Dr. O. P. Raman
Dept of Mathematics

For T.D.C. Part II
Paper - 3
Abstract (Modern) Algebra

1

INTEGRAL DOMAIN

Q. Define an integral domain with examples.

Definition A commutative ring with unity having at least two elements is called an integral domain if there are no divisors of zero in the ring.

Thus an integral domain D is a ring under two binary compositions, addition and multiplication if the following hold :

(i) D is a commutative ring

(ii) D has unity (i.e. the identity element of multiplication)

(iii) D has no divisors of zero

More explicitly, a set D (with at least two elements) is called an integral domain under the binary operations, addition (+) and multiplication (·) if the following postulates hold:

For addition (+)

1. *Closure Law:* $a, b \in D \Rightarrow a + b \in D$.
2. *Commutative Law:* $a + b = b + a$ for all $a, b \in D$.
3. *Associative Law:* $(a + b) + c = a + (b + c)$ for all $a, b, c \in D$.
4. *Existence Law of Identity:* There exists an element $0 \in D$ (called zero element) such that $a + 0 = a$ for all $a \in D$.
5. *Existence Law for Inverse Elements:* $a \in D$ implies there exists an element $x \in D$ (called additive inverse or negative element) such that

$$a + x = 0.$$

The additive inverse of a is written as $-a$.

For multiplication (·)

6. *Closure Law:* $a, b \in D \Rightarrow a \cdot b \in D$.
7. *Associative Law:* $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in D$.
8. *Commutative Law:* $a \cdot b = b \cdot a$ for all $a, b \in D$.
9. *Existence Law of Identity:* There exists an element $1 \in D$ (called unity) such that

$$a \cdot 1 = a \text{ for all } a \in D.$$

(2)

10. *Absence of Divisors of Zero:* $a \cdot b = 0 \Rightarrow$ either $a = 0$ or $b = 0$ or both $a = 0$ and $b = 0$, $\forall$ $a, b \in D$.

11. *For addition* (+) *and multiplication* (·)

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

$$(b + c) \cdot a = b \cdot a + c \cdot a \text{ for all } a, b, c \in D.$$

Ex Prove that the set Z of integers is an integral domain under ordinary addition and multiplication.

Solution As the addition of two integers is an integer, the closure law holds for + . Also we know that the associative and commutative laws of addition hold for integers.

The zero element in Z is 0. The additive inverse of $a \in Z$ is $-a \in Z$.

Hence (Z, +) is an abelian group.

Again the multiplication of two integers is an integer. So the closure law holds for $(\cdot)$. Also we know that the associative law holds for multiplication in Z.

Again we know for any three integers *a*, *b*, *c* we have

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

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

Hence $(R, +, \cdot)$ is a ring.

Now, for two integers *a*, *b* we know

$$ab = ba \text{ and } ab = 0 \Rightarrow \text{ either } a = 0 \text{ or } b = 0.$$

$\therefore$ The commutative law holds and divisors of zero are absent.

Also $1 \in Z$ is the unity element.

$\therefore$ Z is an integral domain under ordinary addition and multiplication.

Fields

Definition

Let F be a set and let two binary operations called addition (denoted by +) and multiplication (denoted by $\cdot$) be defined over the set F. Then the system $(F, +, \cdot)$ is called a *field F* if the following conditions are satisfied :

(1) Laws of addition :

(i) $a + b \in F;\ a, b \in F$ (closure law)

(ii) $a + b = b + a;\ a, b \in F$ (commutative law)

(iii) $a + (b + c) = (a + b) + c;\ a, b, c \in F$ (associative law)

(iv) There exists an element 0 in F called *zero* such that $a + 0 = 0 + a = a\ \forall\ a \in F$.

(v) For each element $a \in F$, there exists an element $-a$ in F called negative of a such that $a + (-a) = (-a) + a + 0$.

(2) Laws of multiplication :

(i) $a \cdot b \in F; a, b \in F$; (closure law)

(ii) $a \cdot b = b \cdot a;\ a, b \in F$ (commutative law)

(iii) $a \cdot (b \cdot c) = (a \cdot b) \cdot c;\ a, b, c \in F$ (associative law)

(iv) There exists an element 1 in F called the *unity element* such that

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

(v) For each *non-zero* element a in F, there exists an element a^{-1} in F called the *inverse* of a such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

(3) Distributive laws :

(i) $a \cdot (b + c) = a \cdot b + a \cdot c;\ a, b, c \in F$

(ii) $(b + c) \cdot a = b \cdot a + c \cdot a;\ a, b, c \in F$

Ex (5) *The set of numbers of the form $a + b\sqrt{2}$ where a and b are rational numbers is a field under addition and multiplication.*

Soln. Let the set be denoted by S.

We will first of all show that the set S is an Abelian group w.r.t. addition.

Let $x = a_1 + b_1\sqrt{2}$, $y = a_2 + b_2\sqrt{2}$ and $z = a_3 + b_3\sqrt{2}$. Then

(i) $x + y = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in S$

(ii) $x + y = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$

and $y + x = (a_2 + a_1) + (b_2 + b_1)\sqrt{2}$

$= (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$, for rational numbers are commutative

$\therefore \quad x + y = y + x.$

(iii) $x + (y + z) = \{a_1 + (a_2 + a_3)\} + \{b_1 + (b_2 + b_3)\}\sqrt{2}$

$= (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3)\sqrt{2}.$

Similarly, $(x + y) + z = (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3)\sqrt{2}$

$\therefore \quad x + (y + z) = (x + y) + z.$

(iv) The zero of S is $0 + 0 \cdot \sqrt{2} = 0$.

(v) The inverse of $a + b\sqrt{2}$ is $-a - b\sqrt{2} \in S$.

