Ch-15 Ring homomorphism

Defⁿ: A ring homomorphism ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations:

i.e. $\phi(a+b) = \phi(a) + \phi(b)$, $\forall\ a, b \in R$.

& $\phi(ab) = \phi(a) \cdot \phi(b)$, $\forall\ a, b \in R$

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

Ex. 1. $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$

defined as $\phi(k) = k \bmod (n)$, then ϕ is ring homomorphism.

$\rightarrow$ let $a, b \in \mathbb{Z}$

$$\phi(a+b) = (a+b) \bmod (n)$$
$$= ((a \bmod (n)) + (b \bmod (n))) \bmod n.$$
$$= \phi(a) + \phi(b)$$

IIIly $\phi(ab) = ab \bmod (n)$

$$((a \bmod (n))(b \bmod n)) \bmod n$$
$$= \phi(a) \cdot \phi(b)$$

$\Rightarrow \phi$ is a ring homomorphism.

2. $\phi : \mathbb{C} \longrightarrow \mathbb{C}$ defined as

$\phi(a+ib) = a - ib$, ϕ is a ring isomorphism

Assignment Q4 $\mathbb{R}^2 = \{(a, b) \mid a \in \mathbb{R}, b \in \mathbb{R}\}$ under operations

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2).$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$$

is it a ring? Is it field / I.D?

Page No.:
Date: / /

Ex.2. Let $a_1+ib_1,\ a_2+ib_2 \in \mathbb{C}$

Then, $\phi(a_1+ib_1+a_2+ib_2) = \phi((a_1+a_2)+i(b_1+b_2))$

$= a_1+a_2-i(b_1+b_2)$

$= a_1-ib_1+a_2-ib_2$

$= \phi(a_1+ib_1)+\phi(a_2+ib_2).$

Now, $\phi((a_1+ib_1)\cdot(a_2+ib_2)) = \phi(a_1a_2-b_1b_2+ia_2b_1+ia_1b_2)$

$= a_1a_2-b_1b_2-i(a_2b_1+a_1b_2)$

$= (a_1-ib_1)\cdot(a_2-ib_2)$

$= \phi(a_1+ib_1)\cdot\phi(a_2+ib_2)$

$\therefore$ ϕ is ring homomorphism.

For 1-1, let $\phi(a_1+ib_1) = \phi(a_2+ib_2)$

$a_1-ib_1 = a_2-ib_2$

Comparing both sides, we have

$a_1 = a_2$ and $b_1 = b_2$.

$\Rightarrow a_1+ib_1 = a_2+ib_2$.

$\therefore$ ϕ is one-one.

For onto, let $z\in\mathbb{C} \Rightarrow z = a+ib$

$\exists\ a-ib\in\mathbb{C}$ s.t.

$\phi(a-ib) = a+ib = z$

$\therefore$ ϕ is onto.

$\Rightarrow$ ϕ is ring isomorphism.

Theorem: Properties of Ring homomorphism

Let ϕ be a homomorphism from ring R to a ring S. Let A be a subring of R and B an ideal of S. Then

i) For any $x\in R$, and any +ve integer n,

$\phi(nx) = n\phi(x)$

& $\phi(x^n) = (\phi(x))^n$

Page No.
Date : / /

$$\phi(nx) = \phi(\overbrace{x + x + x + \cdots + x}^{n \text{ times}})$$
$$= \phi(x) + \phi(x) + \cdots + \phi(x) \quad (\because \phi \text{ is ring homo})$$
$$= n\phi(x)$$

$$\phi(x^n) = \phi(\overbrace{x \cdot x \cdot x \cdots x}^{n \text{ times}})$$
$$= \phi(x) \cdot \phi(x) \cdots \phi(x) \quad (\because \phi \text{ is ring homo})$$
$$= (\phi(x))^n$$

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

→ Let $\phi(a_1)$ & $\phi(a_2) \in \phi(A)$

Then $\phi(a_1) - \phi(a_2) = \phi(a_1 - a_2)$ (ϕ is ring homo)

as $a_1 \in A$, $a_2 \in A$

$\Rightarrow a_1 - a_2 \in A$ ($\because A$ is subring of R)

$\Rightarrow \phi(a_1 - a_2) \in \phi(A)$

Also $\phi(a_1) \cdot \phi(a_2) = \phi(a_1 a_2)$ ($\because a_1 a_2 \in A$, A subring of R)

$\Rightarrow \phi(a_1 a_2) \in \phi(A)$

$\Rightarrow \phi(A)$ is a subring of S.

3) Let A be an ideal of R and ϕ is onto, then $\phi(A) = \{\phi(a) : a \in R\}$ is an ideal of S.

→ Let $s \in S$, $\phi(a) \in \phi(A)$

To show: $s \cdot \phi(a) \in S$ and $\phi(a) \cdot s \in \phi(A)$

→ As ϕ is onto, $s \in S$ $\exists$ $a_s \in R$ such that $\phi(a_s) = s$.

$\phi(a_s \cdot a) = \phi(a_s) \cdot \phi(a) = s\phi(a)$

$\Rightarrow$ As $a_s \cdot a \in A$ ($\because A$ is ideal of R)

$\Rightarrow \phi(a_s \cdot a) \in \phi(A)$

$\Rightarrow s \cdot \phi(a) \in \phi(A)$

lly $\phi(a) \cdot s \in \phi(A)$

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

Page No.
Date : / /

4) B is an ideal of S, $\phi^{-1}(B)$ is an ideal of R.

