11 Unique Factorization Extends to a Polynomial Ring

Let R be a unique factorization domain. The goal of this section is to show that $R[x]$ is also a unique factorization domain. We will make use of unique factorization in $K[x]$ where K is the field of quotients of R.

Recall that for $\mathbb{Z}$ and for $k[x]$, with k a field, a key step in proving unique factorization was to show the equivalence between irreducibility and primality. Let us extend the definition of these concepts to an arbitrary ring.

Definition 11.1. Let R be an integral domain. We say that a **divides** b, written $a|b$, when there is some c such that $ac = b$. An element p in R is **prime** when $p|ab$ implies that either $p|a$ or $p|b$. An element p is **irreducible** when $p = ab$ implies that either a or b is a unit in R.

Observe that p is a prime if and only if $\langle p \rangle$ is a prime ideal.

Some comments on *uniqueness* of factorization

In $\mathbb{Z}$, the unique factorization of an integer is $up_1^{e_1} \cdots p_r^{e_r}$ in which the p_i are distinct *positive* primes, the e_i are positive integers, and u is 1 or -1. In $k[x]$ we stated the unique factorization to be $u(p_1(x))^{e_1} \cdots (p_r(x))^{e_r}$ in which the $p_i(x)$ are distinct *monic* polynomials, the e_i are positive integers, and u is a nonzero constant (an element of k). In each case the uniqueness is up to reordering of the prime power factors, but we did not need to worry about $(2x-2)((1/2x)$ and $(x-1)x$ both being valid factorizations into irreducibles of x^2-x. We chose the monic polynomial once and for all as the one to use in a standard factorization.

Definition 11.2. Let R be an integral domain. Two elements of R are **associates** if they differ by a factor that is a unit. That is, if $r_1, r_2 \in R$ we say r_1 and r_2 are associates when there is a unit $u \in R$ such that $r_2 = ur_1$.

It should be clear that the relation of being associates is an equivalence relation. Additionally, if p is irreducible in R then so are all associates of p.

Henceforth, for our unique factorization domain R we will assume that for each equivalence class of irreducibles (under the relation of being associates) we have chosen a unique representative that will be used in the standard factorization. Unique factorization may then be stated as follows. Let Irr be a set of representatives for the irreducibles, containing one element from each equivalence class of irreducible polynomials (under the relation of being associates).

> Each element of R may be written in a unique way as $u \prod_{p \in \text{Irr}} p^{e_p}$. In which u is a unit, each $e_p \in \mathbb{N}_0$, and only a finite number of the e_p are nonzero.

The gcd of two elements $a, b \in R$ is now uniquely defined. Factor each of a, b into irreducibles and for each irreducible p take the minimum power that divides both a and b. Multiply over all irreducibles to get the gcd. Explicitly, if $a = u\prod_{p\in \text{Irr}} p^{d_p}$ and $b = v\prod_{p\in \text{Irr}} p^{e_p}$, then $\gcd(a,b) = \prod_{p\in \text{Irr}} p^{\min(d_p,e_p)}$. Similarly, $\text{lcm}(a,b) = \prod_{p\in \text{Irr}} p^{\max(d_p,e_p)}$.

The field K is a unique factorization domain only in the most trivial sense; since all nonzero elements are all units, there are no irreducibles. On the other hand, K inherits a meaningful unique factorization because it was constructed from R. An element of K can be written a/b with $a, b \in R$. We may express this "in lowest terms" by factoring a and b and dividing each by their gcd. Thus, using the factorizations in the previous paragraph, we let $P = \{p \in \text{Irr} : d_p > e_p\}$ and $Q = \{p \in \text{Irr} : d_p < e_p\}$, and then

$$\begin{aligned}\frac{a}{b} &= \frac{a/\gcd(a,b)}{b/\gcd(a,b)} \\ &= (uv^{-1})\frac{\prod_{p\in P} p^{d_p-e_p}}{\prod_{p\in Q} p^{e_p-d_p}}\end{aligned}$$

This is in lowest terms—the numerator and denominator have no common irreducible factor—and it is the unique expression of $\frac{a}{b}$ in this form.

