# Chapter 8

# An Introduction to Rings

## 8.1 Definitions and Examples

Recall that a group is a set together with a single binary operation, which together satisfy a few modest properties. Loosely speaking, a ring is a set together with two binary operations (called addition and multiplication) that are related via a distributive property.

**Definition 8.1.** A **ring** $R$ is a set together with two binary operations $+$ and $\cdot$ (called **addition** and **multiplication**, respectively) satisfying the following:

(i) $(R, +)$ is an abelian group.

(ii) $\cdot$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

(iii) The **distributive property** holds: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ for all $a, b, c \in R$.

**Remark 8.2.** We make a couple comments about notation.

(a) We often write $ab$ in place $a \cdot b$.

(b) The additive inverse of the ring element $a \in R$ is denoted $-a$.

**Theorem 8.3.** Let $R$ be a ring. Then for all $a, b \in R$:

(a) $0a = a0 = 0$

(b) $(-a)b = a(-b) = -(ab)$

(c) $(-a)(-b) = ab$

**Definition 8.4.** A ring $R$ is called **commutative** if multiplication is commutative.

**Definition 8.5.** A ring $R$ is said to have an **identity** (or called a **ring with 1**) if there is an element $1 \in R$ such that $1a = a1 = a$ for all $a \in R$.

**Problem 8.6.** Justify that $\mathbb{Z}$ is a commutative ring with 1 under the usual operations of addition and multiplication. Which elements have multiplicative inverses in $\mathbb{Z}$?

**Problem 8.7.** Justify that $\mathbb{Z}_n$ is a commutative ring with 1 under addition and multiplication mod $n$.

**Problem 8.8.** Consider the set $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Which elements have multiplicative inverses in $\mathbb{Z}_{10}$?

**Problem 8.9.** For each of the following, find a positive integer $n$ such that the ring $\mathbb{Z}_n$ does not have the stated property.

(a) $a^2 = a$ implies $a = 0$ or $a = 1$.

(b) $ab = 0$ implies $a = 0$ or $b = 0$.

(c) $ab = ac$ and $a \neq 0$ imply $b = c$.

**Theorem 8.10.** If $R$ is a ring with 1, then the multiplicative identity is unique and $-a = (-1)a$.

**Problem 8.11.** Requiring $(R, +)$ to be a group is fairly natural, but why require $(R, +)$ to be abelian? Suppose $R$ has a 1. Compute $(1 + 1)(a + b)$ in two different ways.

**Definition 8.12.** A ring $R$ with 1 (with $1 \neq 0$) is called a **division ring** if every nonzero element in $R$ has a multiplicative inverse: if $a \in R \setminus \{0\}$, then there exists $b \in R$ such that $ab = ba = 1$.

**Definition 8.13.** A commutative division ring is called a **field**.

**Definition 8.14.** A nonzero element $a$ in a ring $R$ is called a **zero divisor** if there is a nonzero element $b \in R$ such that either $ab = 0$ or $ba = 0$.

**Problem 8.15.** Are there any zero divisors in $\mathbb{Z}_{10}$? If so, find all of them.

**Problem 8.16.** Are there any zero divisors in $\mathbb{Z}_5$? If so, find all of them.

**Problem 8.17.** Provide an example of a ring $R$ and elements $a, b \in R$ such that $ax = b$ has more than one solution. How does this compare with groups?

**Theorem 8.18** (Cancellation Law)**.** Assume $a, b, c \in R$ such that $a$ is not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$.

**Definition 8.19.** Assume $R$ is a ring with 1 with $1 \neq 0$. An element $u \in R$ is called a **unit** in $R$ if $u$ has a multiplicative inverse (i.e., there exists $v \in R$ such that $uv = vu = 1$). The set of units in $R$ is denoted $U(R)$.

**Problem 8.20.** Consider the ring $\mathbb{Z}_{20}$.

(a) Find $U(\mathbb{Z}_{20})$.

(b) Find the zero divisors of $\mathbb{Z}_{20}$.

(c) Any observations?

**Theorem 8.21.** If $U(R) \neq \emptyset$, then $U(R)$ forms a group under multiplication.

**Remark 8.22.** We make a few observations.

(a) A field is a commutative ring $F$ with identity $1 \neq 0$ in which every nonzero element is a unit, i.e., $U(F) = F \setminus \{0\}$.

(b) Zero divisors can never be units.

(c) Fields never have zero divisors.

**Definition 8.23.** A commutative ring with identity $1 \neq 0$ is called an **integral domain** if it has no zero divisors.

