CONTENTS

18-05-16

1

Rings

In this chapter we shall introduce the concepts of *ring*, *integral domain*, *division ring* and *field* and give their examples and basic properties. We also discuss *subrings* and *ideals* of a ring.

1.1 Ring

Definition 1. *A* **ring** *is a non-empty set R with two binary compositions denoted by $+$ and $\cdot$, and satisfying the following properties :*

R.1. $a+b \in R$ *for all* $a, b \in R$.

R.2. $a+b=b+a$ *for all* $a, b \in R$.

R.3. $a+(b+c)=(a+b)+c$ *for all* $a, b, c \in R$.

R.4. *There exists an element denoted by* $0 \in R$ *such that*
$a+0=a$ *for all* $a \in R$.
(0 *is called* **additive identity** *or* **zero element** *in* R)

R.5. *For each* $a \in R$, *there exists an element* $b \in R$ *such that*
$a+b=0$.
(b *is called* **additive inverse** *or* **negative** *of* a *and is written as* $b=-a$, *so that* $a+(-a)=0$)

R.6. $a \cdot b \in R$ *for all* $a, b \in R$.

R.7. $a \cdot (b \cdot c)=(a \cdot b) \cdot c$ *for all* $a, b, c \in R$.

R.8. $a \cdot (b+c)=a \cdot b+a \cdot c$ (*Left distributive law*)

R.9. $(a+b) \cdot c=a \cdot c+b \cdot c$ (*Right distributive law*)
for all $a, b, c \in R$.

We denote a ring as $\{R, +, \cdot\}$.

Remark. Axioms R.1. – R.5. mean that $(R, +)$ is an abelian group and R.6. – R.7. mean that $(R, \cdot)$ is a semi-group.

Definition 2. *A ring is called* **finite** *or* **infinite** *according as it contains finite or infinite number of elements.*

Definition 3. *A ring* $\{R, +, \cdot\}$ *is called a* **commutative ring**, *if*
$a \cdot b=b \cdot a$ *for all* $a, b \in R$.

Definition 4. *A ring* R *is called* **boolean**, *if* $x^2=x$ *for all* $x \in R$.

Definition 5. *A ring* $\{R, +, \cdot\}$ *is called a ring with* **unit element** *or* **unity** *or* **identity**, *if there exists an element* $e \in R$ *such that*
$a \cdot e=e \cdot a=a$ *for all* $a \in R$.

Definition 6. *Let R be a ring with unity e. An element $a \in R$ is called* **invertible**, *if there exists some element $b \in R$ such that*

$$a \cdot b = b \cdot a = e.$$

Definition 7. *If n be a positive integer and a an element of a ring R, we define*

$$a^n = \underbrace{a \cdot a \ldots a}_{n \text{ times}} \quad \text{and} \quad na = \underbrace{a + a + \ldots + a}_{n \text{ times}}.$$

1.2 Examples of Rings

Example 1.2.1. *The set $\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ of integers is a commutative ring under the usual addition and multiplication of integers.* Here 0 is the additive identity and $-a$ is the additive inverse of $a \in \mathbf{Z}$. Note that $1 \in \mathbf{Z}$ is the unit element, since $a \cdot 1 = 1 \cdot a = a \ \forall\ a \in \mathbf{Z}$.

However, $\mathbf{N} = \{1, 2, 3, \ldots\}$ is **not** a ring. (Why ?)

Example 1.2.2. *The set $\mathbf{E} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ of all even integers is a commutative ring without unit element.*

Example 1.2.3. *The sets* **R** *(all real numbers) and* **Q** *(all rational numbers) are commutative rings with unity w.r.t. usual addition and multiplication.*

Example 1.2.4. (Ring of integers modulo $n \equiv \mathbf{Z}_n$)

For any positive integer n, $\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$ is a commutative ring w.r.t. addition and multiplication modulo n, denoted as $\oplus_n$ and $\otimes_n$, respectively.

In particular, $\mathbf{Z}_2 = \{0, 1\}$, $\mathbf{Z}_3 = \{0, 1, 2\}$, $\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ are rings of integers modulo 2, 3 and 6, respectively. In $\mathbf{Z}_6$, $2 \oplus_6 3 = 5$, $3 \oplus_6 4 = 1$, $4 \oplus_6 5 = 3$; $2 \otimes_6 3 = 0$, $4 \otimes_6 5 = 2$ etc.

It may be observed that $\mathbf{Z}_2$ is a boolean ring, since $0^2 = 0$ and $1^2 = 1$ in $\mathbf{Z}_2$.

Example 1.2.5. The Ring of Gaussian Integers $\equiv J[i]$ or $\mathbf{Z}[i]$:

$$\mathbf{Z}[i] = \{m + ni : m, n \text{ are integers}, i = \sqrt{-1}\}$$

is a commutative ring with unity $1\ (= 1 + 0i)$ w.r.t. the usual addition and multiplication of complex numbers.

Example 1.2.6. *The set of all 2×2 matrices :*

$$M_2 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbf{R} \text{ (all reals)} \right\}$$

is a non-commutative ring with unity, under the addition and multiplication of 2×2 matrices. Note that $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the additive identity of M_2 and $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$ is the negative of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Also $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the unity of M_2.

Example 1.2.7. *The set S of all 2×2 matrices over the ring $\mathbf{Z}_2 = \{0, 1\}$ of integers modulo 2 is a finite non-commutative ring.*

Indeed, the ring S has $2^4 = 16$ elements *viz*

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Example 1.2.8. *The set*

$$M = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a \text{ and } b \text{ are real numbers} \right\}$$

is a non-commutative ring without unity, under matrix addition and matrix multiplication.

Notice that $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$

$$\therefore \quad \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

Example 1.2.9. *The set*

$$M = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} : a \text{ and } b \text{ are complex numbers} \right\}$$

is a non-commutative ring with unity, under matrix addition and multiplication. The unity of M_2 is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Here $\bar{a}$ denotes the conjugate of a. Notice that

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}\begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} = \begin{pmatrix} ax - b\bar{y} & ay + b\bar{x} \\ -(\bar{a}\bar{y} + \bar{b}x) & \bar{a}\bar{x} - \bar{b}y \end{pmatrix} \in M.$$

Example 1.2.10. *Let R denote the set of all real-valued continuous functions on $[0, 1]$. Let $f, g \in R$. Define*

$$(f + g)(x) = f(x) + g(x), \ (f \cdot g)(x) = f(x)\, g(x) \ \forall\ x \in [0, 1]$$

Then R is a commutative ring with unity.

It is easy to verify that R is a ring, in which the additive identity is the zero function given by $o(x) = 0 \ \forall\ x \in [0, 1]$.

Indeed, $(f + o)(x) = f(x) + o(x) = f(x) + 0 = f(x) \ \forall\ x \in [0, 1]$.

$\therefore \quad f + o = f$ for all $f \in R$.

The additive inverse of $f \in R$ is $f_1 : [0, 1] \to \mathbf{R}$ such that

$f_1(x) = -f(x)$ for all $x \in [0, 1]$. We have $f + f_1 = o$.

Further $(f \cdot g)(x) = f(x)\, g(x) = g(x) f(x) = (g \cdot f)(x) \ \forall\ x \in [0, 1]$.

$\therefore\ f \cdot g = g \cdot f \ \forall\ f, g \in R$. Hence R *is a commutative ring with unity* $I \in R$, where $I(x) = x \ \forall\ x \in [0, 1]$.

1.3 Some Properties of Rings

Theorem 1.3.1. *If R is a ring and $a, b, c \in R$; then*

1. $a+b=a+c \Rightarrow b=c$. *(Cancellation law w.r.t. +)*
2. $-(-a)=a$.
3. *The zero element of R is unique.*
4. *The additive inverse of any element in R is unique.*

Proof. Since R is a ring, so by definition, $(R, +)$ is a group.

1. By cancellation law in a group $(G, \cdot)$, we know

$$a \cdot b = a \cdot c \Rightarrow b = c. \qquad \ldots(1)$$

Since $(R, +)$ is a group, so writing + for . in (1), we get

$$a+b=a+c \Rightarrow b=c.$$

2. In a group $(G, \cdot)$, we know $(a^{-1})^{-1}=a$. ...(2)

Since $(R, +)$ is a group in which a^{-1} is denoted by $-a$, so by (2),

$$-(-a)=a.$$

3. Let, if possible, 0 and 0′ be two zero elements in R.

Then $0+a=a$ and $a+0'=a \ \forall\ a \in R$. ...(3)

In particular, $0+0'=0'$ and $0+0'=0$.

(Take $a=0'$ and $a=0$ in (3), respectively).

Hence $0=0'$, which shows that the zero element in R is unique.

4. Let, if possible, a' and a'' be two additive inverses of a in R. Then

$$a+a'=a'+a=0 \quad \text{and} \quad a+a''=a''+a=0.$$

Now $a'=a'+0=a'+(a+a'')=(a'+a)+a''=0+a''=a''$.

Hence $a'=a''$, which shows that the additive inverse of any element $a \in R$ is unique.

Theorem 1.3.2. *If R is a ring, then for any $a, b, c \in R$:*

1. $a \cdot 0=0 \cdot a=0$.
2. $a \cdot (-b)=(-a) \cdot b=-(a \cdot b)$.
3. $(-a) \cdot (-b)=a \cdot b$.
4. $a \cdot (b-c)=a \cdot b-a \cdot c$.

If, in addition, R has a unit element 1, then

5. $(-1) \cdot a=-a$.
6. $(-1) \cdot (-1)=1$.

Proof. 1. We know $a+0=a$ for all $a \in R$.

In particular, $0+0=0$ and so $a \cdot (0+0)=a \cdot 0$

$\Rightarrow a \cdot 0+a \cdot 0=a \cdot 0$ (left distributive law)

$\Rightarrow a \cdot 0+a \cdot 0=a \cdot 0+0$.

Hence $a \cdot 0=0$, by cancellation law in the group $(R, +)$.

Similarly, we can show that $0 \cdot a=0$.

2. We know $b+(-b)=0$ for all $b \in R$.

$\therefore$ $a \cdot \{b+(-b)\}=a \cdot 0=0$, by part **1.**

or $a \cdot b+a \cdot (-b)=0$ (left distributive law).

Hence $a \cdot (-b)=-(a \cdot b)$.

Similarly, $\{a+(-a)\} \cdot b=0 \cdot b \Rightarrow a \cdot b+(-a) \cdot b=0$.

Hence $(-a) \cdot b=-(a \cdot b)$.

3. We have $(-a) \cdot (-b)=(-a) \cdot c$, where $c=-b$

$=-(a \cdot c)$, by part **2**

$=-\{a \cdot (-b)\}$

$=-\{-(a \cdot b)\}$, by part **2**

$=a \cdot b$, since $-(-x)=x$ in R.

4. $a \cdot (b-c)=a \cdot \{b+(-c)\}=a \cdot b+a \cdot (-c)=a \cdot b-a \cdot c$, by part **2.**

5. Suppose that R has a unit element 1. Then $a \cdot 1=1 \cdot a=a$.

Now $a+(-1) \cdot a=1 \cdot a+(-1) \cdot a=\{1+(-1)\} \cdot a=0 \cdot a=0$.

Hence $(-1) \cdot a=-a$.

6. Taking $a=-1$ in part **5**, we obtain

$$(-1) \cdot (-1)=-(-1)=1.$$

Notation. *In a ring $\{R, +, \cdot\}$, we shall now write $a \cdot b$ as ab.*

EXAMPLES

Example 1.3.1. *Show that the set $R=\{a+b\sqrt{3} : a, b \in \mathbf{Q}\}$ is a ring under the usual addition and multiplication as binary compositions.*

Solution. It is easy to verify that $(R, +)$ is an abelian group with $0=0+0\sqrt{3}$ as the additive identity and $-a-b\sqrt{3}$ as the additive inverse of $a+b\sqrt{3}$.

Let $x=a+b\sqrt{3}$, $y=c+d\sqrt{3}$ and $z=e+f\sqrt{3} \in R$.

Then $xy=(a+b\sqrt{3})(c+d\sqrt{3})=(ac+3bd)+(ad+bc)\sqrt{3} \in R$,

since $ac+3bd \in \mathbf{Q}$ and $ad+bc \in \mathbf{Q}$.

Now $(xy)z=\{(ac+3bd)+(ad+bc)\sqrt{3}\}(e+f\sqrt{3})$

$=(ace+3bde+3adf+3bcf)+(acf+3bdf+ade+bce)\sqrt{3}$

$=x(yz)$.

Finally,

$x(y+z)=(a+b\sqrt{3})\{(c+e)+(d+f)\sqrt{3}\}$

$=(ac+ae+3bd+3bf)+(ad+af+bc+be)\sqrt{3}$

$=\{(ac+3bd)+(ad+bc)\sqrt{3}\}+\{(ae+3bf)+(af+be)\sqrt{3}\}$

$=xy+xz$.

Similarly, $(x+y)z=xy+yz$. Hence R is a ring.

Note. R is a communicative ring, since $xy=yx \ \forall\ x, y \in R$.

Example 1.3.2. *Show that the set $\mathbf{I}$ of integers with two binary compositions $*$ and o defined by $a * b=a+b-1$, $aob=a+b-ab$ for all integers a and b is a commutative ring with unity.*

Solution. We have $a * b = a + b - 1 \ \forall \ a, b \in \mathbf{I}$. ...(1)

From (1), $a * b \in \mathbf{I} \ \forall \ a, b \in \mathbf{I}$.

Now $a * b = a + b - 1 = b + a - 1 = b * a$. Further

$(a * b) * c = (a + b - 1) * c = (a + b - 1) + c - 1$, by (1)

$= a + (b + c - 1) - 1 = a * (b + c - 1) = a * (b * c)$, by (1).

$\therefore \ (a * b) * c = a * (b * c) \quad \forall \ a, b, c \in \mathbf{I}$.

We have $a * 1 = a + 1 - 1 = a \ \forall \ a \in \mathbf{I}$, using (1).

Thus 1 is the identity in $\mathbf{I}$.

Let $a' = 2 - a$. Then, by (1), we get

$a * a' = a + a' - 1 = a + (2 - a) - 1 = 1$.

Thus $2 - a$ is the inverse of $a \ \forall \ a \in \mathbf{I}$.

We now consider $aob = a + b - ab$. ...(2)

From (2), $aob \in \mathbf{I} \quad \forall \quad a, b \in \mathbf{I}$.

Now $(aob) oc = (a + b - ab) oc = (a + b - ab) + c - (a + b - ab) c$, by (2)

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

$= ao (b + c - bc) = ao (boc)$, by (2).

$\therefore \quad (aob) oc = ao (boc) \quad \forall \quad a, b, c \in \mathbf{I}$.

Finally, $ao (b * c) = ao (b + c - 1)$, by (1)

$= a + (b + c - 1) - a (b + c - 1)$, by (2)

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

$= (aob) + (aoc) - 1$, by (2).

$\therefore \quad ao (b * c) = (aob) * (aoc)$, by (1).

Similarly, $(a * b) oc = aoc * boc$.

Hence $\{\mathbf{I}, *, o\}$ is a ring.

Example 1.3.3. *If $\{R, +, \cdot\}$ be a ring with unit element, show that $\{R, \oplus, \otimes\}$ is also a ring with unit element, where*

$a \oplus b = a + b + 1$ *and* $a \otimes b = a \, . \, b + a + b \quad \forall \quad a, b \in R$.

Solution. We have $a \oplus b = a + b + 1$. ...(1)

From (1) ; $a \oplus b \in R$, as R is a ring and $1 \in R$.

Now $a \oplus b = a + b + 1 = b + a + 1$, since $\{R, +, \cdot\}$ is a ring.

$\therefore \quad a \oplus b = b \oplus a$, by (1).

Using (1) and associative law w.r.t. $+$ in the ring R,

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

Since R is a ring and $1 \in R$, so $-1 \in R$ is the identity in $\{R, \oplus, \otimes\}$.

$[\because \ a \oplus -1 = a - 1 + 1 = a + 0 = a, R$ being a ring$]$

For any $a \in R, a' = -a - 1 - 1 \in R$ is the additive inverse of a in $\{R, \oplus, \otimes\}$.

$[\because \ a \oplus a' = a + (-a - 1 - 1) + 1 = \{a + (-a)\} - 1 + 0 = 0 - 1 = -1]$

We have $a \otimes b = a \, . \, b + a + b$. ...(2)

From (2) ; $a \otimes b \in R$, since $\{R, +, \cdot\}$ is a ring.

Using (2) and associative law w.r.t. '$\cdot$' in the ring R, we get

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

Finally, $a \otimes (b \oplus c) = a \otimes (b + c + 1)$, by (1)

$= a \, . \, (b + c + 1) + a + (b + c + 1)$, by (2)

$= a \, . \, b + a \, . \, c + a \, . \, 1 + a + b + c + 1$,

by distributive law in R

$= (a \, . \, b + a + b) + (a \, . \, c + a + c) + 1$

$(\because \ a \, . \, 1 = a)$

$= a \otimes b + a \otimes c + 1$, by (2)

$\therefore \quad a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$, by (1).

Similarly, $(a \oplus b) \otimes c = a \otimes c \oplus b \otimes c$.

By (2), $a \otimes 0 = a \, . \, 0 + a + 0 = a \quad \forall \quad a \in R$.

Hence $\{R, \oplus, \otimes\}$ is a ring whose unit element is $0 \in R$.

Example 1.3.4. *If $\mathbf{E}$ denotes the set of all even integers, then prove that $\{\mathbf{E}, +, *\}$ is a commutative ring, where $a * b = ab/2$ and $+$ is the usual addition.*

Solution. It is clear that $(\mathbf{E}, +)$ is an abelian group in which 0 is the identity and $-a$ is the additive inverse of $a \in \mathbf{E}$.

We have $a * b = ab/2$. ...(1)

(*i*) (Closure law). Let $a, b \in \mathbf{E}$ so that a and b are even integers. Then $ab/2$ must be an even integer *i.e.*, $a * b \in \mathbf{E}$, by (1).

(*ii*) (Associative law). Let $a, b, c \in \mathbf{E}$. Then by (1), we have

$$a * (b * c) = a * \frac{bc}{2} = \frac{a\,(bc/2)}{2} = \frac{abc}{4}.$$

Similarly, $(a * b) * c = \dfrac{abc}{4}$. $\therefore \quad a * (b * c) = (a * b) * c$.

(*iii*) (Distributive law). We have

$$a * (b + c) = \frac{a\,(b + c)}{2}, \text{ by (1)}$$

$$= \frac{ab}{2} + \frac{ac}{2} = a * b + a * c, \text{ by (1)}.$$

(*iv*) (Commutative law). From (1), $a * b = b * a \ \forall \ a, b \in \mathbf{E}$.

Hence $\{\mathbf{E}, +, *\}$ is a commutative ring.

Example 1.3.5. *Prove that the set S of all ordered pairs (a, b) of real numbers is a commutative ring under the addition and multiplication compositions defined as*

$(a, b) + (c, d) = (a + c, b + d)$ *and* $(a, b) \, (c, d) = (ac, bd)$.

Solution. We have $(a, b) + (c, d) = (a + c, b + d)$. ...(1)

It is clear that $(S, +)$ is an abelian group in which $(0, 0)$ is the identity, since $(a, b) + (0, 0) = (a + 0, b + 0) = (a, b)$ and $(-a, -b)$ is the additive inverse of (a, b), since $(a, b) + (-a, -b) = (0, 0)$.

Let $x = (a, b), y = (c, d)$ and $z = (e, f) \in S$.

