

Suppose identity element $I = (x, y)$ exists in S

then $I * A = A * I = A$ for any $A = (a, b) \in S$

$$\text{Now } A * I = A \Rightarrow (a, b) * (x, y) = (a, b)$$

$$\Rightarrow (ax, ay + b) = (a, b)$$

$$\Rightarrow ax = a \text{ and } ay + b = b$$

$$\Rightarrow x = 1 \text{ and } ay = 0 \Rightarrow y = 0$$

$\therefore I = (1, 0)$ exists in S , since $0, 1 \in \mathbb{Q}$

Definition 1: Ring

A non empty set R with two binary operations denoted by $+$ and \cdot , called addition and multiplication is called a ring if the following axioms are satisfied

(i) $(R, +)$ is an abelian group, with 0 as identity

(ii) (R, \cdot) is a semigroup

(iii) The operation \cdot is distributive over $+$

$$\text{i.e. } a \cdot (b + c) = a \cdot b + a \cdot c$$

$$\text{and } (b + c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in R$$

The additive identity 0 is called the zero element of the ring

Definition 2: A ring $(R, +, \cdot)$ is said to be commutative if

$$a \cdot b = b \cdot a \quad \forall a, b \in R.$$

Note: (1) The multiplicative identity 1 is called the unit element or identity of R .

Definition : Integral domain

A commutative ring $(R, +, \cdot)$ with identity and without zero is called an integral domain.

Definition : Field

A commutative ring $(R, +, \cdot)$ with identity in which every non-zero element has multiplicative inverse is called as field.

Theorem 3 :

Every field is an integral domain

Proof :

Let $(F, +, \cdot)$ be a field. Then it is a commutative ring with identity.

To prove F is an integral domain, it is enough to prove that it has no zero divisors.

Suppose $a, b \in F$ with $a \cdot b = 0$, $a \neq 0$

Since a is non-zero element, its multiplicative inverse a^{-1} exists.

$$\therefore a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0$$

$$\Rightarrow (a^{-1} \cdot a) \cdot b = 0$$

$$1 \cdot b = 0 \rightarrow b = 0$$

$$\text{Thus } ab = 0, a \neq 0 \Rightarrow b = 0$$

$\therefore F$ has no zero divisors

Hence $(F, +, \cdot)$ is an integral domain

Theorem 4: Prove that any finite integral domain is a field

Proof: Let $(R, +, \cdot)$ be a finite integral domain.

$\therefore R$ is a commutative ring with identity and without zero divisors. Hence to prove R is a field.

it is enough to prove that every non-zero element in R has multiplicative inverse

$$\text{Let } R = \{0, 1, a_1, a_2, \dots, a_n\}$$

where 0 is zero of the ring

1 is identity of ring

Let $a \in R$ and $a \neq 0$

Multiplying the non-zero elements of R by a , we get the set $\{a \cdot 1, a \cdot a_1, \dots, a \cdot a_n\}$

Since R is without zero divisors, these elements are all non-zero and they are distinct.

Suppose $aa_r = aa_s$, $r \neq s$,

then $a(a_r - a_s) = 0$

$\Rightarrow a_r - a_s = 0$, since $a \neq 0$

$\Rightarrow a_r = a_s$ which is a contradiction to the fact that a_r and a_s are distinct elements in R

$\therefore aa_r \neq aa_s$

And all the aa_i are distinct from 'a' also

Since R is finite, these $(n+1)$ elements are as same as $(n+1)$ non-zero element of R in some order by pigeon hole principle.

$\therefore 1 = aa_i$ for some $a_i \in R$

Since R is commutative $aa_i = a_i a$

$\therefore aa_i = a_i a = 1 \Rightarrow a_i = a^{-1}$

\therefore every non-zero element in R has multiplicative inverse.

Hence any finite integral domain is a field.