Chapter 10
Special Types of Domains

In this chapter, we begin with a specific and rather familiar sort of integral domain, and then generalize slightly in each section. First, we define a polynomial ring over a field, and show that we have a division algorithm in such a ring. As a result, this polynomial ring is a special type of ring called a Euclidean domain.

Subsequently, we demonstrate that Euclidean domains are principal ideal domains; that is, every ideal is principal. Finally, we prove that principal ideal domains are examples of unique factorization domains, in which we have something similar to the Fundamental Theorem of Arithmetic.

10.1 Polynomial Rings

We are certainly familiar with polynomials having real coefficients. There is no reason why we cannot consider coefficients in other rings.

Definition 10.1. Let R be a ring. Then a **polynomial** with coefficients in R is a formal expression

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

where $a_i \in R$ and n is a nonnegative integer. Suppose that $b_0 + b_1x + \cdots + b_mx^m$ is also a polynomial with coefficients in R. Without loss of generality, let us say that $n \leq m$. Then these polynomials are equal if and only if $a_i = b_i$ for all $i \leq n$ and $b_i = 0$ for all $i > n$. The set of all polynomials with coefficients in R is denoted $R[x]$.

Example 10.1. Let $R = \mathbb{Z}_5$. Then (inserting congruence class brackets for clarity), an example of a polynomial in $R[x]$ would be $f(x) = [3] + [2]x + [4]x^2$. As part of the above definition, we observe that $f(x) = g(x)$, where $g(x) = [3] + [2]x + [4]x^2 + [0]x^3$.

G. T. Lee, *Abstract Algebra*, Springer Undergraduate Mathematics Series,
https://doi.org/10.1007/978-3-319-77649-1_10

Note that the x in a polynomial is not an element of R. It is simply a placeholder in the expression of the polynomial. We could, equally well, define the polynomials in terms of sequences of elements of R (with only finitely many terms different from zero). But nobody thinks of polynomials in that way.

Definition 10.2. Let R be a ring and let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. Further suppose that $a_m \neq 0$ but $a_k = 0$ for all $k > m$. Then the **degree** of $f(x)$ is m, and we write $\deg(f(x)) = m$. The **leading term** of $f(x)$ is a_mx^m, and the **leading coefficient** is a_m. Note that the **zero polynomial**, 0, has no degree, leading term or leading coefficient. A **constant polynomial** has degree 0 (or is the zero polynomial). If R has an identity, then $f(x)$ is **monic** if its leading coefficient is 1.

Example 10.2. In $\mathbb{Q}[x]$, let $f(x) = 3 + 7x - 15x^2 + 0x^3 + 2x^4 + 0x^5$. Then $\deg(f(x)) = 4$, the leading term is $2x^4$ and the leading coefficient is 2. This polynomial is not monic.

We wish to make $R[x]$ into a ring, and so we need addition and multiplication operations. These will be exactly the same as for real polynomials. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$. Adding in terms with zero coefficients if necessary, we may assume that $m = n$. Then

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n.$$

Similarly,

$$f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{m+n}x^{m+n},$$

where

$$c_i = a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \cdots + a_ib_0.$$

Here, we take $a_j = 0$ if $j > n$ and $b_j = 0$ if $j > m$.

Example 10.3. In $\mathbb{Z}_7[x]$, let $f(x) = 5+2x+6x^2$ and $g(x) = 3+x+4x^2+5x^3$. Then $f(x)+g(x) = 1+3x+3x^2+5x^3$ and $f(x)g(x) = 1+4x+5x^2+4x^3+6x^4+2x^5$.

Theorem 10.1. *If R is a ring, then so is $R[x]$.*

Proof. Let us show that $R[x]$ is an abelian group under addition. Clearly the sum of two polynomials is a polynomial. Let $f(x) = a_0+\cdots+a_nx^n$, $g(x) = b_0+\cdots+b_mx^m$ and $h(x) = c_0 + \cdots + c_kx^k$. Then the coefficient of x^i in $f(x) + g(x)$ is $a_i + b_i$, and similarly for $g(x) + f(x)$ (adding in terms with zero coefficients if necessary). Thus, addition is commutative. In the same way, because the addition of coefficients is associative, addition in $R[x]$ is associative. The zero polynomial is the additive identity, and $-f(x) = -a_0 - \cdots - a_nx^n$. Therefore, $R[x]$ is an abelian group under addition.

Evidently, the product of two polynomials is a polynomial. Let us check a distributive law. The coefficient of x^i in $f(x)(g(x) + h(x))$ is

$$a_0(b_i + c_i) + a_1(b_{i-1} + c_{i-1}) + \cdots + a_i(b_0 + c_0).$$

But this is $(a_0 b_i + \cdots + a_i b_0) + (a_0 c_i + \cdots + a_i c_0)$, which is the coefficient of x^i in $f(x)g(x)+f(x)h(x)$. The other distributive law is proved similarly. Finally, we must check that multiplication is associative. But by repeated application of the distributive laws, we see that we may reduce to proving that $(a_u x^u b_v x^v)c_w x^w = a_u x^u(b_v x^v c_w x^w)$, for all $a_u, b_v, c_w \in R$ and all $u, v, w \geq 0$. However, both sides of this equation are equal to $a_u b_v c_w x^{u+v+w}$, and the proof is complete. □

Corollary 10.1. *Let R be a ring. Then*

1. *if R has an identity, then so does* $R[x]$*; and*
2. *if R is commutative, then so is* $R[x]$.

Proof. (1) The constant polynomial 1 is the identity.

(2) Repeatedly applying the distributive laws, we see that we need only check that $a_i x^i$ and $b_j x^j$ commute, where $a_i, b_j \in R$ and $i, j \geq 0$. But $a_i x^i b_j x^j = a_i b_j x^{i+j}$ and $b_j x^j a_i x^i = b_j a_i x^{i+j}$. Since R is commutative, these are equal. □

When our ring is an integral domain, degrees of polynomials behave in a way we would expect.

Theorem 10.2. *Let R be an integral domain, and let* $f(x)$ *and* $g(x)$ *be nonzero polynomials in* $R[x]$, *of degree m and n respectively. Then*

1. $\deg(f(x) + g(x))$ *is at most the larger of m and n (or* $f(x) + g(x) = 0$*); and*
2. $\deg(f(x)g(x)) = m + n$.

Proof. (1) This is clear from the definition of polynomial addition.