Then $xy = (a, b)(c, d) = (ac, bd) \in S$. Also $xy = yx$.

It can be verified that $(xy)z = x(yz)$.

Now $x(y + z) = (a, b)(c + e, d + f)$, by (1)

$= (a(c + e), b(d + f)) = (ac + ae, bd + bf)$

$= (ac, bd) + (ae, bf)$, by (1).

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

Hence R is a commutative ring.

Example 1.3.6. *Prove that a ring R is commutative if and only if $(a + b)^2 = a^2 + 2ab + b^2$ for all $a, b \in R$.*

Solution. Let R be a commutative ring so that $ab = ba$ for all $a, b \in R$.

Now

$$(a + b)^2 = (a + b)(a + b) = a(a + b) + b(a + b),$$
$$= aa + ab + ba + bb, \text{ by distributive laws in } R$$
$$= a^2 + ab + ab + b^2, \text{ since } ab = ba.$$

Hence $(a + b)^2 = a^2 + 2ab + b^2$. ...(1)

Conversely, let (1) be true for all $a, b \in R$. We shall show that R is commutative. From (1), we have

$$(a + b)(a + b) = aa + ab + ab + bb$$

or $aa + ab + ba + bb = aa + ab + ab + bb$, by distributive laws in R.

$\therefore \quad ba = ab$, by cancellation laws in $(R, +)$.

Hence R is commutative.

Example 1.3.7. *If R is a system satisfying all the conditions for a ring with unit element with the possible exception of $a + b = b + a$, prove that the axiom $a + b = b + a$ must hold in R and that R is thus a ring.*

Solution. It is given that $1 \in R$. Consider

$(a + b) \cdot (1 + 1) = (a + b) \cdot 1 + (a + b) \cdot 1$, by left distributive law in R

$= a + b + a + b$, ...(1)

since 1 is the unit element in R.

Again

$(a + b) \cdot (1 + 1) = a \cdot (1 + 1) + b \cdot (1 + 1)$, by right distributive law

$= a \cdot 1 + a \cdot 1 + b \cdot 1 + b \cdot 1$, by left distributive law

$= a + a + b + b$, since 1 is the unit element in R. ...(2)

From (1) and (2), it follows that

$$a + a + b + b = a + b + a + b$$

So $a + b = b + a$, by cancellation law in the group $(R, +)$.

Hence R is a ring.

Example 1.3.8. *Let R be a ring such that $a^2 = a$ for all $a \in R$. Prove that R is commutative.*

Solution. It is given that $a^2 = a \ \forall \ a \in R$. ...(1)

Since $a + a \in R$, so $(a + a)^2 = a + a$, by (1)

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

$\Rightarrow \quad aa + aa + aa + aa = a + a$, by distributive laws

$\Rightarrow \quad a^2 + a^2 + a^2 + a^2 = a + a$

$\Rightarrow \quad a + a + a + a = a + a$, by (1)

$\Rightarrow a + a = 0$, by cancellation laws in the group $(R, +)$ ...(2)

$\therefore \quad a = -a$ for all $a \in R$. ...(3)

Let $a, b \in R$. Then $a + b \in R$ and so $(a + b)^2 = a + b$.

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

$\Rightarrow aa + ba + ab + bb = a + b$, by distributive laws

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

$\Rightarrow \quad a + ba + ab + b = a + b$, by (1)

$\Rightarrow ba + ab = 0$, by cancellation laws in the group $(R, +)$

$\Rightarrow ba = -ab \quad \Rightarrow \quad ba = ab \quad \forall \ a, b \in R$, using (3).

Hence R is a commutative ring.

Example 1.3.9. *If R is a ring with unity satisfying $(xy)^2 = x^2y^2$ for all $x, y \in R$, prove that R is commutative.* [D.U., 1994]

Solution. We have $(xy)^2 = x^2y^2$ for all $x, y \in R$. ...(1)

Replacing y by $y + 1 \in R$ in (1), we obtain

$$[x(y + 1)]^2 = x^2(y + 1)^2 \quad \Rightarrow \quad (xy + x)^2 = x^2(y^2 + 2y + 1)$$

$\Rightarrow \quad (xy)^2 + (xy)x + x(xy) + x^2 = x^2y^2 + 2x^2y + x^2$. ...(2)

Using (1) and cancellation laws of $(R, +)$ in (2), we get

$$xyx + x^2y = 2x^2y \text{ or } xyx = x^2y \quad \forall \quad x, y \in R. \qquad ...(3)$$

Replacing x by $x + 1$ in (3), $(x + 1)y(x + 1) = (x + 1)^2y$

$\Rightarrow \quad (x + 1)(yx + y) = (x + 1)(xy + y)$

$\Rightarrow xyx + xy + yx + y = x^2y + xy + xy + y$. ...(4)

Using (3) and cancellation laws of $(R, +)$ in (4), we get

$$yx = xy \quad \forall \quad x, y \in R.$$

Hence R is a commutative ring.

Example 1.3.10. *Give an example of a non-commutative ring R without unity such that $(xy)^2 = x^2y^2 \ \forall \ x, y \in R$.*

Solution. Consider the ring R of 2×2 matrices :

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \text{ are integers} \right\}.$$

Clearly, R is non-commutative, since

$$\begin{pmatrix}1&1\\0&0\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}1&0\\0&0\end{pmatrix},\ \begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}1&1\\0&0\end{pmatrix}=\begin{pmatrix}1&1\\0&0\end{pmatrix}$$

and so $\begin{pmatrix}1&1\\0&0\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}\neq\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}1&1\\0&0\end{pmatrix}$.

The possible unity $\begin{pmatrix}1&0\\0&1\end{pmatrix}\notin R$.

Let $X=\begin{pmatrix}a&b\\0&0\end{pmatrix}, Y=\begin{pmatrix}c&d\\0&0\end{pmatrix}\in R$ by arbitrary. Then

$$XY=\begin{pmatrix}ac&ad\\0&0\end{pmatrix}, X^2=\begin{pmatrix}a^2&ab\\0&0\end{pmatrix}, Y^2=\begin{pmatrix}c^2&cd\\0&0\end{pmatrix},$$

and $$(XY)^2=\begin{pmatrix}ac&ad\\0&0\end{pmatrix}\begin{pmatrix}ac&ad\\0&0\end{pmatrix}=\begin{pmatrix}a^2c^2&a^2cd\\0&0\end{pmatrix}=X^2Y^2.$$

Example 1.3.11. *Show that a ring R is commutative if and only if $a^2-b^2=(a+b)(a-b)$ for all $a, b\in R$.* [D.U., 1997]

Solution. Let R be commutative. Then $ab=ba\ \forall\ a, b\in R$.

Hence $(a+b)(a-b)=a(a-b)+b(a-b)$

$$=a^2-ab+ba-b^2=a^2-b^2.$$

Conversely, let $a^2-b^2=(a+b)(a-b)$

or $a^2-b^2=a^2-ab+ba-b^2$

or $0=-ab+ba$, by cancellation laws in $(R,+)$

or $ab=ba\ \forall\ a, b, \in R$.

Hence R is a commutative ring.

Example 1.3.12. *Let R be a ring such that for $x\in R$, there exists a unique $a\in R$ satisfying $xa=x$. Show that $ax=x$. Hence deduce that if R has a unique right unity e, then e is the unity of R.*

Solution. We are given $xa=x$. ...(1)

We have $x(a+ax-x)=xa+xax-xx$, by left distributive law

$$=x+xx-xx=x, \text{ using (1)}$$

$\therefore$ $x(a+ax-x)=x$. ...(2)

By the uniqueness of a, (2) gives us

$$a+ax-x=a\Rightarrow ax-x=0\Rightarrow ax=x.$$

(ii) If e is the unique right identity of R, then

$$xe=x\ \forall\ x\in R.$$

By part *(i)*, $ex=x\ \forall\ x\in R$.

Hence $xe=ex=x\ \forall\ x\in R$ means that e is the unity of R.

Example 1.3.13. *Let R be a ring with unity $1\in R$. Suppose for $x\neq 0\in R$, there exists a unique $y\in R$ such that $xyx=x$. Prove that $xy=yx=1$ i.e., x is invertible in R.*

Solution. Let $xa=0$, where $a\in R$. Then

$$x(y+a)x=xyx+xax=x+0x=x.$$

By the uniqueness of y in the relation $xyx=x$, it follows that

$$x(y+a)x=x\Rightarrow y+a=y\Rightarrow a=0.$$

Hence $xa=0\Rightarrow a=0$ for each $a\in R$. ...(1)

Again $xyx=x\Rightarrow xyx-x.1=0$ $(\because 1\in R)$

$\Rightarrow x(yx-1)=0$

$\Rightarrow yx-1=0$, using (1)

$\therefore$ $yx=1$.

Similarly, we can show that

$$ax=0\Rightarrow x(a+y)x=x\Rightarrow a+y=y\Rightarrow a=0. \quad ...(2)$$

and so $xyx=x\Rightarrow (xy-1)x=0\Rightarrow xy-1=0\Rightarrow xy=1$. by (2)

Hence $xy=yx=1$.

Example 1.3.14. *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.*

Solution. We have

$$x(e+y-yx)=xe+xy-xyx=x+e-ex$$

$$=x+e-x=e.$$

By the uniqueness of y satisfying $xy=e$, we get

$$x(e+y-yx)=e\Rightarrow e+y-yx=y\Rightarrow yx=e.$$

Hence $xy=yx=e\Rightarrow x$ is invertible.

EXERCISES

1. If R is a ring and $a, b\in R$, prove that
$$(a+b)^2=a^2+ab+ba+b^2.$$
[**Hint.** $(a+b)^2=(a+b)(a+b)=a(a+b)+b(a+b)$]

2. Define a ring and give an example of (*i*) a non-commutative ring with unity, (*ii*) a non-commutative ring without unity, (*iii*) a commutative ring without unity, (*iv*) a commutative ring with unity.
[**Hint.** (*i*) See Example 1.2.6 ; (*ii*) See Example 1.2.8 ; (*iii*) The ring E of even integers ; (*iv*) The ring **Z** of integers.]

3. If a, b, c are any three elements in a ring R, prove that
(*i*) $a(b-c)=ab-ac$, (*ii*) $(a-b)c=ac-bc$.

4. Prove that the set $S=\{a+b\sqrt{2} : a, b\in \mathbf{Q}\}$ is a commutative ring w.r.t. usual addition and multiplication.

5. Show that the set $\{3n : n\in \mathbf{Z}\}$ is a commutative ring w.r.t. usual addition and multiplication.

6. Let S be a non-empty set and F be the collection of all subsets of S. For any $A, B \in F$, define

$$A + B = A \cup B - A \cap B \text{ and } AB = A \cap B.$$

Prove that F is a commutative ring with unity.

[**Hint.** The additive identity in F is empty set ϕ, since

$$A + \phi = A \cup \phi - A \cap \phi = A - \phi = A.$$

The additive inverse of A is A, since

$$A + A = A \cup A - A \cup A = A - A = \phi.$$

The unity in F is S, since $AS = A \cap S = A \ \forall \ A \in F$.]

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

(*i*) $2a = 0 \ \forall \ a \in R$, (*ii*) $a + b = 0 \Rightarrow a = b$, (*iii*) $ab = ba \ \forall \ a, b \in R$.

[**Hint.** (*i*) See Example 1.3.8 for (*iii*). By equation (2), we have

$$a + a = 0 \Rightarrow 2a = 0 \text{ and } a = -a.$$

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

8. If a, b are any two elements of a ring R and m and n are any two positive integers, then prove that

(*i*) $(m+n)\,a = ma + na$, (*ii*) $m\,(a+b) = ma + mb$,

(*iii*) $m\,(na) = (mn)\,a$, (*iv*) $(na)\,(mb) = (nm)\,(ab)$,

(*v*) $a^m \cdot a^n = a^{m+n}$ (*vi*) $(a^m)^n = a^{mn}$.

[**Hint.** (*ii*) $m\,(a+b) = a+b+a+b+\ldots+a+b$ (m times)

$= (a+a+\ldots+a) + (b+b+\ldots+b)$,

since $a + b = b + a$.

$= ma + mb$.

(*iv*) $(na)\,(mb) = (a+a+\ldots+a)\,(b+b+\ldots+b)$

(n times, m times)

$= a\,(b+\ldots+b) + \ldots + a\,(b+\ldots+b)$ (n times)

(Left distributive law)

$= (ab+\ldots+ab) + \ldots + (ab+\ldots+ab)$ (n times)

(m times, m times)

$= (nm)\,(ab)$]

9. If R is a commutative ring and $a, b \in R$, then for any positive integer n, prove that

$$(a+b)^2 = a^2 + 2_{c_1}\, ab + b^2,$$

$$(a+b)^3 = a^3 + 3_{c_1}\, a^2 b + 3_{c_2}\, ab^2 + b^2,$$

$$\overline{\qquad\qquad\qquad\qquad}$$

$$(a+b)^n = a^n + n_{c_1}\, a^{n-1}\, b + n_{c_2}\, a^{n-2}\, b^2 + \ldots + b^n.$$

10. Let R be a ring such that for $x \in R$, there exists a unique $a \in R$ such that $ax = x$. Show that $xa = x$. Hence deduce that if R has a unique left unity e, then e is the unity of R.

[**Hint.** Consider $(a + xa - x)\,x = ax + xax - xx = x + xx - xx = x$

$\therefore \quad a + xa - x = a \Rightarrow xa = x$.]

11. Let R be a ring and $e \in R$ be such that $ex = x \ \forall \ x \in R$, then e is said to be a *left unity* of R. Show that if R has a unique left unity, then R has unity.

[**Hint.** Compare with Ex. 10 above.]

12. Let R be a ring and $e \in R$ be such that $xe = x \ \forall \ x \in R$, then e is said to be a *right unity* of R. Show that if R has a unique right unity, then R has unity.

[**Hint.** See Example 1.3.12.]

13. Let $a, b, c \in R$ be such that $ba = b$ and $a + c - ac = 0$. Show that $b = 0$.

[**Hint.** $a + c - ac = 0 \Rightarrow ba + bc - bac = 0 \Rightarrow b + bc - bc = 0 \Rightarrow b = 0$.]

14. Show that if $1 - ab$ is invertible in a ring R with unity, then so is $1 - ba$.

15. Let $\{R, +, \cdot\}$ be a ring. Show that the system $\{R, +, o\}$ is also a ring, where $xoy = y \cdot x \ \forall \ x, y \in R$.

The ring $\{R, +, o\}$ is called the **opposite ring** of R, written as R^{opp}.

1.4 Integral Domain and Field

Definition 1. (Zero Divisor)

A non-zero element 'a' of a commutative ring R is called a **zero divisor,** *if there exists some non-zero element b in R such that* $ab = 0$.

Illustrations

1. In the ring M_2 of all 2×2 matrices

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq O, B = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \neq O, \text{ but } AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = O.$$

Thus A and B are zero divisors in M_2.

2. In the ring $\mathbf{Z}_6$ of integers modulo 6, 2 and 3 are zero divisors, since

$$2 \otimes_6 3 = 0 \in \mathbf{Z}_6.$$

Definition 2. (Integral Domain)

A commutative ring is called an **integral domain,** *if it has no zero divisors.* Equivalently,

A commutative ring R is called an **integral domain,** *if*

$ab = 0 \Rightarrow$ *either* $a = 0$ *or* $b = 0$; $a, b \in R$.

Or

$a \neq 0$ *and* $b \neq 0 \Rightarrow ab \neq 0$; $a, b \in R$.

Illustrations

1. The ring $\mathbf{Z}$ of integers is an integral domain, since for any two integers a and b : $ab = 0 \Rightarrow a = 0$ or $b = 0$.

2. The commutative ring $\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ is **not** an integral domain ; since $2 \otimes_6 3 = 0$ but $2 \neq 0$ and $3 \neq 0$ in $\mathbf{Z}_6$.

3. $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$ is an integral domain, since $a \otimes_5 b \neq 0$ for all $a \neq 0$, $b \neq 0$ in $\mathbf{Z}_5$

Definition 3. (Division Ring)
A ring $(R, +, \cdot)$ is called a **division ring** *or a* **skew-field** *if its non-zero elements form a group w.r.t. the composition '$\cdot$'.*

Definition 4. (Field)
A commutative division ring is called a **field**.

Equivalently, A ring $(R, +, \cdot)$ is called a **field**, *if its non-zero elements form an abelian group w.r.t. the composition '$\cdot$'.*

The multiplicative identity of a field R is denoted by 1 and the multiplicative inverse of $a \neq 0 \in R$ is denoted by a^{-1}, so that

$$a\,a^{-1} = a^{-1}\,a = 1.$$

Note. If R is a field, then $a \neq 0 \in R \Rightarrow a^{-1} \in R$.

Remark. *The explicit properties of a field are given below :*

A **field** *is a non-empty set R with two binary compositions denoted by $+$ and $\cdot$ such that for all a, b, c in R ;*

A.1. $a + b \in R$.	**M.1.** $a \cdot b \in R$.
A.2. $a + b = b + a$.	**M.2.** $a \cdot b = b \cdot a$.
A.3. $a + (b + c) = (a + b) + c$.	**M.3.** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
A.4. *There exists an element $0 \in R$ such that* $a + 0 = a\ \forall\ a \in R$.	**M.4.** *There exists an element $1 \in R$ such that* $a \cdot 1 = a\ \forall\ a \in R$.
A.5. *For each $a \in R$, there exists an element $b \in R$ such that* $a + b = 0$.	**M.5.** *For each $a \neq 0 \in R$, there exists an element $a' \in R$ such that* $a \cdot a' = 1$.

A.M. $a \cdot (b + c) = a \cdot b + a \cdot c$.

Example 1.4.1. $\mathbf{Q}$ *(all rationals) and* $\mathbf{R}$ *(all reals) are fields w.r.t. the usual addition and multiplication.*

Example 1.4.2. $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$ *is a field w.r.t. addition and multiplication modulo 5.*

The multiplicative inverses of $1, 2, 3, 4 \in \mathbf{Z}_5$ are 1, 3, 2, 4 ; respectively.

Example 1.4.3. *For any prime p, $\mathbf{Z}_p = \{0, 1, 2, \ldots, p-1\}$ is a field w.r.t. addition and multiplication modulo p.*

For the proof, see the corollary of Theorem 1.5.3. ahead.

Example 1.4.4. *$\{\mathbf{Z}_6, \oplus_6, \otimes_6\}$ is not a field, since, for example, $2 \neq 0 \in \mathbf{Z}_6$ has no multiplicative inverse in $\mathbf{Z}_6$.*

Example 1.4.5. *The set $\mathbf{C} = \{a + bi : a, b \in \mathbf{R}\}$ of complex numbers is a field under usual addition and multiplication of complex numbers.*

It may be observed that $0 = 0 + 0i$ is the additive identity in $\mathbf{C}$. $-a - b\,i$ is the additive inverse of $a + bi$, $1 = 1 + 0i$ is the multiplicative identity in $\mathbf{C}$ and finally, if $z = a + bi \neq 0 \in \mathbf{C}$, then

$$z^{-1} = \left(\frac{a}{a^2+b^2}\right) - \left(\frac{b}{a^2+b^2}\right) i = \frac{a - bi}{a^2+b^2} \in \mathbf{C}$$

is the multiplicative inverse of z, since

$$zz^{-1} = \frac{1}{(a^2+b^2)}(a + bi)(a - bi) = \frac{a^2+b^2}{a^2+b^2} = 1.$$

Example 1.4.6. *The set*

$$S = \left\{ \begin{pmatrix} x & y \\ -\bar{x} & \bar{y} \end{pmatrix} : x, y \in \mathbf{C} \right\}$$

is a division ring, which is not a field.

