# UNIT 10 : FACTORS RING AND RING HOMOMORPHISM

## UNIT STRUCTURE


10.1 Learning Objectives

10.2 Introduction

10.3 Factor Rings : Definition and Examples

10.4 Properties of Factor Rings

10.5 Homomorphism of Rings : Definition and Examples

10.6 Types of Ring Homomorphism

10.7 Properties of Ring Homomorphism

10.8 Let Us Sum Up

10.9 Further Readings

10.10 Answers To Check Your Progress

10.11 Model Questions


## 10.1 LEARNING OBJECTIVES

After going through this unit, you will able to know -

- the concept of factor rings and ring homomorphism
- different types of ring homomorphism
- the concept of ring isomorphism
- fundamental theorem of ring homomorphism
- properties of factor rings and ring homomorphism
- isomorphism theorem of ring.

## 10.2 INTRODUCTION

By definition, a ring R is an additive abelian group and an ideal I of R is necessarily additive subgroup of R. We can talk of the additive quotient group $R/I = \{r+1 : r \in R\}$ of R. We would like to make $R/I$ a ring. Normal subgroups provided us with factor groups, ideal do the job in ring.

In other work with groups, we say that one way to discover information about a group is to examine its interaction with other groups by way of

homomorphisms. It should not be susprisiong to learn that this concept extends to rings with equally profitable results.

Just as a group homomorphism preserves the group operation, a ring homomorphism preserves the ring operations.

## 10.3 FACTOR RING

Let R be a ring and I, an ideal of R. Since a, b $\in$ I $\Rightarrow$ a – b $\in$ I, we find I is a subgroup of R. Again as R is abelian, I will be a normal subgroup of R and thus we can talk of $R/I$, the factor group or quotient group.

$R/I$ = {r+I : r $\in$ R}

= set of all cosets of I in R.

(1) We know $R/I$ forms a abelian group under 'addition' defined by

(r+I) + (s+I) = (r+s) + I

(2) We now define a binary composition on $R/I$ by (r+I) (s+I) = rs+I

We verify that multiplication is well-defined : for this purpose let.

r+I = r′+I and s+I = s′+I for some r, r′, s, s′ $\in$ I

This implies r – r′ $\in$ I and s – s′ $\in$ I

$\Rightarrow$ r–r′ = p and s–s′ = q for some p, q $\in$ I

$\Rightarrow$ r = p+r′ and s = q+s′

$\Rightarrow$ rs = (p+r′)(q+s′)

= pq+ps′+r′q+r′s′

$\Rightarrow$ rs–r′s′ = pq+ps′+r′q

As p, q $\in$ I and I is an ideal of R, pq + ps′ + r′q $\in$ I

Consequently, rs – r′s′ $\in$ I

$\Rightarrow$ rs + I = r′s′ + I

$\Rightarrow$ (r+I) (s+I) = (r′+I) (s′+I)

This shows that multiplication in $R/I$ is well-defined.

Let r+I, s+I, t+I $\in$ $R/I$ where r, s, t $\in$ R.

Multiplication is associative :

(r+I) [(s+I) (t+I)] = (r+I) (st+I)

= (r(st)+I

= (rs)t + I, since r(st) = (rs)t in R.

= (rs + I) (t+I)

= [(r+I) (s+I)] (t+I)

Distributive Laws

(r+I) [(s+I) + (t+I)] = (r+I) [(s+t) +I]

= r(s+t) + I

= (rs+rt) + I

= (rs+I) + (rt + I)

= (r+I) (s+I) + (r+I) (t+I)

Similarly, we can prove that

[(s+I)+(t+I)] (r+I) = (s+I) (r+I) + (t+I) (r+I)

Hence $R/I$ is a ring

**Definition:** Let R be a ring and I be any ideal of R. Then

$R/I$ = {r+I : r ∈ I} is a ring under binary compositions defined by

(r+I) + (s+I) = (r+s) + I

(r+I) (s+I) = rs+I for all r+I, s+I ∈ $R/I$.

This ring is called factor ring or quotient ring of R with respect to the ideal of I.

Remarks : (i) 0+I = I is the zero element of $R/I$.

(ii) If I = R, then $R/I$ is isomorphic to the zero rings {0} and if I ={0}, then $R/I \cong R$.

**Example 1.** Let 4Z {4m : n ∈ z}, where Z is the ring of integers. Then 4H is an ideal of Z and thus $Z/4z$ = {4z, 1+4z, 2+4z, 3+4z} is a factor ring of Z.

This example also shows us that factor ring of an integral domain may not be an integral domain.

Notice (2+4z) (2+4z) = 4 + 4z

= 4z

= zero of $Z/4z$.

but 2 + 4z $\neq$ 4z.

**Example 2.** Let $\mathrm{R} = \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} : a_1, a_2, a_3, a_4 \in Z \right\}$

and $\mathrm{I} = \left\{ \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix} : e_1, e_2, e_3, e_4 \text{ are even integers} \right\}$

It is easy to show that I is a ideal of R.

Then $\mathrm{R}/\mathrm{I}$ is a factor ring of R an it contains 16 element; in fact,

$$\mathrm{R}/I = \left\{ \begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix} + I : r_i \in \{0, 1\} \right\}$$

Let $\begin{bmatrix} 7 & 8 \\ 5 & -3 \end{bmatrix} + \mathrm{I} \in \mathrm{R}/I$. Then we can write

$$\begin{bmatrix} 7 & 8 \\ 5 & -3 \end{bmatrix} + \mathrm{I} = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} + \mathrm{I} \right\} + \left\{ \begin{bmatrix} 6 & 8 \\ 4 & -4 \end{bmatrix} + \mathrm{I} \right\}$$

$$= \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} + \mathrm{I} \right\} + \mathrm{I}, \text{ since } \begin{bmatrix} 6 & 8 \\ 4 & -4 \end{bmatrix} \in \mathrm{I}$$

$$= \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} + \mathrm{I}$$

**Example 3.** Consider the Gaussian ring Z [i] = {a+ib : a, b ∈ Z} where Z is the set of integer. Since $\langle 2–i \rangle$ is an ideal of Z [i], therefore.

$\mathrm{F} = \mathrm{Z}[\mathrm{i}]/\langle 2 - \mathrm{i} \rangle$ is a factor ring of Z [i]

Of course the elements of F have the form

a+ib + $\langle 2–i \rangle$, where a, b ∈ Z.

We have 2– i + $\langle 2–i \rangle$ = $\langle 2–i \rangle$ since 2–i ∈ $\langle 2–i \rangle$

= 0 + $\langle 2–i \rangle$

When dealing with coset representatives, we may treat 2–i as equivalent to zero, so that 2 = i.

For example, 3+4i + $\langle 2–i \rangle$ = 3+4.2 + $\langle 2–i \rangle$

= 11 + $\langle 2–i \rangle$

Similarly, all the elements of F can be written in the form

a+ $\langle 2–i \rangle$ where a ∈ Z

But we can further reduce the set of distinct coset representatives by observing that when dealing with coset representatives,

$2 = i$

$\Rightarrow 2^2 = i^2$ (by sequaring both sides)

$\Rightarrow 4 = -1$

$\Rightarrow 5 = 0$

In this case

$$3+4i + \langle 2-i \rangle = 11+\langle 2-i \rangle$$
$$= 1+5+5+\langle 2-i \rangle$$
$$= 1+\langle 2-i \rangle$$

In this way, we can show that every element of F is equal to one of the following coset :

$0+\langle 2-i \rangle$ , $1+\langle 2-i \rangle$ , $2+\langle 2-i \rangle$ , $3+\langle 2-i \rangle$ , $4+\langle 2-i \rangle$ .