Proposition 11.3. *Any element of K can be uniquely expressed in the form $u\frac{a}{b}$ in which u is a unit, a and b are the product of elements of* Irr*, and a and b are coprime.*

Proving $R[x]$ is a UFD

As we said earlier the key step in proving unique factorization is to show the equivalence between irreducibility and primality.

The first step, an easy one, is that one direction of the equivalence always holds.

Proposition 11.4. *In any integral domain every prime element is irreducible.*

Proof. Look at the proof for $\mathbb{Z}$ and see that it works with little alteration. □

In general rings, irreducible elements are not necessarily prime.

Example 11.5. Here is a domain in which an irreducible element may not be prime. Consider $\mathbb{Z}[\sqrt{-5}]$. One can check that 2,3, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ are all irreducible. One can also verify that the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1, so no two of these irreducibles are associates. Here are two distinct factorizations into irreducibles that are equal

$$\left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right) = 6 = 2\cdot 3$$

The key element in establishing unique factorization is thus to show that when an element of $R[x]$ is irreducible it is also prime. To get started we will use a coarse factorization for elements of $K[x]$.

Definition 11.6. Let $f(x) \in K[x]$ have positive degree and write its coefficients in lowest terms

$$f(x) = u_n \frac{a_n}{b_n} x^n + u_{n-1} \frac{a_{n-1}}{b_{n-1}} x^{n-1} + \cdots + u_1 \frac{a_1}{b_1} x + u_0 \frac{a_0}{b_0}$$

Here each u_i is a unit, a_i and b_i are products of elements of Irr and have no common irreducible factor. Let $A = \gcd(a_1, a_2, \ldots, a_n)$ and let $B = \operatorname{lcm}(b_1, b_2, \ldots, b_n)$. The *unit part* of $f(x)$ is $u_f = u_n$, the **content** of $f(x)$ is $c_f = A/B$, and the **primitive part** of $f(x)$ is $f^*(x) = u_f^{-1}(B/A)f(x)$. Clearly we have $f(x) = u_f c_f f^*(x)$.

We say $f(x) \in K[x]$ is **primitive** when it has positive degree, and $u_f = c_f = 1$. In particular the leading coefficient of f is a product of elements of Irr.

Since the gcd and lcm of a polynomial are uniquely defined—because Irr has a unique representative for each associate class of irreducibles—the factorization of $f(x) \in K[x]$ into the product of its unit part, its content and its primitive part is unique. Note also that a primitive polynomial is actually in $R[x]$ since the lcm of the denominators is 1.

Proposition 11.7. *Let $f(x)$ have positive degree, with content c_f and primitive part $f^*(x)$. Then $f^*(x)$ is a primitive polynomial. That is,*

(1) $f^* \in R[x]$,

(2) $c_f = 1$, *and*

(3) $u_f = 1$.

Proof. (1) Let $f(x)$ be written as follows with each $\frac{a_i}{b_i}$ in lowest terms and define A and B.

$$\begin{aligned} f(x) &= u_n \frac{a_n}{b_n} x^n + u_{n-1} \frac{a_{n-1}}{b_{n-1}} x^{n-1} + \cdots + u_1 \frac{a_1}{b_1} x + u_0 \frac{a_0}{b_0} \\ A &= \gcd(a_1, a_2, \ldots, a_n) \\ B &= \operatorname{lcm}(b_1, b_2, \ldots, b_n) \end{aligned}$$

Then

$$f^*(x) = \frac{a_n}{A} \frac{B}{b_n} x^n + (u_n^{-1} u_{n-1}) \frac{a_{n-1}}{A} \frac{B}{b_{n-1}} x^{n-1} + \cdots + (u_n^{-1} u_1) \frac{a_1}{A} \frac{B}{b_1} x + (u_n^{-1} u_0) \frac{a_0}{A} \frac{B}{b_0}$$

Each $\frac{a_i}{A}$ and each $\frac{B}{B_i}$ is an element of R by the choice of A and B, so $f^*(x) \in R[x]$.

