1

RINGS, INTEGRAL DOMAINS AND FIELDS

1. Introduction.

A set, which is merely a collection of distinct and distinguishable objects, itself has no structure. By introducing one or more binary operations in a set we have given an algebraic structure in it. Now the question arises as to what is an **Algebraic Structure.**

Definition 1.1. Algebraic Structure.

A set with one or more binary operations satisfying certain specified laws (e.g. commutative, associative or distributive) is called an **Algebraic Structure.**

Groups, Rings, Integral domains, fields and vector spaces are the simplest and most basic algebraic structures. In the current chapter we limit ourselves to **Rings, Integral Domais and Fields** which have significant applications in such diverse subjects like Physics, Chemistry, Zoology, Botany, Engineering, Statistics, Managerial Sciences, Informatics (computer science) etc. Moreover, these algebraic structures have many more valuable applications to various branches of Mathematics itself.

2. Rings.

Definition 2.1. Asystem $< R, +, \cdot >$, consisting of a non-empty set R and two internal binary operations + and · called addition and multiplication respectively, is said to be a ring if the following postulates are satisfied :

(Purv., 95, 99; GKP, 91, 94, 96, 99, 2004)

(R_1) : $<R,+>$ is an Abelian group, i.e.

(R_{11}) Associativity : $a + (b + c) = (a + b) + c$, $\forall\ a, b, c \in R$.

(R_{12}) Existence of Additive Identity : $\exists$ an element $0 \in R$ such that $a + 0 = 0 + a = a$, $\forall\ a \in R$.

(R_{13}) Existence of Additive Inverse : for every $a \in R$, $\exists$ an element $-a \in R$ such that $a + (-a) = (-a) + a = 0$.

(R_{14}) Commutativity : $a + b = b + a$, $\forall\ a, b \in R$.

(R_2): $<R, \cdot>$ is a semi group, i.e.

(R_{21}) Associativity : $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \forall\ a, b, c \in R$.

(R_3): Multiplication is left and right distributive over addition, i.e.

(R_{31}) $a \cdot (b + c) = a \cdot b + a \cdot c\ , \forall\ a, b, c \in R$ (Left Distributive Law).

(R_{32}) $(b + c) \cdot a = b \cdot a + c \cdot a\ , \forall\ a, b, c \in R$ (Right Distributive Law).

Note 2.1 The identity of the additive group $<R, +>$ is called the **zero element** of the ring and is denoted by 0.

Definition 2.2. Ring with unity. A ring with multiplicative identity (called unit element) is called a ring with unity or ring with identity element. **(GKP, 2002)**

The multiplicative identity is denoted by 1.

Definition 2.3. Commutative Ring. A ring for which multiplication is commutative is called a commutative ring. **(GKP, 2002)**

Example 2.1. The set R consisting of a single element 0 with two binary operations defined by $0 + 0 = 0$ and $0 \cdot 0 = 0$ is a ring. This ring is called the **Null Ring** or the **Zero Ring.**

Example 2.2. The set of integers with addition and multiplication forms a commutative ring with unit element.

It is called the *ring of integers.*

Example 2.3. The set of even integers with usual addition and multiplication of integers forms a commutative ring without unit element. **(GKP, 94)**

Example 2.4. The sets of rational, real and complex numbers under usual addition and multiplication form commutative rings with unit elements. **(GKP, 96)**

Example 2.5. Let C be the set of all symbols (α, β), where α, β are real numbers. We define

$(\alpha, \beta) = (\gamma, \delta)$ if $\alpha = \gamma$ and $\beta = \delta$ ...(1)

In C we introduce an addition by defining for $x = (\alpha, \beta)$ and $y = (\gamma, \delta)$

$x + y = (\alpha + \beta) + (\gamma + \delta) = (\alpha + \gamma, \beta + \delta)$ ...(2)

It is obvious that $x + y \in C$. Hence C is closed under addition.

We claim that C is an Abelian group under this binary operation.

For addition in C is associative and commutative since it has been defined in terms of addition of real numbers which is associative and commutative.

The additive identity is $(0, 0)$ and the additive inverse of (α, β) is $(-\alpha, -\beta)$.

We now define a multiplication in C by defining for $x = (\alpha, \beta)$, $y = (\gamma, \delta)$

$x \cdot y = (\alpha, \beta) \cdot (\gamma, \delta) = (\alpha\gamma - \beta\delta, \alpha\delta + \beta\gamma)$

It is obvious that $x \cdot y$ is again in C and that $x \cdot y = y \cdot x$.

Also $x \cdot (1, 0) = (1, 0) \cdot x = x \; \forall \; x = (\alpha, \beta) \in C$ so that $(1, 0)$ is a unit element for C.

Further it is easy to show that multiplication is associative in C and that it is distributive over addition.

Thus C forms a commutative ring with unit element.

Example 2.6. The set Z_m of residue classes modulo the positive integer m forms a commutative ring with unit element under addition and multiplication of residue classes.

It is called the ring of residue classes modulo m.

Solution. Let Z_m be the set of residue classes modulo m, i.e.

$Z_m = \{[0], [1], [2], ..., [r_1], ..., [r_2], ..., [m-1]\}$.

(R_1): Obviously $<Z_m, +_m>$ is an Abdian group.

(R_2): $<Z_m, \cdot_m>$ is a commutative monoid, where [1] is the unit element.

(R_3): Since the multiplication of integers is distributive over addition, hence the multiplication is distributive over addition of residue classes.

Thus $<Z_m, +_m, \cdot_m>$ is a commutative ring with unit element [1].

Example 2.7. Prove that the set

$R = \{x + y \cdot 3^{1/3} + z \cdot 9^{1/3} : x, y, z \in Q\}$

is a ring with respect to addition and multiplication. **(GKP, 2001)**

Solution. Evidently elements of R are real numbers.

Let $a, b, c \in R$ be arbitrary, then $\exists\, x_r, y_r, z_r \exists\, \mathbf{Q}$ s.t.

$$a = x_1 + y_1 \cdot 3^{1/3} + z_1 \cdot 9^{1/3},$$
$$b = x_2 + y_2 \cdot 3^{1/3} + z_2 \cdot 9^{1/3},$$
$$c = x_3 + y_3 \cdot 3^{1/3} + z_3 \cdot 9^{1/3}.$$

(R_{11}) $a + b = (x_1 + x_2) + (y_1 + y_2) \cdot 3^{1/3} + (z_1 + z_2) \cdot 9^{1/3} \in R$.

Since $x_1x_2 + 3y_1z_2 + 3z_1y_2, x_1y_2 + x_2y_1 + 3z_1z_2$ etc. $\in \mathbf{Q}$.

(R_{12}) Associativity in the group $<\mathbf{R}, +>$

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

(R_{13}) $a + b = b + a$. For $<\mathbf{R}, +>$ is a commutative group.

(R_{14}) $0 + 0 \cdot 3^{1/3} + 0 \cdot 9^{1/3} \in R$ is the zero element of R.

(R_{15}) $(-x_1) + (-y_1) \cdot 3^{1/3} + (-z_1) \cdot 9^{1/3} \in R$ is the additive inverse of a.

(R_{21}) $ab \in R, a + b \in \mathbf{R}$.

For $ab = (x_1x_2 + 3y_1z_2 + 3z_1y_2) + (x_1y_2 + x_2y_1 + 3z_1z_2) \cdot 3^{1/3} + (x_1z_2 + x_2z_1) \cdot 9^{1/3} \in R.$

(R_{22}) Associativity in the group $<R, \cdot> \Rightarrow (ab)\, c = a\,(bc)$.

(R_{31}) $a\,(b + c) = ab + ac$, (R_{32}) $(b + c)\, a = ba + ca$.

Thus $<R, +, \cdot>$ is a ring.

Example 2.8. *Let R be the ring of real numbers under the usual operations of addition and multiplication between real numbers. Define two compositions $\oplus$ and $\otimes$ in R as follows :*

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

Prove that $<R, \oplus, \otimes>$ is a ring. Determine 0–element and the 1–element of this ring. **(GKP, 2000)**

Solution. It is given that R is a ring of real numbers w.r.t. usual addition and multiplication. Also we know that $<R, +, \cdot>$ is a field. Then

$a, b \in R \Rightarrow a + b, ab \Rightarrow R \Rightarrow a + b + 1 \in R,\ ab + a + b \in R$
$\Rightarrow a \oplus b \in R,\ a \otimes b \in R$
$\Rightarrow R$ is closed w.r.t. $\oplus$ and $\otimes$.

$\mathbf{R_1}$: $<R, \oplus>$ is an Abelian group.

(R_{11}) R is closed w.r.t. the operation $\oplus$.

(R_{12}) $\oplus$ is commutative in R so that $a \oplus b = b \oplus a$.

For $a + b + 1 = b + a + 1$ since $(R, +)$ is Abelian group.

(R_{13}) $\oplus$ is associative in R, *i.e.*, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

For

L.H.S. $= (a + b + 1) \oplus c = (a + b + 1) + c + 1 = a + b + c + 2$

R.H.S. $= a \oplus (b + c + 1) = a + (b + c + 1) + 1$
$= a + b + c + 2$ so that

R.H.S. = L.H.S.

(R_{14}) Let e be identity of R w.r.t. $\oplus$.

Then $a = a \oplus e \Rightarrow a = a + e + 1 \Rightarrow e + 1 = 0 \Rightarrow e = -1 \in R$.

$\exists\ e = -1 \in R$, additive identity.

(R_{15}) If b is the additive inverse of a, then
$b \oplus a = e$ so that $b + a + 1 = -1$ or $b = -a - 2$.
$a \in R \Rightarrow -a - 2 \in R \Rightarrow b \in R$.

Thus every element $a \in R$ has additive inverse $b = -a - 2 \in R$.

$\mathbf{R_2}$: $<R, \otimes>$ is a semigroup.

(R_{21}) R is closed w.r.t. $\otimes$ (already proved).

(R_{22}) $\otimes$ is associative in R, *i.e.*, $(a \otimes b) \otimes c = a \otimes (b \otimes c)$.

For L.H.S. $= (ab + a + b) \otimes c = (ab + a + b)\, c + (ab + a + b) + c$
$= abc + ab + bc + ca + a + b + c$.

R.H.S. $= a \otimes (bc + b + c) = a\,(bc + b + c) + a + (bc + b + c)$
$= abc + ab + bc + ca + a + b + c$.

So that L.H.S. = R.H.S.

R_3: Distributive laws hold in R, *i.e.*,

(R_{31}) $a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c$ and (R_{32}) $(b \oplus c) \otimes a = b \otimes a \oplus c \otimes a$.

For $a \otimes (b \oplus c) = a(b \oplus c) + a + b \oplus c$

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

$= 2a + b + c + ab + ac + 1.$ ...(1)

$a \otimes b \oplus a \otimes c = (ab + a + b) \oplus (ac + a + c)$

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

$= 2a + b + c + ab + ac + 1.$ ...(2)

Equating (1) to (2) we get (R_{31}). Similarly we can prove (R_{32}).

R_4: Let u be 1-element of R so that

$a \otimes u = a \Rightarrow au + a + u = a \Rightarrow au + u = 0 \Rightarrow u(a + 1) = 0$

$\Rightarrow u = 0, a - 1 = 0.$

$\Rightarrow u = 0$. For a is arbitrary so that $a - 1 \neq 0$.

Hence 0 is the 1-element of R.

Thus $<R, \oplus, \otimes>$ is a ring with -1 and 0 as the zero element and 1-element of R respectively.

Example 2.9. *Prove that the set M of $n \times n$ matrices is a non-commutative ring with unity relative to the matrix addition and matrix multiplication, the elements of the matrices being real (rational, integer or complex).*

Solution. Let $A, B, C \in M$ be arbitrary. We know that the sum and product of two $n \times n$ matrices are matrices of the same order. M is closed w.r.t. addition and also the sum and product of two real numbers are real numbers. Consequently

R_1: (R_{11}) $A + B \in M$,

(R_{12}) $A + B = B + A$. For matrix addition is commutative operation.

(R_{13}) $\exists$ zero element $0 \in M$ s.t. $A + 0 = 0 + A = A$,

0 being $n \times n$ zero matrix.

(R_{14}) To each $A \in M$, $\exists$ a unique $-A \in M$

s.t. $A + (-A) = -A + A = 0$.

(R_{15}) $(A + B) + C = A + (B + C)$.

R_2: (R_{21}) $AB \in M$,

(R_{22}) $(AB)C = A(BC)$.

R_3: Since matrix multiplication is distributive over addition.

$\therefore (A + B)C = AC + BC, C(A + B) = CA + CB.$

The above arguments prove that M is a ring w.r.t. the two given operations. Further if I is unit matrix of order n, then $I \in M$ and $AI = IA = A$, so that I is unity element for M.

Also $AB \neq BA$ is general.

Thus M is a non-commutative ring with unity element I w.r.t. the addition and multipplication of matrices.

Theorem 2.1. *if a, b, c are arbitrary elements of a ring R, then*

(i) $a0 = 0a = 0$. **(GKP, 2003)**

(ii) $a(-b) = -(ab) = (-a)b$. **(GKP, 2003)**

(iii) $(-a)(-b) = ab$. **(GKP, 2003)**

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

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

Proof. (i) Since $0 + 0 = 0$

$\therefore \quad a(0+0) = a0$

or $\quad a0 + a0 = a0$, by left distributive law

or $\quad a0 + a0 = a0 + 0$ as $x + 0 = x$

By Cancellation law in $(R, +)$, we get

$$a0 = 0 \qquad \ldots(1)$$

Again $\quad 0 + 0 = 0$ gives

$$(0+0)a = 0a$$

or $\quad 0a + 0a = 0a$, by right distributive law

or $\quad 0a + 0a = 0a + 0$

By Cancellation law in $\langle R, + \rangle$, we get

$$0a = 0 \qquad \ldots(2)$$

Combining (1) and (2), we get the result (i).

(ii) $\quad a(-b+b) = a(-b) + ab$

or $a0 = a(-b) + ab$. For $-b + b = 0$

$0 = a(-b) + ab$, on using (i).

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

$\Rightarrow -(ab) = a(-b)$ ...(3)

Similarly $\quad (-a + a)b = (-a)b + ab$.

But $\quad -a + a = 0$ and $0b = 0$.

Hence the last gives $\quad 0 = (-a)b + ab$.

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

$\Rightarrow -(ab) = (-a)b$. ...(4)

From (3) and (4), $\quad (-a)b = (-ab) = a(-b)$.

Hence the result (ii).

(iii) $\quad (-a)(-b) = -[a(-b)]$, by case (ii).

$= -[-(ab)]$, again by case (ii)

$= ab$. For $-(x) = x \; \forall \; x \in R$.

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

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

$= ab + [-ac]$, by case (ii)

$= ab - ac$.

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

$= ba + (-c)a$

$= ba - [-ca]$

$= ba - ca$.

Theorem 2.2. *If R is a ring with unity element 1, then*

$$(-1)\,a = -a = a\,(-1) \quad \forall\, a \in R$$

and $(-1)(-1) = 1$.

Proof. (i) $(-1+1)\,a = (-1)\,a + 1\,.\,a$

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

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

This $\Rightarrow (-1)\,a = -a$. [For $a + x = 0 \Rightarrow a = -x$]

Again $a(-1+1) = a(-1) + a\,.\,1$

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

or $0 = a(-1) + a$.

This $\Rightarrow a(-1) = -a$. Also we have shown that $(-1)\,a = -a$.

Combining these two, $a(-1) = (-1)\,a = -a$. ...(1)

Taking $a = -1$ in (1),

$$(-1)(-1) = (-1)(-1) = -(-1)$$

or $(-1)(-1) = -(-1) = 1$.

For $-(-x) = x$ in additive group or $(-1)(-1) = 1$.

3. Subring.

Definition 3.1. Any non-empty subset S of a ring $\langle R, +, \cdot\rangle$ is called a subring of $\langle R, +, \cdot\rangle$ iff

$\langle S, +, \cdot\rangle$ is a ring. **(GKP, 90, 91, 92, 95, 97, 98, 2000)**

Definition 3.2. The two subrings $\langle R, +, \cdot\rangle$ and $\langle\{0\}, +, \cdot\rangle$ of the ring $\langle R, +, \cdot\rangle$ are called **improper** or **trivial** subrings of R. Any subring other than these two subrings is called a **proper** or **non-trivial** subring.

Example 3.1. $\langle Z, +, \cdot\rangle$ is a ring. Since $\langle mZ, +, \cdot\rangle$ is also a ring, $\forall\, m \neq 0 \in Z$. Moreover $mZ \subset Z$.

Hence $\langle mZ, +, \cdot\rangle$ is subring of the ring $\langle Z, +, \cdot\rangle$

Example 3.2. The set R of all $n \times n$ matrices with elements as rational numbers, is a ring w.r.t. the operations of matrix addition and matrix multiplication. Similarly the set S of all $n \times n$ matrices with elements as integers, is a ring w.r.t. the operations of matrix addition and matrix multiplication. Hence S is a subring of R.

Example 3.3. The ring of Gaussian integers is a subring of the ring of complex numbers.

Example 3.4. The ring of rational numbers is a subring of the ring of real numbers.

Theorem 3.1. *The necessary and sufficient conditions for a non-empty subset S of a ring R to be a subring of R are*

(*i*) $a, b \in S \Rightarrow a - b \in S$. **(GKP, 84, 87, 92, 95, 96, 97,**

(*ii*) $a, b \in S \Rightarrow ab \in S$. **(GKP., 1999, 2002, 2009; Purv., 1996)**

Proof. Let S be a subring of a ring R so that S itself is a ring.

S is a ring $\Rightarrow$ $\langle S, + \rangle$ is an Abelian group.

Hence $a, b \in S \Rightarrow a, -b \in S$ [Each element of S has additive inverse in S]

$\Rightarrow a + (-b) \in S$ [S is closed w.r.t. (+)]

$\Rightarrow a - b \in S$. Hence the condition (i)

Again S is a ring $\Rightarrow \langle S, \cdot \rangle$ is a semi-group

$\Rightarrow S$ is closed w.r.t. multiplication

$\Rightarrow ab \in S \; \forall \; a, b \in S$. Hence the condition (ii)

Conversely suppose that S is a non-empty subset of a ring R s.t. the conditions (i) and (ii) hold.

To prove that S is a subring of R, it is enough to show that S is a ring.

The condition (i) says that

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

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

i.e. $a \in S \Rightarrow -a \in S$.

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

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

$\Rightarrow a + b \in S$.

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

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

For $\langle R, + \rangle$ is an Abelian group.

Similaly we can show that

$$a + (b + c) = (a + b) + c \; \forall \; a, b, c \in S.$$

The above facts prove that $\langle S, + \rangle$ is an Abelian group.

Associativity of multiplication and distributivity of multiplication over addition hold in S. Since they hold in R.

Thus $\langle S, +, \cdot \rangle$ is a ring.

Theorem 3.2. *The necessary and sufficient conditions that a non-empty subset S of a ring R to be a subring of R are*

(*i*) $S + (-S) = S$. (*ii*) $SS \subset S$.

Proof. Let S be a non-empty subset of a ring R s.t. S is a subring so that S itself is a ring.

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

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

$\Rightarrow a - b \in S$. For S is a subring.

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

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

This $\Rightarrow S + (-S) \subset S$. ...(1)

Again $a \in S \Rightarrow a, 0 \Rightarrow S$ [For 0 is the zero element of S]

$\Rightarrow a \in S, -0 \in -S$

$\Rightarrow a + (-0) \in S + (-S)$

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

Therefore $S \subset S+(-S)$. ...(2)

Combining (2) with (1), we get the condition (i).

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

$\Rightarrow ab \in S$. For S is closed w.r.t. $(\cdot)$

This $\Rightarrow SS \subset S$. Hence the condition (ii).

Conversely suppose that S is a non-empty subset of a ring R s.t. the conditions

(i) and (ii) hold.

Any $a, b \in S \Rightarrow ab \in SS \subset S \Rightarrow ab \in S$

$S+(-S)=S \Rightarrow S+(-S) \subset S$

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

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

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

Thus

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

Hence S is a subring of R due to theorem 3.1.

Theorem 3.3. *The intersection of two subrings is again a subring.*

(GKP, 2003)

Proof. Let S_1 and S_2 be subrings of a ring R.

Now $a, b \in S_1 \cap S_2 \Rightarrow a, b \in S_1$ and $a, b \in S_2$.

Also S_1 and S_2 are subrings

$\Rightarrow a-b \in S_1, ab \in S_1$ and $a-b \in S_2, ab \in S_2$

$\Rightarrow a-b \in S_1 \cap S_2, ab \in S_1 \cap S_2$.

Hence $S_1 \cap S_2$ is a subring of R due to theorem 3.1.

Theorem 3.4. *An arbitrary intersection of subrings is a subring.*

(GKP, 83, 90, 93, 96, 98, 2000)

Proof. Let S_r be a subring of a ring $R \; \forall \; r \in N$

and let $S = \cap \{S_r : r = 1, 2, 3, ...\}$

To prove that S is a subring of R, we have to show that

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

Now $a, b \in S \Rightarrow a, b \in \overset{\infty}{\underset{r=1}{\cap}} S_r \Rightarrow a, b \in S_r \; \forall \; r \in N$

$\Rightarrow a-b \in S_r, ab \in S_r \; \forall \; r$ [For S_r is a subring]

$\Rightarrow a-b \in \overset{\infty}{\underset{r=1}{\cap}} S_r, ab \in \overset{\infty}{\underset{r=1}{\cap}} S_r$

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

Theorem 3.5. *The intersection of the family of subrings which contain a given subset M of a ring R is the smallest subring containing the subset M.*

Proof. Let S_r be a subring of a ring R s.t.

$$M \subset S_r \subset R \; \forall \, r \in \mathrm{N}.$$

Let $$S = \bigcap_{r=1}^{\infty} S_r.$$

Being an arbitrary intersection of subrings, S is a subring of R.

Further $$M \subset S_r \; \forall \, r \in \mathrm{N} \Rightarrow M \cap M \cap \ldots \subset \bigcap_{r=1}^{\infty} S_r = S$$

$$\Rightarrow M \subset S.$$

Thus S is a subring of R s.t. $M \subset S$.

$$\because \quad \bigcap_{r=1}^{\infty} S_r \subset S_r \qquad \forall \, r \in \mathrm{N}$$

or $$S \subset S_r \qquad \forall \, r \in \mathrm{N}.$$

This shows that S is contained in every subring of R. Consequently S is the smallest subring of R.

Example 3.5. *Prove that the set of matrices* $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ *with a, b, c integers, is a subring of the ring of 2 × 2 matrices having elements as integers.*

Solution. Let S denote the set of matrices of the type $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$, where a, b, c are integers.

Let R be the set of 2 × 2 matrices having elements as integers. Evidently $S \subset R$.

