STUDY MATERIALS

(RING THEORY-I)

TOPIC: HOMOMORPHISM

Mathematics Honours
Semester – 4

Paper – C10T Unit - 1

Dr. Sangita Chakraborty
Associate Professor
Department of Mathematics
Kharagpur College

Homomorphism of rings.

Let R and R' be two rings. A mapping $\phi: R \to R'$ is said to be a homomorphism if
(i) $\phi(a+b) = \phi(a) + \phi(b)$, (ii) $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$, $\forall a, b \in R$.

A ring homomorphism $\phi: R \to R'$ is called
(i) a monomorphism, if ϕ is injective;
(ii) an epimorphism, if ϕ is surjective;
(iii) an isomorphism, if ϕ is bijective.

Note: When ϕ is an isomorphism, $\phi^{-1}: R' \to R$ is also a bijection. We say that R and R' are said to be isomorphic rings and written as $R \simeq R'$.

Note: A ring homomorphism ϕ is, in particular, a group " from $(R,+)$ to $(R',+)$.
Hence $\phi(0_R) = 0_{R'}$, $\phi(-a) = -\phi(a)$, $a \in R$.
But, ϕ is not a multiplicative group homomorphism, since $(R-\{0\}, \cdot)$ and $(R'-\{0\}, \cdot)$ are not always groups.

Properties:

① Trivial ring homomorphism; Let R and R' be two rings and $\phi: R \to R'$ be defined by $\phi(r) = 0_{R'}$, $\forall r \in R$. ϕ is a homomorphism, $a+b \in R$ and $a \cdot b \in R$.
Because, for any $a, b \in R$,
$\therefore \phi(a+b) = 0_{R'} = 0_{R'} + 0_{R'} = \phi(a) + \phi(b)$
& $\phi(a \cdot b) = 0_{R'} = 0_{R'} \cdot 0_{R'} = \phi(a) \cdot \phi(b)$

② Let $R = (\mathbb{Z}, +, \cdot)$ and $\phi: R \to R$ be defined by $\phi(x) = 2x$, $x \in \mathbb{Z}$
Let $a, b \in \mathbb{Z}$, $\phi(a+b) = 2(a+b) = 2a + 2b = \phi(a) + \phi(b)$
$\phi(a \cdot b) = 2a \cdot b \neq 4ab = 2a \cdot 2b = \phi(a) \cdot \phi(b)$.
$\therefore \phi$ is not a homomorphism.

③ Let $R = (\mathbb{R}, +, \cdot)$ and $\phi: R \to R$ is defined by
$\phi(x) = |x|$, $x \in \mathbb{R}$
Let $a, b \in \mathbb{R}$. $\phi(a+b) = |a+b| \neq |a| + |b| = \phi(a) + \phi(b)$.
$\therefore \phi$ is not a homomorphism.
$\phi(a \cdot b) = |a \cdot b| = |a| \cdot |b|$.

④ Let $R = M_2(\mathbb{R})$, $R' = (\mathbb{R}, +, \cdot)$ and $\phi: R \to R'$ is defined by
$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \det\begin{bmatrix} a & b \\ c & d \end{bmatrix}$
$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} p & q \\ r & s \end{bmatrix}\right) = \det\begin{pmatrix} a+p & b+q \\ c+r & d+s \end{pmatrix}$
$= (a+p)(d+s) - (b+q)(c+r)$
$\neq \phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) + \phi\left(\begin{bmatrix} p & q \\ r & s \end{bmatrix}\right)$
$\therefore \phi$ is Not.

⑤ Let $R = \mathbb{Z}(\sqrt{2})$ and $\phi : R \to R$ is defined by --

$\phi(a+b\sqrt{2}) = a - b\sqrt{2}$.

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

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

$\phi((a+b\sqrt{2})\cdot(c+d\sqrt{2})) = \phi(\{ac+2bd\}+\sqrt{2}(bc+ad))$

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

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

$\therefore$ ϕ is a homomorphism

⑥ Let $R = (\mathbb{C}, +, \cdot)$ and $\phi : R \to R$ be defined by

$\phi(z) = \bar{z}$, $z \in \mathbb{C}$.

$\phi(z_1+z_2) = \overline{z_1+z_2} = \bar{z}_1 + \bar{z}_2 = \phi(z_1)+\phi(z_2)$, for $z_1, z_2 \in \mathbb{C}$

$\phi(z_1\cdot z_2) = \overline{z_1\cdot z_2} = \bar{z}_1\cdot\bar{z}_2 = \phi(z_1)\cdot\phi(z_2)$

$\therefore$ ϕ is a homomorphism, & ϕ is a bijection

hence ϕ is an isomorphism

Th: 1. Let R and R' be two rings and $\phi : R \to R'$ be a homomorphism. Then

(i) $\phi(0_R) = 0_{R'}$, (ii) $\phi(-a) = -\phi(a)$, $\forall a \in R$.