$\phi^{-1}(B) = \{ r \in R \mid \phi(x) \in B \}$

→ Let $a_1, a_2 \in \phi^{-1}(B)$

To show: $a_1 - a_2 \in \phi^{-1}(B)$ or $\phi(a_1 - a_2) \in B$.

$a_1 \in \phi^{-1}(B)$

$\Rightarrow \phi(a_1) \in B$ $\quad$ ||ly $\quad \phi(a_2) \in B$

$\Rightarrow \phi(a_1) - \phi(a_2) \in B$ $\quad$ ($\because$ B is an ideal of S)

$\Rightarrow \phi(a_1 - a_2) \in B$ $\quad$ ($\because$ B is subring of S)

$\Rightarrow a_1 - a_2 \in \phi^{-1}(B)$

Let $r \in R$ and $a \in \phi^{-1}(B)$

To show: $ra \in \phi^{-1}(B)$ & $ar \in \phi^{-1}(B)$ or $\phi(ra)$ & $\phi(ar) \in B$.

as $r \in R$ $\quad$ as $a \in \phi^{-1}(B)$

$\Rightarrow \phi(r) \in S$ $\quad \Rightarrow \phi(a) \in B$

$\phi(r) \cdot \phi(a) \in B$ $\quad$ ($\because$ B is ideal of S)

$\Rightarrow \phi(ra) \in B$

||ly $\phi(ar) \in B$

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

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

→ Let $\phi(r_1), \phi(r_2) \in \phi(R)$

To show: $\phi(r_1) \cdot \phi(r_2) = \phi(r_2) \cdot \phi(r_1)$

$\phi(r_1) \cdot \phi(r_2) =$ → (ϕ is ring homo)

Consider $\phi(r_1 \cdot r_2) = \phi(r_2 \cdot r_1)$ (R is commutative)

$= \phi(r_2) \cdot \phi(r_1)$ (ϕ is ring homo)

$\Rightarrow \phi(R)$ is commutative.

6. If R has a unity 1 and ϕ is onto, then $\phi(1)$ is unity of S [Also $S \neq \{0\}$].

→ let $s \in S$
To show $s \cdot \phi(1) = s$. or $\phi(1) \cdot s = s$.

As ϕ is onto and $s \in S$
$\exists$ $x \in R$ s.t. $\phi(x) = s$.
$s \cdot \phi(1) = \phi(x) \cdot \phi(1) = \phi(x \cdot 1) = \phi(x) = s$
Also. $\phi(1) \cdot s = \phi(1) \cdot \phi(x) = \phi(1 \cdot x) = \phi(x) = s$
$\therefore$ $\phi(1)$ is unity of S.

7. ϕ is an isomorphism if and only if ϕ is onto and $\text{Ker}\,\phi = \{x \in R \mid \phi(x) = 0\} = \{0\}$.

→ ($\Rightarrow$) Let ϕ is an isomorphism
$\Rightarrow$ ϕ is onto and one-one.
Now, we will show that $\text{Ker}\,\phi = \{0\}$.
let $x \in \text{Ker}\,\phi$
$\Rightarrow$ $\phi(x) = 0$ Also, $\phi(0) = 0$ → ($\because$ R being a ring under $+$, ϕ is group homo)
$\Rightarrow$ $\phi(x) = \phi(0)$ ($\because \phi$ is one-one)
$\Rightarrow$ $x = 0$.

($\Leftarrow$) conversely, We want to show ϕ is one-one.
Let $\phi(x_1) = \phi(x_2)$
$\phi(x_1) - \phi(x_2) = 0$.
$\phi(x_1 - x_2) = 0$.
$\Rightarrow$ $x_1 - x_2 = 0$
$\Rightarrow$ $x_1 = x_2$
$\Rightarrow$ ϕ is one-one.

8. If ϕ is an isomorphism from R onto S, then ϕ^{-1} is an isomorphism from S onto R.
$\phi : R \xrightarrow{iso} S$
$\Rightarrow$ $\phi^{-1} : S \xrightarrow{iso} R$

Page No.:
Date: / /

→ Let $s_1, s_2 \in S$

To show $\phi^{-1}(s_1+s_2) = \phi^{-1}(s_1) + \phi^{-1}(s_2)$ and

$\phi^{-1}(s_1 s_2) = \phi^{-1}(s_1) \cdot \phi^{-1}(s_2)$.

$\exists\ r_1, r_2 \in R$ s.t.

$\phi(r_1) = s_1$ and $\phi(r_2) = s_2$.

Also, $s_1 + s_2 \in S$ $\exists\ r \in R$ s.t. $\phi(r) = s_1 + s_2$

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

$= s_1 + s_2$

$\phi(r) = s_1 + s_2$

$\Rightarrow r = r_1 + r_2$

$\Rightarrow \phi^{-1}(s_1+s_2) = \phi^{-1}(s_1) + \phi^{-1}(s_2)$

As $s_1, s_2 \in S$ $\exists\ r' \in R$ s.t. $\phi(r') = s_1 s_2$

$\phi(r_1 r_2) = \phi(r_1) \cdot \phi(r_2) = s_1 s_2$

$\phi(r') = s_1 s_2$

$\Rightarrow r' = r_1 r_2$

$\Rightarrow \phi^{-1}(s_1 s_2) = \phi^{-1}(s_1) \cdot \phi^{-1}(s_2)$

$\Rightarrow \phi^{-1}$ is ring isomorphism.