To show these 5 cosets are distinct, it is suffices to show that $1+\langle 2-i \rangle$ has additive order 5. We have

$$5(1+\langle 2-i \rangle) = 5+\langle 2-i \rangle$$
$$= 0+\langle 2-i \rangle$$

$\therefore$ $1+\langle 2-i \rangle$ has order 1 or 5.

If the order is actually 1, then

$$1+\langle 2-i \rangle = 0+\langle 2-i \rangle$$
$$= \langle 2-i \rangle$$

$\Rightarrow 1 \in \langle 2-i \rangle$

$\Rightarrow 1 = (2-i)(a+ib)$

$= (2a+b) + (-a+2b)i$, for some integers a and b.

$\Rightarrow 1 = 2a+b$ and $0 = -a+2b$

Solving, we get $b = \frac{1}{5} \notin Z$

Thus $1+\langle 2-i \rangle$ has order 5 and the ring F is essentially the same as the field $Z_5$.

**Definition:** (Prime ideal) Let R be a commutative ring. A proper ideal P of R is called a prime ideal if $a, b \in R$ and $ab \in P \Rightarrow a \in P$ or $b \in P$.

**Example 1.** In an integral domain D, $\langle 0 \rangle$ is a prime ideal because

$ab \in \langle 0 \rangle$ for $a, b \in D$

$\Rightarrow ab = 0$

$\Rightarrow a = 0$ or $b = 0$

$\Rightarrow a \in \langle 0 \rangle$ or $b \in \langle 0 \rangle$

**Example 2.** In Z, the ideal $\langle 3 \rangle = \{3n | n \in Z\}$ is prime, since $ab \in \langle 3 \rangle$

$\Rightarrow 3|ab$

$\Rightarrow 3|a$ or $3|b$

$\Rightarrow a \in \langle 3 \rangle$ or $b \langle 3 \rangle$

In fact every ideal $\langle p \rangle = \{pn | n \in Z\}$, where p is a prime number, is a prime ideal of Z.

**Definition:** (Maximal Ideal) : Let R be a commutative ring. A proper ideal M is called a maximal if for any ideal I of R such that $M \subseteq T \subseteq R$, then I = M or I = R.

**Example 1.** In a division ring D, $\langle 0 \rangle$ is a maximal ideal. Trivially $\langle 0 \rangle \neq D$ as $1 \in D$ and $1 \neq 0$.

Let I be any nonzero ideal of D. Then there exists $x (\neq 0)$ in I. Since D is a division ring, so $x^{-1} \in D$; which gives $1 = xx^{-1} \in I$. Consequently I = D. Hence $\langle 0 \rangle$ is a maximal ideal of D.

**Example 2.** In the ring E of even integers, the ideal $\langle 4 \rangle$ is maximal. As $2 \notin \langle 4 \rangle$, $\langle 4 \rangle \neq E$. Further let I be an ideal of E such that $\langle 4 \rangle \subseteq I \subseteq E$. Then there exists an element $x \in I$ such that $x \notin \langle 4 \rangle$. In other words x is an even integer not divisible by 4. Consequently.

$x = 4n + 2$ for some integer n

$\Rightarrow 2 = x - 4n \in I$ as $4n \in \langle 4 \rangle \subset I$ and $x \in I$.

Thus every even integral multiple of 2 is in I, and E = I. Hence $\langle 4 \rangle$ is a maximal ideal of E.

**Example 3.** The lattice of ideals of $Z_{36}$ (Figure 10.1) shows that only $\langle 2 \rangle$ and $\langle 3 \rangle$ are maximal ideals.

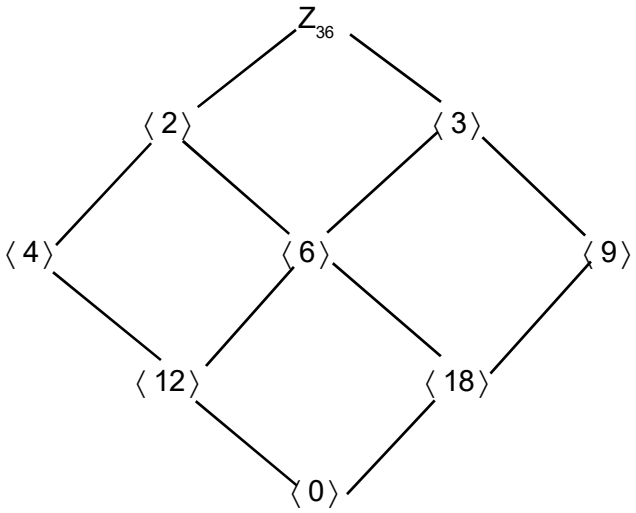



Figure 10.1



**CHECK YOUR PROGRESS**

**Q 1:** Show that $2Z/6Z$ is a factor ring of 2Z. How many elements are in $2Z/6Z$?

**Q 2:** Show that $Z/6Z$ is a factor ring of z.

**Q 3:** Let R [x] denote the ring of polynomial with real co-efficients and let $\langle x^2+1 \rangle$ denote the principal ideal generated by $x^2+1$. Write the factor ring $R[x]/\langle x^2+1 \rangle$.

**Q 4:** Show that 4Z is not a prime ideal of F, the ring of even integers.

**Q 5:** Show that $\langle x^2+1 \rangle$ is not a prime ideal of $Z_2[x]$.

**Q 6:** Show that $\langle x^2+1 \rangle$ is a maximal ideal of R[x].

## 10.4 PROPERTIES OF FACTOR RINGS

**Theorem 10.4.1** Let R be a commutatine ring. An ideal P of R is prime if and only if $R/P$ is an integral domain.

Proof : Let P be a prime ideal of the commutative ring R. We have to prove $R/P$ is an integral domain.

Let $a+P, b+P \in R/P$ such that

$(a+P)(b+P) = 0+P$

$\Rightarrow ab+P = P$

$\Rightarrow ab \in P$

$\Rightarrow a \in P$ or $b \in P$ since P is prime.

$\Rightarrow a+P = P$ or $b+P = P$

$\Rightarrow a+P = 0+P$ or $b+P = 0+P$

This shows that $R/P$ is an integral domain. Conversely, let $R/P$ be an integral domain. We have to prove P is a prime ideal of R.

Let $a, b \in R$ such that

$ab \in P$

$\Rightarrow ab+P = P$

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

$\Rightarrow a+P = P$ or $b+P = P$ Since $R/P$ is an integral domain.

$\Rightarrow a \in P$ or $b \in P$

This shows that P is a prime ideal of R.

**Theorem 10.4.2** Let R be a commutative ring with unity. An ideal M of R is maximal ideal of R if and only if $R/M$ is a field.

**Proof :** Let M be a maximal ideal of a commutative ring R with unity. We have to prove $R/M$ is a field.

Since R is a commutative ring unity, $R/M$ is also a commutative ring with unity. Thus all that we need prove is that non zero elements of $R/M$ have multiplicative inverse.

Let $x+M \in R/M$ be any non zero element.

Then $x+M \neq M$

$\Rightarrow x \notin M$

Let $xR = \{xr : r \in R\}$. It is easy to verify that x R is an ideal of R. Since sum of two ideal is an ideal, M+xR will be an ideal of R.

Again as $x = 0+x.1 \in M+xR$ and $x \notin M$, we get $M \subset M + xR \subseteq R$.

Since M is maximal ideal, so

$M+xR = R$

and then $1 \in R \Rightarrow 1 \in M + xR$

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

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

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

$= M+(xr+M)$ $(\because m \in M \Rightarrow m+M = M)$

$= (0+M) + (xr+M)$

$= (0+xr) + M$

$= xr + M$

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

$\therefore$ r+M is multiplicative inverse of x+M.

Hence $R/M$ is a field.

Conversely, Let $R/M$ be a field. We have to prove M is a maximal ideal of R.

Let I be an ideal of R such that $M \subset I \subseteq R$. Then there exists some $a \in I$ such that $a \notin M$.

