Chapter 4

Rings

Of the three main topics in this book—groups, rings, and fields—the study of rings will probably be the most familiar to the reader. The first section of Chapter 1 concerned the protypical ring, the integers. The main properties examined—quotients and remainders, divisibility, prime numbers, factorization—are familiar from grade school. At the end of that chapter, these properties are extended to the polynomial ring $F[x]$ for F a field. Polynomials over the rational numbers, $\mathbb{Q}$, are a major portion of the secondary school curriculum, although the focus is on the geometry of solutions to polynomial equations more than algebraic properties. Still, the division of polynomials and factorization do play an important role in the curriculum.

In this chapter, we deal with general rings, with the caveat that multiplication is assumed to be commutative. The special roles of the integers and of polynomial rings will be evident, and the properties of divisibility and factorization are major themes. The two GCD Theorems 1.1.4 and 1.3.3 involve a construction that also plays a major role: the GCD of two integers is a linear combination of the two and the GCD of two polynomials is a polynomial combination of the two. Ideals are subsets of a ring that generalize the construction of linear/polynomial combinations of two elements. Ideals are used to define quotient rings in Section 4.4. That following section presents the relatively straightforward generalizations of the isomorphism theorems for groups 2.7.9 2.9.1 3.1.3 and of the related Factor Theorem 2.7.11 and Correspondence Theorem 2.9.2. Key properties of ideals and the relationship to properties of the quotient rings are studied in Section 4.6. The culminating topic of this Chapter is rings of fractions 4.7, which extends the techniques used to derive the rational numbers from the integers.

4.1 Rings

In this section we recall the definition of a ring and introduce three particular types of rings: fields, integral domains, reduced rings. The integers and $F[x]$ provide ways to construct examples and non-examples of these three types of rings using the modular arithmetic introduced in Sections 1.1 and 1.3.

Definition 4.1.1. A **ring** is a set R, with two operations $+$ and $*$ that satisfy the following properties.

(1) $+$ and $*$ are both associative. That is $(a+b)+c = a+(b+c)$ and $a*(b*c) = (a*b)*c$.

(2) $+$ and $*$ are both commutative. That is $a+b = b+a$ and $a*b = b*a$.

(3) $+$ and $*$ both have identity elements. There is some element in R, that we call 0, such that $a+0 = a$, and there is an element, that we call 1, such that $a*1 = a$.

(4) $+$ admits inverses. That is, for each $a \in R$ there is some other element, that we write $-a$, such that $a+(-a) = 0$.

(5) $*$ distributes over $+$. That is $a*(b+c) = a*b+a*c$.

A few comments are in order. Strictly speaking, the definition above is for a **commutative ring with identity**. The modifier "commutative" is referring to commutativity of multiplication, and "with identity" is referring to the multiplicative identity. There is a rich study of rings where multiplication is non-commutative (for example the ring of $n \times n$ matrices over $\mathbb{R}$, see Section 4.3), but treating the subject would spread our efforts too thinly. It is common when treating only commutative rings to simplify the terminology at the outset as we do here: A ring for us is assumed to be commutative and have an identity.

One may also say that a ring R is a commutative group under $+$ and that $R^* = R \setminus \{0\}$ is a commutative *monoid* (look it up!) under $*$, with the additional property that $*$ distributes over $+$.

One can show by induction that a sum of several terms (or a product of several terms) may be computed in any order and that $r*(a_1+a_2+\cdots+a_n) = r*a_1 + r*a_2+\cdots+r*a_n$.

There are a bunch of little results one should verify. Since any ring R is a group under $+$ we already know that the additive identity 0 is unique and that the additive inverse of $r \in R$ is unique (we write it as $-r$). We know that $-(-r) = r$ and that for $s \in R$, $-(r+s) = (-r)+(-s)$ (using commutativity of $+$). Additionally we have the following properties. Proofs are left as an exercise.

Proposition 4.1.2. *Let R be a ring and $r, s \in R$*

(1) For an integer m, we can make sense of mr via

$$\Big(\underbrace{1+1+\cdots+1}_{m\ terms}\Big) * r = \underbrace{r+r+\cdots+r}_{m\ terms}$$

(2) For any $r \in R$, $r * 0 = 0$.

(3) The multiplicative identity element 1 is unique.

(4) The additive inverse and multiplication operate as expected.

- $r * (-s) = -(r * s)$
- $(-r) * (-s) = r * s$

We haven't excluded the possibility that $1 = 0$. In this case for any $r \in R$, $r = r * 1 = r * 0 = 0$. Thus we have a unique situation, a ring that has just one element. We call it the **trivial ring**.

We will write the product without the multiplication symbol when there is no concern about ambiguity, that is rs instead of $r * s$. But for clarity and emphasis on the basic properties of a ring, we will continue to explicitly show the product symbol in this section.

There are three special types of elements in a ring, and, based on their existence or not, three special types of rings.

Definition 4.1.3. An element u of a ring R is a **unit** when there is another element v such that $u * v = 1$. An element a of a ring R is a **zero-divisor** when $a \neq 0$ and there is some $b \neq 0$ in R such that $a * b = 0$. An element a of a ring R is **nilpotent** when there exists some positive integer n such that $a^n = 0$.

Definition 4.1.4. A **field** is a nontrivial ring in which every nonzero element is a unit. An **integral domain** is a nontrivial ring that has no zero-divisors. A nontrivial ring is **reduced** if it has no nilpotent elements other than 0.

Exercises 4.1.5. Prove the results in Proposition 4.1.2, and in addition prove the following.

(a) The inverse of a unit is unique.
(b) The inverse of a unit is also a unit.
(c) A unit cannot be a zero divisor.
(d) A nilpotent element is either 0 or a zero-divisor.

Exercises 4.1.6. Cancellation in integral domains.

(a) Let R be an integral domain. Show that the cancellation law holds: If $ar = as$ then $r = s$.

(b) Let R be an integral domain that is finite. Show that R is a field. (For a nonzero $a \in R$, consider the function $R \longrightarrow R$ that takes r to $a * r$. Use the cancellation law to show injectivity.)

The Integers and $F[x]$ for F a Field

We can now fully appreciate the integers $\mathbb{Z}$, having ignored multiplication when we studied the integers as a group. The integers, the number system we learn in elementary school, form the first example of a ring. One of the key properties of the integers (used in solving a quadratic equation!) is that $ab = 0$ implies $a = 0$ or $b = 0$. In terms defined above, $\mathbb{Z}$ has no zero-divisors, so it is an integral domain.

Let us now turn to modular arithmetic, which we introduced in Section 1.1. We will use $[a]_n$ for the equivalence class of a modulo n and we will omit the subscript n when the modulus is obvious. The following expands on Exercise **??**.

Theorem 4.1.7 (Units, Zero Divisors in $\mathbb{Z}/n$)**.** *Let $n \geq 2$ be an integer and let a be an integer.*

(1) $[a]_n$ *is a unit iff* $\gcd(a, n) = 1$.

(2) $[a]_n$ *is a zero divisor iff* $1 < \gcd(a, n) < n$.

In particular, an element of $\mathbb{Z}/n$ is either 0, or a unit, or a zero-divisor, and these are mutually exclusive.

Proof. Let $d = \gcd(a, n)$. There are three mutually exclusive cases, $d = 1$, $d = n$ and $1 < d < n$.

If $d = 1$ then, by the GCD Theorem 1.1.4 there are integers u, v such that $ua + vn = 1$. Reducing modulo n we have

$$\begin{aligned} [u]_n * [a]_n + [v]_n * [n]_n &= [1]_n \\ [u]_n * [a]_n &= [1]_n \end{aligned}$$

so $[u]_n$ is the multiplicative inverse of $[a]_n$ and $[a]_n$ is a unit in $\mathbb{Z}/n$.

If $d = n$, then $[a]_n = [0]_n$.

If $1 < d < n$ then $a = db$ and $n = dc$ for some integers b and c with $c < n$. Then $[c]_n * [a]_n = [c]_n * [db]_n = [cd]_n * [b]_b = [n]_n * [b]_n = [0]_n$. But $[a]_n \neq [0]_n$ and, since $c < n$, $[c]_n \neq [0]_n$. Thus $[a]_n$ is a zero divisor. $\square$

We are particularly interested in the following special case, to which we will return in depth later.

Corollary 4.1.8. *Let p be a prime number. Then $\mathbb{Z}/p$ is a field; every nonzero element has an inverse.*

When working with the integers modulo a prime we usually use the notation $\mathbb{F}_p$ instead of $\mathbb{Z}/p$ to emphasize that we have a field.

A general theme emphasized in these notes is the similarity between the integers and a polynomial ring over a field $F[x]$. We have similar results when working modulo a polynomial as we did for modular arithmetic.

Theorem 4.1.9 (Units, Zero Divisors in $F[x]/m(x)$)**.** *Let F be a field and let $m(x)$ be a polyomial of degree $\delta > 0$. Let $a(x) \in F(x)$ and let $[a(x)]$ be its congruence class modulo $m(x)$.*

(1) $[a(x)]$ *is a unit iff* $\gcd(a(x), m(x)) = 1$.

(2) $[a(x)]$ *is a zero divisor iff* $\gcd(a(x), m(x))$ *has degree greater than 0 and less than d.*

In particular, an element of $F[x]/m(x)$ is either 0, or a unit, or a zero-divisor, and these are mutually exclusive.

Proof. Let $d(x) = \gcd(a(x), m(x))$. There are three mutually exclusive cases, $d(x) = 1$, $d(x) = m(x)$ and $0 < \deg(d(x)) < \deg(m(x))$. These lead to $[a(x)]$ a unit, $[a(x)] = [0]$ and $[a(x)]$ a zero divisor, respectively. The proof for each case is entirely similar to that for the integers. $\square$

As with the integers, the following case is of special interest and we will return to it in depth later.

Corollary 4.1.10. *Let $m(x)$ be an irreducible polynomial in $F[x]$ for F a field. Then every nonzero element in $F[x]/m(x)$ has an inverse, so $F[x]/m(x)$ is a field. Conversely, if $m(x)$ is reducible, $F[x]/m(x)$ is not even an integral domain.*

Exercises 4.1.11.