Now $$A, B \in S \Rightarrow A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix},$$

where $a_1, b_1, c_1, a_2, b_2, c_2$ are integers.

$$A - B = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{bmatrix} \in S.$$

$$AB = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{bmatrix} \in S$$

i.e. $$AB \in S.$$

For $a_1 a_2$, $a_1 b_2 + b_1 c_2$, $c_1 c_2$ all are integers. Thus A, B $\in$ S $\Rightarrow$ $A - B \in S$, AB $\in$ S. Hence S is a subring of R due to theorem 3.1.

Example 3.6. *Let R be a ring of integers and let*

$$S = \{mx : x \in \mathrm{Z}\},$$

m being a fixed integer,

i.e., $$S = \{0, \pm m, \pm 2m, \pm 3m, \ldots\}.$$

Show that S is a subring of R.

Solution. Any $a \in S \Rightarrow a = mx$ for some $x \in Z \Rightarrow a \in$

For product of two integers is an integer.
This $\Rightarrow S \subset R$.

Now $a, b \in S \Rightarrow \exists$ integers x and y s.t. $a = mx$, $b = my$
$\Rightarrow a - b = m(x - y)$, $ab = m(mxy)$.
Also $x - y$, mxy are integers.
$\Rightarrow a - b \in S$, $ab \in S$.
$\Rightarrow$ S is a subring of R due to theorem 3.1.

Example 3.7. *Prove that a non-empty subset S of a ring $<R, +, \cdot>$ is subring iff*

(*i*) $a, b \in S \Rightarrow a + b, ab \in S$.
(*ii*) $a \in S \Rightarrow -a \in S$.

Solution. Let S be a subring of a ring R so that $<S, +, \cdot>$ is itself a ring.

$<S, +, \cdot>$ is a ring
$\Rightarrow <S, +>$ is a group and $<S, \cdot>$ is a semigroup
$\Rightarrow$ (i).

$a \in S$ and $<S, +>$ is a group $\Rightarrow$ inverse exists in $<S, +>$
$\Rightarrow -a \in S \Rightarrow$ (ii).

Conversely let S be a non-empty subset of a ring R s.t. (i) and (ii) hold.

Let $a, b, c \in S$ be arbitrary.

R_1: $<S, +>$ is an Abelian group. For

(R_{11}) **Closure axiom.** $a + b \in S$, by (i).

(R_{12}) **Existence of inverse.** $a \in S \Rightarrow -a \in S$, by (ii).

(R_{13}) **Existence of identity.**

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

(R_{14}) **Commutative law.** $a + b = b + a$

$a, b \in S \subset R \Rightarrow a, b \in R \Rightarrow a + b = b + a$
as $<R, +>$ is an Abelian group.

(R_{15}) **Associative law.** $(a + b) + c = a + (b + c)$, as a, b, c $\in$ S $\subset$ R and $<$R, +$>$ is an Abelian.

R_2: $<S, \cdot>$ is semigroup. For

(R_{21}) **Closure axiom.** $ab \in S$, by (i).

(R_{22}) **Associative law.** $(ab)c = a(bc)$

as $a, b, c \in S \subset R \Rightarrow a, b, c \in R$ and R is ring
$\Rightarrow (ab)c = a(bc)$.

R_3: **Distributive law.** $a(b + c) = ab + ac$
$(b + c)a = ba + ca$.

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

Example 3.8. *If $<R, +, \cdot>$ is a ring, show that*

$$C_R = \{x \in R : xy = yx \ \forall\, y \in R\}$$

is a subring of R. C_R is called the centre of R. **(GKP, 85)**

Solution. We have

$$C_R = \{x \in R : xy = yx \ \forall\, y \in R\}.$$

Let $x_1, x_2 \in C_R$ be arbitrary. Then

$$x_1, x_2 \in R \qquad \ldots(1)$$

$$\left.\begin{aligned} x_1 y &= y x_1 \\ x_2 y &= y x_2 \end{aligned}\right\} \ \forall y \in R \qquad \ldots(2)$$

(2) $\Rightarrow (x_1 - x_2) y = y (x_1 - x_2)$ ...(3)

(1) $\Rightarrow x_1 - x_2 \in R$ and $x_1 x_2 \in R$ ...(4)

(3) and (4) $\Rightarrow x_1 - x_2 \in C_R$

$$\begin{aligned} (x_1 x_2) y &= x_1 (x_2 y) \\ &= x_1 (y x_2), \text{ by (2)} \\ &= (x_1 y) x_2 \\ &= (y x_1) x_2, \text{ by (2)} \end{aligned}$$

or $(x_1 x_2) y = y (x_1 x_2)$ ...(5)

(4) and (5) $\Rightarrow x_1 x_2 \in C_R$.

Thus

$$x_1, x_2 \in C_R \Rightarrow x_1 - x_2, x_1 x_2 \in C_R.$$

Consequently C_R is a subring of R due to theorem 3.1.

4. Integral Domains and Fields.

Definition 4.1. Zero Divisors.

The non-zero elements a, b of a ring R are called **proper divisors of zero or zero divisors** if $ab = 0$ or $ba = 0$. **(GKP, 2003)**

Example 4.1. The ring of numbers do not have zero divisors. For there exist no two non-zero numbers such that their product is zero.

Example 4.2. The ring of matrices has zero divisors. For example if

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$

then $$AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Hence the ring of matrices has zero divisors.

Example 4.3. In the ring of integers mod 6 under addition and multiplication mod 6, [2] and [3] are zero divisors.

Example 4.4. Consider the ring of residue classes modulo a composite positive integer $m = r\,s$, whre $r < m$, $s < m$.

Then $[r] \neq [o], [s] \neq [o]$

Now $[r] \cdot m\,[s] = [m]$

$\Rightarrow$ $[r] \cdot m\,[s] = [o]$

Hence $[r]$, $[s]$ are zero-divisors.

Example 4.5. Consider the set, of all real valued functions defined over [0, 1], which forms a ring with respect to addition and multiplication defined as follows :

$$(f+g)(x) = f(x) + g(x),$$
$$(fg)(x) = f(x)\,g(x).$$

Let f and g be defined as

$$f(x) = \begin{cases} \frac{1}{3} - x & \text{for } 0 \le x < \frac{1}{3} \\ 0 & \text{for } \frac{1}{3} \le x \le 1 \end{cases}$$

$$g(x) = \begin{cases} 0 & \text{for } 0 \le x \le \frac{1}{3} \\ x - \frac{1}{3} & \text{for } \frac{1}{3} < x \le 1 \end{cases}$$

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

Therefore $fg = 0$ (the zero function)

But $f \neq 0, g \neq 0$.

Hence f, g are zero-divisors.

Definition 4.2. Let $a\ (\neq 0)$, b, c be elements of a ring R.

If $a \cdot b = a \cdot c \Rightarrow b = c$

and $b \cdot a = c \cdot a \Rightarrow b = c$,

then we say that the *restricted cancellation* laws hold in R.

These are called restricted since cancellation by zero does not hold.

Theroem 4.1. A ring R is without zero-divisors if and only if the restricted cancellation laws hold in R. **(GKP, 1987, 91, 93, 95, 99, 2003)**

Proof. Let R contain no zero divisors.

Suppose that $x\ (\neq 0)$, $y \in R$.

Then $x \cdot y = 0 \Rightarrow y = 0$ .....(1)

For otherwise, if $y \neq 0$, then x is a zero-divisor which is contradictory to the hypothesis.

Now let a $(\neq 0)$, b, c $\in$ R. Then

$a \cdot b = a \cdot c \Rightarrow a\,(b - c) = 0$ (by distributive law)

$\Rightarrow b - c = 0$

$\Rightarrow b = c$

Similarly, it can be proved that
$b \cdot a = c \cdot a \Rightarrow b = c$.

Conversely, suppose that the restricted cancellation laws hold in R. Now. if possible, let R have zero-divisors. That is, let
$a \cdot b = 0$ whre $a \neq 0, b \neq 0$.
Then $a \cdot b = 0 = a \cdot 0$
Hence by restricted left cancellation law
$b = 0$,
which contradicts that $b \neq 0$.
Therefore R has no zero-divisors.

Definition 4.3. Integral domain. (GKP, 1993, 98, 2000, Purv., 1997)

A ring is said to be an integral domain if it has no zero-divisors.
Thus a ring R is called an integral domain if $\forall$ a, b $\in$ R, a b = 0 $\Rightarrow$ a = 0 or b = 0.

An Alternate Definition. Integral domain is defined as a commutative ring having no zero-divisors.

Example 4.6. The ring of integers Z is an integral domain.

Example 4.7. The ring of even integers is an integral domain without unit element.

Example 4.8. The ring R = {[0], [1], [2], [3], [4], [5], [6], [7]} under the addition and multiplication modulo 8 is not an integral domain. For [2] $\in$ R, [4] $\in$ R are two non-zero elements such that $[2] \cdot_8 [4] = 0$.

(GKP, 2002)

Example 4.9. The set Q under ordinary addition and multiplication is an integral domain. For

$$a\,b = 0 \Rightarrow a = 0 \text{ or } b = 0 \ \forall\ a, b \in Q.$$

Definition 4.4. Division ring or skew field. A ring R is said to be a **Division ring or skew field** if the set R* of non-zero elements of R forms a multiplicative group.

(GKP, 2000)

Theorem 4.2. A division ring is an integral domain but the converse is not necessarily true.

(GKP, 2000, 2002)

Proof. Let R be a division ring.
If possible let R contain zero divisors. Then, there exist
$a \neq 0, b \neq 0$ in R s.t. $ab = 0$.
$\therefore a^{-1}(ab) = a^{-1} 0$ [$\because a \neq 0$, R being a division ring, a^{-1} exists in R]
or $(a^{-1} a) b = 0$ due to associative law
or $b = 0$ which contradicts the supposition $b \neq 0$.
Hence R contains no zero divisors.
Therefore R is an integral domain.
The converse will be supported by the following example.
Consider the ring <Z, +, $\cdot$> of integers which is an integral domain but

it is not a division ring because non-zero elements do not have multiplicative inverses in Z i.e., $<Z^* = Z-\{0\}, \cdot>$ is not a group.

Theorem 4.3. A finite integral domain is a division ring.

(GKP, 86, 91, 93, 97, 2001)

Proof. Let R be a finite integral domain. Then R contains no zero divisors. Therefore the set R* of non-zero elements of R forms a finite semi group w.r.t. multiplication in which both the cancellation laws hold. Therefore $<R^*, \cdot>$ is a group. Hence R is a division ring.

Definition 4.5. Field. A commutative division ring is called a field.

(GKP, 90, 92, 95, 98, PU, 95, 97, U.P.P.C.S. 98)

Definition 4.6. Field. A field is an algebraic system $<F, +, \cdot>$, consisting of a non-empty set F and two binary operations + and. called addition and multiplication, satisfying the following axioms :

(F_1) : $<F, +>$ is an Abelian group.

(F_2) : $<F^* = F-\{0\}, \cdot>$ is an Abelian group.

(F_3) : Multiplication is distributive over addition.

(GKP, 90, 92, 95, 98; PU, 95, 97; U.P.P.C.S. 98)

Example 4.10. Give an example of a division ring (skew field) which is not a field. **(GKP, 85, 95)**

Solution. Let R be set of matrices of the form

$$A = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$$

where a and b are complex numbers.

Let $B = \begin{bmatrix} c & d \\ -\bar{d} & \bar{c} \end{bmatrix}$,

$C = \begin{bmatrix} p & q \\ -\bar{q} & \bar{p} \end{bmatrix}$ be any two members of R. Then

$$A + B = \begin{bmatrix} a+c & b+d \\ -(\bar{b}+\bar{d}) & \bar{a}+\bar{c} \end{bmatrix}$$

$$AB = \begin{bmatrix} ac-b\bar{d} & ad+b\bar{c} \\ -\bar{b}c-\bar{a}\bar{d} & -\bar{b}d+\bar{a}\bar{c} \end{bmatrix} \quad .....(1)$$

If we take $\alpha = a + c$, $\beta = d + d$, $\gamma = ac - b\bar{d}$, $\delta = ad + b\bar{c}$, then we have

$$A + B = \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} \in R$$

and $$AB = \begin{bmatrix} \gamma & \delta \\ -\bar{\delta} & \bar{\gamma} \end{bmatrix} \in R.$$

(R_1) : (R, +) is an Abelian group.

(R_{11}). **Closure axiom.** $A + B \in R$ (already proved).

(R_{12}). **Commutative law.** $A + B = B + A$.

This follows from the fact that $a + b = b + a$.

(R_{13}). **Existence of identity.**

$$O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R$$

is additive identity s.t. $A + O = O + A = A$.

(R_{14}). **Associative law.** $A + (B + C) = (A + B) + C$.

It follows from the fact that

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

(R_{15}). **Existence of inverse.**

$$-A = \begin{bmatrix} -a & -b \\ \bar{b} & -\bar{a} \end{bmatrix} \in R$$

is inverse of A s.t. $A + (-A) = O$.

(R_2) : $(R, \cdot)$ is a group.

(R_{21}). **Closure Axiom.** $AB \in R$ (already proved).

(R_{22}). **Existence of identity.**

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in R \text{ is identity s.t. } AI = IA = A.$$

(R_{23}). **Associative law.** $(AB)\,C = A\,(BC)$.

For $$(ab)\,c = a\,(bc).$$

(R_{24}). **Existence of inverse.** If $A \neq O$, then

$$A^{-1} = \frac{\text{adj } A}{|A|} = \frac{1}{a\bar{a} + b\bar{b}} \begin{bmatrix} \bar{a} & -b \\ \bar{b} & a \end{bmatrix} \in R$$

is inverse of A s.t. $AA^{-1} = A^{-1}A = I$.

(R_{25}). **Commutative law.** $AB = BA$ is not satisfied here.

For
$$BA = \begin{bmatrix} c & d \\ -\bar{d} & \bar{a} \end{bmatrix} \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$$

$$= \begin{bmatrix} a\,c - \bar{b}\,d & b\,c - \bar{a}\,d \\ -a\,\bar{d} - \bar{b}\,\bar{c} & -b\,\bar{d} + \bar{a}\,\bar{c} \end{bmatrix} \neq BA, \text{ by (1)}$$

or
$$BA \neq AB$$

(R_3) **Distributive law.** $A\,(B + C) = AB + AC$

$$(B + C)\,A = BA + CA.$$

It is true in general in case of matrices.

Thus $(R, +, \cdot)$ is a skew field but not field.

Example 4.11. Prove that the set of all matrices of the form $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$, (where a, b are real numbers) with matrix addition and matrix multiplication

is a ring. Is it a commutative ring. Does it possess the unit element. Has it zero divisors ?

Hint. Take $A = \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}, B = \begin{bmatrix} 0 & c \\ 0 & d \end{bmatrix}$,

then $A + B = \begin{bmatrix} 0 & a+c \\ 0 & b+d \end{bmatrix}, AB = \begin{bmatrix} 0 & ad \\ 0 & bd \end{bmatrix}$.

Since the product of two matrices is not commutative. So the ring is not commutative. The ring possesses zero divisors. For if $A = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, then $AB = O$. It has no unit element.

Example 4.12. If R is a ring satisfying all the conditions for a ring with unity with the possible exception of $a + b = b + a$, prove that the axiom of $a + b = b + a$ must hold in R and that R is thus a ring.

(I.A.S. 1998)

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

by left distributive law

$= a \cdot 1 + a \cdot 1 + b \cdot 1 + b \cdot 1$

$= (a + a) + (b + b) \cdot$ For $1 \cdot x = x \; \forall \in R$

$= a + (a + b) + b$, by associative law for (+).

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

Again $(a + b)(1 + 1) = (a + b) \cdot 1 + (a + b) \cdot 1 = (a + b) + (a + b)$

or $(a + b)(1 + 1) = a + (b + a) + b$. ...(2)

From (1) and (2), $a + (a + b) + b = a + (b + a) + b$.

Applying left cancellation law for addition,

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

Again right cancellation law for addition gives $a + b = b + a$.

Example 4.13. Do the following sets form an integral domain w.r.t. ordinary addition and multiplication ? If so state if they are field :

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

(2) The set of even integers.

(3) The set of positive integers.

Solution. (1) Let $A = \{b\sqrt{2} : b \in Q\}$.

$\forall x, y \in A \Rightarrow \exists a, b \in Q$ s.t. $x = a\sqrt{2}, y = b\sqrt{2}$.

$\Rightarrow xy = (a\sqrt{2})(b\sqrt{2}) = 2ab \notin A \Rightarrow xy \notin A$.

Therefore A is not closed w.r.t. multiplication.

Hence A is not a ring. It means that A is neither an integral domain nor a field.

(2) Let E denote the set of even integers. Then E is a commutative ring. Also E is without zero divisors. For the product of two non-zero even

integers is not zero. $1 \notin E$. For 1 is not an even integer. Hence E is an integral domain. E is not a field.

(3) Let N denote set of positive integers. $0 \notin N$.

$\therefore$ N is not ring.

Hence N is neither an integral domain nor a field.

Example 4.14. Show that the ring of real quaternions is a division ring but not a field. [GKP, 87]

Solution. Consider the set

$Q = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3$ are real numbers and i, j, k are symbols satisfying the following relations$\}$.

$$\begin{cases} i^2 = j^2 = k^2 = ijk = -1 \\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j. \end{cases}$$

We say that two elements $a = a_0 + a_1 i + a_2 j + a_3 k$ and $b = b_0 + b_1 i + b_2 j + b_3 k$ of Q are equal iff

$$a_t = b_t \text{ for } t = 0, 1, 2, 3.$$

We define addition and multiplication in Q as follows :

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

Multiplication is straightforward and it results from multiplying two such elements formally and collecting terms using the relation given above.

The system (Q, +, .) forms non-commutative division ring. For if a, b, $c \in Q$, then

(i) $a + b \in Q$;

(ii) Addition is associative and commutative over Q, since it is defined it terms of addition of real numbers ;

(iii) $0 = 0 + 0i + 0j + 0k$, is the zero element of Q ;

(iv) Additive inverse of $a_0 + a_1 i + a_2 j + a_3 k$ is $-a_0 - a_1 i - a_2 j - a_3 k$;

Thus Q forms an Abelian group under addition.

Moreover, if a, b, $c \in Q$, then

(v) $a . b \in Q$;

(vi) $a . (b . c) = (a . b) . c$

(vii) Unit element of Q is $1 = 1 + 0i + 0j + 0k$;

(viii) If $a_0 + a_1 i + a_2 j + a_3 k \neq 0$, then not all of a_0, a_1, a_2, a_3 are zero simultaneously.

Since a_t's are real, $\beta = a_0^2 + a_1^2 + a_2^2 + a_3^2 \neq 0$.

Therefore

$$\frac{a_0}{\beta}-\frac{a_1}{\beta}i-\frac{a_2}{\beta}j-\frac{a_3}{\beta}k \in Q$$

and $$(a_0 + a_1i + a_2j + a_3k) \cdot \left(\frac{a_0}{\beta}-\frac{a_1}{\beta}i-\frac{a_2}{\beta}j-\frac{a_3}{\beta}k\right) = 1.$$

Consequently the non-zero elements of Q form a group under multiplication.

Moreover, multiplication is distributive over addition.

Therefore the system (Q, +, .) forms a division ring.

However, it can be verified that $ab \neq ba$.

Therefore the system (Q, +, .) will not form a field.

Theorem 4.4. A finite commutative integral domain is a field. [GKP, 1985]

Proof. In the light of theorem 4.3, a finite commutative integral domain is a commutative division ring. Hence it is a field due to definition 4.5.

Example 4.15. The set of rational numbers Q forms a field under usual addition and multiplication.

Example 4.16. The set of real numbers R forms a field under usual addition and multiplication.

Example 4.17. The set C of complex numbers forms a field under usual addition and multiplication. [PU, 1997]

Example 4.18. Determine whether the set ot numbers of the form $a + b\sqrt{2}$ with a and b as integers, is a ring w.r.t. addition and multiplication. If it is a ring, is it a field or an integral domain ? [GKP, 84, 2002]

Solution. Let $R = \{a + b\sqrt{2} : a, b \in Z\}$, where Z = set of integers.

Let $x, y, z \in R$, then $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$, $z = e + f\sqrt{2}$, where $x, y z \in Z$. Here we use the fact that sum, difference and product of two integers are integers.

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

and

$$xy = (ac + 2bd) + (ad + bc)\sqrt{2} \in R$$

as

$$a + c, b + d, ac + 2bd, ad + bc \in Z.$$

(R_1): (R, +) is an Abelian group.

(R_{11}). **Closure axiom.** $x + y \in R$, (already proved).

(R_{12}). **Existence of identity.** $0 + 0\sqrt{2} = 0 \in R$ is identity element s.t.

$$x + 0 = 0 + x = x.$$

(R_{13}). **Commutative law.** $x + y = y + x$.

This follows form the fact that

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

(R_{14}). **Existence of inverse.** $x \in R$ has its inverse

$$-x = -a + (-b)\sqrt{2} \in R \text{ s.t.}$$
$$x + (-x) = -x + x = 0$$

(R_{15}). Associative law. $(x + y) + z = x + (y + z)$

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

(R_2). (R, .) is semi-group. For

(R_{21}). Closure axiom. $xy \in R$, (already proved)

(R_{22}). Associative law. $(xy)z = x(yz)$

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

(R_3) Distributive law. $x(y + z) = xy + xz$

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

Thus (R, +, .) is a ring.

(R_4). Existence of unity. $1 = 1 + 0\sqrt{2} \in R$ is unity element (multiplicative identity) s.t.

$$1 . x = x . 1 = x.$$

(R_5). R has no divisors of zero, i.e.,

$xy = 0 \Rightarrow x = 0, y = 0$

For $xy = 0 \Rightarrow (a + b\sqrt{2})(c + d\sqrt{2}) = 0 + 0\sqrt{2}.$
$\Rightarrow (ac + 2bd) + (ad + bc)\sqrt{2} = 0 + 0\sqrt{2}$
$\Rightarrow ac + 2bd = 0, ad + bc = 0$
$\Rightarrow a, b = 0$, and $c, d = 0$
$\Rightarrow x = a + b\sqrt{2} = 0, y = c + d\sqrt{2} = 0.$

Hence (R, +, .) is an integral domain.

Now we claim that the integral domain (R, +, .) is not a field.

For this we have to show that $x^{-1} \notin R$ for every $x \in R$ s.t. $x \neq 0$.

Let $x = a + b\sqrt{2} \in R$ s.t. $x \neq 0$.

Then
$$x^{-1} = \frac{1}{x} = \frac{1}{a + b\sqrt{2}}$$
$$= \frac{a - b\sqrt{2}}{\left(a + b\sqrt{2}\right)\left(a - b\sqrt{2}\right)}$$
$$= \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$
$$= \frac{a}{a^2 - 2b^2} + \left(\frac{-b}{a^2 - 2b^2}\right)\sqrt{2} \notin R$$

i.e., $x^{-1} \notin R.$

For $\frac{a}{a^2-2b^2}$ and $\frac{-b}{a^2-2b^2}$ are not necessarily integers.

Example 4.19. The set of all residue classes modulo a positive integer p is an integral domain iff p is prime.

