1. Theory

In this note we prove all four isomorphism theorems for rings, and provide several examples on how they get used to describe quotient rings. The isomorphism theorems state:

**Theorem 1.1.** Let $R$ be a ring.

1. Let $\varphi: R \to S$ be a ring homomorphism. Then $R/\ker(\varphi) \cong \text{Im}(\varphi)$.
2. Let $A, B \subseteq R$ be subrings with the additional property that $B$ is an ideal in $R$. Then
   
   $$(A + B)/B \cong A/(A \cap B).$$
3. Let $I \subseteq J \subseteq R$ be ideals in $R$. Then
   
   $$(R/I)/(J/I) \cong R/J.$$  

4. Let $I \subseteq R$ be an ideal. Then there is an order preserving bijection between subrings of $R/I$ and subrings of $R$ containing $I$. Furthermore, this bijection sends ideals to ideals.

**Proof.** We prove the isomorphism theorems as follows. Throughout, for $r \in R$ we let $r = r + I$ in $R/I$.

1. Define a function $\psi: R/I \to S$ via $\psi(r) = \varphi(r)$. To check that $\psi$ is well-defined, suppose $r' \in R$ is another element for which $r = r'$. Then $r - r' \in \ker(\varphi)$ and so $\varphi(r - r') = 0$. This implies that

   $$\psi(r') = \varphi(r') = \varphi(r) = \psi(r)$$

   proving that $\psi$ is well-defined. Next we check that $\psi$ is a homomorphism. This follows since if $\overline{r_1}, \overline{r_2} \in R/\ker(\varphi)$ then

   $$\psi(\overline{r_1} + \overline{r_2}) = \psi(r_1 + r_2) = \varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) = \psi(r_1) + \psi(r_2)$$

   $$\psi(\overline{r_1} \cdot \overline{r_2}) = \psi(r_1r_2) = \varphi(r_1r_2) = \varphi(r_1)\varphi(r_2) = \psi(r_1)\psi(r_2).$$

   Next we check that $\psi$ is injective. If $r \in \ker \varphi$ then $0 = \psi(r) = \varphi(r)$ meaning $r \in \ker \varphi$ and hence $\overline{r} = \overline{0}$. Thus $\psi$ gives an isomorphism of $R/\ker(\varphi)$ onto its image in $S$, but clearly this image is just $\text{Im}(\varphi) = \varphi(R)$.

2. We define a function

   $$\varphi: A \to (A + B)/B$$
by \( \varphi(a) = \overline{a} \). It’s clear that \( \varphi \) is a ring homomorphism since it is the composition of the inclusion map \( A \rightarrow A + B \) followed by the quotient map \( A + B \rightarrow (A + B)/B \), each of which are ring homomorphisms. Next we check that \( \varphi \) is surjective. Let \( x \in A + B \) and \( \overline{x} \in (A + B)/B \). Since \( x \in A + B \), there exists \( a \in A \) and \( b \in B \) with \( x = a + b \). Then \( x - a = b \in B \) showing that \( \overline{x} = \overline{b} \). Thus \( \varphi(a) = \overline{a} = \overline{b} \) and so indeed \( \varphi \) is surjective. Thus the first isomorphism theorem gives

\[
A/ \ker(\varphi) \cong (A + B)/B.
\]

An element \( a \in A \) is contained in \( \ker(\varphi) \) if and only if \( \overline{a} = \overline{0} \) in \( (A + B)/B \), which occurs if and only if \( a \in B \). Thus we see that \( \ker(\varphi) = A \cap B \), and the result follows.

(3) Since there are different ideals in question, we use cosets to emphasize which quotient space we are referring to at every step of the proof. Define a function

\[
\psi: R/I \rightarrow R/J
\]

via \( \psi(r + I) = r + J \). It is important to check that \( \psi \) is well-defined since it is defined in terms of coset representatives. If \( r + I = r' + I \) then \( r - r' \in I \) and as \( I \subseteq J \) we also have \( r - r' \in J \). Thus \( r + J = r' + J \) and indeed \( \psi(r + I) = \psi(r' + I) \). It is clear that \( \psi \) is surjective since any element in \( R/J \) is of the form \( r + J \) for some \( r \in R \) and of course \( \psi(r + I) = r + J \). Thus the first isomorphism theorem tells us that

\[
(R/I)/ \ker(\psi) \cong R/J.
\]

Now \( r + I \in \ker(\psi) \) if and only if \( r + J = 0 + J \), which is equivalent to saying \( r \in J \). Thus we see that \( \ker(\psi) = J/I \) and so the theorem follows.