(a) Find the nilpotent elements of $\mathbb{Z}/8$, of $\mathbb{Z}/12$, and of $\mathbb{Z}/30$.

(b) Under what conditions on n does $\mathbb{Z}/n$ have nonzero nilpotent elements?

(c) Identify the nilpotent elements of $\mathbb{Z}/n$ using the unique factorization of n.

(d) Let F be a field and $m(x) \in F[x]$. Under what conditions on $m(x)$ does $F[x]/m(x)$ have nonzero nilpotent elements? Identify the nilpotents $a(x) \in F[x]/m(x)$ using unique factorization into irreducibles of $m(x)$ and $a(x)$.

4.2 Ring Homomorphisms

As with groups, the functions that preserve structure on rings are of primary interest. We first treat subrings, then introduce homomorphisms.

Definition 4.2.1. Let R be a ring. A subset $T \subseteq R$ is a **subring** of R when T is an additive subgroup of R, T is closed under multiplication, and T contains 1_R.

Example 4.2.2. The ring of integers $\mathbb{Z}$ is a subring of $\mathbb{Q}$. The rings $\mathbb{Z}/n$ have no proper subrings because of the requirement that the unitary element, 1, be contained in a subring. Adding 1 to itself will give all of $\mathbb{Z}_n$.

The polynomial ring $F[x]$ for F a field has many subrings: F itself, any subring of F, and subrings generated by a polynomial. For example, $F[x^2]$ would contain all polynomials in which each term has even degree. One can check that it is indeed a subring of $F[x]$.

Exercises 4.2.3. Suppose R, S are subrings of a ring T.

- **(a)** Show that $R \cap S$ is also a subring of T.
- **(b)** If R and S are integral domains, show that $R \cap S$ is also an integral domain.
- **(c)** If R and S are fields, show that $R \cap S$ is also a field.
- **(d)** More generally, show that for any subset A of T, that the intersection of all rings containing A is a subring of T.
- **(e)** Similarly, show that for any subset A of T, that the intersection of all fields containing A is a subring of T.
- **(f)** Give an example to show that $R \cup S$ may not be a ring.

Definition 4.2.4. Let R, S be rings. A funtion $\varphi : R \longrightarrow S$ is a *ring homomorphism* when

(1) φ is a homomorphism of the additive groups $R, +_R$ and $S, +_S$, and

(2) $\varphi(1_R) = 1_S$, and

(3) for $r_1, r_2 \in R$,

$$\varphi(r_1 *_R r_2) = \varphi(r_1) *_S \varphi(r_2)$$

Notice that the operation on the left-hand side is in R and the operation $*$ on the right-hand side is in S. When we want to be careful we specify the ring for the operation as we did here, but generally this is left to the reader to infer. We say φ *respects addition, multiplication and the identity element.* That is, it *respects* the ring structure. Recall from group theory that it is sufficient to check that a function φ respects the group operation to ensure that φ is a homomorphism. Thus to check if $\varphi : R \longrightarrow S$ is a ring homomorphism one verifies that $\varphi(1_R) = 1_S$, $\varphi(r_1 +_R r_2) = \varphi(r_1) +_S \varphi(r_2)$, and $\varphi(r_1 *_R r_2) = \varphi(r_1) *_S \varphi(r_2)$.

If S is a subring of R then there is a homomorphism, the **inclusion homomorphism**, from S to R.

Proposition 4.2.5. *Let R, S, T be rings. If $\varphi : R \longrightarrow S$ and $\theta : S \longrightarrow T$ are ring homomorphisms then the composition $\theta \circ \varphi$ is also a ring homomorphism.*

The proof is left as an exercise.

Definition 4.2.6. The **kernel** of a ring homomorphism $\varphi : R \longrightarrow S$ is the preimage of 0_S; that is $\{r \in R : \varphi(r) = 0_S\}$. A homomorphism that is injective is called an **embedding**. A homomorphism that is a bijection (injective and surjective) is called an **isomorphism**.

From group theory we know that the kernel is a normal subgroup (since addition in rings is commutative, any subgroup is normal). The kernel has an additional important property, which is item (3) in the following theorem.

Theorem 4.2.7. *Let $\varphi : R \longrightarrow S$ be a homomorphism of rings and let K be the kernel.*

(1) The image of R is a subring of S.

(2) φ is injective if and only if $K = \{0_R\}$.

(3) For any $r \in R$ and any $k \in K$, $r *_R k \in K$.

Proof. We know that $\varphi(R)$ is a subgroup of S. From the requirement that $\varphi(1_R) = 1_S$ we have $1_S \in \varphi(R)$. To show that $\varphi(R)$ is closed under multiplication, let $\varphi(r_1)$ and $\varphi(r_2)$ be arbitrary elements of $\varphi(R)$. Then $\varphi(r_1) *_S \varphi(r_2) = \varphi(r_1 *_R r_2)$, and this is in $\varphi(R)$.

For the properties of the kernel, note first that if φ is injective there can only be one element that maps to 0_S, and that is 0_R. Conversely, suppose $K = \{0_R\}$, and suppose $\varphi(r) = \varphi(r')$. Then $\varphi(r - r') = \varphi(r) - \varphi(r') = 0_S$. Since the kernel is trivial, $r - r' = 0_R$ so $r = r'$. This establishes injectivity.

Let $k \in K$ and $r \in R$. We have

$$\varphi(r *_R k) = \varphi(r) *_S \varphi(k) = \varphi(r) *_S 0_S = 0_S$$

Thus $r *_R k \in K$.

□

As with isomorphisms of groups, the isomorphisms between rings set up an equivalence relation. Every ring is clearly isomorphic to itself via the identity map. The following theorem establishes symmetry and transitivity.

Theorem 4.2.8. *If $\varphi : R \longrightarrow S$ is an isomorphism then φ^{-1} is also an isomorphism. The composition of two isomorphisms is an isomorphism.*

Proof. Let $\varphi : R \longrightarrow S$ be an isomorphism of rings. Then φ is a bijection, so φ^{-1} is also a bijection from S to R. We must show it is a homomorphism. Since φ is a homomorphism, $\varphi(1_R) = 1_S$ and therefore $\varphi^{-1}(1_S) = 1_R$ (since φ is injective, this is the sole preimage).

To show φ^{-1} respects addition and multiplication, let s, s' be arbitrary elements of S. Since φ is a bijection, there are unique $r, r' \in R$ such that $\varphi(r) = s$ and $\varphi(r') = s'$.

$$\begin{aligned}\varphi^{-1}(s *_S s') &= \varphi^{-1}\big(\varphi(r) *_S \varphi(r')\big)\\ &= \varphi^{-1}\big(\varphi(r *_R r')\big)\\ &= r *_R r'\\ &= \varphi^{-1}(s) *_R \varphi^{-1}(s')\end{aligned}$$

This shows φ^{-1} respects multiplication. A completely analogous proof is used for addition. □

Definition 4.2.9. Two rings R, S are **isomorphic** if there is an isomorphism from R to S (and therefore, by the theorem, also an isomorphism from S to R).

Exercises 4.2.10. Let $\varphi : R \longrightarrow S$ be a ring homomorphism.

(a) Show that for any subring R' in R, the image $\varphi(R')$ is a subring of S.

(b) Show that any subring S' of S, the preimage $\varphi^{-1}(S')$ is a subring of R.

The Integers and $F[x]$ for F a Field

The following theorem shows that the Integers are the "original (or initial) ring."

Theorem 4.2.11 (The Initial Ring)**.** *For any ring R there is a unique homomorphism from $\mathbb{Z}$ to R. The kernel is the set of multiples of some integer m. If $m = 0$ then R has a subring isomorphic to $\mathbb{Z}$. If $m > 0$, there is an isomorphism of $\mathbb{Z}/m$ with a subring of R.*

Proof. A homomorphism $\varphi : \mathbb{Z} \longrightarrow R$, if it exists, would have to take $1_{\mathbb{Z}}$ to 1_R. Applying the requirement that a homomorphism respects addition we see inductively that we must have, for $m > 0$,

$$\varphi(m) = \varphi(\underbrace{1_{\mathbb{Z}} + \cdots + 1_{\mathbb{Z}}}_{m \text{ terms}}) = \underbrace{1_R + \cdots + 1_R}_{m \text{ terms}} = m1_R$$

We also must have $\varphi(-m) = -\varphi(m)$. Thus, there is at most one way to define a homomorphism from $\mathbb{Z}$ to R. This function respects addition:

$$\begin{aligned}
\varphi(m+n) &= (m+n)1_R \\
&= \underbrace{1_R + 1_R + \cdots + 1_R}_{m+n \text{ terms}} \\
&= \underbrace{1_R + \cdots + 1_R}_{m \text{ terms}} + \underbrace{1_R + \cdots + 1_R}_{n \text{ terms}} \\
&= m1_R + n1_R \\
&= \varphi(m) + \varphi(n)
\end{aligned}$$

It also respects multiplication:

$$\begin{aligned}
\varphi(mn) &= mn1_R \\
&= \varphi\big(\underbrace{1_R + 1_R + \cdots + 1_R}_{mn \text{ terms}}\big) \\
&= \big(\underbrace{1_R + \cdots + 1_R}_{m \text{ terms}}\big) *_R \big(\underbrace{1_R + \cdots + 1_R}_{n \text{ terms}}\big) \\
&= (m1_R) * (n1_R) \\
&= \varphi(m) *_R \varphi(n)
\end{aligned}$$

If m generates the kernel the first isomorphism theorem for groups says that $\mathbb{Z}/m$ is isomorphic to a subgroup of R. Since multiplication is just repeated addition, this is also an isomorphism of rings.

□

The integer m in the theorem is called the **characteristic** of R.

The Arithmetic Modulo n Theorem 1.1.13 shows that the function taking $a \in \mathbb{Z}$ to $[a]_n \in \mathbb{Z}/n$ is a homomorphism. We actually define addition and multiplication in $\mathbb{Z}/n$ via addition and multiplication in $\mathbb{Z}$, so it is an immediate consequence that the map is a homomorphism.

