# Chapter 1

# Rings

We have spent the term studying groups. A group is a set with a binary operation that satisfies certain properties. But many algebraic structures—such as $\mathbb{R}$, $\mathbb{Z}$, and $\mathbb{Z}_n$—come with two binary operations, usually called addition and multiplication. These structures are examples of ***rings***. In this chapter, we define rings and look at some general properties of rings. However, we will mostly restrict ourselves to the particular kinds of rings known as ***integral domains*** and ***fields***.

**Definition 1.1.** A ***ring*** $R$ consists of a set and two binary operations on that set. We will refer to the operations on the set as ***addition*** and ***multiplication***, and we will denote them as $a+b$ and $ab$ (or occasionally $a \cdot b$). A ring must be an Abelian group under addition. The multiplication operation must be associative ($(a(bc) = (ab)c$ for all $a, b, c \in R$), and multiplication must be distributive over addition, both from the left and from the right ($(a(b+c) = ab+ac$ and $(a+b)c = ac + bc$ for all $a, b, c \in R$).

A ring is, in particular, an Abelian group under addition, so there is an additive identity and every element of the ring has an additive inverse. We will always denote the additive identity of the ring by 0, and the additive inverse of an element $a$ of $R$ will be denoted $-a$. As usual, we will abbreviate $a + (-b)$ as $a - b$, and we will refer to the operation $a - b$ as ***subtraction***.

Note that a ring is **not** a group under multiplication: There does not have to be a multiplicative identity element, and multiplicative inverses do not have to exist. Also note that multiplication is not assumed to be commutative. This allows us to define several special kinds of groups in which multiplication is assumed to have some extra properties. In particular, we will deal exclusively with commutative rings and mostly with commutative rings with identity:

**Definition 1.2.** A ***commutative ring*** $R$ is a ring in which multiplication is commutative. That is, $ab = ba$ for all $a, b \in R$.

**Definition 1.3.** An ***identity*** in a ring $R$ is an element $1 \in R$ that serves as

both a left and right identity for multiplication. That is, $a1 = 1a = a$ for all $a \in R$. We will always denote the multiplicative identity by 1.

In a commutative ring, of course, it is only necessary to assume that 1 is a left identity, since the fact that it is a right identity as well follows immediately by commutativity. Similarly, in a commutative ring, it is enough to assume that multiplication is left-distributive over addition. Many of the algebraic structures that you are familiar with are examples of commutative rings with identity.

**Example 1.1.** The set of integers, $\mathbb{Z}$, is a commutative ring with identity under the usual addition and multiplication operations.

**Example 1.2.** For any positive integer $n$, $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ is a commutative ring with identity under the operations of addition and multiplication modulo $n$.

**Example 1.3.** The set $T = \{0\}$ with addition and multiplication defined by $0 + 0 = 0$ and $0 \cdot 0 = 0$ is a commutative ring with identity. $T$ is called the ***trivial ring***. Note that in $T$, $0 = 1$. The converse is also true: Any ring that satisfies $0 = 1$ is the trivial ring. (See the exercises.)

**Example 1.4.** The rational, real, and complex numbers, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, are commutative rings with identity.

**Example 1.5.** The subset $\mathbb{Q}[i]$of $\mathbb{C}$ defined by $\mathbb{Q}[i] = \{a+bi \mid a, b \in \mathbb{Q}\}$ contains 0 and 1 and is closed under addition and multiplication. $\mathbb{Q}[i]$ is a commutative ring with identity under the operations that it inherits from $\mathbb{C}$.

**Example 1.6.** Let $C([0,1])$ be the set of continuous, real-valued functions from the closed interval $[0,1]$ to $\mathbb{R}$. We can add and multiply functions using pointwise operations. That is, for $f, g \in C([0,1])$, we can define a sum $f+g$ and a product $fg$ by $(f+g)(x) = f(x) + g(x)$ and $(fg)(x) = (f(x))(g(x))$ for all $x \in \mathbb{R}$. With these operations, $C([0,1])$ is a commutative ring with identity. The additive identity is the function with constant value 0. The multiplicative identity is the function with constant value 1. Note that some functions, such as $f(x) = x^2+1$, have multiplicative inverses, while others, such as $g(x) = x - x^2$, do not.

Consider the ring $\mathbb{Z}_{12}$. This ring contains pairs of non-zero elements, such as 4 and 3, whose product is zero (since $4 \cdot 3 = 0$ in the ring $\mathbb{Z}_{12}$). The existence of such elements, called ***zero-divisors***, leads to other surprising properties. For example, in a ring with zero-divisors, the cancellation rule does not hold; that is, it is not possible to conclude from $a \neq 0$ and $ab = ac$ that $b = c$. To avoid these problems, we will work mostly with rings that have no zero-divisors.