(4) Consider the quotient map \( \pi: R \rightarrow R/I \) given by \( \pi(r) = \overline{r} \). For \( S \) a subring of \( R \) containing \( I \), we let \( \overline{S} \) denote \( \pi(S) \). We know that homomorphisms take rings to subrings, so certainly \( \overline{S} \) is a subring of \( R/I \). To show that the map \( S \rightarrow \overline{S} \) is actually a bijection, we must check that \( \pi^{-1}(\overline{S}) = S \). That is, we must check that no other subring maps onto \( S \). To see this, note first that trivially \( S \subseteq \pi^{-1}(\overline{S}) \). For the converse, suppose that \( x \in \pi^{-1}(\overline{S}) \). Let \( \pi(x) = \overline{s} \) for some \( s \in S \). Then \( \pi(x) = \pi(s) \) and so \( x - s \in \ker(\pi) = I \). Thus \( x - s \in I \subseteq S \), and since \( s \in S \) it follows that \( x \in S \) as well. This proves that \( \pi^{-1}(\overline{S}) = S \) and so we indeed have our bijection. The statement about inclusion preserving is clear. It just says that \( \overline{S} \subseteq \overline{S}' \) if and only if \( S \subseteq S' \), which follows from our bijection.

As for ideals, one direction is obvious. Actually, if \( \varphi: R \rightarrow S \) is any ring homomorphism, then \( \varphi^{-1}(J) \) is an ideal in \( R \) whenever \( J \) is an ideal in \( S \). To see this, let \( I = \varphi^{-1}(J) \). It’s clear that \( 0 \in I \),
and if \(a, b \in I\) then
\[
\varphi(a - b) = \varphi(a) - \varphi(b) \in J
\]
showing that \(a - b \in I\). Similarly, if \(r \in R\) then \(\varphi(rI) \subseteq \varphi(r)J \subseteq J\) showing that \(rI \subseteq I\). A similar argument shows that \(Ir \subseteq I\).

The converse may not hold unless \(\varphi\) is surjective, but of course the quotient map \(\pi\) is always surjective. Assuming that \(\varphi\) is surjective, let \(I \subseteq R\) be an ideal. It is clear that \(J = \varphi(I)\) is a subring of \(S\).

This is because if \(x, y \in \varphi(I)\) then there are \(a, b \in I\) so that \(\varphi(a) = x\) and \(\varphi(b) = y\), showing that
\[
x - y = \varphi(a) - \varphi(b) = \varphi(a - b) \in I
\]
. To show closure under products in \(S\) we need to use surjectivity. If \(s \in S\) then there is an \(r \in R\) so that \(\varphi(r) = s\). Then
\[
sJ = \varphi(r)\varphi(I) = \varphi(rI) \subseteq \varphi(I) = J
\]
and similarly for \(Js\).

\(\square\)

2. Examples

The isomorphism theorems are interesting since they tell you, among other things, that you can find all homomorphic images of a ring \(R\) without ever leaving \(R\). That is, all homomorphic images come from quotients of \(R\). Of course, the isomorphism theorems also help you identify quotient rings. In this section, we will use the isomorphism theorems to try to understand quotient rings better.

Example 1

Consider the ring \(R = \mathbb{Z}[x]\) and \(I = (x) = \{xf(x) | f(x) \in R\}\). How should we figure the ring structure of \(R/I\)? One way is to find a set of coset representative and use them to guess at what the ring structure should be. Notice that for \(g(x), h(x) \in R\) we have \(g(x) - h(x) \in I\) if and only if \(g(x)\) and \(h(x)\) have the same constant term. This tells us that a complete set of coset representative is \(n + I\) where \(n \in \mathbb{Z}\). Since \((n + I) + (m + I) = (n + m) + I\) and \((n + I)(m + I) = nm + I\), we should believe that \(R/I\) is isomorphic to \(\mathbb{Z}\).

A different way to see this is to use the isomorphism theorems. What we can do, is try to produce a surjective homomorphism \(\varphi: R \rightarrow \mathbb{Z}\) whose kernel equals \(I\). Then the first isomorphism theorem would show that \(R/I \cong \mathbb{Z}\). To this end, we define \(\varphi\) via
\[
\varphi(a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0) = a_0.
\]
Check to make sure you see that this is indeed a homomorphism and that it is surjective. Then \(g(x) = a_n x^n + \ldots + a_0\) is in the kernel of \(\varphi\) if and only if \(a_0 = 0\), which is the case iff
\[
g(x) = a_n x^n + \ldots + a_1 x = x(a_n x^{n-1} + \ldots + a_1) = xf(x)
\]
for some \( f(x) \in R \). This proves that \( \ker(\varphi) = (x) \) so indeed \( R/I \cong \mathbb{Z} \) by the first isomorphism theorem.

