Third Isomorphism Theorem for Rings:

Let A and B be ideals of a ring R with $B \subseteq A$. Show that A/B is an ideal of R/B and $\frac{R/B}{A/B}$ is isomorphic to R/A.

Proof:

First we will show that B is an ideal of A.

$\because$ B is ideal of $R \Rightarrow B$ is subring of R

$b_1 - b_2 \in B \; \forall \; b_1, b_2 \in B$ —— (1)

and $rb_1 \in B$, $b_1 r \in B \; \forall \; b_1 \in B, r \in R$. —— (2)

Now from eqn (1), $b_1 - b_2 \in B \; \forall \; b_1, b_2 \in B$

Now let $a \in A, b_1 \in B \Rightarrow a \in R, b_1 \in B \Rightarrow ab_1 \in B$

and $a \in A, b_1 \in B \Rightarrow a \in R, b_1 \in B \Rightarrow b_1 a \in B$

$\therefore$ $b_1 - b_2 \in B \; \forall \; b_1, b_2 \in B$ and $ab_1 \in B$, $b_1 a \in B \; \forall \; a \in A, b_1 \in B$

$\therefore$ B is an ideal of A

Therefore, A/B is a well defined set.

Now, TS A/B is an ideal of R/B.

Let $x, y \in A/B \Rightarrow \exists \; a_1, a_2 \in A$ such that $x = a_1 + B$, $y = a_2 + B$

Now, $x - y = (a_1 + B) - (a_2 + B)$
$= (a_1 - a_2) + B \in A/B$ $[\because a_1 - a_2 \in A]$

Now let $r \in R \Rightarrow r + B \in R/B$.

$\therefore$ $r + B \in R/B$, $a_1 + B \in A/B$.

Now $(r+B)(a_1+B) = ra_1 + B \in A/B$ $(\because ra_1 \in A$ as A is an ideal$)$

and $(a_1+B)(r+B) = a_1 r + B \in A/B$ $[\because a_1 r \in A]$

$\therefore$ A/B is an ideal of R/B

Thus, $\dfrac{R/B}{A/B}$ is a well-defined set.

Now Define a mapping $\phi : R/B \longrightarrow R/A$ such that

$\phi(r+B) = r + A$ —— (3)

We will show that ϕ is a homomorphism

Well defmedness:

let $r_1 + B = r_2 + B$

$\Rightarrow r_1 - r_2 \in B \Rightarrow r_1 - r_2 \in A$ $(\because B \subseteq A)$

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

Operation Preserving:

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

and $\phi\{(r_1+B)(r_2+B)\} = \phi\{r_1 r_2 + B\} = r_1 r_2 + A = (r_1 + A)(r_2 + A) = \phi(r_1 + B)\,\phi(r_2 + B)$.

$\therefore \phi$ is a homomorphism from R/B to R/A.

From first Isomorphism theorem,

$$\frac{R/B}{\ker\phi} \cong \phi(R/B) \quad \text{——— (4)}$$

$$\ker\phi = \{r+B \in R/B \mid \phi(r+B) = A\}$$

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

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

$$= A/B \quad \text{——— (5)}$$

Now $\phi(r+B) = r+A$

So, for every element $r+A \in R/A$, $\exists\, r+B \in R/B$ such that

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

Therefore, ϕ is onto

$$\Rightarrow \phi(R/B) = R/A \quad \text{——— (6)}$$

Using eqn (5) & (6) in (4), we have

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

Theorem 2

Ideals are kernels:

Every ideal of a ring R is the kernel of a ring homomorphism of R.

Proof: Let A be an ideal of ring R.
Define a mapping ϕ from R to R/A such that

$$\phi(r) = r + A \quad \text{———} \quad (1)$$

We will show that ϕ is a homomorphism & $\ker\phi = A$.

(i) welldefinedness: let $r_1 = r_2$

$$\Rightarrow r_1 + A = r_2 + A$$
$$\Rightarrow \phi(r_1) = \phi(r_2).$$

(ii) Operation preserving:

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

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

$$= \phi(r_1 r_2)$$

$\therefore \phi$ is a homomorphism from R to R/A

$\Rightarrow \phi$ is a ring homomorphism of R

Now, $\ker\phi = \{r \in R \mid \phi(r) = A\} = \{r \in R \mid r + A = A\}$

$$= \{r \in R \mid r \in A\} = A$$

$\therefore A$ is a kernel of a ring homomorphism defined by (1)

Thus, every ideal of a ring R is ~~ring~~ the kernel of a ring homomorphism of R.

Note:

The mapping defined in eqn ①. is called natural homomorphism from R to R/A.