**Definition 1.4.** An ***integral domain*** $D$ is a commutative ring with identity which has no zero-divisors. That is, if $a$ and $b$ are elements of $D$ such that $ab = 0$, then either $a$ is 0 or $b$ is 0.

We note that $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are integral domains, and that $\mathbb{Z}_n$ is an integral domain if and only if $n$ is prime. With the basic definitions out of the way, we can list some of the basic properties of rings.

**Theorem 1.1.** *Let $R$ be a commutative ring with identity. Then*

1. $0a = 0$ — *zero times anything is zero*
2. $(-1)a = -a$ — *the additive inverse of $a$ is $-1$ times $a$*
3. $a(b - c) = ab - ac$ — *multiplication distributes over subtraction*

*Proof.* Let $a \in R$. Then $0a = (0 + 0)a$, since 0 is the identity for addition. By the distributive rule, $(0 + 0)a = 0a + 0a$. So we get that $0a = 0a + 0a$. Adding $-0a$ to both sides then gives $0 = 0a$, which proves part 1. For part 2, we note that $a + (-1)a = 1a + (-1)a = (1 + (-1))a = 0a = 0$. The fact that $a + (-1)a = 0$ says that $(-1)a$ is the additive inverse of $a$. Since we denote the additive inverse of $a$ by $-a$, this means that $(-1)a = -a$. Finally, for part 3, $a(b-c) = a(b+(-c)) = ab+a(-c) = ab+a(-1)c = ab+(-1)(ac) = ab-ac$. □

**Theorem 1.2.** *Let $D$ be an integral domain. Let $b, c \in D$ and let $a$ be a non-zero element of $D$. Suppose that $ab = ac$. Then $b = c$.*

*Proof.* Adding $-ac$ to both sides of the equation gives $ab - ac = 0$. By the distributive rule, this becomes $a(b - c) = 0$. Since $D$ is an integral domain, we can have $a(b - c) = 0$ only if either $a = 0$ or $b - c = 0$. Since we are assuming that $a$ is not zero, we must have $b - c = 0$. This is equivalent to $b = c$. □

**Theorem 1.3.** *Let $D$ be an integral domain. Let $a$ be an element of $D$ that satisfies $a^2 = a$. Then either $a = 0$ or $a = 1$.*

*Proof.* We can rewrite the equation $a^2 = a$ as $a(a - 1) = 0$. Since $D$ is an integral domain, this implies that either $a = 0$ or $a - 1 = 0$. In the latter case, we have $a = 1$. □

The fact that $a0 = 0$ for any $a$ in a ring shows that a non-trivial ring can never be a group under multiplication, since 0 cannot have a multiplicative inverse. In a commutative ring with identity, a given element might or might not have a multiplicative inverse. If the inverse does exist, then it is unique (by the same proof that is used to show the uniqueness of an inverse in a group). A commutative ring in which every non-zero element has a multiplicative inverse is called a "field":

**Definition 1.5.** Let $R$ be a commutative ring with identity. A ***unit*** in $R$ is an element $a \in R$ that has a multiplicative inverse. That is, there exists an element $a^{-1} \in R$ such that $a \cdot a^{-1} = 1$.

**Definition 1.6.** A ***field*** $F$ is a commutative ring with identity in which every non-zero element is a unit. That is, any $a \in F$ with $a \neq 0$ has a multiplicative inverse. In a non-trivial field, the set $F^* = F \setminus \{0\}$ is an Abelian group under multiplication, with identity 1.

Note that any field $F$ is automatically an integral domain. $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields. $\mathbb{Z}$ is not a field. $\mathbb{Z}_n$ is a field if and only if $n$ is a prime number.

## Exercises

**1.** In Theorem 1.1, what does "$-1$" refer to?

**2.** Show that $\mathbb{Z}_n$ is an integral domain if and only if $n$ is prime.

**3.** Suppose that $R$ is a commutative ring with identity in which $1 = 0$. Show that $R = \{0\}$.

**4.** Show that $\mathbb{Q}[i]$, which was defined in example 5 above, is a field.

**5.** Show that $C([0, 1])$ is not an integral domain by finding two non-zero functions $f$ and $g$ such that $fg = 0$. (Hint: You can't use polynomials or any functions defined by single, simple formulas!)

**6.** Show that any field is an integral domain.

**7.** Show that any finite integral domain is a field. (Hint: Let $a$ be a non-zero element of a finite integral domain, and consider the sequence of powers $a$, $a^2$, $a^3$, ....) Note that from this exercise and exercise 2, it follows that $\mathbb{Z}_n$ is a field if and only if $n$ is prime.

**8.** Find an integer $n$ and an element $a \in \mathbb{Z}_n$ such that $a \neq 0$ and $a \neq 1$, but $a^2 = a$.

**9.** A ***subring*** of a ring can be defined as a subset that is closed under both addition and multiplication. Show by example that a non-trivial subring of a commutative ring with identity does not have to contain the multiplicative identity 1. (Hint: Look at subrings of $\mathbb{Z}$.)

