ABSTRACT ALGEBRA
Rings, Integral Domains, and Fields

J.B. Hart

January 7, 2012

Chapter 1

Introduction to Rings

1.1 What Is a Ring?

The concept of a *group* gives us a mathematical structure sufficiently complex to allow us to solve simple linear equations of the form $ax = b$ and $xa = b$. We now turn attention to developing a mathematical structure which will allow us to manipulate polynomials. In high school algebra, the two most important aspects of polynomial manipulation are factoring and finding roots. The mathematical structures we derive must be complex enough to allow us to study both activities in a meaningful way.

Polynomials naturally involve two binary operations — addition and multiplication. Consequently, our model systems should also have two binary operations, one to play the role of "addition" and the other to play the role of "multiplication". The order in which the terms of a polynomial appear should not matter; hence, our addition should be commutative. Since multiplying two polynomials requires that multiplication distributes over addition, we should require the same of our multiplication operation.

A *ring* is a triple $\mathbb{R} = (R, +, \cdot)$, where R is a set, and $+$ and $\cdot$ are binary operations on R. We require $(R, +)$ to be a commutative group, the operation $\cdot$ to be associative, and $a \cdot (b + c) = ab + ac$ and $(b + c) \cdot a = ba + ca$ for all $a, b, c \in R$. (Note that we adopt the usual juxtaposition of letters ab to denote $a \cdot b$ when no confusion will result.)

The identity element of $(R, +)$ will be denoted by 0_R or simply 0 when no confusion will result. We will call this element the *zero* of the ring. In keeping with the additive notation for the group operation, we will let $-x$ denote the group inverse of x. (NOTE: We are not assuming that $-x = (-1)x$; indeed, this equation might not even make sense in a particular context.)

We do not require that $(R, \cdot)$ be a group. If the operation $\cdot$ gives rise to a (multiplicative) identity, we call it the *unity* of $\mathbb{R}$ and denote it by 1_R (or simply

1). We do not require the multiplication to be commutative. When it is, we say the ring is *commutative*.

In a ring $\mathbb{R} = (R, +, *)$, we typically let a^n denote the product of an element a with itself n times (under the ring multiplication) for any positive integer n. We do not define negative powers of a for rings in general and only define a^0 when $\mathbb{R}$ has unity (in which case $a^0 = 1_R$). We sometimes use the symbol na to represent the *sum* of a with itself n times (under the ring addition). This notation has definite disadvantages (since it can be confusing); and we will usually avoid it.

Rings are very common structures. The set $\mathbb{Z} = (Z, +, \cdot)$ of integers under ordinary integer addition and multiplication forms a commutative ring (with unity). The set $\mathbb{Q} = (Q, +, \cdot)$ of rational numbers under ordinary rational addition and multiplication forms a commutative ring (with unity), as does the set $\mathbb{R} = (R, +, \cdot)$ of real numbers and $\mathbb{C} = (C, +, \cdot)$ of complex numbers.

The set $2Z$ of all even integers forms a commutative ring (without unity) under the usual operations of integer addition and multiplication.

Exercise 1.1.1. Let $\mathbf{G} = (G, *)$ be a commutative group. Prove that $(G, +, \cdot)$ is a ring when $a + b = ab$ and $a \cdot b = e$, where e is the identity of $\mathbf{G}$.

Exercise 1.1.2. Show that the set Z_n of integers modulo n forms a commutative ring with unity under ordinary integer addition and multiplication modulo n.

Exercise 1.1.3. Let $Z[i\sqrt{5}] = \{m + in\sqrt{5} : m, n \in Z\}$, where $i = \sqrt{-1}$. Show that $Z[i\sqrt{5}]$ forms a commutative ring with unity under complex addition and multiplication.

Of course, not all rings are commutative. Let $N_2(Z)$ denote the set of all 2×2 matrices with integer entries. Under matrix addition and multiplication, the triple $\mathbb{N}_2(Z) = (N_2(Z), +, \cdot)$ is a noncommutative ring with unity.

Exercise 1.1.4. In high school algebra, when we see an equation like $ab = ac$, we automatically conclude that $b = c$ (if $a \neq 0$). In the ring $\mathbb{N}_2(Z)$ defined above, find matrices A, B, and C such that A is not the zero-matrix, $AB = AC$, but $B \neq C$. (This tells us that the familiar multiplicative cancellation property of integers does not hold in all rings.)

Exercise 1.1.5. In high school algebra, when we see an equation like $ab = 0$, we automatically conclude that $a = 0$ or $b = 0$. In the ring $\mathbb{Z}_4$, find nonzero elements a and b such that $ab = 0$. (In ring theory, such elements are known as *zero-divisors*.)

Exercise 1.1.6. Show that a ring can possess at most one unity.

Let $\mathbf{G} = (G, \cdot)$ be a group. An *endomorphism* is a mapping $f : G \longrightarrow G$ such that $f(ab) = f(a)f(b)$ for all $a, b \in G$. (An endomorphism is just a homomorphism from $\mathbf{G}$ to itself.) Let $\mathtt{Hom}(\mathbf{G})$ denote the set of all endomorphisms on $\mathbf{G}$.

Exercise 1.1.7. Construct the set $\mathtt{Hom}(\mathbf{Z}_2 \times \mathbf{Z}_2)$, where $\mathbf{Z}_2$ is the additive group of integers modulo 2.

Exercise 1.1.8. Construct the set $\mathtt{Hom}(\mathbf{Z}_4)$, where $\mathbf{Z}_4$ is the additive group of integers modulo 4.

Exercise 1.1.9. Let $\mathbf{G} = (G, *)$ be a commutative group. For all $f, g \in \mathtt{Hom}(\mathbf{G})$, let $f + g$ be defined by $(f + g)(x) = f(x) * g(x)$ and let $f \cdot g$ be defined by $(f \cdot g)(x) = f(g(x))$. Show that $\mathbb{H}(\mathbf{G}) = (\mathtt{Hom}(\mathbf{G}), +, \cdot)$ forms a ring under these operations.

Exercise 1.1.10. Let X be any set and let $\mathtt{Su}(X)$ denote the family of all subsets of X (the so-called *powerset* of X. Show that $\mathbb{S}(X) = (\mathtt{Su}(X), \cup, \cap)$ is a commutative ring with unity.

Exercise 1.1.11. Let $\mathbb{R} = (R, +, *)$ be a ring. An element $a \in R$ is *idempotent* provided $a^2 = a$. We say that $\mathbb{R}$ is idempotent if every element of R is idempotent.

1. Let $\mathbb{R}$ be an idempotent ring. Use the fact that $(a + b)^2 = a + b$ for all $a, b \in R$ to prove that $ab = -ba$.
2. Use the previous result and the uniqueness of the additive inverse to prove that an idempotent ring is commutative.
3. Show that every nonzero element of an idempotent ring has additive order 2.

Exercise 1.1.12. An idempotent ring with unity is called a *Boolean* ring. Let X be any set. For $A, B \in \mathtt{Su}(X)$, let $A + B = A \cup B - (A \cap B)$ denote the *disjoint union* of A and B. Show that $\mathbb{B}(X) = (\mathtt{Su}(X), +, \cap)$ is a Boolean ring.

1.2 Zero-Divisors and Units

In this section, we will introduce several key structural properties for rings. Some of these properties hold for all rings, and some do not. We begin with a fundamental result valid for all rings.

Theorem 1.2.1. *Let $\mathbb{R} = (R, +, \cdot)$ be a ring. For all $a, b \in R$, the following are true.*

1. $0_R \cdot a = 0_R = a \cdot 0_R$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$

Proof. We will prove Claims 1 and 2, and leave Claim 3 as an exercise. To prove Claim (1), we will invoke some group properties. In particular, since $0_R = 0_R + 0_R$, we can say that

$$0_R \cdot a = (0_R + 0_R) \cdot a = 0_R \cdot a + 0_R \cdot a$$

by invoking the distributive property for rings. Now, letting $-(0_R \cdot a)$ denote the additive inverse of $0_R \cdot a$, we have

$$0_R = -(0_R \cdot a) + 0_R \cdot a = -(0_R \cdot a) + [0_R \cdot a + 0_R \cdot a]$$

Now, since the group operation $+$ is associative, we know that

$$-(0_R \cdot a) + [0_r \cdot a + 0_R \cdot a] = [-(0_R \cdot a) + 0_R \cdot a] + 0_R \cdot a = [0_R] + 0_R \cdot a = 0_R \cdot a$$

Thus, we see that $0_R = 0_R \cdot a$, as desired. The fact that $0_R = a \cdot 0_R$ is proven similarly.

To prove Claim 2, we must prove that both $a \cdot (-b)$ and $(-a) \cdot b$ act as additive inverses for $a \cdot b$. Observe that

$$a \cdot (-b) + a \cdot b = a \cdot (-b + b) = a \cdot 0_R = 0_R$$

Thus, $a \cdot (-b) = -(a \cdot b)$, as desired. The other equality is proven similarly. □

Exercise 1.2.2. Prove Claim 3 of Theorem 1.2.1.

