b = b_j b.$$

$$\text{then } (a_i - b_j)b = 0$$

Since  $b \neq 0$  and  $D$  being an integral domain contains no zero divisors, it follows that  $a_i - b_j = 0$   
i.e.  $a_i = b_j$ .which contradicts our supposition. Hence given  $b(\neq 0) \in D$ , there exists  $a \in D$  such that  $a \cdot b = 1$ .  
Thus  $a$  is the multiplicative inverse of  $b(\neq 0)$ .  
So each non-zero element of  $D$  has a multiplicative inverse in  $D$ .Hence  $(D, +, \cdot)$  is a field.

---