6.5.24. Fix a prime number p and consider the set $\mathbb{Q}_p$ of rational numbers a/b, where b is not divisible by p. (The notation $\mathbb{Q}_p$ is not standard.) Show that $\mathbb{Q}_p$ is a principal ideal domain with a unique maximal ideal M. Show that $\mathbb{Q}_p/M \cong \mathbb{Z}_p$.

6.6. Unique Factorization Domains

In the first part of this section, we discuss divisors in a unique factorization domain. We show that all unique factorization domains share some of the familiar properties of principal ideal. In particular, greatest common divisors exist, and irreducible elements are prime.

Lemma 6.6.1. *Let R be a unique factorization domain, and let $a \in R$ be a nonzero, nonunit element with irreducible factorization $a = f_1 \cdots f_n$. If b is a nonunit factor of a, then there exist a nonempty subset S of $\{1, 2, \ldots, n\}$ and a unit u such that $b = u \prod_{i \in S} f_i$.*

Proof. Write $a = bc$. If c is a unit, then $b = c^{-1}a = c^{-1}f_1 \cdots f_n$, which has the required form. If c is not a unit, consider irreducible factorizations of b and c, $b = g_1 \cdots g_\ell$ and $c = g_{\ell+1} \cdots g_m$. Then $a = g_1 \cdots g_\ell g_{\ell+1} \cdots g_m$ is an irreducible factorization of a. By uniqueness of irreducible factorization, $m = n$, and the g_i's agree with the f_i's up to order and multiplication by units. That is, there is a permutation π of $\{1, 2, \ldots, n\}$ such that each g_j is an associate of $f_{\pi(j)}$. Therefore $b = g_1 \ldots g_\ell$ is an associate of $f_{\pi(1)} \cdots f_{\pi(\ell)}$. ■

Lemma 6.6.2. *In a unique factorization domain, any finite set of nonzero elements has a greatest common divisor, which is unique up to multiplication by units.*

Proof. Let $a_1, \ldots, a_s$ be nonzero elements in a unique factorization domain R. Let $f_1, \ldots, f_N$ be a collection of pairwise nonassociate irreducible elements such that each irreducible factor of each a_i is an associate of some f_j. Thus each a_i has a unique expression of the form $a_i = u_i \prod_j f_j^{n_j(a_i)}$, where u_i is a unit. For each j, let $m(j) = \min_i\{n_j(a_i)\}$. Put $d = \prod_j f_j^{m(j)}$. I claim that d is a greatest common divisor of $\{a_1, \ldots, a_s\}$. Clearly, d is a common divisor of $\{a_1, \ldots, a_s\}$. Let e be a common divisor of $\{a_1, \ldots, a_s\}$. According to Lemma 6.6.1, e has the form $e = u \prod_j f_j^{k(j)}$, where u is a unit

and $k(j) \leq n_j(a_i)$ for all i and j. Hence for each j, $k(j) \leq m(j)$. Consequently, e divides d. ■

We say that $a_1, \ldots, a_s$ are *relatively prime* if 1 is a greatest common divisor of $\{a_1, \ldots, a_s\}$, that is, if $a_1, \ldots, a_s$ have no common irreducible factors.

Remark 6.6.3. In a principal ideal domain R, a greatest common divisor of two elements a and b is always an element of the ideal $aR + bR$. But in an arbitrary unique factorization domain R, a greatest common divisor of two elements a and b is not necessarily contained in the ideal $aR + bR$. For example, we will show below that $\mathbb{Z}[x]$ is a UFD. In $\mathbb{Z}[x]$, 1 is a greatest common divisor of 2 and x, but $1 \notin 2\mathbb{Z}[x] + x\mathbb{Z}[x]$.

Lemma 6.6.4. *In a unique factorization domain, every irreducible is prime.*

Proof. Suppose an irreducible p in the unique factorization R divides a product ab. If b is a unit, then p divides a. So we can assume that neither a nor b is a unit.

If $g_1 \cdots g_\ell$ and $h_1 \cdots h_m$ are irreducible factorizations of a and b, respectively, then $g_1 \cdots g_\ell h_1 \cdots h_m$ is an irreducible factorization of ab. Since p is an irreducible factor of ab, by Lemma 6.6.1 p is an associate of one of the g_i's or of one of the h_j's. Thus p divides a or b. ■

Corollary 6.6.5. *Let R be a unique factorization domain domain. Consider the following properties of an nonzero, nonunit element p of R:*

- *pR is a maximal ideal.*
- *pR is a prime ideal.*
- *p is prime.*
- *p is irreducible.*

The following implications hold:

$$pR \text{ maximal} \implies pR \text{ prime} \iff p \text{ prime} \iff p \text{ irreducible}$$

Proof. This follows from Lemma 6.5.18 and Lemma 6.6.4 ■

Example 6.6.6. In an UFD, if p is irreducible, pR need not be maximal. We will show below that $\mathbb{Z}[x]$ is a UFD. The ideal $x\mathbb{Z}[x]$ in $\mathbb{Z}[x]$ is prime but not maximal, since $\mathbb{Z}[x]/x\mathbb{Z}[x] \cong \mathbb{Z}$ is an integral domain, but not a field.