Solution. Let R denote the set of all residue classes modulo a positive integer p so that

$$R = \{[x] : x = 0, 1, 2, 3, ..., p-1\}.$$

Then we know that R is a commutative ring with unity element [1], [0] being the zero element of R. Let [a], [b] $\in$ R be arbitrary so that

$$0 \leq a, b \leq p-1.$$

R will be an integral domain iff it is free from zero divisors, i.e., iff

$$[a] \,.\, p\,[b] = [0] \Rightarrow [a] = [0] \text{ or } [b] = [0].$$

So we have to show that p is prime iff

$$[a] \,.\, p\,[b] = [0] \Rightarrow [a] = [0] \text{ or } [b] = [0].$$

p is prime, $[a] \,.\, p\,[b] = [0] \Rightarrow$ p is prime, $ab \equiv 0 \pmod p$

$\Rightarrow a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$

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

Conversely, suppose,

$$[a] \,.\, p\,[b] = [0] \Rightarrow [a] = [0] \text{ or } [b] = [0].$$

To prove p is prime.

Suppose not. Then p is composite.

p is composite $\Rightarrow$ p is expressible as $p = p_1 p_2$,

where $1 < p_1, p_2 < p$

$\Rightarrow [p] = [p_1 \cdot p_2]$, $[p_1] \neq [0]$, $[p_2] \neq [0]$

$\Rightarrow [p_1 \cdot p_2] = [0]$. For $[p] = [0]$

$\Rightarrow [p_1] = [0]$ or $[p_2] = [0]$, by our assumption. Which is a contradiction,

For $[p_1] \neq [0]$ and $[p_2] \neq [0]$.

Hence our initial assumption is wrong. Therefore p is prime.

Example 4.20. Show that the ring of residue classes modulo p is a field iff p is a prime. **[GKP, 1983, 93, 97, 2000, 2004, U.P.P.C.S. 98]**

Solution. Example 4.19 and Theorem 4.4 serve the purpose.

Theorem 4.5. Every field is an integral domain but the converse is not true.

Proof. Step. I. Let F be a field so that

(1) (F, +) is an Abelian group.

(2) (F', .) is a commutative group, where F' is a set of non-zero elements of F,

(3) the two distributive laws hold in F.

To prove that F is an integral domain, we have to show that

(4) (F, +) is Abelian group,

(5) (F, .) is a semi-group,

(6) F is commutative,

(7) F has unity element,

(8) F has no zero divisors,

(9) the two distributive laws hold in F.

Evidently (1) $\Rightarrow$ (4), (2) $\Rightarrow$ (5), (6) and (7), (3) $\Rightarrow$ (9).

Step II. Remains to prove the condition (8).

For this we have to show that

$$ab = 0;\ a, b \in R \Rightarrow a = 0 \text{ or } b = 0.$$

$ab = 0;\ a, b \in R$ s.t. $a \neq 0 \Rightarrow ab = 0,\ a^{-1}$ exists

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

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

$\Rightarrow b = 0.$

Again $ab = 0;\ a, b \in R$ s.t. $b \neq 0$

$\Rightarrow ab = 0,\ b^{-1}$ exists

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

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

$\Rightarrow a = 0.$

The converse will be supported by an example. The ring of integers is an integral domain but it is not a field, since the non-zero elements are not inversible w.r.t. multiplication.

Definition 4.7. Subfield.

A non-empty subset F' of a field F is a subfield of F if F' is closed w.r.t. the compositions in F and F' itself is a field relative to these operations.

Example 4.21. The set of real numbers is a subfield of the field of complex numbers.

Example 4.22. The set of rational numbers is a subfield of the field of real numbers.

Theorem 4.6. The necessary and sufficient conditions for a non-empty subset F' of a field F be a subfield of F are

(i) $a \in F', b \in F' \Rightarrow a - b \in F'$.

(ii) $a \in F', b \neq 0 \in F' \Rightarrow ab^{-1} \in F'$. [GKP, 1996]

Proof. Let F' be a non-empty subset of a field F s.t. F' is a sub-field of F.

F' is a subfield of F$\Rightarrow$ F' and F both are field and $F' \subset F$

$\Rightarrow$ (F', +) is additive subgroup of (F, +)

$\Rightarrow a - b \subset F' \ \forall\ a, b \in F'$

i.e. $a, b \in F' \Rightarrow a - b \in F'$.

Hence the condition (i).

(F', +, .) is a field $\Rightarrow$ non-zero elements of F' form a multiplicative group.

In view of this

$a, b \in F'$ s.t. $b \neq 0 \Rightarrow a, b^{-1} \in F'$

$\Rightarrow ab^{-1} \in F'$.

Hence the condition (ii).

Conversely suppose that F' is a non-empty subset of F s.t. the conditions (i) and (ii) hold.

The condition (i) says that (F', +) is a subgroup of the Abelian group (F, +). Therefore (F', +) itself is an Abelian group.

$a, b, c \in F' \Rightarrow a, b, c \in F$. Also (F, +, .) is a field

$\Rightarrow (ab)\, c = a\,(bc)$ and

$a\,(b + c) = ab + ac$, $(b + c)\, a = ba + ca$

$\Rightarrow$ Associativity of multiplication and distributivity of multiplication over addition both hold in $F' \subset F$.

The condition (ii) says that

$a \in F', a \neq 0 \Rightarrow aa^{-1} \in F' \Rightarrow 1 \in F'$

$\Rightarrow$ unity element belongs to F'.

Again the condition (ii) gives

$1 \in F', a \in F'$ s.t. $a \neq 0 \Rightarrow 1\, a^{-1} \in F' \Rightarrow a^{-1} \in F'$.

Hence non-zero elements have their inverses in F'.

$a, b \in F' \Rightarrow a, b \in F \Rightarrow ab = ba$. For (F, +, .) is a field.

$\therefore$ $ab = ba \ \forall\ a, b \in F'$.

Thus the non-zero elements of F' form a commutative group.

Hence (F', +, .) is a field.

Definition 4.8. Characteristic of a ring. (GKP, 2007

Let R be a ring with zero element 0 and suppose $\exists$ a positive integer n such that

$na = a + a + \ldots\ldots$ upto n terms $= 0, \forall\ a \in R$.

The smallest such positive integer n is called the characteristic of the ring R.

If there exists no such positive integer, then R is said to be of characteristic

zero or infinite.

Example 4.23. If $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$,

then the ring $\langle Z_6, +_6, \cdot_6 \rangle$ has the characteristic 6.

Solution. Since $6._6 [x] = [0], \forall [x] \in Z_6$ and

$r \cdot_6 [x] \neq 0, \forall [x] \in Z_6$ such that $0 < r < 6$.

Hence the ring $\langle Z_6, +_6, \cdot_6 \rangle$ has characteristic 6.

Definition 4.9. Characteristic of an Integral Domain.

The characteristic of an integral domain R is either 0 or a positive integer n according as the order of the unity element e of R is 0 or n when e is regarded as an element of the additive group of R, i.e., n is a least positive integer s.t. $ne = 0$.

Definition 4.10. Characteristic of a Field.

The characteristic of a field is defined to be the characteristic of an integral domain.

A field with non-zero characteristic is called **Modular Field.**

Example 4.24. The characteristic of the field $(Z_7, +_7, \cdot_7)$ is 7, where $Z_7 = \{[0], [1], [2], [3], [4], [5], [6]\}$.

Definition 4.11. Ordered Integral Domain.

[GKP, 83, 84, 96, 99, P.U. 1996]

An integral domain $(D, +, \cdot)$ is said to be ordered if it contains a subset D^+, s.t.

(i) D^+ is closed w.r.t. addition and multiplication as defined on D, i.e.,

$$a, b \in D^+ \Rightarrow a + b \in D^+, ab \in D^+.$$

(ii) For any $a \in D$, one and only one of the following holds :

$$a = 0, a \in D^+, -a \in D^+.$$

The elements of D^+ are called positive elements of D. Also the elements of $(D - D^+)$ are called negative elements of D.

Definition 4.12. Ordered Field.

A field F is said to be ordered when it is ordered as an integral domain.

Example 4.25. The integral domain of integers (rational or real numbers) is ordered. Since it contains the subset N of all positive integers.

Example 4.26. The integral domain (or field) of complex numbers is not ordered.

Theorem 4.7. The characteristic of a ring with unity is 0 or $n > 0$ according as the unity element 1 regarded as a member of the additive group of the ring has the order zero or n.

Proof. Let R be a ring with unity element 1. If 1 has order zero, then the characteristic of the ring is zero.

Suppose 1 is of finite order n so that

$$1 + 1 + 1 + \ldots \text{ upto n terms} = 0 \text{ i.e., } n1 = 0.$$

Let a be any element of R. Then, we have

$$na = a + a + a + \ldots \text{ upto n terms}$$
$$= 1a + 1a + 1a + \ldots \text{ upto n terms}$$
$$= (1 + 1 + 1 + \ldots \text{ upto n terms})\, a \qquad \text{[by dist. law]}$$
$$= (n1)\, a = 0a = 0.$$

$\therefore$ order of a is = n.

Hence the characteristic of the ring is n.

Theorem 4.8. The characteristic of an integral domain is 0 or $n > 0$ according as the order of any non–zero element regarded as a member of the additive group of the integral domain is either 0 or n. [GKP, 2005]

Proof. Let D be an integral domain.

If a non–zero element of D is of order zero, then the characteristic of D is zero.

Let the order of the non–zero element a be finite and equal to n. Then $na = 0$.

Suppose b is any other non–zero element of D.

We have $na = 0$

$$\Rightarrow (na)\, b = 0$$
$$\Rightarrow (a + a + a + \ldots \text{ upto n terms})\, b = 0$$
$$\Rightarrow (ab + ab + ab + \ldots \text{ upto n terms}) = 0$$
$$\Rightarrow a\,(b + b + b + \ldots \text{ upto n terms}) = 0$$
$$\Rightarrow a\,(nb) = 0.$$

But D is without zero divisors. Therefore $a \neq 0$ and $a\,(nb) = 0 \Rightarrow nb = 0$.

But the order of a is $n \Rightarrow n$ is the least positive integer such that $na = 0$. Also we have $n0 = 0$. Thus n is the least positive integer such that $nx = 0\ \forall\ x \in D$. Hence D is of characteristic n.

Theorem 4.9. Each non–zero element of an integral domain D, regarded as a member of the additive group of D, is of the same order. [GKP, 2005]

Proof. Let D be an integral domain. Suppose a is a non–zero element of D and o (a) is finite and say, equal to n.

Suppose b is any other non–zero element of D and o (b) = m.

We have $o(a) = n \Rightarrow na = 0$

$$\Rightarrow nb = 0 \text{ [See theorem 4.8]}$$
$$\Rightarrow o(b) \leq n \Rightarrow m \leq n.$$

Similarly o (b) = m $\Rightarrow$ mb = 0 $\Rightarrow$ a (mb) = 0

$\Rightarrow$ a (b + b + ... upto m times) = 0

$\Rightarrow$ (ab + ab + ab + ... upto m times) = 0

$\Rightarrow$ (a + a + a .... upto m times) b = 0

$\Rightarrow$ (ma) b = 0

$\Rightarrow$ ma = 0 [$\because$ b $\neq$ 0 and D is without zero divisors]

$\Rightarrow$ o (a) $\leq$ m $\Rightarrow$ n $\leq$ m.

Now m $\leq$ n, n $\leq$ m $\Rightarrow$ m = n. Hence o (a) = o (b).

Also if o (a) is zero, then o (b) cannot be finite. Because o (b) = m $\Rightarrow$ ma = 0 i.e., the order of a is finite. Hence o (b) must also be zero.

Theorem 4.10. The characteristic of an integral domain is either 0 or a prime number.

Proof. Suppose D is an integral domain. Let 0 $\neq$ a $\in$ D. If o (a) is zero, then the characteristic of D is 0. If o (a) is finite, let o (a) = p. Then the characteristic of D will be p. We are to prove that p must be prime.

Suppose p is not prime. Let $p = p_1p_2$, where $1 < p_1, p_2 < p$.

Since D is an integral domain, therefore the product of two non–zero elements of D cannot be equal to 0.

$\therefore$ aa $\neq$ 0 i.e., $a^2 \neq 0$.

Now in an integral domain two non–zero elements are of the same order.

$\therefore$ o (a) = p $\Rightarrow$ o (a^2) = p $\Rightarrow$ $pa^2 = 0$

$\Rightarrow$ $(p_1p_2)\, a^2 = 0$ [$\because$ $p = p_1p_2$]

$\Rightarrow$ ($a^2 + a^2 + a^2 +$ .... upto p_1p_2 terms) = 0

$\Rightarrow$ $(p_1a)\,(p_2a) = 0$

$\Rightarrow$ either $p_1a = 0$ or $p_2a = 0$ $\Rightarrow$ characteristic of D is either p_1 or $p_2 < p$ which is a contradiction [$\because$ D is without zero divisors]

Hence p must be prime.

Theorem 4.11. Let D be an integral domain with unity element 1. If D is an ordered integral domain show that 1 is a positive element of D.

[GKP, 1987]

Proof. Let D be an ordered integral domain with unity element 1. Let D^+ denote the set of positive elements of D.

Suppose 1 $\notin$ D^+.

Now 1 $\neq$ 0. Since 1 $\notin$ D^+ therefore by the definition of an ordered integral domain,

$\therefore -1 \in D^+$

$\Rightarrow (-1)(-1) \in D^+$ [$\because D^+$ is closed with respect to multiplication]

$\Rightarrow 1 \in D^+$ which is a contradiction.

Hence $1 \in D^+$ i.e., 1 is a positive element of D.

Theorem 4.12. The set C of complex numbers is not an ordered integral domain. [GKP, 1983, 86, 92, 94, 96, 99, P.U, 1994, 96]

Proof. Consider $i \in C$.

Since $i \neq 0$ we have by the defining property of an ordered integral domain, either $i \in C^*$ or $-i \in C^*$,

where C^* denotes the set of positive elements of C.

Now $i \in C^* \Rightarrow i.i = -1 \in C^*$,

which is a contradiction to the fact that 1 is positive element of C.

Again $-i \in C^* \Rightarrow (-i)(-i) = -1 \in C^*$,

which is also a contradiction.

Therefore, none of the alternatives, namely,

$$i = 0, \quad i \in C^*, \quad -i \in C^*$$

holds.

Hence C is not ordered.

Theorem 4.13. The field Z_p of residue classes modulo a prime p is not ordered.

Proof. We have

$Z_p = \{[0], [1], [2], ..., [p-1]\}$.

Let Z^+_p denote the set of positive elements in Z_p.

If $[1] \in Z^+_p$, then $[1] +_p [1] = [2] \in Z^+_p$.

Again $[1] \in Z^+_p, [2] \in Z^+_p \Rightarrow [1] +_p [2] = [3] \in Z^+_p$.

Proceeding in this way we obtain

$[1] \in Z^+_p, [p-2] \in Z^+_p \Rightarrow [1] +_p [p-2] = [p-1] \in Z^+_p$, i.e.

$$[-1] \in Z^+_p \ (\because [p] = [o]).$$

Thus both [1] and $[-1] \in Z^+_p$, which is impossible. Hence Z_p is not an ordered integral domain.

5. Ideals and Quotient Rings.

Definition 5.1. Left Ideal.

A non-empty subset *S* of a ring *R* is called a left ideal of *R* if :

(i) S is additive subgroup of R, i.e. $a \in S, b \in S \Rightarrow a-b \in S$.

(ii) $\forall r \in R, \forall s \in S \Rightarrow rs \in S$.

Definition 5.2. Right Ideal.

A non-empty subset *S* of a ring *R* is called a right ideal of R if :

(i) S is additive subgroup of R, i.e. $a \in S, b \in S \Rightarrow a-b \in S$.

(ii) $\forall\, r \in R, \forall\, s \in S \Rightarrow sr \in S$. **[GKP, 90, 92, 98, 2000, 2003; PU, 96]**

Definition 5.3. Ideal.

A non-empty subset S of a ring R is called an ideal or two sided ideal if it is both left and right ideal, i.e. if :

(i) S is additive subgroup of R, i.e. $a \in S, b \in S \Rightarrow a-b \in S$.

(ii) $\forall\, r \in R, \forall\, s \in S \Rightarrow rs \in S, sr \in S$. **[GKP, 2005]**

Definition 5.4. Improper and Proper Ideals.

Let $(R, +, \cdot)$ be a ring. The ideals R and $\{0\}$ are called *improper* or *trivial* ideals of R. Any ideal other than these two ideals is called a proper (*or non-trivial*) ideal of R.

Definition 5.5. Unit and Zero Ideals.

Let $(R, +, \cdot)$ be a ring. The ideals R and $\{0\}$ are called unit ideal and zero ideal (*or null ideal*) of R respectively.

Definition 5.6. Simple Ring.

A ring is called a simple ring if it has no proper ideals.

Example 5.1. The subring of even integers is an ideal of ring integers.

Example 5.2. The set $\{mx : x \in Z\}$ is an ideal of the ring of integers. m being any fixed integer.

Example 5.3. The set S of all matrices of the type $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ with a and b as integers, forms a *left ideal* of the ring S of all 2×2 matrices with elements as integers.

Example 5.4. The set S of all matrices of the type $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$ with a and b as integers, forms a *right ideal* of the ring R of all 2×2 matrices with elements as integers.

Example 5.5. If R is a ring, then the set $\{x \in R : ax = 0\}$ is a *right ideal* of R. a being a fixed element of R.

Example 5.6. If R is a ring, then the set $\{x \in R : xa = 0\}$ is a *left ideal* of R. a being a fixed element of R.

Example 5.7. The set S of integers is a subring of the ring of rational numbers but S is not an ideal of R. For product of a rational and integer is not always an integer.

For example $$2 \in S, \frac{1}{4} \in R \Rightarrow 2 \times \frac{1}{4} = \frac{1}{2} \notin S.$$

Example 5.8. The set S of rational numbers is subring of the ring R of real numbers, but S is not an ideal of R. For product of a rational number

and a real number is not always a rational number. For example

$$2 \in S, \frac{1}{\sqrt{5}} \in R \Rightarrow 2 \times \frac{1}{\sqrt{5}} = \frac{2}{\sqrt{5}} \notin S.$$

Definition 5.7. Smallest Left Ideal Containing a Given Subset.

Let M be any non-empty subset of a ring R. A left ideal S of R, containing M, is called the smallest left ideal of R, if S contains M and S is contained in every left ideal of R, containing M. That is to say, a left ideal S of R, containing M, is called smallest left ideal of R if :

(i) $S \supset M$.

(ii) $M \subset K \subset R$, K is any left ideal of $R \Rightarrow K \supset S$.

Remark 5.1. Similarly we define :

(i) Smallest right ideal containing a given subset.

(ii) Smallest ideal containing a given subset.

Definition 5.8. Let M be a non-empty subset of a ring R. The smallest left ideal S (or R) containing M, is called the **left ideal generated** by M and is denoted by (M). Thus $S = (M)$.

Definition 5.9. Let a be an arbitrary element of a ring R. The set $\{ra + ma : r \in R, m \in Z\}$ is defined as the **left ideal generated by an element a.** The expression for left ideal can be simplified if R is a ring with unity element e. In this case

$$\begin{aligned} ra + ma &= ra + m(ea). \text{ For } a = ea. \\ &= (r + me)\, a \\ &= (r + r')\, a, \text{ where } r' = me \in R \\ &= sa, \text{ where } r + r' = s \in R. \end{aligned}$$

Thus if R is a ring with unity element e, then the left ideal generated by an element $a \in R$ is $\{sa : s \in R\} \subset R$.

Definition 5.10. A left ideal generated by a single element $a \in R$ is also called *principal left ideal* of R. The set

$$\{ra + ma : r \in R, m \in Z\}$$

is principal left ideal of R. a being a fixed element of R.

If R is a ring with unity element e and $a \in R$, then Ra is principal left ideal of R.

Remark 5.2. Similarly we define right ideal generated by a single element. Thus

(i) If a is an arbitrary element of a ring R, then the set

$$\{ar + am : r \in R, m \in Z\}$$

is a right ideal of R, **generated by an element** a.

This set is also defined as **principal right ideal** of R. If R is a ring with unity element e, then aR is defined as right ideal generated by an element

$a \in R$. aR is also defined as principal right ideal of R.

Definition 5.11. Principal Ideal.

An ideal of a ring R is called principal ideal of R if it is generated by a single element of R.

That is to say, the set

$$\{ra + as + ma : r, s \in R \text{ and } m \in Z\}$$

is a principal ideal of R, generated by a single element a ∈ R. This set is also called ideal generated by an element a ∈ R. The expression for principal ideal can be simplified if R is a ring with unity element e.

In this case

$$\begin{aligned} ra + as + ma &= ra + as + m(ea). \text{ For } a = ea \\ &= ra + as + (me)\, a \\ &= ra + as + r'\, a, \text{ where } r' = me \in R \\ &= (r + r')\, a + as \\ &= s'a + as, \text{ where } s' = r + r' \in R. \end{aligned}$$

Hence a principal ideal of R is the set {s'a + as : s, s' ∈ R} if R is a ring with unity element e.

Remark 5.3. If R is a ring with unity elements, then

(i) $Ra = \{ra : r \in R\}$ is a principal left ideal of R.

(ii) $aR = \{ar : r \in R\}$ is a principal right ideal of R.

(iii) $\{ra + ar : r \in R\}$ is a principal ideal of R,

a being an element of R.

Remark 5.4. If R is a ring with unity element e, then the principal ideal generated by e is the whole ring R. For $re = er \; \forall \; r \in R$.

Hence the ring R is called **unit ideal.**

Remark 5.5. If R is a ring with unity element, then the principal ideal generated by the zero element 0 is the ring {0}.

For $0.r = 0 \qquad \forall \; r \in R.$

Hence the ring {0} is called zero ideal.

Definition 5.12. Principal Ideal Ring. (GKP, 2006)

A ring, for which every ideal is a principal ideal, is called principal ideal ring.

The commutative rings are examples of principal ideal rings.

Definition 5.13. Principal Ideal Domain.

An intergral domain is called principal ideal domain if its every ideal is a principal ideal.

Definition 5.14. Prime Ideal.

An ideal S of a ring R is called a prime ideal of R if

$$ab \in S \Rightarrow a \in S \text{ or } b \in S.$$

Notation . If an ideal S of a ring R is generated by an element $a \in R$, then we write. $S = (a)$.

Similarly if an ideal S of a ring R is generated by elements $a, b \in R$, then we write $S = (\{a,b\})$.

Example 5.9. In the ring Z of integers

(i) $S = \{3r : r \in Z\}$ is a prime ideal of R generated by 3 and we also write $S = (3)$.

Here $ab \in S \Rightarrow 3 \mid ab$. Also 3 is prime

$\Rightarrow 3 \mid a$ or $3 \mid b$

$\Rightarrow a \in S$ or $b \in S$

$\Rightarrow S$ is prime.

Similarly (5), (7), (11) etc. are examples of prime ideals. Therefore the set $\{mr : r \in Z\}$ is a prime ideal of the ring of integers for every prime integer m.

