ABSTRACT ALGEBRA II
IDEALS & FACTOR RINGS

MARIO L. GUTIERREZ ABED

Homomorphisms & Factor Rings

Theorem. *Let $\phi\colon \mathcal{R} \longrightarrow \mathcal{R}'$ be a ring homomorphism with kernel H. Then the additive cosets of H form a ring $\mathcal{R}/H$ whose binary operations, defined by choosing coset representatives, are the usual operations of addition and multiplication of cosets. In addition, the map $\mu\colon \mathcal{R}/H \longrightarrow \phi[\mathcal{R}]$ defined by $\mu(a+H) = \phi(a)$ is an isomorphism.*

Remark: It can be shown that the map $\phi\colon \mathbb{Z} \longrightarrow \mathbb{Z}_n$ defined by $\phi(m) = r$ (where $m \in \mathbb{Z}$ and r is the remainder of m when divided by n) is a homomorphism. Since $\ker(\phi) = n\mathbb{Z}$, the above theorem tells us that the ring $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$.

The above theorem can be extended to subrings of a ring $\mathcal{R}$ other than the kernel. That is, it generally applies to ideals[1]:

Theorem. *Let $\mathcal{I}$ be an ideal of of a ring $\mathcal{R}$. Then the additive cosets of $\mathcal{I}$ form a ring $\mathcal{R}/\mathcal{I}$ whose binary operations, defined by choosing coset representatives, are the usual operations of addition and multiplication of cosets. This ring $\mathcal{R}/\mathcal{I}$ is called the **factor ring** (or **quotient ring**) of $\mathcal{R}$ by $\mathcal{I}$.*

Theorem. *Let $\mathcal{I}$ be an ideal of of a ring $\mathcal{R}$. Then $\gamma\colon \mathcal{R} \to \mathcal{R}/\mathcal{I}$, given by $\gamma(x) = x + \mathcal{I}$ is a ring homomorphism with kernel $\mathcal{I}$.*

Theorem (Fundamental Ring Homomorphism Theorem). *Let $\phi\colon \mathcal{R} \to \mathcal{R}'$ be a ring homomorphism with kernel $\mathcal{I}$. Then $\phi[\mathcal{R}]$ is a ring, and the map $\mu\colon \mathcal{R}/\mathcal{I} \to \phi[\mathcal{R}]$ given by $\mu(x+\mathcal{I}) = \phi(x)$ is an isomorphism. If $\gamma\colon \mathcal{R} \to \mathcal{R}/\mathcal{I}$ is the homomorphism given by $\gamma(x) = x + \mathcal{I}$, then for each $x \in \mathcal{R}$, we have $\phi(x) = \mu\gamma(x)$.*

Prime & Maximal Ideals

The following examples show that a ring $\mathcal{R}$ and a factor ring $\mathcal{R}/\mathcal{I}$ may have very different structural properties:

Example: We know that $\mathbb{Z}$ is an integral domain but not a field. Now let p be a prime, so that $\mathbb{Z}_p$ is a field. But $\mathbb{Z}_p$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, so we have that a factor ring of an integral domain may be a field. ▲

[1] Recall that an ***ideal*** is an additive subgroup (which is also a subring) $\mathcal{I}$ of a ring $\mathcal{R}$ satisfying the properties
$$a\mathcal{I} \subseteq \mathcal{I} \qquad \text{and} \qquad \mathcal{I}b \subseteq \mathcal{I} \qquad \forall\, a, b \in \mathcal{R}.$$

Example: We know that $\mathbb{Z} \times \mathbb{Z}$ is not an integral domain because

$$(0,1)(1,0) = (0,0),$$

showing that $(0,1)$ and $(1,0)$ are zero divisors.

Now let $\mathcal{I} = \{(0,n) \mid n \in \mathbb{Z}\}$, which is an ideal of $\mathbb{Z} \times \mathbb{Z}$, and notice that $(\mathbb{Z} \times \mathbb{Z})/\mathcal{I}$ is isomorphic to $\mathbb{Z}$ under the correspondence $[(m,0) + \mathcal{I}] \leftrightarrow m$, where $m \in \mathbb{Z}$. Thus we have that a factor ring of a ring may be an integral domain, even though the original ring is not. ▲

Example: The subset $\mathcal{I} = \{0,3\}$ of $\mathbb{Z}_6$ is easily seen to be an ideal of $\mathbb{Z}_6$, and $\mathbb{Z}_6/\mathcal{I}$ has three elements, namely $0 + \mathcal{I}$, $1 + \mathcal{I}$, and $2 + \mathcal{I}$. These add and multiply in such a fashion as to show that $\mathbb{Z}_6/\mathcal{I} \simeq \mathbb{Z}_3$ under the correspondence

$$(0 + \mathcal{I}) \leftrightarrow 0, \qquad (1 + \mathcal{I}) \leftrightarrow 1, \qquad (2 + \mathcal{I}) \leftrightarrow 2.$$