Polynomial rings over UFD's

The main result of this section is the following theorem:

Theorem 6.6.7. *If R is a unique factorization domain, then $R[x]$ is a unique factorization domain.*

It follows from this result and induction on the number of variables that polynomial rings $K[x_1, \cdots, x_n]$ over a field K have unique factorization; see Exercise 6.6.2. Likewise, $\mathbb{Z}[x_1, \cdots, x_n]$ is a unique factorization domain, since $\mathbb{Z}$ is a UFD.

Let R be a unique factorization domain and let F denote the field of fractions of R. The key to showing that $R[x]$ is a unique factorization domain is to compare factorizations in $R[x]$ with factorizations in the Euclidean domain $F[x]$.

Call an element of $R[x]$ *primitive* if its coefficients are relatively prime. Any element $g(x) \in R[x]$ can be written as

$$g(x) = dg_1(x), \tag{6.6.1}$$

where $d \in R$ and $g_1(x)$ is primitive. Moreover, this decomposition is unique up to units of R. In fact, let d be a greatest common divisor of the (nonzero) coefficients of g, and let $g_1(x) = (1/d)g(x)$. Then $g_1(x)$ is primitive and $g(x) = dg_1(x)$. Conversely, if $g(x) = dg_1(x)$, where $d \in R$ and $g_1(x)$ is primitive, then d is a greatest common divisor of the coefficients of $g(x)$, by Exercise 6.6.1. Since the greatest common divisor is unique up to units in R, it follows that the decomposition is also unique up to units in R.

We can extend this discussion to elements of $F[x]$ as follows. Any element $\varphi(x) \in F[x]$ can be written as $\varphi(x) = (1/b)g(x)$, where b is a nonzero element of R and $g(x) \in R[x]$. For example, just take b to be the product of the denominators of the coefficients of $\varphi(x)$. Factoring $g(x)$ as above gives

$$\varphi(x) = (d/b)f(x), \tag{6.6.2}$$

where $f(x)$ is primitive in $R[x]$. This decomposition is unique up to units in R. In fact, if

$$(d_1/b_1)f_1(x) = (d_2/b_2)f_2(x),$$

where f_1 and f_2 are primitive in $R[x]$, then $d_1b_2f_1(x) = d_2b_1f_2(x)$. By the uniqueness of the decomposition 6.6.1 for $R[x]$, there exists a unit u in R such that $d_1b_2 = ud_2b_1$. Thus $d_1/b_1 = ud_2/b_2$.

Example 6.6.8. Take $R = \mathbb{Z}$.

$$7/10 + 14/5x + 21/20x^3 = (7/20)(2 + 8x + 3x^3),$$

where $2 + 8x + 3x^3$ is primitive in $Z[x]$.

Lemma 6.6.9. *(Gauss's lemma). Let R be a unique factorization domain with field of fractions F.*

(a) *The product of two primitive elements of $R[x]$ is primitive.*
(b) *Suppose $f(x) \in R[x]$. Then $f(x)$ has a factorization $f(x) = \varphi(x)\psi(x)$ in $F[x]$ with $\deg(\varphi), \deg(\psi) \geq 1$ if, and only if, $f(x)$ has such a factorization in $R[x]$.*

Proof. Suppose that $f(x) = \sum a_i x^i$ and $g(x) = \sum b_j x^j$ are primitive in $R[x]$. Suppose p is irreducible in R. There is a first index r such that p does not divide a_r and a first index s such that p does not divide b_s. The coefficient of x^{r+s} in $f(x)g(x)$ is $a_rb_s + \sum_{i<r} a_ib_{r+s-i} + \sum_{j<s} a_{r+s-j}b_j$. By assumption, all the summands are divisible by p, except for a_rb_s, which is not. So the coefficient of x^{r+s} in $fg(x)$ is not divisible by p. It follows that $f(x)g(x)$ is also primitive. This proves part (a).