We have seen in Example 1.2.9 that S is a non-commutative ring with unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ under matrix addition and matrix multiplication. We now proceed to show that every non-zero element of S has its inverse under matrix multiplication. Let

$$A = \begin{bmatrix} a + ib & c + id \\ -(c - id) & a - ib \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S.$$

(Here a, b, c, d are not all zero)

Then

$$A^{-1} = \begin{bmatrix} \frac{1}{k}(a - ib) & -\frac{1}{k}(c + id) \\ \frac{1}{k}(c - id) & \frac{1}{k}(a + ib) \end{bmatrix} \in S, \text{ where } k = a^2 + b^2 + c^2 + d^2 \neq 0$$

Notice that

$$AA^{-1} = \begin{bmatrix} \frac{1}{k}(a^2+b^2+c^2+d^2) & 0 \\ 0 & \frac{1}{k}(a^2+b^2+c^2+d^2) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = A^{-1}A.$$

Hence S is a division ring, which is not a field.

Example 1.4.7. *The set*

$$Q = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \text{ are real numbers}\}$$

where $i^2 = j^2 = k^2 = ijk = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j$

is a division ring, which is not a field.

We define $+$ in Q as follows :

$$(a_0 + a_1 i + a_2 j + a_3 k) + (b_0 + b_1 i + b_2 j + b_3 k)$$
$$= (a_0 + b_0) + (a_1 + b_1)\,i + (a_2 + b_2)\,j + (a_3 + b_3)\,k.$$

It is easy to verify that $(Q, +)$ is an abelian group.

The zero element in Q is $0 = 0 + 0i + 0j + 0k$, the unity in Q is $1 = 1 + 0i + 0j + 0k$, the additive inverse of $a_0 + a_1 i + a_2 j + a_3 k$ is $-a_0 - a_1 i - a_2 j - a_3 k$.

Now we proceed to show that every non-zero element in Q has its multiplicative inverse in Q.

Let $x = a_0 + a_1 i + a_2 j + a_3 k \neq 0 \in Q$, so that a_0, a_1, a_2, a_3 are not all zero.

Then $l = a_0^2 + a_1^2 + a_2^2 + a_3^2 \neq 0$.

Let $y = \frac{1}{l}(a_0 - a_1 i - a_2 j - a_3 k) \in Q$. We see that

$$xy = \frac{1}{l}[(a_0 + a_1 i) + (a_2 j + a_3 k)]\,[(a_0 - a_1 i) - (a_2 j + a_3 k)]$$

$$= \frac{1}{l}[(a_0^2 - a_1^2 i^2) - (a_2 j + a_3 k)(a_2 j + a_3 k) + (a_2 j + a_3 k)(a_0 - a_1 i) - (a_0 + a_1 i)(a_2 j + a_3 k)]$$

$$= \frac{1}{l}[(a_0^2 + a_1^2 - (-a_2^2 - a_3^2) + a_1 a_2 k - a_1 a_3 j - a_1 a_2 k + a_1 a_3 j]$$

$$= l/l = 1.$$

Similarly, $yx = 1$. Further Q is non-commutative, as

$$(2i + 3k)(j - 4k) = 2k + 8j - 3i + 12,$$

$$(j - 4k)(2i + 3k) = -2k - 8j + 3i + 12 \neq (2i + 3k)(j - 4k).$$

Hence Q is a division ring, which is not a field.

The ring Q is called the *ring of real quaternions*.

Example 1.4.8. *The set* $R = \{a + b\sqrt{3} : a, b \in \mathbf{Q}\}$ *is a field under usual addition and multiplication.*

It is easy to verify that R is a commutative ring and $1 = 1 + 0\sqrt{3} \in R$ is the multiplicative identity of R. Finally, if $x = a + b\sqrt{3} \neq 0 \in R$, then its multiplicative inverse is

$$x^{-1} = \left(\frac{a}{a^2 - 3b^2}\right) - \left(\frac{b}{a^2 - 3b^2}\right)\sqrt{3},$$

since $$xx^{-1} = \frac{1}{(a^2 - 3b^2)}(a + b\sqrt{3})(a - b\sqrt{3}) = \frac{a^2 - 3b^2}{a^2 - 3b^2} = 1.$$

Example 1.4.9. *Let C be the set of all ordered pairs* (a, b) *where* a, b *are real numbers. Let the compositions of addition and multiplication in C be defined as*

$$(a, b) + (c, d) = (a + c, b + d), \qquad ...(1)$$

$$(a, b) \cdot (c, d) = (ac - bd, bc + ad). \qquad ...(2)$$

Then C is a field.

From (1), we see that

(i) $(a, b) + (c, d) = (a + c, b + d) \in C$.

(ii) $(a, b) + (c, d) = (c, d) + (a, b)$. $[\because a + c = c + a, b + d = d + b]$

(iii) $(a, b) + (0, 0) = (a + 0, b + 0) = (a, b)\ \forall\ (a, b) \in C$.

Thus $(0, 0)$ is the additive identity in C.

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

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

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

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

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

From (2), we have

(vi) $(a, b) \cdot (c, d) \in C$.

(vii) $(a, b) \cdot (c, d) = (c, d) \cdot (a, b)$. $[\because ac = ca, bd = db]$

(viii) $(a, b) \cdot (1, 0) = (a \cdot 1 - b \cdot 0, b \cdot 1 + a \cdot 0) = (a, b)\ \forall\ (a, b) \in C$.

Thus $(1, 0)$ is the multiplicative identity in C.

(ix) For $(a, b) \neq (0, 0) \in C$, the multiplicative inverse of (a, b) is

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

Using (1) and (2), it can be verified that if $x = (a, b)$, $y = (c, d)$ and $z = (e, f) \in C$, then

(x) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, and

(xi) $x \cdot (y + z) = x \cdot y + x \cdot z$.

Hence C is a field.

1.5 Basic Theorems of Integral Domains and Fields

Theorem 1.5.1. *Let R be a commutative ring. Then R is an integral domain if and only if* $ab = ac \Rightarrow b = c$, *where* $a, b, c \in R$ *and* $a \neq 0$.

Proof. *Condition is necessary*

Let R be an integral domain. Let $ab = ac$; $a, b, c \in R$.

Then $ab - ac = 0$

$\Rightarrow$ $a(b - c) = 0$. ...(1)

Since R is an integral domain, it follows from (1),

either $a = 0$ or $b - c = 0$.

It is given that $a \neq 0$ and so $b - c = 0$. Hence $b = c$.

Condition is sufficient

Let $ab = ac \Rightarrow b = c, \forall\ a, b, c \in R$ and $a \neq 0$. ...(2)

We have to show that R is an integral domain. Firstly we prove that R has no zero divisors.

Let $x, y \in R$ be such that $xy = 0$.

If $x \neq 0$, then $xy = 0 \Rightarrow xy = x0 \Rightarrow y = 0$, by (2)

Similarly, if $y \neq 0$, then $xy = 0 \Rightarrow x = 0$.

Thus R has no zero divisors. Since R is a commutative ring, it follows that R is an integral domain.

Remark. *Cancellation law may not hold in an arbitrary ring.*

Let $A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$ and $C = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ be three elements in the ring M_2 of all 2×2 matrices over integers. Then

$$AC=\begin{bmatrix}1&1\\1&1\end{bmatrix}\begin{bmatrix}1&0\\1&0\end{bmatrix}=\begin{bmatrix}2&0\\2&0\end{bmatrix};$$

$$BC=\begin{bmatrix}2&0\\0&2\end{bmatrix}\begin{bmatrix}1&0\\1&0\end{bmatrix}=\begin{bmatrix}2&0\\2&0\end{bmatrix}.$$

Thus $AC=BC$, but $A\neq B$.

Theorem 1.5.2. *Prove that every field is an integral domain.*

Proof. Let R be any field.

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

Since $a\neq 0\in R$, $a^{-1}\in R$ exists and $aa^{-1}=a^{-1}a=1$.

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

$\Rightarrow (a^{-1}a)\,b=(a^{-1}a)\,c$, by associative law

$\Rightarrow 1\,b=1\,c \Rightarrow b=c$.

Thus R is a commutative ring in which

$ab=ac \Rightarrow b=c\ (a, b, c\in R, a\neq 0)$.

Hence R is an integral domain (See Theorem 1.5.1).

Remark. *The converse of the above theorem is not true.*

For example, the set of integers $\mathbf{Z}$ is an integral domain which is not a field, since $a\neq 0\in \mathbf{Z}$ does not have the multiplicative inverse in $\mathbf{Z}$.

Theorem 1.5.3. *Prove that a finite integral domain is a field.* [D.U., 1999, 96]

Proof. Let $R=\{x_1, x_2, \ldots, x_n\}$ be a finite integral domain.

In order to show that R is a field, we have to prove that R has the unity and that every non-zero element of R has its multiplicative inverse in R. Let $a\neq 0\in R$. Then

$$ax_1, ax_2, \ldots, ax_n \qquad \ldots(1)$$

are n distinct elements of R, for if $ax_i=ax_j$, $i\neq j$;

then by cancellation law in R, $x_i=x_j$, which is a contradiction.

Let r be an arbitrary element of R. Then by (1), we get

$r=ax_l$, for some l satisfying $1\leq l\leq n$.

Since $a\in R$, $a=ax_m$, for some m satisfying $1\leq m\leq n$, by (1).

We have $x_m r=x_m(ax_l)=(x_m a)x_l$

$=(ax_m)x_l$, since R is commutative

$=ax_l=r$.

Since R is commutative, $x_m r=r x_m=r\ \forall\ r\in R$.

It follows that $x_m\in R$ is the unity of R. We write x_m as 1.

Since $1\in R$, $1=ax_p$, for some p satisfying $1\leq p\leq n$, by (1)

$=x_p a$, since R is commutative.

Thus $ab=ba=1$, where $b=x_p\in R$.

This implies that $a^{-1}=b\in R$. Hence R is a field.

Corollary. *Show that the ring $\mathbf{Z}_p$ of integers modulo p is a field if and only if p is prime.* [D.U., 1998]

Proof. *Condition is necessary*

Let $\mathbf{Z}_p$ be a field. Let, if possible, p be not prime. Then

$p=ab$, where $1<a, b<p$; $a, b\in \mathbf{Z}$

$\Rightarrow ab\equiv 0 \pmod p \Rightarrow ab=0$ in $\mathbf{Z}_p$, where $a\neq 0, b\neq 0\in \mathbf{Z}_p$

$\Rightarrow \mathbf{Z}_p$ has zero divisors $\Rightarrow$ $\mathbf{Z}_p$ is not an integral domain

This is a contradiction, since $\mathbf{Z}_p$ is a field implies $\mathbf{Z}_p$ is an integral domain.

Condition is sufficient

We know $\mathbf{Z}_p$ is a finite commutative ring Now we show that $\mathbf{Z}_p$ is an integral domain.

Let $a, b\in \mathbf{Z}_p$ be such that $ab=0$ in $\mathbf{Z}_p$. Then p divides ab.

$\Rightarrow p\mid a$ or $p\mid b$, since p is prime

$\Rightarrow a=0$ or $b=0$ in $\mathbf{Z}_p$

So $ab=0$ in $\mathbf{Z}_p \Rightarrow a=0$ or $b=0$ in $\mathbf{Z}_p$ $(a, b\in \mathbf{Z}_p)$.

Hence $\mathbf{Z}_p$ is a finite integral domain and so $\mathbf{Z}_p$ is a field.

Remark. *As an application of the above corollary, we see that*

$\mathbf{Z}_2=\{0, 1\}$, $\mathbf{Z}_3=\{0, 1, 2\}$, $\mathbf{Z}_5=\{0, 1, 2, 3, 4\}$ etc.

are all fields (finite).

Ex. *What happens if the integral domain is infinite ?* [D.U., 1996]

An infinite integral domain may not be a field. For example, $\mathbf{Z}$ (all integers) is an infinite integral domain, which is not a field.

Theorem 1.5.4. *Let R be a ring such that the equation $ax=b$ has a solution for all $a\neq 0\in R$ and for all $b\in R$. Show that R is a division ring.*

Proof. Firstly, we show that R has no zero divisors, *i.e.*, to show $a\neq 0, b\neq 0\in R \Rightarrow ab\neq 0$.

Let, if possible, $ab=0$; where $a\neq 0, b\neq 0\in R$. Then

$abx=0\ \forall\ x\in R$. ...(1)

Since $b\neq 0$, so for any $r\in R$, there exists some $x\in R$ such that

$bx=r$.

Using in (1), $ar=0\ \forall\ r\in R$. ...(2)

Since $a\neq 0$, $ax=a$ has a solution, say $c\in R$. Then $a=ac \Rightarrow a=0$. by (2).

This is a contradiction.

Hence R has no zero divisors *i.e.*, $ab=0 \Rightarrow$ either $a=0$ or $b=0$. ...(3)

Let $x = e \in R$ be a solution of $ax = a$, $a \neq 0$. Then $ae = a$ and $e \neq 0$.

We have $a(e - e^2) = ae - aee = ae - ae = 0$.

Using (3), $e - e^2 = 0$, as $a \neq 0$. Thus $e^2 = e$. ...(4)

We now proceed to show that e is the unity of R. For any $x \in R$,

$(xe - x)e = xe^2 - xe = xe - xe = 0$, using (4).

It follows that $xe - x = 0$, as $e \neq 0$; using (3).

$\therefore \quad xe = x \; \forall \, x \in R$.

Again $e(ex - x) = e^2x - ex = ex - ex = 0$, by (4).

$\therefore \quad ex - x = 0$ or $ex = x \quad \forall \, x \in R$, using (3).

Hence $xe = ex = x \quad \forall \, x \in R \Rightarrow e$ is the unity of R.

Let $a \neq 0 \in R$. Then $ax = e$ has a solution, say $x = b \in R$.

Then $ab = e$ and $(ba - e)\, b = bab - eb = be - eb = 0$.

Using (3), $ba - e = 0$, as $b \neq 0$. Thus $ab = ba = e \Rightarrow a^{-1} = b \in R$.

Hence R is a division ring.

EXERCISES

1. Prove that the set of all real numbers of the form $a + \sqrt{2}\, b$, where a and b are rational numbers is a field under the usual addition and multiplication.
2. Define a ring and an integral domain. Give an example of a ring which is not an integral domain.
   [**Hint.** $Z_6 = \{0, 1, 2, 3, 4, 5\}$] is a ring, which is not an integral domain.]
3. Prove that every field is an integral domain, but every integral domain is not a field. Give an example of an integral domain which is also a field.
   [**Hint.** The set $\mathbf{Z}$ of integers is an integral domain, which is not a field. The ring $Z_5 = \{0, 1, 2, 3, 4\}$ of integers modulo 5 is both an integral domain and a field.
4. Define a division ring and give an example of it.
5. Give an example of a division ring which is not a field.
   [**Hint.** See Example 1.4.6.]
6. Show that the ring R of real-valued continuous functions on $[0, 1]$ is not an integral domain.
   [**Hint.** Refer to Example 1.2.10. Consider
   $f(x) = \begin{cases} x, & \text{if } x \leq 0 \\ 0, & \text{if } x > 0 \end{cases}$ and $g(x) = \begin{cases} 0, & \text{if } x \leq 0 \\ x, & \text{if } x > 0 \end{cases}$
   Then $f \neq 0 \in R$ and $g \neq 0 \in R$, but $fg = 0$.]
7. Tick the correct answer :
   (*i*) An integral domain is a field.
   (*ii*) A finite integral domain is a field.

   (*iii*) A field is an integral domain.
   (*iv*) A division ring is an integral domain.
   (*v*) A field is a division ring.
8. Show that a non-zero finite integral domain is a field. Give an example of a finite integral domain. [D.U., 1999]
   [**Hint.** See Theorem 1.5.3. $Z_5 = \{0, 1, 2, 3, 4\}$ is a finite integral domain]
9. Prove that the set of all 2×2 matrices over the finite field $Z_3 = \{0, 1, 2\}$ is a finite non-commutative ring of order $3^4 = 81$, under matrix addition and matrix multiplication.
10. Prove that the set of all 3×3 matrices over a finite field is a finite non-commutative ring under matrix addition and matrix multiplication. [D.U., 1994]
    [**Hint.** If F is a field having n elements, then the required ring R has n^9 elements. Further R is non-commutative, since $AB \neq BA$, where
    $$A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$
11. Prove that a division ring R has no zero divisors.
    [**Hint.** Let $a, b \in R$ be such that $ab = 0$. If $a \neq 0 \in R$, then $a^{-1} \in R$.
    $\therefore \quad ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0 \Rightarrow (a^{-1}a)\, b = 0 \Rightarrow 1 \,.\, b = 0 \Rightarrow b = 0$.
    Similarly, for $b \neq 0$, $ab = 0 \Rightarrow a = 0$.]
12. Show that a finite ring with unity and no divisors of zero is a division ring.
    [**Hint.** Similar to Theorem 1.5.3]

1.6 Subring

Definition. *Let $\{R, +, \cdot\}$ be a ring. A non-empty subset S of R is called a* **subring** *of R, if $\{S, +, \cdot\}$ is a ring.*

Illustrations

1. The set $\mathbf{E}$ of even integers is a subring of the ring $\mathbf{Z}$ of integers.
2. The ring of Gaussian integers $\mathbf{Z}[i]$ is a subring of the ring $\mathbf{C}$ of complex numbers.
3. The set $S = \{0, 2\}$ is a subring of the ring $\mathbf{Z}_4 = \{0, 1, 2, 3\}$ of integers modulo 4, under addition and multiplication modulo 4.

Theorem 1.6.1. *A non-empty subset S of a ring R is a subring of R if and only if (i) $a - b \in S$ and (ii) $ab \in S$ for all $a, b \in S$.*

Proof. *The condition is necessary*

Let S be a subring of R. Let $a, b \in S$.

By definition of a ring, $ab \in S$.

Since $(S, +)$ is a group, so $b \in S \Rightarrow -b \in S \Rightarrow a - b \in S$.

Subring Test.

The condition is sufficient

Let the conditions (*i*) and (*ii*) be true. Consequently, for $a \in S$,

$a - a = 0 \in S$.

Again $0 \in S, a \in S \Rightarrow 0 - a = -a \in S$.

Further $a \in S, b \in S \Rightarrow a \in S$ and $-b \in S \Rightarrow a + b \in S$.

Let $a, b, c \in S$. Then $ab \in S$, by condition (*ii*).

Clearly $a(bc) = (ab)c$, $a(b + c) = ab + ac$, $(b + c)a = ba + ca$, are true, since $S \subseteq R$. Hence S is a ring and so S is a subring of R.

Theorem 1.6.2. *The intersection of two subrings of a ring R is a subring of R.*

Proof. Let A and B be two subrings of a ring R.

Clearly $A \cap B$ is non-empty, since $0 \in A \cap B$.

Let $a, b \in A \cap B$. Then $a, b \in A$ and $a, b \in B$.

Since A is a subring of R, $a - b \in A$ and $ab \in A$. [Theorem 1.6.1]

Similarly, $a - b \in B$ and $ab \in B$.

So $a - b \in A \cap B$ and $ab \in A \cap B$. Hence $A \cap B$ is a subring of R, by Theorem 1.6.1.