Exercise 1.2.3. Let $\mathbb{R} = (R, +, *)$ be a ring with unity. Prove that $1_R = 0_R$ if and only if R contains a single element.

Theorem 1.2.1 tells us that some familiar properties from high school algebra hold for arbitrary rings. It is important, however, not to allow this result to lure us into taking too much for granted. In the last section, we saw, for example, that the familiar property of cancellation need not hold in every ring. Of course, cancellation does hold in some rings (like the ring of integers, for example); we will now characterize those rings in which this very convenient property holds.

Let $\mathbb{R} = (R, +, *)$ be a ring and let $a \in R$. We say that a is a *zero-divisor* in $\mathbb{R}$ provided

- $a \neq 0_R$
- There exist $b \neq 0_R$ such that $a * b = 0_R$ or $b * a = 0_R$.

In Exercise 1.1.5 you proved that the ring $\mathbb{Z}_4$ contains zero-divisors. Zero-divisors run counter to our intuition about how multiplication "ought" to work; but they are actually quite common.

Exercise 1.2.4. Show that the ring $\mathbb{N}_2(Z)$ contains zero-divisors.

Exercise 1.2.5. Show that the ring $\mathbb{H}(\mathbf{Z}_2 \times \mathbf{Z}_2)$ contains zero-divisors.

Exercise 1.2.6. Show that an element a of the ring $\mathbb{Z}_n$ is a zero-divisor if and only if $\texttt{gcd}(a, n) > 1$.

Exercise 1.2.7. Let $\mathbb{R} = (R, +, *)$ be a ring and let $a, b \in R$. If a and b are not zero divisors, show that ab and ba are not zero-divisors.

Let $\mathbb{R} = (R, +, *)$ be a ring and let a be a nonzero R. We say that a satisfies the *cancellation law* if, whenever $b, c \in R$ are such that $a*b = a*c$, or $b*a = c*a$, then $b = c$. If every element of R satisfies the cancellation law, then we say that the ring $\mathbb{R}$ is *cancellative*.

We know that the ring $\mathbb{N}_2(Z)$ is not cancellative since it contains elements which do not satisfy the cancellation law. In high school algebra, we know that the cancellation law fails only for one type of equation, namely $0b = 0c$. It turns out this can be generalized.

Theorem 1.2.8. *Let $\mathbb{R} = (R, +, *)$ be a ring. A nonzero element of R satisfies the cancellation law if and only if it is not a zero-divisor.*

Proof. Let a be a nonzero element of R which satisfies the cancellation law. We must prove that a is not a zero-divisor. To this end, suppose $b \in R$ is such that $a * b = 0$ or $b * a = 0$. It will suffice to prove that this forces $b = 0$. By Theorem 1.2.1 we know that $a * 0 = 0$; hence, we know that $a * b = a * 0$. The assumption that a satisfies the cancellation law now tells us that $b = 0$.

Conversely, suppose that a is not a zero-divisor. We want to prove that a satisfies the cancellation law. Since a is not a zero-divisor, we know that whenever $ax = 0$ or $xa = 0$, we must have $x = 0$. Suppose now that $ab = ac$. It follows that $ab - ac = 0$. Now, we know from Theorem 1.2.1 that $-ac = a(-c)$. Hence, we have

$$0 = ab - ac = ab + a(-c) = a(b - c)$$

Therefore, we know that $b - c = 0$, which implies that $b = c$. We can easily modify these arguments and show that assuming instead that $ba = ca$ also implies that $b = c$. Hence, a does indeed satisfy the cancellation law, as desired. □

Exercise 1.2.9. Let $\mathbb{R} = (R, +, *)$ be a finite ring with unity and let $\widehat{R}$ denote the set of all non zero-divisors of R.

1. Let $a \in \widehat{R}$. Show that the set $a\widehat{R} = \{ax : x \in \widehat{R}\}$ contains the same number of elements as $\widehat{R}$. (Hint: Suppose two elements in $a\widehat{R}$ are equal and use cancellation.)
2. Show that for each $a \in \widehat{R}$, there exist $b \in \widehat{R}$ such that $ab = ba = 1$.
3. Show that $\widehat{R}$ forms a group under the ring multiplication.

Corollary 1.2.10. *A ring is cancellative if and only if it contains no zero-divisors.*

We know from experience in high school algebra that the rings of integers, rational, real, and complex numbers are all cancellative. Formal proofs of this would require careful definition of the operations of addition and multiplication on these sets; and as such, are more trouble than we need take on at this time. We will simply take this on faith.

Exercise 1.2.11. Show that the ring $\mathbb{Z}_n$ is cancellative if and only if n is a prime.

Corollary 1.2.12. *The ring $\mathbb{Z}(i\sqrt{5})$ is cancellative.*

Proof. It will suffice to prove that this ring contains no zero-divisors. To this end, let $\alpha = m + in\sqrt{5}$ and let $\beta = u + iv\sqrt{5}$, suppose that $\alpha \neq 0$ and suppose that $\alpha\beta = 0$. We must prove that $\beta = 0$. Observe that

$$\alpha\beta = (mu - 5nv) + i(mv + nu)\sqrt{5}$$

Hence, if $\alpha\beta = 0$, it follows that $mu - 5nv = 0$ and $mv + nu = 0$. Since $\alpha \neq 0$, we know that either $m \neq 0$ or $n \neq 0$. Now, either $m = 0$ or $m \neq 0$.

Suppose first that $m = 0$. This tells us that $n \neq 0$. Furthermore, we must have $5nv = 0$ and $nu = 0$. These facts together tell us that $v = u = 0$ (since the ring of integer does not contain zero-divisors); hence, we know that $\beta = 0$.

Suppose instead that $m \neq 0$. The fact that $mu - 5nv = 0$ tells us that $mu^2 - 5nvu = 0$; and the fact that $mv + nu = 0$ tells us that $m(5v^2) + 5nvu = 0$. Combining these equations tells us that

$$m(u^2 + 5v^2) = 0$$

Since we are assuming that $m \neq 0$, we know that $u^2 + 5nv^2 = 0$ since $\mathbb{Z}$ does not contain zero-divisors. It follows that $u = v = 0$; hence, $\beta = 0$ in this case as well. □

Let $\mathbb{R} = (R, +, *)$ be a ring with unity 1. An element $a \in R$ is a *unit* in R provided there exist $b \in R$ such that $ab = ba = 1$. When a is a unit, it has a multiplicative inverse under the ring multiplication; it is common to use a^{-1} to denote this element.

Exercise 1.2.13. Let $\mathbb{R}$ be a ring with unity 1. If $a \in R$ is a unit, prove that a is not a zero-divisor.

Exercise 1.2.14. Suppose that $\mathbb{R} = (\{0, 1, a, b\}, +, *)$ is a ring. If a and b are units, write out the multiplication table for $\mathbb{R}$.

Exercise 1.2.15. Find elements of the ring $\mathbb{N}_2(Z)$ which are neither zero-divisors nor units.

Exercise 1.2.16. Show that an element of the ring $\mathbb{Z}_n$ is a unit if and only if it is not a zero-divisor.

Exercise 1.2.17. Let $\mathbb{R} = (R, +, *)$ be a ring with unity and let $a, b \in R$. If a and b are units, show that ab is a unit (with $(ab)^{-1} = b^{-1}a^{-1}$).

Exercise 1.2.18. Let $\mathbb{R} = (R, +, *)$ be any ring with unity and let U_R denote its set of units. Show that U_R forms a group under the ring multiplication.

Exercise 1.2.19. Let Z^∞ denote the set of all infinite sequences of integers. If $a \in Z^\infty$, we will let $a[i]$ denote the ith term in a. Define an operation $\oplus$ on Z^∞ as follows: For all $a, b \in Z^\infty$, let $a \oplus b$ be defined termwise by $(a \oplus b)[i] = a[i] + b[i]$. That is, we form $a \oplus b$ by adding a and b together termwise.

1. Show that $(Z^\infty, \oplus)$ is a commutative group.
2. Let R and L be mappings from Z^∞ to Z^∞ defined as follows:

$$R(a)[i] = \begin{cases} 0 & \text{if, } i = 0 \\ a[i-1] & \text{otherwise} \end{cases} \qquad L(a)[i] = a[i+1]$$

   That is, R "shifts" the sequence a one term to the right and L "shifts" the sequence a one term left. Show that R and L are group homomorphisms on Z^∞.
3. Show that $R \cdot L$ is a unit in the ring $\mathbb{H}(Z^\infty)$.
4. Show that neither R nor L is a unit in $\mathbb{H}(Z^\infty)$. (Hence, the converse of Exercise 1.2.17 is false.)