(i) In R, $0_R + 0_R = 0_R$

$\therefore$ $\phi(0_R+0_R) = \phi(0_R)$

or, $\phi(0_R) = \phi(0_R) + \phi(0_R)$, since ϕ is a homo---

or, $\phi(0_R) + 0_{R'} = \phi(0_R) + \phi(0_R)$

By left cancellation law for addition hold in $(R', +)$ group, we get $0_{R'} = \phi(0_R)$.

(ii) In the group $(R, +)$, for $a \in R$,

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

$\therefore$ $\phi(0_R) = \phi(a) + \phi(-a) = \phi(-a) + \phi(a)$

or, $0_{R'} = \phi(a) + \phi(-a) = \phi(-a) + \phi(a)$

$\Rightarrow$ $\phi(-a)$ is the additive inverse of $\phi(a)$ in R'.

$\therefore$ $\phi(-a) = -\phi(a)$.

Th: 2. Let R and R' be two rings and $\phi : R \to R'$ be an onto homo---. Then

(i) if R has a unity I, then R' has $\phi(I)$ as unity

(ii) if a be a unit in R, then $\phi(a)$ is a unit in R' and $[\phi(a)]^{-1} = \phi(a^{-1})$.

Proof: (i) Let $a' \in R'$. Since ϕ is onto, $\exists\, a \in R$ s.t. $\phi(a) = a'$.

We have $a \cdot I = I \cdot a = a$ in R.

$\therefore \phi(a \cdot I) = \phi(I \cdot a) = \phi(a)$

$\Rightarrow \phi(a) \cdot \phi(I) = \phi(I) \cdot \phi(a) = \phi(a)$, since ϕ is homo...

$\Rightarrow a' \cdot \phi(I) = \phi(I) \cdot a' = a'$ in R'. $\forall a' \in R'$.

$\Rightarrow \phi(I)$ is the unity in R'.

(ii) Since a is a unit in R, R is a ring with unity, say I.

$\therefore a^{-1} \in R$ s.t. $a \cdot a^{-1} = a^{-1} \cdot a = I$ in R.

$\Rightarrow \phi(a) \cdot \phi(a^{-1}) = \phi(a^{-1}) \cdot \phi(a) = \phi(I)$, unity in R' as ϕ is onto.

$\Rightarrow \phi(a)$ is a unit in R' and

$$[\phi(a)]^{-1} = \phi(a^{-1}).$$

Homomorphic Image:

Let R and R' be two rings and $\phi : R \to R'$ be a homomorphism. Then the set $\phi(R) = \{\phi(a) : a \in R\}$ $\subset R'$, is called the homomorphic image of R.

Th: Prove that $\phi(R)$ is a subring of R'.

$\phi(R)$ is a nonempty subset of R', since $0_{R'} = \phi(0_R) \in \phi(R)$.

Let $a' \in \phi(R)$, $b' \in \phi(R)$. Then $\exists$ a, b in R s.t.

$\phi(a) = a'$, $\phi(b) = b'$

Now $a' - b' = \phi(a) - \phi(b) = \phi(a) + \phi(-b) = \phi(a + (-b))$

$= \phi(a-b) \in \phi(R)$

and $a' \cdot b' = \phi(a) \cdot \phi(b) = \phi(a \cdot b) \in \phi(R)$.

$\therefore \phi(R)$ is a subring of R'

Th: Let R and R' be two rings and $\phi : R \to R'$ be an epimorphism (onto). If R be a commutative ring, then R' is commutative.

Let $a', b' \in R'$. Since ϕ is onto, $\exists$ $a, b \in R$ s.t.

$\phi(a) = a'$, $\phi(b) = b'$.

$a' \cdot b' = \phi(a) \cdot \phi(b) = \phi(a \cdot b) = \phi(b \cdot a)$, since R is commutative

$= \phi(b) \cdot \phi(a) = b' \cdot a'$.

$\Rightarrow R'$ is commutative.

The converse is NOT True:

Th: Let R and R' be two rings and $\phi : R \to R'$ be a homomorphism. Then

(i) if S be a subring of R, then $\phi(S)$ is a subring of R'.

(ii) if S' " " " " R', then $\phi^{-1}(S') = \{x \in R : \phi(x) \in S'\}$ is a subring of R.