Remark 1. *The union of two subrings of R need not be a subring of R.*

Two subrings of the ring of integers $\mathbf{Z}$ are

$A = \{..., -4, -2, 0, 2, 4, ...\}$, $B = \{..., -6, -3, 0, 3, 6, ...\}$.

Then $A \cup B = \{..., -4, -3, -2, 0, 2, 3, 4, ...\}$.

We see that 3, 2 are in $A \cup B$, but $3 - 2 = 1 \notin A \cup B$.

Thus $A \cup B$ is not a subring of $\mathbf{Z}$.

Remark 2. Theorem 1.6.2 can be easily extended to an arbitrary family of subrings of R.

Theorem 1.6.3. *Show that the centre of a ring R is a subring of R.*

Proof. *The centre of a ring R, denoted by $Z(R)$, is defined as*

$$Z(R) = \{a \in R : xa = ax \text{ for all } x \in R\}.$$

Clearly, $Z(R)$ is non-empty, since $0x = x0 \ \forall \ x \in R \Rightarrow 0 \in Z(R)$.

Let $a, b \in Z(R)$. Then $xa = ax$ and $xb = bx \ \forall \ x \in R$. ...(1)

We shall show that $a - b$ and ab are in $Z(R)$.

Consider $(a - b)x = ax - bx = xa - xb$, by (1).

Thus $(a - b)x = x(a - b) \ \forall \ x \in R \Rightarrow a - b \in Z(R)$.

Again $(ab)x = a(bx) = a(xb)$, by (1)

$= (ax)b = (xa)b$, by (1).

Thus $(ab)x = x(ab) \ \forall \ x \in R \Rightarrow ab \in Z(R)$.

Hence $Z(R)$ is a subring of R.

Theorem 1.6.4. *Show that the centre of a division ring is a field.*

[D.U., 1997]

Proof. Let R be a division ring. The *centre* of R is defined as

$$Z(R) = \{a \in R : xa = ax \ \forall \ x \in R\}. \quad ...(1)$$

By Theorem 1.6.3, $Z(R)$ is a subring of R.

In other words, $Z(R)$ is a ring. We have to show that $Z(R)$ is a field.

Let $a, b \in Z(R)$ be arbitrary.

Using (1), $ax = xa \ \forall \ x \in R$.

In particular, $ab = ba \ \forall \ a, b \in Z(R)$

$\Rightarrow Z(R)$ is a commutative ring.

Since R is a division ring, $1 \in R$ and $1x = x1 \ \forall \ x \in R$.

Thus $1 \in Z(R)$.

Finally, we show that each non-zero element of $Z(R)$ has its multiplicative inverse in $Z(R)$.

Let $a \neq 0 \in Z(R)$ be arbitrary $\Rightarrow a \neq 0 \in R$.

$\Rightarrow \quad a^{-1} \in R$, since R is a division ring.

Let $x \neq 0 \in R$ be arbitrary, so that $x^{-1} \in R$ exists. We have

$a^{-1}x = (x^{-1}a)^{-1} = (ax^{-1})^{-1}$, since $a \in Z(R) \Rightarrow ax^{-1} = x^{-1}a$.

$\therefore \quad a^{-1}x = xa^{-1} \ \forall \ x \neq 0 \in R$.

Obviously, $a^{-1}0 = 0a^{-1}$. Thus $a^{-1}x = xa^{-1} \ \forall \ x \in R$.

It means that $a^{-1} \in Z(R) \ \forall \ a \neq 0 \in Z(R)$.

Hence $Z(R)$ is a field.

EXAMPLES

Example 1.6.1. *Show that the set*

$$S = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbf{Z} \right\}$$

a subring of the ring M_2 of 2×2 matrices over integers.

Solution. Clearly, S is non-empty, since $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S$.

Let $A = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in S$ and $B = \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} \in S$. Then

$A - B = \begin{pmatrix} a - c & 0 \\ b - d & 0 \end{pmatrix} \in S$, $AB = \begin{pmatrix} ac & 0 \\ bc & 0 \end{pmatrix} \in S$.

Hence S is a subring of the ring of 2×2 matrices over integers.

Example 1.6.2. *If a is a fixed element of a ring R, show that*

$$I_a = \{x \in R : ax = 0\} \text{ is a subring of } R.$$

Solution. Since $a0 = 0$, $0 \in I_a$ and so I_a is non-empty.

Let $x, y \in I_a$ so that $ax = 0$, $ay = 0$.

Now $a(x - y) = ax - ay = 0 - 0 = 0$.

$\therefore \quad x - y \in I_a$.

Again $a(xy) = (ax)y = 0y = 0$.

$\therefore \quad xy \in I_a$. Hence I_a is subring of R.

Example 1.6.3. *(a) Give an example of a ring with unity 1 which has a subring with unity $1' \neq 1$.*

(b) Show by means of an example that a subring of a ring with unity may fall to be a ring with unity.

Solution. (a) $M_2 = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbf{Z}\right\}$ is a ring with unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. It is easy to verify that $S = \left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbf{Z}\right\}$ is a subring of M_2 with unity $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, since $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$.

Thus $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

(b) The ring $\mathbf{Z}$ of integers is a ring with unity.

But the set $\mathbf{E}$ of even integers is a subring of $\mathbf{Z}$ without unity.

Example 1.6.4. *Prove or disprove that subring of a non-commutative ring is non-commutative.*

Solution. A subring of a non-commutative ring may be commutative.

The ring M_2 of 2×2 matrices over integers is non-commutative, since

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

and so $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

The set $S = \left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in I\right\}$ is a subring of M_2, which is commutative, since

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}.$$

Example 1.6.5. *Give an example of each of the following with justification :*

(i) Ring which is not commutative but has a subring which is commutative.

(ii) Ring which has no unity but has a subring which has unity.

[D.U., 2000]

Solution. (i) Refer to Example 1.6.4.

(ii) $R = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbf{Z}\right\}$ is a ring which has no unity. The possible unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin R$. It can be verified that none of $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ is a unity of R.

However, $S = \left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbf{Z}\right\}$ is a subring of R, which has $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ as the unity of S.

Example 1.6.6. *Show that $S = \{0, 2, 4, 6, 8\}$ is a subring of $\mathbf{Z}_{10}$ with unity different from that of $\mathbf{Z}_{10}$, the ring of integers modulo 10.*

Solution. We know

$\mathbf{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is a ring with unity 1.

It can be verified that $a \otimes_{10} b \in S$ and $a \ominus_{10} b \in S$, $\forall\ a, b \in S$. For example, $4 \otimes_{10} 6 = 4$, $8 \otimes_{10} 4 = 2$ etc. and $8 \ominus_{10} 6 = 2$, $2 \ominus_{10} 8 = 4$ etc.

Hence S is a subring of $\mathbf{Z}_{10}$, where the unity of S is 6.

$[\because\ 6 \otimes_{10} 0 = 0,\ 6 \otimes_{10} 2 = 2,\ 6 \otimes_{10} 4 = 4,\ 6 \otimes_{10} 6 = 6,\ 6 \otimes_{10} 8 = 8]$

Example 1.6.7. *What can you say about the sum of two subrings of a ring ?*

Solution. *If A and B are two subrings of a ring R, then their* **sum** *is defined as $A + B = \{a + b : a \in A, b \in B\}$.*

We show by an example that the sum of two subrings of R need not be a subring of R.

Let $S = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbf{Z}\right\}$, $T = \left\{\begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} : c \in \mathbf{Z}\right\}$.

By Example 1.6.1, S is a subring of the ring M_2 of 2×2 matrices over integers. Similarly, T is a subring of M_2. The sum of S and T is

$$S + T = \left\{\begin{pmatrix} a & c \\ b & 0 \end{pmatrix} : a, b, c \in \mathbf{Z}\right\}.$$

It is clear that $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} \in S + T$, but

$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix} \notin S + T$. Hence $S + T$ is not a subring of M_2.

Remark. We have seen that

(i) The intersection of two subrings of a ring R is a subring of R.

(ii) The union of two subrings of a ring R may not be a subring of R.

(iii) The sum of two subrings of a ring R may not be a subring of R.

Example 1.6.8. *Let e be idempotent in a ring R. Show that $eRe = \{eae : a \in R\}$ is a subring of R with unity e.*

Solution. *An element $x \in R$ is called* **idempotent**, *if $x^2 = x$.*

We are given that $e^2 = e$. ...(1)

Clearly, eRe is non-empty, since $0 = e0e \in eRe$.

Let $x, y \in eRe$. Then $x = eae$, $y = ebe$ for some $a, b \in R$.

We have $x - y = eae - ebe = e(a-b)e \in eRe$, since $a \in R, b \in R \Rightarrow a - b \in R$.

Further $xy = eaebe = eae^2be = eaebe$, by (1)

$\Rightarrow xy = ere$, where $r = aeb \in R$

$\Rightarrow xy \in eRe$. Hence eRe is a subring of R.

For any $x \in R$, we see that

$ex = eeae = eae = x$, using (1)

$xe = eaee = eae = x$, using (1).

and $ex = xe = x \quad \forall\ x \in eRe$.

$\therefore$ Hence e is the unity of eRe.

Example 1.6.9. *Let R be a ring such that $x^3 = x\ \forall\ x \in R$. Show that R is commutative.*

Solution. It is given that $x^3 = x\ \forall\ x \in R$. ...(1)

In particular, $(x+x)^3 = x + x$

$2x \cdot 2x \cdot 2x = 2x$ or $8x^3 = 2x$ or $8x = 2x$.

or $6x = 0\ \forall\ x \in R$. ...(2)

$\therefore$

Again, by (1), $(x^2 - x)^3 = x^2 - x$

or $x^2 - x = (x^2 - x)(x^2 - x)^2 = x^2(x^2 - x)^2 - x(x^2 - x)^2$

$= x^2(x^4 + x^2 - 2x^3) - x(x^4 + x^2 - 2x^3)$

$= x^2(x \cdot x + x^2 - 2x) - x(x \cdot x + x^2 - 2x)$, by (1)

$= 2x^4 - 2x^3 - 2x^3 + 2x^2 = 2x \cdot x - 4x + 2x^2$, by (1)

$= 4x^2 - 4x$.

$\therefore \quad 3x^2 = 3x\ \forall\ x \in R$. ...(3)

Let $S = \{3x : x \in R\}$.

Then S is a subring of R, since $3x, 3y \in S \Rightarrow 3x - 3y = 3(x-y) \in S$

and $3x \cdot 3y = 9xy = 3(3xy) \in S$.

Let $y \in S$ be arbitrary. Then $y = 3x$, for some $x \in R$.

Now $y^2 = (3x)^2 = 9x^2 = 6x^2 + 3x^2 = (6x)x + 3x^2 = 3x^2 = 3x$, by (2) and (

$\therefore \quad y^2 = y\ \forall\ y \in S$.

Hence S is a commutative subring of R. [See Example 1.3.8]

It follows that $(3x)(3y) = (3y)(3x)\ ; x, y \in R$

$\Rightarrow \quad 6xy + 3xy = 6yx + 3yx \Rightarrow 3xy = 3yx$, using (2).

$\therefore \quad 3xy = 3yx$, for $x, y \in R$. ...(4)

Using (1), $(x+y)^3 = x + y$

or $x + y = (x+y)(x+y)^2 = (x+y)(x^2 + xy + yx + y^2)$

$= x^3 + x^2y + xyx + xy^2 + yx^2 + yxy + y^2x + y^3$

$= x + x^2y + xyx + xy^2 + yx^2 + yxy + y^2x + y$, by (1)

$\therefore \quad x^2y + xyx + xy^2 + yx^2 + yxy + y^2x = 0$. ...(5)

Again $(x-y)^3 = x - y$, by (1)

or $x - y = (x-y)(x^2 - xy - yx + y^2)$

$= x^3 - x^2y - xyx + xy^2 - yx^2 + yxy + y^2x - y^3$

$= x - x^2y - xyx + xy^2 - yx^2 + yxy + y^2x - y$, by (1)

$\therefore \quad -x^2y - xyx + xy^2 - yx^2 + yxy + y^2x = 0$. ...(6)

Adding (5) and (6), we get

$2xy^2 + 2yxy + 2y^2x = 0$. ...(7)

Post-multiplying and pre-multiplying (7) by y, we get, respectively,

$2xy^3 + 2yxy^2 + 2y^2xy = 0$ and $2yxy^2 + 2y^2xy + 2y^3x = 0$.

Using (1), these equations, respectively, become

$2xy + 2yxy^2 + 2y^2xy = 0$, ...(8)

$2yxy^2 + 2y^2xy + 2yx = 0$. ...(9)

Subtracting (9) from (8), we get

$2xy - 2yx = 0$ or $2xy = 2yx$. ...(10)

Subtracting (10) from (4), $xy = yx \quad \forall\ x, y \in R$.

Hence R is commutative.

EXERCISES

1. Show that $S = \{0, 2, 4\}$ and $T = \{0, 3\}$ are subrings of the ring $\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ of integers modulo 6.
2. Show that the intersection of an arbitrary number of subrings of a ring R is a subring of R.
3. Show that the set of matrices $\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right\}$ is a subring of the ring of 2×2 matrices with integral elements.
4. Show that a subring of an integral domain is an integral domain.
5. Let R be the ring of 2×2 matrices over reals. Show that

$$S = \left\{\begin{pmatrix} x & x \\ x & x \end{pmatrix} : x \text{ is a real number}\right\}$$

is a subring of R and has unity different from the unity of R.

[**Hint.** $\begin{pmatrix} x & x \\ x & x \end{pmatrix} - \begin{pmatrix} y & y \\ y & y \end{pmatrix} = \begin{pmatrix} x-y & x-y \\ x-y & x-y \end{pmatrix} \in S$, and

$\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} y & y \\ y & y \end{pmatrix} = \begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} \in S$.

The unity of S is $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$ and the unity of R is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.]

6. Let R be the ring of 3×3 matrices over reals. Show that

$$S=\left\{\begin{pmatrix} x & x & x \\ x & x & x \\ x & x & x \end{pmatrix} ; \text{ is a real number}\right\}$$

is a subring of R and has unity different from the unity of R.

[**Hint.** The unity elements of S and R are, respectively

$$\begin{pmatrix} 1/3 & 1/3 & 1/3 \\ 1/3 & 1/3 & 1/3 \\ 1/3 & 1/3 & 1/3 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.]$$

7. Show that the *normalizer* $N(a)$ of an element a of a ring R :

$$N(a)=\{x\in R : xa=ax\}.$$

is a subring of R.

8. Let R be the ring of all real-valued continuous functions defined on $[0, 1]$. Show that the set

$$S=\{f\in R : f(a)=0\}, \text{ where } a\in[0,1]$$

is a subring of R.

[**Hint.** See Example 1.2.10. Let $f, g\in S$, so that $f(a)=g(a)=0$.

Then $(f-g)(a)=f(a)-g(a)=0$; $(fg)(a)=f(a)\,g(a)=0$]

9. *A non-empty subset S of a field $\{F, +, \cdot\}$ is called a* **subfield** *of F, if $\{S, +, \cdot\}$ is a field.* Show that a subset S of a field F, containing at least two elements, is a subfield of F iff

(*i*) $a-b\in S\ \forall\ a, b\in S$, (*ii*) $ab^{-1}\in S\ \forall\ a\in S, b\neq 0\in S$.

1.7 Idempotent and Nilpotent Elements

Definition 1. *An element a in a ring R is called* **idempotent**, *if $a^2=a$.*

Definition 2. *An element a in a ring R is called* **nilpotent**, *if $a^n=0$ for some positive integer n.*

Remark. If R is a ring with unity 1, then 0 and 1 are idempotent elements of R ($\because 0^2=0, 1^2=1$). Further 0 is always nilpotent.

Illustrations

1. In the ring M_2 of all 2×2 matrices over integers,

$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ are idempotent elements, since

$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ etc. Further

$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ are nilpotent elements, since

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Can you find other idempotent and nilpotent elements in M_2 ?

2. In the ring $\mathbf{Z}_4=\{0, 1, 2, 3\}$ of integers modulo 4 ; 0 and 1 are the only idempotent elements and 0 and 2 are the only nilpotent elements. Notice that $2^2=0$ in $\mathbf{Z}_4$.
3. In the ring $\mathbf{Z}_{10}=\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ of integers modulo 10 ; 0, 1, 5, 6 are the only idempotent elements and 0 is the only nilpotent element. Notice that in $\mathbf{Z}_{10}$, $5^2=5, 6^2=6$.

EXAMPLES

Example 1.7.1. *Prove that the only idempotent elements in an integral domain R with unity are 0 and 1. What happens if R is not an integral domain ?*

Solution. Let $x\in R$ be idempotent, so that $x^2=x$ *i.e.*, $x\,.\,x=x\,.\,1$ as $1\in R$.

$\therefore\ x\,.\,(x-1)=0\Rightarrow x=0$ or $x-1=0$, since R is an integral domain.

Hence $x=0$ or $x=1$.

(*ii*) If R is not an integral domain, we may have idempotent elements other than 0 and 1. For example, $\mathbf{Z}_{10}=\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is not an integral domain, since $2\neq 0$, $5\neq 0\in\mathbf{Z}_{10}$, but $2\otimes_{10}5=0\in\mathbf{Z}_{10}$. The idempotent elements in $\mathbf{Z}_{10}$ are 0, 1, 5, 6. Notice that $5^2=5, 6^2=6$ in $\mathbf{Z}_{10}$.

Example 1.7.2. *If R is an integral domain, then show that R does not possess any non-zero nilpotent element.* [D.U., 2000]

Solution. Let, if possible, $\exists\ a\neq 0\in R$ such that a is nilpotent *i.e.*, $a^n=0$, for some positive integer n.

$\Rightarrow a\,.\,a\,...\,a$ (n times) $=0$

$\Rightarrow a=0$, since R is an integral domain.

This is a contradiction. Hence the result.

Example 1.7.3. *Show that in a ring R, a non-zero idempotent element cannot be nilpotent.*

Solution. Let a be any non-zero idempotent element of R.

Then $a^2=a\Rightarrow a^3=a^2=a\Rightarrow a^4=a$ and so on.

$\therefore\quad a^n=a\neq 0$ for all positive integers n.

Hence a is not nilpotent.

Example 1.7.4. *If a and b are nilpotent elements of a commutative ring R, show that $a+b$ is also nilpotent. Give an example to show that this may fail if R is not commutative.*

Solution. Since a and b are nilpotent, there exist positive integers m and n such that $a^m=0, b^n=0$. ...(1)

Since R is commutative, we can write

$$(a+b)^{m+n} = a^{m+n} + (m+n)_{c_1} a^{m+n-1} b + (m+n)_{c_2} a^{m+n-2} b^2 + \ldots + b^{m+n}$$
$$= a^m . a^n + (m+n)_{c_1} a^m a^{n-1} b + \ldots + b^m b^n$$
$$= 0, \text{ using (1).}$$

Hence $a+b$ is nilpotent.

(ii) The ring M_2 of all 2×2 matrices over the integers is non-commutative, where

$$A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ are nilpotent, since } A^2 = B^2 = O.$$

However, $A+B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is not nilpotent, since

$$(A+B)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } (A+B)^3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Indeed $(A+B)^n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ for all positive integers n.

Example 1.7.5. *Let R be a commutative ring and $a \in R$. Show that if a is nilpotent, then ab is nilpotent for each $b \in R$.*

Solution. Since a is nilpotent, $a^n = 0$ for some $n \in \mathbf{N}$.

