*) Ring homomorphism

Let, $\langle R, +, \cdot \rangle$ and $\langle R', *, \circ \rangle$ be two rings. A mapping $f$ from $R$ to $R'$,

$$f : R \to R'$$

is said to be a homomorphism if

$$f(a+b) = f(a) * f(b) \text{ and}$$
$$f(ab) = f(a) \circ f(b), \forall a, b \in R$$

~~For si~~

Note, For simplicity we write

$$f(a+b) = f(a) + f(b) \text{ and}$$
$$f(ab) = f(a) f(b) \quad \forall a, b \in R$$

Ex: $f : \mathbb{Z} \longrightarrow \mathbb{Z}$

$$f(x) = x \quad \forall x \in \mathbb{Z}$$

Sol^n Let, $a, b \in \mathbb{Z}$

$$f(a+b) = a+b$$
$$= f(a) + f(b)$$
$$f(ab) = ab$$
$$= f(a) f(b)$$

$\therefore f$ is a homomorphism

**Ex:** $f : \mathbb{Q} \to \mathbb{Q}$

$$f(x) = \frac{x}{2}$$

**Sol$^n$:** Let, $a, b \in \mathbb{Q}$

$$f(a+b) = \frac{a+b}{2}$$

$$= \frac{a}{2} + \frac{b}{2}$$

$$\cancel{= f\left(\frac{a}{2}\right) + f\left(\frac{b}{2}\right)}$$

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

$$f(ab) = \frac{ab}{2} \neq \frac{a}{2} \cdot \frac{b}{2}$$

which is not a homomorphism

**Ex:** $f : \mathbb{C} \to \mathbb{C}$

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

**Sol$^n$:** Let, $a+ib,\ c+id \in \mathbb{C}$

$$f\big((a+ib)+(c+id)\big)$$

$$= f\big((a+c) + i(b+d)\big) = (a+c) - i(b+d)$$

$$= (a-ib) + (c-id)$$

$$= f(a+ib) + f(c+id)$$

$$f\big((a+ib).(c+id)\big)$$

$$= f\big((ac-bd) + i(ad+bc)\big) = (ac-bd) - i(ad+bc)$$

$$= (a-ib)(c-id)$$

$$= f(a+ib)\, f(c+id)$$

$\therefore f$ is a homomorphism

## Theorem

If $f: R \to R'$ is a homomorphism then

a) $f(0) = 0'$ [$0, 0'$ are the identities of $R$ and $R'$ respectively]

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

**Proof:** We know that,

$$0 + 0 = 0$$

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

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

$$\Rightarrow f(0) = 0' \text{ [left cancellation]}$$

b) We know that

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

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

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

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

**Defn** Kernel of a homomorphism:

Let, $f: R \to R'$ be a homomorphism the kernel of $f$ is denoted by $\operatorname{Ker}(f)$ and is defined as -

$$\operatorname{Ker}(f) = \{x \in R : f(x) = 0'\}$$

Defn:- (Kernel of a homomorphism):-

Let $f: R \to R'$ be a homomorphism the kernel of $f$ is denoted by $\ker(f)$ and is defined as $\ker(f) = \{x \in R : f(x) = 0\}$

Note:- $\ker(f) \neq \phi$

as $f(0) = 0'$

$\therefore 0 \in \ker(f)$

#

Theorem:- $\ker(f) = \{0\}$ iff $f$ is one-one.

Proof:- Let $\ker(f) = \{0\}$.

let $a, b \in R$

Now, $f(a) = f(b)$

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

$\Rightarrow f(a) + f(-b) = 0$ $[\because f(-a) = -f(a)]$

$\Rightarrow f(a + (-b)) = 0$ $[\because f$ is a homomorphism$]$

$\Rightarrow a + (-b) = 0$ $[\because \ker(f) = \{0\}]$

$\Rightarrow a = b$

$\Rightarrow f$ is one-one.

Conversely, Let $f$ be one-one.

Let $x \in \ker(f)$

$\therefore f(x) = 0$

$\Rightarrow f(x) = f(0)$ $[\because f(0) = 0]$

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

$\Rightarrow \ker(f) = \{0\}$

#

**Theorem:-** For any homomorphism $f$, $Ker(f)$ is a ~~Ker(f~~ subring of $R$.

**Proof:-** ~~Let $Ker(f) = \{0\}$~~ $\{x$

Given $f: R \to R'$ is a homomorphism

To prove:- $Ker(f)$ is a subring of $R$.