Proof: (i) $\phi(S)$ is a non-empty subset of R', since

$0_{R'} = \phi(0_R) \in \phi(S)$

Let $a', b' \in \phi(S)$. Then $\exists$ $a, b \in S$ such that

$\phi(a) = a'$, $\phi(b) = b'$.

Since S is a subring of R, $a \in S, b \in S \Rightarrow a-b \in S$ and $a \cdot b \in S$.

$\therefore$ $\phi(a-b) \in \phi(S)$ and $\phi(a \cdot b) \in \phi(S)$

$\Rightarrow \phi(a) - \phi(b) \in \phi(S)$, and $\phi(a) \cdot \phi(b) \in \phi(S)$

$\Rightarrow a' - b' \in \phi(S)$ $\Rightarrow a' \cdot b' \in \phi(S)$.

$\therefore$ $\phi(S)$ is a subring of R'.

(ii) $\phi^{-1}(S')$ is a non-empty subset of R, since $0_{R'} \in S'$, S' being a subring of R'; Also $\phi(0_R) = 0_{R'}$.

$\therefore$ $0_R \in \phi^{-1}(S')$.

Let $a, b \in \phi^{-1}(S')$. Then $\phi(a) \in S'$, $\phi(b) \in S'$.

Since S' is a subring of R',

$\phi(a) - \phi(b) \in S'$ & $\phi(a) \cdot \phi(b) \in S'$

$\Rightarrow \phi(a-b) \in S'$, $\Rightarrow \phi(a \cdot b) \in S'$

$\Rightarrow a - b \in \phi^{-1}(S')$ $\Rightarrow a \cdot b \in \phi^{-1}(S')$

$\therefore$ $\phi^{-1}(S')$ is a subring of R.

Th: Let R and R' be two rings and $\phi : R \to R'$ be an onto homo... Then

(i) if U be an ideal of R, $\phi(U)$ is an ideal of R';

(ii) if U' " " " " R', $\phi^{-1}(U')$ " " " " R.

(i) Since U is an ideal of R, U is a subring of R

$\Rightarrow \phi(U)$ is a subring of R'.

Let $u' \in \phi(U)$, $r' \in R'$. Then $\exists$ $u \in U$, $r \in R$ s.t.

$\phi(u) = u'$, $\phi(r) = r'$

Since U is an ideal of R, $u \in U, r \in R \Rightarrow r.u \in U, u.r \in U$.

$\therefore$ $\phi(ru) \in \phi(U)$ and $\phi(ur) \in \phi(U)$

$\Rightarrow \phi(r) \cdot \phi(u) \in \phi(U)$; $\phi(u) \cdot \phi(r) \in \phi(U)$

a, $r'u' \in \phi(U)$ and $u' \cdot r' \in \phi(U)$

$\therefore$ $\phi(U)$ is an ideal of R'.

(ii) $\phi^{-1}(U')$ is a non-empty subset of R, since $0_{R'} \in U'$, U' being a subring of R', also $\phi(0_R) = 0_{R'}$

$\therefore$ $0_R \in \phi^{-1}(U')$.

Let $u_1, u_2 \in \phi^{-1}(U')$. Then $\phi(u_1) \in U'$, $\phi(u_2) \in U'$.

Since U' is a subring of R',

$\phi(u_1) - \phi(u_2) \in U'$ & $\phi(u_1) \cdot \phi(u_2) \in U'$

$\Rightarrow \phi(u_1 - u_2) \in U'$ $\Rightarrow \phi(u_1 \cdot u_2) \in U'$

$\Rightarrow u_1 - u_2 \in \phi^{-1}(U')$ $\Rightarrow u_1 \cdot u_2 \in \phi^{-1}(U')$.

$\therefore$ $\phi^{-1}(U')$ is a subring of R.

Since U' is an ideal of R', U' is a subring of R'

Then $\phi^{-1}(U')$ is a subring of R.

Let $u \in \phi^{-1}(U')$, $r \in R$. Then $\exists$ $u' \in U'$, $r' \in R'$ s.t. $\phi(u) = u'$, $\phi(r) = r'$.

Since U' is an ideal of R', $u' \in U'$, $r' \in R' \Rightarrow r' \cdot u' \in U'$ & $u' \cdot r' \in U'$.