This example shows that even if $\mathcal{R}$ is not an integral domain, it is still possible for $\mathcal{R}/\mathcal{I}$ to be a field. ▲

Reamrk: Note that while $\mathbb{Z}$ is an integral domain, $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}_6$ is not. So whereas the preceding examples showed that a factor ring may have a structure that seems "better" than the original ring, this example indicates that the structure of a factor ring may seem "worse" than that of the original ring.

Theorem. *If $\mathcal{R}$ is a ring with unity, and $\mathcal{I}$ is an ideal of $\mathcal{R}$ containing a unit, then $\mathcal{I} = \mathcal{R}$.*

Proof. Let $\mathcal{I}$ be an ideal of $\mathcal{R}$, and suppose that $u \in \mathcal{I}$ for some unit u in $\mathcal{R}$. Then the condition

$$r\mathcal{I} \subseteq \mathcal{I} \quad \forall\, r \in \mathcal{R} \tag{$\dagger$}$$

implies, if we take $r = u^{-1}$ and $u \in \mathcal{I}$, that $1 = u^{-1}u$ is in $\mathcal{I}$. But then ($\dagger$) implies that $r1 = r$ is in $\mathcal{I}$ for all $r \in \mathcal{R}$, so $\mathcal{I} = \mathcal{R}$. □

Corollary. *A field contains no proper nontrivial ideals.*

Proof. Since every nonzero elements of a field is a unit, it follows from the above theorem that an ideal of a field F is either $\{0\}$ or all of F. □

Definition. *An ideal $\mathcal{I}$ in a ring $\mathcal{R}$ is said to be a* ***maximal ideal*** *if $\mathcal{I} \neq \mathcal{R}$ and if whenever $\mathcal{J}$ is an ideal satisfying $\mathcal{I} \subseteq \mathcal{J} \subseteq \mathcal{R}$ then either $\mathcal{J} = \mathcal{I}$ or $\mathcal{J} = \mathcal{R}$.*

Here is one reason why maximal ideals are important:

Theorem. *Let $\mathcal{R}$ be a commutative ring with unity and let $\mathcal{I}$ be an ideal in $\mathcal{R}$. Then the quotient ring $\mathcal{R}/\mathcal{I}$ is a field if and only if $\mathcal{I}$ is a maximal ideal.*

Proof. ($\Rightarrow$) Suppose that $\mathcal{R}/\mathcal{I}$ is a field. By a previous proposition we know that if $\mathcal{N}$ is any ideal of $\mathcal{R}$ such that $\mathcal{I} \subset \mathcal{N} \subset \mathcal{R}$ and $\gamma\colon \mathcal{R} \to \mathcal{R}/\mathcal{I}$ is the canonical homomorphism of $\mathcal{R}$ onto $\mathcal{R}/\mathcal{I}$, then $\gamma[\mathcal{N}]$ is an ideal of $\mathcal{R}/\mathcal{I}$ with

$$\{(0+\mathcal{I})\} \subset \gamma[\mathcal{N}] \subset \mathcal{R}/\mathcal{I}.$$

But this is contrary to a previous corollary which says that a field does not contain any proper nontrivial ideals. Hence if $\mathcal{R}/\mathcal{I}$ is a field, then the ideal $\mathcal{I}$ is maximal.

($\Leftarrow$) Conversely, suppose $\mathcal{I}$ is maximal in $\mathcal{R}$. Observe that if $\mathcal{R}$ is a commutative ring with unity, then $\mathcal{R}/\mathcal{I}$ is also a nonzero commutative ring with unity if $\mathcal{I} \neq \mathcal{R}$, which is indeed the case if $\mathcal{I}$ is maximal.

Now let $(a+\mathcal{I}) \in \mathcal{R}/\mathcal{I}$, with $a \notin \mathcal{I}$, so that $a+\mathcal{I}$ is not the additive identity element in $\mathcal{R}/\mathcal{I}$. Suppose that $a+\mathcal{I}$ has no multiplicative inverse in $\mathcal{R}/\mathcal{I}$. Then the set

$$(\mathcal{R}/\mathcal{I})(a+\mathcal{I}) = \{(r+\mathcal{I})(a+\mathcal{I}) \mid (r+\mathcal{I}) \in \mathcal{R}/\mathcal{I}\}$$

does not contain $1+\mathcal{I}$. We can easily see that $(\mathcal{R}/\mathcal{I})(a+\mathcal{I})$ is an ideal of $\mathcal{R}/\mathcal{I}$, which is nontrivial because $a \notin \mathcal{I}$ and it is also proper because it does not contain $1+\mathcal{I}$.

