9

Rings and Fields

OBJECTIVES

- Introduction
- Rings
- Ring with Unity
- Commutative Rings
- Elementary Properties of a Ring
- Zero Divisors
- Integral Domain
- Field
- Division Ring or Skew Field
- Isomorphism of Rings
- Subrings

9.1 Introduction

In chapter 8 we studied algebraic structures that arise from a single binary operation. Here we will study algebraic structures with more than one operations and hence are richer than groups, semigroups and monoids. Some of these algebraic structures arising from an abelian group, are Rings and Fields will be dealt with in the further sections.

9.2 Rings

Definition : An algebraic structure $< \mathbf{R}, +, \cdot >$ is called a ring if (i) **(R, +)** is an abelian group (ii) **(R, ·)** is a semigroup and (iii) the operation '·' is distributive over the operation '+'.

In other words $< R, +, \cdot >$ is called a ring if the following postulates are satisfied :

(i) $a + b \in R$ and $a \cdot b \in R \ \forall \ a, b \in R$

(ii) Addition is associative i.e.,

$(a + b) + c = a + (b + c) \ \forall \ a, b, c \in R$

(iii) Addition is commutative i.e.,

$a + b = b + a \ \forall \ a, b \in R$

(iv) $\exists \ 0 \in R$ such that $0 + a = a = a + 0 \ \forall \ a \in R$

(v) $\forall \ a \in R \ \exists - a \in R$ such that $(- a) + a = 0 = a + (- a)$

(vi) Multiplication is associative i.e.,

$a \cdot (b \cdot c) = (a \cdot b) \cdot c \ \forall \ a, b, c \in R$

(vii) Multiplication is distributive with respect to addition i.e., $\forall \ a, b, c \in R$

$a \cdot (b + c) = a \cdot b + a \cdot c$ (Left distributive law)

and $(b + c) \cdot a = b \cdot a + c \cdot a$ (Right distributive law)

Example 1. The set R consisting of a single element 0 with two binary operations defined by $0 + 0 = 0$ and $0 \cdot 0 = 0$ is a ring. It is called the **null ring** or the **zero ring**.

Example 2. The set I of all integers is a ring with respect to addition and multiplication of integers as the two ring compositions. This ring is called the **ring of integers**.

Solution. As done in groups (I, +) is an abelian group. Also the product of two integers is also an integer, hence I is closed with respect to multiplication of integers. Further multiplication of integers is associative and it is also distributive with respect to addition of integers. Hence $<I, +, \cdot>$ is a ring.

9.3 Ring with Unity

The ring $<R , +, \cdot>$ is said to be ring with unity if it has identity element with respect to the multiplication composition.

i.e., $\exists \ e \in R$ s.t. $a \cdot e = a = e \cdot a \quad \forall \ a \in R$

9.4 Commutative Rings

If in a ring $\langle R, +, \cdot \rangle$ the multiplication composition is also commutative

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

then R is called a **commutative ring.**

Example 3. The set 2I of all even integers is a commutative ring without unity, the addition and multiplication of integers being the two ring compositions.

Example 4. The sets $\langle Q, +, \cdot \rangle$, $\langle R, +, \cdot \rangle$ are commutative rings with unity.

Example 5. The set C of all complex numbers is a commutative ring with unity, the addition and multiplication of complex numbers being the two ring compositions.

Example 6. The set R = {0, 1, 2, 3, 4, 5} is a commutative ring with respect to '$+_6$' and '$\times_6$' as the two ring compositions.

Solution. We form a composition table for 'R' for the compositions $+_6$ and $\times_6$ as :

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

From the composition tables it is clear that

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

Also $0^{-1} = 0$, $1^{-1} = 5$, $2^{-1} = 4$, $3^{-1} = 3$, $4^{-1} = 2$ and $5^{-1} = 1$.

(ii) R is closed with respect to the composition $\times_6$.

(iii) Also we know that '$\times_6$' is an associative composition in R i.e.,

$a \times_6 (b \times_6 c) = (a \times_6 b) \times_6 c \ \forall\ a, b, c, \in R.$

(iv) Let $a, b, c \in R$

$\therefore\ a \times_6 (b +_6 c) = a \times_6 (b + c).$ $[\because\ b + c \equiv b +_6 c \pmod 6]$

$=$ least non negative remainder when $a \cdot (b + c)$ is divided by 6.

$=$ least non negative remainder when $ab + ac$ is divided by 6.

$= (ab) +_6 (ac)$

$= (a \times_6 b) +_6 ac$ $[\because\ a \times_6 b \equiv ab \pmod 6]$

$= (a \times_6 b) +_6 (a \times_6 c)$

Similarly we can prove that

$(b +_6 c) \times_6 a = (b \times_6 a) +_6 (c \times_6 a)$

Hence multiplication distributes over addition.

(v) Also from the table it is clear that $(a \times_6 b) = (b \times_6 a)$

$\therefore$ $<R, +_6, \times_6>$ is a commutative ring.

(vi) Also $1 \in R$ is the identity element for the composition $\times_6$.

$\therefore$ R is a commutative ring with unity.