$\therefore$ ~~$\phi(r' \cdot u') = \phi(r') \cdot \phi(u') \in U'$~~ & ~~$\phi(u' \cdot r') = \phi(u') \cdot \phi(r') \in U'$~~ $\therefore$ $\phi(r) \cdot \phi(u) \in U'$ & $\phi(u) \cdot \phi(r) \in U'$

a, $\phi(r \cdot u) \in U'$, $\phi(u \cdot r) \in U'$

a, $r \cdot u \in \phi^{-1}(U')$; $u \cdot r \in \phi^{-1}(U')$

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

<u>Note</u>: If $\phi : R \to R'$ be a ring homo... and U be an ideal of R then $\phi(U)$ is an ideal of $\phi(R)$ but may not be an ideal of R'.

~~eg~~. Let $R = \mathbb{Z}$, $R' = \mathbb{Z} \times \mathbb{Z}$ and $\phi : R \to R'$ be defined by $\phi(n) = (n, n)$: $n \in \mathbb{Z}$. (not onto).

Then ϕ is a homo...

$U = 2\mathbb{Z}$ is an ideal of R.

$\phi(2\mathbb{Z}) = \{(2n, 2n) : n \in \mathbb{Z}\}$ is not an ideal of R', since, $(2,2) \in \phi(2\mathbb{Z})$, $(1,3) \in R'$. But $(2,2)(1,3) = (2,6) \notin \phi(2\mathbb{Z})$.

Kernel of ϕ:

Let R and R' be two rings and $\phi: R \to R'$ be a homo...

$\text{Ker}\,\phi = \{a \in R : \phi(a) = 0_{R'}\} \subset R$.

Th: Let R and R' be two rings and $\phi: R - R'$ be a homo... Show that $\text{Ker}\,\phi$ is an ideal of R.

$\text{Ker}\,\phi$ is non-empty subset of R, because $0_R \in R$ and $\phi(0_R) = 0_{R'} \Rightarrow 0_R \in \text{Ker}\,\phi$.

Let $a, b \in \text{Ker}\,\phi$. Then $\phi(a) = 0_{R'} = \phi(b)$.

$\phi(a-b) = \phi(a + (-b)) = \phi(a) + \phi(-b) = \phi(a) - \phi(b) = 0_{R'}$

$\Rightarrow a - b \in \text{Ker}\,\phi$.

Let $r \in R$. Then $\phi(a \cdot r) = \phi(a) \cdot \phi(r) = 0_{R'} \cdot \phi(r) = 0_{R'}$

and $\phi(r \cdot a) = 0_{R'}$.

$\therefore a \in \text{Ker}\,\phi, r \in R \Rightarrow a \cdot r \in \text{Ker}\,\phi$, $r \cdot a \in \text{Ker}\,\phi$

$\therefore \text{Ker}\,\phi$ is an ideal of R.

Th: Let R and R' be two rings and $\phi: R \to R'$ be an onto homomorphism. Then ϕ is an isomorphism iff $\text{Ker}\,\phi = \{0_R\}$

Let ϕ be an isomor--- Then ϕ is one-to-one. We have $\phi(0_R) = 0_{R'} \Rightarrow 0_R$ is the only pre-image of $0_{R'}$

So $\text{Ker}\,\phi = \{0_R\}$.

Conversely, let $\text{Ker}\,\phi = \{0_R\}$.

Let $a, b \in R$ s.t. $\phi(a) = \phi(b)$

Then $\phi(a-b) = \phi(a) - \phi(b) = 0_{R'} \Rightarrow a - b \in \text{Ker}\,\phi$.

Since $\text{Ker}\,\phi = \{0_R\}$, $\therefore a - b = 0_R \Rightarrow a = b$.

$\Rightarrow \phi$ is one-to-one.

$\therefore \phi$ is an isomorphism.

Th Let U be an ideal of a ring R. Then the mapping $\theta : R \to R/U$ defined by $\theta(x) = x + U$, $x \in R$ is an onto homomorphism with kernel U.

Proof: Let $x, y \in R$. Then $\theta(x) = x + U$, $\theta(y) = y + U$

$\theta(x+y) = (x+y) + U = (x+U) + (y+U) = \theta(x) + \theta(y)$

$\theta(xy) = xy + U = (x+U) * (y+U) = \theta(x) * \theta(y)$

$\therefore$ θ is a homomorphism.

The zero element in the quotient ring R/U is U.

$Ker\,\theta = \{x \in R : \theta(x) = U\}$

$\theta(x) = U \Rightarrow x + U = U \Rightarrow x \in U$

$\therefore$ $Ker\,\theta = U$.

Fundamental theorem of ring homomorphism

Let ϕ be a homomorphism of a ring R onto a ring R' with kernel U. Then show that R' is isomorphic to the quotient ring R/U.

Let us define the map $\psi : R/U \to R'$ by

$\psi(a+U) = \phi(a)$, $a + U \in R/U$.