(ii) The ideal $\{4r : r \in Z\} = (4)$ is not prime.

For $ab \in (4) \Rightarrow 4 \mid ab$. Also 4 is composite integer,

does not imply $4 \mid a$ or $4 \mid b$

$\Rightarrow\!\!\!\!\!\!\not\;\; a \in (4)$ or $b \in (4)$.

Hence $ab \in (4)$ does not imply $a \in (4)$ or $b \in (4)$.

Therefore (4) is not prime.

For example $6.2 \in (4)$, but neither 6 nor 2 belongs to (4).

Definition 5.15. Maximal Ideal.

An ideal S of a ring R is called a maximal ideal of R if

(i) S is propely contained in R, i.e., $S \subset R$ and $S \neq R$.

(ii) S' is an ideal of R, $S \subset S' \Rightarrow S' = R$ or $S' = S$.

Example 5.10 Consider the ring R of integers :

$(2) = \{2x : x \in Z\} = \{0, \pm 2, \pm 4, \pm 6, \pm 8, \pm 10, ...\}$

$(3) = \{0, \pm 3, \pm 6, \pm 9, \pm 12, \pm 15, ...\}$

$(4) = \{0, \pm 4, \pm 8, \pm 12, \pm 16, \pm 20, ...\}$

$(5) = \{0, \pm 5, \pm 10, \pm 15, \pm 20, \pm 25, ...\}$

$(6) = \{0, \pm 6, \pm 12, \pm 18, \pm 24, \pm 30, ...\}$

Evidently $(6) \subset (2)$, $(6) \subset (3)$.

Hence if m is a composite, say $m = ab$, then

$$(m) \subset (a), (m) \subset (b).$$

(3), (5), (7) are maximal ideals of the ring of integers.

Definition 5.16. Quotient Ring.

Let S be an ideal of a ring R. Let R/S denote the family of cosets of S in R, i.e., $R/S = \{S + a : a \in R\}$.

Let $S + a$, $S + b$ be arbitrary elements of R/S. Define the operations of

addition and multiplication on R/S as follows :

$$(S + a) + (S + b) = S + (a + b)$$
$$(S + a)(S + b) = S + ab.$$

Then R/S is a ring w.r.t. these operations. (Refer Theorem 5.19).

This ring $(R/S, +, \cdot)$ is called *quotient ring or factor ring or difference ring or residue class ring.* [GKP, 2005]

Theorem 5.1. The quotient ring R/S is an integral domain iff S is prime.

Proof. See theorem 5.22.

Theorem 5.2. The intersection of two left ideals is a left ideal.

Proof. Let S_1 and S_2 be two left ideals of a ring R so that

(i) S_1 and S_2 both are additive subgroups of R,

(ii) $r \in R, a \in S_1 \Rightarrow ra \in S_1$.

and $r \in R, a \in S_2\ ra \in S_2$.

Since intersection of two subgroups is a subgroup and

$$r \in R, a \in S_1 \cap S_2 \Rightarrow r \in R, a \in S_1 \text{ and } a \in S_2$$
$$\Rightarrow r \in R, a \in S_1 \text{ and } r \in R, a \in S_2$$
$$\Rightarrow ra \in S_1 \text{ and } ra \in S_2 \text{ according to (ii)}$$
$$\Rightarrow ra \in S_1 \cap S_2.$$

Hence the result follows.

Theorem 5.3. *To prove that the intersection of any family of left ideals of a ring is a left ideal.*

Proof. Let S_r be a left ideal of a ring R for $r = 1,2,3, \ldots$ so that

(i) S_r is a additive subgroup of R.

(ii) $x \in R, a \in S_r \Rightarrow xa \in S_r$ for $r = 1, 2, 3, \ldots$

Since an arbitrary intersection of subgroups is again a subgroup,

$$x \in R, a \in \bigcap_{r=1}^{\infty} S_r \Rightarrow x \in R, a \in S_r \text{ for } r = 1, 2, 3, \ldots$$
$$\Rightarrow xa \in S_r \text{ for } r = 1, 2, 3, \ldots$$
[This follows from (Ii)]
$$\Rightarrow xa \Rightarrow \bigcap_{r=1}^{\infty} S_r.$$

Hence the result follows.

The intersection of any family of **right ideals** is a right ideal.

The proof is similar to Theorem 5.3.

Theorem 5.4. *The intersection of two ideals is an ideal.*

[GKP, 84, 99, 2004, PU, 96]

Proof. Let S_1 and S_2 be ideals of a ring R so that

(i) S_1 and S_2 both are additive subgroups of R

(ii) $r \in R, a \in S_1 \Rightarrow ra, ar \in S_1$

and $r \in R, a \in S_2 \Rightarrow ra, ar \in S_2$

To prove that $S_1 \cap S_2$ is an ideal of R.

For this we have to prove the following.

(iii) $S_1 \cap S_2$ is additive subgroup of R.

(iv) $r \in R, a \in S_1 \cap S_2 \Rightarrow ra, ar \in S_1 \cap S_2$

Evidently (i) $\Rightarrow$ (iii),

$r \in R, a \in S_1 \cap S_2 \Rightarrow r \in R, a \in S_1$ and $a \in S_2$

$\Rightarrow r \in R, a \in S_1$ and $r \in R, a \in S_2$

$\Rightarrow ra, ar \in S_1$ and $ra, ar \in S_2$ by (ii)

$\Rightarrow ra, ar \in S_1 \cap S_2 \Rightarrow$ (iv).

Theorem 5.5. *Show that the intersection of any arbitrary family of ideals of a ring is itself an ideal.*

Proof. Let, S_r be an ideal of a ring R for $r = 1, 2, 3, \ldots$ so that

(i) S_r is a additive subgroup of R.

(ii) $a \in S_r, x \in R \Rightarrow ax, xa \in S_r$ for $r = 1, 2, 3, \ldots$

To prove that $\bigcap_{r=1}^{\infty} S_r$ is an ideal of R.

For this we have to prove the following :

(iii) $\bigcap_{r=1}^{\infty} S_r$ is additive subgroup of R.

(iv) $x \in R, a \in \bigcap_{r=1}^{\infty} S_r \Rightarrow xa, ax \in \bigcap_{r=1}^{\infty} S_r$.

Evidently (i) $\Rightarrow$ (iii),

For an arbitrary intersection of subgroups is again a subgroup,

$x \in R, a \in \bigcap_{r=1}^{\infty} S_r \Rightarrow x \in R, a \in S_r$ for $r = 1, 2, 3, \ldots$

$\Rightarrow xa, ax \in S_r$ for $r = 1, 2, 3, \ldots$

[This follows from (ii)]

$\Rightarrow xa, ax \in \bigcap_{r=1}^{\infty} S_r$.

Hence the result (iv).

Theorem 5.6. *A field has no proper ideals.*

or

A field F has only two ideals namely {0} and F. (GKP., 2006)

Proof. Let S be an arbitrary ideal of a field F. To prove that F has no proper ideal, *i.e.*, to prove that F has only two improper ideals namely {0} and F.

For this we have to show that

$$S = \{0\} \text{ or } S = F.$$

If $S = \{0\}$, then the theorem is proved.

Consider the case in which $S \neq \{0\}$.

Then $\exists\ a \in S$ s.t $a \neq 0$

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

$a \in S, a^{-1} \in F \Rightarrow a^{-1}\, a \in S$, by def. of ideal $\Rightarrow 1 \in S$

any $x \in F \Rightarrow x \in F, 1 \in S \Rightarrow 1x \in S$ by def. ideal

$\Rightarrow x \in S$

$\therefore$ $F \subset S$. But $S \subset F$. Combining the two,

$S = F$.

This proves the theorem.

Theorem 5.7. *A commutative ring with unity is a field if it has no proper ideals.* (GKP., 2007)

An Alternative Statement. *A commutative ring R with unity, whose only ideals are null ideal and unit ideal, is a field.*

Proof. Let R be a commutative ring with unity element s.t. R has no proper ideals so that the only ideals of R are $\{0\}$ and R.

To prove that R is a field.

We know that a field is a commutative ring with unity s.t. every non-zero element of R has a multiplicative inverse in R.

Let $a \in R$ be arbitrary s.t. $a \neq 0$.

If we show that $a^{-1} \in R$, then the result will follow.

It can be shown that $Ra = \{ra : r \in R\}$ is an ideal of R.

(Refer Theorem 5.11)

By assumption, $Ra = \{0\}$ or R

$1 \in R \Rightarrow 1.a \in Ra \Rightarrow a \in Ra \Rightarrow Rs \neq \{0\}$

$\Rightarrow Ra = R$. For $Ra = R$ or $\{0\}$

Also $1 \in R$. Hence $1 \in Ra$ and so that $\exists\ b \in R$ s.t. $ba = 1$. But R is commutative.

$\therefore$ $ba = ab = 1$.

This $\Rightarrow a^{-1} = b, b \in R \Rightarrow a^{-1} \in R$.

Hence the theorem.

Theorem 5.8. *If R is a commutative ring with unity, then it is a field iff it has no proper ideals.*

Proof. (i) suppose R is a commutative ring with unity s.t. R has no proper ideals.

To prove that R is a field. [For proof refer Theorem 5.7].

(ii) Let R be a commutative ring with unity s.t. it is a field.

To prove that R has no proper ideals, *i.e.*, to prove that R has only improper ideals namely $\{0\}$ and R. [For proof refer theorem 5.6].

Theorem 5.9. *Let R be a ring with unity element such that the only*

right ideals of R are {0} and R. Prove that R is a division ring.

Solution. Recall that a ring R with unity is a division ring if the non-zero elements of R form a multiplicative group.

Let R be a ring with unity element. Let the only right ideals of R be $\{0\}$ and R.

To prove that R is a division ring, we have to show that every non-zero element of R has a multiplicative inverse in R.

Let $a \neq 0 \in R$ be arbitrary. To prove $a^{-1} \in R$.

It can be shown that $aR = \{ar : r \in R\}$ is a right ideal of R. (Refer Theorem 5.11).

By assumption $aR = R$ or $\{0\}$

$$1 \in R \Rightarrow a.1 \in aR \Rightarrow a \in aR \Rightarrow aR \neq \{0\}$$
$$\Rightarrow aR = R.$$

Thus $aR = R$.

Now $1 \in R \Rightarrow 1 \in aR$ ($\because aR = R$) $\Rightarrow \exists\ b \in R$ s.t. $1 = ab$

$\Rightarrow$ Right multiplicative inverse of a is b

$\Rightarrow$ inverse of a is b

$\Rightarrow a^{-1} = b \in R$.

Theorem 5.10. *A division ring is a simple ring.*

Proof. Let R be a division ring so that R is a ring s.t. its non-zero elements form a multiplicative group.

To prove that R is a simple ring, we have to show that R has only two ideals namely $\{0\}$ and R.

Let S be an arbitrary ideal of R. If we show that $S = \{0\}$ or $S = R$ the result will follow.

If $S = \{0\}$, then the theorem is proved.

Consider the case in which $S \neq \{0\}$,

$a \in S \subset R \Rightarrow a \in R, a \neq 0 \Rightarrow a^{-1} \in R$

[For non-zero elements of R form multiplicative group]

$a \in S, a^{-1} \in R \Rightarrow a^{-1} a \in S$, by def. of ideal $\Rightarrow 1 \in S$

any $x \in R \Rightarrow x \in R, 1 \in S \Rightarrow 1x \in S$ by def. of ideal

$\Rightarrow x \in S$

$\therefore\ R \subset S$. But $S \subset R$.

Combining the two, $S = R$.

This proves the theorem.

Theorem 5.11. *If R be a commutative ring and $a \in R$, then show that $Ra = \{ra : r \in R\}$ is an ideal of R.*

Proof. Let R be a commutative ring and let

$$a \in R, Ra = \{ra : r \in R\}.$$

To prove that Ra is an ideal of R.

For this we have to show that

(i) Ra is additive subgroup of R.

(ii) $r \in R, u \in Ra \Rightarrow ru \in Ra, ur \in Ra$.

Let $x, y \in Ra$ be arbitrary, then $\exists\ r,s \in R$ s.t.

$$x = ra, y = sa \qquad ...(1)$$

$r, s \in R \Rightarrow r \in R, -s \in R$. For $(R, +)$ is an Abelian group

$\Rightarrow r + (-s) \in R \Rightarrow r - s \in R \Rightarrow (r - s)\, a \in Ra$

$\Rightarrow x - y \in Ra$, by (1).

Thus $x, y \in Ra \Rightarrow x - y \in Ra$.

This proves the result (i).

(ii) Let $r \in R, u \in Ra$ be arbitrary.

Then $u = r'$ a for some $r' \in R$.

$$ru = r(r'\, a) = (rr')\, a. \qquad ...(2)$$

But $r, r' \in R \Rightarrow rr' \in R$. For $(R, +, \cdot)$ is a ring

$\Rightarrow (rr')\, a \in Ra \Rightarrow ru \in Ra$, by (2).

But $Ra \subset R$ and R is commutative. $\therefore\ ur = ru$.

Consequently, $r \in R, u \in Ra \Rightarrow ru, ur \in Ra$.

Hence the result (ii).

Theorem 5.12. *If R is a commutative ring with unity and $a \in R$, then $Ra = \{ra : r \in R\}$ is a principal ideal of R, generated by a.*

Proof. Let R be commutative ring with unity element e and $a \in R$,

$$Ra = \{ra : r \in R\}.$$

(i) To prove that Ra is an ideal of R.

(Write the proof of Theorem 5.11)

(ii) To prove that $Ra = (a)$, *i.e.*, the ideal Ra is generately by a.

Let S be an ideal generated by an element of a, so that $S = (a)$

$$S = (a) = \{ra + as + ma : r, s \in R \text{ and } m \in Z\} \qquad ...(3)$$

$ra + as + ma = ra + sa + ma$. For R is commutative.

$= ra + sa + m\,(ea)$. For $ea = ae = a$

$= ra + sa + (me)\, a$

$= ra + sa + r'\, a$, where $me = r' \in R$

$= (r + s + r')\, a$

$= xa$, where $x = r + s + r' \in R$

Finally, $ra + as + ma = xa, x \in R$.

Hence, (3) becomes

$$S = \{xa : x \in R\} = Ra.$$

But $S = (a)$. Hence $Ra = (a)$.

Now we have shown that Ra is an ideal generated by a single element

a. By definition, Ra is a principal ideal of R.

Theorem 5.13. *The ring of integers is a principal ideal domain.*

or

The ring of integers is a principal ideal ring.

Proof. Let **Z** denote the ring of integers. Also **Z** is integral domain.

Let S be an ideal of **Z**.

If we show that S is a principal ideal of **Z**, the result will follow :

If $S = \{0\}$, then S is clearly a principal ideal.

Now consider the case in which $S \neq \{0\}$.

Consequently $\exists$ at least an element $a \in S$ s.t. $a \neq 0$.

$a \in S \Rightarrow -a \in S$. For $(S, +)$ is additive subgroup of **Z**.

Of course one of a and $-a$ is necessarily positive. Thus S contains positive integers. Let S^+ be the set of positive elements of S.

We know that every set of positive elements has a least member, say b. Hence S^+ has the least element b.

We claim $S = (b)$, *i.e.*, S is an ideal generated by b.

Let $x \in S$ be arbitrary. By division algorithm, $\exists$ integers q and r s.t.

$$x = bq + r,\ 0 \leq r < b,$$

$$b \in S, q \in Z \Rightarrow bq \in S. \text{ For } S \text{ is an ideal.}$$

$$x \in S, bq \in S \Rightarrow x \in S, -bq \in S. \text{ For } (S, +) \text{ is a group}$$

$$\Rightarrow x + (-bq) \in S \Rightarrow x - bq \in S$$

$$\Rightarrow r \in S.$$

Now $r \in S$, $0 \leq r < b$, b is the least element of S.

Therefore $r = 0$.

$\therefore x = bq$ for some $q \in \mathbf{Z}$.

Hence $$S = \{bq : q \in \mathbf{Z}\} = (b).$$

Thus S is an ideal of **Z**, generated by a single element b. Hence S is a principal ideal.

Theorem 5.14. *Every field is a principal ideal ring.*

Proof. Let F be a field.

To prove that F is a principal ideal ring, we have to show that every ideal of F is a principal ideal.

We know that a field has only two ideals namely {0} and F, by Theorem 5.6 But the null ideal {0} is generated by 0, and unit ideal F is generated by the unity element. Thus both these ideals are principal ideals. Hence the theorem follows.

Theorem 5.15. Sum of two ideals. *Let S_1 and S_2 be ideals of a ring R and let $S_1 + S_2 = \{a_1 + a_2 : a_1 \in S_1, a_2 \in S_2\}$. Then $S_1 + S_2$ is an ideal of R, generated by $S_1 \cup S_2$.*

Proof. Let S_1 and S_2 be ideals of a ring R so that

(i) S_1 and S_2 are additive subgroups of R.

(ii) $r \in R, a_1 \in S_1 \Rightarrow ra_1, a_1 r \in S_1$,

and $r \in R, a_2 \in S_2 \Rightarrow ra_2, a_2 r \in S_2$.

Also let $S_1 + S_2 = \{a_1 + a_2 : a_1 \in S_1, a_2 \in S_2\}$.

To prove that $S_1 + S_2$ is an ideal of R, generated by $S_1 \cup S_2$.

(iii) $S_1 + S_2$ is an additive subgroup of R.

For $a_1 + a_2 \in S_1 + S_2, b_1 + b_2 \in S_1 + S_2$

$\Rightarrow a_1 \in S_1, a_2 \in S_2; b_1 \in S_1, b_2 \in S_2$

$\Rightarrow a_1, b_1 \in S_1$ and $a_2, b_2 \in S_2$

$\Rightarrow a_1 - b_1 \in S_1$ and $a_2 - b_2 \in S_2$, according to (i)

$\Rightarrow (a_1 - b_1) + (a_2 - b_2) \in S_1 + S_2$

$\Rightarrow (a_1 + a_2) - (b_1 + b_2) \in S_1 + S_2$.

For $(R, +)$ is an Abelian group,

i.e., $a_1 + a_2, b_1 + b_2 \in S_1 + S_2 \Rightarrow (a_1 + a_2) - (b_1 + b_2) \Rightarrow S_1 + S_2$.

(iv) $r \in R, a_1 + a_2 \in S_1 + S_2 \Rightarrow r(a_1 + a_2)$ and $(a_1 + a_2) r \in S_1 + S_2$

For $r \in R, a_1 + a_2 \in S_1 + S_2$

$\Rightarrow r \in R, a_1 \in S_1, a_2 \in S_2$

$\Rightarrow r \in R, a_1 \in S_1$ and $r \in R, a_2 \in S_2$

$\Rightarrow ra_1, a_1 r \in S_1$ and $ra_2, a_2 r \in S_2$, by (ii)

$\Rightarrow ra_1 + ra_2 \in S_1 + S_2$ and $a_1 r + a_2 r \in S_1 + S_2$

$\Rightarrow r(a_1 + a_2) \in S_1 + S_2$ and $(a_1 + a_2) r \in S_1 + S_2$.

The conditions (iii) and (iv) taken together declare that $S_1 + S_2$ is an ideal of R.

Remains to prove that $S_1 + S_2$ is generated by $S_1 \cup S_2$ i.e,

$S_1 + S_2 = (S_1 \cup S_2)$.

Since $0 \in S_1, 0 \in S_2$ according to (i)

$a_1 \in S_1 \Rightarrow a_1 \in S_1, 0 \in S_2 \Rightarrow a_1 = a_1 + 0 \in S_1 + S_2$

$\Rightarrow a_1 \in S_1 + S_2$

This $\Rightarrow S_1 \subset S_1 + S_2$.

Similarly we can show that $S_2 \subset S_1 + S_2$.

Now $S_1 \subset S_1 + S_2, S_2 \subset S_1 + S_2$

$\Rightarrow S_1 \cup S_2 \subset (S_1 + S_2) \cup (S_1 + S_2) = S_1 + S_2$

$\Rightarrow S_1 \cup S_2 \subset S_1 + S_2$.

Thus $S_1 + S_2$ is an ideal containing $S_1 \cup S_2$.

Also if S is any ideal of R containing $S_1 \cup S_2$, *then S must contain* $S_1 + S_2$. Consequently $S_1 + S_2$ is the smallest ideal of R, containing $S_1 \cup S_2$, *i.e.* $S_1 + S_2 = (S_1 \cup S_2)$.

Theorem 5.16. *If S_1 and S_2 are left ideals of a ring R, then*

$$S_1 + S_2 = \{a_1 + a_2 : a_1 \in S_1, a_2 \in S_2\}$$

is a left ideal of R, generated by $S_1 \cup S_2$.

Another Statement. *The left ideal generated by the union* $S_1 \cup S_2$ *of two ideals is the set* $S_1 + S_2$ *containing of the elements of R obtained on adding any element of* S_1 *to any element of* S_2.

Proof. Let S_1 and S_2 be left ideals of a ring R so that

(i) S_1 and S_2 are additive subgroups of R.

(ii) $r \in R, a_1 \in S_1 \Rightarrow ra_1 \in S_1$

and $r \in R, a_2 \in S_2 \Rightarrow ra_2 \in S_2$.

Also let $S_1 + S_2 = \{a_1 + a_2 : a_1 \in S_1, a_2 \in S_2\}$.

To prove that $S_1 + S_2$ is a left ideal of R, generated by $S_1 \cup S_2$.

For this we have to prove the following :

(iii) $S_1 + S_2$ is additive subgroup of R.

(iv) $r \in R, a_1 + a_2 \in S_1 + S_2 \Rightarrow r(a_1 + a_2) \in S_1 + S_2$.

(v) $S_1 + S_2 = (S_1 \cup S_2)$.

Now the proof can be completed with the help of Theorem 5.15.

Theorem 5.17. *An ideal S of the ring of integers R is maximal if and only if S is generated by some prime integer.* **(I.A.S. 1997)**

Proof. Let S be an ideal of the ring of integers R. We know that R is a principal ideal ring (Refer Theorem 5.13). Hence S is a principal ideal and therefore we can suppose that this ideal is generated by a single integer, say p. Since p and $-p$ both generate the same ideal and therefore we take p as positive integer. Then we write $S = (p)$.

We have to prove that

(i) p is prime $\Rightarrow S$ is maximal.

(ii) S is maximal $\Rightarrow p$ is prime.

(i) Let p be prime and let S' be an ideal of R s.t. $S \subset S' \subset R$. Since S' is a principal ideal and so we take $S' = (q)$, where q is some positive integer.

$$S \subset S' \Rightarrow (p) \subset (q) \Rightarrow p \in (q)$$
$$\Rightarrow p \in \{qx : x \in Z\}$$
$$\Rightarrow p = qn \text{ for some positive integer } n.$$

Also p is prime.

$$\Rightarrow \text{either } n = 1, q = p; \text{ or } n = p, q = 1$$
$$\Rightarrow q = p \text{ or } q = 1$$
$$\Rightarrow (q) = (p) \text{ or } (q) = (1)$$
$$\Rightarrow S' = S \text{ or } S' = R.$$

Finally $S \subset S' \subset R \Rightarrow S' = S$ or $S' = R$.

