UNIT 9: RINGS, INTEGRAL DOMAINS AND FIELDS

UNIT STRUCTURE

9.1 Learning objectives

9.2 Introduction

9.3 Ring

9.4 Properties of Ring

9.5 Integral Domain

9.6 Field

9.7 Let us Sum up

9.8 Answers to Check Your Progress

9.9 Further Readings

9.10 Model Questions

9.1 LEARNING OBJECTIVES

After going through this unit, you will be able to know

- ring
- properties of ring.
- Integral domain and its properties
- Field and their properties.

9.2 INTRODUCTION

We have discussed group and its various properties, sub group, coset, cyclic group, normal sub groups and quotient group. In this unit we will study ring. Ring is an algebraic structure, i,e., a non-empty set equipped with two binary operations and satisfying certain postulates.In this unit we will study Integral domain and Field. Integral domain and Field are also a Ring satisfying certain postulates.

9.3 RING

A non-empty set R, equipped with two binary operations, called

addition (+) and multiplication (·) is called a ring if the following postulates are satisfied.

(1) R is an additive Abelian group,

(2) R is an multiplicative semigroup

(3) The two distributive laws hold good, viz

a. (b + c) =a.b + a.c. (left distributive law)

(a + b). c = a.c + b.c, (right distributive law) for all a, b, $c \in R$

Note : 1. In order to be a ring, there must be a non-empty set equipped with two binary operations, viz, + and . , satisfying the postulates mentioned above. Later on we will simply write "Let R be a ring". It should be borne in mind that there are two binary operations, viz, + and . , on R.

2. It should also be borne in mind that the binary operations + and . may not be known usual addition and multiplication.

3. Since R is an additive Abelian group, the additive identity, denoted by 0, belongs to R. It is called the zero element of R. Here 0 is a symbol. It should not be confused with the real number zero.

4. If a , $b \in R$, then - $b \in R$ ($\because$ R is an additive group). a+ (– b) is, generally, denoted by a – b.

5. a.b is, generally, written as ab.

Commutative Ring: A ring R is said to be commutative if ab = ba, for all a, $b \in R$.

Ring with unity : A ring R is said to be a ring with unity (or identity) if there exists an element $e \in$ R such that

ae = a = ea, for all $a \in R$.

Note 1. A ring may or may not have a unity.

2. If R is a ring with unity, unity may be same as the zero element. For example, {0} is a commutative ring with unity . Here 0 is the additive as well as the multiplicative identity. It is known as the zero ring.

Theorem 1 : If R is a ring with unity, then unity is unique.

Proof Let R be a ring with unity. If possible, let e and f be two identities of R.

ef = e = fe [$\because$ f is unity]

ef = f = fe [$\because$ e is unity]

$\therefore$ e = f

Note: In view of the above theorem, we write "the unity".

Example 1. Let R = $\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$: a, b are integers$\}$

I (i) Let $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in$ R, $\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \in$ R,

a, b, c, d $\in$ Z

Now $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ 0 & 0 \end{pmatrix} \in R$

$\therefore$ Matrix addition is a binary operation on R.

(ii) We know that matrix addition is associative.

(iii) We have 0 = $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in$ R,

and $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

(iv) For every $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in$ R, we have $\begin{pmatrix} -a & -b \\ 0 & 0 \end{pmatrix} \in$ R such that

$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -a & -b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} -a & -b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$

$\therefore \begin{pmatrix} -a & -b \\ 0 & 0 \end{pmatrix}$ is the additive inverse of $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$.

(v) We know that matrix additive is commutative.

$\therefore$ R is an Abelian group under matrix addition.

II. (i) We have $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix} \in R$

$\therefore$ matrix multiplication is a binary operation on R

(ii) We know that matrix multiplication is associative.

$\therefore$ R is a semigroup under matrix multiplication.

III. We know that matrix multiplication is distributive over matrix addition.

The two distributive laws are satisfied.

$\therefore$ R is a ring under matrix addition and matrix multiplication.

We have $\begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix} \in R$, $\begin{pmatrix}3 & 4\\ 0 & 0\end{pmatrix} \in R$

$$\begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix}\begin{pmatrix}3 & 4\\ 0 & 0\end{pmatrix}=\begin{pmatrix}3 & 4\\ 0 & 0\end{pmatrix}$$

$$\begin{pmatrix}3 & 4\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix}=\begin{pmatrix}3 & 6\\ 0 & 0\end{pmatrix}$$

$$\therefore \begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix}\begin{pmatrix}3 & 4\\ 0 & 0\end{pmatrix} \neq \begin{pmatrix}3 & 4\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix}$$

$\therefore$ R is a non- commutative ring.