Now $a \notin M$.

$\Rightarrow a+M \neq M$

$\Rightarrow$ a+M is a non zero element of $R/M$. Since $R/M$ is a field, therefore a+M has multiplicatine inverse. Let b+M be its inverse.

Then $(a+M)(b+M) = 1+M$

$\Rightarrow ab+M = 1+M$

$\Rightarrow ab-1 \in M$

$\Rightarrow ab-1 = m$ for some $m \in M$.

$\Rightarrow 1 = ab - m \in I$ [$\because a \in I, m \in M \subset I$

$\Rightarrow ab-m \in I$ as $b \in R$]

$\Rightarrow$ I = R (ideal cantaining unity, equal the ring)

Hence M is a maximal ideal of R.

**Remarks :**

(i) $R/M$ being a field contains at least two elements and thus unity and zero elements of $R/M$ are different i.e.

$0+M \neq 1+M$

$\Rightarrow 1 \notin M$

$\Rightarrow M \neq R$.

(ii) In the converse part of above theorem we do not require R to have unity or it to be commulative, i.e., if R is ring and M is an ideal of R such that $R/M$ is a field, then M is mazimal.

Suppose I is an ideal of R such that $M \subset I \subseteq R$. Then there exists $a \in I$

such that $a \notin M$.

Now $a \notin M \Rightarrow a+M \neq M$

$\Rightarrow$ a+M is a non zero element of $R/M$ since $R/M$ is a field, a+M has multiplicative inverse, say, b+M. If c+M is unity of $R/M$ (Note $R/M$ can have unity even if R doesn't have unity), then

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

$$\Rightarrow ab+M = c+M$$

$$\Rightarrow c-ab \in M \subset I$$

But $a \in I \Rightarrow ab \in I$ and so $(c-ab)+ab \in I$

$$\Rightarrow c \in I$$

Let $r \in R$ be any element.

Then (r+M)(c+M) = r+M as c+M is unity in $R/M$

$\Rightarrow$ rc+M = r+M

$\Rightarrow$ r– rc $\in$ M

Since $c \in I, rc \in I \Rightarrow (r-rc)+rc \in I$

$\Rightarrow r \in I$

$\therefore R \subseteq I$

Hence I = R and thus M is maximal ideal of R.

**Corollary 10.4.3** A commutative ring with unity is a field if and only if it has no proper (non tririal) ideals.

**Proof :** Let R be a field. Let A be any ideal of R such that $A \neq \{0\}$. Then there exists at least one $a \in A$ such that $a \neq 0$. Since in a field every non zero element has multiplicative inverse, therefore there exists $a^{-1} \in R$ such that $aa^{-1}=1$.

Now $a \in A, a^{-1} \in A \Rightarrow aa^{-1} \in A$

$\Rightarrow 1 \in A$

$\Rightarrow A = R$

i.e. only ideals that R can have are R and {0}.

i.e. R has no proper ideals.

Conversely, let R has no proper ideals. We have to prove R is a field.

Since R has no proper ideals, so {0} must be a maximal ideal and $R/\{0\}$ is a field.

As $R/\{0\} \cong R$, R is a field.

**Corollary 10.4.4.** If R is a commutative ring with unity, then every maximal ideal of R is prime.

**Proof :** An ideal M of R is maximal $\Leftrightarrow R/M$ is a field (theorem 10.4.2). Thus

M is maximal $\Rightarrow R/M$ is a field

$\Rightarrow R/M$ is an integral domain

$\Rightarrow$ M is prime (theorem 10.4.1)



**CHECK YOUR PROGRESS**

**Q 7:** Let R be a commutative ring. Show that an ideal P of R is a prime ideal if and only if for two ideals A and B of R, $AB \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$.

**Q 8:** Let R be a commutative ring with unity. If every ideal of R is prime, show that R is a field.

## 10.5 HOMOMORPHISM OF RINGS : DEFINITION AND EXAMPLES

**Definition 10.7.1** A ring homomorphism $\phi$ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations, i.e., for all $a, b \in R$

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

and $\phi(ab) = \phi(a)\phi(b)$

A ring homomorphism that is both one-one and onto is called a ring isomorphism.

**Example 1.** Let S be a subring of R. Define $f: S \to R$ by $f(x) = x$ for all $x \in S$

Let $x, y \in S$ then

$f(x+y) = x+y$

$= f(x) + f(y)$

and $f(xy) = xy$

= f(x) f(y)

Thus f is a ring homomorphismfrom S to R.

**Example 2.** Let I be an ideal of a ring R. Then $R/I$ is a factor ring.

Define f : $R \to R/I$ by f(x) = r+I for all $r \in R$.

Let r, $s \in R$

f(r+s) = (r+s) + I

= (r+I) (s+I)

= f(r) + f(s)

and f(rs) = rs+I

= (r+I) (s+I)

= f(r) + f(s)

Thus f is a ring homomorphism from R to $R/I$ .

**Example 3.** Let R be a ring and $M = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in R \right\}$. Then M is a ring under matrix addition and matrix multiplication.

Define f : $M \to R$ by

$$f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a \text{ for all } \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in M$$

Let $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in M$ . Then

$$f\left[\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}\right] = f\begin{pmatrix} a+b & 0 \\ 0 & 0 \end{pmatrix}$$

= a+b

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

and $$f\left[\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}\right] = f\begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$$

= ab

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

Thus f is a ring homomorphism from M to R.

**Example 4.** The set of complex numbers, C is a ring under addition and multiplication. Define $f : C \to C$ by

$$f(a+ib) = a - ib$$

Let $a+ib, c+id \in C$. Then

$$f[(a+ib) + (c+id)] = f[(a+c) + i(b+d)]$$
$$= (a+c)-i(b+d)$$
$$= (a-ib) + (c-id)$$
$$= f(a+ib) + f(c+id)$$

and $$f[(a+ib)(c+id)] = f[(ac-bd)+i(bc+ad)]$$
$$= (ac-bd) - i(bc+ad)$$
$$= ac-iad-ibc + i^2bd$$
$$= a(c-id) - ib(c-id)$$
$$= (a-ib)(c-id)$$
$$= f(a-ib)\, f(c+id)$$

Thus f is ring homomorphism from C to C.

**Example 5.** The set $Z_n = \{0, 1, 2, \ldots., n-1\}$ addition and multiplication modulo n is a commutative ring with unity 1 for all positive integer n. Define $\phi : Z_4 \to Z_{10}$ by $\phi(x) = 5x$

Let $x, y \in Z_4$ and $x+y = 4q_1+r_1$, $xy = 4q_2+r_2$

Where $0 \le r_1, r_2 < 4$. Then

$$\phi(x+y) = \phi(r_1)$$
$$= \phi(x+y-4q_1)$$
$$= 5(x+y-4q_1)$$
$$= 5x+5y-20q_1$$
$$= 5x + 5y$$
$$= \phi(x) + (y)$$

and $$\phi(xy) = \phi(r_2)$$
$$= \phi(xy-4q_2)$$
$$= 5(xy-4q_2)$$
$$= 5xy - 20q_2$$
$$= 5xy$$
$$= (5.\ 5)\, xy$$
$$= (5x)(5y)$$

$= \phi(x)\ \phi(y)$

Hence $\phi$ is a ring homomorphism from $Z_4$ to $Z_{10}$.

**Example 6.** Let R be a commutative ring of characteristic 2. Define $f : R \to R$ by $f(a) = a^2$

Since R is a ring of characteristic zero, so

$2x = 0$ for all $x \in R$.

Let $x, y \in R$. Then

$f(x+y) = (x+y)^2 a$

$= x^2 + 2xy + y^2$ [$\because$ R is commutative]

$= x^2+y^2$ [$\because xy \in R$]

$= f(x) + f(y)$

and $f(xy) = (xy)^2$

$= x^2y^2$ [$\because$ R is commutative]

$= f(x)\ f(y)$

$\therefore$ f is a ring homomorphism from R to R.