**10.** Let $D$ be an integral domain and suppose $R$ is a non-trivial subring of $D$. Suppose that $R$ has a multiplicative identity. Show that the multiplicative identity in $R$ must be the same as the multiplicative identity of $D$. Show by example that the same is not necessarily true when $D$ is simply a commutative ring with identity. (Hint: For an example, look at subrings of $\mathbb{Z}_6$.)

# Chapter 2

# Homomorphisms and Ideals

Homomorphisms between rings can be defined similarly to group homomorphisms: as operation-preserving maps. Many ideas about group homomorphisms carry over to rings. In the case of rings, the analog of a normal subgroup is called an ideal. An ideal can be the kernel of a ring homomorphism, and given an ideal $I$ in a ring $R$, we can form a quotient ring $R/I$. In this chapter, we will look at ring homomorphisms, ideals, and quotient rings. To avoid some of the complications that arise in the more general case, the discussion is restricted to commutative rings. In fact, we will be most interested in integral domains. However, much of what is covered here can be extended to non-commutative rings.

**Definition 2.1.** Let $R$ and $S$ be commutative rings. A ***ring homomorphism*** from $R$ to $S$ is a function $h\colon R \to S$ that is operation preserving for both addition and multiplication. That is for any $a, b \in R$, $h(a+b) = h(a) + h(b)$ and $h(ab) = h(a)h(b)$. A ***ring isomorphism*** is a ring homomorphism that is one-to-one and onto.

In particular, a ring homomorphism from $R$ to $S$ is a homomorphism of the additive groups. When we talk about the "kernel" of a ring homomorphism, we mean its kernel when it is considered as a homomorphism of the additive groups:

**Definition 2.2.** Let $R$ and $S$ be commutative rings, and let $h\colon R \to S$ be a ring homomorphism. We define the ***kernel*** of $h$, denoted $\mathrm{Ker}(h)$, as $\mathrm{Ker}(h) = h^{-1}(0) = \{a \in R \mid h(a) = 0\}$.

$\mathrm{Ker}(h)$ is automatically a subgroup of $R$ considered as an additive group, but it has additional properties owing to the fact that $h$ also preserves multiplication. $\mathrm{Ker}(h)$ is closed under multiplication, but in fact, much more is true: $\mathrm{Ker}(h)$ is closed under multiplication by any element of $R$:

**Theorem 2.1.** *Let $R$ and $S$ be commutative rings, and let $h\colon R \to S$ be a ring homomorphism. Let $K = \mathrm{Ker}(h)$. Then for any $a \in K$ and any $r \in R$, $ar \in K$.*

*Proof.* Suppose $a \in K$ and $r \in R$. Since $a \in K$, $h(a) = 0$. To show that $ar \in K$, we only need to show that $h(ar) = 0$. But $h(ar) = h(a)h(r) = 0 \cdot h(r) = 0$. □

We define an ideal to be a subset of a ring that satisfies the same properties as the kernel of a ring homomorphism:

**Definition 2.3.** Let $R$ be a commutative ring. An ***ideal*** in $R$ is a subset $I \subseteq R$ which is closed under addition and is closed under multiplication by any element of $R$. That is, for any $a, b \in I$ and any $r \in R$, we also have $a + b \in I$ and $ar \in I$. Note that $I = \{0\}$ is an ideal in $R$; it is called the ***trivial ideal***. Also, $R$ is an ideal in $R$. An ideal in $R$ is said to be a ***proper ideal*** if it is a proper subset of $R$.

Ideals play the same role in ring theory that is played by normal subgroups in group theory. Given an ideal $I$ in a ring $R$, we can form a quotient ring $R/I$. We then get a homomorphism $h\colon R \to R/I$ that has kernel $I$. This shows that every ideal is the kernel of some ring homomorphism. Thus, the concepts "ideal" and "kernel of a ring homomorphism" are equivalent.

**Definition 2.4.** Let $R$ be a commutative ring and let $I$ be an ideal in $R$. Since $I$ is a subgroup of the additive group $R$, we can form the quotient group $R/I$. We make $R/I$ into a ring by defining $(a + I)(b + I) = (ab) + I$ for $a, b \in R$. The ring $R/I$ is called a ***quotient ring***. If $R$ is a commutative ring with identity, then $R/I$ is also a commutative ring with identity, and its identity is $1 + I$, where 1 is the identity in $R$.

For this definition to be valid, the multiplication defined on $R/I$ must be well-defined. It must also be associative and must distribute over the addition defined on the additive group $R/I$. The proofs are left as exercises.