Remark 1. As seen from above $2 \times_6 3 = 0$. Thus in a ring it is possible that the product of two non–zero element is equal to the zero element, which is an example of finite ring.

Example 7. The set of all $n \times n$ matrices with their elements as real numbers is a non–commutative ring with unity, with respect to addition and multiplication of matrices as the two ring compositions.

Solution. Let R be the set of all $n \times n$ matrices with their elements as real numbers. We know that sum and product of two $n \times n$ matrices with their elements as real numbers are again $n \times n$ matrices with their elements as real numbers. Hence 'R' is closed with respect to addition and multiplication compositions. Further :

(i) $A + (B + C) = (A + B) + C \quad \forall A, B, C \in R.$

As addition of matrices is associative.

(ii) $A + B = B + A \quad \forall A, B, \in R$

As addition of matrices is commutative.

(iii) If O is the null matrix of order $n \times n$, then $O \in R$ and

$O + A = A + O = A \quad \forall A \in R.$

(iv) For each matrix $A \in R$, $\exists -A \in R$ such that $(-A) + A = O = A + (-A)$.

(v) $(AB)C = A(BC) \quad \forall A, B, C \in R$

As multiplication of matrices is associative.

(vi) $A (B + C) = AB + AC$

and $(B + C) A = BA + CA \; \forall A, B, C \in R.$

As matrix multiplication is distributive with respect to matrix addition.

Hence A is a ring with respect to the two given composition. Also as the multiplication of matrices is not in general commutative therefore the ring is a non–commutative ring.

If I be the unit matrix of type $n \times n$, then $I \in R$ and we have

$I.M = M = M \cdot I \quad \forall M \in R$

Therefore the matrix I is the multiplicative identity.

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

9.5 Elementary Properties of a Ring

Theorem 1. If R is a ring, then for all, $a, b, c \in R$

(i) $a\,0 = 0\,a = 0$

(ii) $a(-b) = -(ab) = (-a)\,b$

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

(iv) $a(b - c) = ab - ac$

(v) $(b - c)a = ba - ca$

Proof. (i) We know that

$a\,0 = a(0 + 0) = a\,0 + a\,0$ (by distributive law)

$\Rightarrow 0 + a\,0 = a\,0 + a\,0$ [$\because 0 + a\,0 = a\,0$]

As R is a group with respect to addition, hence applying the right cancellation law we have

$0 = a\,0$

Similarly $0\,a = (0 + 0)\,a = 0\,a + 0\,a$ (by distributive law)

$\Rightarrow 0 + 0\,a = 0\,a + 0\,a$

$\Rightarrow 0 = 0\,a$ (by right cancellation law)

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

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

$\Rightarrow (-a)\,b = -(ab)$ [$\because$ R is a group with respect to addition composition]

Similarly $a[(-b) + b] = a \cdot 0$ [$\because -b + b = 0$]

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

$\Rightarrow a(-b) = -ab$ [$\because$ R is a group with respect to addition composition]

$\Rightarrow a(-b) = (-a)\,b = -ab$

(iii) $(-a)(-b) = -[(-a)\,b]$ [using property (ii)]

$= -[-(ab)]$ [using property (ii)]

$= ab$ [$\because$ R is a group $\Rightarrow -(-a) = a\ \forall\ a \in R$]

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

$= ab + a(-c)$ [by distributive law]

$= ab + [-(ac)]$ [using property (ii)]

$= ab - ac$

(v) $(b - c)\,a = [b + (-c)]\,a$

$= ba + (-c)a$ [by distributive law]

$= ba + [-(ca)]$ [property (ii)]

$= ba - ca$

9.6 Zero Divisors

Definition : A non zero element 'a' of a ring R is called a zero divisor or a divisor of zero if there exists an element $b \neq 0 \in R$ such that either $ab = 0$ or $ba = 0$.

A ring having zero divisor is said to be **ring with zero divisors.**

Ring without zero divisors : A ring R is without zero–divisors if the product of no two non–zero elements of R is zero, i.e. if $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$.

Example 8. If R is a ring of all 2×2 matrices with their elements as integers, the two compositions being addition and multiplication of matrices, then R is a ring with zero divisors.

Solution. Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ be the two non–zero elements of the ring R.

Then $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = O$ (null matrix).

$BA = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \neq O$ (null matrix)

Hence we have

$AB = O$ where $A \neq O$ and $B \neq O$

Hence R is a ring with zero divisors.

Example 9. Consider $R = \{(0, 1, 2, 3, 4, 5), +_6, \times_6]$

Then R is a ring with zero divisors as $2 \times_6 3 = 0$, i.e., product of two non–zero elements is equal to the zero element of the ring (refer example 6).

Example 10. The ring of integers is a ring without zero divisors as the product of two non–zero integers cannot be equal to the zero integer.

9.7 Cancellation Laws in a Ring

If R is a ring then R is an abelian group with respect to addition. Hence for addition composition the cancellation laws hold in all rings.

We say that cancellation law hold in a ring R if

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

and $a \neq 0$, $ba = ca \Rightarrow b = c$ $\quad \forall\ a, b, c \in R$

Theorem 2. A ring R is without zero divisors if and only if the cancellation laws hold in R.

