Ideals and Quotient Rings

This section of notes roughly follows Sections 7.3–7.4 in Dummit and Foote.

Recall that in the case of a homomorphism ϕ of groups, the fibers of ϕ have the structure of a group (that happens to be isomorphic to the image of ϕ by the First Isomorphism Theorem). In this case, the kernel of ϕ is the identity of the associated quotient group. This naturally led to the notion of a normal subgroup (i.e., those groups that correspond to kernels of homomorphisms). Can we do the same sort of thing for rings?

Let $\phi : R \to S$ be a ring homomorphism with $\ker(\phi) = I$. Note that ϕ is also a group homomorphism of abelian groups and the fibers of ϕ are the cosets $r + I$. That is, if $\phi(r) = a$, then the fiber of ϕ over a is the coset $\phi^{-1}(a) = r + I$.

These cosets naturally have the structure of a ring isomorphic to the image of ϕ:

$$(r+I)+(s+I) = (r+s)+I \tag{1}$$

$$(r+I)(s+I) = (rs)+I \tag{2}$$

The reason for this is that if the fiber of $a \in S$ is $\phi^{-1}(a) = X$ and the fiber of $b \in S$ is $\phi^{-1}(b) = Y$, then the fibers of $a+b$ and ab are $X+Y$ and XY, respectively.

The corresponding ring of cosets is called the **quotient ring** of R by $I = \ker(\phi)$ and is denoted by R/I. The additive structure of the quotient ring R/I is exactly the additive quotient group of the additive abelian group R by the normal subgroup R (all subgroups are normal in abelian groups). When I is the kernel of some ring homomorphism ϕ, the additive abelian quotient group R/I also has a multiplicative structure defined in (2) above, making R/I into a ring.

Question 26. Can we make R/I into a ring for any subring I?

The answer is "no" in general, just like in the situation with groups. But perhaps this isn't obvious because if I is an arbitrary subring of R, then I is necessarily an additive subgroup of the abelian group R, which implies that I is an additive normal subgroup of the group R. It turns out that the multiplicative structure of R/I may not be well-defined if I is an arbitrary subring.

Let I be an arbitrary *subgroup* of the additive subgroup R. Let $r+I$ and $s+I$ be two arbitrary cosets. In order for multiplication of the cosets to be well-defined, the product of the two cosets must be independent of choice of representatives. Let $r+\alpha$ and $s+\beta$ be arbitrary representatives of $r+I$ and $s+I$, respectively ($\alpha, \beta \in I$), so that $r+I = (r+\alpha)+I$ and $s+I = (s+\beta)+I$. We must have

$$(r+\alpha)(s+\beta)+I = rs+I. \tag{3}$$

This needs to be true for all possible choices of $r, s \in R$ and $\alpha, \beta \in I$. In particular, it must be true when $r = s = 0$. In this case, we must have

$$\alpha\beta + I = I. \tag{4}$$

But this only happens when $\alpha\beta \in I$. That is, one requirement for multiplication of cosets to be well-defined is that I must be closed under multiplication, making I a *subring*.

Next, if we let $s = 0$ and let r be arbitrary, we see that we must have $r\beta \in I$ for every $r \in R$ and every $\beta \in I$. That is, it must be the case that I is closed under multiplication on the left by elements from R. Similarly, letting $r = 0$, we can conclude that we must have I closed under multiplication on the right by elements from R.

On the other hand, if I is closed under multiplication on the left and on the right by elements from R, then it is clear that relation (4) above is satisfied.

It is easy to verify that if the multiplication of cosets defined in (2) above is well-defined, then this multiplication makes the additive quotient group R/I into a ring (just check the axioms for being a ring).

We have shown that the quotient R/I of the ring R by a subgroup I has a natural ring structure iff I is closed under multiplication on the left and right by elements of R (which also forces I be a subring). Such subrings are called **ideals**.

Definition 27. Let R be a ring and let I be a subset of R.

