A ring $(R, +, \cdot)$ is called a Boolean ring if $a^2 = a$ for every $a \in R$. For example, $R = \{0, 1\}$ is Boolean ring with respect to operations of addition and multiplication modulo 2. Here $\{R, +\}$ is a abelian group and $\{R, \cdot\}$ is a semi group and multiplication is distributive with respect to addition *i.e.* $1.(1 + 1) = 1.1 + 1.1$ where L.H.S $= 1.(1 + 1) = 1.0 = 0$ and R.H.S $= 1.1 + 1.1 = 1 + 1 =$

Example 4. If R is a Boolean ring *i.e.* $a^2 = a \; \forall \; a \in R$ porve 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 $(a + a)^2 = (a + a)$

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

$\Rightarrow (a + a)a + (a + a)a = a + a$ (by left distibutive law)

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

$\Rightarrow (a + a) + (a + a) = a + a$ ($\because a^2 = a$)

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

$\Rightarrow a + a = 0$ (by left cancellation law for addition in R using (*i*)

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

$\Rightarrow b = a$ (by left cancellation law

$\Rightarrow a = b$

(*iii*) Since $a, b \in R$, then $a + b \in R$

We have $(a + b)^2 = (a + b)$ ($\because a^2 = a$)

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

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

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

$\Rightarrow ab = ba.$ by (*ii*)

$\therefore$ R is commutative ring.

Example 5. If two operations * and o on the set Z of integers are defined as follows: $a * b = a + b - 1$, $a \circ b = a + b - ab$, prove that $(Z, *, \circ)$ is a commutative ring with unity element.

Solution. R1. Closure property:

$$a * b = a + b - 1 \in Z, \; \forall \; a, b \in Z.$$

So, * is a binary operation on Z, *i.e.*, Z is closed under *.

R2. Associativity:

$$a * (b * c) = a * (b + c - 1) = a + (b + c - 1) - 1 = a + b + c - 2$$

and $$(a * b) * c = (a + b - 1) * c = (a + b - 1) + c - 1 = a + b + c - 2$$

$\therefore$ $$a * (b * c) = (a * b) * c, \; \forall \; a, b, c \in Z.$$

Hence the operation * is associative.

R3. Commutativity:

$$a * b = a + b - 1 = b + a - 1 = b * a, \; \forall \; a, b \in Z.$$

$\therefore$ $(Z, *)$ forms a commutative group.

R4. Existence of identity:

If e be the identity element then

$$e * a = a, \forall a \in Z$$

$$\Rightarrow \quad e + a - 1 = a \Rightarrow e = 1 \in Z.$$

$$\therefore \quad 1 * a = 1 + a - 1 = a + 1 - 1 = a * 1 = a, \forall a \in Z.$$

$\therefore$ $1 \in Z$ is the identity element.

R5. Existence of inverse:

Let b be the inverse of $a \in Z$.

$$b * a = 1 \Rightarrow b + a - 1 = 1 \Rightarrow b = 2 - a \in Z$$

$\therefore$ For each $a \in Z$, $\exists\ a^{-1} = 2 - a \in Z$ s.t. $a^{-1} * a = a * a^{-1} = 1$.

R6. Z is closed under o:

$$a \circ b = a + b - ab \in Z, \forall a, b \in Z.$$

So, o is a binary operation on Z, *i.e.*, Z is closed under o.

R7. o is associative:

Now, $a \circ (b \circ c) = a \circ (b + c - bc) = a + (b + c - bc) - a(b + c - bc)$

$$= a + b + c - ab - bc - ca + abc$$

Also, $(a \circ b) \circ c = (a + b - ab) \circ c = (a + b - ab) + c - (a + b - ab)c$

$$= a + b + c - ab - bc - ca + abc.$$

$\therefore$ $a \circ (b \circ c) = (a \circ b) \circ c, \forall a, b, c \in Z.$

Hence o is associative.

R8. o is distributive over *:

Now, $a \circ (b * c) = a \circ (b + c - 1)$

$$= a + (b + c - 1) - a(b + c - 1)$$

$$= 2a + b + c - 1 - ab - ac.$$

Again, $a \circ b = a + b - ab$ and $a \circ c = a + c - ac$

$\therefore$ $(a \circ b) * (a \circ c) = (a + b - ab) * (a + c - ac)$

$$= (a + b - ab) + (a + c - ac) - 1$$

$$= 2a + b + c - 1 - ab - ac.$$

$\therefore$ $a \circ (b * c) = (a \circ b) * (a \circ c), \forall a, b, c \in Z.$

Thus $(Z, *, \circ)$ is a commutative ring with unity element.

Existence of unity:

If e be the unity element then

$$e \circ a = a, \forall a \in Z$$

$$\Rightarrow \quad e + a - ea = a \Rightarrow e(1 - a) = 0 \Rightarrow e = 0 \in Z, \forall a \in Z.$$

$$\therefore \quad 0 \circ a = 0 + a - 0 \cdot a = a + 0 - a \cdot 0 = a, \forall a \in Z.$$

$\therefore$ $0 \in Z$ is the unity element.

o is commutative:

$$a \circ b = a + b - ab = b + a - ba = b \circ a, \forall a, b \in Z.$$

Hence o is commutative.

Ring with Zero Divisor

If a and b are two nonzero elements of a ring R such that $ab = 0$, then a and b are divisors of 0 (or 0 divisors). In particular, a is left divisor of 0 and b is right divisor of 0. Then R is said to be a ring with zero divisors.

In a commutative ring, every left divisor of 0 is also a right divisor of 0 and conversely. Thus there is no distinction between left and right divisors of 0 in commutative ring.

A ring R is called a ring without zero divisors or a ring containing no divisor of zero if $a, b \in R$, $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$ or $a = b = 0$.

For example,

(*i*) The ring of integers do not have zero divisors. For there exist no two non-zero integers such that their product is zero.

(*ii*) Suppose M is ring of all 2×2 matrices with their elements as integers, the addition and multiplication of matrices being the two ring composition. Then M is a ring with zero-divisors.

The null matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$ is the zero element of this ring.

Now $A = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 0 & 3 \end{bmatrix}$ are two non-zero elements of this ring.

We have $AB = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$

Thus the product of two non-zero elements of the ring is equal to the zero element of the ring. Therefore, M is a ring with zero divisors.

An elements a of a ring is called **nilpotent,** if there exists some positive integer n such that $a^n = 0$. A nilpotent elements $a \neq 0$ is a divisor of zero.

In the ring $M_2(R)$, there is an element $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ which is nilpotent, since $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

Theorem 13.1 A ring R has no zero divisors if and only if it satisfies the cancellation laws for multiplication in R *i.e.* for $a, b \in R$, $ab = ac$ and $ba = ca$, where $a \neq 0$, imply $b = c$.

Proof. Suppose R has no zero divisors. Let $ab = ac$, $a \neq 0$. Then $a(b - c) = 0 \Rightarrow b - c = 0$ $\Rightarrow b = c$.

Thus $ab = ac \Rightarrow b = c$. Similarly, $ba = ca \Rightarrow b = c$.

Conversely, let R satisfy the cancellation laws for multiplication.

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

Similarly, $ab = 0$, $b \neq 0 \Rightarrow a = 0$. Consequently, R has no zero divisors.

Example 6. If any elements a has the multiplicative inverse, then a cannot be a divisor of zero, where the underlying set is a ring.

Solution. Let R be a ring and $a \in R$ such that a has inverse $a^{-1} \in R$, so that $a \neq 0$.

To prove that a is not divisor of zero, suppose that a is a divisor of zero so that there exists another elements $b \in R$ such that $b \neq 0$ and $ab = 0$.

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

This is a contradiction to the fact that $b \neq 0$.

Hence the required result follows.

Integral Domain

A ring containing at least two elements is called an Integral domain if it

(*i*) is commutative (*ii*) has unit element and (*iii*) is without zero divisors.

Thus, in an integral domain a product is 0 only when one of the factors is 0; that is $ab = 0$ only, when $a = 0$ or $b = 0$.

For example,

(*i*) The ring of integers $(Z, +, \cdot)$ is an integral domain since it is commutative ring with unity and for any two integers a, b, $ab = 0 \Rightarrow a = 0$ or $b = 0$.

(*ii*) The ring of real numbers $(R, +, \cdot)$ is an integral domain.

(*iii*) The ring of even integers $(2Z, +, \cdot)$ is not an integral domain since it does not contain the unit element, although it is without zero divisors.

(*iv*) The ring $M_2(Z)$ is not an integral domain since it is not commutative. Also $M_2(Z)$ has zero divisors.

For example, $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in M_2(Z)$ and $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ which is a zero element of the ring $M_2(Z)$.