If d divides m there is a well-defined function from $[a]_m$ to $[a]_d$— this is because $d|m$ and $m|(b-a)$ implies $d|(b-a)$—so any two integers that are congruent modulo m are also congruent modulo d. On the other hand if $d \nmid m$, there is no well-defined homomorphism from $\mathbb{Z}/m$ to $\mathbb{Z}/d$: we would have to take $[1]_m$ to $[1]_d$ but

$m[1]_m = [0]_m$ and $m[1]_d \neq [0]_d$. Since the arithmetic on $\mathbb{Z}/m$ is "inherited" from $\mathbb{Z}$, we have:

Theorem 4.2.12 (Homomorphism mod m)**.** *The function $\mathbb{Z} \longrightarrow \mathbb{Z}/n$ taking a to $[a]_n$ is a homomorphism.*

There is a homomorphism from $\mathbb{Z}/m$ to $\mathbb{Z}/d$ if and only if d divides m. The homomomorphism is unique (since it takes $[1]_m$ to $[1]_d$).

We have a similar result for polynomial rings.

Theorem 4.2.13 (Homomorphism mod $m(x)$)**.** *Let F be a field and $m(x) \in F[x]$ The function $F[x] \longrightarrow F[x]/m(x)$ taking $a(x)$ to its equivalence class $[a(x)]$ is a homomorphism.*

There is a homomorphism from $F[x]/m(x)$ to $F[x]/r(x)$ if and only if $r(x)$ divides $m(x)$.

4.3 Constructions

In this section we introduce three ways to construct new rings: using direct products, using an indeterminate to create a polynomial ring, and using matrices to create a noncommutative ring.

Direct Products

In Section 2.3 we showed that the Cartesian product of groups has the structure of a group. Not surprisingly, we have the same situation with rings, but there is one subtle difference, discussed below.

Definition 4.3.1. Let R and S be rings. The Cartesian product $R \times S$, along with the operations below form the **direct product** of R and S.

$$\begin{aligned} -(r, s) &= (-r, -s) \\ (r_1, s_1) +_{R\times S} (r_2, s_2) &= (r_1 +_R r_2, s_1 +_S s_2) \\ (r_1, s_1) *_{R\times S} (r_2, s_2) &= (r_1 *_R r_2, s_1 *_S s_2) \end{aligned}$$

The additive identity and multiplicative identies are of course $(0_R, 0_S)$ and $(1_R, 1_S)$. The following proposition shows that the direct product of rings is in fact a ring and gives other important properties.

Proposition 4.3.2 (Direct Product)**.** *Let R and S be rings.*

(1) The above definition does, indeed, make $R \times S$ a ring.

(2) The associative law for products of several rings holds: $R_1 \times (R_2 \times R_3) \cong (R_1 \times R_2) \times R_3$.

(3) If R' is a subring of R and S' is a subring of S then $R' \times S'$ is a subring of $R \times S$.

(4) The projection maps $p_R : R \times S \longrightarrow R$ and $p_S : R \times S \longrightarrow S$ are surjective homomorphisms.

(5) The construction and the observations above can be generalized to the direct product of any set of rings $\{R_i : i \in I\}$ indexed by a finite set I. (It extends with some modification due to subtle issues when I is infinite.)

The subtle difference between the product of groups and the product of rings is that there does not exist a natural homomorphism $R \longrightarrow R \times S$. The choice that one might expect would be to send r to $(r, 0)$ but this violates the requirement that the multiplicative identity on R should map to the multiplicative identity on $R \times S$.

Exercises 4.3.3. Let R and S be rings and consider $R \times S$.

(a) Identify all the units in $R \times S$.

(b) Identify all of the zero-divisors in $R \times S$.

The following property of the direct product of rings is analogous to the one for groups, Proposition 2.3.6. The proof is easily adapted from the proof for groups.

Proposition 4.3.4 (Universal Property of the Product)**.** *Let R, S and T be rings, and let $\varphi : T \longrightarrow R$ and $\psi : T \longrightarrow S$ be homomorphisms. The function $\alpha : T \longrightarrow R \times S$ defined by $t \longmapsto (\varphi(t), \psi(t))$ is a homomorphism. It is the unique homomorphism such that $p_R \circ \alpha = \varphi$ and $p_S \circ \alpha = \psi$.*

Exercises 4.3.5. An element e in a ring R is **idempotent** when $a^2 = a$. Evidently, both 0_R and 1_R are idempotents. If R and S are rings, then $R \times S$ has two additional idempotents $(1, 0)$ and $(0, 1)$.

(a) let R be a ring with an idempotent e.

(1) Prove that the set $Re = \{re : r \in R\}$ with the operations inherited from R has the structure of a ring, with identity e. It is not a subring of R because the multiplicative identity element is different.

(2) Prove that $(1 - e)$ is also an idempotent in R.

(3) Prove that every element in R may be uniquely expressed as the sum of an element in Re and an element in $R(1 - e)$.

(b) Find the idempotents in $\mathbb{Z}/12$ and comment on the decomposition above.

(c) Find the idempotents in $\mathbb{Z}/30$ and comment on the decomposition above.

Polynomial Rings

We have already discussed polynomial rings that have coefficients in a field, such as $\mathbb{Q}[x]$, $\mathbb{F}_p[x]$. The construction generalizes to any ring. For R a ring, the polynomial ring $R[x]$ is the set of elements of the form

$$a_0 + a_1x + a_2x^2 + \cdots + a_\delta x^\delta$$

with the $a_i \in R$. The sum of two elements and product of two elements are familiar formulas. For example,

$$\begin{aligned}
&(a_0 + a_1x + a_2x^2 + a_3x^3) + (b_0 + b_1x + b_2x^2 + b_3x^3)\\
&\qquad = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + (a_3 + b_3)x^3\\
&(a_0 + a_1x + a_2x^2)(b_0 + b_1x + b_2x^2)\\
&\qquad = a_0b_0 + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2
\end{aligned}$$

Some care is in order to stipulate that, for example, $a_0 + a_1x = a_0 + a_1x + 0x^2$. I'll introduce the following formal definition, but your instincts should be your guide.

Definition 4.3.6. Let R be a ring. A **polynomial** in x over R is a sum $a(x) = \sum_{i=0}^{\infty} a_ix^i$ in which only a finite number of the a_i are nonzero. The **support** of $a(x)$ is the set of powers of x for the nonzero terms $\left\{x^i : a_i \neq 0\right\}$, or depending on the context, the indices of those terms, $\{i : a_i \neq 0\}$. For $a(x)$ nonzero, the **degree** is the maximal index with a nonzero term, $\deg(a(x)) = \max_{i\in\mathbb{N}_{\geq 0}} \{i : a_i \neq 0\}$. We set the degree of the 0 polynomial to be $-\infty$.

The **polynomial ring over R with indeterminate** x is the set of all polynomials.

$$\left\{\sum_{i=0}^{\infty} a_ix^i : a_i \in R, \text{ and } \{i : a_i \neq 0\} \text{ is finite}\right\}$$

The additive inverse of $\sum_{i=0}^{\infty} a_ix^i$ is $\sum_{i=0}^{\infty}(-a_i)x^i$. The sum is defined by

$$\sum_{i=0}^{\infty} a_ix^i + \sum_{i=0}^{\infty} b_ix^i = \sum_{i=0}^{\infty}(a_i + b_i)x^i$$

and the product is defined by $(ax^i) * (bx^j) = abx^{i+j}$ and applying distributivity, commutativity and distributivity. Consequently,

$$(\sum_{i=0}^{\infty} a_ix^i)(\sum_{j=0}^{\infty} b_jx^j) = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} a_ib_jx^{i+j}$$

and we can rearrange the sum using $k = i + j$ and gathering terms in x^k,

$$= \sum_{k=0}^{\infty} x^k \sum_{i=0}^{k} (a_i b_{k-i})$$

As an aside, if we don't require the support to be finite we still get a valid ring, which is called the ring of formal power series.

One should check that all the properties of a ring hold, a somewhat tedious exercise. As an example, for associativity one can show that

$$\Big(a(x)b(x)\Big)c(x) = \sum_m \sum_{\substack{i,j,k \geq 0 \\ i+j+k=m}} a_i b_j c_k = a(x)\Big(b(x)c(x)\Big)$$

Proposition 4.3.7. *For any ring R and $a(x), b(x) \in R$,*

$$\deg\big(a(x)b(x)\big) \leq \deg\big(a(x)\big) + \deg\big(b(x)\big)$$

If R is an integral domain then equality holds, the degree of a product of polynomials is the sum of the degrees of the factors:

$$\deg\big(a(x)b(x)\big) = \deg\big(a(x)\big) + \deg\big(b(x)\big)$$

In particular, if R is an integral domain, then $R[x]$ is also an integral domain.

Proof. Let $\gamma = \deg(a(x))$ and $\delta = \deg(b(x))$. From the formula for the product the degree k term in $a(x)b(x)$ is $\Big(\sum_{i=0}^{k} a_i b_{k-i}\Big)$. When $k > \gamma + \delta$, the kth term will be 0 because for $i > \gamma$, $a_i = 0$, and for $i \leq \gamma$, $k - i > \delta$ so $b_{k-i} = 0$. For $k = \gamma + \delta$ the kth term in the product is $a_\gamma b_\delta$. This may be 0 in a ring with zero-divisors, hence the degree of a product may be less than the sum of the degrees of the factors over a ring R with zero-divisors.

In an integral domain, $a_\gamma b_\delta \neq 0$ since we assume a_γ and b_δ are nonzero. In particular, a product of nonzero polynomials over an integral domain cannot be zero. This proves the proposition. □

The key lemma (1.3.1) that was used to prove the Quotient Remainder Theorem (1.3.2) in $F[x]$ does not apply over an arbitrary ring.

Exercises 4.3.8. Polynomial rings and zero divisors.

- **(a)** Give an example to show the analogue of Lemma 1.3.1 does not hold in the polynomial ring over $\mathbb{Z}/4$.
- **(b)** Show that $\mathbb{Z}/4[x]$ has a polynomial of degree 1 that is a unit (in fact its square is 1).

(c) Give an example of two polynomials of degree 2 in $\mathbb{Z}/8[x]$ such that their product has degree 1. Show that this is not possible in $\mathbb{Z}/4[x]$ and $\mathbb{Z}/6[x]$.