(2) Let $f(x) = a_0 + \cdots + a_m x^m$ and $g(x) = b_0 + \cdots + b_n x^n$. Then we see from the definition of polynomial multiplication that the only term of highest degree in $f(x)g(x)$ is $a_m b_n x^{m+n}$. Furthermore, $a_m \neq 0 \neq b_n$ and, since R is an integral domain, $a_m b_n \neq 0$. Thus, $\deg(f(x)g(x)) = m + n$. □

Note that the second part of the theorem fails if R is not an integral domain. For instance, in $\mathbb{Z}_6[x]$, we have $(2 + 3x)(1 + 2x) = 2 + x$, which does not have degree 2.

Corollary 10.2. *If R is an integral domain, then so is* $R[x]$.

Proof. By Corollary 10.1, $R[x]$ is a commutative ring with identity. Furthermore, $1 \neq 0$. By the preceding theorem, the product of nonzero polynomials cannot be the zero polynomial. □

Why are we so interested in polynomial rings? We now know that if F is a field, then $F[x]$ is an integral domain. But it has another attractive property. Indeed, we have an analogue of the division algorithm with which we are familiar for the integers. Readers who have seen polynomial long division for real polynomials will find the procedure very similar.

Theorem 10.3. (Division Algorithm for Polynomials). *Let F be a field, and let $f(x), g(x) \in F[x]$, with $g(x) \neq 0$. Then there exist unique $q(x), r(x) \in F[x]$ such that*

$$f(x) = g(x)q(x) + r(x),$$

with either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.

Proof. Let us verify the existence of $q(x)$ and $r(x)$. If $f(x) = 0$, there is nothing to do; indeed, we let $q(x) = r(x) = 0$. Therefore, assume that $f(x)$ is not the zero polynomial. We proceed by strong induction on $\deg(f(x))$. Suppose that $\deg(f(x)) = 0$. If $\deg(g(x)) > 0$, then use $q(x) = 0$ and $r(x) = f(x)$. On the other hand, if $\deg(g(x)) = 0$, then $g(x) = b$ is a nonzero constant in F. As F is a field, we have $b^{-1} \in F$, and we can use $q(x) = b^{-1}f(x)$ and $r(x) = 0$.

Thus, suppose that $\deg(f(x)) = n > 0$ and that our result holds for polynomials of smaller degree. Let us write $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Also suppose that $\deg(g(x)) = m$, and write $g(x) = b_0 + b_1x + \cdots + b_mx^m$. If $n < m$, then we can use $q(x) = 0$ and $r(x) = f(x)$. Otherwise, notice that in $f(x) - g(x)b_m^{-1}a_nx^{n-m}$, no term of degree greater than n appears, and the coefficient of x^n is $a_n - b_mb_m^{-1}a_n = 0$; thus, either $f(x) - g(x)b_m^{-1}a_nx^{n-m}$ is the zero polynomial, or it has degree strictly smaller than $f(x)$. By our inductive hypothesis, there exist $q(x), r(x) \in F[x]$ such that $f(x) - g(x)b_m^{-1}a_nx^{n-m} = g(x)q(x) + r(x)$, with $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. But then $f(x) = g(x)(q(x) + b_m^{-1}a_nx^{n-m}) + r(x)$, as required.

Now for uniqueness. Suppose that $f(x) = g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x)$, with $q(x), q_1(x), r(x), r_1(x) \in F[x]$ and each of $r(x)$ and $r_1(x)$ either is 0 or has degree smaller than that of $g(x)$. Then $g(x)(q(x) - q_1(x)) = r_1(x) - r(x)$. Suppose that $q(x) \neq q_1(x)$. By Theorem 10.2, $\deg(g(x)(q(x) - q_1(x))) \geq \deg(g(x))$, but $r_1(x) - r(x)$ cannot possibly have a degree that large. Thus, $q(x) = q_1(x)$ and hence $r(x) = r_1(x)$. □

The proof also shows us how to construct $q(x)$ and $r(x)$. We look only at the leading terms of $f(x)$ and $g(x)$ (say, respectively, a_nx^n and b_mx^m). Assuming that $n \geq m$, we subtract $b_m^{-1}a_nx^{n-m}g(x)$ from $f(x)$ and obtain either the zero polynomial or a polynomial of degree smaller than $\deg(f(x))$. Then repeat.

Example 10.4. Let us apply the division algorithm in $\mathbb{Q}[x]$ with $f(x) = 8x^4 - 4x^3 + 2x^2 + x + 1$ and $g(x) = 2x^2 + 3x + 7$. We take $2^{-1} \cdot 8x^{4-2} = 4x^2$, multiply by $g(x)$ and subtract from $f(x)$.

$$
\begin{array}{rrrrrr}
 & & & 4x^2 & & \\
\cline{2-6}
2x^2+3x+7\big) & 8x^4 & -4x^3 & +2x^2 & +x & +1 \\
 & -8x^4 & -12x^3 & -28x^2 & & \\
\cline{2-4}
 & & -16x^3 & -26x^2 & +x &
\end{array}
$$

Next, take $2^{-1}(-16)x^{3-2} = -8x$, multiply by $g(x)$ and subtract.

$$
\begin{array}{rrrrrr}
 & & & 4x^2 & -8x & \\ \cline{2-6}
2x^2+3x+7\big) & 8x^4 & -4x^3 & +2x^2 & +x & +1 \\
 & -8x^4 & -12x^3 & -28x^2 & & \\ \cline{2-4}
 & & -16x^3 & -26x^2 & +x & \\
 & & 16x^3 & +24x^2 & +56x & \\ \cline{3-5}
 & & & -2x^2 & +57x & +1
\end{array}
$$

Finally, take $2^{-1}(-2)x^{2-2} = -1$, multiply by $g(x)$ and subtract.

$$
\begin{array}{rrrrrr}
 & & & 4x^2 & -8x & -1 \\ \cline{2-6}
2x^2+3x+7\big) & 8x^4 & -4x^3 & +2x^2 & +x & +1 \\
 & -8x^4 & -12x^3 & -28x^2 & & \\ \cline{2-4}
 & & -16x^3 & -26x^2 & +x & \\
 & & 16x^3 & +24x^2 & +56x & \\ \cline{3-5}
 & & & -2x^2 & +57x & +1 \\
 & & & 2x^2 & +3x & +7 \\ \cline{4-6}
 & & & & 60x & +8
\end{array}
$$

We now have a remainder with degree smaller than $\deg(g(x))$, so we are done. Indeed, $f(x) = g(x)(4x^2 - 8x - 1) + (60x + 8)$.

