7.2: Ring Homomorphisms

As we saw with both groups and group actions, it pays to consider structure preserving functions!

Definition 7.1.0

Let \( R \) and \( S \) be rings. Then \( \phi: R \rightarrow S \) is a homomorphism if:

1. \( \phi \) is homomorphism of additive groups: \( \phi(a+b) = \phi(a) + \phi(b) \), and
2. \( \phi \) preserves multiplication: \( \phi(a\cdot b) = \phi(a)\cdot \phi(b) \).

If the homomorphism is a bijection, then it is an isomorphism.

Examples:

1. We have the inclusion homomorphism \( \iota: \mathbb{Z} \rightarrow \mathbb{Q} \), which just sets \( \iota(n) = n \). This map clearly preserves both addition and multiplication.

2. Consider the map \( \phi: \mathbb{Z} \rightarrow \mathbb{Z}_n \) sending \( k \) to \( k \mod n \). We've seen that this is a homomorphism of additive groups, and can easily check that multiplication is preserved. Indeed,
\[
\phi(a) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) = a \cdot \phi(1) = a \mod n.
\]

Thus, \( \phi(ab) = ab \mod n \). But also:
\[
\phi(a) \phi(b) = ab \phi(1) \phi(1) = ab \mod n.
\]
So \( \phi \) is a ring homomorphism.

Notice that every element in \( \mathbb{Z} \) can be written as a sum of many copies of \( 1 \). Then we were able to figure out what the homomorphism does simply by knowing \( \phi(1) \). As an example, consider the map
3. The evaluation map \( \langle e_k \rangle \) is a function from \( \langle R[x] \rangle \) to \( \langle R \rangle \). For any polynomial \( \langle f \rangle \in R[x] \) and \( \langle k \rangle \in R \), we set \( \langle e_k(f) \rangle = f(k) \). This is a ring homomorphism! Let \( \langle f(x) = a_n x^n + \cdots + a_0 x^0 \rangle \) and \( \langle g(x) = b_n x^n + \cdots + b_0 x^0 \rangle \), where \( \langle a_i, b_i \rangle \in R \). (We'll also allowing leading coefficients to be zero in order to make it easy to add \( \langle f \rangle \) and \( \langle g \rangle \) formally.) We then check the ring homomorphism conditions:

a. We have:
\[
\langle e_k(f+g) \rangle = \langle (a_n+b_n)x^n + \cdots + (a_0+b_0)x^0 \rangle & = & \langle a_nk^n + \cdots + a_0k^0 + b_nk^n + \cdots + b_0k^0 \rangle = \langle e_k(f) \rangle + \langle e_k(g) \rangle.
\]
So \( \langle e_k \rangle \) is an additive group homomorphism.

b. Since we know that \( \langle e_k \rangle \) is an additive homomorphism, we only need to check that it is multiplicative on monomials. But that's easy:
\[
\langle e_k((ax^n)(bx^m)) \rangle = \langle abx^{n+m} \rangle = \langle e_k(ax^n)e_k(bx^m) \rangle.
\]
So \( \langle e_k \rangle \) is an additive group homomorphism.

**Exercise 7.1.1**

1. Show that \( \langle \rho: \mathbb{Z} \rightarrow \mathbb{Z}_5 \rangle \) defined by \( \langle \rho(k) = (3k) \% 5 \rangle \) is a ring homomorphism. Find the kernel and image of \( \langle \rho \rangle \).

2. Show that \( \langle \rho: \mathbb{Z} \rightarrow \mathbb{Z}_6 \rangle \) defined by \( \langle \rho(k) = (3k) \% 6 \rangle \) is a ring homomorphism. Find the kernel and image of \( \langle \rho \rangle \).

**Definition 7.1.2**

Let \( \langle R \rangle \) and \( \langle S \rangle \) be rings. Define the direct product \( \langle R \times S \rangle \) as the set \( \{(r,s) \mid r \in R, s \in S\} \) with coordinate-wise operations: \( \langle (r_1, s_1) + (r_2, s_2) = (r_1+r_2, s_1+s_2) \rangle \), and \( \langle (r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2) \rangle \).

Of course, one should verify that this is a ring by checking the ring axioms.

**Exercise 7.1.3**

1. Show that for any rings \( \langle R \rangle \) and \( \langle S \rangle \) that the product \( \langle R \times S \rangle \) is a ring.

2. Show that the inclusion map \( \langle \iota: R \rightarrow R \times S \rangle \) given by \( \langle \iota(a) = (a,0) \rangle \) is a ring homomorphism.

3. Show that the projection \( \langle \pi: R \times S \rightarrow R \rangle \) given by \( \langle \pi((r,s)) = r \rangle \) is a ring homomorphism.
A Small Digression on the Relationship Between Good Computer Science and Good Mathematics

Recall that when we worked with groups the kernel of a homomorphism was quite important; the kernel gave rise to normal subgroups, which were important in creating quotient groups.

For ring homomorphisms, the situation is very similar. The kernel of a ring homomorphism is still called the kernel and gives rise to quotient rings. In fact, we will basically recreate all of the theorems and definitions that we used for groups, but now in the context of rings. Conceptually, we've already done the hard work.

In computer programming, people often speak of the DRY principle: Don't Repeat Yourself, meaning that you shouldn't write the same code more than once. The reason, in computer science, is that it's easier to fix mistakes or make modifications if a given piece of code appears in one distinct place.