Assignment

→ Q. Let R be a finite commutative ring with unity. Then prove that every prime is maximal.

Ex. 1 let $\mathbb{R}[x]$ be a ring of polynomial whose coefficients are from $\mathbb{R}$, then define a map
$$\phi : \mathbb{R}[x] \longrightarrow \mathbb{R} \text{ as}$$
$$\phi(f(x)) = f(1)$$
then ϕ is ring homomorphism.

$\rightarrow$ let $f(x), g(x) \in \mathbb{R}[x]$

$$\phi(f(x) + g(x)) = \phi((f+g)(x)) = (f+g)(1)$$
$$= f(1) + g(1)$$
$$= \phi(f(x)) + \phi(g(x))$$

$$\phi(f(x) \cdot g(x)) = \phi((fg)(x))$$
$$= (fg)(1) = f(1) \cdot g(1)$$
$$= \phi(f(x)) \cdot \phi(g(x)).$$

$\phi(f(x)) = f(b)$, $b \in \mathbb{R}$
then ϕ is ~~group~~ ring homo.

Recall: $\mathbb{Z}_n \longrightarrow \mathbb{Z}_m$
no. of homo?
x x

② $\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_{10}$
$$\phi(x) = 5x$$
$\phi(0) = 0$
$\phi(1) = 5$
$\phi(2) = 0$
$\phi(3) = 5$

$$\phi(1+2) = \phi(3) = 5$$
$$\phi(1+2) = \phi(1) + \phi(2) = 5+0 = 5 \Rightarrow \phi(1+2) = \phi(1) + \phi(2)$$
$$\phi(1 \cdot 2) = 0$$
$$\phi(1) \cdot \phi(2) = \cancel{\phi}5 \cdot 0 = 0$$
$$\Rightarrow \phi(1 \cdot 2) = \phi(1) \cdot \phi(2).$$

Addition let $x, y \in Z_4$

$\phi(x+y) = (5(x+y)) \bmod 10 = 5x + 5y = \phi(x) + \phi(y)$

$= (5x) \bmod 10 + (5y) \bmod 10$

$5(x+y) = 10q + r$ $\quad = (5x - 10q_1) + (5y - 10q_2)$

$5(x+y) - 10q = r$ — ① $\quad = 5(x+y) - 10(q_1 + q_2)$ — ②

from ① & ②

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

To show: $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$

$\phi(x \cdot y) = 5(xy) \bmod 10 = 5xy - 10q$

$\phi(x) \cdot \phi(y) = 5(x) \bmod 10 \cdot (5y) \bmod 10.$

$= ((5x - 10q_1) \cdot (5y - 10q_2)) \bmod 10$

$= (25xy - 50xq_2 - 50yq_1 + 100q_1q_2) \bmod 10$

$= 5xy - 10q$

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

$\therefore \phi$ is ring homomorphism.

Q.4. Let R be a commutative ring with charactertistic 2. Then $\phi: R \rightarrow R$ defined as

$\phi(a) = a^2$ is a homo.

→ As $char(R) = 2$

$\Rightarrow 2x = 0 \quad \forall x \in R.$

let $a, b \in R$

Addition: $\phi(a+b) = (a+b)^2$

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

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

$= a^2 + b^2 + 2ab$ ($\because$ R is comm)

$= a^2 + b^2$ $(2ab = 0)$

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

Page No.:
Date: / /

Multiplication: $\phi(a \cdot b) = (ab)^2$
$= a^2 b^2$ ($\because R$ is commutative)
$= \phi(a) \cdot \phi(b)$.

$\therefore \phi$ is a ring homo.

$\phi(a) = a^4$
$\therefore \phi$ is not ring homo.

Q.5 Divisibility test by 9.

$a_k a_{k-1} \ldots a_0$ is divisible by 9 if $a_k + a_{k-1} + \ldots + a_0$ is divisible by 9.

→ Let n be an integer with decimal representation
$n = a_k a_{k-1} \ldots a_0$
$n = 10^k a_k + 10^{k-1} a_{k-1} + \ldots + a_0$

To show: If 9 divides n then 9 divides $(a_k + a_{k-1} + \ldots + a_0)$

If 9 divides n,
$\Leftrightarrow$ $n \bmod 9 = 0$
$\Leftrightarrow$ $(10^k a_k + 10^{k-1} a_{k-1} + \ldots + a_0) \bmod 9 = 0$
$\Leftrightarrow$ $((10^k a_k) \bmod 9 + (10^{k-1} a_{k-1}) \bmod 9 + \ldots + a_0 \bmod 9) \bmod 9 = 0$
As $10 \bmod 9 = 1$
$\Rightarrow$ $10^m \bmod 9 = 1$

$\Leftrightarrow$ $(a_k + a_{k-1} + \ldots + a_0) \bmod 9 = 0$
$\Leftrightarrow$ 9 divides $a_k + a_{k+1} + \ldots + a_0$.

Kernel of a Ring homomorphism:

Let R and S are two rings and $\phi: R \to S$ is a ring homo then $Ker(\phi)$ is defined as

$$Ker(\phi) = \{ x \in R \mid \phi(x) = 0 \}$$

Thm: $Ker \phi$ is an ideal of R.

→ Let $x_1, x_2 \in Ker \phi$

To show: $x_1 - x_2 \in Ker \phi$

As $x_1 \in Ker \phi$, $x_2 \in Ker \phi$

$\Rightarrow \phi(x_1) = 0$ & $\phi(x_2) = 0$

then $\phi(x_1 - x_2) = \phi(x_1) - \phi(x_2) = 0 - 0 = 0$

$\Rightarrow x_1 - x_2 \in Ker \phi$

Let $x \in R$.