**Remark 8.24.** The Cancellation Law (Theorem 8.18) holds in integral domains for any three elements.

**Theorem 8.25.** Any finite integral domain is a field.

**Example 8.26.** Here are a few examples. Details left as an exercise.

(a) **Zero Ring**: If $R = \{0\}$, we can turn $R$ into a ring in the obvious way. The zero ring is a finite commutative ring with 1. It is the only ring where the additive and multiplicative identities are equal. The zero ring is not a division ring, not a field, and not an integral domain.

(b) **Trivial Ring:** Given any abelian group $R$, we can turn $R$ into a ring by defining multiplication via $ab = 0$ for all $a, b \in R$. Trivial rings are commutative rings in which every nonzero element is a zero divisor. Hence a trivial ring is not a division ring, not a field, and not a integral domain.

(c) The integers form an integral domain, but $\mathbb{Z}$ is not a division ring, and hence not a field.

(d) The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are fields under the usual operations of addition and multiplication.

(e) The group of units $U(\mathbb{Z}_n)$ is the set of elements in $\mathbb{Z}_n$ that are relatively prime to $n$. All other nonzero elements are zero divisors. It turns out that $\mathbb{Z}_n$ forms a finite field if and only if $n$ is prime.

(f) The set of even integers $2\mathbb{Z}$ forms a commutative ring under the usual operations of addition and multiplication. However, $2\mathbb{Z}$ does not have a 1, and hence cannot be a division ring nor a field nor an integral domain.

(g) **Polynomial Ring:** Fix a commutative ring $R$. Let $R[x]$ denote the set of polynomials in the variable $x$ with coefficients in $R$. Then $R[x]$ is a commutative ring. Moreover, $R[x]$ is a ring with 1 if and only if $R$ is a ring with 1. The units of $R[x]$ are exactly the units of $R$ (if there are any). So, $R[x]$ is never a division ring nor a field. However, if $R$ is an integral domain, then so is $R[x]$.

(h) **Matrix Ring:** Fix a ring $R$ and let $n$ be a positive integer. Let $M_n(R)$ be the set of $n \times n$ matrices with entries from $R$. Then $M_n(R)$ forms a ring under ordinary matrix addition and multiplication. If $R$ is nontrivial and $n \geq 2$, then $M_n(R)$ always has zero divisors and $M_n(R)$ is not commutative even if $R$ is. If $R$ has a 1, then the matrix with 1's down the diagonal and 0's elsewhere is the multiplicative identity in $M_n(R)$. In this case, the group of units is the set of invertible $n \times n$ matrices, denoted $GL_n(R)$ and called the **general linear group of degree** $n$ **over** $R$.

(i) **Quadratic Field:** Define $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. It turns out that $\mathbb{Q}(\sqrt{2})$ is a field. In fact, we can replace 2 with any rational number that is not a perfect square in $\mathbb{Q}$.

(j) **Hamilton Quaternions:** Define $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, i, j, k \in Q_8\}$ Then $\mathbb{H}$ forms a ring, where addition is definite componentwise in $i$, $j$, and $k$ and multiplication is defined by expanding products and the simplifying using the relations of $Q_8$. It turns out that $\mathbb{H}$ is a non-commutative ring with 1.

**Problem 8.27.** Find an example of a ring $R$ and an element $a \in R \setminus \{0\}$ such that $a$ is neither a zero divisor nor a unit.

**Definition 8.28.** A **subring** of a ring $R$ is a subgroup of $R$ that is closed under multiplication.

**Remark 8.29.** The property "is a subring" is clearly transitive. To show that a subset $S$ of a ring $R$ is a subring, it suffices to show that $S \neq \emptyset$, $S$ is closed under subtraction, and $S$ is closed under multiplication.

**Example 8.30.** Here are a few quick examples.

(a) $\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$, which in turn is a subring of $\mathbb{C}$.

(b) $2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

(c) The set $\mathbb{Z}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{Q}(\sqrt{2})$.

(d) The ring $R$ is a subring of $R[x]$ if we identify $R$ with set of constant functions.

(e) The set of polynomials with zero constant term in $R[x]$ is a subring of $R[x]$.

(f) $\mathbb{Z}[x]$ is a subring of $\mathbb{Q}[x]$.

(g) $\mathbb{Z}_n$ is *not* a subring of $\mathbb{Z}$ as the operations are different.

**Problem 8.31.** Consider the ring $\mathbb{Z}_{10}$ from Problem 8.8. Let $S = \{0, 2, 4, 6, 8\}$.

(a) Argue that $S$ is a subring of $\mathbb{Z}_{10}$.

