P.R. GOVT COLLEGE (A)
KAKINADA

GUNNAM PRASADA RAO

LECTURER IN MATHEMATICS

RING THEORY-SEM-IV

INTRODUCTION TO RINGS, SUBRINGS, IDEALS, HOMOMORPHISM, POLYNOMIAL RINGS

UNIT-4: HOMOMORPHISM FOR RINGS

Homomorphism (Def): Let R, R^1 be two rings. A mapping $f: R \to R^1$ is said to be a homomorphism if (i) $f(a+b) = f(a) + f(b)$ $\quad (ii) f(ab) = f(a)f(b) \quad \forall\, a, b \in R$

Monomorphism (Def): Let R, R^1 be two rings. A homomorphism $f: R \to R^1$ is called a monomorphism if f is a one-one mapping.

Epimorphism (Def): Let R, R^1 be two rings. A homomorphism $f: R \to R^1$ is called a Epimorphism if f is on-to mapping.

Isomorphism (Def): Let R, R^1 be two rings. A homomorphism $f: R \to R^1$ is called a Isomorphism if f is one-one and on-to mapping.

Note: If $R = R^1$ *then homomorphism is called as Endo morphism. also isomorphism is called as Automorphism.*

Homomorphic image of ring (Def): If $f: R \to R^1$ is a homomorphism then the image set $f(R) = \{f(x) \in R^1 / x \in R\}$ is called the f homomorphic image of R.

Theorem 1: If $f: R \to R^1$ is a homomorphism then (i) $f(0) = 0^1$ *where* $0, 0^1$ *are zero elements of* R, R^1 respectively.(ii) $f(-a) = -f(a) \quad \forall\, a \in R$ (iii) $f(a-b) = f(a) - f(b) \quad \forall\, a, b \in R$

Proof: (i) For $0 \in R$, *we have* $0 + 0 = 0 \Longrightarrow f(0+0) = f(0)$ [$\because$ *f is mapping*]

$\Longrightarrow f(0) + f(0) = f(0)$ [$\because$ *f is homo*]

$\Longrightarrow f(0) + f(0) = f(0) + 0^1$ [$\because f(0) \in R^1$ *so* $xe = x$]

$\Longrightarrow f(0) = 0^1$ [By L.C.L in $(R^1, +)$]

(ii) For $a \in R \Longrightarrow \exists - a \in R \ni a + (-a) = 0 \Longrightarrow f\big(a + (-a)\big) = f(0)$

$\Longrightarrow f(a) + f(-a) = 0^1$ $by(i) \Longrightarrow f(-a) = -f(a)$

(iii) For $a, b \in R$, $\quad f(a-b) = f[a + (-b)] = f(a) + f(-b) = f(a) - f(b) \quad by(ii)$

Theorem 2: The homomorphic image of a ring is a ring. (OR)

If $f: R \to R^1$ is a homomorphism from a ring R to a ring R^1 *then* $f(R)$ *is a subring of* R^1

Proof: Let R, R^1 be two rings and $f: R \to R^1$ is a homomorphism

The homomorphic image of R $= f(R) = \{f(x) \in R^1 / x \in R\}$

To prove that $f(R)$ *is a ring. For this we have to show that* $f(R)$ *is a subring of* R^1

(i) For $0 \in R$, *we have* $f(0) = 0^1 \Longrightarrow f(0) = 0^1 \in f(R) \Longrightarrow f(R) \neq \emptyset$

(ii) By the def of $f(R) \Longrightarrow f(R) \subseteq R^1$

(iii) Let $a^1, b^1 \in f(R)$ *then* $a^1 = f(a),\ b^1 = f(b)$ *where* $a, b \in R$

Since $a, b \in R$ *and* R *is a ring* $\Longrightarrow a - b, ab \in R$

Now $a^1 - b^1 = f(a) - f(b) = f(a - b) \in f(R)$ *and* $a^1 b^1 = f(a) f(b) = f(ab) \in f(R)$

$f(R)$ *is a subring of* R^1

Theorem3: The homomorphic image of a commutative ring is a commutative ring.

