Commutative Ring Theory

Jim Coykendall

August 31, 2005

Chapter 1

Background and Preliminaries

1.1 Basics

Definition 1.1.1. *A set $(R, +, \cdot)$ equipped with two binary operations such that*

1) $(R, +)$ is an abelian group

2) $r(x + y) = rx + ry$ and $(x + y)r = xr + yr$ for all $r, x, y \in R$

3) $r(xy) = (rx)y$ for all $r, x, y \in R$

is called a ring.
If additionally we have:

4) There is a $1_R \in R$ such that $1_R x = x 1_R = x$ for all $x \in R$

Then we say R has an identity.
If we have:

5) $xy = yx$ for all $x, y \in R$

Then we say that R is commutative.

In this tome, we will always assume that R is commutative unless otherwise indicated and we will usually assume that R has an identity as well (we will use the terminology "not necessarily with identity" if we wish to drop this assumption and by default the word "ring" will mean commutative ring with identity).

Example 1.1.2. *$\mathbb{Z}, \oplus\mathbb{Z}, \prod \mathbb{Z}, \mathbb{Z}_n, \mathbb{Z}[\sqrt{d}], \mathbb{Q}, \mathbb{C}, \mathbb{R}, \mathbb{R}[x]$ are all rings (and most of them have identity (which one(s) do not?). The set of continuous functions from $[0, 1]$ to $\mathbb{R}$ with pointwise multiplication is another commutative ring with 1.*

Definition 1.1.3. *Let R be a ring. A subset $T \subseteq R$ is said to be a subring if T is itself a ring. If R has an identity, the convention is that a subring T must contain the identity of R (and so $\mathbb{Z}$ does not have any proper subrings by this convention).*

Example 1.1.4. *Depending on convention, the set $\{\overline{0}, \overline{3}\}$ may or may not be a subring of the ring $\mathbb{Z}_6$.*

Definition 1.1.5. *Let R be a ring and $I \subseteq R$ a nonempty subset. We say that I is an ideal of R if*

1) for all $x, y \in I$, we have $x - y \in I$ and

2) for all $x \in I, r \in R$ we have $rx \in I$.

We will say that an ideal, $I \subseteq R$, is proper if the containment is strict.

Definition 1.1.6. *Let R, T be rings. A function $f : R \longrightarrow T$ is said to be a homomorphism of rings if*

1) $f(x + y) = f(x) + f(y)$ for all $x, y \in R$ and

2) $f(xy) = f(x)f(y)$ for all $x, y \in R$.

We note here that if R and T have identity then we will require that $f(1_R) = 1_T$.

Example 1.1.7.

1. *Let $r \in R$ and define $\phi_r : R[x] \longrightarrow R$ be defined by $\phi(p(x)) = p(r)$. This is an important class of ring homomorphisms.*
2. *The map $\psi_n : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ defined by $\psi(k) = \overline{k}$ (reduction of k modulo n) is a ring homomorphism.*

Example 1.1.8.

1. *The set of subgroups of $\mathbb{Z}$ given by $n\mathbb{Z}$ ($n \in \mathbb{N} \bigcup \{0\}$) is a set of ideals of $\mathbb{Z}$. Show that this is an exhaustive list of ideals.*
2. *If X is an subset of R then $\langle X \rangle = \{\sum r_i x_i | x_i \in X, r_i \in R\}$ is called the ideal generated by X. Show that the ideal generated by X is*

$$\langle X \rangle = \bigcap_{I \supset X} I$$

where the intersection ranges over all ideals containing X.

Definition 1.1.9. *Let R be a ring.*

1) $u \in R$ is called a unit if there is a $v \in R$ such that $uv = 1$.

2) $z \in R$ is called a zero-divisor if there is a nonzero $x \in R$ such that $zx = 0$.

3) $a \in R$ is called idempotent if $a^2 = a$.

4) $t \in R$ is called nilpotent if there is an $n \in \mathbb{N}$ such that $t^n = 0$.

5) A ring where all the nonzero elements are units is called a field.

6) If R (a commutative ring with 1) has no nonzero zero-divisors, then R is called an (integral) domain.