To show: $x x_1 \in Ker \phi$ & $x_1 x \in Ker \phi$

$\phi(x \cdot x_1) = \phi(x) \cdot \phi(x_1) = \phi(x) \cdot 0 = 0$

||ly $\phi(x_1 \cdot x) = 0$

$\Rightarrow x x_1 \in Ker \phi$ & $x_1 x \in Ker \phi$

$\Rightarrow Ker \phi$ is an ideal of R.

Thm: (First Isomorphism Theorem)

Let ϕ be a ring isomorphism from R to S. Then the mapping from $\frac{R}{Ker \phi}$ to $\phi(R)$, given by

$x + Ker \phi \to \phi(x)$ is an isomorphism, In other words $\frac{R}{Ker \phi} \simeq \phi(R)$

→ $\phi: R \xrightarrow{homo} S$

Page No.:
Date: / /

Ker ϕ is an ideal of R.
$\frac{R}{\operatorname{Ker}\phi}$ is a factor ring.

To show: $\psi: \frac{R}{\operatorname{Ker}\phi} \xrightarrow{iso} \phi(R)$

$$\psi(x + \operatorname{Ker}\phi) = \phi(x)$$

Pf: Define $\psi: \frac{R}{\operatorname{Ker}\phi} \longrightarrow \phi(R)$ as $\psi(x+\operatorname{Ker}\phi) = \phi(x)$

Well defined: $x_1 + \operatorname{Ker}\phi = x_2 + \operatorname{Ker}\phi$
$\Leftrightarrow (x_1 - x_2) + \operatorname{Ker}\phi = \operatorname{Ker}\phi$
$\Leftrightarrow (x_1 - x_2) \in \operatorname{Ker}\phi$
$\Leftrightarrow \phi(x_1 - x_2) = 0$
$\phi(x_1) = \phi(x_2)$
$\Leftrightarrow \psi(x_1 + \operatorname{Ker}\phi) = \psi(x_2 + \operatorname{Ker}\phi)$

Onto: let $z \in \phi(R)$
$\exists\ x' \in R$ s.t.
$\phi(x') = z$
then $\psi(x' + \operatorname{Ker}\phi) = \phi(x') = z$
$\Rightarrow \psi$ is onto.

Group preserve:

$$\psi((x_1 + \operatorname{Ker}\phi) + (x_2 + \operatorname{Ker}\phi)) = \psi((x_1+x_2) + \operatorname{Ker}\phi)$$
$$= \phi(x_1 + x_2)$$
$$= \phi(x_1) + \phi(x_2)$$
$$= \psi(x_1 + \operatorname{Ker}\phi) + \psi(x_2 + \operatorname{Ker}\phi)$$

$\psi((r_1+\text{Ker}\phi)\cdot(r_2+\text{Ker}\phi)) = \psi(r_1r_2+\text{Ker}\phi) = \phi(r_1r_2)$

$= \phi(r_1)\cdot\phi(r_2)$

$= \psi(r_1+\text{Ker}\phi)\cdot\psi(r_2+\text{Ker}\phi)$

Thm 15.4 Every ideal of a ring R is the kernel of a ring homomorphism of R. $\phi: R \to \frac{R}{A}$

Pf: Let A be an ideal of R.

Define: $\phi: R \to \frac{R}{A}$

As $\phi(r) = r+A$

To show: ϕ is homo

Also $\text{Ker}\,\phi = A$.

Let $r_1, r_2 \in R$

Pf: $\phi(r_1+r_2) = (r_1+r_2)+A$

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

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

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

$= \phi(r_1)\cdot\phi(r_2)$

$\Rightarrow \phi$ is homo.

To show: $\text{Ker}\,\phi = A$

Let $x \in \text{Ker}\,\phi$

$\Rightarrow \phi(x) = 0$

$\Rightarrow \phi(x) = A$

$\Rightarrow x+A = A$

$\Rightarrow x \in A$

$\Rightarrow \text{Ker}\,\phi \subseteq A$ — (1)

Now, let $x \in A$

$\Rightarrow x+A = A$ $\Rightarrow x \in \text{Ker}\,\phi$

$\Rightarrow \phi(x) = A$ $\Rightarrow A \subseteq \text{Ker}\,\phi$ — (2)

$\Rightarrow \phi(x) = 0$ From (1) & (2)

$A = \text{Ker}\,\phi$.

Theorem 15.5: Let R be a ring with unity e. The mapping $\phi: \mathbb{Z} \longrightarrow R$ given by $\phi(n) = ne$ is a ring homomorphism.

Pf: Let $m, n \in \mathbb{Z}$

To show: $\phi(m+n) = \phi(m) + \phi(n)$

$= me + ne.$

Case 1: Consider m & n are both +ve.

i.e ~~m+~~ $m, n \geq 0$

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

$$= \underbrace{e+e+e+\cdots+e}_{(m+n)\text{- times}}$$

$$= \underbrace{e+e+\cdots+e}_{m\text{- times}} + \underbrace{\cdots+e}_{n\text{ -times}}$$

$$= me + ne$$

Case 2: Consider m & n are both -ve.

i.e. $m, n < 0. \Rightarrow -m, -n > 0.$

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

$$= (-(m+n))(-e)$$

$$\Rightarrow \phi(m+n) = (-m-n)(-e)$$

$$= \underbrace{-e-e-e-e-\cdots-e}_{-m+(-n)\text{ times}}$$

$$= (-m \text{ times}) + (-n \text{ times})$$

$$= -m(-e) + (-n)(-e)$$

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

Case 3. Consider m is +ve and n is -ve.

i.e. $m \geq 0$, $n < 0. \Rightarrow -n > 0$

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

$$= (m-(-n))(e)$$

Page No.:
Date: / /

$= me - n(-e)$

$= \underbrace{e+e+e+\dots+e}_{m\text{ times}} \underbrace{-e-e-\dots-e}_{-n\text{ times}}$

$= me + (-n)(-e)$

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

$\Rightarrow \phi$ preserves addition.