Proof: Let R, R^1 be two rings and $f: R \to R^1$ is a homomorphism

The homomorphic image of R $= f(R) = \{f(x) \in R^1 / x \in R\}$

To prove that
$f(R)$ *is a commutative ring. For this we have to show that* $f(R)$ *is a subring of* R^1

(i) For $0 \in R$, *we have* $f(0) = 0^1 \Longrightarrow f(0) = 0^1 \in f(R) \Longrightarrow f(R) \neq \emptyset$

(ii) By the def of $f(R) \Longrightarrow f(R) \subseteq R^1$

(iii) Let $a^1, b^1 \in f(R)$ *then* $a^1 = f(a),\ b^1 = f(b)$ *where* $a, b \in R$

Since $a, b \in R$ *and* R *is a ring* $\Longrightarrow a - b, ab \in R$

Now $a^1 - b^1 = f(a) - f(b) = f(a - b) \in f(R)$ *and* $a^1 b^1 = f(a) f(b) = f(ab) \in f(R)$

$f(R)$ *is a subring of* R^1

(iv) Let $a^1, b^1 \in f(R)$ *then* $a^1 . b^1 = f(a) f(b) = f(ab) = f(ba) = f(b) f(a) = b^1 . a^1$

$f(R)$ *is a commutative ring*

Kernel of a homomorphism (Def): Let R, R^1 be two rings and $f: R \to R^1$ is a homomorphism then the set of elements in a ring Rwhich is mapped with zero element of R^1 is called as kernel of a homomorphism.

i.e. $kerf = \{x \in R / f(x) = 0^1 \; where \; 0^1$is the zero element of $R^1\}$

Note: 1.By def of $kerf \subseteq R$ (ii) $x \in kerf \Leftrightarrow f(x) = 0^1$

(iii) For $0 \in R, \; we \; havee \; f(0) = 0^1 \Longrightarrow 0 \in kerf \Longrightarrow kerf \neq \emptyset$

Theorem4: Let R, R^1 be two rings and $f: R \to R^1$ is a homomorphism then $kerf$ is an ideal of R

Proof: since $f: R \to R^1$ is a homomorphism

$kerf = \{x \in R / f(x) = 0^1 \; where \; 0^1$is the zero element of $R^1\}$

To prove that $kerf$ is an ideal of R

(i) For $0 \in R, \; we \; havee \; f(0) = 0^1 \Longrightarrow 0 \in kerf \Longrightarrow kerf \neq \emptyset$

(ii) By def of $kerf$ clearly $kerf \subseteq R$

(iii) $Let \; a, b \in kerf \; then \; f(a) = 0^1 \;\; and \; f(b) = 0^1$

$Now \; f(a-b) = f(a) - f(b) = 0^1 - 0^1 = 0^1 \Longrightarrow a - b \in kerf$

Thus $a, b \in kerf \Longrightarrow a - b \in kerf$

(iv) $Let \; a \in kerf, \; r \in R \; then \; f(a) = 0^1$

$Now \; f(ar) = f(a).f(r) = 0^1.f(r) = 0^1 \Longrightarrow ar \in kerf$

$also \; f(ra) = f(r)f(0) = f(r).0^1 = 0^1$

Thus $a \in kerf, \; r \in R \Longrightarrow ar, ra \in kerf \; . \; Hence \; kerf$ is an ideal of R

Theorem5: Let R, R^1 be two rings and $f: R \to R^1$ is a homomorphism then $f \; is \; into - isomorphism (one - one) \Leftrightarrow \; kerf = \{0\}$

Proof: since $f: R \to R^1$ is a homomorphism

Necessary condition ($\Longrightarrow$): Given $f \; is \; into - isomorphism.$

$i.e. f \; is \; one - one \; homomorphism. \quad To \; prove \; that \; \Leftrightarrow \; kerf = \{0\}$

Let $a \; be \; any \; element \; in \; kerf$

By def, $f(a) = 0^1$ *where* 0^1 is the zero element of R^1

$\Rightarrow f(a) = f(0)$ [$\because$ *f is homo*]

$\Rightarrow a = 0$ [$\because$ *f is one − one*] $\Rightarrow kerf = \{0\}$

Sufficient condition($\Leftarrow$): Given $kerf = \{0\}$

To prove that f *is into − isomorphism.*

We show that f *is one − one* (*to given f is homomorphism.*)

Let $a, b \in R$ *and* $f(a) = f(b)$

Now $f(a) = f(b) \Rightarrow f(a) - f(b) = 0^1 \Rightarrow f(a - b) = 0^1 \Rightarrow a - b \in kerf$

Since $kerf = \{0\} \Rightarrow a - b = 0 \Rightarrow a = b \Rightarrow$ *f is one − one*

Fundamental theorem of homomorphism for rings: Let R, R^1 be two rings and $f: R \to R^1$ be onto a homomorphism with kernel K then R^1 *is isomorphic to* $\frac{R}{K}$ (or) Every homomorphic image of a ring is isomorphic to some quotient ring.