Theorem 13.2. A commutative ring R with unity is an integral domain, if and only if, for a non-zero element $a \in R$,

$$a \cdot b = a \cdot c \Rightarrow b = c \; ; b, c \in R.$$

Proof. Let, $c = 0$, then, from the given condition,

$$a \cdot b = a \cdot 0 \Rightarrow b = 0$$

or

$$a \cdot b = 0 \quad \Rightarrow b = 0.$$

Thus, a is not a left divisor of zero. R being a commutative ring a is not a right divisor of zero too. Thus R has no divisor of zero.

Hence R is an integral domain.

Conversely let R be an integral domain and $a (\neq 0) \in R$. Since R contain no divisor of zero, a is not a divisor of zero.

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

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

Hence $b = c.$

Field

A ring containing at least two elements *i.e.* non trivial is called a field if it

(*i*) is commutative (*ii*) has unity and (*iii*) is such that every non-zero element has multiplicative inverse in R.

That is to say, a system $(R, +, \cdot)$ is a field if

(*i*) $(R, +)$ is an abelian group,

(*ii*) $(R', \cdot)$ is a commutative group, where $R' = R - \{0\}$

(*iii*) The distributive laws *i.e.*, $a(b + c) = ab + ac$

$$(b + c)\, a = ba + ca \quad \text{hold for all } a, b, c \in R.$$

For example,

(*i*) The ring of rational numbers $(Q, +, \cdot)$ is a field since it is commutative ring with unity and each non-zero element has mltiplicative inverse.

(*ii*) The set R of all real numbers is a field.

(*iii*) The set C of all complex numbers is a field.

(*iv*) The ring $(\{0, 1, 2, 3, 4\}, +_5, \times_5)$ is a finite field.

An Important property of a field F is that if $x, y \in F$, then

$x + y \in F, x - y \in F, xy \in F, x \div y \in F$, *i.e.*, $xy^{-1} \in F$.

Hence a field is closed with respect to the four arithmetical operations namely, addition, subtraction, multiplication and division.

Theorem 13.3. Every field is an integral domain.

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

Let a, b be elements of F with $a \neq 0$ such that $ab = 0$

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

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

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

Since $b \neq 0$, b^{-1} exist we have

$$ab = 0 \Rightarrow (ab)\, b^{-1} = 0\, b^{-1}$$
$$\Rightarrow a(bb^{-1}) = 0 \Rightarrow a1 = 0 \Rightarrow a = 0.$$

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

But the convese is not true *i.e.*, every intgral domain is not a field. For example, the ring of integers is an integral domain but it is not a field. The only invertible elements of the ring of integers are 1 and –1.

Note. For a field unity and zero are distinct elements *i.e.*, $1 \neq 0$. Let a be any non-zero element of field. Then a^{-1} exists and also non-zero. For $a^{-1} = 0 \Rightarrow aa^{-1} = a0 \Rightarrow 1 = 0 \Rightarrow a1 = a0 \Rightarrow a = 0$, which is a contradiction. Now a field has no zero divisors. Therefore, $1 = a^{-1}\, a \neq 0$.

Since a field has no zero divisors, the product of two non-zero elements will again be a non-zero elements. Also the unit element $1 \neq 0$ and each non-zero multiplication is commutative as well as associative. Therefore, the non-zero elements of a field form an abelian group with respect to multiplication.

Theorem 12.4. Every finite integral domain is a field.

Proof. Let D be a finite integral domain. we shall first show that D has a unit element.

Let $D = \{a_1, a_2, \ldots\ldots a_n\}$ be the distinct elements of D and let $a \in D$ be any non-zero element. Then the elements $aa_1 \ldots\ldots aa_n$ all belong to D and are all distinct, because if $aa_i = aa_j$, then $a(a_i - a_j) = aa_i - aa_j = 0$ and since D is an integral domain, and $a \neq 0$, we have $a_i - a_j = 0$ *i.e.*, $a_i = a_j$. Hence the sets $\{aa_1, aa_2, \ldots\ldots, aa_n\}$ coincide with D. In particualr $aa_k = a$ for some k. We shall show that a_k is the unit element of D. Let a_j be any element of D. Then $a_j = aa_i$ for some i.

Now

$$a_j a_k = a_k a_j = a_k(aa_i) = (a_k a)\, a_i = (aa_k)\, a_i = aa_i = a_j$$

Thus a_k is the unit element of D. The unit element is unique and we shall denote it by 1.

Let $a \in D$, $a \neq 0$. Since $1 \in D$, $aa_i = a_i a = 1$, for some a_i.

Thus a has an inverse with respect to multiplication showing that D is a field.

Characteristic of a Ring

The characteristic of a ring R is the smallest positive integer n if it exists such that $na = 0$ for all $a \in R$. The characteristic of the ring of integers with addition and multiplication modulo n is n. If no such integer exists, the characteristic of R is said to be zero. The characteristic of the ring $(Z, +, .)$ is zero.

Theorem 13.5. If R be a ring with unit element e, then R is of characteristic n iff $ne = 0$ and n is the smallest positive integer.

Proof. (*i*) Suppose n is the smallest positive integer such that $ne = 0$. Then for any $a \in R$,

$$\begin{aligned} na &= a + a + \ldots\ldots a, (n \text{ times}) \\ &= ae + ae + \ldots\ldots ae, (n \text{ times}) \\ &= a(e + e + \ldots e), (n \text{ times}) \\ &= a(ne) = a0 = 0 \end{aligned}$$

Also for $0 < m < n$, $me \neq 0$. Hence the characteristic of R is n.

(*ii*) Suppose no such n exists, then the characteristic of R = 0 for otherwise, there exists some $m > 0$, with $ma = 0$ for all $a \in R$. In particlar $me = 0$, $m > 0$, which is impossible.

Theorem 13.6. The characteristic of an integral domain is either zero or a prime number.

Proof. Suppose the characteristic of $R = n \neq 0$ and n is not prime. Then $n = m_1 m_2$ where m_1 and m_2 are proper divisor of n. For any $a \in R$, $a \neq 0$, we have

$$0 = na^2 = (m_1 m_2) a^2 = (m_1 a)(m_2 a)$$

Since R is an integral domain, $m_1 a = 0$ or $m_2 a = 0$

Suppose $m_1 a = 0$. Then we shall show that $m_1 x = 0$ for all $x \in R$.

Now $m_1 (xa) = (m_1 x) a = x (m_1 a) = x 0 = 0$.

Since $a \neq 0$ and R is an integral domain, then $m_1 x = 0$ for all x, $m_1 < n$.

This contradicts the assumption that the characteristic is n. Hence n is a prime.

Division Ring or Skew Field

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

Thus a commutative division ring is a field. Every field is also a division ring. But a division ring is a field if it is also commutative. That is to say, a system (R, +, .) is a division ring if

(*i*) (R, +) is an abelian group,

(*ii*) (R′, .) is a group, where R′ is the set of non-zero elements of R.

(*iii*) The distributive laws hold.

Theorem 13.7. A skew field contains no divisor of zero.

Proof. Let S be a skew field and $a, b \in S$ be such that

$$a.b = 0 \text{ and } a \neq 0.$$

Now each non-zero element of S is a unity, so a^{-1} exists in S.

Therefore, $a^{-1} . (a.b) = a^{-1} . 0 = 0$

or, $(a^{-1} . a) . b = 0$

or, $1 . b = 0$, that is, $b = 0$.

Thus a is not a left divisor of zero.

Similarly it can be shown that a is not a right divisor of zero.

Theorem 13.8. The non-zero elements of a division ring from a group under multiplication.

Proof. If S * be the set of non-zero elements of the skew field S and the non-zero elements $a, b \in S$, then since S contains no divisors of zero, we have $a.b \neq 0$.

Therefore $a, b \in S^*$ is closed with respect to multiplication. S* being a sub-set, multiplication is associative in S*.

Now, each non-zero element of S is a unity; hence each element of S* has a multiplicative inverse.

Thus $\{S^*, .\}$ is a group.

The following observations are to be noted

1. Every field is an integral domain but converse is not true.
2. Every field is a division ring but converse is not true.
3. A field can be defined as a commutative division ring.

Example 7. Show that $S = \{a + b\sqrt{2} : a, b \in Z\}$ for the operations $+, \times$ is an integral domain but not a field.

Solution. Let $x, y, z \in S$, then there exists $a, b, c, d, , f \in Z$ where $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$, $z = e + f\sqrt{2}$. Since the sum, difference and product of two integers are integers

$$x + y = (a + c) + (b + d)\sqrt{2} \in S$$

$xy = (ac + 2bd) + (ad + bc)\sqrt{2} \in S$ as $a + c, b + d, ac + 2bd, ad + bc \in Z$

Thus S is closed with respect to addition and multiplication.

