9 *Special Domains*

Beyond division with remainder, there are a couple features that distinguish the archetypal rings $\mathbb{Z}$ and $\mathbb{K}[x]$ from other domains. We present a hierarchy of commutative rings that includes commutative domains, unique factorization domains, principal ideal domains, Euclidean domains, and fields.

9.0 Principal Ideal Domains

What are the simplest ideals? We consider a kind of ring having only uncomplicated ideals.

Definition 9.0.0. A *principal ideal domain* is a commutative domain in which every ideal is generated by a single element. A *principal* ideal is any ideal generated by a single ring element.

Division with remainder leads to principal ideals.

Theorem 9.0.1. *Every Euclidean domain is a principal ideal domain.*

Proof. Let I be an ideal in a Euclidean domain R with Euclidean function $\nu\colon R \setminus \{0\} \to \mathbb{N}$. When $I = \langle 0 \rangle$, the ideal I is principal, so we may assume $I \neq \langle 0 \rangle$. By the Well-Ordering 0.2.6 of the nonnegative integers, the set $\{\nu(f) \in \mathbb{N} \mid f \in I \setminus \{0\}\}$ has a minimum, say m. Choose an element g in the ideal I with $\nu(g) = m$. As $g \in I$, we have $\langle g \rangle \subseteq I$. For any element f in I, there exists elements q and r in the Euclidean domain R such that $f = q\,g + r$ and either $r = 0$ or $\nu(r) < \nu(g)$. Since $r = f - q\,g \in I$, our choice of g implies that $r = 0$. We deduce that $f = q\,g$ and $I \subseteq \langle g \rangle$. Thus, we conclude that $I = \langle g \rangle$. □

Remark 9.0.2. Theorem 1.1.2, Theorem 4.0.4, and Problem 8.1.5 show that the ring $\mathbb{Z}$ of integers, the ring $\mathbb{K}[x]$ of univariate polynomials over the field $\mathbb{K}$, and the ring $\mathbb{Z}[\mathrm{i}]$ of the Gaussian integers are Euclidean domains, so these rings are principal ideal domains.

Many commutative domains are not principal ideal domains.

Problem 9.0.3. Show that the ideal $\langle 2, x \rangle$ in $\mathbb{Z}[x]$ is not principal.

Solution. Suppose that there exists an element g in $\mathbb{Z}[x]$ such that $\langle g \rangle = \langle 2, x \rangle$. It would follow that $f\,g = 2$ for some polynomial f in $\mathbb{Z}[x]$. Since $\deg(g) + \deg(f) = \deg(2) = 0$, we would deduce that g is an integer. We would thereby obtain $g = \{\pm 1, \pm 2\}$ because 2 is a prime integer. Because $\langle 2, x \rangle$ is a maximal ideal in $\mathbb{Z}[x]$, the element g cannot be a unit, so $g = \pm 2$. However, we would also have $x \in \langle g \rangle$, so $x = 2\,h$ for some polynomial h in $\mathbb{Z}[x]$ which yields contradiction by mapping to $(\mathbb{Z}/\langle 2 \rangle)[x]$. □

Problem 9.0.4. Demonstrate that the ideal $\langle 2, 1-\sqrt{-3}\rangle$ in $\mathbb{Z}[\sqrt{-3}]$ (which is a subring of the field $\mathbb{C}$) is not principal.

Solution. Suppose that there exists integers a and b such that $\langle a + b\sqrt{-3}\rangle = \langle 2, 1-\sqrt{-3}\rangle$. It follows that $f\,(a + b\sqrt{-3}) = 2$ for some element f in $\mathbb{Z}[\sqrt{-3}]$. Taking absolute values in $\mathbb{C}$ gives $|f|\,(a^2+3b^2) = 2$, so $a^2 + 3b^2 \in \{\pm 1, \pm 2\}$. Because a and b integers, we must have $a = \pm 1$ and $b = 0$ which contradicts the fact that $\langle 2, 1-\sqrt{-3}\rangle$ is a maximal ideal. □

In a principal ideal domain, the sum of two principal ideals is generated by a greatest common divisor.