Now consider the canonical homomorphism $\gamma\colon \mathcal{R} \to \mathcal{R}/\mathcal{I}$ and notice that $\gamma^{-1}[(\mathcal{R}/\mathcal{I})(a+\mathcal{I})]$ is a proper ideal of $\mathcal{R}$ properly containing $\mathcal{I}$. But this contradicts our assumption that $\mathcal{I}$ is maximal, so $a+\mathcal{I}$ must have a multiplicative inverse in $\mathcal{R}/\mathcal{I}$, and thus $\mathcal{R}/\mathcal{I}$ must be a field. □

Example: Since $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$, and $\mathbb{Z}_n$ itself is a field if and only if n is a prime, we see that the maximal ideals of $\mathbb{Z}$ are precisely the ideals $p\mathbb{Z}$ for prime positive integers p. ▲

Corollary. *A commutative ring with unity is a field if and only if it has no proper nontrivial ideals.*

Definition. *An ideal $\mathcal{I} \neq \mathcal{R}$ in a commutative ring $\mathcal{R}$ is a* ***prime ideal*** *if $ab \in \mathcal{I}$ implies either $a \in \mathcal{I}$ or $b \in \mathcal{I}$ for $a, b \in \mathcal{R}$.*

Example: Note that $\mathbb{Z} \times \{0\}$ is a prime ideal of $\mathbb{Z} \times \mathbb{Z}$, for if $(a,b)(c,d) \in \mathbb{Z} \times \{0\}$, then we must have $bd = 0$ in $\mathbb{Z}$. This implies that either $b = 0$, so that $(a,b) \in \mathbb{Z} \times \{0\}$, or $d = 0$, so that $(c,d) \in \mathbb{Z} \times \{0\}$. Note that

$$(\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times \{0\}) \cong \mathbb{Z},$$

which is an integral domain. ▲

Theorem. *Let $\mathcal{R}$ be a commutative ring with unity, and let $\mathcal{I} \neq \mathcal{R}$ be an ideal in $\mathcal{R}$. Then $\mathcal{R}/\mathcal{I}$ is an integral domain if and only if $\mathcal{I}$ is a prime ideal in $\mathcal{R}$.*

Proof. This is a painfully trivial result. Let $\mathcal{R}/\mathcal{I}$ be an integral domain and notice that for any two elements $a+\mathcal{I}, b+\mathcal{I} \in \mathcal{R}/\mathcal{I}$, where $a, b \in \mathcal{R}$, we have

$$(a+\mathcal{I})(b+\mathcal{I}) = ab+\mathcal{I}.$$

Now notice that if $ab+\mathcal{I} = \mathcal{I}$, then we must have that either $a \in \mathcal{I}$ or $b \in \mathcal{I}$, since the coset $\mathcal{I}$ plays the role of 0 in $\mathcal{R}/\mathcal{I}$, and by the definition of an integral domain $\mathcal{R}/\mathcal{I}$ has no zero divisors. But looking at the coset representatives, we see that this condition amounts to saying that $ab \in \mathcal{I}$ implies that either $a \in \mathcal{I}$ or $b \in \mathcal{I}$, which is in fact the definition of a prime ideal. □

Corollary. *Every maximal ideal in a commutative ring $\mathcal{R}$ with unity is a prime ideal.*

Remember well the following results:

For a commutative ring $\mathcal{R}$ with unity:

- An ideal $\mathcal{I}$ of $\mathcal{R}$ is maximal $\iff$ $\mathcal{R}/\mathcal{I}$ is a field.
- An ideal $\mathcal{I}$ of $\mathcal{R}$ is prime $\iff$ $\mathcal{R}/\mathcal{I}$ is an integral domain.
- Every maximal ideal of $\mathcal{R}$ is a prime ideal.

Prime Fields

Theorem. *If $\mathcal{R}$ is a ring with unity 1, then the map $\phi\colon \mathbb{Z} \to \mathcal{R}$ given by*

$$\phi(n) = n \cdot 1 \qquad \forall n \in \mathbb{Z}$$

is a homomorphism from $\mathbb{Z}$ into $\mathcal{R}$.