Here is an additional result about polynomial rings that will be useful. It is similar to The Initial Ring Theorem 4.2.11 for the integers.

Theorem 4.3.9 (Universal property of polynomial rings)**.** *Let R, S be rings and let $\varphi : R \longrightarrow S$ be a ring homomorphism. For any $s \in S$ there is a unique homomorphism from $R[x]$ to S that agrees with φ on R and takes x to s, namely*

$$\begin{aligned} \overline{\varphi} : R[x] &\longrightarrow S \\ \big(\sum_i r_i x^i\big) &\longmapsto \sum_i \varphi(r_i) s^i \end{aligned}$$

Proof. To simplify the notation the summations in the text below are implicitly over the nonnegative integers unless expressed otherwise. If there is a homomorphism $\overline{\varphi}$ taking x to s and agreeing with φ on R then we must have

$$\overline{\varphi}\Big(\sum_i r_i x^i\Big) = \sum_i \overline{\varphi}(r_i x^i) = \sum_i \overline{\varphi}(r_i)\overline{\varphi}(x)^i = \sum_i \varphi(r_i) s^i$$

So there is only one possible way to define $\overline{\varphi}$. The key observation is that $\overline{\varphi}$ is well defined because there is a unique way to write each element of $R[x]$ and we have used this unique formulation to define $\overline{\varphi}$. We also note that the sums are all finite sums.

To show this function is indeed a homomorphism we check that it respects the operations. Here we check just products. As we saw above commutativity, associativity and distributivity in the polynomial ring give

$$(\sum_i a_i x^i)(\sum_j r_j x^j) = \sum_k x^k \sum_{i=0}^{k} (a_i r_{k-i})$$

A similar derivation shows that for $b_i, t_i \in S$

$$(\sum_i b_i s^i)(\sum_i t_i s^i) = \sum_k s^k \sum_{i=0}^{k} (b_i t_{k-i})$$

Thus we have

$$
\begin{aligned}
\overline{\varphi}\Big(\Big(\sum_i a_i x^i\Big)\Big(\sum_i b_i x^i\Big)\Big) &= \overline{\varphi}\Big(\sum_k x^k \Big(\sum_{i=0}^{k} a_i b_{k-i}\Big)\Big) \\
&= \sum_k s^k \Big(\sum_{i=0}^{k} \varphi(a_i b_{k-i})\Big) \\
&= \Big(\sum_i \varphi(a_i) s^i\Big)\Big(\sum_j \varphi(b_j) s^j\Big) \\
&= \overline{\varphi}\Big(\sum_i a_i x^i\Big)\overline{\varphi}\Big(\sum_i b_i x^i\Big)
\end{aligned}
$$

This shows $\overline{\varphi}$ respects products. □

In the first encounter a student has with polynomials they are treated as functions. For a polynomial over $\mathbb{Q}$, one substitutes a rational number for x and computes a rational number as output. Up to this point we have treated polynomials algebraically by adding and multiplying. The previous theorem has applications in which we treat polynomials as functions.

Exercises 4.3.10.

(a) Consider $R = S = \mathbb{Q}$ and $s = 0$. Explain how to apply the theorem to show that evaluating all polynomials in $\mathbb{Q}[x]$ at 0 yields a homomorphism from $\mathbb{Q}[x]$ to $\mathbb{Q}$.

(b) More generally, apply the theorem to the situation where $S = R$ and s is some particular element of R. Interpret the theorem for this situation as saying that "evaluating at a fixed $s \in R$" determines a homomorphism.

(c) Let's apply the theorem to the situation where $S = R[x]$ and the particular element $s(x) \in R[x]$. The theorem says that there is a homomorphism

$$
\begin{aligned}
\varphi : R[x] &\longrightarrow R[x] \\
x &\longrightarrow s(x)
\end{aligned}
$$

Show that an arbitrary $f(x) \in R[x]$ maps to $f(s(x))$. Show that, as a function this is the composition of the function defined by $f(x)$ and the function defined by $s(x)$.

By iteratively applying the polynomial ring construction we can create a polynomial ring in several indeterminates over a ring R.

Definition 4.3.11. The polynomial ring over the ring R in indeterminates $x_1, x_2, \ldots, x_n$, which we write as $R[x_1, x_2, \ldots, x_{n-1}, x_n]$, is defined inductively as $R[x_1, \ldots, x_{n-1}][x_n]$.

An element $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ is called a **monomial**. We will say that $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is the **multidegree** of this monomial. The elements of $R[x_1, x_2, \ldots, x_{n-1}, x_n]$ are finite sums of **terms** of the form $ax_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$.

This has the following important property.

Theorem 4.3.12 (Universal property of polynomial rings)**.** *Let R, S be rings and let $\varphi : R \longrightarrow S$ be a ring homomorphism. For any $s_1, \ldots, s_n \in S$ there is a unique homomorphism from $R[x_1, x_2, \ldots, x_n]$ to S that agrees with φ on R and takes x_i to s_i.*

Matrix Rings

Although we are focusing on rings that are commutative, and moreover, have defined a ring to be commutative, it is worth presenting one very important example of a noncommutative ring.

Definition 4.3.13. Let R be a ring and let n be a positive integer. The $n \times n$ **matrix ring** over R, written $M_n(R)$, is the set of $n \times n$ matrices using the usual formulas for addition and multiplication.

Even for a field, the matrix ring is noncommutative, as you may recall from your experience with linear algebra.

Exercises 4.3.14. Consider $M_2(\mathbb{Q})$ and recall the various spaces associated to a matrix (e.g. rowspace, nullspace).

(a) Show that $A = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ is a zero divisor in $M_2(\mathbb{Q})$. Find a B such that $AB = 0$ (the zero matrix). Find a C such that $CA = 0$.

(b) What characterizes the zero divisors in $M_2(\mathbb{Q})$?

(c) Show that every nonzero element of $M_2(\mathbb{Q})$ (or more broadly $M_n(F)$ for F a field) is either a zero divisor or a unit.

In linear algebra, matrices over a field arise as functions that map one vector space to another. A square matrix maps a vector space to itself. Matrices over a ring can also be treated as functions: an $m \times n$ matrix over R maps a "vector" of length n over R to a "vector" of length m over R, using the familiar formulas for the product of a matrix and vector. I put vector in quotes because R^n is not a vector space when R is not a field. Yet, R^n, with rules for addition and scalar multiplication analogous to those for vector spaces, is an interesting object to study. Modules over a ring are the generalization of vector spaces. The subject is a bit more complex because not every nonzero element is a unit, and, even more challenging, there may be zero-divisors in the ring.

4.4 Ideals and Quotient Rings

For a group $G, *$ the operation can be extended to cosets of a subgroup, provided the subgroup N is normal. This allows for the construction of the quotient group G/N. For rings, we want both addition and multiplication to extend to cosets, and the appropriate subsets of a ring that allow for this are ideals.

Definition 4.4.1. An **ideal** of a ring R is a nonempty subset $I \subseteq R$ which is closed under addition and closed under multiplication by an arbitrary element of R:

$$a + b \in I \qquad \text{if } a, b \in I \tag{4.1}$$

$$ra \in I \qquad \text{if } a \in I \text{ and } r \in R \tag{4.2}$$

We will say that I **absorbs products**.

Proposition 4.4.2. *Let R be a ring.*

If an ideal I of R contains a unit, then $I = R$.

For any $a_1, a_2, \ldots, a_n \in R$, the following set is an ideal of R.

$$I = \{r_1a_1 + r_2a_2 + \cdots + r_na_n : r_i \in R\}$$

Proof. Let R be a ring. Let u be a unit in R with inverse v. If I is an ideal containing u then $uv = 1$ is also in I since I absorbs products. Again, since I absorbs products, for any $r \in R$, $r1 = r \in R$. Thus $I = R$.

Let $a_1, \ldots, a_n$ be arbitrary elements of r. We want to show

$$I = \{r_1a_1 + r_2a_2 + \cdots + r_na_n : r_i \in R\}$$

is an ideal of R. We can see that I is closed under addition because

$$\begin{aligned}&(r_1a_1 + r_2a_2 + \cdots + r_na_n) + (s_1a_1 + s_2a_2 + \cdots + s_na_n)\\ &\quad = r_1a_1 + s_1a_1 + r_2a_2 + s_2a_2 + \cdots + r_na_n + s_na_n\\ &\quad = (r_1 + s_1)a_1 + (r_2 + s_2)a_2 + \cdots + (r_n + s_n)a_n\end{aligned}$$

The first step repeatedly uses commutativity and associativity of addition. The last step uses distributivity. The final expression is in a form that shows it is an element of I.

The product of any $t \in R$ with $r_1a_1 + r_2a_2 + \cdots + r_na_n$ is

$$t\big(r_1a_1 + r_2a_2 + \cdots + r_na_n\big) = (tr_1)a_1 + (tr_2)a_2 + \cdots + (tr_n)a_n$$

using distributivity and associativity of multiplication. The result is in a form to show it is in I. $\square$

Definition 4.4.3. We say I **is generated by** $a_1, a_2, \ldots, a_s$ if $I = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n : r_i \in R\}$. We write $I = \langle a_1, a_2, \ldots, a_n \rangle$. The ideal I is **principal** if there exists some $a \in I$ such that $I = \{ra : r \in R\}$. A ring in which all ideals are principal is called a **principal ideal domain**, or a PID for short.

An ideal generated by several elements may also be generated by a single element, and therefore be principal.

Proposition 4.4.4. *Every ideal in $\mathbb{Z}$ is principal. Every ideal in $F[x]$ for F a field is principal.*

Proof. Let I be an ideal of $\mathbb{Z}$. If $I = \{0\}$, there is nothing to prove. Otherwise, let a be the smallest positive integer in I. Let b be any other nonzero element of I. Then, by the properties of ideals, any linear combination of a and b is in I. By the GCD Theorem 1.1.4, $\gcd(a, b) \in I$. But the gcd of a and b is positive and less than or equal to a. Since a is the smallest positive element of I, we must have $\gcd(a, b) = a$. Consequently, an arbitrary element of I is divisible by a, so $I = \langle a \rangle$ is principal.

The same proof applies to $F[x]$ with minor modification. For I a nonzero ideal of $F[x]$, one uses the monic polynomial of lowest degree in I.

