INTEGRAL DOMAIN

✡ Define an integral domain with examples.

An integral domain D is a ring under two binary operations, addition $(+)$ and multiplication $(\cdot)$ if

1. D is a Commutative ring
2. D has unity (identity element of multiplication)
3. D has no divisors of zero

In other words in more denotative manner, we can say that — A set D, having minimum two elements is called an integral domain under the binary operations of addition $(+)$ and multiplication $(\cdot)$ if the following postulates hold:

For addition $(+)$

1. closure law: $a, b \in D \Rightarrow a+b \in D$
2. Commutative law: $a+b = b+a \ \forall a, b \in D$
3. Associative law: $(a+b)+c = a+(b+c) \ \forall a, b, c \in D$
4. Existence law of identity: $\exists$ an element $0 \in D$ (zero element) such that
$$a+0 = a \quad \forall a \in D$$
5. Existence law for inverse elements:
$$a \in D \Rightarrow \exists x \in D, \text{ such that}$$
$$a+x = 0$$
The additive inverse of a is written as $-a$.

Scanned with CamScan

For multiplication $(\cdot)$

6. Closure law: $a, b \in D \Rightarrow a \cdot b \in D$
7. Associative law: $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in D$
8. Commutative law: $a \cdot b = b \cdot a \quad \forall a, b \in D$
9. Existence law of identity: $\exists$ an element $1 \in D$ (called unity) such that
   $$a \cdot 1 = a \quad \forall a \in D$$
10. Absence of divisors of zero:
    $a \cdot b = 0 \Rightarrow$ either $a = 0$ or $b = 0$ or both a and b are equal to 0, $\forall a, b \in D$
11. For addition $(+)$ and multiplication $(\cdot)$
    $$a \cdot (b + c) = a \cdot b + a \cdot c,$$
    $$(b + c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in D$$

Examples

1. The set of rational numbers (whether real or complex) with binary operation addition $(+)$ and multiplication $(\cdot)$ form an integral domain.
2. The numbers given by $a + \sqrt{5}\, b$ form an integral domain subject to be integers a and b.

Scanned with CamScan

Prove that in an integral domain $(I, +, \cdot)$ the Cancellation law holds

i.e. $a \cdot b = a \cdot c \Rightarrow b = c$ if $a \neq 0$

& $b \cdot a = c \cdot a \Rightarrow b = c$ if $a \neq 0$

where $a, b, c \in I$.

Proof, Let $(I, +, \cdot)$ be an integral domain. So it is obviously a Commutative ring with Unity with no Zero divisors.

$\therefore a \cdot b = 0 \Rightarrow$ either $a = 0$ or $b = 0$

if $a \neq 0$ then $a \cdot b = 0 \Rightarrow b = 0 \quad \ldots (1)$

Again by the property of ring

$a \cdot (b - c) = a \cdot b - a \cdot c$

$\therefore a \cdot b = a \cdot c \Rightarrow a \cdot b - a \cdot c = 0$

$\Rightarrow a \cdot (b - c) = 0$

$\Rightarrow b - c = 0$ [using (1)]

$\Rightarrow b - c + c = 0 + c$

$\Rightarrow b = c$

or $a \cdot b = a \cdot c \Rightarrow b = c$

Again $(b - c) \cdot a = b \cdot a - c \cdot a \quad \ldots (2)$

If $b \neq 0$ then $a \cdot b = 0 \Rightarrow a = 0 \quad \ldots (3)$

$\therefore b \cdot a = c \cdot a \Rightarrow b \cdot a - c \cdot a = 0$

$\Rightarrow (b - c) \cdot a = 0$ [using (2)]

$\Rightarrow b - c = 0$ [using (3)]

$\Rightarrow b - c + c = 0 + c$

$\Rightarrow b = c$

or $b \cdot a = c \cdot a \Rightarrow b = c$

Thus the cancellation laws hold for the integral domain.

Scanned with CamScanner

FIELD

Define Field →

A Commutative ring F Consisting minimum two elements with unity is called a field under binary operation addition (+) and multiplication (·) if every non zero element of F has a multiplicative inverse in F.

More explicitly a set F consisting at least two elements is called a field under binary operations addition (+) and multiplication (·) if the following postulates hold.

For addition (+) →

(1) Closure law: $a, b \in F \Rightarrow a+b \in F$

(2) Commutative law: $a+b = b+a \ \forall a, b \in F$

(3) Associative law: $(a+b)+c = a+(b+c) \ \forall a, b, c \in F$.

(4) Existence law of identity:
$\exists$ an element $0 \in F$ (zero element)
such that $a+0=a \ \forall a \in F$.

(5) Existence of inverse element:
$a \in F \Rightarrow \exists$ an element $x \in F$
where x is an additive or negative inverse element corresponding to a
such that $a+x=0$
So the additive inverse of a is $-a$.