Again, there does not exist any element $X \in G$ such that

$$x\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}=\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}=\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}x \text{, for all } \begin{pmatrix}a & b\\ 0 & 0\end{pmatrix} \in R$$

$\therefore$ R is a ring without unity.

Example 2 Let R be the set of all 2 x 2 matrices over integers.

I. Clearly R is an Abelian group under matrix addition.

II. R is a semigroup under matrix multiplication.

III. The two distributive laws are satisfied.

$\therefore$ R is a ring under matrix addition and matrix multiplication.

We know that matrix multiplication is not, in general, commutative.

$\therefore$ R is a non-commutative ring.

We have $I = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \in R$, and

$AI = A = IA$, for all $A \in R$.

$\therefore$ R is a ring with unity.

Example 3: Let 2Z be the set of all even integers

I. 2Z is an Abelian group under usual addition.

II. 2Z is a multiplicative semigroup.

III. The two distributive laws are satisfied.

$\therefore$ 2Z is a ring under usual addition and multiplication.

Moreover, 2Z is a commutative ring.

2Z is a ring without unity, for $1 \notin 2Z$.

Example 4: Let Z be the set of integers.

I. Z is an Abelian group under usual addition.

II. Z is a multiplicative semigroup.

III. The two distributive laws are satisfied.

$\therefore$ Z is a ring under usual addition and scalar multiplication.

Moreover, Z is a commutative ring . It is also a ring with unity, $1 \in Z$.

Other examples of commutative rings with unity are

- the ring Q of rational numbers
- the ring IR of real numbers.
- the ring C of complex numbers.

Example 5: Let C [a, b] denote the set of all real-valued continuous functions defined on [a, b] ; a, $b \in R$

Let $f, g \in C[a, b]$

We define $(f + g)(x) = f(x) + g(x)$

$(fg)(x) = f(x)\, g(x),\ x \in [a, b]$

I. (i) We have $(f + g)(x) = f(x) + g(x) \in R$

Also, the sum of two continuous functions is continuous.

$\therefore$ f + g is continuous and so $f + g \in C[a, b]$

$\therefore$ addition of functions is a binary operation on C [a, b].

(ii) Let $f, g, h \in C[a, b]$, $x \in [a, b]$

$$\begin{aligned}((f+g)+h)(x) &= (f+g)(x) + h(x) \\ &= \big(f(x) + g(x)\big) + h(x) \\ &= f(x) + \big(g(x) + h(x)\big) \\ &= f(x) + (g+h)(x) \\ &= \big(f + (g+h)\big)(x), \forall x \in [a, b]\end{aligned}$$

$\therefore (f + g) + h = f + (g + h)$

(iii) We have $0 : [a, b] \to R$, $0(x) = 0$, $\forall\, x \in [a, b]$

Clearly $0 \in C[a, b]$, and

$0 + f = f = f + 0$

(iv) For every $f \in C[a, b]$, we define

$-f : [a, b] \to R$, $(-f)(x) = -f(x)$

Clearly $-f \in C[a, b]$, and

$$(f + (-f))(x) = f(x) + (-f)(x) = f(x) - f(x) = 0 = 0(x)$$

$\therefore f + (-f) = 0$

Similarly (–f) + f = 0

(v) (f + g) (x) = f (x) + g (x)

= g (x) + f (x)

= (g + f) (x), $\forall$ x $\in$ [a, b]

$\therefore$ f + g = g + f

$\therefore$ C [a, b] is an Abelian group under addition of functions.

II. (i) (fg) (x) = f (x) g (x) $\in \mathrm{R}$

Also, the product of two continous functions is continuous.

$\therefore$ fg is continuous and so fg $\in$ C [a, b].

$\therefore$ Multiplication of functions is a binary operation on C [a, b]

(ii) ((fg) h) (x) = (fg) (x) h (x)

= (f (x) g (x)) h (x)

= f (x) (g (x) h (x))

= f (x) (gh) (x)

= (f (gh)) (x), $\forall x \in [a, b]$

$\therefore$ (fg)h = f (gh)

$\therefore$ C [a, b] is a semigroup under multiplication of functions.