□

From the proof we see that the ideals of $\mathbb{Z}$ are in one correspondence with the nonnegative integers. Similarly, the principal ideals, other than the 0-ideal, of $F[x]$ are in one to one correspondence with the monic polynomials.

Exercises 4.4.5.

- **(a)** Let R be a subring of a ring S. Let I be an ideal in S. Show that $I \cap R$ is an ideal in R.

Exercises 4.4.6. Let R and S be rings and consider $R \times S$.

- **(a)** Let I be an ideal in R and J and ideal in S. Show that $I \times J$ is an ideal in $R \times S$.
- **(b)** Show that all ideals in $R \times S$ are of the form $I \times J$.

Quotient Rings

A ring R is an abelian group under addition, so, for any subgroup, we can form the quotient group of R by that subgroup. It is natural, when we take the multiplicative structure of R into account, to want the quotient group to also have a multiplicative structure. The necessary property to make this work is the "absorbs products" requirement in the definition of ideal. We have actually seen this appear in Proposition 4.2.7 which said that the kernel of a homomorphism is closed under multiplication by an arbitrary element of R.

We will write cosets of an ideal I in R in the same form as we did for abelian groups. For any $r \in R$, its coset is $r + I$. The coset $r + I$ may be written in other ways; for any $a \in I$, the cosets defined by r and by $r + a$ are the same. For $s \in R$, and $b \in I$ the cosets defined by s and $s + b$ are also the same. We would like to define multiplication of cosets, but for that to work, the product should be independent of the way we name the coset (as $r + I$ or as $(r + a) + I$). In other words we want the products rs and $(r + a)(s + b)$ to define the same cosets. We have

$$(r + a)(s + b) = rs + as + rb + ab$$

Since $a, b \in I$ and I absorbs products, $as + rb + ab \in I$. Thus $rs + I = (r + a)(s + b) + I$, and we have a well-defined product for cosets of I.

The following proposition summarizes this discussion, and we note that multiplication of cosets is determined by multiplication in R so we get a homomorphism from R to R/I.

Proposition 4.4.7. *Let R be a ring and let I be a proper ideal in R (that is $I \neq R$). Let $R/I = \{r + I : r \in R\}$. Then R/I is a ring, with additive structure defined by R/I as the quotient of the abelian group R by its subgroup I, and multiplicative structure defined by*

$$(r + I)(s + I) = rs + I$$

The additive identity is $0 + I$ and the multiplicative identity is $1 + I$.

The function $R \longrightarrow R/I$ that takes r to $r + I$ is a homomorphism of rings.

Example 4.4.8. In $\mathbb{Z}$, the subgroups $\langle n \rangle$ are also ideals, because multiplication is simply repeated addition, and a subgroup is closed under addition. Thus the quotient of $\mathbb{Z}$ by its subgroup $\langle n \rangle$ is a ring.

Example 4.4.9. Let F be a field. We have seen that any ideal in $F[x]$ is principal, generated by some $m(x) \in F[x]$. Every polynomial is congruent modulo $m(x)$ to its remainder upon division by $m(x)$.

We have already seen two familiar examples of quotient rings in Chapter 1, the integers modulo n and, for F a field, $F[x]$ modulo $m(x)$. The treatment of these in Chapter 1 is from a modular arithmetic perspective and we used brackets to define the equivalence class for elements. We now see them each as a quotients of a ring ($\mathbb{Z}$ or $F[x]$ repectively) and we now write the equivalence classes as cosets rather than using brackets. One convenient aspect of working with these quotient rings is that each element can be *uniquely represented* by the remainder upon division by the modulus. One can use $\{0, 1, \ldots, n - 1\}$ as the elements of $\mathbb{Z}/n$ and omit the brackets or coset notation when the context makes clear that we are working in $\mathbb{Z}/n$ rather than $\mathbb{Z}$. Similarly one can use polynomials of degree less than $\deg(m(x))$ as the elements of $F[x]/m(x)$.

Definition 4.4.10. Let R be a ring and I an ideal in R. A **system of representatives** for R/I is a set $S \subseteq R$ such that each $r \in R$ is congruent modulo I to exactly one element of S.

It can be more challenging to find a system or representatives for R/I in other rings, even in $F[x, y]$ with F a field. In polynomial rings over a field, monomial ideals and principal ideals admit a clear system or representatives, but things get much more complicated when there are several polynomial generators or when the base ring is not a field.

Definition 4.4.11. In a polynomial ring $R[x_1, x_2, \ldots, x_n]$, a **monomial ideal** is an ideal generated by monomials.

For the following two examples it is helpful to think of $F[x, y]$ as a vector space over F with basis $x^i y^j$ for $i, j \geq 0$.

Example 4.4.12. Consider a field F and $F[x, y]/\langle x^\alpha y^\beta \rangle$. Since an ideal is closed under multiplication, every monomial $ax^{\alpha'} y^{\beta'}$ with $\alpha' \geq \alpha$ and $\beta' \geq \beta$ is in $\langle x^\alpha y^\beta \rangle$. Since an ideal is closed under addition, and any sum of monomials with x-degree at least α and y-degree at least β is in $\langle x^\alpha y^\beta \rangle$. Conversely, any multiple of $x^\alpha y^\beta$ must be a polynomial whose terms all have x-degree at least α and y-degree at least β. The multidegrees of the monomials in $\langle x^\alpha y^\beta \rangle$ are those in the region marked Γ shown in Figure 4.1.

Given any polynomial we may subtract off the monomials that are multiples of $x^\alpha y^\beta$ and be left with a polynomial that has terms that have x-degree less than α or y-degree less than β. The multidegrees of these monomials are in the region marked Δ in Figure 4.1. These monomials are a basis for the quotient ring $F[x, y]/\langle x^\alpha y^\beta \rangle$. A set of representatives for $F[x, y]/\langle x^\alpha y^\beta \rangle$ is all polynomials whose terms have multidegree in Δ.

Example 4.4.13. Consider a field F and $F[x, y]/\langle x^3, xy, y^2 \rangle$. A monomial that is in $\langle x^3, xy, y^2 \rangle$ has multidegree that is in the region marked Γ in Figure 4.2. As in the previous example any polynomial whose terms involve just monomials with multidegree in Γ will be in $\langle x^3, xy, y^2 \rangle$. Given any other polynomial we may subtract off elements of $\langle x^3, xy, y^2 \rangle$ and be left with a polynomial all of whose terms are in the set Δ in Figure 4.2. The monomials with multidegree in Δ form a basis for a set of representatives for $F[x, y]/\langle x^3, xy, y^2 \rangle$. The set of representatives is all polynomials whose terms have multidegree in Δ.

Figure 4.1

Figure 4.2

Example 4.4.14. Consider now a principal ideal that is non-monomial, $F[x,y]/\langle y^2+x^3\rangle$. In this quotient ring $y^2=-x^3$. Given an arbitary polynomial we can replace y^2 with $-x^3$ and get a polynomial that is equivalent modulo y^2+x^3 and has terms that are at most degree 1 in y. Thus $\{x^i : i \in \mathbb{N}_0\} \cup \{x^i y : i \in \mathbb{N}_0\}$ is a basis for $F[x,y]/\langle y^2+x^3\rangle$. (It should be clear that no sum of these monomials can be a multiple of y^2+x^3.) Alternatively, we could replace each occurence of x^3 with $-y^2$ and obtain a basis $\{y^j : j \in \mathbb{N}_0\} \cup \{xy^j : j \in \mathbb{N}_0\} \cup \{x^2y^j : j \in \mathbb{N}_0\}$.

We have emphasized the strong relationship between the ring integers of $\mathbb{Z}$ and polynomial rings $F[x]$ for F a field. We have seen a couple of examples in $F[x,y]$. There are analogous examples for $\mathbb{Z}[y]$. We substitute a prime, say 2, for x and consider something analogous to a monomial ideal.

Example 4.4.15. Consider the ideal $\langle 4y^3, 8y^2\rangle$ in $\mathbb{Z}[y]$. The multiples of $4y^3$ will all have degree at least 4 (in y) and will have coefficient a multiple of 4. A set of representatives for $\mathbb{Z}[y]/\langle 4y^3, 8y^2\rangle$ is $a_0 + a_1y + a_2y^2 + a_3y^3 + \dots$ in which $a_k \in \{0,1,2,3\}$ for $k \geq 3$ and $a_2 \in \{0,1,2,3,4,5,6,7\}$ and $a_0, a_1 \in \mathbb{Z}$.

Exercises 4.4.16.

- **(a)** Find the nilpotents, zero divisors, and units in $F[x,y]/\langle x^3y^2\rangle$.
- **(b)** Find the nilpotents, zero divisors, and units in $F[x,y]/\langle x^3, y^2\rangle$.
- **(c)** Find the nilpotents, zero divisors, and units in $F[x,y]/\langle x^3, xy, y^2\rangle$.
- **(d)** Find the nilpotents, zero divisors, and units in $F[x,y]/\langle y^2-x^3\rangle$.

Exercises 4.4.17.

- **(a)** We were careful in the last example to use powers of 2 as the coefficients in the ideal in $\mathbb{Z}[y]$. Find a system of representatives for $\mathbb{Z}[y]/\langle 4y^3, 7y^2\rangle$.
- **(b)** Find a system of representatives for $\mathbb{Z}[y]/\langle ay^5, by^4, cy^2, dy\rangle$. [Hint: GCD.]

4.5 Isomorphism Theorems

The First and Third Isomorphism Theorems for rings are quite straightforward extensions of the theorems for groups as are the Factor Theorem and Correspondence Theorem. The first theorem below combines the First Isomorphism Theorem and the Factor Theorem. The Second Isomorphism Theorem, treated at the end of the section, is less central in ring theory.

Theorem 4.5.1 (First Isomorphism and Factor Theorems). *Let $\varphi : R \longrightarrow S$ be a ring homomorphism and let K be the kernel. For any ideal J contained in K the homomorphism φ factors through R/J in the following sense: there is a ring homomorphism $\tilde{\varphi} : R/J \longrightarrow S$ defined by $r + J \longrightarrow \varphi(r)$ such that $\tilde{\varphi} \circ \pi = \varphi$.*

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\pi"'] & S \\ R/J \arrow[ur, dashed, "\tilde{\varphi}"'] & \end{tikzcd}$$

Additionally,

(1) If $J = K$ then $\tilde{\varphi}$ is injective.