First to show that ψ is well-defined.

i.e., if $a' + U = a + U$, then $\psi(a'+U) = \psi(a+U) = \phi(a)$

$a' + U = a + U \Rightarrow a' - a \in U \Rightarrow \phi(a'-a) = 0'$ $\because Ker\,\phi = U$.

$\Rightarrow \phi(a') = \phi(a) \Rightarrow \psi(a'+U) = \phi(a)$

$\therefore$ ψ is well defined

Next to show that ψ is a homomorphism

$\psi[(a+U) + (b+U)] = \psi[(a+b) + U] = \phi(a+b)$

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

And $\psi[(a+U)(b+U)] = \psi[ab + U] = \phi(ab) = \phi(a)\phi(b)$

$= \psi(a+U)\,\psi(b+U)$

$\Rightarrow$ ψ is a homomorphism.

ψ is one-to-one, because

$\psi(a+U) = \psi(b+U) \Rightarrow \phi(a) = \phi(b) \Rightarrow \phi(a) - \phi(b) = 0'$

$\Rightarrow \phi(a-b) = 0' \Rightarrow a - b \in U$

$\Rightarrow a + U = b + U$.

Finally, ψ is onto, because, each element of R'

is of the form $\phi(a)$ for some $a \in R$, and since the pre-image of $\phi(a)$ is $a+U$ in R/U.

Thus ψ is an isomorphism and R/U is isomorphic to R',

Th: Let R and R' be two rings and $\phi: R \to R'$ be an onto homomorphism. Then ϕ is an isomorphism iff $\operatorname{Ker}\phi = \{0\}$.

Let ϕ be an iso....

Then ϕ is one-to-one.

we have $\phi(0) = 0' \Rightarrow 0'$ has a pre-image 0.

Since ϕ is one-to-one, 0 is the only pre-image of $0'$.

So $\operatorname{Ker}\phi = \{0\}$.

Conversely, let $\operatorname{Ker}\phi = \{0\}$.

Let $a, b \in R$ s.t. $\phi(a) = \phi(b)$

Then $\phi(a-b) = \phi(a) - \phi(b) = 0'$

$\Rightarrow a-b \in \operatorname{Ker}\phi$

$\Rightarrow a-b = 0 \Rightarrow a=b$.

$\therefore \phi$ is one-to-one & onto also.

$\therefore \phi$ is an isomorphism

$\operatorname{Ker}\phi = \{a \in R : \phi(a) = 0'\}$, where $\phi: R \to R'$ be a homomorphism.

Theorem: Let R and R' be two rings and $\phi: R \to R'$ be a homo...., Then $\operatorname{Ker}\phi$ is an ideal of R

$\operatorname{Ker}\phi$ is a nonempty subset of R, because $0 \in \operatorname{Ker}\phi$.

Let $a, b \in \operatorname{Ker}\phi$. Then $\phi(a) = 0' = \phi(b)$

$\phi(a-b) = \phi(a+(-b)) = \phi(a) + \phi(-b) = \phi(a) - \phi(b) = 0'$

$\Rightarrow a-b \in \operatorname{Ker}\phi$.

Let $r \in R$. Then $\phi(a \cdot r) = \phi(a) \cdot \phi(r) = 0'$. $\phi(r) = 0'$

and $\phi(r \cdot a) = 0'$

$\therefore a \cdot r \in \operatorname{Ker}\phi$ & $r \cdot a \in \operatorname{Ker}\phi$.

$\therefore \operatorname{Ker}\phi$ is an ideal of R.

2. Let $\phi : R \to R'$ be a ring homomorphism. Prove that
(i) $\phi(na) = n\phi(a)$, $\forall a \in R$ and $\forall n \in \mathbb{Z}$;
(ii) $\phi(a^n) = [\phi(a)]^n$, $\forall a \in R$ and $\forall n \in \mathbb{N}$.

Solution;

(i) Since ϕ is a homomorphism,
Let $n \in \mathbb{Z}^+$, $\phi(na) = \phi(a + a + \cdots n \text{ times})$
$= \phi(a) + \phi(a) + \cdots n$ times,
$= n\phi(a)$, $\forall a \in R$ and $\forall n \in \mathbb{Z}^+$.