Suppose that $f(x)$ has the factorization $f(x) = \varphi(x)\psi(x)$ in $F[x]$ with $\deg(\varphi), \deg(\psi) \geq 1$. Write $f(x) = ef_1(x)$, $\varphi(x) = (a/b)\varphi_1(x)$ and $\psi(x) = (c/d)\psi_1(x)$, where $f_1(x)$, $\varphi_1(x)$, and $\psi_1(x)$ are primitive in $R[x]$. Then $f(x) = ef_1(x) = (ac/bd)\varphi_1(x)\psi_1(x)$. By part (a), the product $\varphi_1(x)\psi_1(x)$ is primitive in $R[x]$. By the uniqueness of such decompositions, it follows that $(ac/bd) = eu$, where u is a unit in R, so $f(x)$ factors as $f(x) = ue\varphi_1(x)\psi_1(x)$ in $R[x]$. ■

Corollary 6.6.10. *If a polynomial in $\mathbb{Z}[x]$ has a proper factorization in $\mathbb{Q}[x]$, then it has a proper factorization in $\mathbb{Z}[x]$.*

Corollary 6.6.11. *The irreducible elements of $R[x]$ are of two types: irreducible elements of R, and primitive elements of $R[x]$ that are irreducible in $F[x]$. A primitive polynomial is irreducible in $R[x]$ if, and only if, it is irreducible in $F[x]$.*

Proof. Suppose that $f(x) \in R[x]$ is primitive in $R[x]$ and irreducible in $F[x]$. If $f(x) = a(x)b(x)$ in $R[x]$, then one of $a(x)$ and $b(x)$ must be a unit in $F[x]$, so of degree 0. Suppose without loss of generality that $a(x) = a_0 \in R$. Then a_0 divides all coefficients of $f(x)$, and, because $f(x)$ is primitive, a_0 is a unit in R. This shows that $f(x)$ is irreducible in $R[x]$.

Conversely, suppose that $f(x)$ is irreducible in $R[x]$ and of degree ≥ 1. Then $f(x)$ is necessarily primitive. Moreover, by Gauss's lemma, $f(x)$ has no factorization $f(x) = a(x)b(x)$ in $F[x]$ with $\deg(a(x)) \geq 1$ and $\deg(b(x)) \geq 1$, so $f(x)$ is irreducible in $F[x]$. ■

Proof of Theorem 6.6.7. Let $g(x)$ be a nonzero, nonunit element of $R[x]$. First, $g(x)$ can be written as $df(x)$, where $f(x)$ is primitive and $d \in R$; furthermore, this decomposition is unique up to units in R. The element d has a unique factorization in R, by assumption, so it remains to show that $f(x)$ has a unique factorization into irreducibles in $R[x]$. But using the factorization of $f(x)$ in $F[x]$ and Gauss's Lemma, we can write

$$f(x) = p_1(x)p_2(x)\cdots p_s(x),$$

where the $p_i(x)$ are elements of $R[x]$ that are irreducible in $F[x]$. Since $f(x)$ is primitive, it follows that $p_i(x)$ are primitive as well, and hence irreducible in $R[x]$, by Corollary 6.6.11.

The uniqueness of this factorization follows from the uniqueness of irreducible factorization in $F[x]$ together with the uniqueness of the factorization in Equation (6.6.2). In fact, suppose that

$$f(x) = p_1(x)p_2(x)\cdots p_s(x) = q_1(x)q_2(x)\cdots q_r(x),$$

where the $p_i(x)$ and $q_i(x)$ are irreducible in $R[x]$. Since $f(x)$ is primitive, each $p_i(x)$ and $q_i(x)$ is primitive, and in particular of degree ≥ 1. By Corollary 6.6.11, each $p_i(x)$ and $q_i(x)$ is irreducible in $F[x]$. By the uniqueness of the irreducible factorization in $F[x]$, after possibly renumbering the $q_i(x)$, we have $p_i(x) = c_i q_i(x)$ for each i for some $c_i \in F$. But then, by the uniqueness of the decompostion of Equation (6.6.2), each c_i is actually a unit in R. ■

A characteriziation of UFDs

We are going to characterize unique factorization domains by two properties. One property, the so–called ascending chain condition for principal ideals, implies the existence of irreducible factorizations. The other property, that irreducible elements are prime, ensures the essential uniqueness of irreducible factorizations.

Definition 6.6.12. We say that a ring R satisfies the *ascending chain condition for principal ideals* if, whenever $a_1R \subseteq a_2R \subseteq \cdots$ is an infinite increasing sequence of principal ideals, then there exists an n such that $a_mR = a_nR$ for all $m \geq n$.

Equivalently, any strictly increasing sequence of principal ideals is of finite length.