(2) If φ is surjective then so is $\tilde{\varphi}$.

(3) If $J = K$ and φ is surjective then $\tilde{\varphi}$ is an isomorphism.

Proof. Let $\varphi : R \longrightarrow S$ be a ring homomorphism with kernel K and J an ideal contained in K. By the Factor Theorem for groups 2.7.11, we know there is well defined group homomorphism $\tilde{\varphi} : R/J \longrightarrow S$. This is because for any $r \in R$ and $j \in J$ we have $\varphi(r + j) = \varphi(r)$, so we can define $\tilde{\varphi}(r + J) = \varphi(r)$ unambiguously. The map is a group homomorphism because

$$\tilde{\varphi}(r_1 + r_2 + J) = \varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) = \tilde{\varphi}(r_1 + J) + \tilde{\varphi}(r_2 + J)$$

Similarly the map respects multiplication because

$$\tilde{\varphi}(r_1 r_2 + J) = \varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2) = \tilde{\varphi}(r_1 + J) * \tilde{\varphi}(r_2 + J)$$

Finally, $\tilde{\varphi}(1_R + J) = \varphi(1_R) = 1_S$, so $\tilde{\varphi}$ is a homomorphism of rings. By construction, $\varphi = \tilde{\varphi} \circ \pi$.

The kernel of $\tilde{\varphi}$ is $\{r + J : \varphi(r) = 0\}$. This is clearly $K/J = \{k + J : k \in K\}$. When $J = K$, $\tilde{\varphi}$ is injective since $\{k + K : k \in K\} = \{0 + K\}$.

Suppose φ is surjective. For any $s \in S$, there is some $\in R$ such that $\varphi(r) = s$. Then $\tilde{\varphi}(r + J) = \varphi(r) = s$, so $\tilde{\varphi}$ is also surjective. If $J = K$ and φ is surjective we have an isomorphism $\tilde{\varphi} : R/K \longrightarrow S$. □

We can derive the Third Isomorphism Theorem as a corollary. Consider the case $\varphi : R \longrightarrow R/K$ and let J be an ideal of R with $J \subseteq K$. The previous theorem says that $\tilde{\varphi} : R/J \longrightarrow R/K$ is a surjective homomorphism. The kernel is $\{r + J : \tilde{\varphi}(r + J) = 0 + K\}$. But $\tilde{\varphi}(r + J) = \varphi(r)$, so the kernel is $\{r + J : r \in K\} = K/J$. Now applying item (3) of the theorem to $\tilde{\varphi}$ we get an isomorphism between $(R/J)/(K/J)$ and R/K.

We can also prove the Third Isomorphism Theorem directly, which we do below.

Theorem 4.5.2 (Third Isomorphism Theorem)**.** *Let R be a ring with ideals K and J such that $J \subseteq K$. Then K/J is an ideal of R/J and $(R/J)/(K/J) \cong R/K$.*

Proof. I claim there is a well defined function from R/J to R/K defined by $\varphi(r+J) = r+K$. We need only check that if $r_1 + J = r_2 + J$ then $r_1 + K = r_2 + K$. This is clearly true because if $r_1 + J = r_2 + J$ then $r_1 - r_2 \in J$. Since $J \subseteq K$ we have $r_1 = r_2 \in K$ so $r_1 + K = r_2 + K$. We clearly also have

$$\begin{aligned}\varphi\big((r_1+J)+(r_2+J)\big) &= \varphi(r_1+r_2+J) \\ &= r_1+r_2+K \\ &= (r_1+K)+(r_2+K) \\ &= \varphi(r_1+K)+\varphi(r_2+K)\end{aligned}$$

and a similar computation holds for multiplication. Thus φ is a homomorphism and it is surjective.

The kernel is $\{r+J : r+K = 0+K\}$, but this is $\{r+J : r \in K\} = K/J$. So by the first isomorphism theorem, $(R/J)/(K/J) \cong R/K$. $\square$

From Theorem 4.5.1 any surjective homomorphism $R \longrightarrow S$ gives rise to an isomorphism between R/K and S where K is the kernel of $R \longrightarrow S$. A strengthening of Theorem 4.5.2 is the following.

Theorem 4.5.3 (Correspondence)**.** *Let $R \longrightarrow S$ be a surjective homomorphism of rings with kernel K. There is a one-to-one correspondence, given by φ, between ideals of S and ideals of R containing K.*

$$\begin{aligned} R &\longrightarrow S \\ I &\longleftrightarrow \varphi(I) \\ \varphi^{-1}(J) &\longleftrightarrow J \end{aligned}$$

The correspondence respects containment, and quotients as follows. For I, I' containing K,

- *$K \le I \le I'$ if and only if $\varphi(I) \le \varphi(I')$.*
- *The map φ induces an isomorphism $R/I \cong S/\varphi(I)$.*

Theorem 4.5.4 (Second Isomorphism)**.** *Let S be a subring of R and let J be an ideal in R.*

(1) $S+J$ is a subring of R.

(2) $S \cap J$ is an ideal in S.

(3) $S/(S\cap J) \cong (S+J)/J$.

Proof. The first two items are left as exercises. Consider the homomorphism $\varphi : S \longrightarrow R/J$, which is the composition of the inclusion map : $S \longrightarrow R$ and the quotient map $R \longrightarrow R/J$. The image of φ is $\{s + J : s \in S\}$ and it is the quotient of the subring $S + J$ in R by the ideal J. The kernel of φ is $S \cap J$. By the first isomorphism theorem, $S/(S \cap J) \cong (S + J)/J$.

□

Exercises 4.5.5.

(a) Prove (1) and (2) of the Second Isomorphism Theorem.

Exercises 4.5.6. Let $\varphi : R \longrightarrow S$ be a homomorphism of rings, not necessarily surjective.

(a) Let J be an ideal in S. Show that $\varphi^{-1}(J)$ is an ideal in R.

(b) Give an example to show that for I an ideal in R, $\varphi(I)$ may not be an ideal in S.

4.6 Operations on Ideals and Properties of Ideals

Intersection, Sum and Product of Ideals

Proposition 4.6.1. *Let I and J be ideals. Then $I \cap J$ is an ideal. More generally, if $\mathcal{A}$ is a set of ideals in R then*

$$\bigcap_{I \in \mathcal{A}} I$$

is an ideal in R.

Proof. Let $a, b \in \bigcap_{I \in \mathcal{A}} I$. Then we have $a, b \in I$ for each $I \in \mathcal{A}$. Since each I is closed under addition, $a + b \in I$ for all $I \in \mathcal{A}$. Consequently, $a + b \in \bigcap_{I \in \mathcal{A}} I$.

Similarly, we can show that $\bigcap_{I \in \mathcal{A}} I$ absorbs products. For $r \in R$ and $a \in \bigcap_{I \in \mathcal{A}} I$ we have $a \in I$ for each $I \in \mathcal{A}$. Since each I absorbs products, $ra \in I$ for each $I \in \mathcal{A}$. Thus $ra \in \bigcap_{I \in \mathcal{A}} I$. □

Definition 4.6.2. Let I and J be ideals. The **sum** of I and J is $I + J = \{a + b : a \in I \text{ and } b \in J\}$. The **product** of I and J is $IJ = \langle ab : a \in I \text{ and } b \in J\rangle$. Similarly for ideals $I_1, \ldots, I_n$ in R we can define

$$I_1 + I_1 + \cdots + I_n = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n : r_k \in R, a_k \in I_k\}$$
$$I_1 I_2 \ldots I_n = \langle a_1 a_2 \cdots a_n : a_k \in I_k \text{ for all } k \in \{1, \ldots, n\}\rangle$$

There is a subtle, but very important, difference in the two definitions. The product of ideals I and J is defined to be *generated* by the set of elements ab with

$a \in I$ and $b \in J$. The sum of I and J is *the set* of all sums $a + b$ with $a \in I$ and $b \in J$. We must show that this set is in fact an ideal.

Proposition 4.6.3. *Let $I_1, \ldots, I_n$ be ideals in R. Then $I_1 + \cdots + I_n$ is also an ideal.*

Proof. We have to show $I_1 + \cdots + I_n$ is closed under sums and that it absorbs products. Consider two arbitrary elements of $I_1 + I_2 + \cdots + I_n$, which we may write as $a_1 + a_2 + \cdots + a_n$ and $b_1 + b_2 + \cdots + b_n$ with $a_k, b_k \in I_k$ for $k = 1, \ldots, n$. Their sum is, after rearranging using commutativity and associativity, $(a_1 + b_1) + (a_2 + b_2) + \cdots + (a_n + b_n)$. Since each $(a_k + b_k) \in I_k$, the sum is an element of $I_1 + I_2 + \cdots + I_n$.

Let $r \in R$ and $a_1 + a_2 + \cdots + a_n$ with $a_k \in I_k$. Then by distributivity

$$r(a_1 + a_2 + \cdots + a_n) = ra_1 + ra_2 + \cdots + ra_n$$

Since each I_k absorbs products, each $ra_k \in I_k$. Thus

$$ra_1 + ra_2 + \cdots + ra_n \in I_1 + I_2 + \cdots + I_n$$

this shows $I_1 + I_2 + \cdots + I_n$ absorbs products. $\square$

Exercises 4.6.4.

(a) In the integers, show that the sum $\langle a \rangle + \langle b \rangle = \langle \gcd(a, b) \rangle$.

(b) In the integers, show that the intersection $\langle a \rangle \cap \langle b \rangle = \langle \operatorname{lcm}(a, b) \rangle$.

(c) Extend these results to $F[x]$ for F a field.