Since R is commutative, therefore

$$(ab)^n = a^n b^n \; \forall \; a, b \in R$$
$$= 0 . b^n = 0.$$

Hence ab is nilpotent for all $b \in R$.

Example 1.7.6. *Let R be a ring and $a, b \in R$. Show that ab is nilpotent implies that ba is nilpotent.*

Solution. Since ab is nilpotent, $(ab)^n = 0$ for some $n \in \mathbf{N}$.

Consider $(ba)^{n+1} = ba \,.\, ba \,.\, ba \ldots ba \; (n+1 \text{ times})$
$$= b\,(ab)\,(ab) \ldots (ab)\,a$$
$$= b\,(ab)^n\,a = b \,.\, 0 \,.\, a = 0.$$

Hence ba is nilpotent.

Example 1.7.7. *Show that $\mathbf{Z}_6$, the ring of integers mod 6, has no non-zero nilpotent element.* [D.U., 1994]

Solution. We know $\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. We have in $\mathbf{Z}_6$, $1^n = 1 \neq 0$, $3^n = 3 \neq 0$, $4^n = 4 \neq 0 \; \forall \; n \in \mathbf{N}$.

Further $2^n = 2$ or $4 \; \forall \; n \in \mathbf{N}$ and $5^n = 5$ or $1 \; \forall \; n \in \mathbf{N}$.

Hence $\mathbf{Z}_6$ has no non-zero nilpotent elements. 0 is obviously nilpotent in $\mathbf{Z}_6$.

Example 1.7.8. *If R is a ring with no non-zero nilpotent elements, then show that for any idempotent $e \in R$, $ex = xe$ for all $x \in R$.*

Solution. Since e is idempotent, $e^2 = e$. ...(1)

For any $x \in R$, we have

$$(exe - ex)^2 = (exe - ex)\,(exe - ex)$$
$$= exe\,(exe - ex) - ex\,(exe - ex)$$
$$= exe^2xe - exe^2x - exexe + exex$$
$$= exexe - exex - exexe + exex = 0, \text{ by (1).}$$

It follows that $exe - ex$ is nilpotent. As given,

$$exe - ex = 0 \text{ or } exe = ex. \qquad ...(2)$$

Similarly, we can show that

$$(exe - xe)^2 = 0 \text{ and so } exe - xe = 0 \text{ or } exe = xe. \qquad ...(3)$$

From (2) and (3), $ex = xe \;\; \forall \;\; x \in R$.

In other words, $e \in Z(R)$, the centre of R.

Example 1.7.9. *In a ring R without unity, show that every idempotent is a zero divisor but is not nilpotent. Suppose now that R has no non-zero nilpotent elements. Prove that any idempotent is in the centre of R.* [D.U., 1998]

Solution. *(i)* Let e be any idempotent in R, so that $e^2 = e$. Since R is a ring without unity, there exists some $x \in R$ such that $xe \neq x$, for otherwise,

$$xe = x \;\; \forall \;\; x \in R \Rightarrow e \text{ is the unity of } R,$$

which is contrary to the given hypothesis.

Now $e^2 = e \Rightarrow xe^2 = xe \Rightarrow (xe - x)\,e = 0 \Rightarrow e = 0$,

since $xe - x \neq 0$. Hence e is a zero divisor.

Let, if possible, e be nilpotent. Then there exists a *least* positive integer n such that $e^n = 0$. ...(1)

Now $e^n = 0 \Rightarrow e^{n-2} \,.\, e^2 = 0 \Rightarrow e^{n-2} \,.\, e = 0 \Rightarrow e^{n-1} = 0$,

which is a contradiction to (1).

Hence e is a zero divisor but is not nilpotent.

(ii) Refer to Example 1.7.8.

Example 1.7.10. *Let R be a ring such that for each $a \in R$ there exists $x \in R$ such that $a^2x = a$. Prove the following :*

(i) R has no non-zero nilpotent elements.

(ii) $axa - a$ is nilpotent and so $axa = a$.

(iii) ax and xa are idempotents.

Solution. *(i)* Let $a \in R$ be any nilpotent element. Then

$$a^n = 0, \text{ for some positive integer } n. \qquad ...(1)$$

As given, for $a \in R$, there exists $x \in R$ such that $a^2x = a$. ...(2)

From (2), $a^{n-2}(a^2x) = a^{n-2}.a \Rightarrow a^n x = a^{n-1} \Rightarrow a^{n-1} = 0$, by (1).

Again from (2), $a^{n-3}(a^2x) = a^{n-3}.a \Rightarrow a^{n-1}x = a^{n-2} \Rightarrow a^{n-2} = 0$ and so on.

Proceeding in this manner, $a = 0$.

Hence R has no non-zero nilpotent elements.

(ii) We have

$$\begin{aligned}(axa-a)^2 &= (axa-a)(axa-a)\\ &= axa(axa-a) - a(axa-a)\\ &= axa^2xa - axa^2 - a^2xa + a^2\\ &= axa^2 - axa^2 - a^2 + a^2, \text{ by (2)}\\ &= 0.\end{aligned}$$

It follows that $axa - a$ is nilpotent in R and so by part (i),

$axa - a = 0$. Hence $axa = a$.

(iii) It is clear that

$$axa = a \Rightarrow ax\,ax = ax \text{ and } xa\,xa = xa$$
$$\Rightarrow (ax)^2 = ax \text{ and } (xa)^2 = xa$$

Hence ax and xa are idempotents.

EXERCISES

1. Define nilpotent and idempotent element of a ring R. Find the idempotent and nilpotent elements in $\mathbf{Z}_6$, the ring of integers modulo 6. [D.U., 1999]

   [**Ans.** 0, 1, 3, 4 are idempotents and 0 is nilpotent]

2. Prove that the only idempotent elements in a field are 0 and 1.
3. Find the idempotent and nilpotent elements in $\mathbf{Z}_5$.

   [**Ans.** 0, 1 are idempotents and 0 is nilpotent]

4. Prove that the set S of all nilpotent elements in a commutative ring R is a subring of R.

   [**Hint.** Refer to Examples 1.7.4 and 1.7.5. Verify that $a - b \in S$, $ab \in S\ \forall\ a, b \in S$.]

5. Prove that the following statements for a ring R are equivalent :
   (*a*) R has no non-zero nilpotent elements.
   (*b*) $a^2 = 0 \Rightarrow a = 0,\ a \in R$.
6. Find the idempotent, nilpotent and invertible elements of $\mathbf{Z}_{20}$.

   [**Ans.** {0, 1, 5, 16} are idempotents, {0, 10} are nilpotents, {1, 3, 7, 9, 11, 13, 17, 19} are invertible elements.]

7. Let a be an idempotent element in a ring R such that $a + b - ab = 0$ for some $b \in R$. Show that $a = 0$.

   [**Hint.** $a + b - ab = 0 \Rightarrow a^2 + ab - a^2b = 0 \Rightarrow a^2 = 0$ $(\because\ a^2 = a)$. Hence $a = 0$]

1.8 Characteristic of a Ring

Definition 1. *A ring R is said to be of* **finite characteristic**, *if there exists a positive integer n such that $na = 0$ for all $a \in R$.*

Definition 2. *If a ring R is of finite characteristic, then the* **characteristic** *of R is defined as the smallest positive integer p such that $pa = 0$ for all $a \in R$. We write it as char $R = p$.*

Definition 3. *A ring R is said to be of* **characteristic zero**, *if $na \neq 0$ for each positive integer n and for each $a \neq 0 \in R$.*

Equivalently, if char $R = 0$, then $na = 0$ for all $a \in R \Rightarrow n = 0$, n being any positive integer.

Remark. *The above definitions can similarly be extended to any integral domain R.*

Illustrations

1. char $\mathbf{Z} = 0$, char $\mathbf{Q} = 0$, char $\mathbf{R} = 0$. Here $\mathbf{Z}$, $\mathbf{Q}$ and $\mathbf{R}$ are the rings of integers, rationals and reals, respectively.
2. char $\mathbf{Z}_2 = 2$, where $\mathbf{Z}_2 = \{0, 1\}$. Notice that 2 is the smallest positive integer such that $2 \otimes_2 0 = 0$ and $2 \otimes_2 1 = 0$.
3. char $\mathbf{Z}_3 = 3$, where $\mathbf{Z}_3 = \{0, 1, 2\}$.

In general, char $\mathbf{Z}_n = n$, where $\mathbf{Z}_n = \{0, 1, 2, ..., n-1\}$ is the ring of integers modulo n.

Theorem 1.8.1. *Prove that the characteristic of any integral domain R is either zero or a prime number.* [D.U., 1996]

Proof. If char $R = 0$, then there is nothing to prove.

Let char $R = n \neq 0$, then n is the **least** positive integer such that $na = 0$ for all $a \in R$. We shall prove that n is prime. If n is not prime, then

$n = lm$, for some integers l and m ; $1 < l, m < n$.

Now $na = 0 \Rightarrow (lm)\,a = 0 \Rightarrow (lm)\,ab = 0b = 0,\ b \in R$

$\Rightarrow$ $ab + ab + ... + ab = 0\ \forall\ a, b \in R$

(lm times)

$\Rightarrow (a + a + ... + a)\,(b + b + ... + b) = 0\ \forall\ a, b \in R$

(l times, m times)

$\Rightarrow$ $(la)\,(mb) = 0\ \forall\ a, b \in R.$ ...(1)

Since R is an integral domain, it follows from (1) that

$la = 0\ \forall\ a \in R$ or $mb = 0\ \forall\ b \in R$,

where $1 < l < n$, $1 < m < n$.

The above two statements contradict the fact that n is the least positive integer such that $na = 0\ \forall\ a \in R$. Hence n must be a prime number.

Corollary. *The characteristic of a field is either zero or a prime number.*

Proof. Every field is an integral domain and so the result follows.

Ex. 1. *Define the characteristic of an integral domain. Prove that the characteristic of an integral domain, if finite, must be a prime number. What is the characteristic of J_p, the ring of integers modulo a prime number p ? Justify your answer.* [D.U., 1999]

Hint. Let char $R = m$ (finite). Then there exists a smallest positive integer n such that $na = 0\ \forall a \in R$. Now proceed like Theorem 1.8.1.

Since p is prime, J_p is an integral domain. Hence char $J_p = p$, since p is the smallest prime number such that $pa = 0\ \forall\ a \in J_p$.

Ex. 2. *Define the characteristic of a ring. What is the characteristic of J_n, the ring of integers modulo, n being any positive integer ?* [D.U., 1996]

Hint. $J_n = \{0, 1, 2, \ldots, n-1\}$, char $J_n = n$.

Ex. 3. *Define characteristic of a ring R. What does it have to do with $(R, +)$, the additive structure of R ?* [D.U., 1998]

Hint. If char $R = n$, then n is the least positive integer such that $na = 0\ \forall\ a \in R \Rightarrow o(a) = n\ \forall\ a \in (R, +)$. Hence $o(a) =$ char R, for all $a \neq 0 \in (R, +)$.

Theorem 1.8.2. *Prove that order of a finite field F is p^n, for some prime p and some positive integer n.*

Proof. Firstly, we show that char $F \neq 0$. Let, if possible, char $F = 0$. By definition,

$$na \neq 0\ \forall\ a \neq 0 \in F \quad \text{and} \quad \forall\ n \in \mathbf{N}. \qquad \ldots(1)$$

It follows that $a, 2a, 3a, \ldots$ belong to F.

Since F is finite, we must have

$ia = ja$ for some positive integers i and j, $i > j$

$\Rightarrow$ $(i-j)a = 0$, where $i - j > 0$.

This contradicts (1) and so char $F \neq 0$.

We know that the characteristic of a field is either zero or a prime number. Since char $F \neq 0$, so char $F = p$, p being some prime number.

Thus p is the smallest positive integer such that $pa = 0\ \forall\ a \in F$

$\Rightarrow$ $o(a) = p$, treating $(F, +)$ as a group.

Since $(F, +)$ is a finite group and $a \in F$, by Lagrange's theorem,

$o(a)$ divides $o(F)$,

$\Rightarrow$ p divides $o(F)$, where p is prime.

Hence $o(F) = p^n$, for some positive integer n.

Corollary. *If R is a finite (non-zero) integral domain, then $o(R) = p^n$, where p is a prime number and n is a positive integer.*

Proof. The result follows, since every finite integral domain is a field.

EXAMPLES

Example 1.8.1. *Let R be a non-zero ring such that $x^2 = x$ for all $x \in R$. Prove that R is a commutative ring of characteristic 2.*

Solution. Refer to Example 1.3.8. Since $x^2 = x\ \forall\ x \in R$, R is commutative and further $2x = 0\ \forall\ x \in R$. [See equation (2) of Example 1.3.8]

Hence char $R = 2$.

Example 1.8.2. *Let R be a commutative ring of characteristic 2. Prove that : $(a+b)^2 = a^2 + b^2 = (a-b)^2\ \forall\ a, b \in R$.*

Solution. Since R is commutative, $(a \pm b)^2 = a^2 \pm 2ab + b^2$.

Hence $(a \pm b)^2 = a^2 \pm 0 \cdot b + b^2 = a^2 + b^2$,

since char $R = 2 \Rightarrow 2a = 0\ \forall\ a \in R$.

Example 1.8.3. *If F is a field of characteristic p, p a prime : then*

$$(a+b)^p = a^p + b^p\ \ \forall\ a, b \in F.$$

Solution. Since char $F = p$, $px = 0\ \forall\ x \in F$. ...(1)

Since F is a field, we can write

$$(a+b)^p = a^p + pa^{p-1}b + \frac{1}{2!}p(p-1)a^{p-2}b^2 + \ldots + pab^{p-1} + b^p$$

$$= a^p + (pb)a^{p-1} + \frac{1}{2!}(p-1)a^{p-2} \cdot b(pb) + \ldots + (pa)b^{p-1} + b^p$$

$$= a^p + b^p, \text{ using (1).}$$

Example 1.8.4. *Let R be a ring with characteristic n. Suppose $ma = 0$ for all $a \in R$ and for some positive integer m. Show that n divides m. Determine characteristic of $\mathbf{Z}_n$.* [D.U., 2000]

Solution. Since char $R = n$, n is the *least* positive integer such that $na = 0\ \forall\ a \in R$. It is given that $ma = 0\ \forall\ a \in R$ and for some positive integer m. By division algorithm, there exist integers q and r such that $m = nq + r$, where $r = 0$ or $0 < r < n$. Consider the case $0 < r < n$.

We have $0 = ma = (nq + r)a = q(na) + ra = 0 + ra = ra$.

$\therefore$ $ra = 0,\ \forall\ a \in R$; where r is a positive integer $< n$.

This is a contradiction to the fact that char $R = n$. Consequently, $r = 0$ and so $m = nq \Rightarrow n$ divides m.

(*ii*) We know $\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$. Clearly, n is the least positive integer such that $na = 0$ in $\mathbf{Z}_n$, $\forall\ a \in \mathbf{Z}_n$. Hence char $\mathbf{Z}_n = n$.

Example 1.8.5. (*i*) *If D is an integral domain and if $na = 0$ for some $a \neq 0$ in D and some integer $n \neq 0$, prove that D is of finite characteristic.* [D.U., 1998, 95]

(*ii*) *What is the relation between the characteristic of D and the number n ?* [D.U., 1995]

Solution. We are given that $na = 0$ for some $a \neq 0 \in D$

$\Rightarrow (na)x = 0x = 0\ \forall\ x \in D$

$\Rightarrow (a + a + \ldots + a)x = 0\ \ \forall\ \ x \in D$

(n times)

$\Rightarrow ax + ax + \ldots + ax = 0\ \ \forall\ \ x \in D$

(n times)

$\Rightarrow a(x + x + \ldots + x) = 0\ \ \forall\ \ x \in D$

$\Rightarrow a(nx) = 0\ \ \forall\ \ x \in D$

$\Rightarrow \quad a = 0$ or $nx = 0 \quad \forall \quad x \in D$, since D is an integral domain.

$\Rightarrow \quad nx = 0 \quad \forall \quad x \in D$, since $a \neq 0$.

Hence the characteristic of D is finite.

(ii) If char $D = m$, then m is the smallest positive integer such that $mx = 0 \ \forall \ x \in D$. It follows that m divides n [see Example 1.8.4]. Hence char D divides n.

Example 1.8.6. *Prove that a finite integral domain has finite characteristic. Give an example of an integral domain which has an infinite number of elements, yet is of finite characteristic.* [D.U., 1997]

Solution. Let D be a finite integral domain. Let char $D = 0$. Then

$$na \neq 0 \ \forall \ a \neq 0 \in D \quad \text{and} \quad \forall \ n \in \mathbf{N}. \qquad \ldots(1)$$

It follows that $a, 2a, 3a, \ldots$ all belong to D.

Since D is finite, we must have $ia = ja$ for some positive integers i and j, $i > j$. Then $(i - j)\,a = 0$, where $i - j > 0$.

This contradicts (1) and so char $D \neq 0$.

We know that the characteristic of any integral domain is either zero or a prime number. Since char $D \neq 0$, therefore

$$\text{char } D = p \text{ (finite)}, \ p \text{ is some prime.}$$

(ii) Let $F = \mathbf{Z}_p = \{0, 1, 2, \ldots, p-1\}$ be the ring of integers modulo p. Then F is an integral domain of characteristic p *i.e.*, $pa = 0 \ \forall \ a \in \mathbf{Z}_p$. $\ldots(2)$

Let $F[x]$ be the ring of polynomials over F. Since F is an integral domain, so $F[x]$ is an integral domain having infinite number of elements with finite characteristic p.

Notice that if $f(x) = a_0 + a_1 x + \ldots + a_r x^r \in F[x]$, then by (2),

$$pf(x) = pa_0 + pa_1 x + \ldots + pa_r x^r = 0 \ \forall \ f(x) \in F[x].$$

Example 1.8.7. *Give an example of an infinite ring having finite characteristic.*

Hint. Refer to Example 1.8.6.

Example 1.8.8. *Show that each non-zero element of an integral domain D, regarded as a member of the additive group of D, is of the same order.*

Solution. Let a be any non-zero element of the additive group $(D, +)$ and let the order of a be n. Then n is the least positive integer such that $na = 0$

$$\Rightarrow \quad (na)\,x = 0x = 0 \quad \forall \quad x \in D$$

$$\Rightarrow (a + a + \ldots + a)\,x = 0 \quad \forall \quad x \in D$$

(n times)

$$\Rightarrow ax + ax + \ldots + ax = 0 \quad \forall \quad x \in D$$

(n times)

$$\Rightarrow a\,(x + x + \ldots + x) = 0 \quad \forall \quad x \in D$$

(n times)

$$\Rightarrow \quad a\,(nx) = 0 \quad \forall \quad x \in D.$$

$$\Rightarrow \quad nx = 0 \quad \forall \quad x \in D, \text{ since } a \neq 0 \in D$$

Hence $\quad o(x) = n \quad \forall \quad x \neq 0 \in D.$

Example 1.8.9. *Let R be a non-zero ring such that $x^3 = x$ for all $x \in R$. Prove that R is a commutative ring of characteristic 6.*

Solution. Refer to Example 1.6.9. R is a commutative ring such that

$$6x = 0 \ \forall \ x \in R. \quad \text{Hence char } R = 6.$$

Example 1.8.10. *Prove that if F is a finite field, its characteristic must be a prime number p and F contains p^n elements for some integer n. Further prove that if $a \in F$, then $a^{p^n} = a$.*

Solution. We know $o(F) = p^n$ [See Theorem 1.8.2].