In mathematics, we have a similar principle: generalization. When you find yourself doing the same thing in different contexts, it means that there's something deeper going on, and that there's probably a proof of whatever theorem you're re-proving that doesn't matter as much on the context. It would be nice, for example, to remember just one concept for quotient groups, quotient rings, quotient vector spaces, and whatever else, instead of a hodgepodge of specific cases of the same basic idea.

For the game of homomorphisms, kernels, and quotients, the generalization involves category theory and universal properties. Category theory is a bit beyond the scope of these notes, but is an essential part of modern mathematics and serves as a bridge between many different fields of mathematical study.

Subring, Kernel, Image, Quotient.

We begin with some definitions.

Definition 7.1.4

Let \((R)\) be a ring. A subset \((S)\) of \((R)\) is a subring if \((S)\) is itself a ring using the same operations as \((R)\). (We don't require that \((S)\) has a multiplicative identity, though.)

For example, take \((R[x])\), the polynomial ring over \((R)\). The set of degree \((0)\) polynomials is closed under addition and multiplication; indeed, this set is just a copy of \((R)\). Thus, \((R)\) is a subring of \((R[x])\).

On the other hand, consider the set of all polynomials of degree greater than or equal to 2 in \((\mathbb{Z}[x])\), which we'll denote \((P_{\{\geq 2\}})\). This is closed under addition (the sum of two polynomials has degree equal to the max of their degrees), and is closed under multiplication (the degree of the product is the sum of the degrees). Thus, it is a subring. However, the multiplicative identity in \((R[x])\) is \((1)\), which has degree 0. So there is no unit in \(P_{\{\geq 2\}}\).

Another example: Take \((2\mathbb{Z})\subset \mathbb{Z}\), the set of even integers. This set is closed under addition and
multiplication, and is thus a subring. (The sum and product of two even integers is still even.) However, the even integers don’t have the number (1), and so there is no unit in (2\mathbb{Z}).

Exercise 7.1.5

Let \((P^n_{\geq 2})\) denote all polynomials in \((\mathbb{Z}_n[x])\) with degree \((\geq 2)\). Is \((P^n_{\geq 2})\) a subring of \((\mathbb{Z}_n[x])\)? Why or why not?

Definition 7.1.6

Let \((\phi: R\rightarrow S)\) be a ring homomorphism. The kernel of \((\phi)\) is \(\{r \in R \mid \phi(r)=0\}\), which we also write as \((\phi^{-1}(0))\). The image of \((\phi)\) is the set \(\{\phi(r) \mid r \in R\}\), which we also write as \((\phi(R))\).

We immediately have the following.

**Proposition 7.1.17**

Let \((\phi: R\rightarrow S)\) be a ring homomorphism. Then the kernel of \((\phi)\) is a subring of \((R)\) and the image of \((\phi)\) is a subring of \((S)\).

**Proof 7.1.8**

Since \((\phi)\) is a homomorphism of commutative additive groups, we know that the kernel and image are closed under addition. The kernel is closed under multiplication, because if \((\phi(a)=\phi(b)=0)\), then \((\phi(ab)=\phi(a)\phi(b)=0)\). The image is closed because if \((x, y \in \phi(R))\), then there exist \((a, b \in R)\) such that \((\phi(a)=x, \phi(b)=y)\). Then \((xy=\phi(a)\phi(b)=\phi(ab)\in \phi(R))\).

Just as kernels of group homomorphisms were special kinds of subgroups, kernels of ring homomorphisms are special kinds of subrings.

Definition 7.1.9

A subring \((I)\) of a ring \((R)\) is an ideal if for any \((x \in I, r \in R)\), \((rx \in I)\) and \((xr \in I)\).

**Proposition 7.1.10**

Let \((K)\) be the kernel of a ring homomorphism \((\phi: R\rightarrow S)\). Then \((K)\) is an ideal.

**Proof 7.1.11**
For any \( x \in K \), we have \( \phi(x) = 0 \). Then \( \phi(rx) = \phi(r) \phi(x) = \phi(r)0 = 0 \). Similarly, \( \phi(xr) = 0 \). Thus, \( K \) is a two-sided ideal.

Ideals are playing exactly the same role as normal subgroups in the groups context; in fact, an ideal is a normal subgroup of the additive group of the ring. In particular, we can form cosets and consider the quotient \( R/I \). Since it's an additive group, cosets of an ideal \( I \) are of the form \( r+I = \{ r+x \mid x \in I \} \).

**Theorem 7.1.12**

If \( I \) is an ideal, then \( R/I \) is a ring.

**Proof 7.1.13**

We know that under addition \( R/I \) is a commutative group. So we just need to show that the multiplication distributes over addition. For this we have:

\[
((r+I)+(q+I))(s+I) = rs+qs+I = (r+I)(s+I) + (q+I)(s+I).
\]

One can also check that the multiplication is associative and commutative if \( R \) is associative and commutative. Likewise, if \( R \) has a unit, then \( 1+I \) acts as a unit in \( R/I \).

Finally, we have the isomorphism theorem.

**Theorem 7.1.14: Isomorphism Theorem**

Let \( R \) and \( S \) be rings, and \( \phi: R \rightarrow S \) a homomorphism. Then the image of \( \phi \) is isomorphic to \( R/I \).

**Proof 7.1.15**

To prove the isomorphism theorem, build a homomorphism from \( R/I \) to the image of \( \phi \), just as we did for groups, and show that it is a bijection.

---

**Contributors**

- Tom Denton (Fields Institute/York University in Toronto)