1.3 Integral Domains and Fields

In many respects, a cancellative ring behaves much like the ring of integers. Cancellative rings are sometimes called *domains*. Note that domains do not have any zero-divisors. With hat tipped to the ring of integers, we say that a commutative, cancellative ring with unity is an *integral* domain.

The ring of integers is, of course, an integral domain, as are the rings of rational, real, and complex numbers under their usual operations of addition and multiplication. In light of Exercise 1.2.11, we know that the ring $\mathbb{Z}_n$ is an integral domain if and only if n is a prime.

The ring $\mathbb{N}_2(Z)$ is not an integral domain since it is not commutative (and since it contains zero-divisors). The ring $2\mathbb{Z}$ of all even integers is commutative and cancellative, but is not an integral domain since it does not possess a unity.

Exercise 1.3.1. The *conjugate* of a complex number $\alpha = a + ib$ (a, b both real) is defined to be the complex number $\overline{\alpha} = a - ib$. Note that $\alpha\overline{\alpha} = a^2 + b^2$. Let $\mathcal{Q}$ denote the set of all matrices of the form

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$$

where α and β are complex numbers.

1. Show that $\mathbb{K} = (\mathcal{Q}, +, \cdot)$ is a noncommutative ring with unity, where $+$ and $\cdot$ represent matrix addition and multiplication, respectively.
2. Show that every nonzero member of $\mathcal{Q}$ is a unit.
3. Explain why $\mathbb{K}$ is a domain. This entity is known as the ring of *quaternions* (or *hypercomplex numbers*). Its elements are used to model rotations in three dimensions.

Exercise 1.3.2. Let $\mathbb{Z} \times \mathbb{Z} = (Z \times Z, \oplus, \otimes)$ where $\oplus$ and $\otimes$ are defined componentwise. Show that this commutative ring is not an integral domain.

Exercise 1.3.3. Consider the set F of all 2×2 matrices of the form

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

where a and b are real numbers. Show that $\mathbb{F} = (F, +, *)$ is an integral domain, where $+$ and $*$ denote matrix addition and multiplication, respectively.

Exercise 1.3.4. Let $2Z$ denote the set of even integers. Define a new operation $*$ on $2Z$ by $a * b = (ab)/2$. Prove that $(2Z, +, *)$ is an integral domain.

Exercise 1.3.5. Let Q denote the set of rational numbers. For $a, b \in Q$, let $a \oplus b = a+b-1$ and let $a \otimes b = ab+a+b$. Show that $(Q, \oplus, \otimes)$ is a commutative ring with unity but is not an integral domain.

Exercise 1.3.6. Let Z^∞ and the operation $\oplus$ be as defined in Exercise 1.2.19. Define an operation $\otimes$ on Z^∞ by $(a \otimes b)[i] = a[i]b[i]$. That is, define the product of two sequences a and b of integers to be the sequence whose terms are the product of the corresponding terms in a and b. Show that $\mathbb{Z}^\infty = (Z^\infty, \oplus, \otimes)$ is an integral domain.

A ring $\mathbb{R} = (R, +, *)$ is called a *division ring* (or a *skew field*) provided it is a domain in which every nonzero element is a unit. A commutative division ring is called a *field*.

The ring of quaternions in Exercise 1.3.1 is a division ring, while the rational, real, and complex numbers under their usual operations are all examples of fields. The ring $\mathbb{Z}_n$ is a field if and only if n is prime.

Exercise 1.3.7. Let F be the set of matrices in Exercise 1.3.3. Show that $(F, +, *)$ is a field by proving that every nonzero member of F is a unit.

Exercise 1.3.8. Let $F = \{a, b, c, d\}$. Define binary operations $+$ and $*$ on F according to the following tables.

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

*	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	c	a
d	a	d	a	d

Show that $(F, +, *)$ is a field. You may assume the operations are associative, and you may assume that $*$ distributes over $+$.

Theorem 1.3.9. *Every finite integral domain is a field.*

Proof. Of course, finiteness is key to this result, since $\mathbb{Z}$ is an integral domain that is not a field. Suppose that $\mathbb{F} = (F, +, *)$ is an integral domain, where $F = \{0, 1, a_1, ..., a_n\}$. We need to prove that every element a_j is a unit. Select any $a_j \in F$ $(1 \leq j \leq n)$ and consider the set

$$G = a_j * F = \{0, a_j, a_j * a_1, a_j * a_2, ..., a_j * a_n\}$$

Since F is closed under $*$, we know that $G \subseteq F$. We will first prove that $G = F$ (so that both sets contain the same number of elements). It will suffice to prove that all the elements of G are distinct. To this end, suppose that $a_j * a_k = a_j * a_m$

for some $a_k, a_m \in F$. Since $\mathbb{F}$ is an integral domain, the cancellation laws tell us that this implies $a_k = a_m$. Hence, the elements of G are all distinct.

Now that we know $G = F$, we know that $1 \in G$; this tells us that $1 = a_j * a_k$ for some $a_k \in F$. The element a_k therefore serves as the multiplicative inverse for a_j.

□

Exercise 1.3.10. Construct the ring $\mathbb{H}(\mathbf{Z}_3, \mathbf{Z}_3)$ and show that it is a field.

Exercise 1.3.11. Let $\mathbb{R} = (R, +, *)$ be a ring. Prove that $\mathbb{R}$ is a division ring if and only if the general linear equations $ax + b = c$ and $xa + b = c$ have unique solutions for all $a, b, c \in R$.

1.4 Subrings and Ideals

In this section, we will explore some important substructures within rings. Subobjects of rings, like subgroups in groups, play many important roles.

Let $\mathbb{R} = (R, +, *)$ be any ring, and let $S \subseteq R$.

1. We say that S is a *subring* of $\mathbb{R}$ provided S is closed under the ring addition and multiplication and is itself a ring under these operations.
2. If $\mathbb{R}$ has unity 1, we say that a subring S of $\mathbb{R}$ is *unital* provided $1 \in S$.
3. If $\mathbb{R}$ is a division ring (or field), then we say a subring S of $\mathbb{R}$ is a *sub division ring* (or *subfield*) provided S is unital; and $a^{-1} \in S$ for every nonzero $a \in S$.

The rings $n\mathbb{Z}$ of all integer multiples of a fixed integer n are all subrings of the ring $\mathbb{Z}$, although none (except for $n = 1$) are unital. The rational numbers form a subfield of the real numbers, and the real numbers form a subfield of the complex numbers.

The singleton $\{0_R\}$ of any ring $\mathbb{R}$ is always a subring; we call it the *trivial* subring of $\mathbb{R}$. Any subring of $\mathbb{R}$ which is a proper subset of R is called a *proper* subring of $\mathbb{R}$ while R is called the *improper* subring of $\mathbb{R}$.

Lemma 1.4.1. *Let $\mathbb{R} = (R, +, *)$ be a ring and let S be a subring of $\mathbb{R}$. If 0 is the additive identity of $\mathbb{R}$, then $0 \in S$ and serves as the additive identity for $(S, +, *)$.*

Proof. By assumption, we know S is a subring in its own right under the operations $+$ and $*$; hence, we know that S possesses an additive identity. Call

this element 0_S. Now, we know that $0_S + 0_S = 0_S$ in S; hence, we know that $0_S + 0_S = 0_S$ in R as well. Thus,

$$0_S + 0_S = 0_S \Rightarrow 0_S = -0_S + 0_S = 0$$

Hence, $0 \in S$ and is the additive identity of $(S, +, *)$.

□

Exercise 1.4.2. Let $\mathbb{R} = (R, +, *)$ be a ring and let S be a subring of $\mathbb{R}$. If $a \in S$, show that the additive inverse (in $\mathbb{R}$) for a is a member of S and serves as the additive identity (in $(S, +, *)$) for a.

Exercise 1.4.3. Show that the set $S = \{0, 2, 4\}$ is a subring of the ring $\mathbb{Z}_6$. Show that S is actually a field, even though $\mathbb{Z}_6$ is not.

Exercise 1.4.4. Suppose that $\mathbb{R} = (R, +, *)$ is a domain. If S is a unital subring of $\mathbb{R}$, prove that S is necessarily a domain. (Hence, unital subrings of a domain are called *subdomains*.)

The set of integers forms a subdomain of the rational numbers; but, of course, does not form a subfield of the rational numbers.

Exercise 1.4.5. Let $\mathbb{R} = (R, +, *)$ be a ring and let $S \subseteq R$ be nonempty. Show that S is a subring of $\mathbb{R}$ if and only if $ab \in S$ and $a - b \in S$ for all $a, b \in S$.

Exercise 1.4.6. Let $D_2(Z)$ be the set of all 2×2 matrices with integers on the main diagonal and 0's on the transverse diagonal. Show that $D_2(Z)$ is a commutative unital subring of $\mathbb{N}_2(Z)$.

Exercise 1.4.7. Let $T_2(Z)$ be the set of all 2×2 matrices with integers on the transverse diagonal and 0's on the main diagonal. Show that $T_2(Z)$ is a commutative non-unital subring of $\mathbb{N}_2(Z)$.