Since non-zero elements of F (which are $p^n - 1$ in number) form a multiplicative group, by Lagrange's theorem,

$$a \in F \ \Rightarrow \ a^{p^n - 1} = e \text{ (multiplicative identity of } F)$$

Hence $\quad a \,.\, a^{p^n - 1} = a \,.\, e$ or $a^{p^n} = a, \ a \in F.$

1.9 Ideals in a Ring

Definition 1. *A non-empty subset S of a ring R is called a* **left ideal** *of R, if*

(i) $(S, +)$ *is a subgroup of* $(R, +)$

i.e., $a \in S$ *and* $b \in S \Rightarrow a - b \in S$.

(ii) $a \in S$ *and* $r \in R \Rightarrow ra \in S$.

Definition 2. *A non-empty subset S of a ring R is called a* **right ideal** *of R, if*

(i) $(S, +)$ *is a subgroup of* $(R, +)$

i.e., $a \in S$ *and* $b \in S \Rightarrow a - b \in S$.

(ii) $a \in S$ *and* $r \in R \Rightarrow ar \in S$.

Definition 3. *A non-empty subset S of a ring R is called an* **ideal** *or a* **two-sided ideal** *of R, if*

(i) $(S, +)$ *is a subgroup of* $(R, +)$

i.e., $a \in S$ *and* $b \in S \Rightarrow a - b \in S$.

(ii) $a \in S$ *and* $r \in R \Rightarrow ar \in S$ *and* $ra \in S$.

In other words, a non-empty subset S of a ring R is an ideal of R, if S is both a left and right ideal of R.

Remark 1. *In a commutative ring, every left ideal or right ideal is a two-sided ideal.*

2. *Since each ideal S of a ring R is a subgroup of the additive group $(R, +)$, $0 \in S$.*

Example 1.9.1. *If $\mathbf{Z}$ be the ring of integers and n be any integer, then $(n) = \{nx : x \in \mathbf{Z}\}$ is an ideal of $\mathbf{Z}$.*

Solution. Let $a, b \in (n)$, so that $a = nx$ and $b = ny$, for some integers x and y. Then $a - b = nx = n\,(x - y)$, where $x - y \in \mathbf{Z}$.

Thus $\quad a - b \in (n)$. Again for any integer r, we see that

$ra = r(nx) = (rn)x = (nr)x = n(rx)$, where rx is an integer.

$\therefore$ $ra \in (n)$. Now $ar = ra \in (n)$.

Hence (n) is an ideal of $\mathbf{Z}$.

Note. $(2) = \{..., -4, -2, 0, 2, 4, ...\}$,

$(3) = \{..., -6, -3, 0, 3, 6, ...\}$ etc. are ideals in $\mathbf{Z}$.

Theorem 1.9.1. *Every ideal of a ring R is a subring of R, but the converse need not be true.*

Proof. *(i)* Let S be an ideal of the given ring R.

Let $a, b \in S$. By definition of an ideal, $a - b \in S$.

Further $a \in S$ and $b \in S \subseteq R$ *(i.e., $b \in R$)* $\Rightarrow$ $ab \in S$.

Hence S is a subring of R (Theorem 1.6.1).

(ii) The converse of part *(i)* is not true. The set $\mathbf{Z}$ of integers is a subring of the ring $\mathbf{Q}$ of rational numbers. However, $\mathbf{Z}$ is not an ideal of $\mathbf{Q}$, since $3 \in \mathbf{Z}, \frac{1}{4} \in \mathbf{Q}$, but $3 \cdot \frac{1}{4} = \frac{3}{4} \notin \mathbf{Z}$.

Theorem 1.9.2. *The intersection of two ideals of a ring R is an ideal of R.*

Proof. Let A and B be any two ideals of R.

We have to show that $A \cap B$ is an ideal of R.

We know that $0 \in A$ and $0 \in B$ and so $0 \in A \cap B$.

Thus $A \cap B$ is non-empty.

Let $x, y \in A \cap B$. Then $x, y \in A$ and $x, y \in B$.

Since A is an ideal of R, $x - y \in A$.

Similarly, $x - y \in B$ and so $x - y \in A \cap B$.

Let $r \in R$. Since A is an ideal of R, $rx \in A$ and $xr \in A$.

Similarly, $rx \in B$ and $xr \in B$.

So $rx \in A \cap B$ and $xr \in A \cap B$ $\forall$ $r \in R$ and $\forall$ $x \in A \cap B$.

Hence $A \cap B$ is an ideal of R.

Remark. *The union of two ideals of a ring R need not be an ideal of R.*

We know

$$A = (2) = \{..., -4, -2, 0, 2, 4, ...\}$$

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

are two ideals in the ring $\mathbf{Z}$ of integers.

Now $A \cup B = \{..., -6, -4, -3, -2, 0, 2, 3, 4, 6, ...\}$

It is easy to see that $3 \in A \cup B$ and $2 \in A \cup B$, but

$3 - 2 = 1 \notin A \cup B$. Hence $A \cup B$ is not an ideal of $\mathbf{Z}$.

Theorem 1.9.3. *The sum of two ideals of a ring R is an ideal of R.*

Or

If A and B are two ideals of a ring R, then $A + B = \{a + b : a \in A, b \in B\}$ is an ideal of R.

Proof. Since $0 \in A$ and $0 \in B$, $0 = 0 + 0 \in A + B$.

Thus $A + B$ is non-empty.

Let $x, y \in A + B$. Then $x = a_1 + b_1$, $y = a_2 + b_2$, for some $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Now

$$x - y = (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2). \quad ...(1)$$

Since A is an ideal of R, $a_1 \in A$ and $a_2 \in A \Rightarrow a_1 - a_2 \in A$.

Similarly, $b_1 - b_2 \in B$. From (1), it follows that $x - y \in A + B$.

Let $r \in R$. Then $rx = r(a_1 + b_1) = ra_1 + rb_1$. ...(2)

Since A is an ideal of R, so $a_1 \in A$ and $r \in R \Rightarrow ra_1 \in A$.

Similarly, $rb_1 \in B$. From (2), it follows that $rx \in A + B$ $\forall$ $r \in R$ and $\forall$ $x \in A + B$. Similarly, $xr \in A + B$.

Hence $A + B$ is an ideal of R.

Theorem 1.9.4. (Product of Two ideals)

If A and B are two ideals of a ring R, then their product AB defined as

$$AB = \left\{ a_1b_1 + a_2b_2 + ... + a_nb_n : a_i \in A, b_i \in B, 1 \le i \le n \text{ and } n \text{ being a positive integer} \right\}$$

is an ideal of R. [D.U., 1994]

Proof. Since A and B are ideals of R, $0 \in A$ and $0 \in B$ and so $0 = 0.0 \in AB$. Thus AB is non-empty.

Let x and y be any two elements of AB. Then

$$x = a_1b_1 + ... + a_nb_n \text{ and } y = \alpha_1\beta_1 + ... + \alpha_m\beta_m;$$

where $a_i \in A, \alpha_j \in A, b_i \in B, \beta_j \in B$; $1 \le i \le n$, $1 \le j \le m$.

Now $x - y = (a_1b_1 + ... + a_nb_n) - (\alpha_1\beta_1 + ... + \alpha_m\beta_m)$

$= a_1b_1 + ... + a_nb_n - \alpha_1\beta_1 - ... - \alpha_m\beta_m$

$= a_1b_1 + ... + a_nb_n + (-\alpha_1)\beta_1 + ... + (-\alpha_m)\beta_m$,

where $-\alpha_j \in A$ for each j, since A is an ideal of R.

It follows that $x - y \in AB$. For any $r \in R$ and $x \in AB$, we have

$rx = r(a_1b_1 + ... + a_nb_n) = r(a_1b_1) + .. + r(a_nb_n)$

$= (ra_1)b_1 + ... + (ra_n)b_n$, where $ra_i \in A$ for each i.

(Notice that $r \in R$ and $a_i \in A \Rightarrow ra_i \in A$, as A is a **left ideal of R**)

Consequently, $rx \in AB$.

Again, $xr = (a_1b_1 + ... + a_nb_n)r = (a_1b_1)r + ... + (a_nb_n)r$

$= a_1(b_1r) + ... + a_n(b_nr)$, where $b_ir \in B$ for each i.

(Notice that $r \in R$ and $b_i \in B \Rightarrow b_ir \in B$, as B is a **right ideal of R**).

Consequently, $xr \in AB$. Hence AB is an ideal of R.

Remark. On carefully examining the above proof, we observe that $rx \in AB$ $\forall$ $r \in R$, $x \in AB$; if A is a **left ideal** of R and $xr \in AB$ $\forall$ $r \in R$, $x \in AB$, if B is a **right ideal** of R.

Hence Theorem 1.9.4 can be restated as :

If A is a left ideal and B is a right ideal of a ring R, then AB is a two-sided ideal of R.

Corollary 1. *If A and B are two ideals of a ring R, then*

$$AB \subseteq A \cap B.$$

Proof. We know that AB and $A \cap B$ are ideals of R.

Let x be any element of AB. Then $x = a_1b_1 + \ldots + a_nb_n$, for some $a_i \in A, b_i \in B$; $1 \le i \le n$.

Now $a_i \in A, b_i \in R \Rightarrow a_ib_i \in A$, as A is a right ideal of R

$\Rightarrow a_1b_1 + \ldots + a_nb_n \in A \Rightarrow x \in A$, as A is an ideal of R.

Again $a_i \in R, b_i \in B \Rightarrow a_ib_i \in B$, as B is a left ideal of R

$\Rightarrow a_1b_1 + \ldots + a_nb_n \in B \Rightarrow x \in B$, as B is an ideal of R.

Hence $x \in A \cap B$ and so $AB \subseteq A \cap B$.

Corollary 2. *If A and B are two ideals of a ring R, then*

$$AB \subseteq A + B.$$ [D.U., 1994]

Proof. We know that $A + B$ and AB are ideals of R.

Let x be any element of AB. Then $x = a_1b_1 + a_2b_2 + \ldots + a_nb_n$, for some $a_i \in A, b_i \in B$; $1 \le i \le n$.

Now $a_1 \in A, b_1 \in R, \Rightarrow a_1b_1 \in A$, as A is a right ideal of R.

Again $a_i \in R, b_i \in B \Rightarrow a_ib_i \in B$, as B is a left ideal of R, $2 \le i \le n$

$\Rightarrow a_2b_2 + \ldots + a_nb_n \in B$, as B is an ideal of R.

$\therefore a_1b_1 + (a_2b_2 + \ldots + a_nb_n) \in A + B \Rightarrow x \in A + B \quad \forall \ x \in AB.$

Hence $AB \subseteq A + B$.

Ex. *Let U and V be two ideals of a ring R. Define $U + V$ and UV. Prove that $U + V$ as well as UV are ideals of R. Show that $UV \subseteq U + V$.* [D.U., 1994]

EXAMPLES

Example 1.9.2. *Show that the set*

$$S = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \text{ are integers} \right\}$$

is a left ideal in the ring M_2 of 2×2 matrices over integers. Further show that S is not a right ideal in M_2.

Solution. Clearly S is non-empty, since $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S$.

Let $X, Y \in S$; so that $X = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, Y = \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}$; $a, b, c, d \in \mathbf{Z}$.

Then $X - Y = \begin{pmatrix} a-c & 0 \\ b-d & 0 \end{pmatrix} \in S$.

Let $A \in M_2$, so that $A = \begin{pmatrix} p & q \\ r & s \end{pmatrix}, p, q, r, s \in \mathbf{Z}$.

Then $AX = \begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} pa+qb & 0 \\ ra+sb & 0 \end{pmatrix} \in S$.

Hence S is a left ideal of M_2.

Also S is not a right ideal of M_2, since

$$P = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \in S \text{ and } T = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \in M_2,$$

but $$PT = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \notin S.$$

Example 1.9.3. *Show that the set*

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \text{ are integers} \right\}$$

is a right ideal of M_2, the ring of 2×2 matrices over integers, which is not a left ideal of M_2.

Solution. Let $X, Y \in S$, so that

$$X = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, Y = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \Rightarrow X - Y = \begin{pmatrix} a-c & b-d \\ 0 & 0 \end{pmatrix} \in S.$$

(Here a, b, c, d are some integers)

For any $A = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in M_2$, we see that

$$XA = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap+br & aq+bs \\ 0 & 0 \end{pmatrix} \in S.$$

Hence S is a right ideal of M_2

Consider $P = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \in S$ and $T = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \in M_2$.

Then $$TP = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \notin S.$$

This shows that S is not a left ideal of M_2.

Example 1.9.4. *If S be an ideal of a ring R and $1 \in S$, prove that $S = R$.* [D.U., 1997]

Solution. We have $1 \in S$. For any $r \in R$; $1r \in S$, as S is an ideal of R. Thus $r \in S \ \forall \ r \in R$ and so $R \subseteq S$. Obviously, $S \subseteq R$. Hence $S = R$.

Example 1.9.5. *If F is a field, prove its only ideals are (0) and F itself.* [D.U., 1997]

Solution. Let U be any ideal of F.

If $U = (0)$, there is nothing to prove.

Let $U \neq (0)$. We shall show that $U = F$.

Since $U \neq (0)$, so there exists some $u \neq 0 \in U \subseteq F$.

Since F is a field and $u \neq 0 \in F$, $u^{-1} \in F$ and $uu^{-1} = u^{-1}u = 1$.

Since U is an ideal of F, $u \in U$ and $u^{-1} \in F \Rightarrow uu^{-1} = 1 \in U$.

For any $x \in F$ and $1 \in U$, $1x = x \in U$, since U is an ideal of F.

Thus $x \in U \; \forall \; x \in F \Rightarrow F \subseteq U$. Obviously, $U \subseteq F$.

Hence $U = F$.

Example 1.9.6. *(a) Let R be a ring with unity. Prove that no proper ideal of R can contain an invertible element of R.* [D.U., 1999, 96]

(b) Deduce that a field F has no proper ideals. [D.U., 1996]

Solution. *(a)* Let A be any proper ideal of R containing an invertible element a *i.e.*, $a \in A$, where $aa^{-1} = a^{-1}a = 1$.

Since $a^{-1} \in R$ and $a \in A$, $1 = a^{-1}a \in A$. ($\because$ A is an ideal of R)

For any $r \in R$ and $1 \in A$, $1 \cdot r = r \in A$ ($\because$ A is an ideal of R)

$\therefore r \in A \;\; \forall \;\; r \in R$ *i.e.*, $R \subseteq A$. Obviously, $A \subseteq R$.

Hence $A = R$ *i.e.*, A is not a proper ideal of R, which is a contradiction. Hence the result.

(b) Let A be any ideal of F. If $A = (0)$, there is nothing to prove. Let $A \neq (0)$. Then there exists some element $a \neq 0 \in A$ *i.e.*, $a \neq 0 \in F$. Since F is a field, a is invertible and $a \in A$. By part *(a)*, $A = F$. Hence F has no proper ideals.

Example 1.9.7. *Let R be a ring and $a \in R$. Show that the set $S = \{r \in R : ra = 0\}$ is a left ideal of R.*

Solution. Since $0a = 0$, $0 \in S$. Thus S is non-empty.

Let $x, y \in S$, so that $xa = 0$ and $ya = 0$.

Now $(x - y)a = xa - ya = 0$. So $x - y \in S$.

For any $r \in R$ and $x \in S$, $(rx)a = r(xa) = r0 = 0$. So $rx \in S$.

Hence S is a left ideal of R.

Example 1.9.8. *Let R be the ring of all real valued, continuous functions on $[0, 1]$. Show that the set $S = \{f \in R : f(\frac{1}{2}) = 0\}$ is an ideal of R.*

Solution. Let $f, g \in S$. Then $f(\frac{1}{2}) = 0$ and $g(\frac{1}{2}) = 0$. ...(1)

Consider $(f - g)(\frac{1}{2}) = f(\frac{1}{2}) - g(\frac{1}{2}) = 0 - 0 = 0$, using (1).

$\therefore \quad (f - g)(\frac{1}{2}) = 0 \Rightarrow f - g \in S$.

Let $f \in S$ and $h \in R$. Then

$$(fh)(\tfrac{1}{2}) = f(\tfrac{1}{2})\, h(\tfrac{1}{2}) = 0 \cdot h(\tfrac{1}{2}) = 0,$$

and $$(hf)(\tfrac{1}{2}) = h(\tfrac{1}{2}) f(\tfrac{1}{2}) = h(\tfrac{1}{2}) \cdot 0 = 0.$$

Thus $fh, hf \in S \; \forall f \in S$ and $h \in R$. Hence S is an ideal of R.

Example 1.9.9. *If U is an ideal of R, then prove that $r(U) = \{x \in R : xu = 0 \; \forall \; u \in U\}$ is an ideal of R.*

Solution. Since $0u = 0 \; \forall \; u \in U$, so $0 \in r(U)$ and thus $r(U)$ is non-empty. Let $x, y \in r(U)$; so that $xu = 0$ and $yu = 0 \; \forall \; u \in U$. ...(1)

We have $(x - y)u = xu - yu = 0 \; \forall \;\; u \in U$, by (1).

Thus $x - y \in r(U)$.

Let $a \in R$ and $x \in r(U)$, so that $xu = 0 \; \forall \; u \in U$ ...(2)

Now $(ax)u = a(xu) = a0 = 0 \; \forall \; u \in U$, by (2).

$\therefore \quad (ax)u = 0 \; \forall \; u \in U \Rightarrow ax \in r(U)$.

Again $(xa)u = x(au) = xy$, where $y = au$.

Since U is an ideal of R, so $a \in R$ and $u \in U \Rightarrow au \in U \Rightarrow y \in U$. ...(3)

From (2) and (3), $xy = 0 \Rightarrow x(au) = 0 \Rightarrow (xa)u = 0$.

Thus $(xa)u = 0 \;\; \forall \;\; u \in U \Rightarrow xa \in r(U)$.

Hence $r(U)$ is an ideal of R.

Note. It may be observed that in (3), we have actually used the fact that U is a left ideal of R only. Thus we have another equivalent statement of Example 1.9.9 as follows :

Example 1.9.10. *If R is a ring and L is a left ideal of R. Then $\lambda(L) = \{x \in R : xa = 0 \; \forall \; a \in L\}$ is a two-sided ideal of R.* [D.U., 1995]

Example 1.9.11. *If U is an ideal of R, then prove that*

$$[R : U] = \{x \in R : rx \in U \text{ for every } r \in R\}$$

is an ideal of R and that it contains U.

Solution. Since U is an ideal of R, so $0 \in U$ *i.e.*, $r0 \in U \; \forall \; r \in R$ ($\because$ $r0 = 0$). Thus $0 \in [R : U]$ and so $[R : U]$ is non-empty.

Let $x, y \in [R : U]$, so that $rx \in U$ and $ry \in U \; \forall \; r \in R$. ...(1)

It follows that $rx - ry \in U \;\; \forall \;\; r \in R$, as U is an ideal of R.

Now $r(x - y) = rx - ry \in U \;\; \forall \;\; r \in R \Rightarrow x - y \in [R : U]$.

Using (1), $(ra)x \in U$, since $ra \in R$.

Thus, $r(ax) = (ra)x \in U \;\; \forall \;\; r \in R \Rightarrow ax \in [R : U]$.

Since U is an ideal of R, so $rx \in U$ and $a \in R$ implies that

$(rx)a \in U \Rightarrow r(xa) \in U \;\; \forall \;\; r \in R \Rightarrow xa \in [R : U]$.

Hence $[R : U]$ is an ideal of R.