**Theorem 2.2.** *Let $R$ be a commutative ring and let $I$ be an ideal in $R$. Then the function $h\colon R \to R/I$ defined by $h(a) = a+I$ for $a \in R$ is a ring homomorphism. Furthermore,* $\mathrm{Ker}(h) = I$. *Thus, a subset of $R$ is an ideal if and only if it is the kernel of some ring homomorphism.*

*Proof.* From group theory, we know that $h$ is a homomorphism of additive groups and that $\mathrm{Ker}(h) = I$. It only remains to show that $h$ preserves the operation of multiplication. But this follows immediately, since for any $a, b \in R$, $h(ab) = (ab) + I = (a + I)(b + I) = h(a)h(b)$. □

**Theorem 2.3.** *Let $R$ and $S$ be a commutative rings, and let $h\colon R \to S$ be a ring homomorphism. Then*

1. *If $J$ is an ideal in $S$, then $h^{-1}(J)$ is an ideal in $R$.*
2. *If $h$ is onto and if $I$ is an ideal in $R$, then $h(I)$ is an ideal in $S$.*

*Proof.* For part 1, suppose that $J$ is an ideal in $S$. From group theory, we already know that $h^{-1}(J)$ is a subgroup of $R$ considered as an additive group, so we only need to show that $h^{-1}(J)$ is closed under multiplication by any

element of $R$. Let $a \in h^{-1}(J)$ and let $r \in R$. We must show that $ar \in h^{-1}(J)$. Since $a \in h^{-1}(J)$, we have by definition that $h(a) \in J$. Also, we have $h(r) \in S$. Since $J$ is an ideal in $S$, it is closed under multiplication by any element of $S$, so $h(a)h(r) \in S$. Since $h(a)h(r) = h(ar)$, we have $h(ar) \in S$. By definition of $h^{-1}(J)$, this means that $ar \in h^{-1}(J)$, which is what we wanted to show.

For part 2, suppose that $h$ is onto and that $I$ is an ideal in $R$. We already know that $h(I)$ is a subgroup of $S$ considered as an additive group, so we only need to show that $h(I)$ is closed under multiplication by any element of $S$. Let $b \in h(I)$, and let $s \in S$. We must show that $bs \in h(I)$. Since $b \in h(I)$, we can find $a \in I$ such that $b = h(a)$. Since $h$ is onto, we can find $r \in R$ such that $s = h(r)$. Since $I$ is an ideal in $R$ and $a \in I$ and $r \in R$, we know that $ar \in I$. It follows then that $h(ar) \in h(I)$. Since $h(ar) = h(a)h(r) = bs$, this means that $bs \in h(I)$, which is what we wanted to show. □

It should be no surprise that an important example of ring homomorphism is the map $h\colon \mathbb{Z} \to \mathbb{Z}_n$ given by $h(a) = a \mod n$ for all $a \in \mathbb{Z}$. The kernel of this homomorphism is the set of all integers that are evenly divisible by $n$. This set is an ideal and so is closed under multiplication by any element of $\mathbb{Z}$. This can be seen directly, of course: If $a$ is evenly divisible by $n$ and $k \in \mathbb{Z}$, then $ka$ is also evenly divisible by $n$.

In the context of rings, it is natural to denote the ideal of integral multiples of $n$ as $n\mathbb{Z}$, with the meaning $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$. This ideal is generated by $n$ in a certain sense, and it will be useful to have a name for an ideal that is generated by a single element in a similar sense. Such an ideal is called a principal ideal.

**Definition 2.5.** Let $R$ be a commutative ring and let $a \in R$. We define the ***principal ideal*** generated by $a$ to be the set $aR = \{ar \mid r \in \mathbb{R}\}$.

The proof of the fact that $aR$ is an ideal is left as an exercise. Note that $aR$ is the smallest ideal in $R$ that contains $a$ in the sense that any ideal $I$ in $R$ that contains $a$ must satisfy $aR \subseteq I$. This is clear since $I$ is closed under multiplication by any element of $R$: Since $a \in I$, we must have $ar \in I$ for every $r \in R$. Principal ideals will play an important role in the next chapter.

We will find a smaller variety of ideals when looking at the other common examples of rings, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. These rings are fields, and the following theorem will imply that fields don't have very many ideals.

**Theorem 2.4.** *Let $R$ be a commutative ring with identity and let $I$ be an ideal in $R$. Let $u \in R$ be a unit. (That is, $u$ has a multiplicative inverse $u^{-1}$.) If $u \in I$, then $I = R$. In particular $I$ is a proper ideal if and only if $1 \notin I$. Furthermore, for any $a \in R$, the principal ideal $aR$ is equal to $R$ if and only if $a$ is a unit.*

*Proof.* Let $u$ be a unit in $R$, and let $I$ be an ideal in $R$ that contains $u$. Since $u \in I$ and $I$ is an ideal, we also have $ur \in I$ for any $r \in R$. Taking $r = u^{-1}$, we get that $uu^{-1} \in I$. That is, $1 \in I$. So, any ideal that contains a unit also contains 1. We show that the only ideal that contains 1 is all of $R$.