7) If R is an ring with no nonzero nilpotents, then R is said to be reduced.

The following theorem gives some justification to the standard assumption that ring homomorphisms between commutative rings with identity preserve identities.

Theorem 1.1.10. *Suppose that $\phi : R \longrightarrow T$ is a nonzero ring homomorphism and T is a domain. Then $\phi(1_R) = 1_T$.*

Proof. Let $\phi(1_R) = a$. Since $\phi(1_R) = \phi(1_R)\phi(1_R)$ we have that $a^2 = a$. Equivalently, we write

$$a^2 - a = 0 = a(a - 1_T).$$

Since T is a domain, we must have that either $a = 0$ (which, it is easy to check, implies that ϕ is the zero homomorphism) or $a = 1_T$. Since ϕ is assumed to be nonzero, we obtain

$$\phi(1_R) = a = 1_T$$

and the result is established. □

Proposition 1.1.11. *Let R and T be rings and $\phi : R \longrightarrow T$ a homomorphism.*

1) $\phi(R) = im(\phi)$ is a subring of T.

2) $ker(\phi)$ is an ideal of R.

Proof. Exercise. □

1.2 Ideals

Definition 1.2.1. *Let $I \subsetneq R$ be a proper ideal and $a, b, x \in R$. We say that:*

1) I is prime $ab \in I$ implies that $a \in I$ or $b \in I$.

2) I is maximal if given an ideal J such that $I \subseteq J \subsetneq R$ implies that $J = I$.

3) I is radical if $x^n \in I$ implies that $x \in I$.

Ideals are precisely kernals of ring homomorphisms and are the analog of "normal subgroups" from group theory. In a manner analogous with the situation from group theory, we make the following construction.

Proposition 1.2.2. *Let I be an ideal of R. The quotient group $R/I = \{r+I | r \in R\}$ is a ring with multiplication given by*

$$(r_1 + I)(r_2 + I) = r_1 r_2 + I.$$

We leave the proof as a routine exercise, but before moving on, we note that if R is commutative, then so is R/I and if R has an identity, then so does R/I (what is it?).

One of the many nice applications of quotient rings is that they provide a nice way to characterize some types of ideals. Additionally, sometimes studying R can be made "easier" if one studies R/I which is oftentimes a simpler structure that preserves important properties (if the ideal, I, is chosen sagaciously).

Theorem 1.2.3. *Let R be a commutative ring with identity and $I \subset R$ a proper ideal.*

1. *I is maximal if and only R/I is a field.*

2. *I is prime if and only if R/I is a domain.*

3. *I is radical if and only if R/I is reduced.*

Proof. Suppose that I is maximal and $a \notin I$. We have to show that the coset $a + I$ is a unit in R/I. By the maximality of I, we have that $(a, I) = R$ and hence there is an $r \in R$ and $m \in I$ such that $ra + m = 1$. It is now easy to see that $(a + I)(r + I) = 1 + I$ and hence R/I is a field.

On the other hand, suppose that R/I is a field and let J be an ideal in R such that $I \subseteq J \subsetneq R$. We have to show that $J = I$. Let $j \in J \setminus I$. Since $j \notin I$ and R/I is a field, $j + I$ is a unit in R/I and so there is a coset $x + I$ such that

$$(j + I)(x + I) = 1 + I = jx + I.$$

We conclude that there is an $\alpha \in I \subseteq J$ such that $jx + \alpha = 1$ and hence $1 \in J$. This is a contradiction. Hence $J \setminus I = \emptyset$, and so $J = I$.

The other parts are similar and left as exercises. □

Corollary 1.2.4. *Any maximal ideal is prime and any prime ideal is radical.*

A direct proof of this result is striaghtforward, but we use the above.

Proof. Field $\implies$ integral domain $\implies$ reduced. □

The next result shows that any commutative ring with identity possess a maximal (hence prime, hence radical) ideal. This result depends on a special case of the axiom of choice called Zorn's Lemma. We briefly recall Zorns' Lemma.

Zorn's Lemma: Let S be a partially ordered set with the property that any chain in S has an upper bound in S. Then S has a maximal element.