(b) Is $S$ a ring with 1? If so, find the multiplicative identity. If not, explain why.

(c) Is $S$ a field? Justify your answer.

**Problem 8.32.** Suppose $R$ is a ring and let $a \in R$. Define $S = \{x \in R \mid ax = 0\}$. Prove that $S$ is a subring of $R$.

**Problem 8.33.** Consider the ring $\mathbb{Z}$. It turns out that $2\mathbb{Z}$ and $3\mathbb{Z}$ are subrings (but you don't need to prove this). Determine whether $2\mathbb{Z} \cup 3\mathbb{Z}$ is a subring of $\mathbb{Z}$. Justify your answer.

## 8.2 Ring Homomorphisms

**Definition 8.34.** Let $R$ and $S$ be rings. A **ring homomorphism** is a map $\phi : R \to S$ satisfying

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

(b) $\phi(ab) = \phi(a)\phi(b)$

for all $a, b \in R$. The **kernel** of $\phi$ is defined via $\ker(\phi) = \{a \in R \mid \phi(a) = 0\}$. If $\phi$ is a bijection, then $\phi$ is called an **isomorphism**, in which case, we say that $R$ and $S$ are **isomorphic rings** and write $R \cong S$.

**Example 8.35.**

(a) For $n \in \mathbb{Z}$, define $\phi_n : \mathbb{Z} \to \mathbb{Z}$ via $\phi_n(x) = nx$. We see that $\phi_n(x+y) = n(x+y) = nx+ny = \phi_n(x)+\phi_n(y)$. However, $\phi_n(xy) = n(xy)$ while $\phi_n(x)\phi_n(y) = (nx)(ny) = n^2xy$. It follows that $\phi_n$ is a ring homomorphism exactly when $n \in \{0, 1\}$.

(b) Define $\phi : \mathbb{Q}[x] \to \mathbb{Q}$ via $\phi(p(x)) = p(0)$ (called **evaluation at 0**). It turns out that $\phi$ is a ring homomorphism, where $\ker(\phi)$ is the set of polynomials with 0 constant term.

**Problem 8.36.** For each of the following, determine whether the given function is a ring homomorphism. Justify your answers.

(a) Define $\phi : \mathbb{Z}_4 \to \mathbb{Z}_{12}$ via $\phi(x) = 3x$.

(b) Define $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ via $\phi(x) = 5x$.

(c) Let $S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$. Define $\phi : \mathbb{C} \to S$ via $\phi(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

(d) Let $T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$. Define $\phi : T \to \mathbb{Z}$ via $\phi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) = a$.

**Theorem 8.37.** Let $\phi : R \to S$ be a ring homomorphism.

(a) $\phi(R)$ is a subring of $S$.

(b) $\ker(\phi)$ is a subring of $R$.

**Problem 8.38.** Suppose $\phi : R \to S$ is a ring homomorphism such that $R$ is a ring with 1, call it $1_R$. Prove that $\phi(1_R)$ is the multiplicative identity in $\phi(R)$ (which is a subring of $S$). Can you think of an example of a ring homomorphism where $S$ has a multiplicative identity that is not equal to $\phi(1_R)$?

Theorem 8.37(b) states that the kernel of a ring homomorphism is a subring. This is analogous to the kernel of a group homomorphism being a subgroup. However, recall that the kernel of a group homomorphism is also a normal subgroup. Like the situation with groups, we can say something even stronger about the kernel of a ring homomorphism. This will lead us to the notion of an **ideal**.

**Theorem 8.39.** Let $\phi : R \to S$ be a ring homomorphism. If $a \in \ker(\phi)$ and $r \in R$, then $ar, ra \in \ker(\phi)$. That is, $\ker(\phi)$ is closed under multiplication by elements of $R$.

## 8.3 Ideals and Quotient Rings

Recall that in the case of a homomorphism $\phi$ of groups, the cosets of $\ker(\phi)$ have the structure of a group (that happens to be isomorphic to the image of $\phi$ by the First Isomorphism Theorem). In this case, $\ker(\phi)$ is the identity of the associated quotient group. Moreover, recall that every kernel is a normal subgroup of the domain and every normal subgroup can be realized as the kernel of some group homomorphism. 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 $\phi$ is also a group homomorphism of abelian groups and the cosets of $\ker(\phi)$ are of the form $r + I$. More specifically, if $\phi(r) = a$, then $\phi^{-1}(a) = r + I$.