Proof: Given that $f: R \to R^1$ is onto a homomorphism

$kerf = \{x \in R / f(x) = 0^1$ *where* $0^1$is the zero element of $R^1\}$

We know that $kerf = K$ is an ideal of R

Now $\frac{R}{K} = \{x + K / x \in R\}$ is a ring under $(i)(x + K) + (y + K) = (x + y + K)$

$(ii)(x + K) \cdot (y + K) = (xy + K) \quad \forall\, x + K, y + K \in \frac{R}{K}$

Define $\emptyset: \frac{R}{K} \to R^1$ *by* $\emptyset(x + K) = f(x) \quad \forall\, x + K \in \frac{R}{K}$

(i) $\emptyset$ **is well defined and one-one:** *Let* $x + K, y + K \in \frac{R}{K}$ *and* $x + k = y + k$

Since $x + k = y + k \Leftrightarrow x - y \in K$

$\Leftrightarrow x - y \in kerf$

$\Leftrightarrow f(x - y) = 0^1$

$\Leftrightarrow f(x) - f(y) = 0^1$

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

$$\Leftrightarrow \emptyset(x+K) = \emptyset(y+K)$$

(ii) $\emptyset$ **is homomorphism:** $Let\ x+K, y+K \in \frac{R}{K}$

(a) $\emptyset[(x+K)+(y+k)] = \emptyset(x+y+k)$

$$= f(x+y)$$

$$= f(x)+f(y) \quad [\because f\ is\ homo\ ]$$

$$= \emptyset(x+K)+\emptyset(y+K)$$

(b) $\emptyset[(x+K).(y+k)] = \emptyset(xy+k)$

$$= f(xy)$$

$$= f(x).f(y) \quad [\because f\ is\ homo\ ]$$

$$= \emptyset(x+K).\emptyset(y+K)$$

(iii) $\emptyset$ **is on-to:** Let $y^1 \in R^1 \quad since\ f\ is\ on-to\ \exists x \in R \ni f(x) = y^1$

For this $x \in R, we\ have\ x+k \in \frac{R}{K}\ so\ that\ = \emptyset(x+K) = f(x)$

$$Foreach\ y^1 \in R^1\ \exists\ x+k \in \frac{R}{K}\ so\ that\ = \emptyset(x+K) = f(x) = y^1$$

$$\therefore \emptyset: \frac{R}{K} \to R^1\ is\ an\ isomorphism\ and\ hence\ \frac{R}{K} \cong R^1$$

Primal ideal (Def): An ideal I of the commutative ring R is said to be prime ideal of R if for all $x, y \in R\ and\ xy \in I \Longrightarrow x \in I\ or\ y \in I.$

Theorem1: An ideal *I* of a commutative ring *R* is prime ideal of *R* $\Leftrightarrow \frac{R}{I}$ *is* an integral domain.

Proof: I is an ideal of commutative ring of R

$\therefore \frac{R}{I} = \{x+I/x \in R\}$ is a commutative ring under $(i)(x+I)+(y+I) = (x+y+I)$

$$(ii)(x+I)\cdot(y+I) = (xy+I)\ \forall\ x+I, y+I \in \frac{R}{I}\ \ also\ \ 0+I\ is\ the\ zero\ element\ of\ \frac{R}{I}$$

Necessary condition ($\Longrightarrow$): $I\ is\ a\ prime\ ideal\ of\ R.\ To\ prove\ that\ \frac{R}{I}\ is$ an integral domain

For this we have to show that $\frac{R}{I}$ $has\ no\ zero\ divisors.$

Let $x+I, y+I \in \frac{R}{I}$ and $(x+I)\cdot(y+I) = 0+I$

Now $(x+I)\cdot(y+I) = 0+I \Rightarrow xy+I = 0+I$

$$\Rightarrow xy - 0 \in I$$

$$\Rightarrow xy \in I$$

$$\Rightarrow x \in I\ or\ y \in I \quad [\because I\ is\ a\ prime\ ideal]$$

$$\Rightarrow x+I = 0+I\ or\ y+I = 0+I$$

$\therefore$ $\frac{R}{I}$ $has\ no\ zero\ divisors.$

Sufficient condition ($\Leftarrow$): Given $\frac{R}{I}$ is an integral domain. To prove $I\ is\ a\ prime\ ideal\ of\ R$

$\forall\ a, b \in R\ and\ ab \in I \Rightarrow ab+I = 0+I \Rightarrow (a+I)(b+I) = 0+I$

Since $\frac{R}{I}$ is an integral domain and hence $\frac{R}{I}$ $has\ no\ zero\ divisors.$

$\Rightarrow (a+I) = 0+I\ or\ (b+I) = 0+I \Rightarrow a \in I\ or\ b \in I \therefore$ $I\ is\ a\ prime\ ideal\ of\ R$

Maximal ideal: Let R be a ring and M be an ideal of $R\ and\ M \neq R$. M is said to be maximal ideal of R if when ever N is an ideal of R such that $M \subseteq N \subseteq R$ them either$M = N$ $or\ N = R$.