(2) We know that $f^*(x) \in R[x]$, so the denominators of its coefficients are all 1. We will show that the gcd of its coefficients is 1 by showing that for any $p \in \text{Irr}$, p does not divide all the coefficients of $f^*(x)$.

Let $p \in \text{Irr}$ be such that $p|B$, and let p^e be the largest power of p that divides B. Then, for some i, p^e divides b_i, but p^{e+1} does not divide b_i. We thus have $p \nmid (B/b_i)$. Since the coefficients of $f(x)$ were in lowest terms, we also have $p \nmid a_i$. Thus $p \nmid (a_i B/b_i)$. This shows that no irreducible that divides B divides all of the $a_i B/b_i$. Consequently, the only irreducibles that divide all of the $a_i B/b_i$ actually divide the a_i and therefore we have

$$\gcd(a_0 B/b_0, \ldots, a_n B/b_n) = \gcd(a_0, \ldots, a_n) = A$$
$$\gcd(a_0 B/Ab_0, \ldots, a_n B/Ab_n) = \gcd(a_0/A, \ldots, a_n/A) = 1$$

(3) The leading term of f^* is a product of irreducibles, since A, a_n, B, b_n are. So $u_f = 1$.

□

Lemma 11.8. *The product of two primitive polynomials is primitive. More generally, let $f(x), g(x) \in K[x]$ both have positive degree. Then $u_{fg} = u_f u_g$, $c_{fg} = c_f c_g$ and $\big(f(x)g(x)\big)^* = f^*(x)g^*(x)$.*

Proof. Suppose that $f(x)$ and $g(x)$ are both in $R[x]$ and that they are both primitive. We will show that for any $p \in \text{Irr}$ there is a coefficient of $f(x)g(x)$ that is not divisible by p. Since p is arbitrary the gcd of all the coefficients is 1.

Since $f(x)$ is primitive, we know that p does not divide all coefficients of $f(x)$. Let i be the smallest integer such that f_i is not divisible by p. Similarly, let j be the smallest integer such that g_j is not divisible by p. Then the $(i+j)$th coefficient of $f(x)g(x)$ is

$$f_0 g_{i+j} + f_1 g_{i+j-1} + \cdots + f_i g_j + \cdots + f_{i+j} g_0$$

We see that p divides every term except it does not divide $f_i g_j$. Thus p does not divide the $(i+j)$th term of $f(x)g(x)$. This was what we needed to show.

Now let $f(x), g(x) \in K[x]$ be arbitrary and $h(x) = f(x)g(x)$. Then $h(x) = u_f c_f f^*(x) u_g c_g g^*(x) = \big(u_f u_g\big)\big(c_f c_g\big)\big(f^*(x)g^*(x)\big)$. The first term is a unit in R, the second term is in K and is a product of irreducibles (or their inverses). The last term is a primitive polynomial in $R(x)$. By the uniqueness of the factorization into unit part, content, and primitive part we are done. □

Corollary 11.9. *Let $m(x) \in R[x]$ have positive degree. Then*

(1) $m(x)$ is irreducible only if it is primitive.

(2) $m(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $K[x]$.

(3) If $m(x)$ is irreducible in $R[x]$ then it is prime in $R[x]$.

Proof. We may assume that the unit part of $m(x)$ is 1.

If $m(x)$ is not primitive then $c_m m^*(x)$ is a nontrivial factorization of $m(x)$, so $m(x)$ is not irreducible.

Let $m(x) \in R[x]$ be primitive with degree $n > 0$. Any factorization of $m(x)$ in $R[x]$ would involve polynomials of degree less than n and would therefore extend to a factorization in $K[x]$. Thus if $m(x)$ is reducible in $R[x]$ then it is also reducible in $K[x]$.

Conversely, suppose that $m(x)$ is reducible in $K[x]$ with $m(x) = f(x)g(x)$ and both $f(x)$ and $g(x)$ having positive degree. Then, $c_m m^*(x) = c_f c_g f^*(x) g^*(x)$. Bust since $m(x)$ is primitive, $c_f c_g = c_m = 1$. And $m(x) = m^*(x) = f^*(x)g^*(x)$. This shows that $m(x)$ is reducible in $R[x]$.