Let $n \in \mathbb{Z}^-$, let $n = -m$ $(m \in \mathbb{Z}^+)$, then
$\phi(na) = \phi(-m a) = \phi[\boxed{(-a)} + (-a) + \cdots m \text{ times}]$
$= \phi(-a) + \phi(-a) + \cdots m$ times
$= \{-\phi(a)\} + \{-\phi(a)\} + \cdots m$ times
$= -m\phi(a) = n\phi(a)$, $\forall a \in R$, $\forall n \in \mathbb{Z}^-$

when $n = 0$, $\phi(na) = \phi(0.a) = \phi(0) = 0' = 0.\phi(a)$
$= n.\phi(a)$, $\forall a \in R$.

$\therefore$ $\phi(na) = n\phi(a)$, $\forall a \in R$ and $\forall n \in \mathbb{Z}$.

(ii) Since ϕ is a ring homomorphism,
$\phi(a^n) = \phi(a.a.\cdots n \text{ times})$, $\forall n \in \mathbb{N}$
$= \phi(a)\cdot\phi(a)\cdots n$ times
$= [\phi(a)]^n$, $\forall a \in R$, $\forall n \in \mathbb{N}$.

3. (i) Prove that the rings $\mathbb{Z}$ and $2\mathbb{Z}$ are not isomorphic.
(ii) " " " " $\mathbb{Z}$ " $\mathbb{Z}\times\mathbb{Z}$ " " "

(i) We know that —
Every isomorphic image of an I.D. is an I.D.
Here the ring $(\mathbb{Z})$ contains no divisors of zero, and is an I.D.
However the ring $(2\mathbb{Z}, +, \cdot)$ does not contains the identity element (Unity)
hence it is not an I.D.
Rings $\mathbb{Z}$ and $2\mathbb{Z}$ are not isomorphic.

(ii) Here $\mathbb{Z}\times\mathbb{Z}$ is a ring with divisors of zero;
eg. Let $(0,1) \in \mathbb{Z}\times\mathbb{Z}$ and $(1,0) \in \mathbb{Z}\times\mathbb{Z}$ be two non-zero elements. And $(0,1)\cdot(1,0) = (0,0)$.
$\therefore$ $\mathbb{Z}\times\mathbb{Z}$ is not an I.D, whereas $\mathbb{Z}$ is an I.D.
$\therefore$ The rings $\mathbb{Z}$ and $\mathbb{Z}\times\mathbb{Z}$ are not isomorphic.

Exercises on Ring Homomorphisms

from S.K. Mapa : Ex-24.

1. Which of the following are ring homomorphisms?

(i) Let $R = (\mathbb{R}, +, \cdot)$ and $\phi : R \to R$ is defined by $\phi(x) = |x|, x \in \mathbb{R}$.

(ii) Let $R = M_2(\mathbb{R})$, $R' = (\mathbb{R}, +, \cdot)$ and $\phi : R \to R'$ is defined by $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \det \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R})$

(iii) Let $R = \mathbb{Z}(\sqrt{2})$ and $\phi : R \to R$ defined by $\phi(a + b\sqrt{2}) = a - b\sqrt{2}$, $a + b\sqrt{2} \in \mathbb{Z}(\sqrt{2})$.

Solution:

(i) Let $a, b \in \mathbb{R}$. Then $a+b \in \mathbb{R}$, $a \cdot b \in \mathbb{R}$.

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

$\therefore$ ϕ is not a ring homomorphism.

eg. Let $a = -3$, $b = 2$, then $|a+b| = |-3+2| = 1$.

But $|a| + |b| = |-3| + |2| = 3 + 2 = 5$.

(ii) Let $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R})$ & $Y = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in M_2(\mathbb{R})$.

$\therefore X + Y \in M_2(\mathbb{R})$, $XY \in M_2(\mathbb{R})$.

Now $\phi(X+Y) = \det(X+Y) = \det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} p & q \\ r & s \end{bmatrix}\right)$

$= \det\left(\begin{bmatrix} a+p & b+q \\ c+r & d+s \end{bmatrix}\right)$.

$= (a+p)(d+s) - (b+q)(c+r)$.

$\phi(X) + \phi(Y) = \det(X) + \det(Y)$

$= (ad - bc) + (ps - qr)$

$\neq \phi(X+Y)$

$\therefore$ ϕ is not a ring homomorphism.

(iii) Let $a + b\sqrt{2} \in \mathbb{Z}(\sqrt{2})$ and $c + d\sqrt{2} \in \mathbb{Z}(\sqrt{2})$.

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

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

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

Also, $\phi[(a+b\sqrt{2}) \cdot (c+d\sqrt{2})] = \phi[(ac+2bd) + (bc+ad)\sqrt{2}]$

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

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

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

$\therefore$ ϕ is a ring homomorphism.

First law of isomorphism :-

Let ϕ be a homomorphism of a ring R onto a ring R' with kernel U. Then U is an ideal of R and R' is isomorphic to the quotient ring R/U.