Note that it is not sufficient to work in $R[x]$, where R is an integral domain. By Corollary 10.2, $R[x]$ is also an integral domain, but we cannot implement the division algorithm if we are unable to take the inverse of the leading coefficient of $g(x)$. Indeed, if we worked in $\mathbb{Z}[x]$, we would be immediately stymied if we tried to perform the division algorithm using $f(x) = 2x^2 + 3x + 5$ and $g(x) = 3x + 7$.

In fact, a polynomial ring over a field is a nice example of a special type of integral domain that we can now discuss.

Exercises

10.1. In $\mathbb{Z}_{11}[x]$, let $f(x) = 2x^3 + 4x^2 + 2x + 5$ and $g(x) = 2x^4 + 5x^3 + 7x + 1$. Find $f(x) - g(x)$ and $f(x)g(x)$.

10.2. Let $f(x) = 3x^5 + x^4 + x^3 + 3x^2 + 2x + 4$ and $g(x) = 2x^3 + 3x^2 + x + 1$ be polynomials in $\mathbb{Z}_5[x]$. Find $q(x), r(x) \in \mathbb{Z}_5[x]$, with $\deg(r(x)) < 3$, such that $f(x) = g(x)q(x) + r(x)$.

10.3. Let $f(x) = 3x^5 + 6x^4 + x^3 + 3x^2 + 2x + 4$ and $g(x) = 2x^3 + 3x^2 + x + 1$ be polynomials in $\mathbb{Z}_7[x]$. Find $q(x), r(x) \in \mathbb{Z}_7[x]$, with $\deg(r(x)) < 3$, such that $f(x) = g(x)q(x) + r(x)$.

10.4. Let R be an integral domain. Show that the units of $R[x]$ are precisely the constant polynomials a, where $a \in U(R)$.

10.5. If F is a field, is $F[x]$ a field?

10.6. Show that $2x + 1$ is a unit in $\mathbb{Z}_4[x]$. Then, for any prime p, find a unit in $\mathbb{Z}_{p^2}[x]$ that is not a constant polynomial.

10.7. For any ring R, show that R and $R[x]$ have the same characteristic.

10.8. If R and S are isomorphic rings, show that $R[x]$ and $S[x]$ are also isomorphic.

10.9. Let S be a subring of R. Show that $S[x]$ is a subring of $R[x]$. In particular, if S is an ideal of R, show that $S[x]$ is an ideal of $R[x]$.

10.10. Let R be a commutative ring with identity and P a prime ideal of R. Show that $P[x]$ is a prime ideal of $R[x]$.

10.2 Euclidean Domains

A Euclidean domain is an integral domain having an additional property.

Definition 10.3. Let R be an integral domain. Then a **Euclidean function** is a function ε from the set of nonzero elements of R to the nonnegative integers such that, for all nonzero $a, b \in R$, we have

1. $\varepsilon(a) \leq \varepsilon(ab)$; and
2. there exist $q, r \in R$ such that $a = bq + r$, and either $r = 0$ or $\varepsilon(r) < \varepsilon(b)$.

Definition 10.4. A **Euclidean domain** is an integral domain having a Euclidean function.

We have already seen several examples of Euclidean domains.

Example 10.5. The integers form a Euclidean domain. We already know that $\mathbb{Z}$ is an integral domain. Define $\varepsilon(a) = |a|$. If a and b are nonzero integers, then $|ab| = |a||b| \geq |a|$. Furthermore, by the division algorithm, there exist $q, r \in \mathbb{Z}$ such that $a = |b|q + r$, with $0 \leq r < |b|$. If $b > 0$, we are done. Otherwise, simply note that $a = b(-q) + r$.

Example 10.6. Any field is a Euclidean domain. See Exercise 10.12.

Example 10.7. If F is a field, then $F[x]$ is a Euclidean domain. Indeed, Corollary 10.2 tells us that it is an integral domain. For any $0 \neq f(x) \in F[x]$, let $\varepsilon(f(x)) = \deg(f(x))$. If $0 \neq g(x) \in F[x]$, then by Theorem 10.2, $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)) \geq \deg(f(x))$. The division algorithm for polynomials completes the proof.

Let us construct a new Euclidean domain.

Example 10.8. Let $R = \{a + bi : a, b \in \mathbb{Z}\}$. We call this the ring of **Gaussian integers**. By Exercises 8.17 and 8.27, R is a subring of $F = \{a + bi : a, b \in \mathbb{Q}\}$ which, in turn, is a subfield of $\mathbb{C}$. We claim that R is a Euclidean domain. It is surely an integral domain, since it is a unital subring of a field and therefore has no zero divisors. It remains to construct a Euclidean function.

Define $\varepsilon : F \to \mathbb{Q}$ via $\varepsilon(a + bi) = a^2 + b^2$. In particular, if $0 \neq a + bi \in R$, then $\varepsilon(a + bi) \in \mathbb{N}$. If $a, b, c, d \in \mathbb{Q}$, then

$$\begin{aligned} \varepsilon((a+bi)(c+di)) &= \varepsilon((ac-bd)+(ad+bc)i) \\ &= (ac-bd)^2 + (ad+bc)^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= (a^2+b^2)(c^2+d^2) \\ &= \varepsilon(a+bi)\varepsilon(c+di). \end{aligned}$$

In particular, if $a + bi$ and $c + di$ are nonzero elements of R, then

$$\varepsilon(a+bi) \leq \varepsilon((a+bi)(c+di)).$$

Take any nonzero $u, v \in R$. Then as F is a field, $uv^{-1} \in F$. Let us write $uv^{-1} = s + ti$, with $s, t \in \mathbb{Q}$. Choose integers m and n such that $|s - m| \leq \frac{1}{2}$ and $|t - n| \leq \frac{1}{2}$. Then

$$\begin{aligned} u - v(m+ni) &= u - v((s+ti) + ((m-s)+(n-t)i)) \\ &= u - v(uv^{-1}) + v((s-m)+(t-n)i) \\ &= v((s-m)+(t-n)i). \end{aligned}$$

Now,

$$\varepsilon((s-m)+(t-n)i) = (s-m)^2 + (t-n)^2 \leq \frac{1}{2}.$$

Therefore,

$$\varepsilon(u - v(m+n)i) = \varepsilon(v)\varepsilon((s-m)+(t-n)i) < \varepsilon(v).$$

Letting $q = m + ni$ and $r = u - v(m + ni)$, we have $u = vq + r$ and we are done.

What is so special about Euclidean domains? Let us begin with some definitions.

Definition 10.5. Let R be a commutative ring with identity. If $a, b \in R$, then we say that a **divides** b, and write $a|b$, if there exists a $c \in R$ such that $b = ac$.