Theorem 9.0.5. *Let R be a principal ideal domain. For any nonzero elements f and g in R, there exists elements r and s in R such that* $\gcd(f,g) = r\,f + s\,g$. *In particular, we have* $\langle \gcd(f,g)\rangle = \langle f, g\rangle$.

A domain in which a greatest common divisor of every pair of nonzero elements is a linear combination of the two elements is a *Bézout domain*.

Proof. Set $I := \langle f, g\rangle$. Since R is a principal ideal domain, there is a element d in R such that $I = \langle d\rangle$. It follows that $d = r\,f + s\,g$ for some elements r and s in R. Both f and g are in I and I is generated by d, so d divides f and g. On the other hand, if an element c in R divides f and g, then c divides $r\,f + s\,g = d$. Hence, we see that $d = \gcd(f,g)$.

Any generator for the ideal $\langle f, g\rangle$ is a greatest common divisor of f and g. Lemma 8.1.9 shows that, for any two greatest common divisors d and e, there exists a unit u in R such that $e = u\,d$ and $d = u^{-1}\,e$. Thus, we have $\langle e\rangle \subseteq \langle d\rangle$ and $\langle d\rangle \subseteq \langle e\rangle$, so $\langle d\rangle = \langle e\rangle$. □

We extend the concept of irreducibility to elements in any commutative ring; compare with Definition 1.2.4.

Definition 9.0.6. A ring element f is *irreducible* if f is nonzero, f is not a unit, and the equation $f = g\,h$ implies that g or h is a unit.

Example 9.0.7. The finite ring $\mathbb{Z}/\langle 6\rangle$ has no irreducible elements because $(\mathbb{Z}/\langle 6\rangle)^{\times} = \{1,5\}$, $2 = (2)(4)$, $3 = (3)(3)$, and $4 = (2)(2)$. Without irreducibles, an element may have many factorizations: $4 = (2)(2) = (2)(2)(2)(2) = (2)(2)(2)(2)(2)(2) = \cdots$.

Lemma 9.0.8. *Let R be a commutative domain. For any prime ideal $\langle g\rangle$ in R, the ring element g is irreducible.*

Proof. Suppose that $g = f\,h$. Since the principal ideal $\langle g\rangle$ is prime, Theorem 8.0.4 shows that the element g divides f or h. We may assume that g divides f and there exists an element q in R such that $g\,f = q\,g$. It follows that $g = f\,h = q\,g\,h$. Since R is a domain, we deduce that $1 = q\,h$, so h is a unit and g is irreducible. □

Example 9.0.9. Consider the subring $\mathbb{C}[x^2, x^3] \subset \mathbb{C}[x]$. Comparing degrees, we see that the elements x^2 and x^3 are irreducible. They are not prime because x^2 divides $(x^3)^2 = x^6$ but x^2 does not divide x^3 and x^3 divides $x^4\,x^2 = x^6$ but x^3 does not divide either x^4 or x^2.

Problem 9.0.10. Demonstrate that $2 \in \mathbb{Z}[\sqrt{-3}]$ is irreducible but the ideal $\langle 2 \rangle$ is not prime.

Solution. Suppose $2 = (a + b\sqrt{-3})(c + d\sqrt{-3}))$ for some integers a, b, c, and d. Taking conjugates gives $2 = (a - b\sqrt{-3})(c - d\sqrt{-3})$. Multiplying these equations gives $4 = (a^2 + 3b^2)(c^2 + 3d^2)$. Since the equation $x^2 + 3y^2 = 2$ has no integral solutions, it follows that $a^2 + 3b^2 = 1$, so $a = \pm 1$ and $b = 0$. Since $2(p + q\sqrt{-3}) = 1$ has no integral solutions, the ring element 2 is not a unit. We see that 2 is irreducible. To see that 2 is not prime, observe that 2 divides $4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$, but 2 does not divide either factor. □