Corollary. *If $\mathcal{R}$ is a ring with unity and characteristic $n > 1$, then $\mathcal{R}$ contains a subring isomorphic to $\mathbb{Z}_n$. If $\mathcal{R}$ has characteristic 0, then $\mathcal{R}$ contains a subring that is isomorphic to $\mathbb{Z}$.*

Theorem. *A field F is either of prime characteristic p and contains a subfield isomorphic to $\mathbb{Z}_p$, or of characteristic 0 and contains a subfield isomorphic to $\mathbb{Q}$.*

Note: The above results indicate that every field contains either a subfield isomorphic to $\mathbb{Z}_p$ for some prime p, or a subfield isomorphic to $\mathbb{Q}$. Hence these fields $\mathbb{Z}_p$ and $\mathbb{Q}$ are the fundamental building blocks on which all fields rest:

Definition. *The fields $\mathbb{Z}_p$ and $\mathbb{Q}$ are **prime fields**.*

Definition. *Let $\mathcal{R}$ be a ring with identity and let $a \in \mathcal{R}$. The **principal ideal** generated by a is the ideal*

$$\langle a \rangle = \{ra \mid r \in \mathcal{R}\}.$$

*An integral domain $\mathcal{R}$ in which every ideal is a principal ideal is called a **principal ideal domain**.*

Example: Every ideal of the ring $\mathbb{Z}$ is of the form $n\mathbb{Z}$, which is generated by n. Thus every ideal of $\mathbb{Z}$ is a principal ideal. ▲

Example: The ideal $\langle x \rangle \in F[x]$ consists of all polynomials in $F[x]$ having zero constant term. ▲

Note: The next theorem is another simple but very important application of the division algorithm for $F[x]$:

Theorem. *If F is a field, every ideal in $F[x]$ is principal.*

Proof. See page 250, *Fraleigh*'s. □

Note: We can now characterize the maximal ideals of $F[x]$. This is a crucial step in achieving our basic goal: to show that any nonconstant polynomial $f(x) \in F[x]$ has a zero in some field E containing F.

Theorem. *An ideal $\langle p(x) \rangle \neq \{0\}$ of $F[x]$ is maximal if and only if $p(x)$ is irreducible over F.*

Proof. ($\Rightarrow$) Suppose that $\langle p(x) \rangle \neq \{0\}$ is a maximal ideal of $F[x]$. Then $\langle p(x) \rangle \neq F[x]$, so $p(x) \notin F$. Now let $p(x) = f(x)g(x)$ be a factorization of $p(x)$ in $F[x]$. Since $\langle p(x) \rangle$ is a maximal ideal and in turn also a prime ideal, we have that

$$f(x)g(x) \in \langle p(x) \rangle \quad \Longrightarrow \quad f(x) \in \langle p(x) \rangle \quad \text{or} \quad g(x) \in \langle p(x) \rangle.$$

In other words, we must have that either $f(x)$ or $g(x)$ has $p(x)$ as a factor. But then we cannot have the degrees of both $f(x)$ and $g(x)$ less than the degree of $p(x)$. This shows that $p(x)$ is irreducible over F.

($\Leftarrow$) Conversely, if $p(x)$ is irreducible over F, suppose that $\mathcal{I}$ is an ideal such that $\langle p(x) \rangle \subseteq \mathcal{I} \subseteq F[x]$. Now we have that $\mathcal{I}$ is a principal ideal, so that $\mathcal{I} = \langle g(x) \rangle$ for some $g(x) \in \mathcal{I}$. But then

$$p(x) \in \mathcal{I} \quad \Longrightarrow \quad p(x) = g(x)q(x) \quad \text{for some } \ q(x) \in F[x].$$

But $p(x)$ is irreducible, which implies that either $g(x)$ or $q(x)$ is of degree 0.

If $g(x)$ is of degree 0, that is, a nonzero constant in F, then $g(x)$ is a unit in $F[x]$, so $\langle p(x) \rangle = \mathcal{I} = F[x]$.

If on the other hand, $q(x)$ is of degree 0, then $q(x) = c$, where $c \in F$, and $g(x) = (1/c)p(x)$ is in $\langle p(x) \rangle$, so $\mathcal{I} = \langle p(x) \rangle$. Thus $\langle p(x) \rangle \subset \mathcal{I} \subset F[x]$ is impossible, so $\langle p(x) \rangle$ is maximal. $\square$

Example: As we have shown on the section on *factorization of polynomials over a field*, the polynomial $f(x) = x^3 + 3x + 2$ is irreducible in $\mathbb{Z}_5[x]$, so $\mathbb{Z}_5[x]/\langle x^3 + 3x + 2 \rangle$ is a field.

As another example, the polynomial $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, so $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$ is a field. ▲