Kernels, ideals and quotient rings

In this lecture we continue our study of rings and homomorphisms, with an emphasis on the notions of kernel, ideal and quotient ring.

Let $\phi : R \to R'$ be a ring homomorphism. We define the *kernel* of ϕ as follows:

$$\ker(\phi) = \{a \in R : \phi(a) = 0\}$$

Note that $\ker(\phi)$ is a subset of the ring R. However, $\phi(1) = 1$, so the only way $1 \in \ker(\phi)$ is if $1 = 0$ in R', i.e. $R' = \{0\}$. Thus in general $\ker(\phi)$ is not a subring of R. However, the kernel of a homomorphism does have the following kind of structure.

▸ **An *ideal* in a ring R is a subset $I \subset R$ satisfying the following: I is a subgroup of R with respect to addition, and for all $a \in I$, $r \in R$ we have $ra \in I$ and $ar \in I$.**

Note that an ideal is also closed under multiplication. However, it is important to note that the identity $1 \in R$ may not be in an ideal. In fact, if $1 \in I$ then for every $r \in R$ we have $r1 = r \in I$, so $R \subset I$. In conclusion, $I = R$ if and only if $1 \in I$.

In general, to check that a non-empty subset $I \subset R$ is an ideal, it suffices to show that (i) for all $a, b \in I$ we have $a + b \in I$, and (ii) for all $a \in I$ and $r \in R$ we have $ra \in I$ and $ar \in I$. Note in (ii) that if R is commutative, you only need to check $ra \in I$ since $ar = ra$.

▸ **Let $\phi : R \to R'$ be a ring homomorphism. Then $\ker(\phi) \subset R$ is an ideal.**

Proof. As $\phi(0) = 0$ we have $\ker(\phi) \neq \varnothing$. Let $a, b \in \ker(\phi)$, i.e. $\phi(a) = \phi(b) = 0$. Then

$$\phi(a + b) = \phi(a) + \phi(b) = 0 + 0 = 0$$

and thus $a + b \in \ker(\phi)$. Next, let $a \in \ker(\phi)$ and $r \in R$. Then

$$\phi(ra) = \phi(r)\phi(a) = \phi(r)0 = 0$$

from which it follows that $ra \in \ker(\phi)$. Similarly $ar \in I$. Thus $\ker(\phi)$ is an ideal in R. □

Examples

1. Consider the homomorphism $\phi_n : \mathbb{Z} \to \mathbb{Z}_n$ which is reduction mod n. Then $\phi_n(k) = k \pmod{n}$ is zero in $\mathbb{Z}_n$ if and only if k is a multiple of n. Thus

$$\ker(\phi_n) = \{an : a \in \mathbb{Z}\} = n\mathbb{Z} \subset \mathbb{Z}$$

In fact every ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}$, which is a good exercise for you to check.

2. For any ring R, consider the "zero" homomorphism $\phi : R \to \{0\}$ which sends everything to 0. Then we have $\ker(\phi) = R$.

3. At the other extreme, we remark that a homomorphism $\phi : R \to R'$ is 1-1 if and only if $\ker(\phi) = \{0\}$. Indeed, if ϕ is 1-1, then $\phi(a) = 0 = \phi(0)$ implies $a = 0$, so $\ker(\phi)$. Conversely, suppose $\ker(\phi) = \{0\}$. Then $\phi(a) = \phi(b)$ implies $0 = \phi(a) - \phi(b) = \phi(a - b)$, so that $a - b \in \ker(\phi) = \{0\}$. We obtain $a - b = 0$, i.e. $a = b$, and thus ϕ is 1-1.

4. Let us consider a more interesting example. Consider the following set:

$$R = \mathbb{Z}[\sqrt{-3}] = \left\{a + b\sqrt{-3} : \ a, b \in \mathbb{Z}\right\} \subset \mathbb{C}$$