Proposition 9.0.11. *Let R be a principal ideal domain. For any element f in R, the following are equivalent:*
(a) *The element f in R is irreducible.*
(b) *The principal ideal $\langle f \rangle$ is nonzero and maximal.*
(c) *The principal ideal $\langle f \rangle$ is nonzero and prime.*

Proof.
(a)$\Rightarrow$(b): Suppose that we have the inclusion $\langle f \rangle \subseteq \langle g \rangle$ for some element g in R. Equivalently, there exists an element q in R such that $f = q\,g$. Since f is irreducible, either g or q is a unit, so $\langle f \rangle = \langle g \rangle$ or $\langle g \rangle = \langle 1 \rangle = R$. Because every ideal is prinicipal, we deduce that $\langle f \rangle$ is maximal.
(b)$\Rightarrow$(c): Every nonzero maximal ideal is a nonzero prime ideal.
(c)$\Rightarrow$(a): Follows from Lemma 9.0.8. □

Exercises

Problem 9.0.12. Consider the subring
$$\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$$
of field $\mathbb{C}$ of complex numbers

- **(i)** Show that the norm function $\mathrm{N}\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ defined by $\mathrm{N}(a + b\sqrt{-5}) = a^2 + 5\,b^2$ is compatible with multiplication, meaning that the norm of a product is equal to the product of the norms of the factors.
- **(ii)** Confirm that $2 + \sqrt{-5}$ is an irreducible element in $\mathbb{Z}[\sqrt{-5}]$.
- **(iii)** Verify that the ideal $\langle 2 + \sqrt{-5} \rangle$ is not prime in $\mathbb{Z}[\sqrt{-5}]$.

9.1 Unique Factorization Domains

When can we factor ring elements? We propose a class of rings in which every element has a unique factorization.

Definition 9.1.0. A commutative domain R is a *unique factorization domain* if, for nonzero element f in R, there exists a unit u in R, finitely many distinct irreducible elements $g_1, g_2, \dots, g_m$ in R, and positive integers $e_1, e_2, \dots, e_m$ such that
$$f = u\,g_1^{e_1}\,g_2^{e_2} \cdots g_m^{e_m} = u \prod_{j=1}^{m} g_j^{e_j}\,,$$

and this factorization is unique up to reordering the factors.

Remark 9.1.1. The Fundamental Theorem of Arithmetic 1.2.10 shows that the ring $\mathbb{Z}$ of integers is a unique factorization domain.

Being a unique factorization domains requires the converse of Lemma 9.0.8 to hold.

Proposition 9.1.2. *Let R be a commutative domain in which every nonzero nonunit is a product of irreducibles. The ring R is a unique factorization domain if and only if, for any irreducible element f in R, the principal ideal $\langle f \rangle$ is prime.*

Proof. We prove each implication separately.

⇒: Suppose that the ring R is a unique factorization domain. For any elements g and h in R such that the product $g\,h$ belongs to the principal ideal $\langle f \rangle$, there exists an element q in R such that $g\,h = q\,f$. Factor g, h, and q into irreducibles. Uniqueness of the factorizations implies that the irreducible $u\,f$, for some unit u in R, appears on the left side. This element arose as a factor of either g or h, so we see that $g \in \langle f \rangle$ or $h \in \langle f \rangle$. Theorem 8.0.4 shows the principal ideal $\langle f \rangle$ is prime.

⇐: Suppose that any principal ideal generated by an irreducible element is prime. Consider two factorizations