(1) I is a **left ideal** (respectively, **right ideal**) of R iff I is a subring and $rI \subseteq I$ (respectively, $Ir \subseteq I$) for all $r \in R$.

(2) I is an **ideal** (or **two-sided ideal**) iff I is both a left and a right ideal.

Here's a summary of everything that just happened.

Theorem 28. Let R be a ring and let I be an ideal of R. Then the additive quotient group R/I is a ring under the binary operations:

$$(r+I)+(s+I) = (r+s)+I \tag{5}$$

$$(r+I)(s+I) = (rs)+I \tag{6}$$

for all $r,s \in R$. Conversely, if I is any subgroup such that the above operations are well-defined, then I is an ideal of R.

As you might expect, we have some isomorphism theorems.

Theorem 29 (First Isomorphism Theorem for Rings)**.** If $\phi : R \to S$ is a ring homomorphism, then $\ker(\phi)$ is an ideal of R and $R/\ker(\phi) \cong \phi(R)$.

If I and J are ideals of R, then it is easy to verify that $I \cap J$, $I + J = \{a + b \mid a \in I, b \in J\}$, and $IJ = \{$finite sums of elements of the form ab for $a \in I, b \in J\}$ are also ideals of R. We also have the expected Second, Third, and Fourth Isomorphism Theorems for rings.

The next theorem tells us that a subring is an ideal iff it is a kernel of a ring homomorphism.

Theorem 30. If I is any ideal of R, then the **natural projection** $\pi : R \to R/I$ defined via $\pi(r) = r + I$ is a surjective ring homomorphism with $\ker(\pi) = I$.

For the remainder of this section, assume that R is a ring with identity $1 \neq 0$.

Definition 31. Let A be any subset of R.

(1) Let (A) denote the smallest idea of R containing A, called the **ideal generated by** A. If A consists of a single element, say $A = \{a\}$, then $(a) := (\{a\})$ is called a **principal ideal**.

(2) $RA := \{r_1a_1 + \cdots + r_na_n \mid r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$, $AR := \{a_1r_1 + \cdots + a_nr_n \mid a_i \in A, r_i \in R, n \in \mathbb{Z}^+\}$, and $RAR := \{r_1a_1r_1' + \cdots + r_na_nr_n' \mid r_i, r_i' \in R, a_i \in A, n \in \mathbb{Z}^+\}$.

Note 32. The following facts are easily verified.

(1) (A) is the intersection of all ideals containing A.

(2) RA, AR, and RAR are the left, right, and two-sided ideals generated by A.

(3) If R is commutative, then $RA = AR = RAR = (A)$.

(4) If R is commutative, then $(a) = Ra = aR$.

Example 33. Here are a couple examples. The details are left as exercises.

(1) In $\mathbb{Z}$, $n\mathbb{Z} = (n) = (-n)$. In fact, these are the only ideals in $\mathbb{Z}$ (since these are the only subgroups). So, all the ideals in $\mathbb{Z}$ are principal. If m and n are positive integers, then $n\mathbb{Z} \subseteq m\mathbb{Z}$ iff m divides n. Moreover, we have $(m,n) = (d)$, where d is the greatest common divisor of m and n.

(2) Consider the ideal $(2,x)$ in $\mathbb{Z}[x]$. Note that $(2,x) = \{2p(x) + xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\}$. Then $(2,x)$ is the collection of polynomials from $\mathbb{Z}[x]$ that have even constant term. In particular, $2, x \in (2,x)$. However, there is no single polynomial in $\mathbb{Z}[x]$ that we can use to generate both 2 and x that only produces polynomials with even constant terms.

Theorem 34. Let I be an ideal of R.

(1) $I = R$ iff I contains a unit.

(2) Assume R is commutative. Then R is a field iff its only ideals are 0 and R.

Loosely speaking, the previous result says that fields are "like simple groups."

Corollary 35. If R is a field, then every nonzero ring homomorphism from R into another ring is an injection.