III. ((f+g) h) (x)= (f + g) (x) h (x)

= (f (x) + g (x)) h (x)

= f (x) h (x) + g (x) h(x)

= (f h) (x) + (gh) (x)

= (fh + gh)(x)

$\therefore$ (f + g) h = fh + gh

Similarly f (g + h) = fg + fh

$\therefore$ C [a , b] is a ring under addition and multiplication of functions.



CHECK YOUR PROGRESS - 1

Q 1: Give an example of a commutative ring with unity having only one element.

Q 2: Give an example of a non-commutative ring without unity.

Q 3: Give an example of a commutative ring without unity.

Q 4: Give an example of a non-commutative ring with unity.

Q 5: Give an example of an infinite commutative ring with unity.

Q 6: Let $IR^2 = \{(a, b) : a, b \text{ are reals}\}$

We define

$(a, b) + (c, d) = (a + c, b + d)$,

$(a, b)(c, d) = (ac, bd)$;

a, b, c, d are reals.

Show that IR^2 is a commutative ring with unity.

9.4 PROPERTIES OF RING

Let R be a ring. Then

(i) $a0 = 0a = 0$; for all $a \in R$

(ii) $a(-b) = (-a)b = -(ab)$; for all $a, b \in R$

(iii) $(-a)(-b) = ab$; for all $a, b \in R$

(iv) $a(b - c) = ab - ac$; for all $a, b, c \in R$

Proof (i) we have

$a0 = a(0 + 0)$

$= a0 + a0$, by left distributive law

$\therefore a0 + 0 = a0 + a0$

$\Rightarrow 0 = a0$, by left cancellation law in the additive group R

i. e $a0 = 0$

Similarly $0a = 0$

(ii) We have $a0 = 0$

This $\Rightarrow a((-b) + b) = 0$, $[\because (-b) + b = 0]$

$\Rightarrow a(-b) + ab = 0$, by left distributive law

$\Rightarrow a(-b)$ is the additive inverse of ab

$\therefore$ i.e., $a(-b) = -(ab)$

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

(iii) We have $(-a)(-b) = l(-b)$, taking $l = -a$

$= -(lb)$, using (ii)

$= -((-a)b)$

$= -(-(ab))$, using (ii)

$= ab$

(iv) $a(b - c) = a(b + (-c))$

$= ab + a(-c)$, by left distributive law

$= ab - ac$, by (ii)

Boolean Ring: Let R be a ring and $a \in R$.

a is called an idempotent element of R if $a^2 = a$.

A ring R is called a Boolean ring, if every element of it is idempotent.

Note: George Boole (1815-1864) of the nineteenth century was ''an essentially self-taught Britisher''. He is famous for his epoch - making book The Laws of Thought.

Theroem 3: Let R be a Boolean ring. Then

(i) $a + a = 0$, for all $a \in R$

i. e. every element of R is its own additive inverse

(ii) $a + b = 0 \Rightarrow a = b$, for all $a, b \in R$

(iii) R is a commutative ring.

Proof : (i) Let $a \in R$. $\therefore a^2 = a$

Also $a + a \in R$

$\therefore (a + a)^2 = a + a$ [$\because$ R is a Boolean ring]

$\Rightarrow (a + a)(a + a) = a + a$

$\Rightarrow (a + a)a + (a + a)a = a + a$, By left distributive law

$\Rightarrow (a^2 + a^2) + (a^2 + a^2) = a + a$, by right distributive law

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

$\Rightarrow a + a = 0$, by left cancellation law in the additive group R

(ii) We have $a + a = 0$

$\therefore a + b = a + a$, by (i)

$\Rightarrow b = a$, by left cancellation law in the additive group R

i.e. $a = b$

(iii) Let $a, b \in R \therefore a^2 = a, b^2 = b$

Also $a + b \in R$

$\therefore (a + b)^2 = a + b$

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

$\Rightarrow (a + b)a + (a + b)b = a + b$, by left distributive law

$\Rightarrow (a^2 + ba) + (ab + b^2) = a + b$

$\Rightarrow (a + ba) + (ab + b) = a + b$

$\Rightarrow$ (a + b) + ba + ab = (a + b) + 0, by associative and commutative law of addition.

$\Rightarrow$ ba + ab = 0, by left cancellation law in the additive group R.

$\Rightarrow$ ab = ba, by (ii)

$\therefore$ R is a commutative ring.