$$g_1\,g_2\,\cdots\,g_m = h_1\,h_2\,\cdots\,h_n$$

where the elements g_j in R and h_k in R are irreducible for all $1 \leqslant j \leqslant m$ and $1 \leqslant k \leqslant n$. We proceed, by induction on $\max(m,n)$, to show that $m = n$ and $g_j = c_j\,h_{\sigma(j)}$ for some units c_j in R and some permutation σ of the set $[m] := \{1, 2, \dots, m\}$. The base case $\max(m,n) = 1$ has $g_1 = h_1$ and the claim is trivial. For the inductive step, the given equation shows that g_m divides $h_1\,h_2\,\cdots\,h_n$. By hypothesis, the principal ideal $\langle g_m \rangle$ is prime, so there exists an index k such that $1 \leqslant k \leqslant n$ and g_m divides h_k. Since h_k is irreducible, there exists a unit c_k such that $g_m = c_k\,h_k$. Canceling the element g_1 from both sides yields $g_1\,g_2\,\cdots g_{m-1} = c_k\,h_1\,h_2\,\cdots\,h_{k-1}\,h_{k+1}\cdots\,h_n$. The induction hypothesis establishes that $m - 1 = n - 1$ and $g_j = c_j\,h_{\sigma'(j)}$ for some units c_j in R, for all $2 \leqslant j \leqslant m - 1$, and some bijection σ' from $\{1, 2, \dots, m{-}1\}$ to $\{1, 2, \dots, k{-}1, k{+}1, m\}$. Setting $\sigma(j) = \sigma'(j)$ if $j \neq m$ and $\sigma(m) = k$ yields the required permutation. □

To demonstrate that every principal ideal domain is a unique factorization domain, we must show that every nonzero nonunit is a product of irreducibles.

Lemma 9.1.3. *Let R be a commutative domain. For any nonzero nonunit f in R that does not admit a factorization into irreducibles, there is a proper inclusion $\langle f \rangle \subset \langle g \rangle$ of principal ideals in R where the element g is another nonzero nonunit that does not admit a factorization into irreducibles.*

Proof. By hypothesis, the element f is not irreducible. Hence, there are nonzero nonunits g and h such that $f = gh$. If both g and h admitted factorizations into irreducibles, then f also would. We may assume that the element g does not admit a factorization into irreducibles. Since h is not a unit, the inclusion $\langle f \rangle \subset \langle g \rangle$ of principal ideals is proper. □

Theorem 9.1.4. *Every nonzero nonunit in any principal ideal domain is a product of irreducibles.*

The assertion is vacuous in a field.

Proof. Let R be a principal ideal domain. Suppose that there exists a nonzero nonunit f_0 in R that does not admit a factorization into irreducibles. Lemma 9.1.3 gives a strict inclusion $\langle f_0 \rangle \subset \langle f_1 \rangle$ where f_1 is a nonzero nonunit that does not admit a factorization into irreducibles. Iterating this step produces an infinite increasing chain $\langle f_0 \rangle \subset \langle f_1 \rangle \subset \langle f_2 \rangle \subset \cdots$ of principal ideals in R. We claim that this is impossible.

Suppose that the principal ideal domain R contains an infinite increasing chain $I_0 \subset I_1 \subset I_2 \subset \cdots$ of ideal. Set $I := \bigcup_{j \in \mathbb{N}} I_j$. The union I is an ideal: every finite set of elements in I lies in a common I_j, so I is closed under addition and multiplication by elements from R because I_j has these properties. Since R is a principal ideal domain, there exists an element g in R such that $I = \langle g \rangle$. The set I is a union, so the element g belongs to I_k for some index k. It follows that $I = \langle g \rangle \subset I_k \subseteq I$ and $I_k = I$. However, this is impossible because the inclusion $I_{k+1} \subset I = I_k$ is proper. We conclude that every nonzero nonunit in R admits a factorization into irreducibles. □

Emmy Noether pioneered the *ascending chain condition*, which asserts that no infinite increasing chain of ideal exists. Rings that satisfy this condition are known as *noetherian rings*. The second paragraph in the proof of Theorem 9.1.4 shows that every principal ideal domain is noetherian.

Corollary 9.1.5. *Any principal ideal domain is a unique factorization domain.*

Proof. Combine Proposition 9.1.2, Proposition 9.0.11 and Theorem 9.1.4. □

Exercises

Problem 9.1.6. Let R be a principal ideal domain. For any two distinct nonzero elements f and g with no common irreducible factor, prove that $\langle f \rangle + \langle g \rangle = \langle 1 \rangle$.