Let $I$ be an ideal that contains 1. Certainly, $I \subseteq R$, so to show that $I = R$, it is sufficient to show that $R \subseteq I$. Let $r \in R$. Since $I$ is an ideal, we know that $ar \in I$ for any $a \in I$. Since $1 \in I$, we can take $a = 1$, giving $1r \in I$. Since $1r = r$, this means $r \in I$. So, $R \subseteq I$.

We have shown that a proper ideal does not contain 1. Conversely, of course, if an ideal does not contain 1, then it is by definition proper. So, an ideal in a commutative ring with identity is proper if and only if it does not contain 1.

To prove the last assertion of the theorem, let $a$ be any element of $R$. If $a$ is a unit, then $aR$ is an ideal that contains a unit, so by the first part of the theorem $aR = R$. Conversely, suppose that $aR = R$. Then, in particular, $1 \in aR$, which means that there is some $b \in R$ with $1 = ab$. This means $b$ is a multiplicative inverse for $a$, and therefor that $a$ is a unit. □

Since every non-zero element in a field is a unit, this theorem shows that a field has no non-trivial, proper ideals. This means that if $F$ is a field and $h\colon F \to R$ is a ring homomorphism, the kernel of $h$ must be either $\{0\}$ or all of $F$. That is, either $h$ maps everything in $F$ to 0, or $F$ is one-to-one.

Fields do play an interesting role as images of ring homomorphisms. To see why, we need to look at maximal ideals.

**Definition 2.6.** Let $R$ be a commutative ring. A ***maximal ideal*** $M$ in $R$ is a proper ideal that is not contained in any larger proper ideal. Equivalently, $M$ is a maximal ideal if it is a proper ideal and for any ideal $I$ such that $M \subseteq I$, it must be the case that either $I = M$ or $I = R$.

Thus, for a maximal ideal $M$ in a ring $R$, there is no ideal $I$ that lies strictly between $M$ and $R$ in the sense that $M \subsetneq I \subsetneq R$. For example, in a field $F$, the trivial ideal $\{0\}$ is a maximal ideal: Since $\{0\}$ and $F$ are the only ideals in $F$, there are no ideals that lie strictly between $\{0\}$ and $F$. Perhaps this fact hints at the following important theorem:

**Theorem 2.5.** *Let $R$ be a commutative ring with identity. Let $I$ be a proper ideal in $R$. Then $I$ is a maximal ideal in $R$ if and only if the quotient ring $R/I$ is a field.*

*Proof.* The proof will use the homomorphism $h\colon R \to R/I$ defined by $h(a) = a + I$ for $a \in R$. Note that this homomorphism is onto, so we can apply both parts of Theorem 2.3.

Suppose that $I$ is a maximal ideal in $R$. We must show that $R/I$ is a field. That is, we must show that every non-zero element $a + I$ in $R/I$ has a multiplicative inverse. Let $a + I$ be a non-zero element of $R/I$. Consider the principal ideal $J$ generated by $a + I$ in $R/I$, and let $\overline{J} = h^{-1}(J)$. By Theorem 2.3, $\overline{J}$ is an ideal in $R$. $\overline{J}$ certainly contains $I$ (since $0 \in J$ and $I = h^{-1}(0)$). Since $I$ is a maximal ideal in $R$, we must have either $\overline{J} = I$ or $\overline{J} = R$. We know that $a \in \overline{J}$, and we know that $a \notin I$ since $h(a) = a + I$ is a non-zero element in $R/I$. This means $\overline{J} \neq I$. So, we must have $\overline{J} = R$. This can only happen if $J$ is all of $R/I$. That is, the principal ideal generated by $a + I$ in $R/I$ is the entire

ring $R/I$. By the previous theorem, $a+I$ must be a unit in $R/I$, which is what we wanted to show.

Conversely, suppose that the quotient ring $R/I$ is a field. Suppose that $J$ is an ideal in $R$ such that $I \subseteq J \subseteq R$. To show that $I$ is maximal, we must show that $J$ can only be $I$ or $R$. Let $K = h(J)$. Note that $h^{-1}(K) = J$. By Theorem 2.3, $K$ is an ideal in $R/I$. Since $R/I$ is a field, $K$ can only be $\{0\}$ or all of $R/I$. If $K = \{0\}$, then $J = h^{-1}(K) = h^{-1}(0) = I$. If $K = R/I$ then $J = h^{-1}(R/I) = R$. So we have that $J$ is either $I$ or $J$, as we wanted to show. □

## Exercises

**1.** Let $R$ be a commutative ring. Show that the intersection of two ideals in $R$ is an ideal.

**2.** Let $R$ be a commutative ring and let $I$ be an ideal in $R$. Show that the multiplication on $R/I$ that was specified in the definition of $R/I$ is well-defined.