Theorem2: An ideal *M* of a commutative ring with unity *R* is maximal ideal of *R* $\Leftrightarrow$ $\frac{R}{M}$ *is* a field.

Proof: M is an ideal of commutative ring with unity of R

$\therefore$ $\frac{R}{M} = \{x+M / x \in R\}$ is a commutative ring with unity under

$(i)(x+M)+(y+M) = (x+y+M)$

$(ii)(x+M)\cdot(y+M) = (xy+M)$ $\forall\ x+M, y+M \in \frac{R}{M}$

$also$ $0+M\ is\ the\ zero\ element\ of\ \frac{R}{M}$ and $1+M\ is\ the\ unity\ element\ of\ \frac{R}{M}$

Necessary condition ($\Rightarrow$): $M\ is\ a\ maximal\ ideal\ of\ R.\ To\ prove\ that\ \frac{R}{M}\ is$ a field

For this we have to show that every non-zero element of $\frac{R}{M}$ $is\ invertiable$

Let $a+M$ be non $-$ zero element of $\in \frac{R}{M}$ so $\therefore a+M \neq 0+M \Longrightarrow a \notin M$ and $a \in R$

we know that $I=\{ra/r \in R\}$ is also an ideal of R

$\therefore M+I=\{p+q/p \in M, q \in I\}$ is also an ideal of R

Since M is a maximal ideal of R so $M \subseteq M+I \subseteq R$

Since $a \notin M$ and $a=0+1. a \in M+I \Longrightarrow M \neq M+I$

Since M is a maximal ideal of R so $M+I=R$

$1 \in R \Longrightarrow 1 \in M+I \Longrightarrow 1=m+ba$ where $m \in M, b \in R$

$\Longrightarrow 1-ba=m \in M \Longrightarrow 1-ba \in M \Longrightarrow 1+M=ba+M$

$\Longrightarrow 1+M=(b+M)(a+M)$

Since $\frac{R}{M}$ is commutative ring $\therefore (a+M)(b+M)=(b+M)(a+M)=1+M$

$a+M \neq 0+M$ has multiplicative inverse of $b+M \in \frac{R}{M}$

$\therefore \frac{R}{M}$ is a field

Sufficient condition ($\Longleftarrow$): Given $\frac{R}{M}$ is a field . To prove M is a maximal ideal of R

Let N be any ideal of R such that $M \subseteq N \subseteq R$

If $M=N$, there is nothing to prove.

If $M \neq N$, to prove that $N=R$ ($N \subseteq R$ and $R \subseteq N$) For this we have to show that $1 \in N$

Since $M \neq N$ and $M \subseteq N \Longrightarrow \exists$ an element $a \notin M$ and $a \in N$

$\therefore a \notin M \Longrightarrow a+M \neq 0+M \in \frac{R}{M} \Longrightarrow a+M$ is a non $-$ zero element of $\frac{R}{M}$

and $\frac{R}{M}$ is a field

so $\exists\, b+M \in \frac{R}{M}$ such that $(a+M)(b+M)=(b+M)(a+M)=1+M$

$\Longrightarrow ab+M=1+M \Longrightarrow ab-1 \in M \Longrightarrow 1-ab \in M \subseteq N \Longrightarrow 1-ab \in N$

$a \in N, b \in R$ and N is a ideal of $R \Longrightarrow ab \in N$

$1 - ab \in N, \quad ab \in N \; and \; N \; is \; an \; ideal \; of \; R \Longrightarrow 1 - ab + ab \in N \Longrightarrow 1 \in N$

Clearly $N \subseteq R \longrightarrow (1)$

Let x be any element of R

$\therefore \; x \in R \Longrightarrow x.1 \in R \Longrightarrow x.1 \in N \; [\because 1 \in N \; , x \in R \; and \; Nis \; an \; ideal \; of \; R \Longrightarrow x.1 \in N \;]$

$\Longrightarrow x \in N \qquad \therefore \; R \subseteq N \longrightarrow (2)$

From (1) &(2) $N = R \therefore$ M is a maximal ideal of R