Exercise 1.4.8. Let $H = \{(m, -m) : m \in S\}$. Show that H is a subgroup of the additive group $\mathbf{Z} \times \mathbf{Z}$ but is not a subring of the ring $\mathbb{Z} \times \mathbb{Z}$.

Let $\mathbb{R} = (R, +, *)$ be a ring and let $S \subseteq R$. We say that S is an *ideal* of $\mathbb{R}$ provided S is a subgroup of $(R, +)$; and, for all $s \in S$ and all $r \in R$, we have $rs \in S$ and $sr \in S$.

Note that every ideal of a ring $\mathbb{R}$ is closed under the ring multiplication. Consequently, since every ideal is assumed to be a subgroup under the addition, it follows from Exercise 1.4.5 that every ideal of $\mathbb{R}$ is a subring of $\mathbb{R}$. Ideals were introduced early in ring theory as an aid to understanding prime factorizations

(we will see how later in this course). They now play an indispensable role in the general theory.

For each fixed integer n, the set nZ of all multiples of n forms an ideal of the ring $\mathbb{Z}$. However, although the integers form a subring of the ring $\mathbb{Q}$ of rational numbers, it does not form an ideal. Likewise, the rational numbers do not form an ideal in the reals, and the reals do not form an ideal in the ring of complex numbers.

Exercise 1.4.9. Show that the set $D_2(Z)$ in Exercise 1.4.6 is not an ideal of the ring $\mathbb{N}_2(Z)$.

Exercise 1.4.10. Let $I = \{3a + (1 + i\sqrt{5})b : a, b \in Z[i\sqrt{5}]\}$. Show that I is an ideal of the ring $\mathbb{Z}[i\sqrt{5}]$.

Exercise 1.4.11. Let $\mathbb{R} = (R, +, \cdot)$ be a ring and let I be an ideal of $\mathbb{R}$. Prove that $I = R$ if and only if $1 \in I$.

Exercise 1.4.12. Consider the ring $\mathbb{N}_2(Z)$ and the set

$$I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in Z \right\}$$

1. Show that I is a subring.
2. Show that I *absorbs left multiplication*; that is, show that $BA \in I$ for all $A \in I$.
3. Show that I does not absorb right multiplication and hence is not an ideal. (This exercise shows that we must check both left and right absorption.)

Exercise 1.4.13. Let $\mathbb{R} = (R, +, *)$ be ring. We let $\mathcal{I}(\mathbb{R})$ denote the set of all ideals of $\mathbb{R}$. Find $\mathcal{I}(\mathbb{Z}_6)$.

Exercise 1.4.14. Find $\mathcal{I}(\mathbb{Z}_2 \times \mathbb{Z}_2)$.

Exercise 1.4.15. Using either of the previous exercises, show by example that the union of two ideals of a ring need not be an ideal.

We know that the union of two ideals in a ring $\mathbb{R}$ need not be an ideal of $\mathbb{R}$. However, under certain circumstances, unions of ideals do produce another ideal.

Let $\mathbb{R} = (R, +, *)$ be a ring and let $\mathcal{F} \subseteq \mathcal{I}(\mathbb{R})$ be nonempty. We say that $\mathcal{F}$ is *directed* if, whenever $F_1, ..., F_n$ is a finite subcollection of $\mathcal{F}$, there exists an ideal $U \in \mathcal{F}$ such that $F_j \subseteq U$ for $1 \leq j \leq n$.

Theorem 1.4.16. *Let $\mathbb{R} = (R, +, *)$ be a ring. If $\mathcal{D}$ is a directed subset of $\mathcal{I}(\mathbb{R})$, then the set $\bigcup \mathcal{D} = \bigcup\{I : I \in \mathcal{D}\}$ is an ideal of $\mathbb{R}$.*

Proof. Since $0 \in \bigcup \mathcal{D}$, we know this set is nonempty. Closure under multiplication is easy to obtain. Indeed, let $a \in \bigcup \mathcal{D}$ and let $r \in R$. We know there exist $I \in \mathcal{D}$ such that $a \in I$. Since I is an ideal of $\mathbb{R}$, we know that $ar \in I$ and $ra \in I$. Hence, $ar \in \bigcup \mathcal{D}$ and $ra \in \bigcup \mathcal{D}$.

To complete the proof, we will need to show that $a - b \in \bigcup \mathcal{D}$ whenever $a, b \in \bigcup \mathcal{D}$. To this end, let $a, b \in \bigcup \mathcal{D}$. It follows that there exist $I, J \in \mathcal{D}$ such that $a \in I$ and $b \in J$. Since $\mathcal{D}$ is directed, there exists an ideal $K \in \mathcal{D}$ such that $I \cup J \subseteq K$. Thus, $a, b \in K$, which implies that $a - b \in K$, since K is an ideal of $\mathbb{R}$. Consequently, we know that $a - b \in \mathcal{D}$.

□

Exercise 1.4.17. Let $\mathbb{R} = (R, +, *)$ be a ring and let $\mathcal{F}$ be a family of subrings of $\mathbb{R}$. Show that $\bigcap \mathcal{F} = \bigcap\{S : S \in \mathcal{F}\}$ is a subring of $\mathbb{R}$. If every member of $\mathcal{F}$ is an ideal, show that $\bigcap \mathcal{F}$ is also an ideal.

Let $\mathbb{R} = (R, +, *)$ be a ring and let $X \subseteq R$. In light of the previous exercise, the set

$$\langle X \rangle = \bigcap\{I \in \mathcal{I}(\mathbb{R}) : X \subseteq I\}$$

is an ideal of $\mathbb{R}$. We call this set the ideal *generated* by the set X. It is the *smallest* ideal of $\mathbb{R}$ that contains X; that is, $X \subseteq \langle X \rangle$ and, whenever I is an ideal such that $X \subseteq I$, then $\langle X \rangle \subseteq I$ as well. We say that a subset Y of an ideal I *generates* the ideal provided $I = \langle Y \rangle$ and refer to Y as a set of *generators* for I. Every ideal has a set of generators, since $I = \langle I \rangle$.

Exercise 1.4.18. In a ring $\mathbb{R}$, what is $\langle \emptyset \rangle$?

Exercise 1.4.19. Let $\mathbb{R} = (R, +, *)$ be a ring and let I be an ideal of $\mathbb{R}$. Let $\texttt{Fin}(I)$ denote the set of all finite subsets of I. Show that the set $\mathcal{D}_I = \{\langle F \rangle : F \in \texttt{Fin}(I)\}$ is directed and that $I = \bigcup \mathcal{D}_I$.

If $I = \langle F \rangle$ for some finite set F, we say that I is *finitely generated*. If $I = \langle \{x\} \rangle$, we say that I is *principal*. We usually write $I = \langle x \rangle$ when $\{x\}$ is a generating set for I.

Exercise 1.4.20. Let $\mathbb{R} = (R, +, *)$ be a ring and let $F \in \texttt{Fin}(R)$. If $\mathcal{D} \subseteq \mathcal{I}(\mathbb{R})$ and $\langle F \rangle \subseteq \bigcup \mathcal{D}$, show that there exist $I \in \mathcal{D}$ such that $\langle F \rangle \subseteq I$.

Exercise 1.4.21. Let $\mathbb{R} = (R, +, *)$ be a commutative ring, and let $a \in R$.

1. Show that $\langle a \rangle = \{ar : r \in R\}$. Hint: Show that $\{ar : r \in R\}$ is the smallest ideal containing a.

2. Show that this description of $\langle a \rangle$ can fail if $\mathbb{R}$ is not commutative.

Exercise 1.4.22. Let $\mathbb{R} = (R, +, *)$ be a commutative ring. Let $F = \{a_1, ..., a_n\} \subseteq R$. Prove that

$$\langle F \rangle = \{a_1 r_1 + ... + a_n r_n : r_1, ..., r_n \in R\}$$

Exercise 1.4.23. Give an elementwise description of $\langle 2 \rangle$ in the ring $2\mathbb{Z}$.

Exercise 1.4.24. Give an elementwise description of $\langle A \rangle$ in the ring $\mathbb{D}_2(Z)$ if

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

Exercise 1.4.25. Every ideal of the ring $\mathbb{Z}_2 \times \mathbb{Z}_2$ is certainly finitely generated (since this ring is finite). Does this ring contains ideals that are not principal?

Exercise 1.4.26. Let $\mathbb{Z}^\infty$ be as defined in Exercise 1.3.6. For $a \in Z^\infty$, let $\texttt{supp}(a)$ be the set of all nonzero terms in a. Show that the set

$$I = \{a \in Z^\infty : \texttt{supp}(a) \text{ is finite}\}$$

is an ideal of $\mathbb{Z}^\infty$ which is not finitely generated.