This is a subring of the complex numbers. Indeed, we have $1 \in R$, and if $a + b\sqrt{-3}$ and $c + d\sqrt{-3} \in R$, then we have $(a + b\sqrt{-3}) - (c + d\sqrt{-3}) = (a - c) + (b - d)\sqrt{-3} \in R$, and also

$$(a + b\sqrt{-3})(c + d\sqrt{-3}) = (ac - 3bd) + (ad + bc)\sqrt{-3} \in R.$$

Having verified that R is a ring, we now define a map

$$\phi : \mathbb{Z}[\sqrt{-3}] \longrightarrow \mathbb{Z}_4$$

as follows: $\phi(a + b\sqrt{-3}) = a + b \pmod 4$. We claim this is a homomorphism. First, we note $\phi(1) = 1 \pmod 4$. Next, we show $\phi(x + y) = \phi(x) + \phi(y)$ for all $x, y \in R$:

$$\begin{aligned}\phi\left((a + b\sqrt{-3}) + (c + d\sqrt{-3})\right) &= \phi\left((a + c) + (b + d)\sqrt{-3}\right) = (a + c) + (b + d)\\ &= (a + b) + (c + d) = \phi(a + b\sqrt{-3}) + \phi(c + d\sqrt{-3}) \pmod 4\end{aligned}$$

Finally, to verify the property $\phi(x)\phi(y) = \phi(xy)$ for all $x, y \in R$ we compute:

$$\phi\left((a + b\sqrt{-3})(c + d\sqrt{-3})\right) = \phi\left((ac - 3bd) + (ad + bc)\sqrt{-3}\right) = ac - 3bd + ad + bc \pmod 4$$
$$\phi(a + b\sqrt{-3})\phi(c + d\sqrt{-3}) = (a + b)(c + d) = ac + bd + ad + bc \pmod 4$$

and they agree modulo 4. Thus ϕ is a ring homomorphism, and it is onto. The kernel is:

$$\ker(\phi) = \{a + b\sqrt{-3} : \ a + b \equiv 0 \pmod 4\} \subset R$$

Quotient rings

Let $I \subset R$ be an ideal in a ring R. Consider the additive cosets $R/I = a + I$ for $a \in R$. In other words, viewing I as a subgroup of the abelian group $(R, +)$ we are taking the quotient group R/I. We define a multiplication on these cosets: for $a + I, b + I \in R/I$ we define

$$(a + I)(b + I) = ab + I$$

This is well-defined because I is an ideal: if $a' + I = a + I$ and $b' + I = b + I$ then we have $a' - a \in I$, $b' - b \in I$. So $a'b' - ab = (a' - a)b + a'(b' - b)$ is in I. Note we are using that $(a' - a)b \in I$ because $a' - a \in I$ and $b \in R$, and similarly for the other term. Thus

$$(a' + I)(b' + I) = a'b' + I = ab + I = (a + I)(b + I)$$

The additive identity in R/I is the coset I, while the multiplicative identity is $1 + I$. The set R/I with the above described structure satisfies the axioms of a ring, and is called the *quotient ring* of R by the ideal I.

Given any ideal $I \subset R$ in a ring there is a canonical ring homomorphism

$$\phi : R \longrightarrow R/I$$

This homomorphism is onto, and $\ker(\phi) = I$. Conversely, every onto homomorphism can be viewed as such a homomorphism to a quotient ring. Explicitly:

▶ **1st Isomorphism Theorem**: **Let $\phi : R \to R'$ be an onto ring homomorphism. Then we have an isomorphism of rings $R/\mathbf{ker}(\phi) \cong R'$.**

The proof is similar to the proof of the 1st isomorphism theorem for groups.

As an example, consider the homomorphism $\phi : \mathbb{Z}[\sqrt{-3}] \to \mathbb{Z}_4$ we defined earlier. This is onto and its kernel $I \subset \mathbb{Z}[\sqrt{-3}]$ is the set of $a + b\sqrt{-3}$ such that $a + b \equiv 0 \pmod 4$. We obtain $\mathbb{Z}[\sqrt{-3}]/I \cong \mathbb{Z}_4$ as rings.

We also have analogues of the 2nd and 3rd isomorphism Theorems, now for rings:

▶ **2nd Isomorphism Theorem**: **Let S be a subring of R and $I \subset R$ an ideal of R. Then $S \cap I$ is an ideal in S and we have an isomorphism of rings:**

$$\frac{S}{S \cap I} \cong \frac{S + I}{I}$$

In this statement, $S + I = \{a + b : a \in S, b \in I\}$ is a subring of R.

▶ **3rd Isomorphism Theorem**: **Let R be a ring and I, J ideals in R with $J \subset I$. Then we have an isomorphism of rings:**

$$\frac{R}{I} \cong \frac{R/J}{I/J}$$

The proofs are similar in spirit to the ones for groups, and we omit them.