CHECK YOUR PROGRESS - 2

Q 1: Let $R = \{a + b\sqrt{2} : a, b \in Z\}$. Show that R is a commutative ring with unity under usual operations of addition and multiplication.

Q 2: If in a ring R, $a^2 = a$ for all $a \in R$, show that 2a = 0 and a + b = 0 $\Rightarrow$ a = b

Q 3: In z,define $\oplus$ and $\otimes$ as $a \oplus b = a + b + 1, a \otimes b = a + b + ab$. Show that Z is a commutative ring under the operations $\oplus$ and $\otimes$. Is it a ring with unity ?

9.5 INTEGRAL DOMAIN

Let us consider the ring R of all 2 x 2 matrices over integers.

Let A = $\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \in R$ and B = $\begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix} \in R$

Here A is not a null matrix, B is not a null matrix, i.e. $A \neq 0$, $B \neq 0$

But AB = $\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}$

= $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$

i.e, AB is a null matrix.

Thus, we see that $A \neq 0$, $B \neq 0$; but AB = O.

Again, let us consider the ring Z of integers. If $a, b \in Z$ and $a \neq 0$, $b \neq 0$, then $ab \neq 0$

Definition: An element a ($\neq 0$) in a ring R is called a zero divisor if there exists an element b ($\neq 0$) in R such that ab = 0 or ba = 0.

We see that the ring R of all 2 x 2 matrices over integers has zero

divisors whereas the ring Z of integers has no zero divisors, for if $a \in Z$, $b \in Z$, $a \neq 0$, $b \neq 0$, then $ab \neq 0$, $ba \neq 0$.

Concellation Laws: Let R be a ring. The additive cancellation laws hold good in R, since R is an additive Abelian group.

So, by cancellation laws in a ring, we mean multiplication laws (cancellation of non zero elements).

The cancellation laws hold good in R if $ab = ac \Rightarrow b = c$, $ba = ca \Rightarrow b = c$; where $a, b, c \in R$, $a \neq 0$.

Theorem 1: The cancellation laws hold good in a ring R if and only if R has no zero divisors.

Proof: Let the cancellation laws hold good in a ring R.

Let $a, b \in R$ such that $ab = 0$

If $a \neq 0$, $ab = 0 \Rightarrow ab = a0 \Rightarrow b = 0$, by cancellation law.

Similarly, if $b \neq 0$, $ab = 0 \Rightarrow ab = 0b \Rightarrow a = 0$.

So there can be no zero divisor.

Conversely, let there be no zero divisors in R.

Let $a, b, c \in R$ and $ab = ac$, $a \neq 0$

$\therefore ab - ac = 0$

$a(b - c) = 0$

$\therefore a \neq 0$ and R is without zero divisors

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

Thus, if $a \neq 0$, $ab = ac \Rightarrow b = c$

similarly, if $a \neq 0$, $ba = ca \Rightarrow b = c$

Thus, the cancellation laws hold good in R.

Definition A commutative ring with unity $e \neq 0$ and containing no zero divisors is called an Integral Domain.

The simplest example of an integral domain is the ring Z of integers. It is a commutative ring, has unity and is without zero divisors.

Note: An integral domain may be considered as a generalisation of Z.

Example 1: Let us consider the set $R = \{a + bi : a, b \text{ are integers}, i = \sqrt{-1}\}$ of Gaussian integers, after the name of C. F. Gauss (1777-1855).

I. (i) Let $a + bi, c + di \in R$,

a, b, c, d are integers, i = $\sqrt{-1}$

(a + bi) + (c + di) = (a + c) + (b + d)i $\in$ R

(ii) Addition of complex numbers is associative.

(iii) We have 0 = 0 + 0i $\in$ R

and 0 + (a + bi) = a + bi = (a + bi) + 0

(iv) For every a + bi $\in$ R, we have (–a) + (–b)i $\in$ R such that

(a + bi) + ((–a) + (–b)i) = 0 =((–a) + (–b)i) + (a + bi)

(v) Addition of complex numbers is commutative.

$\therefore$ R is an Abelian group under addition of complex numbers.

II. (i) (a + bi) (c + di) = (ac – bd) + (ad + bc)i $\in$ R

(ii) Multiplication of complex numbers is associative

$\therefore$ R is a semigroup under multiplication of complex numbers.

III. Clearly the two distributive laws hold good.

$\therefore$ R is a ring

Furthermore, multiplication of complex numbers is commutative.