To show: ϕ preserves multiplication.

To show: $\phi(mn) = (mn)e = (me)(ne) = \phi(m)\cdot\phi(n)$

Case 1: If $m, n \geq 0$

$\phi(mn) = (mn)e$

$= e+e+\dots+e \;\}\; mn$ times

$= \underbrace{(e+e+\dots+e)}_{m\text{ times}}\underbrace{(e+\dots+e)}_{n\text{ times}}$

$= (me)(ne)$

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

Case 2: If $m, n < 0$ then $-m, -n > 0$

$\Rightarrow mn = (-m)(-n)$

$\phi(mn) = (mn)(e) = (-m)(-n)(e)$

$= \underbrace{e+e+\dots+e}_{-m\cdot(-n)\text{ times}}$

$= \underbrace{(e+e+e+\dots+e)}_{-m\text{ times}}\underbrace{(e+e+\dots+e)}_{-n\text{ times}}$

$= (-m)e\cdot(-n)e = (me)(ne)$

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

Case 3: If $m \geq 0$, $n<0$ then $-n>0$.

$\phi(m+n) = mne = m(-n)(-e)$

$= (-mn)(-e)$

$$= \underbrace{-e-e \cdots -e}_{-mn \text{ times}}$$

$$= \underbrace{(e+e+\cdots+e)}_{m \text{ times}} \underbrace{(-e-e \cdots -e)}_{-n \text{ times}}$$

$$= me \cdot (-n)(-e)$$

$$= me \cdot ne$$

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

$\Rightarrow$ ϕ preserves multiplication.

-2020

Corollary 1: If R is a ring with unity and the char of R is $n > 0$, then R contains a subring isomorphic to $\mathbb{Z}_n$. If $char(R) = 0$ then R contains a subring isomorphic to $\mathbb{Z}$.

Pf: Let 'e' be the unity of R and $char(R) = n$, where $n > 0$. Define $S = \{k \cdot e \mid k \in \mathbb{Z}\}$

Claim: $S \approx \mathbb{Z}_n$.

Check that S is a ring or subring of R. (?)

$S = \{e, 2e, 3e, \ldots\}$.

$\phi : \mathbb{Z} \longrightarrow R$ as

$\phi(k) = k \cdot e$.

ϕ is ring homo. (Thm 15.5)

$\phi(\mathbb{Z}) = S$

By 1st isomorphism Thm

$$\frac{\mathbb{Z}}{Ker(\phi)} \approx \phi(\mathbb{Z}) = S.$$

$$\Rightarrow S \approx \frac{\mathbb{Z}}{Ker(\phi)} \quad \text{—— (1)}$$

$$\begin{aligned} Ker\phi &= \{k \in \mathbb{Z} \mid \phi(k) = 0\} \\ &= \{k \in \mathbb{Z} \mid k \cdot e = 0\} \\ &= \{nk \mid k \in \mathbb{Z}\} = \langle n \rangle \end{aligned}$$

(as n is the least +ve integer s.t. $n \cdot e = 0$ then $char(R) = n$)

from (1) $\dfrac{\mathbb{Z}}{\langle n \rangle} \approx S$.

Scanned by CamScanner

Page No.:
Date: / /

And $\frac{\mathbb{Z}}{\langle n\rangle} \approx \mathbb{Z}_n \longrightarrow \frac{\mathbb{Z}}{\langle n\rangle} = \{k + \langle n\rangle\}$

$= \{0+\langle n\rangle, 1+\langle n\rangle, \ldots, n-1+\langle n\rangle\}$

$\Rightarrow \mathbb{Z}_n \approx S \subseteq R$
subring

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

Case 2. If $char(R) = 0$

$\phi: \mathbb{Z} \longrightarrow R$ define as

$\phi(k) = k.e$

$\Rightarrow \phi$ is ring homo (Thm 15.5)

Then. By 1st Iso. Thm

$\frac{\mathbb{Z}}{Ker\phi} \approx \phi(\mathbb{Z}) = S$

$Ker\phi = \{k \in \mathbb{Z} \mid \phi(k) = 0\}$

$= \{k \in \mathbb{Z} \mid k.e = 0\}$

$= \{0\}$

$\frac{\mathbb{Z}}{\{0\}} \approx \mathbb{Z} \approx S \subseteq R$
subring

Corollary 2: $\mathbb{Z}_m$ is a homomorphic image of $\mathbb{Z}$.

Statement: For any +ve integer m, there exists a homomorphism

$\phi: \mathbb{Z} \longrightarrow \mathbb{Z}_m$

Pf: Define $\phi: \mathbb{Z} \longrightarrow \mathbb{Z}_m$ as

$\phi(k) = k \bmod m$ is a ring homo

Consider $k_1, k_2 \in \mathbb{Z}$.