Finally, suppose $m(x)$ is irreducible in $R[x]$ and suppose $m(x)$ divides $f(x)g(x)$ with both factors in $R[x]$. In particular, $m(x)$ and therefore both $f(x)$ and $g(x)$ are primitive. Consider this factorization in $K[x]$: from the previous item, $m(x)$ is irreducible in $K[x]$ so, it is prime in $K[x]$, so it must divide one of $f(x)$ or $g(x)$. Suppose $f(x) = m(x)h(x)$ is a factorization in $K[x]$. We have $c_f = c_m c_h$. But $c_f = c_m = 1$ since $f(x)$ and $m(x)$ are primitive. Consequently, $c_h = 1$ and $h(x) \in R[x]$. Thus we have $m(x)$ divides one factor of the product $f(x)g(x)$ *within* $R[x]$. This shows $m(x)$ is prime. □

Theorem 11.10. *If R is a unique factorization domain, so is $R[x]$.*

Proof. Existence: The proof is similar to that for $k[x]$. We use induction on the degree, starting with the factorization into irreducibles in R, which gives a base step in degree 0. Assume we have factorization into irreducibles for polynomials of degree less than n. Let $f(x) \in R[x]$ have degree n and let its content be c_f and primitive part $f^*(x)$. Since $f(x) \in R$, so is c_f and it has a factorization into irreducibles. If f^* is irreducible itself we are done. If it can be factored then, since $f(x)$ is primitive, each factor must have degree less than n. Each of the factors can be written as a product of irreducibles by the induction hypothesis; so $f^*(x)$ can also be written as the product of irreducibles.

Uniqueness: The proof is entirely analogous to that in the integers or $k[x]$. It follows from the fact that all irreducibles in $R[x]$ are prime as shown in Corollary 11.9.

□

Corollary 11.11. *Let k be a field. The polynomial ring in n variables $k[x_1, \ldots, x_n]$ is a unique factorization domain.*

Proof. Induction on n. □

Exercises 11.12. Discussion items

(a) Prove that every prime is irreducible in an integral domain.

(b) Explain why the "lowest terms" expression of an element of K is unique.

Representatives for the irreducibles in $R[x]$

We can define a set of representatives for irreducibles in $R[x]$ by building on top of Irr_R, the set of representatives for the irreducibles in R. Let $m(x)$ be irreducible in $R[x]$ of degree $n > 1$. We will choose a representative for the set of irreducibles that are associates of $m(x)$. Note that $m(x)$ must be primitive, for otherwise it will factor into its content times its primitive part and the content is either 1 or a product of irreducibles in R.

Factor m_n, the leading coefficient of $m(x)$, as $m_n = u \prod_{p \in Irr} p_p^e$ (with each e_p nonnegative, and only a finite number nonzero, and u a unit in R). We are allowing the possibility that the product is empty, in which case m_n is a unit. We take $u^{-1}m(x)$ as the representative for the associates of $m(x)$. In other words we require the leading term of an element of $\text{Irr}_{R[x]}$ to be a product of elements of Irr_R, disallowing multiplication by a unit in R.

12 Tests for Irreducibility

Let R be a unique factorization domain and let K be its field of quotients. How can we determine if a primitive polynomial $m(x) \in R[x]$ is irreducible? We introduce three tests for irreducibility, each is a straightforward generalization of tests (that you may have seen at some point) for irreducibility in $\mathbb{Q}[x]$.

Leading coefficient and constant term

Proposition 12.1. *Let $m(x) = m_n x^n + m_{n-1}x^{n-1} + \cdots + m_1 x + m_0$ be a primitive polynomial of degree n in $R[x]$. Let r, s be coprime elements of R. Then r/s is a root of $m(x)$, as an element of $K[x]$, if and only if $sx - r$ is a factor of $m(x)$ as an element of $R[x]$. This can occur only if $s|m_n$ and $r|m_0$.*

Consequently, the search for linear factors of $m(x)$ is narrowed to considering those of the form $sx - r$ for s a factor of m_n and r a factor of m_0.