Scanned with CamScan

For multiplication $(\cdot)$

(6) Closure law: $a, b \in F \Rightarrow a \cdot b \in F$

(7) Associative law: $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in F$

(8) Commutative law: $a \cdot b = b \cdot a \quad \forall a, b \in F$

(9) Existence law of identity: (called unity element)

$\exists$ an element $1 \in F$

such that

$$a \cdot 1 = a \quad \forall a \in F$$

(10) Existence law of Inverse for Nonzero elements:

$a \neq 0 \in F \Rightarrow \exists x \in F$

where x is a multiplicative inverse

Corresponding to a such that

$$a \cdot x = 1$$

The multiplicative inverse of a is written as a^{-1} or $\frac{1}{a}$.

(11) Distributive laws:

$$a \cdot (b+c) = a \cdot b + a \cdot c$$

$$(b+c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in F$$

Examples

(1) The set Q of rational number is a field with respect to addition $(+)$ and multiplication $(\cdot)$

(2) The set of real numbers is a field under the binary operation addition $(+)$ and multiplication $(\cdot)$

Scanned with CamScan

Lp62

Q. Prove that the set Z of integers is not a field under ordinary addition and multiplication.

Ans, Let $a \in Z$ and $a \neq 0$

The unity element of Z is 1.

So the multiplicative inverse of a will be x if

$$ax = 1$$

i.e. $x = \frac{1}{a} \notin Z$

So non zero elements of Z donot have their multiplicative inverses in Z.

Hence Z is not a field.

Q. Prove that every field is necessarily an integral domain.

Proof → We know that the Field F is a commutative ring with unity,

Now to prove that F is an integral domain, we have to prove that field F has no zero divisors.

i.e. $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$

Scanned with CamScan

Now Let $a, b \in F$ with $a \neq 0$
Such that $ab = 0$
Since $a \neq 0$, a^{-1} exists
and $ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0$
$\Rightarrow (a^{-1}a)b = 0$
$\Rightarrow 1b = 0$ $[\because a^{-1}a = 1]$
$\Rightarrow b = 0$ $[\because 1 \cdot b = b]$

Similarly let $ab = 0$ and $b \neq 0$
then $ab = 0 \Rightarrow (ab)b^{-1} = 0b^{-1}$
$\Rightarrow a(bb^{-1}) = 0$
$\Rightarrow a \cdot 1 = 0$ $[\because bb^{-1} = 1]$
$\Rightarrow a = 0$ $[\because a \cdot 1 = a]$

Thus in a field F
$ab = 0 \Rightarrow a = 0$ or $b = 0$
So a field F has no Zero divisors.
Thus Every field is necessarily an integral domain.

☆ Every finite integral domain is necessarily a field.
or
Prove that a finite Commutative ring without Zero divisors is a field.

Scanned with CamScan

Proof → Let D be a finite integral domain of n elements, $a_1, a_2, a_3 \ldots a_n$.
By definition, D is an integral domain so it is a commutative ring with unity without zero divisors.
To prove that D is a field, we must show an element $1 \in D$ such that
$1 \cdot a = a \ \forall \ a \in D$
& for every element $a \neq 0 \in D$ there exists an element $b \in D$ such that $ba = 1$

Let $a \neq 0 \in D$
Now n products are $aa_1, aa_2, aa_3 \ldots aa_n$. They are All these are elements of D. They are all distinct.
Suppose that $aa_i = aa_j$ for $i \neq j$
then $aa_i - aa_j = 0$
or $a(a_i - a_j) = 0 \quad \ldots\ldots (1)$
Since D is without zero divisors and $a \neq 0$
So eqn (1) $\Rightarrow a_i - a_j = 0$
$\Rightarrow a_i = a_j$
which contradicts $i \neq j$.
So, In D all the n distinct elements are placed in $aa_1, aa_2, aa_3 \ldots, aa_n$ an order. So one of these elements will be equal to a.
So $\exists$ an element $1 \in D$ such that $a \cdot 1 = a = 1 \cdot a$ [D is commutative]

Scanned with CamScan

Now to show that 1 is the multiplicative identity of D suppose that y be any element of D.
then if $x \in D$,
then $ax = y = xa$
Now, $1 \cdot y = 1 \cdot (ax)$ $\quad [\because y = ax]$
$= (1 \cdot a) \cdot x$
$= ax$ $\quad [\because 1 \cdot a = a]$
$= y$ $\quad [\because ax = y]$
$= y \cdot 1$ $\quad [\because D \text{ is Commutative}]$
Thus $1 \cdot y = y = y \cdot 1 \ \forall y \in D$
Therefore 1 is the unit element of the ring D.
Now $1 \in D$, So one of the n products $aa_1, aa_2, \ldots aa_n$ will be equal to 1.
Thus there exists an element $b \in D$
Such that
$$ab = 1 = ba$$
So b is the multiplicative inverse of the nonzero element $a \in D$.
Thus every nonzero element of D is inversible.
Therefore, D is a field.

Scanned with CamScan