Proof. Let R be a ring without zero divisors. Let $a, b, c \in R$ such that $a \neq 0$ and $ab = ac$.

$\Rightarrow ab - ac = 0 \Rightarrow a(b - c) = 0$

$\Rightarrow b - c = 0$ $\quad$ (as $a \neq 0$)

$\Rightarrow b = c$

Thus left cancellation laws hold in R. Similarly we can show that right cancellation law also holds in R.

Now **conversely** suppose that the cancellation law holds in R.

Let $ab = 0$, $a \neq 0$ $\quad b \neq 0$.....(1)

Then we have $ab = a0$ $\quad (\because a\ 0 = 0)$

Now $a \neq 0 \Rightarrow b = 0$, by left cancellation law which is a contradiction to our assumption (1). Hence R is a ring without zero divisors.

9.8 Integral Domain

Definition : A ring is called an integral domain if it (i) is commutative (ii) has unit element (iii) is without zero divisors.

Example 11. The ring I of integers is a commutative ring with unity and also does not possess zero divisors, hence is an example of integral domain.

Example 12. The algebraic structures (Q, +, ·), (R, +, ·), (C, +, ·) are all integral domains.

Example 13. R = [{0, 1, 2, 3, 4}, $+_5$, $\times_5$] is a finite integral domain.

9.9 Field

Invertible elements in a ring with unity : In a ring every element already possesses additive inverse. If R is a ring with unity, then an element $a \in R$ is called invertible, if there exists $b \in R$ such that $ab = 1 = ba$, and we write $b = a^{-1}$.

Example 14. 1 and – 1 are the invertible elements of the ring of all integers.

Example 15. All n × n non–singular matrices with their elements as real numbers are the invertible elements of the ring of all n × n matrices with elements as real numbers.

Definition : A ring R with at least two elements is called a **field** if it, (i) is commutative (ii) has unity (iii) is such that each non–zero element possesses multiplicative inverse.

Example 16. (Q, +, ·), (R, +, ·) (C, +, ·) are examples of field.

Example 17. (0, 1, 2, 3, 4), $+_5$, $\times_5$) is a finite field.

9.10 Division Ring or Skew Field

A ring R with at least two elements is called a division ring or skew field if (i) it has unity (ii) each non zero element possesses multiplicative inverse.

Hence a commutative division ring is a field and every field is also a division ring.

A field has no zero divisors. Therefore in a field the product of two non–zero elements will again be a non–zero element. Also the unit element $1 \neq 0$ and eacn non–zero element possesses multiplicative inverse which is again a non–zero element. The multiplication is commutative as well as associative. Therefore the non–zero elements of a field form an abelian group with respect to multiplication.

Theorem 3. Every field is an integral domain but the converse is not true.

Proof. Field F is a commutative ring with unity, therefore in order to show that every field is an integral domain we must show that a field has no zero divisors. Let a, b, c ∈ F with $a \neq 0$ and $ab = 0$.

Since $a \neq 0 \Rightarrow a^{-1}$ exists and

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

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

$\Rightarrow 1 \cdot b = 0$

$\Rightarrow b = 0$

Similarly if we suppose $b \neq 0$ and $ab = 0$ then $(ab)\, b^{-1} = 0\, b^{-1}$

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

$\Rightarrow a \cdot 1 = 0$

$\Rightarrow$ a = 0

Hence in a field ab = 0 $\Rightarrow$ either a = 0 or b = 0. Therefore a field has no zero divisors. Hence every field is an integral domain.

But the converse is not true. Consider the example of ring of integers which is an integral domain but not a field as only 1 and – 1 are the invertible elements.

Theorem 4. A finite commutative ring without zero divisors is a field. In other words, every finite integral domain is a field.

Proof. Let D be a finite commutative ring without zero divisors having n elements $d_1, d_2, ..., d_n$. In order to prove that D is a field, we must find an element $1 \in D$ such that $1d = d \ \forall \ d \in D$. Also we should show that for every element $d \neq 0 \in D$ there exists an element $e \in D$ such that ed = 1.

Let $d \neq 0 \in D$. consider the n products $dd_1, dd_2, ..., dd_n$. All these are elements of D. Also they are all distinct. For suppose that $dd_i = dd_j$ for $i \neq j$.

Let $d(d_i - d_j) = 0$ .....(1)

Since D is without zero divisors and $d \neq 0$, therefore (1) implies

$d_i - d_j = 0 \Rightarrow d_i = d_j$, contradicting $i \neq j$

$\therefore$ $dd_1, dd_2, ..., dd_n$ are all n distinct elements of D placed is some order. So one of these elements will be equal to d. Thus there exists an element, say, $f \in D$ such that

df = d = fd [$\because$ D is commutative]

We shall show that this element f is the multiplicative identity of D. Let y be any element of D. Then from the above discussion for some $x \in D$, we shall have dx = y = xd.

Now fy = f(d x) [$\because$ dx = y]

= (fd) x

= dx [$\because$ fd = d]

= y [$\because$ dx = y]

= yf [$\because$ D is commutative]

Thus fy = y = yf, $\forall$ $y \in D$. Therefore f is the unit element of the ring D and let us denote it by 1.