Now we show that $U \subseteq [R : U]$.

Let $x \in U$. Then $rx \in U \; \forall \; r \in R$, as U is an ideal of R.

Now $rx \in U \;\; \forall \; r \in R$ implies that $x \in [R : U] \Rightarrow U \subseteq [R : U]$.

Hence $[R : U]$ is an ideal of R containing U.

Example 1.9.12. *Prove that $Z(R)$, the centre of a ring R, is only a subring of R and need not be an ideal of R.* [D.U., 1995]

Solution. By definition, $Z(R) = \{a \in R : xa = ax \; \forall \; x \in R\}$.

By Theorem 1.6.3, $Z(R)$ is a subring of R.

Let M_2 be the ring of all 2×2 matrices over the integers.

For any $X=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in M_2$ and $A=\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}\in M_2$, we see that

$$AX=\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} ap & bp \\ cp & dp \end{pmatrix}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}=XA.$$

Hence $Z(M_2)=\left\{\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}: p \text{ is an integer}\right\}$.

We proceed to show that $Z(M_2)$ is **not** an ideal of M_2.

For $S=\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\in M_2$, $A=\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\in Z(M_2)$, we have

$$SA=\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}=\begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix}\notin Z(M_2).$$

Hence $Z(M_2)$ is not an ideal of M_2.

Example 1.9.13. *Let N be the set of all nilpotent elements in a commutative ring R. Show that N is an ideal of R. Further prove that there are no non-zero nilpotent elements in the quotient ring R/N.*

[D.U., 1999, 97, 96]

Solution. *(i)* The set of all nilpotent elements of R is

$$N=\{a\in R: a^n=0 \text{ for some positive integer } n\}.$$

Let $a, b\in N$. Then $a^n=0$, $b^m=0$ for some $n, m\in \mathbf{Z}^+$. ...(1)

Since R is commutative, therefore

$$(a-b)^{m+n}=a^{m+n}-(m+n)_{c_1}a^{m+n-1}.b+(m+n)_{c_2}a^{m+n-2}.b^2$$
$$-\ldots+(-1)^{m+n}b^{m+n}$$
$$=a^m.a^n-(m+n)_{c_1}a^{m-1}.a^n+\ldots+(-1)^{m+n}.b^m.b^n$$
$$=0, \text{ using (1).}$$

Thus $a-b\in N$. Let $a\in N$ and $r\in R$. Then

$$(ra)^n=r^n a^n, \text{ since } R \text{ is commutative}$$
$$=r^n.0=0, \text{ using (1). Thus } ra\in N$$

Similarly, $(ar)^n=a^n r^n=0 \Rightarrow ar\in N$. Hence N is an ideal of R.

(ii) Since N is an ideal of R, the quotient ring is

$$\frac{R}{N}=\{r+N: r\in R\}. \qquad \text{(See Chapter 2)}$$

Let $r+N\in R/N$ be any nilpotent element in R/N.

Then $(r+N)^n=\bar{0}$, for some positive integer n

$\Rightarrow$ $(r+N)^n=N$ $(\because \bar{0}\in R/N \Rightarrow \bar{0}=N)$

$\Rightarrow r^n+N=N$, by the multiplication composition in R/N.

$\Rightarrow r^n\in N$

$\Rightarrow (r^n)^m=0$, for some positive integer m

$\Rightarrow r^{nm}=0 \Rightarrow r$ is nilpotent

$\Rightarrow r\in N \Rightarrow r+N=N \Rightarrow r+N=\bar{0}$.

Hence $\bar{0}=N$ is the only nilpotent element of R/N *i.e.*, R/N has no non-zero nilpotent elements.

Ex. *Show that $0+N$ is the only nilpotent element of R/N.*

[D.U., 1996]

Hint. $\bar{0}=N=0+N$.

Example 1.9.14. *Let A and B be any two ideals of a ring R. Show that $A+B$ is an ideal of R generated by $A\cup B$.* [D.U., 1998]

Definition. (Ideal generated by a set) *Let S be any subset of a ring R. An ideal A of R is said to be* **generated** *by S, if*

(i) $S\subseteq A$

(ii) If I is any ideal of R such that $S\subseteq I$, then $A\subseteq I$.

We write the ideal A as $A=\langle S\rangle$. Indeed, $\langle S\rangle$ is the smallest ideal containing S.

Solution. We have to show that $A+B=\langle A\cup B\rangle$.

By Theorem 1.9.3, $A+B$ is an ideal of R.

For any $a\in A$, $a=a+0\in A+B$. Thus $A\subseteq A+B$.

Similarly, $B\subseteq A+B$. Consequently, $A\cup B\subseteq A+B$. ...(1)

Let I be an any ideal of R such that $A\cup B\subseteq I$. ...(2)

We shall prove that $A+B\subseteq I$. ...(3)

Let $x\in A+B$ be arbitrary. Then $x=a+b$, for $a\in A$, $b\in B$.

Since $A\subseteq A\cup B$ and $B\subseteq A\cup B$, so $a, b\in A\cup B$

$\Rightarrow a, b\in I$ $(\because A\cup B\subseteq I)$

$\Rightarrow a+b\in I$, as I is an ideal of R.

$\Rightarrow x\in I$ and so (3) is proved.

From (1), (2) and (3) ; $A+B=\langle A\cup B\rangle$.

Example 1.9.15. *If A and B are two ideals of a ring R, prove that $A\cup B$ is an ideal of R if any only if either $A\subseteq B$ or $B\subseteq A$.*

Solution. *Condition is sufficient*

Let $A\subseteq B$. Then $A\cup B=B$, which is an ideal of R.

Let $B\subseteq A$. Then $A\cup B=A$, which is an ideal of R.

Condition is necessary

Let $A\cup B$ be an ideal of R. We have to show that either $A\subseteq B$ or $B\subseteq A$. Suppose the conclusion is not true. Then $A\nsubseteq B$ and $B\nsubseteq A$. Consequently, there exists some $x\in A$ such that $x\notin B$ and some $y\in B$ such that $y\notin A$.

Now $x \in A,\ y \in B \Rightarrow x, y \in A \cup B \Rightarrow x - y \in A \cup B$,
since $A \cup B$ is an ideal of R. We have
$x - y \in A \cup B \Rightarrow x - y \in A$ or $x - y \in B$.
If $x - y \in A$, then $x \in A \Rightarrow x - (x - y) \in A$, as A is an ideal of R.
$\therefore$ $y \in A$, which is a contradiction.
If $x - y \in B$, then $x = (x - y) + y \in B$, which is again a contradiction.
Hence either $A \subseteq B$ or $B \subseteq A$.

Example 1.9.16. *Let A and B be two ideals of a commutative ring R with unity such that $A + B = R$. Show that $AB = A \cap B$.*

Solution. Since A and B are two ideals of R, AB is an ideal of R and
$AB \subseteq A \cap B$. [See Theorem 1.9.4 and Cor. 1]
Conversely, let $x \in A \cap B$ be arbitrary. Since $R = A + B$ and $1 \in R$,
$1 \in A + B \Rightarrow 1 = a + b$, for some $a \in A, b \in B$.
so $x = x \cdot 1 = x(a + b) = xa + xb$. ...(1)
$\therefore$
Now $x \in A$ and $b \in B \Rightarrow xb \in AB$,
and $x \in B$ and $a \in A \Rightarrow ax \in AB \Rightarrow xa \in AB$,
since R is commutative.
$\therefore$ $xa + xb \in AB$, since AB is an ideal of R.
By (1), $x \in AB \ \forall\ x \in A \cap B$ and so $A \cap B \subseteq AB$.
Hence $AB = A \cap B$.

Remark. *Two ideals A and B of a ring R satisfying $A + B = R$ are called* **co-maximal ideals.**

Example 1.9.17. *If A, B and C are ideals of a ring R, prove that*
$$A(B + C) = AB + AC.$$

Solution. By the given hypothesis, $B + C$, AB, AC, $A(B + C)$ and $AB + AC$ are ideals of R.
For any $b \in B,\ b = b + 0 \in B + C$. ($\because 0 \in C$)
$\therefore$ $B \subseteq B + C$. Similarly, $C \subseteq B + C$
$\Rightarrow$ $AB \subseteq A(B + C)$ and $AC \subseteq A(B + C)$
$\Rightarrow$ $AB + AC \subseteq A(B + C)$. ...(1)
Conversely, let $x \in A(B + C)$ be arbitrary. Then
$x = a_1 t_1 + a_2 t_2 + .. + a_n t_n$, where $a_i \in A,\ t_i \in B + C$.
Since $t_i \in B + C,\ t_i = b_i + c_i$, for some $b_i \in B$ and $c_i \in C$.
$\therefore$ $x = a_1(b_1 + c_1) + a_2(b_2 + c_2) + ... + a_n(b_n + c_n)$
$= (a_1 b_1 + a_2 b_2 + ... + a_n b_n) + (a_1 c_1 + a_2 c_2 + ... + a_n c_n) \in AB + AC$
$\therefore$ $A(B + C) \subseteq AB + AC$. ...(2)
From (1) and (2) $A(B + C) = AB + AC$.

Example 1.9.18. *If A, B, C are ideals of a ring R such that $B \subseteq A$, prove that*
$$A \cap (B + C) = B + (A \cap C) = (A \cap B) + (A \cap C).$$

Solution. By the given hypothesis, $B + C$, $A \cap C$ and $A \cap (B + C)$, $B + (A \cap C)$ are also ideals of R.
Let $x \in A \cap (B + C)$ be arbitrary. Then $x \in A$ and $x \in B + C$.
We have $x \in B + C \Rightarrow x = b + c$, for some $b \in B, c \in C$.
Thus $b + c \in A$ ($\because x \in A$) and $b \in A$ ($\because B \subseteq A$)
$\Rightarrow$ $b + c - b \subseteq A$ ($\because A$ is an ideal of R)
$\Rightarrow$ $c \in A \Rightarrow c \in A \cap C$
$\therefore$ $x = b + c \Rightarrow x \in B + (A \cap C)$.
Consequently, $A \cap (B + C) \subseteq B + (A \cap C)$. ...(1)
Conversely, let $x \in B + (A \cap C)$ be arbitrary.
$\Rightarrow x = b_1 + c_1$, for some $b_1 \in B, c_1 \in A \cap C$
$\Rightarrow x \in B + C$, as $b_1 \in B$ and $c_1 \in C$.
Again $B \subseteq A \Rightarrow b_1 \in A$. Also $c_1 \in A$.
$\therefore$ $x = b_1 + c_1 \in A$, as A is an ideal of R.
Thus $x \in A$. Also $x \in B + C$.
$\therefore$ $x \in A \cap (B + C)$.
Consequently, $B + (A \cap C) \subseteq A \cap (B + C)$. ...(2)
From (1) and (2), we obtain
$$A \cap (B + C) = B + (A \cap C).$$
Since $B \subseteq A$, so $A \cap B = B$. Hence
$$A \cap (B + C) = B + (A \cap C) = (A \cap B) + (A \cap C).$$

Example 1.9.19. *If A, B be two ideals of a ring R, then $AB \subseteq A \cap B$. Give an example to show that there exist ideals A and B such that $AB \neq A \cap B$.*

Solution. By Corollary 1 of Theorem 1.9.4, $AB \subseteq A \cap B$.

Let $A = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbf{Z} \right\}$, $B = \left\{ \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} : c, d \in \mathbf{Z} \right\}$

Then A is a left ideal of M_2 and B is a right ideal of M_2 (M_2 being the ring of all 2×2 matrices over the integers). It follows that AB is an ideal of M_2 [See Theorem 1.9.4].

We have
$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad \\ bc & bd \end{pmatrix}.$$
Consequently, $AB = \left\{ \begin{pmatrix} p & q \\ r & s \end{pmatrix} : p, q, r, s \in \mathbf{Z} \right\}$.

However, $A \cap B = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in \mathbf{Z} \right\}$.

Hence $AB \neq A \cap B$.

For example, $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in AB$, but $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \subseteq A \cap B$.

Example 1.9.20. *If A is a left ideal and B is a right ideal of a ring R, then show that AB is a two-sided ideal of R. What can you say about BA?*

Solution. By Theorem 1.9.4, AB is a two-sided ideal of R.

(ii) Refer to the ideals A and B of M_2 as given in Example 1.9.19.

We see that $\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ac+bd & 0 \\ 0 & 0 \end{pmatrix}$.

Thus $BA = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in \mathbf{Z} \right\}$.

We take $S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in BA$ and $T = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in M_2$. Then

$ST = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \notin BA$ and $TS = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \notin BA$.

Hence BA is neither a left ideal nor a right ideal of M_2.

Example 1.9.21. *If A and B are ideals of a ring R, define*

$$A : B = \{r \in R : rB \subseteq A\},$$

where $$rB = \{rb : b \in B\}.$$

Show that $A : B$ is an ideal of R.

Solution. Let $r_1, r_2 \in A : B$. Then $r_1 B \subseteq A$ and $r_2 B \subseteq A$.

$\therefore$ $(r_1 - r_2)B = r_1 B - r_2 B \subseteq A$, since A is an ideal of R.

Thus $r_1 - r_2 \subseteq A : B$.

Let $r_1 \in A : B$ and $x \in R$. Then $r_1 B \subseteq A$ and

$(xr_1)B = x(r_1 B) \subseteq xA \subseteq A$, since A is an ideal of R.

$\therefore$ $xr_1 \in A : B$.

Again, $(r_1 x)B = r_1 (xB) \subseteq r_1 B \subseteq A$, since B is an ideal of R.

$\therefore$ $r_1 x \in A : B$. Hence $A : B$ is an ideal of R.

Example 1.9.22. *Let R be a commutative ring and let A be an ideal of R. Show that*

$$\sqrt{A} = \{x \in R : x^n \in A \text{ for some positive integer } n\}$$

is an ideal of R such that

(i) $A \subseteq \sqrt{A}$ *(ii)* $\sqrt{\sqrt{A}} = \sqrt{A}$

(iii) If R has unity and $\sqrt{A} = R$, then $A = R$.

Solution. Let $a, b \in \sqrt{A}$. Then $a^m \in A$ and $b^n \in A$, for some positive integers m and n. Since R is commutative,

$$(a-b)^{m+n} = a^{m+n} - (m+n)_{c_1} a^{m+n-1} b + \ldots + (-1)^{m+n} b^{m+n}$$
$$= a^m \cdot a^n - (m+n)_{c_1} a^m \cdot a^{n-1} b + \ldots + (-1)^{m+n} b^m \cdot b^n \in A,$$

since $a^m \in A$, $b^n \in A$ and A is an ideal of R.

Thus $a - b \in \sqrt{A}$. For any $r \in A$, $a \in \sqrt{A}$; we have

$(ra)^m = r^m a^m$, since R is commutative.

Again $r^m a^m \in A$, since $a^m \in A$, $r^m \in R$ and A is an ideal of R.

$\therefore$ $ra \in \sqrt{A}$. Similarly, $ar \in \sqrt{A}$.

Hence $\sqrt{A}$ is an ideal of R.

(i) Obviously, $A \subseteq \sqrt{A}$ $(\because x \in A \Rightarrow x^2 \in A$, as A is an ideal of $R)$

(ii) We have $\sqrt{\sqrt{A}} = \sqrt{S}$, where $S = \sqrt{A}$.

By part *(i)*, $S \subseteq \sqrt{S} \Rightarrow \sqrt{A} \subseteq \sqrt{\sqrt{A}}$.

Conversely, let $x \in \sqrt{\sqrt{A}} \Rightarrow x \in \sqrt{S} \Rightarrow x^n \in S$, for some $n \in \mathbf{N}$

$\Rightarrow x^n \in \sqrt{A} \Rightarrow (x^n)^m \in A$, for some $m \in \mathbf{N}$

$\Rightarrow x^{nm} \in A$, where $nm \in \mathbf{N}$

$\Rightarrow x \in \sqrt{A} \Rightarrow \sqrt{\sqrt{A}} \subseteq \sqrt{A}$.

Hence $\sqrt{\sqrt{A}} = \sqrt{A}$.

(iii) Let $1 \in R$ and $\sqrt{A} = R$. Then $1 \in \sqrt{A} \Rightarrow 1^n \in A$, for some positive integer $n \Rightarrow 1 \in A$ and A is an ideal of $R \Rightarrow 1 \cdot r \in A \ \forall \ r \in R \Rightarrow r \in A \ \forall \ r \in R \Rightarrow R \subseteq A$. Obviously, $A \subseteq R$. Hence $A = R$.

$\sqrt{A}$ is often called the **radical** of A. We also write $\sqrt{A}$ as $N(A)$.

Example 1.9.23. *Let R be a ring with unity. Show that*

$$\langle a \rangle = \{ \sum_{\text{finite}} xay : x, y \in R \}.$$ [D.U., 2000]

Solution. Let $S = \{ \sum_{\text{finite}} xay : x, y \in R \}$.

We have to show that S is the smallest ideal of R, which contains a. First of all, we show that S is an ideal of R. Let $\alpha, \beta \in S$.

Then $\alpha = x_1 a y_1 + \ldots + x_n a y_n$, $\beta = s_1 a t_1 + \ldots + s_m a t_m$;

where $x_i, y_i, s_j, t_j \in R$; $1 \leq i \leq n$, $1 \leq j \leq m$.

We observe that

$$\alpha - \beta = x_1 a y_1 + \ldots x_n a y_n + (-s_1) a t_1 + \ldots + (-s_m) a t_m \in S.$$

For any $r \in R$ and $\alpha \in S$, $r\alpha = (rx_1) a y_1 + \ldots + (rx_n) a y_n \in S$

and $\alpha r = x_1 a (y_1 r) + \ldots + x_n a (y_n r) \in S$, as $r x_i \in R$ and $y_j r \in R$.

Hence S is an ideal of R containing a, since $a = 1 \cdot a \cdot 1 \in S$.

Let T be any ideal of R containing a. We shall prove that $S \subseteq T$. Since T is an ideal of R and $a \in T$, $xa \in T$ and so $xay \in T$, $\forall\ x, y \in R$.

Consequently, $\sum_{\text{finite}} xay \in T$, as T is an ideal of R.

This show that $S \subseteq T$. Hence S is the smallest ideal containing a and so $S = \langle a \rangle$.

Example 1.9.24. *Prove that any non-zero ideal in the Gaussian integers $J[i]$ must contain some positive integer.*

Solution. We know $J[i] = \{m + ni : m, n \text{ are integers}, i = \sqrt{-1}\}$ is an integral domain with unity 1. Further $J[i]$ is a principal ideal domain. [See corollary of Theorem 3.1.1. of chapter 3]

It means every non-zero ideal A of $J[i]$ is generated by a single element of $J[i]$ i.e.,

$$A = \langle m + ni \rangle = \{(m + ni)\, x : x \in J[i]\}.$$

Here $m + ni \neq 0 \in A$ i.e., m and n are not both zero.

Since $m + ni \in A$ and $m - ni \in J[i]$, so

$(m + ni)(m - ni) \in A$, as A is an ideal of $J[i]$

$\Rightarrow \quad m^2 + n^2 \in A$, where $m^2 + n^2$ is a positive integer.

Hence every non-zero ideal in $J[i]$ must contain some positive integer.

EXERCISES

1. If R is a ring and $a \in R$. Show that
$$r(a) = \{x \in R : ax = 0\}$$ is a right ideal of R.

2. If A and B are ideals in a ring R such that $A \cap B = (0)$, prove that for every $a \in A$, $b \in B$, $ab = 0$.

[**Hint.** $a \in A, b \in B$ i.e., $b \in R \Rightarrow ab \in A$ ($\because$ A is an ideal of R)

$a \in A$ i.e., $a \in B \Rightarrow ab \in B$ ($\because$ B is an ideal of R)

Hence $ab \in A \cap B = (0) \Rightarrow ab = 0$.