**3.** Let $R$ be a commutative ring and let $I$ be an ideal in $R$. Show that if $R$ has multiplicative identity 1, then $1 + I$ is a multiplicative identity in $R/I$.

**4.** Deleted. [The problem origianally listed here was incorrect.]

**5.** Suppose that $D$ and $E$ are integral domains, and suppose that $h\colon D \to E$ is a ring homomorphism that maps $D$ **onto** $E$. Show that $h(1) = 1$ (where the 1 on the left means the identity in $D$ and the 1 on the right is the identity in $E$). (Hint: Consider $h(1 \cdot 1)$.

**6.** Let $R$ be a commutative ring and let $a \in R$. Show that the principal ideal $aR$ is in fact an ideal by showing that it is closed under addition and under multiplication by any element of $R$.

**7.** Let $n$ be an integer greater than or equal to 2. Show that the principal ideal $n\mathbb{Z}$ in $\mathbb{Z}$ is a maximal ideal if and only if $n$ is a prime number. (Note in particular that a ring can have many different maximal ideals.)

**8.** Consider the principal ideal $6\mathbb{Z}$ in $\mathbb{Z}$. Find two different ideals $I$ in $\mathbb{Z}$ that satisfy $6\mathbb{Z} \subsetneq I \subsetneq \mathbb{Z}$.

**9.** Show that every ideal in $\mathbb{Z}$ is a principal ideal. (Not all rings have this property. A ring in which it is true is called a ***principal ideal domain***.)

**10.** Consider two principal ideals $a\mathbb{Z}$ and $b\mathbb{Z}$ in $\mathbb{Z}$. Find the intersection $a\mathbb{Z} \cap b\mathbb{Z}$.

# Chapter 3

# Polynomials

One significant factor behind the development of abstract algebra was the effort to find roots of polynomials. The quadratic equation for the roots of a second-degree polynomial was known since ancient times, and formulas for third and fourth-degree polynomials were discovered in modern times. No one, however, was able to find a formula for the roots of a fifth-degree polynomial. One of the major achievements of abstract algebra was the proof—by Evariste Galois in the 1830s—that no such formula is possible. We are not even close to being able to cover this work, but we are in a position to prove an interesting theorem about the existence of roots of polynomials. You are familiar with polynomials in which the coefficients are real numbers. In fact, we can consider polynomials with coefficients in any commutative ring. The basic definitions carry over from the familiar case.

**Definition 3.1.** Let $R$ be a commutative ring. We define the ***ring of polynomials with coefficients in*** $\mathbf{R}$ to be the set of all polynomials of the form $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, where $n$ is a non-negative integer and $a_0, a_1, \ldots, a_n \in R$. Such polynomials are added and multiplied in the usual way, and under these operations, they form a ring. We denote this ring as $R[x]$. If $p(x)$ is the polynomial $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, and if $a_n \neq 0$, then $n$ is called the ***degree*** of $p(x)$. Note that by this definition, a constant polynomial $p(x) = a$, for $a \in R$ with $a \neq 0$ has degree zero. We will also consider the constant polynomial $p(x) = 0$ to have degree 0.

It is assumed that you know what is meant by saying that "polynomials are added and multiplied in the usual way." $R[x]$ is in fact a commutative ring in which the additive identity is the constant polynomial 0. If $R$ has a multiplicative identity, 1, then the constant polynomial 1 is a multiplicative identity in $R[x]$. Also note that we can consider $R$ to be a subring of the polynomial ring $R[x]$ if we identify each $a \in R$ with the constant polynomial with value $a$.

Note that if $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ and $q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$, then the highest order term in the product $p(x)q(x)$ is $a_nb_mx^{n+m}$.

In the general case of a ring $R$ that contains zero-divisors, $a_n b_m$ can be zero even if $a_n \neq 0$ and $b_n \neq 0$. This is very different from familiar polynomials and leads to other undesirable consequences. So we will restrict our discussion to integral domains. (Recall that an integral domain is a commutative ring with identity and no zero-divisors.)

Let $D$ be an integral domain. Let $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ and $q(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m$ be non-zero polynomials in $D[x]$ of degree $n$ and $m$ respectively. That is, $a_n \neq 0$ and $b_m \neq 0$. Since $D$ is an integral domain, it follows that $a_n b_m \neq 0$, and therefor that the product $p(x)q(x)$ is a non-zero polynomial of degree $m + n$. So, the polynomial ring $D[x]$ is also an integral domain. We state this as a theorem:

**Theorem 3.1.** *Let $D$ be an integral domain. Then the polynomial ring $D[x]$ is also an integral domain. In particular, if $F$ is a field, then $F[x]$ is an integral domain (but not a field).*

It follows that the polynomial rings $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, and $\mathbb{Z}_p[x]$ for a prime number $p$ are integral domains.