(*i*) Now (S, +) is an abelian group since it satisfies the following properties

1. Closure axiom. $x + y \in S$ already shown above.

2. Commutative law. $x + y = y + x$

This follows from the fact that

$$(a + c) + (b + d)\sqrt{2} = (c + a) + (d + b)\sqrt{2}$$

3. Associative law. $(x + y) + z = x + (y + z)$

For $[(a + c) + e] + [(b + d) + f]\sqrt{2} = [a + (c + e)] ([(b + d) + f])\sqrt{2}$

4. Existence of additive identity. $(a + b\sqrt{2}) + (0 + 0\sqrt{2}) = (0 + 0\sqrt{2}) + (a + b\sqrt{2})$

$= a + b\sqrt{2}$ so that $(0 + 0\sqrt{2})$ is the additive identity which belongs to S.

5. Existence of additive inverse. $(a + b\sqrt{2}) + (-a - b\sqrt{2}) = (-a - b\sqrt{2}) + (a + b\sqrt{2}) = 0 + 0\sqrt{2}$. So that additive inverse exists for each element of S.

(*ii*) Again (S, ×) is a semigroup since it satisfies the following properties

1. Closure axiom. $xy \in S$, already shown above

2. Associative law. $(xy)z = x(yz)$

For x, y, z are real numbers and real numbers obey associative law for multiplication

3. Distributive law. $x(y + z) = xy + xz$

and $(y + z)x = yx + zx$

Again x, y, z are real numbers and in the set of real numbers multiplication is distributive respect to addition.

4. Existence of multiplicative identity: $(1 + 0\sqrt{2})(a + b\sqrt{2}) = a + b\sqrt{2} = (a + b\sqrt{2})(1 + 0\sqrt{2})$

5. S has no divisors of zero, *i.e.*,

$$xy = 0, x = 0, y = 0$$

For $xy = 0 \Rightarrow (a + b\sqrt{2})(c + d\sqrt{2}) = 0 + 0\sqrt{2}$

$$(ac + 2bd) + (ad + bc)\sqrt{2} = 0 + 0\sqrt{2}$$

$$ac + 2bd = 0, ad + bc = 0$$

$$a, b \neq 0, \text{ and } c, d \neq 0$$

$$x = a + b\sqrt{2} \neq 0, y = c + d\sqrt{2} \neq 0$$

Hence $(S, +, .)$ is an integral domain.

To prove $(S, +, .)$ is not a field, we have to show that x^{-1} for every $x \in S, x \neq 0$

Now $x = a + b\sqrt{2}$, $x^{-1} = \dfrac{1}{a + b\sqrt{2}} = \dfrac{a - b\sqrt{2}}{a^2 - 2b^2} = \dfrac{a}{a^2 - 2b^2} + \left(\dfrac{-b}{a^2 - 2b^2}\right)\sqrt{2} \notin S$

since $\dfrac{a}{a^2 - 2b^2}$ and $\dfrac{-b}{a^2 - 2b^2}$ are not necessarily integers.

$\therefore x^{-1} \notin S$, for every $x \in S$.

Hence $(S, +, .)$ is not a field.

13.3. Subring

Let $(R, +, .)$ be a ring and A be nonempty subset of R. If $(A, +, .)$ is itself a ring under the same compositions of addition and multiplication as in R, then $(A, +, .)$ is said to be a subring of $(R, +, .)$. Thus $(A, +, .)$ is a subring of $(R, +, .)$ if and only if

(*i*) $A \neq \phi$

(*ii*) $(A, +)$ is a subgroup of $(R, +)$

(*iii*) A is closed under multiplication *i. e.*, $a . b \in A$ for every $a, b \in A$.

Two subrings $(\{0\}, +, .)$ and $(R, +, .)$ of the ring $(R, +, .)$ are called **improper** or **trivial** subring of R. Any subrings other than these two subrings is called a **proper** or **nontrivial** subring.

For example,

(*i*) The ring of integers is a subring of the ring of rational numbers which in turn is a subring of the ring of real numbers.

(*ii*) The ring of even integers is a subring of the ring of integers.

(*iii*) Consider $S = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}, x \in R$

Then $(S, +, .)$ is a subring of $(M_2(R), +, .)$ of all 2×2 real matrices. Clearly $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is the identity of S but this identity is not the same as the identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ of $M_2(R)$.

Note: In a ring R with identity, the identity of a subring (if it exists) may not be the same as the identity of R.

Theorem 13.9. The intersection of two subrings of a ring R is a subring of R.

Proof. Let $(S, +, .)$ and $(T, +, .)$ be two subrings of the ring R. Since $(S, +)$ and $(T, +)$ are subgroups of $(R, +)$, both S and T contain the zero of the ring R (or group $(R, +)$). Hence $S \cap T \neq \Phi$. Since the intersection of two subgroups of a group is a group, therefore, $(S \cap T, +)$ is a subgroup of $(R, +)$. Again

$$a, b \in S \cap T \Rightarrow a, b \in S, \text{ and } a, b \in T,$$

$$\Rightarrow ab \in S \text{ and } ab \in T, \text{ as S and T are subrings.}$$

$$\Rightarrow ab \in S \cap T.$$

Hence $S \cap T$ is a subring of R.

Note : (*i*) Intersection of any number of subrings of a ring R is again a subring of R.

(*ii*) Union of two subrings may not be a subring. For example, Consider the ring $(Z, +, .)$ of all integers and the subrings $(2Z, +, .)$ and $(3Z, +, .)$. Here $2Z \cup 3Z$ is not a subring as $4 \in 2Z$, $-3 \in 3Z$ but $4 + (-3) = 1 \notin 2Z \cup 3Z$.

Theorem 13.10. Let $(R, +, .)$ be a ring, then a non-empty subset S of R forms a subring of R if and only if

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

(*ii*) $a, b \in S \Rightarrow a . b \in S$.

Proof. Let S be a subring of R

Now, $a, b \in S \Rightarrow a, -b \in S$, since S is a ring

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

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

Also, $a, b \in S \Rightarrow a . b \in S$, since S is a ring.

Hence both the conditions are satisfied.

Conversely, let a non-empty subset S or R be such that (*i*) $a, b \in S \Rightarrow a - b \in S$ and (*ii*) $a, b \in S \Rightarrow a . b \in S$.

Now, $a \in S, a \in S \Rightarrow a - a \in S$ by (i)

$\Rightarrow$ $0 \in S$ (Existence of identity in S)

$0 \in S, a \in S \Rightarrow 0 - a \in S$ by (i)

$\Rightarrow$ $-a \in S$ (Existence of inverse in S)

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

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

$\Rightarrow$ $a + b \in S$ (S is closed under addition)

Since addition is associative and commutative on R and S is a subset of R, so addition is associative and commutative on S also.

Therefore $(S, +)$ is a commutative group and hence $(S, +)$ is a subgroup of $(R, +)$.

Also, by (*ii*) S is closed under multiplication. Therefore S is a subring of R,

Example 8. Show that the set of matrices $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ is a subring of the ring of 2×2 matrices.

Solution. Let S be the set of all 2×2 matrices of the form $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$.

Now, for any $A = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} \in S, B = \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix} \in S$

$\Rightarrow$ $A - B = \begin{bmatrix} a_1 - a_2 & 0 \\ b_1 - b_2 & 0 \end{bmatrix} \in S$ and $AB = \begin{bmatrix} a_1 a_2 & 0 \\ b_1 a_2 & 0 \end{bmatrix} \in S$.

Hence by Theorem 13.10 the set S of matrices $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ is a subring of the ring of 2×2 matrices.

Ideal

Let A be a nonempty subset of a ring R such that A is an additive subgroup of R *i.e.*, $a - b \in$ A whenever $a, b \in$ A. Then

(*i*) A is a left ideal of R iff $ra \in$ A for each $a \in$ A and $r \in$ R;

(*ii*) A is a right ideal of R iff it is $ar \in$ A for each $a \in$ A and $r \in$ R;

(*iii*) A is an ideal of R iff it is both a left ideal of R and a right ideal of R.

Clearly, if the ring is commutative, the concepts of left, right and both sided ideals

Example 9

(*i*) The subring of even integers is an ideal of ring of integers.

(*ii*) The set $\{nx : x \in Z\}$ is an ideal of the ring of integers, n being any fixed integer.

(*iii*) Let R be a ring. Consider the matrix ring $M_2(R)$, then in $M_2(R)$

(*a*) The subring $A = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in R\right\}$ is a right ideal but not a left ideal of M. That A is a right ideal can be checked. Let $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in A$ and $\begin{pmatrix} x & y \\ c & d \end{pmatrix} \in M_2(R)$

Then $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ c & d \end{pmatrix} = \begin{pmatrix} ax+bc & ay+bd \\ 0 & 0 \end{pmatrix} \in A$

But A is not a left ideal, for $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in A, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in M_2(R)$, then $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \notin A$

(*b*) The subring $B = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in R\right\}$ is a left ideal but not a right ideal.