$\therefore$ R is a commutative ring.

Also R possesses 1 (1=1 + oi)

$\therefore$ R is a ring with unity.

Again we know that the product of two non-zero complex numbers cannot be zero.

$\therefore$ R is without zero divisors.

Thus, R is an integral domain.

9.6 FIELD

Definition: Let R be a ring with unity e $\neq$ 0. If every non-zero element of R has multiplicative inverse in R, then R is called a Division Ring (or a Skew Field).

A commutative division ring is called a field.

The simplest example of a field is the ring IR of real numbers.

It is commutative, has unity and every non-zero element has multiplicative inverse in IR.

Therefore, IR is a field.

Similarly, the ring C of complex numbers is also a field.

Note: The ring z of integers is not a field. (why?)

Example 2: Examine if the ring

R = {a + bi : a, b, are integers, i = $\sqrt{-1}$ }

of Gaussian integers is a field.

Solution: We know that R is a commutative ring with unity.

(Ref. Example 6)

Let a + bi $\in$ R such that a + bi $\neq 0$

Now the multiplicative inverse of a + bi is $\frac{a}{a^2+b^2} + \left(-\frac{b}{a^2+b^2}\right)i$ which is not an element of R.

$\therefore$ R is not a field.

Theorem 2: Every field is an integral domain.

Proof: Let F be a field.

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

$\therefore$ a $\neq$ 0, $a^{-1} \in$ F (F is a field)

Now ab = 0

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

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

$\Rightarrow$ b = 0

Similarly, if b $\neq 0$ and ab = 0, then a = 0

$\therefore$ F has no zero divisors.

Thus, F is a commutative ring with unity and containing no zero divisors.

$\therefore$ F is an integral domain.

Note: The converse of the above theorem is not true, i.e, every integral domain is not a field.

Let us consider the ring Z of integers. We know that Z is an integral domain. But only two elements, viz, –1 and 1 have multiplicative inverses in Z. $\therefore$ Z is not a field.

However we have the following

Theorem 3: A non-zero finite integral domain is a field.

Proof: Let R = {a_1, a_2, a_3, ... a_n} be a finite non-zero integral domain, where all the a_i's are distinct.

Let a_1 be the zero element of R.

Let us consider the non zero elements $a_2, a_3, ..., a_n$.

Let a_p be not the unity of R ($p \neq 1$),i.e., $a_p \neq e$, the unity of R.

Let us consider the products

$a_p a_2,\ a_p a_3, ...,\ a_p a_n$

All these elements belong to R. Also all the elements are distinct, for if

$a_p a_i = a_p a_j$, $2 \leq i \leq n$, $2 \leq j \leq n$, $i \neq j$

then $a_p a_i - a_p a_j = 0$

$\Rightarrow a_p (a_i - a_j) = 0$

$\Rightarrow a_i - a_j = 0$, [$\because a_p \neq 0$ and R is without zero divisors]

$\Rightarrow a_i = a_j$, which is a contradiction

Now one of $a_p a_2, a_p a_3, ..., a_p a_n$ must be unity, Let $a_p a_q = e$, where e is the unity of R

Then $a_p a_q = e = a_q a_p$.

$\therefore a_p$ has multiplicative inverse in R. If a_p is the unity of R, then a_p has multiplicative inverse in R.

Thus, every non-zero element of R has multiplicative inverse in R.

$\therefore$ R is a field.

Theorem 4: A division ring has no zero divisors.

Proof: Let R be a division ring.

Let a, b $\in$ R such that $a \neq 0$ and ab=0

$\therefore a \neq 0$, $a^{-1} \in$ R ($\because$ R is a division ring)

Now ab = 0

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

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

$\Rightarrow b = 0$

Similarly, if $b \neq 0$ and ab = 0, then a = 0.

$\therefore$ R is without zero divisors



CHECK YOUR PROGRESS-3

Q 1: Does the ring Q of rational numbers contain zero divisors?

Q 2: Let R be the ring of all 2 x 2 matrices over integers, Does the cancellation laws hold good in R?

Q 3: Is the ring 2Z of even integers an integral domain?

Q 4: Give an example of an integral domain which is not a field.

Q 5: Does the ring $IR^2 = \{(a, b) : a, b \in IR\}$ contain zero divisiors?



9.7 LET US SUM UP

- A non-empty set R, equipped with two binary operations, called addition (+) and multiplication (·), is called a ring if the following postulates are satisfied.