You might remember that you can do long division with polynomials and find quotients and remainders in much the same way that you do with integers. The ability to write "$b = qa + r$" in the case of integers was a very powerful tool. The same is true for polynomials with coefficients in a field. The proof amounts, basically, to doing the long division. (We need the coefficients to lie in a field $F$ so that we can divide by non-zero elements of $F$. The theorem is stated here without proof. If you want to see a proof, you can find one on pages 286–287 in our textbook.)

**Theorem 3.2.** *(The Division Algorithm for Polynomials) Let $F$ be a field. Let $b(x)$ and $a(x)$ be polynomials in $F[x]$. Then there exist unique polynomials $q(x)$ and $r(x)$ that satisfy: $b(x) = q(x)a(x) + r(x)$, and either $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $a(x)$.*

In the case of $p(x) \in F[x]$, where $F$ is a field, we can use the division algorithm to prove the analog of a basic fact of elementary algebra: $a$ is a root of $p(x)$ if and only if $x - a$ is a factor of $p(x)$. See the exercises. We need some obvious definitions:

**Definition 3.2.** Let $R$ be a ring, and let $p(x) \in R[x]$. Write $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$. For $b \in R$, we define the ***value of*** $p(x)$ ***at*** $b$ to be the element $p(b)$ of $R$ defined by $p(b) = a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n$. In the case where $p(b) = 0$, we say that $b$ is a ***root*** of $p(x)$ in $R$.

Using the division algorithm, we can also prove a fundamental fact about the ring of polynomials with coefficients in a field: Every ideal in such a ring is a principal ideal.

**Theorem 3.3.** *Let $F$ be a field. Let $I$ be an ideal in the polynomial ring $F[x]$. Then $I$ is a principal ideal. That is, there is a polynomial $p(x) \in F[x]$ such that $I = p(x) \cdot F[x] = \{p(x)q(x) \mid q(x) \in F[x]\}$.*

*Proof.* Let $a(x)$ be a non-zero element of $I$ that has minimal degree among all non-zero elements of $I$. We show that $I$ is the principal ideal generated by $a(x)$. Certainly, $a(x) \cdot F[x] \subseteq I$, since $a(x) \in I$ and $I$ is closed under multiplication by arbitrary elements of $F[x]$. We only need to show that $I \subseteq a(x) \cdot F[x]$. Let $b(x)$ be an arbitrary element of $I$. We want to show that $b(x) = a(x)q(x)$ for some $q(x) \in F[x]$. From the division algorithm, we know that $b(x) = a(x)q(x) + r(x)$, for some $q(x), r(x) \in F[x]$ where $r(x)$ is either zero or has degree less than the degree of $a(x)$. But then $r(x) = b(x) - a(x)q(x)$. Since $a(x)$ and $b(x)$ are in the ideal $I$ and $q(x) \in F[x]$, $r(x) \in I$ by closure of $I$ under addition and under multiplication by an arbitrary element of $F[x]$. Since $a(x)$ has minimal degree among non-zero elements of $I$, and $r(x) \in I$, this means that the degree of $r(x)$ cannot be less than the degree of $a(x)$. The only alternative is $r(x) = 0$. So in fact, $b(x) = a(x)q(x)$, as we wanted to show. □

A ring in which every ideal is a principal ideal is called a principal ideal domain, so we have shown that for a field $F$, $F[x]$ is a principal ideal domain. It is interesting to consider the **maximal** ideals in $F[x]$. These are just ideals that are generated by irreducible polynomials.

**Definition 3.3.** Let $F$ be a field, and let $p(x) \in F[x]$. $p(x)$ is said to be ***irreducible over*** **F** if it has degree greater than 0 and if it cannot be written as a product $p(x) = a(x)b(x)$ where $a(x)$ and $b(x)$ are polynomials in $F[x]$ of lower degree than $p(x)$.

For example, the polynomial $x^2 + 1$ is irreducible over $\mathbb{R}$, but it is reducible over $\mathbb{C}$ since it can be written in the form $x^2 + 1 = (x - i)(x + i)$. Similarly, $x^2 - 2$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$.

**Theorem 3.4.** *Let $F$ be a field and let $I$ be an ideal in the polynomial ring $F[x]$. Then $I$ is a maximal ideal in $F[x]$ if and only if $I$ is a principal ideal $I = p(x) \cdot F[x]$, where $p(x)$ is an irreducible polynomial over $F$.*

*Proof.* Suppose that $I$ is a maximal ideal. We know from the previous theorem that $I = p(x) \cdot F[x]$ for some $p(x) \in F[x]$. We know from the proof of that theorem that $p(x)$ has minimal degree among all the elements of $I$. We only need to show that $p(x)$ is irreducible. Suppose not. Then $p(x) = a(x)b(x)$ for some polynomials $a(x)$ and $b(x)$ of lower degree than $p(x)$. Consider the principal ideal $J = a(x) \cdot F[x]$. By Exercise 4, $I \subsetneq J$. Now, $a(x)$ cannot be a constant polynomial, since its degree is equal to the degree of $p(x)$ minus the degree of $b(x)$. Since every element of $J$ has degree greater than or equal to the degree of $a(x)$, $J$ is a proper ideal. We have shown that $I \subsetneq J \subsetneq F[x]$. But this contradicts the fact that $I$ is a maximal ideal. From this contradiction, we conclude that $p(x)$ is irreducible.