**CHECK YOUR PROGRESS**

**Q9:** Let $M = \{a+b\sqrt{2} : a, b \in Z\}$. Then M is a ring under addition and multiplication of real numbers. Define $f : M \to M$ by $f(a+b\sqrt{2}) = a-b\sqrt{2}$ for all $a+b\sqrt{2} \in M$. Examine if f is a ring homomorphism.

**Q10:** Let R be a commutating ring with characteristic p i.e. $px = 0$ for all $x \in R$, where $\phi$ is a prime number. Then show that the mapping $f : R \to R$ defined by $f(x) = x^p$ is a ring homomophism.

**Q11:** Show that the only ring homomorphisms from $Z \to Z$ are the identity and zero mappings.

**Q12:** Let R be a ring with unity 1. Then show that mapping $\phi : Z \to R$ defined by $\phi(n) = n.1$ is a ring homomorphism.

## 10.6 TYPES OF RING HOMOMORPHISM

(I) A ring homomorphism $f : R \to R'$ is called

(i) epimorphism if f is onto.

(ii) monomorphism if f is one-one

(iii) iso morphism if f is one-one and onto.

(II) A ring homomorphism f of a ring R into itself is called an endomorphism.

(III) An endomorphism is called an automorphism if it is an isomorphism.

**Example 1.** Let A be an ideal of a ring R. Then $R/A$ is factor ring of R. Define $f : R \to R/A$ by f(r) = r+A for all $r \in R$. From the definition of addition and multiplication of elements in $R/A$, f is a ring homomorphism.

Let $r+A \in R/A$. Then $r \in R$. Thus for each $r+A \in R/A$, $r \in R$ such that f(r) = r+A

Hence f is onto.

Let $a(\neq 0) \in A$. Then f(a) = a+A = A as $a \in A$.

Also f(0) = 0 + A = A.

$\therefore$ f(a) = f(0) but $a \neq 0$.

This proves that f is not one-one. Hence f is an epimorphism. This map is called Natural homomorphism.

**Example 2.** Let $M = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in R \right\}$ where R is a ring. Define $f : M \to R$ by

$f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a$ for all $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in M$.

Then f is a ring homomorphism.

Let $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in M$ such that

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

$$\Rightarrow a = b$$

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

This proves that f is one-one.

Let a be any element of R. Then $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in M$.

Thus for each $a \in R$, $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in M$ such that

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

This proves that f is onto.

Hence f is an isomorphism and $M \cong R$.

Note : If $f : R \to S$ is a ring isomorphism, then we write $R \cong S$.

## 10.7 PROPERTIES OF RING HOMOMORPHISM

**Theorem 10.9.1.** If $f : R \to S$ is a ring homomorphism,

then (i) $f(0) = 0'$

(ii) $f(-a) = -f(a)$ for all $a \in R$.

Where 0 and $0'$ are zero elements of the rings R and S respectively.

Proof : (i) We have $0 + 0 = 0$

$\Rightarrow f(0+0) = f(0)$

$\Rightarrow f(0) + f(0) = f(0)$ [$\because$ f is ring homomorphism]

$\Rightarrow f(0) + f(0) = f(0)+0'$ [$\because$ $0'$ is zero element of S)

$\Rightarrow f(0) = 0'$ [by left cancellation law]

(ii) We have $a+(-a) = 0$

$\Rightarrow f(a+(-a) = f(0)$

$\Rightarrow f(a) + f(-a) = 0'$ [$\because$ f is ring]

$\Rightarrow f(-a)$ is additive invase of $f(a)$

$\Rightarrow -f(a) = f(-a)$

$\Rightarrow f(-a) = -f(a)$

**Corollarly 10.9.2.** If $f : R \to S$ is a ring homomorphism,

then $f(a-b) = f(a) - f(b)$ for all $a, b \in R$.

Proof : $f(a-b) = f(a+(-b)$

$= f(a) + f(-b)$ [$\because$ f is a ring homomophism]

$= f(a) - f(b)$

**Definition:** Let $f : R \to S$ be a homomorphism.

Then kernal of f is denoted by kerf and define as $\text{kerf} = \{x \in R : f(x) = 0'$, where $0'$ is zero elements.

**Theorem 10.9.4.** If $f : R \to S$ is a homomorphism, then

(i) kerf is an ideal of R.

(ii) Kerf = {0} if and only if f is one-one

**Proof :** (i) As f(0) = 0, $0 \in$ kerf, so kerf $\neq \phi$.

Let x, y $\in$ kerf. Then f(x) = $0'$, f(y) = $0'$, where $0'$ is zero element of S.

Now f(x–y) = f(x) – f(y)

$= 0' - 0'$

$= 0'$

$\Rightarrow$ x–y $\in$ kerf.

Let r $\in$ R. Then f(rx) = f(r) f(x)

$= f(r) .0'$

$= 0'$

$\therefore$ rx $\in$ kerf.

Similarly, we can prove f(xr) = $0'$ which implies xr $\in$ kerf.

Hence kerf is an ideal of R.

(ii) Let f : R $\rightarrow$ S be a ring homomorphism such that kerf = {0}. We have to prove f is one-one.

Let x, y $\in$ R such that

f(x) = f(y)

$\Rightarrow$ f(x) – f(y) = $0'$

$\Rightarrow$ f(x–y) = $0'$ [$\because$ f is a ring homomorphism]

$\Rightarrow$ x–y $\in$ kerf = {0}

$\Rightarrow$ x–y = 0

$\Rightarrow$ x = y

Hence of is one-one

Conversely, let f : R $\rightarrow$ S be a one-one ring homomorphism. We have to prove kerf = {0}.

Let x $\in$ kerf. Then

$\Rightarrow$ f(x) = $0'$

$\Rightarrow$ f(x) = f(0) [$\because$ f(0) = $0'$, where 0 and $0'$ are zero element of R and S respectively]

$\Rightarrow$ x = 0 [$\because$ f is one-one]

$\therefore$ Kerf = {0}

**Theorem 10.9.5.** Let $\phi$ be a ring homomorphism from R to a ring S. Let A be a subring of R and let I be an ideal of S. Then

(i) For any $r \in R$ and any positive integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = [\phi(r)]^n$

(ii) $\phi(A) = \{\phi(a) : a \in A\}$ is a subring of S.

(iii) If A is an ideal and $\phi$ is onto, then $\phi(A)$ is an ideal.

(iv) $\phi^{-1}(I) = \{r \in R : \phi(r) \in I\}$ is an ideal of R.

(v) If R is commutative, then $\phi(R)$ is commutative.

(vi) If R has a unity 1, $S \neq \{0\}$ and $\phi$ is onto, then $\phi(I)$ is the unity of S.

**Proof :** Let $\phi : R \to S$ be a ring homomorphism, A, a subring of R and I, an ideal of S.

(i) Let $r \in R$ and n be an positive integer. Then

$$\phi(nr) = \phi(\underbrace{r+r+r+\ldots+r}_{n \text{ times}})$$

$$= \underbrace{\phi(r) + \phi(r) + \ldots + \phi(r)}_{n \text{ times}} \qquad [\because \phi \text{ is a ring homomorphism}]$$

$$= n\phi(r)$$

and $\phi(r^n) = \phi(\underbrace{r.r.r.\ldots.r}_{n \text{ times}})$

$$= \phi(r).\ \phi(r) \ldots \phi(r) \quad (n \text{ times})$$

$$= [\phi(r)]^n$$

(ii) As $0 \in A$ and $\phi(0) = 0' \in \phi(A)$, where 0 and $0'$ are zero elements of R and S respectively, $\because \phi(A) \neq \phi$.