Q. Show that ideal $\langle x \rangle$ is Prime in $\mathbb{Z}[x]$ but not maximal.

Soln

Define a mapping $\phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$ such that

$$\phi\{f(x)\} = f(0) \qquad \text{—— (1)}$$

We can easily see that ϕ is a homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}$ and ϕ is onto (check!)

∴ Using first isomorphism theorem.

$$\frac{\mathbb{Z}[x]}{\ker\phi} \cong \mathbb{Z} \qquad \text{—— (2)}$$

$$\ker\phi = \{f(x) \in \mathbb{Z}[x] \mid \phi\{f(x)\} = 0\}$$

$$= \{a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x] \mid a_0 = 0\}$$

$$= \{a_1x + a_2x^2 + \dots + a_nx^n \mid a_i \in \mathbb{Z}\}$$

$$= \langle x \rangle$$

from eqn (2), $\dfrac{\mathbb{Z}[x]}{\langle x \rangle} \cong \mathbb{Z}$ —— (3)

We know that $\mathbb{Z}$ is an Integral domain but not a field.

$\Rightarrow \dfrac{\mathbb{Z}[x]}{\langle x \rangle}$ is an Integral domain but not a field.

$\Rightarrow \langle x \rangle$ is a Prime ideal not maximal in $\mathbb{Z}[x]$.

Theorem:

Homomorphism from $\mathbb{Z}$ to a ring with unity

Let R be a ring with unity e. The mapping $\phi : \mathbb{Z} \to R$ given by $n \to ne$ is a ring homomorphism.

Proof:

Given that $\phi : \mathbb{Z} \to R$ such that

$$\phi(n) = ne \quad \text{---} \quad (1) \qquad e \to \text{unity of } R.$$

(i) **Well definedness:**

let $n_1 = n_2 \Rightarrow n_1 e = n_2 e \Rightarrow \phi(n_1) = \phi(n_2)$.

(ii) **Operation preserving:**

(I) **Addition:**

let $m, n \in \mathbb{Z}$

Case-I: $m \geq 0, n \geq 0$.

$$\phi(m+n) = (m+n)e = e + e + \cdots + e \ (m+n \text{ times})$$

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

$$= me + ne \quad = \phi(m) + \phi(n)$$

Case-II: $m \leq 0, n \leq 0 \Rightarrow -m \geq 0, -n \geq 0$

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

$$= (-m)(-e) + (-n)(-e) \quad [\text{using Case I}]$$

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

Case-III: $m \geq 0, n < 0 \Rightarrow m \geq 0, -n > 0$

$$\phi(m+n) = (m+n)e = e + e + \cdots + e \ (m+n \text{ times})$$

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

$= me + (-n)(-e) = me + ne = \phi(m) + \phi(n)$

Case - IV: $m < 0, n \geq 0 \Rightarrow -m > 0, n \geq 0$

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

$= ne + (-m)(-e) = ne + me$

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

Thus, ϕ preserves addition.

(II) Multiplication:

$\phi(mn) = (mn)e = (mn)(e\,e) = (me)(ne) = \phi(m)\phi(n)$

$\left[\because (ma)(nb) = (mn)(ab) \ \forall m, n \in \mathbb{Z}\right]$

So ϕ preserves multiplication as well.

Thus, ϕ is a homomorphism from $\mathbb{Z}$ to R.

Corollary: A ring with unity contains $\mathbb{Z}_n$ or $\mathbb{Z}$

If R is a ring with unity and the characteristic 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 $\mathbb{Z}$.

Proof: Let e be the unity element of R.

Then $S = \{ke \mid k \in \mathbb{Z}\}$ is a subring of R (Check!)

Now, $\phi : \mathbb{Z} \to S$ given by $\phi(k) = ke$ is a homomorphism

and ϕ is onto $\left[\because \text{for every } ke \in S,\ \exists\, k \in \mathbb{Z} \text{ such that } \phi(k) = ke\right]$

From first homomorphism theorem,

$$\frac{\mathbb{Z}}{\ker \phi} \cong S \quad \text{——— (1)}$$

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

$\Rightarrow \ker \phi = \langle |e| \rangle$, where $|e|$ is additive order of unity e.

$\Rightarrow \ker \phi = \langle n \rangle$, where $n = |e|$

If $\text{Char.}\, R = n\ (>0)$,

then from eq^n (1), $\frac{\mathbb{Z}}{\mathbb{Z}\langle n \rangle} \cong S \Rightarrow \mathbb{Z}_n \cong S$

If $\text{Char.}\, R = 0$,

then from eq^n (1), $\frac{\mathbb{Z}}{\langle 0 \rangle} \cong S \Rightarrow \mathbb{Z} \cong S$.