Therefore S' is maximal.

(ii) Let S be maximal.

To prove p is prime.

Suppose the contrary. Then p is composite.

Let us take $p = mn$, where $m, n \neq 1$.

$p = mn \Rightarrow (p) \subset (m) \subset (1) = R, (p) \subset (n) \subset (1) = R$

$\Rightarrow S \subset (m) \subset R$. Also S is maximal

$\Rightarrow (m) = S$ or $(m) = R$.

$(m) = R \Rightarrow (m) = (1)$. For $(1) = R$

$\Rightarrow m = 1$. A contradiction. For $m \neq 1$.

$(m) = S \Rightarrow (m) = (p) \Rightarrow (m) = \{px : x \in \mathbf{Z}\}$

$\Rightarrow m = pr$ for some integer r. Also $p = mn$

$\Rightarrow m = mnr \Rightarrow nr = 1$. For $m \neq 0$

Also n and r integers.

$\Rightarrow r = 1$ and $n = 1$.

In Particular $n = 1$. A contradiction. For $n \neq 1$.

Hence p must be prime.

Theorem 5.18 *Let R be a commutative ring with unity and let a and b be non-zero elements of R. Then $(a) = (b)$ iff a and b are associates.*

Proof. Let R be a commutative ring with unity.

Let $a, b \in R$ be arbitrary s.t. $a, b \neq 0$.

$(a) = \{ax : x \in \mathbf{Z}\}, (b) = \{bx : x \in \mathbf{Z}\}$.

$(a) = (b) \Rightarrow (a) \subset (b)$ and $(b) \subset (a)$

$\Rightarrow a \in (b), b \in (a)$

$\Rightarrow a = br, b =$ as for some $r, s, \in R$

$\Rightarrow b \mid a, a \mid b \Rightarrow a$ and b are associates.

Conversely $a \mid b, b \mid a \Rightarrow b = am, a = bn$ for some $m, n \in R$

$\Rightarrow b \in (a), a \in (b)$

$\Rightarrow (b) \subset (a), (a) \subset (b)$

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

Theorem 5.19. *If S is an ideal of a ring R, then the set*

$$R/S = \{S + a : a \in R\}$$

is a ring for the two operations in R/S defined as

$$(S + a) + (S + b) = S + (a + b)$$

$$(S + a)(S + b) = S + ab \quad \forall\ a, b \in R.$$ **[GKP, 2005]**

Proof I. Let $a, b, c, a', b', c' \in R$ be arbitrary, then $S + a \in R/S$ etc.

First of all we shall show that these operations are well defined. For proving this we have to prove that

$S + a = S + a'$ and $S + b = S + b' \Rightarrow (S + a) + (S + b) = (S + a') + (S + b')$

and $(S + a)(S + b) = (S + a')(S + b')$

$S + a = S + a' \Rightarrow a \in S + a' \Rightarrow a = \alpha + a'$ for some $\alpha \in S$.

Similarly $S + b = S + b' \Rightarrow b = \beta + b'$ for some $\beta \in S$.

Now $a = \alpha + a', b = \beta + b'$.

$\therefore$ $a + b = (\alpha + a') + (\beta + b')$

$= (\alpha + \beta) + (a' + b')$. For (R, +) is an Abelian group

or $(a + b) - (a' + b') = \alpha + \beta$.

But $\alpha, \beta \in S \Rightarrow \alpha + \beta \in S$. For (S, +) is a subgroup of R

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

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

$\Rightarrow (S + a) + (S + b) = (S + a') + (S + b')$.

Thus addition in *R/S* is well defined.

$ab = (\alpha + a')(\beta + b') = \alpha\beta + ab' + a'\beta + a'b'$

$ab - a'b' = \alpha\beta + (ab' + a'\beta)$ ...(1)

Since S is two sided ideal

$\alpha, \beta \in S$ and $a', b' \in R \Rightarrow \alpha b', a'\beta, \alpha\beta \in S$

$\Rightarrow \alpha\beta + \alpha b' + a'\beta \in S$

[For (S, +) is subgroup of R]

$\Rightarrow ab - a'b' \in S$, by (1)

$\Rightarrow S + ab = S + a'b'$

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

$\Rightarrow$ multiplication in R/S is well defined.

Proof II. Next our aim is to show that (R/S, +, ·) is a ring.

(i) R/S is closed w.r.t. (+) and (·),

i.e. $(S + a) + (S + b) \in R/S, (S + a)(S + b) \in R/S$.

For $a, b \in R \Rightarrow a + b, ab \in R$. For (R +, ·) is a ring

$\Rightarrow S + (a + b), S + ab \in R/S$

$\Rightarrow (S + a) + (S + b) \in R/S$

and $(S + a)(S + b) \in R/S$.

(ii) *Addition is commutative in R/S,*

i.e. $(S + a) + (S + b) = (S + b) + (S + a)$.

For (*R*, +) is an Abelian group $\Rightarrow a + b = b + a$

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

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

(iii) *Addition is associative in R/S.*

i.e. $[(S + a) + (S + b)] + (S + c) = (S + a) + [(S + b) + (S + c)]$

For L.H.S. $= [S + (a + b)] + (S + c) = S + [(a + b) + c]$

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

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

$= \text{R.H.S.}$

(iv) *Multiplication is associative in R/S.*

i.e. $[(S+a)(S+b)](S+c) = (S+a)[(S+b)(S+c)]$

For L.H.S. $= (S+ab)(S+c) = S+(ab)c = S+a(bc)$

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

$= \text{R.H.S.}$

(v) *Existence of additive identity.*

$0 \in R \Rightarrow S = S+0 \in R/S.$

Also $(S+a)+(S+0) = S+(a+0) = S+a.$

Thus $\exists$ additive identity $S = 0+S \in R/S.$

(vi) *Existence of additive inverse,*

$S+(-a) = S-a \in R/S$ is additive inverse of $S+a \in R/S.$

For $a \in R \Rightarrow -a \in R$

$\Rightarrow S+(-a) \in R/S$

$\Rightarrow (S+a)+[S+(-a)] = S+(a-a) = S+0 = S$

$\Rightarrow S-a$ is additive inverse of $S+a \in R/S.$

(vii) *Multiplication is distributive over addition, i.e.,*

$(S+a)[(S+b)+(S+c)] = (S+a)(S+b)+(S+a)(S+c)$ ...(2)

$[S+b)+(S+c)](S+a) = (S+b)(S+a)+(S+c)(S+a)$ ...(3)

For L.H.S. of (2) $= (S+a)[S+(b+c)] = S+a(b+c)$

$= S+(ab+ac) = (S+ab)+(S+ac)$

$= (S+a)(S+b)+(S+a)(S+c)$

$= \text{R.H.S. of (2).}$

Similarly we can prove (3).

Hence $(R/S, +, \cdot)$ is a ring. R/S is called Quotient ring.

Theorem 5.20. Suppose R/S is a quotient ring. Then show that

(i) if R is commutative, the R/S is commutative.

(ii) if R has a unity element 1, so also has R/S namely $S+1$.

Proof. (i) R is commutative,

$\Rightarrow ab = ba \quad \forall\ a, b \in R$

$\Rightarrow S+ab = S+ba$

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

$\Rightarrow R/S$ is commutative.

(ii) R has unity element 1

$\Rightarrow 1 \in R$ and $a.1 = 1.a = a\ \forall\ a \in R$

$\Rightarrow S+1 \in R/S$ and $S+(a.1) = S+(1.a) = S+a$

$\Rightarrow S+1 \in R/S$ and $(S+a)(S+1) = (S+1)(S+a) = S+a$

$\Rightarrow S+1 \in R/S$ is unity element of R/S.

Theorem 5.21. An ideal S of a commutative ring R with unity is maximal iff the residue class (Quotient) ring R/S is a field.

Proof. Let R be a commutative ring with unity element so that R/S is a commutative ring with unity element. The zero element and unit element of R/S are S and S + 1 respectively.

Step I. Suppose the ideal S is maximal in R.

By assumption, R/S is a commutative ring with unity. Hence if we show that every non-zero element of R/S has a multiplicative inverse in R/S, then it will be proved that R/S is a field.

Let S + a be a non-zero element of R/S so that $S + a \neq S$. Consequently $a \notin S$.

Our aim is to prove that $(S + a)^{-1} \in R/S$.

(a) is principal ideal of R generated by a. Since sum of two ideals is an ideal.

Hence S + (a) is an ideal of R.

$a \notin S \Rightarrow$ S is properly contained in S + (a).

Also S is maximal ideal of R.

$\Rightarrow S + (a) = R.$

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

$S + (a) = R, 1 \in R \Rightarrow 1 \in S + (a)$

$\Rightarrow \exists\ b \in S, \alpha \in R$ s.t. $1 = b + \alpha a$

$\Rightarrow 1 - \alpha a = b \in S \Rightarrow 1 - \alpha a \in S$

$\Rightarrow S + 1 = S + \alpha a \Rightarrow S + 1 = (S + \alpha)(S + a)$

$\Rightarrow (S + \alpha)(S + a) = (S + 1)$

= unity element of R/S

$\Rightarrow (S + a)^{-1} = S + \alpha$ [For R/S is commutative]

Also $\alpha \in R$.

$\Rightarrow (S + a)^{-1} = S + \alpha, S + \alpha \in R/S$

$\Rightarrow (S + a)^{-1} \in R/S.$

Hence R/S is a field.

Step II. Suppose R/S is a field.

Let S′ be an ideal of R s.t. $S \subset S'$, $S \neq S'$. If we show that $S' = R$, the result will follow.

To prove $R \subset S'$.

Let $x \in R$ be arbitrary s.t. $x \notin S$ so that $S + x \neq S$.

$\because$ $S \subset S'$, $S' \neq S$.

Hence $\exists\ y \in S'$ s.t. $y \notin S$ so that $S + y \neq S$.

Finally, S + x and S + y are non-zero elements of R/S which is a field. Hence $\exists$ a non-zero element $S + z \in R/S$ s.t.

$$(S+y)(S+z) = S+x$$

[We may take $S+z = (S+y)^{-1}(S+x)$]

$$(S+y)(S+z) = S+x \Rightarrow S+yz = S+x$$
$$\Rightarrow yz - x \in S \subset S'$$
$$\Rightarrow yz - x \in S'.$$

Also $y \in S'$, $z \in R$; S' is an ideal of $R \Rightarrow yz \in S'$.

Again $yz \in S'$, $yz - x \in S' \Rightarrow yz - (yz - x) \in S' \Rightarrow x \in S'$

[For $(S', +)$ is a subgroup of S]

Thus, any $x \in R \Rightarrow x \in S'$.

Hence $R \subset S'$.

S' is an ideal of $R \Rightarrow S' \subset R$,

$S' \subset R$, $R \subset S' \Rightarrow S' = R$. Hence S is maximal in R.

Theorem 5.22. Let S be an ideal of a commutative ring with unity element. Then R/S is an integral domain iff S is prime.

Proof. Let S be an ideal of a commutative ring R with unity element so that the quotient ring R/S is commutative and has unity element. Let $a, b \in R$ be arbitrary. We know that a commutative ring with unity is an integral domain iff it has no zero divisors.

To prove that R/S is an integral domain iff S is prime, i.e., to prove that R/S has no zero divisors iff S is prime, i.e. is prime iff

$$(S+a)(S+b) = S \Rightarrow S+a = S, \text{ or } S+b = S.$$

Suppose S is prime. Then

$$(S+a)(S+b) = S \Rightarrow S+ab = S$$
$$\Rightarrow ab \in S$$
$$\Rightarrow a \in S \text{ or } b \in S. \text{ For S is prime}$$
$$\Rightarrow S+a = S \text{ or } S+b = S.$$

Conversely suppose

$$(S+a)(S+b) = S \Rightarrow S+a = S \text{ or } S+b = S \qquad \ldots(1)$$

From (1), $S+ab = S \Rightarrow S+a = S$ or $S+b = S$.

i.e. $ab \in S \Rightarrow a \in S$ or $b \in S$.

Hence S is prime.

Theorem 5.23. Let R be a commutative ring with unity. Then every maximal ideal of R is a prime ideal.

Proof. Firstly we shall prove a lemma.

Lemma. Let S be an ideal of a commutative ring with unity element. Then R/S is an integral domain iff S is prime.

Prove it as in Theorem 5.22.

Now we come to the proof of the main theorem. Let R be a commutative ring with unity element. Let S be a maximal ideal of R. Then R/S is a field.

(Refer Theorem 5.21). Every field is an integral domain.

Hence R/S is an integral domain. Now applying the lemma, we find that S is a prime ideal.

The converse of this theorem is not true, because every prime ideal is not necessarily a maximal ideal.

Example 5.11. *If R is a finite commutative ring (i.e., has only a finite number of elements) with unity element, prove that every prime ideal of R is a maximal ideal of R.*

Solution. Let R be a finite commutative ring with unity element and let S be a prime ideal of R.

S is prime ideal $\Rightarrow$ R/S is an integral domain. (Refer Theorem 5.22)
Also R is finite.
$\Rightarrow$ R/S is a finite integral domain
$\Rightarrow$ R/S is a field (Refer Theorem 4.4)
$\Rightarrow$ S is maximal ideal of R, by Th. 5.21.

Example 5.12. If A, B are two ideals of a ring, then the product

$$AB = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in A, b_i \in B \right\},$$

where n is a positive integer, is an ideal of R. Hence show that

$$AB \subset A \cap B.$$

An Alternate Statement. If S_1 and S_2 are two ideals of a ring R, then the set of all elements of the form $b_1b_2 + c_1c_2 + \ldots + l_1l_2$, where $b_1, \ldots, l_1 \in S_1$ and $b_2, \ldots, l_2 \in S_2$, is an ideal of R.

Solution. Suppose S_1 and S_2 are ideals of a ring R so that :

(i) S_1 and S_2 are additive subgroup of R.

(ii) $b_1 \in S_1, r \in R \Rightarrow b_1r, rb_1 \in S_1$.

and $b_2 \in S_2, r \in R \Rightarrow b_2r, rb_2 \in S_2$.

Let $S = S_1S_2$.

$S = \{b_1b_2 + c_1c_2 + \ldots l_1l_2; b_1, c_1, \ldots, l_1 \in S_1 \text{ and } b_2, c_2, \ldots, l_2 \in S_2\}$

Let $x, y \in S$ be arbitrary, then we can write.

$$x = b_1b_2 + c_1c_2 + \ldots + l_1l_2,$$
$$y = p_1p_2 + q_1q_2 + \ldots u_1u_2,$$

where $b_1, c_1, \ldots, l_1, p_1, q_1, \ldots u_1 \in S_1$

and $b_2, c_2, \ldots, l_2, p_2, q_2, \ldots, u_2 \in S_2$.

(iii) To prove that S is additive subgroup of R.

For this we have to show that $x, y \in S \Rightarrow x - y \in S$

$$x - y = (b_1b_2 + c_1c_2 + \ldots l_1l_2) - (p_1p_2 + q_1q_2 + \ldots + u_1u_2)$$
$$= b_1b_2 + c_1c_2 + \ldots + l_1l_2 + (-p_1)\, p_2 + (-q_1)\, q_2 + \ldots + (-u_1)\, u_2.$$

The condition (i) says that

$$p_1, q_1, \ldots, u_1 \in S_1 \Rightarrow -p_1, -q_1, \ldots, -u_1 \in S_1.$$

Now $b_1, c_1, \ldots, l_1, -p_1, -q_1, \ldots, -u_1 \in S_1$

and $b_2, c_2, \ldots, l_2, p_2, q_2, \ldots, u_2 \in S_2$.

By def. of S,

$$b_1b_2 + c_1c_2 + \ldots + l_1l_2 + (-p_1)\,p_2 + (-q_1)\,q_2 + \ldots + (-u_1)\,(u_2) \in S$$

i.e. $$x - y \in S.$$

(iv) To prove $r \in R, x \in S \Rightarrow rx, xr \in S$.

$$rx = r\,[b_1b_2 + c_1c_2 + \ldots + l_1l_2]$$
$$= (rb_1)\,b_2 + (rc_1)\,c_2 + \ldots (rl_1)\,l_2.$$

According to the condition (ii),

$r \in R$ and $b_1, c_1, \ldots, l_1 \in S_1 \Rightarrow rb_1, rc_1, \ldots, rl_1 \in S_1$

Also $b_2, c_2, \ldots, l_2 \in S_2$

$\Rightarrow (rb_1)\,b_2 + (rc_1)\,c_2 + \ldots + (rl_1)\,l_2 \in S$

$\Rightarrow rx \in S.$

Similarly $xr = b_1\,(b_2r) + c_1\,(c_2r) + \ldots + l_1\,(l_2r)$.

According to (ii),

$r \in R$ and $b_2, c_2, \ldots, l_1 \in S_2 \Rightarrow b_2r, c_2r, \ldots, l_2r \in S_2$

$\Rightarrow b_1\,(b_2r) + c_1(c_2r) + \ldots + l_1\,(l_2r) \in S$

$\Rightarrow xr \in S.$

The conditions (iii) and (iv) say that S is an ideal of R.

Remains to prove that $S_1S_2 \subset S_1 \cap S_2$.

Let $s \in S_1S_2$ be arbitrary, then we can write

$$s = \sum_{i=1}^{n} a_ib_i, \quad \text{where } a_i \in S_1, b_i \in S_2\ \forall\ i.$$

$a_i \in S_1 \Rightarrow a_i \in R.$

$a_i \in R, b_i \in S_2 \Rightarrow a_ib_i \in S_2$, by def. of ideal.

$b_i \in S_2 \Rightarrow b_i \in R.$

$a_i \in S_1, b_i \in R \Rightarrow a_ib_i \in S_1$, by def. of ideal.

$a_ib_i \in S_1, a_ib_i \in S_2 \Rightarrow a_ib_i \in S_1 \cap S_2.$

S_1, S_2 are ideals of R $\Rightarrow S_1 \cap S_2$ is ideal of R

$\Rightarrow S_1 \cap S_2$ is additive subgroup of R.

Therefore $a_ib_i \in S_1 \cap S_2 \quad \forall\ i \Rightarrow s = \sum_{i=1}^{n} a_ib_i \in S_1 \cap S_2.$

Thus any $s \in S_1S_2 \Rightarrow s \in S_1 \cap S_2.$

Hence $S_1S_2 \subset S_1 \cap S_2.$

Example 5.13. Find the principal ideal generated by 5, in the ring of

integers.

Solution. The ring of integers is a commutative ring with unity. Hence

$$(5) = \{5x : x \in Z\}$$
$$= \{0, \pm 5, \pm 10, \pm 15, \pm 20, ...\}.$$

Example 5.14. Let R be the ring of all real valued continuous functions on the closed interval [0, 1]. Let

$$M = \{f(x) \in R : f\left(\frac{1}{2}\right) = 0\}.$$

Prove that M is maximal ideal of R.

Solution. (i) To prove that M is additive subgroup of R. Let $f(x), g(x) \in M$ be arbitrary, then $f\left(\frac{1}{2}\right) = 0 = g\left(\frac{1}{2}\right)$.

$$f\left(\frac{1}{2}\right) - g\left(\frac{1}{2}\right) = 0 - 0 = 0.$$

Thus $f(x), g(x) \in M \Rightarrow f(x) - g(x) \in M.$ ...(1)

This proves the result (i).

(ii) Let $f(x) \in R, g(x) \in M$, then $g\left(\frac{1}{2}\right) = 0.$

Now $f\left(\frac{1}{2}\right) g\left(\frac{1}{2}\right) = \left[f\left(\frac{1}{2}\right)\right](0) = 0.$

$$g\left(\frac{1}{2}\right) f\left(\frac{1}{2}\right) = 0.f\left(\frac{1}{2}\right) = 0.$$

Thus $f(x) \in R, g(x) \in M \Rightarrow f(x)\, g(x) \in M$ and $g(x) f(x) \in M.$ ...(2)

From (1) and (2), it follows that M is an ideal of R.

(iii) To prove that M is maximal ideal of R. Let $\exists$ an ideal U of R s.t. $M \subset U$ and $M \neq U$. There $\exists\ g(x) \in U$ and $g(x) \notin M$ so that $g\left(\frac{1}{2}\right) = a \neq 0.$

Write $f(x) = g(x) - a$ ...(3)

Then $f\left(\frac{1}{2}\right) = g\left(\frac{1}{2}\right) - a = a - a = 0$, showing there by

$$f(x) \in M \subset U \text{ or } f(x) \in U.$$

Finally, $f(x) \in U, g(x) \in U.$

This $\Rightarrow g(x) - f(x) \in U$, by def. of ideal

$\Rightarrow a \in U$, by (2) $\Rightarrow 1 = aa^{-1} \in U \Rightarrow 1 \in U$

any $h(x) \in R \quad \Rightarrow h(x) \in R, 1 \in U \Rightarrow 1h(x) \in U$

$\Rightarrow h(x) \in U.$

$\therefore \quad R \subset U.$ But $U \subset R.$

Combining the two, $R = U.$

Thus any ideal U containing $M \Rightarrow U = R.$

Hence M is a maximal ideal of R.

Example 5.15. *Show that the set of integers is a subring but not an ideal of the ring of rational numbers.*

Solution. Recall that a subset S of a ring R is a subring if

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

Since difference and product of two integers is an integer and therfore

$$a, b \in Z \Rightarrow a - b \in Z, ab \in Z.$$

Also $$Z \subset Q.$$

These facts imply that Z is a subring of Q.

By def. of ideal, Z is an ideal of Q if

$$q \in Q, a \in Z \Rightarrow qa, aq \in Z.$$

This is not satisfied. For product of an integer and a rational number is not always an integer

$$\left[5 \in Z, \frac{9}{16} \in Q \Rightarrow 5 \times \frac{9}{16} \notin Z\right].$$

Hence Z is not an ideal of Q.

Example 5.16. *Show that the set of rational numbers is a subring but not an ideal of the ring of real numbers.*

Solution. Evidently $Q \subset R.$

$$a, b \in Q \Rightarrow a - b \in Q, ab \in Q$$

[For difference and product of two rational numbers are rational numbers].

Therefore Q is a subring of R.

Now Q will be an ideal of R if

$$r \in R, a \in Q \Rightarrow ar \in Q,$$

i.e. product of a rational number and a real number is a rational number.

This condition is not satisfied in general.

For $$\sqrt{3} \in R, \frac{5}{2} \in Q \Rightarrow \frac{5}{2} \times \sqrt{3} \notin Q.$$

Since $\frac{5\sqrt{3}}{2}$ is not a rational number.

Hence Q is a subring but not an ideal of R.

Example 5.17. *Show that the ring* $(\{[0], [1], [2], [3], [4]\}, +_5, \times_5)$ *has no proper ideals.*

Solution. Since the given ring is a field and a field has no proper ideals. In particular the given field has no proper ideals. It can be easily verified as follows :

Let $$R = \{[0], [1], [2], [3], [4]\},$$

$$(0) = \{0\}.$$

$(1) = \{1 \times_5 x : x \in R\}$.