Let $\phi(x), \phi(y) \in \phi(A)$. Then

$\phi(x) - \phi(y) = \phi(x-y)$ $[\because \phi$ is a ring homomorphism$]$

$\in \phi(A)$ $[\because x, y \in A \Rightarrow x-y \in A]$

and $\phi(x)\,\phi(y) = \phi(xy)$ $[\because \phi$ is a ring homomorphism$]$

$\in \phi(A)$ $[\because x, y \in A \Rightarrow xy \in A]$

$\therefore \phi(A) = \{\phi(x) : x \in A\}$ is a subring of S.

(iii) Let A be an ideal of R and $\phi : R \to S$ be a onto ring homomorphism.

We have to prove $\phi(A)$ is an ideal of S.

As $0 \in A$ and $\phi(0) = 0' \in \phi(A)$, $\phi(A) \neq \phi$

Let $x, y \in A$. Then $\phi(x), \phi(y) \in \phi(A)$ and

$\phi(x) - \phi(y) = \phi(x-y)$ $[\because \phi$ is a ring homomorphism$]$

$\in \phi(A)$ [$\because x, y \in A \Rightarrow x-y \in A$]

Let $s \in S$. Since $\phi: R \to S$ is onto, so there exists $r \in R$ such that $\phi(r) = s$.

$s\phi(x) = \phi(r)\ \phi(x)$

$= \phi(rx)$. [$\because \phi$ is a ring homomorphism]

$\in \phi(A)$ [As A is an ideal, $r \in R$, $r \in A \Rightarrow rx \in A$]

Similarly $\phi(x)s \in \phi(A)$.

Thus $\phi(A)$ is an ideal of S.

(iv) We have to prove $\phi^{-1}(I) = \{r \in R : \phi(r) \in I\}$ is an ideal of R, where I is an ideal of S.

Since $0' = \phi(0) \in I$, so $0 \in \phi^{-1}(I)$ and hence $\phi^{-1}(I) \neq \phi$.

Let $r_1, r_2 \in \phi^{-1}(I)$. Then $\phi(r_1), \phi(r_2) \in I$.

Since I is an ideal of S, so

$\phi(r_1) - \phi(r_2) \in I$

$\Rightarrow \phi(r_1 - r_2) \in I$ [$\because \phi$ is a ring homomorphism]

$\Rightarrow r_1 - r_2 \in \phi^{-1}(I)$

Let $r \in R$. Then $\phi(r) \in S$.

$\phi(rr_1) = \phi(r)\phi(r_1) \in I$ as I is an ideal of S.

Which implies that $rr_1 \in \phi^{-1}(I)$.

Similarly, $r_1 r \in \phi^{-1}(I)$

Hence $\phi^{-1}(I)$ is an ideal of R.

(v) Let R be a commutative ring. We have to prove $\phi(R)$ is also commutative ring.

As $0 \in R$ and $\phi(0) = 0' \in \phi(R)$, $\phi(R) \neq \phi$.

Let $\phi(x), \phi(y) \in \phi(R)$. Then $x, y \in R$. Since R is a commutative ring, therefore $xy = yx$.

Now $\phi(x)\phi(y) = \phi(xy)$ [$\because \phi$ is a ring homomorphism]

$= \phi(yx)$

$= \phi(y)\phi(x)$

This proves that $\phi(R)$ is commutative.

(vi) Let R has unity 1, $S \neq \{0\}$ and $\phi$ is onto. We have to prove $\phi(I)$ is unity in S.

Let $s \in S$. Since $\phi: R \to S$ is an onto ring homomorphism, therefore

these exist $r \in R$ such that $\phi(r) = S$.

Now $\phi(I)\, s = \phi(I)\, \phi(r)$

$= \phi(I.r)$

$= \phi(r)$

$= s$

Similarly, $s\phi(I) = s$

This proves that $\phi(I)$ is unity in S.

**Theorem 10.9.6.** (Fundamental Theorem of ring Homomorphism) If $f:R \to S$ be onto homomorphism then S is isomorphic to a quotient ring of R. In fact, $S \cong R/\text{Ker}\, f$

**Proof :** Let $f:R \to S$ be onto ring homomorphism.

Define $\phi : R/\text{Ker}\, f \to S$ by

$\phi(x+I) = f(x)$ for all $x \in R$, where $I = \ker f$.

Let $x+I, y+I \in R/\text{Ker}\, f$ such that

$x+I = y+I$

$\Rightarrow x-y \in I = \ker f$

$\Rightarrow f(x-y) = 0'$ where $0'$ is zero element of S.

$\Rightarrow f(x) - f(y) = 0'$

$\Rightarrow f(x) = f(y)$

$= \phi(x+I) = \phi(y+I)$

This shows that $\phi$ is well defined.

Let $r_1+I\ r_2+I \in R/\text{Ker}\, f$ : Then

$\phi[(r_1+I)+(r_2+I) = \phi[(r_1+r_2)+I]$

$= f(r_1+r_2)$

$= f(r_1) + f(r_2)$ [$\because$ f is a ring homomorphism]

$= \phi(r_1+I) + \phi(r_2+I)$

and $\phi[(r_1+I)+(r_2+I) = \phi[(r_1r_2)+I]$

$= f(r_1r_2)$

$= f(r_1)\,.\, f(r_2)$

$= \phi(r_1+I)\,\phi(r_2+I)$

$\therefore \phi$ is a ring homomorphism

Let $s \in S$. Since $f:R \to S$ is onto ring homomorphism, therefore there

exists $r \in R$ such that $f(r) = s$.

Since $r \in R$, so $r+I \in R/\text{Ker } f$ and

$\phi(r+I) = f(r) = s$.

We find $r+I$ in $R/\text{Ker } f$ as pre-image of s under $\phi$ showing there by that $\phi$ is onto.

Let $r_1+I, r_2+I \in R/\text{Ker } f$ such that

$\phi(r_1+I) = \phi(r_2+I)$

$\Rightarrow f(r_1) = f(r_2)$

$\Rightarrow f(r_1) - f(r_2) = 0'$

$\Rightarrow f(r_1 - r_2) = 0'$

$\Rightarrow r_1 - r_2 \in \ker f = I$

$\Rightarrow r_1+I = r_2+I$

This shows that $\phi$ is one-one and hance $\phi$ is an isomorphism.

Thus $R/\text{Ker } f \cong S$.

**Theorem 10.9.7.** (First Theorem of ring Isomorphism) :

Let A, B ($B \subseteq A$) be two ideals of a ring R. Then

$$R/A \cong \frac{R/B}{A/B}$$

**Proof :** Define $f : \frac{R}{B} \to \frac{R}{A}$ by

$f(r+B) = r+A$.

Let $r_1+B, r_2+B \in R/B$ such that

$r_1+B = r_2+B$

$\Rightarrow r_1 - r_2 \in B \subseteq A$

$\Rightarrow r_1 - r_2 \in A$

$\Rightarrow r_1+A = r_2 + A$

$\Rightarrow f(r_1+B) = f(r_2+B)$

This shows that f is well defined.

Again, let $r_1+B, r_2+B_1 \in R/B$

$f[(r_1+B)+(r_2+B)] = \phi[(r_1+r_2) + B]$

$= (r_1+r_2) + A$

$= (r_1+A)+(r_2+A)$

$= \phi(r_1+B) + \phi(r_2+A)$

and $f[(r_1+B)(r_2+B)] = \phi(r_1r_2+B)$

$= r_1r_2 + A$

$= (r_1+A)(r_2+A)$

$= \phi(r_1+B)\ \phi(r_2+A)$

This shows that f is ring homomorphism.

Let $r+A \in R/A$. Then $r \in R$ and $r+B \in R/B$.

Thus for each $r+A \in R/A$ there exists $r+B \in R/B$ such that f(r+B)= r+A.