3. Prove that the intersection of two left (right) ideals of a ring R is a left (right) ideal of R. What can you say about the intersection of a left ideal and a right ideal of R ?

[**Hint.** If A is a left ideal of R and B is a right ideal of R, then $A \cap B$ need not be even a one-sided ideal of R. Let us take

$$A = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbf{Z}\right\} \text{ and } B = \left\{\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} : c, d \in \mathbf{Z}\right\}.$$

Then A is a left ideal and B is a right ideal of the ring M_2 of 2×2 matrices over the integers [See Examples 1.9.2 and 1.9.3].

We have $A \cap B = \left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbf{Z}\right\}$.

Clearly, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in A \cap B$ and $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in M_2$.

But $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \notin A \cap B$,

$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \notin A \cap B$]

4. If A and B are two left (right) ideals of a ring R, then show that $A + B$ is a left (right) ideal of R.

[**Hint.** See Theorem 1.9.3]

5. What can you about the sum of a left ideal and a right ideal of R ?

[**Hint.** Refer to the left ideal A and right ideal B of M_2 as given in Ex. 3. We have

$$A + B = \left\{\begin{pmatrix} x & z \\ y & 0 \end{pmatrix} : x, y, z \in \mathbf{Z}\right\}.$$

Clearly, $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in A + B$ and $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in M_2$. But

$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix} \notin A + B$ and

$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix} \notin A + B$.

Thus $A + B$ need not be even a one-sided ideal of M_2.]

6. If A is a left ideal and B is a right ideal of a ring R, then show that AB is a two-sided ideal of R, whereas BA need not be even a one-sided ideal of R.

[**Hint.** (*i*) See the Remark of Theorem 1.9.4 for the proof of the fact that AB is a two sided ideal of R.

(*ii*) Take the left ideal A and the right ideal B of M_2 as given in Ex. 3. We see that

$$\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} cd + ab & 0 \\ 0 & 0 \end{pmatrix}.$$

Thus $BA = \left\{\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in \mathbf{Z}\right\}$.

As shown in Ex. 3 above, BA is not even a one-sided ideal of M_2.]

7. If A, B be two ideals of a ring R, then show that $AB \subseteq A \cap B$. Give an example to show that there exist ideals A and B such that $AB \neq A \cap B$.

[**Hint.** (*i*) See Corollary 1 of Theorem 1.9.4.

(*ii*) Let A be the left ideal of M_2 and B the right ideal of M_2 as given in Ex. 3. Then

$$A \cap B = \left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbf{Z}\right\} \text{ and } AB = \left\{\begin{pmatrix} x & y \\ z & t \end{pmatrix} : x, y, z, t \in \mathbf{Z}\right\} = M_2,$$

since $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad \\ bc & bd \end{pmatrix}$.]

8. If A, B be two ideal of a ring R, then show that $AB \subseteq A + B$. Give an example to show that there exist ideals A and B such that $AB \neq A + B$.
[**Hint.** See Cor. 2 of Theorem 1.9.4]

9. Give an example of two ideals A and B of R such that $A \subseteq B \subseteq R$, where A is an ideal of B, B is an ideal of R, but A is not an ideal of R.

[**Hint.** Let $R = \left\{ \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ 0 & 0 & z \end{pmatrix} : x_i, y_i, z \text{ are integers} \right\}$,

$B = \left\{ \begin{pmatrix} 0 & 0 & x \\ 0 & 0 & y \\ 0 & 0 & 0 \end{pmatrix} : x, y \text{ are integers} \right\}$,

$A = \left\{ \begin{pmatrix} 0 & 0 & x \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} : x \text{ is an integer} \right\}$.

Then A is an ideal of B, B is an ideal of R. But A is not an ideal of R, since $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \notin A$.

10. Let R be the ring of all real-valued, continuous functions on $[0, 1]$. Show that the set $S = \{f \in R : f(\frac{2}{3}) = 0\}$ is an ideal of R.

[**Hint.** Similar to Example 1.9.8.]

11. If R is a commutative ring and $a \in R$, then prove that
$Ra = \{ra : r \in R\}$ is an ideal of R.

[**Hint.** $x, y \in Ra \Rightarrow x = r_1 a, y = r_2 a \Rightarrow x - y = (r_1 - r_2)\, a \in Ra$, since $r_1 - r_2 \in R$. For any $r \in R$, $rx = r(r_1 a) = (rr_1)\, a \in Ra$. R is commutative $\Rightarrow xr = rx \in Ra$ i.e., $xr \in Ra$.]

12. For any element a of a ring R, prove that
$Ra = \{xa : x \in R\}$ is a left ideal of R.

[**Hint.** See Ex. 11 above.]

13. Consider the ring $\mathbf{Z}$ of integers and an ideal M of $\mathbf{Z}$ consisting of all multiples of a prime p. Let N be an ideal of $\mathbf{Z}$ such that $M \subset N \subset \mathbf{Z}$. Show that $N = M$ or $N = \mathbf{Z}$. [D.U., 2000]

[**Hint.** Let $M = (p) = \{px : x \in \mathbf{Z}\}$, $N = (n) = \{nx : x \in \mathbf{Z}\}$.
$M \subset N \Rightarrow p \in (n) \Rightarrow p = nx$, for $x \in \mathbf{Z}$. Since p is prime, either $n = 1$ or $n = p \Rightarrow$ either $(n) = (1)$ or $(n) = (p) \Rightarrow$ either $N = \mathbf{Z}$ or $N = M$. Also see Example 2.6.6 of Chapter 2.

14. Let R be a ring with unity and A be any proper ideal of R. Show that no element of A can have a multiplicative inverse.

[**Hint.** See Example 1.9.6(*a*)]

15. Show that the set $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbf{Z} \right\}$ is a subring of the ring M_2 of 2×2 matrices over the integers. Also prove that S is neither a left nor a right ideal of M_2.

16. If S is an ideal of a ring R and T is any subring of R, then show that S is an ideal of $S + T$.
[**Hint.** First show that $S + T$ is a subring of R.]

17. Show that if A is an ideal of a ring R, then $A + A = A$.
[**Hint.** For any $a \in A$, $a + 0 \in A + A$ and so $A \subseteq A + A$. Conversely, let $x \in A + A \Rightarrow x = a_1 + a_2$ for some $a_1, a_2 \in A \Rightarrow x \in A$, since A is an ideal of $R \Rightarrow A + A \subseteq A$. Hence $A + A = A$.]

18. If R is a ring and A is a left ideal of R, prove that
$Ann\,(A) = \{x \in R : xa = 0\ \forall\ a \in A\}$
is a two-sided ideal of R. [D.U., 1996]
[**Hint.** Compare with Example 1.9.10]

19. Consider the ring R of all 3×3 matrices of the form :

$$R = \left\{ \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}, a, b, c, d, e, f \text{ are real numbers} \right\}.$$

Show that the set $I = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} : a \text{ is real} \right\}$

is a left ideal of R, which is not a right ideal of R.

20. Let A be an ideal of a ring R such that $A \neq R$. Show that if R has unity, then $1 \notin A$.
[**Hint.** If $1 \in A$, then $A = R$ [See Example 1.9.4], which is a contradiction.]

1.10 Simple Ring

Definition. *A ring R is called a* **simple ring**, *if*
(*i*) *there exist two elements a, b in R such that $ab \neq 0$.*
(*ii*) *R has no proper ideals i.e., the only ideals of R are $\{0\}$ and R.*

Illustration

The ring $\mathbf{Z}_2 = \{0, 1\}$ modulo 2 is a simple ring, since $1 \otimes_2 1 = 1 \neq 0$ and $\mathbf{Z}_2$ has no proper ideals.

(Notice that $\mathbf{Z}_2$ is a field and a field has no proper ideals).

Theorem 1.10.1. *Prove that a division ring is a simple ring.*

Proof. Let R be a division ring. Since $1 \in R$, so $1 \,.\, 1 = 1 \neq 0$. Next we show that R has no proper ideals. Let A be any ideal of R. If $A = \{0\}$, there is nothing to prove. Let $A \neq \{0\}$. Then there exists some $a \neq 0 \in A \subseteq R$. So $a^{-1} \in R$ exists such that $aa^{-1} = a^{-1}a = 1$. Since A is an ideal of R, so $a \in A$ and $a^{-1} \in R \Rightarrow aa^{-1} \in A \Rightarrow 1 \in A \Rightarrow 1 \,.\, x \in A\ \forall\ x \in R$

$\Rightarrow x \in A \ \forall x \in R \Rightarrow R \subseteq A$. Obviously, $A \subseteq R$.

Hence $A = R$ and so R is a simple ring.

Theorem 1.10.2. *Let R be a commutative simple ring with unity. Prove that R is a field.* [D.U., 1998]

Or

If R be a commutative ring with unity whose only ideals are $\{0\}$ are R, then show that R is a field.

Proof. We are given that R is a commutative ring with unity (*i.e.*, $1 \in R$). Then R becomes a field if we just prove that each non-zero element of R has its multiplicative inverse. Let $a \neq 0 \in R$ be arbitrary.

Let $aR = \{ax : x \in R\}$. ...(1)

We proceed to show that aR is an ideal of R.

Since $0 = a0 \in aR$, aR is non-empty.

Let $\alpha, \beta \in aR$ be arbitrary. Then by (1), we have

$\alpha = ax, \beta = ay$, for some $x, y \in R$

$\Rightarrow \alpha - \beta = ax - ay = a(x - y) \in aR$, since $x - y \in R$.

For any $r \in R$, $\alpha \in aR$; $\alpha r = (ax)\, r = a\,(xr) \in aR$, since $xr \in R$.

Since R is commutative, $r\alpha = \alpha r \in aR$.

Thus aR is an ideal of R. Since the only ideals of R are $\{0\}$ and R, it follows that

$$aR = \{0\} \quad \text{or} \quad aR = R.$$

Since $1 \in R$, so $a \,.\, 1 = a \in aR$ and $a \neq 0$. Consequently, $aR \neq \{0\}$.

Hence $aR = R$. Since $1 \in R = aR$, we have

$1 = ab$ for some $b \in R$.

$\Rightarrow \quad 1 = ab = ba$, since R is commutative

$\Rightarrow \quad a^{-1} = b \in R$. Hence R is a field.

Ex. *Prove that a commutative ring R with unity is a field if and only if it has no proper ideals.*

[**Hint.** See the above theorem and Example 1.9.5 (*i.e.*, a field has no proper ideals]

EXAMPLES

Example 1.10.1. *Show that the set of 2×2 matrices of the form*

$$S = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} : \begin{array}{l} a \text{ and } b \text{ are complex numbers} \\ \text{and } \bar{a}, \bar{b} \text{ their conjugates} \end{array} \right\}$$

is a simple ring.

Solution. By Example 1.4.6, S is a division ring under matrix addition and matrix multiplication. Hence by Theorem 1.10.1, S is a simple ring.

Example 1.10.2. *Define a simple ring and give an example of it.*

Please try yourself.

Example 1.10.3. *Show that* $M_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbf{Q} \right\}$ *is a simple ring.*

Solution. We know M_2 is a ring under matrix addition and matrix multiplication and has unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. We can find two elements A and B in M_2 such that $AB \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. For example,

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \Rightarrow AB = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

If we show that M_2 has no proper ideals, then M_2 becomes a simple ring. Let A be any ideal of M_2. If $A = \{0\}$, 0 being a 2×2 null matrix, then there is nothing to prove. Let $A \neq \{0\}$. Then there exists a non-zero matrix $X \in A$ of the form $X = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$.

Since X is a non-zero matrix, at least one of the 4 entries in X is non-zero. Let $a_{12} \neq 0 \in \mathbf{Q}$.

We choose four matrices in M_2 as follow :

Let $P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, Q = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, S = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, T = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

We have

$$PXQ = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_{12} & 0 \\ 0 & 0 \end{pmatrix},$$

$$SXT = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ a_{11} & a_{12} \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & a_{12} \end{pmatrix}.$$

Since $X \in A$ and A is an ideal of M_2, therefore $PXQ + SXT \in A$

$$\Rightarrow \quad \begin{pmatrix} a_{12} & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & a_{12} \end{pmatrix} \in A \Rightarrow \begin{pmatrix} a_{12} & 0 \\ 0 & a_{12} \end{pmatrix} \in A.$$

Since $a_{12} \neq 0 \in \mathbf{Q}$, $a_{12}^{-1} \in \mathbf{Q}$. Consequently,

$$\begin{pmatrix} a_{12}^{-1} & 0 \\ 0 & a_{12}^{-1} \end{pmatrix} \in M_2 \text{ and } \begin{pmatrix} a_{12} & 0 \\ 0 & a_{12} \end{pmatrix} \in A.$$

Since A is an ideal of M_2,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_{12} & 0 \\ 0 & a_{12} \end{pmatrix}\begin{pmatrix} a_{12}^{-1} & 0 \\ 0 & a_{12}^{-1} \end{pmatrix} \in A.$$

Thus A is an ideal of M_2 containing the unity

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ of } M_2 \text{ and so } A = M_2.$$

Hence M_2 is a simple ring.

Example 1.10.4. *Let R be a ring with unity. If R has no right ideals except R and $\{0\}$, then prove that R is a division ring.* [D.U., 1999]

Solution. We are given that $1 \in R$ and so R becomes a division ring if we show that each non-zero element in R has its multiplicative inverse in R. Let $a \neq 0 \in R$ be arbitrary. Let $aR = \{ax : x \in R\}$. ...(1)

Since $0 = a \,.\, 0 \in aR$, aR is non-empty.

Let $\alpha, \beta \in aR$ and $r \in R$. Then

$\alpha = ax$, $\beta = ay$, for some $x, y \in R$, by (1)

$\Rightarrow \quad \alpha - \beta = ax - ay = a(x - y) \in aR$, as $x - y \in R$,

and $\quad \alpha r = (ax) r = a(xr) \in aR$, as $xr \in R$.

Thus aR is a right ideal of R and so by the given hypothesis,

$aR = \{0\}$ or $aR = R$.

Since $1 \in R$ and $a = a \,.\, 1 \in aR$ and $a \neq 0$, so $aR \neq \{0\}$.

Hence $aR = R$. Since $1 \in R$, so $1 \in aR$. Consequently,

$1 = ab$, for some $b \in R$. ...(2)

From (2), it follows that each non-zero element of R has a *right* inverse.

Since $b \neq 0 \in R$ (for otherwise, $1 = ab = 0$, a contradiction), there exists some $c \in R$ such that $bc = 1$. ...(3)

We have $ba = ba \,.\, 1$, since 1 is the unity of R

$= (ba)(bc)$, using (3)

$= b(ab)\, c$

$= (b \,.\, 1)\, c$, by (2)

$= bc$

$= 1$, by (3)

$\therefore \quad ab = ba = 1$

$\Rightarrow \quad a^{-1} = b \in R$.

Hence R is a division ring.

Example 1.10.5. *Let R be a ring with unity. If R has no left ideals except R and $\{0\}$, then prove that R is a division ring.*

Hint. Let $Ra = \{xa : x \in R\}$. Then Ra is a left ideal of R. Now proceed like Example 1.10.4.

Example 1.10.6. *If R be a ring having more than one element such that $aR = R \;\forall\; a \neq 0 \in R$, then R is a division ring.*

Solution. Firstly, we show that $xy = 0 \Rightarrow x = 0$ or $y = 0$; $x, y \in R$. ...(1)

If $x \neq 0$ and $y \neq 0$, then by the given hypothesis, $xR = R$, $yR = R$.

Now $\quad 0 = xy \;\Rightarrow\; 0 \,.\, R = (xy)\, R = x\,(yR) = xR = R$.

$\therefore R = \{0\}$, a contradiction to the fact that R has more than one element.

Hence *(1)* is proved.

Since $R \neq \{0\}$, there exists some $a \neq 0 \in R$. Further $aR = R$.

Now $a \in R \;\Rightarrow\; a \in aR \;\Rightarrow\; a = ae$ for some $e \in R$.

It may be noted that $e \neq 0$, for otherwise $a = a0 = 0$, a contradiction.

Since $a \neq 0$, therefore

$$ae = a \Rightarrow ae^2 = ae \Rightarrow a(e^2 - e) = 0 \Rightarrow e^2 - e = 0, \text{ using (1)}$$

$\therefore \quad e^2 = e$. ...(2)

Let $x \in R$ be arbitrary. Then

$(xe - x)\, e = xe^2 - xe = xe - xe = 0$, using (2)

$\Rightarrow \quad xe - x = 0$, since $e \neq 0$ and using (1)

$\Rightarrow \quad xe = x \;\forall\; x \in R \Rightarrow e$ is the right unity of R. ...(3)

Now we show that each non-zero element of R has a right inverse.

Let $x \neq 0 \in R$. By the given hypothesis, $xR = R$.

Since $e \in R$, $e \in xR \Rightarrow e = xy$, for some $y \in R$.

$\Rightarrow y$ is a right inverse of x. ...(4)

From (3) and (4), it follows that R is a division ring.

Example 1.10.7. *Let R be a ring such that the only right ideals of R are $\{0\}$ and R. Prove that either R is a division ring or that R is a ring with a prime number of elements in which $ab = 0$ for every $a, b \in R$.*

Solution. Let $A = \{a \in R : ar = 0 \;\forall\; r \in R\}$ or $A = \{a \in R : aR = 0\}$. ...(1)

We shall prove that A is a right ideal of R.

Let $a, b \in A$. Then $ar = 0$ and $br = 0 \;\forall\; r \in R$.

We have $\quad (a - b)\, r = ar - br = 0 - 0 = 0 \;\forall\; r \in R$.

$\therefore \quad a - b \in A$.

Let $a \in A$ and $x \in R$. Then $ar = 0 \;\forall\; r \in R$. ...(2)

We have $(ax)\, r = a\,(xr) = ar_1$, where $r_1 = xr \in R$.

By (2), $\quad ar_1 = 0$ and so $(ax)\, r = 0 \;\forall\; r \in R$.

Thus $ax \in R$ and so A is a right ideal of R.

According to the given hypothesis, $A = \{0\}$ or $A = R$.

Case I. Let $A = \{0\}$. Then $aR = \{0\} \Rightarrow a = 0$.

In other words, $aR = R \;\forall\; a \neq 0 \in R$.

Hence R is a division ring. [See Example 1.10.6]

Case II. Let $A = R$. Then by (1), $ar = 0 \;\forall\; a \in R$ and $\forall\; r \in R$

or $\quad ab = 0 \;\;\forall\; a, b \in R$. ...(3)

Let H be **any** subgroup of the additive group $(R, +)$.

Then $\quad x - y \in H \;\forall\; x \in H, y \in H$.

For $x \in H \subseteq R$, $\; r \in R \;\Rightarrow\; xr = 0 \in H$, using (3).

Thus H is a right ideal of R.

According to the given hypothesis, R has only two right ideals $\{0\}$ and R. Hence $(R, +)$ can have only two subgroups $\{0\}$ and $(R, +)$ *i.e.*, $(R, +)$ has no proper subgroups. Consequently, $(R, +)$ must be a cyclic group of prime order [by Lagrange's Theorem]. Hence R has a prime number of elements such that $ab = 0 \;\forall\; a, b \in R$, using (3).