Problem 9.1.7. Let R be a unique factorization domain such that the sum of two principal ideals in R is again a principal ideal. Prove that R is a principal ideal domain.

9.2 Non-Euclidean Principal Ideal Domains

How close is a principal ideal domain to being Euclidean? These two classes of commutative domains are distinct but the difference is surprisingly small. We start by demonstrating that a principal ideal domain is "just" a Euclidean domain with more general notion of a Euclidean function.

Definition 9.2.0. Let R be a commutative domain. A *Dedekind–Hasse function* is a function $\delta \colon R \setminus \{0\} \to \mathbb{N}$ such that, for all nonzero element f and g in R, either g divides f or there exists elements s and t in R such that $\delta(s\,f + t\,g) < \delta(g)$.

Remark 9.2.1. Any Euclidean function $\nu \colon R \setminus \{0\} \to \mathbb{N}$ is a Dedekind–Hasse function with $(s,t) = (1, -q)$ and $f - q\,g = r$.

Proposition 9.2.2. *A commutative domain is a principal ideal domain if and only if it possesses a Dedekind–Hasse function.*

Proof. Let R be a commutative domain. We establish the two implications separately.

$\Rightarrow$: Suppose that R has a Dedekind–Hasse function $\delta \colon R \setminus \{0\} \to \mathbb{N}$ and let I be a nonzero ideal. By the Well-Ordering 0.2.6 of the nonnegative integers, the set $\{\delta(f) \in \mathbb{N} \mid f \in I \setminus \{0\}\}$ has a minimum, say m. Choose an element g in the ideal I with $\delta(g) = m$. As $g \in I$, we have $\langle g \rangle \subseteq I$. Consider an element f in I such that g does not divide f. There exists elements s and t in R such that $\delta(s\,f + t\,g) < \delta(g)$. Since $s\,f + t\,g$ is in I, this contradicts our choice of g. We deduce that g does divide f and $I \subseteq \langle g \rangle$. Thus, we obtain $I = \langle g \rangle$.

$\Leftarrow$: Suppose that R is a principal ideal domain. Corollary 9.1.5 shows that R is a unique factorization domain. Define the function $\delta \colon R \setminus \{0\} \to \mathbb{N}$ by $\delta(f) = 2^e$ where e is the number of irreducible factors appearing in the factorization of f. Consider an element f in R and a nonzero element g in R. Suppose that g does not divide f. There exists a nonzero element r in R such that $\langle f, g \rangle = \langle d \rangle$. In particular, there exists elements s and t in R such that $s\,f + t\,g = d$. It follows that d divides g. However, g does not divide d, because this would imply that g divides f. We deduce that there are strictly fewer irreducible elements in the factorization of d than in the factorization of g, so $\delta(r) < \delta(g)$. We conclude that δ is the required Dedekind–Hasse function. □

Nevertheless, there is a difference between a principal ideal domain and a Euclidean domain. To exhibit this difference, we document a characteristic of a Euclidean domain.

Lemma 9.2.3. *For any Euclidean domain R that is not a field, there exists an element g in R such that the quotient ring $R/\langle g \rangle$ has a system of distinct representative consisting of the 0 and units in R.*

Proof. Let $\nu \colon R \setminus \{0\} \to \mathbb{N}$ be a Euclidean function on R. There exists a nonzero nonunits in R because R is not a field. By the

Well-Ordering 0.2.6 of the nonnegative integers, the set

$$\{\nu(f) \in \mathbb{N} \mid f \text{ is a nonzero nonunit in } R\}$$

has a minimum, say m. Choose a nonzero nonunit g in the ring R with $\nu(g) = m$. For any element f in R, division with remainder implies that there exists elements q and r in R such that $f = q\,g + r$ and either $r = 0$ or $\nu(r) < \nu(g)$. When $r \neq 0$, the inequality $\nu(r) < \nu(g)$ forces r to be a unit. Since $f + \langle g \rangle = r + \langle g \rangle$, we conclude that the quotient ring $R \,/\, \langle g \rangle$ has a system of distinct representatives consisting of the 0 and units in R. □

Proposition 9.2.4. *The quotient ring* $\mathbb{R}[x,y] \,/\, \langle x^2 + y^2 + 1 \rangle$ *is a principal ideal domain but not a Euclidean domain.*

Sketch of Proof. We address the two assertions separately.