Of course, this agrees with our definition of divisibility in $\mathbb{Z}$. We are very much interested in extending the notion of a greatest common divisor as well. For an arbitrary ring, this is problematic, as there is no particular notion of ordering. But for a Euclidean domain, we have ε!

Definition 10.6. Let R be a Euclidean domain, and let $a, b \in R$, not both zero. Then a nonzero element d of R is said to be a **greatest common divisor** (or **gcd**) if

1. $d|a$ and $d|b$; and
2. whenever c is an element of R satisfying $c|a$ and $c|b$, we have $\varepsilon(c) \leq \varepsilon(d)$.

Certainly a gcd must exist. Indeed, 1 is a common divisor of any two elements, so the set of common divisors is not empty. Furthermore, by definition of a Euclidean function, if $c|a$ and $a \neq 0$, then $\varepsilon(c) \leq \varepsilon(a)$. Thus, there is an upper bound on the ε values of the common divisors, so we can select one having the largest possible value.

Notice that we called d "a gcd", not "the gcd". Indeed, this definition does not produce a unique gcd. In particular, in $\mathbb{Z}$, we see that both 5 and -5 would meet the description of "a gcd" of 10 and 35. However, when we say "the gcd", we will still mean the positive one; that is, $(10, 35) = 5$, not -5.

Similarly, if F is a field, suppose that $d(x)$ is a gcd of $f(x)$ and $g(x)$. If u is a nonzero element of F, we see immediately that $ud(x)$ also divides both $f(x)$ and $g(x)$, and that $\deg(ud(x)) = \deg(d(x))$. Thus, $ud(x)$ is also a gcd. But again, we can choose a specific gcd here.

Definition 10.7. Let F be a field and let $f(x)$ and $g(x)$ be polynomials in $F[x]$, not both the zero polynomial. By **the gcd** of $f(x)$ and $g(x)$ we mean a monic gcd. When we write $(f(x), g(x))$, we mean specifically this monic gcd.

For more general Euclidean domains, we cannot easily single out a particular gcd in this manner. But we will see that, in fact, the gcds are all related to each other in a nice way. While proving this, we can produce some other interesting results. For instance, the Euclidean domain is so named because there is a Euclidean algorithm just like in $\mathbb{Z}$.

Theorem 10.4 (Euclidean Algorithm for Euclidean Domains). *Let R be a Euclidean domain. Take $a, b \in R$ with $b \neq 0$. If $b|a$, then b is a gcd of a and b. Otherwise, apply the division algorithm repeatedly. To wit, write*

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{k-2} &= r_{k-1}q_k + r_k \\ r_{k-1} &= r_kq_{k+1} + 0, \end{aligned}$$

where all $q_i, r_i \in R$ and $r_i \neq 0$, with $\varepsilon(r_1) < \varepsilon(b)$ and $\varepsilon(r_j) < \varepsilon(r_{j-1})$ for all $j \geq 2$. Then r_k is a gcd of a and b.

Proof. If $b|a$, then b is a common divisor of a and b. Also, if $c|b$, then $\varepsilon(c) \leq \varepsilon(b)$, and so b is a gcd. Assume that b does not divide a, and we perform the division algorithm repeatedly, as indicated.

Note, first of all, that this process must end, as the $\varepsilon(r_i)$ are strictly decreasing integers and cannot be negative. Suppose that $c|a$ and $c|b$, say $a = ca_1$ and $b = ca_2$, with $a_i \in R$. Then $r_1 = c(a_1 - a_2q_1)$, and hence $c|r_1$. Similarly, any common divisor of b and r_1 must also divide a. Thus, the set of common divisors of a and b is precisely the same as the set of common divisors of b and r_1. In particular, they have the same set of gcds.

By the same argument, the gcds of b and r_1 are the same as those of r_1 and r_2. We then repeat this and find that the gcds of a and b are the same as the gcds of r_k and 0. But as everything divides 0, we are looking only for the largest value of ε among the divisors of r_k. However, as if $u|v$ and $v \neq 0$, then $\varepsilon(u) \leq \varepsilon(v)$, we see that r_k is a gcd of r_k and 0, as required. □

Corollary 10.3. *Let R be a Euclidean domain. Take $a, b \in R$ with $b \neq 0$. Let d be the gcd of a and b found in the preceding theorem. Then there exist $u, v \in R$ such that $d = au + bv$.*

Proof. If $b|a$, then $d = b = a(0) + b(1)$. Assume otherwise. We have $d = r_k = r_{k-2} + r_{k-1}(-q_k)$, a multiple of r_{k-2} plus a multiple of r_{k-1}. But the preceding equation is $r_{k-3} = r_{k-2}q_{k-1} + r_{k-1}$. Thus,

$$d = r_{k-2} + (r_{k-3} + r_{k-2}(-q_{k-1}))(-q_k).$$

We have written d as a multiple of r_{k-3} plus a multiple of r_{k-2}. Now move backwards through the equations, and we will eventually write d as a multiple of a plus a multiple of b. □

Example 10.9. Let us apply the Euclidean algorithm and its corollary in $\mathbb{Z}_7[x]$, starting with $f(x) = 2x^3 + 4x^2 + x + 1$ and $g(x) = 6x^3 + 4x^2 + 4x + 5$. We write

$$\begin{aligned} 2x^3 + 4x^2 + x + 1 &= (6x^3 + 4x^2 + 4x + 5)(5) + (5x^2 + 2x + 4) \\ 6x^3 + 4x^2 + 4x + 5 &= (5x^2 + 2x + 4)(4x + 2) + (5x + 4) \\ 5x^2 + 2x + 4 &= (5x + 4)(x + 1) + 0. \end{aligned}$$

Thus, $5x + 4$ is a gcd of $f(x)$ and $g(x)$. Now let us apply the method discussed in the proof of the preceding corollary. We have

$$\begin{aligned} 5x + 4 &= g(x) - (5x^2 + 2x + 4)(4x + 2) \\ &= g(x) - (f(x) - g(x)(5))(4x + 2) \\ &= f(x)(3x + 5) + g(x)(6x + 4). \end{aligned}$$

If we want to use $(f(x), g(x))$, we must make it monic. Now, $5^{-1} = 3$, and therefore $(f(x), g(x)) = 3(5x + 4) = x + 5$. Then we get

$$x + 5 = 3(5x + 4) = f(x)(2x + 1) + g(x)(4x + 5).$$

Corollary 10.4. *Let R be a Euclidean domain, and let $a, b \in R$ with $b \neq 0$. Let d be the gcd of a and b found in Theorem 10.4. Then if $c \in R$ is a divisor of both a and b, then $c|d$.*

Proof. We have $d = au + bv$, for some $u, v \in R$. If $c|a$ and $c|b$, then $c|d$. □

Let us now discuss how the gcds of two elements of a Euclidean domain relate to each other.

