16 November 2021 15:13

Ring:

A binary structure $(R, +, \cdot)$ is a ring

if ① $(R, +)$ is an abelian group

② $(R, \cdot)$ is a Semigroup → Closure
→ Associativity

③ Distributive laws are
Satisfied.

Commutative Ring:

Ring R is commutative

if $a \cdot b = b \cdot a \ \forall a, b \in R$

Ring with unity:

Ring R is called ring with unity

if R contains multiplicative
Identity (unity)

Integral Domain:

Integral domain:

A commutative ring with unity is called an integral domain if it has no zero divisors.

$(\mathbb{Z}, +, \cdot)$ $(\mathbb{Z}_6, +_6, \cdot_6)$ → not an I.D.

Field:

A commutative ring with unity is called a field if every nonzero element is a unit.

or

every nonzero element has its multiplicative inverse.

$(\mathbb{Z}, +, \cdot)$ is not a field $\left((2)^{-1} = \frac{1}{2} \notin \mathbb{Z} \right)$

$(\mathbb{Q}, +, \cdot)$ is a field

$(\mathbb{R}, +, \cdot)$ is a field.

Theorem: Every field is an Integral

Theorem: Every field is an Integral Domain but converse need not be true.

Example. $(\mathbb{Z}, +, \cdot)$ is an I.D. but not a field.

Field with Nine Elements: $\mathbb{Z}_3 = \{0, 1, 2\}$

$$\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\}$$

$$\mathbb{Z}_4[i] = \{a + bi \mid a, b \in \mathbb{Z}_4\} \quad : \mathbb{Z}_4 = \{0, 1, 2, 3\}$$

Check, whether it is a field or not.

$$\mathbb{Z}_4[i] = \{0, 1, 2, 3, i, 1+i, 2+i, 3+i, 2i, 1+2i, 2+2i, 3+2i, 3i, 1+3i, 2+3i, 3+3i\}$$

$2 \neq 0$, Consider inverse of 2.

Theorem: Every finite integral domain is a field is a field.

Proof :-

Let D be a finite integral domain with unity 1. Let a be any nonzero element of D.

We need to show that a is a unit, that is, a has its multiplicative inverse in D.

If $a = 1$, then $a^{-1} = (1)^{-1} = 1 \in D$ and we are done.

If $a \neq 1$ and $a \in D$.

then $a^2 \in D$, $a^3 \in D$, $a^4 \in D$, ... ($\because$ D is an I.D.)

Now consider the sequence of elements

$a, a^2, a^3, a^4, \ldots$

$\because$ D is finite, so there must be two positive integers i and j such that

$$a^i = a^j \quad \text{for } i > j \qquad \text{——— } (1)$$

$\Rightarrow a^{i} a^{-j} = a^{j} a^{-j}$ ($\because 1 \in D$ and D is an I.D.)

$\Rightarrow a^{i-j} = 1$ —— (2)

$\Rightarrow i-j > 1$ ($\because a \neq 1$)

$\Rightarrow i-j-1 > 0$ —— (3)

Now $a^{i-j-1} a = a^{i-j} = 1$ (from eq (2))

$\Rightarrow a^{-1} = a^{i-j-1} \in D$

$\Rightarrow a^{-1} \in D$

$\Rightarrow a$ is a unit in D.

$\because a$ is an arbitrary nonzero element of D

Thus, every nonzero element of D is a unit

$\Rightarrow D$ is a field.

Therefore, every finite integral domain is a field.

Corollary: