2 Introduction to Rings, Integral Domains and Fields

§ 2.1 INTRODUCTION

So far we have studied an algebraic structure known as group consisting of a non-empty set and one binary operation satisfying certain axioms. In this chapter we shall study another important algebraic structure known as ring, consisting of a non-empty set and two binary operations satisfying certain axioms.

§ 2.2 RING

(Purvanchal 95, 99; Gorakhpur 96, 99, 2004, 15)

An algebraic system $(R, +, \cdot)$ consisting of a non-empty set R and two binary operations $+$ and $\cdot$ called addition and multiplication respectively, is called a ring if the following axioms are satisfied :

R_1) $(R, +)$ forms an abelian group *i.e.*

(i) $\forall \quad a, b \in R, a + b \in R$ (closure law for addition)

(ii) $(a + b) + c = a + (b + c) \quad \forall \quad a, b, c \in R$
(associative law for addition)

(iii) $\exists$ an element $0 \in R$ called additive identity such that
$a + 0 = a \quad \forall \quad a \in R$
(Existence of additive identity)

(iv) To each $a \in R$, $\exists - a \in R$ called additive inverse of a such that
$a + (-a) = 0$ (Existence of additive inverse)

(v) $a + b = b + a \quad \forall \quad a, b \in R$ (Commutative law for addition)

R_2) $(R, \cdot)$ forms a semigroup *i.e.*

(i) $\forall \quad a, b \in R, \quad a \cdot b \in R$ (Closure law for multiplication)

(ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c), \quad \forall \quad a, b, c \in R$
(Associative law for multiplication)

R_3) Multiplication over addition is left and right distributive
i.e. $\forall \quad a, b, c \in R,$

(i) $a \cdot (b + c) = a \cdot b + a \cdot c$

(ii) $(b + c) \cdot a = b \cdot a + c \cdot a.$

If multiplication in a ring $(R, +, \cdot)$ is commutative *i.e.* $a \cdot b = b \cdot a \quad \forall$ $a, b \in R$, we say that the ring $(R, +, \cdot)$ is a commutative ring.

If $\exists$ an identity element for multiplication in ring R, usually denoted by 1, so that $a \cdot 1 = 1 \cdot a = a \ \forall \ a \in R$, then we say that the ring $(R, +, \cdot)$ is with unit element or with identity element.

Example 1. The set Z of integers with usual addition and multiplication forms a commutative ring with unit element.

Let Z be the set of integers, then

R_1) $(Z, +)$ is an abelian group, since

(i) $\forall \ a, b \in Z, a + b \in Z$

(since the sum of two integers is an integer)

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

(since addition is associative in Z)

(iii) $\exists$ integer zero, $0 \in Z$ such that

$$a + 0 = a, \quad \forall \quad a \in Z$$

(iv) To each $a \in Z$, $\exists - a \in Z$ such that

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

(v) $\forall \ a, b \in Z, \ a + b = b + a$

(since addition is commutative in Z)

R_2) $(Z, \cdot)$ is a semigroup, since

(i) $\forall \ a, b \in Z, a \cdot b \in Z$

(since the product of two integers is an integer)

(ii) $\forall \ a, b, c \in Z, (a \cdot b) \, . \, c = a \cdot (b \cdot c)$

(since multiplication is associative in Z)

R_3) The multiplication over addition of integers is left and right distributive *i.e.*

$$\forall \quad a, b, c \in Z,$$

(i) $a \cdot (b + c) = a \cdot b + a \cdot c$

(ii) $(b + c) \cdot a = b \cdot a + c \cdot a$

Therefore $(Z, +, \cdot)$ is a ring.

It is a commutative ring, since multiplication of integers is commutative *i.e.* $\forall \ a, b \in Z,$

$$a \cdot b = b \cdot a$$

It has unit element $1 \in Z$ such that

$$1 \cdot a = a \cdot 1 \quad \forall \quad a \in Z$$

Hence $(Z, +, \cdot)$ is a commutative ring with unit element.

Example 2. *The sets Q, R, C of rational numbers, real numbers, complex numbers respectively form commutative rings with unit elements under usual addition and multiplication.*

We can prove in similar manner that the systems $(Q, +, \cdot)$ and $(R, +, \cdot)$ are commutative rings with unit elements.

Now we shall prove that the system $(C, +, \cdot)$ is a ring.

R_1) $(C, +)$ is an abelian group

R_2) $(C, \cdot)$ is semigroup, since

(i) $\forall \quad z_1 = a + ib, \; z_2 = c + id \in C,$

$$z_1 \cdot z_2 = (ac - bd) + i(bc + ad) \in C$$

(ii) Multiplication of complex numbers is associative *i.e.*

$$\forall \quad z_1, z_2, z_3 \in C, \; (z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$$

R_3). Multiplication over addition of complex numbers is left and right ditributiv

i.e. $\forall \; z_1, z_2, z_3 \in C,$

$$z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3$$

and $$(z_2 + z_3) \cdot z_1 = z_2 \cdot z_1 + z_3 \cdot z_1$$

Therefore $(C, +, \cdot)$ is a ring.

It is a commutative ring, since multiplication of complex numbers is commutati

i.e. $\forall \quad z_1, z_2 \in C,$

$$z_1 \cdot z_2 = z_2 \cdot z_1,$$

It has unit element $1 = 1 + i0 \in C$, such that $\forall \quad z = a + ib \in C,$

$$1 \cdot z = z \cdot 1$$

Hence $(C, +, \cdot)$ is a commutative ring with unit element.

Example 3. The set $Q(\sqrt{p}) = \{a + b\sqrt{p} : a, b \in Q, p$ is any prime$\}$ forms a ring under usual addition and multiplication of real numbers.

(Gorakhpur 1986, 99, 200

Solution.

R_1) $(Q\sqrt{p}, +)$ is an abelian group, since

(i) $\forall \quad x = a + b\sqrt{p}, y = c + d\sqrt{p} \in Q\sqrt{p},$

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

(ii) For $x = a + b\sqrt{p}, y = c + d\sqrt{p}, z = e + f\sqrt{p} \in Q\sqrt{p},$

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

$$= ((a + c) + e) + ((b + d) + f)\sqrt{p}$$

$$= (a + (c + e)) + (b + (d + f))\sqrt{p}$$

(since addition is associative in Q)

$$= x + (y + z)$$

(iii) $\exists \; 0 = 0 + 0\sqrt{p} \in Q\sqrt{p},$

called additive identity such that $\forall \quad x = a + b\sqrt{p} \in Q\sqrt{p},$

$$x + 0 = x.$$

(iv) To each $x = a + b\sqrt{p} \in Q\sqrt{p}, \; \exists - x = -a - b\sqrt{p} \in Q\sqrt{p},$ called additive inverse of x such that $x + (-x) = 0$

(v) $\forall \quad x = a + b\sqrt{p}, \quad y = c + d\sqrt{p} \in Q\sqrt{p}$

$$x + y = (a + c) + (b + d)\sqrt{p}$$

$$= (c + a) + (d + b)\sqrt{p} = y + x.$$

R_2) $(Q\sqrt{p}, \cdot)$ is a semi group, since

(i) $\quad x = a + b\sqrt{p}, \; y = c + d\sqrt{p} \in Q\sqrt{p},$

$$x \cdot y = (ac + bdp) + (ad + bc)\sqrt{p} \in Q\sqrt{p}$$

(ii) $\forall\ x, y, z \in Q\sqrt{p}$,

$$(x \cdot y)\, z = x \cdot (y \cdot z) \quad i.e.$$

multiplication is associative.

R_3) Multiplication over addition is left and right distributive in $Q\sqrt{p}$.

(i) $\forall\ x, y, z \in Q\sqrt{p}$

$$x \cdot (y + z) = (a + b\sqrt{p})\,\{(c + e) + (d + f)\sqrt{p}\}$$
$$= ac + ae + ad\sqrt{p} + af\sqrt{p} + bc\sqrt{p} + be\sqrt{p} + bdp + bfp$$

and $x \cdot y + x \cdot z = ac + ad\sqrt{p} + bc\sqrt{p} + bdp + ae + af\sqrt{p} + be\sqrt{p} + bfp.$

This shows that $x \cdot (y + z) = x \cdot y + x \cdot z$

Similarly, we can prove that

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

Hence $(Q\sqrt{p}, +, \cdot)$ is a ring.

Example 4. Consider the set $Z \times Z$ with addition and multiplication defined a follows :

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

and $(a, b).(c, d) = (ac, bd)\ \forall\ a, b, c, d \in Z.$

Then $Z \times Z$ forms a commutative ring with unit element.

Solution.

R_1) $(Z \times Z, +)$ is an abelian group, since

(i) $\forall\ x = (a, b),\ y = (c, d) \in Z \times Z$

$$x + y = (a + c, b + d) \in Z \times Z.$$

(ii) Addition is associative *i.e.* $\forall\ x = (a, b),$

$$y = (c, d),\ z = (e, f) \in Z \times Z$$
$$(x + y) + z = ((a + c) + e, (b + d) + f)$$
$$= (a + (c + e), b + (d + f))$$

(since addition is associative in Z)

$$= x + (y + z).$$

(iii) $\exists\ 0 = (0, 0) \in Z \times Z$ *s.t.* $\forall\ x \in Z \times Z,$

$$x + 0 = (a + 0, b + 0) = (a, b) = x$$

(iv) To each $x = (a, b) \in Z \times Z$, $\exists\ -x = (-a, -b) \in Z \times Z$ *s.t.*

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

(v) $\forall\ x, y \in Z \times Z,$

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

R_2) $(Z \times Z, \cdot)$ is a semigroup, since

(i) $\forall\ x, y \in Z \times Z$

$$x \cdot y = (ac, bd) \in Z \times Z.$$

(ii) $\forall\ x, y, z \in Z \times Z,$

$$(x \cdot y) \cdot z = ((ac)\, e, (bd)\, f)$$
$$= (a(ce), b(df))$$
$$= x \cdot (y \cdot z).$$

R_3) Multiplication over addition is left and right distibutive in $Z \times Z$ *i.e.*

(i) $x \cdot (y + z) = (a, b)\,.\,(c + e, d + f)$

$$= (ac + ae, bd + bf)$$
$$= (ac, bd) + (ae, bf)$$
$$= x \cdot y + x \cdot z$$

Similarly, we can prove that

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

Therefore, $(Z \times Z, +, \cdot)$ is a ring.

It is commutative ring, since multiplication is commutative *i.e.*

$$x \cdot y = (ac, bd) = (ca, db) = y \cdot x.$$

It has unit element $(1, 1) \in Z \times Z$,

since $\forall \quad (a, b) \in Z \times Z$,

$$(a, b) \cdot (1, 1) = (a, b).$$

Hence $(Z \times Z, +, \cdot)$ is a commutative ring with unit element.

Example 5. The set Z_m of residue classes modulo a positive integer m is a ring with respect to addition and multiplication of residue classes.

Solution.

Let $$Z_m = \{\bar{0}, \bar{1}, \bar{2}, ..., \bar{r}_1, ... \bar{r}_2, ..., \overline{m-1}\}$$

be the set of residue classes modulo m.

R_1) $(Z_m, +)$ is an abelian group.

(Example 10, art. 1.18)

R_2) $(Z_m, \cdot)$ is a semi-group, since

(i) $\forall \quad \bar{r}_1, \bar{r}_2 \in Z_m$

$$\bar{r}_1 \cdot \bar{r}_2 = \overline{r_1 r_2} = \bar{r} \in Z_m,$$

where r is the least non-negative remainder, when $r_1 r_2$ is divided by m

(ii) Multiplication of residue classes is associative *i.e.*

$$\forall \quad \bar{r}_1, \bar{r}_2, \bar{r}_3 \in Z_m$$

$$(\bar{r}_1 \cdot \bar{r}_2) \cdot \bar{r}_3 = (\overline{r_1 r_2}) \cdot \bar{r}_3$$
$$= \overline{(r_1 r_2) r_3}$$
$$= \overline{r_1 (r_2 r_3)}$$
$$= \bar{r}_1 \cdot (\bar{r}_2 \cdot \bar{r}_3).$$

R_3) Multiplication over addition is left and right distributive in Z_m.

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

It is a commutative ring, since multiplication of residue classes is commutative

It has unit element $\bar{1}$.

Therefore $(Z_m, +, \cdot)$ is a commutative ring with unit element.

Example 6. Show that the ... of ...

2.3 PROPERTIES OF RINGS

Let $(R, +, \cdot)$ be a ring. Then for $a, b, c \in R$

(i) $a \cdot 0 = 0 \cdot a = 0$, *(Purvanchal 96; Gorakhpur 97)*

(ii) $a(-b) = (-a) \cdot b = -(a \cdot b)$ *(Purvanchal 96; Gorakhpur 97, 99)*

(iii) $(-a) \cdot (-b) = a \cdot b$ *(Gorakhpur 99)*

(iv) $a \cdot (b - c) = a \cdot b - a \cdot c$ *(Gorakhpur 99, 2011)*

and $(b - c) \cdot a = b \cdot a - c \cdot a$. *(Gorakhpur 2011)*

Proof.

(i) $a \cdot 0 = a \cdot (0 + 0)$

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

Therefore $a \cdot 0 + a \cdot 0 = a \cdot 0 + 0$ ($x + 0 = x$ in a group)

Hence $a \cdot 0 = 0$.

(Left concellation law of addition in a group)

Similarly, we can prove that

$0 \cdot a = 0$

(ii) We have $a \cdot (-b) + a \cdot b = a \cdot (-b + b)$ (distributive law)

$= a \cdot 0$

$= 0$ by (i)

Therefore $a \cdot (-b)$ is additive inverse of $a \cdot b$.

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

Similarly, we can prove that

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

(iii) $(-a) \cdot (-b) = -(a \cdot (-b))$ by (ii)

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

$= a \cdot b$ [because $-(-x) = x$ in a group]

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

$= a \cdot (b + 0)$

$= a \cdot b$

or $a \cdot (b - c) = a \cdot b - a \cdot c$

Similarly, we can prove that

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

Example 1. If the ring R has the multiplicative identity 1, prove that $1 \neq 0$ unless $R = \{0\}$

Solution. If $1 = 0$ and $a \in R$, then

$a = a \cdot 1 = a \cdot 0 = 0$

Hence $R = \{0\}$

Example 2. Let $P(S)$ be power set of a given set.

Then $(P(S), \Delta, \cap)$ is a commutative ring with identity element.

Solution.

R_1) $(P(S), \Delta)$ is an abelian group, since

(i) $\forall\ A, B \in P(S)$

$A \Delta B = (A - B) \cup (B - A) \in P(S)$

(ii) The symmetric difference is associative *i.e.* $\forall\ A, B, C \in P(S)$,

$(A \Delta B) \Delta C = A \Delta (B \Delta C)$

(iii) $\exists\, \phi \in P(S)$ such thant $\forall\ A \in P(S)$,

$A \Delta \phi = (A - \phi) \cup (\phi - A)$

$= A \cup \phi$

$= A$

i.e. ϕ is additive identity.

(iv) Additive inverse of $A \in P(S)$ is A

since $A \Delta A = (A - A) \cup (A - A)$

$= \phi \cup \phi = \phi$

(v) Symmetric difference is commutative *i.e.*

$\forall\ A, B \in P(S)$

$A \Delta B = (A - B) \cup (B - A)$

$= (B - A) \cup (A - B)$

$= B \Delta A$

R_2) $(P(S), \cap)$ is a semigroup, since

(i) $\forall\ A, B \in P(S)$,

$A \cap B \in P(S)$

(ii) Intersection is associative *i.e.*

$\forall\ A, B, C \in P(S)$,

$(A \cap B) \cap C = A \cap (B \cap C)$

R_3) Intersection over symmetric difference is left and right distributive

$\forall\ A, B, C \in P(S)$

$A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$

and $(B \Delta C) \cap A = (B \cap A) \Delta (C \cap A)$

Therefore $(P(S), \Delta, \cap)$ is a ring.

It is commutative ring, since intersection is commutative *i.e.* $\forall\ A,\ B \in P(S)$

$$A \cap B = B \cap A$$

It has multiplicative identity S, since $\forall\ A \in P(S)$

$$A \cap S = A$$

Hence $(P(S), \Delta, \cap)$ is a commutative ring with identity.

Example 3. 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 element 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.

Solution.

(i) For any $a, b \in R$, we have

$$\begin{aligned} c(a+b) - c(b+a) &= c(a+b) + (-c)(b+a) \\ &= ca + cb + (-c)b + (-c)a \\ &= ca + cb - cb - ca \\ &= 0 + 0 \\ &= 0. \end{aligned}$$

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

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

That is addition is commutative.

Hence R is a ring.

(ii) We have

$$(1+1)(a+b) = 1(a+b) + 1(a+b) \text{ (by distributive law)}$$
$$= a + b + a + b \text{ (since 1 is multiplicative identity)}$$

Again

$$\begin{aligned} &(1+1)(a+b) \\ &= (1+1)a + (1+1)b \quad \text{(by distributive law)} \\ &= a + a + b + b \quad \text{(by distributive law)} \end{aligned}$$

Therefore

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

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

(by left and right cencellation laws)

Hence R is a ring.

Example 4. If R is a ring with unity element 1, then prove that

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

(ii) $(-1).(-1) = 1.$

Solution. We know if 1 be the unity element in the ring R, then

$$a.1 = 1.a = a \quad \forall\ a \in R \qquad \text{...(i)}$$

(i) Now $[1 + (-1)].a = 1.a + (-1).a, \forall\ a \in R$

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

or $o = a + (-1)\,a$

or $(-1)a = -a$

Again from (i) we get $a = a \cdot 1$

or $a + a.(-1) = a.1 + a.(-1)$, adding $a.(-1)$ on the right of both sides

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

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

(ii) From part (i) we have $a\,.\,(-1) = -a$

Replacing a by (-1) in this result we get $(-1).(-1) = -(-1)$

i.e., $(-1).(-1) =$ additive inverse of (-1), where -1 is itself the additive inverse of 1 in R.

$= 1$ **Hence proved.**

§ 2.4 RING WITH ZERO-DIVISORS AND RING WITHOUT ZERO-DIVISORS

Let R be a ring. An element $(a \neq 0) \in R$ is said to be a left zero-divisor if there exists a non- zero element $b \in R$ such that $ab = 0$.

An element $(a \neq 0) \in R$ is said to be a right zero-divisor if there exists a non-zero element $b \in R$ such that $ba = 0$.

An element which is both left and right zero-divisor is called a zero-divisor or proper zero-divisor.

A ring which contains zero divisors is called a ring with zero divisor.

A ring which contains no zero-divisor, is called a ring without zero-divisors.

Example 1. The ring of residue classes modulo a composite positive integer m, is a ring with zero divisors.

Solution. Let $Z_m = \{\bar{0}, \bar{1}, \ldots\ldots, \overline{m-1}\}$ be a ring of residue classes modulo a composite positive integer m. Then

$$m = rs, \quad \text{where } 0 < r < m, \ 0 < s < m$$

Now $\bar{m} = \bar{r}\,\bar{s} = \bar{0}$.

But $\bar{r} \neq \bar{0}$ and $\bar{s} \neq \bar{0}$.

Therefore $\bar{r}, \bar{s}$ are zero-divisors

Hence Z_m is a ring with zero divisors

Example 2. The ring Z_6 of residue classes, modulo 6, is a ring with zero divisors.

Example 3. The rings I, Q and R of integers, rational numbers, and real numbers are rings without zero- divisors.

§ 2.5. CANCELLATION LAWS IN A RING.

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

$$a \cdot b = a \cdot c \Rightarrow b = c \text{ (left cancellation law)}$$

$$b \cdot a = c \cdot a \Rightarrow b = c \text{ (Right cancellation law)}$$

hold, we say that the restricted cancellation laws hold in R.

Theorem A ring R is without zero divisors iff the restricted cancellation laws hold in R. ***(Purvanchal 93, 98, 99; Gorakhpur 99, 2010, 15)***

Proof. Suppose that R is a ring without zero divisors

i.e. $ab = 0 \Rightarrow a = 0$ or $b = 0$ or both are zero.

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

$$a \cdot b = a \cdot c \Rightarrow a \cdot (b - c) = 0 \quad \text{(by distributive law)}$$

Since $a \neq 0$, therefore $b - c = 0$

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

Thus $a \cdot b = a \cdot c \Rightarrow b = c.$

Similarly, we can prove 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 be a ring with zero divisors *i.e.* $a \cdot b = 0$ where $a \neq 0, b \neq 0$

Now $a \cdot b = 0$

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

$\Rightarrow b = 0$, since restricted cancellation laws hold,

which is a contradiction to our assumption that $b \neq 0$.

Hence R is a ring without zero-divisors.

§ 2.6 DIVISION RING OR SKEW FIELD *(Purvanchal 97)*

A ring R is called a division ring or skew field if the set R^* of non-zero elements in R forms a multiplicative group.

Thus a division ring must have identity 1. since $1 \in R^*$, we have $1 \neq 0$.

Consequently a division ring must have at least two elements.

Example. The rings Q, R and C of rational numbers, real numbers and complex numbers respectively are commulative division rings.

This example is called the ring of real quaternions. This ring was first described by the Irish mathematician Hamilton. Initially it was extensively used in the study of mechanics; today its primary interest is that of an important example, although it still plays key roles in geometry and number theory.

Let Q be the set of all symbols $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, where all the numbers $\alpha_0, \alpha_1, \alpha_2$, and α_3 are real numbers. We define two such symbols, $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ and $\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$, to be equal if and only if $\alpha_i = \beta_i$ for $i = 0, 1, 2, 3$. In order to make Q into a ring we must define operations + and $\cdot$ for its elements as

1. For any $X = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, and $Y = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$ in $Q, X + Y = (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) + (\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k) =$
$(\alpha_0 + \beta_0) + (\alpha_1 + \beta_1) i + (\alpha_2 + \beta_2) j + (\alpha_3 + \beta_3) k$

and

2. $X \cdot Y = (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) \cdot (\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k) =$
$(\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3) + (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2) i +$

$$(\alpha_0\beta_2 + \alpha_2\beta_0 + \alpha_3\beta_1 - \alpha_1\beta_3)j + (\alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1)k.$$

where

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

It can be remembered by $ij = k, jk = i, ki = j$; while going around counter-clockwise we get the negatives.

It may be prove that Q is a non-commutative ring in which $0 = 0+0i + 0j + 0k$ and $1 = 1 + 0i + 0j + 0k$ serve as the zero and unit elements respectively. Now if $X = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ is not 0, then not all of $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ are 0; since they are real. Therefore $\beta = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \neq 0$. Thus

$$Y = \frac{\alpha_0}{\beta} - \frac{\alpha_1}{\beta} i - \frac{\alpha_2}{\beta} j - \frac{\alpha_3}{\beta} k \in Q.$$

A simple computation now shows that $X \cdot Y = 1$. Thus the nonzero elements of Q form a non-abelian group under multiplication. A ring in which the nonzero elements form a group is called a division ring or skewfield.

3. It may be verified that $X \cdot Y \neq Y \cdot X$ thus the division ring is non commutative.

§ 2.7. INTEGRAL DOMAIN

(Gorakhpur 93, 2004; Poorvanchal 92, 93, 95, 2015)

A commutative ring with unit element having at least two elements, and no divisors of zero is called an integral domain.

From the above definition it is obvious that a ring is an integral domain if (i) It is commutative, (ii) it possesses an unit element, (iii) it has atleast two elements and (iv) it is without zero divisors.

The System $(D, +, .)$ is an integral domain if the following postulates are satisfied :

D_1 : The system $(D, +, .)$ is an abelian group, so we have the following properties :

(i) Closure property.

$$a \in D, b \in D \Rightarrow a + b \in D, \ \forall\ a, b \in D.$$

(ii) Associativity of addition.

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

(iii) Existence of zero (or additive identity)

$$a + 0 = a = 0 + a, \ \forall\ a \in D.$$

(iv) Existence of additive inverse (or negative)

$$a + (-a) = 0 = (-a) + a, \ \forall\ a \in D.$$

(v) Commutativity of addition.

$$a + b = b + a, \ \forall\ \ a, b \in D.$$

D_2 : The system $(D, .)$ is an abelian semi-group with unity, so we have the following properties :

(i) Closure property.

$$a \in D, b \in D \Rightarrow a . b \in D \ \ \forall\ a, b \in D$$

(ii) Associativity of multiplication.

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

(iii) Existence of unity.

$$a \,.\, 1 = 1 \,.\, a = a,\ \forall\ a \in D.$$

(iv) Commutativity of multiplication.

$$a \,.\, b = b \,.\, a,\ \forall\ a, b \in D.$$

D_3 : Multiplication composition is right and left distributive with respect to addition :

$a \,.\, (b + c) = a \,.\, b + a \,.\, c$ and $(b + c) \,.\, a = b \,.\, a + c \,.\, a,\ \forall\ a, b, c \in D.$

D_4 : If the product of two elements is zero, then one of them at least is zero.

i.e. $a \,.\, b = 0 \Rightarrow a = 0$ or $b = 0$, $\forall\ a, b \in D$

i.e. product of non-zero element is non-zero

Theorem : A finite integral domain is a division ring.

(Gorakhpur 97)

Proof : Let D be a finite integral domain. Then D is a ring without zero divisors. Let D^* be the set of non zero elements of D, *i.e.* $D^* \subset D$, then cancellation law for multiplication holds in D^*. Therefore D^* is a finite semigroup with respect to multiplication in which concellation laws hold. Hence D^* forms a group w.r.t. multiplication and therefore D is a division ring.

Example 1. Prove that the ring of integers is an integral domain.

Solution . It can easily be proved that the set of integers is a commutative ring with unit elements.

Also this ring does not possess zero divisiors because if a, b are any two integers (*i.e.* elementrs of this ring) such that $a \,.\, b = 0$ then either a or b or both must be zero.

The number of elements of the set of integers is more than two

Hence according to the definition of integral domain the ring of integers is an integral domain.

Example 2. Show that the set E of even integers is not an integral domain with respect to addition and multiplication.

Solution. We can easily prove that the set E of even integers is a commutative ring with respect to ordinary addition and multiplication but with no unit element (*i.e.* unity).

Also this ring $(E, +, .)$ does not possess zero divisors because if a, b are any two even integers (*i.e.* elements of E) such that $a \,.\, b = 0$, then either a or b or both must be zero.

Hence according to the definition of integral domain the ring $(E, +, .)$ is not an integral domain.

Example 3. Prove that the ring of complex numbers C is an integral domain.

Solution. Let $C = \{a + bi : a, b \in R\}$.

It is easy to prove that C is a commutative ring with unity.

The zero element $0 + 0 \,.\, i$ and unit element $1 + 0 \,.\, i$

§ 2.8. FIELD (Gorakhpur 2015)

Definition I. If every element $a \neq 0$ of an integral domain has a multiplicative inverse a^{-1} in the integral domain, then it (the integral domain) is called a *field* and is generally denoted by F.

Definition II. A ring F whose non-zero elements form an abelain, multiplicative group is known as a *field*.

Definition III. A system $(F, +, .)$ having atleast two elements (*i.e.* the additive and multiplicative identities) is called a field F, if

$\mathbf{F_1}$: the system is an abelian group with respect to addition.

$\mathbf{F_2}$: the distributive laws are satisfied,

and $\mathbf{F_3}$: the subset of non-zero elements of F is an abelian multiplicative group.

A field is generally written as $(F, +, .)$ or simply as F.

Postulates for Field :

The system $(F, +, .)$ is a field if the following postulates are satisfied

$\mathbf{F_1}$: The system $(F, +)$ is an abelian group, so we have the following properties:

(i) Closure property.

$$a \in F, b \in F \Rightarrow a + b \in F, \ \forall\ a, b \in F.$$

(ii) Associativity of addition.

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

(iii) Existence of additive identity.

$$a + 0 = a = 0 + a, \ \forall\ a \in F$$

(iv) Existence of additive inverse :

$$a + (-a) = 0 = (-a) + a, \ \forall\ a \in F$$

(v) Commutativity of addition.

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

$\mathbf{F_2}$: Multiplication composition is left and right distributive with respect to addition :

$a \,.\, (b + c) = a \,.\, b + a \,.\, c$ and $(b + c) \,.\, a = b \,.\, a + c \,.\, a, \ \forall\ \ a, b.c \in F$

$\mathbf{F_3}$: The subset of non-zero elements of F forms an abelian multiplicative group and so we have the following properties :

(i) Closure property.

$$a \in F, b \in F \Rightarrow a \,.\, b \in F \ \ \forall\ a, b, \in F$$

(ii) Associativity of multiplication.

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

(iii) Existence of multiplicative identity.

$$a \,.\, 1 = a = 1 + a, \ \forall\ a \in F$$

(iv) Existence of multiplicative inverse :

$$a \,.\, a^{-1} = 1 = a^{-1} \,.\, a, \ \forall\ a \in F, a \neq 0$$

(v) Commutativity of multiplication.

$$a \,.\, b = b \,.\, a, \ \forall\ a, b \in F$$

Definition IV : A commutative division ring is called a field.

Examples of Field. The rings of real numbers, rational numbers and complex numbers are fields as each one of them is a commutative ring with unity and each non-zero element of each of the above rings possesses multiplicative inverse.

COMPARISON OF RING, INTEGRAL DOMAIN AND FIELD

S.No.	Ring $(R, +, .)$	Integral Domain $(D, +, .)$	Field $(F, +, .)$
(i)	$(R, +)$ is an abelian group	$(D, +)$ is an abelian group	$(F, +)$ is an abelian group
(ii)	(.) is associative	(.) is associative	(.) is associative
(iii)	Distributive laws are satisfied	Distributive laws are satisfied	Distributive laws are satisfied
(iv)	.....	(.) is commutative	(.) is commutative
(v)	.....	Unity belongs to D	Unit belongs to F
(vi)	.....	.....	Multiplicative inverse of each non-zero element of F exists and belongs F
(vii)	may or may not possess proper zero divisors	does not posses proper zero divisors	does not possess proper zero divisors.

From the above table, it is clear that the only difference between an integral domain and field is that every non-zero element of a field possesses a multiplicative inverse whereas in an integral domain it is not so.

An important property of a field F.

If $a, b \in F$,. then

$$a + b \in F, a - b \in F, a \,.\, b \in F, \quad ab^{-1} \in F \text{ for } b \neq 0$$

§2.9. THEOREMS ON FIELD AND INTEGRAL DOMAIN

Theorem 1. *Every field is an integral domain.*

(Gorakhpur 94, 2010; Poorvanchal 92, 94, 96;)

Proof. Here we have to show only that a field F has no zero divisor as it is a commutative ring with unity.

Let a, b be the elements of the field F with $a \neq 0$ such that

$$ab = 0$$

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

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

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

$$\Rightarrow eb = 0, \qquad \because a^{-1}a = e$$

(e multiplicative identity)

$$\because eb = b$$

i.e. $a \neq 0, ab = 0 \Rightarrow b = 0$

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

$\therefore$ A field has no zero divisors and hence every field is an integral domain.

Theorem 2. *Every integral domain is not necessarily a field.*

(Gorakhpur 94; Purvanchal 92, 94, 96)

For example the ring of integers *i.e.* (**I**, +, .) is an integral domain but is not a field as the only inversible elements of the ring of integers are 1 and -1. The other non-zero elements of **I** do not possess the multiplicative inverse.

Theorem 3. *A* **finite** *integral domain (or a finite commutative ring without zero divisors) is a field.* ***(Gorakhpur 91, 95, 2016; Purvanchal 92, 93)***

Proof. Let a finite integral domain consisting of the n elements $a_1, a_2, a_3, ..., a_n$ be denoted by D.

As D is an integral domain so it is a commutative ring with unity element.

Let a be any non-zero element of D.

Consider the set $D' = \{ax : x \in D \text{ and } x \neq 0\}$

For this we have $ax = ay \Rightarrow x = y$, since the cancellation law holds in D'. $x \neq 0$ so the number of elements of D' is $n - 1$. Also unity element 1 is an element of D'.

Hence to each non-zero element a of D there exists a non-zero element x of D' such that $ax = 1$.

i.e. each non-zero element of D has multiplicative inverse. Also D has no divisors. Hence the theorem.

§ 2.10. CHARACTERISTIC OF A RING

(Gorakhpur 2005, 07, 11)

Let $(R, +, .)$ be a ring with 0 as its zero elements. If there exists a positive integer n such that

$$na = a + a + a + \ldots \text{ to } n \text{ terms} = 0 \ \forall \ a \in R$$

then such smallest positive integer n is called the characterisitc of the ring $(R, +, .)$

If no such positive integer n exists, then the ring $(R, +, .)$ is said to be of characteristic zero or infinite.

Example : *The rings of integers, of rational numbers, of real numbers are of characteristic zero as there exists no positive integer n for which* $n \, . \, a = 0$, $\forall \ a \in$ *the set of integers or of rational numbers or real numbers.*

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

Proof. Since e is the unity element of the ring R (say).

so $o(e) = o \Rightarrow$ characteristic of ring R is 0

Let $o(e) = n = a$ finite number so that n is the least positive integer such that $ne = 0$.

Also as $ea = a = ae \ \forall \ a \in R$

$\therefore$ $na = n(ea)$

$= (ne)\, a = 0 \, . \, a, \ ne = 0$

$= 0$

$\therefore$ n is the leat positive integer such that $na = 0$

i.e. characteristic of the ring R is n, by definition.

Example 1. *Find the characteristic of the ring* $(I_4, +_4, \cdot_4)$ *of integers modulo 4.*

Solution. Here we have $\mathbf{I_4} = \{0, 1, 2, 3\}$ and we get

$0 +_4 0 +_4 0 +_4 0 = 0$

$1 +_4 1 +_4 1 +_4 1 = 4 = 0 \pmod 4$

$2 +_4 2 +_4 2 +_4 2 = 8 = 0 \pmod 4$

$3 +_4 3 +_4 3 +_4 3 = 12 = 0 \pmod 4$

i.e. $4a = 0, \ \forall \ a \in \mathbf{I_4}$

Hence the given ring has characteristic 4.

§ 2.11. CHARACTERISTIC OF AN INTEGRAL DOMAIN

Let e be the unity element of $(\cdot)$ of the integral domain $(D, +, .)$

Let $\lambda e = e + e + e + \ldots$ to λ terms.

For the additive cyclic group generated by the unity element e interpreting the above relations additively, we have

(i) $pe + qe = (p + q)\, e$, where p and q are integers.

(ii) $0 \,.\, e = 0$

(iii) $q\,(pe) = p\,(qe) = (pq)\, e$

(iv) $(-\lambda)\, e = \lambda\,(-e)$

The cyclic group generated by e, the unity element of D, is isomorphic to the additive group of integers. Also it is isomorphic to the additive group of residue classes modulo m, where m can be proved to be prime. Hence the order n of the cyclic group generated by the unity element e of an integral domain $(D, +, .)$ is called the characteristic of the integral domain.

Theorem 1. *If $(D, +, .)$ is a finite integral domain, then $(D, +)$ is a finite abelian group.*

We know that characteristic of $(D, +, .)$ is the order of the unity element e of the group $(D, +)$.

$\therefore$ $(D, +)$ is a finite group $\Rightarrow o\,(e)$ is finite.

$\Rightarrow$ characteristic of D is finite.

Theorem 2. *The characteristic of an integral domain $(D, +, .)$ is either 0 or a prime number.* ***(Gorakhpur 2010, 13)***

Proof. The charateristic of D is either 0 or $n > 0$

If the characteristic of D is 0, then the theorem is proved partially.

If the characteristic of D is $n > 0$, then we are to prove that n is a prime number.

Let n be a composite integer *i.e.* not prime. Then we can write $n = n_1 n_2$, where $1 < n_1, n_2 < n$

Now characteristic of D is n

$\Rightarrow o(e) = n$, where e is the unity element of $(D, +, .)$

$\Rightarrow ne = 0$

$\Rightarrow n_1 n_2 e = 0 \because n = n_1 n_2$

$\Rightarrow n_1 (n_2 e) = 0$

$\Rightarrow (n_1 e)(n_2 e) = 0$

$\Rightarrow n_1 e = 0$ or $n_2 e = 0$ as D has no zero divisors

$\Rightarrow$ characteristic of D is either n_1 or n_2.

which is a contradiction that characteristic of D is n.

Hence n is not composite.

$\therefore n$ is prime.

Theorem 3. *The characteristic of an integral domain $(D, +, .)$ is 0 or $n > 0$ according as the order of any non-zero element regarded as a member of the group $(D, +)$ is either 0 or n.* ***(Gorakhpur 2005)***

Proof. Let a be a non-zero element regarded as a member of $(D, +)$

If $o(a) = 0$, then the charactyeristic of D is also zero.

If $o(a) = n$ (which is finite), then $na = 0$.

Let b be another non-zero element of D, then

$$na = 0 \Rightarrow (n a) . b = 0 . b$$
$$\Rightarrow (a + a + a + \ldots n \text{ times}) . b = 0$$
$$\Rightarrow a . (b + b + b + \ldots . n \text{ times}) = 0$$
$$\Rightarrow a . (n b) = 0$$

Since $(D, +, .)$ is an integral domain so it is without zero divisors and $a \neq 0$ then $a . (nb) = 0 \Rightarrow nb = 0$

But as $o(a) = n$, so n is the least positive integer such that $na = 0$

Hence n is the least positive integer such that $nk = 0, \forall k \in D$ and therefore the characteristic of $(D, +, .)$ is n

Theorem 4. Each non-zero element of an integral domain $(D, +, .)$, regarded as an element of a group $(D, +)$ is of the same order.

Proof. Let a, b be any arbitary non-zero element of the integral domain $(D, +, .)$ such that $a \neq b$.

Let $o(a) = n$ and $o(b) = m$, where a, b are regarded as elements of $(D, +)$ so that $na = 0, mb = 0$

Now $o(a) = n \Rightarrow na = 0$

$\Rightarrow nb = 0$, as in theorem 3 above

$\Rightarrow o(b) \leq n$

$\Rightarrow m \leq n$, since $o(b) = m$

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

$\Rightarrow a \,.\, (mb) = a \,.\, 0$

$\Rightarrow a \,.\, (b + b + b + \ldots m \text{ times}) = 0$

$\Rightarrow (a \,.\, b + a \,.\, b + a \,.\, b + \ldots m \text{ times}) = 0$

$\Rightarrow (a + a + a + \ldots m \text{ times}) \,.\, b = 0$

$\Rightarrow (ma) \,.\, b = 0$

$\Rightarrow ma = 0, \qquad \because b \neq 0$

$\Rightarrow o(a) \leq m$

$\Rightarrow n \leq m, \qquad \because o(a) = n$

Thus we have $m \leq n$ and $n \leq m$.

So $m = n$ *i.e.* $o(b) = o(a)$

Hence any two non-zero elements of the integral domain $(D, +, .)$ have the same order when these are regarded as members of the additive group $(D, +)$.

Also if $o(a) = 0$ and we suppose that $o(b) = m$ (which is finite), then we have $o(b) = m \Rightarrow o(a) = m \Rightarrow m = 0$ as proved above.

So $o(b)$ is also zero.

Theorem 5. In an integral domain $(D, +, .)$, all non-zero elements generate additive cyclic groups of the same order which is equal to the characteristic of the integral domain.

Proof. Let e be the unity element and a be any non-zero element of the integral domain $(D, +, .)$.

Case I. If the characteristic of the integral domain $(D, +, .)$ is zero.

Then if m be the order of the cyclic group we have

$me \neq 0$ if $m \neq 0$

Now $ma = m(e \,.\, a) = (me) \,.\, a \neq 0$, if $m \neq 0, a \neq 0$

So $ma = 0$ only if $m = 0$

$\therefore$ The additive cyclic group generated by any non-zero element a is of order zero.

Case II. If the characteristic of the integral domain $(D, +, .)$ is a prime number p (say), then

$pa = p(a \,.\, e) = p(e \,.\, a) \qquad \because a \,.\, e = a = e \,.\, a$

$= (pe) \,.\, a = 0 \,.\, a = 0$

Also $ma = m(a \,.\, e) = m(e \,.\, a) = (me) \,.\, a$

$\therefore$ $ma = 0 \Rightarrow me = 0$

i.e. $ma = 0 \Rightarrow m = \lambda p$, where $a \neq 0, m \neq 0$

$\therefore$ p is the least integer m such that $ma = 0$

$\therefore$ The additive cyclic group generated by any non-zero element a is of order p.

§ 2.12. Characteristic of a field.

Definition. Let $(F, +, .)$ be a field and let e be the unity of this field. Then by the definition of a field we know that $(F, +)$ is an abelian group.

If the order of e [considered as a member of the abelian group $(F, +)$] is zero, then the **characteristic of the field** is zero.

Again, if the order of e is finite, say p then the **characteristic of the field** F is p.

Fields with non-zero characteristic are called **Modular Fields.**

Example (i) Consider the field $(R, +, .)$ of real numbers. The unity of this field is 1. The order of 1 [considered as a member of $(R, +)$] is zero. Therefore the charateristic of the field $(R, +, .)$ is zero.

Example (ii) The characteristic of the field $(I_5, +_5, \cdot_5)$ of integers modulo 5 is 5. ***(Gorakhpur 92)***