Proof: First to show that $U = \text{Ker}\,\phi (\subseteq R)$ is an ideal.

$\text{Ker}\,\phi = \{a \in R ;\ \phi(a) = 0'\}$.

Let $a, b \in U$. Then $\phi(a) = 0' = \phi(b)$

$\therefore\ \phi(a-b) = \phi(a) + \phi(-b) = \phi(a) - \phi(b) = 0'$

$\Rightarrow\ a - b \in U$ ——— (i)

Also, if $u \in U, r \in R$, then $\phi(u.r) = \phi(u).\phi(r) = 0'.\phi(r) = 0'$

and $\phi(r.u) = \phi(r).\phi(u) = \phi(r).0' = 0'$.

$\Rightarrow\ u.r \in U$ and $r.u \in U$ ——— (ii)

(i) & (ii) together prove that U is an ideal of R.

Therefore, quotient ring R/U exists.

Let us define a mapping $\psi : R/U \to R'$ by

$\psi(a+U) = \phi(a),\quad a+U \in R/U$.

First to show that ψ is well defined,

i.e, if $a'+U = a+U$, then $\psi(a'+U) = \psi(a+U) = \phi(a)$.

Now $a'+U = a+U \Rightarrow a'-a \in U \Rightarrow \phi(a'-a) = 0'$ [$\because \text{Ker}\,\phi = U$]

$\Rightarrow \phi(a') = \phi(a) \Rightarrow \psi(a'+U) = \phi(a)$.

$\therefore\ \psi$ is well defined — proved.

Next to show that ψ is a homomorphism

$\psi[(a+U)+(b+U)] = \psi[(a+b)+U] = \phi(a+b) = \phi(a)+\phi(b)$

$= \psi(a+U) + \psi(b+U)$ ---- (iii)

And $\psi[(a+U).(b+U)] = \psi[a.b+U] = \phi(a.b) = \phi(a).\phi(b)$

$= \psi(a+U).\psi(b+U)$ --- (iv)

(iii) & (iv) show that ψ is a homomorphism.

ψ is one-one, because, $\psi(a+U) = \psi(b+U)$

$\Rightarrow \phi(a) = \phi(b) \Rightarrow \phi(a) - \phi(b) = 0'$

$\Rightarrow \phi(a-b) = 0' \Rightarrow a-b \in U$

$\Rightarrow a+U = b+U$.

ψ is onto, because, each element of R' is of the form $\phi(a)$ for some $a \in R$ and since the pre-image of $\phi(a)$ is $a+U \in R/U$.

$\therefore\ \psi$ is an isomorphism and R/U is isomorphic to R'.

Second law of isomorphism:

Let R be a ring and S, T be two ideals of R such that $S \subset T \subset R$, then $R/T \cong \frac{R/S}{T/S}$.

Proof: Since S & T are ideals of R and $S \subset T \subset R$, then R/S, R/T exist.

Let $r \in T$ and $s \in S$

$\Rightarrow r \in R, s \in S \Rightarrow r.s$ and $s.r \in S$ [$\because S$ is an ideal of R]

$\Rightarrow S$ is an ideal of $T \Rightarrow T/S$ exists.

Now $T/S \subset R/S$, since $a+S \in T/S \Rightarrow a \in T \Rightarrow a \in R$
$\Rightarrow a+S \in R/S$.

Also T/S is an ideal of R/S, since, for $a+S \in T/S$, $b+S \in T/S$

$\Rightarrow a \in T, b \in T \Rightarrow a-b \in T, a.b \in T$ [T being an ideal of R is a subring of R]

$\Rightarrow a-b \in R, a.b \in R$.

$\Rightarrow (a-b)+S \in R/S$, and $a.b+S \in R/S$

$\Rightarrow (a+S)-(b+S) \in R/S$ and $(a+S).(b+S) \in R/S$

$\Rightarrow T/S$ is a subring of R/S. ——— (i)

Also $a+S \in T/S$ and $r+S \in R/S$ for $r \in R$

$\Rightarrow a \in T, r \in R$

$\Rightarrow a.r \in T, r.a \in T$ [$\because T$ is an ideal of R]

$\Rightarrow a.r+S \in T/S$ and $r.a+S \in T/S$.

$\Rightarrow (a+S).(r+S) \in T/S$ and $(r+S).(a+S) \in T/S$ ——— (ii)

(i) & (ii) prove that T/S is an ideal of R/S

$\Rightarrow \frac{R/S}{T/S}$ exists.