Conversely, suppose that $I = p(x) \cdot F[x]$, where $p(x)$ is an irreducible polynomial over $F$. We want to show that $I$ is maximal. Suppose not. Then there is an ideal $J$ in $F[x]$ such that $I \subsetneq J \subsetneq F[x]$. Since every ideal in $F[x]$ is principal, $J = b(x) \cdot F[x]$ for some $b[x] \in F[x]$. Since $p(x) \in I \subseteq J = b[x] \cdot F[x]$, we must have $p(x) = b(x)a(x)$ for some $a(x) \in F[x]$. Now, $a(x)$ can't be zero, since $p(x)$

is not. Also, $a(x)$ cannot be a non-zero constant $a(x) = a$, since if it were we would have $b(x) = a^{-1}p(x)$, which would imply $I = J$. This means that both $a(x)$ and $b(x)$ must be polynomials of lower degree than $b(x)$. But that means that $p(x)$ is not irreducible over $F$. This contradiction shows that $I$ must be maximal. □

We also know from the previous chapter that an ideal $I$ in $F[x]$ is maximal if and only if $F[x]/I$ is a field. Let $p(x)$ be an irreducible polynomial over $F$. Let $E$ be the quotient ring $F[x]/(p(x) \cdot F[x])$. Since $p(x) \cdot F[x]$ is a maximal ideal in $F[x]$, $E$ is also a field. Furthermore, the field $E$ contains an isomorphic copy of $F$ in a natural way (identifying $a \in F$ with the coset $a + (p(x) \cdot F[x])$ in $F[x]/(p(x) \cdot F[x])$). We consider $F$ to be a subfield of $E$ and say that $E$ is an ***extension field*** of $F$. Since $F \subseteq E$, we can consider $p(x)$ to be a polynomial over $E$. The punch line to this whole excursion into the theory of polynomial rings is the fact that $p(x)$ has a root in $E$. That is, given an irreducible polynomial $p(x)$ over a field $F$, we have constructed an extension field $E$ of $F$ in which $p(x)$ has a root.

**Theorem 3.5.** *Let $F$ be a field and let $p(x) \in F[x]$ be an irreducible polynomial over $F$. Let $E$ be the field $F[x]/(p(x) \cdot F[x])$, and let $\phi\colon F[x] \to E$ be the homomorphism that maps $g(x) \in F[x]$ to the coset $g(x) + (p(x) \cdot F[x])$ in $E$. Let $a = \phi(x)$. Then $a$ is a root of $p(x)$ in $E$.*

*Proof.* $p(a) = p(\phi(x)) = \phi(p(x)) = 0$ □

As an example of this theorem, consider the polynomial $x^2 + 1$, which is an irreducible polynomial over $\mathbb{R}$. By the theorem, $x^2 + 1$ has a root in the field $\mathbb{R}[x]/((x^2 + 1) \cdot \mathbb{R}[x])$. It can be shown that this field is in fact isomorphic to the field of complex numbers $\mathbb{C}$. So, we have found a roundabout but elegant construction for the complex numbers in which they arise out of a general construction that works for manufacturing a root for any irreducible polynomial over any field.

## Exercises

1. Let $D$ be an integral domain. What are the *units* in the polynomial ring $D[x]$?
2. Let $F$ be a field and let $p(x)$ be a polynomial with coefficients in $F$. Let $a \in F$. Show that the remainder when $p(x)$ is divided by the polynomial $x - a$ is the constant polynomial with value $p(a)$. Deduce that $a$ is a root of $p(x)$ if and only if $p(x) = (x - a)q(x)$ for some $q(x) \in F[x]$.
3. Let $F$ be a field. Show that a polynomial $p(x) \in F[x]$ of degree 2 is irreducible if and only if it has no root in $F$.
4. Let $F$ be a field. Let $p(x) \in F[x]$. Suppose that $p(x) = a(x)b(x)$ where $a(x)$ and $b(x)$ are polynomials in $F[x]$ of lower degree than $F[x]$. Show that the principal ideal $p(x) \cdot F[x]$ is a proper subset of the principal ideal $a(x) \cdot F[x]$.
5. Let $F$ be a field and let $p(x)$ be any polynomial of degree greater than zero in $F[x]$. Prove that there is an extension field of $F$ in which $p(x)$ has a root. (Note that $p(x)$ is not assumed to be irreducible!)