**Example 2**

What about a slightly harder example like \( R = \mathbb{Z}[x] \) and \( I = (5, x) = \{ 5f(x) + xg(x) \mid f(x), g(x) \in R \} \). Again, we could try to find coset representatives for \( I \) in \( R \), but there is an easier way. Since the ideal \( (x) \) is a subset of \( (5, x) \), we may use the third isomorphism theorem to say:

\[
R/I \cong \left( \mathbb{Z}[x]/(x) \right)/((5, x)/(x)).
\]

We just checked that \( \mathbb{Z}[x]/(x) \cong \mathbb{Z} \), but what about \( (5, x)/(x) \)? Here, the second isomorphism theorem comes to our rescue! The ideal \( (5, x) \) equals the sum \( (5) + (x) \). So what we’re trying to analyze is

\[
(5 + (x))/(x)
\]

which should be the same as

\[
(5)/(5 \cap (x)).
\]

Now \( f(x) \in (5) \cap (x) \) if and only if every coefficient of \( f(x) \) is a multiple of 5 and \( f(x) \) has no constant term. This shows that \( (5) \cap (x) = (5x) \). Thus what we’re after is

\[
(5)/(5x).
\]

Now this is a quotient we should be able to handle. The ideal \( (5) = \{ 5f(x) \mid f(x) \in \mathbb{Z}[x] \} \). This ideal consists of all polynomials whose coefficients are multiples of 5, and we are declaring that two such polynomials are equivalent of their difference is in the ideal \( (5x) \), which is the same as declaring that they have the same constant term. This should hopefully convince you that the coset representatives of \( (5x) \) in \( (5) \) consists of integer multiples of 5. What we’ve just done is prove:

\[
\mathbb{Z}[x]/(5, x) \cong \left( \mathbb{Z}[x]/(x) \right)/((5, x)/(x)) \cong \mathbb{Z}/5\mathbb{Z}.
\]

In particular, we’ve just shown that the ideal \( (5, x) \) is maximal in \( \mathbb{Z}[x] \). In fact, one can extend this argument to show that if \( p \) is a prime in \( \mathbb{Z} \) then \( (p, x) \) is a maximal ideal in \( \mathbb{Z}[x] \) since

\[
\mathbb{Z}[x]/(p, x) \cong \mathbb{Z}/p\mathbb{Z}.
\]

**Example 3**

Let’s try a non-commutative example. Consider \( R = M_2(\mathbb{Z}) \) and let \( I = \{ M \in R \mid \text{all entries of } M \text{ are a multiple of } 5 \} \). We can prove that \( I \) is an ideal and explicitly describe \( R/I \) in one step with the isomorphism theorems. Consider a function \( \varphi: M_2(\mathbb{Z}) \to M_2(\mathbb{Z}/3\mathbb{Z}) \) given by reducing the entries of a matrix modulo 3. You can easily check that \( \varphi \) is a homomorphism and that it is surjective. What is the kernel of \( I \)? Well, it consists of all matrices in \( R \) with entries all multiples of 3. This is precisely \( I = M_2(3\mathbb{Z}) \). Thus \( I \) is an ideal in \( R \) and

\[
M_2(\mathbb{Z})/M_2(3\mathbb{Z}) \cong M_2(\mathbb{Z}/3\mathbb{Z}).
\]

**Example 4**
Consider the ring $R = \mathbb{Z}[i]$ and let $I = (1+i)$. We would like to understand the ring $R/I$. First off, notice that $(1+i)(1-i) = 2$ so $2 \in I$. This shows that $(2) \subseteq I$, so we can use the third isomorphism theorem to say that

$$R/I \cong (\mathbb{Z}[i]/(2))/((1+i)/(2)).$$

The ring $\mathbb{Z}[i]/(2)$ shouldn’t be too hard to understand. Notice that two elements $a + bi$ and $c + di$ are equivalent modulo $(2)$ if and only if their difference, $(a - c) + (b - d)i \in (2)$, which is to say that both $a \equiv c \mod 2$ and $b \equiv d \mod 2$. Thus we see that the ideal $(2)$ in $\mathbb{Z}[i]$ has four cosets! We can write representatives as $0, 1, i, 1+i$. Next we need to analyze $(1+i)/(2)$. In the ring $\mathbb{Z}[i]/(2)$ we see that $(1+i)$ consists of the set $\{0, 1+i\}$. Thus $(1+i)$ has two coset representatives in $\mathbb{Z}[i]/(2)$, consisting of $0+(1+i)$ and $1+(1+i)$. This shows us that the ring $R/I = \mathbb{Z}[i]/(1+i)$ consists of two elements, and it shouldn’t be hard to convince yourselves that

$$R/I \cong \mathbb{Z}/2\mathbb{Z}.$$

Notice, for example, that we’ve just proved something interesting about the ideal $(1+i)$ in $\mathbb{Z}[i]$. Since $\mathbb{Z}/2\mathbb{Z}$ is a field, the ideal $(1+i)$ is maximal!