(i) R is an additive Abelian group

(ii) R is a multiplicative semigroup

(iii) The two distributive laws hold good, viz.,

$a \cdot (b + c) = a.b + a.c$, (left distributive law)

$(a + b).c = a.c + b.c$, (right distributive law)

for all $a, b, c \in R$

- A ring R is said to be commutative if $ab = ba$, for all $a, b \in R$
- A ring R is said to be a ring with unity (or identity) if there exists an element $e \in R$ such that

  $ae = a = ea$, for all $a \in R$
- An element $a(\neq 0)$ in a ring R is called a zero divisor if there exists an element $b (\neq 0)$ in R such that $ab = 0$ or $ba = 0$
- A commutative ring with unity $e \neq 0$ and containing no zero divisors is called an integral domain
- Let R be a ring with unity $e \neq 0$.

  If every non-zero element of R has multiplicative inverse in R, then R is called a division ring (or a skew field).

A commutative division ring is called a field.

- Every field is an integral domain, but every integral domain is not a field.
- A non-zero finite integral domain is a field.



9.8 ANSWERS TO "CHECK YOUR PROGRESS"

CHECK YOUR PROGRESS-1

Ans to Q No1: {0} is a commutative ring with unity. It should be noted that, in this ring, 0 is the additive as well as the multiplicative identity.

Ans to Q No 2: The ring R = $\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$: a, b are integers$\}$ is a non-commutative ring without unity.

Ans to Q No 3: The ring 2Z of even integers is a commutative ring without unity.

Ans to Q No 4: The ring R of all 2 x 2 matrices over integers is a non-commutative ring with unity.

Ans to Q No 5: The ring Z of integers is an infinite commutative ring with unity.

Ans to Q No 6: IR^2 = {(a, b) : a, b are reals}

I. (i) Let (a, b), (c, d) $\in$ IR^2, where a, b, c, d are reals

Now (a, b) + (c, d) = (a + c, b + d) $\in$ IR^2

(ii) Let (a, b), (c, d), (e, f) $\in$ IR^2

((a, b) + (c, d)) + (e, f) = (a + c, b + d) + (e, f)

= ((a + c) + e, (b + d) + f)

= (a + (c + e), b + (d + f))

= (a, b) + (c + e, d + f)

= (a, b) + ((c, d) + (e, f))

$\therefore$ addition is associative.

(iii) We have (0, 0) $\in$ IR^2,

and (0, 0) + (a, b) = (a, b) = (a, b) + (0, 0)

$\therefore$ (0, 0) is the additive identity.

(iv) For every $(a, b) \in IR^2$, we have $(-a, -b) \in IR^2$ such that (a, b) + (–a, –b) = (0, 0) = (–a, –b) + (a, b)

$\therefore$ (–a, – b) is the additive inverse of (a, b).

(v) $(a, b) + (c, d) = (a + c, b + d)$

$= (c + a, d + b)$

$= (c, d) + (a, b)$

$\therefore$ addition is commutative.

$\therefore IR^2$ is an additive Abelian group.

II. (i) $(a, b)(c, d) = (ac, bd) \in IR^2$

(ii) $((a, b)(c, d))(e, f) = (ac, bd)(e, f)$

$= ((ac) e, (bd) f)$

$= (a (ce), b (df))$

$= (a, b) (ce, df)$

$= (a, b) ((c, d) (e, f))$

$\therefore$ multiplication is associative.

$\therefore IR^2$ is a multiplicative semigroup.

III. $(a, b)((c, d) + (e, f)) = (a, b)(c + e, d + f)$

$= (a (c + e), b (d + f))$

$= (ac + ae, bd + bf)$

$= (ac, bd) + (ae, bf)$

$= (a, b)(c, d) + (a, b)(e, f)$

Similarly $((a, b) + (c, d))(e, f) = (a, b)(e, f) + (c, d)(e, f)$

$\therefore IR^2$ is a ring

Furthermore, $(a, b)(c, d) = (ac, bd)$

$= (ca, db)$

$= (c, d)(a, b)$

$\therefore IR^2$ is a commutative ring.

Again, $(1, 1) \in IR^2$, and

$(a, b)(1, 1) = (a1, b1) = (a, b) = (1, 1)(a, b)$

$\therefore$ (1, 1) is the unity.

$\therefore IR^2$ is a ring with unity.