Proposition 4.6.5. *Let $I_1, \ldots, I_n$ be ideals. Then*

$$I_1 I_2 \cdots I_n \subseteq I_1 \cap I_2 \cap \cdots \cap I_n$$

Proof. The product $I_1 I_2 \cdots I_n$ is generated by elements of the form $a_1 a_2 \cdots a_n$ with each $a_k \in I_k$. Since each I_k absorbs products, $a_1 a_2 \cdots a_n \in I_k$ for all k. Thus $a_1 a_2 \cdots a_n \in I_1 \cap I_2 \cap \cdots \cap I_n$. Since the generators of $I_1 I_2 \cdots I_n$ are all in $I_1 \cap I_2 \cap \cdots \cap I_n$ we have

$$I_1 I_2 \cdots I_n \subseteq I_1 \cap I_2 \cap \cdots \cap I_n$$

$\square$

The sum of an arbitrary set of ideals in R (including an infinite set) is defined in a similar fashion, but requires care because we must restrict to finite sums.

Definition 4.6.6. Let $\mathcal{A}$ be a set of ideals in R. The **sum** of these ideals is

$$\sum_{I\in\mathcal{A}} I = \left\{\sum_{I\in\mathcal{B}} a_I : a_I \in I, \text{ and } \mathcal{B} \text{ is a finite subset of } \mathcal{A}\right\}$$

Exercises 4.6.7. Let $\varphi : R \longrightarrow S$ be a homomorphism.

(a) For I and ideal in R show that $\varphi^{-1}(\varphi(I)) = I + K$ where $K = \ker\varphi$. In particular, if I contains K, then $\varphi^{-1}\varphi(I) = I$.

Maximal, Prime and Radical Ideals

There are three key properties that ideals may have.

Definition 4.6.8. Let I be a proper ideal of R (that is $I \neq R$). An ideal I is **maximal** if the only ideal properly containing I is R. The ideal I is **prime** when $ab \in I$ implies that either $a \in I$ or $b \in I$. The ideal I is **radical** when $a^n \in I$ for $n \in \mathbb{N}$ implies $a \in I$.

In any integral domain, the zero ideal is prime. This follows directly from the definition of integral domain, $ab = 0$ implies $a = 0$ or $b = 0$.

Let I be a nonzero ideal in the integers, and let d be its positive generator. If d is not a prime number, say $d = ab$ with $a, b < d$, then I is not a prime ideal since $ab \in I$, but $a, b \notin I$. If d is a prime number then $ab \in I$ implies that $d|ab$, and by primality of d, either $d|a$—and therefore $a \in I$—or $d|b$—and then $b \in I$. Consequently, I is prime. We conclude that, for the integers, an ideal is prime if and only if it is generated either by 0 or a prime integer.

Exercises 4.6.9.

(a) Show that the nonzero prime ideals in $\mathbb{Z}$ are also maximal ideals. [Suppose p is a prime number. Try to enlarge $\langle p\rangle$ and show that you get all of $\mathbb{Z}$.]

(b) Let I be a nonzero ideal in $\mathbb{Z}$. We know I is principle; let a be the smallest positive integer in I. Show that I is radical if and only if the prime factorization of a is $a = p_1p_2\cdots p_r$ for *distinct* primes p_i.

(c) Extend these results to $F[x]$ for F a field.

Theorem 4.6.10. *All prime ideals are radical. All maximal ideals are prime.*

Proof. Let P be a prime ideal. We will show that if $a^n \in P$ then $a \in P$. This establishes that P is a radical ideal. Suppose $a^n \in P$. Let $m \leq n$ be the smallest power of a that lies in P. If $m > 1$, then we have $a * a^{m-1} = a^m \in P$. By primality, either a or a^{m-1} is in P. This contradicts our assumption on m. Thus $m = 1$ and $a \in P$.

Let M be a maximal ideal. We will show that $ab \in M$ implies either a or b is in M. This establishes that M is prime. Let $ab \in M$. Suppose that $a \notin M$. Since M is a maximal ideal $M + \langle a \rangle = R$. Consequently there is some $m \in M$ and $r \in R$ such that $m + ra = 1$. Multiplying both sides by b we get $mb + rab = b$. Since $ab \in M$, we have $b = mb + rab \in M$. Thus if $ab \in M$ and $a \notin M$ then $b \in M$, as was to be shown. □

The proof that a maximal ideal is prime echoes the proof that an irreducible integer (or polynomial in $F[x]$ for F a field) is prime, Theorem 1.1.9.

Now we show that these properties of ideals are intimately connected with properties of the quotient ring.

Theorem 4.6.11. *Let R be a ring and I and ideal in R.*

- *I is a maximal ideal if and only if R/I is a field.*
- *I is a prime ideal if and only if R/I is an integral domain.*
- *I is a radical ideal if and only if R/I is reduced.*

Proof. We will prove one direction for each claim and leave the other as an exercise.

Suppose I is maximal. Let $r + I$ be an arbitrary element of R/I with $r + I \neq 0 + I$. Since I is maximal, $I + \langle r \rangle = R$, so there is some $a \in I$ and $s \in R$ such that $a + sr = 1$. Then $sr + I = (1 - a) + I = 1 + I$, because $a \in I$. Consequently, $s + I$ is the inverse of $r + I$. Thus an arbitrary nonzero element of R/I has an inverse, and R/I is a field.

Suppose I is a prime ideal. Let $r+I$ and $s+I$ be such that $(r+I)(s+I) = 0+I$. Then $rs + I = 0 + I$ so $rs \in I$. Since I is prime, either $r \in I$ or $s \in I$. Thus, either $r + I = 0 + I$ or $s + I = 0 + I$. This shows R/I has no zero-divisors.

Suppose I is a radical ideal. Suppose that $r + I$ is nilpotent in R/I; that is $(r + I)^n = 0 + I$. Then $r^n + I = 0 + I$, so $r^n \in I$. Since I is radical, we must have $r \in I$, and consequently $r + I = 0 + I$. This shows that R/I has no nonzero nilpotent elements, so R/I is reduced.

□

Exercises 4.6.12. Let $\varphi : R \longrightarrow S$ be a homomorphism of rings and let J be an ideal in S. From Exercise 4.5.6 we know that $\varphi^{-1}(J)$ is an ideal in R.

(a) If J is a radical ideal, show that $\varphi^{-1}(J)$ is a radical ideal in R.

(b) If J is a prime ideal, show that $\varphi^{-1}(J)$ is a prime ideal in R.

(c) Using $R = \mathbb{Z}$ and $S = \mathbb{Q}$ show that $\varphi^{-1}(J)$ may not be maximal when J is maximal.

Exercises 4.6.13.

(a) Show that the intersection of two radical ideals is radical.

(b) Illustrate with an example from $F[x]$ for F a field.

(c) Given an example in $F[x]$ to show that the intersection of two prime ideals may not be prime.

Exercises 4.6.14.

(a) Let $N = \{a \in R : a^n = 0 \text{ for some } n \in \mathbb{N}\}$ be the set of all the nilpotent elements in a ring R. Show that N is an ideal of R. It is called the **nilradical** of R.

(b) Show that R/N is reduced (it has no nonzero nilpotent elements).

(c) Show that N is contained in the intersection of all prime ideals in R. (The reverse containment is also true, but much more difficult to prove.)

(d) Show that if $a \in N$ then $1 - a$ and $1 + a$ are units.

Comaximality and the Chinese Remainder Theorem

Recall that two integers a, b are *coprime* if they have no common factor other than 1. A consequence—the GCD Theorem 1.1.4—is that some linear combination of a and b is equal to 1. Interpreting this in the context of ideals, the ideal $\langle a, b\rangle$ generated by the two coprime integers is all of $\mathbb{Z}$. We can extend this notion of coprime integers (or polynomials) to ideals in a general ring R.

For any two integers m, n we have a homomorphism $\mathbb{Z}/mn \longrightarrow \mathbb{Z}/m$ and $\mathbb{Z}/mn \longrightarrow \mathbb{Z}/n$. This gives a homomorphism into the direct product by Proposition 4.3.4: $\mathbb{Z}/mn \longrightarrow \mathbb{Z}/m \times \mathbb{Z}/n$. The Chinese Remainder Theorem says this is an isomorphism when m, n are coprime.

Theorem 4.6.15 (Chinese Remainder Theorem)**.** *Let m, n be coprime integers. The natural maps from Theorem 4.2.12 give an isomorphism $\mathbb{Z}/mn \longrightarrow \mathbb{Z}/m \times \mathbb{Z}/n$.*

The proof is based on the GCD Theorem, which says that there are integers u and v such that $mu+nv = 1$. More generally we have the property of comaximality for ideals, and a Chinese Remainder Theorem for comaximal ideals whose proof essentially mimics the proof of the Chinese Remainder Theorem for integers.

Definition 4.6.16. Two ideals I and J in a ring R are **comaximal** if $I + J = R$.

Theorem 4.6.17. *Let I and J be proper ideals of R that are comaximal. Then $IJ = I \cap J$ and $R/IJ \cong R/I \times R/J$.*

Proof. Since I and J are comaximal there exist $a \in I$ and $b \in J$ such that $a+b = 1$. We now show that the homomorphism $R \longrightarrow R/I \times R/J$ is surjective. The image of a in R/J is $a + J = (1 - b) + J = 1 + J$ because $b \in J$. The image of a in R/I is $a + I = 0 + I$ because $a \in I$. Similarly, the image of b is $1 + I$ in R/I and it is $0 + J$ in R/J. Thus for an arbitrary element $(r_1 + I, r_2 + J)$ in $R/I \times R/J$, there is a preimage, $r_1 a + r_2 b$.

The kernel of $R \longrightarrow R/I \times R/J$ is $I \cap J$ so the proof is complete once we show $IJ = I \cap J$. We already know that $IJ \subseteq I \cap J$. Let $c \in I \cap J$. Then $ac + bc = c$, but ac and bc are both in IJ so we have expressed an arbitrary element of $I \cap J$ as a sum of two elements in IJ. Thus $IJ = I \cap J$. $\square$

4.7 Fractions

Dealing with fractions is one of the big challenges for primary school students. A key reason for the difficulties is that a fraction can be written in an infinite number of equivalent ways (for example $1/2 = 2/4 = 3/6 \ldots$) and it is necessary to use multiple expressions for a number in order to do arithmetic with fractions. Underlying our use of fractions is an equivalence relation on ordered pairs of integers; which is not something we dare to explain to students. In this section we show that the method used to construct the rational numbers from the integers extends with little modification to an arbitrary ring.

First let's consider some examples to show that there are other rings of interest in between the integers and the rational numbers, that is, rings properly containing $\mathbb{Z}$ but properly contained in $\mathbb{Q}$.