These cosets naturally have the structure of a ring isomorphic to the image of $\phi$:

$$(r + I) + (s + I) = (r + s) + I \tag{8.1}$$

$$(r + I)(s + I) = (rs) + I \tag{8.2}$$

The reason for this is that if $\phi^{-1}(a) = X$ and $\phi^{-1}(b) = Y$, then the inverse image 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 $I$ (all subgroups are normal in abelian groups). When $I$ is the kernel of some ring homomorphism $\phi$, the additive abelian quotient group $R/I$ also has a multiplicative structure defined in (2) above, making $R/I$ into a ring.

*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 group $R$. 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

$$(r+\alpha)(s+\beta)+I = rs+I. \tag{8.3}$$

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

$$\alpha\beta + I = I. \tag{8.4}$$

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 if and only if $I$ is closed under multiplication on the left and right by elements of $R$ (which also forces $I$ to be a subring). Such subrings are called **ideals**.

**Definition 8.40.** Let $R$ be a ring and let $I$ be a subset of $R$.

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

(b) $I$ is an **ideal** (or **two-sided ideal**) if $I$ is both a left and a right ideal.

Here's a summary of everything that just happened.

**Theorem 8.41.** 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:

$$(r+I)+(s+I) = (r+s)+I \tag{8.5}$$

$$(r+I)(s+I) = (rs)+I \tag{8.6}$$

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 $R$.

**Theorem 8.42.** Suppose $I$ and $J$ are ideals of the ring $R$. Then $I \cap J$ is an ideal of $R$.

As you might expect, we have some isomorphism theorems.

**Theorem 8.43** (First Isomorphism Theorem for Rings)**.** If $\phi : R \to S$ is a ring homomorphism, then $\ker(\phi)$ is an ideal of $R$ and $R/\ker(\phi) \cong \phi(R)$.

We also have the expected Second, Third, and Fourth Isomorphism Theorems for rings. The next theorem tells us that a subring is an ideal if and only if it is a kernel of a ring homomorphism.

**Theorem 8.44.** 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 8.45.** Let $A$ be any subset of $R$. Let $(A)$ denote the smallest ideal 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**.

**Remark 8.46.** The following facts are easily verified.

(a) $(A)$ is the intersection of all ideals containing $A$.

(b) If $R$ is commutative, then $(a) = aR := \{ar \mid r \in R\}$.

**Example 8.47.** 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 $n\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if $m$ divides $n$. Moreover, we have $(m, n) = (d)$, where $d$ is the greatest common divisor of $m$ and $n$.

**Problem 8.48.** Consider the ideal $(2, x)$ in $\mathbb{Z}[x]$. Note that $(2, x) = \{2p(x)+xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\}$. Argue that $(2, x)$ is not a principal ideal, i.e., there is no single polynomial in $\mathbb{Z}[x]$ that we can use to generate $(2, x)$.

**Theorem 8.49.** Assume $R$ is a commutative ring with $1 \neq 0$. Let $I$ be an ideal of $R$. Then $I = R$ if and only if $I$ contains a unit.

**Theorem 8.50.** Assume $R$ is a commutative ring with $1 \neq 0$. Then $R$ is a field if and only if its only ideals are $(0)$ and $R$.

Loosely speaking, the previous results say that fields are "like simple groups" (i.e, groups with no non-trivial normal subgroups).

**Corollary 8.51.** If $R$ is a field, then every nonzero ring homomorphism from $R$ into another ring is an injection.

## 8.4 Maximal and Prime Ideals

In this section of notes, we will study two important classes of ideals, namely **maximal** and **prime** ideals, and study the relationship between them. Throughout this entire section, we assume that all rings have a multiplicative identity $1 \neq 0$.

**Definition 8.52.** Assume $R$ is a commutative ring with 1. An ideal $M$ in a ring $R$ is called a **maximal ideal** if $M \neq R$ and the only ideals containing $M$ are $M$ and $R$.

**Example 8.53.** Here are a few examples. Checking the details is left as an exercise.

(a) In $\mathbb{Z}$, all the ideals are of the form $n\mathbb{Z}$ for $n \in \mathbb{Z}^+$. The maximal ideals correspond to the ideals $p\mathbb{Z}$, where $p$ is prime.

(b) Consider the integral domain $\mathbb{Z}[x]$. The ideals $(x)$ (i.e., the subring containing polynomials with 0 constant term) and $(2)$ (i.e, the set of polynomials with even coefficients) are not maximal since both are contained in the proper ideal $(2, x)$. However, as we shall see soon, $(2, x)$ is maximal in $\mathbb{Z}[x]$.