Theorem 1.2.5. *Let R be a commutative ring with identity. Then R has a maximal ideal. More specifically, is $I \subset R$ is a proper ideal, then I is contained in a maximal ideal.*

Proof. We begin by proving the second, slightly stronger statement.

Let $I \subset R$ be a proper ideal and $S = \{J \subsetneq R | J \text{ is an ideal with } I \subseteq J\}$. Note that the set S is nonempty since $I \in S$.

To apply Zorn, we must show that any chain in S has an upper bound in S. To this end, let $\mathfrak{C} = \{J_\alpha\}_{\alpha \in \Lambda}$ be a chain in S (that is, if J_α and J_β are elements of $\mathfrak{C}$, then $J_\alpha \subseteq J_\beta$ or $J_\beta \subseteq J_\alpha$). Let $M = \bigcup_{\alpha \in \Lambda} J_\alpha$. It is clear that if M is an element of S, then M is our desired upper bound.

To see that M is an element of S, we must show that it is a proper ideal containing I. To see that M is an ideal, we first let $x, y \in M$. Since $M \bigcup \alpha \in \Lambda$ we have that for some $\alpha, beta$, $x \in J_\alpha$ and $y \in J_\beta$ without loss of generality, we will assume that $J_{alpha} \subseteq J_\beta$ and hence $x, y \in J_\beta$. Since J_β is an ideal, we have that $x - y \in J_\beta \subseteq M$. Also since $x \in J_\beta$ and J_β is an ideal, then $rx \in J_\beta \subseteq M$ for all $r \in R$. This establishes the fact that M is an ideal.

Now we have to establish that M is a *proper* ideal. If M is not proper, then $1 \in M = \bigcup_{\alpha \in \Lambda} J_\alpha$ and hence $1 \in J_\alpha$ for some $\alpha \in \Lambda$, but this is a contradiction since each J_α is assumed to be proper.

Since any chain has an upper bound, we apply Zorn's lemma to obtain that the set S has a maximal element $\mathfrak{M}$, hence $I \subseteq \mathfrak{M}$ where $\mathfrak{M}$ is a maximal ideal.

The weaker statement now follows since we can take I to be the zero ideal (which is proper, since R has an identity).

□

1.3 Operations on Ideals and the Homomorphism Theorems

Theorem 1.3.1. *Let $A_1, A_2, \cdots, A_n, B$ be ideals of R. Then the following sets form ideals of R.*

1. $A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n | a_i \in A_i\}$.
2. $A_1 A_2 \cdots A_n = \{\sum_{i=1}^{k} a_1 a_2 \cdots a_n | a_i \in A_i\}$.

Additionally, we have the following.

a) $(A_1 + A_2) + A_3 = A_1 + (A_2 + A_3)$.

b) $(A_1 A_2) A_3 = A_1 (A_2 A_3)$.

c) $B(A_1 + A_2 + \cdots + A_n) = BA_1 + BA_2 + \cdots + BA_n$.

Proof. Exercise. □

Theorem 1.3.2. *If $\phi : R \longrightarrow T$ is a ring homomorphism, then ϕ induces an isomorphism*

$$\overline{\phi} : R/ker(\phi) \longrightarrow im(\phi).$$

Proof. We define $\overline{\phi}(r + \ker(\phi)) = \phi(r)$. We will first show that $\overline{phi}$ is well-defined.

Suppose that $x + \ker(\phi) = y + \ker(\phi)$. This means that $x - y \in \ker(\phi)$ and hence $\phi(x - y) = 0$ (equivalently, $\phi(x) = \phi(y)$), and hence $\overline{\phi}(x + \ker(\phi)) = \overline{\phi}(y + \ker(\phi))$.

With this in hand, it is easy to see that $\overline{\phi}$ is a homomorphism. It remains to show that $\overline{\phi}$ is one to one and onto. The "onto" part is easy (since the target is $\text{im}(\phi)$). To see that $\overline{\phi}$ is one to one, we assume that $x+\ker(\phi)$ is in the kernal of $\overline{\phi}$. This means that $\phi(x) = 0$ and hence $x \in \ker(\phi)$ and so the coset $x + \ker(\phi)$ is the zero coset. □

Bibliography