⑥

Hence S is an additive Abelian group. Again,

(i) $x \cdot y = (a_1 a_2 + 2b_1 b_2) + (a_1 b_2 + b_1 a_2)\sqrt{2} \in S$

(ii) $y \cdot x = (a_2 a_1 + 2b_2 b_1) + (a_2 b_1 + b_2 a_1)\sqrt{2}$
$= (a_1 a_2 + 2b_1 b_2) + (a_1 b_2 + b_1 a_2)\sqrt{2}$

$\therefore xy = yx.$

(iii) $x \cdot (y \cdot z) = (a_1 + b_1\sqrt{2})\{(a_2 + b_2\sqrt{2})(a_3 + b_3\sqrt{2})\}$
$= (a_1 + b_1\sqrt{2})\{(a_2 a_3 + 2b_2 b_3) + (a_2 b_3 + b_2 a_3)\sqrt{2}\}$
$= \{a_1 a_2 a_3 + 2(a_1 b_2 b_3 + a_2 b_3 b_1 + a_3 b_1 b_2)\}$
$+ \sqrt{2}\{2b_1 b_2 b_3 + (a_2 a_3 b_1 + a_3 a_1 b_2 + a_1 a_2 b_3)\}$

Similarly,
$(x \cdot y) \cdot z =$ " " " " " " "
$\therefore x \cdot (y \cdot z) = (x \cdot y) \cdot z.$

(iv) The unity element is $1 + 0 \cdot \sqrt{2} = 1.$

(v) The multiplicative inverse of a non-zero element $a + b\sqrt{2}$ is

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$
$$= \left(\frac{a}{a^2 - 2b^2}\right) - \left(\frac{b}{a^2 - 2b^2}\right)\sqrt{2} .$$

Thus the non-zero elements of S form an Abelian group w.r.t. multiplication.
The distributive laws can be satisfied similarly by actual calculation.
Hence the set S is a field.

6. **Every field is an integral domain but the converse is not necessarily true.**

Proof : Since a field F is a commutative ring with unity, therefore in order to show that every field is an integral domain, we should show that a field has no zero divisors.

Let $a, b \in F$ with $a \neq 0$ such that $ab = 0$.

We shall show that $b = 0$.

Since $a \neq 0$, a^{-1} exists and we have

$$\begin{aligned} ab = 0 &\Rightarrow a^{-1}(ab) = a^{-1}(0) = 0 \\ &\Rightarrow (a^{-1}a)b = 0 \\ &\Rightarrow 1b = 0; \because a^{-1}a = 1 \\ &\Rightarrow b = 0; \because 1b = b. \end{aligned}$$

Similarly, let $b \neq 0$ and $ab = 0$.

Then we have,

$$\begin{aligned} ab = 0 &\Rightarrow (ab)b^{-1} = 0b^{-1} \\ &\Rightarrow a(bb^{-1}) = 0 \\ &\Rightarrow a \cdot 1 = 0 \\ &\Rightarrow a = 0. \end{aligned}$$

This establishes the fact that if $a, b \in F$, then $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Hence a field has no zero divisors.

Therefore every field is an integral domain.

But the converse is not true. i.e., every integral domain is not necessarily a field.

Example of an integral domain which is not a field.

The ring of integers I is a commutative ring with unity. Also I does not possess zero divisors. We know that if $a, b \in I$, such that $ab = 0$, then either a or b must be zero.

Hence the ring of integers I is an integral domain but it is not a field since the multiplicative inverse of any non-zero integer $\in I$ does not belong to I.

(The multiplicative inverse comes out to be a rational number).

Theorem

A finite commutative ring without zero divisors is a field.

Or,

Every finite integral domain is a field.

Proof : Let D be a finite commutative ring without zero divisors having n elements $a_1, a_2, a_3, \ldots, a_n$. In order to prove that D is a field (i) we must produce an element $1 \in D$ such that $1a = a \; \forall \, a \in D$ and (ii) we should show that every non-zero element of D has inverse i.e., for every element $a \neq 0 \in D$ there exists an element $b \in D$ such that $ba = 1$.

Let $a \neq 0 \in D$.

Consider the n products $aa_1, aa_2, aa_3, \ldots, aa_n$. All these are elements of D since D is an integral domain and therefore it is closed with respect to multiplication.

All these elements are distinct.

Suppose on the contrary that $aa_i = aa_j$ for $i \neq j$.

Then $a(a_i - a_j) = 0$ ...(1)

Since D is without zero divisors and $a \neq 0$,

$\therefore$ (1) $\Rightarrow a_i - a_j = 0 \Rightarrow a_i = a_j$ contradicting $i \neq j$.

Hence $aa_1, aa_2, aa_3, \ldots, aa_n$ are all the n distinct elements of D placed in some order. So one of these elements will be equal to a. Thus there exists an element, say a_p such that $aa_p = a = a_p a$; $\because$ D is commutative.

We shall show that this element a_p is multiplicative identity of D.

Let y be an element of D.

Then from the above discussion, for some $x \in D$, we shall have $ax = y = xa$.

Now, $a_p y = a_p(ax)$; $\because \; ax = y$

$= (a_p a)x$

$= ax$; $\because \; a_p a = a$

$= y = ya_p$; $\because$ D is commutative.

Thus $a_p y = y = ya_p \; \forall \; y \in D$.

Therefore a_p is the unity element of the ring D. Let us denote it by 1.

Now $1 \in D$. Therefore from the above discussion, one of the n products $aa_1, aa_2, \ldots, aa_n$ will be equal to 1. Thus there exists an element say $b \in D$ such that $ab = 1 = ba$.

$\therefore$ b is the multiplicative inverse of the non-zero element $a \in D$. Thus every non-zero element of D is inversible.

Hence D is a field.