- We prove that the ring $\mathbb{R}[x,y] / \langle x^2 + y^2 + 1 \rangle$ is not a Euclidean domain. Regarding the ring $\mathbb{R}[x,y]$ as $(\mathbb{R}[x])[y]$, division with remainder establishes that any polynomial in $\mathbb{R}[x,y]$ has a unique expression of the form $q\,(y^2 + x^2 + 1) + (a + b\,y)$ where q is in $\mathbb{R}[x,y]$ and a and b are in $\mathbb{R}[x]$. Hence, the quotient ring $\mathbb{R}[x,y] / \langle x^2 + y^2 + 1 \rangle$ has a system of distinct representatives $a + b\,y$ for some a and b in $\mathbb{R}[x]$. Since $y^2 = -1 - x^2$ in the quotient ring $\mathbb{R}[x,y] / \langle x^2 + y^2 + 1 \rangle$, we can think of this ring as
$$(\mathbb{R}[x])\big[\sqrt{-1 - x^2}\big] := \big\{a + b\sqrt{-1 - x^2} \mid a, b \in \mathbb{R}[x]\big\}.$$
We claim that the units in the ring R are precisely the units in the field $\mathbb{R}$. Consider the norm function $\mathrm{N}\colon R \to \mathbb{R}[x]$ defined, for any a and b in $\mathbb{R}[x]$, by
$$\mathrm{N}(a + b\,y) = (a + b\,y)(a - b\,y) = a^2 - b^2\,y^2 = a^2 + (x^2 + 1)\,b^2 .$$
For any a, b, c, and d in $\mathbb{R}[x]$, we have
$$\begin{aligned} \mathrm{N}\big((a + b\,y)(c + d\,y)\big) &= \mathrm{N}\big((a\,c - (x^2 + 1)\,b\,d) + (a\,d + b\,c)\,y\big) \\ &= \big((a\,c - (x^2 + 1)\,b\,d) + (a\,d + b\,c)\,y\big)\big((a\,c - (x^2 + 1)\,b\,d) - (a\,d + b\,c)\,y\big) \\ &= \big((a + b\,y)(c + d\,y)\big)\big((a - b\,y)(c - d\,y)\big) \\ &= \big((a + b\,y)(a - b\,y)\big)\big((c + d\,y)(c - d\,y)\big) \\ &= \mathrm{N}(a + b\,y)\ \mathrm{N}(c + b\,y) . \end{aligned}$$
Since N is a multiplicative function, a unit in R must have a norm that is a unit in $\mathbb{R}[x]$ or equivalently a unit in $\mathbb{R}$. The only way for $a^2 + (x^2 + 1)\,b^2$ to belong to $\mathbb{R}$ is to have $b = 0$ and $a \in \mathbb{R}$.
Suppose that R is a Euclidean domain. By Lemma 9.2.3, there would be a nonzero nonunit g in R such that the quotient ring $R / \langle g \rangle$ has a system of distinct representative consisting of the 0 and units in R. Hence, the composition of the canonical ring homomorphisms $\mathbb{R} \to \mathbb{R}[x] \to R \to R \,/\, \langle g \rangle$ is surjective. Since every ring homomorphism from a field is injective, this composition is a ring isomorphism. Choosing real numbers r and s such that $x + \langle g \rangle = r + \langle g \rangle$ and $y + \langle g \rangle = s + \langle g \rangle$, it follows that $r^2 + s^2 + 1 = 0$ in $\mathbb{R}$ which is a contradiction.
- To prove that R is a principal ideal domain, one exhibits a Dedekind–Hasse function. □