Thus, IR^2 is a commutative ring with unity

CHECK YOUR PROGRESS - 2

Ans to Q No 1: It can be easily verified that R is a commutative ring with

$0 = 0 + 0\sqrt{2}$

as additive identity and $1 = 1 + 0\sqrt{2}$ as the multiplicative identity or unity R.

Ans to Q No 2: Properties of Rings ((i), (ii))

Ans to Q No 3: It can be easily verified that Z is a commutative ring under the given operations.Also $a \otimes 0 = 0 = 0 \otimes a \ \ \forall a \in Z$ .Hence,it is a ring with unity 0.

CHECK YOUR PROGRESS - 3

Ans to Q No 1: No. If a, b$\in$Q and a $\neq 0$, b $\neq 0$, then ab$\neq 0$

Ans to Q No 2: No. Cancellation laws hold good in a ring if and only if it has no zero divisors. The ring of all 2 x 2 matrices over integers contains zero divisors. So cancellation laws do not hold good in the ring of all 2 x 2 matrices over integers.

For example

$$\begin{pmatrix}1 & 3\\ 3 & 9\end{pmatrix}\begin{pmatrix}3 & 3\\ 5 & 7\end{pmatrix} = \begin{pmatrix}18 & 24\\ 54 & 72\end{pmatrix}$$

$$\begin{pmatrix}1 & 3\\ 3 & 9\end{pmatrix}\begin{pmatrix}6 & 9\\ 4 & 5\end{pmatrix} = \begin{pmatrix}18 & 24\\ 54 & 72\end{pmatrix}$$

i. e. $\begin{pmatrix}1 & 3\\ 3 & 9\end{pmatrix}\begin{pmatrix}3 & 3\\ 5 & 7\end{pmatrix} = \begin{pmatrix}1 & 3\\ 3 & 9\end{pmatrix}\begin{pmatrix}6 & 9\\ 4 & 5\end{pmatrix}$,

i. e. AB = AC, but B $\neq$ C,

where $A = \begin{pmatrix}1 & 3\\ 3 & 9\end{pmatrix}, B = \begin{pmatrix}3 & 3\\ 5 & 7\end{pmatrix}, C = \begin{pmatrix}6 & 9\\ 4 & 5\end{pmatrix}$

Ans to Q No 3: The ring 2Z of even integers is not an integral domain, since it does not contain the multiplicative identity.

Ans to Q No 4: The ring Z of integers is an integral domain, but not a field. Only –1 and 1 have multiplicative inverses in Z,

Ans to Q No 5: Yes.

(7, 0) $\in$ IR^2, (0, 13) $\in$ IR^2 ,(7, 0) $\neq$(0, 0), (0, 13) $\neq$(0, 0).

But (7, 0) (0, 13) = (0, 0).



9.9 FURTHER READINGS

1) Lanski, Charles : *Concepts in Abstract Algebra*, (First Indian edition, 2010) American Mathematical Society.
2) Vasistha, A. R. : *Modern Algebra (Abstract algebra),* Krishna Prakashan Media (p) Ltd. Meerut-250001 (U. P).
3) Vinberg, E. B. : *A course in Algebra* (First Indian edition, 2009), American Mathematical Society).
4) Vatsa, B. S. and Vatsa, Suchi : *Modern Algebra*, New Age International (p) Ltd., New Delhi-110002.
5) Sen, M. K, Ghosh, Shamik and Mukhopadhyay, Parthasarthi : *Topics in Abstract Algebra,* Universities Press (India) Pvt. Ltd., Hyderabad, 500029.



9.10 MODEL QUESTIONS

Q 1: Let Z be the set of integers, We define (+) and (·) on Z as follows

a (+) b = a + b – 1,

a (·) b = a + b – ab, for all a, b $\in$ Z

Examine Z is a commutative ring with unity under (+), (·).

Q 2: Prove that a ring R is commutative if and only if

$(a + b)^2 = a^2 + 2ab + b^2$, for all a, b $\in$ R

[Here a^2 means aa]

Q 3: Let R = {(a, b) : a, b are reals}. We define

(a, b) + (c, d) = (a + c, b + d)

(a, b) (c, d) = (ac – bd, bc + ad)

Prove that R is a field.

Q 4: Let R = {$a + b\sqrt{2}$: a, b are rational numbers}. show that R is a field under usual addition and multiplication.

Q 5: Let R be a commutative ring with unity and is without zero divisors. Show that the only idempotent elements are the zero element and the unity element.

*** ***** ***