Let $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in B$ and $\begin{pmatrix} x & y \\ c & d \end{pmatrix} \in M_2(R)$

Then $\begin{pmatrix} x & y \\ c & d \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ax+by & 0 \\ ac+bd & 0 \end{pmatrix} \in B$

But $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in B$ and $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(R)$, then $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \notin B$

(*c*) The subring $C = \left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in R\right\}$ is neither a left ideal nor a right ideal.

Note. An ideal S of a ring R is a subring of R but every subring of R is not an ideal. For examples (*i*) The set S of integers is a subring of the ring of rational numbers but S is not an ideal of R. For product of a rational and integer is not always an integer as

$$2 \in S, 1/6 \in R \Rightarrow 2 \times 1/6 = 1/3 \notin S.$$

(*ii*) The set S of rational numbers is a subring of the ring R of real numbers, but S is not an ideal of R. For product of a rational numbers and a real numbers is not always a rational number. For example,

$$2 \in S, 1/\sqrt{3} \in R \Rightarrow 2 \times 1/\sqrt{3} = 2/\sqrt{3} \notin S$$

Quotient Ring

Let (R, +) be a ring and I be an ideal of R. A ring R is an additive abelian group and hence (I, +) is a subgroup of the abelian group (R, +). Again every subgroup of an abelian group is normal. So I is a normal subgroup of R and hence the quotient group (R/I, +) is defined under normal addition of cosets *i.e.*, $(a + I) + (b + I) = a + b + I$ for all $a, b \in R$. In this group, the identity is the zero coset I and the inverse of $a + I$ is $-a + I$ for all $a \in R$.

Given an ideal I of a ring (R, +, .), the normal addition and multiplication of cosets, namely, $(a + I) + (b + I) = a + b + I$ and $(a + I)(b + I) = ab + I$ for all $a, b \in R$, make (R/I, +, .) a ring.

Given an ideal I of a ring R, the ring R/I is called the **quotient ring** or **factor ring of R** or **residue class** ring of R modulo I. If R is a commutative ring with identity, then R/I is also so.

13.4. Ring Homomorphism

A mapping of a ring R to a ring S is called a ring homomorphism or simply a homomorphism if it satisfies the following properties:

For all $a, b \in R$,

(*i*) $f(a + b) = f(a) + f(b)$.

(*ii*) $f(ab) = f(a) f(b)$.

the definition shows that a ring homomorphism is a group homomorphism of the additive group (R, +) and it preserves the products.

A homomorphism $f: R \to S$ is called an **epimorphism** if f is onto. It is called a **monomorphism** if it is 1 – 1 and **isomorphism** if it is both 1 – 1 and onto. A homomorphism f of a ring R into itself is called an **endomorphism.** An endomorphism is called an **automorphism** if it is an isomorphism.

Example 10. (*i*). The most trivial examples are the identity homomorphisms. Let R be a ring and let $I : R \to S$ be the identity function. Then I is a ring homomorphism which is 1 – 1 and onto and hence is an isomorphism.

(*ii*) Let S be a subring of R. Define $f: R \to S$ by $f(x) = x$ for all $x \in S$. then clearly for any $x, y \in S, f(x + y) = x + y = f(x) + f(y)$ and $f(xy) = xy = f(x) f(y)$. Thus f is a ring homomorphism from S to R. It is called an **inclusion map**.

Kernel of a Ring Homomorphism

If f is a homomorphism of a ring R into a ring R′, then the set S of all those elements of R which are mapped onto the zero element of R′ is called the kernel of the homomorphism f.

Thus if f is homomorphism of R into R′, then S is the kernel of f if $S = \{x \in R : f(x) = o'$ where o' is the zero element of R′$\}$.

Theorem 13.11. If f is a homomorphism of R into R′ with kernel S, then S is an ideal of R.

Proof. Let f be a homomorphism of a ring R into a ring R′. Let o, o' be the zero elements of R, R′ respectively. Let S be the kernel of f. Then $S = \{x \in R : f(x) = o'\}$.

Since $f(0) = o'$, therefore, at least $o \in S$. Thus $S \neq \Phi$. Let $a, b \in S$. Then $f(a) = o', f(b) = o'$. Again $f(a - b) = f[a + (-b)] = f(a) + f(-b) = f(a) - f(b) = o' - o' = o'$. Therefore, $a - b \in S$.

Also if r be any element of R, then $f(ar) = f(a) f(r) = o' f(r) = o'$ and $f(ra) = f(r) f(a) = f(r)\, o' = o'$. So $ar \in S$ and $ra \in S$.

Thus $a, b \in S, r \in R \Rightarrow (a - b) \in S, ar \in S, ra \in S$. Hence S is an ideal of R.

Properties of Ring Homomorphism

Let f be a homomorphism from a ring R to a ring S. Let A be a subring and B an ideal of S.

1. For any $r \in R$ and any positive integer $n, f(nr) = n f(r)$ and $f(r^n) = (f(r))^n$
2. $f(A) = \{f(a) : a \in A\}$ is a subring of S.
3. If A is an ideal and f is onto S, then $f(A)$ is an ideal.
4. If R is commutative, then $f(R)$ is commutative.
5. If R has a unity 1, $S \neq \{0\}$, and f is onto, then $f(1)$ is the unity of S.
6. f is an isomorphism if and only if f is onto and Ker $f = \{r \in R : f(r) = o\} = \{0\}$
7. If f is an isomorphism from R onto S, then f^{-1} is an isomorphism from S onto R.

Polynomial Ring

An expression of the form

$$a_0 + a_1 x + a_2 x^2 + \ldots\ldots\ldots\ldots a_n x^n + \ldots\ldots\ldots$$

is called a polynomial. It is completely determined by the sequence of coefficients

$$a_0, a_1, a_2, \ldots\ldots\ldots\ldots, a_n, \ldots\ldots\ldots$$

Let R be a ring. A polynomial over R is defined by an expression of the form

$$f(x) = \Sigma a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots\ldots\ldots\ldots$$

where $a_i \in R$ and $a_i = 0$ for all but a finite number of values of i. The a_i are co-efficients of $f(x)$. If for some $i > 0$ it is true that $a_i \neq 0$, the largest such value of i is the degree of $f(x)$. If no such $i > 0$ exists, then $f(x)$ is of degree zero. Here x is an indeterminate. A polynomial consisting of only a single term a_0 of the ring R is known as a constant polynomial.

The set of all polynomials $f(x)$ is denoted by R $[x]$.

Addition and Multiplication in R [x]

Let R be a commutative ring and let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots + a_1 x + a_0$$

and

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots\ldots + b_1 x + b_0 \quad \text{belong to } R[x].$$

Then

$$f(x) + g(x) = (a_s + b_s) x^s + (a_{s-1} + b_{s-1}) x^{s-1} + \ldots\ldots + (a_1 + b_1) x + a_0 + b_0$$

where s is the maximum of m and n, $a_i = 0$ for $i > n$, and $b_i = 0$ for $i > m$. Also,

$$f(x)\, g(x) = c_{m+n} x^{m+n} + c_{m+n-1} x^{m+n-1} + \ldots\ldots + c_1 x + c_0$$

where

$$c_k = a_k b_0 + a_{k-1} b_1 + \ldots\ldots + a_1 b_{k-1} + a_0 b_k$$

for

$$k = 0, \ldots\ldots, m + n.$$

It can be shown that the set R $[x]$ of all polynomials in an indeterminate x with coefficients in a ring R is a ring under polynomial addition and multiplication. If R is commutative, then so is R $[x]$ and if R has unity 1, then 1 is also unity of R $[x]$.

SOLVED EXAMPLES

Example 11. *For the set $I_4 = \{0, 1, 2, 3\}$, show that the modulo 4 system is a field.*

Solution. The composition table for addition and multiplication modulo 4 is given below.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

From the above tables we observe the following :

1. **Closure axiom.** All the entries in both the tables belong to I_4. Hence I_4 is closed with respect to both operations.

2. **Commutative law.** The entries of 1st, 2nd, 3rd, 4th rows are identical with the corresponding elements of the 1st, 2nd, 3rd, 4th columns respectively in both the tables. Hence I_4 is commutative with respect to both operations.

3. **Associative law.** The associative law for addition and multiplication

$$a +_4 (b +_4 c) = (a +_4 b) +_4 c \text{ for all } a, b, c \in I_4$$

$$a \times_4 (b \times_4 c) = (a \times_4 b) \times_4 c \text{ for all } a, b, c \in I_4$$

can easily be verified. For example $2 +_4 (1 +_4 3) = 2 +_4 0 = 2$ and $(2 +_4 1) +_4 3 = 3 +_4 3 = 2$.