Proof. Clearly if $sx - r$ is a factor of $m(x)$ in $R[x]$ then it is also a factor of $m(x)$ in $K[x]$ and consequently r/s is a root of $m(x)$.

Suppose that r/s is a root of $m(x)$ considered in $K[x]$. Then by the Roots-Factors theorem, $x - r/s$ is a factor of $m(x)$ so $m(x) = (x - r/s)g(x)$ for some $g(x) \in K[x]$. Since $m(x)$ is primitive and the content of $x - r/s$ is $1/s$ (or some associate of it), the content of $g(x)$ must be s (or the appropriate associate). Furthermore $m(x) = (sx - r)(g(x)/s)$ is a factorization of $m(x)$ in $R[x]$. Since the leading term of $m(x)$ is the product of the leading terms of the two factors, $s|m_n$. Similarly, the constant term is the product of the constant terms of the two factors, so $r|m_0$. □

This narrows the search for a linear factor of a primitive polynomial $m(x)$, but it doesn't help determine higher degree factors. For $m(x)$ of degree 2 or 3, $m(x)$ is irreducible if it has no linear factor. For $m(x)$ of degree n, $m(x)$ is irreducible if it has no factor of degree $\lfloor n/2 \rfloor$ or less. The following more general result can help with higher degree.

Proposition 12.2. *Let $m(x) = m_n x^n + m_{n-1}x^{n-1} + \cdots + m_1 x + m_0$ be a primitive polynomial of degree n in $R[x]$. Suppose $m(x)$ has a factorization in $R[x]$ as $m(x) = a(x)b(x)$. Then*

(1) $a(x)$ and $b(x)$ are primitive with degrees adding to n;

(2) the product of the leading terms of $a(x)$ and $b(x)$ is m_n;

(3) the product of the constant terms of $a(x)$ and $b(x)$ is m_0.

We know that $\mathbb{Z}$ is a UFD and that $\mathbb{Q}[x]$ is a UFD. Theorem 11.10 established that $\mathbb{Z}[x]$ is a UFD. It may be counterintuitive, but to prove that an $m(x) \in \mathbb{Q}[x]$ is irreducible, it is useful to consider its primitive part $m^*(x) \in \mathbb{Z}[x]$. Using the previous proposition is one way. The next exercises are examples. We will treat two other methods in the next subsections.

Exercises 12.3.

(a) For what integer values of u does $y^3 + uy + 2$ factor in $\mathbb{Q}[x]$?

(b) For what values of $u(x) \in \mathbb{Q}[x]$ does $y^3 + u(x)y + x$ factor in $\mathbb{Q}[x, y]$?

Exercises 12.4.

(a) For what integer values of u does $f(y) = y^4 + uy^2 + 4$ factor in $\mathbb{Q}[x]$? Consider separately the case when $f(y)$ has a root, and when it factors as a product of irreducible quadratics.

(b) For what values of $u(x) \in \mathbb{Q}[x]$ does $y^4 + u(x)y^2 + x^2$ factor in $\mathbb{Q}[x, y]$? Consider separately the case when $f(y)$ has a root in $\mathbb{Q}[x]$ and when it factors as a product of irreducible quadratics.

Exercises 12.5. Use the general theorem above to show that one of the polynomials over $\mathbb{Z}$ below is irreducible and to factor the other.

(a)

(b)

Exercises 12.6. Consider the polynomials below over $\mathbb{F}_2[x]$. Use Proposition **??** to factor one of the polynomials to show that the other is irreducible.

(a)

(b)

Reducing modulo a prime ideal

Given a ring R and ideal J in R, there is a natural homomorphism from $R[x]$ to $R/J[x]$ that simply reduces each coefficent of a polynomial modulo J: the image of $a(x) = \sum a_i x^i$ is $\bar{a}(x) = \sum \bar{a}_i x^i$ where $\bar{a}_i$ is $a_i + J$, the congruence class of a_i in R/J.