Let, $a, b \in Ker(f)$

$\therefore f(a) = 0, \quad f(b) = 0$

Now,
$$
\begin{aligned}
f(a-b) &= f(a+(-b)) \\
&= f(a) + f(-b) \\
&= f(a) - f(b) \quad [\because f(-a) = -f(a)] \\
&= 0 - 0 \\
&= 0
\end{aligned}
$$

$\therefore a-b \in Ker(f)$.

Again,
$$
\begin{aligned}
f(ab) &= f(a) f(b) \\
&= 0 \cdot 0 \\
&= 0
\end{aligned}
$$

$\therefore ab \in Ker(f)$

Hence, $Ker(f)$ is a subring of $R$.

**Theorem:-** $Ker(f)$ is an ideal of $R$.

**Proof:-** Given $f: R \to R'$ is a homomorphism.

Let, $a, b \in Ker(f)$

$\therefore f(a) = 0, \quad f(b) = 0$

Now, $f(a-b) = f(a+(-b))$
$= f(a) + f(-b)$
$= f(a) - f(b)$ $[\because f(-a) = -f(a)]$
$= 0 - 0$
$= 0$

$\therefore a-b \in Ker(f)$.

Let $a \in Ker(f)$ and $r \in R$.
$\therefore f(ar) = f(a) \cdot f(r)$
$= 0 \cdot f(r)$
$= 0$

Similarly, $f(ra) = f(r) \cdot f(a)$
$= f(r) \cdot 0$
$= 0$.

$\therefore ar, ra \in Ker(f)$
Hence, $Ker(f)$ is an ideal of $R$.

* Isomorphism:- ($\cong$)

A homomorphism $f: R \to R$ is called an isomorphism if $f$ is - one-one and onto.

Eg: (1) $f: \mathbb{Z} \to \mathbb{Z}$
$f(x) = x \ \forall \ x \in \mathbb{Z}$, Here $Ker(f) = 0$

(2) $f: \mathbb{R} - \mathbb{R}$
$f(x) = 0$
$f(x+y) = 0$

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

$\Rightarrow \cancel{f(x+}= f(x) + f(y)$

$f(xy) = 0 = 0 \cdot 0$

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

This is not a isomorphism

$\because \ker(f) = \mathbb{R}$

Theorem:— If $f \to \mathbb{R} \to \mathbb{R}'$ is an onto homomorphism and $R$ is a ring of unity then $f(1)$ is the unity of $R'$

Proof:- Let $a' \in R'$ be any element.

$\because a' \in R'$,

$\therefore \exists\, a \in R$ such that $f(a) = a'$ [$\because f$ is onto]

Now $a' \cdot f(1) = f(a) \cdot f(1) = f(a \cdot 1) = f(a) = a'$

Similarly,

$f(1) \cdot a' = f(1) f(a) = f(1 \cdot a) = f(a) = a'$

$\therefore f(1)$ is the unity of $R'$.

Q. Give an example of a ring homomorphism $f: R \to R'$ where $1$ is the unity of $R$ but $f(1)$ is not the unity of $R'$.

Sol$^n$: $f: R \to \mathbb{R}$

$f(x) = 0$.

$f(1) = 0$

**Theorem:-** For any +ve integer $m, n$ $m\mathbb{Z} \cong n\mathbb{Z}$ iff $m = n$

**Proof:-** ~~Let f : mZ~~

Let $f : m\mathbb{Z} \to n\mathbb{Z}$ be an isomorphism.

$$\therefore f(\underbrace{m + m + \cdots + m}_{m\text{-times}}) = \underbrace{f(m) + f(m) + f(m) + \cdots + f(m)}_{m\text{-times}}$$

$$\Rightarrow f(m \cdot m) = m f(m)$$

$$\Rightarrow f(m) \cdot f(m) = m f(m) \quad [\because f \text{ is an isomorphism and } \ker(f) = \{0\}]$$

$$\Rightarrow f(m) = m \longrightarrow (\text{I})$$

Since, $f$ is onto

~~There~~

$\therefore \exists\, mr \in m\mathbb{Z}$

such that $f(mr) = n$

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

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

$$\Rightarrow r f(m) = n$$

$$\Rightarrow f(m) \mid n \longrightarrow (\text{II})$$

Again as $m \in m\mathbb{Z}$

$\therefore f(m) \in n\mathbb{Z}$

$\therefore \exists\, k \in \mathbb{Z}$ such that

$$f(m) = nk$$

$$\Rightarrow n \mid f(m) \longrightarrow (\text{III})$$

$\therefore$ From (ii) and (iii), we have

$f(m) = n$ —— (iv)

$\therefore$ From (i) and (iv) we have,

$m = n$ [$\because f$ is a funct$^n$].