A ring in which every ideal is principal is called a *principal ideal ring* (or PIR). In light of the previous exercises, we see that not every ring is a PIR. The following theorem presents another example.

Theorem 1.4.27. *The ring $\mathbb{Z}[i\sqrt{5}]$ is not a PIR.*

Proof. We will show by way of counterexample that the ideal I described in Exercise 1.4.10 is not principal. Suppose by way of contradiction that $I = \langle \alpha \rangle$ for some $\alpha = 3a + b(1 + i\sqrt{5})$. It is easy to see that both 3 and $1 + i\sqrt{5}$ are members of I. Thus, it must be true that there exist $\beta, \gamma \in I$ such that

$$3 = \beta\alpha \qquad 1 + i\sqrt{5} = \gamma\alpha$$

Since $|3|^2 = 9$ and $|1 + i\sqrt{5}|^2 = 6$, it follows that $|\alpha|^2$ must divide both 9 and 6. Consequently, we know that $|\alpha| = 1$, or $|\alpha| = 3$. We will prove that neither case is possible.

First, notice that, if we let $a = m + in\sqrt{5}$ and $b = p + iq\sqrt{5}$, then every element of I has the form

$$(3m + p - 5q) + i(3n + p + q)\sqrt{5}$$

This representation tells us every element $u + iv\sqrt{5} \in I$ has the property that $u - v$ is divisible by 3. Consequently, we know that $1 \notin I$ and $-1 \notin I$. However, these are the only two elements of $\mathbb{Z}[i\sqrt{5}]$ with modulus 1. Hence, we know that $|\alpha| \neq 1$.

It follows that we must have $|\alpha| = 3$. Hence, we must have

$$9 = |\alpha|^2 = (3m + p - 5q)^2 + 5(3n + p + q)^2$$

This tells us that $9 = x^2+5y^2$ for two numbers x and y such that $x-y$ is divisible by 3. Thus, there are only three possibilities — $x = \pm 3$ and $y = 0$, or $x = 2$ and $y = -1$ or $x = -2$ and $y = 1$. If $y = 0$, then $\alpha = \pm 3$. If this is the case, then $1+i\sqrt{5} = \pm 3\gamma$ for some $\gamma \in I$, which is clearly impossible. If $x = 2$ and $y = -1$, then setting $3 = (u + iv\sqrt{5})(2 - i\sqrt{5})$ implies that $3 = 9v$ — an impossibility if v is an integer. If $x = -2$ and $y = 1$, then setting $3 = (u + iv\sqrt{5})(-2 + i\sqrt{5})$ implies that $3 = -9v$ — again a possibility if v is an integer.

We may now conclude that the element α does not exist. Hence, the ideal I is not principal in $\mathbb{Z}[i\sqrt{5}]$.

□

Of course, we would not have introduced the term "PIR" if such rings do not exist. The following result proves that there are such entities.

Theorem 1.4.28. *The ring $\mathbb{Z}$ is a PIR.*

Proof. Let I be an ideal of $\mathbb{Z}$. We must find an integer a such that $I = \langle a \rangle$. If $I = \{0\}$, there is nothing to show, so suppose that I contains nonzero elements. Since I is a subgroup of $(Z, +)$, it follows that I contains positive elements. Let a be the smallest positive member of I. We will prove that a is a generator for I. To this end, suppose that $b \in I$. By the division algorithm, there exist integers q and r such that $b = aq + r$ and $0 \leq r < a$. Since I is an ideal, we know that $aq \in I$. Now, since $r = b - aq$, it follows that $r \in I$ as well. Consequently, we must have $r = 0$ (otherwise, I would contain a positive element strictly smaller than a). Hence, b is an integer multiple of a. Therefore, we know that

$$I = \{aq : q \in Z\} = \langle a \rangle$$

□

As you can see, showing that a particular ideal is not principal can be a daunting task. Sometimes, however, there are easier ways to determine whether or not a given ring is a PIR, as the following result shows.

Let $\mathbb{R}$ be a ring and let $\mathcal{C} \subseteq \mathcal{I}(\mathbb{R})$. We say that $\mathcal{C}$ is a *chain* if, whenever $I, J \in \mathcal{C}$, then either $I \subseteq J$, or $J \subseteq I$.

Exercise 1.4.29. Identify all chains of ideals in the ring $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Let $\mathbb{R}$ be a ring and let $\mathcal{C} = \{I_1, I_2, I_3, ...\}$ be a countable chain in $\mathcal{I}(\mathbb{R})$. We say that $\mathcal{C}$ is *ascending* provided $I_1 \subseteq I_2 \subseteq ... \subseteq I_n \subseteq ....$ We say that $\mathbb{R}$ satisfies the *ascending chain condition* (or ACC) if every ascending chain in $\mathcal{I}(\mathbb{R})$ is finite.

Let $\mathbb{R}$ be a ring and let $\mathcal{C} = \{I_1, I_2, ..., I_n, ...\}$ be an ascending chain of ideals in $\mathbb{R}$. If $\mathcal{C}$ is finite then there exists an ideal $I_m \in C$ such that $I_j \subseteq I_m$ for all j. The ideal I_m is said to be the *largest* member of $\mathcal{C}$.

Exercise 1.4.30. Show that the ring $\mathbb{Z}^\infty$ defined in Exercise 1.3.6 fails to satisfy the ACC by finding an infinite ascending chain of principal ideals in $\mathbb{Z}^\infty$.

Exercise 1.4.31. If $\mathbb{R}$ is a PIR, show that $\mathbb{R}$ satisfies the ACC. Hint: Note that a nonempty chain $\mathcal{C}$ of ideals is directed; consider $\bigcup \mathcal{C}$.

Note that rings which satisfy ACC need not by PIR's — just consider the ring $\mathbb{Z}_2 \times \mathbb{Z}_2$. Consequently, the converse of Exercise 1.4.31 is false.

1.5 Product and Quotient Rings

We have already encountered two examples of product rings, namely $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z} \times \mathbb{Z}$. In both cases, the underlying set is the cartesian product of two rings, and the operations are defined componentwise. We will now extend this idea.

A set X is said to be *indexed* by a set I provided there exists a bijection $f : I \longrightarrow X$. We call f an *indexing* of X by the set I, and we typically let x_i denote the element $f(i)$ for each $i \in I$.

Let $\mathcal{X} = \{X_i : i \in I\}$ be a family of sets indexed by the set I. We define the *direct product* of these sets to be the set of all mappings $t : I \longrightarrow \bigcup \mathcal{X}$ such that $t(i) \in X_i$ for each $i \in I$. We use the symbol $\prod_{i \in I} X_i$ to denote this set of mappings. The elements $t(i)$ are called the *coordinates* of the mapping t.

If $\mathcal{X} = \{X_1, ..., X_n\}$ is a finite collection of sets, then we can let the index set be the cardinal number $N = \{1, ..., n\}$. In this case, a member t of $\prod_{i \in N} X_i$ can be identified with an ordered n-tuple $(x_1, ..., x_n)$, where each $x_i = t(i)$. Consequently, for finite families of sets, we identify the direct product with the standard cartesian product. The previous discussion can be extended to countably infinite direct products as well. Indeed, the set Z^∞ of all sequences of integers can be thought of as the direct product of countably many copies of the set Z of integers.

Let $\mathcal{R} = \{\mathbb{R}_i : i \in I\}$ be a family of rings indexed by a set I, where each

$\mathbb{R}_i = (R_i, +_i, *_i)$. Let

$$\prod_{i\in I} \mathbb{R}_i = (\prod_{i\in I} R_i, \oplus, \otimes)$$

where $t \oplus s$ and $t \otimes s$ are defined by $(t \oplus s)(i) = t(i) +_i s(i)$ and $(t \otimes s)(i) = t(i) *_i s(i)$ for each $i \in I$. (That is, the operations are defined coordinate-wise on t and s.)

Exercise 1.5.1. Let $\mathcal{R} = \{\mathbb{R}_i : i \in I\}$ be a family of rings indexed by a set I.

1. Show that $\prod_{i\in I} \mathbb{R}_i$ is a ring.
2. Show that $\prod_{i\in I} \mathbb{R}_i$ has unity if and only if each $\mathbb{R}_i$ has unity.
3. Show that $t \in \prod_{i\in I} \mathbb{R}_i$ is a unit if and only if each $t(i)$ is a unit in $\mathbb{R}_i$.
4. Show that $\prod_{i\in I} \mathbb{R}_i$ is commutative if and only if each $\mathbb{R}_i$ is commutative.

The previous exercise shows that direct product rings inherit many important properties from their factor rings. However, a direct product of integral domains need not be an integral domain (consider the ring $\mathbb{Z} \times \mathbb{Z}$). In particular, an element of a direct product can be a zero-divisor when at least one of its coordinates is not a zero-divisor in the corresponding factor ring.