Proposition 12.7. *Let $m(x) \in R$ be a primitive polynomial of degree $n > 1$. Suppose that J is an ideal J in R such that $m_n \notin J$. Let $\bar{m}(x)$ be the element of $R/J[x]$ obtained by reducing the coefficients of m modulo J. If $\bar{m}(x)$ is irreducible then so is $m(x)$.*

Proof. We will show the logically equivalent statement: if $m(x)$ is reducible then so is $\bar{m}(x)$. Suppose $m(x)$ is reducible and $m(x) = a(x)b(x)$ is a factorization in $R[x]$ with $\deg(a(x))$ and $\deg(b(x))$ both greater than 1. Note that the leading coefficient of $m(x)$ is the product of the leading coefficients of $a(x)$ and $b(x)$. Since m_n is not in J, the leading coefficients of $a(x)$ and $b(x)$ are not in J. Thus $\deg(\bar{a}(x)) = \deg(a(x))$ and similarly $\deg(\bar{b}(x)) = \deg(b(x))$.

Reducing each coefficient modulo J we have in $R/J[x]$, $\bar{m}(x) = \bar{a}(x)\bar{b}(x)$. Since the leading coefficients of $\bar{a}(x)$ and $\bar{b}(x)$ are non zero, we have a nontrivial factorization of $\bar{m}(x)$, as was to be proved. □

Exercises 12.8.

(a) Show that $y^4 + 7y^3 + 2y^2 + 1$ is irreducible in $\mathbb{Q}[y]$.

(b) Show that $y^4 + (x^3 + 7)y^3 + x^2y^2 + x^2 + 2x + 3$ is irreducible in $\mathbb{Q}[x, y]$.

Eisenstein's criterion

Proposition 12.9 (Eisenstein)**.** *Let $m(x) \in R[x]$ be a primitive polynomial of degree $n > 1$. Suppose that there is a prime ideal P in R such that*

(1) $m_n \notin P$.

(2) $m_i \in P$ for $i = 0, \ldots, n-1$

(3) $m_0 \notin P^2$

Then $m(x)$ is irreducible.

Proof. We assume $m(x)$ satisfies the properties above and that it factors as $m(x) = a(x)b(x)$. We show that one of the factors is an invertible element of R (in particular, of degree 0). Since this is true for an arbitrary factorization, $m(x)$ is irreducible.

Since the leading coefficient of m is not in P, the leading coefficients of $a(x)$ and $b(x)$ are also not in P. The constant term of m is in P but not P^2. Since $m_0 = a_0b_0$ and P is prime, exactly one of a_0 and b_0 is in P and the other is not. Let us assume $a_0 \in P$ and $b_0 \notin P$. Let t be minimal such that $a_t \notin P$ (we know the leading coefficient of $a(x)$ is not in P, so there exists such a t). Then we have

$$m_t = a_0b_t + a_1b_{t-1} + \cdots + a_{t-1}b_1 + a_tb_0$$

Each term a_ib_{t-i} is in P except the last, which is not, so $m_t \notin P$. By our assumptions on $m(x)$, the only coefficient not in P is m_n. Thus $t = n$, $a(x)$ has degree n and $b(x)$ has degree 0. Since $m(x)$ is primitive, $b(x)$ must be a unit. □

Exercises 12.10. Use Eisenstein's criterion to show that the following are irreducible polynomials

(a) In $\mathbb{Q}[y]$, $(y^p - 1)/(y - 1)$ (hint: substitute $y = z + 1$).

(b) In $k[x, y]$, for any field k, $y^2 + x^2 - 1$ is irreducible.

(c) In $k[x, y]$, for any field k, $y^n - x^3 - x^2$ is irreducible.

Exercises 12.11. Show these are irreducible over any field.

(a) $xy^2 - z$

(b) $xy^2 - z^2$

(c) $x^2 + y^2 + z^2 - 1$ (this took me two steps)

(d) $-4x^3z + 3x^2y^2 - 4y^3 + 6xyz - z^2$, the tangent surface to the twisted cubic. (I couldn't do this.)