Definition 10.8. Let R be a commutative ring with identity. If $a, b \in R$, then we say that a and b are **associates** if there exists a unit u of R such that $b = au$.

Note that if $b = au$, where u is a unit, then $a = bu^{-1}$. Thus, if a is an associate of b, then b is an associate of a.

Example 10.10. In $\mathbb{Z}$, the only units are 1 and -1, so the only associates of a are a and $-a$.

Example 10.11. Let F be a field. The units in $F[x]$ are the nonzero constants. (See Exercise 10.4.) Thus, the associates of $f(x)$ are of the form $af(x)$, where $0 \neq a \in F$.

Lemma 10.1. *Let R be an integral domain. Then a and b are associates in R if and only if $a|b$ and $b|a$.*

Proof. If a and b are associates, the fact that $a|b$ and $b|a$ follows from the definition. Suppose that $a|b$ and $b|a$, say $b = ar$ and $a = bs$, with $r, s \in R$. Then $a = ars$. If $a = 0$, then $b = 0$, so $a = b \cdot 1$. Otherwise, by cancellation, $rs = 1$, and hence r is a unit. □

Theorem 10.5. *Let R be a Euclidean domain. Take $a, b \in R$, not both 0. Let d be any gcd of a and b. Then $c \in R$ is a gcd of a and b if and only if c and d are associates.*

Proof. Suppose that c is a gcd of a and b. Let g be the gcd of a and b found in Theorem 10.4. By Corollary 10.4, c and d divide g. Applying the division algorithm, we have $c = gq + r$, where $q, r \in R$ and either $r = 0$ or $\varepsilon(r) < \varepsilon(g)$. Suppose the latter. Now, $c|g$, and therefore $c|r = c - gq$. But then $\varepsilon(c) \leq \varepsilon(r)$. However, if c and g are both gcds, we must have $\varepsilon(c) = \varepsilon(g)$, giving us a contradiction. Therefore, $r = 0$ and $g|c$. By the preceding lemma, g and c are associates, say $c = gu$, with u a unit in R. By the same argument, $d = gv$, where v is a unit in R. Then $c = duv^{-1}$, where uv^{-1} is a unit in R, and hence c and d are associates.

Conversely, let c and d be associates. Then since $d|a$ and $d|b$, we have $c|a$ and $c|b$ as well. Furthermore, since $c|d$ and $d|c$ we can only have $\varepsilon(c) = \varepsilon(d)$. Therefore, c is a gcd of a and b. □

We can now feel better about Definition 10.7, where we referred to "the" monic gcd of $f(x)$ and $g(x)$ in $F[x]$. As any two gcds are associates, and the only units are nonzero elements of F, there can only be one gcd that is monic.

Time to tidy up! We can strengthen Corollary 10.3. It actually applies to any gcd, not just the one found in Theorem 10.4.

Theorem 10.6. *Let R be a Euclidean domain. Take $a, b \in R$, not both 0. Let d be a gcd of a and b. Then there exist $u, v \in R$ such that $d = au + bv$.*

Proof. Without loss of generality, assume that $b \neq 0$, and calculate the gcd g of a and b from Theorem 10.4. Then by Corollary 10.3, $g = au + bv$, for some $u, v \in R$. But by Theorem 10.5, $d = gw$, for some unit w of R. Thus, $d = auw + bvw$. □

We conclude by strengthening Corollary 10.4.

Theorem 10.7. *Let R be a Euclidean domain. Take $a, b \in R$, not both 0. Then the following are equivalent for an element d of R:*

1. *d is a gcd of a and b; and*
2. *$d|a$, $d|b$, and if $c|a$ and $c|b$, then $c|d$.*

Proof. Suppose (1) holds. Without loss of generality, assume that $b \neq 0$. By definition, $d|a$ and $d|b$. Suppose that $c|a$ and $c|b$. If g is the gcd of a and b found in Theorem 10.4, then by Corollary 10.4, $c|g$. But Theorem 10.5 tells us that $g|d$. Thus, $c|d$.

Conversely, suppose that (2) holds. Then d is a common divisor of a and b. Suppose that c is another common divisor of a and b. Then by assumption, $c|d$. But this means that $\varepsilon(c) \leq \varepsilon(d)$; hence, d is a gcd. □

A nice feature of Theorem 10.7 is that it shows that gcds in a Euclidean domain do not depend upon the particular Euclidean function that is used.

Exercises

10.11. In an integral domain, if a and ab are associates, show that $a = 0$ or b is a unit.

10.12. Show that every field is a Euclidean domain.

10.13. Let R be a Euclidean domain. Let n be the smallest value of $\varepsilon(s)$, for all $0 \neq s \in R$. Show that for each $0 \neq a \in R$ we have $\varepsilon(a) = n$ if and only if a is a unit.

10.14. Find all units in the ring of Gaussian integers.

10.15. In $\mathbb{Q}[x]$, let $f(x) = 3x^4 + 7x^3 + 13x^2 + 7x + 6$ and $g(x) = 2x^4 + 7x^3 + 13x^2 + 11x + 3$. Find $(f(x), g(x))$.

10.16. In $\mathbb{Z}_5[x]$, let $f(x) = 3x^4 + 3x^3 + x + 1$ and $g(x) = 2x^3 + 4x^2 + x + 1$. Find $(f(x), g(x))$.

10.17. Taking $f(x)$ and $g(x)$ as in Exercise 10.15, find $u(x), v(x) \in \mathbb{Q}[x]$ such that $(f(x), g(x)) = f(x)u(x) + g(x)v(x)$.

10.18. Taking $f(x)$ and $g(x)$ as in Exercise 10.16, find $u(x), v(x) \in \mathbb{Z}_5[x]$ such that $(f(x), g(x)) = f(x)u(x) + g(x)v(x)$.

10.19. Find a gcd for $5 + 7i$ and $1 + 3i$ in the ring of Gaussian integers.

10.20. Let R be a Euclidean domain having the following additional property: for every $a, b \in R$ such that a, b and $a + b$ are all nonzero, $\varepsilon(a + b)$ is no bigger than the larger of $\varepsilon(a)$ and $\varepsilon(b)$. (For example, if F is a field, the degree function on $F[x]\backslash\{0\}$ has this property.) Show that in the second part of the definition of a Euclidean function, the elements q and r are uniquely determined.

10.3 Principal Ideal Domains

Let us discuss another sort of integral domain with a nice property.