Now $1 \in D$. Therefore from the above discussion one of the n products $dd_1, dd_2, ..., dd_n$ will be equal to 1. Thus there exists an element, say $e \in D$ such that

de = 1 = ed

$\therefore$ e is the multiplicative inverse of the non–zero element $d \in D$. Thus every non–zero element of D is invertible.

Hence D is a field. **Hence Proved.**

9.11 Isomorphism of Rings

A ring R is said to be isomorphic to another ring R' if there exists a one–one mapping f of R into R' such that

$f(a + b) = f(a) + f(b)$

and $f(ab) = f(a)\, f(b) \quad \forall\ a, b \in R$

If the above mapping 'f' is onto then f is said to be isomorphism of R onto R'.

Example 18. Let R be the ring of integers under ordinary addition and multiplication. Let R' be the set of all even integers. Let is define multiplication in R' to be denoted by '*' by the relation

$$a * b = \frac{ab}{2}$$

where ab is the ordinary multiplication of two integers a and b.

(i) Prove that (R', +, *) is a commutative ring, where + stands for ordinary addition of integers.

(ii) Prove that R is isomorphic to R'.

(iii) What is the unit element of R ?

Solution. It is obvious that R' is an abelian group with respect to addition.

Closure : Also if a and b both are even integers then $\frac{ab}{2}$ is also an even integer.

Therefore $a * b = \frac{ab}{2} \in R', \forall\ a, b, \in R'$

$\therefore$ R' is closed with respect to *.

Associativity : $\forall\ a, b, c \in R'$

$$a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{a\left(\frac{bc}{2}\right)}{2} = \frac{\left(\frac{ab}{2}\right)c}{2} = \left(\frac{ab}{c}\right) * c$$

$$= (a * b) * c$$

$\therefore$ * is associative.

Commutative : $\forall\ a, b, \in R'$

$$a * b = \frac{ab}{2} = \frac{ba}{2} = b * a$$

$\therefore$ * is commutative.

Distributive : $\forall\ a, b, c \in R'$, we have

$$a * (b + c) = \frac{a(b+c)}{2} = \frac{ab}{2} + \frac{ac}{2} = (a * b) + (a * c)$$

Similarly

$$(b + c) * a = \frac{(b+c)a}{2} = \frac{ba}{2} + \frac{ca}{2} = (b * a) + (c * a)$$

$\therefore$ $*$ is distributive with respect to $+$.

$\therefore$ $(R', +, *)$ is a commutative ring.

(ii) Let $f : R \to R'$ such that $f(r) = 2r$, $\forall\ r \in R$

Then mapping f is obviously one–one and onto.

Also $\forall\ r_1, r_2 \in R$ we have

$$f(r_1 + r_2) = r(r_1 + r_2) = 2r_1 + 2r_2 = f(r_1) + f(r_2)$$

and $(r_1 r_2) = 2(r_1 r_2) = \frac{(2r_1)(2r_2)}{2}$

$$= (2r_1) * (2r_2) = f(r_1) * f(r_2)$$

$\therefore$ The mapping 'f' is an isomorphism from R onto R'.

(iii) '1' is the unit element of R. $f(1) = 2$ and as f is an isomorphism of R onto R', therefore 2 must be the unit element of R'.

Also $\forall\ a \in R'$, $2 * a = \frac{2a}{2}$

$\therefore$ 2 is the unit element of R'.

9.12 Subrings

Let R be a ring. A non–empty subset S of the set R is said to be a subring of R if S is closed with respect to the operations of addition and multiplication in R and S itself is a ring for these operations.

Theorem 5. The necessary and sufficient conditions for a non–empty subset S of a ring R to be a subring of R are

(i) $a \in S, b \in S \Rightarrow a - b \in S$

(ii) $a \in S, b \in S \Rightarrow ab \in S$

Proof. Conditions are necessary

Let $(S, +, \cdot)$ is a subring of $(R, +, \cdot)$.

Since S is a group with respect to addition, so $b \in S \Rightarrow -b \in S$.

Also S is closed with respect to addition so $a \in S, b \in S \Rightarrow a \in S, -b \in S$

$\Rightarrow a + (-b) = a - b \in S$.

Again, S is closed with respect to multiplication so

$$a \in S, b \in S \Rightarrow ab \in S$$

Hence the conditions are necessary.

Conditions are sufficient

Let S be a non–empty subset of R and the conditions :

(i) $a \in S, b \in S \Rightarrow a - b \in S$ (ii) $a \in S, b \in S \Rightarrow ab \in S$ are satisfied.

Now (i) $\Rightarrow a \in S, a \in S \Rightarrow a - a = 0 \in S$ i.e., zero element belongs to S.

Since $0 \in S$ so (i) $\Rightarrow 0 \in S, a \in S \Rightarrow 0 - a = -a \in S$

$\Rightarrow$ each element of S possesses additive inverse.

Also, $a \in S, b \in S \Rightarrow a \in S, -b \in S$

$\Rightarrow a - (-b) = a + b \in S$

$\therefore$ S is closed with respect to addition.