4. **Existence of Identity.** 0 is the additive identity and 1 is the multiplicative identity for I_4. For $0 +_4 a = a$ for all $a \in I_4$ and $1 \times_4 a = a$ for all $a \in I_4$, $a \neq 0$

5. **Existence of inverse.** The additive inverses of 0, 1, 2, 3 are 0, 3, 2, 1 respectively. The multiplicative inverses of non-zero elements 1, 2, 3 are 1, 2, 3 respectively.

6. Distributive law. Multiplication is distributive over addition, *i.e.*,

$$a \times_4 (b +_4 c) = a \times_4 b + a \times_4 c$$

For $(b +_4 c) \times_4 a = b \times_4 a +_4 c \times_4 a.$

$a \times_4 (b +_4 c) = a \times_4 (b + c)$. For $b +_4 c = b + c \pmod 4$

= least positive remainder when $a \times (b + c)$ is divided by 4.

For = least positive remainder when $ab + ac$ is divided by 4.

$= ab +_4 ac = a \times_4 b +_4 a \times_4 c$

Similarly we can prove the other distributive law. $a \times_4 b \equiv a \times b \pmod 4$

Thus $(I_4, +_4, \times_4)$ is a field.

Example 12. Show that the set S of all matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, where $a, b \in R$ is a field with respect to matrix addition and matrix multiplication.

Solution. Let $M(a, b) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$

1. **Closer axiom:** Here $M(a, b) + M(c, d) = M(a + c, b + d)$ and $M(a, b)\, M(c, d) = M(ac - bd, ad + bc)$. Thus S is closed for addition and multiplication.
2. **Commutative law:** $M(a, b), M(c, d) \in S$

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

for all $M(a, b)$ and $M(c, d) \in S$ which can easily be verified.

3. **Associative law:** Addition and multiplication for matrices over R being associative, addition and multiplication in S is associative.
4. **Existence of Identity:** $M(0, 0)$ is the additive of $M(a, b)$ and $M(1, 0)$ is the multiplicative identity as

$$M(a, b) + M(0, 0) = M(0, 0) + M(a, b) = M(a, b)$$
$$M(a, b)\, M(1, 0) = M(a, b) = M(1, 0)\, M(a, b)$$

for all $M(a, b) \in S$.

5. **Existence of Additive Inverse:** $M(-a, -b)$ is additive inverse of $M(a, b)$, since $M(a, b) + M(-a, -b) = M(0, 0)$.
6. **Existence of Multiplicative Invers:** If $a^2 + b^2 \neq 0$, then the matrix

$$M\left(\frac{a}{a^2+b^2}, \frac{b}{a^2+b^2}\right)$$

is the multiplicative inverse, of $M(a, b)$. For, putting

$$c = \frac{a}{a^2+b^2}, d = -\frac{b}{a^2+b^2}$$

in above, we have

$$M(a, b)\, M\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right) = M(1, 0),$$

and also

$$M\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right) M(a, b) = M(1, 0).$$

7. **Distributive law:** Since matrix multiplication distributes itself over matrix addition for matrices over R, it is true for all matrices in S.

Hence S is a field.

Example 13. Find the characteristic in the ring $(I_6, +_6, \cdot_6)$ where $I_6 = \{0, 1, 2, 3, 4, 5\}$.

Solution. The ring of integers modulo 6 has characteristic 6 since $6x = 0$ for every x in the ring. Obviously no integer smaller than 6 satisfies this property. For instance, 5 can not be the characteristic, since $5(3) = 3$ in I_6 and $3 \neq 0$.

Example 14. In an integral domain D, show that if $ab = ac$ with $a \neq 0$ then $b = c$.

Solution: Since $ab = ac$ we have

$$ab - ac = 0 \text{ and so } a(b - c) = 0$$

Since $a \neq 0$, we must have $b - c = 0$, since D has no zero divisors. Hence $b = c$.

Example 15. Let $R_1 = \left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in R\right\}$ where R is a ring.

Define $f : R_1 \to R$ by $f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a$ for all $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in R_1$. Show that f is isomorphism.

Solution: Here $f\left(\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}\right) = f\begin{pmatrix} a+b & 0 \\ 0 & 0 \end{pmatrix} = a + b = f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + f\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$

Also $f\left(\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}\right) = f\begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} = ab = f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} f\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$

Again $f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = f\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow a = b \Rightarrow \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$

So f is one-one. Clearly f is onto.

Hence f is an isomorphism.

Example 16. Let R be a Boolean ring (i.e., all its elements are idempotent, $a^2 = a$ for all $a \in R$). Then the characteristic of R is 2 and R is commutative.

Solution. Let $a \in R$. Now, $a + a = (a + a)^2 = (a + a)(a + a) = a(a + a) + a(a + a) = a^2 + a^2 + a^2 + a^2 = a + a + a + a$. This implies that $2a = 4a$ and so $0 = 2a$. Hence, $2.1 = 0$ since a was arbitrary. Hence the characteristic of R is 2.

To show that R is commutative, let $a, b \in R$.

Then $a + b = (a + b)^2 = (a + b)(a + b) = a^2 + ab + ba + b^2 = a + ab + ba + b$. This implies that $0 = abb + ba$.

Hence $ab = ab + 0 = ab + ab + ba$

or $ab = 2ab + ba = ba$ since $2ab = 0$.

Thus, R is commutative.

13.8. More about Ideals

Every ring R always posses two ideals; one R itself and the other consisting of 0 only. They are called **improper ideals** of R. These are respectively known as the unit ideal and the null ideal. Any ideal other than these two ideals is called **proper ideals.** A ring having no proper ideals is called a simple ring.

Theorem 13.12. *Prove that the intersection of two ideals of R is an ideal of R.*

Solution. Let S and T be two ideals of R. Then S and T are subgroups of R under addition. Therefore, $S \cap T$ is also a subgroup of R under addition.

Now, to show that $S \cap T$ is an ideal of R, we have to show that

$$r \in R, s \in S \cap T \Rightarrow rs \in S \cap T, sr \in S \cap T.$$

Now, $$s \in S \cap T \Rightarrow s \in S, s \in T.$$

But S and T are ideals of R. Therefore,

$$r \in R, s \in S \Rightarrow rs \in S, sr \in S$$

and $$r \in R, s \in S \Rightarrow rs \in T, sr \in T.$$

Now, $$rs \in S, rs \in T \Rightarrow rs \in S \cap T$$

and $$sr \in S, sr \in T \Rightarrow sr \in S \cap T$$

$\therefore$ $S \cap T$ is also an ideal of R.

Theorem 13.13. *A field has no proper ideals, i.e. if F is a field then its only ideals are (0) and F itself.*

Proof. Let S be any arbitrary ideal of the field F. *If* $S = \{0\}$, then the theorem is proved. Let $S \neq \{0\}$ and let a be any non-zero element of S.

Now, $$a \in s, S \subset F \Rightarrow a \in F \Rightarrow a^{-1} \in F \text{ as } a \neq 0.$$

Since S is an ideal, therefore

$$a \in S, a^{-1} \in F = aa^{-1} \in S \Rightarrow 1 \in S.$$

Now, let x be any element of F. $1 \in S, x \in F \Rightarrow 1x \in S \Rightarrow x \in S$. Thus, each element of F belongs to S. Therefore, $F \subseteq S$. But $S \subseteq F$, hence $S = F$.

Thus, only ideals of F are (0) and F itself.

Theorem 13.14. *For two ideals A and B of a ring R, $A \cup B$ is an ideal of R if and only if either $A \subseteq B$ or $B \subseteq A$.*

Proof. If $A \subseteq B$ then $A \cup B = B$ is an ideal of R. Again $B \subseteq A \Rightarrow A \cup B = A$ is an ideal of R.

Conversely, Let $A \cup B$ be an ideal of R. Suppose that neither A is contained in B nor B is contained in A. Then there exist elements $x \in A - B$ any $y \in B - A$. Now, $x \in A, y \in B \Rightarrow x, y \in A \cup B$. As $A \cup B$ is an ideal, this in turn implies $x - y \in A \cup B$. So, either $x - y \in A$ or $x - y \in B$. In case $x - y \in A$. we get $y = x - (x - y) \in$ A. This contradicts the choice of y. Similarly, if $x - y \in B$ then $x = (x - y) + y \in B$ which is a contradiction. Hence our supposition is wrong. In other words, either $A \subseteq B$ or $B \subseteq A$.

Theorem 13.15. *If R is a commutative ring and $a \in R$, then*

$$Ra = \{ra : r \in R\} \text{ is an ideal of } R.$$

Proof. In order to prove that Ra is an ideal of R, we have to prove that Ra is a subgroup of R under addition and that if $u \in Ra$ and $x \in R$ then xu and ux are also in Ra. But R is commutative ring, therefore $xu = ux$. Thus, we only need to check that xu is in Ra.