$\phi(k_1 + k_2) = (k_1+k_2) \bmod m$

$= ((k_1 \bmod m) + (k_2 \bmod m)) \bmod m$

$= k_1 \bmod m + k_2 \bmod m$

$= \phi(k_1) + \phi(k_2)$

Page No.:
Date: / /

$$\phi(k_1k_2) = (k_1k_2) \bmod m$$
$$= ((k_1 \bmod m)\cdot(k_2 \bmod m)) \bmod m$$
$$= k_1 \bmod m \cdot k_2 \bmod m$$
$$= \phi(k_1)\cdot \phi(k_2)$$

$\Rightarrow \phi$ is a ring homo.

Corollary 3: If F is a field with characteristic p. then F contains a subfield which is isomorphic to $\mathbb{Z}_p$ (if $p>0$) or isomorphic to field of rational numbers (if $p=0$).

Pf: Case 1: if $p>0$

$Char(F) = p$

then p is prime [$\because$ characteristic of an I.D is either prime or 0)

And F being a field is a ring then By Corollary 1, F has a subring isomorphic to $\mathbb{Z}_p$ and as p is prime.

$\mathbb{Z}_p$ is a field.

$\Rightarrow \mathbb{Z}_p$ is subfield which is isomorphic to a subfield of F.

Case 2: If $p=0$

Then, by corollary 1, F has a subring which is isomorphic to $\mathbb{Z}$.

i.e. $\underset{\text{subring}}{S \subseteq F}$ & $S \approx \mathbb{Z}$

Define : $T = \{ab^{-1} \mid a,b \in \mathbb{Z}\}$

then T is subfield of F.

let $a_1b_1^{-1}$ & $a_2b_2^{-1} \in T$

Page No.:
Date: / /

$$a_1b_1^{-1} + a_2b_2^{-1} = (a_1b_2 + a_2b_1)(b_1^{-1}b_2^{-1})$$
$$(a_1b_1^{-1})\cdot(a_2b_2^{-1}) = (a_1a_2)(b_1b_2)^{-1}$$

We need to show that $T \approx \mathbb{Q} \to$ set of rationals
Define $\phi : T \to \mathbb{Q}$ as set of rationals.

$$\phi(ab^{-1}) = \frac{a}{b}$$

Then ϕ is isomorphism (?)
Then F has a subfield which is isomorphic to $\mathbb{Q}$.

-2020

Field of Quotients:

5.6 Let D be an I.D. ~~Define F=~~ Then there exists a field F that contains a subring isomorphic to D.

Proof: Let $S = \left\{ \frac{a}{b} ; a, b \in D, b \neq 0 \right\}$

Define a relation $\sim$ on S as

$$\frac{a}{b} \sim \frac{c}{d} \text{ iff } ad = bc.$$

then '$\sim$' is an equivalence relation.

Reflexive: $\frac{a}{b} \sim \frac{a}{b}$ as $ab = ba$ [D is I.D] $\Rightarrow$ Commutative

Symmetric: Let $\frac{a}{b} \sim \frac{c}{d} \Rightarrow ad = bc$.

To show $\frac{c}{d} \sim \frac{a}{b}$

As $ad = bc$
$\Rightarrow da = cb$
$\Rightarrow \frac{c}{d} \sim \frac{a}{b}.$

Page No.:
Date: / /

Transitive: let $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in S$

s.t. $\frac{a}{b} \sim \frac{c}{d}$ and $\frac{c}{d} \sim \frac{e}{f}$ — ①

$\Rightarrow ad = bc$ and $\Rightarrow cf = de$

To show: $\frac{a}{b} \sim \frac{e}{f}$, i.e. $af = be$

As $cf = de$

$\Rightarrow adcf = bcde$

$\Rightarrow af = be$ [D is I.D. $\Rightarrow$ cancellation is possible]

$\Rightarrow$ '$\sim$' is an equivalence relation.

Define F be the set of equivalence classes of S and let $\left[\frac{a}{b}\right]$ denotes the equivalence class of $\frac{a}{b}$.

Define following operations on F

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad+bc}{bd}\right]$$

$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right] \quad ②$$

let $\frac{a}{b} \approx \frac{a'}{b'}$ and $\frac{c}{d} \approx \frac{c'}{d'}$

To show: $\frac{a}{b} + \frac{c}{d} \approx \frac{a'}{b'} + \frac{c'}{d'} \Rightarrow$ also $\frac{ad+bc}{bd} \approx \frac{a'd'+b'c'}{b'd'}$

$\frac{a}{b} \cdot \frac{c}{d} \approx \frac{a'}{b'} \cdot \frac{c'}{d'} \Rightarrow \frac{ac}{bd} \approx \frac{a'c'}{b'd'}$

$\Rightarrow (ac) b'd' = bda'c'$

$\frac{a}{b} \approx \frac{a'}{b'}$ and $\frac{c}{d} \approx \frac{c'}{d'}$

$\Rightarrow ab' = ba'$ $\Rightarrow cd' = dc'$

Page No.:
Date: / /

Consider $(ad+bc)b'd' = adb'd' + bcb'd'$
$= ab'dd' + cd'bb'$
$= ba'dd' + dc'bb'$
$= a'd'bd + b'c'bd$
$(ad+bc)b'd' = (a'd'+b'c')bd$

$\Rightarrow \dfrac{ad+bc}{bd} \approx \dfrac{a'd'+b'c'}{b'd'}$

$\Rightarrow \dfrac{a}{b} + \dfrac{c}{d} \approx \dfrac{a'}{b'} + \dfrac{c'}{d'}$

Now, consider $acb'd' = ab'cd'$
$= ba'dc'$
$acb'd' = bda'c'$

$\Rightarrow \dfrac{ac}{bd} \approx \dfrac{a'c'}{b'd'}$

$\Rightarrow \dfrac{a}{b} \cdot \dfrac{c}{d} \approx \dfrac{a'}{b'} \cdot \dfrac{c'}{d'}$

$\Rightarrow$ '.' , '+' are well defined.