As S is a subset of R, therefore, associativity and commutativity for addition must hold in S, since they hold in R.

Then (S, +) is an abelian group.

From (ii) S is closed for multiplication.

Also associativity of multiplication and distributivity of multiplication over addition must hold in S as they hold in R.

Hence Proved.

Hence S is a subring of R.

Example 19. The set of integers is a subring of the ring of rational numbers.

Solution. If $a, b \in I \Rightarrow a - b \in I$ and $a\,b \in I$. Therefore I is a subring of the ring of rational numbers.

Example 20. Let R be the ring of integers. Let m be any fixed integer and let S be any subset of R such that

$S = \{....., -3m, -2m, -m, 0, m, 2, 3m .....\}$

Then show that S is a subring of R.

Solution. Let $a = rm$, $b = sm$ be two elements of S, where r and s are some integers. Then $a - b = rm - sm = (r - s)\,m = p\,m \in S$

$(ab) = (rm)\,(sm) = (r\,s\,m)\,m = q\,m \in S$

as $r, s \in I \Rightarrow r - s \in I$

as $r, s, m \in I \Rightarrow r\,s\,m \in I$

Hence S is a subring of R.

ILLUSTRATIVE EXAMPLES

Example 21. If a, b, c, d are any elements of ring R, prove that

$(a - b)(c - d) = (ac + bd) - (ad + bc)$.

Solution. We have

$(a - b)(c - d) = (a - b)c - (a - b)d$ [$\because a(b - c) = ab - ac$]

$= (ac - bc) - (ad - bd) = (ac - bc) - ad + bd$

$= (ac + bd) - bc - ad$ [$\because$ addition is commutative and associative]

$= (ac + bd) - (bc + ad)$.

Example 22. If R is a ring such that $a^2 = a \ \forall \ a \in R$ prove that

(i) $a + a = 0 \ \forall \ a \in R$ i.e., each element of R is its own additive inverse.

(ii) $a + b = 0 \Rightarrow a = b$.

(iii) R is a commutative ring.

Solution. (i) $a \in R \Rightarrow a + a \in R$

Now $(a + a)^2 = (a + a)$[given]

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

$\Rightarrow (a + a)a + (a + a)a = a + a$ [Left distributive law)

$\Rightarrow (a^2 + a^2) + (a^2 + a^2) = a + a$ [Right distributive law]

$\Rightarrow (a + a) + (a + a) = a + a$ [$\because a^2 = 0$]

$\Rightarrow (a + a) + (a + a) = (a + a) + 0$ [$\because a + 0 = a$]

$\Rightarrow (a + a) = 0$ [by left cancellation law for addition in R.

(ii) We have just proved that $a + a = 0$.

$\therefore \ a + b = 0 \Rightarrow a + b = a + a \Rightarrow b = a$, by left cancellation law for addition in R.

(iii) We have

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

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

$\Rightarrow (a + b)a + (a + b)b = a + b$ [Left distributive law]

$\Rightarrow (a^2 + ba) + (ab + b^2) = a + b$ [Right distributive law]

$\Rightarrow (a + ba) + (ab + b) = a + b$ [$\because a^2 = a, b^2 = b$]

$\Rightarrow (a + b) + (ba + ab) = (a + b) + 0$ [by commutativity and associativity of addition]

$\Rightarrow ba + ab = 0$ [by left cancellation law for addition in R]

$\Rightarrow ab = ba.$ [by part (ii) of this equation]

$\therefore$ R is a commutative ring.

Example 23. Do the following sets form integral domains with respect to ordinary addition and multiplication? If so state if they are fields.

(i) The set of numbers of the form $b\sqrt{2}$ with b rational.

(ii) The set of even integers.

(iii) The set of positive integers.

Solution. (i) Let $A = \{b\sqrt{2} : b \in Q\}$.

We have $3\sqrt{2}$ and $5\sqrt{2}$. Then $(3\sqrt{2})(5\sqrt{2}) = 30$.

Now 30 cannot be put in the form $b\sqrt{2}$ where b is a rational number. Therefore $30 \notin A$. Thus A is not closed with respect to multiplication.

Hence A cannot be a ring.

(ii) Let R be the set of all even integers. Then R is a ring with respect to addition and multiplication of integers. Also the multiplication is a commutative composition. R is without zero divisors since the product of two non–zero even integers cannot be equal to zero which is the zero element of this ring. Since the integer $1 \notin R$, therefore R is a ring without unity.

R will be an integral domain as we do not require the existence of the unit element for the integral domain.

But R is not a field since the multiplicative identity does not exist.

(iii) Let N be the set of positive integers. Since the integer $0 \notin N$, therefore the additive identity does not exist. So N will not be a ring.

Example 24. Prove that the set R of all ordered pairs (a, b) of real numbers is a commutative ring with zero divisors under the addition and multiplication of ordered pairs defined as

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

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

$\forall\ (a, b), (c, d) \in R.$

Solution. We see that R is closed with respect to the two compositions since a + c, b + d, ac, bd are all real numbers. Now let (a, b), (c, d), (e, f) be any elements of R. Then we observe :

Associativity of addition : We have

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

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

$$= (a + (c + e), b + (d + f)) \quad [\because \text{ addition of real numbers is associative}]$$

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

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

$\therefore$ addition in R is associative.