$= \{1 \times_5 [0], 1 \times_5 [1], 1 \times_5 [2], 1 \times_5 [3], 1 \times_4 [4]\}$

$= \{[0], [1], [2], [3], [4]\} = R.$

Similarly $(2) = \{2 \times_5 [0], 2 \times_5 [1], 2 \times_5 [2], 2 \times_5, [3] 2 \times_5 [4]\}$

$= \{[0], [2], [4], [1], [3]\} = \{[0], [1], [2], [3], [4]\} = R.$

$(3) = \{3 \times_5 [0], 3 \times_5 [1], 3 \times_5 [2], 3 \times_5 [3], 3 \times_5 [4]\}$

$= \{[0], [3], [1], [4], [2]\} = \{[0], [1], [2], [3], [4]\} = R.$

$(4) = R.$

Finally, $(0) = \{0\}, (1) = (2) = (3) = (4) = R.$

Example 5.18. *If a is an element of a ring R, show that*

$$S = \{x \in R : ax = 0\}$$

is a right ideal of R.

Solution. To prove the required result, we have to show that

(i) $(S, +)$ is additive subgroup of R, i.e.,

$$x, y \in S \Rightarrow x - y \in S.$$

(ii) $r \in R, x \in S \Rightarrow xr \in S.$

(i) $x, y \in S \Rightarrow ax = 0, ay = 0 \Rightarrow ax - ay = 0 - 0 = 0$

$\Rightarrow a(x - y) = 0, x - y \in R$

[For $x, y \in S \Rightarrow x, y \in R \Rightarrow x - y \in R$.

Also $(R, +)$ is a group].

$\Rightarrow x - y \in S$, by construction of S.

(ii) $r \in R, x \in S \Rightarrow r \in R, ax = 0 \Rightarrow a(xr) = (ax)\, r = 0.\, r = 0$

$\Rightarrow a(xr) = 0, xr \in R$

$\Rightarrow xr \in S.$

Example 5.19. *If A is a left ideal of a ring R,*

and $$\lambda(A) = \{x \in R : xa = 0 \ \forall\ a \in A\}.$$

then $\lambda(A)$ is a two sided ideal of R.

Solution. To prove that $\lambda(A)$ is an ideal of R, we have to prove that

(i) $\lambda(A)$ is a additive subgroup of R.

i.e., $$b_1, b_2 \in \lambda(A) \Rightarrow b_1 - b_2 \in \lambda(A).$$

(ii) $b \in \lambda(A), x \in R \Rightarrow bx, xb \in \lambda(A).$

Now $\forall\ b_1, b_2 \in \lambda(A) \Rightarrow b_1 a = 0 = b_2 a\ \forall\ a \in A$ and $b_1, b_2 \in R$

$\Rightarrow (b_1 - b_2)a = 0\ \forall\ a \in A$

and $b_1 - b_2 \in R$

$\Rightarrow b_1 - b_2 \in \lambda(A)$. Hence (i).

$b \in \lambda(A), x \in R \Rightarrow b, x \in R$ s.t. $ba = 0\ \forall\ a \in A$

$\Rightarrow xb \in R$ s.t. $(xb)\, a = x\, 0 = 0\ \forall\ a \in A$

$\Rightarrow xb \in \lambda(A).$

Again $x \in R, a \in A \Rightarrow xa \in A$. For A is left ideal.

$b \in \lambda(A), xa \in A \Rightarrow b(xa) = 0 \Rightarrow (bx)\, a = 0 \ \forall\, a \in A$

$\Rightarrow bx \in \lambda(A)$.

Finally, $b \in \lambda(A), x \in R \Rightarrow bx, xb \in \lambda(A)$. Hence (ii).

Example 5.20. If S is an ideal of a ring R and

$$[R : S] = \{x \in R : rx \in S \quad \forall\, r \in R\},$$

then prove that [R : S] is an ideal of R.

Solution. To prove the required result, we have to prove that

(i) [R : S] is an additive subgroup of R, i.e.,

$$x, y \in [R : S] \Rightarrow x - y \in [R : S]$$

(ii) $x \in [R : S], r \in R \Rightarrow rx, xr \in [R : S]$.

Obviously $x, y \in [R : S] \Rightarrow rx \in S, ry \in S \ \forall\, r \in R$ and $x, y \in R$

$\Rightarrow rx - ry \in S$. For S is ideal.

$\Rightarrow r(x - y) \in S \ \forall\, r \in R$ and $x - y \in R$

$\Rightarrow x - y \in [R : S]$. Hence (i).

$x \in [R : S], s \in R \Rightarrow rx \in S$ and $x, s \in R \quad \forall\, r \in R$

$\Rightarrow (rx)\, s = r\,(xs) \in S$

$\forall\, r \in R$ and $xs \in R$

For S is ideal.

$\Rightarrow xs \in [R : S]$, by def. of $[R : S]$.

Again $x \in [R : S], s \in R \Rightarrow rx \in S \quad \forall\, r \in R$

$\Rightarrow$ in particular, $sx \in S$. For $s \in R$.

$\Rightarrow r\,(sx) \in S \quad \forall\, r \in R$. For S is ideal.

$\Rightarrow sx \in [R : S]$, by def. of $[R : S]$.

Finally, $x \in [R : S], s \in R \Rightarrow sx, xs \in [R : S]$. Hence (ii)

Example 5.21. *The set S of all 2 × 2 matrices of the form* $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ *with a, b as integers, is a left ideal but not right ideal in the ring of 2 × 2 matrices with elements as integers.*

Solution. Let $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}, B = \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}$ be any two elements of S, then a, b, c, d are integers so that a – c, b – d are also integers,

$$A - B = \begin{bmatrix} a - c & 0 \\ b - d & 0 \end{bmatrix} \in S$$

$$\therefore \ A, B \in S \Rightarrow A - B \in S.$$

Hence S is a additive subgroup of R.

Let $C = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$ be any element of R ,then x, y, z, w $\in$ Z.

$$CA = \begin{bmatrix} x & y \\ z & w \end{bmatrix}\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} ax+by & 0 \\ az+wb & 0 \end{bmatrix} \in S$$

For $ax + by, ax + wb \in Z.$

Thus $C \in R, A \in S \Rightarrow CA \in S.$

Therefore S is a left ideal of R.

Remains to prove that S is not a right ideal of R.

Now $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \in S$ and $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in R$

and $$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \notin S.$$

For the second column is non-zero. This declares that S is not a right ideal of R.

Example 5.22. *The set S of all 2 ×2 matrices of the form* $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ *with a, b as integers is a right ideal but not a left in the ring of all 2 × 2 matrices with elements as integers.*

Solution. Let $A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}$ be arbitrary elements of S.

Then a, b, c, d $\in$ **Z** so that a – c, b – d $\in$ **Z**

$$A - B = \begin{bmatrix} a-c & b-d \\ 0 & 0 \end{bmatrix} \in S.$$

$$\therefore\ A, B \in S \Rightarrow A - B \in S.$$

This $\Rightarrow$ (S, +) is subgroup of R.

Let $C = \begin{bmatrix} x & z \\ y & w \end{bmatrix}$ be any element of R.

$$AC = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} x & z \\ y & w \end{bmatrix} = \begin{bmatrix} ax+by & ax+bw \\ 0 & 0 \end{bmatrix} \in S.$$

i.e., $A \in S, C \in R \Rightarrow AC \in S.$

Consequently S is a right ideal of R.

Now $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \in S, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \in R$

and $$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \notin S,$$

showing thereby S is not a left ideal of R.

Example 5.23. *Give an example of a ring R, right ideal A and a left ideal B such that $A \cap B$ is neither left nor a right ideal of R.*

Solution. Consider the ring R of 2×2 matrices whose elements are real numbers.

Case I. Let A be the set of 2×2 matrices of the form $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$, where a, b are real.

Prove as in example 5.22 that A is right ideal.

Case II. Let B be the set of 2×2 matrices of the form $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$, where a, b are real.

Prove as in example 5.21 that B is left ideal.

Case III. Take $C = A \cap B$. Then C is the set of 2×2 matrices of the form $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, where a is real.

Let $P = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ and $C_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, then $P \in R$ and $C_1 \in C$.

$$C_1 P = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \notin C.$$

This $\Rightarrow$ C is not right ideal

$$PC_1 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \notin C.$$

This $\Rightarrow$ C is not left ideal.

Hence C is neither left nor right ideal of R.

Example 5.24. Show that S is an ideal of S + T, where S is any ideal of R and T is any subring of R. [I.A.S. 96]

Solution. Let S be an ideal and T be a subring of R so that

(i) S is additive subgroup of R, i.e.,

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

(ii) $a \in S, r \in R \Rightarrow ra, ar \in S$.

(iii) $a, b \in T \Rightarrow a - b \in T$.

(iv) $a, b \in T \Rightarrow ab \in T$.

Let $x, y \in S + T$ be arbitrary. Then $\exists$ s, s′ $\in$ S and t, t′ $\in$ T s.t.

$$x = s + t,\ y = s' + t'.$$

Now

$$x - y = (s + t) - (s' + t')$$
$$= (s - s') + (t - t').$$

For (R, +) is an Abelian group.

$\in S + T$, according to (i) and (iii).

Hence $x, y \in S + T \Rightarrow x + y \in S + T$ ...(1)

$xy = (s + t)(s' + t') = ss' + st' + ts' + tt'$ ...(2)

$s, s' \in S \Rightarrow ss' \in S$, by (ii).

$t, t' \in T \Rightarrow tt' \in T$, by (iv).

According to (ii)

$s, s' \in S$ and $t, t' \in R \Rightarrow st', ts' \in S$

$\Rightarrow st' + ts' \in S$, by (i)

Also $ss' \in S$

$ss' + st' + ts' \in S$, by (i)

$\Rightarrow (ss' + st' + ts') + tt' \in S + T$,

$x, y \in S + T \Rightarrow xy \in S + T$ ...(3), by (2)

(1) and (3), $\Rightarrow S + T$ is a subring of R.

Any $s \in S \Rightarrow s \in S, 0 \in T$.

[For T is a subring of $R \Rightarrow 0 \in T$]

$\Rightarrow s + 0 \in S + T$

$\Rightarrow s \in S + T$.

This $\Rightarrow S \subset S + T$.

$S + T$ is a subring of $R \Rightarrow S + T \subset R$.

Finally, $S \subset S + T \subset R$.

Also $S + T$ is a subring of R ans S is an ideal of R.

This $\Rightarrow$ S is an ideal of $S + T$.

Exmaple 5.25. *Show that the set S of all matrices of the form* $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ *with a and b as integers, forms a subring of the ring R of all 2 × 2 matrices with elements as integers. Also prove that S is neither left nor right ideal of R.*

Solution. Let $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ and $B = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$ be any two elements of S,

Then $a, b, c, d \in \mathbf{Z}$ so that $a - c, b - d \in Z$.

Now $A - B = \begin{bmatrix} a-c & 0 \\ 0 & b-d \end{bmatrix} \in S$.

$$AB = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in S.$$

Thus we have shown that

$A, B \in S \Rightarrow A - B \in S, AB \in S$.

Also obviously $S \subset R$.

This declares that S is a subring of R.

Since $\begin{bmatrix}1 & 0\\ 0 & 2\end{bmatrix}\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}=\begin{bmatrix}1 & 2\\ 6 & 8\end{bmatrix}\notin S.$

This $\Rightarrow$ S is not a right ideal of R.

Also $\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 2\end{bmatrix}=\begin{bmatrix}1 & 4\\ 3 & 8\end{bmatrix}\notin S.$

This $\Rightarrow$ S is not a left ideal of R.

Finally, S is neither left nor right ideal of R.

Example 5.26. *If m is a fixed integer, the set* $S = \{mx : x \in \mathbf{Z}\}$ *is an ideal of the ring of integers.*

Solution. Let $x, y \in S$ be arbitrary, then

$$x = mx_1,\ y = my_1 \text{ for some } x_1, y_1 \in Z.$$

$$x - y = mx_1 - my_1 = m(x_1 - y_1) \in S.$$

[For $x_1, y_1 \in \mathbf{Z} \Rightarrow x_1 - y_1 \in \mathbf{Z}$],

i.e., $x - y \in S.$

Let $r \in \mathbf{Z}$. Then $rx = r(mx_1) = m(rx_1) \in S.$

[For $r, x_1 \in \mathbf{Z} \Rightarrow rx_1 \in Z$ and Z is a commutative ring].

i.e., $rx \in S$. Also $xr = rx.$

Thus $x, y \in S \Rightarrow x - y \in S,$

$r \in Z, x \in S \Rightarrow rx, xr \in S.$

Hence S is an ideal of **Z**.

Example 5.27. *An ideal S in a ring R is necessarily a subring of R.*

Solution. Let S be an ideal of a ring R so that :

(i) (S, +) is additive subgroup of R,

i.e., $a, b \in S \Rightarrow a - b \in S$ ...(1)

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

In view of (ii), $a, b \in S \Rightarrow ab, ba \in S.$ ...(2)

The statements (1) and (2) prove that S is a subring of R.

Example 5.28. *The set E of even integers is an ideal of the ring of integers.*

Solution. $E = \{2x : x \in \mathbf{Z}\}.$

Replacing m by 2 in Example 5.26, we shall get the required result.

6. Homomorphism of rings.

Definition 6.1. Homomorphism into. A mapping f from a ring R into a ring R' is said to be a homomorphism of R into R' if

(i) $f(a + b) = f(a) + f(b)\ \forall\ a, b \in R.$

(ii) $f(ab) = f(a)\, f(b)$ for all $a, b \in R.$ (GKP., 2005, 2007)

Definitions 6.2. Homomorphism onto. A mapping f from a ring R

onto a ring R′ is said to be a homomorphism of R onto R′ if

(i) $f(a+b) = f(a) + f(b)\ \forall, a, b \in R$.

(ii) $f(ab) = f(a)\, f(b)$ for all, $a, b \in R$.

Also then R′ is said to be a homomorphic image of R.

Theorem 6.1. If f is a homomorphism of a ring R into a ring R′, then

(i) $f(0) = 0'$, where 0 is the zero element of the ring R and 0′ is the zero element of R′.

(ii) $f(-a) = -f(a)\ \forall\ a \in R$. **[GKP, 2005]**

Proof. (i) Let $a \in R$. Then $f(a) \in R'$. We have

$f(a) + 0' = f(a)$ [$\because$ 0′ is the additive identity of R′]

$= f(a+0) = f(a) + f(0)$.

Now R′ is a group with respect to addition. Therefore

$f(a) + 0' = f(a) + f(0)$

$\Rightarrow 0' = f(0)$. [by left cancellation law].

(ii) Let a be any element of R. Then $-a \in R$.

We have $0' = f(0) = f[a + (-a)] = f(a) + f(-a)$.

$\therefore$ f (−a) is the additive inverse of f (a) in the ring R′. Thus $f(-a) = -f(a)$.

Theorem 6.2. Let ϕ be a homomorphic mapping of a ring R into a ring R′. Let S′ be the homorphic image of R in R′. Then S′ is a subring of R′. **[GKP, 2001]**

Proof. Since S′ is the image of R in R′ under the mapping ϕ, therefore $\phi(R) = S' \subset R'$.

Let a′, b′ be any two elements of S′. Since $S' = \phi(R)$, therefore there exist elements $a, b \in R$ such that $\phi(a) = a'$, $\phi(b) = b'$.

We have $a' - b' = \phi(a) - \phi(b) = \phi(a-b)$.

[$\because \phi$ is a homomorphism]

Now $a - b \in R$ is such that $a' - b' = \phi(a - b)$. Therefore

$a' - b' \in S'$.

Further $a'\, b' = \phi(a)\, \phi(b) = \phi(ab) \in S'$, since $ab \in R$.

Thus $a', b' \in S' \Rightarrow a' - b' \in S'$ and $a'\, b' \in S'$.

Therefore S′ is a subring of R′.

Definition 6.3. Kernel of a ring homomorphism. If f is a homomorphism of a ring R into a ring R′, then the set S of all those elements of R which are mapped onto the zero element of R′ is called the kernal of the homomorphism f.

Thus if f is a homomorphism of R into R′, then S is the kernel of f if $S = \{x \in R : f(x) = 0'$, where 0′ is the zero element of R′$\}$.

Theorem 6.3 If f is a homomorphism of a ring R into a ring R′ with

kernel S, then S is an ideal of R. [GKP, 1985, 2003, 2005]

Proof. Let f be a homomorphism of a ring R into a ring R'. Let 0, 0' be the zero elements of R, R' respectively. Let S be the kernel of f. Then $S = \{x \in R : f(x) = 0'\}$.

Since $f(0) = 0'$, therefore at least $0 \in S$. Thus S is not empty.

Let $a, b \in S$. Then $f(a) = 0'$, $f(b) = 0'$.

We have $f(a - b) = f[a + (-b)] = f(a) + f(-b)$

$= f(a) - f(b) = 0' - 0' = 0'$.

$\therefore a - b \in S$.

Also if r be any element of R, then

$f(ar) = f(a)\, f(r) = 0'\, f(r) = 0'$

and $f(ra) = f(r)\, f(a) = f(r)\, 0' = 0'$.

$\therefore ar \in S, ra \in S$.

Thus $a, b \in S, r \in R \Rightarrow (a - b) \in S, ar \in S, ra \in S$.

$\therefore$ S is an ideal of R.

Theorem 6.4 The homomorphism ϕ of a ring R into a ring R' is an isomorphism of R into R' if any only if $I(\phi) = \{0\}$, where $I(\phi)$ denotes the kernel of ϕ.

Proof. Let ϕ be a homomorphism of a ring R into a ring R'. Let 0, 0' be the zero elements of R, R' respectively. Let $S = I(\phi)$ be the kernel of ϕ. Then S is an ideal of R and

$$S = \{a \in R : \phi(a) = 0'\}.$$

Suppose ϕ is an isomorphism of R into R'. Then ϕ is one-one. Let $a \in S$. Then

$\phi(a) = 0'$ [by def. of kernel]

$\Rightarrow \phi(a) = \phi(0)$ [$\because \phi(0) = 0'$]

$\Rightarrow a = 0$. [$\because \phi$ is one–one]

Thus $a \in S \Rightarrow a = 0$. In other words 0 is the only element of R which belongs to S. Therefore $S = \{0\}$.

Conversely suppose that $S = \{0\}$. Then to prove that ϕ is an isomorphism of R into R' i.e., to prove that ϕ is one-one.

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

$\Rightarrow \phi(a) - \phi(b) = 0'$ [$\because \phi(a), \phi(b)$ are in the ring R']

$\Rightarrow \phi(a - b) = 0'$ [$\because \phi$ is a homomorphism]

$\Rightarrow a - b \in S$ [by def. of kernel]

$\Rightarrow a - b = 0$ [$\because S = \{0\}$]

$\Rightarrow a = b$.

$\therefore \phi$ is one–one. Hence ϕ is an isomorphism of R into R'.

Theorem 6.5. Suppose R is a ring, S an ideal of R. Let f be a mapping

from R to R/S defined by $f(a) = S + a \ \forall\ a \in R$. Then f is a homomorphism of R onto R/S. (GKP, 2006)

Proof. Consider the mapping $f : R \to R/S$ such that

$$f(a) = S + a \ \forall\ a \in R.$$

Let $S + x$ be any element of R/S. Then $x \in R$.

We have $f(x) = S + x$. Therefore the mapping f is onto R/S.

Let $a, b \in R$, Then

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

Also $f(ab) = S + ab = (S + a)(S + b) = f(a)\, f(b)$.

$\therefore$ f is a homomorphism of R onto R/S.

Thus every quotient ring of a ring is a homomorphic image of the ring.

Theorem 6.6. Fundamental theorem of homomorphism of rings.

Every homomorphic image of a ring R is isomorphic to some residue class ring (quotient ring) thereof. (GKP, 2007)

Proof. Let R′ be the homomorphic image of a ring R and f be the corresponding homomorphism. Then f is a homomorphism of R onto R′. Let S be the kernel of this homomorphism. Then S is an ideal of R. Therefore R/S is a ring of residue classes of R relative to S. We shall prove that $R/S \cong R'$.

If $a \in R$, then $S + a \in R/S$ and $f(a) \in R'$. Consider the mapping $\phi : R/S \to R'$ such that

$$\phi(S + a) = f(a) \ \forall\ a \in R.$$

First we shall show that the mapping ϕ is well defined i.e., if $a, b \in R$ and $S + a = S + b$, then $\phi(S + a) = \phi(S + b)$.

We have $S + a = S + b$

$\Rightarrow a - b \in S$

$\Rightarrow f(a - b) = 0'$ [i.e. zero element of R′]

$\Rightarrow f[a + (-b)] = 0' \Rightarrow f(a) + f(-b) = 0' \Rightarrow f(a) - f(b) = 0'$

$\Rightarrow f(a) = f(b) \Rightarrow \phi(S + a) = \phi(S + b)$.

$\therefore \phi$ is well-defined.

ϕ is one-one. We have $\phi(S + a) = \phi(S + b)$

$\Rightarrow f(a) = f(b) \Rightarrow f(a) - f(b) = 0'$

$\Rightarrow f(a) + f(-b) = 0' \Rightarrow f(a - b) = 0'$

$\Rightarrow a - b \in S$ [$\because$ S is kernel of f]

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

$\therefore \phi$ is one-one.

ϕ is onto R′. Let y be any element of R′. Then $y = f(a)$ for some $a \in R$ because f is onto R′. Now $S + a \in R/S$ and we have $\phi(S + a) = f$

(a) = y. Therefore ϕ is onto R'.

Finally we have

$$\phi[(S+a)+(S+b)] = \phi[S+(a+b)] = f(a+b)$$
$$= f(a)+f(b) = \phi(S+a)+\phi(S+b).$$

Also $\phi[(S+a)(S+b)] = \phi(S+ab) = f(ab) = f(a)\,f(b)$
$$= [\phi(S+a)][\phi(S+b)].$$

$\therefore$ ϕ is an isomorphism of R/S onto R'.

Hence $R/S \cong R'$.

Ex. 6.1 *Show that every homomorphic image of a commutative ring is commutative.*

Solution. Let R be a commutative ring. Let f be a homomorphic mapping of R onto a ring R'. Then R' is a homomorphic image of R.

Let a', b' be any two elements of R'. Then f(a) = a', f(b) = b' for some a, b $\in$ R because f is onto R'. We have

$$a'b' = f(a)\,f(b) = f(ab)$$
$$= f(ba) \qquad [\because \text{R is commutative}]$$
$$= f(b)\,f(a) = b'a'.$$

$\therefore$ R' is a commutative ring.