Show that F is a field under operation $\oplus$.
Additive identity $= \left[\dfrac{0}{1}\right]$

Additive Inverse of $\left[\dfrac{a}{b}\right] = \left[\dfrac{-a}{b}\right]$

Multiplicative identity $= \left[\dfrac{1}{1}\right]$

Multiplicative inverse of $\left[\dfrac{a}{b}\right] = \left[\dfrac{b}{a}\right]$

0 – additive identity of D
1 – multiplicative identity of D.

& Check other properties.

Page No.
Date

distributive: $\left(\left[\frac{a}{b}\right]+\left[\frac{c}{d}\right]\right)\cdot\left[\frac{e}{f}\right] = \left(\left[\frac{ad+bc}{bd}\right]\right)\cdot\left[\frac{e}{f}\right]$

$$= \left[\frac{(ad)e+(bc)e}{(bd)f}\right]$$

$$\left[\frac{a}{b}\right]\cdot\left[\frac{e}{f}\right]+\left[\frac{c}{d}\right]\cdot\left[\frac{e}{f}\right] = \left[\frac{ae}{bf}\right]+\left[\frac{ce}{df}\right]$$

$$= \left[\frac{aedf+cebf}{bfdf}\right]$$

$$= \left[\frac{(ad+bc)ef}{bdff}\right] \approx \left[\frac{(ad+bc)e}{bdf}\right]$$

Now, Define $\phi : D \longrightarrow F$ as $\phi(x) = \left[\frac{x}{1}\right]$

Check ϕ is ring homo. and $\ker\phi = \{0\}$. (?)

Then By 1st Iso Thm.

$$\frac{D}{\ker\phi} \approx \phi(D)$$

$$\Rightarrow D \approx \phi(D) \subseteq F.$$

Ex 1. $D = \mathbb{Z}[x]$, then Quotient field of D is

$F = \left\{ \frac{f(x)}{g(x)} \, , \, f(x), g(x) \in D. \; g(x) \neq 0 \right\}$.

Q.3 (a) Is $2\mathbb{Z}$ isomorphic to $3\mathbb{Z}$?

(b) Is $2\mathbb{Z}$ isomorphic to $4\mathbb{Z}$?

Q.12 Let ϕ be a ring homo from $\mathbb{Z}_n$ to $\mathbb{Z}_m$. Prove that $\phi(1)$ is idempotent of $\mathbb{Z}_m$ (i.e $[\phi(1)]^2 = \phi(1)$).

Q.14 Determine all ring homo from $\mathbb{Z}_6$ to $\mathbb{Z}_6$.

" " " " " $\mathbb{Z}_{20}$ to $\mathbb{Z}_{20}$.

Page No.:
Date: / /

Q.15 Determine all ring homo from $\mathbb{Z}$ to $\mathbb{Z}$.

3.(a) Define $\phi : 2\mathbb{Z} \longrightarrow 3\mathbb{Z}$ as

$$\phi(x) = 3x.$$

let $\phi(x_1) = \phi(x_2)$

$$3x_1 = 3x_2$$

$$x_1 = x_2$$

$\therefore$ ϕ is (1-1)

let $z \in 3\mathbb{Z}$

$\Rightarrow z = 3(x) \quad \exists \quad \phi(x) = z.$

$\therefore$ ϕ is onto.

let $x, y \in 2\mathbb{Z}$

$$\Rightarrow \phi(x+y) = 3(x+y)$$

$$= 3x + 3y$$

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

$$\phi(x \cdot y) = 3(xy)$$

$$\neq \phi(x) \cdot \phi(y)$$

No. $2\mathbb{Z}$ is not isomorphic to $3\mathbb{Z}$.

b) No.

12. $\phi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$

$\phi(1) = \phi(1 \cdot 1) = \phi(1) \cdot \phi(1)$ $\quad$ ($\because \phi$ is homo)

$$= (\phi(1))^2$$

14. $\phi : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_6$.

$\phi(x) = ax$ $\quad$ for some a.

$\Rightarrow \phi(1) = a$

for ϕ be an homo $a^2 = a$ $\quad$ (from Q12).

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

as $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9 = 3$, $4^2 = 16 = 4$,

$5^2 = 25 = 1$

for ϕ be an homo $a^2 = a$
possibilities for a are $0, 1, 3 \& 4$
$\therefore$ there are 4 homo from $\mathbb{Z}_6 \to \mathbb{Z}_6$.

b) $\phi: \mathbb{Z}_{20} \longrightarrow \mathbb{Z}_{30}$
$\phi(x) = ax$
$\phi(1) = a$
then $a^2 = a$ as ϕ is ring homo
$\mathbb{Z}_{30} = \{0, 1, 2, \ldots, 29\}$
possibilities of a are ~~0, 1, 2, 4, 5, 10, 20, 6,~~
Then $a = 0, 1,$

15. $\phi: \mathbb{Z} \longrightarrow \mathbb{Z}$
$\phi(x) = ax$
Then $a^2 = a$ ($\because \phi$ is ring homo).
Then $\phi(x) = 0$
and $\phi(x) = 1$ are two ring homo from $\mathbb{Z}$ to $\mathbb{Z}$

Q. Determine all ring homo from $\mathbb{Z}_4$ to $\mathbb{Z}_6$
$\phi: \mathbb{Z}_4 \longrightarrow \mathbb{Z}_6$
$\phi(x) = ax$ $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.
$\phi(1) = a$
Then $a^2 = a$.
possibilities of $a = 0, 1, 3$.
$\therefore$ There are two ring homo from $\mathbb{Z}_4 \to \mathbb{Z}_6$.
$\phi(x) = 0$
$\phi(x) = 3x$.