$\therefore$ ~~Hence~~ $\because S \subseteq R \Rightarrow R$ contains a subring isomorphic to $\mathbb{Z}_n$ or $\mathbb{Z}$.

<u>Corollary 2</u> <u>$\mathbb{Z}_m$ is a homomorphic image of $\mathbb{Z}$</u>

The mapping $\phi : \mathbb{Z} \to \mathbb{Z}_m$ given by $x \to x \pmod{m}$ is a ring homomorphism.

Proof:- $\because \mathbb{Z}_m$ is a ring with unity 1.

and ~~...~~ in the ring $\mathbb{Z}_m$, the integer $x \pmod{m} = x.1$

from above theorem $\phi : \mathbb{Z} \to \mathbb{Z}_m$ such that $\phi(x) = x \pmod{m}$

is a ring homomorphism.

Corollary 3: A field contains $\mathbb{Z}_p$ or $\mathbb{Q}$

If F is a field of characteristic p, then F contains a subfield isomorphic to $\mathbb{Z}_p$. If F is a field of characteristic 0, then F contains a subfield isomorphic to the set of rational numbers.

Proof:

If F has characteristic p,
then by corollary 1, F contains a ~~subfield~~ subring isomorphic to $\mathbb{Z}_p$.
We know that $\mathbb{Z}_p$ is a field for every prime p.
$\therefore$ F contains a subfield ~~of F~~ isomorphic to $\mathbb{Z}_p$.

If F has characteristic 0,
then F contains a subring S isomorphic to $\mathbb{Z}$.
Now define a set $T = \{ab^{-1} \mid a, b \in S,\ b \neq 0\}$ —— ①
We will show that T is isomorphic to $\mathbb{Q}$ and T is a subfield of F.

try yourself

$\therefore$ $S \subseteq F \ni T \subseteq F$.

Now Define a mapping $\phi : T \to \mathbb{Q}$ such that

$$\phi(ab^{-1}) = \frac{a}{b} \quad \text{——} \quad ②$$

Well definedness:

let $x, y \in T \ni x = a_1 b_1^{-1}$, $y = a_2 b_2^{-1}$, $a_1, a_2, b_1, b_2 \in S$
$b_1 \neq 0$, $b_2 \neq 0$

let $x = y \Rightarrow a_1 b_1 - a_2 b_2$

$\Rightarrow a_1(b_1^{-1} b_1) = a_2(b_2^{-1} b_1)$

$\Rightarrow a_1 b_2 = a_2 b_1 b_2^{-1} b_2$ [$\because S$ is commutative $a \cdot S \cong R$]

$\Rightarrow a_1 b_2 = a_2 b_1 \Rightarrow \frac{a_1}{b_1} = \frac{a_2}{b_2}$

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

Operation preserving:

$\phi(x+y) = \phi(a_1 b_1^{-1} + a_2 b_2^{-1}) = \phi((a_1 b_2 + a_2 b_1)(b_1 b_2)^{-1})$

$= \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} = \frac{a_1}{b_1} + \frac{a_2}{b_2}$

$= \phi(a_1 b_1^{-1}) + \phi(a_2 b_2^{-1}) = \phi(x) + \phi(y)$

$\phi(xy)$

$= \phi\{(a_1 b_1^{-1})(a_2 b_2^{-1})\} = \phi\{a_1 a_2 b_1^{-1} b_2^{-1}\} = \phi\{a_1 a_2 b_2^{-1} b_1^{-1}\}$

$= \phi\{(a_1 a_2)(b_1 b_2)^{-1}\} = \frac{a_1 a_2}{b_1 b_2}$

$= \left(\frac{a_1}{b_1}\right)\left(\frac{a_2}{b_2}\right) = \phi(a_1 b_1^{-1}) \phi(a_2 b_2^{-1})$

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

$\therefore \phi$ is Operation Preserving.

$\text{Ker } \phi = \{ab^{-1} \in T \mid \phi(ab^{-1}) = 0\} = \{ab^{-1} \in T \mid \frac{a}{b} = 0\}$

$= \{ab^{-1} \in T \mid a = 0\} = \{0\}$

$\therefore \phi$ is one one.

Since, for every $a/b \in \mathbb{Q}$, $\exists\, ab^{-1} \in T$ such that $\phi(ab^{-1}) = a/b$.

$\therefore \phi$ is onto

So ϕ is isomorphism from T to $\mathbb{Q}$ $\Rightarrow T \cong \mathbb{Q}$.