Thus f is onto and hence f is a ring epimorphism. By fundamental theorem of ring homomorphism.

$$\frac{R/B}{\text{Ker } f} \cong R/A$$

and ker f = $\{r+B \in R/B : f(r+B) = A\}$

$= \{r+B \in R/B : r+A = A\}$

$= \{r+B \in R/B : r \in A\}$

$= A/B$ since $B \subseteq A \subseteq R$.

Thus $R/A \cong \dfrac{R/B}{A/B}$

**Theorem 10.9.8.** (Secong theorem of ring isomorphism) :

Let A, B be two ideals of a ring R. Then

$$A+B/B \cong \frac{B}{A \cap B}$$

**Proof :** Define $f : B \to \dfrac{A+B}{A}$ by

$f(b) = B + A$ for all $b \in B$

Let $b_1, b_2 \in B$ such that

$b_1 = b_2$

$\Rightarrow b_1+A = b_2+A$

$\Rightarrow f(b_1) = f(b_2)$

This show that f is well defined.

Again, let $b_1, b_2 \in B$. Then

$f(b_1+b_2) = (b_1+b_2)+A$

$= (b_1+A) + (b_2+A)$

$= f(b_1) + f(b_2)$

and $f(b_1b_2) = b_1b_2+A$

$= (b_1+A)(b_2+A)$

$= f(b_1)\, f(b_2)$

This shows that f is a ring homomorphism.

Let $x+A \in {}^{A+B}\!/_{A}$ be any element. Then

$x \in A+B$

$\Rightarrow$ $x = a+b$ for some $a \in A$, $b \in B$.

Now $x+A = (a+b) + A$

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

$= A+(b+A)$ [$\because$ $a+A = A$ as $a \in A$]

$= (0+A) + (b+A)$

$= (0+b) + A$

$= b + A$

$= f(b)$

i.e. be is the pre-image of x+A under f. Thus f is onto.

By fundamental theorem of ring homomorphism

${}^{A+B}\!/_{A} \cong {}^{B}\!/_{\text{Ker } f}$

and $\ker f = \{b \in B : f(b) = A\}$

$= \{b \in B : b+A = A\}$

$= \{b \in B : b \in A\}$

$= A \cap B$

Hence ${}^{A+B}\!/_{A} \cong {}^{B}\!/_{A \cap B}$



## CHECK YOUR PROGRESS

**Q13:** Show that $Z_n \cong {}^{Z}\!/_{\langle n \rangle}$.

**Q14:** If R is a ring with unity and the characteristic of R is n>0, then show that R contains a subring isomorphic to $Z_n$. If the characteristic of R is 0, then R contains a subring isomorphic to Z.



## 10.8 LET US SUM UP

- Let R be a ring and let I be a subring of R. The set $R/I$ = {r+I : r ∈ R} is a ring under the operations.

  (r+I) + (s+I) = (r+s) + I

  and (r+I) (s+I) = rs+I

  if and only if I is an ideal of R.
- A prime ideal P of a commutative ring R is a proper ideal of R such that a, b ∈ R and ab ∈ P imply a ∈ P or b ∈ P.
- A maximal ideal M of a commutative ring R is a proper ideal of R such that, whenever I is an ideal of R and M ⊆ I ⊆ R, than I=M or I=R.
- Let R be a commutative ring. An ideal P of R is prime if and only if $R/P$ is an integral domain.
- Let R be a commutative ring with unity. An ideal M of R is maximal ideal of R if and only if $R/M$ is a field.
- A ring homomorphism $\phi$ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations, i.e., for all a, b ∈ R.

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

  and $\phi(ab) = \phi(a)\phi(b)$
- A ring homomorphism f : R → S is called

  (i) epimorphism if f is onto.

  (ii) monomorphism if f is one-one.

  (iii) isomorphism if f is one-one and onto.
- If f : R → S is a ring homomorphism, then

  (i) f(0) = 0′

  (ii) f(–a) = –f(a)

  Where 0 and 0′ are the zero elements of the ring R an S respectively.
- If f : R → S is a ring homomorphism, then

  (i) Ker f is an ideal of R.

  (ii) Ker f = {0} if and only if f is one-one.
- Let $\phi$ be a ring homomorphism from a ring R to a ring S. Let A be a

subring of R and let I be an ideal of S. Then

(i) for any $r \in R$ and and any positive integer n,

$\phi(nr) = n\phi(r)$ and $\phi(r^n) = [(r)]^n$

(ii) $\phi(A) = \{\phi(a) : a \in A\}$ is a subring of S.

(iii) If A is an ideal of R and $\phi$ is onto, then $\phi(A)$ is an ideal of S.

(iv) $\phi^{-1}(I) = \{r \in R : \phi(r) \in I\}$ is an ideal of R.

(v) If R is commutative, then $\phi(R)$ is commutative.

(vi) If R has a unity 1, $S \neq \{0\}$ and $\phi$ is onto, then $\phi(I)$ is the unity of S.

- If $f : R \to S$ be onto homomorphism, then S is isomorphic to a quotient ring of R.
- Let A, B ($B \subseteq A$) be two ideals of a ring R. Then

$$R/A \cong \frac{R/B}{A/B}$$

- Let A and B be two ideals of a ring R. Then $(A+B)/A \cong B/(A \cap B)$



## 10.9 FURTHER READINGS

1) Gallian, Joseph A. : Contemporary Abstract algebra (8th Ed, Cengage Learning India Private Ltd, Delhi 110092.

2) Fraleigh, Johu B. : A first course in Abstract Algebra (2003), Pearson Education (singapure) Pvt. Ltd, India Branch, Delhi 110092.

3) Khanna, V. K. and Bhambri, S. K. : A course in Abstract Algebra (2002), Vikas Publishing House Pvt. Ltd, New delhi 110014.

4) Singh, S. and Zameeruddin, Q. : Modern Algebra (2002), Vikas Publishing House Pvt. Ltd, New Delhi 110014.



## 10.10 ANSWERS TO CHECK YOUR PROGRESS

**Ans to Q No 1:** We have $2Z = \{\ldots., -4, -2, 0, 2, 4, 6, 8, 10, 12, \ldots.\}$ and $6Z = \{\ldots., -12, -6, 0, 6, 12, \ldots.\}$

Since 2Z is a ring under addition and multiplication and 6Z is an ideal of 2Z, so $2Z/6Z$ is a factor ring and

$2z/6z$ = {0+6Z, Z+6Z, 4+6Z}

Here the operations are essentially modulo 6 arithmetic. For example

(4+6Z) + (4+6Z) = 8 + 6Z

= 2+(6+6Z)

= 2+6Z [$\because$ 6 $\in$ 6Z]

and (2+6Z) (4+6Z) = 2.4 + 6Z

= 8+6Z

= 2+(6+6Z)

= 2+6Z [$\because$ 6 $\in$ 6Z $\Rightarrow$ 6+6Z=6Z]

**Ans to Q No 2:** Since the set of integers Z is a ring under addition and multiplication and 6Z = { . . . . ., –12, –6, 0, 6, 12, . . . . .} is an ideal of Z, so $Z/6Z$ is a factor ring and

$Z/6Z$ = {0+6Z, I+6Z, 2+6Z, 3+6Z, 4+6Z, 5+6Z}

**Ans to Q No 3:** R[x] = the ring of polynomials with real coefficients and $\langle x^2+1 \rangle$ = the principal ideal gesscrated by $\langle x^2+1 \rangle$

= {f(x) $(x^2+1)$ : f(x) $\in$ R[x]}

Then $R[x]/\langle x^2+1\rangle$ is a factor ring and

$R[x]/\langle x^2+1\rangle$ = {g(x) + $\langle x^2+1 \rangle$ : g(x)$\in$R[x]}

Note that if g(x) is any member of R[x], then we write g(x) = q(x) $(x^2+1)$ +r(x), where q(x) is the quotient and r(x) is the remainder upon dividing g(x) by $x^2+1$. In particular, r(x) = 0 or deg (r(x)) < deg $(x^2+1)$.

or deg (r(x)) $\subset$ 2;

So that r(x) = ax+b for some a, b$\in$R.