Commutativity of addition : We have

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

$\therefore$ addition in R is commutative.

Existence of additive identity : We have $(0, 0) \in R$.

Also $(0, 0) + (a, b) = (0 + a, 0 + b) = (a, b)$.

Existence of additive inverse : If $(a, b) \in R$, then $(-a, -b) \in R$ and we have

$(-a, -b) + (a, b) = (-a + a, -b + b) = (0, 0)$.

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

Associativity of multiplication : We have

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

$= (a\ (ce), b\ (df))$ [$\because$ multiplication of real numbers is associative]

$= (a, b)\ (ce, df) = (a, b)\ ((c, d)\ (e, f))$

$\therefore$ multiplication in R is associative.

Distributive laws : We have

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

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

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

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

Similarly we can show that the other distributive law also holds good.

$\therefore$ R is a ring with respect to the given compositions.

Commutativity of multiplication : We have

$(a, b)\ (c, d) = (ac, bd) = (ca, db) = (c, d)\ (a, b)$.

$\therefore$ R is a commutative ring.

Existence of multiplicative identity : We have

$(1, 1) \in R$. If $(a, b) \in R$, then $(1, 1)\ (a, b) = (1a, 1b) = (a, b) = (a, b)\ (1, 1)$.

$\therefore$ $(1, 1)$ is the multiplicative identity and is therefore the unit element of the ring.

So R is a ring with unity.

The zero element of this ring is the ordered pair $(0, 0)$.

Now in order to show that R is a ring with zero divisors we should show that there exist two non–zero elements of R whose product is equal to the zero element of R. Obviously neither $(3, 0)$ nor $(0, 5)$ is equal to the zero element of R. But $(3, 0)\ (0, 5) = (3 \times 0, 0 \times 5) = (0, 0)$ which is the zero element of R.

$\therefore$ R is a ring with zero divisors.

Example 25. Let C be the set of the ordered pairs (a, b) of real numbers. Addition and multiplication in C are defined by the equations

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

$(a, b)\ (c, d) = (ac - bd, bc + ad)$

Prove that C is a field.

Solution. We see that C is closed ith respect to the two compositions since $a + c$, $b + d$, $ac - bd$, $bc + ad$ are all real numbers. Now let (a, b), (c, d), (e, f) be any elements of C. Then we make the following observations :

Associativity of addition : We have

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

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

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

Commutativity of addition : We have

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

Existence of additive identity : We have $(0, 0) \in C$.

Also $(0, 0) + (a, b) = (0 + a, 0 + b) = (a, b)$.

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

Existence of additive inverse : If $(a, b) \in C$, then $(-a, -b) \in C$. We have

$$(-a, -b) + (a, b) = (-a + a, -b + b) = (0, 0).$$

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

Associativity of multiplication : We have

$$[(a, b)\ (c, d)]\ (e, f) = (ac - bd, bc + ad)\ (e, f)$$

$$= ((ac - bd)\ e - (bc + ad)\ f, (bc + ad)\ e + (ac - bd)\ f)$$

$$= (a\ (ce - df) - b\ (de + cf)\ ,\ b\ (ce - df) + a(de + cf))$$

$$= (a, b)\ (ce - df, de + cf) = (a, b)\ ((c, d)\ (e, f)).$$

Distributive laws : We have

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

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

$$= ((ac - bd) + (ae - bf), (bc + a\ d) + (be + af))$$

$$= (ac - bd, bc + ad) + (ae - bf, be + af) = (a, b)\ (c, d) + (a, b)\ (e, f).$$

Similarly we can show that the other distributive law also holds good.

Therefore C is a ring with respect to the two compositions.

$(0, 0)$ is the unit element of the ring.

Commutativity of multiplication : We have

$$(a, b)\ (c, d) = (ac - bd, bc + ad) = (ca - db, da + cb) = (c, d)\ (a, b).$$

Existence of multiplicative identity : We have $(1, 0) \in C$.

If $(a, b) \in C$, then $(a, b)(1, 0) = (a1 - b0, b1 + a0) = (a, b) = (1, 0)(a, b)$

Therefore (1, 0) is the unit element of the ring.

Existence of multiplicative inverse of each non–zero element of C : Let (a, b) be any non–zero element of C. Then a and b are not both simultaneously zero. If (c, d) is the multiplicative inverse of (a, b), then we should have

$$(a, b)(c, d) = (1, 0)$$

or, $(ac - bd, bc + ad) = (1, 0)$.

By the definition of the equality of two ordered pairs, we have

$$ac - bd = 1 \text{ and } bc + ad = 0.$$

Solving these equations for c, d, we get

$$c = \frac{a}{a^2+b^2}, \; d = \left(-\frac{b}{a^2+b^2}\right)$$

Now $a \neq 0$ or $b \neq 0 \Rightarrow a^2 + b^2 \neq 0$. Therefore either c or d or both are non–zero real numbers.

Thus $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$ is the multiplicative inverse of (a, b).