Now, let $u, v \in Ra$. Then $u = r_1a$, $v = r_2a$ for some $r_1, r_2 \in$ R.

We have $u - v = r_1a - r_2a = (r_1 - r_2)a \in Ra$ since $r_1 - r_2 \in R$.

Thus $u, v \in Ra \Rightarrow u - v \in Ra$. Hence Ra is a subgroup of R under addition.

Now let $x \in R$.

Then $xu = x(r_1a) = (xr_1)\, v \in Ra$ since $xr_1 \in R$.

Hence, Ra is an ideal of R.

Theorem 13.16. *A commutative ring with unity is field if it has no proper ideals.*

Proof. Let R be a commutative ring with unity having no proper ideals i.e., the only ideals of R are (0) and R itself. In order to show that R is a field, we should show that each non-zero element of R possesses multiplicative inverse.

Let a be any non-zero element of R then the set $Ra = \{ra : r \in R\}$ is an ideal of R.

Since $1 \in R$, therefore $1a = a \in Ra$. Thus, $0 \neq a \in Ra$.

Therefore, the ideal $Ra \neq (0)$.

Since R has no proper ideals, therefore the only possibility is that Ra. Thus, every element of R is a multiple of a by some element of R. In particular, $1 \in R$ then there exists an element $b \in R$ such that $ba = 1$. But R is commutative, so $ab = ba = 1$. Therefore, $a^{-1} = b$, $b \in R \Rightarrow a^{-1} \in R$. Hence each non-zero element of R possesses multiplicative inverse.

Hence R is a field.

Principal Ideal

The intersection of all ideal containing an arbitrary subset M of a ring is called the ideal generated by M and written as (M).

It is evident that (M) is the smallest ideal containing all elements of the set M. In particular if M consists of single element, say a, of the ring R, then it denoted by (a) in place of (M).

An ideal such as (a) generated by a single element of the ring is called a **principal ideal**.

If every ideal in R is a principal ideal, then R is called a **principal ideal ring,** i.e. if every ideal S of R is of the form $S = (a)$ for some $a \in S$. An integral domain is called **Principal Ideal Domain** if its every ideal is a principal ideal.

Example 17. Find the principal ideal generated by in the ring of integers $(Z, +, .)$.

Solution. We know that Z is a commutative ring with unity so that (3) consists of all the elements of the form $3r$, $r \in Z$. Then the Principal ideal generated by 3 is

$(3) = \{..., -6, -3, 0, 3, 6, ...\}$

Example 18. Find all the principal ideals of the ring.

$[\{0, 1, 2, 3, 4, 5\}, +_6, \times_6]$.

Solution. Since it is commutative ring with unity, we have the following principal ideals.

(*i*) $(0) = \{0\}$

(*ii*) $(1) = \{0, 1, 2, 3, 4, 5\}$

(*iii*) $(2) = \{0, 2, 4, 2, 4\} = \{0, 2, 4\}$,

since $2 \times_6 0 = 0$, $2 \times_6 1 = 2$, $2 \times_6 2 = 4$

and $2 \times_6 3 = 0$, $2 \times_6 4 = 2$, $2 \times_6 5 = 4$

(*iv*) $(3) = \{0, 3, 0, 3, 0, 3\} = \{0, 3\}$

(*v*) $(4) = \{0, 4, 2, 0, 4, 2\} = \{0, 2, 4\}$

(*vi*) $(5) = \{0, 5, 4, 3, 2, 1\} = \{0, 1, 2, 3, 4, 5\}$

Since $(1) = (5)$ and $(2) = (4)$, the only principal ideal of this ring are the zero ideal, the unit ideal, the ideal $\{0, 3\}$ and the ideal $\{0, 2, 4\}$.

Theorem 13.17. The ring of integers is a principal ideal ring.

Proof. Let $(Z, +, .)$ be the ring of integers. Obviously, Z is a commutative ring with unity and without zero divisors. Therefore, Z will be a principal ideal ring if every ideal in Z is a principal ideal.

Let S be any ideal of the ring of integers. If S is the null ideal, then $S = (0)$ so that S is a principal ideal. Let $S \neq (0)$. Now, S contains at least one-zero integer, say a. Since S is a subgroup of R under addition, therefore $a \in S \Rightarrow -a \in S$.

This shows that S contains at least one positive integer because if $0 \neq a$, then one of a and $-a$ must be positive.

Let S_+ be the set of all positive integers in S. Since S_+ is not empty, therefore by the well ordering principal S_+ must possess a least positive integer. Let s be this least element. We will now show that $S = (s)$ is the principal ideal.

Suppose that n is any integer in S. Then by division algorithm, there exist integers q and r such that $n = qs + r$ with $0 \leq r < s$.

Now, $\quad s \in S, q \in Z \Rightarrow qs \in S$ as S is an ideal

and $\quad n \in S, qs \in S \Rightarrow n - qs \in S$ as S is a subgroup of the additive group of Z

$\Rightarrow \quad r \in S. \quad [n - qs = r]$

But $0 \leq r < s$ and s is the least positive integer such that $s \in S$. Hence r must be 0.

$\therefore \quad n = qs$.

Thus, $n \in S \Rightarrow n = qs$ for some $q \in Z$.

Hence S is a principal ideal of Z generated by s.

Since S was an arbitrary ideal in the ring of integers, therefore the ring of integers is a principal ideal ring.

Theorem 13.18. *Every field is a principal ideal domain.*

Proof. We know that a field has no proper ideals. The only ideals of a field are (*i*) the zero ideal $\{0\}$ which is a principal ideal generated by 0, and (*ii*) the field itself which is also a principal ideal generated by the unity element 1. Hence a field is always a principal ideal ring.

Maximal Ideal

An ideal $M \neq R$ in a ring R is said to be a maximal ideal of R if whenever U is an ideal of R such that $M \subseteq U \subseteq R$, then either $R = U$ or $M = U$. In other words, an ideal M of a ring R is said to be maximal ideal if there exists no ideal properly contained in R which itself properly contains M.

Example 19. Consider the ring of integers $(I, +, .)$. The ideal (5) of the ring is maximal, since the only ideal containing (5) is I. On the other hand, the ideal (6) is not maximal since it is a proper subset of the ideal (3) which in turn is a proper subset of the unit ideal $(1) = I$

Note that in a ring of integers, (0) is a prime ideal, but not a maximal ideal.

A field F has only two ideals f and (0). It is easy to see that (0) is the only maximal ideal of F.

Theorem 13.19 *An ideal S of the ring of integers $(I, +, .)$ is maximal if and only if S is generated by some prime integer.*

Proof. We know that every ideal of $(I, +, .)$ is a principal ideal. Suppose S is an ideal of I generated by p so that $S = (p)$. Since p and $-p$ generate the same ideal, we can take p as positive.

Then we first prove S is maximal if p is prime. Let p be a prime integer such that $(p) = S$.

Let T be any ideal of I such that

$$S \subset T \subset I.$$

Now, I being a principal ideal ring, T must be a principal ideal so that we may write $T = (q)$ where q is some positive integer.

Now, $\quad S \subset T$

$\Rightarrow \quad (p) \subset T$

$\Rightarrow \quad p \in T$

$\Rightarrow \quad p = nq$ for some positive integer n.

But $q = 1 \Rightarrow n = p$ or $q = p$, $n = 1$. [$\because p$ is prime]

And $q = 1 \Rightarrow I = (1) = I$

$q = p \Rightarrow I = (p) = S$

Thus, either $I = I$ or $I = S$.

Hence S is maximal ideal of Z.

Now, let $(p) = S$ be a maximal ideal. We will show that p is prime. If possible let p be a composite integer. Then

$$p = mn,\ m,\ n \neq 1$$

It is evident that

$$(p) \subset (m) \subset I$$

But since (p) is maximal, we have

Either $(m) = (p)$ or $(m) = I$

If $(m) = I$ then $m = 1$ which is a contradiction.

And if $(m) = (p)$, them $m \in (p)$, so that $m = pr$ for some integer r.

Also $p = m\,n = prn$ but $p \neq 0$, therefore, $r\,n = 1$

Again since, r, n are integers and $r\,n = 1$, we see that either $r = n = 1$ or $r = n = -1$, so that $n \neq 1$ which is again a contradiction. Hence p must be a prime integer.

Theorem 13.20. *Let R be a commutative ring with unity and M be an ideal of R. Then M is a maximal ideal if and only if R/M is a field.*

Proof. Let M be a maximal ideal in R. Then R being commutative with unity, R/M is also commutative with unity. The zero element and the unity element of the ring R/M are respectively M and $1 + M$ where 1 is the unity element of R. If $1 + M = 0 + M$, then $1 \in M$ which implies $M = R$, so M can not be a maximal ideal. Now, to prove that R/M is a field, we show that every non-zero element of R/M has a multiplicative inverse.