Thus g(x)+$\langle x^2+1 \rangle$ = q(x) $(x^2+1)$ + r(x) + $\langle x^2+1 \rangle$

= r(x) + $\langle x^2+1 \rangle$

Since the ideal $\langle x^2+1 \rangle$ absorbs the term q(x) $(x^2+1)$

Hence $R[x]/\langle x^2+1\rangle$ = {ax+b+$\langle x^2+1 \rangle$ : a, b$\in$R}.

**Ans to Q No 4:** 4Z is an ideal of E, the ring of even integers. But it is not prime since, 2.2$\in$4Z but 2$\notin$4Z.

**Ans to Q No 5:** $\langle x^2+1 \rangle$ is an ideal of $Z_2[x]$. But it is not prime ideal of $Z_2[x]$, since $(x+1)^2 = x^2 + 2x + 1 = x^2+1 \in \langle x^2+i \rangle$ but $x+1 \notin \langle x^2+1 \rangle$.

**Ans to Q No 6:** Let A be an ideal of R[x] such that

$\langle x^2+1 \rangle \subset A \subseteq R[x]$.

We have to prove A = R[x] by showing that A contains some nor zero real number c.

Let $f(x) \in A$ such that $f(x) \notin \langle x^2+1 \rangle$. Then $f(x)=q(x)(x^2+1) + r(x)$

Where $r(x) \neq 0$ and deg (r(x)) < 2. It follows that r(x) = ax+b, where a, b are not both zero and $ax+b = r(x) = f(x) – q(x)(x^2+1) \in A$ since $f(x) \in A$ and $\langle x^2+1 \rangle \subset A$.

Thus $(ax+b)(ax–b) \in A$ and $a^2(x^2+1) \in A$

$\Rightarrow a^2x^2–b^2 \in A$ and $a^2x^2+a^2 \in A$

$\Rightarrow (a^2x^2+a^2) – (a^2x^2–b^2) \in A$

$\Rightarrow a^2+b^2 \in A$

Also $a^2+b^2 \neq 0$ as a and b are not both zero.

Thus $1 = (a^2 + b^2) \cdot \frac{1}{a^2 + b^2} \in A$

$\therefore$ A = R[x]

Hence $\langle x^2+1 \rangle$ is a maximal ideal of R[x].

**Ans to Q No 7:** Let P be a prime ideal of R and let $AB \subset P$ for two ideal A, B of R. We have to prove $A \subseteq P$ or $B \subseteq P$.

Suppose $A \not\subseteq P$. Then there exists some element $a \in A$ such that $a \notin P$.

Since $AB \subseteq P$, so $aB \subseteq P$

$\Rightarrow ab \in P$ for all $b \in B$.

Since P is prime, so $ab \in P \Rightarrow a \in P$ or $b \in P$. But $a \notin P$, hence $b \in P$ for all $b \in P$.

$\therefore B \subseteq P$

Similarly we can show if $B \not\subseteq P$, then $A \subseteq P$. Conversely

Let $AB \subseteq P$

$\Rightarrow A \subseteq P$ or $B \subseteq P$ for two ideals A and B of R. We have to prove P is prime. Let $ab \in P$ for a, $b \in R$.

Let A and B be the ideals generated by a and b. Then $A = \langle a \rangle$, $B = \langle b \rangle$. If $x \in AB$ is any element then it is of the type.

$x = a_1b_1+a_2b_2 + \ldots + a_nb_n$ where $a_i \in A$, $b_i \in B$.

$= (\alpha_1 a)(\beta_1 b) + (\alpha_2 a)(\beta_2 b) + \ldots + (\alpha_n a)(\beta_n b)$

for $\alpha_i\beta_i \in R$ as $a_i \in A = \langle a \rangle$ and $b_i \in B = \langle b \rangle$.

Thus $x = (\alpha_1 \beta_1)(ab) + (\alpha_2 \beta_2)(ab) + \ldots + (\alpha_n \beta_n) + (ab)$

$= (\alpha_1 \beta_1 + \alpha_2 \beta_2) + \ldots + \alpha_n \beta_n)(ab)$

Since $ab \in P$ and P is an ideal, so $x \in P$ and hence

$AB \subseteq P$

$\Rightarrow A \subseteq P$ or $B \subseteq P$

$\Rightarrow \langle a \rangle \subseteq P$ or $\langle b \rangle \subseteq P$

$\Rightarrow a \in P$ or $b \in P$

$\Rightarrow$ P is prime.

**Ans to Q No 8:** Let R be a commutative ring with unity and every ideal of R is prime. We have to show R is a field. We first show that R is an integral domain.

Let $ab \in R$ such that $ab = 0$

Then, $ab \in \{0\}$ which is an ideal of R and is, therefore, prime ideal.

Thus

$a \in \{0\}$ or $b \in \{0\}$

$\Rightarrow a = 0$ or $b = 0$

Thus R is an integral domain.

To show R is a field it is sufficient to show that every nonzero element of R has multiplicative inverse.

Let a be a nonzero element of R and let

$a^2R = \{a^2r | r \in R\}$.

Then $a^2R$ is an ideal of R and is therefore prime ideal.

Now $a.a = a^2 = a^2.1 \in a^2R$. $\Rightarrow a \in a^2R$

$\Rightarrow a = a^2b$ for some $b \in R$

$\Rightarrow a(1-ab) = 0$

$\Rightarrow 1-ab = 0$ as $a \neq 0$ and R is an integral domain

$\Rightarrow ab = 1$

Which shows that b is multiplicative inverse of a. Hence R is a field.

**Ans to Q No 9:** We have $M = \{a+b\sqrt{2} : a, b \in Z\}$ and M is a ring under usual addition and multiplication of real numbers.

Define $f : M \to M$ by $f(a+b\sqrt{2}) = a - b\sqrt{2}$ for all $a+b\sqrt{2} \in M$. We have

to examine f is a ring homomorphism.

Let $a+b\sqrt{2}$ , $c+d\sqrt{2} \in M$

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

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

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

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

and $f[(a+b\sqrt{2})(c+d\sqrt{2}) = f[(ac+2bd)+(ad+bc)\sqrt{2}]$

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

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

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

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

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

$\therefore$ f is ring homomorphism.

**Remark :** Since f is ring homomorphism of the ring M into itself, therefore f is an endomorphism on M. We can also show that f is one-one and onto. This f is an automorphism on M.

**Ans to Q No 10:** We have R is a commutative ring with characteristic p, i.e. px =0 for all $x \in R$, where p is a prime number.

Define $f : R \to R$ by $f(x) = x^p$. We have to show f is a ring homomorphism.

Let $x, y \in R$. Then

$f(x+y) = (x+y)^p$

$= x^p + {}^pC_1 x^{p-1} y + {}^pC_2 x^{p-2} y^2 + \ldots + y^p$

Since p is prime and characteristic of R is p, so

$p \mid {}^pC_1 \Rightarrow {}^pC_1 x^{p-1} y = 0$

$p \mid {}^pC_2 \Rightarrow {}^pC_2 x^{p-2} y^2 = 0$

$p \mid {}^pC_{p-2} \Rightarrow {}^pC_{p-2} x^2 y^{p-2} = 0$

$p \mid {}^pC_{p-1} \Rightarrow {}^pC_{p-1} x y^{p-1} = 0$

$\therefore f(x+y) = x^p + y^p$

$= f(x) + f(y)$

Also $f(xy) = (xy)^p$

$= y^p x^p$

$= x^p y^p$ [$\because$ R is commutative]

$= f(x).\ f(y)$

This f is a ring homomorphism.