Ex. 6.2 *If R is a ring with unit element 1 and ϕ is a homomorphism of R onto R', prove that $\phi(1)$ is the unit element of R'.* (GKP. 2006)

Solution. Since ϕ is a homomorphism of R onto R', therefore R' is a homomorphic image of R. If 1 is unity element of R, then $\phi(1) \in R'$. Let a' be any element of R'. Then $a' = \phi(a)$ for some a $\in$ R, since ϕ is onto R'. We have

$$\phi(1)\,a' = \phi(1)\,\phi(a) = \phi(1a) = \phi(a) = a'$$

and $$a'\,\phi(1) = \phi(a)\,\phi(1) = \phi(a1) = \phi(a) = a'.$$

$\therefore$ $\phi(1)$ is the unity element of R'.

Ex. 6.3. *If R is a ring with unit element 1 and ϕ is a homomorphism of R into an integral domain R' such that kernel of ϕ i.e., $I(\phi) \neq R$, then prove that $\phi(1)$ is the unit element of R'.*

Solution. ϕ is a homomorphism of a ring R into an integral domain R'. Then kernel of ϕ

$$= I(\phi) = \{x : x \in R \text{ and } \phi(x) = 0' \in R'\}.$$

Since $I(\phi) \neq R$, therefore there exists an element a $\in$ R such that

$$\phi(a) \neq 0' \in R'.$$

We have $\phi(1)\,\phi(a) = \phi(1a) = \phi(a)$.

Now let b' be any element of R'. We have

$$\phi(a)\,b' = \phi(a)\,b'$$
$$\Rightarrow \phi(1)\,\phi(a)\,b' = \phi(a)\,b' \qquad [\because \phi(1)\,\phi(a) = \phi(a)]$$

$\Rightarrow \phi(a)[\phi(1)\, b'] = \phi(a)\, b'$

[$\because \phi(1), \phi(a) \in R'$ which, being an integral domain, is a commutative ring]

$\Rightarrow \phi(a)[\phi(1)\, b'] - \phi(a)\, b' = 0'$

$\Rightarrow \phi(a)[\phi(1)\, b' - b'] = 0'$

$\Rightarrow \phi(1)\, b' - b' = 0'$

[$\because \phi(a) \neq 0'$ and R' is without zero divisors]

$\Rightarrow \phi(1)\, b' = b' = b'\, \phi(1)$. [$\because R'$ is a commutative ring]

Thus $\phi(1)\, b' = b' = b'\, \phi(1)\ \forall\ b' \in R'$.

$\therefore \phi(1)$ is the unit element of R'.

Ex. 6.4. *Prove that any homomorphism of a field is either an isomorphism or takes each element into 0.*

or

Show that a field has no proper homomorphic image.

Solution. Let ϕ be a homomorphism of a field F into a ring R. Let S be the kernel of ϕ. Then S is an ideal of the field F. We know that a field has no proper ideals. Therefore either S=F or S={0}.

If S=F, then by definition of kernel of ϕ, we have $\phi(x)=0\ \forall\ x \in F$. Thus in this case ϕ takes each element of F into the zero element of R. In other words in this case $\phi(F)$ is the zero subring of the ring R.

If S={0}, then the kernel consists of zero element alone. So in this case ϕ is an isomorphism of F into R. [See theorem 6.4]. Since the isomorphic image of a field is a field, therefore in this case $\phi(F)$ is a field isomorphic to the field F.

7. Field of Quotients of An Integral Domain.

Definition 7.1. A field F is said to be the **quotient field** of an integral domain R if

(i) $F \subset R$.

(ii) F′ is the smallest field containing R, i.e.,

$\Rightarrow \forall\ F' \supset R$ s.t. F′ is a field $\Rightarrow F \subset F'$.

Example 7.1. Q is the quotient field of the integral domain Z of integers.

Definition 7.2. A ring R **can be embedded** in a ring R′ if $\exists$ a ring isomorphism $f : R \xrightarrow{\text{onto}} S'$, S′ being a subring of R′.

, R′ is called an extension of R if R can be embedded in R′. Also then f is called embedding of R into S′.

Definition 7.3. Let R be a ring. Then the set

$$\{a/b : a, b \in R \text{ and } b \neq 0\}$$

is called the set of quotients of R.

Theorem 7.1. A ring R without unity element can be embedded in a ring with unity.

Proof. Suppose R is a ring without unity element and Z is a ring of integers. Also suppose

$$R' = R \times Z = \{(a,b) : a \in R, b \in Z\}.$$

Let $(a,m), (b,n), (c,p) \in R'$ be arbitrary, then

$$a, b, c \in R \text{ and } m, n, p \in Z.$$

We define the operations of addition and multiplication on R' as follows :

$$(a, m) + (b, n) = (a + b, m + n) \quad ...(1)$$

$$(a, m)(b, n) = (ab + na + mb, mn) \quad ...(2)$$

Since $a, b \in R$ and $m, n \in Z \Rightarrow a + b \in R, m + n \in Z$

$\Rightarrow (a, m) + (b, n) \in R'$, by (1)

Since $a, a \in R \Rightarrow a + a \in R \Rightarrow 2a \in R$.

Hence $a, b \in R$ and $m, n \in Z \Rightarrow ab, na, mb \in R$ and $mn \in Z$

$\Rightarrow ab + na + mb \in R$ and $mn \in Z$

$\Rightarrow (ab + na + mb, mn) \in R'$

$\Rightarrow (a, m)(b,n) \in R'$ by (2).

Thus we have shown that R' is closed w.r.t. addition and multiplication defined as above.

To prove that $(R', +, \cdot)$ is a ring with unity.

1. Commutative law for addition. $(a, m) + (b, n) = (b, n) + (a, m)$.

Since (R, +) and (Z, +) both are commutative groups and so

$(a,m) + (b, n) = (a + b, m + n) = (b + a, n + m) = (b, n) + (a, m)$.

2. Existence of zero element. $(0, 0) \in R'$ is the additive identity, where the first zero is the zero of R and the second zero is the zero of Z. For

$$(0, 0) + (a, m) = (o + a, o + m) = (a, m).$$

3. Existence of inverse. $(-a, -m) \in R'$ is the additive inverse of $(a, m) \in R'$. For $a \in R, m \in Z \Rightarrow -a \in R, -m \in Z$ and $(a, m) + (-a, -m) = (a - a, m - m) = (0, 0) =$ zero of R'.

4. Associative law of addition.

$$[(a, m) + (b, n)] + (c,p) = (a,m) + [(b,n) (+c,p)]$$

For L.H.S. $= (a + b, m + n) + (c,p) = ([a + b] + c, [m + n] + p)$

$= (a + [b + c], m + [n + p]) = (a,m) + [(b,n) + (c,p)]$

$=$ R.H.S.

5. Associative law of multiplication.

$$[(a, m)(b, n)](c,p) = (a, m)[(b, n)(c, p)]$$

For L.H.S. $= (ab + na + mb, mn)(c, p)$

$= (abc + nac + mbc + pab + npa + mpb + mnc, mnp)$

and R.H.S. $= (a, m)(bc + pb + nc, np)$

$= (a[bc + pb + nc] + m[bc + pb + nc] + npa, mnp)$

$= (abc + pab + nac + mbc + mpb + mnc + npa, mnp)$

$= (abc + nac + mbc + pab + npa + mpb + mnc, mnp)$

$=$ L.H.S.

6. Distributive law.

$$(a, m)[(b,n) + (c,p)] = (a,m)(b,n) + (a,m)(c,p)$$

For L.H.S. $= (a, m)(b + c, n + p)$

$= (a[b + c] + m[b + c] + [n + p]a, m[n + p])$

$= (ab + ac + mb + mc + na + pa, mn + mp)$

R.H.S. $= (ab + mb + na, mn) + (ac + mc + pa, mp)$

$= (ab + mb + na + ac + mc + pa, mn + mp)$

$= (ab + ac + mb + mc + na + pa, mn + mp)$

$=$ L.H.S.

Similarly we can prove the other distributive law.

7. Existence of Unity Element. $(0, 1) \in R'$ is unity element.

For $(0, 1)(a, m) = (0a + 1a + 0m, 1m) = (a, m)$.

Take $S' = R \times \{0\} \subset R \times Z = R'$ so that $S' \subset R'$.

To prove that S' is a subring of R'.

Let $(a, 0), (b, 0) \in S'$ be arbitrary.

Now $(a, 0) - (b, 0) = (a - b, 0) \in S'$

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

$= (ab, 0) \in S'$.

Hence S' is a subring of R'.

Define a map $f : R \to S' = R \times \{0\}$ s.t.

$f(a) = (a, 0)$.

f is one-one.

For $f(a) = f(b) \Rightarrow (a, 0) = (b, 0) \Rightarrow a = b$.

f is onto.

For given any $(a, 0) \in S' \Rightarrow a \in R$ s.t. $f(a) = (a, 0)$.

f preserves addition and multiplication compositions.

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

$$f(ab) = (ab, 0) = (a, 0)(b, 0) = f(a)\,f(b).$$

Thus $\exists$ an isomorphism $f : R \xrightarrow{\text{onto}} S'$ and S' is a subring of R' which is a ring with unity.

$\therefore$ By def., R can be embedded in R'.

Theorem 7.2. If R is an integral domain, then it is possible to construct a field (quotient field) from the elements of an integral domain and this

quotient field will contain a sub-system D isomorphic to R.

or

An integral domain can be embedded in a field. [GKP, 2005]

Proof. Let R′ denote the set of non-zero elements of the integral domain R. Form the cartesian product

$$R \times R' = \{(a,b) : a \in R, b \in R'\}.$$

Define a relation ~ on $R \times R'$ as follows :

$$(a,b) \sim (c,d) \text{ iff } ad = bc.$$

Let (a, b), (c, d), (g, h) be arbitrary elements of $R \times R'$. This relation is

reflexive : $(a, b) \sim (a, b)$. For $ab = ba$.

symmetric : $(a, b) \sim (c,d) \Rightarrow (c,d) \sim (a,b)$

For $(a, b) \sim (c, d) \Rightarrow ad = bc$

$\Rightarrow cb = da$. For $(R, \cdot)$ is commutative

$\Rightarrow (c, d) \sim (a, b)$.

transitive: $(a, b) \sim (c, d), (c, d) \sim (g, h)$

$\Rightarrow (a, b) \sim (g, h)$.

For $(a, b) \sim (c, d), (c, d) \sim (g, h) \Rightarrow ad = bc, ch = dg$

$\Rightarrow adh = bch, bch = bdg \Rightarrow adh = bdg$

$\Rightarrow d(ah - bg) = 0 \Rightarrow ah - bg = 0$

For $d \neq 0$ and R has no zero divisors.

$\Rightarrow (a, b) \sim (g, h)$.

Hence ~ is an equivalence relation.

Now this equivalence relation ~ will partition the set $R \times R'$ into mutually disjoint equivalence classes. Denote the equivalence class containing (a, b) by $\frac{a}{b}$. Then, by definition,

$$\frac{a}{b} = \{(x, y) \in R \times R' : (x, y) \sim (a, b)\}.$$

Let F be the family of all equivalence classes thus obtained.

Then $$F = \left\{\frac{a}{b} : (a,b) \in R \times R'\right\}.$$

Here F is called set of quotients.

Let $\frac{a}{b}, \frac{c}{d}, \frac{g}{h}$ be arbitrary elements of F.

Obviously $\frac{a}{b} = \frac{c}{d}$ iff $(a,b) \sim (c, d)$, i.e. iff $ad = bc$.

Also $\frac{a}{b} = \frac{ax}{bx}$ $\forall x \in R'$.

For $abx = bax$, i.e., $(a, b) \sim (ax, bx)$.

We define the operations of addition and multiplication on F as follows :

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \text{ and } \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

$b, d \in R' \Rightarrow b, d \neq 0$. Also R has no zero divisors

$$\Rightarrow bd \neq 0 \Rightarrow \frac{ad+bc}{bd}, \frac{ac}{bd} \in F$$

$$\Rightarrow \frac{a}{b}+\frac{c}{d} \in F, \frac{a}{b}\cdot\frac{c}{d} \in F$$

$\Rightarrow$ F is closed w.r.t. (+) and (·).

First of all we are to show that these operations are well defined. Though it appears that these definitions of addition and multiplication depend on some particular elements. We shall show that infact there is no such dependence.

For proving this we have to prove that if

$$\frac{a}{b}=\frac{a'}{b'}, \frac{c}{d}=\frac{c'}{d'} \text{ then}$$

$$\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'} \text{ and } \frac{a}{b}\cdot\frac{c}{d}=\frac{a'}{b'}\cdot\frac{c'}{d'}.$$

To prove that $\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}$, we have to prove that

$$\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}, \text{ i.e., } (ad+bc)\,b'd' = bd\,(a'd'+b'c')$$

Observe that

$$\begin{aligned}(ad+bc)\,b'd' &= ad\,b'd'+bc\,b'd' = (ab')\,(dd')+(bb')\,(cd')\\ &= (ba')\,(dd')+(bb')\,(dc'). \text{ For } ab' = ba',\ cd' = dc'\\ &= bd\,(a'd'+b'c'), \text{ which was desired.}\end{aligned}$$

Again to prove $\frac{a}{b}\cdot\frac{c}{d}=\frac{a'}{b'}\cdot\frac{c'}{d'}$ we have to prove that

$$\frac{ac}{bd}=\frac{a'c'}{b'd'}, \text{ i.e., } ac.b'd' = bd.a'c'.$$

Now $ac.b'd' = (ab')\,(cd') = (ba')\,(dc')$

$= bd.a'c'$, which was desired.

To prove (F, +, ·) is a field.

(1) F is closed w.r.t. (+) and (·) (previously shown).

(2) Addition is commutative in F, i.e., $\frac{a}{b}+\frac{c}{d}=\frac{c}{d}+\frac{a}{b}$.

For $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{da+cb}{db}=\frac{cb+da}{db}=\frac{c}{d}+\frac{d}{b}$.

(3) Multiplication is commutative in F, i.e., $\frac{a}{b}\cdot\frac{c}{d}=\frac{c}{d}\cdot\frac{a}{b}$.

For $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{d}\cdot\frac{a}{b}$.

(4) Addition is associative in F, i.e.,

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{g}{h}=\frac{a}{b}+\left(\frac{c}{d}+\frac{g}{h}\right).$$

For L.H.S. $=\dfrac{ad+bc}{bd}+\dfrac{g}{h}=\dfrac{h(ad+bc)+bdg}{bdh}$

$$=\frac{had+hbc+bdg}{bdh}=\frac{had+b(ch+dg)}{bdh}$$

$$=\frac{a}{b}+\frac{ch+dg}{dh}=\frac{a}{b}+\left(\frac{c}{d}+\frac{g}{h}\right)$$

$=$ R.H.S.

(5) Multiplication is associative in F, i.e.,

$$\left(\frac{a}{b}\cdot\frac{c}{d}\right)\cdot\frac{g}{h}=\frac{a}{b}\cdot\left(\frac{c}{d}\cdot\frac{g}{h}\right).$$

For L.H.S. $=\dfrac{ac}{bd}\cdot\dfrac{g}{h}=\dfrac{(ac)g}{(bd)h}=\dfrac{a(cg)}{b(dh)}=\dfrac{a}{b}\cdot\dfrac{cg}{dh}=\dfrac{a}{b}\cdot\left(\dfrac{c}{d}\cdot\dfrac{g}{h}\right)$

$=$ R.H.S.

(6) $\dfrac{0}{x}\in F$ is additive identity of F $\forall\ x\in R'$.

For $\dfrac{a}{b}+\dfrac{0}{x}=\dfrac{ax+b0}{bx}=\dfrac{ax}{bx}=\dfrac{a}{b}$. For $(ax, bx)\sim(a, b)$.

(7) Additive inverse of any element $\dfrac{a}{b}\in F$ is $-\dfrac{a}{b}\in F$.

For $\dfrac{a}{b}\in F\Rightarrow a\in R, b\in R',\Rightarrow -a\in R, b\in R'\Rightarrow -\dfrac{a}{b}\in F$

$$-\frac{a}{b}+\frac{a}{b}=\frac{-ab+ba}{b^2}=\frac{0}{b^2}=\frac{0}{x}.\ \text{For}\ (0, b^2)\sim(0, x)$$

i.e., $$\frac{-a}{b}+\frac{a}{b}=\frac{0}{x}=\text{zero element of F.}$$

(8) $\dfrac{x}{x}\in F$ is multiplicative identity of F $\forall\ x\neq 0$.

For $$\frac{a}{b}\cdot\frac{x}{x}=\frac{ax}{bx}=\frac{a}{b},\ \text{i.e.}\ \frac{a}{b}\cdot\frac{x}{x}=\frac{a}{b}$$

$$x\neq 0\Rightarrow x\in R'\Rightarrow\frac{x}{x}\in F.$$

(9) Every non-zero element of F has multiplicative inverse in F.

Let $\dfrac{a}{b}\in F$ s.t. $\dfrac{a}{b}\neq\dfrac{0}{x}$. This $\Rightarrow a, b\neq 0\Rightarrow\dfrac{a}{b}\in F$

$\dfrac{a}{b}\cdot\dfrac{b}{a}=\dfrac{ab}{ba}=\dfrac{x}{x}$. For $abx=bax\Rightarrow(ab, ab)\sim(x, x)$,

i.e., $$\frac{a}{b}\cdot\frac{b}{a}=\frac{x}{x}=\text{unity element of F.}$$

Hence $\dfrac{b}{a}\in F$ is the multiplicative inverse of $\dfrac{a}{b}$.

(10) Distributive laws hold

$$\frac{a}{b}\left(\frac{c}{d}+\frac{g}{h}\right)=\frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{g}{h}$$

and $$\left(\frac{c}{d}+\frac{g}{h}\right)\frac{a}{b}=\frac{c}{d}\cdot\frac{a}{b}+\frac{g}{h}\cdot\frac{a}{b}.$$

For $$\frac{a}{b}\left(\frac{c}{d}+\frac{g}{h}\right)=\frac{a}{b}\left(\frac{ch+dg}{dh}\right)=\frac{a(ch+dg)}{bdh}$$

$$=\frac{ach+adg}{bdh}=\frac{ac}{bd}+\frac{ag}{bh}$$

$$=\frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{g}{h}=\text{R.H.S.}$$

Similarly we can prove the other distributive law. Hence $(F, +, \cdot)$ is a field. This field is called **field of quotients of the integral domain R.**

Remains to prove that F contains a subset D s.t. $D \cong R$.

Write $D=\left\{\frac{a}{1}:a\in R\right\}$. Clearly $D\subset F$.

Define a map $f: D\to R$ s.t. $f\left(\frac{a}{1}\right)=a\ \forall\ a\in R$.

We claim f is a ring isomorphism onto.

f is one-one:

For $$f\left(\frac{a}{1}\right)=f\left(\frac{b}{1}\right);\ a, b\in R\Rightarrow a=b\Rightarrow\frac{a}{1}=\frac{b}{1}.$$

f is onto.

For any $a\in R\Rightarrow\exists\ \frac{a}{1}\in D$ s.t. $f\left(\frac{a}{1}\right)=a$.

f preserves compositions in D and R.

Let $a,b\in R$ be arbitrary. Then

$$f\left(\frac{a}{1}+\frac{b}{1}\right)=f\left(\frac{1.a+1.b}{1.1}\right)=f\left(\frac{a+b}{1}\right)=a+b=f\left(\frac{a}{1}\right)+f\left(\frac{b}{1}\right).$$

$$f\left(\frac{a}{1}\cdot\frac{b}{1}\right)=f\left(\frac{ab}{1.1}\right)=f\left(\frac{ab}{1}\right)=ab=f\left(\frac{a}{1}\right)f\left(\frac{b}{1}\right).$$

Thus $$f\left(\frac{a}{1}+\frac{b}{1}\right)=f\left(\frac{a}{1}\right)+f\left(\frac{b}{1}\right)\ \text{ and }\ f\left(\frac{a}{1}\cdot\frac{b}{1}\right)=f\left(\frac{a}{1}\right)f\left(\frac{b}{1}\right).$$

Thus $f: D\to R$ is a ring isomorphim onto. Hence $D\cong R$.

Theorem 7.3. The quotient field F of an integral domain R is minimum extension of R to a field, that is to say any field K containing R, contains a subfield K′ isomorphic to the quotient field of R.

or The quotient field F of an integral domain is the smallest field of R. (GKP., 2006)

Proof. Let K be a field containing an integral domian R. Let F be the

quotient field of R so that

$$F = \left\{\frac{a}{b} : a, b \in R \text{ and } b \neq 0\right\}.$$

$a, b \in R$ and $b \neq 0 \Rightarrow a, b \in K$ and $b \neq 0$. For $R \subset K$

$\Rightarrow ab^{-1} \in K$. For K is field.

Let K' be a subset of K containing elements of the form ab^{-1}, where a, $b \in R$ s.t. $b \neq 0$.

Then $K' \subset K$. Now we shall show that K' is a subfied of K and K' is isomorphic to the quotient field F.

(i) To prove that K' is a subfield of K.

For this we have to show that

$$x, y \in K' \Rightarrow x - y \in K' \quad \ldots(1)$$

$$x, y \in K' \text{ and } y \neq 0 \Rightarrow xy^{-1} \in K' \quad \ldots(2)$$

$x, y \in K' \Rightarrow x = ab^{-1}, y = cd^{-1}$, for some a, b, c, d $\in R$ s.t. b, d $\neq 0$

$\Rightarrow x - y = ab^{-1} - cd^{-1} = add^{-1}b^{-1} - cbb^{-1}d^{-1}$

$= (ad - cb)\, b^{-1}d^{-1}$.

For $b^{-1}d^{-1} = d^{-1}b^{-1}$

$\Rightarrow x - y = (ad - cb)\,(db)^{-1} \in K'$

For $ad - cb \in R$ and $bd \neq 0$

$\Rightarrow x - y \in K'$. Which is (1).

$x, y \in K'$ s.t. $y \neq 0 \Rightarrow x = ab^{-1}, y = cd^{-1} \neq 0$ for some a, b, c, d $\in R$ s.t., b, d $\neq 0$

$\Rightarrow xy^{-1} = (ab^{-1})\,(cd^{-1})^{-1} = ab^{-1}\,dc^{-1} = adb^{-1}c^{-1}$

s.t. b, c, d $\neq 0$.

[For $cd^{-1} \neq 0 \Rightarrow c, d \neq 0$ and R is commutative.]

$\Rightarrow xy^{-1} = (ad)\,(cb)^{-1}$ s.t. $cb \neq 0$ and ad, cb $\in R$

$\Rightarrow xy^{-1} \in K'$. Which is (2).

(ii) To prove that $F \cong K'$.

Define a map $f : F \to K'$ s.t. $f\left(\frac{a}{b}\right) = ab^{-1}\ \forall\ \frac{a}{b} \in F$.

f is one-one.

For $f\left(\frac{a}{b}\right) = f\left(\frac{c}{d}\right) \Rightarrow ab^{-1} = cd^{-1} \Rightarrow ab^{-1}b = cd^{-1}b$

$\Rightarrow ae = cbd^{-1} \Rightarrow ad = cbd^{-1}d = cb$

$\Rightarrow ad = cb \Rightarrow (a, b) \sim (c, d)$

$\Rightarrow \frac{a}{b} = \frac{c}{d}$.

f is onto.