We now define a mapping $\psi : R/S \to R/T$ by

$$\psi(a+S) = a+T, \quad \forall a \in R$$

$\therefore \psi[(a+S)+(b+S)] = \psi[(a+b)+S] = (a+b)+T$
$= (a+T)+(b+T)$
$= \psi(a+S)+\psi(b+S)$

And $\psi[(a+S).(b+S)] = \psi[a.b+S] = a.b+T$
$= (a+T).(b+T) = \psi(a+S).\psi(b+S)$

$\therefore R/T$ is a homomorphic image of R/S.
or, ψ " " homomorphism.

$\text{Ker}\,\psi = \{a+S \in R/S : \psi(a+S) = T$, the zero of $R/T\}$
$= \{a+S \in R/S : a+T = T\}$
$= \{a+S \in R/S : a \in T\} = T/S$

So $\frac{R/S}{T/S}$ forms a quotient ring of R/S.
Therefore, by the First theorem of isomorphism,

the homomorphic image R/T of R/S is isomorphic to $\frac{R/S}{T/S}$. $\therefore R/T \cong \frac{R/S}{T/S}$ proved.

Third law of isomorphism :-

Let S be an ideal of a ring R and T be any subring of R, then $(S+T)/S \cong T/(S\cap T)$.

Proof: To show: $S+T = \{a+b : a \in S, b \in T\}$ is a subring of R.

Let $x, y \in S+T$. Then $x = a+b$, $y = c+d$; $a, c \in S$, $b, d \in T$.

$x-y = (a+b)-(c+d) = (a-c)+(b-d) \in S+T$ [since S & T are subrings of R]

$x.y = (a+b).(c+d) = \underbrace{a.c + a.d + b.c}_{\in S} + \underbrace{b.d}_{\in T} \in S+T$

[$\because$ T is a subring of $R \Rightarrow b.d \in T$
S is an ideal of R and $b, d \in T \Rightarrow b, d \in R$
$\therefore a.d + b.c \in S$. Also $a.c \in S$, for S is a subring]

$\therefore$ $S+T$ is a subring of R.

Again, $S \subset S+T$, is an ideal of $S+T$, since
$a \in S$, $r \in S+T$; $r = x+y$, $x \in S$, $y \in T$.
$\Rightarrow a.r = a.(x+y) = a.x + a.y \in S$

Similarly $r.a \in S$.

Thus S is an ideal of $S+T$.
$\Rightarrow (S+T)/S$ exists, i.e., $(S+T)/S$ forms a quotient ring of $S+T$, a subring of R.

We now define a map $\psi : T \to (S+T)/S$ by
$\psi(t) = \cancel{S+t}\ t+S$, $\forall t \in T$.

To show ψ is a homomorphism:

$\psi(t_1+t_2) = (t_1+t_2)+S = \cancel{(t_1+t_1)+(S+t_2)}\ (t_1+S)+(t_2+S) = \psi(t_1)+\psi(t_2)$,

and $\psi(t_1 \cdot t_2) = t_1 \cdot t_2 + S = (t_1+S)\cdot(t_2+S) = \psi(t_1)\cdot\psi(t_2)$

$\therefore$ ψ is a homomorphism. $\forall\, t_1, t_2 \in T$.

Also ψ is onto, since $t+S \in (S+T)/S$

$\Rightarrow t \in S+T \Rightarrow t = s+t_1$, for some $s \in S$, $t_1 \in T$.

$\Rightarrow t+S = (s+t_1)+S = (s+S)+(t_1+S)$

$= S+(t_1+S) = t_1+S$

[$\because$ S is the zero element in $(S+T)/S$]

$\Rightarrow \psi(t) = t_1+S$, $t \in T$.

Thus for every t_1+S in $(S+T)/S$, $\exists\, t \in T$ s.t.

$\psi(t) = t_1+S \Rightarrow \psi$ is onto.

$\Rightarrow (S+T)/S$ is the homomorphic image of T under ψ.

Also $\ker\psi = \{t \in T : \psi(t) = S$, the zero of $(S+T)/S\}$

$= \{t \in T : t+S = S\}$

$= S \cap T$ [$\because$ $t+S = S \Rightarrow t \in S$]

$\Rightarrow \ker\psi = S\cap T$, is an ideal of T.

$\Rightarrow T/(S\cap T)$ is a quotient ring of T.

Therefore, by first law of isomorphism of a ring, it follows that $(S+T)/S$ (homomorphic image of ψ) is isomorphic to the quotient ring $T/(S\cap T)$ of T.

i.e., $\underline{(S+T)/S \cong T/(S\cap T)}$.