Exercise 1.5.2. Let $\mathbb{R} = (R, +, \cdot)$ and $\mathbb{S} = (S, \oplus, \odot)$ be rings. If I is an ideal of $\mathbb{R}$ and J is an ideal of $\mathbb{S}$, then prove that $I \times J$ is an ideal of $\mathbb{R} \times \mathbb{S}$.

It is also possible in some circumstances to take a ring and "divide" it into a family of "factor" rings. The process follows the methods used for constructing quotient groups. Let $\mathbb{R} = (R, +, \cdot)$ be a ring and let S be a subring of $\mathbb{R}$. We know that $(R, +)$ is a (commutative) group and that S is a (normal) subgroup of $(R, +)$. Hence, it makes sense to talk about the *cosets* generated by S in the group $(R, +)$. These sets will have the form

$$a + S = \{a + s : s \in S\} = S + a = \{s + a : s \in S\}$$

where $a \in R$. We will let $\mathcal{C}_S = \{a + S : a \in R\}$ denote the set of all cosets generated by S. From group theory we already know a great deal about the structure of $\mathcal{C}_S$. For example, we know that

- For all $a \in R$, we have $a \in a + S$.
- We have $a + S = S$ if and only if $a \in S$.
- If $b \in a + S$, then $b + S = a + S$.
- If $b \notin a + S$, then $(a + S) \cap (b + S) = \emptyset$.
- There is a bijection between S and $a + S$ for all $a \in R$.

Thus, the cosets of $(R, +)$ form a collection of pairwise disjoint sets all of which have the same cardinality as the original set S. Moreover, since S is automatically normal in $(R, +)$ (because $(R, +)$ is commutative), we know that we can make $\mathcal{C}_S$ into a (commutative) group by defining

$$(a + S) \oplus (b + S) = (a + b) + S$$

The identity of the group $(\mathcal{C}_S, \oplus)$ will be the set S; the inverse of any coset $a+S$ will be the coset $(-a) + S$.

In group theory, we must have the subgroup S be normal in the group before the relation $\oplus$ defined above is actually a binary function. We would like to make $\mathcal{C}_S$ into a ring as well as a group — doing this will require us to use ideals, which are the ring-theoretic analogs of normal subgroups.

Theorem 1.5.3. *Let $\mathbb{R} = (R, +, \cdot)$ be a ring and let S be a subring of $\mathbb{R}$. The following statements are equivalent:*

1. *The set S is an ideal of $\mathbb{R}$;*
2. *The binary relation $\otimes$ defined on $\mathcal{C}_S$ by $(a + S) \otimes (b + S) = (ab) + S$ is a function.*
3. *The triple $(\mathcal{C}_S, \oplus, \otimes)$ is a ring.*

Proof. We first prove that Claim 1 implies Claim 2. To this end, suppose that $a+S = c+S$ and $b+S = d+S$. We must show that $(ab)+S = (cd)+S$. It will suffice to prove that $cd \in ab + S$; that is, it will suffice to find some $s \in S$ such that $cd = ab + s$. Now, we know that there exist $t, u \in S$ such that $c = a + t$ and $d = b + u$. Consequently, we know that

$$cd = (a + t)(b + u) = ab + tb + au + tu$$

Since S is assumed to be an ideal, we know that tb, au and tu are all members of S. Hence, it follows that $s = tb + au + tu \in S$ as well. Thus, we see that $cd = ab + s$, which implies that $cd \in ab + S$, as desired.

We now prove that Claim 2 implies Claim 3. We already know that $(\mathcal{C}_S, \oplus)$ is a commutative group. It is easy to see that $\otimes$ as defined is associative. Indeed, suppose that $a, b, c \in R$. Note that

$$[(a + S) \otimes (b + S)] \otimes (c + S) = (ab + S) \otimes (c + S) = [(ab)c] + S$$

Now, we know that $(ab)c = a(bc)$. Hence, since we are assuming that $\otimes$ is a *function*, we know that $(ab)c + S = a(bc) + S$. Since

$$a(bc) + S = (a + S) \otimes ((bc) + S) = (a + S) \otimes [(b + S) \otimes (c + S)]$$

we have established that $\otimes$ is associative. It remains to prove that $\otimes$ distributes over $\oplus$. Again, the fact that $\otimes$ is a function will be crucial. Let $a, b, c \in R$. Observe that

$$(a + S) \otimes [(b + S) \oplus (c + S)] = (a + S) \otimes [(b + c) + S] = (a(b + c)) + S$$

Now, we know that $a(b + c) = ab + ac$. Hence, since $\otimes$ is a function, it follows that $(a(b + c)) + S = (ab + ac) + S$. Since we know

$$(ab + ac) + S = ((ab) + S) \oplus ((ac) + S)$$

we have established left distributivity. Right distributivity is verified in similar fashion.

Finally, we will prove that Claim 3 implies Claim 1. To this end, suppose that $(\mathcal{C}_S, \oplus, \otimes)$ is a ring. This certainly implies that $\otimes$ is binary function. Let $s \in S$ and let $a \in R$. We need only show that $as \in S$ and that $sa \in S$. Note that

$$(as) + S = (a + S) \otimes (s + S) = (a + S) \otimes S = S$$

since S is the (additive) identity for the ring. Therefore, we see that $as + S = S$¡ which implies that $as \in S$, as desired. The proof that $sa \in S$ is similar.

□

Let $\mathbb{R} = (R, +, \cdot)$ be a ring and let I be an ideal of $\mathbb{R}$. The *quotient ring* generated by I is the ring

$$\mathbb{R}/\mathbb{I} = (\mathcal{C}_I, \oplus, \otimes)$$

of cosets generated by I.

Note that, in practice, quotient rings are constructed exactly the same way we construct quotient groups — the whole process hinges on properly identifying the cosets. The rest is simple.

Exercise 1.5.4. Consider the ring $\mathbb{Z}_{12}$.

1. Construct the ideal $I = \langle 4 \rangle$ in this ring.
2. Construct $\mathcal{C}_I$ for this ideal.
3. Construct the addition and multiplication tables for the quotient ring $\mathbb{Z}_{12}/\mathbb{I}$.

Exercise 1.5.5. Consider the ring $\mathbb{Z} \times \mathbb{Z}$. Let $I = \{(m, 0) : m \in Z\}$.

1. Show that I is an ideal.
2. Describe the cosets of I.

3. Prove that the quotient $(\mathbb{Z} \times \mathbb{Z})/\mathbb{I}$ is an integral domain.

Exercise 1.5.6. Let p be a prime number and let T denote the set of all rational numbers (in lowest terms) whose denominators are not divisible by p.

1. Prove that T is a ring under rational addition and multiplication.
2. Let I denote the subset of T whose numerators are multiples of p. Prove that I is an ideal of $(T, +, \cdot)$.
3. Determine the cosets of I in the ring $(T, +\cdot)$.

Exercise 1.5.7. Let $\mathbb{R} = (R, +, \cdot)$ and let I be an ideal of $\mathbb{R}$. For $a, b \in R$, set $a \equiv b \,\mathtt{mod}(I)$ if and only if $a - b \in I$.

1. Show that the relation $\equiv$ is an equivalence relation on R.
2. Show that $a + I = b + I$ if and only if $a \equiv b \,\mathtt{mod}(I)$.

Exercise 1.5.8. Let $\mathbb{R} = (R, +, \cdot)$ be any ring and let I be an ideal of $\mathbb{R}$. Prove the following statements.

1. If $\mathbb{R}$ is commutative, then $\mathbb{R}/\mathbb{I}$ is commutative.
2. If $\mathbb{R}$ has a unity 1, then $\mathbb{R}/\mathbb{I}$ has a unity, namely $1 + I$.

Exercise 1.5.9. Let $3\mathbb{Z}$ denote the ring of all integer multiples of 3 and let $I = 6Z$.

1. Show that I is an ideal of $3\mathbb{Z}$.
2. Show that $3\mathbb{Z}/\mathbb{I}$ is a field.
3. Explain why the converse of Exercise 1.5.8 (2) is false.

Exercise 1.5.10. Let $\mathbb{R} = (R, +, \cdot)$ be a noncommutative ring and let I be an ideal of $\mathbb{R}$. Prove that $\mathbb{R}/\mathbb{I}$ is commutative if and only if $ab - ba \in I$ for all $a, b \in I$.

Exercise 1.5.11. Let $\mathbb{R} = (R, +, \cdot)$ be a commutative ring and let I be an ideal of $\mathbb{R}$. Prove that $\mathbb{R}/\mathbb{I}$ has a unity if and only if there exist $\epsilon \in R$ such that $\epsilon a - a \in I$ for all $a \in R$.

Exercise 1.5.12. Let $\mathbb{R} = (R, +, \cdot)$ be any ring and let I be a proper ideal of $\mathbb{R}$. Prove that the following statements are equivalent.

1. The quotient $\mathbb{R}/\mathbb{I}$ contains no zero-divisors.
2. Whenever $a, b \in R$ are such that $ab \in I$, then either $a \in I$ or $b \in I$.