**Ans to Q No 11:** Let $f : Z \to Z$ be a non zero ring homomorphism (i.e. $f(x) \neq 0$ for any $x \neq 0$).

Now $[f(1)]^2 = f(1)\ f(1)$

$= f(1.1)$ [$\because$ f is a ring homomorphism]

$= f(1) \neq 0$

= f(1) is idempotent in f(Z).

Since the only non zero idempotent in Z is 1, we find f(1) = 1. Now for any $x \in X$,

if x>0, $f(x) = f(1+1+. . .+1)$

x times

$= f(1) + f(1) + . . .+ f(1)$ [$\because$ f is a ring homomorphism]

$= xf(1)$

$= x.1$

$= x$

if x<0, then let $x = -y$

$f(x) = f(-y)$

$= -f(y)$

$= -\ f(1+1+1+ . . .+1)$

$= -\ [f(1) + f(1) + y \text{ times} + f(1)]$ [$\because$ f is a ring homomorphism]

$= -y\ f(1)$

$= y\ .\ 1$

$= -\ y$

$= x$

Hence f(x) = x for all $x \in Z$ as the result f(0) = 0 holds for any ring homomorphism. This only homomorphism from Z to Z are the identity and zero mapping.

**Ans to Q No 12:** We have R is a ring with unity 1. Define $\phi : Z \to R$ by $\phi$ (n) = n.1. We have to prove $\phi$ is a ring homomorphism.

Let $m, n \in R$. Then

$\phi(m+n) = (m+n).1$

$= m.1 + n.1$

$= \phi(m)+\phi(n)$

So, $\phi$ preserves addition

$\phi(mn) = (mn).1$

$= (mn).(1.1)$

$= (m.1)(n.1)$ [$\because$ (m.a) (n.b)=(mn).(ab) for all integer m, n]

$= \phi(m)\ \phi(n)$

So, $\phi$ preserves multiplication as well.

Hence $\phi$ is a ring homomorphism.

**Ans to Q No 13:** We have $Z_n = \{0, 1, 2, 3, \ldots, n-1\}$

and $Z/\langle n\rangle = \{\langle n\rangle, 1+\langle n\rangle, 2+\langle n\rangle, \ldots, (n-1)+\langle n\rangle\}$

Define $\phi: Z/\langle n\rangle \to Z_n$ by

$\phi(r+\langle n\rangle) = r,\ 0 \le r \le n-1$

Let $r+\langle n\rangle = s+\langle n\rangle$ and suppose $r \neq s$.

Then $r-s \in \langle n\rangle$.

$\Rightarrow n|r-s$

$\Rightarrow n \le r-s$, where $r, s \le n$.

Thus we get a contradiction. This contradiction implies that r = s and so $\phi$ is well defined.

Also we can show that $\phi$ is one-one and onto.

Let $r+\langle n\rangle, s+\langle n\rangle \in Z/\langle n\rangle$

$\phi\ [(r+\langle n\rangle)+(s+\langle n\rangle)] = \phi[(r+s)+\langle n\rangle]$

$= \phi[(nq+t)+\langle n\rangle]$ for some q, t; $0 \le t \le n$.

$= \phi(t+\langle n\rangle)$ [$\because nq \in \langle n\rangle$]

$= t$

$= r \oplus_n s$ where $\oplus_n$ is addition modulo n.

$= \phi(r+\langle n\rangle) \oplus_n \phi(s+\langle n\rangle)$

$\phi[(r+\langle n\rangle)(r+\langle n\rangle)] = \phi[rs+\langle n\rangle]$

$= \phi[nq'+t'+<n>]$ for some $q', t'$; $0 \le t' \le n$

$= \phi(t'+\langle n\rangle)$ [$\because nq' \in \langle n\rangle$]

$= t'$

$= r \otimes_n s$, where $\otimes_n$ is multiplication modulo n.

$= \phi(r+\langle n\rangle) \otimes_n \phi(s+\langle n\rangle]$

From above, we can conclude that $\phi$ is a ring homomorphism and hence an isomorphism. Thus $Z/\langle n\rangle \cong Z_n$

**Ans to Q No 14:** Let 1 be the unity in R and let S = {k.1 : k∈Z) Then the mapping $\phi : Z \to S$ given by $\phi(k) = k.1$ is a ring epimorphism. Hence by foundamental theorem of ring homorphism $Z/\ker\phi \cong S$, where

$\ker\phi = \{kZ : \phi(k) = 0\}$

$= \{k \in Z : k.1 = 0\}$

$= \{k \in Z : n|k\}$ as char R = n>0.

$=\{k \in Z : k = n.s$ for some integer s}

$= \langle n\rangle$

So, when R has characteristic n,

$S \cong Z/\langle n\rangle \cong Zn$

Also, when R has characteristic 0,

$S \cong Z/\langle 0\rangle \cong Z$



## 10.12 MODEL QUESTIONS

**Q 1:** Given an example of a non-commutative ring R and an ideal I of R such that $R/I$ is a field.

[Hint. Take $R = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in Q\right\}$

$$I = \left\{\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} : x \in Q\right\}$$

**Q 2:** How many elements are in $Z[i]/\langle 3+i\rangle$ ?

Give reasons for your answer.

**Q 3:** Let R be a ring and let I be an ideal of R. Prove that the factor ring $R/I$ is commutative if and only if rs–sr ∈I for all r and s in R.

**Q 4:** Prove that $I = \langle 2+2i \rangle$ is not a prime ideal of Z [i]. How many elements are in $Z[i]/I$ ?

**Q 5:** Let R be the ring of all real-valued continuous functions on the closed interval [0, 1]. Let $M = \{f \in R : f(\frac{1}{3}) = 0\}$. Show that M is a maximal ideal of R.

**Q 6:** Let R be a finite non-zero commutative ring. Show that every prime ideal of R is a maximal ideal of R.

**Q 7:** Prove that in Z, an ideal $\langle n \rangle$ is maximal if and only if n is prime.

**Q 8:** Give an example of a ring that has exactly two maximal ideals.

**Q 9:** Give an example of a commutative ring that has a maximal ideal that is not a prime ideal.

**Q 10:** If R is a commutative ring with unity and A is proper ideal of R, show that $R/A$ is a commutative ring with unity.

**Q 11:** Show that the relation of isomorphism in rings is an equivalence relation.

**Q 12:** Show that homomorphic image of a commutative ring is commutative. Prove also that the converse may not hold.

**Q 13:** Show that homomorphic image of a ring with unity is a ring with unity but the converse is not true.

**Q 14:** $2z = \{2n : n \in Z\}$ and $8Z = \{8n : n \in Z\}$. Show that $2Z/8Z$ and $Z_4$ (ring of integers modulo 4) are isomorphic as group but not as ring.

**Q 15:** Show that $f : C \to R_2$ given by $f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ is a monomorphism, where $C = \{a+ib : a, b \in R\}$ and $R_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R \right\}$.

**Q 16:** Let $Z[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in Z\}$ and $H = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} : a, b \in Z \right\}$. Show that $Z[\sqrt{2}]$ and H are isomorphic as rings.

**Q 17:** Consider the mapping $\phi : M_2(Z) \to Z$ given by $\phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = a$, where

$M_2(Z) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R \right\}$ and Z = the set of integers. Prove or disprove that this is a ring homormorphism.

**Q 18:** Let $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in Z \right\}$. Prove or disprove that the mapping $\phi : R \to R$ given by $\phi \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = a$ is a ring homomorphism.

**Q 19:** Is the mapping $\phi : Z_5 \to Z_{30}$ given by $\phi(x) = 6x$ a ring homomorphism?

**Q 20:** Is the mapping $\phi : Z_{10} \to Z_{10}$ given by $\phi(x) = 2x$ a ring homomorphism?

*** ***** ***