(c) The zero ring has no maximal ideals.

(d) Consider the abelian group $\mathbb{Q}$ under addition. We can turn $\mathbb{Q}$ into a trivial ring by defining $ab = 0$ for all $a, b \in \mathbb{Q}$. In this case, the ideals are exactly the additive subgroups of $\mathbb{Q}$. However, $\mathbb{Q}$ has no maximal subgroups, and so $\mathbb{Q}$ has no maximal ideals.

The next result states that rings with an identity $1 \neq 0$ always have maximal ideals. It turns out that we won't need this result going forward, so we'll skip its proof. However, it is worth noting that all known proofs make use of Zorn's Lemma (equivalent to the Axiom of Choice), which is also true for the proofs that a finitely generated group has maximal subgroups or that every vector spaces has a basis.

**Theorem 8.54.** In a ring with 1, every proper ideal is contained in a maximal ideal.

For commutative rings, there is a very nice characterization about maximal ideals in terms of the structure of their quotient rings.

**Theorem 8.55.** Assume $R$ is a commutative ring with 1. Then $M$ is a maximal ideal if and only if the quotient ring $R/M$ is a field.

**Example 8.56.** We can use the previous theorem to verify whether an ideal is maximal.

(a) Recall that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ and that $\mathbb{Z}_n$ is a field if and only if $n$ is prime. We can conclude that $n\mathbb{Z}$ is a maximal ideal precisely when $n$ is prime.

(b) Define $\phi : \mathbb{Z}[x] \to \mathbb{Z}$ via $\phi(p(x)) = p(0)$. Then $\phi$ is surjective and $\ker(\phi) = (x)$. By the First Isomorphism Theorem for Rings, we see that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. However, $\mathbb{Z}$ is not a field. Hence $(x)$ is not maximal in $\mathbb{Z}[x]$. Now, define $\psi : \mathbb{Z} \to \mathbb{Z}_2$ via $\psi(x) = x \mod 2$ and consider the composite homomorphism $\psi \circ \phi : \mathbb{Z} \to \mathbb{Z}_2$. It is clear that $\psi \circ \phi$ is onto and the kernel of $\psi \circ \phi$ is given by $\{p(x) \in \mathbb{Z}[x] \mid p(0) \in 2\mathbb{Z}\} = (2, x)$. Again by the First Isomorphism Theorem for Rings, $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}_2$. Since $\mathbb{Z}_2$ is a field, $(2, x)$ is a maximal ideal.

**Definition 8.57.** Assume $R$ is a commutative ring with 1. An ideal $P$ is called a **prime ideal** if $P \neq R$ and whenever the product $ab \in P$ for $a, b \in R$, then at least one of $a$ or $b$ is in $P$.

**Example 8.58.** In any integral domain, the 0 ideal $(0)$ is a prime ideal. What if the ring is not an integral domain?

**Remark 8.59.** The notion of a prime ideal is a generalization of "prime" in $\mathbb{Z}$. Suppose $n \in \mathbb{Z}^+ \setminus \{1\}$ such that $n$ divides $ab$. In this case, $n$ is guaranteed to divide either $a$ or $b$ exactly when $n$ is prime. Now, let $n\mathbb{Z}$ be a proper ideal in $\mathbb{Z}$ with $n > 1$ and suppose $ab \in \mathbb{Z}$ for $a, b \in \mathbb{Z}$. In order for $n\mathbb{Z}$ to be a prime ideal, it must be true that $n$ divides either $a$ or $b$. However, this is only guaranteed to be true for all $a, b \in \mathbb{Z}$ when $p$ is prime. That is, the nonzero prime ideals of $\mathbb{Z}$ are of the form $p\mathbb{Z}$, where $p$ is prime. Note that in the case of the integers, the maximal and nonzero prime ideals are the same.

**Theorem 8.60.** Assume $R$ is a commutative ring with 1. Then $P$ is a prime ideal in $R$ if and only if the quotient ring $R/P$ is an integral domain.

**Corollary 8.61.** Assume $R$ is a commutative ring with 1. Every maximal ideal of $R$ is a prime ideal.

**Example 8.62.** Recall that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. Since $\mathbb{Z}$ is an integral domain, it must be the case that $(x)$ is a prime ideal in $\mathbb{Z}[x]$. However, as we saw in an earlier example, $(x)$ is not maximal in $\mathbb{Z}[x]$ since $\mathbb{Z}$ is not a field. This shows that the converse of the previous corollary is not true.