Definition 10.9. A **principal ideal domain** (or **PID**) is an integral domain in which every ideal is principal.

A field F is an obvious example of a PID; indeed, its only ideals are (0) and $F = (1)$. But we can obtain others through the following theorem.

Theorem 10.8. *Every Euclidean domain is a PID.*

Proof. Let R be a Euclidean domain with Euclidean function ε, and I an ideal of R. If $I = \{0\}$, then $I = (0)$, and there is nothing to do. Assume that $I \neq \{0\}$. Among the nonzero elements of I, choose b so that $\varepsilon(b)$ is as small as possible. (Since ε takes on values that are nonnegative integers, there must be a smallest such value.) We claim that $I = (b)$. Take $a \in I$. As ε is a Euclidean function, we have $a = bq + r$, where $q, r \in R$ and either $r = 0$ or $\varepsilon(r) < \varepsilon(b)$. If $r = 0$, then $b|a$, as required. Otherwise, we note that $a, b \in I$, and since I is an ideal, $r = a - bq \in I$. But by the minimality of $\varepsilon(b)$, this is impossible. □

Example 10.12. Since $\mathbb{Z}$ is a Euclidean domain, it is a PID.

Example 10.13. Let F be a field. Since $F[x]$ is a Euclidean domain, it is a PID.

Proving that an integral domain is not a Euclidean domain can be a bit tricky; it is often simpler to show that is not a PID, from which it follows that it is not a Euclidean domain.

Example 10.14. We claim that $\mathbb{Z}[x]$ is not a PID, and hence not a Euclidean domain. To prove this, consider the set I of all $f(x) \in \mathbb{Z}[x]$ whose constant terms are divisible by 5. We saw in Exercise 9.2 that I is an ideal. But it is not principal. Indeed, suppose that $I = (f(x))$. Then as the constant polynomial 5 is in I, we see that $f(x)|5$. In view of Theorem 10.2, $f(x)$ is a constant polynomial. As it divides 5, the constant must be in $\{\pm 1, \pm 5\}$. However, $(1) = (-1) = \mathbb{Z}[x]$, whereas $(5) = (-5) = 5\mathbb{Z}[x]$, which does not include x. But $x \in I$, and therefore $5\mathbb{Z}[x] \neq I$.

We might, at this point, ask if every PID is a Euclidean domain. The answer is no, but this is not obvious. Theodore S. Motzkin showed that there is a subring of the complex numbers that is a PID but not a Euclidean domain. We will not use this fact, but the interested reader can find an accessible proof in the paper of Wilson [1].

Let us explore a couple of other properties of PIDs. The following theorem shows that a PID has the **ascending chain condition**.

Theorem 10.9. *Let R be a PID. Suppose that R has ideals I_k, $k \in \mathbb{N}$, such that $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$. Then there exists a positive integer n such that $I_k = I_n$ for all $k \geq n$.*

Proof. Let $I = \bigcup_{k=1}^{\infty} I_k$. We claim that I is an ideal. Certainly $0 \in I_1 \subseteq I$. If $a, b \in I$, then there exist positive integers k and l such that $a \in I_k$ and $b \in I_l$. Let m be the larger of k and l. Then $a, b \in I_m$, and hence $a - b \in I_m \subseteq I$. Similarly, if $a \in I$, say $a \in I_k$, and $r \in R$, then $ra \in I_k \subseteq I$. Thus, I is an ideal. As R is a PID, we must have $I = (c)$ for some $c \in I$. But then $c \in I_n$, for some positive integer n. It now follows that $I = (c) \subseteq I_n$. That is, $I = I_n$, and hence $I_k = I_n$ for all $k \geq n$. □

We are familiar with the notion of a prime positive integer. Let us extend the idea.

Definition 10.10. Let R be an integral domain. Then an element p of R is **prime** if it is not zero, not a unit, and if $p|ab$, with $a, b \in R$, then $p|a$ or $p|b$.

We observe that the definition of a prime positive integer that we introduced in Chapter 2 is different. However, Theorem 2.7 assures us that the definitions are equivalent, for positive integers. Of course, the positive integers do not form a ring, so in $\mathbb{Z}$, we see that the primes are $\pm 2, \pm 3, \pm 5, \ldots$. (Note that 1 and -1 are units, so we exclude them.)

We have an easy lemma.

Lemma 10.2. *Let R be an integral domain, and take $0 \neq p \in R$. Then p is prime if and only if (p) is a prime ideal.*

Proof. Let p be prime. If $(p) = R$, then there exists an $r \in R$ such that $rp = 1$; hence, p is a unit. But primes cannot be units, so this is impossible. If $ab \in (p)$, then $p|ab$, and hence $p|a$ or $p|b$. Thus, $a \in (p)$ or $b \in (p)$, and (p) is a prime ideal. Conversely, suppose that (p) is a prime ideal and $p|ab$. Then $ab \in (p)$, and hence $a \in (p)$ or $b \in (p)$. That is, $p|a$ or $p|b$. Furthermore, if p is a unit, then by Theorem 9.2, $(p) = R$, which contradicts the assumption that (p) is a prime ideal. Thus, p is prime. □

Definition 10.11. Let R be an integral domain, and take $p \in R$. We say that p is **irreducible** if it is not zero, not a unit, and if $p = ab$, with $a, b \in R$, then either a or b must be a unit.

This is, essentially, the definition we used for a prime positive integer. As we noted above, in the integers, these concepts are equivalent. What is the general situation?

Theorem 10.10. *Let R be an integral domain. Then every prime in R is irreducible.*

Proof. Let p be a prime, and suppose that $p = ab$, with $a, b \in R$. Then $p|ab$, so $p|a$ or $p|b$. Without loss of generality, say $p|a$. But $a|p$ as well. By Lemma 10.1, p and a are associates. Thus, by Exercise 10.11, b is a unit, as required. □

Unfortunately, the converse is not true in general.

Example 10.15. Let $R = \{a + b\sqrt{5}i : a, b \in \mathbb{Z}\}$. It is easy to check that R is a unital subring of $\mathbb{C}$, and hence an integral domain. We can define a function called a **norm** on R via $N(a + b\sqrt{5}i) = a^2 + 5b^2$. If $u, v \in R$, then $N(uv) = N(u)N(v)$. (This is the same calculation as in Example 10.8.) We claim that 3 is irreducible in R. If $3 = uv$, then $9 = N(3) = N(u)N(v)$. Noting that the norms of elements of R are nonnegative integers, we can only have $N(u) = N(v) = 3$ or, without loss of generality, $N(u) = 1$ and $N(v) = 9$. But the equation $a^2 + 5b^2 = 3$ has no solution in the integers, so $N(u) = N(v) = 3$ is impossible. Also, the only solutions to $a^2 + 5b^2 = 1$ are $a \in \{1, -1\}$ and $b = 0$. However, 1 and -1 are units in R. Also, 3 is clearly not a unit, and the claim is proved. Nevertheless, 3 is not prime. To see this, we note that $(2 + \sqrt{5}i)(2 - \sqrt{5}i) = 9$. Of course, $3|9$, but 3 does not divide $2 + \sqrt{5}i$ or $2 - \sqrt{5}i$.