Hence C is a field.**Hence Proved.**

Example 26. Prove that the set of residue classes modulo p is a commutative ring with respect to addition and multiplication of residue classes. Further show that the ring of residue classes modulo p is a field if and only if p is prime.

Solution. Let I_p be the set of residue classes modulo p. Then I_p has p distinct elements. Thus $I_p = \{[0], [1]2, [2]3, ..., [p - 1]\}$.

Let $[a], [b] \in I_p$. Then we define addition and multiplication of residue classes as follows :

$[a] + [b] = [a + b]$, (addition)

$[a][b] = [ab]$ (multiplication)

Since $[a + b]$ and $[ab]$ are both residue classes modulo p, therefore I_p is closed with respect to addition and multiplication.

Now let [a], [b], [c] be any elements of I_p. Then we observe :

Commutativity of addition

$[a] + [b] = [a + b]$ (by def. of addition of residue classes)

$= [b + a]$ ($\because$ addition of integers is commutative)

$= [b] + [a]$

Associativity of addition : We have

$([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)]$

$= [a] + [b + c] = [a] + ([b] + [c])]$.

Existence of additive identity : We have $[0] \in I_p$.

If $[a] \in I_p$ then $[0] + [a] = [0 + a] = [a]$. Therefore [0] is the addictive identity.

Existence of additive inverse : Let $[a] \in I_p$. Then $[-a] \in I_p$. We have $[-a] + [a] = [-a + a] = [0]$. Therefore $[-a]$ is the additive inverse of [a].

Associativity of multiplication : We have

$$([a]\,[b]\,[c] = [ab]\,[c] = [(ab)\,c] = [a\,(bc)] = [a]\,[bc] = [a]\,([b]\,[c])].$$

Commutativity of multiplication : We have

$$[a]\,[b] = [ab] = [ba] = [b]\,[a].$$

Distributive laws : We have

$$[a]\,([b] + [c]) = [a]\,[b + c] = [a\,(b + c)] = [ab + ac]$$
$$= [ab] + [ac] = [a]\,[b] + [a]\,[c]$$

Similarly $([b] + [c])\,[a] = [b]\,[a] + [c]\,[a]$.

Thus I_0 is a commutative ring. Note that it is a finite ring because it has p elements. Now suppose that p is a prime number. Then we have to prove that I_p is a field. Let $[a], [b] \in I_p$. Then

$$[a]\,[b] = [0] \Rightarrow [ab] = [0]$$

$\Rightarrow$ p is a divisor of ab i.e., $p \mid ab$

$\Rightarrow p \mid a$ or $p \mid b$. [Note that if a and b are any two integers and p is a prime number, then $p \mid ab \Rightarrow p \mid a$ or $p \mid b$]

$\Rightarrow [a] = [0]$ or $[b] = [0]$.

Thus I_p is without zero divisors. Therefore I_p is an integral domain. But every finite integral domain is a field. Hence I_p is a field.

Conversely suppose that I_p is a field. The I_p is an integral domain. Therefore I_p is without zero divisors. We are to prove that p is a prime number. Suppose p is not prime, but p is composite. Let $p = mn$, where $1 < m < p$, $1 < n < p$. Then

$$[mn] = [p]$$
$$\Rightarrow [m]\,[n] = [0] \qquad (\because [p] = [0])$$

Also $[m] \neq [0]$, since $1 < m < p$. Similarly $[n] \neq [0]$.

Thus $[m]\,[n] = [0]$ while neither $[m] = [0]$ nor $[n] = [0]$.

Therefore, I_p possesses zero divisors and thus we get a contradiction. Hence p must be prime.

Example 27. Let R be the ring of all 2×2 matrices over the field of real numbers. Let M be a subset of R and let the elements of M be matrices of the type

$$\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$$

i.e., matrices in which the elements of second column are all zero.

The M is a subring of R.

Solution. Let $A = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix}$, be any two elements of M.

Then $A - B = \begin{bmatrix} a_1 - a_2 & 0 \\ a_2 - b_2 & 0 \end{bmatrix}$. Also $AB = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}\begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix} = \begin{bmatrix} a_1a_2 & 0 \\ b_1b_2 & 0 \end{bmatrix}$.

Now A – B and AB are both members of M since the second column of A – B and also of AB consists of zeros only.

∴ M is a subring of R.

Example 28. Show that the set of matrices $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ is a subring of the ring of 2 × 2 matrices with integral elements.

Solution. Let R be the ring of 2 × 2 matrices with integral elements and let M be the subset of R and let the elements of M be matrices of the type $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$.

Let $A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$, $B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$ be any two elements of M.

Then $A - B = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{bmatrix}$ which is obviously an element of M.

Also $AB = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 & a_1b_2 + b_1c \\ 0 & c_1c_2 \end{bmatrix}$ which is obviously an element of M.

∴ M is a subring of R.

Example 29. Let S = {1, 2} and R = P(S) where P(S) is power set of S i.e., R = {ϕ, {1}, {2}, {1,2}}. Define the operation '+' and '·' on R by

$A + B = A \nabla B = \{x \mid x \in A \text{ or } x \in B, \text{ but not both}\}$ **(symmetric difference)**

$A \cdot B = A \cap B$ = intersection of A and B.

