1 Ring Isomorphism Theorems

Theorem 1 (First Isomorphism) Let $f : R \to S$ be a homomorphism of rings. Then $\ker(f)$ is an ideal of $R$, and

$$R/\ker(f) \cong \text{im}(f).$$

Remark. What is the intuition for this isomorphism? The ring $R/\ker(f)$ takes $R$ and identifies elements in the same $\ker(f)$ coset. So $r, s$ are in the same $\ker(f)$ coset if and only if $r = s + I$ if and only if $r - s \in I$ if and only if $f(r - s) = 0$ if and only if $f(r) = f(s)$.

Example. Let $R = \mathbb{R}[x]$ and $S = \mathbb{C}$. Define homomorphism $\phi : R \to S$ by

$$\phi(p(x)) = p(i).$$

Then $\ker(\phi) = (x^2 + 1)$. The map $\phi$ is surjective, so

$$R/(x^2 + 1) \cong \mathbb{C}.$$ 

Why does this make sense? Well, $\mathbb{R}[x]$ is the set of polynomials in the variable $x$ where we add the relation $x^2 = -1$, but this is precisely like what the complex numbers are!

Proof. We have already proven that $\ker(f)$ is an ideal of $R$. Let $I = \ker(f)$. Define homomorphism $\psi : R/I \to \text{im}(f)$ by

$$\psi(r + I) = f(r).$$

• $\psi$ is a homomorphism:

$$\psi((r + I)(s + I)) = \psi(rs + I) = f(rs) = f(r)f(s) = \psi(r + I)\psi(s + I)$$

$$\psi((r + I) + (s + I)) = \psi((r + s) + I) = f(r + s) = f(r) + f(s) = \psi(r + I) + \psi(s + I)$$

• $\psi$ is surjective: If $f(r) \in \text{im}(\psi)$ then $\psi(r + I) = f(r)$

• $\psi$ is injective: Suppose $f(r) = f(s)$. Then $f(r) - f(s) = 0$ and hence $f(r - s) = 0$ so $r - s \in \ker(\phi)$ so $r + I = s + I$.

Theorem 2. (Second Isomorphism Theorem for Rings) Let $A$ be a subring and let $B$ be an ideal of $R$. Then $A + B = \{a + b \mid a \in A, b \in B\}$ is a subring of $R$, $A \cap B$ is an ideal of $A$ and

$$(A + B)/B \cong A/(A \cap B)$$
• (Third Isomorphism Theorem for Rings) Let $I, J$ be ideals of $R$ with $I \subseteq J$. Then $J/I$ is an ideal of $R/I$ and 
$$ (R/I)/(J/I) \cong R/J. $$

• (Fourth Isomorphism Theorem / Lattice Isomorphism Theorem for Rings) Let $I$ be an ideal of $R$. The correspondence

$$ A \leftrightarrow A/I $$

is an inclusion preserving bijection between the set of subrings $A$ of $R$ that contain $I$ and the set of subrings of $R/I$. Furthermore, $A$ (a subring containing $I$) is an ideal of $R$ if and only if $A/I$ is an ideal of $R/I$.

**Example.** Let $R = \mathbb{Z}$ and $I$ be the ideal $12\mathbb{Z}$. The ring $R/I = \mathbb{Z}/12\mathbb{Z}$ has ideals

$$ 2\mathbb{Z}/12\mathbb{Z}, 3\mathbb{Z}/12\mathbb{Z}, 4\mathbb{Z}/12\mathbb{Z}, 6\mathbb{Z}/12\mathbb{Z}, 12\mathbb{Z}/12\mathbb{Z} = 0. $$

The corresponding ideals of $R$ are

$$ 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}, 12\mathbb{Z}, $$

which are ideals containing $I$.

**Properties of Ideals**

**New Ideals from Old Ideals**

**Definition.** Let $I, J$ be ideals of a ring $R$

- Define the sum of $I$ and $J$ by $I + J = \{a + b \mid a \in I, b \in J\}$.
- Define the product of $I$ and $J$, denoted by $IJ$, to be the set of all finite sums of elements of the form $ab$ with $a \in I, b \in J$.
- Define the intersection of $I$ and $J$ by $IJ$.

The sum, product and intersection are all ideals.

1. Let $I = 6\mathbb{Z}$ and $J = 10\mathbb{Z}$. Then by definition

$$ I + J = \{6n + 10m \mid m \in \mathbb{Z}\}. $$

Every element of $I + J$ is even. Moreover, $2k = 6(2k) + 10(−k)$ so every even number is in $I + J$. Thus $I + J = 2\mathbb{Z}$. In general, $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ where $d = \gcd(m, n)$. This follows from Math 55.

2. Let $I$ be the ideal in $\mathbb{Z}[x]$ consisting of polynomials with integer coefficients whose constant term is even. Two polynomials $2$ and $x$ are contained in $I$, so both $4$ and $x^2$ are contained in $I^2$, and hence $x^2 + 4$. Note $x^2 + 4$ cannot be written as a single product of elements from $I$. 

2
2 Principal Ideals

Definition. Let \( R \) be a ring. The ideal generated by a single element \( a \in R \) is the smallest ideal containing \( a \) (smallest with respect to subset containment). We call this the principal ideal generated by \( a \), and it is denoted by \((a)\).

In a general ring \((a) \neq \{a\}\). We might think that it is enough to consider the set \(\{ras \mid r, s \in R\}\) but this is still not quite enough because this is not closed under addition. However, we actually have
\[
(a) = \{r_1a_1s_1 + \cdots + r_na_ns_n \mid r_i, s_i \in R\}.
\]

Proposition 3 If \( R \) is a commutative ring, then \((a) = \{ra \mid r \in R\}\).

Proof Sketch If \( R \) is commutative, \(r_1a_1s_1 + \cdots + r_na_ns_n = (r_1s_1 + \cdots + r_ns_n)a\)

Definition. Let \( R \) be a ring with an identity. If \( A \subset R \) we define
\[
(A) = \{r_1a_1s_1 + \cdots + r_na_ns_n \mid r_i, s_i \in R, a_i \in A\}.
\]