Lemma 6.6.13. *A unique factorization domain satisfies the ascending chain condition for principal ideals.*

Proof. For any nonzero, nonunit element $a \in R$, let $m(a)$ denote the number of irreducible factors appearing in any irreducible factorization of a. If b is a proper factor of a, then $m(b) < m(a)$, by Lemma 6.6.1. Now if $a_1R \underset{\neq}{\subseteq} a_2R \underset{\neq}{\subseteq} \cdots$ is a strictly increasing sequence of principal ideals, then for each i, a_{i+1} is a proper factor of a_i, and, therefore, $m(a_{i+1}) < m(a_i)$. If follows that the sequence is finite. ■

Lemma 6.6.14. *If an integral domain R satisfies the ascending chain condition for principal ideals, then every nonzero, nonunit element of R has at least one factorization by irreducibles.*

Proof. This is exactly what is shown in the proof of Lemma 6.5.17. ■

Lemma 6.6.15. *If every irreducible element in an integral domain R is prime, then an element of R can have at most one factorization by irreducibles, up to permutation of the irreducible factors, and replacing irreducible factors by associates.*

Proof. This is what was shown in the proof of Theorem 6.5.19. ■

Proposition 6.6.16. *An integral domain R is a unique factorization domain if, and only if, R has the following two properties:*

(a) *R satisfies the ascending chain condition for principal ideals.*
(b) *Every irreducible in R is prime.*

Proof. This follows from Lemma 6.6.4 and Lemmas 6.6.13 through 6.6.15. ■

Example 6.6.17. The integral domain $\mathbb{Z}[\sqrt{-5}]$ (see Example 6.5.13) satisfies the ascending chain condition for principal ideals. On the other hand, $\mathbb{Z}[\sqrt{-5}]$ has irreducible elements that are not prime. You are asked to verify these assertions in Exercise 6.6.6.

Example 6.6.18. The integral domain $R = \mathbb{Z} + x\mathbb{Q}[x]$ (see Example 6.5.14) does not satisfy the ascending chain condition for principal ideals, so it is not a UFD. However, irreducibles in R are prime. You are asked to verify these assertions in Exercise 6.6.7.

Exercises 6.6

6.6.1. Let R be a unique factorization domain.

(a) Let b and $a_0, \ldots, a_s$ be nonzero elements of R. For $d \in R$, show that bd is a greatest common divisor of $\{ba_1, ba_2, \ldots, ba_s\}$ if, and only if, d is a greatest common divisor of $\{a_1, a_2, \ldots, a_s\}$.
(b) Let $f(x) \in R[x]$ and let $f(x) = bf_1(x)$, where f_1 is primitive. Conclude that b is a greatest common divisor of the coefficients of $f(x)$.

6.6.2.

(a) Let R be a commutative ring with identity 1. Show that the polynomial rings $R[x_1, \ldots, x_{n-1}, x_n]$ and $(R[x_1, \ldots, x_{n-1}])[x_n]$ can be identified.
(b) Assuming Theorem 6.6.7, show by induction that if K is a field, then, for all n, $K[x_1, \ldots, x_{n-1}, x_n]$ is a unique factorization domain.

6.6.3. (The rational root test) Use Gauss's lemma (or the idea of its proof) to show that if a polynomial $a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ has a rational root r/s, where r and s are relatively prime, then s divides a_n and r divides a_0. In particular, if the polynomial is monic, then its only rational roots are integers.

6.6.4. Generalize the previous exercise to polynomials over a unique factorization domain.

6.6.5. Complete the details of this alternative proof of Gauss's Lemma: Let R be a UFD. For any irreducible $p \in R$, consider the quotient map $\pi_p : R \longrightarrow R/pR$, and extend this to a homomorphism $\pi_p : R[x] \longrightarrow (R/pR)[x]$, defined by $\pi_p(\sum a_i x^i) = \sum_i \pi_p(a_i)x^i$, using Corollary 6.2.8.

(a) Show that a polynomial $h(x)$ is in the kernel of π_p if, and only if, p is a common divisor of the coefficients of $h(x)$.
(b) Show that $f(x) \in R[x]$ is primitive if, and only if, for all irreducible p, $\pi_p(f(x)) \neq 0$.
(c) Show that $(R/pR)[x]$ is integral domain for all irreducible p.
(d) Conclude that if $f(x)$ and $g(x)$ are primitive in $R[x]$, then $f(x)g(x)$ is primitive as well.

6.6.6. Show that $\mathbb{Z}[\sqrt{-5}]$ satisfies the ascending chain condition for principal ideals but has irreducible elements that are not prime.

6.6.7. Show that $R = \mathbb{Z} + x\mathbb{Q}[x]$ does not satisfy the ascending chain condition for principal ideals. Show that irreducibles in R are prime.

6.7. Noetherian Rings

This section can be skipped without loss of continuity.

The rings $\mathbb{Z}[x]$ and $K[x, y, z]$ are not principal ideal domains. However, we shall prove that they have the weaker property that every ideal is finitely generated—that is, for every ideal I there is a finite set S such that I is the ideal generated by S.

A condition equivalent to the finite generation property is the *ascending chain condition for ideals*.

Definition 6.7.1. A ring (not necessarily commutative, not necessarily with identity) satisfies the *ascending chain condition (ACC) for ideals* if every strictly increasing sequence of ideals has finite length.

We denote the ideal generated by a subset S of a ring R by (S).