Remember that I is considered to be the "zero" of the quotient.

Let $\mathbb{R} = (R, +, \cdot)$ be a ring. A proper ideal I of $\mathbb{R}$ is said to be *prime* provided it satisfies the equivalent conditions in Exercise 1.5.12. Note that the ideal $I = \{(m, 0) : m \in Z\}$ is a prime ideal of $\mathbb{Z} \times \mathbb{Z}$. It is generally easier to check to the second condition when we want to verify that an ideal is prime, but either condition may be used. The next result motivates our use of the term "prime" when describing these ideals.

Theorem 1.5.13. *A nontrivial ideal I of $\mathbb{Z}$ is prime if and only if $I = \langle p \rangle$ for some prime p.*

Proof. We already know that every ideal of $\mathbb{Z}$ is principal. Hence, we know that $I = \langle n \rangle$ for some positive integer n. We must prove I is prime as an ideal if and only if n is prime as an integer.

First, suppose that I is a prime ideal. Since I must be proper, it follows that $n \neq 1$. Suppose by way of contradiction that $n = pq$ for some integers $1 < p < n$ and $1 < q < n$. Since we know that $n \in I$, it follows that $pq \in I$. Now, since I is assumed to be prime, it follows that either $p \in I$ or $q \in I$. However, since I consists only of *integer* multiples of n, this is not possible. Hence, we must conclude that n is prime.

Now, suppose that n is prime. We know that $I = \{kn : k \in Z\}$. Since n is prime, we know that $q \notin I$ for any prime $q \neq n$ (since no such prime can be a multiple of n). Hence, we know that I is proper. Suppose now that $a, b \in Z$ are such that $ab \in I$. It follows that $ab = kn$ for some integer n; which implies that $n|(ab)$. Since n is prime, this tells us (by Euclid's Lemma) that either $n|a$ or $n|b$. Therefore, we know that either $a \in I$ or $b \in I$, as desired.

□

Exercise 1.5.14. Let $\mathbb{R}$ be a ring. What must be true if $\langle 0 \rangle$ is a prime ideal in $\mathbb{R}$?

Exercise 1.5.15. Show that $I = \langle (3, 0) \rangle$ is not a prime ideal in $\mathbb{Z} \times \mathbb{Z}$.

Exercise 1.5.16. Show that $I = \{(0, a) : a \in \mathbb{Z}_3\}$ is a prime ideal of $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Exercise 1.5.17. Suppose that $\mathbb{R} = (R, +, \cdot)$ is a commutative ring with unity and suppose that I is an ideal of $\mathbb{R}$. Prove that $\mathbb{R}/\mathbb{I}$ is an integral domain if and only if I is prime.

Exercise 1.5.18. Let $\mathbb{R} = (R, +, \cdot)$ be a ring. An element $a \in R$ is *nilpotent* provided $a^n = 0$ for some positive integer n. If P is a prime ideal of $\mathbb{R}$, prove that P contains every nilpotent element of $\mathbb{R}$. (The previous exercise is helpful.)

Exercise 1.5.19. Let $\mathbb{R}$ be a principal ideal domain (PID) and let $I = \langle p \rangle$ be a prime ideal of $\mathbb{R}$. If there exist $c, d \in R$ such that $p = cd$, prove that one of c or d is a unit. (This fact allows us to generalize the notion of "prime" to more general rings.)

Let $\mathbb{R} = (R, +, \cdot)$ be a ring. A proper ideal I of $\mathbb{R}$ is *maximal* provided there does not exist an ideal J such that $I \subset J \subset R$.

An ideal I in a ring $\mathbb{R}$ is maximal provided there is no ideal "between" it and the whole ring. Sometimes we say that I is *covered* by $\mathbb{R}$. A ring may possess many maximal ideals. For example, in $\mathbb{Z}_6$, the ideals $I = \{0, 2, 4\}$ and $J = \{0, 3\}$ are both maximal.

Exercise 1.5.20. Show that $I = \langle 3 \rangle$ is maximal in $\mathbb{Z}$. Show that $\langle 6 \rangle$ is not maximal in $\mathbb{Z}$.

Exercise 1.5.21. Show that an ideal in $\mathbb{Z}$ is maximal if and only if it is prime.

Exercise 1.5.22. Find a prime ideal of $\mathbb{Z} \times \mathbb{Z}$ that is not maximal.

Theorem 1.5.23. *Let $\mathbb{R} = (R, +, \cdot)$ be a commutative ring with unity. An ideal M of $\mathbb{R}$ is maximal if and only if the quotient $\mathbb{R}/\mathbb{M}$ is a field.*

Proof. Suppose that $\mathbb{R}/\mathbb{M}$ is a field. It follows that the unity $1 + M$ of $\mathbb{R}/\mathbb{M}$ cannot be equal to the identity M (since the identity of a ring cannot have a multiplicative inverse). Consequently, we know that $1 \notin M$. It follows that M is proper. Now, suppose that there exists an ideal J of $\mathbb{R}$ such that $M \subseteq J \subseteq R$. We must prove that $M = J$ or $J = R$. Suppose that $M \neq J$. It follows that there exist $a \in J - M$; hence we know that $a + M \neq M$. Consequently, we know that $a + M$ has a multiplicative inverse in $\mathbb{R}/\mathbb{M}$. Call this inverse $b + M$. This tells us that $(ab) + M = 1 + M$, which in turn tells us that $ab - 1 \in M$ (see Exercise 1.5.7). Thus, we know that $1 = ab - m$ for some $m \in M$. Since $m \in J$ and $a \in J$ by assumption, it follows that $1 \in J$. This implies that $J = R$, as desired (see Exercise 1.4.11).

On the other hand, suppose that M is maximal in $\mathbb{R}$. We must show that every non-identity element of $\mathbb{R}/\mathbb{M}$ is a unit. To this end, suppose that $a \notin M$ and consider the coset $a + M$. We must find a multiplicative inverse for $a + M$ in the quotient. First, observe that, since M is maximal, we know that M is proper in $\mathbb{R}$. Hence, we know by Exercise 1.4.11 that $1 \notin M$. Thus, we

know that $1+M \neq M$; and this coset clearly serves as the unity of the quotient. Consequently, to find a multiplicative inverse for $a+M$, we must find an element $b \in R$ such that $(ab) + M = 1 + M$; that is, we must find $b \in R$ such that $1 - ab \in M$. Consider the set

$$J = \{m + ab : m \in M, b \in R\}$$

Note that $M \subseteq J$ by construction (just let $b = 0$). Furthermore, J is an ideal of $\mathbb{R}$. Indeed, J is certainly a subring since, for $m, n \in M$ and $b, c \in R$, we have

$$(m + ab) - (n + ac) = (m - n) + a(b - c) \in J$$

since $m - n \in M$ and $b - c \in R$. It is also easy to see that J is closed multiplication. Indeed, if $r \in R$, note that

$$r(m + ab) = (rm) + a(rb) \in J$$

since $rm \in M$ and $rb \in R$. (Note that the commutativity of $\mathbb{R}$ is crucial here.) Thus, since J is an ideal that contains M, it follows that $J = R$. This tells us that $1 \in J$ (by Exercise 1.4.11). Thus, we know that there exist $b \in R$ such that $1 = m + ab$. Consequently, we see that $1 - ab \in M$, as desired.

□

Exercise 1.5.24. Let $2\mathbb{Z}$ denote the ring of even integers.

1. Show that $M = 4Z$ is a maximal ideal in $2\mathbb{Z}$.
2. Show that $2\mathbb{Z}/\mathbb{M}$ is not a field. Why does this not contradict the previous theorem?

1.6 Homomorphisms

We will conclude this chapter with a notion for rings that has a familiar analog in groups — that of a ring *homomorphism*. Because ring homomorphisms share much in common with group homomorphisms, much of this section will be familiar.

Let $\mathbb{R} = (R, +, \cdot)$ and $\mathbb{S} = (S, \oplus, \odot)$ be rings. A mapping $f : R \longrightarrow S$ is called a ring *homomorphism* provided $f(a+b) = f(a) \oplus f(b)$ and $f(a \cdot b) = f(a) \odot f(b)$. We say that f *preserves the ring operations* if this is the case.

A ring homomorphism that is one-to-one is called a *monomorphism* or an *embedding*. A ring homomorphism that is onto is called an *epimorphism*. A ring homomorphism that is a bijection is called an *isomorphism*. When there is an isomorphism between two rings, we say that the rings are *isomorphic*. Isomorphic rings, like isomorphic groups, are mathematically indistinguishable. The following result is a direct analog of the corresponding result for groups. We leave its proof as an exercise.