Let $x + M \in \dfrac{R}{M}$ be any non-zero element.

Then $x + M \neq M \Rightarrow x \notin M$

Let $$xR = \{xr \mid r \in R\}$$

It is easy to verify that xR is an ideal of R. Since sum of two ideals is an ideal, $M + xR$ will be an ideal of R.

Again as $x = 0 + x.1 \in M + xR$ and $x \notin M$, we find

$$M \subset M + xR \subseteq R$$

M, maximal $\Rightarrow$ $M + xR = R$

Thus, $1 \in R \Rightarrow 1 \in M + xR$

$\Rightarrow$ $1 = m + xr$ for some $m \in M$, $r \in R$

$\Rightarrow$ $1 + M = (m + xr) + M$

$= (m + M) + (xr + M) = xr + M$

$= (x + M)(r + M)$

$\Rightarrow$ $(r + M)$ is multiplicative inverse of $x + M$

Hence $\dfrac{R}{M}$ is a field.

Conversely, let $\frac{R}{M}$ be a field.

Let I be any ideal of R such that, $M \subset I \subseteq R$ then for some $a \in I$, such that, $a \notin M$

Now, $a \notin M \Rightarrow a + M \neq M \Rightarrow a + M$ is a non-zero element of $\frac{R}{M}$, which being a field, $a + M$ has multiplicative inverse. Let $b + M$ be its inverse. Then

$$(a + M)(b + M) = 1 + M$$
$$\Rightarrow \quad ab + M = 1 + M$$
$$\Rightarrow \quad ab - 1 \in M$$
$$\Rightarrow ab - 1 = m \text{ for some } m \in M$$
$$\Rightarrow 1 = ab - m \in I \text{ (using def. of ideal)}$$
$$\Rightarrow I = R \text{ (ideal containing unity, equals the ring)}$$

Hence M is maximal ideal of R.

Note : $\frac{R}{M}$ being a field contains at least two elements and thus unity and zero elements of $\frac{R}{M}$ are different i.e., $0 + M \neq 1 + M$ i.e., $1 \in M$ or that $M \neq R$.

Example 20. In the ring $Z[i]$, show that $I = \{a + bi \in Z[i] \mid a, b \text{ are both even}\}$ is an ideal of $Z[i]$, but not a maximal ideal of $Z[i]$.

Solution. Let $x = a + bi, y = c + di \in I$ and $u = r + si \in Z[i]$. There exist $r_1, r_2, r_3, r_4 \in Z$ such that $a = 2r_1$, $b = 2r_2$, $c = 2r_3$, $d = 2r_4$. Then $x - y = (a + bi) - (c + di) = (a - c) + (b - d)I = 2(r_1 - r_3) + 2(r_2 - r_4)\, i \in I$, and $ux = (r + si)(a + bi) = (ra - sb) + (rb + sa)i = 2(rr_1 - sr_2) + (2(rr_2 + sr_1)i \in I$. Since $Z[i]$ is a commutative ring, it follows that I is an ideal of $Z[i]$.

Let $J = \{a + bi \in Z[i] \mid 2 \text{ divides } a^2 + b^2\}$. Since $0 + 0i \in J$, $J \neq \phi$. Let $x = a + bi, y = c + di \in J$ and $u = r + si \in Z[i]$. Then $2 \mid a^2 + b^2$ and $2 \mid c^2 + d^2$.

Now, $x - y = (a - c) + (b - d)i$. Since $(a - c)^2 + (b - d)^2 = (a^2 + b^2) + (c^2 + d^2) - 2(ac + bd)$, it follows that $2 \mid (a - c)^2 + (b - d^2)$. Again, $ux = (r + si)(a + bi) = (ra - sb) + (rb + sa)i$ and $(ra - sb)^2 + (rb + sa)^2 = r^2(a^2 + b^2) + s^2(a^2 + b^2)$. Hence $2 \mid (ra - sb)^2 + (rb + sa)^2$ implies that $ux = ux \in J$. Consequently, J is an ideal. Now, $1 + 2i \in Z[i]$, but $1 + 2i \notin J$. Hence $J \neq Z[i]$. Again $1 + 1i \in J$ but $1 + 1i \notin I$, whence we find that $1 \subset J \subset Z[i]$. Consequently, I is not a maximal ideal.

Prime Ideal

An ideal $P \neq R$ of a ring R is called a prime ideal if $ab \in P \Rightarrow a \in P$ or $b \in P$.

Theorem 13.21. Let R be a commutative ring with identity. Then every maximal ideal of R is prime.

Proof. Let I be a maximal ideal of R. Then I is a proper ideal of R. Let $a, b \in R$ such that $ab \in I$. Further assume that $a \notin I$. Let $J = \{ra + x \mid r \in R \text{ and } x \in I\}$.

It can easily be shown that J is an ideal of R; $a = 1a + 0 \in J$ and if $x \in I$, then $x = 0a + x \in J$. Hence $I \subset J$. Since I is a maximal ideal, it follows that $J = R$. Now, $1 \in J$, so there exist $r \in R$ and $x \in I$ such that $1 = ra + x$. Then $b = r(ab) + xb$. Since $ab \in I$ and $x \in I$, we find that $r(ab) \in I$ and $xb \in I$. Hence $b \in I$. Therefore, I is a prime ideal of R.

One should note that the converse of the above theorem is not true as (0) is a prime ideal of Z which is not maximal.

SOLVED EXAMPLES

Example 21. Do the following sets form an integral domain under ordinary addition and multiplication? If so state whether they are fields:

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

(*ii*) the set of even integers.

(*iii*) the set of positive integers.

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

Observe that $2\sqrt{2}, 3\sqrt{2} \in S$, but $(2\sqrt{2})(3\sqrt{2}) = 12 \notin S$ because 12 cannot be put in the form $b\sqrt{2}$ where b is a rational number. Thus S is not closed under multiplication. Hence S is not a ring, *i.e.*, S is neither an integral domain nor a field.

(*ii*) Let E denotes the set of all even integers (including zero). Then it can be verified that the set E is a ring under addition and multiplication a binary operations. Also the multiplication is a commutative operation and hence E is a **commutative ring.** E is without zero divisors because the product of two non-zero even integers cannot be equal to zero which is the zero element of this ring. But the integer $1 \notin E$. So, E is a commutative ring without zero-divisors and without unity. Therefore $(E, +, .)$ is not an integral domain and hence it is not a field also.

(*iii*) Let N denotes the set of all positive integers. Now N does not contain the additive identity since $0 \notin N$. So N is not a ring. Hence $(N, +, .)$ is neither an integral domain nor a field.

Example 22. Let $(F, +, .)$ be a field and $a, b \in F$ with $b \neq 0$. Then show that $a = 1$ when $(ab)^2 = ab^2 + bab - b^2$.

Solution. We have $(ab)^2 = ab^2 + bab - b^2$

$\Rightarrow$ $(ab)(ab) = (ab)b + bab - b \,.\, b$

$\Rightarrow$ $(aba) \,.\, b = (ab + ba - b)b$

$\Rightarrow$ $a(ba) = ab + ba - b$, by right cancellation law

$\Rightarrow$ $a(ab) = ab + ab - b$ $\quad (\because\ ab = ba)$

$\Rightarrow$ $(aa)b = 2ab - b \Rightarrow (aa)b = (2a - 1)b$

$\Rightarrow$ $aa = 2a - 1 \Rightarrow aa = a + a - 1$

$\Rightarrow$ $aa - a - a + 1 = 0 \Rightarrow (a - 1) \,.\, (a - 1) = 0$

$\Rightarrow$ $a - 1 = 0$

$\therefore$ $a = 1$.

Example 23. In a field F, prove that $a^2 = b^2$ implies either $a = b$ or $a = -b \ \forall\ a, b \in F$.

Solution. Now $(a - b) \,.\, (a + b) = (a - b) \,.\, a + (a - b) \,.\, b$, by right distributive law

$= a \,.\, a - b \,.\, a + a \,.\, b - b \,.\, b$, by left distributive law

$= a^2 - a \,.\, b + a \,.\, b - b^2$ $\quad (a \,.\, b = b \,.\, a \ \forall\ a, b \in F)$

$= a^2 - b^2 = a^2 - a^2$ $\quad (\because\ a^2 = b^2)$

$= 0$

$\therefore$ Either $a - b = 0$ or, $a + b = 0$

i.e., either $a = b$ or, $a = -b$.