For any $ab^{-1} \in K'$ is the f image of $\frac{a}{b} \in F$ s.t. $f\left(\frac{a}{b}\right) = ab^{-1}$.

Further $$f\left(\frac{a}{b}+\frac{c}{d}\right) = f\left(\frac{a}{b}\right)+f\left(\frac{c}{d}\right).$$

For L.H.S. $= f\left(\frac{ad+bc}{bd}\right) = (ad+bc)(bd)^{-1}$

$= (ad+bc)(d^{-1}b^{-1})$

$= add^{-1}b^{-1} + bcd^{-1}b^{-1} = ab^{-1} + bb^{-1}cd^{-1}$

$= ab^{-1} + cd^{-1}$

$= f\left(\frac{a}{b}\right) + f\left(\frac{c}{d}\right) = \text{R.H.S.}$

Also $$f\left(\frac{a}{b}\cdot\frac{c}{d}\right) = f\left(\frac{a}{b}\right)\cdot f\left(\frac{c}{d}\right).$$

For L.H.S. $= f\left(\frac{ac}{bd}\right) = (ac)(bd)^{-1} = acd^{-1}b^{-1} = (ab^{-1})(cd^{-1})$

$= f\left(\frac{a}{b}\right) f\left(\frac{c}{d}\right) = \text{R.H.S.}$

Hence $f : F \to K'$ is a ring isomorphism onto, i.e., $F \cong K'$. **Proved.**

Deduction. The quotient field of a finite integral domain coincides with itself.

Proof. Suppose R is finite integral domain. Then R is a field. It means that the smallest field containing R is R itself. Also the quotient field of R is the smallest field containing R. Thus the quotient field of R is R itself.

Theorem. 7.4. Any two isomorphic integral domains have isomorphic quotient fields.

Proof. Let D and D′ be isomorphic integral domians so that ∃ a ring isomorphism $f : D \xrightarrow{\text{onto}} D'$.

Let a, b, c. d ∈ D be arbitrary s.t. f(a) = a′, f(b) = b′, f(c) = c′, f(d) = d′. Also we have

$$f(a+b) = f(a) + f(b) = a' + b' \quad \ldots(1)$$

$$f(ab) = f(a)\,f(b) = a'b'. \quad \ldots(2)$$

Let F and F′ be quotient fields of D and D′ respectively.

Then $$F = \left\{\frac{a}{b} : a, b \in D \text{ and } b \neq 0\right\},$$

$$F' = \left\{\frac{a'}{b'} : a', b' \in D' \text{ and } b' \neq 0\right\}.$$

Our aim is to show that $F \cong F'$.

Consider the map $\psi : F \to F'$ s.t. $\psi\left(\frac{a}{b}\right) = \frac{a'}{b'}$.

Let $\frac{a}{b}, \frac{c}{d} \in F$, then a, b, c, d ∈ D s.t. b, d ≠ 0.

It means that $f(a), f(b), f(c), f(d) \in D'$, i.e.,
$a', b', c', d' \in D'$ s.t. $b', d' \neq 0$.

First we shall show that the map ψ is well defined, i.e., if $\frac{a}{b} = \frac{c}{d}$, then $\psi\left(\frac{a}{b}\right) = \psi\left(\frac{c}{d}\right)$. We have $\frac{a}{b} = \frac{c}{d} \Rightarrow ad = bc \Rightarrow f(ad) = f(bc) \Rightarrow f(a) f(d) = f(b) f(c) \Rightarrow \frac{f(a)}{f(b)} = \frac{f(c)}{f(d)} \Rightarrow \psi\left(\frac{a}{b}\right) = \psi\left(\frac{c}{d}\right)$. Hence ψ **is well defined.**

ψ is one-one.

For $\psi\left(\frac{a}{b}\right) = \psi\left(\frac{c}{d}\right) \Rightarrow \frac{a'}{b'} = \frac{c'}{d'} \Rightarrow a'd' = b'c' \Rightarrow f(a) f(d) = f(b) f(c)$
$\Rightarrow f(ad) = f(bc) \Rightarrow ad = bc$. For f is one-one.
$\Rightarrow (a, b) \sim (c, d) \Rightarrow \frac{a}{b} = \frac{c}{d}$.

ψ is onto.

Since f is an isomorphism onto.

$\therefore$ Corresponding to elements $a', b' \in D'$ s.t. $b' \neq 0$ we have a preimage $a, b \in D$ s.t. $b \neq 0$. Then every element $\frac{a'}{b'} \in F'$ has a pre-image $\frac{a}{b} \in F$ s.t. $\psi\left(\frac{a}{b}\right) = \frac{a'}{b'}$.

ψ preserves addition and multiplication compositions.

$$\psi\left[\left(\frac{a}{b}\right) + \left(\frac{c}{d}\right)\right] = \psi\left(\frac{a}{b}\right) + \psi\left(\frac{c}{d}\right).$$

For L.H.S. $= \psi\left(\frac{ad + bc}{bd}\right) = \frac{a'd' + b'c'}{b'd'} = \frac{f(a) f(d) + f(b) f(c)}{f(b) f(d)}$

$$= \frac{f(a) f(d)}{f(b) f(d)} + \frac{f(b) f(c)}{f(b) f(d)} = \frac{f(a)}{f(b)} + \frac{f(c)}{f(d)}$$

$$= \frac{a'}{b'} + \frac{c'}{d'} = \psi\left(\frac{a}{b}\right) + \psi\left(\frac{c}{d}\right) = \text{R.H.S.}$$

Lastly $\psi\left(\frac{a}{b} \cdot \frac{c}{d}\right) = \psi\left(\frac{a}{b}\right) \cdot \psi\left(\frac{c}{d}\right)$.

For L.H.S. $= \psi\left(\frac{ac}{bd}\right) = \frac{a'c'}{b'd'} = \frac{a'}{b'} \cdot \frac{c'}{d'} = \psi\left(\frac{a}{b}\right)\psi\left(\frac{c}{d}\right) = \text{R.H.S.}$

Consequently ψ is a ring isomorphism onto, i.e., $F \cong F'$.

Problems.

1. Show that the set of numbers of the form $a + b\sqrt{3}$ with a and b as rational numbers is a field.
2. Find whether the set of numbers

$$R = \left\{a + b\sqrt{2} + c\sqrt{3} : a, b, c \in Z\right\}$$

is a ring w.r.t. addition and multiplication.

3. Find whether the set

$$R = \left\{a + b2^{\frac{1}{3}} + c4^{\frac{1}{3}} : a, b, c \in Q\right\}$$

is an integral domain or a field.

[HINT : It is an integral domain. Proceed similar to example 2.7.]

4. Prove that the set Z of integers is a ring in which addition and multiplication are defined below indicated by $\oplus$ and $\odot$ respectively $a \oplus b = a + b - 1$, $a \odot b = a + b - ab$,

where $a, b \in Z$.

[HINT : Example 2.8. Here 0–element is 1 and 1–element is 0.]

5. Show that the set

$D = \{a + b\sqrt{3} : a, b \in R\}$ is an integral domain w.r.t. addition and multiplication of numbers. Are there any elements in this domain other than ± 1, which possess multiplicative inverse ?

[HINT : Example 4.18]

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

Solution. Let $R = \{a + ib : a, b \in Z\}$, so that R is a set of Gaussian integers. Let $x = a + ib$ and $y = c + id$ be arbitrary elements of R so that a, b, c, d are integers.

$$x + y = (a + ib) + (c + id) = (a + c) + i(b + d)$$
$$xy = (a + ib)(c + id) = (ac - bd) + i(bc + ad).$$

Since numbers in the brackets on R.H.S. of both equations are integers and so L.H.S. of both equations are Gaussian integers. Hence R is closed w.r.t. (+) and (·).

Let $z = e + if \in R$.

(i) (R, +) is an Abelian group. For

(A_1). **Closure axion.** $x + y \in R$, (already proved)

(A_2). **Existence of identity.** $0 = 0 + i0 \in R$ is additive identity s.t.

$$x + 0 = 0 + x = x.$$

(A_3). **Commutative law.** $x + y = y + x$.

(A_4). **Associative law.** $(x + y) + z = x + (y + z)$.

Addition is commutative as well as associative in R. For (C, +) is an

Abelian group, where

C = set of complex numbers.

(A_5). Existence of inverse. $x = a + ib \in R$ has its inverse $-x = -a + i(-b) \in R$ s.t.

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

(ii) $(R_1, \cdot)$ is not Abelian, $R_1 = R - \{0\}$. For

(B_1). Closure axiom. $xy \in R_1$, already proved.

(B_2). Existence of identity. $1 = 1 + i(0) \in R$ is multiplicative identity s.t.

$$x \cdot 1 = 1 \cdot x = x.$$

(B_3). Commutative law. $xy = yx$.

For
$$\begin{aligned} xy &= (ac - bd) + i(bc + ad) \\ &= (ca - db) + i(cb + da) \\ &= (c + id)(a + ib) = yx. \end{aligned}$$

(B_4). Associative law. $(xy)z = x(yz)$.

(B_5). Existence of inverse. If $x \neq 0 \in R$, then its multiplicative inverse

$$x^{-1} = \frac{1}{x} = \frac{1}{a+ib}$$

$$= \frac{a}{a^2+b^2} + i\left(\frac{-b}{a^2+b^2}\right) \notin R$$

For $\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}$ are not integers.

(iii) **Distributive law.** $x(y + z) = xy + xz$,

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

For multiplication of complex numbers is distributive over addition.

Hence $(R, +, \cdot)$ is not fied as (B_5) is not satisfied.

(iv) $xy = 0 \Rightarrow x = 0, y = 0$, i.e., R has no zero divisors.

Hence $(R, +, \cdot)$ is an integral domain.

7. If in a ring R with unity, $(xy)^2 = x^2y^2 \ \forall\ x, y \in R$, then prove that R is commutative.

[HINT : Let R be a ring with unity, then $1 \in R$. Let $x, y \in R$ be arbitrary and

$$(xy)^2 = x^2y^2 \qquad ...(1)$$

$$x, y \in R \Rightarrow 1 + x, 1 + y \in R \qquad ...(2)$$

By virtue of (1), we get

$$[(1 + x)y]^2 = (1 + x)^2 y^2$$

or
$$(y + xy)^2 = (x^2 + 2x + 1)y^2$$

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

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

Using (1), $y^2 + yxy + xy^2 + x^2y^2 = x^2y^2 + 2xy^2 + y^2$

Cancellation law in (R, +) gives

$$yxy = xy^2 \qquad ...(3)$$

Replacing y by 1 + y in (2),

$$(1 + y)\,x\,(1 + y) = x\,(1 + y)^2$$

or $$(x + yx)\,(1 + y) = x\,(1 + y^2 + 2y)$$

or $$x + yx + xy + yxy = x + xy^2 + 2xy$$

or $$yx + yxy = xy^2 + xy$$

Using (2), $$yx + xy^2 = xy^2 + xy$$

or $$yx = xy. \quad]$$

8. Prove that a ring R is commutative iff $(a + b)^2 = a^2 + 2ab + b^2$, $\forall\ a, b \in R$.

9. Consider the set $Z \times Z$ with addition and multiplication defined as follows :

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

and $(a, b) \cdot (c, d) = (ac, bd)$, $\forall\ a, b, c, d \in Z$. Then $Z \times Z$ forms a commutative ring with unit element. **[GKP, 1986]**

10. Prove that for any prime p, the set

$$Q(\sqrt{p}) = \{a + b\sqrt{p} : a, b \in Q\}$$

forms a ring under the operations of usual addition and multiplication of real numbers. **[GKP, 1985, 86, 99, PU, 1989]**

[HINT : $(Q\sqrt{p}, +)$ is an Abelian group

(i) for $x = a+b\sqrt{p}$, $y=c+d\sqrt{p} \in Q\sqrt{p}$,

$x + y = a+c + (b+d)\sqrt{p} \in Q\sqrt{p}$,

(ii) for $x = a+b\sqrt{p}$, $y=c+d\sqrt{p}$, $z=e+f\sqrt{p} \in Q\sqrt{p}$,

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

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

(iii) $0 = 0 + 0\sqrt{p} \in Q\sqrt{p}$ is the additive identity because

$x + 0 = (a+b\sqrt{p}) + 0 = x$,

(iv) for $x = a + b\sqrt{p} \in Q\sqrt{p}$, $-x = -a-b\sqrt{p} \in Q\sqrt{p}$ is the additive inverse because $x + (-x) = 0$,

(v) for $x = a+b\sqrt{p}$, $y = c+d\sqrt{p} \in Q\sqrt{p}$

$x + y = (a+c) + (b+d)\sqrt{p} \Rightarrow (c+a) + (d+b)\sqrt{p} = y+x$.

$(Q\sqrt{p}, \cdot)$ is a semi group

$$x \cdot y = (a+b\sqrt{p})(c+d\sqrt{p})$$
$$= (ac+bdp) + (ad+bc)\sqrt{p} \in Q\sqrt{p}$$

and $\forall\ x, y, z \in Q\sqrt{p} \Rightarrow (x \cdot y).\ z = x.\ (y \cdot z)$ associative law holds.

Distributive laws hold for all $x, y, z \in Q\sqrt{p}$

$\Rightarrow x \cdot (y+z) = x \cdot y + x \cdot z$

and $(y+z) \cdot x = y \cdot x + z \cdot x$ in which

$$x.(y+z) = (a+b\sqrt{p})[(c+e) + (d+f)\sqrt{p}]$$
$$= ac+ae+ad\sqrt{p} + af\sqrt{p} + bc\sqrt{p} + be\sqrt{p} + bdp+bfp.$$
$$= x \cdot y + x \cdot z. \quad]$$

11. Let $(R, +, \cdot)$ be a system which satisfies all the postulates for a ring except that of commutativity of addition. Prove that

(i) If R contains an elements c that can be left cancelled in the sense that

$ca = cb \Rightarrow a = b$, then R is a ring ;

(ii) If R has a multiplicative identity 1, then it is a ring. **(GKP, 2000)**

[HINT : (i) $c(a+b)-c(b+a)$
$= c(a+b) + (-c)(b+a)$
$= ca+cb+(-c)b+(-c)a$
$= ca+cb-cb-ca$
$= 0.$

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

Therefore $a+b = b+a.$ (by left cancellation law)

That is addition is commutative in R.

Hence R is a ring.

(ii) $(1+1)(a+b) = 1(a+b)+1(a+b)$ (by distributive law)
$= a+b+a+b$ (by distributive law)

Again $(1+1)(a+b) = (1+1)a+(1+1)b$ (by distributive law)
$= a+a+b+b$ (by distributive law)

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

so that $b+a = a+b.$ (by cancellation laws)]

12. Consider the set R of all real valued functions defined over the closed interval [0, 1]. Define addition and multiplication in R as follows :

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

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

where f and g are any two elements in R.

Prove that R is a commutative ring with unit element.

[HINT : The zero element of R is the zero map. That is, it is the

constant function which has the value zero for all x in [0, 1].

The unit element is the constant function which has value 1 for every value of x in [0, 1]. Other axioms can easily be verified.]

13. Consider the set R of all real valued functions of a real variable. We define addition and multiplication in R as follows :

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

and $$(f \cdot g)(x) = f[g(x)] \qquad \forall\, f, g \in R.$$

Prove that these operations define the structure of a non-commutative ring with unit element.

[HINT : The unit element is the identity map given by I(x)=x for all real x.

The ring is non-commutative. For, if we take

$$f(x) = x^2 \text{ and } g(x) = e^{-|x|},$$

then $$(f \cdot g)(x) = f[g(x)] = f(e^{-|x|}) = e^{-2|x|}$$

and $$(gf)(x) = g[f(x)] = g(x^2) = e^{-|x^2|}$$

so that $$f \cdot g \neq g \cdot f.$$

Of course it is easy to see that $(f \cdot g)(x) \neq (g \cdot f)(x)$ for at least $x = 3$. Note the difference in the multiplication.]

14. Let R_2 be the set of all 2×2 matrices whose elements are real numbers. For any two matrices $A = (a_{ij})$, $B = (b_{ij})$, define

$$A+B = (a_{ij}+b_{ij}) \text{ and } AB = (c_{ij}),$$

where

$$C_{ij} = \sum_{k=1}^{2} a_{ik} b_{kj}.$$

Show that under these operations R_2 is a ring.

This ring is called the ring of 2×2 matrices over the reals.

15. Whether the union of two subrings is a subring or not ? Give example in support of your answer. [GKP, 2003]

16. Prove that the direct (respectively inverse) image of a subring under a ring homomorphism is a subring.

[HINT : Let S be a subring of R and let $f(s_1), f(s_2) \in f(S)$, where $s_1, s_2 \in S$.

Then $$f(s_1) - f(s_2) = f(s_1 - s_2) \in f(S) \text{ and}$$

$$f(s_1) \cdot f(s_2) = f(s_1 s_2) \in f(S).$$

Hence f(S) is a subring of R.

The other part can similarly be proved.]

17. If R is a ring and $a \in R$, show that

$$N(a) = \{r \in R : ar = ra\}$$

is a subring of R and that the centre of R is a subring of N(a). N(a) is called the normalizer of the element a in R.

18. Let R be a ring and $a \in R$ be a fixed element, Prove that $Ra = \{ra : r \in R\}$ is a subring of R. **[GKP, 2004]**

19. Prove that the set Z_3 of residue classes modulo 3 is an integral domain.

20. Prove that a commutative ring with identity is a field if it has no proper ideals, i.e. it is simple. **[GKP, 84, 96, PU, 95]**

21. Give an example of an infinite commutative ring without zero divisors which is not a field.

[HINT : $< Z, +, \cdot >$.]

22. Let R be a non-zero finite integral domain. Prove that R is a field.

23. Let a and b be arbitrary elements of a ring R whose characteristic is 2 and ab = ba. Then show that $(a + b)^2 = a^2 + b^2 = (a - b)^2$.

[HINT : Let $ab = ba = x \in R$.

Characteristic of R is two $\Rightarrow 2x = 0 \quad \forall x \in R$

$\Rightarrow x + x = 0$.

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

$= a^2 + ab + ba + b^2 = a^2 + (x + x) + b^2 = a^2 + 0 + b^2$

$= a^2 + b^2$.

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

$= a^2 - ab - ba + b^2 = a^2 - (x + x) + b^2 = a^2 - 0 + b^2$

$= a^2 + b^2$.

Thus $(a + b)^2 = a^2 + b^2 = (a - b)^2$.]

24. If R is a ring in which $x^2 = x$ for every x in R, prove that R is commutative ring of characteristic 2. **(I.A.S. 1997)**

[HINT: Let R be a ring s.t.

any $x \in R \Rightarrow x^2 = x$. ...(1)

To prove that

(i) characteristic of R is 2, i.e., $x + x = 0 \quad \forall x \in R$.

(ii) R is commutative, i.e., $xy = yx \quad \forall x, y \in R$.

(i) $(x+x)^2 = (x+x)(x+x) = x(x+x) + x(x+x)$

$= (x^2 + x^2) + (x^2 + x^2)$, by distributive law

$= (x + x) + (x + x)$, by (1).

But $(x+x)^2 = x + x$, by virture of (1).

Hence $x + x = (x + x) + (x + x)$

or $(x + x) + 0 = (x + x) + (x + x)$.

Left cancellation law for addition in R gives $0 = x + x$. ...(2)

(ii) Let $x, y \in R$ be arbitrary. Then

$x + y = (x + y)^2$, by virtue of (1)
$= (x + y)(x + y)$
$= x(x + y) + y(x + y)$
$= (x^2 + xy) + (yx + y^2)$, by distributive law
$= (x + xy) + (yx + y)$, again by (1)
$= (x + y) + (xy + yx)$. For (R, +) is commutative

Finally, $x + y = (x + y) + (xy + yx)$

or $(x + y) + 0 = (x + y) + (xy + yx)$.

Left cancellation law of addition in R gives $0 = xy + yx$.

Taking $xy = x'$, $yx = y'$, we get

$x' + y' = 0$

$x' + y' = 0 \Rightarrow x' + y' = 0 = x' + x'$, by (2)
$\Rightarrow x' + y' = x' + x'$
$\Rightarrow y' = x'$, by left cancellation law
$\Rightarrow yx = xy$.]

25. Prove that the set of all numbers of the form $a + b\sqrt{p}$ is a field w.r.t. ordinary addition and multiplication, where a, b, p are rational numbers and p is a prime positive. (GKP., 2008)

[HINT: Let $R = \{a + b\sqrt{p} : a, b \in Q\}$.

(R, +, ·) is a commutative ring with unity element $1 + 0\sqrt{p} = 1$. Zero element being $0 + 0\sqrt{p}$. Let $a + b\sqrt{p}$ be a non-zero element of R so that at least one of a and b is non-zero. Multiplicative inverse of $a + b\sqrt{p}$ is

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

At least one of a and b is non-zero $\Rightarrow a^2 - pb^2 \neq 0$. Hence non-zero elements of R have multiplicative inverse in R. Hence R is a field.]

26. Prove that the set

$Z_7 = \{[0], [1], [2], [3], [4], [5], [6]\}$

forms a field w.r.t. addition and multiplication module 7.

27. If D is an integral domain, then show that $D' = \{me : m \in Z\}$ is a sub integral domain of D. e being a unity element of D.

28. If R be a ring and $a \in R$, than show that

$aR = \{ar : r \in R\}$ is an ideal of R. [GKP, 2000]

[HINT : Theorem 5.11.]

29. Let R be a ring with unity element such that the only left ideals of R are {0} and R. Show that R is a division ring.

[**Hint :** Theorem 5.9]

30. If S is an ideal of a ring R, then $R \simeq R/S$, i.e., R/S is a homomorphic image of R.

or

Every quotient ring is homomorphic image of the ring.

[**Hint :** Let S be a ideal of a ring R, then R/S is a quotient ring. Consequently the map

$$g : R \to R/S \text{ s.t. } g(a) = S + a.$$

Evidently g is well defined.

Let $a, b \in R$ be arbitrary.

(i) g is onto.

For any $R + a \in R/S$ is g-image of $a \in R$ s.t. $g(a) = S + a$.

(ii) $g(a + b) = g(a) + g(b)$.

For L.H.S. $= g(a + b) = S + (a + b) = (S + a) + (S + b)$

$= g(a) + g(b) = R.H.S.$

(iii) $g(ab) = g(a)\, g(b)$.

For L.H.S. $= g(ab) = S + ab = (S + a)(S + b)$

$= g(a)\, g(b) = R.H.S.$

Hence the map $g : R \to R/S$ is a homomorphism onto.

Therefore $R \simeq R/S$.

It is the converse of fundamental theorem of rings.]

31. Let $I = 4Z$ in the ring $R = (Z, +, .)$. Find the elements of the quotient ring R/I (the set of cosets of I in R). **[GKP, 2005]**

[HINT : $R/I = Z/4Z = \{[0], [1], [2], [3]\}$.]

32 Examine whether the mapping $f : Z \to xZ$ defined by $(fm) = xm$ $m \forall Z$ $m \in Z$ is a ring homomorphism. (GKP, 2007)

—x—