Exercise 1.6.1. Let $\mathbb{R} = (R, +, \cdot)$ and $\mathbb{S} = (S, \oplus, \odot)$ be rings and let $f : R \longrightarrow S$ be a ring homomorphism. Then the following statements are true:

1. We have $f(0_R) = 0_S$.
2. For all $a \in R$, we have $f(-a) = -f(a)$.
3. If T is a subring of $\mathbb{R}$, then $f(T) = \{f(t) : t \in T\}$ is a subring of $\mathbb{S}$.
4. If U is a subring of $\mathbb{S}$, then $T = \{t \in R : f(t) \in U\}$ is a subring of $\mathbb{R}$.
5. If $\mathbb{R}$ has a unity 1, then $f(1)$ is the unity of the subring $f(R)$.
6. If $\mathbb{R}$ is commutative, then $f(R)$ is commutative in $\mathbb{S}$.

As an example, consider the mappings $f : Z_2 \times Z_3 \longrightarrow Z_6$ and $g : Z_2 \times Z_3 \longrightarrow Z_6$ defined by

$$f[(a,b)] = (3a + 2b)\texttt{mod}(6) \qquad g[(a,b)] = (3a - 2b)\texttt{mod}(6)$$

Are either of these mappings ring homomorphisms? First, observe that both preserve the ring addition. (We leave this as an exercise.) Thus, both are group homomorphisms. (In fact, the mapping f is a group isomorphism.) However, the mapping f does not preserve the ring multiplication. Observe that

$$f[(1,2) * (1,1)] = f[(1,2)] = (3+4)\texttt{mod}(6) = 1$$
$$f[(1,2)] * f[(1,1)] = (3+4)\texttt{mod}(6) * (3+2)\texttt{mod}(6) = 5$$

Thus, even though f is a group isomorphism, it is not a ring homomorphism. On the other hand, the mapping g does preserve the ring multiplication. Indeed,

$$\begin{aligned} g[(a,b) * (c,d)] &= g[(ac, bd)] \\ &= (3ac - 2bd)\texttt{mod}(6) \\ &= (9ac - 6ad - 6bc + 4bd)\texttt{mod}(6) \\ &= (3a - 2b)\texttt{mod}(6) * (3c - 2d)\texttt{mod}(6) \\ &= g[(a,b)] * g[(c,d)] \end{aligned}$$

Note that we used the facts that $6ad \equiv 6bc \equiv 0\,\texttt{mod}(6)$ and $-2bd \equiv 4bd\,\texttt{mod}(6)$ in the calculation above. Thus, g is a ring homomorphism. In fact, g is a ring isomorphism.

Exercise 1.6.2. Consider the ring $\mathbb{Z}_{28}$.

1. Show that $U = \{0, 4, 8, 12, 16, 20, 24\}$ is a subring of $\mathbb{Z}_{28}$.
2. Show that the mapping $f : Z_7 \longrightarrow \mathbb{Z}_{28}$ defined by $f(x) = 8x\,\texttt{mod}(28)$ is an embedding with $f(Z_7) = U$.

Exercise 1.6.3. Let $\mathbb{R} = (R, +, \cdot)$ and $\mathbb{S} = (S, +, *)$ be rings. Show that $\mathbb{R} \times \mathbb{S}$ is isomorphic to $\mathbb{S} \times \mathbb{R}$.

Exercise 1.6.4. Let $\mathbb{R} = (R, +, \cdot)$ and $\mathbb{S} = (S, +, *)$ be rings. Show that the mapping $\pi_1 : R \times S \longrightarrow R$ defined by $\pi_1[(a, b)] = a$ is a ring epimorphism from $\mathbb{R} \times \mathbb{S}$ to $\mathbb{R}$. Maps which take a ring product to a fixed coordinate are called *projection homomorphisms*.

Exercise 1.6.5. Let $f : Z_{12} \longrightarrow Z_4$ be defined by $f(x) = x \mathtt{mod}(4)$.

1. Show that f is a ring epimorphism from $\mathbb{Z}_{12}$ to $\mathbb{Z}_4$.
2. Show that the set $T = \{a \in Z_{12} : f(a) = 0 \,\mathtt{mod}(4)\}$ is an ideal.

Exercise 1.6.6. Let $\mathbb{R} = (R, +, \cdot)$ and $\mathbb{S} = (S, +, *)$ be rings and let $f : R \longrightarrow S$ be a ring homomorphism. Show that the set $\mathtt{ker}(f) = \{a \in R : f(a) = 0_S\}$ is always an ideal of $\mathbb{R}$. This set is called the *kernel* of f.

Exercise 1.6.7. Let $\mathbb{R} = (R, +, \cdot)$ and $\mathbb{S} = (S, +, *)$ be rings. Show that the kernel of the projection homomorphism $\pi_1 : R \times S \longrightarrow R$ defined in Exercise 1.6.4 is the set $\mathtt{ker}(f) = \{(0_R, s) : s \in S\}$.

Exercise 1.6.8. Let $\mathbb{R} = (R, +, \cdot)$ be any ring and let I be an ideal of $\mathbb{R}$.

1. Show that the mapping $\nu_I : R \longrightarrow \mathcal{C}_I$ defined by $\nu_I(a) = a + I$ is an epimorphism between $\mathbb{R}$ and $\mathbb{R}/\mathbb{I}$. This map is called the *quotient homomorphism*.
2. Show that $\mathtt{ker}(\nu_I)) = I$.

Exercise 1.6.9. Let $\mathbb{R} = (R, +, \cdot)$ be a ring with unity and let $\mathbb{S} = (S, \oplus, \odot)$ be a ring. Suppose that $f : R \longrightarrow S$ be a homomorphism. If $a \in R$ is a unit, show that $f(a)$ is a unit in $f(R)$.

Exercise 1.6.10. Consider the mapping $f : Z_3 \longrightarrow Z_6$ defined by $f(x) = 4x \,\mathtt{mod}(6)$.

1. Show that f is a homomorphism between $\mathbb{Z}_3$ and $\mathbb{Z}_6$.
2. Show that $f(2)$ is not a unit in $\mathbb{Z}_6$. Why does this not contradict Exercise 1.6.9?

Exercise 1.6.11. Let $\mathbb{R} = (R, +, \cdot)$ and $\mathbb{S} = (S, +, *)$ be rings and let $f : R \longrightarrow S$ be a homomorphism. Show that f is one-to-one if and only if $\mathtt{ker}(f) = \{0_R\}$.

We have already seen that ideals perform in rings much the same role as normal subgroups play for groups. This analogy can be extended further, as the following theorems show.

Corollary 1.6.12. *Let $\mathbb{R} = (R, +\cdot)$ be a ring. A subset I of R is an ideal of $\mathbb{R}$ if and only if there exists a ring $\mathbb{S} = (S, \oplus, \otimes)$ and a homomorphism $f : R \longrightarrow S$ such that $I = \mathtt{ker}(f)$.*

Proof. In light of Exercise 1.6.8, if I is an ideal of $\mathbb{R}$, we need only consider the quotient ring $\mathbb{S} = \mathbb{R}/\mathbb{I}$ and the quotient mapping $\nu_I : R \longrightarrow \mathcal{C}_I$.

On the other hand, if I is the kernel of a homomorphism f, it follows from Exercise 1.6.6 that I is an ideal of $\mathbb{R}$.

□

Theorem 1.6.13. *Let $\mathbb{R} = (R, +, *)$ and $\mathbb{S} = (S, \oplus, \odot)$ be rings. If $f : R \longrightarrow S$ is an epimorphism, then there exists a unique isomorphism $\varphi : \mathcal{C}_I \longrightarrow S$ such that $\varphi \circ \nu_I = f$, where $I = \mathtt{ker}(f)$.*

Proof. Every ring homomorphism is a group homomorphism. Consequently, by the Fundamental Homomorphism Theorem for groups, we know there exists a unique group isomorphism $\varphi : \mathcal{C}_I \longrightarrow S$ defined by $\varphi(a + I) = f(a)$. We need only prove that φ preserves the ring multiplication. To this end, suppose that $a + I, b + I \in \mathcal{C}_I$. Observe that

$$\varphi((a + I) \otimes (b + I)) = \varphi((ab) + I) = f(ab) = f(a) \odot f(b) = \varphi(a + I) \odot \varphi(b + I)$$

□

The previous result is known as the *Fundamental Homomorphism Theorem for Rings*. As an example of how this can be used, let n be a fixed positive integer and consider the ideal nZ of $\mathbb{Z}$. The mapping $f : Z \longrightarrow Z_n$ defined by $f(x) = x \,\mathtt{mod}(n)$ is clearly a ring epimorphism. Moreover, the kernel of this mapping is the ideal nZ. Hence, we know at once that the quotient $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$.

Exercise 1.6.14. Let $\mathbb{R}$ and $\mathbb{S}$ be rings.

1. Show that $\mathbb{R}$ can be embedded into $\mathbb{R} \times \mathbb{S}$ as an ideal.
2. Use the Fundamental Homomorphism Theorem to prove that $(\mathbb{R} \times \mathbb{S})/\mathbb{R}$ is isomorphic to $\mathbb{S}$.