PROBLEM SET

RINGS AND FIELDS

Problem Set 13.1

1. Prove that for all a, b, c, d in a ring R
   (*i*) $(a + b)(c + d) = ac + ad + bc + bd$
   (*ii*) $(a - b)(c - d) = (ac + bd) - (ad + bc)$
   (*iii*) $(a - b)(c + d) = ac + ad - (ad + bc)$
   (*iv*) $(a - b)^2 = a^2 - ab - ba + b^2$.
2. Prove that for all a, b in a ring R
   $(a + b)^2 = a^2 + 2ab + b^2$ if R is commutative.
3. Define a ring. Give examples of the following
   (*i*) A commutative ring without identity
   (*ii*) A non commutative ring with identity
   (*iii*) Neither commutative nor has a unit element
   (*iv*) Integral domain but not a field.
4. Prove that the set E of all even integers is a commutative ring with respect to usual addition and multiplication, but it has no unit element.
5. If R is a ring and $a, b, c \in R$, then show that
   (*i*) $-(a + b) = -a - b$
   (*ii*) $a - (b + c) = (a - b) - c$
6. Let R be a ring with unity e. If for some $x \in R$ there exists unique $y \in R$ such that $xy = e$, prove that x is invertible.
7. Let E be a set consisting of a single element e. define
   $e + e = e ; e = e$
   Is (E, +, .) a ring ? If yes, is it commutative ? Does it has a multiplicative unity and a zero divisor?
8. Show that the set R of real numbers with the composition o and * by
   $a \circ b = a + b + 1$ and $a * b = ab + a + b$
   is a ring. Determine 0-element and the 1-element of the ring.
9. Show that the set of integers with the composition o and * defined by
   $a \circ b = a + b + 1$ and $a * b = ab + a + b$
   is a ring.
10. Prove that the set of all matrices of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $a, b, c, d \in Q$ is not a commutative ring with respect to matrix addition and multiplication. Does it has unit element? Does it possess zero divisor?
11. Show that the set of all matrices of the form $\begin{bmatrix} x & y \\ -y & x \end{bmatrix}$; $x, y \in Z$
    is a commutative ring with respect to matrix addition and multiplication. Does it have division of zero? Does it have unity?
12. In the ring (S, +, .). S is a set of 2×2 matrices of the form $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ where a, b, c are even integers and + and . are respectively matrix addition and multiplication. Show that (S, +, .) is a non commutative ring with no unity element.
13. Give an example of a ring in which $a^2 = a$ for all a (such a ring is called a **Boolean ring**). Show that in a Boolean ring $2a = 0$ for all a. Deduce that a Boolean ring is commutative.
14. Do the following sets form an integral domain with respect to addition and multiplication ? If so state if they are field.
    (*i*) The set A of numbers of the form $b\sqrt{2}$, $b \in Q$.
    (*ii*) The set E of even integers.
    (*iii*) The set Z^+ of positive integers.

15. A Gaussian integer is a complex number $a + ib$, where a and b are integers. Show that the set of Gaussian integers forms an integral domain under ordinary addition and multiplication. Is it a field?

16. Show that, in a field F,
   (*i*) $(-a)\,b = -(ab)$, $a, b \in F$;
   (*ii*) $(-a)(-b)^{-1} = ab^{-1}$;
   (*iii*) $(a^{-1})^{-1} = a$

17. Let S be a set of all 2×2 matrices of the form $\begin{bmatrix} 0 & 0 \\ a & b \end{bmatrix}$ where a and b are integers. Show that S is a ring and not a field.

18. Show that the set $\{0, 1, 2, 3, 4, 5, 6\}$ is a field with respect to addition modulo 7 and multiplication modulo 7 as the two compositions.

19. For the set $\{0, 1, 2, 3, 4\}$, show that the modulo 5 system is a field.

20. Show that the set of numbers $\{a + b\sqrt{3} : a, b \in R\}$ is an integral domain with respect to addition and multiplication of numbers.

21. Show that the set of numbers of the form $a + b\sqrt{2}$ with a and b as rational numbers is a field.

22. If in a commutative ring R, a and b are nilpotent elements then prove that $a + b$ and ar for all $r \in R$ are nilpotent.

23. Explain with example the difference between a field and skew field.

24. If J and K are ideals in a ring. Prove that $J \cap K$ is an ideal in R.

25. If $f(x) = 2x^3 + x^2 + 2x + 2$ and $g(x) = 2x^2 + 2x + 1$, find (*a*) $f(x) + g(x)$ and $f(x)\,g(x)$ (*b*) $f(x) +_3 g(x)$ and $f(x) \times_3 g(x)$.

26. If $f(x) = 3x^2 + 5x + 2$, $g(x) = 2x^2 + 4x + 1$, find (*a*) $f(x) + g(x)$ and $f(x) \times g(x)$ (*b*) $f(x) +_6 g(x)$ and $f(x) \times_6 g(x)$.

27. Let $R = \left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix} : a, b \in Z\right\}$ and f be the mapping that takes $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ to $a - b$.
   (*i*) Show that f is a homomorphism. (*ii*) Determine the kernel of f.

28. Consider the mapping from $M_2(Z)$ into Z given by $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \to a$. Prove or disprove that this is a ring homomorphism.

29. Show that the set M of all 2×2 matrices of the form $\begin{bmatrix} 0 & a \\ a & b \end{bmatrix}$; a, b integers is a left ideal but not a right ideal in the ring of all 2×2 matrices with elements as integers.

ANSWERS 13.1

10. yes, yes

11. No, yes

14. (*i*) is not closed w.r.t. multiplication, hence not a ring. That means neither an integral domain nor a field.
(*ii*) Unit element $1 \notin E$. E is not an integral domain. E will be an integral domain if the definition does not require the existence of the unit element. E is not a field since the multiplicative identity does not exist. (*iii*) Neither an integral domain nor a field.

25. (*a*) $2x^3 + 3x^2 + 4x + 3$, $4x^5 + 6x^4 + 8x^3 + 9x^2 + 6x + 2$
(*b*) $2x^3 + x$, $x^5 + 2x^3 + 2$

26. (*a*) $5x^2 + 9x + 3$, $6x^4 + 22x^3 + 23x^2 + 13x + 2$
(*b*) $2x^3 + 3x^2 + 3x + 3$, $4x^4 + 4x^3 + 5x^2 + x + 2$.

27. Ker $f = \left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in Z\right\}$

28. Multiplication is not preserved.

SHORT/MULTIPLE CHOICE QUESTIONS

1. The number of binary operations required for a set to be a ring is

(*a*) 1 (*b*) 2 (*c*) 3 (*d*) none of these

2. The member of unit element of the ring $(Z, +, .)$

(*a*) 2 (*b*) 3 (*c*) 1 (*d*) infinite

3. If R is a ring without zero divisors, then $x \, . \, y = 0$ implies

(*a*) $x = 0$ or $y = 0$ (*b*) $x = 0$ and $y = 0$ (*c*) $x = 0, y \neq 0$ (*d*) $x \neq 0, y = 0$

4. A ring $(R, +, .)$ is said to be commutative if it is commutative with respect to

(*a*) multiplication (*b*) addition (*c*) both (*d*) none of these

5. Which of the following is a ring?

(*a*) z under x and $+$ (*b*) z under $+$ and x

(*c*) the set $\{1, w, w^2\}$ under x and $+$ (*d*) none of these

6. A division ring and a field must contain at least

(*a*) one element (*b*) finite number of elements

(*c*) two elements (*d*) infinite number of elements

7. If R is a ring such that $a^2 = a$, $\forall\, a \in R$, then R is called

(*a*) Integral domain (*b*) Boolean ring (*c*) Division ring (*d*) Field

8. A finite commutative ring with identity is a field if

(*a*) R has no zero divisors (*b*) R has an unique multiplicative identity

(*c*) The no. of elements in R is prime. (*d*) The no. of elements in R is a power of prime.

9. In $(Z_8, +_8, \times_8)$ the number of zero divisors are

(*a*) 3 (*b*) 4 (*c*) 5 (*d*) 6

10. Fill up the blank.

(*a*) Let R be a ring. An element a R is called ____ if $a^2 = a$ and _____ if $a^n = 0$ for some positive integer

(*b*) The only idempotents in an integral domain are _____ and _____

(*c*) Let R be a commutative ring with unity, the R is called an _____ if R has no zero divisor.

11. State true of false

(*a*) Every field is an integral domain.

(*b*) If a and are two zero divisors, then $a + b$ is also a zero in a Ring.

(*c*) In a finite field F, $a^2 + b^2 = 0$ implies $a = 0$ and $b = 0$ for all $a, b \in F$.

(*d*) The characteristic of an infinite ring is alwasys 0.

(*e*) Every field is a division ring.

ANSWERS

1. (*b*) **2.** (*a*) **3.** (*a*) **4.** (*a*) **5.** (*b*) **6.** (*c*)

7. (*b*) **8.** (*a*) **9.** (*a*)

10. (*a*) Idempotent, nilpotent (*b*) 0, 1 (*c*) Integral domain

11. (*a*) True (*b*) False (*c*) False (*d*) False (*e*) True