Prove that (R, +, ·) is a ring without zero divisors.

Solution. The composition tables can be constructed as follows

+	ϕ	{1}	{2}	{1,2}
ϕ	ϕ	{1}	{2}	{1,2}
{1}	{1}	ϕ	{1,2}	{2}
{2}	{2}	{1,2}	ϕ	{1}
{1,2}	{1,2}	{2}	{1}	ϕ

·	ϕ	{1}	{2}	{1,2}
ϕ	ϕ	ϕ	ϕ	ϕ
{1}	ϕ	{1}	ϕ	{1}
{2}	ϕ	ϕ	{2}	{2}
{1,2}	ϕ	{1}	{2}	{1,2}

From table (1) it is obvious that (R, +) is an abelian group.

From table (2) it is clear that '·' is binary and associative in R. Also table is symmetric about the leading diagonal so the operation '·' is commutative. Further {1, 2} is the unit element for '·'.

Hence R is a commutative ring with unity.

Again, from table (2),

$\{1\} \cdot \{2\} = \phi$

Where $\{1\} \neq \phi$, $\{2\} \neq \phi$

Thus $(R, +, \cdot)$ is a ring without zero divisors.

Example 30. Define the binary operations $\oplus$ and $\odot$ on Z by $x \oplus y = x + y - 7$ and $x \odot y = x + y - 3xy$, $\forall\ x, y \in Z$. Is $(Z, \oplus, \odot)$ is a ring ? If not then why ?

Solution. It can be easily verified that $(Z, \oplus)$ is an abelian group and $(Z, \odot)$ is a semigroup. Now we check the distributive property i.e.,

$x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$

$$\begin{aligned} \text{LHS} &= x \odot (y \oplus z) \\ &= x \odot (y + z - 7) \\ &= x + (y + z - 7) - 3x\,(y + z - 7) \\ &= 22x + y + z - 3xy - 3xz - 7 \end{aligned} \quad \text{.....(1)}$$

Also,

$$\begin{aligned} \text{RHS} &= (x \odot y) \oplus (x \odot z) \\ &= (x + y - 3xy) \oplus (x + y - 3xz) - 7 \\ &= 2x + y + z - 3xy - 3xz - 7 \end{aligned} \quad \text{.....(2)}$$

(1) and (2) $\Rightarrow$ LHS $\neq$ RHS i.e.,

$x \odot (y \oplus z) \neq (x \odot y) \oplus (x \odot z)$

Thus distributive property does not hold in Z.

Hence $(Z, \oplus, \odot)$ is not a ring.

EXERCISE 9

Q.1 Define a ring giving an example of

(i) a non–commutative ring with unity

(ii) a commutative ring with unity.

Q.2 Define a field. Prove that every field is an integral domain, but there exist some integral domains which are not fields.

Q.3 Give an example of :

(i) a non–commutative ring

(ii) ring without zero divisors

(iii) division ring

(iv) a ring which is not an integral domain.

Q.4 Prove that a ring R is commutative if and only if $(a + b)^2 = a^2 + 2ab + b^2\ \forall\ a, b, \in R$.

Q.5 Let p be a prime number. Prove that the set of integers I_p,

$I_p = \{0, 1, 2, 3, ... p-1\}$

forms a field with respect to addition and multiplication modulo p.

Q.6 Let k, m be fixed integers. Find all values for k, m for which $(Z, \oplus, \odot)$ is a ring number the binary operation.

$x \oplus y = x + y - k$; $x \odot y = x + y - m\ x\ y$.

Ans. $k = m = \pm 1$

Q.7 Show that $Z[\sqrt{-5}]$, the set of complex numbers $a + b\sqrt{-5}$ where a and b are integers is an integral domain.

Q.8 Prove that the set of matrices

$$\begin{bmatrix} p & q \\ -\bar{p} & \bar{q} \end{bmatrix}$$

where p, q are complex numbers and $\bar{p}$ and $\bar{q}$ are their complex conjugates respectively, is a skew field for matrix addition and matrix multiplication.

Q.9 Let R be the set of all real valued functions on $(-\infty, \infty)$. Define $(f + g)(x) = f(x) + g(x)$ and $(f \times g)(x) = f(g(x))$ for every x in $(-\infty, \infty)$. Is R a ring with respect to these two operations.

[**Ans.** No; distributive law does not hold)

Q.10 Prove that in a field :

(i) $\frac{a}{b} = \frac{c}{b} \Leftrightarrow ad = bc$

(ii) $\frac{a}{b} - \frac{c}{b} = \frac{ad - bc}{bd}$

(iii) $(-a)^{-1} = -(a^{-1})$

(iv) $\frac{(-a)}{(-b)} = \frac{a}{b}$

Q.11 Show that the set of matrices $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ is a subring of the ring of 2×2 matrices with integral elements.

Q.12 Prove that an arbitrary intersection of subrings is a subring.

Q.13 Show that the set of matrices $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, a, b being real, forms a field isomorphic to the field of complex number.

□□□