The good news, however, is that in a PID, primeness and irreducibility are equivalent.

Theorem 10.11. *Let R be a PID and $p \in R$. Then p is prime if and only if p is irreducible.*

Proof. In view of Theorem 10.10, we only need to show the converse. Let p be irreducible, and let $I = (p)$. We claim that I is a maximal ideal of R. If not, suppose that J is an ideal of R with $I \subsetneq J \subsetneq R$. Since R is a PID, we have $J = (a)$, for some $a \in J$. Now, $p \in I \subseteq J$, so $p = ab$, for some $b \in R$. As p is irreducible, either a or b is a unit. If a is a unit, then by Theorem 9.2, $J = R$, which is not permitted. Therefore, b is a unit. But then $a = pb^{-1} \in I$. Thus, $J \subseteq I$, which is also not allowed. On the other hand, if $I = R$, then p is a unit, which is impossible. Our claim is proved.

By Theorem 9.22, a maximal ideal is necessarily prime. Lemma 10.2 completes the proof. □

Exercises

10.21. With R as in Example 10.15, show that $1 + 2\sqrt{5}i$ is irreducible, but not prime.

10.22. Let S be $\{a + b\sqrt{3}i : a, b \in \mathbb{Z}\}$, a subring of $\mathbb{C}$. Show that $1 + \sqrt{3}i$ is irreducible, but not prime.

10.23. Show that R and S from the preceding two exercises are not PIDs.

10.24. Let R be an integral domain. Show that an associate of an irreducible element is irreducible, and an associate of a prime element is prime.

10.25. If R is a Euclidean domain, does it follow that $R[x]$ is a Euclidean domain? Prove that it does, or give an explicit counterexample.

10.26. Let R be a PID. Show that every proper ideal of R is a subset of a maximal ideal of R.

10.27. Let R be an integral domain and p a prime in R. If $p|a_1a_2\cdots a_n$, with $a_i \in R$, show that some a_i is divisible by p.

10.28. Let R be a PID and $0 \neq a \in R$. Show that a is irreducible if and only if (a) is a maximal ideal.

10.29. Let R be an integral domain, but not a field. Show that there exist infinitely many ideals $I_1, I_2, \ldots$ of R such that I_{n+1} is a proper subset of I_n for all n.

10.30. Let R be an integral domain. If $R[x]$ is a PID, show that R is a field.

10.4 Unique Factorization Domains

We now reach our main conclusion, which is that every PID has an analogue of the Fundamental Theorem of Arithmetic.

Definition 10.12. Let R be an integral domain. We say that R is a **unique factorization domain** (or **UFD**) if

1. every nonzero, nonunit element of R can be written as a product of one or more irreducibles; and
2. the product is unique up to order and associates; that is, if $p_1p_2\cdots p_k = q_1q_2\cdots q_l$, for some irreducibles p_i and q_i, then $k = l$ and, after rearranging, each p_i is an associate of q_i.

Theorem 10.12. *Every PID is a UFD.*

Proof. Let R be a PID. We shall prove that R satisfies the first part of the definition of a UFD. Take any nonzero nonunit $a_1 \in R$, and suppose that a_1 is not a product of irreducibles. If a_1 is irreducible then we have an immediate contradiction. Therefore, we may write $a_1 = a_2 b_2$, where a_2 and b_2 are nonunits in R. If a_2 and b_2 are both products of irreducibles then again, we have a contradiction, as a_1 is then a product of irreducibles. Without loss of generality, let us say that a_2 is not a product of irreducibles. In particular, it is not irreducible, so write $a_2 = a_3 b_3$, where a_3 and b_3 are nonunits, and so forth. Then we have $a_{i+1} | a_i$ for all positive integers i. Furthermore, as b_{i+1} is not a unit, we see that a_i and a_{i+1} are not associates. By Lemma 10.1, a_i does not divide a_{i+1}. In particular, $a_i \in (a_{i+1})$, but $a_{i+1} \notin (a_i)$, so $(a_i) \subsetneq (a_{i+1})$ for all positive integers i. But this contradicts Theorem 10.9, and we see that each nonzero nonunit is a product of irreducibles.

Now let us verify the uniqueness. Suppose that $p_1 \cdots p_k = q_1 \cdots q_l$, where the p_i and q_i are irreducible, and $k \leq l$. Then $p_1 | q_1 \cdots q_l$. By Theorem 10.11, p_1 is prime. Thus, p_1 divides one of the terms in the product. After rearranging, we may assume that $p_1 | q_1$. Let us write $q_1 = p_1 u_1$, with $u_1 \in R$. As q_1 is irreducible and p_1 is not a unit, we see that u_1 is a unit, and hence p_1 and q_1 are associates. Thus, $p_1 p_2 \cdots p_k = u_1 p_1 q_2 \cdots q_l$. Cancelling, we have $p_2 \cdots p_k = u_1 q_2 \cdots q_l$. Now, $p_2 | u_1 q_2 \cdots q_l$, and since p_2 is prime, it divides a term in the product. Since a divisor of a unit is a unit, we cannot have $p_2 | u_1$, and therefore $p_2 | q_i$, for some $i \geq 2$. Rearranging, we have $p_2 | q_2$. Just as before, we see that $q_2 = p_2 u_2$, for some unit u_2. Repeating, we find that p_i and q_i are associates, $1 \leq i \leq k$. If $k = l$, we are done. Otherwise, we have $1 = u_1 \cdots u_k q_{k+1} \cdots q_l$. But nonunits cannot divide 1, so we have a contradiction. □

Our examples of UFDs will largely be PIDs.

Example 10.16. As we already knew from the Fundamental Theorem of Arithmetic, $\mathbb{Z}$ is a UFD.

Example 10.17. For any field F, $F[x]$ is a UFD.

There are also UFDs that are not PIDs. In fact, $\mathbb{Z}[x]$ is such a ring. We opt to postpone the proof of this until Section 11.2.

What sort of integral domains are not UFDs? Either of the two conditions could fail. Let us first consider one where nonzero nonunit elements are not necessarily products of irreducibles.