Page No.:
Date: / /

Q.29. Let R and S be commutative ring with unity. If $\phi : R \xrightarrow{\text{onto}} S$ is ring homo. The characteristic of R is non-zero. Prove that characteristic of S divides char(R).

Proof: As $\phi : R \to S$ is onto & homo
Let e & 1 be the unity of R and S respectively.
Now, for $1 \in S$, $\exists\ x \in R$ s.t.

$$\phi(x) = 1$$

Let char(R) = n, $n > 0$
To show: char(S) | n.
As ϕ is homo $\phi(0) = 0$.

$$\phi(nx) = 0$$

$$\phi(\underbrace{x + x + \dots + x}_{n \text{ times}}) = 0$$

$$\Rightarrow \phi(x) + \phi(x) + \dots + \phi(x) = 0$$

$$\Rightarrow 1 + 1 + \dots + 1 = 0$$

$$\Rightarrow n \cdot 1 = 0.$$

then, char(S) $\leq n$.
$\Rightarrow$ char(S) | n.

Q.30. $R \to$ commutative ring with unity.
& char(R) = p - prime no.

$\phi : R \to R$
$\phi(x) = x^p$

Show that ϕ is ring homo.

$\rightarrow$ Let $x, y \in \phi$
Consider $\phi(x+y) = (x+y)^p$

$$= {}^pC_0 x^p + {}^pC_1 x^{p-1} y + \dots + {}^pC_p y^p$$

$$= x^p + y^p$$

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

Also char(R) = p
$p \cdot x = 0$
$\forall x \in R$

$\phi(xy) = (xy)^p$
$= (xy)(xy) \cdots (xy)$
$= x^p y^p$
$= \phi(x) \cdot \phi(y)$
$\therefore \phi$ is a ring homo.

Q 32. Show that a homo from a field onto a ring with more than one element must be an isomorphism.

$\rightarrow$ $\phi : F \xrightarrow[\text{homo}]{\text{onto}} S$
To show: ϕ is isomorphism (i.e. ϕ is 1-1).
$\ker \phi = \{ y \in F \mid \phi(y) = 0 \}$
Let $s \in S$ be a non-zero element.
$\exists$ $x \in F$ s.t. $\phi(x) = s$.
We will show that $\ker \phi = \{0\}$.
Let $z \in \ker\phi$ & $z \neq 0$.
$\Rightarrow \phi(z) = 0$

$\phi(x) = \phi(1 \cdot x) = \phi(z \cdot z^{-1} \cdot x)$ ($\because F$ is a field)
$= \phi(z) \cdot \phi(z^{-1}x)$ (ϕ is homo)
$= 0 \cdot \phi(z^{-1}x)$
$= 0.$

Contradiction.
$\Rightarrow \ker\phi = \{0\}$
$\Rightarrow \phi$ is 1-1
$\Rightarrow \phi$ is iso.

Q 45. $D \rightarrow$ I.D. Let F be the field of quotients of D. Show that if E is any field that contains D, then E contains a subfield isomorphic to F.

Page No.:
Date: / /

$\rightarrow$ $D \subseteq E \rightarrow$ field

$D \subseteq F \rightarrow$ Quotient field . $\{ \frac{a}{b} \mid a, b \in D, b \neq 0 \}$

To show: $F \approx S \subseteq E$.

Define $S = \{ ab^{-1} \mid a, b \in D, b \neq 0 \}$

$\phi : S \rightarrow F$ as

$\phi(ab^{-1}) = \frac{a}{b}$ isomorphism.

$\Rightarrow$ ~~S~~ $F \approx S \subseteq D \subseteq E$

$\Rightarrow F \approx S \subseteq E$.

Note: For an I.D D, its field of quotients is the smallest field ~~in~~ containing D.

Ch-12

Guidelines

Q45 Proof: $D \subseteq E \rightarrow$ field

$D \subseteq F \rightarrow$ quotient field $\{ \frac{a}{b} \mid a, b \in D, b \neq 0 \}$

To show: $F \approx S \subseteq E$

Define: $S = \{ ab^{-1} \mid a, b \in D, b \neq 0 \}$

$\phi : S \rightarrow F$ as

$\phi(ab^{-1}) = \frac{a}{b}$ (isomorphism)

Q29. $(a+b)$ is unit in R (commutative)

$a \rightarrow$ unit $b^2 = 0$

$\rightarrow$ let $c = a^{-1} - a^{-2}b$

then $c \in R$

and $c(a+b) = (a^{-1} - a^{-2}b)(a+b)$

$= a^{-1}a + a^{-1}b - a^{-1}b - a^{-2}b^2 = 1$

llly $(a+b)c = 1$

$\therefore$ c is inverse of $a+b$

$\Rightarrow$ ~~$\exists$~~ $(a+b)$ is unit in R.