Example 4.7.1. One can verify that the following sets are in fact subrings of $\mathbb{Q}$.

- $R = \left\{a/2^i : a \in \mathbb{Z}, i \in \mathbb{N}_0\right\}$.
- $S = \{a/b : a \in \mathbb{Z}$ and b is an odd integer$\}$.
- $T = \left\{a/100^i : a \in \mathbb{Z}, i \in \mathbb{N}_0\right\}$.

Exercises 4.7.2. For the rings R, S, and T:

(a) Identify all the units in each of these rings.

(b) Show that in each of these rings every ideal is principal, generated by some nonnegative integer.

(c) In $\mathbb{Z}$, any two distinct positive integers generate different ideals. Show that is not true in R, S, T. For each of these rings, identify a set of integers that uniquely define all ideals.

(d) Which of these ideals are prime?

The rings in the previous example and exercise are all constructed via the process we now describe.

Definition 4.7.3. Let R be an integral domain. A subset D of $R \setminus \{0\}$ that contains 1 and is closed under multiplication is called a **multiplicatively closed set**.

Let D be a multiplicatively closed set in R. Define a relation on $R \times D$ by

$$(r_1, d_1) \sim (r_2, d_2) \quad \text{when} \quad r_1 d_2 = r_2 d_1$$

Proposition 4.7.4. *The relation above is an equivalence relation. Under this relation for any $r \in R$ and $c, d \in D$, $(r, d) \sim (rc, dc)$*

Proof. The relation is reflexive:$(r, d) \sim (r, d)$ since $rd = rd$.

The relation is symmetric: Suppose $(r_1, d_1) \sim (r_2, d_2)$ so $r_1 d_2 = r_2 d_1$. Then $r_2 d_1 = r_1 d_2$ so $(r_2, d_2) \sim (r_1, d_1)$.

The relation is transitive: Suppose $(r_1, d_1) \sim (r_2, d_2)$ and $(r_2, d_2) \sim (r_3, d_3)$. Then $r_1 d_2 = r_2 d_1$ and $r_2 d_3 = r_3 d_2$. Multiplying the first by d_3 and the second by d_1 we get

$$r_1 d_2 d_3 = r_2 d_1 d_3 = r_2 d_3 d_1 = r_3 d_2 d_1$$

Since R is an integral domain, we can cancel d_2 (see Exercise 4.1.6) to obtain $r_1 d_3 = r_3 d_1$. This shows $(r_1, d_1) \sim (r_3, d_3)$.

The final claim follows from the definition of the relation $rdc = drc$. It may be seen as simplification of fractions. □

A key step in the above proof involved the cancellation for integral domains. The construction of rings of fractions can be generalized to arbitrary rings provided D contains no zero-divisors. It can be generalized to allow D to contain zero-divisors with one small modification to the definition of the equivalence relation.

Theorem 4.7.5. *Let D be a multiplicatively closed set in R. Let $[r, d]$ denote the equivalence class of (r, d). The operations*

- $[r, c] + [sd] := [rd + sc, cd]$, *and*
- $[r, c] \star [s, d] := [rs, cd]$,

are well defined. The set $R \times D/\sim$ with these operations is a ring with additive identity $[0, 1]$ and multiplicative identity $[1, 1]$. We denote this ring $D^{-1}R$. The map $R \longrightarrow D^{-1}R$ taking r to $[r, 1]$ is an embedding.

Proof. Let (r, c) and (s, d) be in $S \times D$. Since D is multiplicatively closed, $cd \in D$ so both $(rd + sc, cd)$ and (rs, cd) are in $S \times D$ and their equivalence classes exist.

To show that the operations are well defined, suppose two different representatives for each equivalence class: $(r, c) \sim (r', c')$ and $(s, d) \sim (s', d')$. We want to show that the formula for the equivalence class of the product (and for the sum) is independent of the representatives chosen. We deal with the product first. We want to show that $(rs, cd) \sim (r's', c'd')$, which reduces to $rsc'd' = r's'cd$. We know

$$rc' = r'c \tag{4.3}$$
$$sd' = s'd \tag{4.4}$$

Multiplying the first equation by sd' and the second by rc' we get

$$rc'sd' = r'csd' = r'csd' = r'cs'd$$

Rearranging the factors on the first and last terms gives $rsc'd' = r's'cd$.

For the sum we want to show $(rd+sc, cd) \sim (r'd'+s'c', c'd')$. Multiplying (4.3) bu dd' we get $rc'dd' = r'cdd'$, and multiplying (4.4) by cc' gives $sd'cc' = s'dcc'$. Adding the two equations

$$\begin{aligned} rc'dd' + sd'cc' &= r'cdd' + s'dcc' \\ (rd+sc)c'd' &= (r'd'+s'c')cd \end{aligned}$$

This establishes $(rd+sc, cd) \sim (r'd'+s'c', c'd')$.

Verifying the claims about the additive and multiplicative identity are routine computations. Verification of commutativity and associativity are more involved by fairly straightforward and are left to the reader. We next show that multiplication distributes over addition.

$$\begin{aligned} [r,c]\Big([s,d]+[t,f]\Big) &= [r,c]\Big[sf+td, df]\Big) \\ &= [rsf+rtd, cdf] \\ [r,c]*[s,d]+[r,c]*[t,f]\Big) &= [rs,cd]+[rt,cf] \\ &= [rscf+rtcd, cfcd] \qquad = [rsf+rtd, cdf] \end{aligned}$$

The function $\iota : R \longrightarrow D^{-1}R$ taking r to $[r,1]$ takes the identity to the identity element of R to the identity element of $D^{-1}R$. It respects sums since $[r,1]+[s,1] = [r*1+s*1, 1*1] = [r+s, 1]$ which is the image of $r+s$. The map ι respects products since $[r,1]*[s,1] = [rs, 1*1]$ which is the image of rs. Thus ι is a homomorphism. Suppose $\iota(r) = \iota(s)$. Then $[r,1] = [s,1]$. By the definition of the equivalence relation, $r*1 = s*1$. This shows ι is injective. □

The ring $D^{-1}R$ is often called a **localization** of R.

Exercises 4.7.6.

(a) Let $D = \{30^i : i \in \mathbb{N}_0\}$. Verify that D is multiplicatively closed in $\mathbb{Z}$. Identify all of the prime ideals in $D^{-1}\mathbb{Z}$.

(b) Let $D = \{(x^3 - x)^i : i \in \mathbb{N}_0\}$. Verify that D is multiplicatively closed in $\mathbb{Q}[x]$. Identify all of the prime ideals in $D^{-1}\mathbb{Q}[x]$.

(c) Under what conditions on D does $D^{-1}\mathbb{Z}$ have just one maximal ideal?

(d) Let D be multiplicatively close I be an

Exercises 4.7.7. In this exercise we characterize all localizations of $\mathbb{Z}$.

(a) Let $D = \{d_1, d_2, \ldots, d_t\} \subseteq \mathbb{Z} \setminus \{0\}$. What is the smallest multiplicatively closed subset of $\mathbb{Z}$ containing D and 1? What if D is an infinite subset of $\mathbb{Z} \setminus \{0\}$? We will abuse notation and write $D^{-1}\mathbb{Z}$ for the localization due to the smallest multiplicatively closed subset of $\mathbb{Z} \setminus \{0\}$ containing D.

(b) Suppose $D \subseteq N \subseteq \mathbb{Z} \setminus \{0\}$. Show that there is an injective ring homomorphism $D^{-1}\mathbb{Z} \to N^{-1}\mathbb{Z}$.

(c) Show that any localization of $\mathbb{Z}$ is of the form $P^{-1}\mathbb{Z}$ where P is a subset of the set of primes in $\mathbb{N}$. [You need to identify the set P for a given D and show that $P^{-1}\mathbb{Z} \cong D^{-1}\mathbb{Z}$].

(d) Let P be a subset of the prime integers. Identify all the ideals in $P^{-1}\mathbb{Z}$. Which ideals are prime?

Exercises 4.7.8. Let R be an integral domain and let D be a multiplicative subset of R. We will consider R as a subset of $D^{-1}R$ via the embedding $\varphi : R \longrightarrow D^{-1}R$ which takes r to $r/1$.

(a) Let $D^{-1}I = \{a/s : a \in I, s \in D\}$. Show $D^{-1}I$ is an ideal in $D^{-1}R$.

(b) Show that $D^{-1}I = D^{-1}R$ if and only if $I \cap D \neq \emptyset$.

(c) Let J be an ideal of $D^{-1}R$. Show that $J \cap R$ is an ideal in R.

Parts a - c show we have a function from the set of ideals in $D^{-1}R$ to the set of ideals in R given by $J \mapsto J \cap R$ and a function from the set of ideals in R to the set of ideals in $D^{-1}R$ given by $I \mapsto D^{-1}I$.

(d) Show that $I \mapsto D^{-1}I$ is surjective: That is, show that every ideal in $D^{-1}R$ is $D^{-1}I$ for some ideal I in R. (Hints: If J is an ideal in $D^{-1}R$ then an element of J may be written a/s for $a \in R$ and $s \in D$. Show that $D^{-1}(J \cap R) = J$.)

(e) Show that these two maps of ideals respect intersections. For example, $D^{-1}(I \cap I') = D^{-1}(I) \cap D^{-1}(I')$.

(f) The map $I \mapsto D^{-1}I$ is not injective. Show that it is injective on prime ideals that don't meet D. Conclude that the functions $J \mapsto J \cap R$ and $I \mapsto D^{-1}I$ give a 1-1 correspondence between prime ideals of $D^{-1}R$ and prime ideals of R not meeting D.

Exercises 4.7.9. Let R be an integral domain. A multiplicatively closed set $D \subseteq R$ is *saturated* when

$$xy \in D \Longleftrightarrow x \in D \text{ and } y \in D.$$

There is a theorem saying D is saturated if and only if $R \setminus D$ is a union of prime ideals. Prove one direction of this result as follows.

(a) Let $\mathcal{P}$ be a set of prime ideals and let $D = R \setminus \Big(\cup_{P \in \mathcal{P}} P \Big)$. Show that D is multiplicatively closed and saturated.