Example 10.18. Let R be the subset of $\mathbb{Q}[x]$ consisting of all polynomials with an integer constant term. It is easy to see that R is a unital subring of $\mathbb{Q}[x]$. As $\mathbb{Q}[x]$ is an integral domain, so is R. We claim that the only units of R are the constant polynomials 1 and -1. Indeed, a unit is necessarily a unit in $\mathbb{Q}[x]$ as well. By Exercise 10.4, our unit is a nonzero constant a. But as the constant term of an element of R must be an integer, we see that if $af(x) = 1$, then a can only be ± 1, proving the claim. In particular, x is a nonzero nonunit. If we write $x = p_1(x) \cdots p_k(x)$, a product of irreducibles, then all but one of the $p_i(x)$ (say $p_1(x)$) are integers and $p_1(x) = qx$, for some $0 \neq q \in \mathbb{Q}$. But qx is not irreducible; indeed, $qx = 2\left(\frac{q}{2}x\right)$, and neither 2 nor $\frac{q}{2}x$ is a unit. Thus, x is not a product of irreducibles, and R is not a UFD.

Even if every nonzero nonunit is a product of irreducibles, this product may not be unique.

Example 10.19. Consider the ring $R = \{a + b\sqrt{5}i : a, b \in \mathbb{Z}\}$ from Example 10.15. We noted in that example that 3 is irreducible. Applying a similar argument, we can see that $2 + \sqrt{5}i$ and $2 - \sqrt{5}i$ are irreducible. (We do have to check that they are not units, but if $uv = 1$, then $N(u)N(v) = N(1) = 1$, and as we noted in Example 10.15, this must mean that $u = v = \pm 1$.) Thus, we can write $9 = 3 \cdot 3 = (2+\sqrt{5}i)(2-\sqrt{5}i)$, giving two different products of irreducibles. As the only units are ± 1, we see that 3 is not an associate of $2 + \sqrt{5}i$ or $2 - \sqrt{5}i$. Therefore, our factorization is not unique.

We close with a few remarks concerning divisibility in a UFD.

Theorem 10.13. *Let R be a UFD, and let a and b be nonzero nonunit elements of R. Then there exist irreducibles $p_1, \ldots, p_k$, none of which are associates, such that $a = up_1^{m_1} \cdots p_k^{m_k}$ and $b = vp_1^{n_1} \cdots p_k^{n_k}$, for some units $u, v \in R$ and some nonnegative integers m_i and n_i. Furthermore, $a|b$ if and only if $m_i \leq n_i$ for all i.*

Proof. Write each of a and b as a product of irreducibles. List all of the irreducibles that appear, and if some are associates, say $q_1, q_2, \ldots$, then delete all but one. Let $p_1, \ldots, p_k$ be the irreducibles that remain. Then a can be written as a product of irreducibles, each of which is an associate of some p_i, and so can be written as a product of a unit and p_i. Gathering the units together, we obtain our expression for a, and similarly for b.

If $m_i \leq n_i$ for all i, then we see that $b = avu^{-1}p_1^{n_1-m_1} \cdots p_k^{n_k-m_k}$; hence, $a|b$. Conversely, without loss of generality, suppose that $m_1 > n_1$. If $a|b$, then write $b = ac$. As R is an integral domain, we can use cancellation, and obtain

$$p_1^{m_1-n_1} p_2^{m_2} \cdots p_k^{m_k} c = u^{-1} v p_2^{n_2} \cdots p_k^{n_k}.$$

Here, c is either a unit or a product of irreducibles. By unique factorization, p_1 must be an associate of one of $u^{-1}vp_2, p_3, \ldots, p_k$. But by our choice of the p_i, this is impossible. □

A UFD does not necessarily have anything comparable to a Euclidean function, so we cannot order elements in any logical way. However, we can obtain the equivalent form of a gcd given in Theorem 10.7.

Theorem 10.14. *Let R be a UFD. Take any nonzero nonunits $a, b \in R$, and write them in the form $a = up_1^{m_1} \cdots p_k^{m_k}$, $b = vp_1^{n_1} \cdots p_k^{n_k}$, as in Theorem 10.13. Let $d = p_1^{l_1} \cdots p_k^{l_k}$, where l_i is the smaller of m_i and n_i, for all i. Then $d|a$, $d|b$, and if $c|a$ and $c|b$, then $c|d$.*

Proof. Theorem 10.13 tells us that $d|a$ and $d|b$. Suppose that $c|a$ and $c|b$. If c is a unit, then surely $c|d$. Suppose it is not. Then write $a = cr$, with $r \in R$. Now c can be written as a product of irreducibles, and r is a unit or a product of irreducibles. By unique factorization, all of these irreducibles must be associates of the p_i. Using Theorem 10.13 again, we can write $c = wp_1^{j_1} \cdots p_k^{j_k}$, where w is a unit and $j_k \leq m_k$, for all k. By the same argument, as $c|b$, we have $j_k \leq n_k$, and hence $j_k \leq l_k$, for all k. Therefore, $c|d$. □

Exercises

10.31. Show that $1 + i$ is prime in the ring R of Gaussian integers.

10.32. In the ring of Gaussian integers, which of the numbers 3, 5 and 7 are irreducible?

10.33. Must a unital subring of a UFD be a UFD? Prove that it must, or give an explicit counterexample.

10.34. Let R be a UFD. Suppose that a and b are nonzero nonunit elements of R. If d_1 and d_2 are gcds of a and b (in the sense discussed in the second part of Theorem 10.7), show that d_1 and d_2 are associates.

10.35. Let $R = \{a+b\sqrt{6}i : a, b \in \mathbb{Z}\}$. Find $a, b, c, d \in R$ such that $10 = ab = cd$, but a, b, c and d are all irreducible and neither of $\{a, b\}$ is an associate of either of $\{c, d\}$. Conclude that R is not a UFD.

10.36. Let R be a UFD, and let p be an irreducible element of R. If a and b are nonzero nonunits of R, and $p|ab$, writing both a and b as products of irreducibles, show that p is an associate of at least one of the irreducibles appearing in at least one of these products.

10.37. Show that every irreducible in a UFD is prime.

10.38. Let R be a UFD. Suppose that there exist $a_1, a_2, \ldots \in R$ such that $(a_1) \subseteq (a_2) \subseteq \cdots$. Show that there exists an i such that $(a_i) = (a_{i+1})$.

Reference

1. Wilson, J.C.: A principal ideal ring that is not a Euclidean ring. Math. Mag. **46**, 34–38 (1973)