Theorem 3.3.17 (Second Isomorphism Theorem)
Let A and B be two ideals of a ring R. Then

$$A+B/A \simeq B/A\cap B$$

Proof: Define a mapping $f: B \to A+B/A$ by

$$f(b) = b+A \quad \text{for all } b \in B$$

f is well defined. Now let $b_1, b_2 \in B$

Then $f(b_1+b_2) = b_1+b_2+A = (b_1+A)+b_2+A = f(b_1)+f(b_2)$

$f(b_1b_2) = b_1b_2+A = (b_1+A)(b_2+A) = f(b_1)f(b_2)$

So, f is a homomorphism. Let $x+A \in A+B/A$

then $x \in A+B \Rightarrow x = a+b,\ a \in A,\ b \in B$

So, $x+A = (a+b)+A = \cancel{(a+A)+(b+A)}$

$= \cancel{(b+a)+A = (b+A)+(a+A)}$

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

So, $x+A = b+A = f(b)$. So, f is onto.

By first isomorphism theorem, $A+B/A \simeq B/\text{Ker} f$ ---(1)

Now $x \in \text{Ker} f \Leftrightarrow f(x) = A \Leftrightarrow x+A = A$

$\Leftrightarrow x \in A\cap B$ (as $\text{Ker} f \subseteq B$)

Hence $\text{Ker} f = A\cap B$

So, from (1), $A+B/A \simeq B/A\cap B$

Theorem 3.3.18 (Third Isomorphism Theorem) Let A and B be two ideals of a ring R such that $B \subseteq A$. Then

$$R/A \simeq R/B \big/ B/A$$

Proof: Define a mapping $f : R/B \to R/A$ by

$$f(r+B) = r + A \quad \text{for all } r+B \in R/B$$

f is well defined as, if $r_1 + B = r_2 + B$ then

$$r_1 - r_2 \in B \subseteq A \Rightarrow r_1 - r_2 \in A \Rightarrow r_1 + A = r_2 + A$$

$$\text{So,} \quad f(r_1+B) = f(r_2+B).$$

Let $r_1 + B, r_2 + B \in R/B$. Then

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

Now $$f((r_1+B)(r_2+B)) = f(r_1r_2+B) = r_1r_2+A = (r_1+A)(r_2+A)$$
$$= f(r_1+B)\, f(r_2+B)$$

So, f is a homomorphism. Let $r + A \in R/A$

So, $r \in R$. So, $r+B \in R/B$ and $f(r+B) = r+A$

So, f is onto. So, f is an onto ~~homompo~~ homomorphism. So, by first isomorphism theorem,

$$R/A \simeq \frac{R/B}{\ker f} \quad \ldots (1)$$

Now $$r+B \in \ker f \Leftrightarrow f(r+B) = A$$
$$\Leftrightarrow r+A = A$$
$$\Leftrightarrow r \in A$$
$$\Leftrightarrow r+B \in A/B$$

So, we get $\ker f = A/B$

So, by (1), $$R/A \simeq \frac{R/B}{A/B}$$

Note: First Isomorphism Theorem is also called fundamental theorem of homomorphism.

Theorem 3.3.19 Let N be an ideal of a ring R then $\exists$ a bijection between the set of ideals of R containing N and the set of ideals of R/N

Proof: Let $f: R \to R/N$ be the natural homomorphism defined by $f(r) = r + N$. Now if A be an ideal of R. Now if A be any ideal of R then as $f: R \to R/N$ is an onto homomorphism, $f(A)$ is an ideal of R/N.

Again, $f(A) = \{f(a) : a \in A\}$

$$= \{a + N : a \in A\}$$
$$= A/N$$

Let now $\mathcal{B}$ be the set of all ideals of R, which contain N and $\mathcal{B}'$ be the set of all ideals of R/N

Define $\phi : \mathcal{B} \to \mathcal{B}'$ by $\phi(A) = f(A) = A/N$ for all $A \in \mathcal{B}$

ϕ is clearly well defined

Again $\phi(A) = \phi(B) \Rightarrow f(A) = f(B) \Rightarrow A/N = B/N$

If $a \in A$, then $a + N \in A/N \Rightarrow a + N \in B/N$

$$\Rightarrow a + N = b + N \text{ for some } b \in B$$
$$\Rightarrow a - b \in N \subseteq B$$
$$\Rightarrow a - b = b' \text{ for some } b' \in B$$
$$\Rightarrow a = b + b' \in B$$

So, $A \subseteq B$

Similarly, $B \subseteq A$. So, $A = B$, showing that ϕ is injective

To show that ϕ is surjective, let $X \in \mathcal{B}'$, then X is an ideal of R/N. Define $A = \{x \in R : f(x) \in X\}$

We can easily check (check it) that A is an ideal of R

Again $n \in N = \ker f \Rightarrow f(n) = N$ = zero of R/N

As $0 + N = N \in X$, as ideals of R/N contain zero element.

So, $f(n) \in X \Rightarrow n \in A$.

So, $N \subseteq A$. So, $A \in \mathcal{B}$

Now $\phi(A) = X$. So, ϕ is onto.

So, ϕ is bijective. So, $\exists$ a bijection between the set of all ideals of R containing N and the set of ideals of R/N.

Worked out exercises

1. Show that $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$

Solution: We have $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$

and $\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}\}$

Define $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ by $\phi(r + n\mathbb{Z}) = \bar{r}$, $0 \le r \le n-1$

Let $r + n\mathbb{Z} = s + n\mathbb{Z}$ and suppose $r \ne s$

Then $r - s \in n\mathbb{Z} \Rightarrow n$ divides $r-s \Rightarrow n \le r - s$

where $r, s \le n$. We thus get a contradiction.

So, $r = s$ and $\bar{r} = \bar{s}$. ϕ is well defined. Clearly ϕ is injective (prove it). Again $\phi(r + n\mathbb{Z} + s + n\mathbb{Z}) = \phi((r+s) + n\mathbb{Z})$

$= \phi((nq + t) + n\mathbb{Z})$ for some integer q, t such that $0 \le t < n$ and $r + s = nq + t$

So, $\phi(r + n\mathbb{Z} + s + n\mathbb{Z}) = \phi(t + n\mathbb{Z}) = \bar{t} = \bar{r} + \bar{s}$

$= \phi(r + n\mathbb{Z}) + \phi(s + n\mathbb{Z})$

Again $\phi((r + n\mathbb{Z})(s + n\mathbb{Z})) = \phi(rs + n\mathbb{Z}) = \phi(nq' + k + n\mathbb{Z})$ for some integer q', k such that $0 \le k < n$ and $rs = q'n + k$