Conversely, let $m = n$.

define $f : m\mathbb{Z} \to m\mathbb{Z}$.

by $f(x) = x \ \forall \ x \in m\mathbb{Z}$

$\therefore$ ~~$m\mathbb{Z} \cong \mathbb{Z}$~~

Theorem:- (The fundamental theorem ~~for~~ of ring homomorphism.)

If $f : R \to R'$ be an onto homomorphism then $R'$ is isomorphic to a quotient ring of $R$, infact —

$$R' \cong \frac{R}{\mathrm{Ker} f}$$

Proof:- Let $f : R \to R'$ be an onto homomorphism

Define a mapping $\phi$ as

$\phi : \frac{R}{\mathrm{ker} f} \to R'$ such that

$\phi(x + I) = f(x)$, $x \in R$ and $I = \mathrm{ker} f$

Well-defined:-

Let, ~~$x + I = y + I$~~

$x + I, \ y + I \in \frac{R}{\mathrm{Ker} f}$ and

Let $x + I = y + I$

$\Rightarrow x - y \in I = \mathrm{ker} f$ [$\because aH = bH \Rightarrow ab^{-1} \in H$; $a + H = b + H \Rightarrow a - b \in H$]

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

$\Rightarrow f(x) - f(y) = 0$ [$\because f$ is homomorphism]

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

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

$\therefore \phi$ is well defined.

Homomorphism :—

Let $a = x+I$, $b = y+I$.

$\therefore a+b = (x+I)+(y+I)$

$= (x+y)+I$

$\therefore \phi(a+b) = \phi((x+y)+I)$

$= f(x+y)$

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

~~$\phi$ is one-one :—~~

~~Let, $f(x) = f(y)$~~

~~$\therefore \phi(a\,b) =$~~

Now, $a.b = (x+I)(y+I)$

$= xy+I$

$\phi(ab) = \phi(xy+I)$

$= f(xy)$

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

$= \phi(a).\phi(b)$. $\therefore \phi$ is homomorphism

$\phi$ is one-one :—

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

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

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

$\Rightarrow f(x-y) = 0$ [$\because f$ is homomorphism]

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

$\Rightarrow x + I = y + I.$

$\therefore \phi$ is one-one.

$\phi$ is onto:-

Let $y' \in R'$ be any element

~~$\exists\, x \in R'$ such that~~

Since, $f$ is onto., therefore

$\exists\, y \in R$ such that $f(y) = y'$

$\Rightarrow \phi(y+I) = y'$

$\therefore \phi$ is onto.

Hence, $\phi$ is an isomorphism.

$$\therefore \frac{R}{\ker f} \cong R'$$

Q. Let $I$ be an ideal of a ring $R$, then show that

(a) If $R$ is commutative then $\frac{R}{I}$ is also commutative

(b) If $1$ is the unity of $R$, then $1+I$ is the unity of $R/I$

Proof:- (a) ~~Let $a, b \in R$~~ ~~$a, b \in I$~~

Page - 367
368

Let, $a+I$, $b+I \in \frac{R}{I}$ be any two elements, where $a, b \in R$

Now $(a+I)(b+I) = ab + I$
$= ba + I$ [$\because R$ is commutative]
$= (b+I)(a+I)$

$\because a+I$, $b+I$ are any two arbitary elements in $R/I$, therefor $\frac{R}{I}$ is commutative

Let $a+I \in \frac{R}{I}$ be any element

~~$\because a+I$~~
~~$\exists a \in R$ such that~~

$\because 1 \in R$, $\therefore 1+I \in \frac{R}{I}$

$\therefore$ Now, $(a+I)(1+I) = a.1 + I = a+I$

and $(1+I)(a+I) = 1.a + I = a+I$ [$\because 1$ is unity of $R$]

Hence, $1+I$ is the unity of $R/I$.